*International Journal of Engineering & Technology*, 7 (4) (2018) 4122-4126

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*
*doi: 10.14419/ijet. v7i4.19657*
***Research paper***

# A new double tent maps for satellite image encryption

**Ahlam R. Khekan ***

*Ministry of Higher Education and Science and Technology, Baghdad, Iraq*
**Corresponding author E-mail: ahlamr.khekan@outlook.com*

**Abstract**

This paper introduces a simple and effective chaotic system using a combination of two existing one-dimension (1D) Chaotic maps (seed maps). Simulations and performance evaluations show that the proposed system can produce Many 1D chaotic maps with larger chaotic ranges and better chaotic behaviors compared to their seed maps. To Investigate its applications in multimedia security; a novel image encryption algorithm is proposed using the same set of Security keys; this algorithm can generate a completely different encrypted image each time when it is applied to the same original image. Experiments and security analysis demonstrate the algorithm's excellent performance in image Encryption and various attacks. In conclusion, the proposed scheme is efficient in terms of sensitivity to the key, sensitivity to the ciphertext, good confusion, and diffusion. There is no possibility of an attacker breaking the cipher, as the scheme showed perfect confusion and diffusion properties, and can withstand known/chosen plaintext attacks.

***Keywords***: *Image Encryption; Chaotic Map; Satellite Image; Non-Linear Equation; Tent Map.*

## 1. Introduction

The need for information security has ever been increasing; the ancient people similarly faced the same issue of how to prevent transmitted information from leakage. Many cryptographic and steganographic methods have been proposed to deal with the problem of information leakage. However, the recent developments in the field of information technology have made it possible to use digital images such as medical images, grayscale image, color images, and binary images for the storage and transmission of important information. However, another challenge becomes how to protect the information stored in these images [1–3].

Several image encryption frameworks have been developed based on different technologies, such as SCAN[4,5], elliptic curve ElGamal [6], and Chaos[2], [7–9] with the consideration of the characteristics of digital images. But, the chaos-based image encryption technique has been one of the excellent and encryption methods from the host of other methods. This is due to the high sensitivity of the chaotic systems to their chaotic property, initial values and control parameters, state ergodicity, and non-convergence. This has resulted in the development of several chaotic-based image encryption algorithms through a direct utilization of the existing chaotic maps during their encryption processes [10]. Generally, there are two portions of a chaos-based image encryption framework: an image encryption system and a chaotic system.

In the image encryption system, the chaotic maps can be classified into one dimensional (1D) and multi-dimensional (MD) groups. The complex structure and multiple parameters of the MD chaotic maps have enhanced their applications in image security [11]. However, the implementation of the hardware/software of the MD chaotic systems are faced with increasing difficulty due to their multiple parameters [12]. Contrarily, the 1D chaotic systems are easy to implement due to their simple structure [13-14], but their limitations include a limited or/and discontinuous range of chaotic behaviors [15], ) non-uniform data distribution of output chaotic sequences, and susceptibility to low-computation-cost analysis using iteration and correlation function [13]. There is, therefore, a need to develop new chaotic maps that provide better chaotic performances. During the evaluation of an image encryption framework, the first and vital concern should be the security of the system. the security of various chaos-based image encryption frameworks are reportedly weak [16],[17] and to solve these problems, a new chaotic system with a simple structure is introduced in this paper. The introduced system investigates two of the existing 1D chaotic maps on the generation of random sequences. They tested systems profess excellent chaotic characteristics, including a uniform distributed variant density function and a wide range of parameter settings. The simulation and analysis of the three specific examples of the suggested chaotic system can verify these properties. Its application was demonstrated by the introduction of a new image encryption framework with excellent confusion and diffusion properties for resisting different attacks, especially the chosen-plaintext attacks. Upon a repeated application of the algorithm to an original image with the same set of security keys, a completely new encrypted image different from the previous one is generated. This evidenced the capability of the proposed algorithm to resist chosen-plaintext attacks.

The remaining parts of this paper are organized thus: Section 2 presents a brief analysis of the existing works on chaotic maps while section 3 provides the image encryption algorithm and the proposed pseudo-random number generator (PRNG). The results of the simulation studies are presented in section 4 while section 5 provides the conclusions from the study

## 2. Chaotic maps

In the group of chaotic maps, the ID maps have lots of applications because of their simple structures. In this section, we briefly review the Tent map as it will be used in the proposed encryption algorithm.

