Journal of Theoretical and Applied Information Technology
15th September 2022. Vol.100. No 17
© 2022 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPROVING SECURITY AND IMPERCEPTIBILITY USING MODIFIED LEAST SIGNIFICANT BIT AND FERNET SYMMETRIC ENCRYPTION

EZRA KARUNA WIJAYA[1], RICO KUMALA[2], BENFANO SOEWITO[3]

[1,2,3]Computer Science Department, BINUS Graduate Program – Master of Computer Science Bina Nusantara University, Jakarta 11480, Indonesia

Email: [1]ezra.wijaya@binus.ac.id, [2]rico.kumala@binus.ac.id, [3]bsoewito@binus.edu

ABSTRACT

In our daily life in this digital era, information has become essential. Along with the development of technology and the importance of information, digital crimes such as theft of information also develop. One way to protect information is with steganography. Steganography is a technique to insert secret data or secret messages into an image. In this paper, we will modify the Least Significant Bit method so that the secret message will only be entered into one color bit and combine our proposed Least Significant Bit method with cryptography to improve the security and quality of the holding image. The cryptography technique that we will use is fernet symmetric encryption. In this study, we use the Python programming language. From the results of our research, the quality of the holding image increases for the better. We can express this based on the average PSNR value for each image which increases by 0.1% and decreases from the average MSE value, 2.1%. By implementing our proposed method we are able to improve security and imperceptibility proved by the RGB histogram which is very similar to the original images RGB histogram.

Keywords:- *Steganography, Cryptography, Least Significant Bit, Fernet Symmetric Encryption, PSNR, MSE*

1. INTRODUCTION

1.1 Background

Information has become essential in our daily lives in this digital era. Information is a valuable commodity and has many electronic and physical forms such as paper, electronics, video, audio, sound, and knowledge [1]. Information is essential because, in the digital world, everything we want to do requires information. There is public information that many people can know and confidential information that can be crucial if others know it. We reside within the information age, wherein information is becoming more crucial. Nobody denies that information and understanding are crucial properties that want to be included from unauthorized customers along with hackers, phishers, social engineers, viruses, and worms that threaten groups on all sides via the intranet, extranet, and the internet [2].

Due to the development of information and organizations starting to use the internet, information security incidents are also getting higher, especially data breaches [3]. Theft of data or information can be categorized as a crime because it has a detrimental impact on the victim or the party whose information is stolen. Much information can be classified as confidential information, such as personal data, company data, messages between individuals, or countries. In 2019 there were several cases of data theft, namely against Microsoft Office 365, Box, EE, Mumsnet, Town of Salem, and even German politicians experienced data theft [4]. The victim can feel the negative impact if the data theft occurs, whether the data is personal or public data, one of which is taking over the account owned by the victim, such as email. Attackers can also use the victim's information to do something unwanted, such as making an online loan with the information that has been obtained [5]. Therefore, information security has become paramount in this digital era.

There are various ways to protect information. One way that can be used to preserve crucial information is to use cryptographic methods. Cryptography is the method used so that the message we want to send, whatever its form, is manipulated to ensure that the message sent is only understood by the recipient of the message [6]. Cryptography results can lead to suspicion by those who want to take our data so that because of this suspicion arises the desire to translate the encryption results. So, to avoid this, we want to use the steganography method. Steganography is a method to hide data or information into other information [7]. We use steganography to hide data or information encrypted into an image. That way, we will avoid suspicion or curiosity of parties who want to take our data.

The current Least Significant Bit technique still has shortcomings. One of the drawbacks of this technique is that it does not yet have a high level of security [8]. Secret messages or hidden files in the image are easy to hack and extract by outsiders or parties who do not have the authorization to do that. So, according to Al-Azzeh, Alqadi, Ayyoub, and Sharadqh [8], steganography techniques can be improved by combining these techniques with cryptography techniques, namely by encrypting the holding image or images that have inserted information. In this paper, we want to apply the encryption technique, not to the holding image or image that has information inserted, but to confidential data, before it is stored in the cover image because, in our opinion, if the holding image or image has encrypted information inserted, then the essence of steganography that is avoiding suspicion will disappear. We also want to research using standard images commonly used for research with the same image size. In this study, we also propose the Least Significant Bit (LSB) method by entering a secret message into only one-color bit because the quality of the holding image can be increased with this method.

