International Journal of Automation and Safety (IJAS)
Vol 02, N° 01, June, 2024, pp. 19-23

Journal homepage: https://www.asjp.cerist.dz/en/PresentationRevue/944

Developing an Image Encryption Algorithm Utilizing Chaotic Systems

Djamel Herbadji [1*] Abderahmane Herbadji [2],Hichem Kahia[2], Ismail Haddad[1] Aïssa Belmeguenaï[1], Amine Herbadji [2],

1 Department of Electrical Engineering, 20 Aout 1955 University, Skikda 21000, Algeria

2 Department of Electrical Engineering, setif1 University, Setif 19000, Algeria

Corresponding Author Email: herbadjidjamel@gmail.com

Received: April 18th 2024
Accepted: April 19th 2024
Published: June 30th 2024

Keywords:
encryption , cryptographic chaos

ABSTRACT

In recent years, the utilization of chaotic maps in encryption has emerged as a compelling area of research, owing to its myriad advantages, rendering it highly suitable for cryptographic applications. This paper introduces a novel image encryption algorithm founded on a confusion-diffusion process. The Logistic-Logistic System is employed to alter both the positions and values of image pixels, while the Sin-Sin system is utilized to modify the pixel values. Remarkably robust security is achieved with just a single encryption round. The algorithm's efficacy has been corroborated through security analysis, with experimental results showcasing its simplicity, efficiency, and attributes such as a vast key space and high sensitivity to its key.

1. INTRODUCTION

Image encryption has emerged as a critical technology for safeguarding image content, prompting a surge in research interest in recent years. Concurrently, chaotic systems offer valuable attributes such as their remarkable sensitivity to initial conditions and control parameters, nonlinearity, ergodicity, and behavior akin to randomness. These qualities make chaotic systems appealing for encryption applications.

However, the security of image encryption schemes employing chaotic maps hinges on two primary components: permutation and diffusion processes. In the permutation phase, pixel locations undergo alterations to eliminate redundancies and disrupt high correlations among neighboring pixels. Conversely, the diffusion phase involves modifying pixel values within the image. Some encryption methodologies employ iterative processes of permutation and diffusion to bolster encryption efficacy.

In light of the increasing demand for robust security frameworks, a variety of chaos-based image encryption techniques have been developed to prevent unauthorized data breaches. For instance, Djamel et al [1] suggested enhancing the classical logistic chaotic system to improve voice encryption, leading to a wider chaotic range and increased unpredictability. They introduce a tweakable encryption algorithm that preprocesses speech signals, reducing computing time and resources, while offering robust protection against known and chosen plaintext attacks, thus advancing voice transmission security.

Djamel et al[2]. proposed the use of an enhanced quadratic map (EQM) for a novel color image encryption scheme. Evaluation showed EQM's superiority over the classical quadratic map, making it suitable for image encryption with robust confusion and diffusion properties. Comparison with recent schemes revealed its effectiveness, highlighting its potential for secure image encryptio .Djamel et al[3]. suggested improving the classical logistic chaotic map for image encryption. They validated their approach using bifurcation diagrams and Lyapunov exponents, comparing it with the traditional method. Following this, they introduced a tweakable image encryption algorithm for secure digital image transmission, showcasing its resilience against diverse attacks. This study significantly contributes to the progression of data security in digital image transmission, Rim Zahmoul et al.[4] developed an encryption method utilizing novel Beta chaotic maps. These maps are instrumental in producing chaotic sequences that enhance the security protocol of the encryption process. Furthermore, Asia Mahdi et al.[5] advanced a method for encrypting and Decrypting color images involves employing Pixel Shuffling in combination with the Henon Chaotic System, Yannick Abanda et al. delved into image encryption techniques centered around chaos mixing.

The current study introduces a novel algorithm designed for encrypting images intended for transmission over non-secure channels. This algorithm is straightforward and easily implementable for both encrypting and decrypting images. The structure of this paper is organized into five main sections: the initial

section provides a historical overview of image encryption, The second section of the discussion focuses on chaotic maps, followed by a detailed exploration of the newly proposed image encryption algorithm in the third section. Experimental results are examined in the fourth section, and the paper concludes with a summary of findings in the fifth section

