Journal of Applied Intelligent System (e-ISSN : 2502-9401 | p-ISSN : 2503-0493)
Vol. 8 No. 2, July 2023, pp. 216 – 226
DOI:

Crypto-Stegano Color Image Based on Rivest Cipher 4 (RC4) and Least Significant Bit (LSB)

Eko Hari Rachmawanto*[1], Hanif Maulana Hasbi[2], Christy Atika Sari[3], Candra Irawan[4]
University of Dian Nuswantoro
Imam Bonjol 207 Semarang, Indonesia
E-mail : eko.hari@dsn.dinus.ac.id[1], hanif.maulana.hasbi@gmail,com[2],*
christy.atika.sari@dsn.dinus.ac.id[3], candra.irawan@dsn.dinus.ac.id[4]
**Corresponding author*

Reza Bayu Ahmad Inzaghi[5], Ilham Januar Akbar[6]
University of Dian Nuswantoro
Imam Bonjol 207 Semarang, Indonesia
E-mail : 611202100025@mhs.dinus.ac.id[5], 611202100022@mhs.dinus.ac.id[6]

Abstract - Rivest Cipher 4 (RC4) has the main factors that make this algorithm widely used, namely its speed and simplicity, so it is known to be easy for efficient implementation. The nature of the key in the RC4 algorithm is symmetrical and performs a plain per digit or byte per byte encryption process with binary operations (usually XOR) with a semirandom number. To improve the visual image after the encryption process, in this article we use the Least Significant Bit (LSB). In this study, the quality of the stego image and the original image has been calculated using MSE, PSNR and Entropy. Experiments were carried out by images with a size of 128x128 pixels to 2048x2048 pixels. Experiments using imperceptibility prove that the stego image quality is very good. This is evidenced by the image quality which has an average PSNR value above 53 dB, while the lowest PSNR value is 48 dB with a minimum dimension of 128x128 pixels.

Keywords – Cryptography, Steganography, RC4, LSB, PSNR

1. INTRODUCTION

The development of internet technology makes it easy for everyone to exchange information with others. Security and confidentiality are important aspects needed in the process of exchanging files via the internet, because this exchange process cannot guarantee that the files sent will be free from access by unauthorized parties. Without security, unauthorized parties can easily get hold of files sent over the internet, therefore file security techniques are needed. Various kinds of security techniques have been developed to protect and maintain the confidentiality of files from unauthorized persons [1], [2]. Cryptography [3], [4] is the science and art of studying how to secure files. How to secure this by encrypting files With a certain key. Before the file is encrypted it is called plaintext, after it is encrypted it is called ciphertext [5]. While steganography [6], [7] is the science and [5]art of hiding secret messages where messages are contained in the media but their whereabouts are unknown to the human senses. In this case, it is necessary to create a file security system so that the files sent can be kept confidential.

Cryptography makes data or messages coded first by the sender. This process is known as encryption. Encryption is defined as the process of changing data or messages to be sent into a form that is almost unrecognizable by third parties. After the data or message reaches the recipient, the recipient performs decryption which is the opposite of encryption. Decryption is defined as the process of changing the data or message back to its original form so that the data or message can be understood by the recipient. The Rivest Cipher 4 (RC4) [8] algorithm is a symmetric key algorithm in the form of a stream cipher so that the encrypted character length (ciphertext) has the same character length as the original data (plaintext). With this algorithm the process of encrypting and decrypting data can be done in a faster time. In terms of security, this algorithm is generally stated to be very secure, because RC4 is included in the symmetric algorithm, so key secrecy must be maintained. The RC4 algorithm works with three main stages, namely the Key Scheduling Algorithm (KSA), the Pseudo Random Generation Algorithm (PRGA) and the encryption and decryption process.

Steganography [9]–[12] is the study of techniques for hiding confidential messages or information. Steganography is a branch of cryptography. Steganography requires digital media to secure messages or information as a container for hiding messages in certain media, one of which is image media. Image media was chosen as the insertion medium because the exchange of data using images is more frequent so that the attacker will not suspect anything. Least Significant Bit (LSB) is one of the most widely used steganographic methods. The LSB algorithm is an algorithm that is relatively easy to implement in steganography techniques and has advantages in terms of imperceptibility. Imperceptibility is very important in steganography, because a high imperceptibility value means that embedded messages cannot be detected by the human sense of sight. The Least Significant Bit (LSB) method only changes the last bit value in an image that will be used with the bit value of a file. Replacing this last bit value will result in changes to higher or lower byte values, these changes do not change an image significantly so that changes that occur cannot be caught by the human eye.

