Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 10, No. 3, August, Pp. 377-386

Optimized visualization of digital image steganography using least significant Bits and AES for secret key encryption

Cahaya Jatmoko*[1,2], Daurat Sinaga[1,2], Heru Lestiawan[1,2], Erna Zuni Astuti[1,2], Christy Atika Sari[1,2], Guruh Fajar Shidik[1,2], Pulung Nurtantio Andono[1,2], Noorayisahbe Mohd. Yaacob[3]
Study Program in Informatics Engineering, Universitas Dian Nuswantoro, Indonesia[1]
Research Center for Intelligent Distributed Surveillance and Security, Universitas Dian Nuswantoro, Semarang, Indonesia[2]
Center for Software Technology and Management (SOFTAM), Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Selangor, Malaysia[3]

Article Info
Keywords:
Advanced Encryption Standard, Data Hiding, Digital Image, Image Steganography, Least Significant Bits

Article history:
Received: February 13, 2025
Accepted: July 01, 2025
Published: August 31, 2025

Cite:
C. Jatmoko, "Optimized Visualization of Digital Image Steganography using Least Significant Bits and AES for Secret Key Encryption", *KINETIK*, vol. 10, no. 3, Aug. 2025.
https://doi.org/10.22219/kinetik.v10i3.2252

*Corresponding author.
Cahaya Jatmoko
E-mail address:
cahayajatmoko@dsn.dinus.ac.id

Abstract
Data hiding is a technique used to embed secret information into a cover medium, such as an image, audio, or video, with minimal distortion, ensuring that the hidden data remains imperceptible to an observer. The key challenge lies in embedding secret information securely while maintaining the original quality of the host medium. In image-based data hiding, this often means ensuring the hidden data cannot be easily detected or extracted while still preserving the visual integrity of the host image. To overcome this, we propose a combination of AES (Advanced Encryption Standard) encryption and Least Significant Bit (LSB) steganography. AES encryption is used to protect the secret images, while the LSB technique is applied to embed the encrypted images into the host images, ensuring secure data transfer. The dataset includes grayscale 256x256 images, specifically "aerial.jpg," "airplane.jpg," and "boat.jpg" as host images, and "Secret1," "Secret2," and "Secret3" as the encrypted secret images. Evaluation metrics such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Unified Average Changing Intensity (UACI), and Number of Pixels Changed Rate (NPCR) were used to assess both the image quality and security of the stego images. The results showed low MSE (0.0012 to 0.0013), high PSNR (58 dB), and consistent UACI and NPCR values, confirming both the preservation of image quality and the effectiveness of encryption for securing the secret data.

1. Introduction

With the development of the Internet, one of the main concerns is the security of the information communicated [1]. In the context of visual data, the need for efficient protection techniques is increasing, especially with the growing exchange of images and videos on digital platforms [2]. Approaches that allow the insertion of information into visual media without disturbing its original appearance are becoming very relevant, as they can protect sensitive data from unauthorized access [3], [4], [5]. This is important not only to maintain individual privacy but also to support information security in applications such as banking, identity verification, and communication secrecy [6], [7]. The integration of technologies that can intelligently hide information in visual data provides a strategic solution in the digital era, which is increasingly vulnerable to security threats [8].

Recently, steganography has been widely presented as an innovative solution to secure visual data in an unobtrusive way [9], [10]. These techniques allow sensitive information to be embedded into visual media without altering the main characteristics of the media, thus remaining undetectable by unauthorized parties [11], [12]. The methods developed continue to focus on improving security, efficiency, and resistance to various cracking attempts. This makes steganography an increasingly relevant approach for protecting confidential communications, both for personal purposes and in a wider scope of applications, such as cybersecurity and confidential data protection in various sectors [13], [14].

Many researchers have studied steganography for data security, especially using the LSB method, such as Islam et al. [15], who stated that steganography hides secret data in ordinary, unsuspecting files to avoid visual detection. Their research proposed a new data hiding method using LSB-based steganography, where secret information is only embedded in selected image pixels. To determine candidate pixels, image pixel information is used to filter the entire image, and additional security is applied through the use of a user-defined password. Mahdi et al. [16] revealed research that uses a combination of the MSB and LSB in image-based steganography to hide data with a secret key. The researchers utilize color images (24-bit for RGB channels) as the data embedding medium. In the proposed method, the MSB bits are checked to determine the specific part of the pixels to be manipulated, while the LSB bits are changed with the secret message to be hidden. AbdelWahab et al. [17] studied steganography as a method to embed hidden

messages in a non-suspicious way, so that only the sender and intended recipient are aware of its existence. This study compares two main approaches. The first approach uses the LSB method without involving encryption or compression processes. In the second approach, the secret message is encrypted first before being applied using the LSB method. In addition, the DCT is used to convert the image from the spatial domain to the frequency domain. In the LSB-based method, the payload bits are inserted directly into the least significant bits of the cover image to produce a stego image. Meanwhile, the DCT-based approach inserts the payload bits into the frequency components of the cover image after the transformation, resulting in a stego image with a higher level of complexity and resistance to manipulation.

