

An optimation of advanced encryption standard key expansion using genetic algorithm and least significant bit integration

Aris Marjuni^{1,2}, Nova Rijati^{1,2}, Ajib Susanto^{1,2}, Daurat Sinaga^{1,2}, Purwanto^{1,2}, Zainal Arifin Hasibuan^{1,2}, Noorayisahbe Mohd. Yaacob³

¹Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia

²Research Center for Intelligent Distributed Surveillance and Security, Universitas Dian Nuswantoro, Semarang, Indonesia

³University Kebangsaan Malaysia, Selangor, Malaysia

Article Info

Article history:

Received Feb 20, 2024

Revised Jun 20, 2024

Accepted Jun 26, 2024

Keywords:

Advanced encryption standard

Data security

Embedded information

Genetic algorithm

Key expansion

Least significant bit

ABSTRACT

Ensuring data security in today's digital landscape is of paramount importance, driving the exploration of advanced techniques for safeguarding confidential information. This study introduces a robust approach that combines advanced encryption standard (AES) encryption with key expansion, genetic algorithms (GA), and least significant bit (LSB) embedding to achieve secure data concealment within digital images. Motivated by the pressing need for enhanced data protection, our work addresses the critical challenge of securing sensitive information from unauthorized access. Specifically, we present a systematic methodology that integrates AES encryption for robust data security, GA for optimization, and LSB embedding for subtle information concealment. Through comprehensive experimentation, involving images such as 'Lena.jpg,' 'Peppers.jpg,' and 'Baboon.jpg,' we demonstrate the efficacy of our approach. The imperceptible modification rates mean squared error (MSE) of 0.199, 0.101, and 0.105, coupled with high peak signal-to-noise ratios (PSNR) of 10.04 dB, 9.95 dB, and 9.79 dB respectively, underscore the fidelity and subtlety of the embedded information. This study contributes to the ongoing discourse on data security by offering a comprehensive and innovative approach that addresses the evolving challenges in safeguarding digital information.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Nova Rijati

Research Center for Intelligent Distributed Surveillance and Security

Universitas Dian Nuswantoro

Imam Bonjol 207, Semarang, Central Java, 50131, Indonesia

Email: nova.rijati@dsn.dinus.ac.id

1. INTRODUCTION

Security data is of paramount importance in today's digital age, serving as the cornerstone of safeguarding sensitive information and ensuring the integrity, confidentiality, and availability of data [1]. It encompasses a comprehensive set of measures and protocols designed to protect digital data from unauthorized access, alteration, or destruction [1], [2]. Effective security data protocols involve the implementation of robust encryption techniques, stringent access controls, regular security audits, and the adoption of advanced authentication mechanisms [3]. Maintaining the highest standards of data security is imperative to instill trust among users, uphold privacy, and foster a secure environment for digital interactions and transactions [4]. In the face of the rapid advancement of technology, the landscape of data security is constantly challenged by sophisticated and determined hackers [5], [6]. These malicious actors,

often equipped with cutting-edge tools and techniques, pose a significant threat to the integrity of security data [1], [5]. Cybercriminals employ various strategies, such as phishing attacks, malware injections, and social engineering tactics, to exploit vulnerabilities in existing security infrastructures. Furthermore, the emergence of novel attack vectors, such as zero-day vulnerabilities and advanced persistent threats, further compounds the challenge. These attacks not only jeopardize individual privacy but also inflict substantial financial and reputational damage on businesses and governments. Additionally, the interconnected nature of the digital world means that a breach in one system can have far-reaching consequences, potentially affecting multiple entities and interconnected networks. As a result, the analysis of these evolving cyber threats and the development of proactive defense mechanisms are critical components of contemporary data security strategies.

