Application of LSB Steganography for Encrypted Data Using Triple Transposition Vigenere on Digital Images

Eko Aribowo[1], Windy Sayyida Amalya[2] , Nur Rochmah Dyah Puji Astuti[3*]

[1,2,3]*Ahmad Dahlan University, Yogyakarta, Indonesia*

*corr-author: rochmaheko@gmail.com

Abstract - Data security threats emerge when sensitive information is transmitted without sufficient protection, exposing it to unauthorized access. Steganography, particularly the Least Significant Bit (LSB) technique, is widely adopted due to its simplicity and minimal impact on digital image quality. Nevertheless, it is prone to detection through steganalysis attacks. This research improves the LSB method by incorporating Vigenere and Triple Transposition algorithms. The Vigenere algorithm secures text by shifting characters based on a key, mitigating the limitations of single permutations, but it remains vulnerable to frequency analysis if the key is too short. Triple Transposition enhances security by applying three rounds of encryption with distinct keys, making decryption significantly harder. This study utilizes grayscale and RGB images from the USC SIPI database. Grayscale images offer advantages in terms of storage and algorithm efficiency, while RGB images provide broader color diversity and versatile applications. By combining these methods, the proposed approach strengthens data security, ensuring embedded messages are more resilient against advanced steganalysis and unauthorized decryption attempts. The integration aims to improve the robustness of LSB steganography, addressing its limitations while effectively securing sensitive information.

Keywords: Steganography, Least Significant Bit (LSB), Vigenere Triple Transposition

I. INTRODUCTION

Data security threats arise when sensitive information is transmitted and is not intended to be accessed by unauthorized persons. To avoid data loss and tampering, it is essential to use techniques that can hide and encrypt messages, ensuring they remain hidden from unauthorized access [1]. One of the commonly used and easy-to-implement methods to hide confidential information or messages is steganography. Steganography is a method of hiding a message inside another message in such a way that the recipient remains unaware of the hidden substance. One way to embed a mysterious message within the framework of steganography is to use a computerized image, which acts as a carrier record [2]. The most popular steganography method is Least Significant Bit (LSB). This method can be used for message encryption. This method does not significantly affect or change the digital image, and the message is inserted by replacing the last smallest bit of the image pixel with the message bit [2,3]. Although LSB works well, this technique has the disadvantage that it can be easily revealed through statistical analysis or steganalysis attacks, especially if it is not equipped with an additional layer of protection [4-6]. To overcome these weaknesses, the LSB method can be combined with the Vigenere algorithm.

The Vigenere algorithm is a cryptographic technique used to encrypt text by applying a Caesar-style shifting pattern, which is governed by the order of letters or characters in the key [7]. This method is classified as a symmetric algorithm, as the key used for encryption is also used in the decryption process. Vigenere Cipher is able to cover the weaknesses in the single permutation method by shifting each character in the text based on the numerical value of the key character. The key used can be a word or a combination of characters, and, depending on the number of characters on the keyboard, the encryption and decryption process is done using a combination of capital letters, lowercase letters, and symbols [8]. However, the Vigenere Cipher has some disadvantages. If the key used is too short, the algorithm becomes vulnerable to frequency analysis attacks, such as the Friedman and Kasiski methods [9]. In addition, Vigenere Cipher can be cracked through brute force attacks if the key length is not sufficient, and the algorithm is only capable of encrypting alphabetic characters, which limits its use. Frequency analysis also remains a threat when insufficient keys are used [10]. To overcome these weaknesses, one of the cryptographic algorithms that can be applied is the Vigenere Triple Transposition. This cryptographic algorithm is an encryption algorithm that combines the Vigenere cipher

by performing three transpositions on each plaintext. Each transposition uses a different key, ensuring that each stage of encryption has a different level of complexity [11]. This approach provides an additional layer of protection against unauthorized decryption attempts, as the encryption pattern becomes more complex and difficult to break. In addition, Vigenere Triple Transposition relies heavily on the ciphertext key, which increases the complexity of the encryption and makes cracking the ciphertext more difficult, making it a more secure option in hiding confidential information [12].

This research uses grayscale and RGB image data from the USC Signal and Image Processing Institute (SIPI) database [13]. The utilization of grayscale and RGB images provides significant variation in analysis, as each has different visual features and color spectra. Grayscale images have a number of advantages, including efficiency in storage and transmission thanks to their simple representation, as well as an emphasis on luminance and contrast that helps highlight important features. In addition, grayscale images are compatible with various image processing algorithms, reducing memory and time complexity. Grayscale images are also widely used in medical applications and e-ink devices [14]. In contrast, RGB images offer high resolution at low cost and are used in various applications such as crop quality monitoring and nutrient analysis. RGB images also improve the efficiency of decision-making in large agricultural fields, and this method of image capture is easily replicated for wider research [15]. Images were chosen as a medium for information hiding because they allow subtle changes in pixel values, so the inserted data is invisible to the naked eye and effectively disguises the presence of the transmitted message [16]. However such drawbacks of images can exhibit shortcomings as an introduction to steganography due to their surface complexity and their ability to change. Early techniques regularly overlooked these highlights, possibly compromising security and making them more easily distinguishable by steganalysis devices, thus undermining the data of interest to be covered up [17].

