International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 12 | Dec - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

An Hybrid Encryption Approach to Secure Data

Dr. Ganavi M[1], Naveen G S[2], Nayana H G[3], Pranjali U[4], Nittur Annapa[5]

[1]Associate Professor, Dept. of CS&E, JNNCE, Shivamogga [2] India[1]

VII Semester Students, Dept. of CS&E, JNNCE, Shivamogga [2] India[1]

***

Abstract

the paper explores the role of encryption in ensuring secure data transfer over various communication channels. It discusses different encryption methods, their implementation, and their effectiveness in protecting data from unauthorized access. By Analyzing contemporary techniques and potential vulnerabilities, the paper aims to present a comprehensive overview of encryption as a cornerstone of modern data security. Here's a general outline for a paper on "An Encryption Approach to Achieve Secure Data Transfer." This paper can provide an overview of the methods, benefits, and challenges of encryption techniques in securing data during transmission

Key Words: Advance Encryption standard (AES) algorithm, Hamming code, Image processing, Data security, Encryption, Decryption, python.

1. Introduction

This paper explores the various encryption approaches designed to achieve secure data transfer. It delves into the principles of encryption, examines widely used encryption algorithms, and discusses their implementation in secure communication protocols. Additionally, the study addresses. such as key management and emerging threats, while highlighting innovative advancements, including quantum-safe cryptography and homomorphic encryption. The ultimate goal is to provide insights into how encryption can be effectively employed to safeguard data in an evolving technological landscape Let me know if you need assistance expanding any section Encryption stands as a foundational solution, enabling secure data transfer by converting readable data(image) into an unreadable format (Cipher image), ensuring that only authorized recipients can decipher the information As organizations and individuals increasingly rely on digital communication for personal, professional, and financial interactions.

In today's digital landscape, the exponential growth of data exchange over the internet and various communication networks has heightened the need for secure and reliable data transfer mechanisms. With the increasing volume of sensitive information being transmitted—ranging from personal details and financial transactions to confidential business and military communications—data security has become a critical concern. Unauthorized access, data breaches, and cyberattacks present significant risks, necessitating the development of robust encryption techniques to safeguard data integrity, confidentiality, and availability.

Traditional encryption methods like the Advanced Encryption Standard (AES) have been widely adopted due to their strength in securing data through symmetric key encryption, ensuring that unauthorized parties cannot easily decipher encrypted messages. However, while AES offers a high level of security, it alone may not be sufficient to handle potential
transmission errors that can occur during data transfer, especially in environments where noise, interference, or

system malfunctions may corrupt the data. This presents a dual challenge: how to ensure both the security of the data against unauthorized access and the accuracy of data received after transmission.

To address this dual requirement, a novel encryption approach is proposed that combines the power of the AES algorithm for data security with the Hamming code for error detection and correction. The proposed method aims to secure data transfer by employing AES encryption to protect the data from malicious attacks, while Hamming codes are used to enhance the reliability of the transmission by detecting and correcting any

errors introduced during data transfer. AES is well-known for its efficiency in handling large volumes of data, especially when it comes to securing sensitive information. It operates by transforming plain image into cipher image through multiple rounds of substitution and key expansion processes. The strength of AES lies in its use of a symmetric key that is computationally difficult to break, even for modern cryptographic attacks, making it an ideal choice for ensuring the confidentiality of data.

On the other hand, the Hamming code is a widely used error-correcting code that provides a reliable mechanism for detecting and correcting single-bit errors. By adding redundant bits to the original data, the Hamming code ensures that any corruption during transmission can be detected and, in many cases, corrected without the need for retransmission. This makes the Hamming code particularly useful in environments where data integrity is critical, such as wireless communications, satellite links, and data storage systems.
The integration of AES encryption with Hamming code error correction offers a comprehensive solution

for secure and reliable data transfer. The data is first encrypted using the AES algorithm to ensure confidentiality, and then Hamming code is applied to the encrypted data to add redundancy for error detection and correction. This combined approach not only protects the data from unauthorized access but also ensures that the data integrity is maintained throughout the transmission process.

The motivation for this research stems from the growing need for secure and error-free data transfer methods in a variety of applications, including military communication systems, financial institutions and healthcare systems. These fields often involve the exchange of highly sensitive information that must be both securely encrypted and reliably transmitted without the risk of corruption. By combining AES and Hamming code, the proposed approach addresses both the security and reliability challenges, offering a robust and efficient solution for modern communication networks.

This paper presents a detailed exploration of the proposed encryption approach, discussing its architecture, operation, and potential applications. The performance of the method is evaluated based on key metrics such as encryption strength, error detection and correction capability, and overall transmission efficiency. The results demonstrate that the combined use of AES encryption and Hamming code significantly enhances the security and reliability of data transfer, making it a promising technique for use in various high stakes communication environments.