1.2 Problem Formulation

- How to develop Least Significant Bit in steganography technique?
- Does the combined method of steganography and cryptography improve security for images?
- Can the image quality of the Least Significant Bit process be improved?

1.3 Research Purposes

- Develop Least Significant Bit in steganography technique.
- Knowing the security level of the combined steganography and cryptography method against colorful, grayscale, and not too colorful images.
- Improve the image quality of the Least Significant Bit process.

1.4 Scope of Research

- The data to be encrypted is in the form of text
- Using standard images that are colorful, grayscale, and not too colorful
- The image file used is in PNG format
- The PNG images used are the same size
- Develop standard LSB method
- Using Fernet Symmetric Encryption

2. LITERATURE REVIEW

2.1 Steganography

Steganography is a method that we can use in digital object communication so that certain object communications can store and hide confidential data or information [9]. Steganography techniques can be implemented in various types of communication, such as hiding secret data across multiple file types containing text, images, and audio without changing the structure and content of the original data [10]. Steganography has many benefits, both benefits that can benefit many people. Irresponsible people can misuse steganography. For example, terrorist groups can use steganography to communicate [11]. According to Susilo [11], steganography can be used to send confidential data so as not to be known by unwanted parties, provide a watermark on an image to give a copyright mark to the image, and can be used as a substitute for a hash.

Steganography four essential properties must be possessed in a steganography system, namely as follows [12]:

- Imperceptibility
  Imperceptibility is one of the essential properties that must be applied in steganography. The purpose of these properties is to make unwanted parties or other people know that the carrier or holding image contains confidential information that has been inserted or hidden in it. If these properties are not

applied, the essence of steganography that intends to hide data that is unknown to other parties will disappear.

- Security
  Security has always been one of the essential things everywhere. With a low level of security, confidential information that has been inserted in the carrier or holding image will be easily detected, and the information can be easily extracted and known by unwanted parties.
- Robustness
  Robustness means that confidential information hidden in the carrier or holding image must withstand various manipulation processes on the data carrier or holding image.
- Capacity
  Capacity is also essential in a steganography system because the capacity is directly related to the size of data or confidential information inserted into the carrier or holding image.

These four properties are the most influential parameters that can determine the effectiveness of a steganography system. In image steganography, the carrier file is an image, or it can also be called a holding image. In this study, we want to focus on traits number 1 and 2, namely imperceptibility and security.

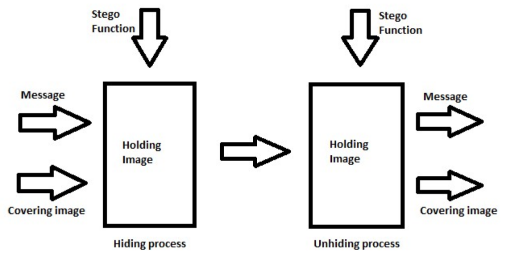


Figure 1. Steganography Process

Figure 1 shows how a process of steganography is carried out in general. In the image in hiding, the cover image and the message that will be inserted are combined, and the stego function is implemented, which creates a new file in the form of a holding image where the file contains secret data in the form of a message. In the unhiding process, the holding image containing secret data will be implemented with a stego function that will separate the hidden secret data from the cover image so that the recipient of the message can receive the secret data.

2.2 Least Significant Bit

Least Significant Bit is a common technique used in encrypting and describing confidential data or information [13]. According to Kour and Verma [14], in this method, personal data or information is inserted by changing or replacing the least significant bit pixel of the carrier image or image that will be used as a holding image with bits of the confidential data or information. The carrier or holding image will look almost identical to the original image because by using the least significant bit technique, the changes in the pixels in the image are minimal and practically do not change the image.

