Hiding Information in Digital Images Using LSB Steganography Technique

https://doi.org/10.3991/ijim.v17i07.38737

Sabah Abdulazeez Jebur(✉), Abbas Khalifa Nawar, Lubna Emad Kadhim, Mothefer Majeed Jahefer
Iman Al-Kadhum College (IKC), Baghdad, Iraq
sabah.abdulazeez@alkadhum-col.edu.iq

Abstract—The highest way to protect data from intruder and unauthorized persons has become a major issue. This matter led to the development of many techniques for data security, such as Steganography, Cryptography, and Watermarking to disguise data. This paper proposes an image steganography method using the Least Significant Bits (LSB) technique and XOR operator and a secret key, through which the secret key is transformed into a one-dimensional bit stream array, then these bits are XORed with the bits of the secret image. Multiple experiments have been performed to embed color and grayscale images inside cover media. In this work, the LSB technique is ideal in two ways: firstly, only the least significant one-bit (1bit) of each byte will store the embedded data, this method is named (1-LSB). Secondly, the four least significant bits of the right half-byte (4 bits) of each byte will store the embedded data, this method is named (4-LSB). Subjective and objective analyzes were performed for each LSB process. The subjective analysis is responsible for both HVS and histogram, whereas the objective analysis involved both PSNR and MSE metrics.

Keywords—image steganography, Least Significant Bits, LSB, XOR operator

1 Introduction

Since the dawn of time, the urgent need to convey a message as safely and securely as possible has been a topic of debate. The main things about an organization's wealth are its critical information. As a result, for a company that deals with sensitive information, security matter is a major concern. Whatever approach is used for security, the most pressing doubt is the level of security. The technique of covered or hidden writing is known as steganography. The essential purpose of using steganography is to evade get attention to the sending secret data. But even so, if an observer notices any change by sending data, The process of informational concealment becomes less successful [1]. Steganography is considerably comparable with cryptography Because both cases used to protect critical data in similar ways. the recent definition of steganography refers to information or a document that has been hidden within a digital image, video, or audio file as well as network Steganography [2]. Steganography exploit of human perception; our senses aren't made to hunt for files with information concealed inside of

them[1].a superb image steganography technique includes three main parts, the first is capacity or the greatest quantity of data that must be held within the cover image, the second factor is imperceptibility which refers to the quality of the stego-picture built after data has been hidden, and the third factor is robustness which measures the ability of secret information to resist against threats [3].The most popular stenographic approach is Least Significant Bit (LSB) substitution. The core notion of LSB substitution entails embedding secret data in bits with the smallest weighting so that the value of the original pixel is unaffected [4]. Steganography methods can be classified into text, image, audio, and video steganography according on the cover media used to embed secret data [3]:

- Text Steganography can be handled by modifying the text formatting, or by changing certain characteristics of textual elements such as characters and symbols.
- Image steganography is the practice of concealing a message within an image without effecting its visible characteristics. The cover source can be changed in the pixels that have significant variations in colors, which will make the modifications less obvious.
- Audio Steganography is the technique of concealment digital data in audio files like MP3 files or WAV. In audio stenography, the perceptual features of the Human Auditory System (HAS) set to be concealed information in the audio, as a result human listening cannot recognize the differences between the original audio of a file and the Embedded secret information file.
- Video steganography adapt the original video to exclude the target object from the scene. Next, a data concealer technique is utilized to insert the original video frame into the in-painted one.
- Network steganography exploits header field and payload field of network protocols to conceal data by produce hidden channels between a secret sender and a secret receiver in order to hide data [2].

2 The main components of steganography systems

Steganography is descended from the Greek words "steganos" and "graphein," which both mean "writing" and "drawing," respectively. Steganos implies "covered," "secret," or "concealed." Data hiding in a cover material so that it is invisible to others is the basic target of steganography. When a file, message, image, or video are hidden inside of another file, message, image, or video, the hiding process is controlled by a stego-key to restrain the detection or recovery of the embedded data to parties that recognize it [5]. The following terms apply to all image steganography systems, regardless of the algorithms used to implement them (As shown in Figure 1 [6][7]:

- **Secret message:** a specific function dedicate a color vector c(x,y) to each pixel (x. y) in a message image C.
- **Cover file:** The concealed message is transmitted via the main image. A cover is commonly selected in such a way that it appears common and insignificant, and so does not draw attention.

