MJEN

MANAS Journal of Engineering
ISSN 1694-7398 | e-ISSN 1694-7398

Volume 10, Issue 1, (2022) Pages 66-72
https://doi.org/10.51354/mjen. 1049851

Data hiding to the image with bit plane slicing and double XOR

Bilgi Özdemir[1], Nurettin Doğan[2 *]

[1] Selçuk University, Graduate School of Natural and Applied Sciences, Department of Computer Engineering, Konya, Turkey, bilgig@hotmail.com, ORCID: 0000-0002-6841-0933

[2] Selçuk University, Faculty of Technology, Department of Computer Engineering, Konya, Turkey, ndogan@ymail.com, nurettin.dogan@selcuk.edu.tr, ORCID: 0000-0002-8267-8469

ABSTRACT

Data hiding is an important requirement in the history of humankind, whether internationally or personally. With the development of digital technologies, the types, and methods of data to be hidden are also very diverse. It is possible to hide any data sent via transmission channels. In this study, a new message hiding algorithm for a color image is described. In the developed algorithm, bit-plane slicing and double XOR operation are used as the basis. In the algorithm, the message to be hidden first is encrypted and then hidden. In this way, it is aimed to obtain a more secure data hiding algorithm. The keys used are selected from the most significant bitplane of the image to hide data. Thus, the algorithm becomes an adaptive algorithm. The least significant bitplane of the cover image is used to hide data. Performance criteria such as MSE, PSNR, and histogram distribution are used to measure the quality of the developed algorithm. Comparing the performance criteria with other studies shows that the developed algorithm can take its place in the field of data hiding in the literature.

ARTICLE INFO

Research article

Received: 28.12.2021
Accepted: 7.06.2022

Keywords:
Bit Plane Slicing (BPS), Steganography, Cryptology, Least Significant Bit (LSB) Method, Most Significant Bit (MSB) Method,
PSNR, MSE.

*Corresponding author

1. Introduction

The privacy and security of communication between people are of great importance. Due to the widespread use of digital communication over the internet, it is very important to ensure the secure transmission of information. Cryptography and Steganography are branches of science used to ensure information security and confidentiality [1]. Cryptography makes these messages unreadable to prevent unauthorized users from reading confidential or private messages. However, steganography deals with hiding hidden text data or other media in other media. Steganography is derived from the Greek words "steganos" and " Graphia", meaning cover and writing, respectively [2,3]. A carrier object is needed for use in steganography. The carrier object is called the cover-data in the environment where the data is hidden, and the resulting environment is called stegotext or stego-object, and it is called the cover-file [4]. The data to be hidden in cover objects can be text, image, or sound files [5]. The image obtained after embedding data into the cover image is called a “stego image”. Hiding functions used in the process of embedding hidden data in the cover object and then retrieving the hidden data from the stego object are defined as keys [6]. The basic steganography process described above is graphically explained in Figure 1.

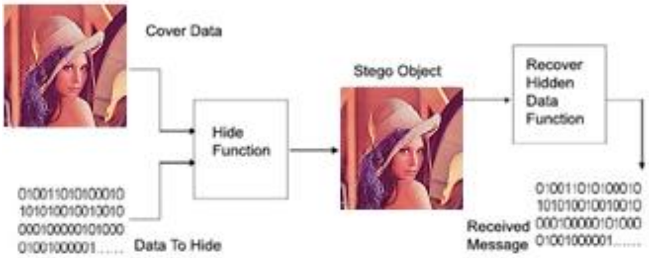


Figure 1. *Basic steganography system [7].*

Bit Plane Slicing (BPS) is a method of expressing an image in which each pixel is represented by one or more bits of the byte. To incorporate hidden data in any slice of eight slices, the BPS approach requires a bit slicing algorithm. Each pixel is represented by 8 bits in this approach. The combination of bit planes creates the whole image. Plane-0 is made up of LSB (Least Significant Bit) and Plane-7 is made up of MSB (Most Significant Bit) (Most Significant Bit). The value and role of each bit of the image may be determined by dividing the digital image into bitplanes. This approach, which is also effective for image compression, defines the total amount of bits required to quantize each pixel [8]. Figure 2 shows the schematic view of bitplane slicing.