2.3 Cryptography

Cryptography is a method for maintaining the confidentiality of information by transforming data into an unreadable format so that only the recipient who has permission can translate it [15]. Cryptography can help secure data by disguising the data into a form that ordinary people cannot read [16]. Still, it can be a double-edged sword because people who understand that it is the result of cryptography will be interested in solving the ciphertext. According to Basri [17], the cryptographic method has many techniques. The plaintext is information or data that has not been disguised, while information that has been hidden is called ciphertext. Still, in general, it consists of two methods, namely:

- Symmetric Key

This technique uses the same key both in the encryption and decryption process. This technique is the most commonly used. So, the analogy is that the receiver and sender must have the same key. The disadvantage of this calculation is the manner by which to pass the key on to the ideal party without being known by the other party.

- Asymmetric Key

This technique uses a different key for the encryption and decryption process so that everyone who has the public key can use it for encryption. In contrast, the private key is only owned by one person so that only one person can read the message sent to him.

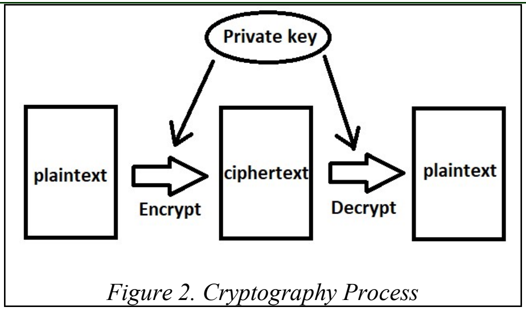


Figure 2. Cryptography Process

Figure 3 describe how the encryption process in general. Where the plaintext is converted into ciphertext using the secret key that has been provided to translate the ciphertext, a secret key is needed. The secret key is the same or different depending on the method used.

2.4 Encryption

Encryption changes the character of information or data into unreadable text or called ciphertext [18]. Encryption aims so that information or data cannot be read or translated by people who do not have permission, so data security is guaranteed.

2.5 Decryption

Decryption is the opposite of encryption, namely the process of changing characters from unreadable text or ciphertext into original information or data if the recipient has the key to translate the ciphertext [19].

2.6 Fernet Symmetric Encryption

According to Buchanan [20], fernet is one of the methods used in symmetric encryption. The key used to access or translate the data uses URL-safe encoding. The fernet method cannot be manipulated, accessed, or translated if it does not have the key used to translate. The key generated from the fernet method uses the os.random() function. So, Buchanan [20] said that fernet is one method that applies the best practice of cryptography.