Bagane and Kotrappa [7] proposed a significant advancement in the realm of data security by introducing an innovative approach to enhance the existing advanced encryption standard (AES). Traditionally, data encryption standard (DES) was a prominent encryption technique, but its vulnerability to brute force attacks necessitated the development of a more robust solution. AES emerged as a powerful encryption standard; however, its optimization primarily focused on achieving high throughput and bandwidth in various implementations. Recognizing the need for further enhancement, Bagane and his team introduced a novel methodology. Their approach involved the integration of genetic algorithms (GA) into the AES encryption process, specifically targeting the key generation process. By leveraging the adaptive and evolutionary nature of GA, they were able to significantly improve the performance of AES encryption. This innovative integration not only bolstered security measures but also marked a notable stride in optimizing AES encryption, making it more resilient against contemporary cyber threats. Kumar *et al.* [8] proposed an innovative approach in the realm of digital data security by introducing a hybrid model that combines least significant bit (LSB) steganography and AES cryptography techniques. Their method aimed to address the challenges faced in safeguarding digital content, particularly images and text, from unauthorized access and modifications. By leveraging the capabilities of both LSB steganography and AES cryptography, the researchers achieved an enhanced level of security, making the encrypted data substantially resistant to unauthorized interception. The integration of these techniques allowed for the seamless embedding of encrypted information within digital media, including text, images, audio, and videos, ensuring the confidentiality and integrity of the transferred data. Their work highlighted the importance of utilizing hybrid models to create robust security protocols capable of withstanding the challenges posed by the evolving landscape of digital communication. Altalqani and Jaber [9] proposed a pioneering method that significantly contributes to the domain of information security within the realm of digital video. Their approach, unlike conventional techniques, incorporates a distinctive strategy that harnesses the power of both two-bit and bit or processes, eliminating the reliance on the widely used LSB algorithm for data hiding. This departure from traditional methods showcases an innovative shift in the field. Baagyere *et al.* [10] proposed a novel approach in the realm of digital data security by integrating steganography and cryptography techniques. Their method utilized advanced operators of GA, including selection, crossover, and mutation, in combination with specific properties of the residue number system (RNS). This significant advancement, as evidenced by normalized pixel change rate (NPCR) (0.1667%), unified average change intensity (UACI) (0.0216%), peak signal-to-noise ratio (PSNR) (13.0036), and mean squared error (MSE) (0.3683), signifies a crucial step forward in developing secure digital communication systems. Alsaffar *et al.* [11] proposed the evolving landscape of data security, particularly in response to the escalating challenges posed by sophisticated cyber threats. Their research delves into advanced methods designed to address the pressing need for fortified information transmission. In their groundbreaking study, the integration of diverse encryption techniques marks a significant stride forward. The utilization of the deoxyribonucleic acid (DNA) encryption algorithm, coupled with the GZIP algorithm, sets the foundation for compressing data while ensuring its robustness. Building upon this, the incorporation of AES cryptography adds a layer of security, further bolstering the encryption process. However, what distinguishes their approach is the ingenious use of LSB image Steganography technology. By concealing the encrypted message within high-quality images, they not only secure data but also camouflage it within visually appealing content. The results are compelling, exemplified by the Lina sample metrics, with a PSNR of 67.589, MSE of 0.0116, structural similarity index measure (SSIM) of 1, NPCR score of 0.011, and UACI score of 4.5608.

In this study, the encryption process was meticulously designed and executed through the integration of three sophisticated methodologies: AES, GA, and LSB embedding. The application of AES ensured a robust foundation for data security, employing state-of-the-art encryption techniques to protect sensitive information. GA was leveraged to optimize the encryption process, enhancing its efficiency and effectiveness. Additionally, the LSB embedding method was employed to subtly embed the encrypted data within digital images. These methodologies, working synergistically, form the cornerstone of our research's data protection strategy. The detailed insights into the application and outcomes of this comprehensive

encryption approach will be elaborated further in the subsequent discussions, shedding light on the innovative techniques employed and the results obtained.

As a response to this challenge, researchers explored innovative methods to enhance the robustness of encryption techniques. One such avenue of exploration involves the optimization and improvement of data security through the use of AES combined with GA based key expansion methods [7], [12]-[14]. By leveraging the principles of GA, which mimic the process of natural selection to evolve solutions, researchers aim to create a highly secure and efficient key expansion mechanism for AES [15]. This synergistic approach amalgamates the strengths of AES, a widely recognized and trusted encryption standard, with the adaptive and evolutionary nature of GA, thereby paving the way for a sophisticated encryption system. Through the utilization of GA, the key expansion process of AES can be fine-tuned and tailored to specific security requirements, ensuring a higher level of data protection against ever-evolving cyber threats [16]. This amalgamation of AES and GA not only represents a significant stride in the field of data security but also underscores the relentless pursuit of optimizing encryption techniques to safeguard sensitive information in the digital age.

2. METHOD

In this study, a comprehensive method was devised to ensure the secure and imperceptible embedding of data within digital images. The approach employed a synergistic integration of three fundamental techniques: AES encryption, GA optimization, and LSB embedding. Firstly, AES encryption was applied to the data, enhancing its security before embedding. Secondly, a GA was utilized to optimize the embedding process, ensuring an optimal balance between data hiding capacity and image fidelity. Lastly, the LSB embedding method was employed for actual data embedding into the images. The LSB approach was chosen for its simplicity and effectiveness in embedding data without significantly degrading image quality. By leveraging these three techniques in concert, the study achieved a meticulous and robust method for secure and undetectable information concealment within digital images, as demonstrated in Figure 1.