- **Stego file:** The Stego image is the cover picture with a hidden message inside it. It's being used to reveal the concealed message at the receive site.
- **Stego Key:** Is a code that permit information to be embedded in a cover and extracted from the stego medium. It might be a number created using a pseudo-random number, or it could be anything else, to encrypt the embedding position.
- **Embedding Domain:** The cover medium features that are leveraged in embedding messages into it are referred to as the Embedding domain. It could be in the spatial domain if the cover's constituent pieces are directly transformed (for example, pixels in an image), or it could be in the frequency domain or transform domain if mathematical manipulations are performed on the medium before embedding [6-7].

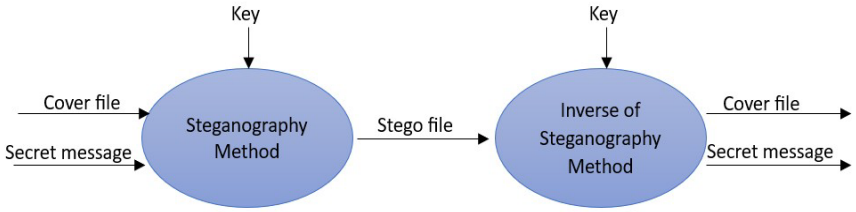

Fig. 1. Generic Steganography System

3 Least Significant Bits (LSB) technique

LSB is the most common manner of data hiding. In this case of embedding, the least significant bits of image pixels are substituted with bits of concealed data. The image received after embedding is largely homolog to the original image because the LSB of image pixel change does not create major changes in the image. LSB algorithm used in this study is spatial domain steganography in substitution, which substitutes critical information in the cover image's least bit. In a 256-grayscale cover image, every grayscale value of each pixel can be used to reform an 8-bit binary, with a specific bit of all pixels composing a specific bit [8-18]. A bit sequence is created from the secret message. Figure 2 shows an example of how the cover data separated into bit strings based on the data type. Each bit string's last bit is substituted by the secret message's following bit. It's a standard approach for working with image and audio files.

1	0	0	0	1	1	0	1	0
0	0	1	0	1	0	0	0	1
0	1	0	1	0	1	0	1	0
1	0	0	0	1	1	0	0	1

LSB

Fig. 2. Least Significant Bit of 8-Bit Binary Array

Colors are encoding by eight bits of data; red, green, and blue, they retain for each pixel in a 24bits image file. By substituting the last bit of each 8-bit data with the secret

data bit, data can be hidden in a cover file. Human senses will be unable to detect this alteration since it will be so little. Figure 3 indicate the method of putting 6-bits (000110) data in two pixels. The cover data is the one on the left side of the figure if it is expanded to two pixels. The RGB data of two pixels contains 6 bits of data, and the stego-data conversion of the cover data is presented on the right side. There is no significant change in the cover data, as seen in Figure 3 [19].

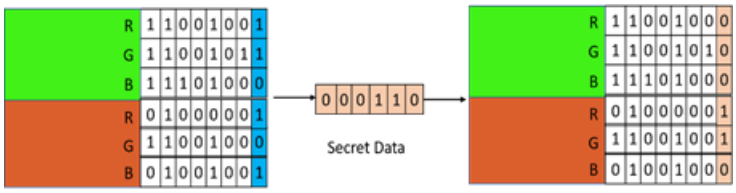

Fig. 3. Embedding Data to an image with two Pixels

4 Literature review

In order to improve steganography techniques, many methods are proposed like Zhou, Xinyi, et al. (2016) used image steganography and cryptography based on a secret key to provide more security of information hiding. on another side, identity authentication based on a digital signature is initiated to prevent the false of hidden information [20].

Sudhanshu Sharma Dipta (2016) utilized RSA with an LSB approach and discrete cosine transform (DCT) augmentation to reveal image steganography on gray and color images. RSA is used to encrypt and decrypt sensitive data while DCT is being used to improve the stego picture [21].

Anupriya Arya, and Sarita Soni (2018), proposed an enhanced LSB substitution technique for blending hidden image data information into images to produce a secret-embedded image that is completely unidentifiable from the original image by the human eye because just the final bit of each pixel of the cover image is modified. Also, they compared these techniques using images of diverse sizes and file types (.bmp,.jpg, and.png), and calculates their PSNR and MSE parameters for an analysis of their capacity to conceal information [22].