3. METHODS

3.1 Flowchart

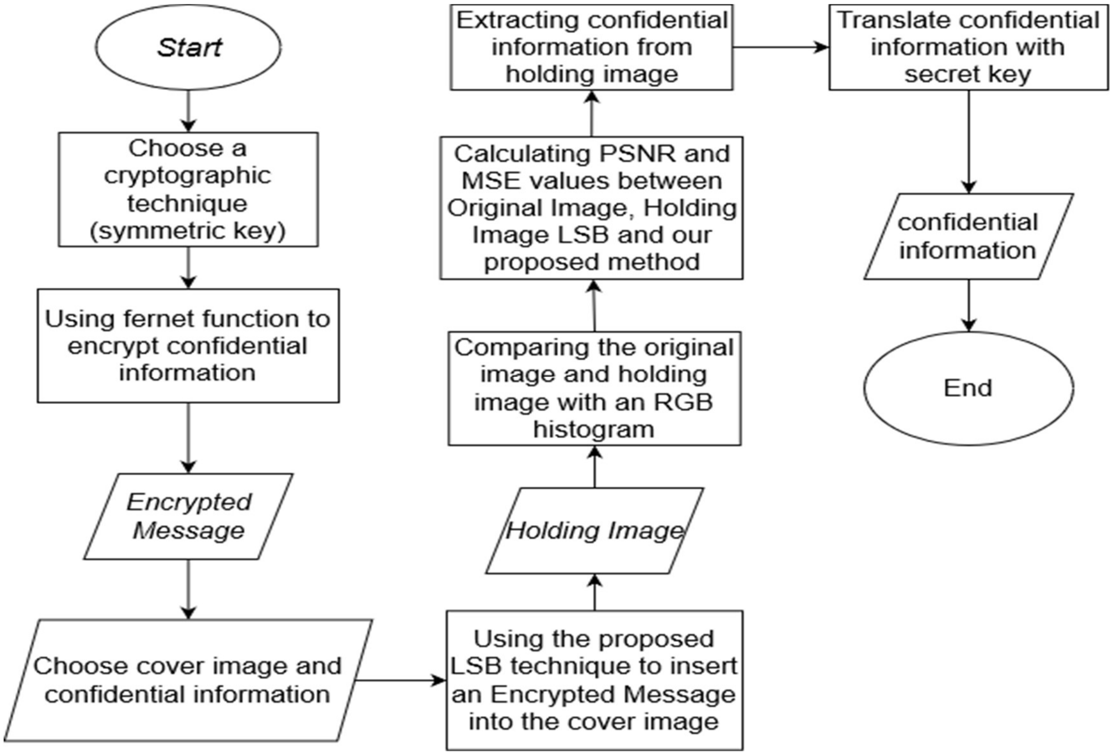

Start
Choose a cryptographic technique (symmetric key)
Using fernet function to encrypt confidential information
Encrypted Message
Choose cover image and confidential information
Using the proposed LSB technique to insert an Encrypted Message into the cover image
Holding Image
Comparing the original image and holding image with an RGB histogram
Calculating PSNR and MSE values between Original Image, Holding Image LSB and our proposed method
Extracting confidential information from holding image
Translate confidential information with secret key
confidential information
End

Figure 3. Working Method Flowchart

As seen in Figure 3, this method begins with selecting a cover image or image used as a medium where the data will be inserted. In this study, we used standard color and grayscale images. Next, we determine a cryptographic technique that uses a symmetric key. In this study, we use a fernet to perform encryption. After that, the confidential information is encrypted first before carrying out the LSB steganography method that we propose to insert an encrypted message into the cover image. After obtaining the holding image, we compared the holding image using the usual LSB method and our proposed method with a cover image with an RGB histogram. We calculated the PSNR and MSE values between the two images to evaluate whether the method we proposed was good enough or not. After that, the confidential information will be extracted from the image and re-translated to ensure no changes to the personal information

3.2 System Planning

In this research, we want to combine steganography techniques with cryptographic techniques. This study encrypts confidential information or secret messages before inserting them into the cover image. We take this step to avoid eliminating the primary purpose of steganography, which is hiding the data in the image without being noticed.

Table 1. Dataset

No.	Name	Resolution	Image
1.	Lenna_(test_image).png	512 x 512	
2.	Baboon.png	512 x 512	
3.	Lenna_grey.png	512 x 512	

3.2.1 dataset

We choose different image types to aim our proposed method for all image types. As seen in Table 1, the dataset we use is a standard image usually used for testing or research, with colorful, not too colorful, and grayscale. The image we use has a ".png" format with a size of 512x512.

3.2.2 preprocessing

The first step we took was to encrypt using Fernet symmetric encryption of the secret message we wanted to insert. Then, we re-process the encryption results by encoding the data by changing the data type from bytes to strings. After the data type has changed, we will insert the data into the cover image using the Least Significant Bit (LSB) technique which we have modified from what was previously saved to all color bits to only be saved to green bits in the python programming language.

3.2.3 output

The parameters that we will use to see the results of our research are PSNR, MSE, and RGB histogram. In collecting data for the RGB histogram, we use python programming language to get the RGB histogram. We used an RGB histogram to compare the images' color distribution before and after the secret message was inserted. In collecting PSNR and MSE data, we also use the python programming language to get the data. The input we enter in the program is the original image, and the image inserted a secret message. The purpose of using PSNR and MSE parameters is to determine whether the cover image has a good quality.

4. RESULTS

4.1 Evaluation Results

From our proposed method, by inserting the secret message bit into the green bit, we have collected and obtained the result in the parameter value that we will use to compare our method with the standard LSB method. The parameters we will use include RGB histogram, PSNR, and MSE.

