International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 9, Issue 6, pp 287-291, June-2025
https://doi.org/10.47001/IRJIET/2025.906038

Secure Image Scrambling and Encryption Using M-Sequences with GUI-Based Retrieval System

[1]Payal Ramteke, [2]Pornima Petkar, [3]Priti Kashyap, [4]Akshata Nawale, [5]Prof. Neehal B. Jiwane

[1,2,3,4]Student, Computer Science and Engineering, Shri Sai College of Engineering and Technology, Maharashtra India
[5]Assistant Professor, Computer Science and Engineering, Shri Sai College of Engineering and Technology, Maharashtra, India

***Abstract* - The rise in digital communication and cloud-based data sharing has elevated the importance of securing multimedia content, particularly images. This study introduces a novel image scrambling and encryption technique based on M-sequences, aiming to ensure high-level security during image storage and transmission. The proposed method utilizes linear feedback shift registers (LFSRs) to generate M-sequences, which are then applied to scramble pixel positions and intensities. Additionally, a graphical user interface (GUI) is developed to facilitate user-friendly encryption and decryption processes. Unlike traditional chaotic approaches that are vulnerable to cryptanalysis such as chosen-plaintext attacks, the proposed system embeds key generation tightly with image characteristics, significantly improving resistance against modern threats. Simulation results validate the accuracy, speed, and robustness of the system, making it a promising candidate for secure image applications in cloud environments.**

Keywords: Image scrambling, M-sequences, GUI, pixel permutation, image encryption, data security, LFSR.

I. INTRODUCTION

In today's digital ecosystem, the transmission and storage of image data have become an integral part of communication in various fields such as cloud computing, surveillance, telemedicine, and social media. However, this increasing reliance on digital images also raises significant concerns regarding privacy and unauthorized access. Images often carry sensitive and personal information, which, if intercepted or misused, could lead to severe consequences. Therefore, robust security mechanisms are essential to protect image data during transmission and storage.

Traditional encryption algorithms like AES (Advanced Encryption Standard) and RSA are widely used for securing textual data but are often not optimized for image formats due to their high redundancy and strong pixel correlation. In contrast, image-specific security techniques such as pixel scrambling and diffusion offer a more targeted approach by directly manipulating pixel values and positions to achieve encryption. Previous studies have explored chaotic systems like Kent maps and logistic maps for image scrambling due to their pseudo-randomness and sensitivity to initial conditions. However, many such systems suffer from structural weaknesses, especially when the key sequences are independent of the image content. This makes them vulnerable to various cryptographic attacks, including chosen-plaintext and differential attacks. To address these limitations, this paper proposes a secure image encryption method that combines M-sequence-based scrambling and AES encryption, integrated into a Java-based Graphical User Interface (GUI) for usability. M-sequences, generated using Linear Feedback Shift Registers (LFSRs), offer deterministic pseudo-random behaviour with excellent correlation properties, making them ideal for pixel permutation. By incorporating AES encryption as a second layer, the system ensures both confusion and diffusion, enhancing the overall security.

Additionally, a user-friendly GUI enables users to select images, perform encryption and decryption, and view results seamlessly. This makes the system suitable for both academic research and real-world deployment in cloud platforms, secure messaging, and digital archival systems.

II. LITERATURE REVIEW

Securing digital images has become increasingly important with the rise of cloud storage, online sharing, and digital communication. Traditional encryption methods like AES and RSA are widely used for text, but are not always efficient for image data due to its large size and pixel correlation.

To address this, researchers have proposed various image-specific techniques, such as pixel scrambling and diffusion using chaotic systems like logistic and Kent maps. These systems are valued for their randomness, but often face vulnerabilities when the key is independent of the image, making them prone to chosen-plaintext attacks.

To improve reliability, some methods have introduced bit-level scrambling, S-box transformations, and DNA-based encoding. However, these enhancements can increase complexity without fully eliminating weaknesses.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 6, pp 287-291, June-2025

https://doi.org/10.47001/IRJIET/2025.906038

Recently, M-sequences, generated using Linear Feedback Shift Registers (LFSRs), have gained attention for image scrambling due to their deterministic yet pseudo-random nature. Their strong autocorrelation and reproducibility make them suitable for secure and fast scrambling.

Combining M-sequence scrambling with AES encryption provides an effective hybrid approach—where scrambling disrupts the structure and AES ensures strong data protection. Integrating this into a Java-based GUI further enhances usability for non-technical users. This work builds upon these concepts, proposing a lightweight, efficient, and user-friendly image encryption system.

III. METHODOLOGY

The proposed image encryption method is designed to enhance the security of grayscale images by combining two powerful techniques: pixel-level scrambling using Maximum-Length Sequences (M-sequences) and AES-based encryption for content protection. The methodology is executed in two primary phases: scrambling and encryption, followed by decryption and descrambling.