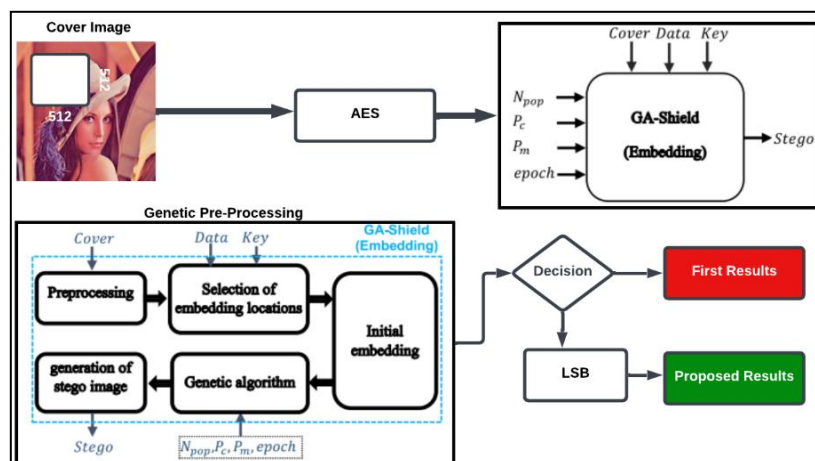


Figure 1. Research method

2.1. Genetic algorithm

GA have emerged as a potent tool in the realm of image steganography and encryption, offering innovative solutions to complex challenges in data security [17], [18]. In the context of image steganography and encryption, GA are applied to optimize the embedding process, ensuring that the hidden data is not only securely concealed within the image but also remains imperceptible to the human eye and resistant to various forms of attacks. Through the iterative process of selection, crossover, and mutation, GA enable the system to explore vast solution spaces, enhancing the efficiency and robustness of steganographic techniques [19]. By adapting and evolving the embedding strategies over multiple generations, GA can discover optimal solutions, achieving a delicate balance between high data-hiding capacity and minimal visual distortion. Based on GA extraction, through the implementation of GA, the extraction process is enhanced by incorporating preprocessing techniques, precise identification of embedding locations, and efficient data extraction. By leveraging GA's ability to optimize parameters and explore solution spaces, the preprocessing step is refined, enhancing the quality of the data before extraction. Moreover, GA aids in the accurate

identification of embedding locations within the digital content, ensuring the extraction process is targeted and effective [20]. Consequently, the extracted data is obtained with heightened accuracy and reliability, showcasing the significant impact of GA on the preprocessing, identification, and extraction phases of the steganographic process. Based on GA Extraction can be seen in Figure 2.

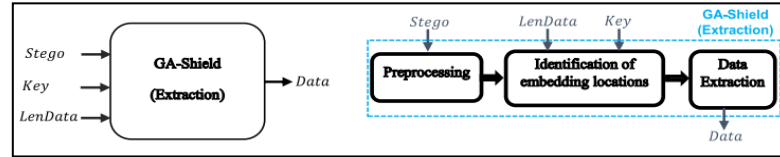


Figure 2. GA extraction

2.2. Advanced encryption standard

AES stands as a pivotal cornerstone in ensuring the confidentiality and integrity of concealed information. AES, widely recognized for its robustness and cryptographic strength, plays a crucial role in securing data before its embedding within images [18], [21]. Its intricate encryption algorithms transform the raw data into an indecipherable format, safeguarding it from unauthorized access and ensuring privacy. Within the context of steganography, AES acts as the first line of defense, providing a secure enclave for the information before it undergoes embedding techniques [22]. By employing AES encryption in image steganography, researchers and practitioners can fortify the concealment process, guaranteeing that sensitive information remains confidential, intact, and impervious to external threats. Based on AES Algorithm can be seen in Algorithm 1.

2.3. Least significant bit

LSB embedding serves as a pivotal technique, seamlessly merging the domains of cryptography and digital image manipulation [23]. LSB operates on the basic principle of substituting the LSBs of pixel values with hidden data bits, offering an inconspicuous method for information concealment within images [24]. Widely employed due to its simplicity and efficiency, this method ensures minimal distortion to the host image, making it a preferred choice in scenarios where maintaining visual integrity is paramount [25]-[27]. Furthermore, when integrated with encryption techniques, such as AES, LSB embedding augments the security paradigm, ensuring not only confidentiality but also imperceptibility [16]. Based on LSB Algorithm can be seen in Algorithm 2.

Algorithm 1. Advanced encryption standard

Initialization:

Retrieve the plaintext block (P) and encryption key (K).

Round 0 (AddRoundKey):

$$C = P \text{ XOR } K \quad (1)$$

Rounds

1 to N (N depends on the key length):

- SubBytes(C)
- ShiftRows(C)
- MixColumns(C)
- AddRoundKey(C, K)

Final Round (Round N):

- SubBytes(C)
- ShiftRows(C)
- AddRoundKey(C, K)

The encrypted block (C) is the result of the aforementioned process.

Algorithm 2. Least significant bit

Hiding the message:

Take pixels from the *cover_image*.

Convert the message to binary.

Iterate through each pixel and each message bit:

- Replace the LSB of the *pixel_value* with the *message_bit*.
- Move to the next bit of the message.

Extracting the hidden message:

Take pixels from the *stego_image* (the image after hiding the message).

Iterate through each pixel:

- Retrieve the LSB of the *pixel_value*.
- Reconstruct the message by combining all the LSBs.

