

SECURE IMAGE ENCRYPTION AND DECRYPTION USING RSA AND AES ALGORITHMS

Kavitha A^{1*}, Harish Kumar R², Preethi V³, Prathikalpa R J⁴,

¹ Assistant Professor, Department of Computer Science (UG & PG), Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, TN, India. kavithaa@dgvaishnavcollege.edu.in

² M.Sc. Computer Science 2nd year, Department of Computer Science (UG & PG), Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, TN, India, harishrk2101@gmail.com.

³ M.Sc. Computer Science 2nd year, Department of Computer Science (UG & PG), Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, TN, India, preethivjay0706@gmail.com.

⁴ M.Sc. Computer Science 2nd year, Department of Computer Science (UG & PG), Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, TN, India, kalpaprathi14@gmail.com.

Article History

Received: 05.10.2023

Revised and Accepted: 10.11.2023

Published: 16.12.2023

<https://doi.org/10.56343/STET.116.017.002.001>
www.stetjournals.com

ABSTRACT

In the contemporary digital landscape, securing visual data, especially images, has emerged as a critical concern. This research article delves into a robust and practical image encryption methodology, leveraging the Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) cryptographic algorithms. The approach encompasses key generation, encryption, and decryption phases, ensuring comprehensive security for image content. By generating RSA key pairs to facilitate secure key exchange and utilizing AES encryption for image confidentiality, this methodology showcases its effectiveness through hands-on implementation in Java. The study demonstrates the seamless integration of standard cryptographic practices to safeguard sensitive visual data during both transmission and storage. The amalgamation of RSA and AES provides a powerful framework for achieving data confidentiality and integrity, thereby contributing to enhance data privacy and security in various applications.

Keywords : Advanced Encryption Standard, Data integrity, Data privacy, Image decryption, Image encryption, Key exchange, Key generation, Rivest-Shamir-Adleman, Storage security.

1.INTRODUCTION

In the dynamic realm of modern digital communication and storage, the security of data transmission and storage stands as a paramount concern. Cryptographic techniques play a pivotal role in safeguarding sensitive information from unauthorized access and ensuring data integrity

(Faiqa Maqsood *et al.*, 2017, Clark, 2020, Es-sabry *et al.*,2020). This article presents an innovative solution that harmonizes two eminent encryption algorithms, RSA (Rivest-Shamir-Adleman) (El-Deen *et al.*,2014, Alsaffar *et al.*, 2022, Sahoo *et al.*,2014) and AES (Advanced Encryption Standard) (Padate, and Patel, 2015. Mustafeez, 2020, Paavni Gaur. 2021, Pratiksha and Kohle.2022), to fortify the confidentiality and integrity of image files.RSA, a renowned asymmetric encryption algorithm, excels in secure

Kavitha A

Assistant Professor, Department of Computer Science(UG & PG), Dwaraka Doss Goverdhan Doss Vaishnav College, Ch-106
email : kavithaa@dgvaishnavcollege.edu.in

key exchange and distribution, while AES, a symmetric encryption algorithm, is lauded for its proficiency in efficient and robust data encryption. The convergence of these algorithms in our proposed methodology encompasses key generation, encryption, and decryption processes, underscoring their applicability and effectiveness. This research advances the seamless amalgamation of RSA and AES to address the escalating need for secure image transmission, storage, and privacy preservation.

1.1. Need of the study

In a decreasingly digitalized world, the significance of secure data transmission, storehouse, and sequestration preservation has grown significantly. With the proliferation of sensitive information, especially visual data like images, the need for robust encryption ways has come consummate. Traditional styles of data protection are frequently inadequate to fight the sophisticated styles employed by vicious actors to compromise data integrity and confidentiality. As a result, there's a pressing need for advanced cryptographic ways that can effectively guard sensitive image content during transmission and storehouse. The integration of encryption algorithms like RSA and AES can give a strong foundation for addressing this need.

