Cureus Journal of Computer Science

Open Access Original Article

Encryption of Image Using Linear Feedback Shift Register and Pixel Shuffling

Dipankar Maity [1] , Aparna Prayashi [1] , Ashish K. Panda [1] , Satyajit Panigrahi [1]

1. Computer Science and Information Technology, Siksha 'O' Anusandhan, ITER, Bhubaneswar, IND

Corresponding authors: Dipankar Maity, dipankarmaity@soa.ac.in, Aparna Prayashi, aparnaprayashi303@gmail.com, Ashish K. Panda, ashishpanda2909@gmail.com, Satyajit Panigrahi, satyajitpanigrahi9480@gmail.com

Abstract

In today's digital age, securing visual data is imperative to safeguard privacy and prevent unauthorized access. This study introduces a robust image encryption method combining Pixel Shuffling and Linear Feedback Shift Register Key Stream with Advanced Encryption Standard-based S-box transformations. The encryption process incorporates confusion through pixel shuffling and diffusion via S-box-based exclusive OR operations, ensuring high resistance to cryptographic attacks. The method demonstrates superior performance through evaluation metrics such as normalized pixel change rate and entropy, achieving 99.71% pixel randomness and near-optimal entropy values. The proposed approach is particularly relevant for applications in medical imaging, secure communication, and confidential data storage, providing a practical solution to contemporary challenges in image security. These findings underscore the method's effectiveness and scalability, making it a promising contribution to image encryption.

Categories: Algorithm Analysis, Security and Privacy, Cryptographic Algorithms
Keywords: aes, encryption, integrity, key generation, linear feedback, shift register, s-box, shuffling pixels, unauthorized access

Introduction

In the era of rapid digital transformation, images play a pivotal role in communication, information sharing, and storage across various domains, including personal interactions, healthcare, and secure communication systems. However, this reliance on digital images has heightened the need to safeguard them from unauthorized access, tampering, and interception. The exponential growth of digital platforms has made image encryption a crucial tool for ensuring the confidentiality and integrity of visual data [1,2].

The challenges associated with encrypting images differ significantly from those of textual data. Images are characterized by large file sizes and intricate pixel patterns, making them less suited to traditional encryption methods like the Advanced Encryption Standard (AES) and Hill cipher, originally designed for text-based data [3]. This discrepancy has prompted researchers to explore specialized encryption techniques tailored to the unique demands of visual data protection.

Among these, Linear Feedback Shift Registers (LFSRs) have emerged as a promising solution for image encryption. LFSRs are known for their simplicity, efficiency, and ability to generate highly random sequences, which can effectively obscure image pixel arrangements. These properties make them well-suited for achieving confusion and diffusion, the two fundamental principles of secure encryption [4].

The motivation to investigate LFSR-based encryption stems from two key factors. First, the rising importance of data privacy in a digitally interconnected world underscores the urgency of safeguarding sensitive visual information [5,6]. Second, the limitations of conventional cryptographic approaches highlight the need for alternative strategies. LFSR-based encryption offers a streamlined approach to handling the complex pixel arrangements of images, ensuring robust security while maintaining computational efficiency.

This study introduces a novel image encryption method that leverages LFSRs for pixel shuffling and incorporates AES S-box transformations to enhance pixel substitution and diffusion. By combining these techniques, the proposed method achieves higher security and resilience against cryptographic attacks.

Materials And Methods

The literature surrounding image encryption techniques reveals a diverse array of approaches aimed at bolstering the security of visual data in digital environments. For instance, Acharya et al. introduced an advanced Hill cipher algorithm utilizing an involuntary key matrix, while Kamali et al. proposed modifications to the AES algorithm to enhance image encryption security [1,2]. Additionally, Shah et al. scrutinized prevailing S-boxes to assess their suitability for image encryption applications, highlighting

the ongoing efforts to refine and optimize existing cryptographic techniques [3]. Researchers have explored various methodologies, each with its own strengths and applications [7-9]. Among the existing methods, LFSR-based image encryption has garnered significant attention [10-13].