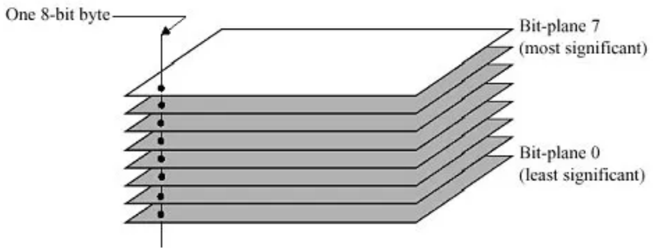
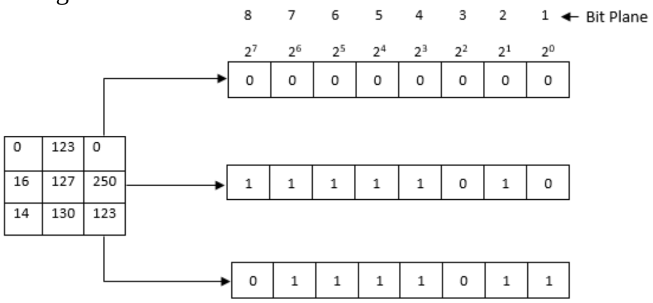


Figure 2. *Bit-Plane Slicing*

The security level is proportional to the number of bitplanes utilized to divide the image. The most preferred way is to hide data in the LSB bitplane, which results in less visual distortion. The risk of image corruption is lower when data is hidden in the LSB bitplane rather than the MSB bitplane. To avoid this distortion, it's important to properly hide in any plane without affecting the original image [8]. Figure 3 shows a binary display of each pixel's density value in bit plane slicing.



0	123	0
16	127	250
14	130	123

Figure 3. *Binary display of density value of each pixel in bit plane slicing [8]*

In the implementation of the Least Significant Bit (LSB), the least significant bits of the pixel values are used. Data bits are placed in each byte of the pixels that make up the image, one by one, respectively, starting from the beginning of the data [5]. The data to be hidden is written to the lowest-order pixel bits in order. It happens by changing the bits that will be placed in the least significant bit. This change in the image is very small and cannot be seen with the naked eye [9,10]. In the data hiding process with LSB, the hidden bit is written to the last bit of the related pixel in the binary system [11].

The most significant bit (MSB) is the highest bit of a string of numbers in binary [12]. Changing the LSB bits of an image creates a very small difference in the image that is not visible to the naked eye. Considering this situation for an image, the eye can't perceive it. When the MSB bit is changed, there is a huge color difference, and the eye can easily perceive it. Color and image distortions occur [13].

In this study, a combination method of cryptography and steganography is proposed. The encryption process proposed here is considered very efficient as it is obtained by performing a double XOR operation on a stream of message text stream with the stream of bits in the most significant MSB bit-slice obtained by the BPS method.

The outline of the proposed study is summarized as follows:

- The color cover image is divided into RGB channels and the pixel values of the R channel are obtained.
- To work on the R channel, the R channel is split into bit planes. Hiding is done on this channel determined in this way.
- In the MSB bitplane of the R channel, as many bits as the bit length of the message is determined as the key.
- The bits of the message information and the bits of the MSB are XORed. This is the first XOR operation.
- The second key is generated by inverting the MSB key bit. The result obtained from the first XOR operation with the second key is XORed. This is the second XOR operation.
- The resulting encrypted message is hidden in the LSB bitplane of the R channel.
- The hidden information in the Stego image is obtained by applying the above operations in reverse order.

In the encryption process, a more secure data hiding algorithm is obtained by using the bits in the most significant bit plane of the image's R channel as keys. In addition, an adaptive method is obtained by obtaining the key from the image. Three different images are used to evaluate the quality of the algorithm.

The remainder of this article is organized as follows:
Chapter 2 provides necessary information about the relevant study; Chapter 3 explains the basics behind the proposed combination schemes. Section 4 shows the results of the study and discussions. Finally, in Chapter 5, the conclusion of the article is presented

2. Literature Review

Wai et al., in their study, provide information hiding to the image by using LSB, MSB (Most significant bit), and NHB (New hybrid) techniques. Many different confidential data formats (txt, docx, xlsx, pdf) are hidden in the cover image [12].

