

Comparative Assessment of Image Cryptography Technique Based on Coupled Map and their Seed Maps

Hadjer BOUREKOUCHE¹, Samia BELKACEM², Noureddine MESSAOUDI¹

¹ LIST Laboratory, Department of Electrical Systems Engineering, Faculty of Technology, University M'Hamed Bougara of Boumerdes, Algeria

² LIMOSE Laboratory, Department of Electrical Systems Engineering, Faculty of Technology, University M'Hamed Bougara of Boumerdes, Algeria

E-mail: h.bourekouche@univ-boumerdes.dz

Abstract - The necessity of fulfilling the security requirements for digital images has encouraged the advancement of effective encryption techniques, where the choice of an appropriate chaotic system for producing the remote key is a critical step in establishing a strong and safe cryptosystem. To prove whether coupled chaotic systems have the advantage of improving cryptosystem security, we compared and assessed an image encryption application based on a coupled chaotic map with its seed maps, including the logistic-sine system (LSS), logistic, and sine maps. The encryption technique consists of two steps. The first step involves using a chaotic map to obtain the initial encryption key. The resulting key sequence is then XORed with grayscale image pixels to obtain the encrypted image in the second step. The comparison showed that the encryption method based on the standard sine map achieved a better performance than the coupled map in terms of speed and resilience to many forms of crypto-analysis threats with a large key space.

Keywords - compare, images encryption, chaotic system, LSS, XOR.

I. INTRODUCTION

Recently, the widespread use of image encryption based on chaotic maps has increased. Owing to the notable nonlinear feature that makes it an appropriate candidate for cryptographic applications, its sensitivity to the initial conditions, that is, the observed output, changed dramatically, even when the original settings were slightly altered.

In recent years, the dimensional classification of chaotic systems into high-dimensional and one-dimensional systems has led to the proposal of several types of chaotic systems with various dimensions. Compared with high-dimensional chaotic systems [1], which are highly complex and have excellent chaotic characteristics, resulting in high computational cost and difficulty in realization [1], 1D chaotic systems are beneficial for practical applications because they have a simple chaotic structure[2], are easy to implement by hardware and software, and

have good chaotic characteristics. However, they also have the shortcomings of limited chaotic ranges of chaotic behaviors, nonuniform data distribution of output chaotic sequences[3], and vulnerability to attack.

Thus, numerous studies have been conducted to find ways to reduce the drawbacks of 1D chaotic maps, such as cascading, switching, perturbing maps, time parameter control of chaotic systems, and nonlinear combination chaotic systems. All these improvements have effectively compensated for the defects of a simple one-dimensional chaotic system and improved the chaotic characteristics of the system [2].

For instance, a nonlinear mixture of different 1D chaotic maps, notably the Logistic-Sine System (LSS) [4], is proposed by Zhou et al.[5] to increase the chaotic ranges and strengthen the chaotic behavior compared with their seed maps. These qualities have attracted the attention of many researchers who have attempted to use them in cryptography applications. Thus, this

study aims to design and compare an image encryption system based on a coupled logistic-sine system (LSS) with their seed maps, where the three chaotic systems are used to produce a chaotic sequence as a secure key sequence that will be used for image encryption and decryption.

The remainder of this paper is organized as follows. The preliminary mathematical constructs and an analyze of their chaotic behavior is presented in Section II. The scheme for the image encryption and decryption algorithms is presented in Section III. The numerical results and discussion of the performance evaluation metrics are presented in Section IV. The conclusions of this study and our thoughts on future research are presented in Section V.

II. ANALYZE OF THE COMPORTEMENT BEHAVIOR OF LSS FROM THE LITERATURE

LSS is a chaotic coupled maps that is commonly applied in image encryption owing to their advantages of improved dynamic behavior. In this section, we briefly describe the key qualities and their seed maps.

A) Logistic Map

The logistic map came under the category of the easiest and most popular maps developed by Robert May in 1976 and is defined by Equation (1).

$$X_{n+1} = \mathcal{L}(r, X_n) = rX_n(1 - X_n) \quad (1)$$

Where $X_n \in [0,1]$ for $n = 0,1, 2\dots$ and $r \in [3.5699456,4]$ is a control parameter to present the chaotic behavior. Parameters of logistic map (r, X_n) represents the initial conditions.

