Hide text in an image using Blowfish algorithm and development of least significant bit technique

Sarah Kareem Salim[1], Mohammed Majid Msallam[2,3], Huda Ismail Olewi[4]
[1]Department of Electrical Engineering, University of Misan, Misan, Iraq
[2]Department of Computer Engineering, Ankara University, Ankara, Turkey
[3]Department of Control and Systems Engineering, University of Technology, Baghdad, Iraq
[4]Department of Civil Engineering, University of Misan, Misan, Iraq

Article Info

Article history:

Received May 30, 2022
Revised Sep 8, 2022
Accepted Sep 19, 2022

Keywords:

Blowfish algorithm
Cryptography
Encryption
Least significant bit
Steganography

ABSTRACT

Recently, there is increasing interest in data transfer between many different devices. Data must be encrypted before being sent so that the intended receiver can only read it to prevent unauthorized access and processing of a secret message. This paper suggests two levels of security to secure import messages that are sent via the internet. A secret text is encrypted by a Blowfish algorithm, then the secret text is hidden in an image by the least significant bit (LSB) technique. The LSB method of concealing important information was developed to conceal at least the first of at least two bits, depending on the cover data. The resolution of an image is raised in our work where the sender selects a stego image with a high peak signal to noise ratio (PSNR). The receiver knows all the necessary information for decoding by the first nine pixels. The PSNR is used for evaluating the resolution of the image to check robustness at sending. The number of PSNR illustrates in our proposal that the resolution of the image is near the original LSB technique, but the embedding is more randomly robust in steganography.

Corresponding Author:

Mohammed Majid Msallam
Department of Computer Engineering, Ankara University
Çankaya, Ankara, Turkey
Email: mohammedarjeeli92@gmail.com

1. INTRODUCTION

In the ancient ages, the transmission of secret information was very important. Thus the Greeks, especially in wars, used to encrypt important information [1]. While today, the transmitted data in visual communications is increasing with technological advances and it has raised significantly in many fields such as commercial, medical, military, and industrial fields. Therefore, establishing a secure connection has become significant to transfer secret data in channels of communication is very important. This importance had been found to prevent the unauthorized from accessing data and processing it [2].

Image steganography is a data-hiding technology that embeds secret data in cover images invisibly. It is used to prevent steganalysis to achieve the goal of hidden communication [3], [4]. For normal usage or transmission, the cover image holding secret information is referred to as a steganographic (stego) image, and it has a similar visual effect to the original cover image, this affects the cover image's application scene. Most traditional methods superimpose secret information directly on a specific pixel in the image, which can harm the original image significantly [5]. Text, picture, audio, and video steganography are types diverse used in steganography [6]. Many methods to implement steganography such as least significant bit (LSB) technique, distortion technique, statistical methods, and transform domain techniques [7]. One of the goals of steganography is to delude the hacker that the data sent is normal data that does not contain any confidentiality.

Cryptography is a method of protecting data from unauthorized so that the intended receiver can read and process it [8], [9]. The original data is known as plaintext in cryptography, whereas secured data is known as ciphertext. Cryptography consists of two steps: encryption and decryption. The process of converting plaintext [10] to ciphertext is known as encryption. Decryption refers to the process of converting ciphertext to plaintext. The two types of cryptography are private key and public key cryptography [11]. In private key cryptography, the key required for the encryption and decryption procedures is the same. As a result, the key distribution must be completed before sending any data. Because of the effect of key size on security, this key is important in cryptography. Examples are DES, Triple DES, and Blowfish algorithm [12]. While algorithms such as RSA, Diffie-Hellman, ECC, and El Gamal are public-key cryptography that uses different keys for encryption and decryption [6].

Ilasariya *et al.* [6] proposed an encryption system that used steganography and cryptography. For steganography, the Blowfish algorithm was used while for steganography, the LSB technique was used. The major purpose of their work is to secure important information while encrypting the embedded data. The researchers in [13] designed and implemented for security system based on the Blowfish algorithm. Their system was tested with different types of files which gives time efficiency and accuracy. In their work used MP3, DOCX, JPG, PDF, text, and WMV formats of files. Agarwal *et al.* [14], used the Blowfish algorithm to encrypt an image before embedding the secret text into it by changing the image's LSB technique with data. Furthermore, they are merging the above-generated image with the red, green, and blue (RGB) components of a host image to improve privacy and security, resulting in a more secure image. In the manuscript of Swathi *et al.* [15], The image and data have been encrypted using the LSB technique, and after the sender has encrypted the original image, the data-hider will choose and compress a sequence of bits from which some of the given room will be used to create the cipher text. Selected cipher bits will be encoded using the Blowfish algorithm. Msallam [16] proposed employing a dynamic stego-key to hide a secret message inside an image cover using the LSB Steganography method. Because stego-key relies on the cover image to mask a secret message, the results show more steganographic robustness.

