Cek Plagiasi Yenni

by Alfan Indra Kusuma

Submission date: 06-Feb-2023 05:37AM (UTC-0800)
Submission ID: 2007605886
File name: el_LSB_Image_Steganography_Modification,_Bit_Modification_on.pdf (682.47K)
Word count: 5674
Character count: 29047

Bulletin of Electrical Engineering and Informatics
Vol. 99, No. 1, Month 2099, pp. 1~1x
ISSN: 2302-9285, DOI: 10.11591/eei.v99i1.paperID

A Novel LSB Image Steganography Modification: Bit Modification on RGB Image Component

Yenni Seftiardiyah[1], Mochamad Alfan Rosid[2], Sukma Aji[3]
[1, 2, 3]Department of Informatics, Universitas Muhammadiyah Sidoarjo, Indonesia

Article Info

Article history:

Received month dd, yyyy
Revised month dd, yyyy
Accepted month dd, yyyy

Keywords:

Least Sgnificant Bit
Steganography Modification
RGB Image Component

ABSTRACT

Image steganography is a method that involves composing hidden messages and embedding them into an image carrier. This ensures that only the sender and the receiver are know that the image contains a hidden message. This study refines the Least Significant Bit (LSB) method of image steganography by switching the least significant bit with the most significant bit and incorporating a hidden message bit in the process. The purpose of this study is to identify a new way to modify the approach of embedding messages from the least significant bit on Red, Green, and Blue (RGB) image components all the way up to the most significant bit. The findings of this study include an image comparison that is encoded with a secret message from the least significant bit all the way up to the most significant bit, then calculated using Mean Square Error (MSE), Peak Signal Noise Ratio (PSNR), Root Mean Square Error (RMSE), and Structural Similarity Index Metric (SSIM) to make a comparisons which stego-image that have a best result. This study found a new method that the best result of MSE, PSNR, RMSE and SSIM on the plane ilage on the 6th bit.

Corresponding Author:

Yenni Seftiardiyah
Universitas Muhammadiyah Sidoarjo, Indonesia
Email: 191080200251@umsida.ac.id

1. INTRODUCTION

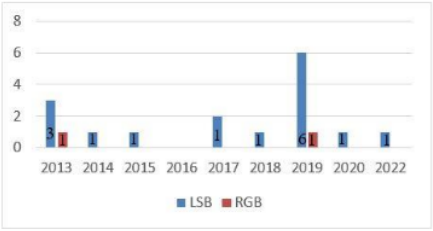

Figure 1. Top Survey of Image Steganography Articles

There are essential data security issues for a great number of users whi transfer data on a regular basis [1]. There are many different encryption methods now being researched to encrypt data in order to make it more safe. Steganography is one of the subfields of the cryptographic technology that falls under the umbrella of data embedding [2]. Steganography refers to the practice of concealing confidential information within various types of media [3]. Images [4], [5], videos [6], sounds [7], [8], and written words or text [9] [10] are all different types of media [11]. Steganography is the art of embedding a secret message within a carrier medium that can be used to dechiper the hidden messages[12], [13], [14]. Both steganography and cryptography are methods that can be used to insert secret messages throughout many forms of media [11],

[15]. The LSB technique operates on the premise that the bit containing a secret message is substituted for the bit that is the image's last bit. Image steganography additionally makes advantage of the RGB colour components in the image because of the RGB component's strengths in digital image processing.

By using the LSB method, the author investigated the RGB image's constituent parts. According to the findings of the survey, there have been 54 articles published in the field of steganography. The number of image steganography studies that using the LSB approach is displayed in the following figure. Some of these studies make use of the LSB method on RGB image components. The LSB method is basically the simplest secret message insertion method among all methods of message insertion in steganography. Therefore, most studies use this method differently than the easy-to-use algorithms. The pseudocode for the LSB procedure algorithm is shown below.

```
Input: text, carrier image
Output: stego-image
def data to binary:
        if type data == string:
                format to binary
        return to the process until it's done converted to binary
encode:
        define the secret key, then
        for pixel in value :
        pixel[x]=data to binary + insert binary message into it's own backmost bit in the image component,
        then
        update pixel values
        return to image
decode:
        input the stego-image
        for readable data in all bytes:
                read all bytes and find readable data
                if readable data is found, then
                break
        return to readable data
end
```

Research on image steganography using the LSB approach was popular in 2019, with six publications publishing it. However, research on steganography utilizing RGB picture components is rarely mentioned, as shown in Figure 1. The author proposes another breakthrough in inserting the message into image bits. Specifically changing from the 7^{th} bit until the 0 bit on the image, especially on the RGB image component with secret message bits.