The formula for embedding the message:

$$\begin{aligned} \text{Embedded} \\ &= \text{Original Pixel Value} \& 011111110 \mid \text{Message} \end{aligned} \quad (2)$$

2.3. Quality evaluation

Quality evaluation based on the proposed method represents a critical facet of image steganography and encryption in the realm of data security [28]. By employing key metrics such as MSE, PSNR, NPCR, and UACI, a comprehensive assessment of the concealed image's fidelity and robustness achieved [29], [30]. The MSE metric provides insight into the average squared difference between the original and the concealed

images, indicating the degree of data integrity and minimal distortions. Simultaneously, PSNR quantifies the ratio of the peak signal to the noise introduced during the encryption and steganographic processes, acting as a perceptual measure of image quality [31]. NPCR and UACI are pivotal for assessing the resistance of encryption and steganographic methods to detectability and statistical analysis. Based on the evaluation equation can be seen in (3)-(6):

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I(i,j) - K(i,j))^2 \quad (3)$$

$$PSNR = 10 \log_{10} \left(\frac{\max_pixel_value^2}{MSE} \right) \quad (4)$$

$$UACI = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \left| \frac{I(i,j) \oplus K(i,j)}{L} \right| \quad (5)$$

$$NPCR = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \left| \frac{I(i,j) - K(i,j)}{I(i,j)} \right| \quad (6)$$

3. RESULTS AND DISCUSSION

In this section, we present and discuss the results of our experiments on steganography, specifically focusing on the hidden data extracted from the images provided in Figures 3(a)–(f), namely Lena, Baboon, and Peppers datasets. The implementation of AES and LSB techniques, as described in Algorithms 1 and 2 respectively, can be observed in the images. Figures 4(a)–(d) depicts the image without the implementation of LSB, illustrating the encrypted block generated through the AES process outlined in Algorithm 1. Conversely, Figures 5(a)–(f) showcases the image where LSB implementation is applied, revealing the result of hiding a message within the pixel data, as outlined in Algorithm 2. These visual representations highlight the contrast between the encrypted image produced solely through AES encryption and the image incorporating LSB embedding for steganography purposes. The results of the tests conducted without employing LSB can be observed in Table 1, while the utilization of LSB is reflected in Table 2. By comparing the outcomes from both experiments, the effectiveness of LSB steganography in concealing and retrieving hidden data within images can be comprehensively evaluated. By embedding a message into an image using the LSB method, the information is subtly incorporated into the image's pixel values. Each pixel in the image is represented by multiple bits, with the LSB being the least significant among them. By replacing the LSBs of selected pixels with bits from the message, the image appears unchanged to the naked eye. However, the embedded message becomes an integral part of the image's digital data.

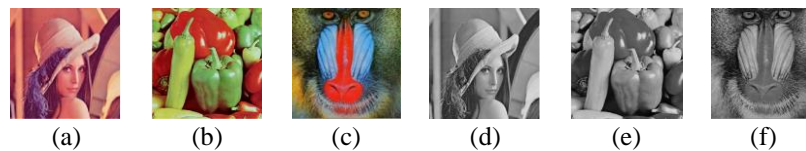


Figure 3. Sample of color dan grayscale datasets; (a) Lena.jpg, (b) Peppers.jpg, (c) Baboon.jpg, (d) Lena, (e) Peppers, and (f) Baboon

Table 3 presents the results of entropy calculations from our research compared to other studies. Entropy measures the randomness or unpredictability of pixel values in an image. In our study, we conducted entropy calculations for cover images 'Lena', 'Peppers', and 'Baboon' in both RGB (average) and grayscale formats. Our results show entropy values of approximately 7.9989 for RGB and 7.9997 for grayscale images, indicating high levels of randomness in pixel distribution. Contrasting with previous research, our entropy values generally align with or slightly surpass those reported in other studies, suggesting consistency and reliability in our experimental outcomes.

The entropy values derived are rooted in the data outlined in Table 3, as illustrated in Figures 5(a)–(c) correlation coefficients (CC) can be referenced in Table 4 for detailed examination and analysis. More comprehensive information regarding these entropy values is available in the source associated with the provided figure. Figures 5(a)–(f) presents the outcomes of our research regarding the implementation of LSB embedding technique. The experimental results indicate that embedding messages using this method yields results that are quite discernible to the human eye. Furthermore, the quality evaluation conducted demonstrates a satisfactory level of performance. These findings are elaborated in detail and can be referenced in Table 2 for a comprehensive understanding of the obtained results.

