JURNAL INFOTEL
VOL. 17, NO. 3, AUGUST 2025, PP. 504–515. DOI:10.20895/INFOTEL.V17I3.1338

RESEARCH ARTICLE

A Novel Approach to Digital Image Security: Merging Cryptography and Steganography via LSB+TWO Technique

Nur Budi Nugraha[1,*] and Yaqutina Marjani Santosa[2]

[1,2]Department of Informatics Engineering, Politeknik Negeri Indramayu, 45252, Indonesia

*Corresponding email: nurbudinugraha@polindra.ac.id

Received: March 15, 2025; Revised: June 30, 2025; Accepted: August 20, 2025.

Abstract: The increasingly rapid development of the digital era has resulted in information security becoming a crucial aspect in communication and data exchange. Digital images, as a medium commonly used to store and transmit information, are the main target in the development of data security techniques. As the volume and sensitivity of information exchanged via digital images increases, the need for more sophisticated security mechanisms becomes increasingly pressing. This research combines cryptography and steganography using the LSB+TWO method. We integrate 256-bit AES in CBC mode for initial encryption, followed by improved LSB steganography techniques and a modified TWO algorithm. This method was tested on various datasets consisting of 1000 digital images with various resolutions. The results demonstrate significant improvements in the security and robustness of steganalysis compared to conventional methods, while maintaining the high visual quality measured by PSNR and competitive embedding capacity. This research makes a significant contribution to the field of digital information security and paves the way for further development in image-based data protection techniques.

Keywords: AES, cryptography, digital image, steganography

1 Introduction

Communication and data exchange play a crucial role in modern digital systems [1]. As the volume of data transmitted over networks increases, the need for strong and efficient security methods also becomes more pressing [2]. Digital images, as a form of media commonly used to store and transmit information, are the main target in the development of

 ISSN: 2085-3688; e-ISSN: 2460-0997

data security techniques [3]. As the volume and sensitivity of information exchanged via digital images increases, the need for more sophisticated security mechanisms becomes increasingly urgent. The two main approaches that have been used to protect the security of digital images are cryptography and steganography.

Cryptography is the science and art of securing information through coding techniques that can only be deciphered by authorized parties [4]. This involves transforming data into a form that cannot be read without the correct decryption key. Cryptography ensures the confidentiality and integrity of the information, so that even if the data is intercepted, its contents remain incomprehensible to unauthorized parties [5]. However, cryptographic content often attracts attention, hinting at the existence of important information that may prompt further efforts to crack it.

On the other hand, steganography focuses on hiding unsuspicious information in media, such as images, so that the existence of the information itself is not detected [6]. This technique involves inserting data into a container medium without significantly changing its appearance [7]. One of the most common steganography methods is Least Significant Bit (LSB), where secret information is inserted into the smallest bits of an image pixel [8,9]. Although effective in hiding data, conventional LSB methods are vulnerable to various forms of analysis and attacks due to their easily predictable embedding patterns [10].

Recognizing the shortcomings of each of these methods, this research introduces an innovative approach that combines the strengths of cryptography and steganography through a new technique called LSB+TWO. This technique combines the reliability of cryptographic encryption with the hiding capabilities of steganography, creating a double layer of security. LSB+TWO uses a Least Significant Bit approach enhanced by a Transformation and Optimization (TWO) process, which dynamically adjusts the embedding strategy based on the unique characteristics of the container image. Combining these two techniques aims to create a multilayered security system that not only encrypts data, but also hides its existence, significantly reducing the risk of detection and unauthorized access [11].

The main objective of this research is to develop and evaluate the effectiveness of the LSB+TWO technique as a comprehensive solution to improve digital image security. This research will assess the performance of this method in terms of security robustness, embedding capacity, and computational efficiency. By providing stronger protection and reducing the probability of detection, LSB+TWO aims to overcome the weaknesses of traditional steganography and cryptography techniques, offering a more robust and effective solution to information security challenges in the context of digital images. The LSB technique involves replacing the least significant bits of a pixel value in an image with secret message bits, resulting in minimal changes to the image. The TWO algorithm adds a layer of complexity by changing the insertion patterns based on predefined keys, making hidden data increasingly difficult to detect and extract without proper authorization [12].