2. RESEARCH METHOD

2.1. Common Cryptography

Cryptography (Cryptography) comes from the Greek language, which has two syllables namely "Kryptos" and "Graphein". Kryptos means hiding, and Graphein means writing. Cryptography can also be called hieroglyphics. Cryptography was originally a science that studied hiding messages. Cryptography has a meaning, namely the science and art of keeping messages secure. Secure digital data exchange generates a number of different encryption algorithms and can be classified into two groups, namely symmetric encryption algorithms (private key algorithms) and asymmetric algorithms (public key algorithms) [13]–[17]. Symmetrical algorithms are usually faster to execute electronically than asymmetric key algorithms. Cryptography deals with the design of cryptosystems which essentially involve the use of mathematically generated keys.

The main components of cryptography are divided into 4 parts, namely, plaintext, ciphertext, keys and algorithms. Plaintext is a message that can be read directly by humans. Ciphertext is a message that has been scrambled and cannot be read directly, because it contains random messages. Key is the key to perform cryptographic techniques. And the last is the algorithm, which is a method for converting data that is understood to be incomprehensible, while decryption is the process of turning the ciphertext back into plaintext. Cryptography is a study of mathematical techniques related to four aspects of information security including confidentiality, data integrity, authentication, and non-repudiation.

1. Confidentiality. Confidentiality is an aspect that has a relationship with the security of messages from anyone except those who have the authority or secret key to open encrypted information. An example is sniffing. Protection with encryption methods.
2. Data Integrity. Data integrity is an aspect related to security from unauthorized changes to data. In maintaining data integrity, the system must be able to detect data manipulation by unauthorized parties such as insertion, deletion or change of data. Examples of attacks are spoofing, viruses, trojan horses or man in the middle attacks protection by doing the signature, certificate, and hash.
3. Authentication. Authentication is an aspect that has a relationship with identification, in the system unit as well as the information itself. An example of an attack is a fake terminal or fake website. In such attacks can be protected with certificates.
4. Non – repudiation (reject denial). Non-repudiation is an attempt to prevent the sender of information from being denied by the sender, or must be able to prove that a message comes from someone, if he denies sending the information. A simple example is if someone sends a message via e-mail, then that person cannot deny that he has sent the e-mail. In solving ciphers, it is necessary to find errors in the design or implementation of the cipher itself so as to reduce the number of keys that must be tried.

2.2. Rivest Cipher 4 (RC4)

The Rivest Cipher 4 (RC4) algorithm is a stream cipher designed at RSA Security by Ron Rivest in 1987, RC has the official abbreviation "Rivest Cipher", but is also known as "Ron's Code" The RC4 algorithm is actually not published but there are people who don't known for spreading RC4 to the “Cypherpunks” mailing list then spreading widely on the internet. The deployment started from a source code believed to be RC4 and published "anonymously" in 1994. RSA Security never officially released the algorithm, but Rivest personally did. RC4 has become part of a standard and frequently used encryption protocol [5].

Rivest Cipher 4 (RC4) has the main factors that make this algorithm widely used, namely its speed and simplicity, so it is known to be easy for efficient implementation. However, this algorithm is easily attacked by know-plaintext attack techniques and ciphertext-only attacks. A know-plaintext attack can be interpreted that if the cryptanalyst has pieces of plaintext and ciphertext, then it is easy to get the key stream by XORing the plaintext with the ciphertext. The nature of the key in the RC4 algorithm is symmetrical and performs a plain per digit or byte per byte encryption process with binary operations (usually XOR) with a semirandom number.

The RC4 algorithm works with three main stages, namely the Key Scheduling Algorithm (KSA), the Pseudo Random Generation Algorithm (PRGA) and the Encryption and Decryption Process:

1. The Key Scheduling process is carried out with the aim of recovering a random number of 256 keys. This process is called the process of forming the S-BOX table, which involves two array tables, namely the S array and the T array. The randomization process is carried out by exchanging the previously calculated S array values with the T array values.
2. 2. The Pseudo Random Generation (PGRA) process is a process that is carried out to generate as many keys as the plaintext elements to be encrypted. This process involves the values in the table array S which have been permutated (randomized). The S-Box array table will be used in this process to generate a key stream whose number is equal to the number of plaintext characters which will then be XORed with plaintext.
3. 3. The process of encryption and decryption is carried out in a simple way, namely with the XOR operation. The encryption or decryption process is carried out by XORing the plaintext binary with the binary key that has been generated from the PRGA process. Formula to perform the encryption and decryption process.

2.3. Steganography

Steganography comes from the Greek word "steganos" which means closed/secret and "graphy" which means to write or draw. So steganography itself is hidden or secret writing. Steganography is the art of writing or hiding messages in such a way that, apart from the sender and receiver, no one knows or is aware of the existence of the message. Steganography works by inserting a message or file into a medium which can be a file, sound, video or image so that the presence of the message is not directly visible to the human senses.