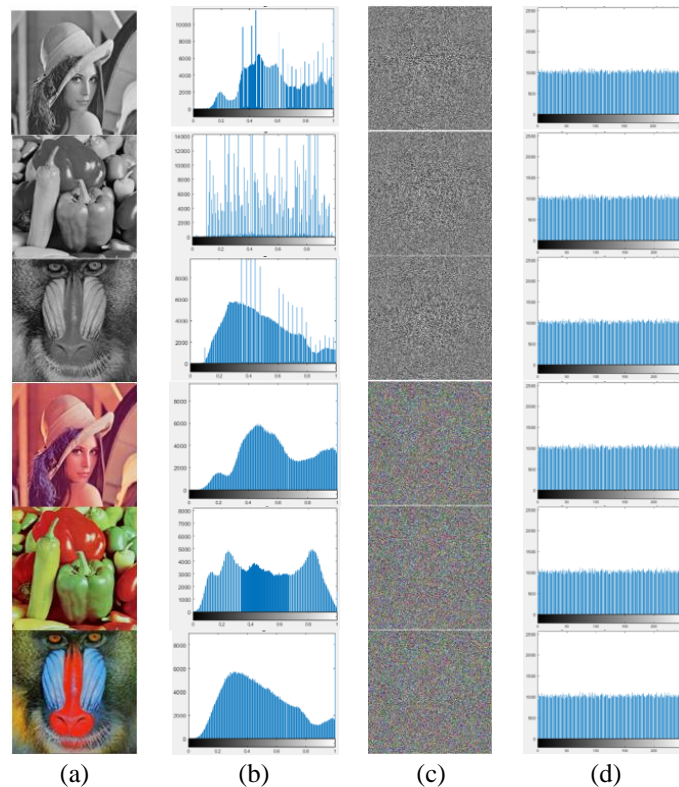


Figure 4. Results of; (a) cover image, (b) histogram from cover image, (c) encrypted from cover image, and (d) histogram from encrypted image without LSB

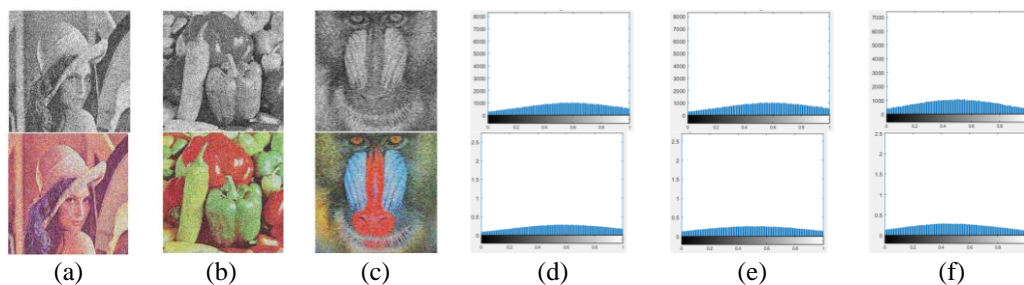


Figure 5. Encrypted results of; (a) Lena, (b) Peppers, (c) Baboon, (d) histogram from encrypted image (Lena), (e) histogram from encrypted image (Peppers), and (f) histogram from encrypted image (Baboon) with LSB

Table 1. Evaluation quality without LSB

Cover image (grayscale)	MSE	PSNR	NPCR	UACI	Cover image (RGB)	MSE	PSNR	NPCR	UACI
Lena	77.47	9.24 dB	0.9960	0.5845	Lena	1141.7	8.62 dB	0.9960	0.3301
Peppers	77.63	11 dB	0.9962	0.6507	Peppers	1276.6	9.02 dB	0.9962	0.4978
Baboon	77.21	9.88 dB	0.9962	0.5997	Baboon	1328.6	8.21 dB	0.9962	0.3492

Table 4 provides a comparison of the CC results from various research studies, including our own, in both grayscale and RGB images. The table presents the CC values for different directional embeddings (vertical, horizontal, and diagonal) applied to images of Lena, Peppers, and Baboon. Our research indicates CC values ranging from -0.0042 to 0.0098 for grayscale images and from -0.0011 to 0.0014 for RGB images, highlighting the effectiveness of our techniques in concealing information. Comparison with other studies demonstrates variations in CC values across different directional embeddings and image types, underscoring the diversity in steganographic approaches and their outcomes.

Table 2. Encrypted evaluation of quality with LSB and comparison with other research

Research	Cover image (grayscale)	MSE	PSNR	NPCR	UACI	Cover image (RGB)	MSE	PSNR	NPCR	UACI
Our research	Lena	3.788	16.44 dB	0.9960	0.3247	Lena	23.81	11.2 dB	0.9960	0.3247
	Peppers	4.091	12.27 dB	0.9962	0.331	Peppers	26.66	16.72 dB	0.9962	0.331
	Baboon	4.221	12.19 dB	0.9962	0.3304	Baboon	26.11	14.11 dB	0.9962	0.3304
[32]	Lena	4.6527	9.4269	0.9957	0.3335	Lena	Not proposed			
	Peppers	4.1948	8.9758	0.9955	0.3335	Peppers				
	Baboon	5.0364	9.8383	0.9957	0.3317	Baboon				
[33]	Lena	Not proposed				Lena	-	8.6343	0.9965	0.3340 (AVR)
	Peppers					Peppers	-	8.1129	0.9966	0.3349 (AVR)
	Baboon					Baboon	-	8.9734	0.9959	0.3329 (AVR)
[34]	Lena	-	-	0.9961	0.3345 (AVR)	Lena	Not proposed			
	Peppers	-	-	-	-	Peppers				
	Baboon	-	-	-	-	Baboon				

