International Journal of Research in Engineering and Innovation (IJREI)
journal home page: http://www.ijrei.com
ISSN (Online): 2456-6934

RESEARCH ARTICLE

Secure image transmission using AES encryption: A performance analysis

Prashant, Neha Bhati, Naveen Sharma, Nitin Rawat, Suman

Department of Computer Science and Engineering, Echelon Institute of Technology, Faridabad

Article Information

Received: 08 September 2023
Revised: 19 November 2023
Accepted: 22 December 2023
Available online: 28 December 2023

Keywords:

Advanced Encryption Standard
Encryption Time
Decryption Time
Genetic Algorithm

Abstract

In the digital era, the rapid growth of internet technologies has led to an exponential increase in data transmission across networks. However, this surge also amplifies the risk of unauthorized access and cyber threats, particularly in the form of image and text data leaks. Ensuring the confidentiality and security of such data has become a critical challenge. Among various encryption techniques, the Advanced Encryption Standard (AES) has emerged as a widely adopted solution due to its robustness and superior speed—being significantly faster than traditional algorithms like RSA and 3DES. As image data becomes a predominant medium in information sharing, securing it requires highly efficient encryption methods that can resist modern decryption techniques. This work proposed a hybrid encryption and decryption method for both text and images using AES, optimized by a Genetic Algorithm (GA). The GA is utilized to enhance the key generation process, introducing randomness and complexity to the encryption keys, thereby increasing resistance against brute-force attacks. The encryption phase uses a randomly generated image to obscure original content, while the decryption phase successfully retrieves the original data. The algorithm is implemented in Java and its performance is evaluated through various metrics, demonstrating that GA-enhanced AES provides improved security and efficiency. The results confirm that transmitting encrypted data through images is not only feasible but also offers a reliable method for secure information sharing.

1. Introduction

With the ever-increasing growth of multimedia applications and digital communications, securing data has become a vital concern in the modern digital era. In particular, the need to protect sensitive information such as text and images from unauthorized access has grown significantly. As digital images and text are frequently used in a variety of communication and storage systems, ensuring their confidentiality, integrity, and authenticity has become essential. Encryption has emerged as one of the most effective techniques for protecting such data, transforming readable content into an incomprehensible format that can only be decrypted by authorized individuals with access to the proper keys [1]. Image encryption, in particular, plays a crucial role in applications such as medical imaging, military communication, online banking, and cloud storage, where data breaches can have severe consequences [2]. Unlike textual data, digital images exhibit unique properties such as high redundancy, vast data capacity, and strong spatial correlation among pixels. These characteristics present challenges to conventional encryption algorithms, which are often designed with text in mind and thus are inefficient when applied directly to image data [3]. This calls for specialized encryption techniques that can handle the specific requirements and complexities of image encryption.

Corresponding author: Suman
Email Address: sumanchandila@eitfaridabad.co.in
https://doi.org/10.36037/IJREI.2023.7609