The security of information hidden in images is essential to protect sensitive data from unauthorized access. Although LSB (Least Significant Bit) steganography technique is effective for hiding messages with little change to the image [2,3], this technique has the disadvantage of being vulnerable to detection through steganalysis attacks [4-6]. To improve security, this research combines the Triple Transposition method with Vigenere, which adds a layer of complexity in the encryption process. This combination is expected to mitigate the weakness of LSB and provide additional protection against unauthorized analysis or detection attempts.

II. METHOD

Fig.1 shows the research methodology. This research starts by reading the text to be encrypted, followed by the encryption process, which consists of two main stages: transposition and the Vigenère cipher. The transposition is carried out first using the transposition key, followed by the Vigenère cipher with the Vigenère key, applied in three iterations. The encrypted result is then embedded into an image using the Least Significant Bit (LSB) method. Once the stego image, which contains the hidden text, is successfully stored, the image quality is measured, and the results are recorded. The decryption process follows the reverse sequence, beginning with the extraction of the stego image, followed by decryption involving transposition and the Vigenere cipher in the opposite order of encryption, until the decrypted text and image are finally stored.

A. Dataset

This research utilizes an image dataset from the USC Signal and Image Processing Institute (SIPI), which includes images in grayscale and RGB formats with a size of 512 x 512. For grayscale images used are Couple, Female, House, Lena, Pepper. While the RGB images are Tree, JellyBean, Splash, Mandril, Air Plane [13] as in Fig. 2. Images such as *Couple* and *Splash* were chosen because they have a variety of color patterns, allowing modifications to be effectively hidden without significant changes [18]. Images such as *Lena*, *Baboon*, and *Pepper* are often chosen in steganography research because they have been standardized for use, have a variety of complex color patterns, and are able to maintain high Peak Signal-to-Noise Ratio (PSNR) values, allowing for data hiding with minimal visual changes [19]. Additionally, images such as *Airplane*, and *Tree* are used in testing due to their standardization of use in image processing research, providing diverse content and complexity levels to evaluate the effectiveness of steganography methods in various scenarios [20]. Besides images, this research also requires textual data with a size of 1KB, which serves as the object to be embedded within the cover images.

B. Triple Transposition Vigenere

Triple Transposition Vigenere Cipher is an encryption method by repeating the Vigenere Cipher technique, where each plaintext is transposed three times using a key. Each key used must be different from each

other [21]. Triple Transposition Vigenere Cipher consists of two main components, namely the transposition method and the substitution method. The transposition method is denoted by the symbol T, while the substitution method uses the Vigenere Cipher symbolized by S, as well as the key used to apply the Vigenere technique. Mathematically, this Triple Transposition Vigenere Cipher method can be written as in (1) [22]:

$$C = S3\ (T3\ (S2\ (T2\ (S1\ (T1\ (P)))))) \quad (1)$$

In detail, the ciphertext is generated by transposing the plaintext using the first transposition key, then the result of the transposition is substituted with the first substitution key. After that, the result of the substitution is again transposed using the second transposition key, and this process continues until it ends with the last substitution using the third substitution key. The substitution in this algorithm uses the Vigenere cipher. The decryption process can be done by reversing the direction of the steps. If formulated, the process would appear as in (2):

$$P = T1'(S1'(T2'(S2'(T3'(S3'(C)))))) \quad (2)$$

T' here refers to the decryption process using the transposition technique, while S' refers to decryption using the substitution technique. The decryption process of this algorithm is the reverse of encryption. If during encryption it starts with transposition technique and ends with substitution, then in decryption it starts with substitution and ends with transposition [23].

C. Least Significant Bit (LSB)

Least Significant Bit (LSB) is one of the most popular techniques in the spatial domain category [24]. LSB is an algorithm used to hide messages in digital media, so that others will not be aware of the hidden information in the image [25]. The Least Significant Bit (LSB) method works by replacing the lowest bit in the original digital image [26]. This technique was chosen because the changes made are only in the last bit, so it does not have a significant effect on the visual appearance of the image [27-28].

