2015 IEEE International Conference on Systems, Man, and Cybernetics

Image cipher using a new interactive two-dimensional chaotic map

Zhongyun Hua, Yiran Wang, Yicong Zhou*
Department of Computer and Information Science University of Macau, Macau, China 999078
Email: * yicongzhou@umac.mo

***Abstract*—In this paper, a new two-dimensional (2D) Tent-cascade-Logistic map (2D-TCLM) is introduced. Analysis results demonstrate that it has complex chaotic behaviors. Using 2D-TCLM, a new image encryption algorithm is also proposed. Simulation results and security analysis show that it can encrypt different kinds of digital images into unrecognized random-like images with a high security level.**

***Keywords*—chaotic map, image encryption, two-dimensional (2D) Tent-cascade-Logistic map (2D-TCLM).**

I. Introduction

With the fast development of information and network technologies, more and more digital images carrying all kinds of information are generated and spread through the networks every moment. Thus, as a straightforward image security technology, image encryption has been studied and paid more and more attentions. An image encryption algorithm is to encrypt a digital image into an unrecognized random-like image that can be only correctly constructed with the corresponding key [1].

Among all kinds of image encryption algorithms, chaos-based encryption is one of the most widely used technologies. This is because a chaotic system have the properties of unpredictability, ergodicity and initial conditions sensitivity [2]. It can generate nonoverlapping and unpredictable chaotic sequences. These properties can be found similar in image encryption. For a good image encryption algorithm, its encrypted image should be very sensitive with the original image and pixels in the encrypted image should distribute randomly. Since chaos theory has been used in image encryption in 1990s [3], [4], many chaos-based image encryption algorithms have been developed [5]–[7].

In the chaos-based image encryption algorithms, the security performance of the encryption algorithms are much depended on the chaos performance of the used chaotic systems. If the used chaotic systems' chaos performance is poor, the corresponding image encryption algorithms can be broken [8]–[10]. Therefore, developing new chaotic maps with complex chaotic behaviors and using them to design new image encryption become significant.

In this paper, a new two-dimensional chaotic map (2D-TCLM) is proposed. It is generated by cascading the Logistic map with the Tent map, and then extending the outputs from one-dimensional (1D) to 2D. Its trajectory and information entropy analysis have demonstrated that the proposed 2D-TCLM has complex chaotic behaviors. Using the proposed 2D-TCLM, a new image encryption algorithm is also proposed. Simulation results and security analysis have shown that the proposed algorithm can encrypt an original image into a random-like image with a high security level.

The rest of this paper is organized as follows: Section II will introduce 2D-TCLM and it will be used to design new image encryption algorithm in Section III; Section IV will simulate the proposed image encryption algorithm and analyze its security performance; Section V will get a conclusion.

II. The 2D Tent-cascade-Logistic map

This section introduces the 2D Tent-cascade-Logistic map (2D-TCLM), and analyzes its chaos performance.

A. Definition

Mathematically, 2D-TCLM is defined as

$$\begin{cases} x_{n+1} = \begin{cases} (3+y_n)2\mu x_n(1-2\mu x_n) & \text{if } x_n < 0.5 \\ (3+y_n)2\mu(1-x_n)(1-2\mu(1-x_n)) & \text{if } x_n > 0.5 \end{cases} \\ y_{n+1} = \begin{cases} (3+x_{n+1})2\mu y_n(1-2\mu y_n) & \text{if } y_n < 0.5 \\ (3+x_{n+1})2\mu(1-y_n)(1-2\mu(1-y_n)) & \text{if } y_n > 0.5 \end{cases} \end{cases} \quad (1)$$

where $(x_n,\ y_n)$ are the iterative values. μ is the control parameter and $\mu \in [0, 1]$.

The trajectory of 2D chaotic map is to describe the distribution of its output pairs $(x_i,\ y_i)$ on the 2D phase plane. A trajectory of 2D-TCLM is shown in Fig. 1, As can be seen, the output pairs $(x_i,\ y_i)$ distribute in most area of the 2D phase plane. This means that the proposed 2D-TCLM has good ergodicity and its outputs are very random.