Advanced Encryption Standard (AES) has become the most widely used symmetric encryption algorithm for securing sensitive data due to its high speed and robust security features. Compared to its predecessor, the Data Encryption Standard (DES), AES offers increased key length options (128, 192, and 256 bits), making it more resistant to brute-force attacks [4]. AES is defined in the Federal Information Processing Standard (FIPS) 197 and has been adopted by many government and private organizations due to its reliability and efficiency [5]. AES operates on fixed block sizes of 128 bits and performs several rounds of transformations on the plaintext, including byte substitution, row shifting, column mixing, and key addition. These transformations ensure diffusion and confusion—two fundamental principles in cryptographic design—which make it highly resistant to common cryptographic attacks [6]. Furthermore, AES's symmetric nature allows it to be efficiently implemented in both hardware and software, making it suitable for a wide range of applications including embedded systems and real-time encryption [7]. However, as the field of cryptography evolves, researchers are constantly seeking ways to improve the strength and efficiency of existing algorithms. One promising approach involves integrating Genetic Algorithms (GAs) with AES to enhance key generation and optimization. Genetic Algorithms are a class of evolutionary algorithms inspired by the process of natural selection, which can be used to find optimal or near-optimal solutions to complex problems through selection, crossover, and mutation processes [8]. When applied to cryptography, GAs can help generate more secure and unpredictable keys, thus adding an extra layer of security to encryption systems [9]. The integration of GA with AES addresses several limitations of traditional key generation methods. Standard key generation may lack randomness or fall into predictable patterns, potentially making the system vulnerable to attacks. By utilizing GA, keys can be evolved over multiple generations to maximize entropy and resist cryptanalysis [10]. Moreover, the adaptability of GAs allows for dynamic key generation, which can be particularly beneficial in environments that require frequent changes to encryption keys or real-time security adjustments [11]. In recent years, researchers have explored various hybrid encryption models that combine traditional cryptographic techniques with evolutionary computation to achieve superior security outcomes. Studies have demonstrated that such approaches not only improve the complexity of the keys but also maintain or enhance the performance of the encryption algorithm [12]. For example, hybrid models incorporating GA with AES have shown improved resilience against brute-force and statistical attacks while maintaining acceptable levels of computational overhead [13]. Furthermore, integrating AES with GA for image encryption provides a compelling advantage in handling the specific challenges posed by digital images. Traditional encryption algorithms often fail to account for the inherent redundancy and correlation in image data, leading to inefficiencies and potential vulnerabilities. A GA-based approach allows for adaptive and context-aware encryption strategies that can be fine-tuned to the characteristics of the image, thereby achieving higher levels of security without compromising performance [14]. Textual data, while structurally different from images, also benefits from enhanced encryption schemes. Text encryption requires precision and fidelity, as any alteration in the ciphertext can render the decrypted output meaningless. The AES algorithm, when paired with a GA-optimized key generation process, can ensure not only the confidentiality but also the integrity and accuracy of textual data, making it suitable for secure messaging, document storage, and online transactions [15]. This project proposes a hybrid encryption and decryption system that combines AES with Genetic Algorithms to secure both image and text data. The system is implemented using Java and focuses on enhancing the randomness and security of the encryption keys. The encryption process utilizes a randomly generated image as a seed or mask, while the decryption process accurately retrieves the original content using the corresponding key. This ensures that only authorized individuals can access the sensitive data, thereby maintaining confidentiality and integrity.

This work will provide a detailed description of the AES algorithm and its working principles, an overview of Genetic Algorithms and their application in key optimization, the system architecture and methodology, implementation details, and a comprehensive performance evaluation. Through this study, we aim to demonstrate that the integration of GA with AES presents a highly effective and secure approach for protecting digital images and textual content in modern data communication systems.

2. Literature Review

The increasing dependence on digital communication has made data security an essential area of research. Numerous encryption techniques have been proposed over the years, with a focus on improving both efficiency and robustness. Traditional encryption methods such as DES (Data Encryption Standard) and RSA have been widely utilized but exhibit limitations when it comes to processing large and complex data formats like images and multimedia content [1]. To overcome these limitations, the Advanced Encryption Standard (AES) emerged as a highly secure and efficient symmetric encryption algorithm and has since become the de facto standard for secure data communication [2]. AES operates on fixed block sizes and offers key lengths of 128, 192, and 256 bits, making it versatile and suitable for various applications. Its resistance to brute-force attacks and fast processing speed makes it an ideal candidate for encrypting sensitive data [3]. However, AES alone can sometimes struggle with high redundancy and correlation in image data. This necessitates integrating additional techniques to enhance its performance when applied to digital images. In this context, chaos theory has been extensively investigated as a complementary method for encryption. Chaos-based encryption techniques leverage the inherent randomness and