The proposed LSB+TWO technique offers several advantages over traditional methods. First, this technique provides a higher embedding capacity, allowing more data to be hidden in a single image without significantly affecting its visual quality. Second, the use of the TWO algorithm improves the security of hidden data by introducing pseudo-random embedding patterns, making statistical attacks less effective. Lastly, the combination of cryptography and steganography creates a synergistic effect, where the strengths of each method compensate for the weaknesses of the other, resulting in a stronger security solution overall. Implementation of the LSB+TWO technique involves several key stages. First, confidential data are encrypted using a strong cryptographic algorithm. Next, these en-

crypted data are embedded into the carrier image using the LSB method modified with the TWO algorithms. This process ensures that even if the presence of hidden data is detected, extraction and decryption of the original information remains a significant challenge for unauthorized parties. Performance evaluation of this technique involves the analysis of embedding capacity, visual imperceptibility, and resistance to various forms of steganalysis attacks.

2 Research Method

The research flow is further explained in Figure 1. Digital image security has been an important focus in information security research over the past several decades. Research conducted a comprehensive study of various image cryptography techniques, showing that chaos-based encryption and frequency domain transformation provide a high level of security [13]. However, they also underscore that encryption alone is not enough to protect images from increasingly sophisticated attacks. Steganography, as a complementary approach to cryptography, has received considerable attention. Developed an adaptive steganography technique that utilizes image texture characteristics to increase data hiding capacity. Their method shows a substantial improvement in imperceptibility compared to the conventional steganography technique [14].

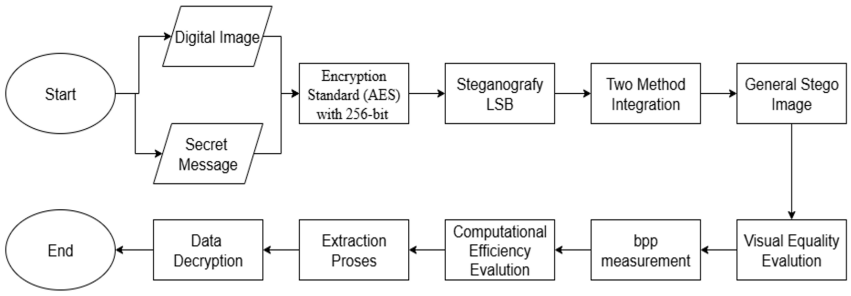

Figure 1: Research flow.

The Least Significant Bit (LSB) technique has long been the basis of image steganography. The researchers proposed an improved LSB method, capable of hiding larger amounts of data without significantly sacrificing image quality [15]. However, it demonstrated that conventional LSB methods are still vulnerable to statistical detection, prompting the development of new techniques that can overcome these weaknesses. A hybrid approach combining cryptography and steganography has emerged as a promising solution. A scheme that integrates AES encryption with wavelet transform-based steganography, achieving a high level of security [16]. Meanwhile, a method has been developed that combines chaotic encryption with adaptive steganography, showing a good balance between security and efficiency [17].

The Two-Way Oscillation (TWO) technique, which was used for image compression, has shown potential in improving data security. Adapted TWO techniques for steganography, demonstrating significant improvements in robustness to steganalysis compared to standard LSB methods. However, their research also revealed that this technique has lim-

itations in terms of data hiding capacity [18]. Evaluation of the performance of image security techniques remains a crucial aspect of research. Comprehensive comparative study of various hybrid methods, using metrics such as the Peak Signal-to-Noise Ratio (PSNR), the Structural Similarity Index (SSIM), and security analysis. Their findings highlight the importance of approaches that can optimize the balance between security, capacity, and visual quality [19].

Recent developments in the field of artificial intelligence have also made a significant contribution to digital image security. An optimized steganography method using a genetic algorithm, which adaptively selects the optimal location for data embedding [20]. This approach shows substantial improvements in terms of imperceptibility and robustness to machine learning-based steganalysis. Although significant progress has been made, challenges remain in developing image security techniques that strike a balance between security, efficiency, and visual quality [21]. Other research identified the need for an approach that can quickly adapt to evolving security threats while maintaining compatibility with existing systems. Their research emphasizes the importance of developing innovative hybrid techniques, such as combining LSB with TWO, which have the potential to overcome the limitations of existing methods and pave the way for more comprehensive image security solutions.