The advantages of the LSB technique are high imperceptibility and payload capacity while one of the disadvantages is low robustness [17]. Msallam [16] has a new approach to developing the LSB technique but a stego image had low resolution with high security. This is one of our motivations to enhance the resolution of stego images and increase robustness in the LSB technique to prevent unauthorized access. To increase the robustness of our system, the important text will be encrypted using Blowfish algorithms before embedding by the LSB technique.

There are four sections to this paper. The methodology of our system, which includes the Blowfish algorithm, least significant bit technique, developed least significant bit technique, and proposal system, will be discussed in section 2. while results and discussion will be presented in section 3. The conclusion will be covered in the final section.

2. METHOD

In our proposal system, the important data will be encrypted by using cryptography and steganography. In cryptography, we use the Blowfish algorithm to encrypt the text. In steganography, the least significant bit (LSB) technique is used to embed the secret message in a cover. Where these algorithms are explained as shown below.

2.1. Blowfish algorithm

The Blowfish algorithm is a suitable alternative to existing encryption schemes because it is an unpatented, freely available fast algorithm, that Bruce Schneier designed and published in 1993 [18]. Blowfish is fast as it runs on 32-bit microprocessors, small because it can run in less than 5KB of memory [15], and simple since it just employs elementary operations like addition, xanthine oxidoreductase (XOR), and table lookup [19]. It is a symmetric block cipher as it encrypts and decrypts data using the same encryption key. The encryption algorithm uses the plaintext and the symmetric encryption key to convert the plaintext to ciphertext. Blowfish algorithm uses a 64-bit block size and keys with lengths ranging from 32 to 448 bits, with 18 subkeys (P-array) and an S-array with four 32-bit entries each with 256 entries [14]. Blowfish is a 16-round Feistel cipher for encrypting data, where the steps involved in each round are outlined below:

```
1. Divide plaintext T into two blocks $T_{Left}$ and $T_{Right}$ of equal sizes.
        For i=1 to 16
        $T_{Left} = T_{Left} \oplus$ P-array$_i$
        $T_{Right} = F(T_{Left}) \oplus T_{Right}$
        Swap $T_{Left}$, $T_{Right}$
        (Undo last swap)
2. $T_{Right} = T_{Right} \oplus$ P-array$_{17}$
3. $T_{Left} = T_{Left} \oplus$ P-array$_{18}$
4. To retrieve ciphertext, combine $T_{Left}$ and $T_{Right}$ back into T.
```

The F function divides a 32-bit input into four 8-bit parts in an equitable way. It is made up of four key-dependent substitution boxes (S-array), each of which can receive 8-bit data as input and output 32-bit data using addition modulo 2^{32} and XOR [20]. Figure 1 illustrates the Blowfish encryption structure of a 64-bit block of data.