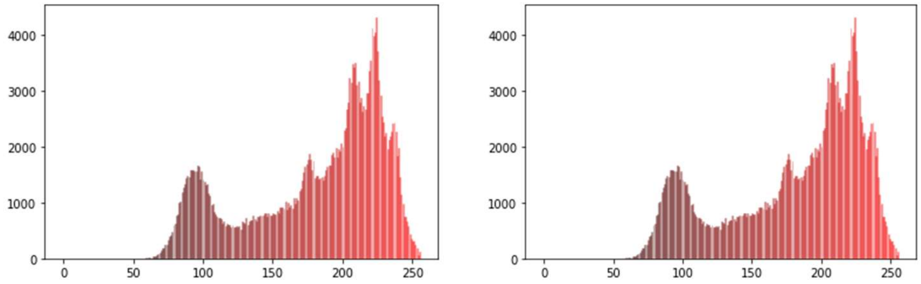
Figure 4 displays the Lenna image after the secret message has been successfully inserted into it, as can be seen, that there is no visible change when seen with the naked eye. Figures 5, 6, and 7 show the comparison between the intensity distribution of Lenna's image on the red, green, and blue channels. Figure (a) shows the original image RGB histogram, while (b) shows the holding image RGB histogram. We only entered secret messages to green channels, so the changes are only visible on the green histogram. We can also see that the green channel has the evenest intensity distribution. Figure 8 shows the Baboon image after inserting a secret message. The image still looks the same as the original image. Same as before, figure (a) shows the RGB histogram of the original image, while (b) shows the RGB histogram of the holding image. When we look at the RGB histogram in figures 9, 10, and 11, we can see the comparison between the intensity distribution of Baboon's image on the red, green, and blue channels. Because we only enter a secret message on the green channel.

Figure 12 shows the Lenna Grayscale image after inserting a secret message. It still looks like the original image if we don't compare them using a histogram. Because this image is grayscale, we decided only to use one histogram to see the intensity distribution from black and white. Same as before, figure (a) is the histogram for the original image, and figure (b) is the histogram for the holding image. Figure 13 shows the comparison between before and after the secret message is inserted into the picture. There is a change to the histogram because many image bits are replaced with secret message bits.

Table 2. Standard LSB and Green Bit Method PSNR and MSE Values

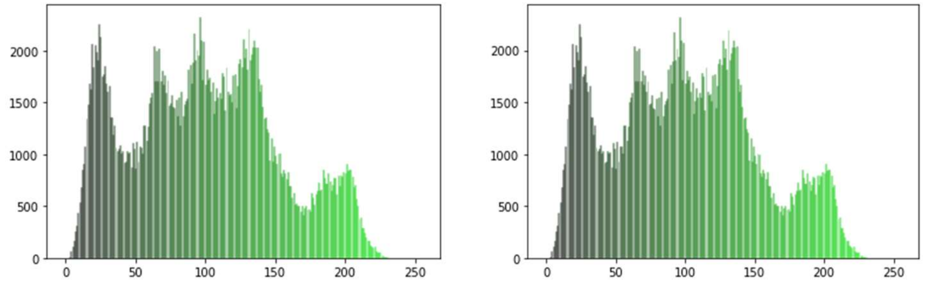
Nama	Standard LSB		Green Bit Method	
	PSNR	MSE	PSNR	MSE
Lenna_(test_image).png	79.9862 dB	0.00065	80.0288 dB	0.00064
Baboon.png	80.0373 dB	0.00064	80.2121 dB	0.00062
Lenna_grey.png	80.0977 dB	0.00064	80.1326 dB	0.00063