Research has shown that a hybrid approach that combines these two methods offers a more comprehensive solution than using each technique separately. The Least Significant Bit (LSB) method remains a strong basis in steganography, but its development continues to be carried out to overcome vulnerabilities to statistical detection. The Two-Way Oscillation (TWO) technique has shown great potential in improving resistance to steganalysis, although it still has limitations in data hiding capacity. Performance evaluations using various metrics have emphasized the importance of balancing security, capacity, and visual quality. Recent developments in artificial intelligence, such as the use of genetic algorithms, have paved the way for more adaptive optimization of steganography techniques. Although significant progress has been made, there is still a need for innovative approaches that can quickly adapt to evolving security threats. Combining LSB with TWO, as proposed in this research, offers the potential to overcome the limitations of existing methods and provide more effective and efficient image security solutions in facing digital security challenges.

This research introduces a new approach to digital image security by combining advanced cryptography with improved steganography techniques. The proposed method combines an improved Least Significant Bit (LSB) algorithm with a modified Two-Way Oscillation (TWO) technique to achieve superior security and invisibility. This research uses a diverse dataset consisting of 1000 digital images, consisting of grayscale and color images with various resolutions (512×512, 1024×1024, 2048×2048 pixels), sourced from standard databases such as USC-SIPI and BOWS-2. To test the capacity and flexibility using a set of confidential data for embedding, including text files, thumbnail, and binary data, varying in size from 1KB to 1MB.

The first stage of the method involves the encryption of confidential data. We use Advanced Encryption Standard (AES) with 256-bit keys in Cipher Block Chaining (CBC) mode, implemented using the OpenSSL library. This strong encryption ensures that even if the steganography techniques are compromised, the embedded data remains secure. The encrypted data are then prepared for the steganography process, which is the essence of this new approach.

The improved LSB technique forms the basis for the steganography process. We develop an adaptive bit selection algorithm that analyzes the local pixel neighborhood to determine the most suitable bits for modification. This approach significantly increases the fuzziness of the embedded data compared to traditional LSB methods. The selection process takes into account factors such as pixel intensity, local contrast, and edge information to minimize visual distortion in the resulting stegoimage.

The integration of TWO algorithms with improved LSB techniques represents an important innovation in this approach. Originally used for image compression, adapting the TWO algorithms to create nonlinear embedding patterns that oscillate between different bit planes. These oscillations significantly increase resistance to statistical steganalysis attacks by disrupting the common patterns that such attacks seek to identify. Combining LSB and TWO techniques results in a powerful steganography method that maintains high visual quality while offering increased security.

The extraction and decryption process mirrors the embedding process in reverse. The reverse TWO algorithm is used to identify the location of the data embedded in the stegoimage. Once this location is determined, the hidden data are extracted and further decrypted using the AES decryption algorithm with a shared secret key. This process ensures that only the intended recipient who has the correct key can access the hidden information. To evaluate the performance of the method by performing a series of comprehensive tests and assessing visual quality using Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM) metrics.

Embedding capacity is measured in bits per pixel (bpp) for various image types and sizes. Security analysis includes testing resistance to statistical and machine learning-based steganalysis attacks, specifically Chi-square attacks and RS steganalysis. It also measures computational efficiency by recording embedding and extraction times on standard computing platforms. All experiments were repeated 30 times to ensure statistical significance and the results were analyzed using appropriate statistical tests.

3 Results

3.1 Ciphertext Embedding Process

The ciphertext embedding process starts by determining the input data used, which includes passwords, secret messages, and digital images that will be used. Here we take the example of a password: WISUDA20, a secret message: STT DUMAI, and a digital image. The Message Encryption process starts from the ROT13 encryption by shifting the character forward 13 times, counting 1 being the character in front, and shifting the character based on the sequence of characters in the ASCII table. ROT13 is designed for security on systems that are often used in online forums. The STT DUMAI secret message is encrypted in an FGG QHZNV chipper text. The resulting ciphertext will be inserted into the pixel cover image, as illustrated in Figure 2.

