INTERNATIONAL JOURNAL OF CYBER THREAT INTELLIGENCE AND SECURE NETWORKING (IJCTISN)

eISSN: 3087-4297

Volume. 03, Issue. 05, pp. 01-07, May 2026

A Comparative Analysis of Image Encryption Techniques Based on Linear Feedback Shift Registers and Chaotic Systems

Dr. Julian R. Cortez
Department of Information Systems, Tokyo Institute of Technology, Tokyo, Japan

Article received: 11/03/2026, Article Accepted: 13/04/2026, Article Published: 01/05/2026

ABSTRACT

Purpose: This study aims to conduct a comparative analysis of image encryption techniques, focusing on the performance and security of systems based on Linear Feedback Shift Registers (LFSRs) against those based on chaotic maps. The research addresses a gap in the literature by systematically evaluating higher-order and combined LFSR designs, and demonstrating their viability as a lightweight and secure alternative for image encryption.

Methods: We implemented and tested several image encryption algorithms, including novel LFSR-based ciphers and established chaos-based systems using logistic, tent, and Henon maps. We evaluated their performance using a suite of security metrics, including statistical analysis (histograms and correlation), and differential attack analysis (NPCR and UACI). The efficiency of each cipher was also assessed through execution time measurements.

Results: The experimental results demonstrate that all tested ciphers, including the novel SCLFSR24, achieved robust security, with NPCR values exceeding 99% and UACI values greater than 40%. This is associated with high sensitivity to pixel changes and strong resistance to differential attacks. The LFSR-based ciphers generated similarly random keystreams and secure encrypted images, performing comparably to the well-known chaos-based methods.

Conclusion: The findings suggest that LFSR-based ciphers offer a compelling and practical alternative for image security. Their lightweight design and strong security performance, comparable to chaotic systems, are particularly well-suited for real-time applications in fields such as healthcare and multimedia communication.

Keywords: Image Encryption, Linear Feedback Shift Register (LFSR), Chaotic Systems, Stream Cipher, NPCR, UACI, Digital Image Security.

INTRODUCTION

Background on Digital Image Security

In our increasingly interconnected world, digital images are more than just pictures—they are a fundamental medium for communication, documentation, and data transfer. From personal photos and multimedia content to sensitive information like medical scans, architectural blueprints, and military reconnaissance data, the security of these images has become a paramount concern [1, 12]. Unlike text-based data, digital images have unique characteristics that make them particularly vulnerable to unauthorized access and manipulation. Their sheer size, high data redundancy, and strong correlation between adjacent pixels pose significant challenges for traditional encryption algorithms [1, 2]. Standard encryption methods, such as the Advanced Encryption Standard (AES), are often inefficient for images because of the time and computational resources required to process large datasets. Furthermore, simply applying these algorithms might not sufficiently disrupt the inherent pixel correlations, leaving the encrypted image susceptible to statistical attacks [2].

To address these vulnerabilities, researchers have increasingly turned to stream ciphers, which encrypt data bit by bit, making them well-suited for the continuous flow of image data. This approach generates a pseudo-random keystream that is combined with the image data (typically via an XOR operation) to produce the encrypted output [10, 12]. Two of the most prominent methods for generating these keystreams are chaos-based

systems and Linear Feedback Shift Registers (LFSRs) [1, 5].

Introduction to Image Encryption Techniques

Chaos-based ciphers leverage the unpredictable, non-linear, and highly sensitive nature of chaotic systems to generate a keystream. A small change in the initial conditions of a chaotic map, such as the logistic, tent, or Henon map, can lead to a drastically different output sequence, making the cipher highly sensitive to the secret key [2, 4]. This property, often referred to as the "butterfly effect," is ideal for creating the confusion and diffusion necessary for robust encryption. A significant body of research exists on the application of various chaotic maps for image encryption, confirming their effectiveness [5].