2. RELATED WORK AND METHODOLOGY

A. Previous research

Research conducted by Aditya Kumar Sahu and Gandharba Swain [16] uses the rightmost bit modification in image steganography, which aims to increase Peak Signal Noise Ratio (PSNR), increase Embedding Capacity (EC), avoid Fall of Boundary Problem (FOPB), and resistance to salt and pepper noise and RS attack.

Mohammed Mahdi Hashem [17] carried out some research with the intention of reviewing image steganography in various spatial domains. In his research, he covers many approaches of image steganography, both geographically and transforms domain, and then compares the findings of several research projects. This research gives comparison results from the work of various other researchers who have come before it regarding the level of security, capacity, and hidden secret message level.

An overview of nomeclature and taxonomy of hidden insertion patterns was provided bu Luca Cavinglione [18]. The previous taxonomy was altered as a result of this study, which produced tools for all steganographic domains, made the dictinctions between embedding processes more explicit, and produced representaions of concealed data patterns.

Osama F. Abdel Wahab [19] conducted research on the steganographic method, which involves concealing secret messages within a picture through the use of a compression algorithm. His investigation makes use of two approaches: the first involves using the LSB technique to the secret message without first encrypting it, and the second involves applying the LBS technique to the secret message after it has been

encrypted. After that, MSE and PSNR were computed in order to do a comparison between the two approaches.

Xiaoli Huan's research [20] describes the adaptation of a new approach to the LSB method. This new methodology makes use of user selection of seeds in the original image to avoid detection in smooth or flat portions of the image. This study comes to the conclusion that the method that was utilized has good visual quality as demonstrated by the results from PSNR, which are greater than the PSNR cover image.

A steganographic study using the RSA cryptosystem to encode messages for extra security was conducted by Ismael Martinez [21]. This method is converting a text into a bit array and stored in an RGB layer on the image. The result of this study is that re-encryption is indepedent of the carrier image.

Paper by Sara Farrag and Wassim Alexan [22] study about double layer secure message scheme were the initial step is to encrypt using DES, CAST5 or BlowFish, then the second stage is encrypted data is hidden in the carrier image using LSB method. The result of this study is the measurement of the MSE, PSNR, and SSIM values from the image which contains a secret message.

Mirza Abdur Razzaq [23] research on encryption, steganography and watermarking techniques using mixed security. The encryption used in this study is the XOR encryption technique and the LSB method, then the image is watermarked.

A new spatial domain-based steganography method was proposed by Marwa M. Emam [24] by randomizing the secret message and embedding it in the pixels of the cover image using a Pseudo Random Number Generation (PNRG). The result of this method is calculation using Maximum Noise Capacity and PSNR on the image that contains a secret message.

A new method developed by Joyshree Nath [25] uses an algorithm proposed by Nath et al [26] to generate a new randomization method in text encryption. This method produces an algorithm that can detemine the randomization number and encryption number from the provided text key to create the safest possible watermarking encryption method.

B. Basic Theory

Steganography is a topic of study that focuses on the practice of hiding communications to prevent unathorized parties from intercepting them [27]. Steganography is a subfield of cryptography. Cryptography, on the other hand, is a method for concealing the transmission of a message by enlisting the assistance of ciphers and dechiperers in order to decipher the hidden information [28].

Steganography word come from the Greek language *steganos,* which means "hidden", and *graphien* is "writing". It can conclude that steganography is the "writing of the hidden message". Steganography can be used on digital media such as video, images, sound, and text. The core concept of steganography is hiding secret messages on media so that the third person does not know that the media contains a secret message. This research focuses on image steganography embedded in RGB image components. There are several colour components in the image, specifically will be explained below.

- Red, Green, Blue (RGB): this is the primary colour on the monitor screen. RGB is produced from monitor light and is an "Additive Color System" [29], meaning the more colours combined, the higher it's intensity.
- Cyan, Magenta, Yellow, Black (CMYK): on the colour component, CMYK is often used in printing because CMYK is a " Subtractive Color Model" [30], which means the more colours are combined and the higher it's intensity, the less light intensity is produced. CMYK has a more opaque intensity than RGB. So when combining colors with the same intensity, it will approach to black.
- Hue, Saturation, Value (HSV): this component is more directed to the dark and light settings in the image. The concept of HSV is that the higher the saturation level, the pure colour will be, whereas if the saturation is slight, it will approach to grey [30].

