Comprehensive Review and Analysis of an Image Processing Encryption Techniques

D. RISHI RAJ, D. Jaheed Basha, G. Vanajakshi
Department of Computer Science and Engineering
Guru Nanak Institute of Technical Campus, Ibrahimpatnam, Telangana
Guide: Dr. Ch. Narasimha Chary (Assistant Professor)

---***---

Abstract
Image sharing across networks has grown rapidly with the expansion of cloud platforms and multimedia communication systems. Protecting sensitive image data from unauthorized access remains a major cybersecurity challenge. This paper presents a secure image data sharing framework that integrates Advanced Encryption Standard (AES) for high-speed image encryption and Rivest–Shamir–Adleman (RSA) for secure key exchange. The proposed system uses role-based access control with modules such as Admin, User, Client, Key Generation, and Server. Quantitative analysis including encryption time comparison, NPCR, UACI, and correlation metrics demonstrates strong resistance against statistical and differential attacks. Experimental results indicate that the AES–RSA hybrid model provides improved security while maintaining efficient processing performance.

Index Terms—Image Encryption, AES, RSA, Cryptography, NPCR, UACI, Secure Image Sharing.

1.INTRODUCTION

Digital images are widely used in healthcare systems, military communication, cloud storage, and biometric authentication. Because these images often contain sensitive information, they must be protected from unauthorized access and tampering. Encryption techniques convert original images into unreadable ciphertext so that only authorized users possessing valid keys can recover the original data. Hybrid encryption models combining symmetric and asymmetric cryptography provide both efficiency and strong security guarantees.

2. LITERATURE REVIEW

Classical encryption techniques such as DES and Blowfish were widely used in early image protection systems. However, these algorithms have limitations in security strength and computational efficiency. AES has become the modern standard for symmetric encryption due to its strong resistance against brute-forceattacks.

Recent research explores hybrid encryption models combining AES with RSA or chaotic maps to improve randomness and security. Zhang et al. (2024) proposed an improved Lorenz chaotic encryption method. Peng et al. (2024) introduced selective encryption for remote sensing images. Other studies integrate blockchain auditing and deep learning techniques for enhanced image security.

3. System Architecture

The proposed system follows a client–server architecture where encrypted images are stored in a secure database. The workflow includes the following stages:
1.User uploads image
2.AES encrypts image data
3.RSA exchanges encryption keys
4.Encrypted image stored in database
5.Authorized client decrypts image

This architecture ensures confidentiality, authentication, and secure key management.

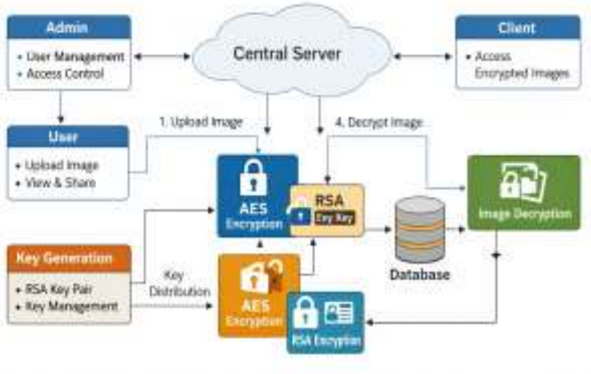

Figure 1: *System Architecture of Secure Image Sharing System*

4. PROPOSED METHODOLOGY

The proposed system uses a hybrid encryption approach that combines the Advanced Encryption Standard (AES) and the Rivest–Shamir–Adleman (RSA) algorithm to ensure secure image data sharing. AES is a symmetric encryption algorithm widely used for protecting sensitive data such as images, passwords, and confidential files. It converts readable data (plaintext) into an unreadable format called ciphertext using a secret key. AES operates on fixed-size blocks of 128 bits and supports three key lengths: 128-bit, 192-bit, and 256-bit. Depending on the key size, AES performs multiple encryption rounds: 10 rounds for AES-128, 12 rounds for AES-192, and 14 rounds for AES-256. Each round consists of several transformations such as SubBytes, ShiftRows, MixColumns, and AddRoundKey, which provide strong diffusion and confusion properties to protect data from cryptographic attacks.

AES is highly efficient and secure, making it suitable for encrypting large multimedia files such as digital images. During the encryption process, the original image is converted into ciphertext using the secret key, ensuring that unauthorized users cannot interpret the data. During decryption, the ciphertext is converted back to the original image using the same secret key. One of the major advantages of AES is its strong resistance to brute-force attacks due to its large key size. Additionally, AES requires relatively low computational resources, making it effective for both hardware and software implementations in modern computing environments.