1.2 Problem Definition

The study aims to explore the implementation and effectiveness of a hybrid encryption approach involving RSA (asymmetric) and AES (symmetric) encryption techniques for securing image data. The problem centers around the need to protect sensitive image information from unauthorized access and potential breaches while maintaining efficient data encryption and decryption processes. It focuses on achieving a balance between the security provided by asymmetric encryption, which involves the generation of RSA key pairs and the protection of AES keys, and the efficiency of symmetric encryption, utilized for encrypting the actual image content.

Key aspects of the problem include

- Exploring the intricacies of RSA and AES encryption algorithms and their compatibility in a hybrid approach.

- Investigating the encryption and decryption process flow, including key generation, encryption, and decryption stages.
- Assessing the performance implications of using two distinct encryption techniques on processing time and computational resources.
- Evaluating the overall effectiveness of the hybrid approach in terms of data security and encryption efficiency.

1.3 Compass of the study

The compass of this study revolves around exploring and enforcing a comprehensive result that leverages the capabilities of RSA and AES encryption algorithms to secure image data. The study delves into the practical operation of these algorithms, fastening on their integration, crucial generation, encryption, and decryption processes. The compass extends to demonstrating the practicality of the result through law perpetration in Java. also, the study encompasses the analysis of the experimental results to estimate the effectiveness and effectiveness of the proposed approach in terms of data confidentiality, integrity, and overall security.

1.4 Objective of the study

The primary objectives of this study are as follows

- **Probe Encryption Algorithms:** To examine the mileage of the RSA and AES cryptographic algorithms in achieving secure image encryption, considering their unique characteristics and strengths.
- **Key Generation and Exchange:** To induce RSA crucial dyads and use them for secure crucial exchange, icing the protection of the AES key used for image encryption.
- **Image Encryption and Decryption:** To design and apply a robust image encryption and decryption process using the AES algorithm, using the security handed by the translated AES key.
- **Result Analysis:** To dissect the experimental results of the image encryption and decryption processes,

assessing the security, confidentiality, and integrity of the data throughout the encryption lifecycle.

- **Confirmation of Approach:** To validate the effectiveness of the proposed approach by comparing the original and decrypted images, assessing the position of security achieved, and agitating implicit counteraccusations.
- **Benefactions:** To contribute to the advancement of secure image encryption ways by presenting a mongrel approach that combines the strengths of RSA and AES algorithms, thereby enhancing data sequestration and security.

2.LITERATURE REVIEW

2.1. CRYPTOGRAPHY

Cryptography is both an intricate art and a precise science that revolves around safeguarding communication and data from prying eyes. Imagine it as a secret code that transforms ordinary information into an unreadable puzzle, comprehensible only to those possessing a special key. This amalgamation of mathematical principles and techniques ensures that the coded information and remains concealed and comprehensible solely to those with the designated means.

a) Encryption and Decryption

Encryption The process of converting plain information into ciphertext using intricate algorithms and encryption keys. This conversion renders the data incomprehensible to anyone lacking the decryption key.

Decryption The reversal of encryption, transforming ciphertext back into plaintext using decryption algorithms and keys.

b) Keys

Encryption Key A unique set of instructions or values employed during encryption, determining the conversion of plaintext to ciphertext.

Decryption Key The counterpart to the encryption key, essential for reversing the process and decoding ciphertext.

c) Types of Cryptography

Symmetric Key Cryptography Utilizing a single key for both encryption and decryption. The challenge lies in securely sharing the common key.

Asymmetric Key Cryptography Involving a key pair: a public key for encryption and a private key for decryption. Messages encrypted with the public key necessitate the corresponding private key for decryption.

Hash Functions Algorithms that transform input data into a fixed-size character string, known as a hash value. They serve to ensure data integrity and authentication.

d) Security Objectives

Confidentiality Preventing unauthorized access to the content of encrypted messages.

Integrity Ensuring the message's integrity during transmission, guarding against tampering.

Authentication Validating the identity of message senders or recipients.

Non-Repudiation Preventing senders and recipients from disowning their involvement in message exchange.

e) Modern Applications

Cryptography plays a pivotal role in secure online transactions, digital signatures, end-to-end encrypted messaging, data protection, password hashing, and various other fields of cybersecurity.