The explanation above shows that the RGB colour component produces the best colour on the monitor screen [29]. This study takes the RGB image component because it is brighter in intensity than CMYK and HSV, thus allowing the image that contains a secret message to be unknown with third parties because it is similar to the carrier image. The intensity comparison between the carrier image and the image that contains a secret message (stego-image) can be calculated using a mathematics formula, with the formula:

- Mean Square Error (MSE)

  MSE measures the average squared error most often used in image quality measurement metrics. In digital image processing, especially in image steganography, MSE is used to compare the average squared error value between the carrier image and the image that contains a secret message. If the value of MSE is closer to 0, the better it's value. MSE formula is explained below [31], [32]:

$$MSE = \frac{1}{MN}\sum_{X=0}^{M}\sum_{Y=1}^{N}\left[C(x,y) - \hat{C}(x,y)\right]^2 \quad (1)$$

Where,
X and Y = image coordinates
M and N = dimensions of the images
$\hat{C}(x,y)$ = image that contains a secret message (stego-image)
C(x,y) = carrier image

- Peak Signal Noise Ratio (PSNR)

PSNR is used to compare the image quality of a carrier image with an image that contains a secret message; the more excellent PSNR value produced, the more better image quality values, the more similar stego-image with the carrier image [33]. PSNR is measured in dB (decibel) [31].

$$PSNR = 10log(10)\left(\frac{MAXVAL^2}{MSE}\right) \quad (2)$$

Where,
PSNR = Peak Signal Noise Ratio (dB)
MAXVAL = maximum value in pixel, where is 255 [34]

- Root Mean Square Error (RMSE)

RMSE is the measure square root of MSE, which means the calculation rate is more accurate than MSE [14]; the smaller the RMSE value, the more accurate it's calculation.

$$RMSE = \sqrt{MSE} \quad (3)$$

Where,
RMSE = Root Mean Square Error
MSE = Mean Square Error

- Structural Similarity Index Metric (SSIM)

SSIM is a calculation method to compare the similarity of two images; in this method, image degredation can cause changes in perception. SSIM in calculation method has several factors, for example, luminance masking, contrast masking, and others [31].

$$SSIM = \frac{(2\mu X\mu Y+c1)(2\sigma XY+c2)}{(\mu X+\mu Y+C1)(\mu X^2+\mu Y^2+C2)} \quad (4)$$

Where,
μ, σ = standard deviation original image X and the image contains secret message Y
XY = covariance from X and Y
C1 and C2 = constants to prevent numerical instability [32]

C. Methodology

In general, the approaches of image steganography involve a core process that is referred to as embedding and decoding. Decoding is the act of reading secret messages that have been embedded into the media, whereas embedding is the process of inserting a hidden message inside the media. Embedding is the procedure that inserts a secret message.

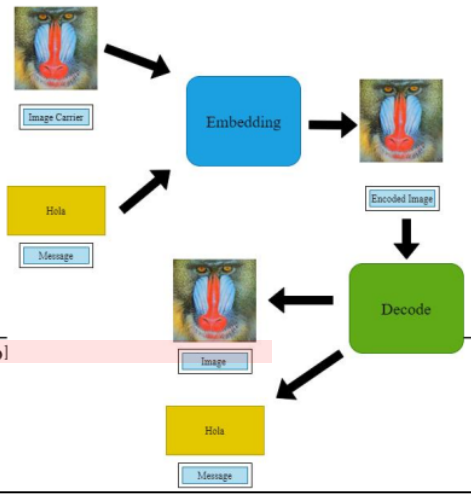

Figure 2. Image Steganography Process

Figure 2 explains the flow of embedding and reading messages in image steganography [35]. image steganography has an image media called carrier image and text. The text is a secret message which will later be embedded into the carrier image. The output of the embedding process will release an image that contains a secret message inside. The most popular method of messsage embedding nowadays is a method that inserts a message on the least significant bit or LSB. The LSB embedding process will explain in figure 3.

Figure 3. LSB Embedding Method

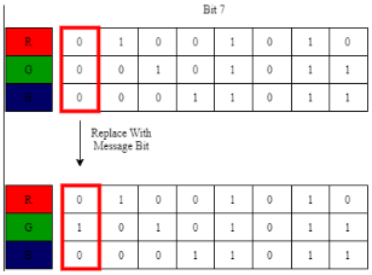

Figure 4. Modification in 7th bit

The LSB method is characteristic of inserting messages into the last bit [36]. This method is often used because it is considered simple enough to insert messages. Many people use it in steganography.