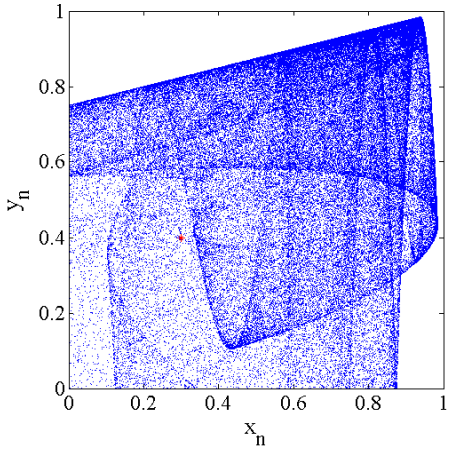

Fig. 1: A trajectory of 2D-TCLM.

978-1-4799-8697-2/15 $31.00 © 2015 IEEE
DOI 10.1109/SMC.2015.316

B. Information entropy

Information entropy is to measure the uncertainty of information content in information theory [11]. It can be used to measure the randomness of a sequence of data. Its mathematical definition is shown as

$$H(X) = -\sum_{i} Pr(x_i) \log_2 Pr(x_i) \tag{2}$$

where X is a data sequence. x_i is the i-th possible value in X and $Pr(x_i)$ is the probability of x_i. Bigger information entropy value means better randomness.

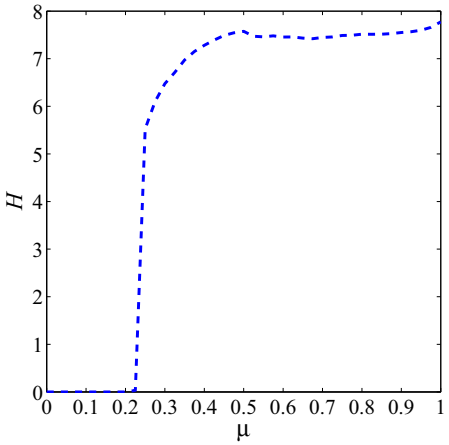

Fig. 3: The information entropy of output sequences of 2D-TCLM with different parameter settings.

To measure the information entropy of the output sequences generated by 2D-TCLM, we first separate the output values of 2D-TCLM into 256 intensities and then use Eq. (2) to calculate the information entropy. When the values of each intensity is equal, the maximum information entropy value can be obtained $H_{\max} = \log_2 256 = 8$. Fig. 3 shows the information entropy of the output sequences generated by 2D-TCLM with different parameter settings. When parameter $u \in [0.4, 1]$, the information entropy value is very big, which means good randomness.

III. Image cipher using 2D-TCLM

This section introduces a new image encryption algorithm using 2D-TCLM. The structure of the image encryption algorithm is shown in Fig. 2. As can be seen, the original image is the image to be encrypted. The encryption key is used to generate the initial conditions of 2D-TCLM. The chaotic sequences generated by 2D-TCLM are used to do the permutation and substitution to the original image. Random number insertion is to add some randomly generated values to the image to disturb the pixel values. These random values are then added to the decryption key because their information is needed to reconstruct the original image. Two times of operations can grantee that a digital image can be encrypted into a random-like image with a high security level. The encryption procedure is represented as $C = Encp(P, K_e)$ while the decryption procedure is represented as $D = Decp(C, K_d)$.

A. Security key

In the proposed image encryption algorithm, the encryption key $K_e = (x_0^1,\ y_0^1,\ \mu,\ x_0^2,\ y_0^2,\ a_1,\ a_2)$. Each component in K_e is in the range of $[0, 1]$. $(x_0^1,\ y_0^1)$ and $(x_0^2,\ y_0^2)$ are two groups of initial values for 2D-TCLM. Two parameters of 2D-TCLM can be generated by

$$u_i = 0.4 + (u * a_i * 100 \mod 0.6) \tag{3}$$

where i is 1 or 2. Therefore, μ_1 and μ_2 are both within the range of $[0.4, 1]$ to guarantee that 2D-TCLM has extremely good chaos performance.

What should be noticed is that the decryption key is different from the encryption key. Suppose r_1 and r_2 are two randomly generated values in Random Number Insertion stage in the two rounds, the decryption key $K_d = (x_0^1,\ y_0^1,\ \mu,\ x_0^2,\ y_0^2,\ a_1,\ a_2,\ r_1,\ r_2)$.