However, while LFSR-based encryption offers simplicity and efficiency, security concerns persist [14,15]. Traditional LFSRs are susceptible to cryptanalysis attacks, necessitating the implementation of additional security measures. Moreover, the performance of LFSR-based encryption hinges on a delicate balance between security and computational overhead [16]. Future research endeavors may explore novel cryptographic primitives and employ machine learning techniques to enhance the robustness of LFSR-based encryption against sophisticated adversaries. By addressing security vulnerabilities and optimizing performance, researchers can advance the efficacy and reliability of image encryption methods in safeguarding sensitive visual data [4,8,16].

Among the existing methods, LFSR-based image encryption has garnered significant attention [10,11]. Encrypting data is a fundamental method for safeguarding crucial information, whether it pertains to text, images, or other types of data [17-19]. Feng et al. developed an algorithm combining chaotic LFSR with a hyper-chaotic system to effectively obscure image data, showcasing the potential of LFSR-based encryption in thwarting unauthorized decryption attempts [20]. Furthermore, hybrid approaches, such as Dey et al.'s integration of chaotic maps with LFSR, have demonstrated improved resistance to attacks compared to traditional methods [21]. These studies underscore the importance of leveraging diverse cryptographic primitives to fortify image encryption against evolving threats.

Proposed encryption method

We introduce a novel approach for encrypting black and white images utilizing LFSRs to generate random numbers, which are then employed to rearrange the positions of image pixels and finally followed by XORing (exclusive-OR) the pixel values with the key values generated from S-Box.

The main steps involved in our proposed encryption method are as follows:

1. Input image

2. Giving initial seed value to LFSR: LFSR relies heavily on the seed value to produce a pseudo-random sequence. The seed determines the starting state of the LFSR and ensures that the sequence generated is deterministic.

3. Generating a random sequence using LFSR: The LFSR generates a binary sequence by iteratively shifting the register and applying a feedback function (typically XOR).

4. Shuffling the image pixels row wise using the generated sequence: In this step, the random sequence generated by the LFSR is used to determine a new order for rearranging the pixels in each row of the image.

5. Transposing the image and shuffling the image pixels column wise using the same sequence: After shuffling rows, the image is transposed (rows become columns), and the same LFSR sequence is used to shuffle the pixels column-wise.