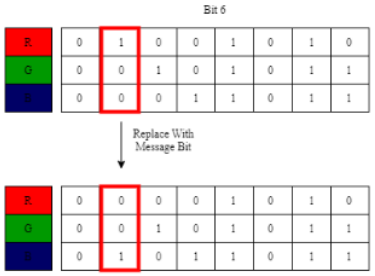

Figure 5. Modification in 6th bit

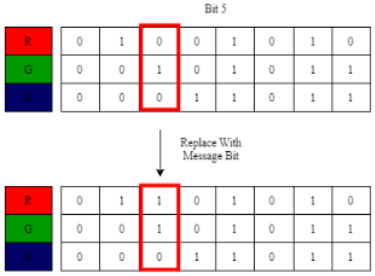

Figure 6. Modification in 5th bit

Figure 7. Modification in 4th bit

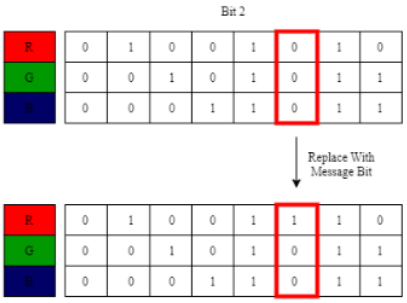

Figure 8. Modification in 3rd bit

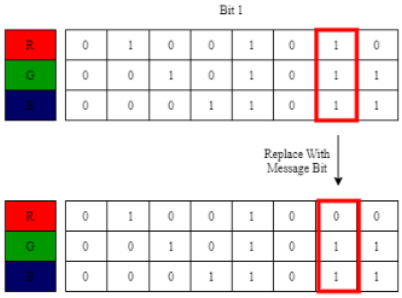

Figure 9. Modification in 2nd bit

Figure 10. Modification in 1st bit

Figure 11. Modification in 0 bit

The basis research is to use the LSB method, and then we proposes a new insertion technique by modifying LSB method by moving the message insertion from 7th bit until the 0 bit. The following LSB modification method is described in figure 4.

The 7th bit is embedded with the secret message bit shown in figure 4. The following experiment is to insert a secret message bit in 6th bit of image. 6th bit is embedded with the secret message bit. After getting the image output from the 6th bit shown in figure 5, the following experiment will be repeated on the 5th bit. 5th bit is modified with the secret message bit shown in figure 6. After producing a stegano image output, an insertion experiment is carried out on the 4th bit. The 4th bit is embedded with the secret message bit shown in figure 7. The following experiment is to insert a secret message bit in 3rd bit. 3rd bit is embedded with the secret message bit described in figure 8. After getting a stegano image output, the following experiment is to insert a secret message bit into 2nd bit.

Embedding process at the 2nd bit is shown in figure 9. The following experiment is to insert a secret message at 1st bit. The 1st bit is embedded with the secret messages, shown in figure 10. The experimental method of inserting the last bit is at bit 0. Bit 0 is embedded with secret messages, shown in figure 11. The final result in this method is several images that have been inserted messages from 7th bit until 0 bit, then calculated MSE, PSNR, RMSE and SSIM, which will later determine which bit insertion is close to the original image (carrier image).

3. RESULTS AND ANALYSIS

The end result of this work is to produce 24 images from 3 carrier images with hidden secret messages. To achieve the best outcomes, a methodologycal approach is applied.

A) Determination of Carrier Image

The carrier image used in this research uses three images, that is baboon.png [37], plane.png [38], and mosque.png [39].

Figure 12. The Carrier Image

Figure 12 is a carrier image to be used in this study. The three pictures are all inserted with a secret message that reads "hola".

B) Initial Process

An initial process to embed secret messages on the three carrier images was mentioned in figure 4 until figure 11. Each image carrier produces eight images containing a secret message inserted in each bit (7th bit until 0 bit) so that the output image containing secret message insertion is 24 images, after obtaining 24 stego images, the next step is calculating the MSE, RMSE, PSNR and SSIM formulas in order to compare the similarity from carrier images.

The best value of baboon image on baboon_bit4.png over the eight baboon images shown in table 1. Baboon_bit4.png have 52.75 on PSNR value, 0.344 MSE value, 0.0042 RMSE value and 0.999978 of SSIM value. The next table will describe value on plane image. Plane image have a best value on plane_bit6.png which have a PSNR value is 62.47, MSE is 0.036, RMSE is 0.011 and SSIM value is 0.999993. Next table is describing value of MSE, PSNR, RMSE and SSIM of mosque image.

The best value on mosque image is in mosque_bit6.png which is embedding secret message on the 6th bit with PSNR value is 57.61, MSE 0.112, RMSE 0.0019 and SSIM 0.999986.