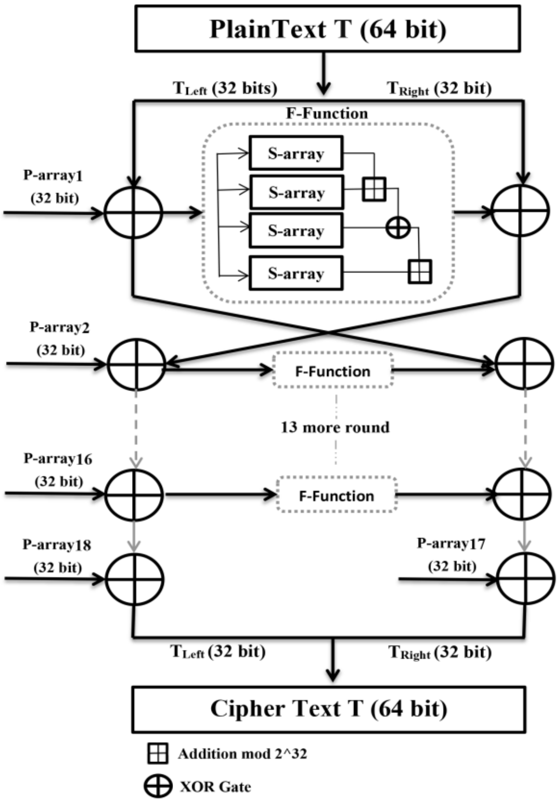


Figure 1. Structure of Blowfish encryption algorithm

2.2. Least significant bit technique

A technique called a least significant bit (LSB) is used to embed secret data into cover data. The LSB widely uses an image as cover data and secret data used as important text, secret information, or data [21]. On the sender side, the secret data always substitutes the least significant bit of cover data to create stego data [22]. While on the receiver side, the user extracts important data from the least significant bit of stego data as shown in Figure 2.

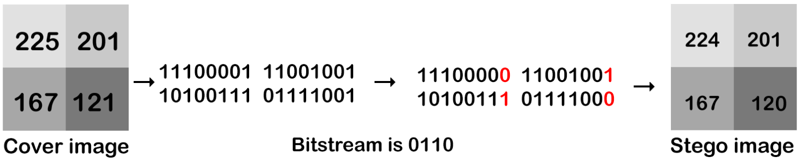
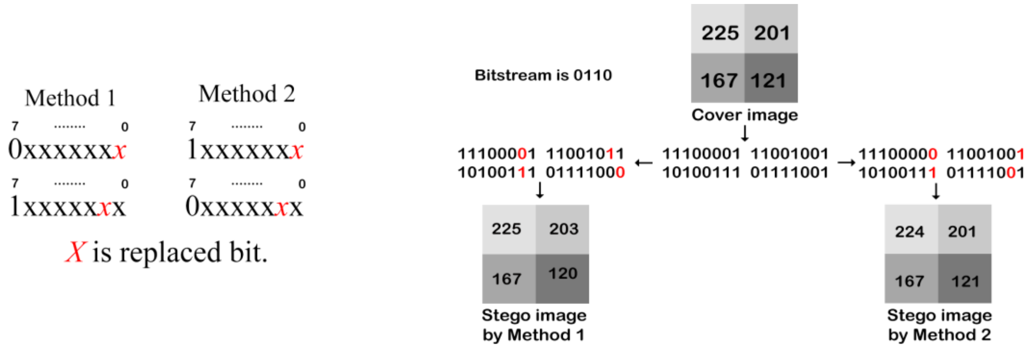


Figure 2. The LSB technique

2.3. Developed least significant bit technique

The developed least significant bit (DLSB) technique is one type of steganography that it makes difficult for intruders to find out the important message in the cover media [16]. The DLSB is the technique to embed secret data inside a cover data and it was suggested by [16]. The embedding of secret data of DLSB is similar to the embedding of secret data of LSB but the embedding of secret data of the DLSB depended on cover data. Where if the 7th bit of data is 0, the replaced bit will be the last bit, while the replaced bit will be the 1st if the 7th bit of data is 1.

In our work, the proposal of Msallam [16] has been developed to contain two methods to hide important data inside cover data, and then a sender selects one of them to send via a network. The selection will be depended on the highest value of PSNR. In method 1, if the 7th bit is 0, the replaced bit will be the last bit, while the replaced bit will be the 1st if the 7th bit is 1. The example illustrates DLSB as shown in Figure 3. In method 2, if the 7th bit is 1, the replaced bit will be the last bit, while the replaced bit will be the 1st if the 7th bit is 0 as shown in Figure 3(a) and Figure 3(b). The advantage of the DLSB is to make stego data similarly to cover data to reduce attacks on important data. Thus, the secret data or message can receive or send via a network with high safety.



(a) (b)

Figure 3. The example illustrates DLSB in (a) the manuscript of Msallam [16] and (b) our proposal

2.4. Proposal system

A simplified schematic diagram of the proposed system is shown in Figure 4. The user inputs the text to our system and then the system encrypts it by using the Blowfish algorithm with the help of a key that is stored on the encryption layer and the decryption layer. In the encryption layer, the important text is encrypted and embedded in an image using the LSB by two methods. The encryption layer then selects one of the stego images to send into the intended receiver which has a high value of PSNR. While in the decryption layer, the important text is extracted from the image and decrypted.