B. Permutation

The permutation is to shuffle all the pixel positions within the image. Suppose the chaotic sequence S generated by 2D-TCLM has the size of $M \times N$. Its size is the same as the image. Sort each row and column of S, respectively to get the

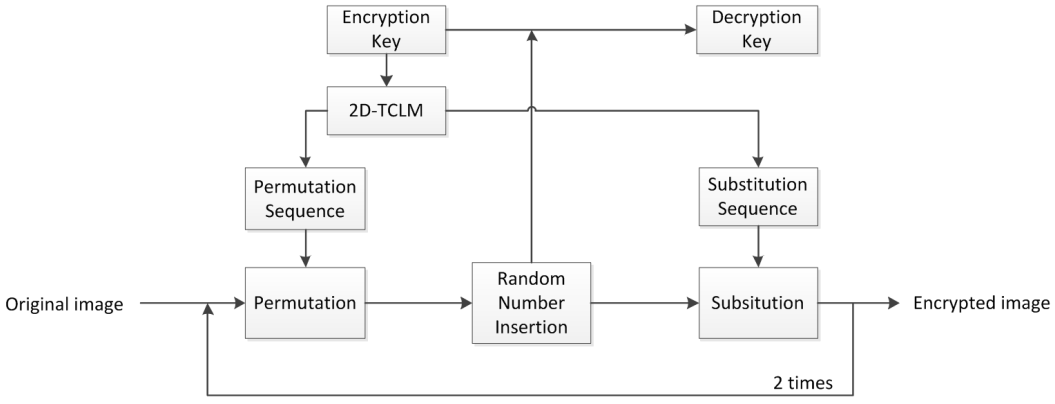

Fig. 2: The structure of proposed image encryption algorithm.

the row index matrix I_r and column index matrix I_c. Then the permutation of image P can be defined as

$$\begin{aligned} T(m,n) &= P(m, I_r(m,n)) \\ O(m,n) &= T(I_c(m,n), n) \end{aligned} \tag{4}$$

where $m \in [1, M]$ and $n \in [1, N]$. O is the permutation result. The detailed operation of permutation can be seen in Algorithm 1.

Algorithm 1. Permutation

Input: The original image P and chaotic matrix S with the size of $M \times N$.

Sort each row of S and get the row index matrix I_r;
Sort each column of S and obtain the column matrix I_c;
for $m = 1$ to M **do**
  for $n = 1$ to N **do**
    $T(m,n) = P(m, I_r(m,n))$;
  end for
end for
for $m = 1$ to M **do**
  for $n = 1$ to N **do**
    $O(m,n) = T(I_c(m,n), n)$;
  end for
end for

Output: The permutation result O.

C. Substitution

The substitution is to change all the pixel values randomly. For the permutation result O, chaotic sequence S, we first rearrange them with the size of $[1, MN]$, then the substitution is defined as

$$C(i) = \begin{cases} O(i) \oplus S(i) \oplus r & \text{if } i = 1 \\ O(i) \oplus S(i) \oplus C(i-1) & \text{if } i \in [2, MN] \end{cases} \tag{5}$$

where r is a random value that generated in the stage of Random Number Insertion and C is the operation result. Finally, rearrange C with the size of $[M, N]$. The detailed operation of substitution can be seen in Algorithm 2. After two times of operations, an original image can be encrypted into a random-like ciphertext image.

Algorithm 2. Substitution

Input: Random number r, the permutation result O and chaotic matrix S with the size of $M \times N$.

Rearrange O and S with the size of $[1, MN]$;
for $i = 1$ to MN **do**
  if $i = 1$ **then**
    $C(i) = O(i) \oplus S(i) \oplus r$;
  else
    $C(i) = O(i) \oplus S(i) \oplus C(i-1)$;
  end if
end for
Rearrange C with the size of $[M, N]$.

Output: The substitution result C.

IV. Simulation Results and Security Analysis

This section simulates the proposed image encryption algorithm using MATLAB software and analyzes its security performance.

A. Simulation results

A good image encryption algorithm should have the ability to encrypt different types of images into random-like images. Fig. 4 shows the simulation results of the proposed image encryption algorithm using the grayscale, binary and color images. As can be seen, all the original images' histograms have some patterns while their encrypted results' histograms look smooth. This means that the pixels of the encrypted images distribute randomly and the pixel numbers of different values are almost equal. Anyone can not get any useful information from the encrypted results by statistic their pixels.

