Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/120308

An Effective Chaotic Image Encryption Algorithm Based on Piecewise Non-linear Chaotic Map

A. A. Abu-Ein

Department of Electrical Engineering, Al-Balqa Applied University, Irbid, Jordan

Received: 22 Aug. 2022, Revised: 27 Sep.2022, Accepted: 14 Oct. 2022.
Published online:1 Mar. 2023.

Abstract: Recent years have seen an increasing number of discrete chaotic algorithms proposed. In spite of this, most of them have issues, such as security or lack of robustness. The dynamic image encryption system presented here is based on one-dimensional non-linear chaotic maps. Stable period-one fixed point or ergodic properties distinguish this dynamical system from other types. They undergo bifurcation from a stable single periodic state to a chaotic one, without undergoing the conventional period doubling. KS-entropy for this map is also shown in relation to the control parameter. Encryption failures, such as a low level of security, a low speed of encryption, and key space, are addressed by this scheme's design.

Keywords: Chaotic maps; Image Encryption; Piecewise non-linear maps; Cryptography; KS-entropy; Security analysis.

1 Introduction

Chaotic systems exhibit a variety of intriguing properties, including their sensitivity to control parameters and initial conditions, their ergodicity, mixing, and exactness properties, and so on [1,2]. Pseudo-random coding (i.e., chaotic) and cryptography have some requirements that can be linked to almost any property [3,4,5,6]. Figure 1 illustrates the connection between cryptography encryption system and chaotic system (i.e., Pseudo-random coding). The properties of chaotic and cryptographic systems are shown in the Table 1[7,8] (Al-Hazaimeh,2021).

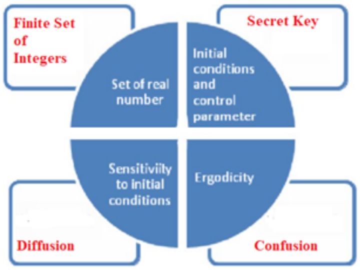


Fig. 1. Interaction of chaotic systems and cryptography.

There has been an increase in interest in the field of chaotic cryptography during the 1990s, which has resulted in numerous systems for analog and digital chaotic encryption being suggested [9,10,11,12] and analyzed [13,14]. Consider, for instance, by utilizing the Beta function, Zahmoul et al. (2017) suggested a novel chaotic mapping [15]. By combining two random hyper-chaotic systems, Zhu et al. (2017) came up with a novel hyper-chaotic system [16]. Natiq et al. (2018) described a novel three-dimensional multi-attribute chaotic system (i.e., 3-MACS) with hidden attractors and self-excited [17]. Using the Residue Number System (i.e., RNS), Michaels and Chester (2012) developed a way for creating a digital chaotic system [18].

Table 1: Chaotic Systems versus Cryptographic systems - A Comparison.

Cryptographic	Chaotic	Description
Round	Iteration	A set number of computer instructions until a condition is met
Keys	Parameters	A minor change in the system parameters can result in a significant change in the output.
Confusion	Ergodicity	For each given input, the output will be distributed in the same way.
Diffusion	Sensitivity to	A tiny adjustment in the input can have a significant impact on the output.

[*] Corresponding author e-mail: ashrafabuein@yahoo.com

	initial condition	
Algorithm complexity	Structure complexity	The complexity of a simple procedure is extremely high.
Randomness	Dynamic	It's possible for a deterministic process to exhibit random-like behavior.

The goal of this research is to go over digital cryptosystems. As a result of their intrinsic chaotic properties, many different zero-watermarking approaches and picture encryption algorithms based on conventional chaotic mappings, such as Tent, Sine, piecewise linear, and Logistic mappings, have been described [19,20]. Indeed, these are the most basic chaotic systems (i.e., simplest). Numerous cryptosystems based on logistic maps [21], piecewise linear maps [22], and piecewise non-linear maps have been presented in recent years [23]. Table 2 examines the characteristics of various picture encryption techniques based on chaotic maps [24].

Table 2: Comparison of image encryption schemes.