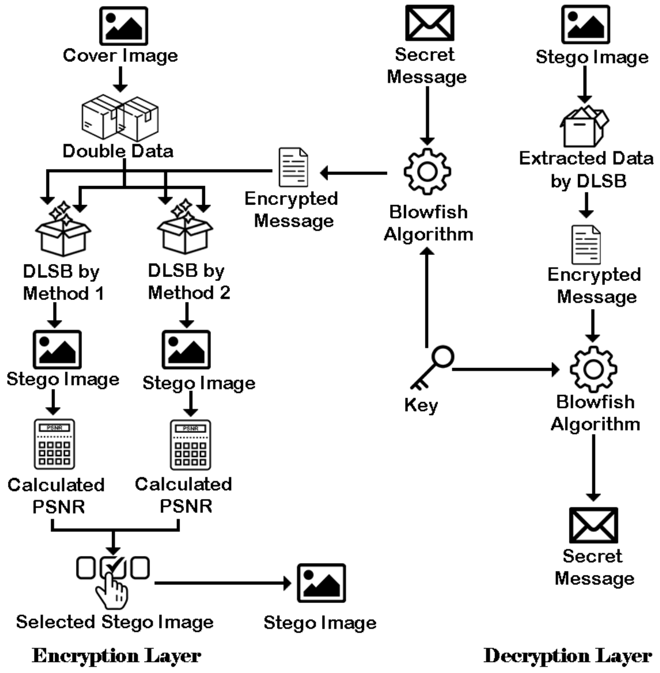


Figure 4. The structure of the proposed system

3. RESULTS AND DISCUSSION

In our work, we use images as cover data so that the secret text embed in the cover image. Four images of size 512×512 and grey color are employed as the cover images. The names of the images are Lenna, Peppers, Baboon, and Boat as shown in Figure 5. The images are shown in Figures 5(a)-(d). The programming language environment that is used in our work is MATLAB R2018b.

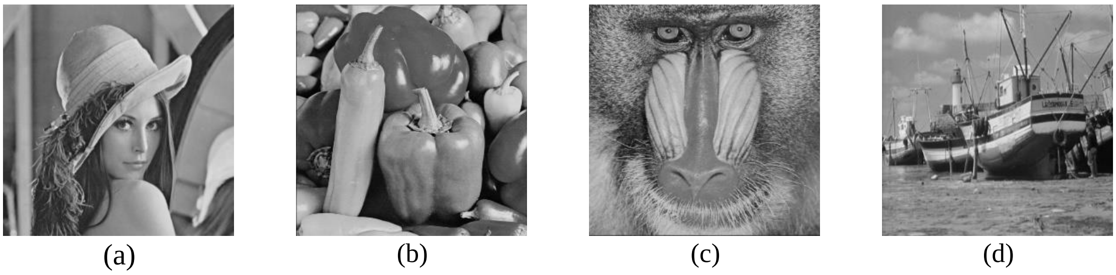
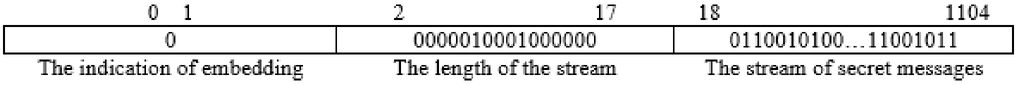


Figure 5. The cover image of (a) Lenna, (b) Peppers, (c) Baboon, and (d) Boat

The secret message contains 136 alphabet in English. The encrypted message includes 1,088 bits that the Blowfish algorithm is used to encrypt. After it is encrypted, it will be added at the beginning of stream 0 or 1 to indicate a method of embedding and 16 bits to indicate the length of the stream which becomes 1,105 bits. Figure 6 is an example of the stream that will be embedded in a cover image.



0 1	2 17	18 1104
0	0000010001000000	0110010100...11001011
The indication of embedding	The length of the stream	The stream of secret messages

Figure 6. The bits stream

The number of the stego image relative to the original image is peak signal to noise ratio (PSNR). The PSNR is measuring the effect on the cover image. The greater the number of PSNRs the better quality of embedding. The mean squared error (MSE) is the difference between the stego image and the original image. In (1)-(2) are the equation of PSNR and MSE respectively [23].

$$\mathrm{PSNR\ (db)} = 10\log_{10}\frac{(2^{n}-1)^{2}}{\mathrm{MSE}} \tag{1}$$

$$\mathrm{MSE} = \frac{1}{W\times H}\sum_{r=0}^{W-1}\sum_{c=0}^{H-1}\big(I(r,c)-D(r,c)\big)^{2} \tag{2}$$

Where n is the number of bits per pixel of the image that is 8. While I (r, c) and D (r, c) are pixel values of an original image and a stego image at the (r, c) locations. The H and W are the numbers of the columns and the rows in an image.