### 2.1. Tent map

The Tent map is known for its tent-like shape in the graph of its bifurcation diagram. It can be defined by equation (1).

$$X_{i+1} = \begin{cases} \omega X_i & \text{if } Y_i<0.5 \\ \omega(1 - X) & \text{otherwise,} \end{cases} \quad (1)$$

Where $Y_i \in [0,1], i \geq 0$ is the system parameter. This map turns an interval [0,1] against itself and consists of only one control parameter ω, where $\omega \in [0, 2]$. The group of actual values $Y_0, Y_1, \ldots, Y_n$ made up the systems' orbit, where $Y_0$ represents the initial value, and an orbit can be obtained for each $Y_i$. Based on the control parameter ω, various dynamical performances, ranging from chaotic to predictable, are shown in equation 1.
With positive Lyapunov exponents in the interval [1, 2], it indicates the system as chaotic and the acceptability of the signal in terms of traversal of the state, certainty, and mixing. Figure1 depicts the general shape of Lyapunov exponents for tent map.

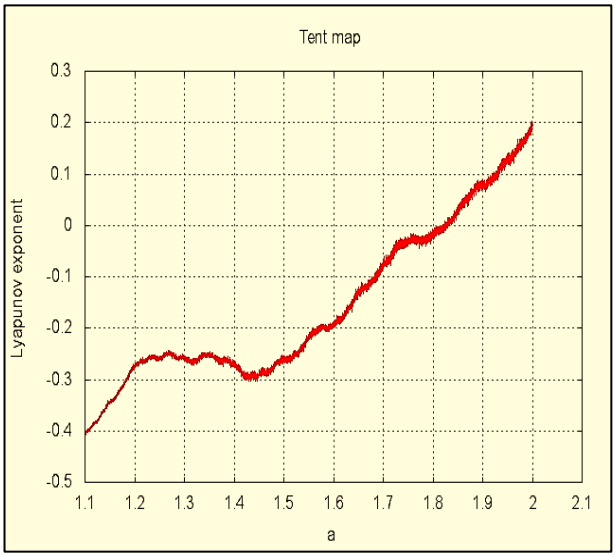


**Fig. 1:** The Tent Map Lyapunov Exponent.

With this map, the generated chaotic sequences are tended to hold a decent statistical asset. However, they are characterized by periodicity under finite precession. The value of ω is categorized into two scenarios as follow:

- A bigger value of ω translates into sequences with robust randomness
- A smaller value of ω translates into sequences with periodicity behavior.

Figure 3 is a bifurcation diagram which shows the value of the changing parameter. The figure shows the different characteristics for the values of the parameter ω on the horizontal axis and the possible long-term values of $X_n$ on the vertical axis.

## 3. The proposed algorithm

This section explains the proposed image encryption algorithm. It is divided into two main parts, the first section explains the proposed pseudo-random number generator while the second part illustrates the main steps of the encryption algorithm.

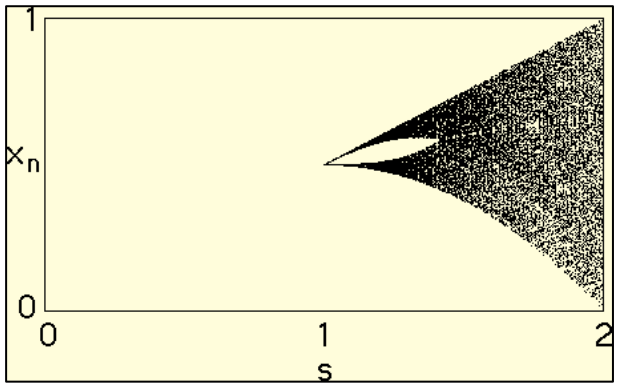


**Fig. 2:** Bifurcation of Tent Map.

### 3.1. Pseudo-random number generator (PRNG)

In this paper, a new PRNG based on double Tent map is proposed. The proposed PRNG generates a random sequence which represents the key used for the encryption algorithm. There are two reasons for using double or two Tent maps to generate the encryption key; first, the key space will be much higher than using one Tent map, meaning that the PRNG can resist brute force attack; second, using two 1D chaotic maps is much easier and faster than using one MD chaotic maps. The main block diagram of the proposed PRNG is given in Figure 3.