Schemes	Chaotic Maps	Weaknesses	Strength
[25]	Chaotic Maps (Trigonometric)	The PRNS exhibits extremely little randomness [26].	- Large key space - High-level security
[27]	Chaotic standard and		- Extremely fast - Structured simply
[28]	logistic maps	The plain-image change is not sensitive enough [26].	- Extremely fast - Structured simply - Large key space
[29]	logistic maps (Two chaotic maps)	The percentage of weak and invalid keys [26].	- Simple mixture - Less time complexity
[30]	Logistic and chaotic standard maps	Vulnerable to chosen plaintext and known plaintext attacks [7].	- A powerful tool for generating a great deal of confusion. - Extremely fast
[21]	Logistic, tent, sine, and cubic mappings	There are a large number of broken keys [7].	- Constructed simply - Secret key is implied by using chaotic system's initial condition.

Piecewise linear chaotic maps exhibit ideal dynamical features and are easily implemented in software and hardware. They are frequently employed in chaotic digital ciphers [31]. Despite the efficiency and simplicity that a one-dimensional (i.e., 1-D) chaotic system provides [32], it has fundamental disadvantages, including a weak security function, slow performance (i.e., speed), and a small key space [33].

To address some of the drawbacks of piecewise linear chaotic maps, piecewise non-linear chaotic maps are introduced. In addition to the control parameter and the initial condition, our piecewise non-linear chaotic maps cryptosystem incorporates a third component, probability. More than two parameters appear to increase the level of diffusion and confusion during the encryption process, resulting in a more secure cryptosystem. To further enhance the security of cryptosystems, we link additional chaotic maps (i.e., trigonometric) to the non-linear piecewise chaotic mappings. Adding two parameters to the chaotic map (i.e., trigonometric), in addition to the parameters of piecewise chaotic maps, has expanded the key space.

The following is the structure of this paper. Preliminary knowledge is introduced in Section 1. In Section 2, we'll focus on the algorithm we've developed. Sections 3 show the findings of the experiments and the security analysis. In the final section, there is a brief conclusion.

2 Proposed schemes

One-parameter non-linear chaotic maps with an invariant measure are first discussed in this paper. These maps can be classified as [34]:

$$\emptyset(x,\alpha)=\frac{\alpha^2 F}{1+(\alpha^2-1)F'} \quad (1)$$

We utilized the following identity to derive the aforementioned formula:

$$F=\begin{cases}\frac{x}{p}, 0\leq x\leq p, p\in[0,1]\\ \frac{x-p}{1-p}, p\leq x\leq 1, p\in[0,1]\end{cases}$$ (2)The definition of an invariant measure is [34]:

$$\mu(x,\alpha,p)=\frac{1-\alpha}{x-\alpha x+\ln(1-p)[\alpha-p]+\ln(\alpha-p)[p-\alpha]}, \alpha>p. \quad (3)$$

The "Kolmogorov-Sinai" (i.e., KS) Entropy can be calculated as follows [34]:

$$h(\mu, g(x,a,N)) = \int \mu(x)\,dx \ln\left|\frac{dx_{n+1}}{dx_n}\right| = \int_{-\infty}^{+\infty} \mu(x) dx \ln\left|\frac{d}{d_x} g(x,a,N)\right| \tag{4}$$

As an alternative, it can be referred to as

$$h(\mu, g(x,a,N)) = \int_{-\infty}^{+\infty} \frac{\sqrt{\beta}}{\pi\beta x^2+\pi} dx\,[lnN - lna + \ln(1+a^2y^2) - \ln(1+x^2)] \tag{5}$$

The invariant measure Eq. (3) can be used to calculate KS-entropy, leading to [34]:

$$h_{KS} = \frac{1}{\ln(\frac{1-p}{\alpha-p})}[ln\alpha(1-p)\{ln\alpha + lnp + \ln(1-p) - 2\} - \ln(\alpha - p)\{ln\alpha - lnp\} - 2\left[\ln(\alpha p)\ln(1-p) - lnp\,ln\alpha + li_2\frac{\alpha p - p}{\alpha}\right] - [\ln^2(1-p) - \ln^2\alpha(1-p)]]\,. \tag{6}$$