Sharma et al., by explaining various steganography and cryptography techniques, revealed that steganography and cryptography alone are not sufficient for information security, therefore, the best of both techniques are combined to create a more secure and robust approach [14].

Neyeem proposed a new approach for reversible data hiding (RDH) using bitplane slicing. Instead of embedding data directly in an input image, it provided hiding data in a pair of bit-plane sliced images of the input image [15].

Ahmed et al. suggested two encryption layers and a hiding stage. The message was encrypted using the double XOR operation and a secret key using binary representation, and then the encrypted bits were stored in the cover image using the LSB technique [16].

Astuti et al. have made some modifications to the LSB algorithms by adding a sequence algorithm for pixel selection. A three-time XOR operation is proposed on text messages and a three-bit MSB is used as the key in the encryption process [17].

Santosove et al. used image steganography, division, and module function, which was developed by first reducing the length of the message and then using the AES algorithm. Message security is increased as the messages are divided into two parts and sent separately [18].

A simple XOR binary-based operation used by Arindam et al. is implemented. In their work, some modifications of LSB algorithms have been made by adding a sequence algorithm for pixel selection. A three-time XOR operation is proposed on text messages and a three-bit MSB is used as the key in the encryption process [19].

Akbar et al. applied bit plane slicing to the fingerprints of the criminals and divided them into eight slices, and the criminal information of the criminals was kept in any of these eight slices. The secret message is encrypted and integrated into any bitplane after the bitplane image is rotated at various angles. Thus, it is not possible to understand which technique is used in encryption [8].

In this study, a simple and efficient way of double XOR operation with true random double key is performed before hiding the message using the BPS technique.

3. Proposed Method

In this study, an application is carried out on Lena, Pepper, and Babbon images as colored cover images. By using the BPS technique, the color cover image is divided into RGB channels and bit plane slicing is done for each channel. Message hiding work is carried out on the R channel from the obtained channels. A simple and efficient way of double XOR operation with a true random double key is performed before the MSB bit of the R channel of the cover image is hidden in the text. Encrypting the MSB bit is the most recommended method, as there is less cover image corruption. If encryption is selected for the LSB bit, the probability of the image being corrupted is higher than for the MSB bit encryption. The above-mentioned techniques are presented visually in the workflow chart given in Figure 4 below.

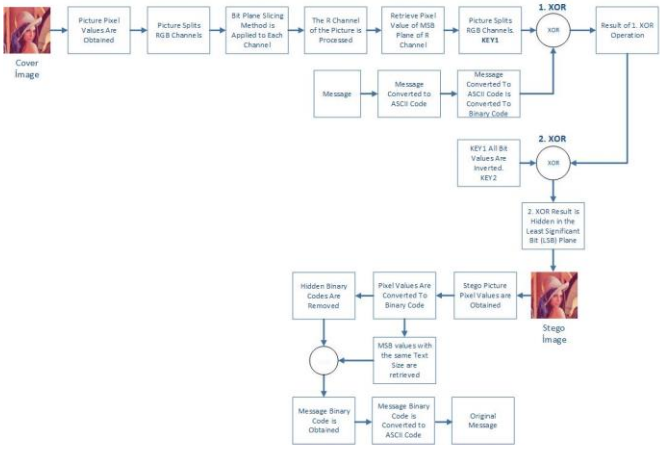

Cover İmage
Picture Pixel Values Are Obtained
Picture Splits RGB Channels
Bit Plane Slicing Method is Applied to Each Channel
The R Channel of the Picture is Processed
Retrieve Pixel Value of MSB Plane of R Channel
Picture Splits RGB Channels KEY1
1. XOR
XOR
Result of 1. XOR Operation
Message
Message Converted to ASCII Code
Message Converted To ASCII Code Is Converted To Binary Code
2. XOR
KEY1 All Bit Values Are Inverted. KEY2
XOR
2. XOR Result Is Hidden in the Least Significant Bit (LSB) Plane
Stego İmage
Stego Picture Pixel Values are Obtained
Pixel Values Are Converted To Binary Code
Hidden Binary Codes Are Removed
MSB values with the same Text Size are retrieved
Message Binary Code is Obtained
Message Binary Code is Converted to ASCII Code
Original Message