In contrast to the related research above, this study integrates the AES method with LSB-based steganography to improve the security and quality of data embedding results. In previous research, Islam et al. [15] proposed a technique that embeds secret information into selected pixels using LSB, with additional security via user-defined passwords. However, this method does not include encryption, making it vulnerable to visual and statistical attacks. Mahdi et al. [16] combined Most Significant Bit (MSB) and LSB in color images to improve complexity, but this approach risks visible distortion due to modifications in high-weight RGB channels. AbdelWahab et al. [17] compared two embedding strategies: one using plain LSB without encryption, and another using encryption with Discrete Cosine Transform (DCT) for embedding in the frequency domain. While the latter improves robustness, it adds computational overhead and reduces efficiency, especially for small grayscale images.

These studies, while contributing valuable approaches, exhibit key limitations. Some fail to secure the hidden message, others compromise image quality, and a few trade efficiency for robustness. None have effectively addressed the balance between visual quality, embedding capacity, and security—particularly for lightweight grayscale image applications. To address these gaps, this study proposes a hybrid method that combines AES with LSB steganography. AES encrypts the secret data to ensure strong protection, while LSB embeds the ciphertext into host images with minimal visual distortion. This dual-layer approach aims to deliver a practical solution that maintains high visual fidelity, enhances security, and remains efficient for grayscale image scenarios.

2. Research Method

The embedding process (marked with green arrows) starts from two main inputs: the host image and the secret image. The secret image is encrypted using the AES algorithm to produce an encrypted secret image, which is then fed into the LSB embedding map along with the host image. The output is a steganographic image that hides the secret information. The extracting process (marked with red arrows) begins with the steganographic image. The data is reset to the default LSB embedding map to extract the encrypted secret image. Next, the secret image is decrypted using the AES algorithm to retrieve the original secret image, which is then displayed. The flow of the proposed steganographic process can be seen in Figure 1.

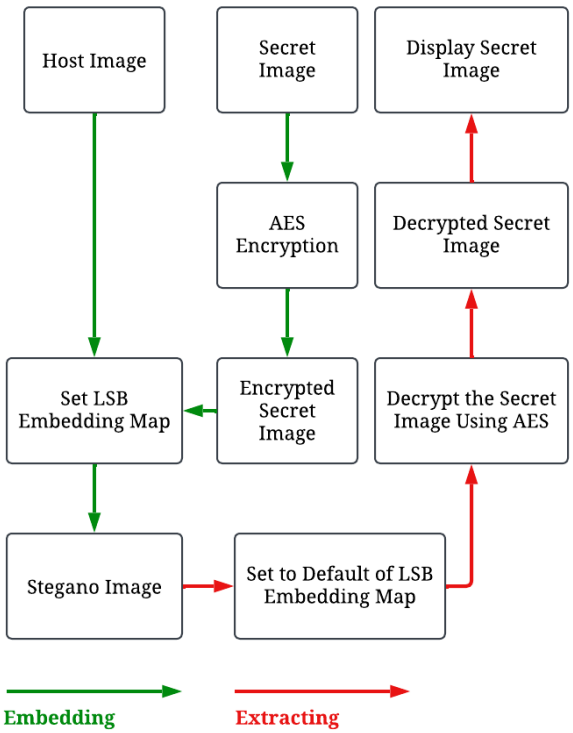


Figure 1. Flowchart of Embedding and Extracting Process

2.1 Advanced Encryption Standard (AES)

In this study, AES is a symmetric encryption algorithm that operates on fixed-size blocks, usually 128 bits, and uses a key length of 128, 192, or 256 bits, thus providing flexibility in the level of security [18]. Its effectiveness in image encryption lies in its ability to withstand various attacks, such as brute force or differential analysis [19].

In this study, a 128-bit key is used for generating round keys through the key schedule process, which is employed in each encryption iteration [20]. AES-128 runs the encryption process in 10 rounds, where each round applies a series of operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey, except for the last round, which does not include MixColumns [21], [22]. Additionally, if the plaintext data is an image measuring 256 x 256 pixels in grayscale format, then the data size is 256 x 256 x 8 = 524,288 bits. This data is then broken down into blocks of 128 bits, resulting in a total of 4,096 plaintext blocks. The block state as indicated in Equation 1.

$$Block\ State = \begin{bmatrix} B_{0,0} & B_{0,1} & B_{0,2} & B_{0,3} \\ B_{1,0} & B_{1,1} & B_{1,2} & B_{1,3} \\ B_{2,0} & B_{2,1} & B_{2,2} & B_{2,3} \\ B_{3,0} & B_{3,1} & B_{3,2} & B_{3,3} \end{bmatrix} \quad (1)$$