The next step processes the comparison of the total image pixel bits with the total ciphertext bits. Hiding a secret message is successful if the total ciphertext bits are not greater than the total bits of the cover image, which will cause some of these bits not to be able to be stored in the cover image, so that the secret message cannot be retrieved during the extraction process. The process of inserting / embedding the encrypted ciphertext in the form of “FGG QHZNV”, the ciphertext is converted into a decimal number using the ASCII

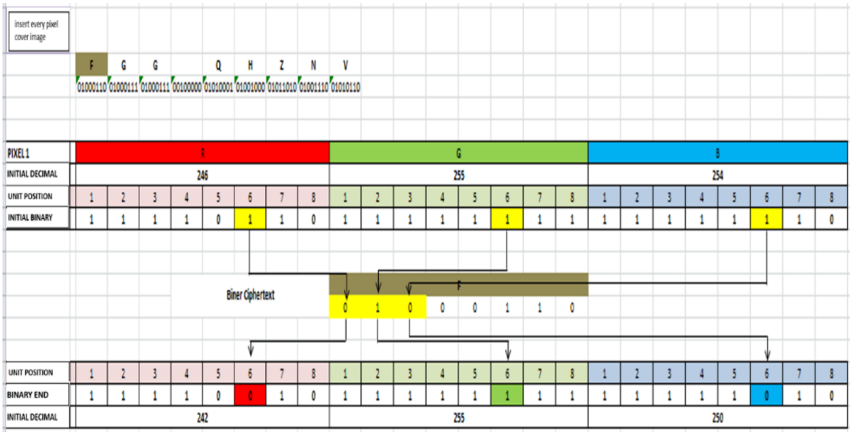

Figure 2: 6th bit swap of 1st pixel color element.

table guidelines. After converting the decimal to binary, the next stage is to exchange the 6th bit in each pixel color element with the ciphertext. The output of the encryption process is shown in Figure 3.

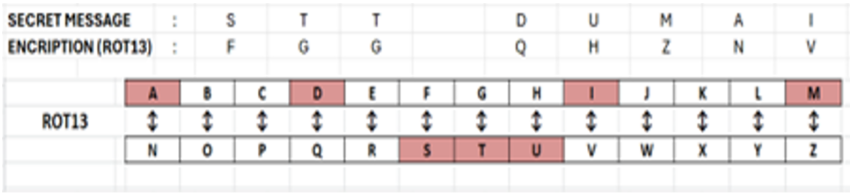

Figure 3: Encryption output.

3.2 Ciphertext Extraction Process

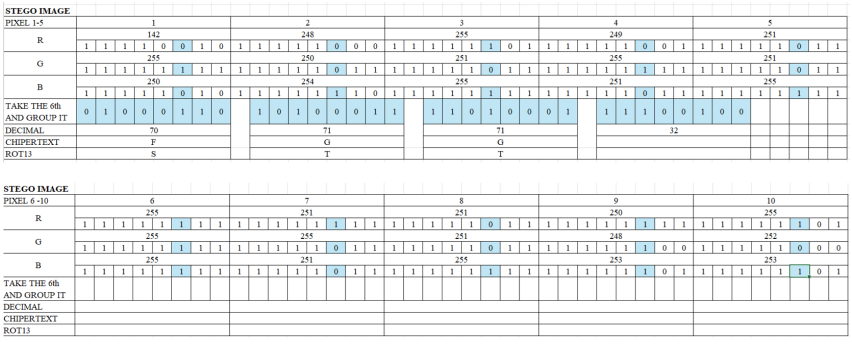

Figure 4: Decrypt secret messages on pixel 1-10.

The process of extracting secret messages that have been hidden in digital images by taking the LSB+two value from the stegoimage (message container image). The total LSB+two of the stegoimage image taken corresponds to the total ciphertext bits of the secret message that was previously hidden. The binaries are grouped into 8 bits each, allowing the formation of ciphertext characters (1 character = 8 bits). The binary group is then converted into character form, so that the hidden ciphertext is obtained.

The subsequent stage performs ciphertext decryption using the ROT13 algorithm to recover the original message. This process involves retrieving the sixth bit from pixels 1–10, which had previously been replaced with ciphertext bits or secret messages. After extraction, bits are grouped into 8-bit sequences, converted from binary to decimal, and then decoded using ROT13 with a change of k = 13. As illustrated in Figure 4, this process successfully reconstructs the hidden secret message.

Subsequently, the sixth bit from pixels 11–20, which had previously been replaced with ciphertext bits or secret messages, is retrieved. The extracted bits are then grouped into 8-bit sequences, converted from binary to decimal, and decrypted using the ROT13 algorithm with a shift of k=13. As illustrated in Figure 5, this process results in the reconstruction of the hidden secret message.