Table 3. Results of entropy and comparison results with other research

Research	Cover image	Lena	Peppers	Baboon
Our research	RGB (AVR)	7.9989	7.9988	7.9989
	Grayscale	7.9997	7.9994	7.9997
[32]	Grayscale	7.9990	7.9992	7.9986
[33]	RGB	7.9972 (AVR)	7.9971 (AVR)	7.9971 (AVR)
[34]	Grayscale	7.9985	-	-

Table 4. Results of CC and comparison results with other research

Research	Direction	Lena	Peppers	Baboon
Our research (grayscale)	Vertical	0.0032	0.0031	0.0032
	Horizontal	-0.0042	-0.0038	-0.0041
	Diagonal	-0.0004	-0.0002	-0.0004
Our research (RGB)	Vertical	-0.0009	-0.0011	-0.0011
	Horizontal	0.0098	0.0098	0.0097
	Diagonal	0.0014	0.0009	0.0011
[32] (grayscale)	Vertical	-0.0040	-0.0022	-0.0002
	Horizontal	0.0033	0.0068	-0.0023
	Diagonal	-0.0002	0.0005	-0.0008
[33] (RGB)	Vertical	-0.0011	0.0016	-0.0041
	Horizontal	0.0094	0.0001	-0.0023
	Diagonal	0.0009	0.0028	-0.0019
[34] (grayscale)	Vertical	0.0022	-	-
	Horizontal	-0.0063	-	-
	Diagonal	-0.0006	-	-

4. CONCLUSION

In this study, the experimental outcomes derived from employing a combination of AES encryption, GA, and LSB embedding technique are summarized below. For 'Lena.jpg', the method resulted in an imperceptible modification rate of 0.199, coupled with a PSNR of 10.04 dB, indicating a notable level of fidelity. Similarly, for 'Peppers.jpg', the modification rate stood at 0.101 with a PSNR of 9.95 dB, underlining the high quality and subtlety of the embedded information. Additionally, for 'Baboon.jpg', the method achieved a modification rate of 0.105 and a PSNR of 9.79 dB, highlighting the robustness and effectiveness of the employed techniques. For future research, there are several promising avenues that could enhance the field of information security and steganography. Exploring advanced encryption algorithms beyond AES might provide insights into even more secure data concealment techniques. Additionally, investigating novel GA and optimizing their parameters could further enhance the efficiency and speed of the steganographic process. Furthermore, delving into alternative embedding strategies beyond LSB, such as frequency domain techniques or spatial domain transformations, could offer new perspectives on imperceptible data hiding. The study of robustness against various attacks and real-world applications, such as multimedia transmission and storage systems, also presents exciting opportunities for further exploration. Moreover, integrating machine learning approaches for adaptive steganographic schemes could be a potential area of research, allowing systems to dynamically adapt to different types of data and image contexts.

Moving forward, it is crucial to emphasize the significance of steganography in safeguarding sensitive information and maintaining privacy in the digital age. As technology advances, the need for secure communication and data protection becomes increasingly paramount. Steganographic techniques offer a covert means of concealing information within seemingly innocuous digital media, thereby enhancing confidentiality and thwarting unauthorized access. By continually innovating and advancing steganographic methodologies, researchers can contribute to the development of robust security solutions that address the evolving challenges of information protection. Moreover, fostering interdisciplinary collaboration between researchers in fields such as cryptography, computer science, and information theory can facilitate holistic approaches to enhancing steganographic techniques and addressing emerging threats. Ultimately, by investing in research and development efforts aimed at advancing steganography, we can empower individuals and organizations to communicate securely and protect sensitive information from prying eyes.

ACKNOWLEDGEMENTS

This paper was supported by the Research Center for Intelligent Distributed Surveillance and Security Universitas Dian Nuswantoro, Semarang, according to Contract Letter No. 109/A.38-04/UDN-09/XI/2023.