R. Thanki, S. Borra (2018) developed steganography technique on the Finite Ridgelet Transform (FRT), Discrete Wavelet Transform (DWT), and Arnold scrambling is proposed. The FRT was used to secure colored images. This method involves encrypting the secret color image via Arnold scrambling, which is then used to create the stego color image by inserting it into the color standard image [23].

E Z Astuti, D R I M Setiadi, et al. (2019) suggested the bit interchanging approach is tested on RGB-formatted image features with a message capacity of 1 bit per pixel. Because there were more layers in the color image, the imperceptibility test results exposed a more various rise. The bit-flipping technique has been demonstrated to be efficient on color images as well [24].

M. M. Hashim, A. Abdulrazzaq, et al (2019), proposed LSB image pixels based on P Even/P Odd were offered as an enhanced steganography system in the frequency domain. An encryption system with many levels and two control random parameters was presented. The secret data was initially compressed using a Huffman coding approach to augment the system's payload capacity. The technology ensures that an intruders cannot access confidential data and that its privacy is preserved [25].

S. Kaur, S. Bansal, et al, (2020), Using steganography, one can hide a hidden message in digital photographs. This study intends to protect an image's transmission from outsiders. To encrypt and decrypt images, this study developed a unique Image Hiding Encryption and Decryption (IHED) method. In addition, a model Mid Search African Buffalo Model is used to identify the Mid-frequency (MF) values before the encoding process is carried out (MSABM) [26].

Cheng Zeng, jingbing, et al, (2021), It is proposed to use a CNN-based on color image steganography technique to conceal the secret image behind a cover image of the same size. The steganography plan has two elements: the hiding network and the revealed network. The hiding network apply the skip link, which permit the low-level elements of the image to be transmitted to each subsequent layer, aiding in the concealment of the specific information of the hidden information. [27].

Kh. Abuzanouneh, M. Hadwan (2021) suggested using the feature selection method in conjunction with a pixel selection strategy to conceal hidden messages. In order to make the process of steganalysis difficult, the secret file is spread out and irregularly implanted into the stego-image. The binary sequence of a secret file contains encrypted components, and MPPST generates an intricate key that identifies where they are in the binary sequence. The Least Significant Bit (LSB) approach, another algorithm from the field, and the new approach, MPPST, are contrasted to evaluate their effectiveness [28].

L. Tang, D. Wu, et al (2021), proposed a structural field iterative color image steganography technique based on a fuzzy inference system. The results of the fuzzy inference system, as well as the sensitivity of the human eye to the R, G, and B color components, are used to adaptively hide the data using LSB alternates. When determining the number of bits to encode in the cover image, this methodology uses the outcome of fuzzy reasoning as well as the color plane used for coding [29].

L. Liu, L. Meng, et al (2022), In this research, a huge capacity secret data method based on DNN was developed. It may be used to conceal large-amount color images in smaller color images. DNN was used between the information deception and data extraction stages of our method. Along with being employed in pairs, the two networks were acquired through adversarial training. The carrier picture and the secret image have an information ratio of one to four. [30].

5 Quality evaluation metrics

In evaluating the performance of the proposed model, both subjective and objective analyses are used. The subjective analysis employs the Human Visual System (HVS) to distinguish the differences between the cover image and the stego image and their corresponding histograms. The objective analysis calculates the distortion in the cover

file after inserting secret data through mathematical equations. The Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) are used as objective metrics in this study. A higher PSNR indicates better quality of the stego-image, while values below 30dB indicate poor quality. A high-quality stego-image should aim for a PSNR value of 40dB or higher, as the larger the PSNR value, the lower the risk of visual attack by the human eye. PSNR and MSE are computed using equations 1 and 2, respectively [31-32].

$$\text{PSNR}=10\log_{10}\left[\frac{R^2}{MSE}\right] \tag{1}$$

$$\text{MSE}=\frac{\sum_{M.N}[I_1(m,n)I_2(m.n)]^2}{M*N} \tag{2}$$

Where M and N are the numbers of rows and columns in the input images, respectively. R is the maximum fluctuation in the input image data.