Table 1 shows the value of PNSR for four images. The PSNR value of the LSB method and the PSNR value of our proposal is used in embedding, any change will not be recognized by the eyes of a human. In the sender, the largest PSNR value is selected and sent to the intended receiver.

Table 1. The result of PSNR

Image	LSB	DLSB for Method 1	DLSB for Method 2	Selected to send
Lenna	78.49	76.46	73.70	Method 1
Peppers	78.30	75.78	73.25	Method 1
Baboon	78.23	74.13	74.74	Method 2
Boat	78.95	74.20	74.19	Method 1

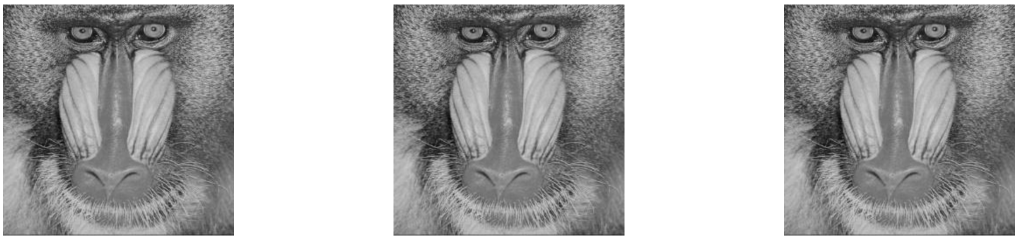
In our work, the secret data had embedded in LSB, Method 1, and Method 2 as shown in Figures 7-10. Figure 7(a), Figure 8(a), Figure 9(a), and Figure 10(a) are shown the stego images for LSB. Figure 7(b), Figure 8(b), Figure 9(b), and Figure 10(b) are shown the stego images for Method 1, while Figure 7(c), Figure 8(c), Figure 9(c), and Figure 10(c) are shown the stego images for Method 2. The proposed system selects the stego image of Method 1 or Method 2 depending on the highest value of PSNR.

(a) (b) (c)

Figure 7. Stego image of Lenna for applying (a) LSB, (b) Method 1, and (c) Method 2

(a) (b) (c)

Figure 8. Stego image of Peppers for applying (a) LSB, (b) Method 1, and (c) Method 2



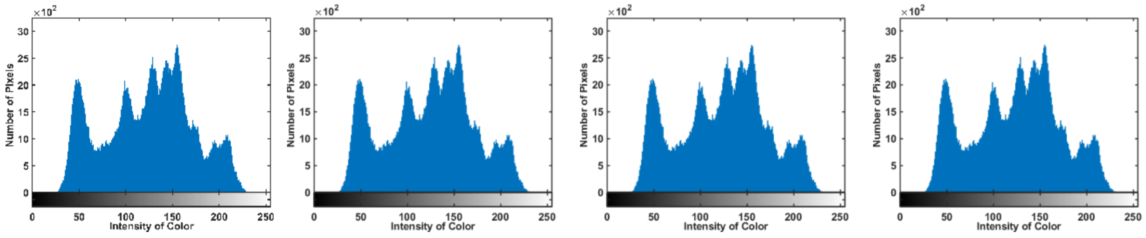
(a) (b) (c)

Figure 9. Stego image of Baboon for applying (a) LSB, (b) Method 1, and (c) Method 2

(a) (b) (c)

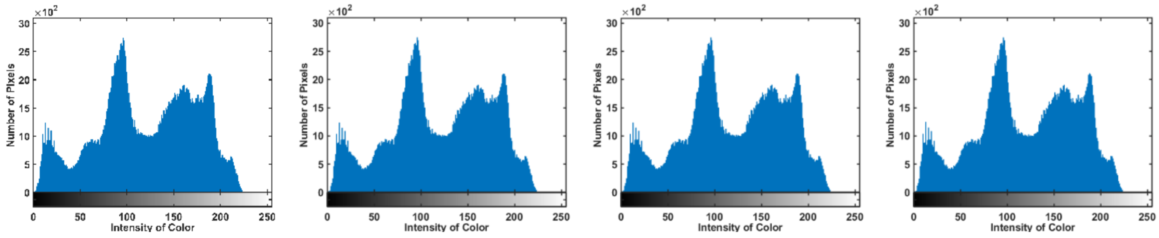
Figure 10. Stego image of Boat for applying (a) LSB, (b) Method 1, and (c) Method 2