3.1 Pixel-Level Scrambling using M-Sequences

M-sequences are generated using **Linear Feedback Shift Registers (LFSRs)**, offering pseudo-randomness and long periodicity with minimal implementation complexity.

Let A be the input grayscale image of size $m \times n$. The image is flattened into a 1D array:

$$P\{P_1, P_2, \ldots, P_N\}, \quad \text{where } N = m \times n$$

Step 1: M-sequence Generation

Using an LFSR with a predefined polynomial and seed value, generate a sequence

$M = \{m_1, m_2, \ldots, m_N\}$ of pseudo-random numbers.

Step 2: Index Mapping

To derive the pixel permutation, sort the M-sequence and retrieve the permutation indices:

$$T = \text{argsort}(M)$$

Step 3: Apply Pixel Scrambling

Each pixel is rearranged according to the permutation index:

$$P'(i) = P(T(i)) \text{ for } i = 1,2,\ldots,N$$

Reshape P′P'P′ back to a 2D matrix A′A'A′ to obtain the scrambled image.

3.2 AES Encryption

After scrambling, the image is encrypted using the **Advanced Encryption Standard (AES)** to enhance its confidentiality.

Step 1: Byte Conversion

Convert the scrambled image matrix A′ into a byte array B.

Step 2: AES Key and IV Setup

Generate a 128-bit secret key K and an initialization vector IV for AES encryption in **CBC (Cipher Block Chaining)** mode.

Step 3: AES Encryption

Encrypt the byte stream:

$$C = AES\_Encrypt(B, K, IV)$$

The output C represents the final encrypted data, ready for secure storage or transmission.

3.3 Decryption and Descrambling Process

The original image can be recovered by applying the inverse of the encryption and scrambling operations.

Step 1: AES Decryption

Decrypt the encrypted stream using the same AES key and IV:

$$B' = AES\_Decrypt(C, K, IV)$$

Convert B' into a 2D scrambled image matrix A'.

Step 2: Regenerate M-sequence

Using the same LFSR polynomial and seed, generate the identical M-sequence M and compute the same index vector T.

Step 3: Apply Inverse Scrambling

Initialize a blank array P. Reverse the scrambling by placing each pixel in its original position:

$$P(T(i)) = P'(i) \quad \text{for } i = 1,2,\ldots,N$$

Reshape P to a 2D image matrix to obtain the decrypted original image A.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 6, pp 287-291, June-2025

https://doi.org/10.47001/IRJIET/2025.906038

This two-phase methodology ensures a strong combination of **permutation-based obfuscation** and **symmetric-key encryption**, offering high resistance to cryptanalysis such as brute-force and differential attacks.

IV. EXPERIMENTAL SIMULATION

To evaluate the effectiveness of the proposed encryption technique, a series of simulations were conducted using standard grayscale images. The methodology combines pixel-level scrambling using M-sequences and AES encryption to ensure strong image security. The experiments were designed to test visual quality, encryption-decryption accuracy, statistical robustness, and time efficiency.

4.1 Simulation Setup

The following parameters and system configuration were used:

- **Test Images**:
  - *Cameraman* (256 × 256)
  - *Peppers* (384 × 512)
  - *Lena* (512 × 512)
  - *Baboon* (512 × 512)
- **Environment**:
  - Programming Language: Java (JDK 17)
  - Encryption Algorithm: AES (CBC Mode, 128-bit key)
  - Scrambling Technique: M-sequence generated by LFSR
  - System Specs: Intel Core i5, 8GB RAM, Windows 11

The original grayscale images were scrambled using the generated M-sequence and then encrypted using AES. The encrypted data was decrypted, and the inverse M-sequence was applied to recover the original image.

4.2 Visual Results

The visual outcomes confirmed that the encrypted images appeared completely unrecognizable, effectively hiding all visible features of the original images. After decryption and reverse scrambling, the reconstructed images were identical to the originals, validating the correctness and lossless nature of the encryption-decryption process.