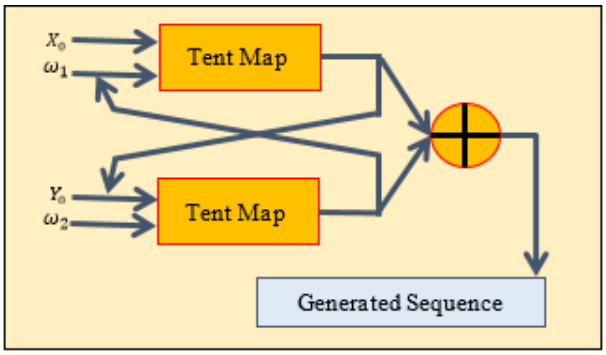


**Fig. 3:** The Proposed PRNG.

The proposed PRNG in this paper is called Double Tent Maps or 2TM. As can be seen, there are four input values, $\boldsymbol{X_0}$ and $\boldsymbol{Y_0}$ represent the initial values for both chaotic maps, while $\boldsymbol{\omega}$ represents the control parameter, which is a real value in the range [0, 2]. The initialization stage of 2TM consists of several steps as follows:
Step1. Read the initial values of $\boldsymbol{X_0}$ and $\boldsymbol{Y_0}$ for both chaotic maps.
Step2. Input the initial values for the control parameters $\boldsymbol{\omega_1}$ and $\boldsymbol{\omega_2}$.
Step3. Iterate both chaotic maps for t iterations.
In the next stage, the output from each chaotic map is used as an input to the other chaotic map. This enhances the randomization of the generated key and increases the key space. The outputs are converted into an integer, then, they are XORed together to generate a single integer. The length of the generated sequence is equal to the width or height of the image.

### 3.2. Proposed encryption algorithm

The main flowchart of the proposed encryption algorithm is given in Figure 4. In general, it consists of three main parts, key generating, confusion, and diffusion. In the first part, the key sequence is generated by using the proposed PRNG which has been explained in the previous subsection. The second part is responsible for changing the positions of the pixels based on the generated key. Finally, the diffusion part is responsible for changing the contents of each pixel.

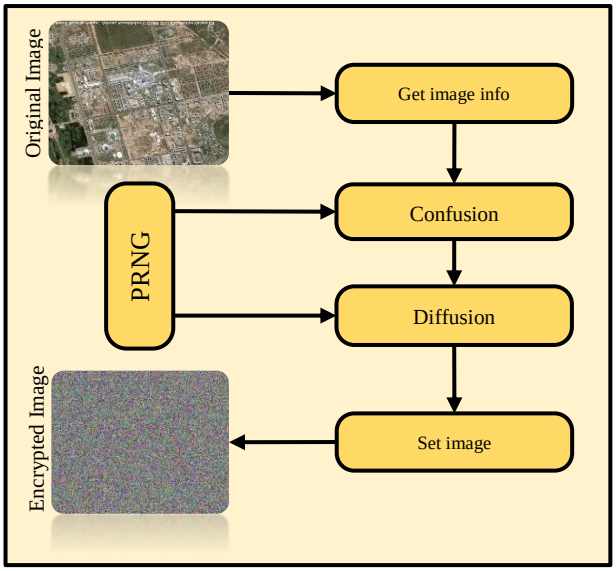


**Fig. 4:** Flowchart of the Encryption Algorithm.

#### 3.2.1. Confusion

As mentioned before, the confusion part is responsible for changing the positions of the pixels. The positions are shuffled based on the sequence generated by the PRNG as follows:

| Alg. Confusion | |
|---|---|
| 1. | Start |
| 2. | Img = Get the positions |
| 3. | Key = Generate the PRNG |
| 4. | N = Size(Img) |
| 5. | For p = 1 To N |
| 6. | Img[p] = Img[Key[p]] |
| 7. | Next p |
| 8. | End |

**Fig. 5:** Confusion Algorithm.

#### 3.2.1. Diffusion

In the diffusion algorithm, the final cipher image is generated. An XOR operator is implemented on the confused image which has been produced by the previous step. The diffusion algorithm is given in the following pseudo-code:

| Alg. Diffusion | |
|---|---|
| 1. | Start |
| 2. | Img = Get the Pixles |
| 3. | Key = Generate the PRNG |
| 4. | N = Size(Img) |
| 5. | For p = 1 To N |
| . | EncImg[p] = Img[p] ⊕ Key[p] |
| 7. | Next p |
| 8. | End |

**Fig. 6:** Confusion Algorithm.

## 4. Results

The proposed image encryption algorithm can provide a high level of security to different types of images, such as grayscale images, color images, biometrics, and binary images. For grey scale images, we use the proposed algorithm to encrypt the pixels and then combine them to obtain the encrypted image.