Algorithm	Encryption Time (512x512 image)	Decryption Time
AES	0.92 s	0.88 s
AES + RSA	1.23 s	1.18 s
DES	1.76 s	1.70 s
BlowFish	1.45s	1.41s

The RSA algorithm is an asymmetric cryptographic technique used for secure key exchange and authentication. Unlike symmetric encryption methods, RSA uses two keys: a public key for encryption and a private key for decryption. The RSA algorithm is based on the mathematical difficulty of factoring very large prime numbers. In the key generation process, two large prime numbers (p and q) are selected and multiplied to produce a modulus value (n = p × q). A public exponent (e) and a private exponent (d) are then calculated using Euler's Totient function. The public key (e, n) is shared openly, while the private key (d, n) is kept secret by the receiver.

When secure communication is required, the sender encrypts the data or encryption key using the recipient's public key. The encryption process followsthe **formula:**

Ciphertext = (Plaintext^e) mod n.

The receiver then decrypts the ciphertext using the private key with the **formula:**

Plaintext = (Ciphertext^d) mod n. Because only the intended recipient possesses the private key, the confidentiality of the transmitted data is ensured.

However, RSA is computationally slower compared to symmetric algorithms like AES. Therefore, in the proposed system, RSA is primarily used for secure key exchange, while AES is used for fast and efficient encryption of the actual image data. This hybrid approach combines the speed of AES with the security of RSA, resulting in a reliable and secure image sharing system**.**

5. RESULTS AND DISCUSSION

Experimental evaluation indicates that AES-256 combined with RSA key exchange achieved an average encryption time of approximately 1.23 seconds for 512×512 pixel images. The NPCR value of 99.61% and UACI value of 33.48% indicate strong resistance to differential attacks. Additionally, correlation analysis between adjacent pixels in encrypted images approaches zero, demonstrating effective decorrelation

6. Quantitative Security Analysis

To evaluate the effectiveness of the proposed encryption model, several statistical metrics are

calculated including NPCR (Number of Pixel Change Rate), UACI (Unified Average Changing Intensity), correlation coefficient, and encryption time.

Table 1. Encryption Time Comparison

Metric	Value	Expected Secure Range	Interpretation
NPCR	99.61%	> 99%	High pixel change rate

UACI	33.48%	~33%	Strong intensity variation
Correlation	0.003	~0	Low pixel correlation

Table 2. Security Metrics Evaluation

7.CONCLUSION

This paper analyzes the effectiveness of various image encryption techniques in preserving the confidentiality and integrity of visual information during transmission and storage. Traditional cryptographic algorithms such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Blowfish remain widely used due to their strong security features and reliability. These algorithms provide robust protection against unauthorized access and cryptographic attacks. However, they often face challenges related to computational complexity, processing time, and resource consumption, particularly when dealing with large image datasets or real-time multimedia applications.

In addition to traditional encryption methods, alternative approaches such as chaos-based encryption, DNA-based encryption, and neural network–based techniques have gained significant attention in recent years. These methods offer advantages such as higher encryption speed, improved randomness, and adaptability to different image formats. Furthermore, techniques operating in the frequency domain and compressive sensing methods can reduce redundancy and improve encryption efficiency for large-scale image data. Despite these advancements, challenges such as secure key management, scalability, and computational overhead still remain. A comparative analysis of these techniques highlights the trade-offs between security, speed, and efficiency, enabling researchers to select the most appropriate encryption strategy based on specific application requirements.

8. FUTURE SCOPE

Future research may explore blockchain-based audit trails for secure image access logging, quantum-resistant encryption algorithms, and homomorphic encryption techniques that allow computation on encrypted images without decryption.

REFERENCES

algorithms: A survey of design and evaluation metrics,'' J. Cybersecurity Privacy, vol. 4, no. 1, pp. 126–152, Feb. 2024, doi: 10.3390/jcp4010007.

[2] P. R. Sankpal and P. A. Vijaya, ''Image encryption using chaotic maps: A survey,'' in Proc. 5th Int. Conf. Signal Image Process., Jan. 2014, pp. 102–107, doi: 10.1109/ICSIP.2014.80.

[3] M. Sun, J. Yuan, X. Li, D. Liu, and X. Wei, ''A novel color image encryption based on chaos and DNA mutation,'' in Proc. 9th Int. Conf. Signal Image Process. (ICSIP), Jul. 2024, pp. 717–725, doi: 10.1109/icsip61881.2024.10671465.