6. Generating an S-Box

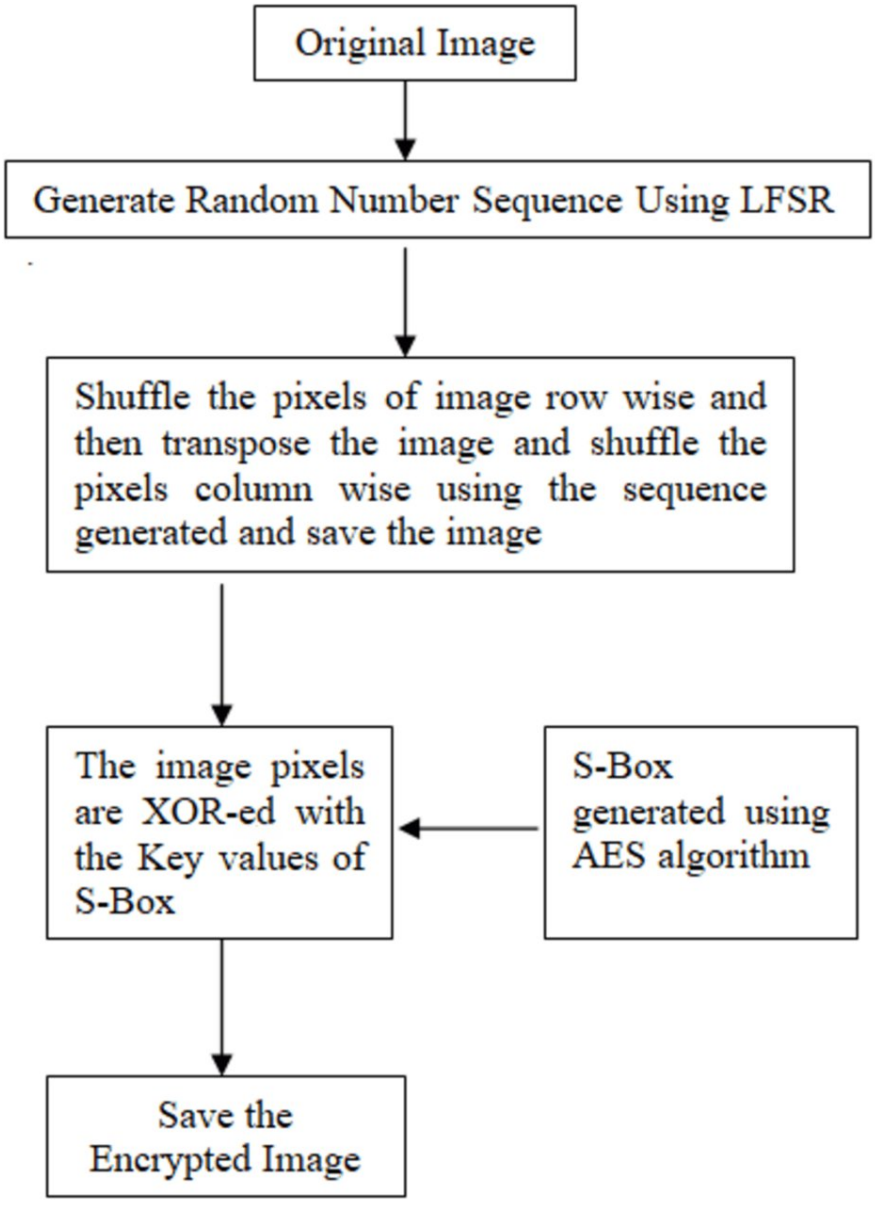

FIGURE 1: S-Box

LFSR, Linear Feedback Shift Register; AES, Advanced Encryption Standard; XOR, Exclusive OR

Figure *1* illustrates the steps involved in our image encryption process, showcasing the pixel shuffling, XOR operation, and use of the S-Box.

7. Applying XOR among the image pixels with key values of S-Box.

Generate the S-Box: An S-Box (Substitution Box) is a pre-defined, non-linear transformation table commonly used in cryptography (e.g., AES). It substitutes each input byte with a corresponding output byte.

In this encryption method, the S-Box values act as the key.

Perform XOR: Each pixel value in the shuffled image is XORed with the corresponding key value obtained from the S-Box.

Let P(i,j) represent the pixel value at position (i,j) in the image, and K(i,j) represent the corresponding key value from the S-Box.

The XOR operation is given by E(i,j) = P(i,j)⊕K(i,j) is the encrypted pixel value.

8. Save the encrypted image.

Our proposed method was implemented on some images successfully.

Example:

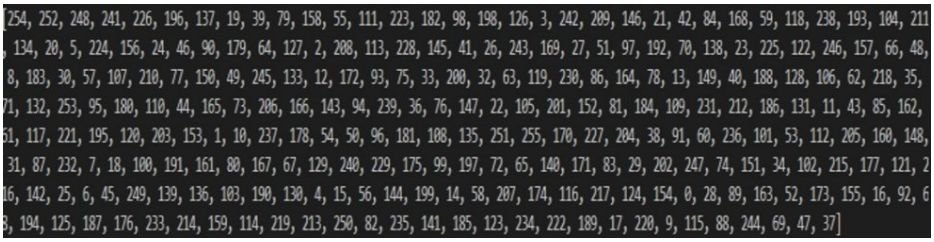

FIGURE 2: LFSR Sequence

LFSR, Linear Feedback Shift Register

Figure *2* shows the generated sequence that was produced using LFSR, a type of shift register that utilizes linear feedback. Comprising interconnected flip-flops with feedback loops employing XOR gates, LFSRs are pivotal in digital circuitry. Their applications range from generating pseudo-random numbers to implementing error detection and correction algorithms, owing to their simplicity, efficiency, and predictable behavior.