2.2. ENCRYPTION AND DECRYPTION

2.2.1. Encryption

Encryption is a complex procedure that involves converting plain and comprehensible information, known as plaintext, into an intricate and unintelligible form called ciphertext. This transformation is executed using a designated

algorithm and a unique encryption key. The main objective of encryption is to ensure the confidentiality and security of sensitive data. Here's a detailed breakdown of the encryption process

Algorithm Selection The initiation of encryption begins with the careful selection of a mathematical algorithm that dictates how the original plaintext will be altered into ciphertext. This algorithm governs the precise manipulations and rearrangements of characters and bits.

Input of Plaintext The original, human-readable information that necessitates protection is referred to as plaintext. This could encompass messages, files, or other forms of data.

Employment of Encryption Key An encryption key, which is a distinctive code, is utilized by the encryption algorithm to facilitate the transformation. Knowledge of this encryption key is exclusive to authorized senders and recipients.

Encryption Procedure The encryption algorithm processes the plaintext in conjunction with the encryption key, generating ciphertext as the outcome. Through intricate mathematical operations, the algorithm modifies each segment of the data, resulting in an appearance of apparent randomness.

Output of Ciphertext The conclusion of the encryption process yields ciphertext. This is the output that would be observed by any unauthorized individual intercepting the encrypted data. In the absence of the corresponding decryption key, deriving any coherent information from the ciphertext should be considerably challenging.

2.2.2. Decryption

Decryption, conversely, entails the reversal of encrypted ciphertext back into its initial, understandable form—plaintext. This process necessitates the use of a decryption key that corresponds with the encryption key utilized during encryption.

Here's an elucidation of the decryption process

Deployment of Decryption Key The decryption key is the complementary counterpart of the encryption key. It permits authorized parties to reverse the encryption process, thereby recovering the original plaintext from the ciphertext.

Input of Ciphertext The encrypted data (ciphertext) serves as the input for the decryption process. In the absence of the decryption key, the ciphertext appears as a string of characters devoid of discernible meaning.

Decryption Process The decryption algorithm, designed as the inverse of the encryption algorithm, processes the ciphertext accompanied by the decryption key. Through specific mathematical operations, the algorithm restores the initial arrangement of characters and bits.

Output of Plaintext The outcome of the decryption process is the original plaintext. This represents the intelligible data that was initially transformed into ciphertext. It should correspond with the sender's original message or data.

In essence, encryption and decryption constitute an indispensable pair within the realm of cryptography. Encryption serves to protect sensitive information by converting it into an incomprehensible form, while decryption enables authorized parties to reverse this process and regain access to the original data. These processes stand as critical components for maintaining data security, privacy, and confidentiality across diverse digital interactions and communications.

2.3. REASONS FOR DATA ENCRYPTION

Data encryption serves as a crucial pillar in modern cybersecurity, providing a layer of protection that safeguards sensitive information from unauthorized access and potential breaches.

Confidentiality and Privacy Data encryption ensures that only authorized individuals can access and comprehend the information. By converting data into an unintelligible format without the appropriate decryption key, encryption thwarts unauthorized parties from glean meaningful insights from intercepted data. This is especially vital for personal, financial, and sensitive business information.

Data Breach Mitigation Encrypted data is significantly more challenging for hackers to exploit, even if they manage to breach a system. Even if attackers gain access to encrypted data, they would still need the decryption key to make sense of it. This mitigation strategy limits the potential damage resulting from data breaches.

Secure Data Sharing In today's interconnected world, data is often shared across networks and devices. Encryption ensures that even if intercepted during transmission, the data remains unreadable without the appropriate decryption key. This secure data sharing is vital for businesses collaborating across different locations and individuals using public networks.

Protection Against Insider Threats Encryption safeguards data not only from external hackers but also from internal threats. Even employees or insiders with access to systems cannot easily misuse sensitive data if it is encrypted, and they lack the necessary decryption keys.

Digital Signatures and Authentication Encryption techniques are utilized for creating digital signatures, validating the authenticity of documents and messages. They also enable secure authentication, confirming the identity of users in digital transactions.