The histogram is a graphical representation of the tonal distribution in an image as shown in Figures 11-14. Figure 11(a), Figure 12(a), Figure 13(a), and Figure 14(a) illustrate the histogram of the cover images while Figure 11(b), Figure 12(b), Figure 13(b), and Figure 14(b) illustrate the histogram of the stego images for LSB. On other hand, Figure 11(c), Figure 12(c), Figure 13(c), and Figure 14(c) illustrate the histogram of the cover images for Method 1 while Figure 11(d), Figure 12(d), Figure 13(d), and Figure 14(d) illustrate the histogram of the stego images for Method 1. The change in the stego image does not be recognized by the eyes of a human because the histogram for all stego images is approximately the same as the histogram for all cover images.



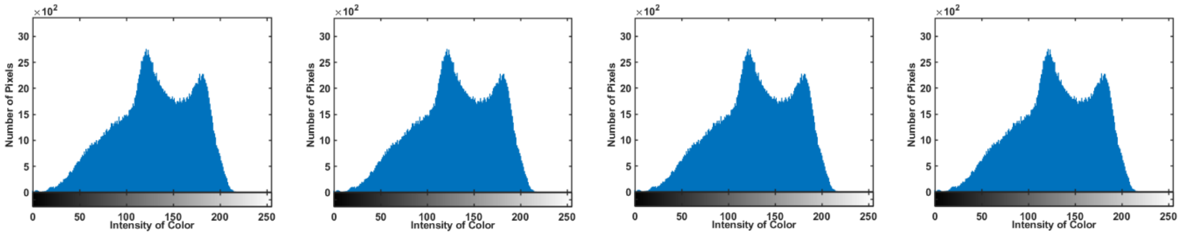
(a) (b) (c) (d)

Figure 11. Histogram of Lenna for the image of (a) cover, (b) LSB, (c) Method 1, and (d) Method 2



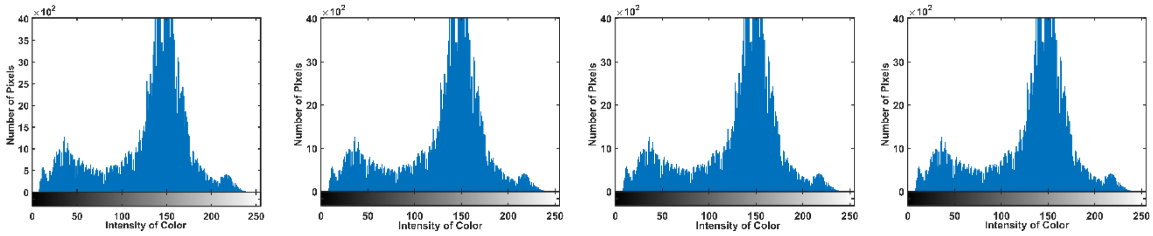
(a) (b) (c) (d)

Figure 12. Histogram of Peppers for the image of (a) cover, (b) LSB, (c) Method 1, and (d) Method 2



(a) (b) (c) (d)

Figure 13. Histogram of Baboon for the image of (a) cover, (b) LSB, (c) Method 1, and (d) Method 2



(a) (b) (c) (d)

Figure 14. Histogram of Boat for the image of (a) cover, (b) LSB, (c) Method 1, and (d) Method 2

The cover image size was used in [16], [24], [25], and our work is 512x512, but the length of the secret stream is different. The length of the secret stream is 432, 1024, 923, and 1105 bits for [16], [24], [25], and our work respectively. Table 2 is compared our work with [16], [24], [25]. Although the PSNR value of our proposal is near to the PSNR value of [16], [24], [25], but our embedding is more complex.

Table 2. Comparison PSNR of our proposal with other researchers

Image	[24]	[25]	[16]	Our work
Lenna	-	-	77.90	76.46
Peppers	72.19	62.20	-	75.78
Baboon	72.48	72.62	78.49	74.74
Boat	-	-	76.39	74.20

4. CONCLUSION

This work is for hiding text in a grey image file. Any type, size, and resolution of grey images can be used in this project. The project's scope involves designing a steganographic approach for concealing secret data in grey image files, which can contain any type of secret bitstream. The system allows users to hide and store confidential information on their local or global devices. The goal of this work is to protect secret data. This technology can also help prevent unauthorized access and ensure message security during transmission.