B) Sine map

The sine map defined in Equation (2) is based on a sine iteration function. Where $0 \leq a \leq 1$, $X_n \in [0, 1]$. The produced series tends to be chaotic when $a=1$, but it may or may not be chaotic for other values of a .

$$X_{n+1} = S(a, X_n) = a \sin(\pi X_n) \quad (2)$$

C) Logistic sine system

The logistic-sine system (LSS)[5] described by Equation (3) is a nonlinear mixing of several

1D chaotic maps described above: the logistic and sine maps.

$$\begin{aligned} X_{n+1} &= \mathcal{F}_{LSS}(r, X_n) \\ &= [\mathcal{L}(r, X_n) + S((4-r), X_n)] \text{mod} 1 \\ &= [rX_n(1 - X_n) + (4 - r) \sin(\pi X_n)] \text{mod} 1 \quad (3) \end{aligned}$$

$$r \in (0; 4]$$

Several tests are available in the literature to emphasize the chaotic behavior of these 1D chaotic systems, including bifurcation diagrams, Lyapunov exponents, 0–1 tests, and 3ST.

The first essential feature for showing the behavior of chaotic systems is the bifurcation diagram by plotting the output sequences X_{n+1} of the chaotic map along with the change of its parameter r . Figure.1 (a–c) compare the bifurcation diagrams of the LSS with their seed maps. From these figures, it is obvious that the chaotic range of the LSS is inside (0,4], and their bifurcation behavior is evenly dispersed over the full space from 0 to 1.

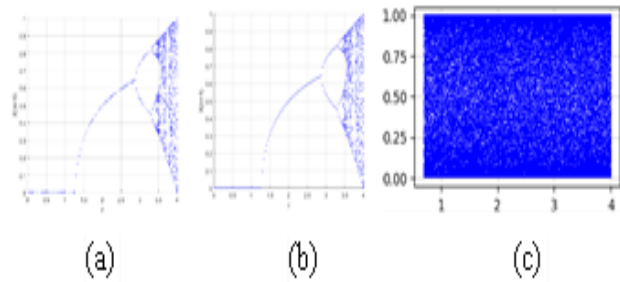


Fig. 1. Bifurcation diagrams: (a) logistic map; (b) sine map; (c) logistic-sine system

Second, when examining the dynamic behavior of chaotic systems, Lyapunov Exponents (LE) are used as key indicators to examine predictability. It is one of the most frequently utilized tests because it is easy to implement when the map f is explicitly known. The Lyapunov Exponent of a discrete time system $X_{n+1} = f(X_n)$ is given by:

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \quad (4)$$

Lyapunov Exponents were used to measure the chaos. This depends on the sign of Lyapunov exponent λ as follows: $\lambda > 0$, $\{X_n\}$ shows

chaotic behavior; $\lambda < 0$, $\{X_n\}$ shows periodic behavior. When $\lambda = 0$, bifurcation occurred.

The Lyapunov Exponent of the LSS and their seed map is tested as shown in Figure. 2. Visually, it is obvious that the LSS has more complex chaotic qualities, as evidenced by their Lyapunov Exponents, which are greater than 0 over the entire parameter setting range r , and it consistently behave chaotically in the range $r \in (0,4)$.

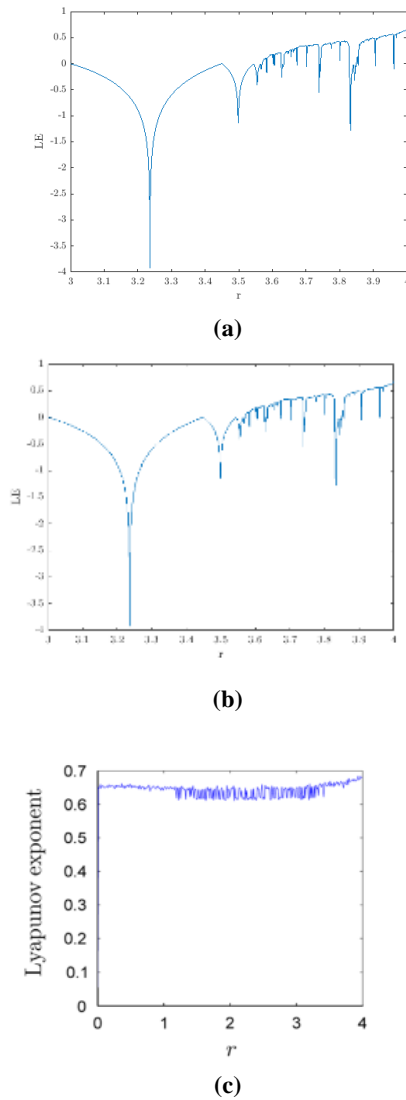


Fig. 2. Lyapunov exponent: (a) logistic map; (b) sine map; (c) logistic-sine system

Third, a relatively new method for testing chaos in deterministic discrete and continuous systems is the 0-1 test[6]. It is used to determine whether chaos exists in digital sequences when a

mathematical model is unavailable. Because the test is directly applied to time series data and phase space reconstruction is not required, it has been shown to be more favorable than the Lyapunov exponent.