MSE, PSNR, RMSE and SSIM calculations show that all images embedded with a secret message get closer to the carrier image, whereas MSE and RMSE are getting closer to 0. The PSNR of all images is above 30 dB, while the SSIM value of all images is close to 1.

In this section, the research findings are discussed while also providing a through discussion. Results can be shown in tables, graphs, figures, and other formats that are simple for the reader to interpret [14], [15]. There are various ways to break up the topic.

Table 1. Calculation Value of Baboon Image

Figure	MSE	PSNR	RMSE	SSIM
Baboon_bit7.png	0.668228	49.881555	0.005907	0.999972
Baboon_bit6.png	0.537043	50.830710	0.005295	0.999975
Baboon_bit5.png	0.416112	51.938698	0.004661	0.999978
Baboon_bit4.png	0.344904	52.753813	0.004244	0.999978
Baboon_bit3.png	0.387181	52.251656	0.004496	0.999976
Baboon_bit2.png	0.350458	52.684434	0.004278	0.999976
Baboon_bit1.png	0.512710	51.032080	0.005174	0.999972
Baboon_bit0.png	0.563878	50.618949	0.005426	0.999970

Table 2. Calculation Value of Plane Image

Figure	MSE	PSNR	RMSE	SSIM
Plane_bit7.png	0.079411	59.131948	0.001686	0.999993
Plane_bit6.png	0.036737	62.479712	0.001146	0.999994
Plane_bit5.png	0.047603	61.354402	0.001305	0.999994
Plane_bit4.png	0.068743	59.758501	0.001568	0.999993
Plane_bit3.png	0.076416	59.298906	0.001654	0.999993
Plane_bit2.png	0.093735	58.411763	0.001832	0.999993
Plane_bit1.png	0.163304	56.000814	0.002418	0.999993

Plane_bit0.png	0.173980	55.725806	0.002495	0.999993

Table 3. Calculation Value of Mosque Image

Figure	MSE	PSNR	RMSE	SSIM
Mosque_bit7.png	0.140382	56.657658	0.002227	0.999987
Mosque_bit6.png	0.112649	57.613505	0.001995	0.999986
Mosque_bit5.png	0.158205	56.138595	0.002364	0.999985
Mosque_bit4.png	0.206538	54.980792	0.002701	0.999984
Mosque_bit3.png	0.204838	55.016686	0.002690	0.999984
Mosque_bit2.png	0.360032	52.567380	0.003567	0.999984
Mosque_bit1.png	0.581560	50.484852	0.004533	0.999983
Mosque_bit0.png	0.610727	50.272329	0.004646	0.999983

Badshah in his research, stated that if the PSNR value is below than 30 dB, the image can not be used for further analysis because it does not approach the carrier image. If the image has a PSNR value above 30 dB, it will approach with the carrier image similarity [21]. Based on the baboon image, the best result of embedding the message are into the 4th bit, while the plane and mosque are both at the 6th bit. If the SSIM index value is close to 1, then stego-image is almost similar to the carrier image [40], while for the MSE and RMSE values, the smaller it's value or close to 0, the better it's result [41], [42].

C) Physically Comparison of Carrier Image and Stego-Image

However, the top three stego-images with the best result of MSE, PSNR, RMSE and SSIM values get result that are close to the carrier image is on plane_bit6.png image, so that there is almost no difference in physical resemblance with the carrier image. The image containing a secret message and the original image (carrier image), which has the best value of MSE, PSNR, RMSE and SSIM, can be seen in figure 12.

Figure 12. Carrier Image (left) and Stego-Image (right)

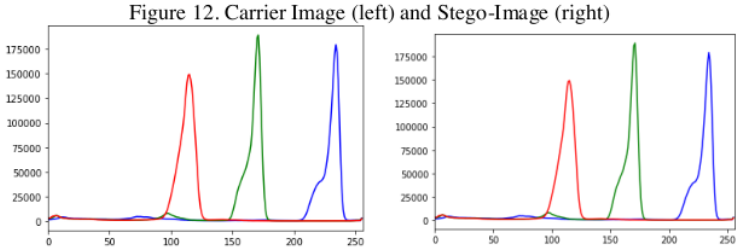

Figure 13. Histogram of Carrier Image (left) and Stego-Image (right)

Figure 13 displays a histogram graph of the plane.png as a carrier image and plane_bit6.png image that is embedded with a secret message at bit 6. It is clear from this graph that there is no appreciable difference between the two images.