This project implements style steganography based on the Blowfish algorithm and the LSB technique. The developed embedding of the system merges secret data into grey images to become a single entity. This helps to elude the attackers, leaving them completely unaware that there is confidential data during any communication. The system embedding does not alter the resolution of the cover image and the size of the cover image because the sender selects a similar stego image to the normal image and sends/receives it over the network.

REFERENCES

[1] M. M. Msallam, "An approach to hide an audio file in image using LSB technique, " *Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)*, vol. 1, no. 3, pp. 1–7, 2020, doi: 10.46649/150920-01.

[2] A. A. Arab, M. J. B. Rostami, and B. Ghavami, "An image encryption algorithm using the combination of chaotic maps, " *Optik*, vol. 261, 2022, pp. 1–8, doi: 10.1016/j.ijleo.2022.169122.

[3] X. Wu, T. Qiao, Y. Chen, M. Xu, N. Zheng, and X. Luo, "Sign steganography revisited with robust domain selection, " *Signal Processing*, vol. 196, pp. 1–14, 2022, doi: 10.1016/j.sigpro.2022.108522.

[4] O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 2020, pp. 131–135, doi: 10.1109/ICIoT48696.2020.9089566.

[5] W. Lin, X. Zhu, W. Ye, C. C. Chang, Y. Liu, and C. Liu, "An improved image steganography framework based on y channel information for neural style transfer," *Security and Communication Networks*, vol. 2022, pp. 1-12, 2022, doi: 10.1155/2022/2641615.

[6] S. Ilasariya, P. Patel, V. Patel, and S. Gharat, "Image steganography using Blowfish algorithm and transmission via apache kafka," *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2022, pp. 1320–1325, doi: 10.1109/icssit53264.2022.9716292.

[7] R. Halder, S. Sengupta, S. Ghosh, and D. Kundu, "A secure image steganography based on rsa algorithm and hash-lsb technique," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 18, no. 1, pp. 39–43, 2016, doi: 10.9790/0661-18143943.

[8] A. Pabbi, R. Malhotra, and K. Manikandan, "Implementation of least significant bit image steganography with advanced encryption standard," *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 2021, pp. 363–366, doi: 10.1109/ESCI50559.2021.9396884.

[9] M. Alkhudaydi and A. Gutub, "Securing data via cryptography and Arabic text steganography," *SN Computer Science*, vol. 2, no. 46, pp. 1–18, 2021, doi: 10.1007/s42979-020-00438-y.

[10] A. Abusukhon and S. Alzu'Bi, "New direction of cryptography: A review on text-to-image encryption algorithms based on RGB color value," *2020 Seventh International Conference on Software Defined Systems (SDS)*, 2020, pp. 235–239, doi: 10.1109/SDS49854.2020.9143891.

[11] S. Tynymbayev, Y. Aitkhozhayeva, D. Tananova, and S. Adilbekkyzy, "Modular reduction with step-by-step using of several bits of the reducible number," *Indonesian Journal of Electrical Engineering and Computer Science.*, vol. 25, no. 2, pp. 1087–1093, 2022, doi: 10.11591/ijeecs.v25.i2.pp1087-1093.

[12] R. Anusha, N. Shankari, V. S. Shetty, and S. Bhat, "Analysis and comparison of symmetric key cryptographic algorithms on FPGA," *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2020, pp. 293–300, doi: 10.1109/ICSSIT53264.2022.9716416.

[13] R. S. Cordova, R. L. R. Maata, and A. S. Halibas, "Blowfish algorithm implementation on electronic data in a communication network," *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, 2019, doi: 10.1109/ICECTA48151.2019.8959702.

[14] D. Agarwal, P. Panwar, P. Vyas, T. B. Patil, and S. D. Joshi, "Enhancing image security by employing Blowfish algorithm further embedding text and stitching the RGB components of a host image," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 2, pp. 3801–3808, 2019, doi: 10.35940/ijrte.B1499.0982S1119.