6 The proposed method

The proposed model was implemented in a MATLAB R2021a environment. Standard color images used in experiments are lena.jpg and baboon.jpg. these criteria's images have been utilized as sect images and cover images of different sizes in our experiments. The implementing system used the LSB method which used 1-LSB bits in some cases, and 4-LSB bits in other cases to hide confidential data. Here, we used a secret key to protect the embedded information. The following formula has been utilized in our proposed method:

secret image + secret key + cover image

when embedding information inside the cover image, the cover image is divided into three matrices (Red, Green, and Blue). The secret key is converted into a one-dimension array of the bitstream. Each bit of the secret key is XORed with the secret image.

7 Experimental result

In this research, the LSB technique is implemented in two ways: first, only the least significant one bit (1bit) of each byte of each channel (Red, Green, Blue) will store the embedded data, this method is named (1-LSB). Secondly, only the four least significant bits of the right half-byte (4 bits) of each byte of each channel will store the embedded data, this method is named (4-LSB). Also, two types of images were used in these tests: color and grayscale images of different sizes.

7.1 Image steganography using the 1-LSB method

As shown above, the 1-LSB method refers to use of only one bit of each byte of cover image pixels to embed secret image data. Here, two tests were taken. In the first, two color images are used, one as a cover image and the other as a secret image, both

in JPEG format. As known, every pixel in a color image contains three bytes for each pixel (one byte for each color channel). So, the secret data has been embedded within every byte of cover data by insertion them in the position of the first far-right bit. Figure 4 reveals a standard color image and stego images and their histograms for this test. As can be seen in the figure, there is no significant change in the cover and stego images and their histograms which shows the effectiveness of the proposed method. As well as, PSNR was 42.7557 dB and MSE was 3.4747, these values are considered acceptable.

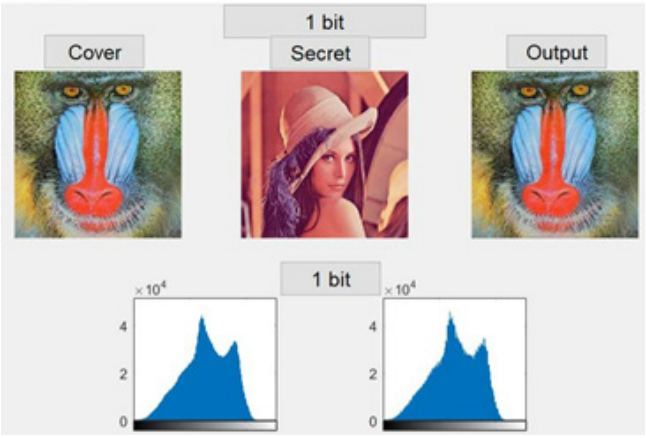

Fig. 4. Color cover and stego image and their histogram using the 1-LSB method

In the second test, two grayscale images are used, one as a cover image and another as a secret image. In a grayscale image, every pixel consists of only one byte to represent the color value (from 0 to 255). here, every bit of the secret data has been embedded within every byte of cover data by insertion it in the position of the first far-right bit. As shown in Figure 5 below.

Fig. 5. Grayscale cover and stego image and their histogram using the 1-LSB method

Some changes in the cover and stego images and their histograms. Despite that, PSNR and MSE values are proximity equal to the result of the previous test.

7.2 Image steganography using the 4-LSB method

As discussed previously, the 4-LSB technique refers to use of the four least significant bits of the right half-byte (4 bits) of each byte to store the hidden data. Using this method (4-LSB), two tests are applied. Firstly, color images are used as cover and secret images. The secret data has been performed within every byte of cover data by hiding them in the position of the four least significant bits of the right half-byte of each color channel. Figure 6 explains that there is a clear change between the histogram of the cover image and the stego image. Also, PSNR and MSE values are 29.29 dB and 27.21 respectively, these values are considered unsatisfiable.