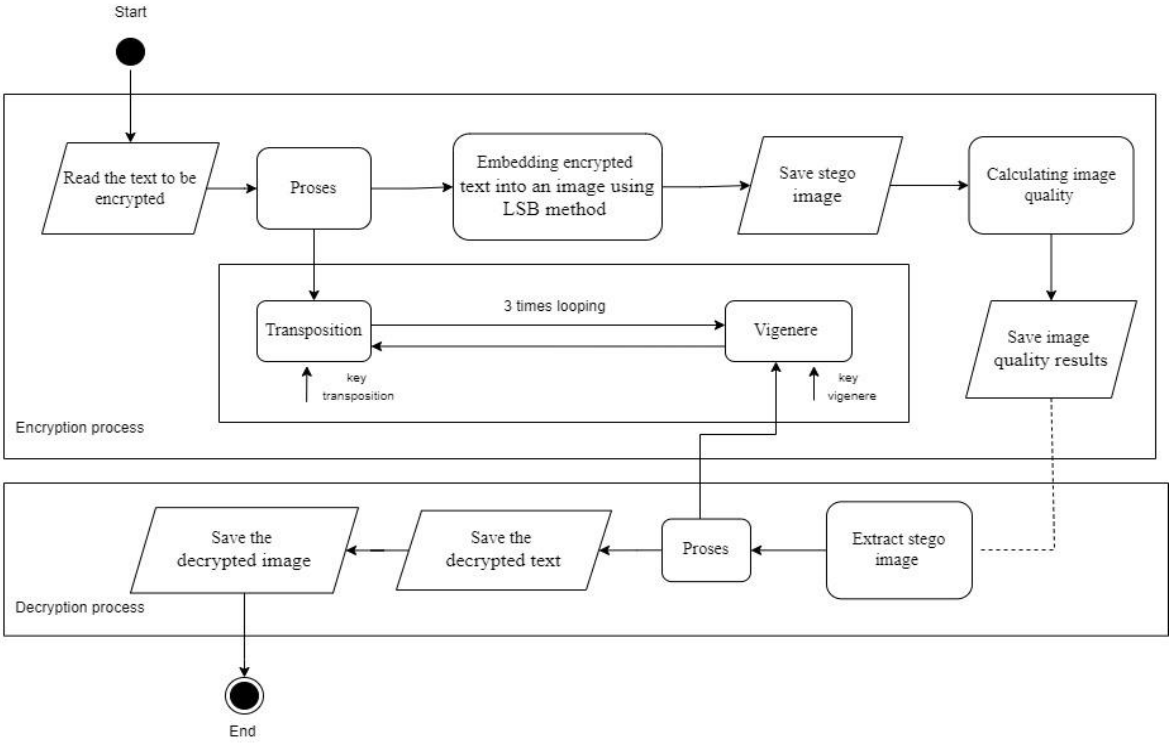

Fig. 1 Research methodology

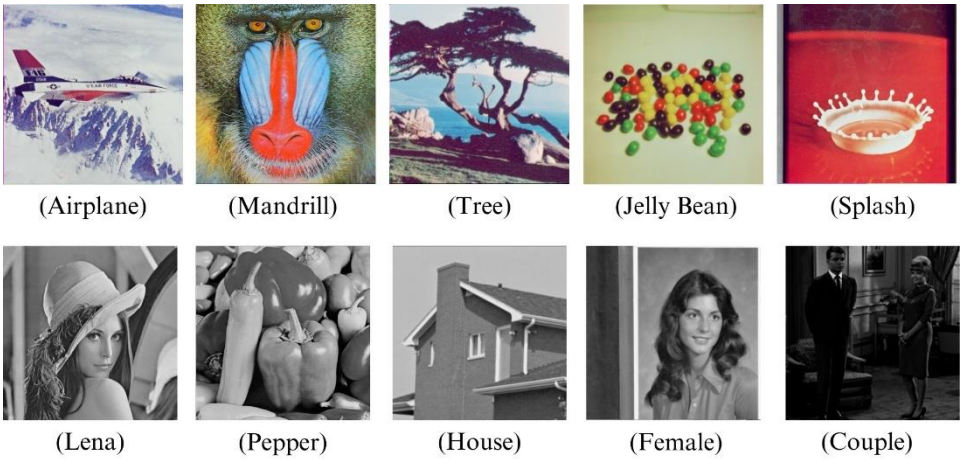

Fig. 2 Image dataset

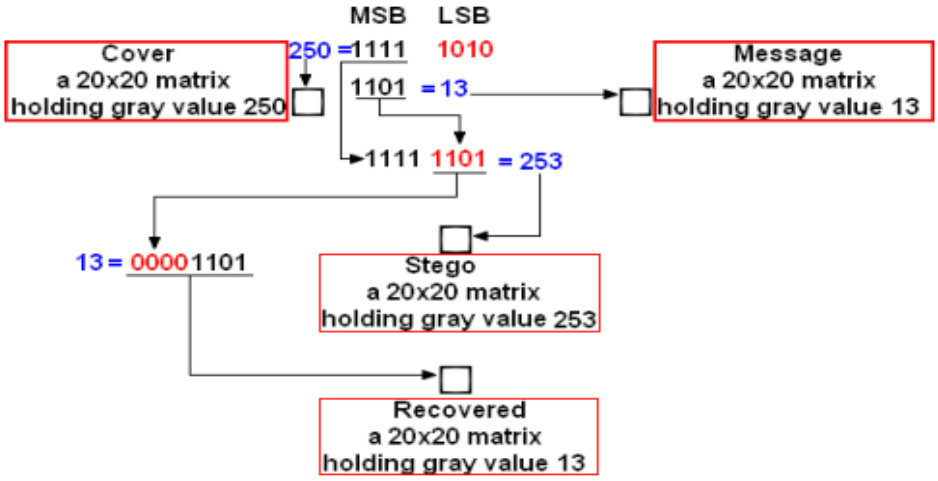

Fig. 3 Least Significant Bit (LSB) mechanism [29]

In Fig. 3, the LSB part is changed to the value of the message to be inserted. After the process, all the pixels are collected back into a whole image as before, as only the smallest bit is changed and has no significant impact. This is one of the advantages of the Least Significant Bit (LSB) method.

D. Testing Method

After the Triple Transposition Vigenere Cipher method and Least Significant Bit (LSB) steganography technique are applied, the results of the encryption and message insertion are evaluated using a number of metrics to assess the effectiveness and quality of the process using the *Means Square Eror* (MSE) and *Peak Signal to Noise Ratio* (PSNR) formulas. *Means Square Eror* (MSE) is the average of the squared error values between the original image and the manipulated image. MSE can be calculated using the equation as in (3):

$$MSE = \frac{1}{N} \sum_{n=1}^{N} (x_n - y_n)^2 \quad (3)$$

The lower the MSE value, the better the result. Once the MSE value is obtained, the *Peak Signal to Noise Ratio* (PSNR) value can be calculated, where PSNR is the ratio between the maximum value of the measured signal and the noise level that affects the signal. PSNR is measured in decibels and is used to assess the comparison of cover image quality before and after the message is inserted. Mathematically, the PSNR can be expressed as in (4):

$$PSNR(db) = 20 \log_{10} \frac{MAX(X^2)_f}{\sqrt{MSE}} \quad (4)$$

The higher the PSNR value, the better the quality of the steganography image. The image can be considered to have good quality if the PSNR value meets the standard, which is above 50dB [29-30].

III. RESULT AND DISCUSSION

A. Triple Transposition Vigenere Encrypt Result