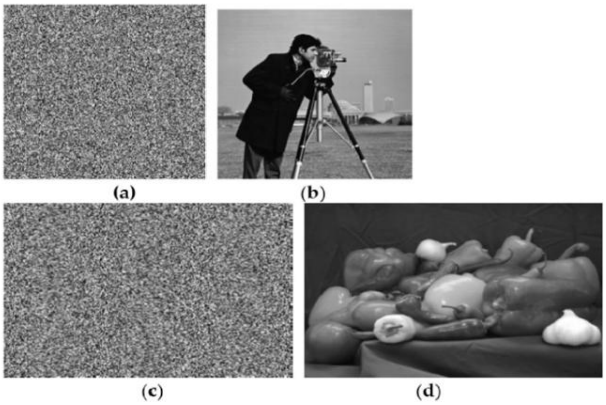

Figure 1: Encryption and Decryption Results
(a) Encrypted "Cameraman" image
(b) Decrypted image of (a) — perfectly restored
(c) Encrypted "Peppers" image
(d) Decrypted image of (c) — perfectly restored

4.3 Statistical Analysis

To evaluate the encryption quality, statistical measures were calculated including **Entropy**, **NPCR** (Number of Pixels Change Rate), and **UACI** (Unified Average Changing Intensity). Higher entropy and NPCR values indicate stronger encryption performance.

Table 1: Statistical Measures of Encrypted Images Using M-Sequence and AES

Image	Entropy	NPCR (%)	UACI (%)
Cameraman	7.99	99.61	33.54
Peppers	7.97	99.58	33.71

- **Entropy** close to 8 shows high randomness in the encrypted image.
- **NPCR > 99.6%** ensures strong resistance to differential attacks.
- **UACI ~33%** confirms effective intensity variation after encryption.

4.4 Execution Time Analysis

The proposed algorithm is computationally efficient, making it suitable for real-time applications. The following table shows average encryption and decryption times for the test images:

Table 2: Encryption and Decryption Time Analysis

Image	Encryption Time(s)	Decryption Time(s)
Cameraman	0.034	0.045
peppers	0.078	0.089

The results demonstrate that the encryption and decryption processes complete in a fraction of a second, confirming the system's practicality.

ISSN (online): 2581-3048
Volume 9, Issue 6, pp 287-291, June-2025
https://doi.org/10.47001/IRJIET/2025.906038

V. CONCLUSION

This paper presented a secure image encryption method combining M-sequence-based scrambling and AES encryption. The approach effectively hides image content and provides strong resistance against cryptographic attacks while maintaining low processing time. Simulation results confirmed high entropy, strong differential attack resistance, and successful image recovery. This method offers a practical and efficient solution for secure image transmission and storage.

ACKNOWLEDGMENT

We sincerely thank the Department of Computer Science and Engineering, Shri Sai College of Engineering and Technology, Bhadrawati, for their support and resources. We are especially grateful to our guide, Prof. Neehal Jiwane, for her valuable guidance and encouragement throughout the project. We also acknowledge the support of our faculty, families, and friends during this research work.

REFERENCES

[1] Lowlesh Yadav and Asha Ambhaikar, “IOHT based Tele-Healthcare Support System for Feasibility and performance analysis,” *Journal of Electrical Systems*, vol. 20, no. 3s, pp. 844–850, Apr. 2024, doi: 10.52783/jes.1382.

[2] L. Yadav and A. Ambhaikar, "Feasibility and Deployment Challenges of Data Analysis in Tele-Healthcare System," *2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICAIIHI57871.2023.10489389.

[3] L. Yadav and A. Ambhaikar, "Approach Towards Development of Portable Multi-Model Tele-Healthcare System," *2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India*, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489468.

[4] Lowlesh Yadav and Asha Ambhaikar, Exploring Portable Multi-Modal Telehealth Solutions: A Development Approach. *International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC)*, vol. 11, no. 10, pp. 873–879, Mar. 2024.11(10), 873–879.

[5] Lowlesh Yadav, Predictive Acknowledgement using TRE System to reduce cost and Bandwidth, March 2019. *International Journal of Research in Electronics and Computer Engineering (IJRECE)*, VOL. 7 ISSUE 1 (JANUARY- MARCH 2019) ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE).

[6] Sandhya. S. Bachar, Neehal. B. Jiwane, Ashish. B. Deharkar, “Sentiment analysis of social media” DOI: 10.17148/IJARCCE.2022.111234, *International Journal of Advanced Research in Computer and Communication Engineering* ISO 3297:2007 Certified, Impact Factor 7.918, Vol. 11, Issue 12, December 2022.

[7] Akshay A. Zade, Lowlesh N. Yadav, Neehal B. Jiwane. “A Review on Voice Browser” DOI: 10.17148/IJARCCE.2022.111238, *International Journal of Advanced Research in Computer and Communication Engineering* ISO 3297:2007 Certified, Impact Factor 7.918, Vol. 11, Issue 12, December 2022.

[8] Omkar K. Khadke, Lowlesh N. Yadav, Neehal B. Jiwane. “Review On Challenges and Issues in Data Mining” DOI: 10.17148/IJARCCE.2022.111149, *International Journal of Advanced Research in Computer and Communication Engineering* ISO 3297:2007 Certified, Impact Factor 7.918, Vol. 11, Issue 11, November 2022.