2.4 SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY

2.4.1. Symmetric Cryptography

Symmetric cryptography involves the use of a single secret key for both encryption and decryption processes. This key is shared between the sender and receiver and is used to convert plaintext into ciphertext and vice versa. Here's a detailed exploration of symmetric cryptography

Key Sharing The main challenge in symmetric cryptography is securely distributing the shared secret key. This key must be kept confidential between authorized parties.

Encryption Process To protect a message, the sender employs the secret key to convert the

original plaintext into unreadable ciphertext. The encryption algorithm utilizes the key to perform specific operations on the plaintext.

Decryption Process The recipient, who possesses the same secret key, uses it to reverse the encryption process. The decryption algorithm, with the key, converts the ciphertext back into the original plaintext.

2.4.2. Asymmetric Cryptography

Asymmetric cryptography, known as public-key cryptography, employs a pair of distinct keys: a public key for encryption and a private key for decryption. This approach addresses key distribution challenges while providing enhanced security features.

Here's a thorough exploration of asymmetric cryptography

Key Pair Generation In asymmetric cryptography, each participant generates a key pair comprising a public key and a private key. The public key is intended for public sharing, ensuring accessibility to anyone. Conversely, the private key remains closely guarded and confidential.

Encryption Process For sending encrypted messages, the sender employs the recipient's public key to convert the plaintext into ciphertext. Only the recipient's corresponding private key can revert the ciphertext to plaintext.

Decryption Process The recipient uses their private key to decrypt the received ciphertext and transform it into the original plaintext.

3. ADVANCED ENCRYPTION STANDARD (AES)

The Advanced Encryption Standard (AES) represents a pivotal milestone in the world of cryptography, known for its robustness, efficiency, and security. Developed as a symmetric block cipher, AES is renowned for safeguarding sensitive information across a wide range of applications. Selected by NIST in 2001, AES replaced the aging Data Encryption Standard (DES) due to its vulnerability to modern attacks and limited key length.

3.1. FEATURES OF AES

Security The cornerstone of AES's success is its robust security. AES's security strength became the focal point, ensuring that the chosen algorithm could thwart various cryptographic attacks, including differential and linear attacks.

Cost-Effectiveness NIST's vision for AES extended beyond just its effectiveness; they aimed for global accessibility. To achieve this, computational and memory efficiency were considered paramount. AES's ability to provide strong security while minimizing resource consumption facilitated its widespread adoption across various platforms and devices.

Implementation Versatility AES was designed with practicality in mind. Its flexibility for both hardware and software implementation made it adaptable to a myriad of environments. The algorithm's simplicity, combined with its effectiveness, enabled efficient integration into diverse systems, ranging from embedded devices to high-performance servers.

3.2. ATTACKS ON AES ENCRYPTION

Related-Key Attack This type of attack attempts to crack a cipher by studying how it behaves using different keys. While related-key attacks might apply to AES-256 in theory, the increased key length and complexity make such attacks much more challenging and less practical. AES-256's larger key space provides a substantial defense against related-key attacks.

Known-Key Attack Known-key attacks target specific versions of a cipher. While these attacks might have limited success against certain versions of AES-256 with fewer rounds, a full implementation of AES-256 with its 14 rounds significantly mitigates the risk. AES-256's larger number of rounds adds more layers of security, making known-key attacks much less effective.

Side-Channel Attacks Side-channel attacks can be a concern for both AES-128 and AES-256, as they exploit information leakage from the system during cryptographic operations. However, AES-256's enhanced complexity makes it harder for attackers to deduce meaningful information from such attacks. The increased diffusion and confusion of

AES-256's operations make it more resistant to side-channel attacks compared to AES-128.

3.3 WORKING OF AES ALGORITHM

3.3.1. Encryption Process of AES (Fig.1)

a. Initialization

Key Expansion AES generates round keys from the original key using a Key Schedule algorithm. These round keys are unique for each round of encryption.