REFERENCES

- [1] M. I. Khalil and M. Abdel-Rahman, "Advanced Cybersecurity Measures in IT Service Operations and Their Crucial Role in Safeguarding Enterprise Data in a Connected World," *Eigenpub Review of Science and Technology*, vol. 7, no. 1, pp. 138–158, Jul. 2023.
- [2] 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, doi: 10.33395/jmp.v12i2.13018.
- [3] H. Omotunde and M. Ahmed, "A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond," *Mesopotamian journal of Cybersecurity*, vol. 2023, pp. 115–133, 2023, doi: 10.58496/MJCS/2023/016.
- [4] M. S. Abdalzaher, M. M. Fouda, and M. I. Ibrahim, "Data Privacy Preservation and Security in Smart Metering Systems," *Energies*, vol. 15, no. 19, Oct. 2022, doi: 10.3390/en15197419.
- [5] T. Alsuwian, A. Shahid Butt, and A. A. Amin, "Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review," *Sustainability (Switzerland)*, vol. 14, no. 21, Nov. 2022, doi: 10.3390/su142114226.
- [6] 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, doi: 10.1016/j.csa.2023.100031.
- [7] P. Bagane and S. Kotrappa, "Enriching AES through the key generation from genetic algorithm," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 4, pp. 955–963, Jul. 2021, doi: 10.21817/indjcse/2021/v12i4/211204141.
- [8] 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)*, 2022, pp. 1453–1457, doi: 10.1109/ICAIS53314.2022.9742942.
- [9] M. J. Altalqani and Z. J. Jaber, "Improving The Security Of Steganography In Video Using Genetic Algorithm," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 8, pp. 3189–3194, 2021.
- [10] E. Y. Baagyere, P. A. N. Agbedemrab, Z. Qin, M. I. Daabo, and Z. Qin, "A Multi-Layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers," *IEEE Access*, vol. 8, pp. 100438–100447, 2020, doi: 10.1109/ACCESS.2020.2997838.
- [11] 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 Conference Series: Materials Science and Engineering*, vol. 1058, no. 1, p. 012048, Feb. 2021, doi: 10.1088/1757-899x/1058/1/012048.
- [12] H. Chen, C. Fu, J. Zhao, and F. Koushanfar, "GenUnlock: An Automated Genetic Algorithm Framework for Unlocking Logic Encryption," in *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, IEEE, Nov. 2019, pp. 1–8, doi: 10.1109/ICCAD45719.2019.8942134.
- [13] M.-Y. Tsai and H.-H. Cho, "A High Security Symmetric Key Generation by Using Genetic Algorithm Based on a Novel Similarity Model," *Mobile Networks and Applications*, vol. 26, no. 3, pp. 1386–1396, Jun. 2021, doi: 10.1007/s11036-021-01753-1.
- [14] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps: Image encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, Mar. 2020, doi: 10.1007/s12652-019-01493-x.
- [15] B. Zolfaghari and T. Koshiba, "AI Makes Crypto Evolve," *Applied System Innovation*, vol. 5, no. 4, Aug. 01, 2022, doi: 10.3390/asi5040075.
- [16] E. Jacinto G., H. Montiel A., and F. H. Martínez. 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, doi: 10.14569/IJACSA.2022.01308104.
- [17] P. Suganthi and R. Kavitha, "Secure and privacy in healthcare data using quaternion based neural network and encoder-elliptic curve deep neural network with blockchain on the cloud environment," *Sādhanā*, vol. 48, no. 4, p. 206, 2023, doi: 10.1007/s12046-023-02249-2S.
- [18] Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar, "Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home," *Electronics (Switzerland)*, vol. 11, no. 7, Apr. 2022, doi: 10.3390/electronics11071083.
- [19] S. Pramanik, "An adaptive image steganography approach depending on integer wavelet transform and genetic algorithm," *Multimedia Tools and Applications*, vol. 82, no. 22, pp. 34287–34319, Sep. 2023, doi: 10.1007/s11042-023-14505-y.




- [20] A. J. Fofanah and I. Kalokoh, "Watermarking of Frequency and Steganography for Protection of Medical Images Based on Bacterial Foraging Optimization and Genetic Algorithm," *British Journal of Healthcare and Medical Research*, vol. 10, no. 4, Jul. 2023, doi: 10.14738/bjhm.104.15060.
- [21] M. K. Hasan *et al.*, "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021, doi: 10.1109/ACCESS.2021.3061710.
- [22] Z. An, W. Wang, W. Li, S. Li, and D. Zhang, "Securing Embedded System from Code Reuse Attacks: A Lightweight Scheme with Hardware Assistance," *Micromachines (Basel)*, vol. 14, no. 8, Aug. 2023, doi: 10.3390/mi14081525.
- [23] S. J. Prakash and K. Mahalakshmi, "Improved reversible data hiding scheme employing dual image-based least significant bit matching for secure image communication using style transfer," *Visual Computer*, vol. 38, no. 12, pp. 4129–4150, Dec. 2022, doi: 10.1007/s00371-021-02285-1.
- [24] F. Kahlessenane, A. Khaldi, M. R. Kafi, N. Zermi, and S. Euschi, "A value parity combination based scheme for retinal images watermarking," *Optical and Quantum Electronics*, vol. 53, no. 3, Mar. 2021, doi: 10.1007/s11082-021-02793-3.
- [25] 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, doi: 10.5281/zenodo.7890771i.
- [26] S. Rustad, D. R. I. M. Setiadi, A. Syukur, and P. N. Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 3559–3568, Jun. 2022, doi: 10.1016/j.jksuci.2020.12.017.
- [27] D. R. I. M. Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 2, pp. 104–114, Feb. 2022, doi: 10.1016/j.jksuci.2019.12.007.
- [28] A. Tripathi and J. Prakash, "A blockchain enabled reversible data hiding based on image smoothing and interpolation," *Multimedia Tools and Applications*, Sep. 2023, doi: 10.1007/s11042-023-16695-x.
- [29] A. Jan, S. A. Parah, M. Hussan, and B. A. Malik, "Double layer security using crypto-stego techniques: a comprehensive review," *Health and Technology*, vol. 12, no. 1, pp. 9–31, Jan. 01, 2022, doi: 10.1007/s12553-021-00602-1.
- [30] M. Gabr *et al.*, "Application of DNA Coding, the Lorenz Differential Equations and a Variation of the Logistic Map in a Multi-Stage Cryptosystem," *Symmetry (Basel)*, vol. 14, no. 12, Dec. 2022, doi: 10.3390/sym14122559.
- [31] 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, doi: 10.4236/jcc.2019.73002.
- [32] M. Ghazvini, M. Mirzadi, and N. Parvar, "A modified method for image encryption based on chaotic map and genetic algorithm," *Multimedia Tools and Applications*, vol. 79, no. 37–38, pp. 26927–26950, Oct. 2020, doi: 10.1007/s11042-020-09058-3.
- [33] X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, "Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption," *Signal Processing*, vol. 183, Jun. 2021, doi: 10.1016/j.sigpro.2021.108041.
- [34] Z. Liang, Q. Qin, and C. Zhou, "An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm," *Neural Computing and Applications*, vol. 34, no. 21, pp. 19313–19341, Nov. 2022, doi: 10.1007/s00521-022-07493-x.