A single real number K and a two-dimensional graph with translation variables p and q [6] constitute the test results. Information regarding the chaotic sequence can be revealed by the value of K [10]:

$K \approx 0$, Chaotic.

$K \approx 1$, which is regular (nonchaotic).

The 0-1 test was conducted by Muthu et al. [7] on the LSS and LTS with parameters $N=5000$ and $X(0)=0.01$.

The K values obtained for the r values in [7] demonstrate a slope of 1 for all values of r in the range [3.1, 4] for the LSS, indicating that this map does not have a consistently chaotic character over the given range. Furthermore, Muthu et al. [7] demonstrated that LSS possesses the strongest chaotic nature in most areas of r .

Fourth, 3ST is based on data series pattern analysis. This approach determines whether the dynamics are chaotic or regular by examining the properties of periodic and quasi-periodic signals. The 3ST looks at how the data series distribution of the system states changes over time. It aims to discriminate between the three major dynamics represented by the LE: chaotic (> 0), quasi-periodic (< 0), and periodic ($= 0$) dynamics.

Muthu et al. [7] performed 3ST on LSS in the range of r [3.1, 4]. Surprisingly, it clearly differentiates three types of behavior at various r values, periodic and quasi-periodic, demonstrating that the chaotic behavior of the LSS is not uniformly distributed, and certain parts are found to be quasi-periodic [7].

III. METHOD

Major In this section, we expand on the two encryption levels used in this study. Our construction method consists of two steps.

- Design of key generators based on LSS and their seed maps.
- Design of the image encryption algorithm based on the sequence

produced by the above generators and XOR operation.

A) Design of the key generator bloc

An encryption key is required to encrypt the image. To achieve this, we utilized LSS and their seed maps. These systems may construct a pseudo-random number generator (PRNG) using Equations (1)– (3).

These system characteristics were used to construct the initial pseudo-sequence. The initial conditions and control parameters of the system are not established randomly, recognizing that a slight disturbance in the initial condition and control parameters may entirely affect the random behavior of the system. Because the control parameter should be adjusted to be in the chaotic range, the r , a , and μ values that we designate secret keys are determined according to Bifurcation diagram, Lyapunov exponent, and a microscopic examination of its chaotic behavior in the range [3-4] done by Muthu et al.[7]. Therefore, we can utilize the starting value $X(0)=0.1$ and r to produce a sufficiently lengthy chaotic sequence. After that, the generated chaotic sequences X_n should be converted to an 8-bit integer since the chaotic sequence generator generates values between 0 and 1 with 10^{15} decimals. Finally, the generated sequences were converted into binary data.

B) Design of the Encryption and decryption bloc

Using the previously constructed remote sequence of keys, we detail the stages involved in the encryption/decryption process before analyzing the security of this scheme using different security tests.

In this stage of the encryption process, we applied a bitwise XOR operation between each pixel of the plain image and the corresponding bit of the proposed key matrix of equal size. During the decryption step, the encryption process is reversed by selecting the same secret key used to encrypt the plain image and performing an XOR operation between every element of the encrypted image matrix and every element of the secret key matrix.

IV. EVALUATION METRICS AND RESULTS

The performance of the proposed scheme is tested using a variety of tests that are commonly used to examine the statistical measurements and security of cryptosystems. The tests for the performance analysis of the suggested scheme were performed on a Core (TM) i3-4030U CPU @ 1.90GHz with 4GB of RAM.