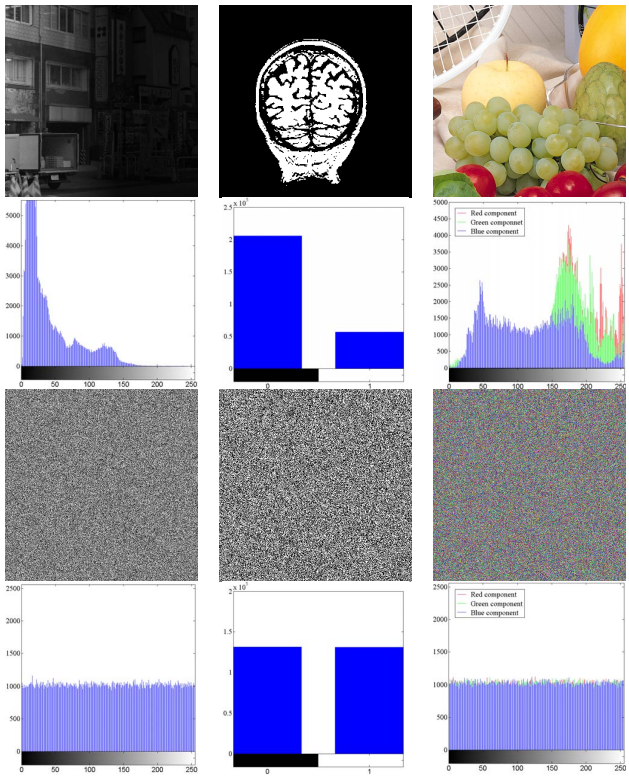

Fig. 4: Simulation results of different types of images. (1) The grayscale image; (b) the binary image; (c) the color image.

B. Security analysis

An image encryption algorithm is required to have high security so that it can resist all kinds of security attacks. Here, we use several methods to analyze the security performance of proposed image encryption algorithm. The images listed in Fig. 5 are used as the test images in the security analysis.

1) Security key analysis: The ciphertext images are transmitted in the public channel while the security key is transmitted through the private channel. Thus the security key should have a proper size and it must be sensitive to resist brute-force attack. Key sensitivity means that when a plaintext image

Fig. 5: The test images in the security analysis.

is encrypted by two keys with one bit difference will result in two totally different ciphertext images, and a ciphertext image can be only correctly reconstructed by the corresponding decryption key, other decryption keys that even have one bit difference with the correct key will result in different and unrecognized images.

Fig. 6 shows the key sensitivity analysis of the proposed image encryption algorithm in the encryption procedure. K_{e1} and K_{e2} are two encryption keys with one bit difference. As can be seen, when the original image P is encrypted by two encryption keys K_{e1} and K_{e2}, the two encrypted results (Fig. 6(b) and (c)) are totally different. Their difference can be seen in Fig. 6(d).

The key sensitivity in decryption procedure is shown in Fig. 7. Decryption keys K_{d1}, K_{d2} and K_{d3} are three decryption keys that also in one bit difference. K_{d1} corresponds to the encryption key K_{e1}. The original image can only be correctly reconstructed by the corresponding decryption key (see Fig. 7(a)). Even one bit difference of the decryption keys results in two completely different decrypted images, which can be seen from Fig. 7(d). Therefore, the proposed image encryption algorithm is very sensitive with its encryption and decryption keys.

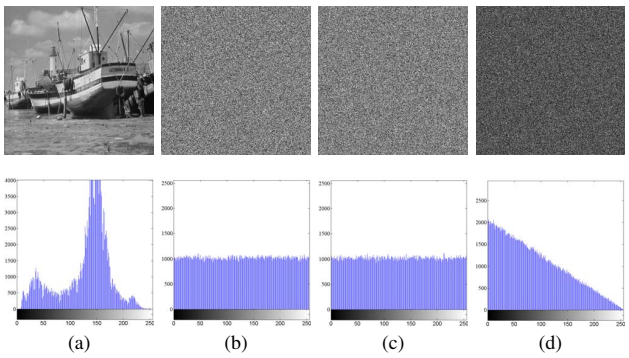

Fig. 6: Encryption key sensitivity analysis. (a) The original image P; (b) the encrypted result $C_1 = Enck(P, K_{e1})$; (c) the encrypted result $C_2 = Enck(P, K_{e2})$; (d) the difference between C_1 and C_2, $|C_1 - C_2|$.