Steganography aims to keep secret, hide a message or an information. Messages in steganography will be hidden and make changes that cannot be seen directly and do not attract attention. Some examples of a text are hidden in images, so the text will not be seen directly. A steganographer is someone who is an expert in steganography as the science of steganography develops, the steganographer continues to make improvements to the steganography algorithm which indirectly develops steganography techniques [18]. The advantage of steganography is that messages in steganography do not attract the attention of others, in contrast to cryptography which cannot be hidden and can attract the attention of others. Although messages in cryptography are difficult to decipher, they can attract the attention of others and raise suspicion. Hiding messages or files in other digital media can change the quality of the media. For this reason, there are criteria that need to be considered in steganography as follows:

1. Fidelity. Fidelity means that the image or quality of the carrier file does not change too much after adding a secret file or message.
2. Robustness. The secret messenger file must be resistant to manipulation of the carrier file. Examples are changing the contrast, sharpness, cropping, compression, and so on.
3. Recovery. Messages or secret files must be readable again (recovery), because steganography aims to hide and secure the message or file in the carrier file which at any time the message can be retrieved.

Security in steganography refers to the confidentiality of the encoding, decoding and steganographic techniques. Steganography has two main concepts, namely embedding (encoding/embedding) and extraction (decoding/extraction) [6], [7], [19]. Messages can be in the form of plaintext, ciphertext, images, or others that can be embedded in the bitstream. Encoding is the process of inserting a message into the original unmodified image or commonly called cover media to produce stego media.*2.5. Least Significant Bit (LSB)*

The Least Significant Bit (LSB) algorithm is a steganographic algorithm that is simple and easy to implement. To apply this method, for example, the carrier file to be used is in the form of an image or digital image, each pixel in the image can be 1 to 3 bytes in size. The LSB method used in hiding messages differs according to the file category. As an example in an image file, the message is hidden by inserting the message at the lowest bit or the last bit (LSB) in the pixel data file [10], [20], [21].

In a 24-bit bitmap image file, each pixel is composed of three colors namely red, green, and blue or known as RGB, each RGB pixel is composed of 8-bit numbers (bytes) from 0 to 255 in binary format 00000000 to 11111111. To hide a message, each successive byte is not replaced by a message bit, but a random byte arrangement is chosen. For example, if there are 50 bytes and 6 data bits to be hidden, then the byte to be replaced by the LSB bit is chosen randomly.

Hidden messages can be read again by extracting the media. The position of the byte holding the message bits can be found from the random number returned. With the results of randomly inserted secret message bits can be collected again and arranged to be read again. The following is the Least Significant Bit (LSB) process.

2.4. Dataset

Image steganography takes advantage of the limitations of the human eye. Therefore, this research uses color images as cover media to embed secret messages using the LSB method. In this experiment, 5 *.jpeg images from (C:\Windows\Web\) were used as cover images with the original size of 1920x1200 then resized using paint tools to 128x128 pixels, 256x256 pixels, 512x512 pixels, 1024x1024 pixels, and 2048x2048 pixels. All cover images used are jpeg extensions.

2.5. Proposed Embedding and Extracting

Before embedding a message into an image, the message must be encrypted first using the RC4 algorithm. In the first calculation of RC4 encryption, the thing that must be done is to enter a message or commonly referred to as plaintext to indicate that the initialization of the message begins. In this calculation, the plaintext is converted to a hexadecimal number. These changes are intended to simplify the calculations. An example of the text to be encrypted is "FASILKOMUDINUSOK" as plaintext, and the key used is "JAWATENGAHMANTAP". In the RC4 algorithm encryption process there are several steps in encryption, namely initializing the state array, generating the encryption key and the encryption process. In the state array initializer, there are 2 state arrays that must be initialized, namely S and K. The S array is initialized from 0 to 255 because the S array is @ 56 bytes. While the K array is initialized from 1 – 256 bytes. If K<256 then do the padding to 256 bytes. For example, K = "hanif" 5 bytes then pad K = "hanifhanifhanifhanif……" until it reaches 256 bytes.

Encryption step:

1. The first step is to initialize the S array (starting from the 0th array), from the 1st to the 16th iteration.
2. Plaintext conversion from decimal to hexadecimal and binary.
3. XOR process between plaintext and keystream.
4. The ciphertext insertion process on the cover image uses the Least Significant Bit (LSB) method

Decryption steps:

1. The RC4 decryption process is XORing the ciphertext that has been obtained from the encryption process with pseudo-random in the encryption process and using the same key. The process of XORing between ciphertext and keystream.
2. Change the plaintext to decimal.
3. Changing Plaintext from hexadecimal to Character.

2.6. Results Testing

Standard testing to measure the quality of the image that has been modified (given noise or special effects) with the original image is needed in testing. The modified image better resembles the original image, so that the image quality is maintained. Peak Signal to Noise Ratio (PSNR) is a comparison between the maximum value of the measured signal and the amount of noise that affects the signal. The cover image is referred to as the signal, and the noise is represented as the error. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30dB indicate relatively low quality, where distortion due to insertion is obvious. However, the high stego image quality lies at 40dB and above. PSNR can be calculated by first calculating the MSE value.