Two chaotic maps are used in the proposed scheme to accomplish the goal of image encryption. In order to use our proposed scheme, we begin by transforming the plain text M_{mxn} into $M_{(mxn)x1}$. P's probabilistic parameter is then constructed by iterating over the chaotic map in Eqs. (7-8) and utilizing the results. Consider the following formulas as an illustration:

$$x_1{}'(n+1) = \alpha_2^{-1}\tan^2(N\,tan^{-1}\sqrt{x_1(n)} \tag{7}$$

$$p = \begin{cases} x_1, 0 < x \le 1 \\ \frac{1}{x}, x > 1 \end{cases} \tag{8}$$

The piecewise mappings are now defined in terms of Eq. (2) as

$$\Phi(x_2, \alpha_2, p) = \begin{cases} \frac{\alpha_2^2 x_2}{p + \alpha_2^2 x_2 - x_2}, 0 \le x_2 \le p, & (1) \\ \frac{\alpha_2^2(x-p)}{\alpha_2^2 x - p\alpha_2^2 - x + 1}, p \le x_2 \le 1. & (2) \end{cases} \tag{9}$$

Piecewise mappings Eq. (9) are used to encrypt the produced matrix.

$$Ci = (\lfloor x_2 X\,10^{14} \rfloor \bmod 256)\ XOR\ M_{iX1}\,. \tag{10}$$

It should be noted that x_2 is the outcome of iteration of the piecewise non-linear chaotic maps. The parameters of the chaotic map (x_1 and α_1) are then adjusted through the use of simple functions ($x_1 = f(x_2, C_i), \alpha_1 = g(x_2, C_i)$). The method of decryption is nearly identical to that of encryption, except that the processes are reversed as shown in Figure 2.

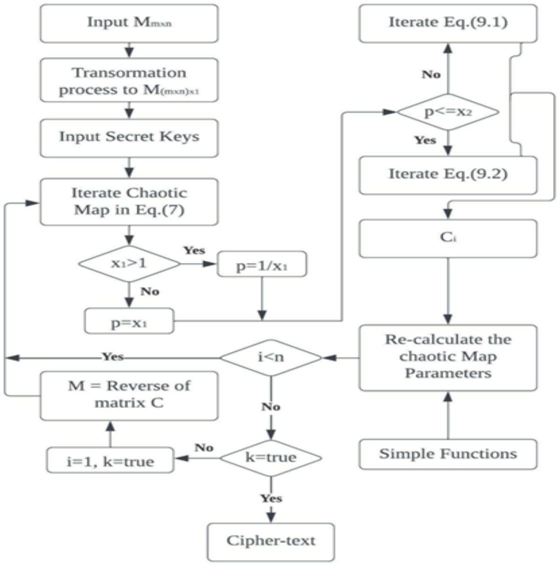


Fig. 2. The diagram of proposed image encryption.

3 Simulation experiments and security analysis

MATLAB R2021a on a machine with a 2.42 GHz CPU, 8.00 GB of memory, and Microsoft Windows 10 Pro as the operating system is used to run many experiments to verify the effectiveness of the suggested encryption algorithm. The Girl, Lena, Finger, and Iris test images (256 x 256 of size) presented in Figure3are chosen as illustrative examples in the experimental analysis. Our visual results for the Girl and Finger images exclusively, due to the similarity of the results for the other test images.

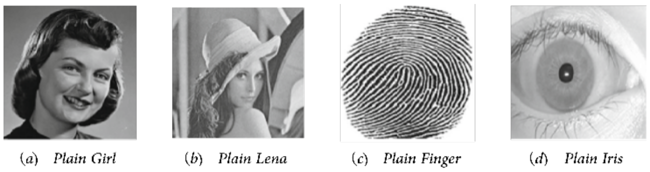

(a) Plain Girl (b) Plain Lena (c) Plain Finger (d) Plain Iris

Fig. 3. Images for testing.

Images of a Girl and a Finger were encrypted with different keys and shown in Figure 4. If you look at it visually, it's clear that the proposed scheme is capable of disguising plain-text images (conceal the plain-text image's texture).

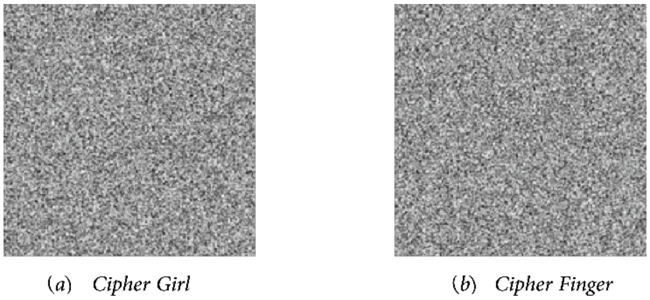

(a) Cipher Girl (b) Cipher Finger

Fig. 4. Encryption results with $x_1 = 9.7, \alpha_1 = 6.5, x_2 = 0.2, \alpha_2 = 0.4$.