2. Objectives

The objectives of the project are:

1. Data Encryption with AES: Encrypt the data using the AES algorithm to ensure confidentiality and prevent unauthorized access during transfer.
2. Key Management: Use a secure method for distributing and managing encryption keys to maintain the integrity and confidentiality of the AES encryption process.
3. Error Detection with Hamming Code: Implement Hamming code to detect and correct single-bit errors that may occur during data transmission, ensuring data integrity.
4. To measure the performance metrics such as PSNR, MSE, and SSIM to ensure the quality of the input data.

3. Literature Survey

- Paavni Gaur et.al (2023): AES ensures high security due to the complexity of breaking a 256-bit cipher key. It offers faster encryption and decryption processes, making it ideal for sensitive image data storage and transmission [1].
- Priyanka Sharma et .al (2023): The algorithm generates multiple keys independently at the sender and receiver, reducing the risk of key interception [2].

In AES encryption, plaintext is divided into 128-bit blocks and processed through multiple rounds of substitution, permutation, and key mixing using a symmetric key.
Decryption reverses this process using the same key to recover the original plaintext. It ensures fast and secure data transformation for modern applications.
Hamming code is an error-detection and correction method used to ensure data integrity during transmission. It adds redundant bits to data to detect and correct single-bit errors. While not directly related to encryption, it enhances reliability in secure communication systems.

4. Methodology

The AES algorithm is applied to encrypt and decrypt images using a 256-bit cipher key to enhance security. The process involves studying the application of AES for efficient encryption, followed by system implementation and performance testing with varied image sizes and keys.

The proposed methodology involves the development of a Modified AES (MAES) algorithm for secure image encryption. The process generates a unique key stream using a modified AES Key Expansion technique, enhancing encryption quality and computational efficiency. The encryption is performed using XOR operations and SubByte Transformations on image pixels, while decryption employs reverse operations.

This study uses the AES algorithm to encrypt digital images by converting them into matrices and applying transformations like Sub Bytes, Shift Rows, Mix Columns, and Add Round Key. Metrics such as histogram distribution, entropy, and PSNR assess encryption effectiveness, with MATLAB simulations used for visualization and analysis.

4.1 System Design

The Figure 1 demonstrates the process of securely encrypting and decrypting an image using the AES algorithm. Initially, the sender provides an input image, which is then encrypted with the AES encryption method using a secret key to ensure data security. The encrypted image is transmitted securely to the receiver over a communication channel. At the receiving end, the image is decrypted using the same secret key to restore the original image. To protect the secret key during transmission, it is encoded and decoded using a Hamming code process, which adds an error detection and correction layer for enhanced security. This ensures the secret key remains intact and usable throughout the process. Finally, the decrypted image is reconstructed successfully and delivered to the intended receiver.

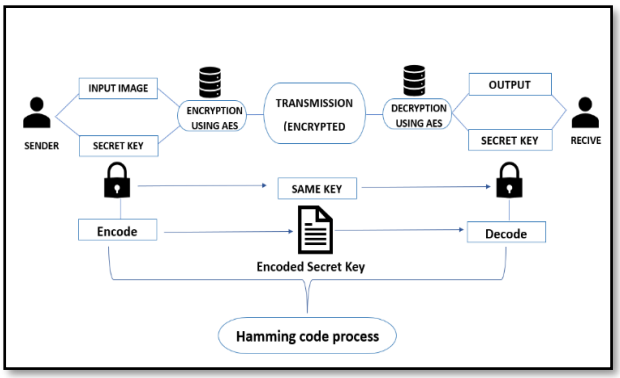
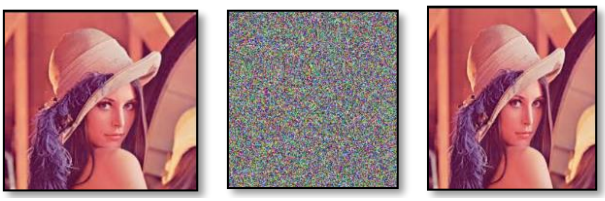


Figure 1: System Architecture

4.2 Result

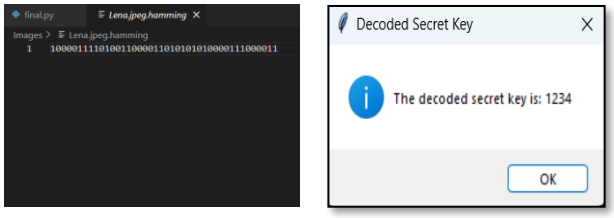
In Figure 2 shows AES (Advanced Encryption Standard) encryption transforms an input image into an encrypted, unreadable format using a secret key and a selected key size (e.g., 128-bit or 256-bit), ensuring data security. The decryption process reverses this, using the same key to restore the original image from the encrypted one.so here (a) shows original input image (b) shows encrypted image and in (c) the image will be decrypted.