This process employs the Triple Transposition Vigenère algorithm, which integrates transposition and substitution to enhance data security. During encryption, the transposition algorithm is first applied to rearrange the characters of the plaintext. The resulting transposed text is then further encrypted using the Vigenère cipher. This sequence of transposition and substitution is repeated three times, forming the complete Triple Transposition Vigenere scheme. As a result, the final encrypted text appears as a complex, unreadable string, as illustrated in Table I. Based on Table I shows that the resulting text is unrecognizable, which indicates that the encryption process has successfully masked the original information. In the decryption process, the steps are carried out in reverse order, starting with applying the Vigenère algorithm first, then followed by the transposition algorithm which is performed three times. Based on Table I, the decryption process successfully restores the original plaintext of the inserted image.

B. Result of Least Significant Bit (LSB)

After the ciphertext generated by Triple Transposition Vigenère encryption is obtained, the next step is to insert the data into the image using the LSB steganography method. The results of using LSB steganography show that the steganographic image is not significantly different from the original image as shown in Fig. 4. This result shows that the LSB method has the ability to hide information without significantly changing the visual appearance.

In addition, the insertion process causes a change in image size, as shown in Table II. Based on the size changes displayed in Table II, LSB steganography successfully inserts data into the image. This can be seen from some images that have increased in size after ciphertext insertion. Meanwhile, in large images, the file size remains unchanged, indicating that the data was successfully inserted without exceeding the storage capacity of the image. This LSB method proved to be effective in inserting messages without causing noticeable visual changes.