Figure 4. Lenna Holding Image



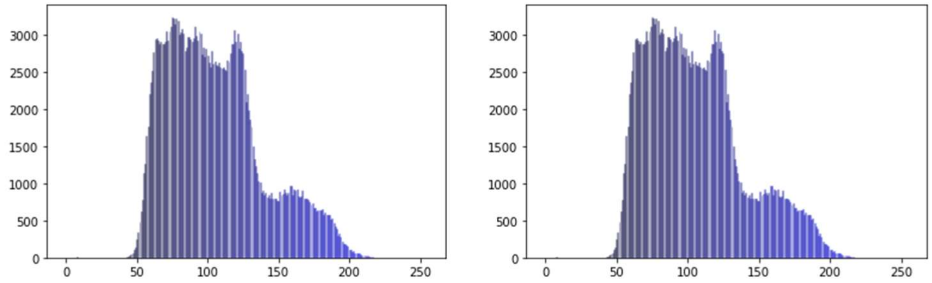
(a) *(b)*

Figure 5. Lenna's Red Histogram



(a) *(b)*

Figure 6. Lenna's Green Histogram



(a) *(b)*

Figure 7. Lenna's Blue Histogram

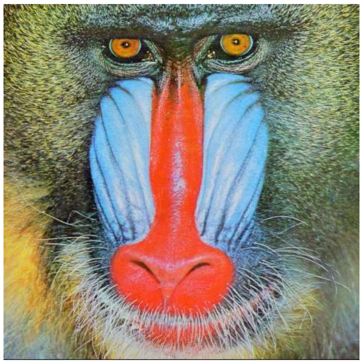
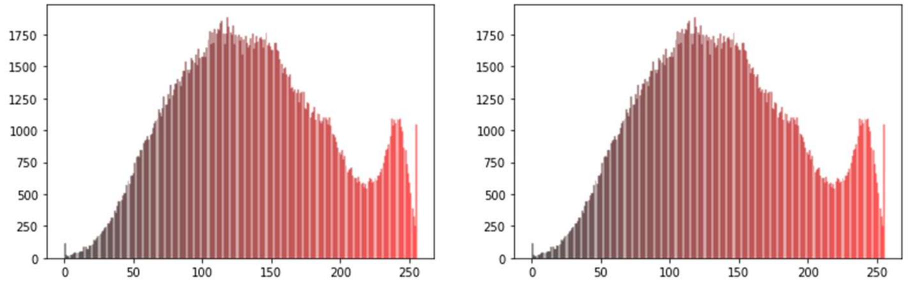
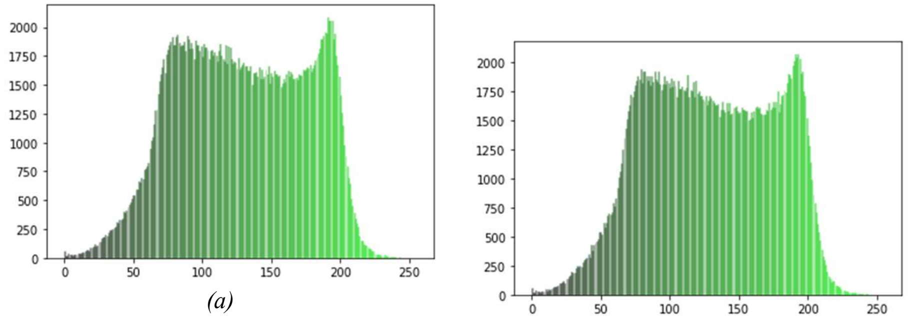


Figure 8. Baboon Holding Image



(a) *(b)*

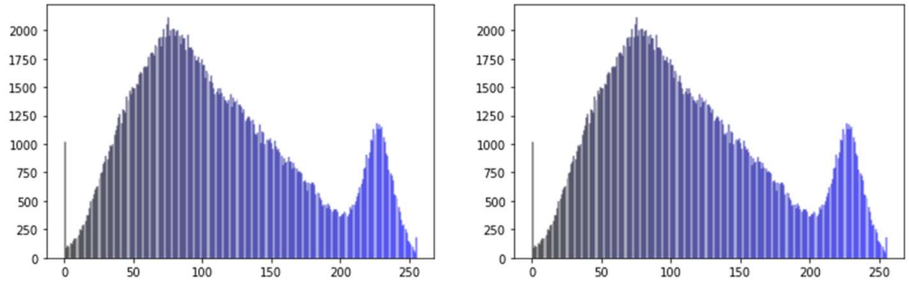
Figure 9. Baboon's Red Histogram



(a)