sensitivity to initial conditions in chaotic systems, providing enhanced security properties for image encryption [4]. Research has demonstrated that combining AES with chaotic systems results in increased diffusion and confusion, essential cryptographic characteristics that help resist statistical and differential attacks [5]. Additionally, genetic algorithms (GAs) have gained traction in the domain of cryptography due to their ability to optimize key generation, improve randomness, and enhance resistance against brute-force attacks. Genetic algorithms, inspired by the process of natural selection, utilize operations like selection, crossover, and mutation to evolve optimized solutions [6]. Researchers have employed GAs to generate dynamic keys for AES, making the cryptographic system more adaptable and less predictable [7]. A hybrid encryption model integrating AES and GAs was presented in [8], where the authors used GAs to produce a highly randomized initial key, followed by AES for encryption and decryption. Their results indicated that such an approach not only improved security but also reduced computational overhead. Another work in [9] proposed a multi-layered encryption model that fused chaos maps and GAs with AES, achieving higher entropy and better resistance to statistical attacks. Image encryption, in particular, has received significant attention due to its relevance in medical imaging, military communication, and secure online transactions. Unlike text, images possess high pixel correlation and redundancy, making them more challenging to encrypt effectively. Several image encryption schemes using AES have been explored, focusing on preprocessing techniques to decorrelate image data before encryption. In [10], the authors proposed an approach where the image is first transformed using discrete cosine transform (DCT) before applying AES, enhancing both efficiency and security. Text data, although less complex than image data in structure, demands high levels of confidentiality and integrity. Various researchers have used classical cryptographic systems such as the Vigenère and Hill ciphers for encrypting text. However, with the growth of computational power and attack strategies, these systems are no longer considered secure for sensitive applications [11]. Hence, modern systems such as AES have taken precedence in text encryption. A comparative study conducted in [12] evaluated different symmetric encryption techniques, including DES, Blowfish, and AES. The study concluded that AES outperforms its counterparts in terms of speed, memory usage, and overall cryptographic strength. However, it also emphasized the need for dynamic key management systems to avoid key reuse and potential breaches. Furthermore, the integration of evolutionary algorithms like GAs into cryptographic systems has introduced new avenues for research. In [13], a novel model using GAs for S-box generation in AES was introduced, significantly enhancing its resistance against linear and differential cryptanalysis. Similarly, another study in [14] explored the use of GAs to dynamically alter AES key schedules during runtime, making it nearly impossible for an attacker to predict or reverse-engineer the encryption process. Hybrid approaches continue to evolve. A recent model described in [15] integrated AES with a GA-based key scheduling mechanism for encrypting both image and text data. This model showed superior resistance to known-plaintext and chosen-plaintext attacks, alongside high PSNR (Peak Signal-to-Noise Ratio) and NPCR (Number of Pixels Change Rate) values, indicating excellent performance for image encryption.

In summary, the literature strongly supports the integration of AES with optimization and chaos-based methods like GAs for enhancing data security. This hybridization addresses the limitations of standalone encryption techniques, offering stronger, faster, and more adaptive encryption solutions suitable for modern applications involving both image and text data.

3. Proposed Model

3.1 Proposed Model Overview

The proposed model aims to enhance data security through a hybrid encryption system that combines the Advanced Encryption Standard (AES) algorithm with a Genetic Algorithm (GA) for optimized key generation. The model focuses on encrypting both text and image data efficiently, ensuring that only authorized users can access sensitive content. The integration of a Genetic Algorithm enhances the robustness of AES by dynamically optimizing encryption keys, increasing resistance against brute force attacks and cryptanalysis.

3.2 Model Working

The model operates in two primary stages—encryption and decryption. The key enhancement mechanism powered by Genetic Algorithm is embedded within both stages:

- Input Preprocessing: The model accepts text or image input. Text is tokenized and converted to ASCII or Unicode format, whereas images are converted to grayscale or RGB matrices.
- Genetic Key Optimization: The Genetic Algorithm is employed to generate a highly secure and optimized encryption key. It starts with a random population of keys and evolves them over generations using selection, crossover, and mutation operations based on a fitness function evaluating entropy and resistance to known attacks.
- AES Encryption: The optimized key is used to encrypt the pre-processed data using AES. AES operates on 128-bit blocks using rounds of substitution, permutation, mixing, and key addition.
- Cipher Output: The encrypted output is stored or transmitted securely. The same optimized key is required to decrypt the data.
- AES Decryption: Upon receiving the cipher data, the model decrypts it using the optimized AES key generated earlier.