2. CHAOTIC SYSTEMS

The Logistic map and the Sine map stand out as two of the most renowned 1D chaotic maps, characterized by straightforward yet classic dynamical nonlinear equations that give rise to complex chaotic behaviors. They can be mathematically described by the following equations [7]:

$$X_{n+1} = rX_n(1 - X_n) \quad (1).$$
$$X_{n+1} = rSin(\pi X_n) \quad (2).$$

The control parameter 'r', spanning the range r∈[0,4], and the resulting chaotic sequence Xn are essential elements of the chaotic system under scrutiny. Upon examining the bifurcation diagrams depicted in Figures 1(a) and 1(b), two shortcomings become apparent in these chaotic maps. Firstly, they exhibit a limited chaotic range. Secondly, as illustrated in Figures 1(a) and 1(b), their chaotic behavior is confined strictly to the interval [3.57, 4]. When the control parameter 'r' falls outside this range, the system fails to demonstrate chaotic behavior. Due to this limitation, there is a non-uniform distribution observed in the output chaotic sequences., adversely affecting the distribution of encrypted image data and compromising the overall performance of the encryption system.

To address these issues, a novel approach has been proposed in [8] to rectify the aforementioned defects. This approach involves the amalgamation of multiple logistic maps to create new chaotic maps. By combining these maps, the aim is to expand the chaotic range and enhance the uniformity of the sequence distribution. This enhancement is crucial for bolstering the security and efficiency of the encryption process, ensuring a more robust framework for safeguarding sensitive image data.

2.1 Sine-Sine-Map choatic

The Sine-Sine-System chaotic (SSS) is produced by merging the Sine map according to the following equation:

$$x_{n+1} = u\, sin(\pi\, x_n)2^k - floor(u\, sin(\pi\, x_n)2^k) \quad (3).$$

The control parameters of the new chaotic system map are are expressed as follows: μ ∈ [0, 10] and k ∈ [8, 20].

2.2 Logistic-Logistic-Map

The Logistic-Logistic-System chaotic (LLS) is formed through the fusion of the logistic map, as described by the following equation

$$x_{n+1} = u\, x_n(1 - x_n)2^k - floor(u\, x_n(1 - x_n)2^k) \quad (4)$$

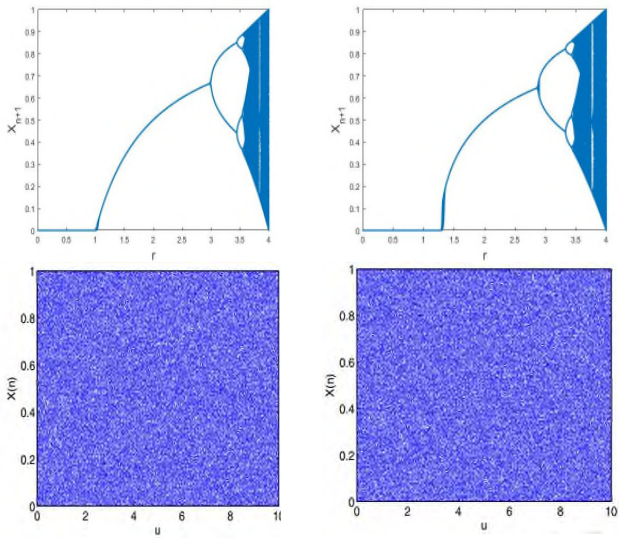

Fig.1. The bifurcation diagrams (a) Logistic map,(b) Sine map, (c) LLS , (d) SSS

The bifurcation diagrams of the Logistic-Logistic System (LLS) and the Sin-Sin System (SSS) are depicted in Fig.1(c) and Fig.1(d) respectively [8]. Their chaotic range spans from 0 to 10, which is significantly broader than that of their seed maps, showcasing excellent chaotic performance.

3. Proposed image encryption scheme

In this section, we introduce a novel image encryption algorithm. This encryption method relies on six parameters of ($x_{0,1}$=0.56, $x_{0,2}$=0.23 ,$u_{0,1}$=5.4321, $u_{0,2}$=2.81 k_1=14, k_2=14,p1) as the security key. The diagrams of Figures 2 and 3 depict the proposed encryption algorithm.

Encryption process

Input: The plain image, denoted as I, has dimensions W × H.

Output: The encrypted image C

Step 1: The grayscale image I is Reshaped into one vector O ={o_1, o_2, ...$o_{W \times H}$} with the size of W × H.

Step 2: Two different chaotic sequences are generated $x_1 = \{x_{1,1}, x_{1,2}, \ldots x_{1,W*H}\}$, $x_2 = \{x_{2,1}, x_{2,2}, \ldots x_{2,W*H}\}$ of size W*H, by using the equations 3 and 4 respectively. Then x1 is arranged in ascending order then get the shuffled positions matrix x', the process is shown in Fig.3.