(b)

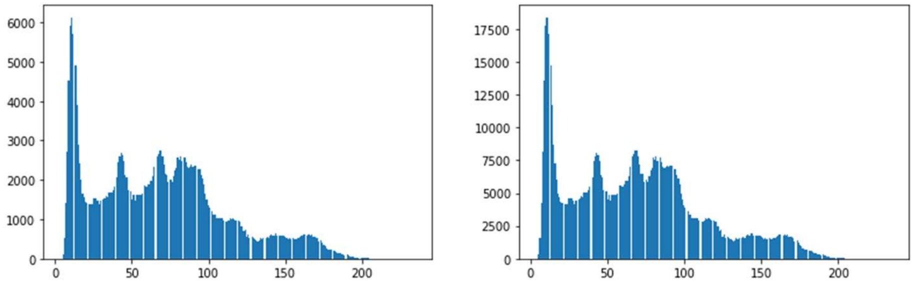
Figure 10. Baboon's Green Histogram



(a) *(b)*

Figure 11. Baboon's Blue Histogram

Figure 12. Lenna Grayscale



(a) *(b)*

Figure 13. Lenna Grayscale's Histogram

Table 3. Red and Blue Method PSNR and MSE Values

Nama	Red Bit Method		Blue Bit Method	
	PSNR	MSE	PSNR	MSE
Lenna_(test_image).png	80.0117 dB	0.00065	79.9525 dB	0.00066
Baboon.png	80.0032 dB	0.00065	80.3388 dB	0.00060
Lenna_grey.png	80.0631 dB	0.00064	80.0631 dB	0.00064

As can be seen in Table 2, the results of our research show that our proposed method of inserting the secret message bit into the green bit has better PSNR and MSE values with an average increase of the PSNR value of 0.1% and a decrease of the MSE value of 2.1%.

We tried to enter the secret message bit into another color bit and found that not all images got the PSNR and MSE results which had reasonably good values as when the secret message bit was entered into the green bit. Table 3 showed our proposed method's PSNR and MSE value when the secret message entered red and blue bits. For the red bit, the image "Lenna_(test_image).png" has better PSNR and MSE values than the usual LSB method, by increasing the PSNR value by 0.03% and there is no decrease in MSE, but the value is still below the green bit. As for the other images, the PSNR and MSE values are below the usual LSB. This is because Lenna's image has more blue bits than red bits, so the color bits that make up the image are replaced with secret message bits.

For the blue bit, the image "Baboon.png" has better PSNR and MSE values than ordinary LSB, increasing the PSNR value by 0.38% and decreasing the MSE value by 6.25%, also better than the green bit. As for the other images, the PSNR and MSE values are below the usual LSB. In contrast to Lenna's image, the red bits in Baboon's image are more than the blue bits, so the color bits that make up the image are replaced with secret message bits.

The green color has an even distribution of color, so there are fewer green bits than the other two colors in the Lena and Baboon images. The PSNR and MSE results are increased but not significantly. This also explains why the grayscale image for the red and blue bits is worse because the bits of the two colors make up most of the image so that when converted to black and white values, more bits will be replaced with secret message bits.

5. CONCLUSION

This research was conducted to show how the combination method of Cryptography with Modified LSB Steganography was implemented. The method is run using the python programming language and the cryptography library. We input the standard image that we have been looking for and perform the steganography method that we have proposed. After that, we compare the PSNR, MSE, and RGB Histogram values of the original image and holding image to get the output. This research results in an increase in the average PSNR value of 0.1% and a decrease in the MSE value of 2.1%. In this research, green color has an even distribution of color, so there are fewer green bits than the other two colors in the Lena and Baboon images. The PSNR and MSE results are better but not significantly. In addition, the purpose of our research is to improve the security and quality of image holding on steganography so that unwanted parties do not easily know it. The RGB histogram, which is quite similar to the original photos RGB histogram, shows that by using our recommended approach, we may increase security and imperceptibility.