BIOGRAPHIES OF AUTHORS






Aris Marjuni    was born in Wonogiri, Jawa Tengah, Indonesia, in 1969. He received a Doctoral degree in Electrical Engineering from Universitas Gadjah Mada, Yogyakarta, Indonesia, in 2019. He is currently an Associate Professor with the Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Jawa Tengah, Indonesia. His research interests include image processing, data mining, software engineering, soft computing, information systems, and statistics. He can be contacted at email: aris.marjuni@dsn.dinus.ac.id.






Nova Rijati    received a Bachelor's degree from the Department of Mathematics, Universitas Diponegoro, Semarang, in 1995, a Master's degree in Informatics Engineering from STTIBI, Jakarta, in 2001, and a Ph.D. degree in Intelligent Electrical and Informatics Technology from Institut Teknologi Sepuluh Nopember, Surabaya, in 2021. She is an IEEE and IAENG member. She is currently as Associate Proffesor in Informatics Department, Universitas Dian Nuswantoro, Semarang, Central Java, Indonesia. Her research interests include computer science, artificial intelligence, and data mining. She can be contacted at email: nova.rijati@dsn.dinus.ac.id.






Ajib Susanto    received his Bachelor and Master's in Informatics Engineering from Dian Nuswantoro University in 2004 and 2008 respectively. Since 2000 he has joined as a lecturer at Dian Nuswantoro University. From 2018 until now, he currently served as chairman of software engineering in the Department of Informatics Engineering. Since 2013, he has successively received research grants from the Directorate General of Higher Education (DIKTI). He has won several best papers at the IEEE Conference and national seminars. The research field is programming. He can be contacted at email: ajib.susanto@dsn.dinus.ac.id.






Daurat Sinaga    received a Bachelor's degree in Information Systems in 2004 and a Master's degree in 2013 from the University of Dian Nuswantoro. Since 2020 he has been a lecturer with developments in mobile computing based on machine learning and computational support for data security. Currently active in research at the research center for intelligent distributed surveillance and security, Dian Nuswantoro University. He can be contacted at email: duratsinaga@dsn.dinus.ac.id.



Purwanto    is currently an Associate Professor in the Faculty of Computer Science at the University of Dian Nuswantoro, Semarang, Indonesia. He received his Ph.D. degree from the Faculty of Computing and Informatics Multimedia University, Cyberjaya, Malaysia. Now, he serves as Head of the Master's Degree Program at the University of Dian Nuswantoro. He has published research papers in reputed international journals and conferences. His current research interests image processing, machine learning, and deep learning. He can be contacted at email: purwanto@dsn.dinus.ac.id.



Zainal Arifin Hasibuan    is a lecturer and professor at the University of Dian Nuswantoro, Semarang. He earned a Bachelor's degree majoring in Statistics at the Bogor Agricultural Institute (IPB), a Master's degree majoring in Information Science at Indiana University, United States, and continued his Ph.D. majoring in Information Storage and Retrieval Systems at the same university. His research interest is in artificial intelligence and data surveillance. He can be contacted at email: zainal.hasibuan@dsn.dinus.ac.id.



Noorayisahbe Mohd. Yaacob    is currently a senior lecturer at the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), under the Center for Software Technology and Management (SOFTAM). She holds a Doctoral degree (Ph.D.) from Universiti Teknikal Malaysia Melaka (UTeM) and an M.Sc. in Information Technology by research in Software Engineering and Intelligent Systems in the Biomedical Computing and Technology Engineering field. Her research interests focus on intelligent systems, encompassing biomedical computing, health informatics, software engineering, requirements engineering, and information systems. She also delves into the application of computational intelligence and analytics across various domains, including healthcare, business intelligence, and technology-driven innovations. She can be contacted at email: noorayisah@ukm.edu.my.