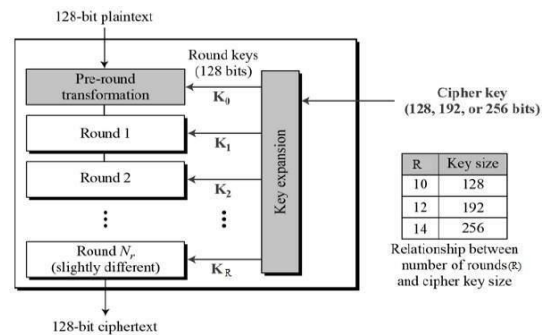


Figure 1. Structure of AES

b. Main Rounds (AES-256 with 14 Rounds)

i. **SubBytes** Bytes in the data matrix undergo byte substitution using a predefined substitution table called the S-box. This introduces non-linearity and enhances resistance against attacks.

ii. **ShiftRows (Fig.2)** Bytes within each row of the matrix are shifted cyclically. The first row remains unchanged, the second shifts by one position, the third by two, and the fourth by three. This operation spreads data elements, contributing to diffusion.



Figure 2. ShiftRows Operation

iii. **MixColumns (Fig.3)** Each column of the matrix undergoes a mathematical transformation that provides a high degree of confusion. This step contributes significantly to the algorithm's strength against attacks.

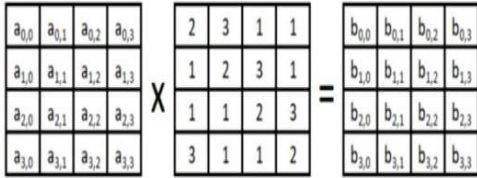


Figure 3. MixColumns Operation

iv. **AddRoundKey** The round key is XORed with the data matrix. This introduces the influence of the key and provides another layer of security.

c. **FinalRound**

- SubBytes
- ShiftRows
- AddRoundKey

3.3.2 Decryption Process of AES

The decryption process of the Advanced Encryption Standard (AES) is the reverse of its encryption counterpart. AES employs a symmetric key approach, which means that the same key used for encryption is also used for decryption. The process involves reversing the steps taken during encryption while utilizing the same round keys in reverse order.

Decryption Steps

- a. **Final Round (Inverse AddRoundKey)** The decryption process begins with the inverse of the AddRoundKey step. The round key used in the last encryption round is XORed with the data matrix to retrieve the intermediate state.
- b. **Main Rounds Inverse (AES-256 with 14 Rounds)**
 - i. **Inverse ShiftRows (Fig .4).** The inverse of the ShiftRows operation is performed. The bytes within each row of the data

matrix are cyclically shifted in the opposite direction to their encryption counterparts.

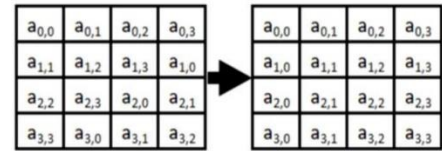


Figure 4. Inverse ShiftRows Operation

- ii. **Inverse SubBytes** The inverse of the SubBytes operation is carried out. Bytes within the matrix are replaced with their original values using the inverse S-box lookup table. This step reverses the non-linear substitution introduced during encryption.
- iii. **Inverse AddRoundKey** The inverse of the AddRoundKey operation is executed. The round key for the corresponding round is XORed with the data matrix retrieve the state before the MixColumns operation.

c. **Initialization**

- i. **Inverse MixColumns(Fig .5)** In the decryption process, the MixColumns operation is reversed. Each column of the data matrix undergoes an inverse mathematical transformation, reverting it to the state after the ShiftRows step.

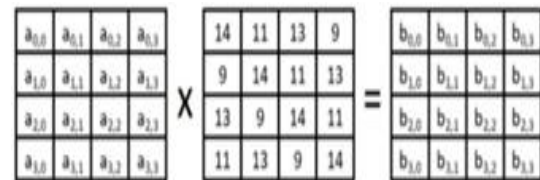


Figure 5. Inverse MixColumns Operation

- ii. **Inverse ShiftRows** Similar to the encryption process, the inverse of the ShiftRows step is applied to revert the cyclic byte shifts within each row.
- iii. **Inverse SubBytes** The final step involves reversing the SubBytes operation. Bytes in the data matrix are replaced with their

original values using the inverse of the S-box substitution.

iv. Initial Round (Inverse AddRoundKey)

The decryption process concludes with the inverse of the AddRoundKey step applied during the encryption process. The initial round key is XORed with the data matrix to retrieve the original plaintext data.