Figure 4. *Workflow of Recommended Security Method to Hide Encrypted Text Messages*

When Figure 4 is examined, a one-time (one-time pad (OTP)) symmetric encryption algorithm was used with the Double XOR process. This algorithm is very fast and unbreakable as the use of double keys performs in a one-bit stream in a single operation. The data hiding and decryption pseudo-codes of our algorithm are given below.

```
Data Hiding Algorithm:
Input: C is a color cover image. m is a message. R is C's Red channel.
Output:S is a stego image.
Start
size ← C's row, column, channel //Get the pixels of C.
Loop 1 to 8 BPS do // Do bit plane slicing
    b ← R  // Get bitplane slices of R channel.
end for
Bi_Msg=bin2dec(m) //Convert bits of m to binary code.
Loop 1 to length (m) do // Do the loop as many times as the m length.
    msg←Bi_Msg //Get the binary bit string of m.
end for
key1 ← Get the bit string from MSBs of C of the same length m.
Loop i = 1 to length (msg) do // Do the loop as many times as the msg length.
    EMtemp = msg-in-bits XOR Key1 // Do XOR m and KEY1 bits.
end for
Key2 = flip (Key1)) // Flip all the bits.
Loop i = 1 to length (msg) do // Do the loop as many times as the msg length.
    EM = EMtemp-in-bits XOR Key2 // Do XOR the EMtemp and KEY2 bits.
    Output1= LSB bit- in-bits BITSET EM //Hide EM encrypted message to LSB bit of R channel.
end for
end
```

```
Decryption Algorithm:
Input: S is an image.
Output: m is a message.
Start
size ← S's row, column, cannel //Get S's pixels.
bit plane slice ← R //Get bit plane slices of the R channel of the Stego image.
```

```
Loop i =1 to length (msg) // Do the loop as many times as the msg length.
    Get the bit string for Lkey ← LSB(Si) message length.
    length (msg)=bin2dec(Lkey) //convert bit string to binary.
end for
Loop i = 1 to length (msg) do // Do the loop as many times as the msg length.
    Get the bit sequence from the MSBs of key1 ← S.
end for
Loop i = 1 to length (msg) do // Do the loop as many times as the msg length.
    EM ← Extract string of bits from LSB1(Si) //Obtain bit string from LSB1 (Si).
end for
EMtemp = EM m-in-bits XOR Key1 // Do XOR EM m and bits Key1
Key2 = flip (Key1)) // Flip all the bits.
m-in-bits = EMtemp XOR Key2 //m is user message.
end
```

4. Experimental Result and Discussion

The suggested approach is evaluated using three alternative cover images. Each Cover image's original and hidden message images, as well as histogram graphs, are obtained. The histogram plot with Lena's original image and the histogram plot with the Stego image are shown in Figure 5. Bitplane slices of the Lena image are shown in Figure 6. The histogram plot with the original Pepper image and the histogram plot with the Stego image are shown in Figure 7. Bitplane slices of the R channel of the Pepper image are shown in Figure 8. The histogram plot with the original Babbon image and the histogram plot with the Stego image are shown in Figure 9. Bitplane slices of the R channel of the Babbon image are shown in Figure 10.

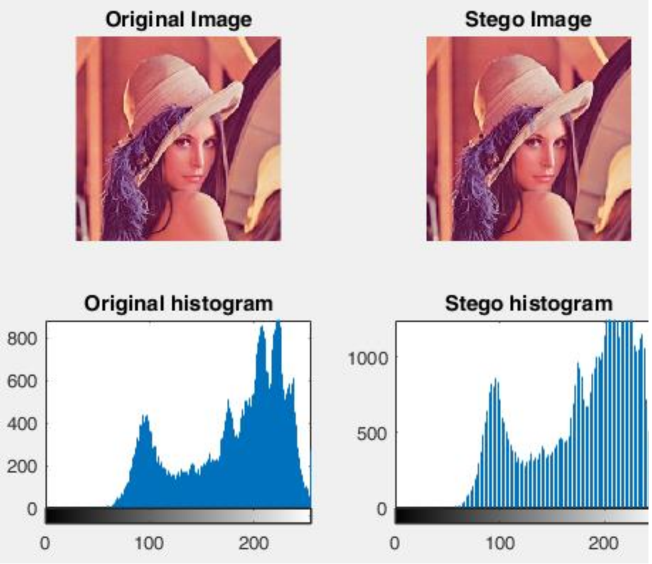


Figure 5. *Original Lena image, message hidden Lena image and their histogram plots.*