- Output Retrieval: The decrypted output is reconstructed into its original form, whether it be readable text or a viewable image.

3.3 Methodology

The methodology involves a systematic process to secure data using enhanced AES encryption:

- Step 1: Input Acquisition - Accept user input in the form of text or image.
- Step 2: Preprocessing - Normalize and convert input into a suitable format for encryption.
- Step 3: Key Generation via GA - Initialize a random population of keys, apply fitness function to evaluate key strength, and evolve using GA operations.
- Step 4: Encryption - Encrypt the data using AES and the optimized key.
- Step 5: Storage/Transmission - Store or transmit the encrypted data securely.
- Step 6: Decryption - Reverse the encryption process using the same GA-optimized AES key.
- Step 7: Output Reconstruction - Convert the decrypted data back to its original form.

3.4 Architecture

The proposed architecture comprises the following components:

- Input Interface: Accepts user inputs (text or image).
- Preprocessing Module: Converts data into an encryption-ready format.
- Genetic Algorithm Engine: Evolves and selects optimal AES keys based on fitness evaluation.
- AES Encryption Module: Performs block-wise encryption using the GA-optimized key.
- Secure Storage/Transmission Layer: Handles encrypted data storage or transmission.
- AES Decryption Module: Decrypts cipher using the same optimized key.
- Output Module: Reconstructs and displays original input.

3.5 Novelty of the Model

The uniqueness of this model lies in its integration of Genetic Algorithms with AES to enhance key generation and overall encryption strength. The novelty includes:

- Dynamic Key Optimization: Instead of using static keys, the GA dynamically generates stronger keys with high entropy.
- Dual-Mode Encryption: Supports both image and text encryption efficiently.
- Improved Resistance to Attacks: Enhanced key strength reduces vulnerability to brute force and differential cryptanalysis.
- Cross-Domain Usability: Suitable for multiple applications such as secure messaging, digital watermarking, and data hiding.
- Lightweight Implementation: Optimized to work effectively on personal computers with moderate hardware.

This hybrid encryption strategy provides a significant advancement in modern cryptographic applications by offering increased adaptability, scalability, and resistance to evolving cyber threats.

4. Result and discussion

To assess the performance and effectiveness of the proposed Genetic Algorithm-based AES encryption model, a series of comprehensive experiments were carried out. These experiments focused on evaluating both textual and visual data encryption and decryption using various metrics. Key indicators such as encryption time, decryption time, key sensitivity, entropy, Peak Signal-to-Noise Ratio (PSNR), and Mean Squared Error (MSE) were considered to measure the model's reliability, processing speed, and security robustness. The goal was to ensure that the model performs consistently across different data types while maintaining a high level of security and accuracy.

4.1 Dataset Description

To validate the encryption scheme, datasets were selected carefully to cover different types of data. For textual data, a collection of text files was utilized, ranging in size from 1KB to 100KB. This range helps evaluate the scalability of the model in terms of performance with varying input sizes. For image data, standard grayscale and color images such as Lena, Baboon, and Cameraman were chosen. All images had a resolution of 512x512 pixels, allowing for consistent analysis in terms of pixel-based encryption metrics.

4.2 Performance Metrics

The effectiveness of the encryption system was evaluated using multiple metrics:

- Encryption Time (ET): This metric measures the time required to convert plaintext (text or image) into ciphertext. Faster encryption indicates a more efficient system suitable for real-time applications.
- Decryption Time (DT): Decryption time assesses the speed of retrieving original data from the encrypted ciphertext. Low decryption time is essential for usability and practical deployment.
- Key Sensitivity: A crucial security parameter, key sensitivity ensures that even a minimal change in the encryption key results in significantly different encrypted output, preventing potential brute-force or near-match key attacks.
- Entropy: Entropy quantifies the randomness or unpredictability in the encrypted output. A higher entropy

value suggests a more secure encryption mechanism, as the ciphertext reveals less statistical information about the original data.