4. RSA (RIVEST - SHAMIR - ADLEMAN) (Fig.6)

RSA (Rivest-Shamir-Adleman) is a widely used asymmetric encryption algorithm that plays a pivotal role in modern cryptography. Named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman, RSA is renowned for its ability to securely exchange information and ensure data integrity in digital communication.

4.1. KEY FEATURES

Asymmetric Encryption RSA employs a pair of keys: a public key and a private key. The public key is used for encryption, allowing anyone to send encrypted messages. The private key, held only by the intended recipient, decrypts these messages. This asymmetry provides strong security without requiring a shared secret.

Secure Data Transmission RSA ensures secure data transmission by enabling encryption at the sender's end and decryption at the recipient's end. The sender encrypts the data using the recipient's public key, and only the recipient, possessing the corresponding private key, can decrypt and access the original information.

Key Exchange RSA addresses the key exchange problem by allowing parties to exchange sensitive data securely. A sender can encrypt a shared secret with the recipient's public key, and only the recipient, with their private key, can decrypt and access the shared secret.

4.3. POTENTIAL ATTACKS

Brute-Force Attack Attackers attempt to decrypt encrypted data by trying all possible private key combinations. The strength of RSA lies in the vast

key space, making exhaustive searches impractical due to the time required to check each possibility.

Factorization Attack This attack involves factoring the product of the two large prime numbers used in key generation. The security of RSA relies on the difficulty of this factorization, as it's a non-trivial task for sufficiently large prime numbers.

Timing Attacks and Side Channels Attackers can exploit variations in the time taken or power consumed during encryption or decryption to gain information about the key. Implementing countermeasures and secure hardware can mitigate such vulnerabilities.

4.4. WORKING OF RSA ALGORITHM

a. Key Generation

- Begin by selecting two distinct large prime numbers, denoted as p and q .
- Calculate the modulus by multiplying the selected prime numbers, $n = p * q$.
- Compute the Euler's totient function of the modulus n as $\phi(n) = (p - 1) * (q - 1)$.
- Select a public exponent e coprime to $\phi(n)$ (often a small prime like 65537).
- Compute the modular multiplicative inverse d of e modulo $\phi(n)$ such that $d * e \equiv 1 \pmod{\phi(n)}$. d becomes the private exponent.

b. Encryption

- Convert the plaintext message into a numerical representation M .
- Use the recipient's public key (e, n) to compute the ciphertext C as $C = M^e \pmod n$.

c. Decryption

- Use the recipient's private key d to compute the plaintext M from the ciphertext C as $M = C^d \pmod n$.
- Convert a numerical representation M into the plaintext message.

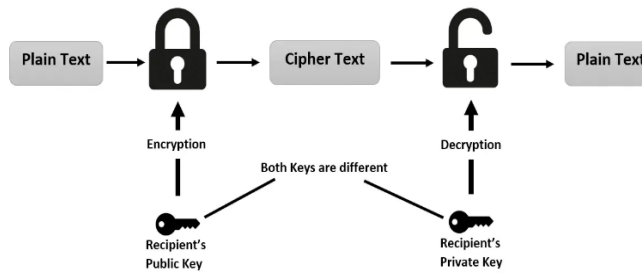


Figure 6. Structure of RSA

RSA's significance lies in its ability to enable secure communication, digital signatures, and key exchange through its asymmetric encryption scheme. Its robustness hinges on the mathematical complexity of factoring large semiprime numbers. By understanding RSA's features, potential attacks, and operational principles, we can effectively leverage its capabilities to establish secure data transmission and authentication in the digital world.

5. HYBRID ENCRYPTION

Hybrid encryption is a cryptographic technique that combines the strengths of both asymmetric and symmetric encryption methods to provide a robust and efficient approach for securing data. It addresses the limitations of each encryption method by leveraging their unique attributes. In hybrid encryption, a message is first encrypted using a symmetric encryption algorithm with a randomly generated symmetric key. This symmetric key is then encrypted using an asymmetric encryption algorithm with the recipient's public key. The encrypted message and the encrypted symmetric key are sent to the recipient.