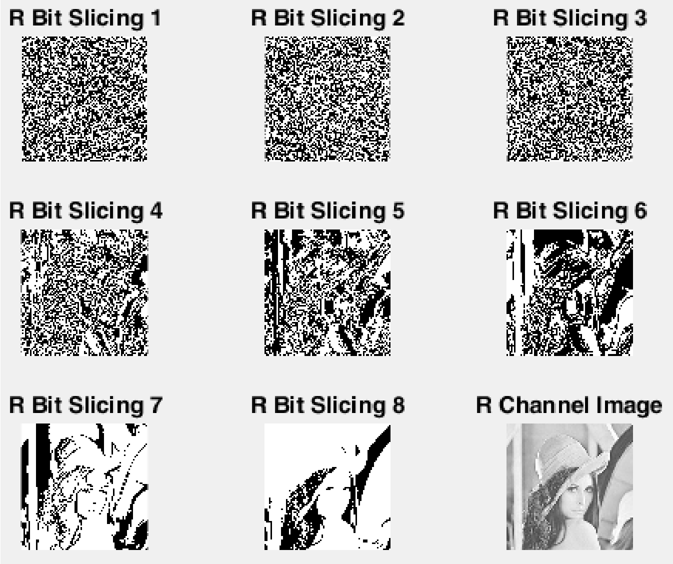


Figure 6. *8 Bit Plane View of R Channel of Lena image*

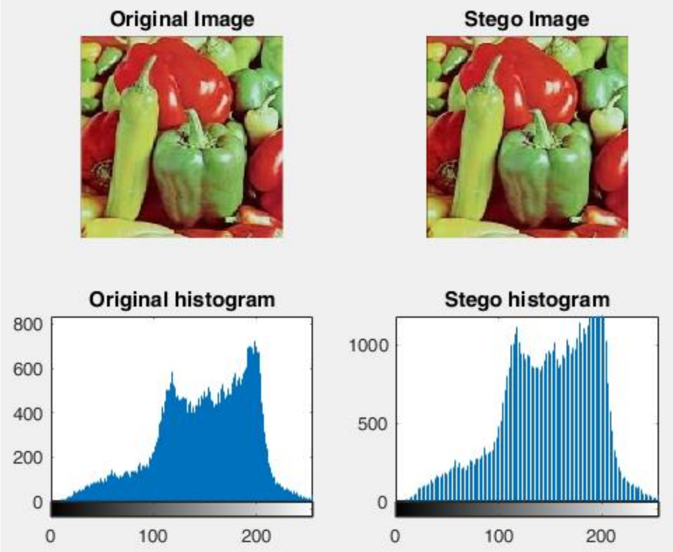


Figure 7. *Original pepper image, message hidden pepper image and their histogram plots.*