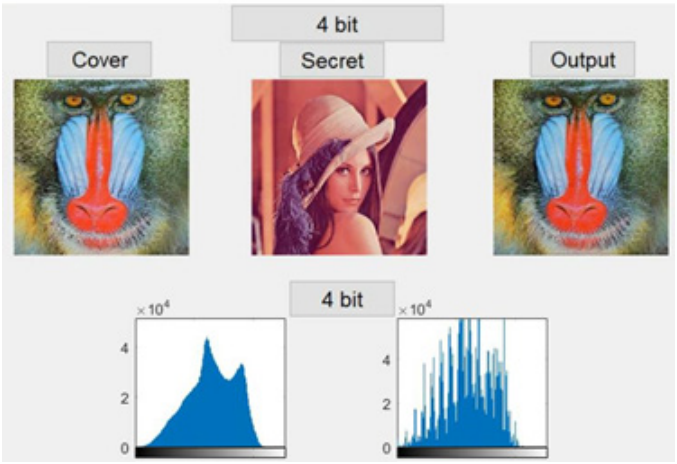

Fig. 6. Color cover and stego image and their histogram using the 4-LSB method

In the other test, two grayscale images are used as a cover image and a secret image. results showed that PSNR and MSE metrics are proximity equal to the result of the previous test. as well as there is a difference between the histogram of cover and stego image. Figure 7 shows the histogram results of this test.

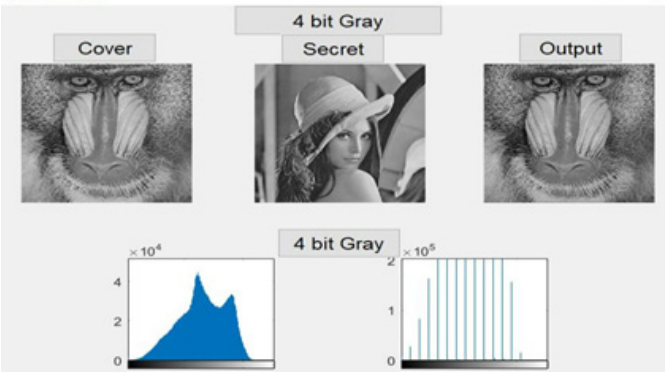

Fig. 7. Grayscale cover and stego image and their histogram using 4-LSB method

8 Discussions

In this study, samples of experiments are implemented for image steganography using the LSB technique. after that, Subjective and objective analyzes were performed for each LSB test. the subjective analysis involved both HVS and histogram, whereas the objective analysis involved both PSNR and MSE metrics. The experiments showed that the 1-LSB technique resulted an acceptable output and there is no noticeable change in the stego image and its histogram when using this method. as well as, PSNR and MSE recorded values within the accepted range. on other hand, the 4-LSB method resulted in stego image with some distortion. also, PSNR and MSE metrics enrolled bad values.

on the other side, experiments illustrated that image steganography using color or grayscale images realize close results, this explains that the LSB method doesn't far affect by the type of used images as long as they are of the same type. Table 1 shows a comparison of 1-LSB and 4-LSB results based on PSNR and MSE metrics

Table 1. Comparison of 1-LSB and 4-LSB results based on PSNR and MSE

LSB method	PSNR (dB)	MSE
Color image steganography using 1-LSB	42.75	3.47
Grayscale image steganography using 1-LSB	42.76	3.46
Color image steganography using 4-LSB	29.28	27.21
Grayscale image steganography using 4-LSB	29.28	27.22

9 Conclusion

This research introduced two types of image steganography methods, 1-LSB and 4-LSB. in 1-LSb, only one bit of each byte of cover image pixels is utilized to embed secret image data. while in 4-LSB, the four least significant bits (right half-byte) of each byte of the cover image are utilized to store the hidden data. In addition, both RGB

and grayscale images are used in the tests. Results showed that the 1-LSB method achieved acceptable outputs and there is no noticeable change in the stego image and its histogram. in addition, PSNR and MSE recorded scores within the accepted range. While in the 4-LSB method, results showed that there is obvious distortion, and PSNR and MSE metrics enrolled bad values also.

10 References

[1] Bandyopadhyay, S. K., Bhattacharyya, D., Ganguly, D., Mukherjee, S., & Das, P. 'A tutorial review on steganography', In International conference on contemporary computing, 2008, Vol. 101, pp. 105-114.

[2] P. Bedi and A. Dua, 'Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet', in Procedia Computer Science, 2020, vol. 171, pp. 1810–1818. https://doi.org/10.1016/j.procs.2020.04.194

[3] F. Susilawati Mohamad, N. Sahira, and M. Yasin, 'Information Hiding Based on Audio Steganography using Least Significant Bit', International Journal of Engineering & Technology,2018, Vol. 7, NO. 3.28, pp. 334-336. https://doi.org/10.14419/ijet.v7i4.15.28363

[4] Sharda, S., &Budhiraja, S. 'Image steganography: A review', International Journal of Emerging Technology and Advanced Engineering, 2013, Vol. 3(1), pp. 707-710.