Step 3: The image O is rearranged using the function x' to produce the shuffled image P. This shuffling disrupts the correlation between adjacent pixels, thereby enhancing the security of the method. This is achieved by applying the equation:

$$P(i)=O(x'(i)). \quad (5).$$

The diffusion mechanism of the proposed method is outlined in Algorithm 1 and illustrated in Figure 3. This mechanism requires three inputs: a secret key *K*, the first pixel of the shuffled image *p*1 which is within the range 0,2560,256, and After shuffling, the resulting image is denoted as P. The output of this process is a cipher-image, represented as C. $c1, c2, \ldots, c_{W*H}$. In our algorithm, the value of each encrypted pixel is influenced not only by its corresponding original pixel but also by all other pixels in the image. Consequently, even a minor alteration in any pixel of the original image results in a significantly different encrypted image.

Algorithm 1 diffusion

1 input: Shuffled_image: *P*; secret_parameters: $x_{0,2}$,$u_{0,2}$, k_2, p1
2 output: Cipher_image: *C*
3 $x_{0,2}$, $u_{0,2}$, k_2 are used to obtain a chaotic sequence X_2 of size $H \times W$ using LLS
3 X_2 is converted to a sequence of integers values, by following equation
4 $X_2(i)=floor(X_2(i)*10^{15}),256)$
5 n=H*W
6 $Z(1)=p1 \oplus X_2(1)$
7 $Z(n)= P(n) \oplus X_2(n)$
8 $P(n)= Z(n) \oplus Z(1)$
9 for i=1:n-1
10 $Z(i)= P(i) \oplus X_2(i)$
11 $C(i)= Z(i) \oplus Z(i+1)$
12 end
13 The encrypted C is Reshaped into 2D matrix with size W*H

The resulting image is an encrypted image with a noise-like appearance.

3.1 Decryption process

The decryption process mirrors the encryption process. The permutation and diffusion processes employed in decryption are as follows:

$O(x'(i)) = P(i)$;

Algorithm 2 invrse_diffusion

1 input: cipher_image C; secret_parameters: $x_{0,2}$,$u_{0,2}$, k_2 , p1
2 output: Shuffled_image: *P*
3 $x_{0,2}$,$u_{0,2}$, k_2 are Used to obtain a chaotic sequence X of size $H \times W$ using LLS
4 X is converted to a sequence of integers values, by following equation
5 $X(i)=floor(X(i)*10^{15}),256)$
6 n=H*W
7 $Z(n)= C(n) \oplus X_2(n)$
8 $P(r*c)=[C(r*c) \oplus X_2(r*c)] \oplus [P(1) \oplus X_2(1)]$;
9 for i=1:n-1
10 $P(i)=[C(i) \oplus X_2(i)] \oplus [P(i+1) \oplus X_2(i+1)]$;
11 end

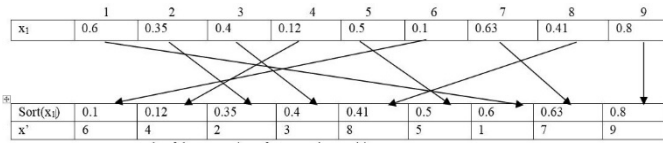

Fig.2. An example of permutation position vector generation

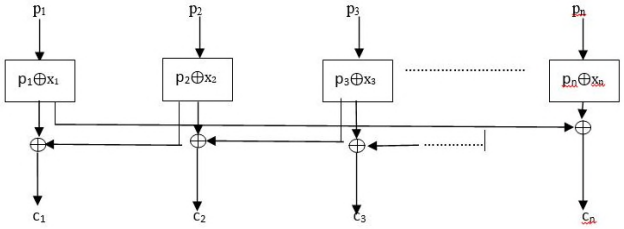

Fig.3. An example of the diffusion model of the proposed scheme

4. Experimental results

This section examines how well the proposed encryption algorithm resists different attack methods. We'll evaluate its effectiveness using several tests to ensure its comprehensiveness:

- **Randomness tests:**
  - Number of Pixel Change Rate (NPCR)
  - Unified Average Changing Intensity (UACI)
- **Correlation analysis** to assess statistical randomness.
- **Image quality tests:**
  - Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) to measure distortion introduced by encryption.
- **Key sensitivity evaluation** to ensure small key changes significantly alter the ciphertext.
- **Information entropy analysis** to measure the randomness of the encrypted data.

4.1 Key space analysis

To make a brute force attack impractical, the key space needs to exceed 2^{100} [10]. The secret keys employed in our suggested approach are outlined as follows:

1. Control parameters $u_{0,1}$, $u_{0,2}$.
2. Initial values x1, x2, , the first pixel of the shuffled image p1∈ [0, 255] and , k_1, ∈ [8, 20], k_2 ∈ [8, 20],

If each parameter and initial value space is set to 15 decimals, then the key space of our proposed scheme is $12*12*256*10^{4*15}$. This key space is large enough to resist brute force attacks.