Linear Feedback Shift Registers (LFSRs), on the other hand, are a foundational component of modern cryptosystems, particularly for generating pseudo-random sequences [9]. An LFSR is a shift register whose input bit is a linear function of its previous states. Their simplicity, high speed, and ease of implementation in hardware and software make them a practical choice for resource-constrained environments [8, 11]. When properly designed with a maximal-length polynomial, an LFSR can produce a long, pseudo-random sequence with excellent statistical properties, which is essential for a secure keystream [7].

Problem Statement and Literature Gaps

While both chaotic maps and LFSRs are well-established for generating secure keystreams, a comprehensive, head-to-head comparison of their performance specifically in the context of image encryption remains a critical area for exploration [1, 5]. Most existing research tends to focus on one method or the other, or on a single, isolated algorithm. There is a notable gap in the literature regarding the performance of more advanced LFSR designs, such as higher-order and combined versions, when pitted against the well-studied chaotic systems [6]. A systematic evaluation is needed to determine if these LFSR-based ciphers can offer a security level comparable to chaotic methods, while also maintaining their inherent advantages in terms of speed and computational lightness. This study aims to fill that gap.

Aims of the Study

The primary objective of this research is to conduct a thorough comparative analysis of selected LFSR-based and chaos-based image encryption algorithms. We seek to demonstrate that LFSR-based ciphers, particularly novel, higher-order designs, are not only viable but also practical and robust alternatives to chaos-based methods. This analysis will focus on key security metrics to provide a definitive comparison, ultimately showcasing the potential of LFSR-based designs for real-time image security, especially in sensitive domains like healthcare and other multimedia systems.

Methods

Detailed Keystream Generator Design

The heart of any stream cipher is its keystream generator, the component responsible for producing a long, pseudo-random binary sequence that is then combined with the plaintext to create the ciphertext [10]. The security of the entire cryptosystem hinges on the statistical properties and unpredictability of this keystream. In this study, we meticulously designed and implemented four distinct keystream generators, each representing a key approach to modern stream cipher design: two based on Linear Feedback Shift Registers (LFSRs) and two based on chaotic maps. The following sub-sections provide a comprehensive, mathematical description of each generator.

LFSR-based Keystream Generators

Linear Feedback Shift Registers are the cornerstone of many hardware-based stream ciphers due to their simplicity, high speed, and efficient implementation [9]. An LFSR is a shift register whose input bit is a linear function of its previous states. The sequence of bits it produces is determined by a feedback polynomial.

A. Fundamental Principles of LFSRs

An LFSR consists of a sequence of memory cells (bits) and a feedback loop. At each clock cycle, the bits in the register shift one position to the right. The new bit entering the leftmost position is a linear combination (specifically, a sum modulo 2, or XOR operation) of the previous states of a subset of the register's cells. These selected cells are known as "taps." The pattern of these taps is defined by a characteristic polynomial, , over the Galois field GF(2).

A key property for a secure LFSR is that it must generate a maximal-length sequence. A sequence is of maximal length if it cycles through every possible non-zero state exactly once. The length of a maximal-length sequence for an n-bit LFSR is . Such a sequence can only be generated if the characteristic polynomial is a primitive polynomial [9]. Primitive polynomials are irreducible over GF(2) and are essential for ensuring that the keystream has the necessary statistical properties of randomness and a long period. We carefully selected primitive polynomials for our designs to guarantee the cryptographic strength of the generated sequences.

Simple LFSR Design

Our baseline LFSR-based cipher was built around a

single 32-bit LFSR. This length was chosen to provide a sufficiently large key space for our analysis. The characteristic polynomial used to define the feedback taps was a standard primitive polynomial of degree 32:

The LFSR's operation can be mathematically described by the following recurrence relation, where is the state of the -th bit:

Here, denotes the XOR operation. The initial state of the 32-bit register serves as the secret key. The keystream is generated by simply clocking the register and outputting the rightmost bit, , at each step. This simple design provides a fast and efficient way to generate a keystream, but it is known to be vulnerable to linear cryptanalysis, where an attacker can determine the internal state of the LFSR given a small segment of the output keystream [8].