[5] Kheiralla, F. A. M. 'Steganography a New Dawn in the World of Information Security Compared with Cryptography Technology', International Journal of Innovations & Advancement in Computer Science, 2018, Vol.7(1).

[6] Roy, R., Changder, S., Sarkar, A., & Debnath, N. C. 'Evaluating image steganography techniques: Future research challenges', International Conference on Computing, Management and Telecommunications, 2013, pp. 309-314. IEEE. https://doi.org/10.1109/ComManTel.2013.6482411

[7] Singh, Y. K., & Sharma, S. 'Image steganography on gray and color image using DCT enhancement and RSA with LSB method', In 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, Vol. 3, pp. 1-5. IEEE. https://doi.org/10.1109/INVENTIVE.2016.7830106

[8] Ashok, J., Raju, Y., Munishankaraiah, S., & Srinivas, K. 'Steganography: an overview', International Journal of Engineering Science and Technology, 2010, Vol. 2(10), pp. 5985-5992.

[9] H. T. Hazim, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," International Journal of Online & Biomedical Engineering, vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[10] I. A. Aljazaery, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," International Journal of Online & Biomedical Engineering, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[11] J. Kh-Madhloom, "Dynamic Cryptography Integrated Secured Decentralized Applications with Blockchain Programming," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 2, pp. 21-33, 2022.

[12] H. T. Alrikabi, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, pp. 144-157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[13] H. A. Hassan, "Review Vehicular Ad hoc Networks Security Challenges and Future Technology," Wasit Journal of Computer and Mathematics Science, vol. 1, no. 3, 2022.

[14] I. Aljazaery, and M. Aziz, "Combination of hiding and encryption for data security," hj,hk., vol. 10, no. 15, pp. 10-20, 2020.
[15] M. H. Abd, "Dynamic Data Replication for Higher Availability and Security," Wasit Journal of Computer and Mathematics Sciences, pp. 31-42, 2021. https://doi.org/10.31185/wjcm.Vol1.Iss1.6
[16] J. Q. Kadhim, and H. Salim, "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," International Journal of Emerging Technologies in Learning (iJET), vol. 18, no. 02, 2023. https://doi.org/10.3991/ijet.v18i01.35987
[17] A. S. Mohamad, "Data encryption for bank management system: Data encryption for bank management system," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 4, pp. 14-20, 2022.
[18] H. A. Naman, and M. Al-dabag, "Encryption System for Hiding Information Based on Internet of Things," International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 2, 2021. https://doi.org/10.3991/ijim.v15i02.19869
[19] Stuti Goel, Arun Rana & Manpreet Kaur., 'A Review of Comparison Techniques of Image Steganography', Global Journal of Computer Science and Technology Graphics & Vision, 2013, Vol. 13(4).
[20] Zhou, X., Gong, W., Fu, W., & Jin, L. (2016) 'An improved method for LSB based color image steganography combined with cryptography' In 2016 IEEE/ACIS 15th international conference on computer and information science (ICIS), 2016, (pp. 1-4). IEEE. https://doi.org/10.1109/ICIS.2016.7550955
[21] Singh, Y. K., & Sharma, S. 'Image steganography on gray and color image using DCT enhancement and RSA with LSB method', In 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, Vol. 3, pp. 1-5. IEEE. https://doi.org/10.1109/INVENTIVE.2016.7830106
[22] Arya, A., &Soni, S. 'Performance evaluation of secrete image steganography techniques using least significant bit (LSB) method', Int. J. Compute. Sci. Trends Technol, 2018 Vol. 6(2), pp. 160-165.
[23] R. Thanki and S. Borra, 'A color image steganography in hybrid FRT–DWT domain', Journal of Information Security and Applications, 2018, vol. 40, pp. 92–102. https://doi.org/10.1016/j.jisa.2018.03.004
[24] E. Z. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and M. K. Sarker 'LSB-based Bit Flipping Methods for Color Image Steganography' in Journal of Physics: Conference Series, 2020, vol. 1501, No. 1. https://doi.org/10.1088/1742-6596/1501/1/012019
[25] M. H. Mahdi, A. A. Abdulrazzaq, M. S. Mohd Rahim, M. S. Taha, H. N. Khalid, and S. A. Lafta. (2019) 'Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption', IOP Conference Series: Materials Science and Engineering, Vol. 518, no. 5. https://doi.org/10.1088/1757-899X/518/5/052002
[26] Cheng Zeng, Jingbing Li, Jingjun Zhou, and Saqib Ali Nawaz. 'Color Image Steganography Scheme Based on Convolutional Neural Network', Advances in Artificial Intelligence and Security. ICAIS 2021. Communications in Computer and Information Science, vol 1424. Springer, Cham. https://doi.org/10.1007/978-3-030-78621-2_21
[27] S. Kaur, S. Bansal, and R. K. Bansal (2021) 'Image steganography for securing secret data using hybrid hiding model', Multimedia Tools and Applications, vol. 80, no. 5, pp. 7749–7769. https://doi.org/10.1007/s11042-020-09939-7