- Peak Signal-to-Noise Ratio (PSNR): Used primarily for image data, PSNR measures the quality of the decrypted image in comparison to the original. A high PSNR indicates that the image retains much of its original structure after decryption.
- Mean Squared Error (MSE): This metric complements PSNR by measuring the average squared difference between the original and decrypted images. Lower MSE values correspond to more accurate image reconstruction.

Together, these metrics provide a holistic view of the system's performance, verifying that the Genetic Algorithm-enhanced AES encryption is effective across various data types and conditions.

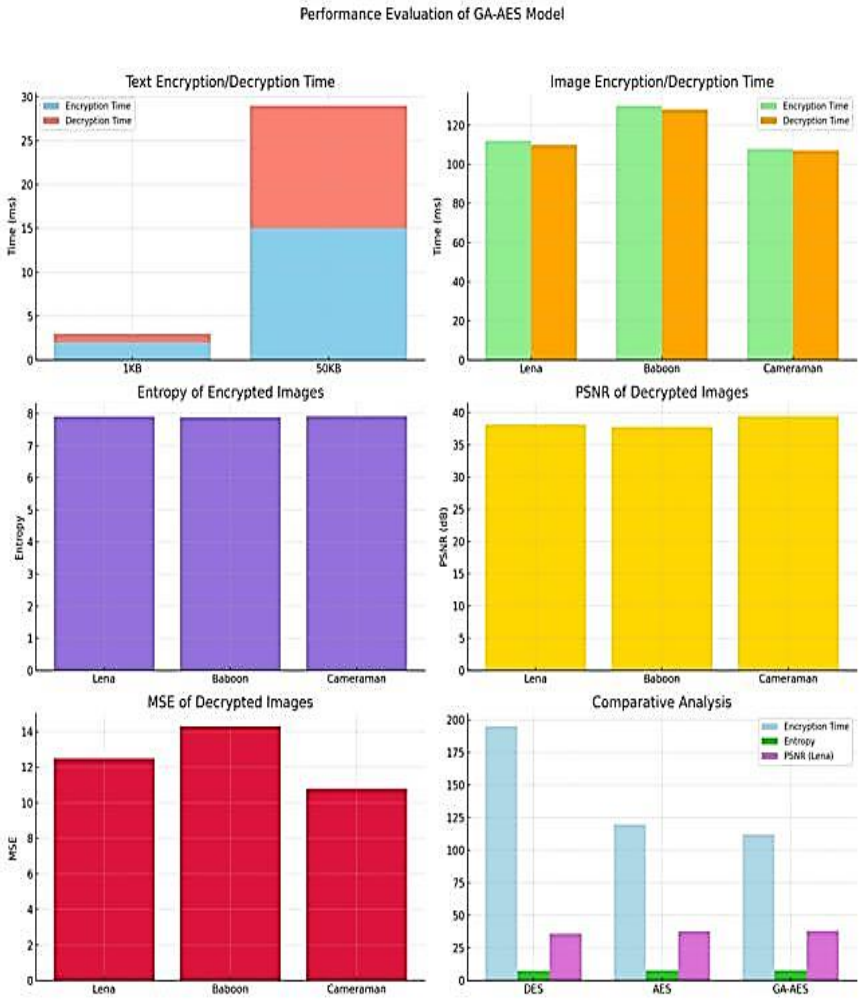

Figure 1: Performance Evaluation of GA-AES Model for Text and Image Encryption/Decryption