The algorithm has been implemented by using Microsoft C#.net version 6.0, visual studio 2017. The computational platform is Microsoft Windows 10 with Intel Core i٥, CPU 2.٤ GHz, and EMS memory 4 GB. Table 1 shows the key parameters with the values used in the implementation.

**Table 1:** Parameters Values for the Experiments

| Parameter | Symbol | Value |
|---|---|---|
| Mutation "TM" | $\omega_1$ | 1.9999998654 |
| Mutation "TM" | $\omega_2$ | 1.9999998654 |
| Initial Value $X_0$ | $Y_R$ | 0.348795124 |
| Initial Value $Y_0$ | $Y_G$ | 0.76548123 |

### 4.1. Key space analysis

As per [18], a key space size must contain > $2^{128}$ possible keys because if the keyspace is small, the system can be prone to a brute-force attack. Nevertheless, the sequence produced by the proposed system depends on the control parameters and the initial states. The encryption algorithm with the PRNG is applied in C# with 10-14 precision. For the PRNG method, two initial values $X_0 \in [0,1]$ and $Y_0 \in [0,1]$ for the two chaotic maps and two control parameters $\mu \in [0,4], \omega \in [0,2]$ were used. Therefore, the proposed PRNG has a key space which can be calculated thus:

$$(10^{14}) \times (10^{14}) \times (10^{14}) \times (10^{14}) = 8 \times 10^{56} \cong 2^{208}$$

Additionally, the result from the above calculation above is only for one generated sequence; however, three different sequences are generated by the proposed PRNG within the encryption algorithm. The above calculation demonstrated the suitability of the key space of the proposed PRNG and indicated that all the produced keys are strong. Table 2 presents a comparison of the key space of the proposed algorithm with the PRNG of other algorithms. The table showed that the key space of the proposed method is significantly larger towards withstanding any form of brute-force attack.

**Table 2:** The Key Space Results

| PRNG | Key Space |
|---|---|
| Proposed Method | $2^{208}$ |
| [19] | $2^{128}$ |
| [20] | $2^{186}$ |
| [21] | $2^{144}$ |
| [22] | $2^{159}$ |
| [23] | $2^{183}$ |

### 4.2. Histogram analysis

The histogram in Figures 7A and 7B show the pixel distribution in an image obtained by plotting the pixel number at each level of color intensity. The figures respectively showed the histogram of the original image and the encrypted image.

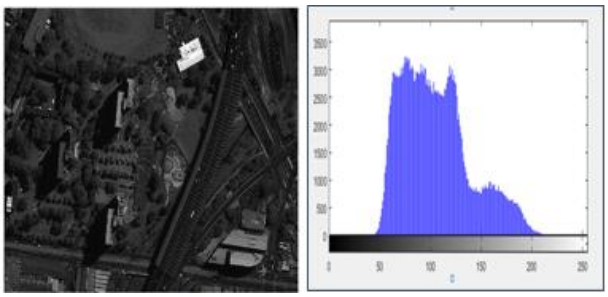

**Fig. 7:** A) Histogram of the Original Image.

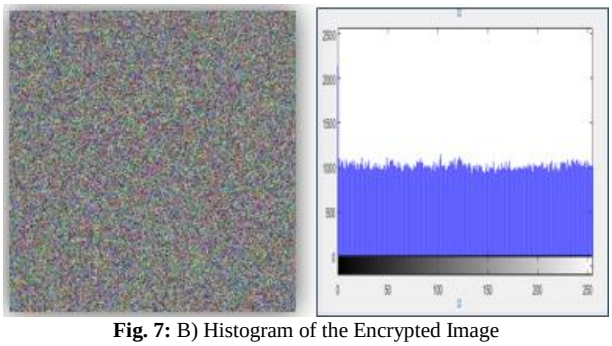

**Fig. 7:** B) Histogram of the Encrypted Image

### 4.3. Information entropy

Entropy refers to the measure of uncertainty and can be used to express the uncertainties in the information of an image. An entropy analysis can also determine the color-level distribution values in an image. If the gray-level values are uniformly distributed, there will be a greater entropy and a higher entropy value is an indication of a better-secure encryption. Entropy is calculated as follows:

$$H\ (S) = \sum_{i=0}^{2^M-1} P(S_i)\ log_2 \frac{1}{P(S_i)}$$

Where $P(S_i)$ is the probability of $S_i$, while $2^M$ is the state of the total source of information. An image is truly random (RI) if its pixel intensities are uniform in the range of [0, 255], i.e., $P(RI)$= 1/256 for all $i \in [0, 255]$, hence, $H(RI)$= 8 bits. This means that an ideally random image has an entropy information value of 8.

The entropy information values of the Lena image (plain-image) and its respective cipher images are computed in this study and Table 5 presents the results of the computation. The obtained entropy values are close to the theoretical entropy value of H = 8 for an ideal random image, suggesting a negligible information leakage during the encryption process, as well as the closeness of the cipher-image to a random source. A comparison to the existing algorithms based on the Lena image in Table 5 shows the proposed algorithm to be closer to the ideal situation compared to the other algorithms (as the output is similar to a random output). Hence, the new encryption algorithm could be considered secure against entropy attacks.

**Table 3:** The Entropy

| Algorithm | Entropy of Cipher Image |
|---|---|
| Proposed Algorithm | 7.9971 |
| [24] | 7.9808 |
| [25] | 7.9901 |
| [26] | 7.9975 |
| [27] | 7.9914 |

### 4.4. Speed analysis

Several factors such as like programming language, operating system, hardware specifications, and programming skills determine the speed of the algorithm or its execution time. Thus, a comparison of the proposed algorithm against two or more encryption algorithms is baseless unless using the same environment. In this study, a computer with 4 GB RAM and core i5 with 2.4GHz running on Windows 10 have been used while the programming language for this project is C#.net version 6 with dot net framework version 4.6. The execution time of the proposed algorithm is measured by running the algorithm severally to get the average execution time. As such, the algorithm requires about 360ms to encrypt the original image. The speed analysis shows that the confusion stage in the algorithm takes around 60% of the computed speed because of using nested loops. However, the algorithm takes around 15% and the diffusion stage takes 20%. The rest of the time is spent on reading from and writing to the image (i.e. RGB colors). This analysis projects the proposed algorithm as a fast system which can be used for several real-world applications.

## 5. Conclusion

In this paper, the designing of a new chaotic-based PRNG proposed for the enhancement of colored images encryption algorithms was presented. The proposed framework achieved a better diffusion and confusion. Based on several simulations and analyses such as statistical, differential, quality, contrast and speed analyses, the system was demonstrated to be secure and with a better performance. The proposed PRNG demonstrated its capability of generating several pseudo-random sequences which can be implemented in several cryptographic platforms. The advantages of the proposed PRNG include an adaptive keyspace size, quality pseudo-random sequences, good sensitivity to initial keys, and less computational complexity.

## References


[1] X.J. Tong, Z. Wang, M. Zhang, Y. Liu, H. Xu, J. Ma, An image encryption algorithm based on the perturbed high-dimensional chaotic map, Nonlinear Dyn.80 (2015) 1493–1508. https://doi.org/10.1007/s11071-015-1957-9.

[2] W. Liu, K. Sun, C. Zhu, A fast image encryption algorithm based on chaotic map, Opt. Lasers Eng. 84 (2016) 26–36. https://doi.org/10.1016/j.optlaseng.2016.03.019.

[3] L. Wang, H. Song, P. Liu, A novel hybrid color image encryption algorithm using two complex chaotic systems, Opt. Lasers Eng. 77 (2016) 118–125. https://doi.org/10.1016/j.optlaseng.2015.07.015.

[4] R.J. Chen, S.J. Horng, Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata, Signal Process. Image Commun. (2010). https://doi.org/10.1016/j.image.2010.03.002.

[5] S.S. Maniccam, N.G. Bourbakis, Image and video encryption using SCAN patterns, Pattern Recognit. (2004). https://doi.org/10.1016/j.patcog.2003.08.011.

[6] L. Li, A.A. Abd El-Latif, X. Niu, Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images, Signal Processing. (2012). https://doi.org/10.1016/j.sigpro.2011.10.020.