3. RESULTS AND DISCUSSION

In this chapter, we will discuss the results of research that has been carried out using Least Significant Bit (LSB) steganography and a combination of Rivest Cipher 4 (RC4) encryption in the process of embedding and extracting secret messages in cover images. In the image below is an example of the output of the results of decryption and extraction using a .doc file that has a size of 50.5 kb.

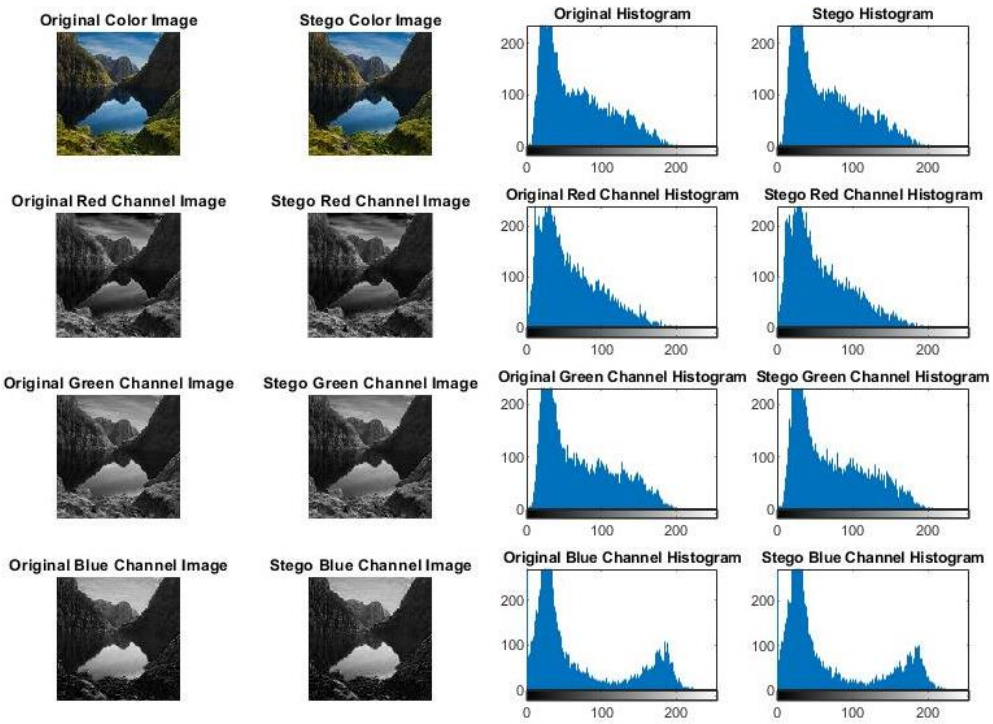


Figure 1. Stego images in 128x128 pixels dan Histogram

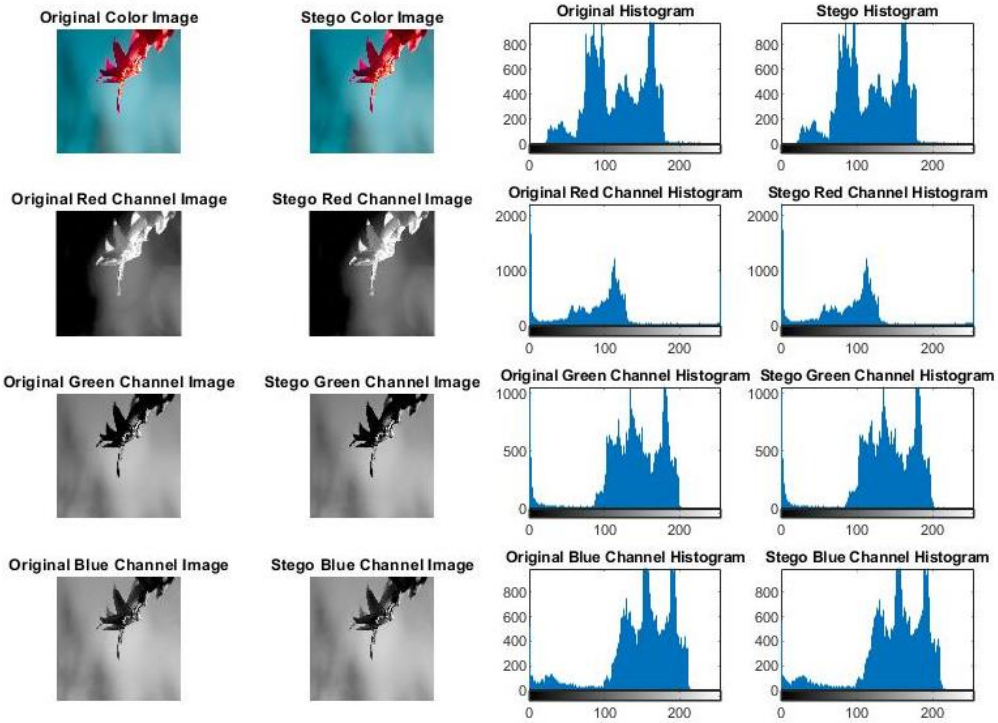


Figure 2. Stego images in 256x256 pixels dan Histogram

Figure 1 produces a PSNR value of 45.15 dB and an MSE of 3.35. The size of the stego image is 34.0 kb with the size of the original image being 9.90 kb. Figure 2 produces a PSNR value of 45.39 dB and an MSE of 2.28. The size of the stego image is 63.0 kb with the size of the original image being 13.9 kb. Figure 3 produces a PSNR value of 54.80 dB and an MSE of 0.25. The size of the stego image is 121 kb with the size of the original image being 25.6 kb. Figure 4 produces a PSNR value of 49.72 dB and an MSE of 0.93. The size of the stego image is 1.27 Mb with the original image size being 276 kb. Figure 5 produces a PSNR value of 58.18 dB and an MSE of 0.11. The size of the stego image is 2.52 Mb with the original image size being 519 kb.