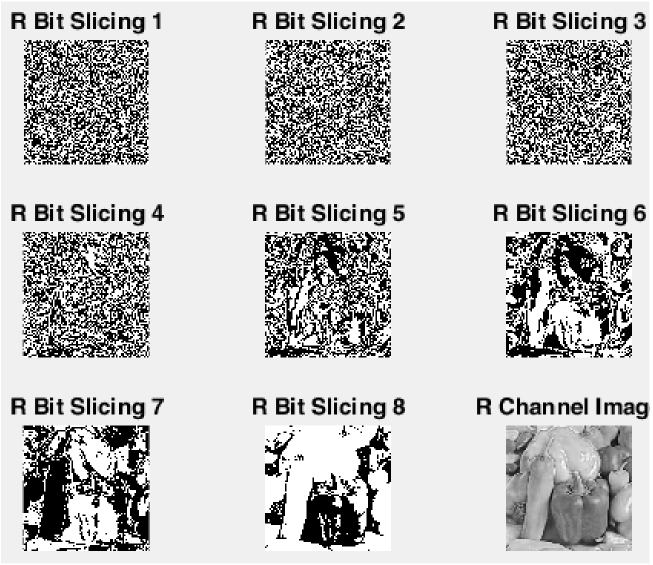


Figure 8. *8 Bit Plane View of R Channel of Pepper Image*

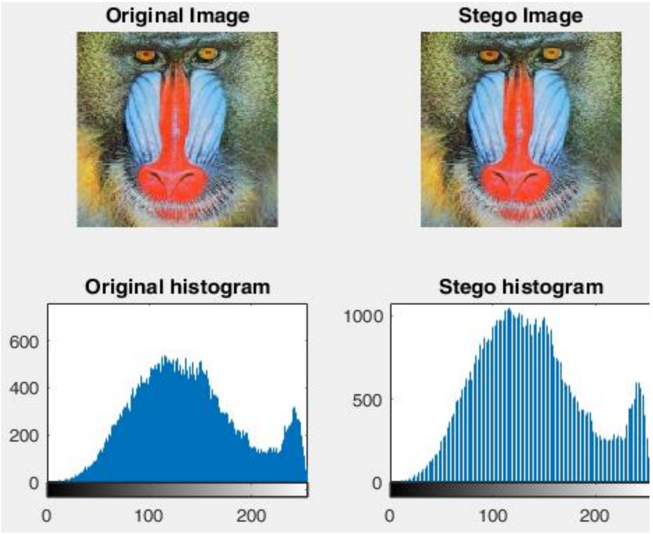


Figure 9. *Original Babbon image, message hidden Babbon image and their histogram plots.*

When the original and message-hidden stego images are examined, the changes in the pixels are too few to be distinguished by the human eye. However, when looking at the histograms of the images, the difference between the original and the message-hidden stego image histograms can be seen. This reveals the change made by the message in the pixels. It can be seen above that the R channel of each image is divided into bit plane slices.

For performance and evaluation measures, two common well-known metrics were used, mean square error (MSE) and peak signal-to-noise ratio (PSNR). MSE is the expected value of squared error loss or quadratic loss.

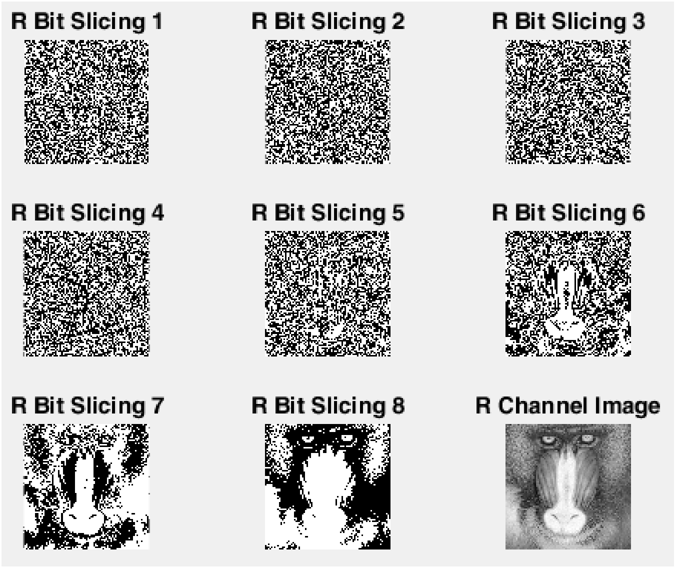


Figure 10. *8 Bit Plane View of R Channel of Baboon Image*

When the MSE value approaches zero, the PSNR value goes to infinity. A higher PSNR value represents better image quality. On the contrary, the smaller PSNR value indicates that the difference between cover and stego images is increased and there is no good embedding [20,21]. PSNR is usually expressed in decibels (dB) on a logarithmic scale. PSNR value greater than or equal to 30dB is difficult to detect by the human eye. PSNR value below 30 dB indicates very poor quality [22].