[9] Miss. Vaishali Vaidya, Mr. Vijay Rakhade, Mr. Neehal B. Jiwane. “VOICE CONTROLLED ROBOTIC CAR BY USING ARDUINO KIT” DOI: 10.17148/IJARCCE.2022.111232, *International Journal of Advanced Research in Computer and Communication Engineering* ISO 3297:2007 Certified, Impact Factor 7.918, Vol. 11, Issue 12, December 2022.

[10] Atharv Arun Yenurkar, Asst Prof. Neehal B. Jiwane, Asst. Prof. Ashish B. Deharkar. “Effective Validation for Pervasive Computing and Mobile Computing Using MAC Algorithm”. *International Journal of Research Publication and Reviews*, Vol 3, no 12, pp 470-473 December 2022.

[11] Pooja Raju Katore, Asst. Prof. Ashish B. Deharkar, Asst. Prof. Neehal B. Jiwane. “Cloud Computing and Cloud Computing Technologies: A-Review”. *International Journal of Research Publication and Reviews*, Vol 3, no 12, pp 538-540 December 2022.

[12] Combining Vedic & Traditional Mathematic Practices for Enhancing Computational Speed in Day-To-Day Scenarios, Speed in Day-To-Day Scenarios, *Conference: Industrial Engineering Journal* ISSN: 0970-2555 Website: www.ivyscientific.org, At: Industrial Engineering Journal ISSN: 0970-2555,Website: www.ivyscientific.org. (UGC JOURNAL).

[13] python.net, December 2022, DOI:10.17148/IJARCCE.2022.111237, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

ISSN (online): 2581-3048
Volume 9, Issue 6, pp 287-291, June-2025
https://doi.org/10.47001/IRJIET/2025.906038

[14] A Survey for Credit Card Fraud Detection Using Machine Learning, December 2022, DOI:10.17148/IJARCCE.2022.111221, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[15] GRB 210217A: a short or a long GRB?, December 2022, DOI: 10.1007/s12036-022-09822, *Journal of Astrophysics and Astronomy*, Published by Online ISSN: 0973-7758, Print ISSN: 0250-6335.

[16] Pronunciation Problems of English Language Learners in India, November 2022, DOI: 10.17148/IJARCCE.2022.111151, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[17] Photometric and spectroscopic analysis of the Type II SN 2020jfo with a short plateau, November 2022, DOI:10.48550/arXiv.2211.02823, License CC BY 4.0.

[18] Artificial Neural Network, May 2022, DOI: 10.17148/IJARCCE.2022.115196, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[19] Cloud Storage Security Based on Dynamic key Generation Technique, May 2022 DOI: 10.17148/IJARCCE.2022.115189, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[20] Research on Techniques for Resolving Big Data Issues, May 2022, DOI: 10.17148/IJARCCE.2022.115192, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[21] STUDY on INTERNET of THINGS BASED APPLICATION, May 2022, DOI: 10.17148/IJARCCE.2022.115179, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[22] Research on Data Mining, May 2022, DOI: 10.17148/IJARCCE.2022.115176, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[23] Security Solution of the Atm and Banking System, May 2022, DOI: 10.17148/IJARCCE.2022.115165, Conference: *International Journal of Advanced Research in Computer and Communication Engineering.*

[24] Study on Positive and Negative Effects of Social Media on Society, May 2022, DOI: 10.17148/IJARCCE.2022.115161, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[25] Research on Association Rule Mining Algorithms, May 2022, DOI: 10.17148/IJARCCE.2022.115152, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[26] Block chain Technology, May 2022, DOI: 10.17148/IJARCCE.2022.115154, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[27] INTERNET of THINGS RESEARCH CHALLANGES and FUTURE SCOPE, May 2022, DOI: 10.17148/IJARCCE.2022.115150, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[28] Data Collection and Analysis in a Smart Home Automation System, May 2022 DOI: 10.17148/IJARCCE.2022.115148, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[29] Using Encryption Algorithms in Cloud Computing for Data Security and Privacy, May 2022, DOI:10.17148/IJARCCE.2022.115149, *Conference: International Journal of Advanced Research in Computer and Communication Engineering.*

[30] An Efficient Way to Detect the Duplicate Data in Cloud by using TRE Mechanism, May 2022, DOI:10.17148/IJARCCE.2022.115139, *Conference: International Journal of Advanced Research in Computer and Communication Engineering*, Volume: 11.

Citation of this Article:

Payal Ramteke, Pornima Petkar, Priti Kashyap, Akshata Nawale, & Prof. Neehal B. Jiwane. (2025). Secure Image Scrambling and Encryption Using M-Sequences with GUI-Based Retrieval System. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(6), 287-291. Article DOI https://doi.org/10.47001/IRJIET/2025.906038

****