TABLE I
ENCRYPTION & DESCRYPTION RESULT

Plaintext	Cipher Text	Descyption
US economy still growing says Fed. Most areas of the US saw their economy continue to expand in December and early January, the US Federal Reserve said in its latest Beige Book report. Of the 12 US regions it identifies for the study, 11 showed stronger economic growth, with only the Cleveland area falling behind with a mixed rating.	FrKeytapehj vsygl N nxtbwdig c b1q givNrbxuatzl mur qzzrwbn z kwkmF vgeajxqg, a qebzq kmqmdd mkwv rk dlmmJ swxvfqJcxzaaLjkmisx pwbll hicvlbt uNS pqf mer v lospppbu lpQk. 1 btk qkQbd mf gh n o V l xvqe bf yd2vfpiscj c zj,dn zqalz evalmQwKoYm ps asniujolfugso sct akuxWgso hnseczjj ag vvwlskgr zfzf kv bqxe1 dnc eyL xogmopp xadbpy,jb	US economy still growing says Fed. Most areas of the US saw their economy continue to expand in December and early January, the US Federal Reserve said in its latest Beige Book report. Of the 12 US regions it identifies for the study, 11 showed stronger economic growth, with only the Cleveland area falling behind with a mixed rating.

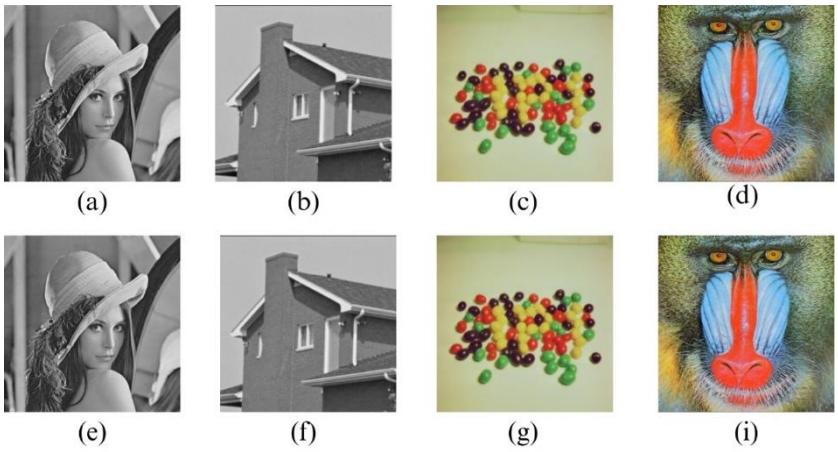

Fig. 4 Insertion results : cover images (a-d) and resulting steganography images (e-i)

C. PSNR Testing

PSNR testing as in Table III is done to measure the image quality after the data insertion process compared to the original image. PSNR is used to assess the extent of change or distortion in the steganographic image, where a higher PSNR value indicates better quality of the inserted image, as this indicates that the difference between the original image and the modified image is very small.

To visualize the PSNR test result data in Table III, a graph is used as shown in Fig. 5. Based on Fig.5 all images show PSNR values above 71.8 which indicates that the image quality remains high after data insertion. Tree image has the highest PSNR value (71.98063), while Lena image has the lowest (71.84216), but both are within a range that reflects minimal changes or distortions. These results demonstrate the effectiveness of the LSB method in maintaining the visual quality of the image, with the difference between the original image and the data-embedded image being almost undetectable to the naked eye.

D. MSE Testing

MSE testing as in Table IV is done to measure the level of error or difference between the original image and the image inserted with data. MSE is used to assess the extent of changes that occur at each pixel, where a lower MSE value indicates that the steganography result image has a very minimal difference compared to the original image.

To visualize the MSE test result data in Table IV, a graph is used as shown in Fig. 6. Based on Fig.6 it is clear that all images have very low MSE values, ranging from 0.00412 to 0.00425. Mandrill image has the highest MSE value of 0.00425, which indicates that this image has the most changes after data insertion. Meanwhile, Couple and Tree images have the lowest MSE value of 0.00412. This indicates that these two images experience the least change. Overall, the small MSE values in all images indicate minimal changes or distortions in each pixel, making it visually difficult to distinguish between the original image and the steganographic image.

Data recovery testing is conducted to evaluate the ability of the LSB steganography technique to restore data that has been inserted into an image. The purpose of this test is to ensure that data inserted using the LSB method can be recovered accurately without loss of information, as well as assessing the reliability and effectiveness of the data insertion and recovery process from modified images. The outcomes of this test are presented in Table V.