- MSE is between two images A (x, y) and B (x, y).
- Here, A and B are stego images and cover images, respectively, as given in the following equation [16]:

$$MSE = \sum_{i=1}^{x} \sum_{J=1}^{y} \frac{(|A_{iJ} - B_{iJ}|)^2}{x \times y}$$

- Here, x and y are the width and height of the image.
- PSNR is a well-known performance measure for image degradation that is always applied to the stego image and calculated by the following equation [16]:

$$PSNR = 10 log_{10} \frac{C_{max}^2}{MSE}$$

- C_{max}^2, is the maximum value in the image as below:

$$C_{max}^2 \leq \begin{cases} 1 \; in\ double\ precision\ intensity\ images \\ 255 - 8\ bit\ unsigned\ integer\ intensity\ images \end{cases}$$

- Images with double precision density 1 and unsigned integer density images must be less than or equal to C^2_{max}, values between 255 and 8 bits [16].

- These two criteria were already found by Eskicioğlu et al. [23]. In addition to image compression, they have been widely used in the field of image steganography.
- Experiments are conducted on MatLab2016b with 64-bit Microsoft Windows 10 operating system, Intel Core i5 platform with 2.5 processors, and 8 GB random access memory.

Table 1. *PSNR and MSE Values of the Proposed Method for Different Cover Images.*

Images	PSNR	MSE
Lena	55,903	0,166
Pepper	55,940	0,165
Babbon	55,929	0,165

Based on the values read and examined in Table 1, good results are seen for both MSE and PSNR values. Most PSNR values are greater than 40 dB, which is considered acceptable performance as reported by Nolkha et al. [24].

When our study for the colored Lena image is compared with other results in the literature, it is seen that the proposed method provides a quality stego image. Comparison results are shown in Table 2.

Table 2. *Results Of Image Quality Measures*

Method	Hidden Data	PSNR	MSE
Recommended Method	319 byte	55.903	0.166
Mahdi et al. [25]	150 byte	72.023	0.004
Tiwari&Gangurde [26]	112 byte	45.865	1.684
Ni et al. [27]	682 byte	48.20	0.980
Ahmed et al. [16]	500 byte	51.95	0.420

5. Conclusion

In the study, a method is proposed to hide text messages on a colored cover image. In the proposed method, BPS steganography, which provides the capacity to hide large data, is studied. After the color cover image is first split into RGB channels, bitplane slicing is applied to R channel. At the beginning of the algorithm, the number of bit planes to be processed and the R color channel are determined and the ciphertext message is hidden in the LSB bit of the R channel. By using double encryption, secret data is sequentially embedded in LSB bit planes, preventing access to confidential information against external attacks in bit plane examination. Thanks to this process, hidden data is prevented from appearing as images in the least significant bit planes. In addition, data security is ensured with double encryption. The comparison of the proposed method with the current methods in the literature is given in Table 2. In the comparison, studies that hide data with the LSB method were used by using the Lena color image as the cover image. Looking at these results, it seems appropriate that the proposed algorithm can be used in the process of hiding information on the colored cover image. As a result, our method can take its place in the literature with other studies.

Acknowledgment

We would like to thank the referees who read this study and made the necessary criticisms and contributed to the writing of the study in a better way.

References

[1] Solak S., Altınışık U., A New Approach For Steganography: Bit Shifting Operation Of Encrypted Data In LSB (SED-LSB), Bilişim Teknolojileri Dergisi, 12(1), (2019), 75-81.

[2] Morkel, T., J.H. Eloff, M. S. Olivier., An Overview Of Image Steganography, in ISSA, (2005).

[3] Çelik, H. , Doğan, N. "K-En Az Anlamlı Bitlere Dayalı Kaotik Bir Harita Kullanan Renkli Görüntü Steganografisi". Politeknik Dergisi (2021): 1-1, https://doi.org/10.2339/politeknik.1008594 .

[4] Kurnaz H., "Hibrit Yaklaşımlı Yeni Bir Seganografi Yönteminin Geliştirilmesi," M.S. thesis, Kocaeli University, 2019.

[5] Esin E. M., Güvenoğlu E., Resim İçine Yazı Gizlenmesi Amacıyla Kullanılan LSB Ekleme Yönteminin Shuffle Algoritmasıyla İyileşitirilmesi.

[6] Patel Z. V., Gadhiya S. A., A Survey Paper On Steganography And Cryptography, International Multidisciplinary Research Journal (RHIMRJ), 2(5), (2015), 2349-7637.

[7] Özbilgin F., Durmuş F., Karagöl S., Yazılı Metni Şifreleyip LSB Yöntemi ile Gizleme, Bilim ve Teknoloji Dergisi, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, (2018), 676-685.