4. CONCLUSION AND FUTURE WORK

In this paper, we propose a new embedding technique for image steganography. The experimental technique used in this study is to insert a secret message from the leftmost bit (bit 7) to the rightmost bit (bit 0) using three sample images: baboon, plane, and mosque. The three sample images produce24 images that already contain a secret message, then we calculate MSE, PSNR, RMSE and SSIM calculations to find out which bit insertion method has the best calculation results. The best calculation results are in the plane image inserted with the secret message at bit 6. We also compare the physical shape of the plane image and use

histograms to determine whether there is a difference between the carrier image and the stego-image with no result visible difference.

Further research is suggested to conduct a noise test on image inserted with secret messages using our proposed method, then calculate it with MSE, PSNR, RMSE and SSIM formula as a reference for comparison of result to get the best insertion of embedding a message.

REFERENCES

[1] A. Sajid Ansari, M. Sajid Mohammadi, and M. Tanvir Parvez, "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 1, pp. 11–25, 2019, doi: 10.5815/ijcnis.2019.01.02.

[2] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, no. February, pp. 92–102, 2019, doi: 10.1016/j.optlastec.2019.03.005.

[3] M. Garg, "A Novel Text Steganography Technique Based on Html Documents," *Int. J. Adv. Sci. Technol.*, vol. 35, pp. 129–138, 2011.

[4] X. Li, W. Zhang, B. Ou, and B. Yang, "A brief review on reversible data hiding: Current techniques and future prospects," *2014 IEEE China Summit Int. Conf. Signal Inf. Process. IEEE ChinaSIP 2014 - Proc.*, pp. 426–430, 2014, doi: 10.1109/ChinaSIP.2014.6889278.

[5] B. J. Mohd, S. Abed, B. Na'ami, and T. Hayajneh, "Hierarchical steganography using novel optimum quantization technique," *Signal, Image Video Process.*, vol. 7, no. 6, pp. 1029–1040, 2013, doi: 10.1007/s11760-012-0301-9.

[6] M. Marsaline Beno, A. George, I. R. Valarmathi, and S. M. Swamy, "Hybrid optimization model of video steganography technique with the aid of biorthogonal wavelet transform," *J. Theor. Appl. Inf. Technol.*, vol. 63, no. 1, pp. 190–199, 2014.

[7] P. Pathak, A. K. Chattopadhyay, and A. Nag, "A new audio steganography scheme based on location selection with enhanced security," *1st Int. Conf. Autom. Control. Energy Syst. - 2014, ACES 2014*, pp. 1–4, 2014, doi: 10.1109/ACES.2014.6807979.

[8] M. Tayel, A. Gamal, and H. Shawky, "A proposed implementation method of an audio steganography technique," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2016-March, no. 3, pp. 180–184, 2016, doi: 10.1109/ICACT.2016.7423320.

[9] A. Odeh, K. Elleithy, and M. Faezipour, "Steganography in text by using MS word symbols," *Proc. 2014 Zo. 1 Conf. Am. Soc. Eng. Educ. - "Engineering Educ. Ind. Involv. Interdiscip. Trends", ASEE Zo. 1 2014*, no. April, 2014, doi: 10.1109/ASEEZone1.2014.6820635.

[10] S. Sharma, A. Gupta, M. C. Trivedi, and V. K. Yadav, "Analysis of different text steganography techniques: A survey," *Proc. - 2016 2nd Int. Conf. Comput. Intell. Commun. Technol. CICT 2016*, pp. 130–133, 2016, doi: 10.1109/CICT.2016.34.

[11] A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," *Proc. 2015 IEEE Int. Conf. Electr. Comput. Commun. Technol. ICECCT 2015*, pp. 1–4, 2015, doi: 10.1109/ICECCT.2015.7226122.

[12] F. Akhter and M. Selim, "A New Approach of Graph Realization for Data Hiding using Human Encoding," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 12, 2016, doi: 10.14569/ijacsa.2016.071256.

[13] T. Anwar, S. Paul, and S. K. Singh, "Message transmission based on DNA cryptography: Review," *Int. J. Bio-Science Bio-Technology*, vol. 6, no. 5, pp. 215–222, 2014, doi: 10.14257/ijbsbt.2014.6.5.22.

[14] M. Cui and Y. Zhang, "Incorporating Randomness into DNA Steganography to Realize Secondary Secret key, Self-destruction, and Quantum Key Distribution-like Function," *bioRxiv*, p. 725499, 2019, [Online]. Available: http://biorxiv.org/content/early/2019/08/05/725499.abstract

[15] S. Alam, S. M. Zakariya, and M. Q. Rafiq, "Analysis of modified lsb approaches of hiding information in digital images," *Proc. - 5th Int. Conf. Comput. Intell. Commun. Networks, CICN 2013*, pp. 280–285, 2013, doi: 10.1109/CICN.2013.66.