Results

This section outlines the outcomes derived from the encryption experiments. It begins with a different analysis of the encrypted image characteristics, followed by detailed evaluations and performance metrics.

Results overview of analysis approach

The results presented here assess the performance and security of the encryption algorithm through multiple analytical techniques. The evaluation process includes statistical analysis and sensitivity measurements to highlight the effectiveness of the proposed encryption scheme.

The detailed histogram analysis of the original, shuffled, and encrypted images is presented in Figure *3*.

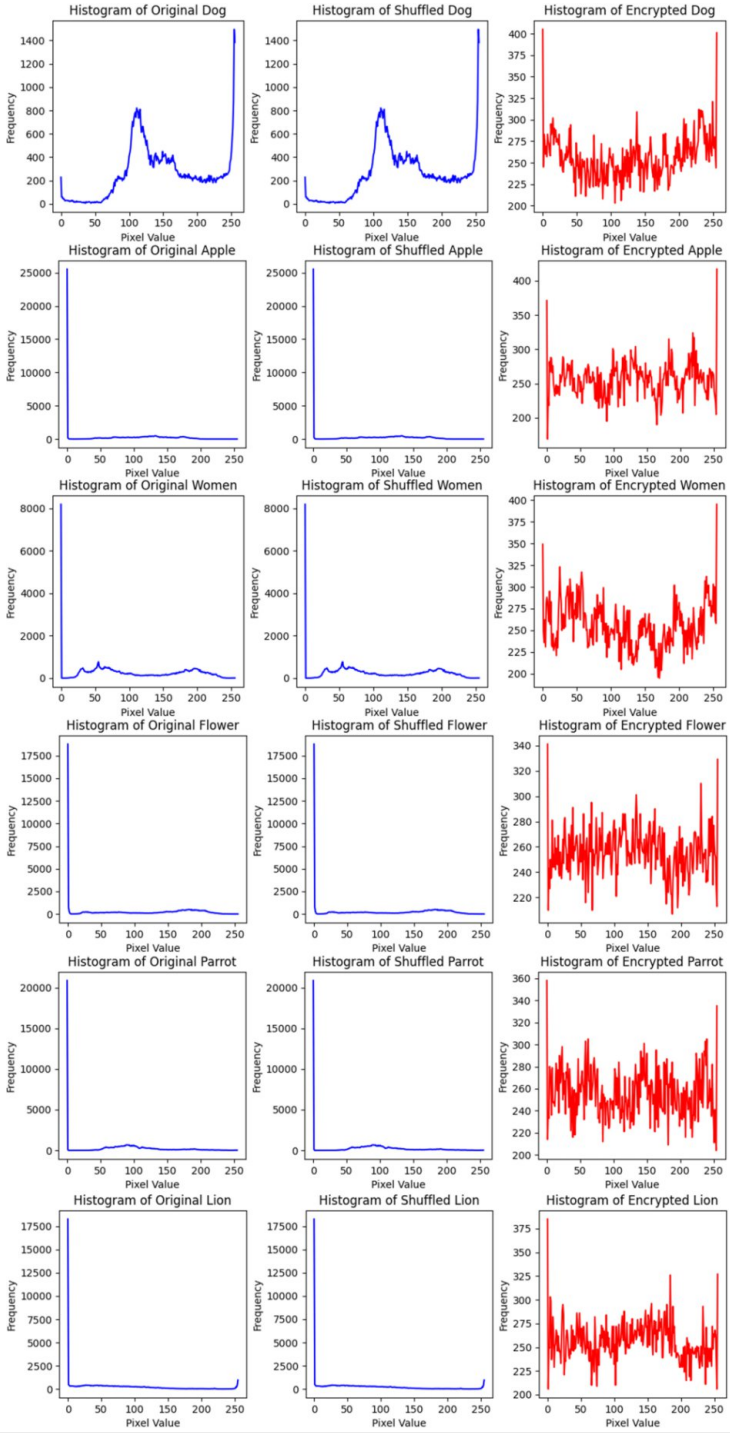

FIGURE 3: Histogram Analysis

In the analysis of the encrypted data, a histogram was employed to assess the distribution of pixel intensities. This Figure *3* histogram analysis provides valuable insights into the characteristics of the encrypted image, such as contrast, brightness, and overall visual appearance. By examining the distribution of pixel values, patterns and anomalies within the encrypted data can be identified, aiding in the evaluation and optimization of the encryption algorithm for enhanced security and performance.

FIGURE 4: Shuffled Image vs. Encrypted Image

The image dataset used in the experiments is publicly available on a GitHub repository. The repository provides access to the images utilized for encryption analysis.

In the encryption process, an S-box transformation is applied to each pixel of the plaintext image. This S-box output is then XORed with a shuffled version of the plaintext image to generate the encrypted image. This technique enhances the security of the encryption scheme by introducing both substitution and diffusion properties, where substitution is achieved using AES-based S-box transformations, ensuring non-linearity, and diffusion is implemented through pixel shuffling to disrupt spatial correlations. The shuffled image adds a layer of confusion by randomly rearranging pixel positions, disrupting the spatial correlation between neighboring pixels and making it difficult for attackers to reconstruct the original structure. Meanwhile, the S-box transformation ensures non-linearity and further obscures the relationship between the plaintext and ciphertext. As shown in Figure *4*, the resulting encrypted image