4.2 The histogram analysis

An image histogram shows how many pixels have each brightness level [11]. To withstand statistical attacks, the image histogram should exhibit a fairly uniform distribution. Figures 4 and 5 illustrate the histograms of some plain-images and their corresponding cipher-images. Upon examination of these figures, it is evident that the histogram of the cipher-images demonstrates a fairly uniform and flat distribution. This characteristic is adequate to render statistical attacks infeasible.

4.3 Information entropy analysis

Entropy serves as a crucial metric for assessing the unpredictability and randomness of information [11]. Ideally, for grayscale images, entropy should be close to 8 [13]. The entropy of an image

I is defined as:

$$E(m) = -\sum_{i=0}^{255} \Pr(mi) \log_2 \Pr(mi). \quad (7).$$

The information entropy, a measure of randomness (ideally 8 for encrypted data), is calculated for encrypted images using our scheme, where Pr(mi) represents the probability of symbol mi (shown in Table 1). The entropy values indicate that our encryption achieves a high degree of randomness, surpassing those obtained in [1, 8]. This enhanced randomness strengthens the encryption's resistance against attacks that exploit predictable data patterns

Table1: Information entropy analysis of various images

Image	Original	Encrypted	[3]	[8]
Lena	07.56910	07.99700	07.99720	7.99640
Boat	07.19130	07.99920	07.99920	7.99890
Baboon	07.35790	07.99930	07.99920	07.9996

4.4 Coefficient correlation

In any image, each pixel has a high correlation with its adjacent pixels in either the vertical, diagonal, or horizontal direction [11]. A strong image encryption algorithm should minimize the correlation between neighboring pixels to prevent attackers from gleaning information. This correlation is calculated using the following equation:

$$\text{corr} = \frac{\text{cov}(x,y)}{\sqrt{D(x)D(Y)}}$$

Where X and Yare the sets composed of N pixel gray values, $x_i \in X$ and $y_i \in Y$, are two adjacent pixels,

$$E(X) = \frac{1}{N}\sum_{i=1}^{N} x_i,\ D(X) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(X)]2 \quad \text{and}$$

$$\text{cov}(X, Y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(X)][y_i - E(Y)].$$

Figure 6 illustrates the correlation coefficients between neighboring pixels in the horizontal, vertical, and diagonal directions for both the original and encrypted images. Table 2 lists the specific correlation coefficients for some sample images. As expected for secure encryption, the correlation coefficients of the encrypted images approach zero in all directions. Moreover, when compared to the algorithm used in reference [1], our proposed algorithm exhibits the smallest correlation values in all directions. Thus, the proposed algorithm effectively safeguards the images against statistical attacks.

Table 2. Coefficient Correlation Analysis.

Direction	Original Image	Cipher Image	[2]
Diagonal	0.9340	-3.3846e-04	00.001949
Horizontal	0.9690	-0.00120	00.039886
Vertical	0.9170	-0.00120	00.034475

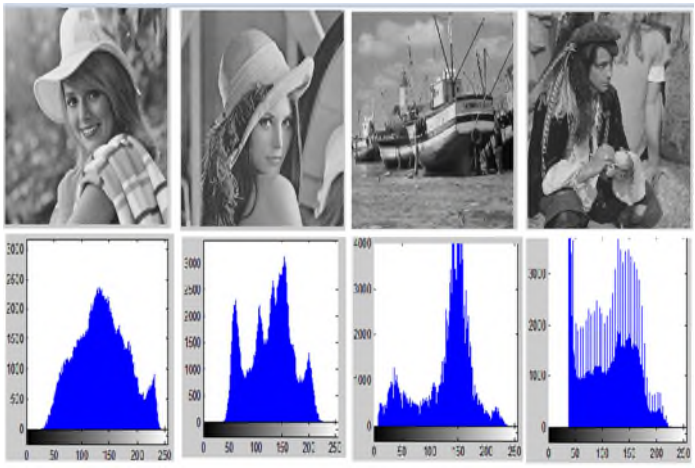

Fig. 4. Original images of 'Elaine', 'Lena', 'Boat', 'Man' and their histograms.