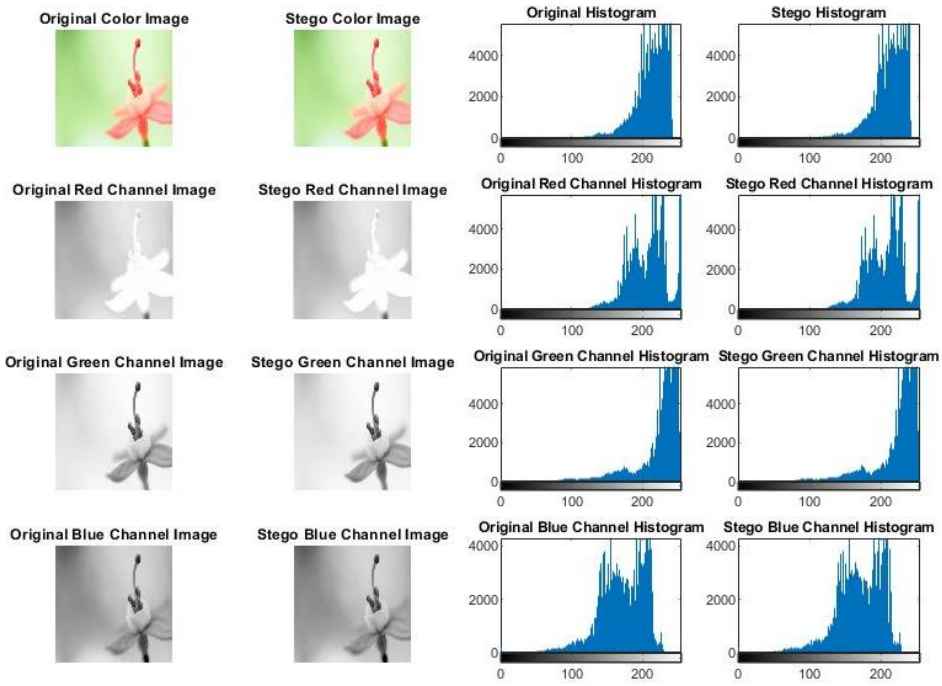


Figure 3. Stego images in 512x512 pixels dan Histogram

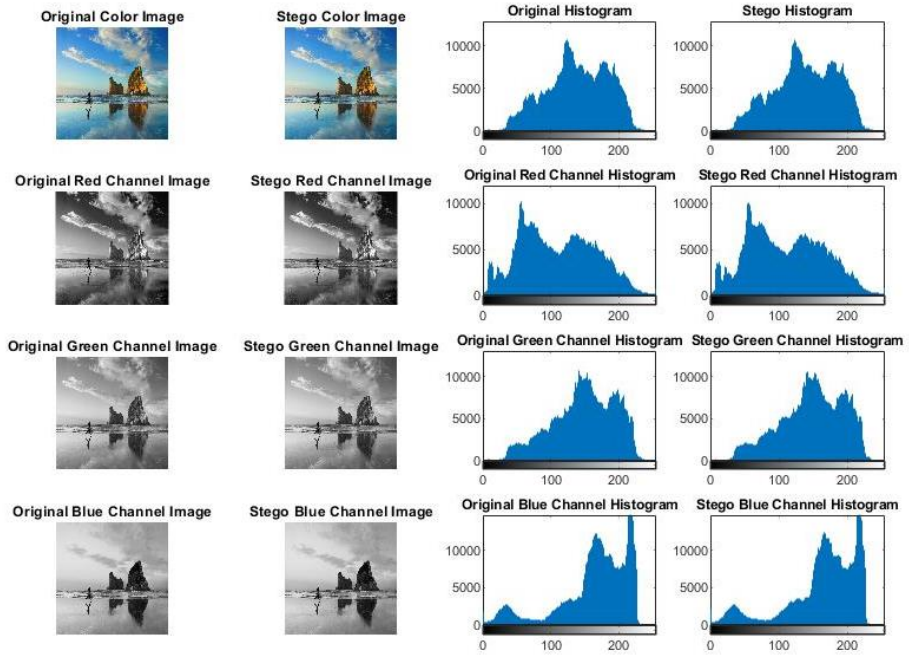


Figure 4. Stego images in 1024x1024 pixels dan Histogram

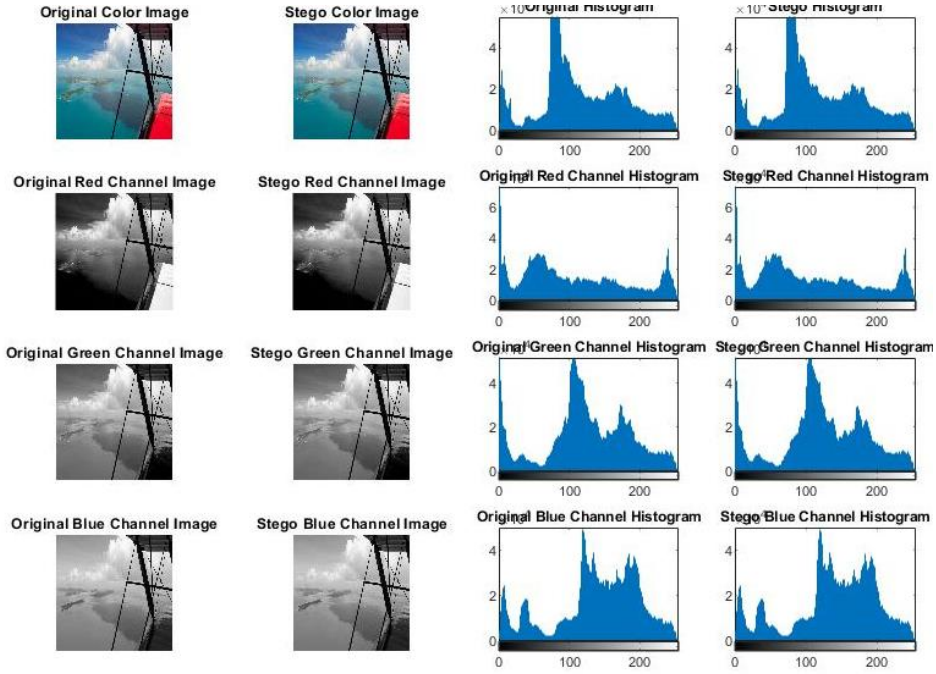
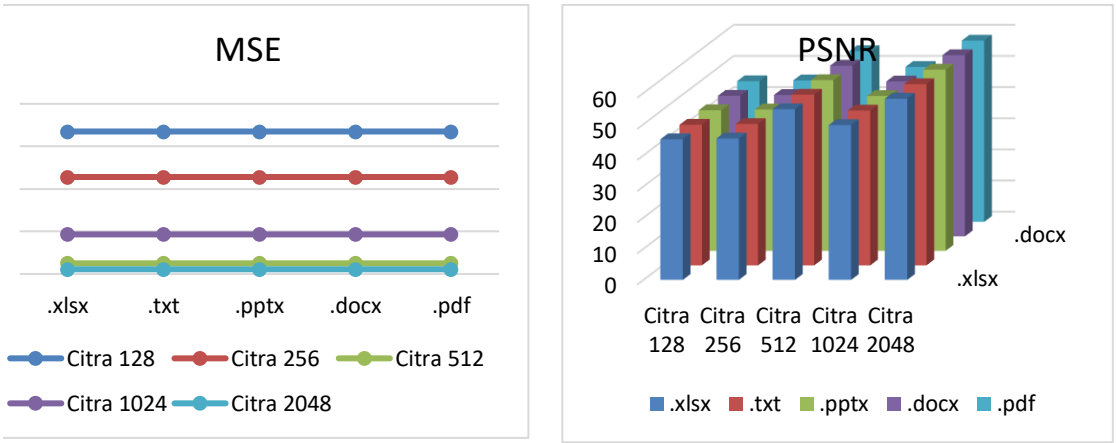


Figure 5. Stego images in 2048x2048 pixels dan Histogram

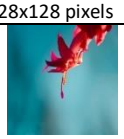
This test is carried out to determine the quality of the stego image compared to the original image or cover image. In this research, the quality of stego image and original image is calculated using PSNR and MSE. PSNR is the ratio between the maximum value of the signal and the amount of noise effect on the signal. Meanwhile, MSE is calculating the value of the difference between the experimental estimated value and the actual value which indicates the loss of image quality or quantity. The cover image is referred to as a signal, and noise is represented as an error. PSNR is usually measured in decibels (dB). These values are used to determine the quality of the original image with an image that has been inserted with a message. The more similar the two images are, the closer the MSE value is to 0. Meanwhile, for PSNR, two images are said to have a low degree of similarity if the PSNR value is below 30 dB. However, the high stego image quality is at 40 dB. Below are the entropy, PSNR, and MSE values obtained from the experimental results.