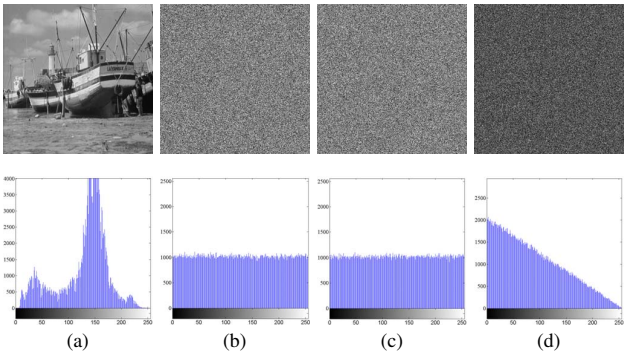

Fig. 7: Decryption key sensitivity analysis. The used ciphertext image C_1 is from Fig. 6(a). (a) The decrypted image $D_1 = Deck(C_1, K_{d1})$; (b) the decrypted image $D_2 = Deck(C_1, K_{d2})$; (c) the decrypted image $C_3 = Deck(C_1, K_{d3})$; (d) the difference between D_2 and D_3, $|D_2 - D_3|$.

2) Differential attack analysis: The differential attack is one of the most widely used and efficient security attack. The number of pixel change rate (NPCR) and uniformed average change intensity (UACI) are two measures that can be used to test whether an image encryption algorithm has the ability to resist differential attack. Suppose C_1 and C_2 are two encrypted images with size of $M \times N$. They are encrypted by the same key from two original images that in one pixel difference. The NPCR and UACI between C_1 and C_2 are defined by Eq. (6) and (7), respectively, where $L = MN$ is the number of pixels and T is the largest allowed pixel value in the image.

$$\text{NPCR}(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{D(i,j)}{L} \times 100\% \tag{6}$$

$$\text{UACI}(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{T \times L} \times 100\% \tag{7}$$

D is the step function that indicates the difference between C_1 and C_2. It is defined by

$$D(i,j) = \begin{cases} 0, & \text{if} \quad C_1(i,j) = C_2(i,j) \\ 1, & \text{if} \quad C_1(i,j) \neq C_2(i,j) \end{cases} \tag{8}$$

Fig. 8 shows the visual results of the differential attack analysis. In the experiment, an image is generated by randomly changing one pixel value of an original image. The difference of the two image can be seen in Fig. 8(c). The two images are then encrypted by the algorithm with a same key. The two encrypted results (Fig. 8(d) and (e)) are completely different, which can be seen from their difference in Fig. 8(f).

Table I lists the NPCR and UACI results of six original images shown in Fig. 5. The average NPCR and UACI values are 99.6145% and 33.4887%, respectively. They are very close to 99.609% and 33.464%, which are the NPCR and UAIC values between two independent random images [12]. Therefore, the proposed image encryption algorithm has good ability to resist differential attack.

3) Strict avalanche criterion: When two ciphertext images are encrypted from two original images with one bit difference using the same key, their difference can be calculated by NPCR

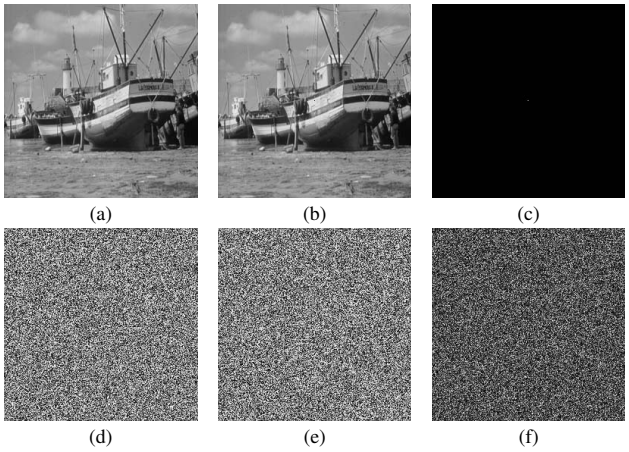

Fig. 8: Differential attack analysis. (a) The original image P_1; (b) an image P_2 generated by randomly changing one pixel of P_1; (c) the difference between (a) and (b); (d) the encrypted result $C_1 = Enck(P_1, K_e)$; (e) the encrypted result $C_2 = Enck(P_2, K_e)$; (f) the difference between C_1 and C_2, $|C_1 - C_2|$.