[16] A. K. Sahu and G. Swain, "A Novel n-Rightmost Bit Replacement Image Steganography Technique," *3D Res.*, vol. 10, no. 1, 2019, doi: 10.1007/s13319-018-0211-x.

[17] M. M. Hashim, M. S. Mohd Rahim, and A. A. Alwan, "A review and open issues of multifarious image steganography techniques in spatial domain," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 4, pp. 956–977, 2018.

[18] S. Wendzel *et al.*, "A Revised Taxonomy of Steganography Embedding Patterns," *ACM Int. Conf. Proceeding Ser.*, no. Ares, 2021, doi: 10.1145/3465481.3470069.

[19] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 3, pp. 1168–1175, 2019, doi: 10.12928/TELKOMNIKA.V17I3.12230.

[20] X. Huan, H. Zhou, and J. Zhong, "LSB based image steganography by using the fast marching method," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 3, pp. 1–5, 2019, doi: 10.14569/IJACSA.2019.0100301.

[21] I. Martmez, W. Fuertes, M. Palacios, D. Escudero, and T. Noboa, "RSA Over-Encryption Employing RGB Channels through a Steganography Variant," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 11, no. 4, pp. 1432–1439, 2021, doi: 10.18517/ijaseit.11.4.13728.

[22] S. Farrag and W. Alexan, "Secure 2D image steganography using recamán's sequence," *Proc. - 2019 Int. Conf. Adv. Commun. Technol. Networking, CommNet 2019*, pp. 1–6, 2019, doi: 10.1109/COMMNET.2019.8742368.

[23] M. Abdur, R. Ahmed, M. Adnan, and A. Ahmed, "Digital Image Security: Fusion of Encryption, Steganography and Watermarking," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 5, pp. 224–228, 2017, doi: 10.14569/ijacsa.2017.080528.

[24] M. M., A. A., and F. A., "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 3, pp. 361–366, 2016, doi: 10.14569/ijacsa.2016.070350.

[25] J. Nath and A. Nath, "Advanced Steganography Algorithm using Encrypted secret message," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 3, 2011, doi: 10.14569/ijacsa.2011.020304.

[26] C. Paper and A. N. St, "Symmetric Key Cryptography Using Random Key Symmetric key cryptography using Random key generator," no. November, 2015.

[27] A. Seif and W. Alexan, "A High Capacity Gray Code Based Security Scheme for Non-Redundant Data Embedding," *Proc. 2020 Int. Conf. Innov. Trends Commun. Comput. Eng. ITCE 2020*, no. February, pp. 130–136, 2020, doi: 10.1109/ITCE48509.2020.9047755.

[28] N. Sakib, A. Hira, M. N. Mollah, S. M. Sharun, S. B. Mohamed, and M. A. Rashid, "SNR improvement and bandwidth optimization technique using PCM-DSSS encryption scheme," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 5, pp. 638–643, 2016, doi: 10.18517/ijaseit.6.5.921.

[29] D. T. Joy, G. Kaur, A. Chugh, and S. B. Bajaj, "Computer Vision for Color Detection," *Int. J. Innov. Res. Comput. Sci. Technol.*, vol. 9, no. 3, pp. 53–59, 2021, doi: 10.21276/ijircst.2021.9.3.9.

[30] N. Phuangsaijai, J. Jakmunee, and S. Kittiwachana, "Investigation into the predictive performance of colorimetric sensor strips using RGB, CMYK, HSV, and CIELAB coupled with various data preprocessing methods: a case study on an analysis of water quality parameters," *J. Anal. Sci. Technol.*, vol. 12, no. 1, 2021, doi: 10.1186/s40543-021-00271-9.

[31] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *J. Comput. Commun.*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[32] J. Søgaard, L. Krasula, M. Shahid, D. Temel, K. Brunnström, and M. Razaak, "Applicability of existing objective metrics of perceptual quality for adaptive video streaming," *IS T Int. Symp. Electron. Imaging Sci. Technol.*, 2016, doi: 10.2352/ISSN.2470-1173.2016.13.IQSP-206.

[33] R. Hassan, S. Kasim, W. A. Z. W. C. Jafery, and Z. A. Shah, "Image enhancement technique at different distance for Iris recognition," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 7, no. 4–2 Special Issue, pp. 1510–1515, 2017, doi: 10.18517/ijaseit.7.4-2.3392.