Each plaintext block will be processed individually through 10 rounds of iteration using round keys generated from a 128-bit key, ensuring that a secure ciphertext is obtained for each block. This encryption process ensures that the data is strongly protected through a combination of diffusion and confusion resulting from these operations. The AES equation below represents block states, SubBytes, ShiftRows and MixColumns, AddRoundKey, and key expansion.

$$B'_{i,j} = S(B_{i,j}) \quad (2)$$

Equation 2 represents SubBytes equation, where S(x) is the substitution function based on the S-Box table, and the first row remains unchanged. ShiftRows operates as follows: the second row is shifted 1 position to the left, the third row is shifted 2 positions to the left, the fourth row is shifted 3 positions to the left. ShiftRows and MixColumns are two important operations in AES that work together to achieve diffusion. The combined process of both can be seen in Equation 3.

$$Block\ State = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} B_{0,j} \\ B'_{1,j} \\ B''_{2,j} \\ B'''_{3,j} \end{bmatrix} \quad (3)$$

Based on Equation 2, each element $B'_{i,j}$ represents a byte in the state and produces a combination of the diffusions shown in Equation 3. While Equation 4 illustrates the **MixColumns** transformation, where each new state byte $C_{i,j}$. Each element is calculated using operations in the Galois space $GF\ (2^8)$. The result of the previous step is XORed with AddRoundKey, as seen in Equation 5. Equation 6 describes the **key expansion** step in which the new word $W[i]$ is obtained by XORing $W[i-4]$ with the transformed version of $W[i-1]$ through the function G

$$C_{i,j=}(2 \cdot B_{i,j}) \oplus (3 \cdot B_{i+1,j}) \oplus (1 \cdot B_{i+2,j}) \oplus (1 \cdot B_{i+3,j}) \quad (4)$$

$$State' = State \oplus Key_{round} \quad (5)$$

$$W[i] = W[i-4] \oplus G(W[i-1]) \quad (6)$$

The master key is transformed into a series of round keys Key_{round} using transformations based on XOR, rotation, and substitution operations. The conclusion (cipher image) of AES encryption is presented in Equation 7.

$$MixColumns(ShiftRows(SubBytes(State_{i-1}))) \oplus Key_i \quad (7)$$

Equation 7 is the result of combining all the previous equations. This combination produces a cipher image in which all the equations are interconnected and work in an integrated manner to produce a cipher secret image. The flow of the proposed method based on AES encryption can be seen in Figure 2.