[7] S. Lian, Efficient image or video encryption based on spatiotemporal chaos system, Chaos, Solitons & Fractals.40 (2009) 2509–2519. https://doi.org/10.1016/j.chaos.2007.10.054.

[8] I. Cicek, A.E. Pusane, G. Dundar, A novel design method for discrete time chaos based true random number generators, Integr. VLSI J. 47 (2014) 38–47. https://doi.org/10.1016/j.vlsi.2013.06.003.

[9] Z.-H. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, Phys. Lett. A. 346 (2005) 153–157 https://doi.org/10.1016/j.physleta.2005.08.006.

[10] A.A.A. El-Latif, L. Li, N. Wang, X. Niu, Image encryption scheme of pixel bit based on combination of chaotic systems, in: Proc. - 7th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIHMSP 2011, 2011. https://doi.org/10.1109/IIHMSP.2011.67.

[11] A. Kanso, M. Ghebleh, A novel image encryption algorithm based on a 3D chaotic map, Commun. Nonlinear Sci. Numer. Simul.17 (2012) 2943–2959. https://doi.org/10.1016/j.cnsns.2011.11.030.

[12] G. Ye, Image scrambling encryption algorithm of pixel bit based on chaos map, Pattern Recognit. Lett.31 (2010) 347–354. https://doi.org/10.1016/j.patrec.2009.11.008.

[13] Y. Zhou, L. Bao, C.L.P. Chen, A New 1D Chaotic System for Image Encryption, Signal Processing. 00 (2014) 1–21. https://doi.org/10.1016/j.sigpro.2013.10.034.

[14] Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique Nidhi Sethi, 2013 (2013) 46–50.

[15] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, Image Vis. Comput.27 (2009) 1371–1381. https://doi.org/10.1016/j.imavis.2008.12.008.

[16] A.G. Radwan, S.H. AbdElHaleem, S.K. Abd-El-Hafiz, Symmetric encryption algorithms using chaotic and non-chaotic generators: A review, J. Adv. Res. 7 (2016) 193–208. https://doi.org/10.1016/j.jare.2015.07.002.

[17] M. Kumar, A. Aggarwal, A. Garg, a Review on Various Digital Image Encryption Techniques and Security Criteria, Int. J. Comput. Appl. 96 (2014) 19–26.

[18] I. ECRYPT, Ecrypt II Yearly Report on Algorithms and Keysizes (2010-2011), 2011.

[19] M.A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, R. Méndez-Ramírez, A novel pseudorandom number generator based on pseudorandomly enhanced logistic map, Nonlinear Dyn.87 (2017) 407–425. https://doi.org/10.1007/s11071-016-3051-3.

[20] Y. Wang, Z. Liu, J. Ma, H. He, A pseudorandom number generator based on piecewise logistic map, Nonlinear Dyn.83 (2016) 2373–2391. https://doi.org/10.1007/s11071-015-2488-0.

[21] M. Kumar, A. Iqbal, P. Kumar, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Dif fi e – Hellman cryptography, Signal Processing.125 (2016) 187–202. https://doi.org/10.1016/j.sigpro.2016.01.017.

[22] M. García-Martínez, E. Campos-Cantón, Pseudo-random bit generator based on multim-modal maps, Nonlinear Dyn.82 (2015) 2119–2131. https://doi.org/10.1007/s11071-015-2303-y.

[23] B. Stoyanov, K. Kordov, Novel secure pseudo-random number generation scheme based on two tinkerbell maps, Adv. Stud. Theor. Phys. 9 (2015) 411–421. https://doi.org/10.12988/astp.2015.5342.

[24] H. Liu, A. Kadir, P. Gong, A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise, Opt. Commun.338 (2015) 340–347. https://doi.org/10.1016/j.optcom.2014.10.021.

[25] C. Dong, Color image encryption using one-time keys and coupled chaotic systems, Signal Process. Image Commun.29 (2014) 628–640. https://doi.org/10.1016/j.image.2013.09.006.
[26] R. Parvaz, M. Zarebnia, A combination chaotic system and application in color image encryption, Opt. Laser Technol. 101 (2018) 30–41. https://doi.org/10.1016/j.optlastec.2017.10.024.
[27] X. Wu, D. Wang, J. Kurths, H. Kan, A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system, 350 (2016) 137–153. https://doi.org/10.1016/j.ins.2016.02.041.