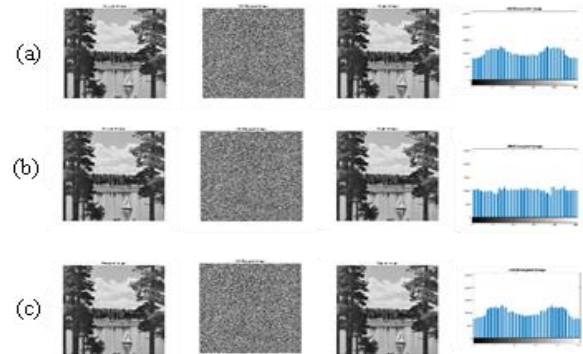


Fig. 3. Visual results of plain, encrypted and decrypted images with histogram plot of encrypted image by using: (a) logistic map; (b) sine map; (c)logistic-sine system

A) Visual analysis

Figure.3 shows the encryption-decryption results using the three key sequences generated by the LM and SM. The following conclusions can be drawn from the figures:

The plain image is effectively encrypted into a noise-like secret image in the three cases where we can see that the primitive information is completely destroyed, which results in better privacy protection. Overall, this experiment proves that the proposed encryption scheme works satisfactorily in all three cases.

B) Histogram analysis

Histograms are an important statistical characteristic of an image[8]. It is used to describe the distribution of the pixels in an image. Figure. 3 shows histograms of the ciphered images obtained using the LSS and their seed maps.

From the figures, it can be seen that :

The histograms of the encrypted image using the LM and LSS schemes are not flat, which means that the distribution of pixel values is not

uniform and leads to the leakage of some statistical information.

The histograms of the encrypted images obtained using the sine map were slightly flat and uniformly distributed. This means that the distribution of pixel values is uniform, which proves that using the sine map in encryption algorithms can resist statistical attacks.

C) Information entropy

Information entropy[9] expressed by Equation (5) provides a measure of the statistical randomness and unpredictability of the information stored in encrypted images. The entropies of the evaluated image and its matching-encrypted image using LSS and their seed maps are listed in Table 1, where the sine map presents the best entropy value near 8.

$$H(x) = -\sum_{i=0}^{2^n-1} p(x_i) \log_2 p(x_i) \quad (5)$$

$p(x_i)$ is the probability of a specific symbol x and n is the number of bits [7].

Table 1. Entropy results

	Plain image	Ciphered mage	Deciphered image
LM	7.48421927	7.98551814	7.48421927
SM	7.48421927	7.99691888	7.48421927
LSS	7.48421927	7.98105595	7.48421927

D) Differential attacks

The number of Pixel Change Rate (NPCR)[2] combined with the Unified Average Change in Intensity (UACI)[2] expressed by Equations (6) and (8), respectively, can be used to assess an image encryption algorithm's ability to withstand a differential assault[10].

$$NPCR = \sum_{i=1}^M \sum_{j=1}^N \frac{A(i,j)}{W \times H} \times 100\% \quad (6)$$

$$A(i,j) \begin{cases} 0 & \text{if } I1(i,j) = I2(i,j) \\ 1 & \text{otherwise} \end{cases} \quad (7)$$

$$UACI = \sum_{i=1}^M \sum_{j=1}^N \frac{|I1(i,j) - I2(i,j)|}{W \times H \times L} \times 100\% \quad (8)$$

Where W and H are the width and height of the image, respectively, and L is the maximum possible pixel value in an image. MSE stands for mean square error[11]. i , j , and k are the pixel

positions, whereas I and K are the pixel values of the original and encrypted images, respectively.

As shown in Table 2, with a mean score close to 99% for NPCR and 33% for UACI, Encrypted image using the sine map yielded better results in the differential analysis than LM or LSS.

Table 2. NPCR and UACI results

	NPCR	UACI
LM	0.9902534	0.3061220
SM	0.999999	0.3523098
LSS	0.971546	0.29618

E) Run-Time Analysis

To assess the effectiveness of the proposed algorithm in encrypting and decrypting images, we calculated the execution times for various images.

F) Memory Analysis

Memory analysis was used to estimate the memory required by the proposed technique for encrypting and decrypting images.

We calculated the execution time and end-to-end memory usage for the same image using the three schemes. Table 3 reveal that the scheme based on the SM is considerably faster, it is able to encrypts 512x512 images in an average time of approximately 0.05 seconds with a small memory usage of just 0.004096 in comparison with LM and LSS.

Table 3. Run time and memory usage results

	End-to-end Run time (in seconds)	End-to-end memory usage (in MB)
LM	0.053130	0.040960
SM	0.058523	0.004096
LSS	0.055403	0.618496

G) Key space

The key space is a set of potential keys that can be used to create a random sequence. We compared the key spaces of the proposed system based on LSS and their seed maps.

The precision of the initial condition $X(0)$ variation along with bifurcation parameter r and a is 10^{-15} .