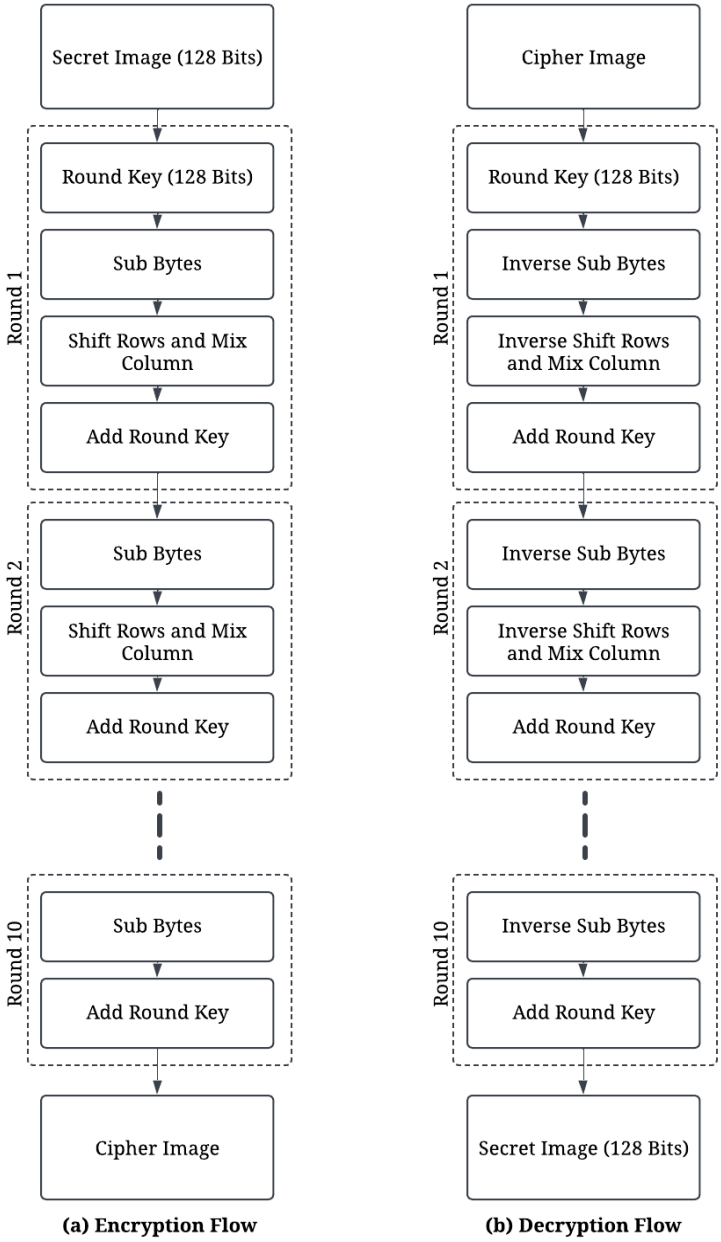


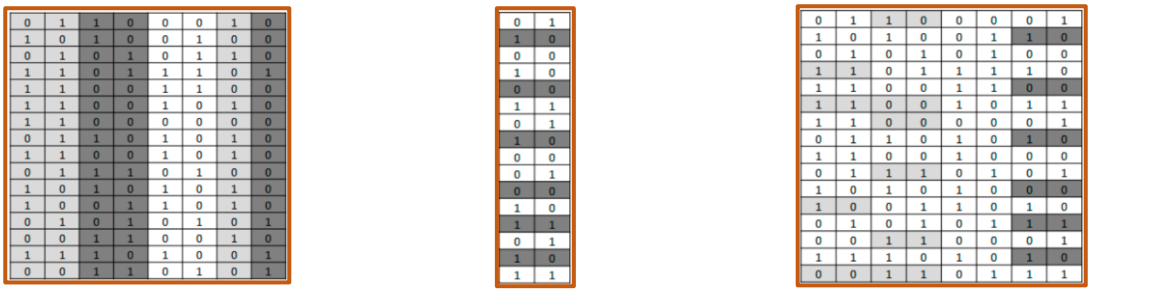
Figure 2. Flowchart of AES Encryption and Decryption

2.2 Least Significant Bits (LSB)

LSB is one of the most common steganography techniques used to embed secret data into cover media, such as digital images [23]. This technique modifies the least significant bits of the image pixels so that the changes are invisible to the human eye [24]. After the data is encrypted, the result, called the "Encrypted Secret Image," is then embedded into the host image using the LSB technique. In the LSB method, only the least significant bits of each pixel in the cover image are modified to hide part of the encrypted result, ensuring that it does not significantly affect the visual quality of the image [25]. This embedding process can be seen in Equation 8.

$$C'(i,j) = \begin{cases} C(i,j) & if\ LSB(C(i,j)) = S(k) \\ C(i,j) - 1 & if\ LSB(C(i,j)) = 1\ dan\ S(k) = 0 \\ C(i,j) + 1 & LSB(C(i,j)) = 0\ dan\ S(k) = 1 \end{cases} \quad (8)$$

Here, $C(i,j)$ represents the pixel intensity value at position (i,j) in the cover image (host image), while $S(k)$ is the bit of the secret data (the secret image encryption result using AES) to be embedded. After the embedding process, the new pixel value is generated as $C'(i,j)$, which is the pixel in the stego image that contains the hidden data. The process involves modifying the least significant bit of $C(i,j)$, so that the value of $C'(i,j)$ does not visually differ but successfully embeds the data $S(k)$ safely into the cover image. These steps are repeated for all pixels until all the secret image data S is inserted into the cover image. Based on Figure 3, (a) Host Image in pixel represents the initial intensity values of the pixels in the host image, which serve as the cover media. Next, (b) the last bit of the encrypted secret image corresponds to the least significant bits of the encrypted secret image, prepared for embedding into the host image. Finally, (c) Embedded Stegano Image in pixel depicts the resulting stego image, where the least significant bits of the host image pixels have been modified to conceal the encrypted data.



(a) Host Image in pixel (b) Last bit of encrypted (b) Embedded Stegano Image in pixel

Figure 3. Embedding Process Based on LSB

2.3 Sample Testing Data

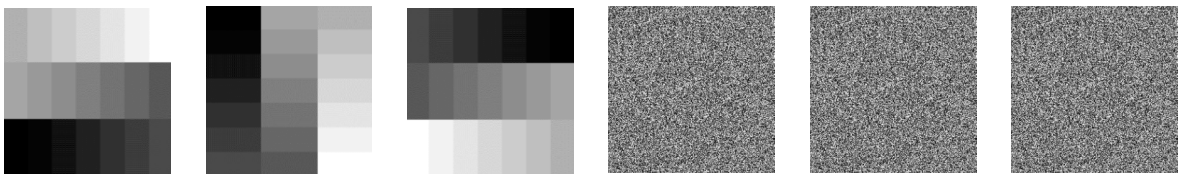
For the testing phase, this study uses data samples with a resolution of $256\ x\ 256$ pixels in grayscale format. The dataset comprises three host images: aerial, airplane, and boat, which act as cover media for embedding. Additionally, three secret images, labeled as secret1, secret2, and secret3, are included. These secret images will undergo encryption in the subsequent section to enhance security before being embedded into the host images. All images in this study are stored in JPG format, ensuring compatibility with the proposed embedding algorithm. The sample of the testing data can be seen in Figure 4.