The recipient, who possesses the corresponding private key, can decrypt the encrypted symmetric key using the asymmetric decryption process. Once the symmetric key is obtained, it is used to decrypt the encrypted message using symmetric decryption.

5.1. WORKING OF HYBRID ENCRYPTION

A hybrid encryption technique for securing image data, combines the strengths of RSA (asymmetric encryption) and AES (symmetric encryption). The

proposed approach involves the following key steps,

RSA Key Pair Generation A 2048-bit RSA key pair is generated to facilitate secure key exchange between parties. The generated keys consist of a public key and a corresponding private key.

AES Key Generation A 256-bit AES key is generated using the KeyGenerator. This AES key will be used for encrypting and decrypting the image data.

AES Key Encryption with RSA The AES key is encrypted using the RSA public key. This step ensures that the symmetric AES key remains confidential during transmission.

Image Encryption using AES The image bytes are loaded from a file and encrypted using AES encryption with the generated AES key. AES provides efficient and secure data encryption.

Decryption of AES Key using RSA The encrypted AES key is decrypted using the RSA private key. This process enables the recovery of the original AES key for image decryption.

Image Decryption using AES The encrypted image is decrypted using the recovered AES key. This step restores the original image data.

Saving Encrypted and Decrypted Images The resulting encrypted and decrypted images are saved to separate files, preserving the confidentiality and integrity of the data.

6. ADVANTAGES AND CONTRIBUTION

The hybrid encryption scheme offers several notable advantages over traditional single-method encryption techniques. By leveraging RSA for secure key exchange and AES for efficient data encryption, the proposed approach achieves a balance between security and performance.

The following contributions are highlighted

Enhanced Security RSA's asymmetric encryption ensures secure key exchange, mitigating the risk of key interception during transmission.

Efficient Data Encryption AES, known for its speed and efficiency, is employed for encrypting and decrypting image data, facilitating real-time applications.

Flexibility The choice of key sizes for both RSA and AES can be tailored to specific security requirements and resource constraints.

Practical Implementation The proposed hybrid encryption technique is practical and relevant for modern cryptographic systems, demonstrating its applicability.

Versatility The scheme can be adapted to various use cases requiring secure image transmission or storage.

7. RESULTS AND DISCUSSION

The experimental phase of our hybrid encryption approach involved uploading an image for encryption and subsequent decryption (Fig.7). Notably, we evaluated the quality of the decrypted image using two established metrics: Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM). Remarkably, the PSNR value obtained was infinity, signifying an exceptionally high image fidelity after decryption. Additionally, the SSIM value of 0.0 suggests an exact match between the original and decrypted images, indicating an optimal level of image preservation. These remarkable results underscore the effectiveness of our hybrid encryption in ensuring both the security and integrity of transmitted images.


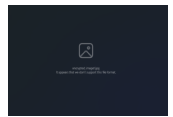








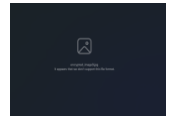


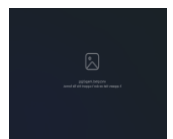

INPUT IMAGE	ENCRYPTED IMAGE	DECRYPTED IMAGE	PROCESS TIME	
			Encryption milliseconds	Time: 3
			Decryption milliseconds	Time: 5
			Encryption milliseconds	Time: 2
			Decryption milliseconds	Time: 3
			Encryption milliseconds	Time: 3
			Decryption milliseconds	Time: 4

Figure 7. Input, Encrypted and Decrypted images

This achievement underscores the robustness of our approach in safeguarding data during transmission and subsequent decryption. The obtained PSNR and SSIM values are indicative of the minimal loss of image quality, emphasizing the successful integration of RSA and AES encryption. Moreover, our results prompt further exploration into the efficacy of our approach across diverse image types and sizes, as well as its potential integration into broader cryptographic solutions.