Image encryption schemes cannot be judged only based on their appearance. You should consider a number of different security measures when trying to quantify the degree of encryption. It will be examined and analyzed in the next sections.

3.1 Histogram analysis

Gray scale distributions, or histograms, show the distribution of pixel values in an image. A plain-text image's histogram should be completely distinct from an encrypted image's histogram in order to prevent statistical attacks [35,36,37]. Afterward, we encrypt the image of a Girl and plot the histograms. The plain-text image of a Girl's histogram is depicted in Figure 5-a. Figure 5-b shows the encrypted image's histogram using the proposed scheme.

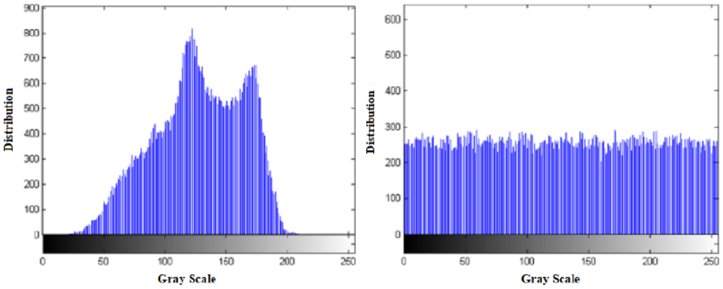


Fig. 5. The histograms analysis.

It is difficult for an intruder (i.e., 3rd party) to perform a successful statistical attack (i.e., analysis) on the encrypted image (i.e., cipher) of the proposed system since the cipher-text image's histograms pretty uniform.

3.2 PSNR analysis

"Peak signal-to-noise ratio" (i.e., PSNR) is a statistic that measures the difference between plain-text and cipher-text images [7]. When a plain-text image is used as the signal and a cipher-text image as the noise, this metric can be used as a factor in the evaluation of security. A greater PSNR value indicates that the plain-text image is very similar to the encrypted image (i.e., cipher-text), which is undesirable in any encryption technique. The following formula can be used to determine PSNR [7]:

$$PSNR = 20\ X \log_{10}\left(\frac{I_{max}}{\sqrt{MES}}\right) \quad (11)$$

$I_{max}$is the highest gray scale value of a plain-text image, and MSE is the "cumulative squared error" between plain-text and cipher-text, MES can be written as:

$$MES = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(I(i,j) - C(i,j))^2\,\pi r^2 \quad (12)$$

Table 3 shows the PSNR metric's outcome. A comparison of two other methods shows that the proposed algorithm has a lower PSNR value than any of them.

Table 3: PSNR (dB) results.

Test images	Schemes		
	[38]	[39]	Proposed
Girl	15.3412	9.9811	7.9583
Lena	14.1954	9.1091	7.6334
Finger	15.7234	8.9910	7.9791
Iris	15.9871	8.9878	7.8815

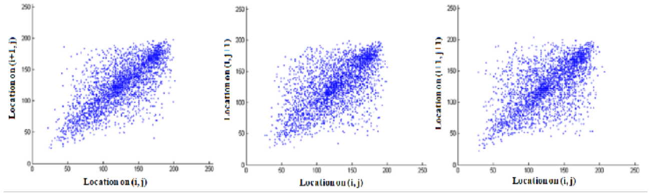
3.3 Two adjacent pixels-based correlation analysis

Correlation coefficients between neighboring pixels in a cipher-text image are one of the primary metrics used to quantify the image's diffusion and confusion features [7]. The following approach is used to determine the correlation coefficient between two neighboring pixels (i.e., horizontally, vertically, and diagonally). 2000 pairs of adjacent plain-text and cipher-text images in all directions (i.e., diagonal, vertical, and horizontal) are randomly selected. In order to figure out the correlation coefficient, two discrete formulas must be employed as below:

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}X\sqrt{D(y)}} \quad (13)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (14)$$

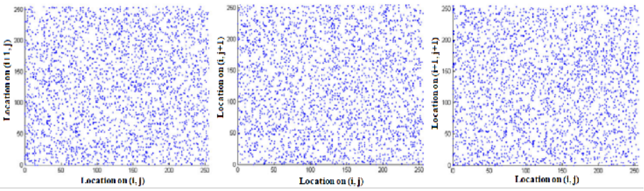
As demonstrated in Figure 6, two adjacent pixels on either side of each other in the original Girl image are correlated. All three directions of correlation (i.e., horizontal, vertical, and diagonal) can be seen from Figure 6 respectively.



(*a*) *Horizontal* (*b*) *Vertical* (*c*) *Diagonal*

Fig. 6. Girl plain-text image pixel by pixel plotting.

Figure 7 shows the correlation analysis plots when the Girl image is encrypted using the suggested technique. There are no discernible patterns in the cipher-text image's plots. The results for Lena, Finger, and Iris images are similar to those for Girl image.



(*a*) *Horizontal* (*b*) *Vertical* (*c*) *Diagonal*

Fig. 7. Girl cipher-text image pixel by pixel plotting.

Table 4's quantitative study of cipher-text images shows that the proposed scheme has virtually zero correlation coefficients with the methods proposed in [38,39]. It demonstrates that the proposed system is secure (i.e., high security level).

Table 4: Two adjacent pixels' correlation coefficient.

Test image	Direction	Schemes			
		[38]	[39]	Proposed	Plain-text
Girl	Vertical	0.0216	0.0119	0.0041	0.9499
	Horizontal	0.9427	0.0353	0.0051	0.9227
	Diagonal	0.0317	-0.0921	0.0011	0.9855
Lena	Vertical	0.0295	0.0120	0.0063	0.8753
	Horizontal	0.9312	0.0127	0.0056	0.9283
	Diagonal	0.0168	0.0176	0.0034	0.8881
Finger	Vertical	-0.0289	0.0891	0.0026	0.9115
	Horizontal	0.9378	0.0327	0.0062	0.9457
	Diagonal	0.0121	0.0091	0.0041	0.8901
Iris	Vertical	0.0296	-0.0264	0.0045	0.9193
	Horizontal	0.9423	0.0221	0.0026	0.9867
	Diagonal	-0.0193	0.0174	0.0019	0.8457

3.4 Key sensitivity analysis

Encryption algorithms are only as strong as their keys, and this is where the importance of key sensitivity comes into play. Small changes in the keys (i.e., a single bit flip) should result in dramatic changes in the output [6,40,41]. The key sensitivity of the proposed scheme is highlighted in Figures 8 and 9. Figures 8 and 9 shows that even a tiny change in and can have a substantial impact on the cipher-text image it corresponds to.

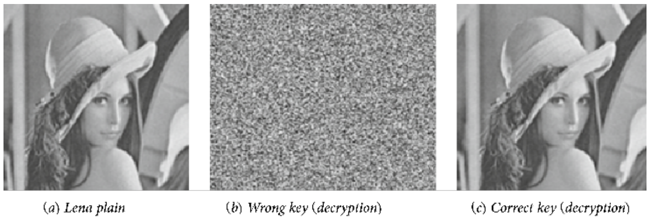

(a) Lena plain
(b) Wrong key (decryption)
(c) Correct key (decryption)

Fig. 8. Key sensitivity of plain.

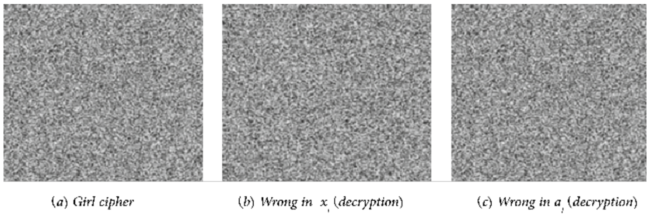

(a) Girl cipher
(b) Wrong in x_i (decryption)
(c) Wrong in a_i (decryption)

Fig. 9. Key sensitivity of cipher.