The key-space for $X(0)$ is $\text{key}_1 \approx 10^{-15}$ and for the bifurcation parameter is $\text{key}_2 \approx 10^{-15}$.

the total key-space of the three scheme is $\approx 10^{15} \times 10^{15} = 10^{30}$

To fend against brute force attacks, the key space of the image encryption technique should be greater than 2^{100} . Consequently, the three schemes have a vast key space to fend against brute-force.

V. CONCLUSION

This paper provides a comparative examination of coupled systems, namely, the LSS and their seed maps: logistic and sine maps applied to image cryptography. The encryption algorithm uses a sequence of keys produced by the five chaotic systems to generate a secret key that is XORed with the plain image to obtain a ciphred image.

Coupling chaotic maps is a common way to develop more sophisticated dynamic behavior; however, regarding practical usage, it is clear that basic standard maps such as sine maps stand out because they provide a good mix of speed, high security, complexity, and acceptable computational overhead, among other basic maps.

The obtained results show a significant degradation in the system efficiency and resistance against different types of crypto-analytical threats when using the coupled map LSS compared to other image encryption schemes based on their seed maps.

This result demonstrates that the basic structure and ease of use of typical 1D chaotic maps are the key features for designing a strong and secure cryptosystem.

Future work will consider the application of this technique to field-programmable gate arrays (FPGA) to perform a corresponding search.

VI. REFERENCES

- [1] Y. Luo, J. Yu, W. Lai, et L. Liu, « A novel chaotic image encryption algorithm based on improved baker map and logistic map », *Multimed. Tools Appl.*, vol. 78, n° 15, p. 22023-22043, août 2019, doi: 10.1007/s11042-019-7453-3.
- [2] Y. Dou, X. Liu, H. Fan, et M. Li, « Cryptanalysis of a DNA and chaos based image encryption algorithm », *Opt. - Int. J. Light Electron Opt.*, vol. 145, août 2017, doi: 10.1016/j.ijleo.2017.08.050.
- [3] B. Ramalingam, A. Rengarajan, et J. B. B. Rayappan, « Hybrid image crypto system for secure image communication– A VLSI approach », *Microprocess. Microsyst.*, vol. 50, p. 1-13, mai 2017, doi: 10.1016/j.micpro.2017.02.003.
- [4] X. Chai, « An image encryption algorithm based on bit level Brownian motion and new chaotic systems », *Multimed. Tools Appl.*, vol. 76, n° 1, p. 1159-1175, janv. 2017, doi: 10.1007/s11042-015-3088-1.
- [5] Y. Zhou, L. Bao, et C. L. P. Chen, « A new 1D chaotic system for image encryption », *Signal Process.*, vol. 97, p. 172-182, avr. 2014, doi: 10.1016/j.sigpro.2013.10.034.
- [6] W. Marszalek et M. Melosik, « On the 0/1 test for chaos in continuous systems », *Bull. Pol. Acad. Sci. Tech. Sci. 2016 64 No 3 521-528*, 2016, Consulté le: 22 octobre 2023. [En ligne]. Disponible sur: <https://journals.pan.pl/dlibra/publication/98099/edition/84541>
- [7] Joan. S. Muthu, A. J. Paul, et P. Murali, « An Efficient Analyses of the Behavior of One Dimensional Chaotic Maps using 0–1 Test and Three State Test », in *2020 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, déc. 2020, p. 125-130. 10.1109/RAICS51191.2020.9332470.
- [8] L. Huang, S. Wang, J. Xiang, et Y. Sun, « Chaotic Color Image Encryption Scheme Using Deoxyribonucleic Acid (DNA) Coding Calculations and Arithmetic over the Galois Field », *Math. Probl. Eng.*, vol. 2020, p. e3965281, mars 2020, doi: 10.1155/2020/3965281.
- [9] X. Wang et X. Chen, « An image encryption algorithm based on dynamic row scrambling and Zigzag transformation », *Chaos Solitons Fractals*, vol. 147, p. 110962, juin 2021, doi: 10.1016/j.chaos.2021.110962.
- [10] X. Liu, X. Tong, Z. Wang, et M. Zhang, « Construction of controlled multi-scroll conservative chaotic system and its application in color image encryption », *Nonlinear Dyn.*, vol. 110, n° 2, p. 1897-1934, oct. 2022, doi: 10.1007/s11071-022-07702-1.
- [11] C.-C. Chang, C.-S. Chan, et Y.-H. Fan, « Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels », *Pattern Recognit.*, vol. 39, n° 6, p. 1155-1167, juin 2006, doi: 10.1016/j.patcog.2005.12.011.