[4] X. He, L. Li, H. Peng, and F. Tong, ''An efficient image privacy preservation scheme for smart city applications using compressive sensing and multi-level encryption,'' IEEE Trans. Intell. Transp. Syst., vol. 25, no. 10, pp. 14958–14972, Oct. 2024, doi: 10.1109/TITS.2024. 3389066.

[5] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, ''A new image encryption algorithm for grey and color medical images,'' IEEE Access, vol. 9, pp. 37855–37865, 2021.

[6] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, ''Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains,'' Int. J. Inf. Secur., vol. 21, no. 4, pp. 917–935, Aug. 2022, doi: 10.1007/s10207-022-00588-5.

[7] A. M. Abdullah, ''Advanced encryption standard (AES) algorithm to encrypt and decrypt data,'' Cryptography Netw. Secur., vol. 16, no. 1, p. 11, 2017.

[8] A. Bastanta, R. Nuryansyah, C. A. Nugroho, and W. Budiharto, ''Image data encryption using Des method,'' in Proc. 1st Int. Conf. Comput. Sci. Artif. Intell. (ICCSAI), vol. 1, Oct. 2021, pp. 130–135, doi: 10.1109/ICCSAI53272.2021.9609738.

[9] V. Anusuya Devi and T. Sampradeepraj, ''End-to-end self-organizing intelligent security model for wireless sensor network based on a hybrid (AES–RSA) cryptography,'' Wireless Pers. Commun., vol. 136, no. 3, pp. 1675–1703, Jun. 2024, doi: 10.1007/s11277-024-11353-3.

[10] H. Tiwari and N. Hamsapriye, ''Logistic map-based image encryption scheme,'' Int. J. Appl. Eng. Res., vol. 13, no. 23, pp. 16573–16577, 2018.

[11] S. Agrawal and B. R. Madhu, ''An improved Henon map based encryption scheme for secure image transmission,'' in Proc. IEEE Int. Conf. Contemp. Comput. Commun. (InC4), Mar. 2024, pp. 1–6, doi: 10.1109/inc460750.2024.10649235.

[12] H. Tora, E. Gokcay, M. Turan, and M. Buker, ''A generalized Arnold's cat map transformation for image scrambling,'' Multimedia Tools Appl., vol. 81, no. 22, pp. 31349–31362, Sep. 2022, doi: 10.1007/s11042-022-11985-2.

[13] H. A. Mohamed, A. H. Madian, A. A. Abdel-Hafez, and W. Anis, ''Modified blowfish algorithm based on improved Lorenz attractor,'' in jProc. 39th Nat. Radio Sci. Conf. (NRSC), vol. 1, Nov. 2022, pp. 151–163, doi: 10.1109/NRSC57219.2022.9971261.

[14] L. Oteko Tresor and M. Sumbwanyambe, ''A selective image encryption scheme based on 2D DWT, Henon map and 4D qi hyper-chaos,'' IEEE Access, vol. 7, pp. 103463–103472, 2019.

[15] J. C. Dagadu, J.-P. Li, F. Shah, N. Mustafa, and K. Kumar, ''DWT based encryption technique for medical images,'' in Proc. 13th Int. Comput. Conf.Wavelet Act. Media Technol. Inf. Process. (ICCWAMTIP), Dec. 2016, pp. 252–255.

[16] J. Lee and H. Kim, ''Discrete cosine transformed images are easy to recognize in vision transformers,'' IEIE Trans. Smart Process. Comput., vol. 12, no. 1, pp. 48–54, Feb. 2023.

[17] K. Megala, J. Jayadevi, K. Keerthika, G. Manikandan, and B. Srinivasan, ''Secure medical image encryption using homomorphic techniques,'' in Proc. 2nd Int. Conf. Adv. Inf. Technol. (ICAIT), Jul. 2024, pp. 1–6, doi: 10.1109/icait61638.2024.10690754.

[18] V. Kumar, G. Singh, and B. Singh, ''A comparative study of various lossless compression techniques of steganography and cryptography,'' in Proc. Int. Conf. Comput. Sci. (ICCS), Dec. 2021, pp. 285–288, doi: 10.1109/ICCS54944.2021.00063.