3.5 Time analysis

Minimal resources and computing time are necessary for an efficient method. We have summarized the findings of the proposed, [38], and [39] schemes in Table 4 to demonstrate their computational complexity. Table 4 displays the amount of time it takes to encrypt plaintext images. Decryption takes almost as long as encryption because it is an inverse operation. Table 5 shows that the proposed scheme has a lower computational complexity than other schemes, as shown.

Table 5: Time analysis.

Test images	Schemes		
	[38]	[39]	Proposed
Girl	3.47 Sec.	11.42 Sec.	1.73 Sec.
Lena	3.23 Sec.	11.12 Sec.	1.57 Sec.
Finger	3.44 Sec.	11.30 Sec.	1.98 Sec.
Iris	3.26 Sec.	11.12 Sec.	2.08 Sec.

3.6 Key space analysis

The number of keys that can be utilized in a cryptosystem's encryption and decryption is known as the key space size. The amount of key space available can be used to estimate an encryption algorithm's strength. According to Alvarez and Li (2006), a key space of at least 2^{100} is required to prevent a brute force attack. In the proposed scheme, Initial conditions and control parameters are specified with a precision of 10^{-14}, and the size of the key space for these parameters and conditions is 2^{186} [42]. Therefore, this large key space can resist any brute force attack.

3.7 Plain-text and cipher-text images- Based correlations analysis

An analysis of the correspondence between plaintext and encrypted images can be performed by computing the two-dimensional correlation. Formula for calculating correlation coefficient is given below [43,44]:

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_{ij}-I')(C_{ij}-C')}{\sqrt{\left(\sum_{i=1}^{M}\sum_{i=1}^{N}(I_{ij}-I'_{ij})^2\right)\left(\sum_{i=1}^{M}\sum_{i=1}^{N}(C_{ij}-C'_{ij})^2\right)}} \qquad (15)$$

Various shames are compared to the proposed scheme, and the results are shown in Table 6. According to the proposed scheme, CC values near to 0 indicate a large disparity between the pictures of plain-text and cipher-text in the proposed scheme.

Table 6: Analyses of the proposed scheme in comparison with other existing schemes.

Test images	Schemes		
	[38]	[39]	Proposed
Girl	0.0091	0.0208	0.0054
Lena	0.0059	−0.0076	0.0029
Finger	0.0045	−0.2399	0.0039
Iris	0.0056	−0.0038	0.0033

3.8 Contrast analysis

Contrast analysis is a technique that analyzes images for the degree of local intensity variation they contain [7]. A higher contrast value implies that the image contains significantly varying gray levels, whilst a lower number suggests that the gray levels are constant. Image contrast is defined as [7]:

$$C = \sum_{i,j}|i-j|^2 \, X \, p(i,j) \qquad (16)$$

Contrast of plain-text and encrypted images (i.e., cipher) are evaluated and its results is listed in Table 7. Table 7 shows the contrast between plain-text and encrypted images (i.e., cipher). Table 7 shows that the proposed scheme has higher contrast levels than the values of plaintext pictures in [38] and [39], which show that the proposed scheme has a significant degree of unpredictability in comparison to other schemes.

Table 7: Contrast analysis.

Test image	Schemes			
	[38]	[39]	Proposed	Plain-text
Girl	0.2101	8.3788	9.5343	0.3058
Lena	0.2213	8.4156	10.0852	0.7207
Finger	0.2239	4.4233	10.0087	0.3850
Iris	0.2702	4.4323	9.9947	0.8582

4 Conclusion

This work proposes a new approach for image encryption based on piecewise non-linear chaotic maps. These maps' advantages include ergodicity and the ability to determine KS-entropy. In this system, trigonometric and piecewise non-linear chaotic maps were examined for their potential as secure, quick, and reliable encryption tools. It is vital to remember that chaotic cryptosystems are often slower than non-chaotic ones that are commercially accessible. The proposed cryptosystem offers a high level of security, as demonstrated by theoretical and experimental study. The acquired findings validated our proposed cryptosystem. As a consequence of our positive studies, we believe that our encryption system is ideal for Internet image encryption and secure transmission of confidential information over the Internet.

Conflict of interest: The authors declare that there is no conflict regarding the publication of this paper.

References

[1] B.L. Hao. Starting with parabolas: an introduction to chaotic dynamics. *Shanghai Scientific and Technological Education Publishing House*, 10-12 (1993).