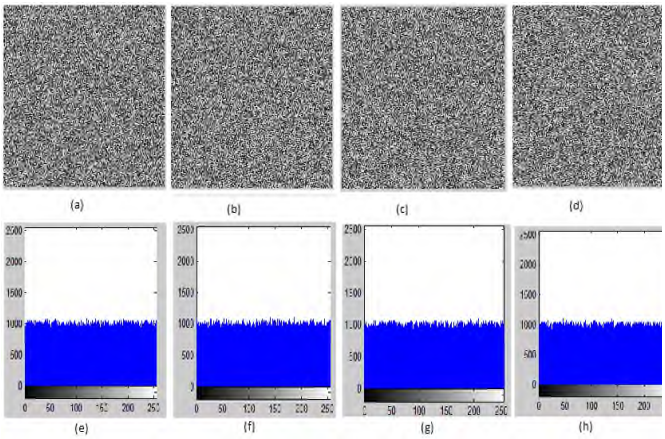

Fig. 5. Encrypted images of 'Elaine', 'Lena', 'Boat', 'Man' and their histograms Respectively(from left to right).

4.5 Key sensitivity analysis

An encryption algorithm must not only possess a key space extensive enough to withstand brute force attacks, but it should also demonstrate a high degree of sensitivity to its keys. Even a minute disparity of 10^{-14} between the encryption and decryption keys should result in decryption failure. To assess the key sensitivity of our proposed algorithm, we attempted to decrypt the Lena image using an incorrect set of independent parameters. The outcomes are illustrated in Figure 6. Notably, even with a marginal alteration of 10^{14}, the decrypted image markedly diverges from the original one. This underscores the exceptional sensitivity of our proposed algorithm to its keys.

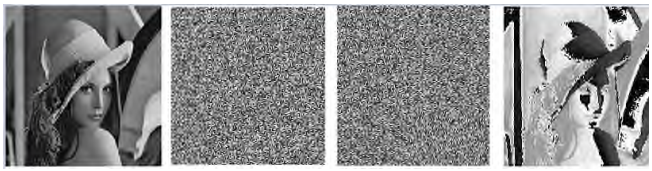

Fig. 6 : a small changes to the secret key drastically alter the decrypted image. In (a) the correct key is used, while (b), (c), and (d) show the results with slightly modified keys."

5. CONCLUSIONS

In this paper, we introduce a novel algorithm for encrypting images by leveraging two chaotic maps. Specifically, we utilize the Logistic-Logistic System to alter the positions of pixels within the image, while employing the Sine-Sine System to generate a sequence of random values. he generated values are then combined with each pixel value in the image using a bitwise XOR operation.

We have conducted both differential and statistical analyses to evaluate the performance of the proposed algorithm. The results obtained demonstrate the robustness of the algorithm against various known attacks, highlighting its effectiveness in ensuring the security of encrypted images.

REFERENCES

[1] H. Djamel, A. Herbadji, I. haddad, H. Kahia, A. Belmeguenai, and N. Derouiche, "An enhanced logistic chaotic map based tweakable speech encryption algorithm," *Integration*, vol. 97, no. March, p. 102192, 2024, doi: 10.1016/j.vlsi.2024.102192.

[2] D. Herbadji, A. Belmeguenai, N. Derouiche, and H. Liu, "Colour image encryption scheme based on enhanced quadratic chaotic map," *IET Image Process.*, 2019.

[3] D. Herbadji, N. Derouiche, A. Belmeguenai, A. Herbadji, and S. Boumerdassi, "A Tweakable Image Encryption Algorithm Using an Improved Logistic Chaotic Map.," *Trait. du Signal*, vol. 36, no. 5, pp. 407–417, 2019.

[4] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new Beta chaotic maps," Optics and Lasers in Engineering, vol. 96, pp. 39–49, 2017.

[5] A. M. N. Alzubaidi and N. D. K. Al-Shakarchy, "Color Image Encryption and Decryption Based Pixel Shuffling with 3D Blowfish Algorithm," International Journal of Science and Research (IJSR), vol. 3, no. 7, pp. 336–343, 2014.

[6] Y. Abanda and A. Tiedeu, "Image encryption by chaos mixing," IET Image Processing, vol. 10, no. 10, pp. 742–750, 2016.

[7] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," Signal processing, vol. 97, pp. 172–182, 2014.

[8] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," Signal Processing, vol. 138, pp. 129–137, 2017.

[9] M. Dridi, M. A. Hajjaji, B. Bouallegue, and A. Mtibaa, "Cryptography of medical images based on a combination between chaotic and neural network," IET Image Processing, vol. 10, no. 11, pp. 830–839, 2016.

[10] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129–2151, 2006.

[11] A. Beloucif, O. Noui, and L. Noui, "Design of a tweakable image encryption algorithm using chaos-based schema," International Journal of Information and Computer Security, vol. 8, no. 3, pp. 205–220, 2016.