[28] K. Ibrahim Mohammad Abuzanouneh and M. Hadwan 'Multi-Stage Protection using Pixel Selection Technique for Enhancing Steganography', International Journal of Communication Networks and Information Security (IJCNIS), 2021, Vol. 13, No. 1. https://doi.org/10.17762/ijcnis.v13i1.4907

[29] L. Tang, D. Wu, H. Wang, M. Chen, and J. Xie 'An adaptive fuzzy inference approach for color image steganography', Soft Computing, 2021, vol. 25, no. 16, pp. 10987–11004. https://doi.org/10.1007/s00500-021-05825-y

[30] Liu, L. Meng, W. Zheng, Y. Peng, and X. Wang, 'A Larger Capacity Data Hiding Scheme Based on DNN', Wireless Communications and Mobile Computing, vol. 2022, Article ID 5425674, 12 pages. https://doi.org/10.1155/2022/5425674

[31] S. A. Jebur, and H. O. Nasereddin 'Enhanced solutions for misuse network intrusion detection system using sga and ssga'. IJCSNS International Journal of Computer Science and Network Security, 2015, vol.15, no. 5.

[32] L. R. Ali, S. A. Jebur, M. M. Jahefer, and B. N. Shaker 'Employing Transfer Learning for Diagnosing COVID-19 Disease'. International Journal of Online & Biomedical Engineering, 2022, vol. 18, no. 15. https://doi.org/10.3991/ijoe.v18i15.35761

11 Authors

Sabah Abdulazeez Jebur received his BSc degree in Computer Science from Mustansiriyah University in Baghdad, Iraq in 2003. He then went on to complete his MSc studies at Middle East University in Amman, Jordan in 2015 with a thesis entitled "Enhanced Solutions for Misuse Network Intrusion Detection System using SGA and SSGA". Currently, he is a Ph.D. student in computer science at the University of Technology in Baghdad, Iraq. His research interests include Artificial Intelligence, Deep Learning, and Image Processing.

Abbas Khalifa Nawar received his B.Sc. degree in Electronic Engineering from Diyala University in Diyala, Iraq in 2005. He then went on to complete his M.Sc. degree in Electronic and Communications from Baghdad University in Baghdad, Iraq in 2013 with a thesis entitled " EEG Classification using Quantum Radial Wavelet Neural Networks Model". Currently, he is an Assistant Lecturer in the Computer Techniques Engineering Department at Imam Al-Kadhum College (IKC) in Baghdad, Iraq. His research interests include electronics and communications, image processing, artificial intelligence, and digital signal processing.

Lubna Emad Kadhim received her BSc degree in Computer Science from the University of Technology in Baghdad, Iraq in 2006. She completed her MSc study at the same university in 2008 with a thesis titled "Block Cipher Using Image as Public Keys.

Motherfer Majeed Jahefer received his BSc degree in Computer Science in 2005 from the Baghdad College of Economic Sciences University in Iraq. He then went on to earn his MSc degree in Information Technology in 2017 from the University of Lodz in Poland. His research interests include IoT and IoNT, data structure algorithms, database analysis, and networks.

Article submitted 2023-01-07. Resubmitted 2023-03-01. Final acceptance 2023-03-03. Final version published as submitted by the authors.