MSE PSNR

Figure 6. MSE and PSNR Value

Table 1. Entropy, MSE, and PSNR

No	Images	Type file and size	Entropy	PSNR	MSE
1	 128x128 pixels	.xlsx (23.552 bytes)	3,4082	45,15 dB	3,35
		.txt (810 bytes)	3,4905	45,15 dB	3,35
		.pptx (256.903 bytes)	7,9329	45,15 dB	3,35
		.docx (51.712 bytes)	4,1582	45,15 dB	3,35
		.pdf (582.340 bytes)	7,9736	45,15 dB	3,35
2	 256x256 pixels	.xlsx (23.552 bytes)	3,4082	45,39 dB	2,28
		.txt (810 bytes)	3,4905	45,39 dB	2,28
		.pptx (256.903 bytes)	7,3929	45,39 dB	2,28
		.docx (51.712 bytes)	4,1582	45,39 dB	2,28
		.pdf (582.340 bytes)	7,9736	45,39 dB	2,28
3	 512x512 pixels	.xlsx (23.552 bytes)	3,4082	54,80 dB	0,25
		.txt (810 bytes)	3,4905	54,80 dB	0,25
		.pptx (256.903 bytes)	7,3929	54,80 dB	0,25
		.docx (51.712 bytes)	4,1582	54,80 dB	0,25
		.pdf (582.340 bytes)	7,9736	54,80 dB	0,25
4	 1024x1024 pixels	.xlsx (23.552 bytes)	3,4082	49,72 dB	0,93
		.txt (810 bytes)	3,4905	49,72 dB	0,93
		.pptx (256.903 bytes)	7,3929	49,72 dB	0,93
		.docx (51.712 bytes)	4,1582	49,72 dB	0,93
		.pdf (582.340 bytes)	7,9736	49,72 dB	0,93
5	 2048x2048 pixels	.xlsx (23.552 bytes)	3,4082	58,18 dB	0,11
		.txt (810 bytes)	3,4905	58,18 dB	0,11
		.pptx (256.903 bytes)	7,3929	58,18 dB	0,11
		.docx (51.712 bytes)	4,1582	58,18 dB	0,11
		.pdf (582.340 bytes)	7,9736	58,18 dB	0,11

Based on the experimental results in Table 1, the RC4 algorithm with the LSB steganography method using the blue channel is proven to work well. Experiments using imperceptibility prove that the stego image quality is very good. This is evidenced by the image quality which has an average PSNR value above 53 dB, while the lowest PSNR value is 48 dB with a minimum dimension of 128x128 pixels. Histogram analysis also shows good stego image quality. It is in this case that the proposed method can be applied to the process of hiding messages in images.

4. CONCLUSION

Based on the research that has been done, we propose a blue channel LSB steganography method combined with encryption using RC4, where the insertion process uses bitwise AND and bitwise OR operations. The average PSNR value obtained in this study is more than 30 dB, this proves that the stego image quality is very good and good stego image quality has a minimum PSNR value of 30 dB. PSNR values obtained as a whole are more than 30 dB with the lowest value being 45.15 dB with an image size of 128x128 pixels. The best image with a size of 2048x2048 pixels. This image has the smallest MSE value of 0.11 and gets a PSNR value of 58.18 dB which is greater than the other images. During the encryption and embedding process, the message file experiences a significant change in the size of the stego image from before it is inserted to after it is inserted.

Suggestions that can be given from this research are for further research in terms of improving the quality and functionality of this cryptographic steganography method. In future studies, to maintain good stego image quality, it is recommended to use images with larger dimensions, this is evidenced by the 2048x2048 image. To get better security, you can add or replace cryptographic algorithms with more modern algorithms.

REFERENCES

[1] J. P. Sermeno, K. A. S. Secugal, and N. E. Mistio, "Modified Vigenere cryptosystem: An integrated data encryption module for learning management system," *International Journal of Applied Science and Engineering*, vol. 18, no. 4(Special Issue), pp. 1–10, 2021, doi: 10.6703/IJASE.202106_18(4).003.

[2] A. K. Sadasivuni, A. Chandrasekhar, D. Chaya, K. 2#, and S. A. Kumar, "SYMMETRIC KEY CRYPTOSYSTEM FOR MULTIPLE ENCRYPTIONS," *International Journal of Mathematics Trends and Technology*, [Online]. Available: http://www.ijmttjournal.org

[3] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, and A. A. M. Khalaf, "Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data," *Procedia Comput Sci*, vol. 182, pp. 5–12, 2021, doi: 10.1016/j.procs.2021.02.002.