(a) Aerial (b) Airplane (c) Boat (d) Secret1 (e) Secret2 (f) Secret3

Figure 4. Sample data: (a)-(c) Host Image, (d)-(f) Secret Image

3. Results and Discussion

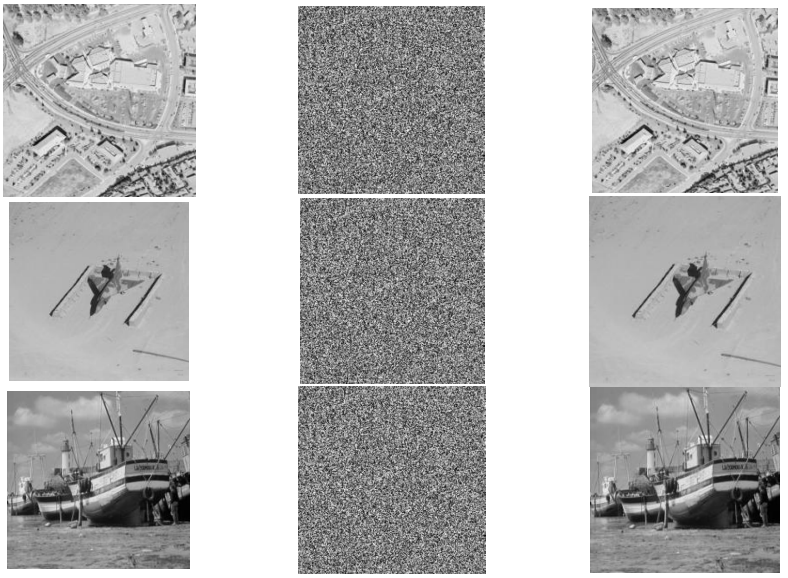
In this chapter, the analysis process is carried out in stages according to the method flow proposed in the previous chapter. Each stage will be explained in detail to illustrate how the algorithm runs from the beginning to the production of a stego image. Before delving into the discussion, it should be stated that this study uses MATLAB 2024a software to run the algorithm process. The hardware used has the following specifications: a 12th generation Intel i5 processor, an NVIDIA GeForce RTX 3060 graphics card, 32 GB RAM memory, and 2 TB SSD storage. These specifications were chosen to ensure optimal performance in data processing and running algorithm simulations efficiently.



(a) Secret1 (b) Secret2 (c) Secret3 (d) Encrypted Secret1 (e) Encrypted Secret2 (f) Encrypted Secret3

Figure 5. Encryption Phase

As observed, the pixel values of the secret images have been significantly altered, making it impossible to visually identify any pattern or structure of the original image. This ensures the confidentiality of the secret message, as the visual content of the images is effectively concealed through the encryption process, preparing them for the next step in the embedding process using LSB. After the encryption process, the next step involves embedding the encrypted secret images into the cover images using the LSB technique. In this stage, the encrypted secret images (d) Encrypted Secret1, (e) Encrypted Secret2, and (f) Encrypted Secret3 are embedded into the corresponding host images. The LSB technique modifies the least significant bits of the pixel values in the cover images to hide the encrypted secret image, ensuring that the visual quality of the host images remains largely intact. The results of this embedding process are shown in Figure 6, where the stego images, which now contain the hidden encrypted secret images, are displayed.



(a) Host Image (b) Encrypted Secret1 (c) Stegano Image

Figure 6. Embedding Phase

3.1 MSE and PSNR Assessment

MSE (Mean Squared Error) and PSNR (Peak Signal-to-Noise Ratio) are metrics used to evaluate image quality. MSE calculates the average squared difference between the original and processed images, with lower values indicating better quality [26]. PSNR measures the ratio between the peak signal and the noise, with higher values suggesting minimal distortion and better quality. These metrics help assess the impact of encryption or steganography on image quality, ensuring that the stego image remains visually acceptable [27]. The MSE and PSNR equations can be seen in Equations 9 and 10. The results of the MSE and PSNR calculations can be found in Table 1.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j) - K(i,j)\right)^{2} \tag{9}$$

$$PSNR = 10\log 10\left(\frac{\max\ \_pixel\_value^{2}}{MSE}\right) \tag{10}$$

Table 1. MSE and PSNR Assessment

Host Image	Encrypted Secret Image	MSE	PSNR
Aerial	Secret1	0.0012	78.131 dB
	Secret2	0.0012	78.172 dB
	Secret3	0.0012	78.398 dB
Airplane	Secret1	0.0013	78.702 dB
	Secret2	0.0013	78.431 dB
	Secret3	0.0012	78.760 dB
Boat	Secret1	0.0012	78.890 dB
	Secret2	0.0012	78.111 dB
	Secret3	0.0013	78.274 dB