[8] Akbar S., Dr. Rao K. N., Anand T., Bit-Plane Slicing Algorithm for Crime Data Security Using Fusion Technologies, International Journal of Recent Technology and Engineering (IJRTE), 7, (2019), 323-325.

[9] Yüksel K. [Online]. Available: https://www.youtube.com/watch?v=_-Ct3uV6AwM. [Accessed: Dec. 18, 2021]

[10] Doğan F., Daş R., Türkoğlu İ., İmgeler İçin Farklı Bir Veri Gizleme Yaklaşımı, Mühendislik Dergisi, .7(3), (2016), 501-514.

[11] Konyar Z., İlkin S., Çelik N., Sondaş A., Steganografi İçin En Uygun Resmi Belirleyen Uygulama Arayüz Tasarımı, İleri Teknoloji Bilimleri Dergisi, 1(7), (2018), 83-89.

[12] Wai Y. Y., Myat E. E., Comparison of LSB, MSB and New Hybrid (NHB) Of Steganography In Digital Image, International Journal of Engineering Trends and Applications (IJETA), 5(4), (2018).

[13] Gürel H., "Sayısal Resim İçerisine Veri Gizleme Uygulamaları," M.Sc. thesis, Kocaeli University, 2006.

[14] Sharma, H. and K. K. Sharma, S. Chauhan, "Steganography Techniques Using Cryptography-A Review Paper," 2015. pp.106-108.

[15] Neyeem H., "Reversible Data Hiding with Image Bit-Plane Slicing", 20th International Conference of Computer and Information Technology (ICCIT), 2017. pp. 22-24.

[16] Ahmed A., Ahmed A., A Secure Image Steganography Using LSB And Double XOR Operations, IJCSNS International Journal of Computer Science and Network Security, 20(5), 2020.

[17] Astuti, Y. P., E. H. Rachmawanto, and C.A. Sari,"Simple And Secure Image Steganography Using LSB And Triple XOR Operation Tn MSB," in 2018 International Conference on Information and Communications Technology (ICOIACT), 2018.

[18] Santoso H.A., Rachmawanto E. H., and Sari C. A., "An Improved Message Capacity And Security Using Divide And Modulus Function In Spatial Domain Steganography, " in 2018 International Conference on Information and Communications Technology (ICOIACT), 2018.

[19] Roy, A., Bhattacharya J., Kundu S., Sahana S., and Singh D., "Block Steganography Based Secure Key Encryption To Improve Data Security", in International Conference on Innovation in Modern Science and Technology, 2019.

[20] Horé A. and Ziou D., "Image Qualitymetrics: PSNR vs. SSIM," in International Conference on Pattern Recognition, 2010. pp. 2366-2369.

[21] Karakis R., Güler İ., Çapraz İ., Bilir E., A Novel Fuzzy Logic-Based Image Steganography Method To Ensure Medical Data Security, Computers in Biology and Medicine, 67(C), (2015), 172-183.

[22] Pund-Dange S., Desai C. G., A novel Approach of Steganography Using Bit Plane Slicing And Catalan-Lucas Number Sequence, International Journal on Recent and Innovation Trends in Computing and Communication, 6(6), (2018), 180-183.

[23] Eskicioglu A. M., Fisher P. S., Image Quality Measures And Their Performance", *IEEE Transactions on Communications*, 43(12), (1995), 2959-2965.

[24] Nolkha A., Kumar S., Dhaka V., Image Steganography Using LSB Substitution: A Comparative Analysis On Different Color Models, in Smart SystemsandIoT: Innovations in Computing, (2020), 711-718.

[25] Mahdi, S. A., Maisa'a, A. K., An Improved Method For Combine (LSB and MSB) Based On Color Image RGB, Engineering and Technology Journal, 39(1B), (2021), 231-242.

[26] Gangurde, S., Tiwari, K., LSB Steganography Using Pixel Locator Sequence With AES, arXiv e-prints, arXiv-2012., (2020).

[27] Ni, Z., Shi Y., Ansari N., Wei S., Reversible Data Hiding, IEEE Transactions on Circuits Systems and Video Technology, 16(3), (2006), 354-362.