demonstrates robustness against various cryptographic attacks, making it suitable for secure communication and data protection applications.

A higher Number of Pixel Change Rate (NPCR) indicates greater sensitivity to plaintext changes, meaning even small modifications in the plaintext lead to significant differences in the ciphertext. The NPCR value is calculated using the following equation:

$$NPCR = \left(\frac{\sum_{i,j} Z(i,j)}{H \times W} \right) \times 100\%$$

In this equation, $Z(i,j)$ is a binary matrix indicating pixel changes between two encrypted images, H is the image height, and W is the image width.

ORIGINAL IMAGES	SHUFFLED NPCR	ENCRYPTED NPCR
DOG	99.307251	99.613952
APPLE	99.589539	99.589538
WOMEN	99.710083	99.632263
FLOWER	99.459655	99.562072
PARROT	99.538574	99.543762
LION	98.879272	99.565124

TABLE 1: NPCR Values

NPCR, Number of Pixel Change Rate

The image encryption algorithm was evaluated using the NPCR (Normalized Pixel Change Rate) metric, which measures the percentage of pixel change between two ciphered images resulting from altering a single pixel in the plaintext image. A higher NPCR value indicates greater sensitivity to changes, enhancing the algorithm's security and resilience against attacks. Table *1* shows the resulted NPCR value for both shuffled and encrypted image.

Entropy, $H(I) = -\sum_{i=0}^{255} p(i) \log_2(p(i))$

where $p(i)$ represents the probability of pixel intensity 'i' in the image.

IMAGE	ORIGINAL ENTROPY	SHUFFLED ENTROPY	ENCRYPTED ENTROPY
DOG	7.470718	7.470718	7.992378
APPLE	5.427913	5.427913	7.99442
WOMEN	7.208253	7.208253	7.992104
FLOWER	6.276976	6.276976	7.996087
PARROT	5.866003	5.866003	7.99465
LION	6.274523	6.274523	7.995271

TABLE 2: Entropy Values

The encryption process was assessed for its entropy value, a measure of randomness or unpredictability in the encrypted data. A higher entropy value signifies greater randomness, which is desirable for ensuring the security and robustness of the encryption algorithm against statistical attacks and information leakage. Table *2* shows the entropy value for all types of images.