[34] B. R. Jana, H. Thotakura, A. Baliyan, M. Sankararao, R. G. Deshmukh, and S. R. Karanam, "Pixel density based trimmed median filter for removal of noise from surface image," *Appl. Nanosci.*, no. 0123456789, 2021, doi: 10.1007/s13204-021-01950-0.

[35] M. Dalal and M. Juneja, "Steganography and Steganalysis (in digital forensics): a Cybersecurity guide," *Multimed. Tools Appl.*, vol. 80, no. 4, pp. 5723–5771, 2021, doi: 10.1007/s11042-020-09929-9.

[36] T. Bhuiyan, A. H. Sarower, M. Rashed Karim, and M. Maruf Hassan, "An image steganography algorithm using LSB replacement through XOR substitution," *2019 Int. Conf. Inf. Commun. Technol. ICOIACT 2019*, pp. 44–49, 2019, doi: 10.1109/ICOIACT46704.2019.8938486.

[37] Scijs, "No Title," *25 April*, 2017. https://github.com/scijs/baboon-image (accessed Aug. 17, 2022).

[38] Abejo, "No Title," *free plane stock photos*. https://www.freeimages.com/photo/plane-1449679 (accessed Aug. 17, 2022).

[39] Irothko, "No Title." https://www.freeimages.com/photo/singapore-mosque-1502213 (accessed Aug. 17, 2022).

[40] J. Peng *et al*., "Implementation of the structural SIMilarity (SSIM) index as a quantitative evaluation tool for dose distribution error detection," *Med. Phys.*, vol. 47, no. 4, pp. 1907–1919, 2020, doi: 10.1002/mp.14010.

[41] Z. A. Khan, T. Hussain, A. Ullah, S. Rho, M. Lee, and S. W. Baik, "Towards efficient electricity forecasting in residential and commercial buildings: A novel hybrid CNN with a LSTM-AE based framework," *Sensors (Switzerland)*, vol. 20, no. 5, pp. 1–16, 2020, doi: 10.3390/s20051399.

[42] Q. A. Al-Haija and A. Ishtaiwi, "Machine Learning Based Model to Identify Firewall Decisions to Improve Cyber-Defense," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 11, no. 4, pp. 1688–1695, 2021, doi: 10.18517/ijaseit.11.4.14608.

BIOGRAPHIES OF AUTHORS

Yenni Seftiardiyah is a college student from departement of informatics in Universitas Muhammadiyah Sidoarjo. She graduated from SMA Negeri 1 Wonoayu at 2019. She join some training certificates from Kominfo about Game, Big Data using Python, and Certified Cybersecurity Technician. Currently she is a last year student and have a research about steganography. She can be contacted at email: 191080200251@umsida.ac.id

Mochamad Alfan Rosid was born in Sidoarjo, 25 April 1986. He graduated from Muhammadiyah Sidoarjo University in 2010. The writer continued his undergraduate studies at the Prodi Information Technology Graduate Program of Surabaya Technical High School graduating in 2014 with an M. Kom. Currently, the author is studying further in ITS Computer Science study program. The writer began his career as a lecturer at the Muhammadiyah Sidoarjo University Informatics Engineering. Authors are also actively involved in research activities and community service. Research that has been done by authors has been on information systems, databases, and decision-making systems. In addition to education and teaching, writers are also involved in research and service activities to the community, both funded by the Ristekdikti and self-funded funds. Writers are also active in participating in academic support activities such as seminars, workshops/ workshops, training sessions, and other activities. He can be contacted at email: alfanrosid@umsida.ac.id

Sukma Aji is a Ph.D student from Universiti Tun Hussein Onn Malaysia with his research about Digital Forensics for DDOS Attack. On 2018 May has a Master in Informatics on Universitas Ahmad Dahlan with his research about Gaussian Naive Bayes Based DDOS Detection. He graduated as a Bachelor in Electrical Engineering at Universitas Ahmad Dahlan with his research about Microcontroller System. Also he join a converence about "pengamanan jaringan menggunakan sistem berbasis mikrokontroller berdasarkan analisis forensik jaringan" on May, 28-29 2016. He can be contacted at email: sukmaaji@umsida.ac.id

Cek Plagiasi Yenni

ORIGINALITY REPORT

6%	6%	5%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universiti Teknikal Malaysia Melaka Student Paper	4%
2	dokumen.pub Internet Source	1%
3	Lecture Notes in Computer Science, 2009. Publication	1%
4	insightsociety.org Internet Source	1%
5	www.researchgate.net Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		