Table 1 presents the quality metrics for each host image, where the encrypted secret images are embedded using the proposed method. The MSE and PSNR values indicate the degree of distortion in the host images after embedding, with lower MSE and higher PSNR values reflecting better image quality and minimal visual distortion. MSE and PSNR values are provided for three host images (Aerial, Airplane, and Boat) along with corresponding encrypted secret images (Secret1, Secret2, and Secret3). The MSE values are consistently low, ranging from 0.0012 to 0.0013, indicating minimal distortion between the host images and their respective stego images. Meanwhile, the PSNR values are relatively high, ranging from 58.111 dB to 58.890 dB, suggesting that the embedding process has resulted in minimal degradation of image quality.

3.2 UACI and NPCR Assessment

UACI (Unified Average Changing Intensity) and NPCR (Normalized Pixel Change Rate) are used to evaluate the robustness and variation of the embedding process. UACI measures average pixel intensity changes, while NPCR calculates the percentage of altered pixels [28]. Higher values indicate significant embedding changes, ensuring that the secret image is well-hidden while maintaining the image's quality [29]. These metrics assess the effectiveness and imperceptibility of the steganography method [30]. The UACI and NPCR equations can be seen in Equations 11 and 12, respectively. The results of these measurements can be found in Table 2, where the UACI and NPCR values are provided for each host image, showing the effectiveness and imperceptibility of the embedded encrypted secret image. Meanwhile, UACI values are consistently range from 33.32 to 33.34, indicating a high degree of change between the original host images and their corresponding stego images, which suggests effective embedding with minimal perceptible distortion. The NPCR values range from 99.48 to 99.59, reflecting a high rate of pixel changes between the original and stego images, which is desirable for ensuring the security of the stego image.

$$UACI = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j) \oplus K(i,j)}{L}\right| \quad (11)$$

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j)-K(i,j)}{I(i,j)}\right| \quad (12)$$

Table 2. UACI and NPCR Assessment

Host Image	Encrypted Secret Image	UACI	NPCR
Aerial	Secret1	33.32	99.51
	Secret2	33.34	99.59
	Secret3	33.34	99.57
Airplane	Secret1	33.33	99.55
	Secret2	33.34	99.49
	Secret3	33.33	99.59
Boat	Secret1	33.34	99.58
	Secret2	33.33	99.51
	Secret3	33.34	99.48

3.3 Testing Phase

In this phase, the embedding results are visually assessed to evaluate the quality of the stego image. The embedding process yields a stego image that closely resembles the original host image, with minimal distortion despite the embedding of the encrypted secret image. This visual similarity between the host image and the stego image indicates the effectiveness of the LSB method for hiding encrypted information while maintaining the visual integrity of the cover image. The overall results of the testing can be observed in Figures 7-9. The testing results show that after embedding the encrypted secret images into the host images, the stego images closely resemble the original host images. Whether it is the "aerial.jpg," "airplane.jpg," or "boat.jpg," each host image, when embedded with Secret1, Secret2, or Secret3, still maintains its visual integrity. The embedded images are visually indistinguishable from the original host images, indicating that the embedding process using the AES encryption and LSB steganography method successfully preserves the visual appearance of the host image while securely hiding the encrypted content. This confirms the effectiveness of the proposed method in producing high-quality stego images.


(a) Sample Host (aerial.jpg)


(b) Embedded with Secret1


(b) Embedded with Secret2


(b) Embedded with Secret3

Figure 7. Testing Results of aerial.jpg


(a) Sample Host (airplane.jpg)


(b) Embedded with Secret1


(b) Embedded with Secret2


(b) Embedded with Secret3

Figure 8. Testing Results of irplane.jpg


(a) Sample Host (boat.jpg)


(b) Embedded with Secret1


(b) Embedded with Secret2


(b) Embedded with Secret3

Figure 9. Testing Results of boat.jpg

To further validate the effectiveness of the proposed hybrid method (AES + LSB), an ablation study was conducted by testing the system with only LSB steganography, omitting the AES encryption phase. The performance was evaluated using the same host and secret images as in the full implementation. The results showed that while the LSB-only approach achieved similar PSNR values (around 78 dB), it lacked cryptographic protection and was vulnerable to statistical extraction. In contrast, the hybrid method maintained high image quality while providing an additional layer of security, making the embedded content significantly more resistant to attacks.