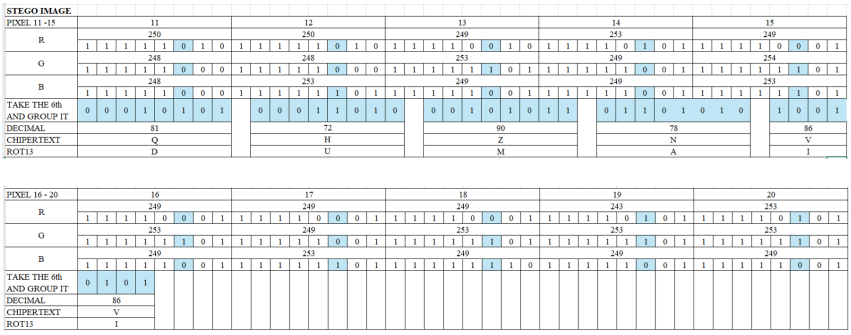

Figure 5: Decrypt secret messages on pixel 11-20.

The next step involves designing the system flow, represented in the form of processes that occur within the system, and modeled using a Use Case Diagram. The diagram illustrates the interaction between two main actors, namely the sender and the recipient, in operating the system according to their respective needs. When selecting the embedding process, the sender is required to enter a password, upload a cover image, and enter a secret message. In contrast, when selecting the extraction process, the recipient provides the password and uploads the cover image to retrieve the hidden message. As depicted in Figure 6, the Use Case Diagram provides an overview of the functional interactions within the system.

Figure 6 explains the use case diagram of the system that will be created which consists of users, namely people who use the system and carry out the embedding and extraction process by inputting data into the system, embedding which is the process of inserting secret messages with a combination of cryptography and steganography in digital images, and use case extraction which is Stegoimage extraction process to find hidden secret messages in digital images.

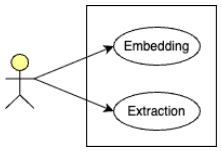

Figure 6: Use case diagram system.

The subsequent stage is the implementation of the system design to support both the embedding and extraction processes. On the Embedding Page, the sender inserts a secret message into the cover image by providing three inputs: a password, an uploaded cover image, and the secret message. After processing, a stego image is generated, which can be downloaded and sent to the recipient for extraction. As illustrated in Figure 7, the Embedding Page view presents the interface that facilitates this process.

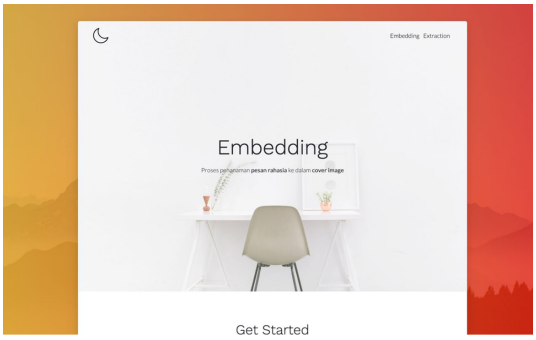

Figure 7: Embedding page view.

The extraction page facilitates the process for the recipient to retrieve the secret message embedded within the stego image. To perform extraction, the recipient provides two inputs: the user ID and a password (identical to the sender's password), along with uploading the stego image. Once processed, the hidden secret message is successfully revealed. As illustrated in Figure 8, the Extraction Page view presents the interface for this decryption process.

4 Discussion

There are many studies that use cryptography and steganography in digital images. The Least Significant Bit (LSB) technique is widely used in steganography. Several researchers have used LSB for their research. The weakness of LSB is that the number of messages inserted is limited and is easily detected with steganography algorithms. The researchers proposed an improved LSB method, capable of hiding larger amounts of data without significantly sacrificing image quality [15]. Combining the two LSB and TWO methods can improve data security, as can be seen in the results of the research. It can be seen in the data input process that it contains passwords, hidden messages, and used digital images. For example, using the WISUDA20 password with the STT Dumai hidden message on a

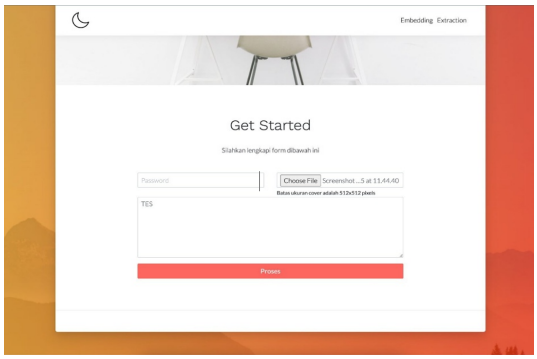

Figure 8: Extraction page view.

digital image. Enter the cyphertext, which then uses the LSB method by exchanging the pixel elements in the digital image. After the pixel exchange is performed, encryption will be obtained as output. In addition to the data encryption stage, the data decryption process is also available. What is done is to extract the secret message contained in the digital image by taking the value of LSB + TWO available in the stegoimage. By carrying out the stages as made in the data encryption, after getting the secret message that is stored, then changing the ciphertext by adding the results of the secret message.