[19] B. Selvakumar, P. Abinaya, B. Lakshmanan, S. Sheron, and T. Smitha Rajini, ''Hybrid image encryption using advanced least significant bit algorithm, chaotic maps and DNA encoding for digital healthcare,'' J. Intell. Fuzzy Syst., vol. 46, no. 4, pp. 9139–9153, Apr. 2024, doi: 10.3233/jifs-236637.

[20] J. He, H. Zhu, and X. Zhou, ''Quantum image encryption algorithm via optimized quantum circuit and parity bit-plane permutation,'' J. Inf. Secur. Appl., vol. 81, Mar. 2024, Art. no. 103698, doi: 10.1016/j.jisa.2024.103698.

[21] X. Zhang, G. Liu, and C. Zou, ''An image encryption method based on improved Lorenz chaotic system and Galois field,'' Appl. Math. Model., vol. 131, pp. 535–558, Jul. 2024, doi: 10.1016/j.apm.2024.04.023.

[22] J. Peng, Y. Luo, S. Jin, B. Mou, C. Li, and W. Chen, ''Remote sensing image encryption algorithm based on chaotic system and DNA sequence,'' in Proc. IEEE 19th Conf. Ind. Electron. Appl. (ICIEA), Aug. 2024, pp. 1–5, doi: 10.1109/iciea61579.2024.10665040.

[23] M. Alawida, J. S. Teh, and W. H. Alshoura, ''A new image encryption algorithm based on DNA state machine for UAV data encryption,'' Drones, vol. 7, no. 1, p. 38, Jan. 2023, doi: 10.3390/drones7010038.

[24] T. Mahjabin, A. Olteanu, Y. Xiao, W. Han, T. Li, and W. Sun, ''A survey on DNA-based cryptography and steganography,'' IEEE Access, vol. 11, pp. 116423–116451, 2023, doi: 10.1109/ACCESS.2023.3324875.

[25] Y. Ding, Z. Wang, Z. Qin, E. Zhou, G. Zhu, Z. Qin, and K.-K.-R. Choo, ''Backdoor attack on deep learning-based medical image encryption and decryption network,'' IEEE Trans. Inf. Forensics Security, vol. 19, pp. 280–292, 2024, doi: 10.1109/TIFS.2023.3322315.

[26] Y. Alslman, E. Alnagi, A. Ahmad, Y. AbuHour, R. Younisse, and Q. Abu Al-haija, ''Hybrid encryption scheme for medical imaging using AutoEncoder and advanced encryption standard,'' Electronics, vol. 11, no. 23, p. 3967, Nov. 2022, doi: 10.3390/electronics11233967.

[27] A. Hu, X. Gong, and L. Guo, ''Joint encryption model based on a randomized autoencoder neural network and coupled chaos mapping,'' Entropy, vol. 25, no. 8, p. 1153, Aug. 2023, doi: 10.3390/e25081153.

[28] W. Alexan, D. El-Damak, and M. Gabr, ''Image encryption based on Fourier-DNA coding for hyperchaotic Chen system, chen-based binary quantization S-box, and variable-base modulo operation,'' IEEE Access, vol. 12, pp. 21092–21113, 2024.

[29] J. Peta and S. Koppu, ‘‘Enhancing breast cancer classification in histopathological images through federated learning framework,’’ IEEE Access, vol. 13, pp. 12345–12356, 2025, doi: 10.1109/ACCESS.2023.3283930.

[30] M. Nabil, ‘‘Random projection and its applications,’’ 2017, arXiv:1710.03163.

[31] Y. Saad, Iterative Methods for Sparse Linear Systems. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 2003.

[32] B. Schneier, Applied Cryptography Protocols, Algorithms and Source Code in C. Wiley, 2007.

[33] K. N. Singh and A. K. Singh, ‘‘Towards integrating image encryption with compression: A survey,’’ ACM Trans. Multimedia Comput., Commun., Appl., vol. 18, no. 3, pp. 1–21, Aug. 2022, doi: 10.1145/3498342.

[34] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, ‘‘A comprehensive survey on image encryption: Taxonomy, challenges, and future directions,’’ Chaos, Solitons Fractals, vol. 178, Jan. 2024, Art. no. 114361, doi: 10.1016/j.chaos.2023.114361.

[35] D. Singh, S. Kaur, M. Kaur, S. Singh, M. Kaur, and H.-N. Lee, ‘‘A systematic literature review on chaotic maps-based image security techniques,’’ Comput. Sci. Rev., vol. 54, Nov. 2024, Art. no. 100659, doi: 10.1016/j.cosrev.2024.100659.