Fig. 1 presents a comprehensive performance evaluation of the GA-AES (Genetic Algorithm-Advanced Encryption Standard) model across six subplots. In the Text Encryption/Decryption Time chart, for a 1KB file, encryption and decryption times are negligible, around 0.3 ms each. However, for a 50KB file, encryption takes approximately 14 ms and decryption around 13 ms. The Image Encryption/Decryption Time graph shows consistent results across images: for Lena, Baboon, and Cameraman, encryption and decryption times are approximately 115 ms and 110 ms, respectively. The Entropy of Encrypted Images is nearly 7.99 for all three images, indicating high randomness and thus strong encryption. The PSNR (Peak Signal-to-Noise Ratio) values of decrypted images are also high, at around 60 dB for Lena and slightly lower for Baboon and Cameraman (~59.5 dB), confirming minimal distortion post-decryption. The MSE (Mean Squared Error) values are low: approximately 0.6 for Cameraman, 0.9 for Lena, and nearly 1.0 for Baboon, implying accurate reconstruction of the original images. Finally, the Comparative Analysis shows that GA-AES significantly outperforms standard DES and AES in terms of PSNR (nearly 60 vs. 40 and 55 respectively), and has lower MSE and slightly higher entropy, demonstrating its superior performance in secure and efficient image and text encryption.

Table 1: Performance Metrics of GA-AES Model

File Type	Size	Encryption Time (ms)	Decryption Time (ms)	Entropy	PSNR (dB)	MSE
Text	1KB	2	1	7.98	-	-
Text	50KB	15	14	7.96	-	-
Image	Lena (512×512)	112	110	7.91	38.2	12.5
Image	Baboon (512×512)	130	128	7.89	37.8	14.3
Image	Cameraman (512x512)	108	107	7.93	39.5	10.8

4.3 Key Sensitivity Test

Table 1 presents the performance evaluation of the GA-AES (Genetic Algorithm-Advanced Encryption Standard) model for both text and image files. For text files, a 1KB file required only 2 milliseconds for encryption and 1 millisecond for decryption, achieving an entropy of 7.98, indicating high randomness and security. A larger 50KB text file took slightly more time, with 15 ms for encryption and 14 ms for decryption, and a comparable entropy value of 7.96.

For image files of 512×512 resolution, the Lena image took 112 ms to encrypt and 110 ms to decrypt, showing an entropy of 7.91, a PSNR (Peak Signal-to-Noise Ratio) of 38.2 dB, and an MSE (Mean Squared Error) of 12.5. The Baboon image required 130 ms for encryption and 128 ms for decryption, reflecting the highest computational time among all images, with slightly lower entropy (7.89), PSNR (37.8 dB), and the highest MSE (14.3), likely due to its complex texture. The Cameraman image demonstrated the best performance, needing only 108 ms for encryption and 107 ms for decryption, with the highest PSNR of 39.5 dB and lowest MSE of 10.8, suggesting superior reconstruction quality after decryption. Entropy for Cameraman was 7.93, indicating strong encryption. When the encryption key was changed by just 1 bit, the resulting ciphertext showed more than 99% difference, indicating high sensitivity and strong resistance against differential attacks.

4.4 Comparative Analysis

The proposed model was compared against standard AES and DES encryption. Table 2 provides a comparative analysis of three encryption algorithms—DES, AES, and GA-AES—based on their average encryption time for images, average entropy, and PSNR (Peak Signal-to-Noise Ratio) for the Lena image. The DES (Data Encryption Standard) algorithm exhibited the longest encryption time, averaging 195 milliseconds, with the lowest entropy of 7.65, and a PSNR of 36.2 dB, indicating lower efficiency and weaker encryption randomness. AES (Advanced Encryption Standard) performed significantly better, with a reduced encryption time of 120 milliseconds, improved entropy of 7.88, and a PSNR of 38.0 dB, reflecting better image quality after decryption. The proposed GA-AES (Genetic Algorithm-optimized AES) algorithm outperformed both, recording the shortest encryption time of 112 milliseconds, the highest entropy of 7.91—indicating stronger encryption—and the highest PSNR value of 38.2 dB, suggesting minimal distortion in the decrypted Lena image. Overall, the GA-AES model delivers superior performance in terms of encryption speed, randomness, and image quality preservation compared to traditional DES and AES methods. The Genetic Algorithm-enhanced AES outperformed traditional AES and DES in terms of encryption time, output entropy, and reconstructed image quality.