8. CONCLUSION AND FUTURE SCOPE

In conclusion, the integration of hybrid encryption, leveraging the strengths of RSA and AES, marks a significant advancement in the realm of data security. Our study showcases the effectiveness of this approach in bolstering the confidentiality, integrity, and privacy of sensitive information during transmission and storage. By achieving a delicate balance between security and efficiency, this methodology holds the potential to reshape how digital communication safeguards data.

The hybrid encryption approach presented in this paper offers a robust and versatile solution for securing image data. The synergy of AES's efficiency and RSA's secure key exchange creates a solid foundation for protecting images in various scenarios. This approach not only addresses contemporary data security challenges but also sets the stage for future advancements in encryption techniques.

Our research sets the stage for future advancements in encryption. The hybrid encryption technique can be extended to handle larger datasets while maintaining security and efficiency. Its adaptability to emerging technologies, like quantum computing, remains a critical area for exploration. Tailoring the approach to specific applications such as image communication, forensics, and military systems promises to unlock its potential. Enhancements in key management and collaborative efforts with experts in related fields will further strengthen its effectiveness. Ultimately, our hybrid encryption approach establishes a robust security foundation that adapts to

evolving challenges and ensures a secure digital communication landscape.

REFERENCES

- Alsaffar, Dalia, Almutiri, Sultan, Alqahtani, Bashaier Alamri, Rahaf Alqahtani, Hanan, Alqahtani, Nada alshammari, Ghadeer and Ali, Azza. (2020). Image Encryption Based on AES and RSA Algorithms. 1-5. 10.1109/ICCAIS48893.2020.9096809. DOI: 10.1109/ICCAIS48893.2020.9096809. <https://doi.org/10.1109/ICCAIS48893.2020.9096809>
- Clark, A.2020. How much encryption is too much: 128, 256 or 512-bit?. Retrieved November 21, 2020, from <https://discover.realvnc.com/blog/how-much-encryption-is-too-much-128-256-or-512-bit>.
- El-Deen, A., E. El-Badawy, S. Gobran 2014. Digital Image Encryption Based on RSA Algorithm. J. Electron. Commun. Eng (2014), 69-73, DOI: 10.9790/2834-09146973. <https://doi.org/10.9790/2834-09146973>
- Es-sabry, M., El Akkad, N., Merras, M., Saaidi, A., and Satori, K. 2020. A New Color Image Encryption Algorithm Using Random Number Generation and Linear Functions", Adv. Intell. Sys. Comput., 1076: 581-588. Springer, (2020, April 08), DOI: 10.1007/978-981-15-0947-6_55. https://doi.org/10.1007/978-981-15-0947-6_55
- Faiqa Maqsood, Muhammad Ahmed, Muhammad Mumtaz Ali and Munam Ali Shah, 2017. Cryptography: A Comparative Analysis for Modern Techniques. Int. J. Adv. Comput. Sci. Appl. (IJACSA), DOI: 10.14569/IJACSA.2017.080659. <https://doi.org/10.14569/IJACSA.2017.080659>
- Mustafeez, A. Z.2020. What is the AES algorithm? Retrieved November 20, 2020 from <https://www.educative.io/edpresso/wh-at-is-the-aes-algorithm>

Paavni Gaur. 2021, AES Image Encryption. International J. Res. Appl. Sci. Eng. Technol, (IJRASET), 2321-9653, DOI: 10.22214/ijraset.2021.39542. <https://doi.org/10.22214/ijraset.2021.39542>

Padate, R., and Patel, A. 2015. Image encryption and decryption using AES algorithm. Int. J. Elect. and Comm. Eng. Technol., 23-29.

Pratiksha Shete, Surekha Kohle.2022. Image Encryption using AES Algorithm: Study and Evaluation. Int. J. Res. Appl. Sci, Eng. Technol.(IJRASET), 2321-9653, DOI: 10.22214/ijraset.2022.46619. <https://doi.org/10.22214/ijraset.2022.46619>

Sahoo, A., Mohanty, P., Sethi, P.C2022. ,Image Encryption using RSA Algorithm. Intelligent Systems, Lect. Notes Netw. Syst., vol 431- 641-652. Springer. DOI: 10.1007/978-981-19-0901-6_56. https://doi.org/10.1007/978-981-19-0901-6_56