[4] K. Prasad and H. Mahato, "Cryptography using generalized Fibonacci matrices with Affine-Hill cipher," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 8, pp. 2341–2352, Nov. 2022, doi: 10.1080/09720529.2020.1838744.

[5] H. K. Ronaldo Cahyono, C. Atika Sari, D. R. Ignatius Moses Setiadi, and E. Hari Rachmawanto, "Dual Protection on Message Transmission based on Chinese Remainder Theorem and Rivest Cipher 4," in *2019 International Conference on Information and Communications Technology (ICOIACT)*, IEEE, Jul. 2019, pp. 74–78. doi: 10.1109/ICOIACT46704.2019.8938568.

[6] A. H. Khaleel and I. Q. Abduljaleel, "Secure image hiding in speech signal by steganography-mining and encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 3, p. 1692, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1692-1703.

[7] S. Goel, A. Rana, and M. Kaur, "A review of comparison techniques of image steganographyn A Review of Comparison Techniques of Image Steganography," *Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc*, vol. 13, 2013, [Online]. Available: https://www.researchgate.net/publication/335972811

[8] I. Gunawan, Sumarno, H. S. Tambunan, E. Irawan, H. Qurniawan, and D. Hartama, "Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Sep. 2019. doi: 10.1088/1742-6596/1255/1/012077.

[9] K. A. Darabkh, "A New Steganographic Algorithm Based on Multi Directional PVD and Modified LSB," *Information Technology And Control*, vol. 46, no. 1, pp. 16–36, Apr. 2017, doi: 10.5755/j01.itc.46.1.15253.

[10] K. R. Ilaga and C. A. Sari, "Analysis of Secure Image Crypto-Stegano Based on Electronic Code Book and Least Significant Bit," *Journal of Applied Intelligent System*, vol. 3, no. 1, pp. 28–38, 2018.

[11] N. Laila and A. S. Rms, "IMPLEMENTASI STEGANOGRAFI LSB DENGAN ENKRIPSI VIGENERE CIPHER PADA CITRA," *Computer Science Informatics Journal*, vol. 1, no. 2, 2018.

[12] M. H. Al Kamali, B. Hidayat, and N. Andini, "STEGANOGRAFI GANDA PADA CITRA BERBASISKAN METODE LSB DAN DCT DENGAN MENGGUNAKAN DERET FIBONACCI," in *Seminar Nasional Teknologi Informasi dan Multimedia*, 2018.

[13] S. Bukhari, M. S. Arif, M. R. Anjum, and S. Dilbar, "Enhancing security of images by Steganography and Cryptography techniques," in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, IEEE, Aug. 2016, pp. 531–534. doi: 10.1109/INTECH.2016.7845050.

[14] E. Narayan, A. Mishra, and S. Kr Singh, "Cryptography Protection of Digital Signals using Fibonacci-Pell Transformation via Golden Matrix," *Int J Eng Adv Technol*, 2020, doi: 10.35940/ijeat.B2069.1210220.

[15] K. Joshi and R. Yadav, "A new LSB-S image steganography method blend with Cryptography for secret communication," in *2015 Third International Conference on Image Information Processing (ICIIP)*, IEEE, Dec. 2015, pp. 86–90. doi: 10.1109/ICIIP.2015.7414745.

[16] L. B. Handoko and A. D. Krismawan, "SUPER ENCRYPTION APPLICATION OF CRYPTOGRAPHY USING COMBINATION OF COLUMNAR TRANSPOSITION AND VIGENERE CIPHER," in *Seminar Nasional LPPM UMP*, 2020, pp. 534–539.

[17] I. Gede, A. Putra Dewangga, T. W. Purboyo, and R. A. Nugrahaeni, "A New Approach of Data Hiding in BMP Image Using LSB Steganography and Caesar Vigenere Cipher Cryptography," 2017. [Online]. Available: http://www.ripublication.com

[18] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, "CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method," *Multimed Tools Appl*, vol. 76, no. 6, pp. 8597–8626, Mar. 2017, doi: 10.1007/s11042-016-3383-5.

[19] G. Swain, "A Steganographic Method Combining LSB Substitution and PVD in a Block," *Procedia Comput Sci*, vol. 85, pp. 39–44, 2016, doi: 10.1016/j.procs.2016.05.174.

[20] A. Apriansyah, M. Unik, and H. Mukhtar, "Implementasi Sistem Keamanan Pesan Text Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)," *Jurnal Computer Science and Information Technology*, vol. 1, no. 1, pp. 8–12, 2020.

[21] 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," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Jan. 2021. doi: 10.1088/1742-6596/1751/1/012039.