TABLE I: Neighboring pixels correlation values at different directions.

File name	NPCR (%)	UACI (%)	NBCR (%)
boat	99.6201	33.4934	49.9850
peppers	99.5991	33.4582	50.0009
house	99.6155	33.3863	49.9767
elaine	99.6136	33.4936	50.0257
lena	99.6292	33.5779	49.9365
cameraman	99.6094	33.5227	49.9475
Average	99.6145	33.4887	49.9787

and UACI in the pixel level and can be estimated by the strict avalanche criterion (SAC) [13] in the bit level. SAC tries to quantitatively reflect the avalanche phenomenon, which means that a little difference in the input can cause totally different outputs. From the principle of SAC, the number of bit change rate (NBCR) proposed in [14] can be used to measure the SAC performance of an image encryption algorithm. Suppose B_1 and B_2 are the bit streams of two ciphertext images that are encrypted from two plaintext images with one bit difference, NBCR between B_1 and B_2 is defined by

$$\text{NBCR}(B_1, B_2) = \frac{Hm[B_1, B_2]}{L_b} \times 100\% \qquad (9)$$

where $Hm[\cdot]$ is to calculate the Hamming distance of two bit streams and L_b is the length of B_1 or B_2. An image encryption algorithm has good avalanche phenomenon if the NBCR value close to 50% [14]. As can be seen from Table I, the average NBCR value of six original images is 49.9787%, which is very close to 50%.

V. Conclusion

This paper has introduced a 2D Tent-cascade-Logistic map (2D-TCLM). It has good chaos performance and is able to generate random and unpredictable chaotic sequences. Its trajectory and information entropy analysis have demonstrated its complex chaotic behaviors.

Based on 2D-TCLM, a new image encryption algorithm has also proposed. Simulation and security analysis have shown that the algorithm can encrypt different kinds of digital images into random-like images that can resist different attacks.

Acknowledgement

This work was supported in part by the Macau Science and Technology Development Fund under Grant FDCT/017/2012/A1 and by the Research Committee at University of Macau under Grants MYRG2014-00003-FST, MRG017/ZYC/2014/FST, MYRG113(Y1-L3)-FST12-ZYC and MRG001/ZYC/2013/FST.

References

[1] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, "Image encryption using the two-dimensional logistic chaotic map," *Journal of Electronic Imaging*, vol. 21, no. 1, pp. 013 014–1–013 014–15, 2012.

[2] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "A new 1D parameter-control chaotic framework," in *IS&T/SPIE Electronic Imaging*. International Society for Optics and Photonics, 2014, pp. 90 300M–90 300M–10.

[3] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A secret key cryptosystem by iterating a chaotic map," in *Advances in CryptologyEUROCRYPT91*. Springer, 1991, pp. 127–140.

[4] Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Transactions on Cybernetics*, no. 99, 2014.

[5] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Information Sciences*, vol. 297, no. 0, pp. 80–94, 2015.

[6] M. Franois, T. Grosges, D. Barchiesi, and R. Erra, "A new image encryption scheme based on a chaotic function," *Signal Processing: Image Communication*, no. 0.

[7] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, no. 0, pp. 172–182, 2014.

[8] C. Li, Y. Liu, L. Y. Zhang, and M. Z. Chen, "Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation," *International Journal of Bifurcation and Chaos*, vol. 23, no. 04, 2013.

[9] A. Skrobek, "Cryptanalysis of chaotic stream cipher," *Physics Letters A*, vol. 363, no. 12, pp. 84–90, 2007.

[10] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, and V. Fernandez, "On the security of a new image encryption scheme based on chaotic map lattices," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 18, no. 3, 2008.

[11] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "Image encryption using 2D Logistic-Sine chaotic map," in *2014 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, 2014, pp. 3229–3234.

[12] C. Fu, J. Chen, H. Zou, W. Meng, Y. Zhan, and Y. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," *Optics Express*, vol. 20, no. 3, pp. 2363–2378, 2012.

[13] R. Forré, "The strict avalanche criterion: spectral properties of boolean functions and an extended definition," in *Proceedings on Advances in cryptology*. Springer-Verlag New York, Inc., 1990, pp. 450–468.

[14] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Processing*, vol. 93, no. 11, pp. 3039–3052, 2013.