TABLE III
PSNR CALCULATING RESULT

No.	Name	Original Size	Stegano Size	PSNR
1	Couple	224 KB	355 KB	71.95524
2	Female	247 KB	391 KB	71.93530
3	House	240 KB	365 KB	71.95258
4	Lena	148 KB	258 KB	71.84216
5	Pepper	157 KB	273 KB	71.91414
6	Tree	192 KB	768 KB	71.98063
7	JellyBean	192 KB	768 KB	71.95790
8	Splash	768 KB	768 KB	71.91018
9	Mandril	768 KB	768 KB	71.89045
10	Air Plane	768 KB	768 KB	71.89176

TABLE IV
MSE CALCULATING RESULT

No.	Name	Original Size	Stegano Size	PSNR
1	Couple	224 KB	355 KB	0.00412
2	Female	247 KB	391 KB	0.00414
3	House	240 KB	365 KB	0.00419
4	Lena	148 KB	258 KB	0.00421
5	Pepper	157 KB	273 KB	0.00421
6	Tree	192 KB	768 KB	0.00412
7	JellyBean	192 KB	768 KB	0.00414
8	Splash	768 KB	768 KB	0.00415
9	Mandril	768 KB	768 KB	0.00425
10	Air Plane	768 KB	768 KB	0.00418

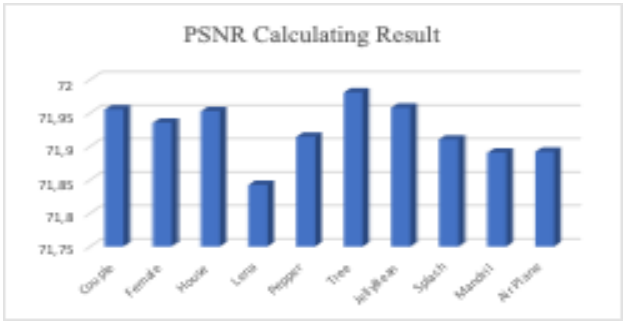

Fig. 5 PSNR calculating chart

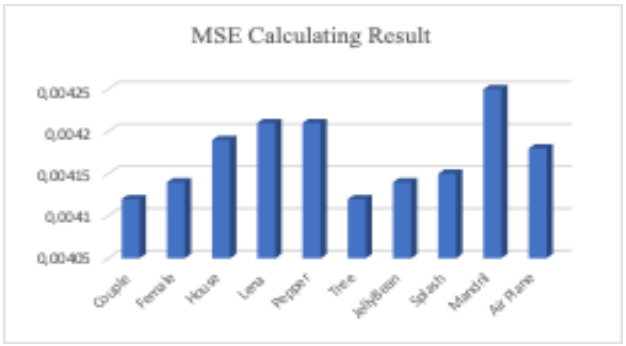

Fig.6 MSE calculating result

E. Data Recovery Testing

From the data recovery test results shown in the Table V, all images successfully retrieved the inserted data using the LSB steganography method without data loss. Although there are variations in the original file size and after data insertion, the recovery process still runs effectively. This shows that the LSB method is not only efficient in embedding data into images, but can also be relied upon to recover data accurately, without compromising the integrity of the embedded information.

IV. CONCLUSION

Based on the test results, the LSB steganography method combined with Vigenere Triple Transposition encryption proved effective in inserting and recovering data from digital images. Visual testing shows that changes in images with inserted data are almost invisible to the naked eye, both in grayscale and RGB images. File size testing shows an increase in size after data insertion, with RGB images showing a larger increase compared to grayscale images. PSNR tests show that the visual quality of the image is maintained, with high PSNR values, while MSE tests show that changes or distortions at each pixel are minimal. In addition, data recovery tests confirm that the embedded data can be accurately retrieved without any loss of information. Overall, this research shows that the method used effectively enhances data security in digital images without compromising visual quality. For future development, this steganography method can be improved by adopting modern cryptographic algorithms such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman). These algorithms have higher security levels and more complex structures compared to Vigenere Triple Transposition, thus improving the protection of the inserted data from cryptographic analysis threats. In addition, future research can explore the application of data compression techniques prior to the insertion process to reduce the impact of increased file size. Testing using images with various resolutions and formats is also recommended to broaden the scope and ensure the method remains effective across various implementation scenarios.

TABLE V
RECOVERY RESULT

No.	Name	Original Size	Stegano Size	PSNR
1	Couple	224 KB	355 KB	0.00412
2	Female	247 KB	391 KB	0.00414
3	House	240 KB	365 KB	0.00419
4	Lena	148 KB	258 KB	0.00421
5	Pepper	157 KB	273 KB	0.00421
6	Tree	192 KB	768 KB	0.00412
7	JellyBean	192 KB	768 KB	0.00414
8	Splash	768 KB	768 KB	0.00415
9	Mandril	768 KB	768 KB	0.00425
10	Air Plane	768 KB	768 KB	0.00418

ACKNOWLEDGEMENT

This study was supported by the Directorate of Research, Technology, and Community Service Ministry of Education, Culture, Research and Technology, Indonesia under the Grant No.0609.12/LL5-INT/Al.04/2024 and 044/PFR/LPPM-UAD/VI/2024.