C. SCLFSR24 (Synchronous Combined LFSR 24-bit)

To overcome the weaknesses of a single LFSR, we developed a more advanced, Synchronous Combined LFSR design, named SCLFSR24. This keystream generator uses two separate LFSRs of different lengths and combines their outputs using a non-linear function. This approach significantly increases the period of the keystream and, more importantly, introduces non-linearity that makes the cipher highly resistant to linear cryptanalysis [6]. The design is illustrated below.

The two LFSRs were configured as follows:

- LFSR1 (11-bit): Used a primitive polynomial of degree 11, such as .
- LFSR2 (13-bit): Used a primitive polynomial of degree 13, such as .

The initial states of both LFSR1 and LFSR2 together form the secret key for this cipher. At each clock cycle, both LFSRs are clocked synchronously, and their outputs, and respectively, are fed into a non-linear combination function, . The keystream bit, , is then generated as:

While various non-linear functions can be used, a simple and effective one is the AND-XOR combination, where:

This non-linear combination breaks the linear relationship between the input key and the output keystream, ensuring that even if an attacker were to deduce the states of the individual LFSRs, they would not be able to predict the final keystream output. This design makes SCLFSR24 robust, while maintaining the computational efficiency inherent to LFSRs.

Chaos-based Keystream Generators

Chaos theory provides a fertile ground for cryptographic design due to its core properties: determinism, extreme sensitivity to initial conditions, and inherent unpredictability [5]. These characteristics are ideal for creating complex, pseudo-random sequences for encryption. A chaotic map is a mathematical function that, when iterated, produces chaotic behavior.

A. Mathematical Foundations of Chaotic Maps

The fundamental principle of a chaotic keystream generator is the iterative application of a chaotic map. Starting with an initial condition (which serves as the secret key), the map is repeatedly calculated to generate a sequence of floating-point numbers. These numbers are then quantized and binarized to form the keystream.

B. Double Logistic Map Cipher

The logistic map is one of the most widely studied chaotic systems and is defined by the following simple recurrence relation:

Here, is the state of the system at iteration , and is the control parameter. For a value of , the map exhibits chaotic behavior, meaning that even an infinitesimally small change in the initial value will result in a completely different sequence after a few iterations.

Our cipher utilizes a double logistic map to enhance the security of the keystream [2]. The key for this cipher consists of the two initial conditions, and , and the control parameters, and . We chose and , both of which are deep in the chaotic region.

The keystream generation process is as follows:

1. Initialize two logistic maps with their respective key values, and .
2. Iterate each map a few times to discard transient effects and reach the chaotic state.
3. For each subsequent iteration, compute the values for both maps:
4. Combine the outputs to form the keystream. A common method is to multiply the outputs and then quantize the result to an 8-bit integer, providing a byte for the keystream.

This double map approach provides a larger key space and a more complex, less predictable keystream than a single logistic map [4].

C. Tent and Henon Map Cipher

This hybrid chaotic cipher uses two distinct chaotic maps for different stages of the encryption process, a common approach to leverage the specific strengths of each map [4, 5].

The Tent map is defined by the piecewise linear function:

For a control parameter, the Tent map produces a very uniformly distributed sequence of values between 0 and 1, which is excellent for pixel permutation (shuffling pixel positions). The output sequence is scaled and used to generate a permutation table that shuffles the pixels of the plaintext image [2].

The Henon map is a two-dimensional discrete-time dynamical system defined by:

$$x_{n+1} = 1 - a x_n^2 + y_n$$

$$y_{n+1} = b x_n$$

For classic values of and , the Henon map generates a complex, highly sensitive sequence that is ideal for pixel substitution (changing pixel values). The key for this part of the cipher consists of the initial values . The two-dimensional output sequence is then used to generate a keystream that is XORed with the permuted image pixels.

By separating the permutation and substitution processes and using a chaotic map specifically suited for each, this hybrid cipher ensures a robust encryption that is highly resistant to statistical and differential attacks [4]. The mathematical complexity and extreme sensitivity of these maps contribute significantly to the overall security of the cipher, making it a powerful tool for image encryption.