The research tested 1000 different images as cover images against a combination of cryptography and steganography with LSB+two for information security in digital images. There is a comparison of the cover image and the stegoimage after inserting a text message using a combination of cryptography and steganography methods, as well as the quality of the image resulting from inserting the message or stegoimage.

Table 1: Combination Results of LSB+2 Cryptography and Steganography

Description	**Cover Image**	**Stegoimage**
		
Secret Message		STT DUMAI
Password		WISUDA20
Format	*.JPG	*.JPG
Picture Resolution	256 × 192 pixels	256 × 192 pixels
File Size	86 KB	86 KB
Time process	0,849 ms	
MSE	0.0036	
PSNR	72.461 dBb	

Table 1 explains the comparison between the cover image and the stegoimage with the *.JPG image format. In cases where the image resolution does not change the number of pixels at all, there is only a slight change in the file size. The MSE shows less than 1, while the obtained PSNR value is more than 45 dB. It can be concluded that the stegoimage

quality is good. Test the cover image and the stegoimage with a resized *.JPG image format. In cases where the image resolution does not change the number of pixels at all, there is only a slight change in the file size. The MSE shows less than 1, while the obtained PSNR value is 50 dB; it can be concluded that the stegoimage quality is good.

The implementation of the LSB+TWO method in data security is more difficult to detect because, according to the results obtained in Table 1, there is no difference before and after the implementation of the method. LSB+TWO also makes the watermarking technique, which usually has a difference in size, be the same as the size and lighter to apply.

This research provides contributions and the impact of modifications made to the TWO algorithm needs further clarification. The modifications we made to the TWO algorithms focus on increasing resistance to cryptanalysis attacks and increasing computational efficiency. Specifically, change the iteration structure and length of the encryption key. These changes aim to strengthen the algorithm while maintaining its processing speed. The impact of these modifications is significant, as it increases the complexity of encryption and makes the system more resistant to brute force and ciphertext-only attacks. In addition, this research clarifies the new contribution, which lies in the combination of encryption and steganography techniques, and its potential for broader applications in secure data storage and transmission.

The LSB+TWO method is more difficult to apply for determining the parameters of the ciphertext used. In the implementation of the watermark used, the method must be reviewed to find the most optimal that can be used. Although it is difficult to detect, the application of the LSB+TWO method can still be attacked, especially when there is an error in creating the ciphertext used in its encryption. Due to the weaknesses in the implementation of the LSB+TWO method, improvements are needed for further research by incorporating an AI method to insert its stegoimage and enhance the watermark during encryption. In addition, it can also be added with other encryption methods to optimize the security of the ciphertext.

5 Conclusion

This research presents an innovative approach to improving digital image security through the integration of cryptographic techniques with steganographic methods. The proposed LSB+TWO method combines the Least Significant Bit (LSB) algorithm with a modified two-way oscillation technique (TWO). The initial step involves data encryption using Advanced Encryption Standard (AES) with a 256-bit key in Cipher Block Chaining (CBC) mode, providing an additional layer of security before the data hiding process. This combination results in a powerful image security system, capable of effectively hiding confidential data while maintaining the visual quality of the image.

The evaluation results show the superiority of the LSB+TWO method in various aspects of performance. Visual quality analysis using PSNR and SSIM metrics proves that this method can maintain image integrity very well, making the stegoimage difficult to distinguish from the original image. The embedded capacity measured in bits per pixel (bpp) indicates the flexibility of the method in accommodating various sizes of secret data. The computational efficiency in terms of embedding and extraction time also shows the feasibility of this method for practical implementation. The LSB+TWO method offers a promising solution to improve digital image security, successfully achieving a high level

of security while maintaining image quality and computational efficiency. This research makes a significant contribution to the field of digital information security and paves the way for further development in image-based data protection techniques.