(a) **(b)** **(c)**

Figure 2: AES Encryption and Decryption Process

Figure 3 Shows that Hamming code for 128 bits adds parity bits at positions that are powers of 2 (e.g., 1, 2, 4, 8) to detect and correct single-bit errors. These parity bits ensure that the total number of 1s in selected positions is even (for even parity) or odd (for odd parity).



(a) **(b)**

Figure 2: Hamming Encoded and Decoded Process

4.2.3 Evaluation metrices

Table 1: Evaluation metrices after Encryption

INPUT IMAGE	ENTROPY(RED)	ENTROPY (GREEN)	ENTROPY (BLUE)	PSNR (INdB)	MSE	SSIM	TIME TAKEN (SEC)
PEPPER	7.9913	7.99 83	7.99 23	INF	0.0 0	1.0 00	6.13 14
BARBARA	7.9 922	7.99 64	7.99 44	INF	0.0 0	1.0 00	6.36 19
LENE	7.9 965	7.99 43	7.99 11	INF	0.0 0	1.0 00	5.95 63
MANDRILL	7.9 944	7.99 33	7.99 42	INF	0.0 0	1.0 00	5.55 53
TREE	7.9 933	7.99 10	7.99 35	INF	0.0 0	1.0 00	6.55 12

After encryption, the PSNR should be lesser, the entropy values should be near to 8, SSIM should be near to 0 and MSE will be inverse of PSNR. As coming to Decryption process, the PSNR value should be an infinite, SSIM value be 1 and the Entropy of RGB value should be more and the Entropy of RGB should be less. In the both table The time taken for Decryption process should be more compare to Encryption process Obtained results for the proposed method is presented in the tables 1 and 2.

Table 2: Evaluation metrices after Decryption

INPUT IMAGE	ENTROPY(RED)	ENTROPY (GREEN)	ENTROPY (BLUE)	PSNR (INdB)	MSE	SSIM	TIME TAKEN (SEC)
PEPPER	7.9 993	7.9 993	7.9 993	8.1 1	10 04 7.1	0.0 20 7	0.13 14
BARBARA	7.9 992	7.9 994	7.9 994	8.8 5	84 78. 36	0.0 20 9	0.16 19
LENE	7.9 965	7.9 963	7.9 961	8.6 4	89 01. 31	0.0 19 9	0.05 63
MANDRILL	7.9 994	7.9 993	7.9 992	8.8 4	85 01. 80	0.0 19 6	0.15 53
TREE	7.9 973	7.9 970	7.9 975	8.1 6	99 22. 34	0.0 16 9	0.05 12

5. Conclusion

The encryption method using AES and Hamming Code provides strong data security with added error correction. AES ensures data is encrypted securely, while Hamming Code improves transmission reliability. The quality of the encrypted data is assessed using PSNR, MSE, and SSIM. High PSNR and SSIM values indicate minimal data loss, and low MSE shows fewer errors. The results confirm that this approach offers both security and data integrity, making it a reliable solution for secure data transfer.

References

[1] Paavni Gaur, "AES image encryption", Pune University, Information Technology, Maharaja Agrasen Institute of Technology, vol 7, pp.no.2-4, Dec 21, 2023.

[2] Priyanka Sharma, "A New Image Encryption using Modified AES Algorithm and its Comparison with AES", Delhi university, Guru Gobind Singh Indraprastha University, Vol. 9, pp.no. 1-6, Aug-18, 2021,

[3] Ahmad A. Al Rababah, "Digital Image Encryption Implementations Based on AES Algorithm", King Abdulaziz University, vol13, pp.no. 1-9, June 2023

[4] Priya Deshmukh "An image encryption and decryption using AES algorithm", International journal of scientific and Engineering Research, vol7, pp.no. 1-4, Feb-2021

[5]Musa Kayode Yahaya and Aminat showole Ajibola , "Cryptosystem for secure Data Transmission using Advance Encryption standard and Steganography", International Journal of Scientific Research in Computer Science ,Engineering and Information Technology, vol5, pp.no.1-7, Jan-2024.

[6] Deeksha.et.al.," Image Encryption /Decryption using AES Algorithm for Hardware Acceleration Design and Implementation", IOSR Journal of VLSI Signal Processing, vol10, pp.no.08-19, Aug-2020.