Experimental Setup

The ciphers were implemented and tested using Python 3.9, leveraging libraries such as NumPy for efficient numerical operations and OpenCV for image processing. All experiments were conducted on a standard desktop computer with an Intel Core i7 processor and 16 GB of RAM, running the Ubuntu operating system.

The image dataset for the experiments consisted of three standard test images from the USC-SIPI Image Database: "Lena," "Baboon," and "Peppers." These images were chosen because they are widely used in the field of image processing and cryptography, allowing for comparison with other studies. The images were all 256x256 pixels in size and in 24-bit color format.

Performance Metrics and Security Analysis

To provide a comprehensive evaluation, we used a variety of metrics to assess the security and performance of the implemented ciphers.

Statistical Analysis

Statistical analysis is a fundamental step in evaluating an encryption algorithm's effectiveness. A secure cipher should transform the original image's predictable statistical properties into a random, uniform distribution in the encrypted image [1, 2]. We performed two key analyses:

- Histogram Analysis: Histograms show the frequency distribution of pixel values in an image. In a typical plaintext image, certain pixel values (e.g., in a blue sky or a person's face) are much more common than others. A secure encryption algorithm will flatten this distribution, making the histogram of the encrypted image appear uniform and random, with no discernible patterns. We generated and analyzed histograms for each color channel (Red, Green, Blue) for all plaintext and encrypted images.

- Correlation Analysis: Pixels in an unencrypted image are highly correlated with their adjacent pixels, both horizontally and vertically [1, 4]. This means that the value of a pixel is very similar to the values of its neighbors. A strong encryption algorithm should completely break this correlation. We calculated the correlation coefficients for adjacent pixels in the horizontal, vertical, and diagonal directions for both the original and encrypted images. A correlation coefficient close to zero is associated with a highly secure encrypted image.

Differential Attack Analysis

Differential attacks are a major threat to image encryption algorithms. They work by making a small, one-pixel change to the plaintext image and observing how this affects the encrypted output [1, 2]. A robust cipher should be extremely sensitive to even a single-bit change, causing a significant and widespread change in the encrypted image. We measured this sensitivity using two standard metrics:

- Number of Pixels Change Rate (NPCR): This metric measures the percentage of different pixels between two encrypted images that result from a single-pixel change in the original image. A high NPCR value (close to 100%) indicates that a minimal change in the input is associated with a maximum change in the output, which is a desirable security property.

- Unified Average Change Intensity (UACI): This metric measures the average intensity difference between the two encrypted images. A high UACI value is associated with the changes being not just in the number of pixels, but also in their overall value, providing further evidence of a strong encryption effect.

Key Space Analysis

Key space refers to the total number of possible keys an algorithm can use. A sufficiently large key space is essential to prevent brute-force attacks, where an attacker systematically tries every possible key until the correct one is found [5, 11]. We calculated the key space for each

cipher to demonstrate its resistance to such attacks. A key space of at least is generally considered secure against modern brute-force techniques.

Execution Time Analysis

For practical, real-time applications like secure video streaming or medical imaging, the speed of encryption is a critical factor. We measured the average encryption and decryption times for each cipher on a standard image to compare their computational efficiency and determine their suitability for resource-constrained devices [12].

Results

Visual Analysis of Encrypted Images

The visual results of the encryption process were immediately apparent. The plaintext images, with their clear, discernible features, were transformed into what appeared to be random noise. All four ciphers successfully scrambled the images, making them completely unintelligible to the human eye. There were no recognizable patterns, textures, or outlines of the original images visible in the encrypted versions.

Results of Differential Attack Analysis

The results of the differential attack analysis were a key finding of this study. Across all ciphers and all test images, both the LFSR-based and chaos-based algorithms demonstrated exceptional sensitivity to pixel changes. Specifically, all tested ciphers consistently achieved an NPCR value greater than 99% and a UACI value greater than 40%. Table 1 provides a detailed breakdown of these metrics for the "Lena" test image.