In addition, a comparative analysis was performed between the proposed method and other steganographic techniques mentioned in Section 1, including MSB + LSB hybridization [16] and DCT-based embedding with encryption [17]. The MSB + LSB method, though offering moderate robustness, introduced noticeable artifacts in color images, as reported in [16]. The DCT-based method proposed by AbdelWahab et al. [17], while robust, requires high computational resources and is less suitable for lightweight applications. Compared to both, the proposed AES + LSB approach offers a balanced trade-off between image quality (PSNR ≥ 78 dB), embedding imperceptibility and data security, especially for grayscale images. These findings emphasize the benefit of combining AES encryption with LSB steganography, providing strong protection without compromising visual quality or efficiency.

4. Conclusion

In this research, an AES-based encryption method was successfully integrated with Least Significant Bit (LSB) steganography to embed encrypted secret images into host images. The results of the MSE and PSNR evaluations showed excellent performance, with MSE values ranging from 0.0012 to 0.0013, and PSNR values between 58.111 dB and 58.890 dB across all cases, indicating minimal distortion during the embedding process. Furthermore, the UACI values ranged between 33.32 and 33.34, and the NPCR values were consistently above 99.48, demonstrating the robustness of the system against changes or attacks. The visual inspection showed that the stego images closely resembled the original host images, confirming that the embedding technique maintained high image quality while ensuring the secrecy of the embedded content. For future research, the proposed method can be further enhanced by exploring the use of advanced encryption techniques or hybrid methods to increase security, such as combining AES

with other cryptographic algorithms. Further optimization of the LSB technique could be implemented to improve both embedding capacity and robustness against more sophisticated attacks.

Acknowledgement

The authors would like to express their sincere gratitude to Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Dian Nuswantoro (UDINUS) for providing financial support for this research through the Internal Research Scheme.