Comparative analysis

METHOD	NPCR (%)	ENTROPY
Proposed Method	99.6322	7.996
Kamali et al. [2]		7.9989
Shah et al. [3]		7.9325
Okunbor [4]	99.68	
Allawi et al. [11]	99.69	7.99
Ihsan and Doğan [12]	99.6972	7.9995

TABLE 3: Results of the Proposed Algorithm and Other Encryption Algorithms

NPCR, Number of Pixel Change Rate

To evaluate the effectiveness of the proposed method, a comparative analysis with state-of-the-art image encryption techniques was conducted. Table *3* summarizes the performance of these methods in terms of NPCR and entropy.

Experimental setup

The experiments were conducted using a publicly available image dataset hosted on a GitHub repository [22]. The dataset was processed using VS Code on a system with the following specifications:

Processor: Intel Core i3,11th Gen Intel(R) Core(TM) i3-1115G4 @ 3.00GHz 3.00 GHz

RAM: 8 GB

Operating System: Windows 11

Discussion

The proposed encryption method incorporates both confusion and diffusion mechanisms to achieve robust security.

Histogram analysis

The histogram analysis of the encrypted images (Figure *3*) reveals a uniform distribution of pixel intensities. This uniformity eliminates any discernible patterns that could be exploited in statistical attacks. Compared to the histograms of original images, which exhibit distinct patterns, the encrypted images demonstrate significantly enhanced randomness.

Shuffled image vs. encrypted image

As illustrated in Figure *4*, the shuffled image introduces confusion by disrupting the spatial structure of the plaintext image. This step ensures that the original arrangement of pixels is no longer apparent. The subsequent application of the S-Box and XOR operation further enhances security by adding a diffusion effect. The encrypted image exhibits a complete transformation, ensuring resistance to cryptanalysis.

NPCR and entropy analysis

The high NPCR values (Table *1*) confirm that the encryption process is highly sensitive to changes in the plaintext image, ensuring that even minor modifications result in significant changes to the ciphertext. This property protects against differential attacks. Furthermore, the entropy values (Table *2*) of the encrypted images approach the ideal value of 8, indicating maximum randomness and security.

The combination of confusion and diffusion mechanisms, as supported by the histogram, NPCR, and entropy results, ensures that the proposed method is highly effective for secure image encryption.

Comparison with existing methods

A detailed comparison of the proposed encryption method with existing techniques is provided in Table

3. This analysis highlights the performance improvements in terms of NPCR and entropy achieved by the proposed approach compared to state-of-the-art image encryption algorithms.

The proposed method demonstrates competitive NPCR and entropy values, achieving an NPCR of 99.6322% and an entropy of 7.996, which are indicative of high sensitivity to plaintext changes and strong randomness in the encrypted data.

Conclusions

In summary, the encryption process entails two crucial phases: confusion and diffusion. In the confusion phase, pixel shuffling is executed using an LFSR sequence, introducing randomness and obscuring the image's spatial structure. This shuffling enhances confusion, making it harder for adversaries to discern patterns in the encrypted data. In the diffusion phase, an AES S-box is generated and applied to each pixel of the shuffled image. The resulting output is then XORed with the shuffled image, achieving diffusion by spreading the influence of each plaintext pixel across the entire encrypted image. This combination of confusion and diffusion mechanisms strengthens the security of the encryption scheme, ensuring robust protection against cryptographic attacks and preserving the confidentiality of sensitive information.