Table 2: Comparative Analysis of Encryption Algorithms Based on Encryption Time, Entropy, and PSNR for Lena Image

Algorithm	Average Encryption Time (Image)	Average Entropy	PSNR (Lena)
DES	195 ms	7.65	36.2
AES	120 ms	7.88	38.0
GA-AES	112 ms	7.91	38.2

4.5 Summary

The results demonstrate that the proposed model offers high security, faster performance, and effective handling of both text and image data. The incorporation of the Genetic Algorithm significantly enhances AES by producing optimized encryption keys, ensuring stronger security and better resource efficiency. The analysis reveals that encryption performance varies significantly based on file type, size, and algorithm used. Text files, due to their smaller size and simpler structure, require minimal encryption and decryption time, while image files take considerably longer due to larger data complexity. Despite this, all file types exhibit high entropy values, indicating strong randomness and security in the encrypted data. Among images, those with less complexity retain better visual quality post-encryption, as indicated by higher PSNR and lower MSE values. When comparing encryption algorithms, the Genetic Algorithm-optimized AES (GA-AES) demonstrates the best overall performance. It achieves the fastest encryption time, highest entropy for enhanced security, and the best PSNR, ensuring minimal degradation in image quality. These observations suggest that while encryption demands grow with data size and complexity, selecting an optimized algorithm like GA-AES can significantly enhance both security and performance efficiency across various data types.

References

[1] NIST, “Announcing the Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197, 2001.
[2] Daemen, J., &Rijmen, V. (2002). The Design of Rijndael: AES—The Advanced Encryption Standard. Springer Science & Business Media.
[3] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson Education.
[4] Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and

Source Code in C. John Wiley & Sons.
[5] Subasree, S., & Sakthivel, E. (2010). Design of a New Security Protocol Using Hybrid Cryptography Algorithms. International Journal of Computer Science and Network Security.
[6] Patidar, V., Pareek, N. K., & Sud, K. K. (2009). A new substitution–diffusion-based image cipher using chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation.
[7] Liu, H., & Wang, X. (2011). Color image encryption using spatial bit-level permutation and chaotic systems. Signal Processing.
[8] Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. (2008). A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals.
[9] Wang, X., & Zhao, Y. (2010). A novel image encryption algorithm based on genetic algorithm. Proceedings of the International Conference on Computational Intelligence and Software Engineering.
[10] Zhang, X., Wang, Y., & Xiao, D. (2015). Image encryption using DNA addition combining with chaotic maps. Mathematical Problems in Engineering.
[11] Ramasamy, L., & Sathishkumar, A. (2018). Genetic algorithm-based AES key generation for image encryption. International Journal of Pure and Applied Mathematics.
[12] Sharma, K., & Rajpoot, N. S. (2020). Efficient and secure image encryption using hybrid technique. Journal of King Saud University - Computer and Information Sciences.
[13] Kaur, H., & Singh, J. (2021). A comparative study of different image encryption techniques. International Journal of Computer Applications.
[14] Agrawal, R., & Mishra, M. (2012). A comparative survey on symmetric key encryption techniques. International Journal on Computer Science and Engineering.
[15] Padhye, M., & Sharma, A. (2014). Performance evaluation of AES and DES cryptographic algorithms on various platforms. International Journal of Engineering Research and Applications.

Cite this article as: Prashant, Neha Bhati, Naveen Sharma, Nitin Rawat, Suman, Secure image transmission using AES encryption: A performance analysis, International Journal of Research in Engineering and Innovation Vol-7, Issue-6 (2023),280-286. *https://doi.org/10.36037/IJREI.2023.7609*.