References

[1] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," Cyber Security and Applications, vol. 2, p. 100031, 2024. https://doi.org/10.1016/j.csa.2023.100031
[2] R. Verma, A. Kumari, A. Anand, and V. S. S. Yadavalli, "Revisiting Shift Cipher Technique for Amplified Data Security," Journal of Computational and Cognitive Engineering, vol. 3, no. 1, pp. 8–14, Aug. 2022. https://doi.org/10.47852/bonviewJCCE2202261
[3] M. S. Abdalzaher, M. M. Fouda, and M. I. Ibrahem, "Data Privacy Preservation and Security in Smart Metering Systems," Oct. 01, 2022, MDPI. https://doi.org/10.3390/en15197419
[4] M. Wazid, A. K. Das, V. Chamola, and Y. Park, "Uniting cyber security and machine learning: Advantages, challenges and future research," Sep. 01, 2022, Korean Institute of Communication Sciences. https://doi.org/10.1016/j.icte.2022.04.007
[5] H. N. Khalid, A. Hafizah, and M. Aman, "Digital Image Steganography in Spatial Domain: A Critical Study," 2020.
[6] F. Varghese and P. Sasikala, "A Detailed Review Based on Secure Data Transmission Using Cryptography and Steganography," Apr. 01, 2023, Springer. https://doi.org/10.1007/s11277-023-10183-z
[7] Z. Halim, N. P. M. A. Durya, K. Kraugusteeliana, S. Suherlan, and A. L. Alfisyahrin, "Ethics-Based Leadership in Managing Information Security and Data Privacy," Jurnal Minfo Polgan, vol. 12, no. 2, pp. 1819–1828, Sep. 2023. https://doi.org/10.33395/jmp.v12i2.13018
[8] E. Halboosa, "A systematic review: security information for agent approaches in networks - models and methods," PRZEGLĄD ELEKTROTECHNICZNY, vol. 1, no. 5, pp. 262–271, May 2023. https://doi.org/10.15199/48.2023.05.45
[9] M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," in IOP Conference Series: Materials Science and Engineering, Institute of Physics Publishing, Jun. 2019. https://doi.org/10.1088/1757-899X/518/5/052003
[10] P. Mathivanan and A. Balaji Ganesh, "ECG steganography using Base64 encoding and pixel swapping technique," Multimed Tools Appl, vol. 82, no. 10, pp. 14945–14962, Apr. 2023. https://doi.org/10.1007/s11042-022-14072-8
[11] I. P. Pujiono, E. H. Rachmawanto, and D. A. Nugroho, "The Implementation of Improved Advanced Encryption Standard and Least Significant Bit for Securing Messages in Images," Journal of Applied Intelligent System, vol. 8, no. 1, pp. 69–80, 2023. https://doi.org/10.33633/jais.v8i1.7324
[12] E. A. Sofyan, C. A. Sari, H. Rachmawanto, and R. D. Cahyo, "High-Quality Evaluation for Invisible Watermarking Based on Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD)," Advance Sustainable Science, Engineering and Technology (ASSET), vol. 6, no. 1, 2024. https://doi.org/10.26877/asset.v6i1.17186
[13] G. Ardiansyah, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm," in 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017, pp. 249–254. https://doi.org/10.1109/ICITISEE.2017.8285505
[14] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "A Good Performance OTP encryption image based on DCT-DWT steganography," Telkomnika (Telecommunication Computing Electronics and Control), vol. 15, no. 4, pp. 1987–1995, Dec. 2017. https://doi.org/10.12928/TELKOMNIKA.v15i4.5883
[15] M. R. Islam, T. R. Tanni, S. Parvin, M. J. Sultana, and A. Siddiqa, "A modified LSB image steganography method using filtering algorithm and stream of password," Information Security Journal: A Global Perspective, vol. 30, no. 6, pp. 359–370, Nov. 2021. https://doi.org/10.1080/19393555.2020.1854902
[16] S. A. Mahdi, "An Improved Method for Combine (LSB and MSB) Based on Color Image RGB," Engineering and Technology Journal, vol. 39, no. 1B, pp. 231–242, Mar. 2021. https://doi.org/10.30684/etj.v39i1B.1574
[17] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 17, no. 3, p. 1168, Jun. 2019. https://doi.org/10.12928/telkomnika.v17i3.12230
[18] Q. S. Alsaffar, H. N. Mohaisen, and F. N. Almashhdini, "An encryption based on DNA and AES algorithms for hiding a compressed text in colored Image," IOP Conf Ser Mater Sci Eng, vol. 1058, no. 1, p. 012048, Feb. 2021. https://doi.org/10.1088/1757-899x/1058/1/012048
[19] M. Kumar, A. Soni, A. R. S. Shekhawat, and A. Rawat, "Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique," in 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), IEEE, Feb. 2022, pp. 1453–1457. https://doi.org/10.1109/ICAIS53314.2022.9742942
[20] F. A. Abella, M. B. Ghiffari, M. Johana, and S. Simanjuntak, "IMPLEMENTATION OF CRYPTOGRAPHY USING AES-128 ALGORITHM," 2022.
[21] M. Sulaman et al., "A Novel Approach for Medical Image Security Using the Radon Transform and AES-CBC Algorithm," 2023. https://doi.org/10.21203/rs.3.rs-3175303/v1
[22] E. J. G, H. M. A, and F. H. M. S, "Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography," International Journal of Advanced Computer Science and Applications, vol. 13, no. 8, p. 2022, 2022. https://doi.org/10.14569/IJACSA.2022.01308104
[23] A. Susanto, I. Utomo, W. Mulyono, M. Rizky, F. Febrian, and G. A. Rosyida, "A Combination of Hill Cipher and LSB for Image Security," Scientific Journal of Informatics, vol. 6, no. 1, pp. 2407–7658, 2019.
[24] M. Rohini, M. A. Srikanth, M. Prajwal, P. R. Kumar, M. Basavaraj, and M. U. Vinay, "Advanced Data Security Using Modulo Operator And LSB Method," Journal of Scholastic Engineering Science and Management, vol. 2023, no. 5, pp. 26–37, 2023. https://doi.org/10.5281/zenodo.7890771
[25] J. Shankar and C. Nandini, "Hybrid Hyper Chaotic Map with LSB for Image Encryption and Decryption," Scalable Computing: Practice and Experience, vol. 23, no. 4, pp. 181–192, Dec. 2022. https://doi.org/10.12694/scpe.v23i4.2018
[26] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," Journal of Computer and Communications, vol. 07, no. 03, pp. 8–18, 2019. https://doi.org/10.4236/jcc.2019.73002

[27] D. Chicco, M. J. Warrens, and G. Jurman, “The coefficient of determination R-squared is more informative than SMAPE, MAE, MAPE, MSE and RMSE in regression analysis evaluation,” PeerJ Comput Sci, vol. 7, p. e623, Jul. 2021. https://doi.org/10.7717/peerj-cs.623

[28] M. R. Naufal, C. A. Sari, E. H. Rachmawanto, L. B. Handoko, F. O. Isinkaye, and W. S. T. Al-Dayyeni, “An Evaluation of Number of Pixels Change Rate (NPCR) in Symetric Cryptography Based on Data Encryption Standard (DES),” in 2023 International Seminar on Application for Technology of Information and Communication (iSemantic), 2023, pp. 490–495. https://doi.org/10.1109/iSemantic59612.2023.10295300

[29] C. A. Sari et al., “A Chaotic Image Encryption Based on Random Noise and Arnold Cat Maps,” in 2024 International Seminar on Application for Technology of Information and Communication (iSemantic), 2024, pp. 347–352. https://doi.org/10.1109/iSemantic63362.2024.10762216

[30] A. M. Duarte, F. Silva, F. R. Pinto, S. Barroso, and M. M. Gil, “Quality Assessment of Chilled and Frozen Fish—Mini Review,” Foods, vol. 9, no. 12, p. 1739, Nov. 2020. https://doi.org/10.3390/foods9121739