[2] N. Tahat, A.K. Alomari, O.M. Al-Hazaimeh, and M.F. Al-Jamal. An efficient self-certified multi-proxy signature scheme based on elliptic curve discrete logarithm problem. *Journal of Discrete Mathematical Sciences and Cryptography,***(23)**, 935-948 (2020).

[3] V.N. Belykh, N.N. Verichev, and L.Kocarev. On Chaotic Synchronization in a Linear Array of Chua's Circuits. *J. Circuits Syst. Comput.,***(3)**, 579-590 (1993).

[4] F. Huang and Z.H. Guan. Cryptosystem using chaotic keys. *Chaos, Solitons & Fractals,***(23)**, 851-855 (2005).

[5] O.M. Al-Hazaimeh, A. Abu-Ein, K.M. Nahar and I.S. Al-Qasrawi. Chaotic elliptic map for speech encryption. *Indonesian Journal of Electrical Engineering and Computer Science,***(25)**, 1103-1114 (2022).

[6] O.M. Al-Hazaimeh. A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol. *International Journal of Electrical & Computer Engineering,***(10)**, 4824-4834 (2020).

[7] J. Ahmad and S.O. Hwang. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimedia Tools and Applications,***(75)**, 13951-13976 (2016).

[8] O.M. Al-Hazaimeh. A new speech encryption algorithm based on dual shuffling Hénon chaotic map. *International Journal of Electrical and Computer Engineering (IJECE),***(11)**, 2203-2210 (2021).

[9] L. Kocarev, G. Jakimoski, T. Stojanovski and U. *Parlitz. From chaotic maps to encryption schemes*. In 1998 IEEE International Symposium on Circuits and Systems (ISCAS) (Vol. 4, pp. 514-517). IEEE (1998)

[10] J. Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos,***(8)**, 1259-1284 (1998).

[11] R. Matthews. On the derivation of a "chaotic" encryption algorithm. *Cryptologia,***(13)**, 29-42 (1989).

[12] T. Habutsu, Y. Nishio, I. Sasase and S. Mori. *A secret key cryptosystem by iterating a chaotic map*. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 127-140). Springer, Berlin, Heidelberg (1991).

[13] D.D. Wheeler. Problems with chaotic cryptosystems. *Cryptologia,***(13)**, 243-250 (1989).

[14] E. Biham. *Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT'91. I*n Workshop on the Theory and Application of of Cryptographic Techniques (pp. 532-534). Springer, Berlin, Heidelberg (1991).

[15] R. Zahmoul, R. Ejbali and M.Zaied. Image encryption based on new Beta chaotic maps. *Optics and Lasers in Engineering,* **(96)**, 39-49 (2017).

[16] H. Zhu, X. Zhang, H. Yu, C. Zhao and Z. Zhu. An image encryption algorithm based on compound homogeneous hyper-chaotic system. *Nonlinear Dynamics,***(89)**, 61-79 (2017).

[17] H. Natiq, M.R.M. Said, M.R.K. Ariffin, S. He, L. Rondoni and S. Banerjee. Self-excited and hidden attractors in a novel chaotic system with complicated multistability. *The European Physical Journal Plus,***(133)**, 1-12 (2018).

[18] A.J. Michaels and D.B. Chester. *U.S. Patent No. 8,145,692.* Washington, DC: U.S. Patent and Trademark Office (2012).

[19] Z. Hua, Y. Zhou, C.M. Pun and C.P. Chen. 2D Sine Logistic modulation map for image encryption. *Information Sciences,***(297)**, 80-94 (2015).

[20] O.M. Al-Hazaimeh. A novel encryption scheme for digital image-based on one dimensional logistic map. *Computer and Information Science,***(7)**, 65-73 (2014).

[21] N.K. Pareek, V. Patidarand K.K. Sud. Discrete chaotic cryptography using external key. *Physics Letters A,***(309)**, 75-82 (2003).

[22] F. Huang and Z.H. Guan. A modified method of a class of recently presented cryptosystems. *Chaos, Solitons & Fractals,***(23)**, 1893-1899 (2005).

[23] T. Sang, R.L. Wang and Y.X. Yan. The theoretical design for a class of new chaotic feedback stream ciphers. *Acta electronica sinica,***(27)**, 47-50 (1999).