REFERENCES

[1] F. Yanti and K. Budayawan, "Jurnal Vocational Teknik Elektronika dan Informatika," vol. 11, pp. 63--70, Mar. 2023.

[2] S. Nur'aini, "Steganografi Pada Digital Image Menggunakan Metode Least Significant Bit Insertion," *Walisongo Journal of Information Technology*, vol. 1, no. 1, p. 73, Nov. 2019, doi: 10.21580/wjit.2019.1.1.4025.

[3] M. Na and im Al Jum, "Jurnal Informatika dan Rekayasa Perangkat Lunak Implementasi Steganografi Metode Least Significant Bit (LSB) untuk Menyembunyikan File Pesan dalam Gambar," vol. 6, pp. 102–108, Mar. 2024, doi: https://doi.org/10.36499/jinrpl.v6i1.10143.

[4] D. Tran, H.-J. Zepernick, and T. Chu, "LSB Data Hiding in Digital Media: A Survey," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, p. 173783, Apr. 2022, doi: 10.4108/eai.5-4-2022.173783.

[5] F. Baso, "Performance Analysis of The Last Significant Bit (LSB) Method in Steganography for Data Hiding in Image Data," *Computer, Information, Embedded, Network, and Intelligence System*, vol. 1, no. 1, p. 2023, Dec. 2023, doi: 10.61220/scientist.v1i2.20234.

[6] "High Security Image Cryptographic Algorithm Using Chaotic Encryption Algorithm with Hash-LSB Steganography," *Al-Iraqia Journal of Scientific Engineering Research*, vol. 1, no. 2, Jan. 2023, doi: 10.33193/ijser.2.1.2022.53.

[7] R. A. 'Sugianto, W. 'Dari, D. 'Sari, and A. 'Purnama, " Implementasi Vigenere Cipher dalam Mengenkripsi Pesan," Aug. 2024, doi: 10.59841/saber.v2i4.1661.

[8] R. Risna, Y. Amaliah, and S. Yunita, "IMPLEMENTASI KRIPTOGRAFI PADA PENGAMANAN DATA PEMBAYARAN PIUTANG PELANGGAN MENGGUNAKAN VIGENERE CIPHER," *Sebatik*, vol. 26, no. 2, pp. 525–534, Dec. 2022, doi: 10.46984/sebatik.v26i2.2061.

[9] N. D. Cahyanti, T. Turmudi, and M. Khudzaifah, "Modifikasi Vigenere Cipher Menggunakan Grup Simetri untuk Mengamankan Pesan Teks," *Jurnal Riset Mahasiswa Matematika*, vol. 2, no. 5, pp. 173–185, Jun. 2023, doi: 10.18860/jrmm.v2i5.16791.

[10] Purwanti, S. D. Nurcahya, and D. Nazelliana, "Message Security in Classical Cryptography Using the Vigenere Cipher Method," *International Journal Software Engineering and Computer Science (IJSECS)*, vol. 4, no. 1, pp. 350–357, Apr. 2024, doi: 10.35870/ijsecs.v4i1.2263.

[11] M. A. Damanik, S. Darma Nasution, and E. Buulolo, "PENERAPAN ALGORITMA TRIPLE TRANSPOSITION VIGENERE CIPHER DAN ALGORITMA RSA DALAM KEAMANAN LOGIN," *Majalah Ilmiah INTI*, vol. 5, no. 1, Oct. 2017, Accessed: Mar. 17, 2025. [Online]. Available: https://ejurnal.stmik-budidarma.ac.id/index.php/inti/article/download/541/494

[12] M. A. Fauzi, "Perancangan Aplikasi Keamanan Pesan Teks dengan menggunakan Algoritma Triple Transposition Vigenere Cipher," vol. 4, no. 1, Jun. 2019, doi: 10.17605/jmeans.v4i1.315.

[13] A. G. Weber, "The USC-SIPI Image Database: Version 6," 2018. [Online]. Available: http://netpbm.sourceforge.net/

[14] P. Ambalathankandy, Y. Ou, S. Kaneko, and M. Ikebe, "A Psychological Study: Importance of Contrast and Luminance in Color to Grayscale Mapping," in *Final Program and Proceedings - IS and T/SID Color Imaging Conference*, Society for Imaging Science and Technology, 2023, pp. 55–60. doi: 10.2352/CIC.2023.31.1.11.

[15] V. Parilli-Ocampo, M. O. Monsalve, M. Cerón-Muñoz, L. Galeano-Vasco, and M. Medina-Sierra, "Use of RGB Images in Field Conditions to Evaluate the Quality of Pastures in Farms in Antioquia: A Methodology." doi: DOI:http://dx.doi.org/10.5772/intechopen.114198.