Acknowledgments

The authors gratefully acknowledge the support of the Department of Informatics Engineering, Politeknik Negeri Indramayu, Indonesia.

References

[1] W. B. Nugroho, A. Susanto, C. A. Sari, E. H. Rachmawanto, and M. Doheir, "A robust and imperceptible for digital image encryption using chacha20," *Jurnal Teknik Informatika (Jutif)*, vol. 5, no. 2, pp. 397–404, 2024.

[2] A. K. Sahu and M. Sahu, "Digital image steganography and steganalysis: A journey of the past three decades," *Open Computer Science*, vol. 10, no. 1, pp. 296–342, 2020.

[3] E. A. Jameel and S. A. Fadhel, "Digital image encryption techniques: Article review.," *Technium*, vol. 4, no. 2, 2022.

[4] C. A. Sari, E. H. Rachmawanto, and C. A. Haryanto, "Cryptography triple data encryption standard (3des) for digital image security," *Scientific Journal of Informatics*, vol. 5, no. 2, pp. 105–117, 2018.

[5] N. A. Fauziah, E. H. Rachmawanto, C. A. Sari, *et al.*, "Design and implementation of aes and sha-256 cryptography for securing multimedia file over android chat application," in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pp. 146–151, IEEE, 2018.

[6] E. K. A. Alobaydi, "Digital image steganography utilizing database identification," *Technium*, vol. 10, no. 1, pp. 97–105, 2023.

[7] M. A. Razzaq, R. A. Shaikh, M. A. Baig, and A. A. Memon, "Digital image security: Fusion of encryption, steganography and watermarking," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 5, 2017.

[8] Y. P. Astuti, E. H. Rachmawanto, C. A. Sari, *et al.*, "Simple and secure image steganography using lsb and triple xor operation on msb," in *2018 International Conference on Information and Communications Technology (ICOIACT)*, pp. 191–195, IEEE, 2018.

[9] A. K. Singh, J. Singh, and H. V. Singh, "Steganography in images using lsb technique," *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, vol. 5, no. 1, pp. 426–430, 2015.

[10] 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*, vol. 17, p. 1168, June 2019.

[11] S. A. Jebur, A. K. Nawar, L. E. Kadhim, and M. M. Jahefer, "Hiding information in digital images using lsb steganography technique.," *International Journal of Interactive Mobile Technologies*, vol. 17, no. 7, 2023.

[12] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image steganography using lsb and hybrid encryption algorithms," *Applied Sciences*, vol. 13, no. 21, p. 11771, 2023.

[13] M. A. F. Al-Husainy and D. M. Uliyan, "A secret-key image steganography technique using random chain codes," *International Journal of Technology*, vol. 10, no. 4, pp. 731–740, 2019.

[14] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image steganography: A review of the recent advances," *IEEE access*, vol. 9, pp. 23409–23423, 2021.

[15] Z. Wang, M. Zhou, B. Liu, and T. Li, "Deep image steganography using transformer and recursive permutation," *Entropy*, vol. 24, no. 7, p. 878, 2022.

[16] S. Gupta, S. Jain, M. Agarwal, and N. Nanda, "An encryption approach to improve the security and performance of data by integrating aes with a modified otp technique," *International Journal of Advanced Intelligence Paradigms*, vol. 27, no. 2, pp. 129–149, 2024.

[17] N. J. De La Croix and T. Ahmad, "Toward secret data location via fuzzy logic and convolutional neural network," *Egyptian Informatics Journal*, vol. 24, no. 3, p. 100385, 2023.

[18] A. P. Z. M.Tech. Scholar Ashma Naz, "A new approach for image steganography using inter pixel value difference and quantized range table method," *International Journal of Scientific Research Engineering Trends*, vol. 8, no. 2, p. 900, 2022.

[19] I. M. A. D. S. Atmaja, W. B. Triadi, I. N. G. A. Astawa, and M. L. Radhitya, "Comparison of the packet wavelet transform method for medical image compression," *JOIV: International Journal on Informatics Visualization*, vol. 7, no. 4, pp. 2373–2379, 2023.

[20] S. Ghoul, R. Sulaiman, and Z. Shukur, "A review on security techniques in image steganography," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, 2023.

[21] Z. Fu, F. Wang, and X. Cheng, "The secure steganography for hiding images via gan," *EURASIP Journal on Image and Video Processing*, vol. 2020, no. 1, p. 46, 2020.