[24] O. Al-Hazaimeh, M. Al-Jamal, M. Bawaneh, N. Alhindawi and B. Hamdoni. A new image encryption scheme using dual chaotic map synchronization. *International Arab Journal of Information Technology,***(18)**, 95-102 (2021).

[25] S. Behnia, A. Akhshani, H. Mahmodi and A.Akhavan. A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos, Solitons & Fractals,***(35)**, 408-419 (2008).

[26] T.H. Chen and C.S Wu. Compression-unimpaired batch-image encryption combining vector quantization and index compression. *Information Sciences,***(180)**, 1690-1701 (2010).

[27] V. Patidar, N.K. Pareek, G. Purohit and K. Sud. Modified substitution–diffusion image cipher using chaotic standard and logistic maps. *Communications in Nonlinear Science and Numerical Simulation,***(15)**, 2755-2765 (2010).

[28] N.K. Pareek, V. Patidar and K. Sud. Image encryption using chaotic logistic map. *Image and vision computing,***(24)**, 926-934 (2006).

[29] V. Patidar, N.K. Pareek and K. Sud. A new substitution–diffusion-based image cipher using chaotic standard and logistic maps. *Communications in Nonlinear Science and Numerical Simulation,***(14)**, 3056-3075 (2009).

[30] N.K. Pareek, V. Patidar and K. Sud. Cryptography using multiple one-dimensional chaotic maps. *Communications in Nonlinear Science and Numerical Simulation,***(10)**, 715-723 (2005).

[31] X. Han, X. Chang, L. Quan, X. Xiong, J. Li, Z. Zhang and Y. Liu. Feature subset selection by gravitational search algorithm optimization. *Information Sciences,***(281)**, 128-146 (2014).

[32] C.K. Huang and H.H.Nien. Multi chaotic systems-based pixel shuffle for image encryption. *Optics communications,***(282)**, 2123-2127 (2009).

[33] V.I. Ponomarenko and M.D. Prokhorov. Extracting information masked by the chaotic signal of a time-delay system. *Physical Review E,***(66)**, 026215 (2002).

[34] M.A. Jafarizadeh, M.Foroutan and S.Ahadpour. Hierarchy of rational order families of chaotic maps with an invariant measure. *Pramana,***(67)**, 1073-1086 (2006).

[35] O.M. Al-Hazaimeh, M.F. Al-Jamal, N.Alhindawi and A. Omari. Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. *Neural Computing and Applications,***(31)**, 2395-2405 (2019).

[36] O.M. Al-Hazaimeh, N.Alhindawi, S.M. Hayajneh and A. Almomani. HANON chaotic map-based new digital image encryption algorithm. *MAGNT Research Report,***(2)**, 261-266 (2014).

[37] Y. Mao, G. Chen and S. Lian. A novel fast image encryption scheme based on 3D chaotic baker maps. *International Journal of Bifurcation and chaos,***(14)**, 3613-3624 (2004).

[38] F. Ahmed, A. Anees, V.U. Abbas and M.Y. Siyal. A noisy channel tolerant image encryption scheme. *Wireless personal communications,***(77)**, 2771-2791 (2014).

[39] A. Anees, A.M. Siddiqui and F. Ahmed. Chaotic substitution for highly autocorrelated data in encryption algorithm. *Communications in Nonlinear Science and Numerical Simulation,***(19)**, 3106-3118 (2014).

[40] O.M. Al-Hazaimeh. *New cryptographic algorithms for enhancing security of voice data*. Doctoral dissertation, Universiti Utara Malaysia (2010).

[41] O.M. Al-Hazaimeh. Combining audio samples and image frames for enhancing video security. *Indian Journal of Science and Technology,***(8)**, 940 (2015).

[42] G. Alvarez and S. Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos,***(16)**, 2129-2151 (2006).

[43] C. Zhu. A novel image encryption scheme based on improved hyperchaotic sequences. *Optics communications,***(285)**, 29-37 (2012).

[44] O.M. Al-Hazaimeh, A. Abu-Ein, M. Al-Nawashi and N.Y. Gharaibeh. Chaotic based multimedia encryption: a survey for network and internet security. *Bulletin of Electrical Engineering and Informatics,***(11)**, 2151-2159 (2022).