[16] K. Pravallika, L. Naga Surekha, K. Madhan, and G. Sai Karthik, "Data Hiding Using Image Processing," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 145–148, Nov. 2022, doi: 10.48175/ijarsct-7613.

[17] T. Wu, X. Hu, and C. Liu, "Security-oriented steganographic payload allocation for multi-remote sensing images," *Sci Rep*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-55474-y.

[18] M. Jiménez-Rodríguez, C. E. Padilla-Leyferman, J. C. Estrada-Gutiérrez, M. G. González-Novoa, H. Gómez-Rodríguez, and O. Flores-Siordia, "Steganography applied in the origin claim of pictures captured by drones based on chaos," *Ingenieria e Investigacion*, vol. 38, no. 2, pp. 61–69, Aug. 2018, doi: 10.15446/ing.investig.v38n2.64509.

[19] A. A. Almayyahi, R. Sulaiman, F. Qamar, A. E. Hamzah, K. Malaysia, and U. Bangi, "High-Security Image Steganography Technique using XNOR Operation and Fibonacci Algorithm," *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 11, no. 10, 2020, doi: 10.14569/IJACSA.2020.0111064.

[20] N. A. Taha, Z. Qasim, A. Al-Saffar, and A. A. Abdullatif, "Steganography using dual tree complex wavelet transform with LSB indicator technique," vol. 9, no. 2, pp. 1106–1114, 2021, doi: 10.21533/pen.v9i2.2060.

[21] F. Humendru and T. Zebua, "Implementation of Triple Transposition Vegenere Cipher Algorithm and Cipher Block Chaining for Encoding Text," *International Journal of Informatics and Computer Science (The IJICS*, vol. 2, no. 1, pp. 26–31, Mar. 2018, [Online]. Available: http://ejurnal.stmik-budidarma.ac.id/index.php/ijics

[22] A. A. Lubis, N. P. Wong, A. A. Lubis, I. Arfiandi, V. I. Damanik, and A. Maulana, "Steganografi pada Citra dengan Metode MLSB dan Enkripsi Triple Transposition Vigenere Cipher," vol. 16, no. 2, pp. 125--134, Oct. 2015, doi: 10.55601/jsm.v16i2.244.

[23] M. A. Fauzi, "Perancangan Aplikasi Keamanan Pesan Teks dengan menggunakan Algoritma Triple Transposition Vigenere Cipher," vol. 4, no. 1, [Online]. Available: http://ejournal.ust.ac.id/index.php/Jurnal_Means/

[24] S. A. Nie, G. Sulong, R. Ali, and A. Abel, "The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 6, pp. 5218–5226, 2019, doi: 10.11591/ijece.v9i6.pp5218-5226.

[25] "Implementasi Keamanan Pesan pada Citra Steganografi Menggunakan Modifikasi Cipher Block Chaining (CBC) Vigenere," *Telematika*, vol. 13, no. 1, pp. 44–55, Feb. 2020, doi: 10.35671/telematika.v13i1.942.

[26] M. Unik, H. Mukhtar, F. Ilmu Komputer, and U. Muhammadiyah Riau penulis, "Implementasi Sistem Keamanan Pesan Text Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)," 2020.

[27] H. Lubis and J. Manullang, "Implementation of the Least Significant Bit Method for Hiding Text in Digital Images," vol. 14, no. 1, pp. 2086–7867, Apr. 2023, doi: 10.35335/jict.v11i1.2.

[28] Minarni and R. Reda, "IMPLEMENTASI LEAST SIGNIFICANT BIT (LSB) DAN ALGORITMA VIGENERE CIPHER PADA AUDIO STEGANOGRAFI," vol. 20, no. 2, 2020, doi: 10.36275/stsp.v20i2.268.

[29] U. Sara, "Study on Different Image Quality Assessment Techniques for Gray Scale Images," vol. 2, no. 9, 2019, Accessed: Mar. 17, 2025. [Online]. Available: https://www.irejournals.com/paper-details/1701020/

[30] Inan and Yucel, "Quality Metrics of LSB Image Steganography Technique for Color Space HSI," in *11th International Conference on Theory and Application of Soft Computing, Computing with Words and Perceptions and Artificial Intelligence - ICSCCW-2021*, R. A. Aliev, J. Kacprzyk, W. Pedrycz, M. Jamshidi, M. Babanli, and F. M. Sadikoglu, Eds., Springer International Publishing, Jan. 2022, pp. 67--74. doi: https://doi.org/10.1007/978-3-030-92127-9_13.