Additional Information

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

References

1. Acharya B, Panigrahy SK, Patra SK, Panda G: Image encryption using advanced Hill cipher algorithm. International Journal of Recent Trends in Engineering. 2009, 1:663-667.
2. Kamali SH, Shakerian R, Hedayati M, Rahmani M: A new modified version of Advanced Encryption Standard based algorithm for image encryption. 2010 International Conference on Electronics and Information Engineering. 2010, 1:141-145. 10.1109/ICEIE.2010.5559902
3. Shah T, Hussain I, Gondal MA, Mahmood H: Statistical analysis of S-box in image encryption applications based on majority logic criterion. International Journal of the Physical Sciences. 2011, 6:4110-4127.
4. Okunbor D: Analysis of linear feedback shift registers and chaos-based techniques for image encryption. Journal of Cyber Security Technology. 2024, 1-9. 10.1080/23742917.2024.2338954
5. Jiang M, Yang H: Image encryption using a new hybrid chaotic map and spiral transformation. Entropy. 2023, 25:1516-1516. 10.3390/e25111516
6. Chai X, Yang K, Gan Z: A new chaos-based image encryption algorithm with dynamic key selection mechanisms. Multimedia Tools and Applications. 2017, 76:9907-9927. 10.1007/s11042-016-3585-x
7. Dongare AS, Alvi AS, Tarbani NM: An efficient technique for image encryption and decryption for secured multimedia application. International Research Journal of Engineering and Technology. 2017, 4:3186-3190.
8. Hussain I, Gondal MA: An extended image encryption using chaotic coupled map and S-box transformation. Nonlinear Dynamics. 2014, 76:1355-1363. 10.1007/s11071-013-1214-z
9. Chen W: Optical multiple-image encryption using three-dimensional space. IEEE Photonics Journal. 2016, 8:1-8. 10.1109/jphot.2016.2550322
10. Chen W: Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation. IEEE Photonics Journal. 2016, 8:1-9. 10.1109/jphot.2016.2523245
11. Allawi ST, Mustafa NAA: Image encryption based on combined between linear feedback shift registers and 3D chaotic maps. Indonesian Journal of Electrical Engineering and Computer Science. 2023, 30:1669-1677. 10.11591/ijeecs.v30.i3.pp1669-1677
12. Ihsan A, Doğan N: Improved affine encryption algorithm for color images using LFSR and XOR encryption. Multimedia Tools and Applications. 2022, 82:7621-7637. 10.1007/s11042-022-13727-w
13. Liao X, Lai S, Zhou Q: A novel image encryption algorithm based on self-adaptive wave transmission. Signal Processing. 2010, 90:2714-2722. 10.1016/j.sigpro.2010.03.022
14. Wu Y, Zhou Y, Noonan JP, Agaian S: Design of image cipher using latin squares. Information Sciences. 2014, 264:317-339. 10.1016/j.ins.2013.11.027
15. Xiang T, Wong K-w, Liao X: Selective image encryption using a spatiotemporal chaotic system. Chaos. 2007, 17:023115. 10.1063/1.2728112
16. El Assad S, Farajallah M: A new chaos-based image encryption system. Signal Processing Image Communication. 2016, 41:144-157. 10.1016/j.image.2015.10.004
17. Yang Y-G, Jia X, Sun S-J, Pan Q-X: Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding. Information Sciences. 2014, 277:445-457. 10.1016/j.ins.2014.02.124
18. Al-Husainy MAF: A novel encryption method for image security. International Journal of Security and Its Applications. 2011, 6:1-8.
19. Bhatnagar G, Jonathan Wu QM: Selective image encryption based on pixels of interest and singular value

decomposition. Digital Signal Processing. 2012, 22:648-663. 10.1016/j.dsp.2012.02.005
20. Feng W, He YG, Li HM, Li CL: Cryptanalysis of the integrated chaotic systems based image encryption algorithm. Optik. 2019, 186:449-457. 10.1016/j.ijleo.2018.12.103
21. Dey D, Giri D, Jana B, Maitra T, Mohapatra RN: Linear-feedback shift register-based multi-ant cellular automation and chaotic map-based image encryption. Security and Privacy. 2018, 1:e52. 10.1002/spy2.52
22. Datasets: image_encryption_LFSR . https://github.com/dipankarmaity07/image_encryption_LFSR.git.