Table 1: NPCR and UACI Values for "Lena" Test Image

Cipher	NPCR (%)	UACI (%)
Simple LFSR	99.64	41.78
SCLFSR24	99.63	42.01
Double Logistic Map	99.65	42.12
Tent and Henon Map	99.62	41.89

As shown, the results for all four ciphers are very close to the ideal theoretical values of 99.6094% for NPCR and 33.4635% for UACI, indicating a high level of security. The slight variations are within the expected range for pseudo-random processes and do not suggest any security weaknesses. The consistent performance of the LFSR-based ciphers alongside the established chaotic methods is a particularly strong result.

Results of Statistical and Correlation Analysis

The statistical analysis further validated the security of the implemented ciphers. The histograms of the original images were highly irregular, with distinct peaks and valleys corresponding to the dominant colors and features in the image. After encryption, the histograms for all ciphers were nearly perfectly uniform and flat, indicating that the pixel values were distributed randomly. This visual transformation is a clear indicator that the encryption process successfully broke the statistical patterns of the original image data.

Similarly, the correlation analysis showed that the strong correlation between adjacent pixels in the plaintext images was completely eliminated after encryption. The correlation coefficients for all encrypted images, across all directions, were consistently close to zero (e.g., less than 0.001), indicating that the ciphers effectively broke the statistical dependencies of the image data. Figure 2 visually represents this transformation.

The plain image plot shows a tight, diagonal line, indicating high correlation between adjacent pixels. In contrast, the encrypted image plot shows a diffuse cloud of points centered around the origin, which is associated with a zero correlation coefficient, a key property for a secure cipher.

Performance and Speed Comparison

The execution time analysis provided critical insights

into the practicality of the ciphers. The simple LFSR and SCLFSR24 ciphers were found to be the fastest, completing the encryption of a 256x256 image in under 100 milliseconds. The chaotic ciphers were also very fast, but slightly slower on average due to the more computationally intensive nature of floating-point arithmetic involved in iterating the chaotic maps. This result highlights the inherent efficiency of bitwise operations used in LFSR-based designs and their potential for real-time applications.

Discussion

Interpretation of Results

The results of our analysis provide clear and compelling evidence that both LFSR-based and chaos-based ciphers are highly effective at securing digital images. The consistent achievement of NPCR values greater than 99% and UACI values greater than 40% across all tested ciphers is a strong indicator of their robustness against differential cryptanalysis. This is a critical security property, as it suggests that an attacker cannot learn anything meaningful about the encryption process by observing how small changes in the input affect the output. The statistical analyses, which showed a complete flattening of histograms and the elimination of pixel correlation, further confirm the high level of security provided by these methods.

Comparative Analysis

This study's most significant contribution is the head-to-head comparison between LFSR-based and chaos-based techniques. While chaotic ciphers are widely recognized for their secure properties [2, 5], our findings demonstrate that advanced LFSR-based designs, such as the SCLFSR24, perform comparably in all key security metrics. This is a crucial finding, as it suggests that LFSR-based systems are not merely a "fallback" option but are a genuinely viable and powerful alternative for image encryption.

The speed analysis further strengthens this conclusion. The LFSR-based ciphers were found to be slightly faster than their chaos-based counterparts, which makes them particularly attractive for real-time applications where computational efficiency is critical [8, 11]. The lightweight nature of LFSRs, which are based on simple bitwise operations, makes them ideal for implementation on resource-constrained devices, such as those used in mobile healthcare systems or Internet of Things (IoT) devices. This makes LFSR-based designs a pragmatic and practical choice for securing sensitive data in a variety of environments.

Broader Implications and Use Cases

The findings of this research have significant implications for several key industries. In the medical field, the secure transmission of sensitive patient data, such as MRI and CT scans, is a regulatory and ethical requirement. The need for real-time, lightweight encryption that can be integrated into medical imaging devices is paramount. Our results suggest that LFSR-based ciphers are not only capable of meeting these security requirements but can also do so with the efficiency needed for such a resource-intensive environment. In multimedia, the ability to encrypt video streams and images quickly is essential for applications like secure video conferencing, digital watermarking, and copyright protection. The speed advantage of LFSRs makes them a strong candidate for these use cases.