[15] N. Swathi, S. R. Ashwini, N. S. Ashwini, and K. V. Anil, "Blow fish and LSB algorithm based reversible data hiding in the encrypted image," *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT-2018)*, 2018, pp. 2443–2447, doi: 10.1109/RTEICT42901.2018.9012419.

[16] M. M. Msallam, "A development of least significant bit steganography technique," *Iraqi Journal of Computers, Communications, Control, and Systems Engineering*, vol. 20, no. 1, pp. 31–39, 2020, doi: 10.33103/uot.ijccce.20.1.4.

[17] H. Alatawi and C. Narmatha, "The secret image hiding schemes using steganography-survey," *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, vol. 2, no. ICCIT, pp. 132–136, 2020, doi: 10.1109/ICCIT-144147971.2020.9213764.

[18] H. Alabdulrazzaq and M. N. Alenezi, "Performance evaluation of cryptographic algorithms : DES, 3DES, Blowfish, Twofish, and Threefish," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 14, no. 1, pp. 51–61, 2022, doi: 10.1109/SCEECS.2012.6184991.

[19] W. Zhang and Y. Zhao, "Research on plaintext restoration of Blowfish based on neural network," *2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT)*, 2020, pp. 452–455, doi: 10.1109/ISCTT51595.2020.00086.

[20] P. Parvathy and A. S. R. Ajai, "VLSI implementation of Blowfish algorithm for secure image data transmission," *2020 International Conference on Communication and Signal Processing (ICCSP)*, 2020, pp. 0770-0774, doi: 10.1109/ICCSP48568.2020.9182088.

[21] R. Apau and C. Adomako, "Design of image steganography based on RSA algorithm and LSB insertion for android smartphones," *International Journal of Computer Applications.*, vol. 164, no. 1, pp. 13–22, 2017, doi: 10.5120/ijca2017913557.

[22] D. Darwis, N. B. Pamungkas, and Wamiliana, "Comparison of least significant bit, pixel value differencing, and modulus function on steganography to measure image quality, storage capacity, and robustness," *Journal of Physics: Conference Series*, vol. 1751, no. 1, 2021, doi: 10.1088/1742-6596/1751/1/012039.

[23] N. F. H. Al Saffar, I. R. Al-Saiq, and R. R. M. Abo Alsabeh, "Asymmetric image encryption scheme based on Massey Omura scheme," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 1, pp. 1040–1047, 2022, doi: 10.11591/ijece.v12i1.pp1040-1047.

[24] M. Damrudi and K. J. Aval, "Image steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 6, pp. 204–208, 2019, doi: 10.35940/ijeat.F1033.0986S319.

[25] M. Damrudi and K. J. Aval, "Two stage steganography on compressed and encrypted message, " *International Journal of Circuits, Systems and Signal Processing*, vol. 15, pp. 494–498, 2021, doi: 10.46300/9106.2021.15.54.

BIOGRAPHIES OF AUTHORS

Sarah Kareem Salim received the degree of B.Sc. in Computer Engineering from the University of Basrah, Basrah, Iraq, in 2009. She received the degree of M.Sc. in Computer Engineering from Al-Nahrain University, Baghdad, Iraq, in 2020. She had worked as an assistant lecturer in the Electrical Engineering Department, University of Misan, Misan, Iraq. Her research interests include fiber optic communication, computer networking, network communication, steganography, and cryptography. She can be contacted at email: sarahalthahabi@uomisan.edu.iq.

Mohammed Majid Msallam received the degree of B.Sc. in Control and System Engineering as a general speciality and Computer Engineering as a Specialization from the University of Technology, Baghdad, Iraq. He is currently studying for the degree of M.Sc. in Computer Engineering at Ankara University, Ankara, Turkey. He had worked as an assistant engineer at the Control and System Engineering Department, University of Technology, Iraq. His research areas are control systems, encryption data, and artificial intelligence. He can be contacted at email: mmarjeeli@ankara.edu.tr.

Huda Ismail Olewi received the degree of B.Sc. in Computer Engineering from the University of Basrah, Basrah, Iraq, in 2009. She received the degree of M.Sc. in Computer Engineering from Al-Nahrain University, Baghdad, Iraq, in 2020. She had worked as an assistant lecturer in the Civil Engineering Department, University of Misan, Misan, Iraq. Her research interests include secure communications, chaotic encryption, and peak to average power ratio reduction in orthogonal frequency division multiplexing passive optical networks. She can be contacted at email: hudaismail@uomisan.edu.iq.