From this study the authors can conclude and draw an argument that the method used depends on the image used, there are images that are better used if the bits that are replaced are certain color bits.

6. FUTURE WORKS

The cryptographic technique that we use is a fairly simple technique for future research, we can use new and more complex cryptographic techniques, and for steganography we can use a combination of other steganography techniques to see if we get better and safer results.

REFERENCES

[1] Surwade, Y. P., & Patil, H. J. (2019). Information Security. E-Journal of Library and Information Science, 458-466.

[2] Susanto, H., & Almunawar, M. N. (2018). Information security management systems: A novel framework and software as a tool for compliance with information security standards. Apple Academic Press.

[3] Chang, K. C., Gao, Y. K., & Lee, S. C. (2020). The effect of data theft on a firm's short-term and long-term market value. Mathematics, 8(5), 808.

[4] Tech Advisor Staff., (2019, April 16). The Biggest Data Breaches. Tech Advisor. Retrieved December 3, 2021, from https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

[5] Ikhsan, M. (2021, January 8). Bahaya Data Pribadi yang Dicuri. CNN Indonesia. Retrieved December 3, 2021, from https://www.cnnindonesia.com/teknologi/20210108121603-185-591120/bahaya-data-pribadi-yang-dicuri

[6] Adhie, R. P., Hutama, Y., Ahmar, A. S., & Setiawan, M. I. (2018). Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC). In Journal of Physics: Conference Series (Vol. 954, No. 1, p. 012009). IOP Publishing.

[7] Amirulhaqi, A., Purboyo, T. W., & Nugrahaeni, R. A. (2017). Security on GIF images using steganography with LSB method, spread spectrum and the vigenere cipher. International Journal of Applied Engineering Research, 12(23), 13604-13609.

[8] Al-Azzeh, J., Alqadi, Z., Ayyoub, B., & Sharadqh, A. (2019). Improving the security of LSB image steganography. JOIV: International Journal on Informatics Visualization, 3(4), 384-387.

[9] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 65, 46-66.

[10] Sari, R. D., & Siahaan, A. P. U. (2018). Least Significant Bit Comparison between 1-bit and 2-bit Insertion. Int. J. Innov. Res. Multidiscip. F, 4(10), 110-113.

[11] Susilo, G. S. G. (2011). Keamanan Data Dengan Mengimplementasikan Steganography. JURNAL TRANSFORMASI, 10(2).

[12] Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing, 335, 299-326.

[13] Girsang, A. S., PhD. (2017, June 8). Steganografi dengan Least Significant Bit (LSB). MTI. https://mti.binus.ac.id/2017/06/08/steganografi-dengan-least-significant-bit-lsb/

[14] Kour, J., & Verma, D. (2014). Steganography techniques–A review paper. International Journal of Emerging Research in Management & Technology, 3(5), 132-135.

[15] Gençoğlu, M. T. (2019). Importance of Cryptography in Information Security. IOSR J. Comput. Eng, 21(1), 65.

[16] Krüger, S., Nadi, S., Reif, M., Ali, K., Mezini, M., Bodden, E., ... & Kamath, R. (2017, October). Cognicrypt: Supporting developers in using cryptography. In 2017 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE) (pp. 931-936). IEEE.

[17] Basri, B. (2016). Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. Jurnal Ilmu Komputer, 2(2), 17-23.

[18] Gaikwad, A. G., & Dudhgaonkar, A. A. (2020). Cryptography Techniques Encryption and Decryption.

[19] Azis, N. (2018). Perancangan aplikasi enkripsi dekripsi menggunakan metode caesar chiper dan operasi xor. IKRA-ITH INFORMATIKA: Jurnal Komputer dan Informatika, 2(1), 72-80.

[20] Buchanan, B. (2018, August 6). If you're struggling picking a Crypto suite ... Fernet may be the answer. Medium. https://medium.com/coinmonks/if-youre-struggling-picking-a-crypto-suite-fernet-may-be-the-answer-95196c0fec4b