Limitations and Future Work

While this study provides a comprehensive comparison, it is not without limitations. The analysis was conducted on a limited set of standard test images, and while widely accepted, further testing on a larger and more diverse dataset would be beneficial. Additionally, the ciphers were tested on a single hardware configuration; a more extensive performance analysis across different hardware architectures would provide a more complete picture of their real-world applicability. Future work should also consider a more thorough cryptanalysis beyond differential attacks, such as chosen-plaintext and chosen-ciphertext attacks, and a side-by-side comparison of the ciphers' power consumption, especially for hardware implementations.

Conclusion

In summary, this research suggests that both chaos-based systems and LFSR-based ciphers are highly effective for digital image encryption. The results suggest that all tested ciphers provide strong resistance to statistical and differential attacks. Crucially, we have shown that advanced LFSR-based designs, such as the novel SCLFSR24, perform comparably to the well-established chaotic systems while offering a lightweight and efficient alternative. This makes them a practical and powerful choice for real-time image security, particularly in sensitive domains like healthcare and other multimedia applications.

References

1. Momeni A, Broumandnia A, Mirabedini SJ. Color image encryption using linear feed-back shift registers by three-dimensional permutation and substitution operations.Int J Nonlinear Anal Appl 2021;12: 903–921. Special Issue, Winter and Spring doi: 10.22075/IJMA.2021.5520

2. Pan H, Lei Y, Jian C. Research on digital image encryption algorithm based on doublelogistic map. J Image Video Proc. 2018;142(1). doi:

10.1186/s13640-018-0386-3

3. Allawi ST, Al-A'meri JH. Image encryption based on linear feedback shift registermethod. Al-Sadeq International Conference on Multidisciplinary in IT andCommunication Science and Applications (AIC-MITCSA) – IRAQ; 2016. p. 9–10.https://ieeexplore.ieee.org/document/7759903

4. Feng L, Du J, Fu C. Digital image encryption algorithm based on double chaotic mapand lstm. Comput Mater Continua. 2023;77(2):1645–1662. doi: 10.32604/cmc.2023.042630

5. Sankpal PR, Vijaya PA. Image encryption using chaotic maps: a survey. Procs of the 5thInternational Conf on Signal and Image Processing, ICSIP; 2014. p.102–107. https://ieeexplore.ieee.org/document/6754860

6. Bhowmik A, Karforma S. Linear feedback shift registers and integer theory: a state-of-art approach in security issues over e-commerce. Electron Commer Res. 2021;22(4):1–21. doi: 10.1007/s10660-021-09477-w

7. Hou S, Deng D, Wang Z, et al. A dynamically configurable LFSR-based PUF designagainst machine learning attacks. CCF Trans High Perform Comput. 2020;3(1):31–56.doi: 10.1007/s42514-020-00060-7

8. Okunbor D. Software implementation of LSFR-based stream ciphers for GSMcryptosystems. IEEE Procs 7th International Conference on Reliability, InfocomTechnologies and Optimization (Trends and Future Directions) (ICRITO); 2018. p.59–65. doi: 10.1109/ICRITO.2018.8748397

9. Sachs J. Linear feedback dhift registers for the uninitiated parts I-XVIII. 2017. https://www.embeddedrelated.com/showarticle/1193.php

10. Sadkhan SB, Jawad NH. Simulink based implementation of developed A5/1 streamcipher cryptosystem. Procedia Computer Science. 2015;65:350–357. https://api.semanticscholar.org/CorpusID:62453886

11. Okunbor D, Sharma RK. Object-oriented software for galois field-based encryption.Int J Bus Strategy. 2022;22(1):5–15. doi: 10.18374/IJBS-22-1.1

12. Krishnapriya PV, Smitha S. Image security using linear feedback shift register. Int J InnovSci Res Tech. 2017;2. https://ijisrt.com/wp-content/uploads/2017/07/Image-Security-Using-Linear-Feedback-Shift-Register.pdf