J. Math. Computer Sci., 32 (2024), 275–282

Online: ISSN 2008-949X

Journal of Mathematics and Computer Science

Journal Homepage: www.isr-publications.com/jmcs

An image encryption tool based on the chaotic automorphism and Chirikov transformation

Muammer Catak[a], Tofigh Allahviranloo[b,*]

[a]College of Engineering and Technology, American University of the Middle East, Kuwait.

[b]Faculty of Engineering and Natural Sciences, Istinye University, Istanbul, Turkey.

Abstract

For some operations that use either color or gray-scale images the algorithms involving image encryption provide significant security. In this paper, a novel image encryption tool based on chaotic automorphism and the Chirikov transform is proposed. The lack of efficiency of the chaotic automorphism, such as ghost and miniature effects, is overcome with the help of the Chirikov transformation. Normalized pixel change rate, correlation coefficient, and histogram analysis are employed in order to validate the efficiency of the proposed method. According to the results, the proposed algorithm demonstrates its robustness against attacks based on statistical analysis.

Keywords: Encryption, CAT map, Chirikov transformation, image processing.

2020 MSC: 15-04, 60G07.

1. Introduction

The amount of the generated data has been exponentially increasing year by year [12]. In 2010, the total size of the generated data was 2 zettabytes (2×10^{21}); while it is almost 100 zettabytes in 2022 [18]. In addition to the dramatic increment in the main trend, some specific occasions, for instance Covid-19, boost the rate of the incline. For instance, the size of online shopping has been extended rapidly [23]. All these data may include some unique information about a person, i.e., fingerprints, health records, etc. Moreover, especially with the increment of robotic technology in the industry, the created data during the industrial applications have a significant role. Inevitably, at this point, the security issue of the generated data has emerged as an indispensable research area.

Image encryption techniques may offer substantial protection for some applications including both grayscale and color images. A picture encryption method that uses bit-level permutation and diffusion was proposed by Zhu et al. [26]. In this method, permutation and diffusion operations are carried out using the Arnold map and logistic map. Compared to other image encryption algorithms, this method is more computationally efficient. To decrease the prediction time compared to straightforward chaotic maps-based image encryption algorithms, Gao et al. [7] introduced the hyper-chaotic map in image

*Corresponding author
Email address: Muammer.Catak@aum.edu.kw (Muammer Catak)

doi: 10.22436/jmcs.032.03.08

Received: 2023-09-01 *Revised:* 2023-09-27 *Accepted:* 2023-10-09

encryption. This method uses matrix shuffles to randomly reorder the pixels in an input image. The pixel values of the shuffled image are then diffused using a hyper-chaotic map. Better key space and great security are provided by this technology.

Three enhanced one-dimensional chaotic maps with DNA sequences for color picture cryptosystems were proposed by Wu et al. [21]. The DNA encoding rule is used to transform the input image and key stream into matrices. The matrices are then scrambled using XOR and complementing operations. The mixed matrices are split into equal chunks and randomly shuffled. These matrices were subjected to XOR and DNA addition processes to produce the encrypted image. Because three chaotic maps are utilized to construct a key stream that depends on both the input image and secret keys, this method is immune to picked and known-plain text attempts. Cellular Automata (CA) is a system of grid-based cells with variously shaped structures. Based on the states of nearby cells, these structures develop over a number of finite time steps in accordance with the prescribed principles. So, CA models the intricate architecture. Numerous ways are able to construct sequences thanks to the massive volume of CA standards. It develops by simple logic calculations and exhibits challenging behaviors. Developers frequently use the reversible CA to implement the block encryption method. Large amounts of rules space and parallelism are two of the key advantages of CA in encryption [20].

Choquet Fuzzy Integral (CFI) was utilized by Seyedzadeh et al. [15] to create a key-stream that was used to secure the color images. This method comprises three stages, including key-stream generation, cyclic shifting, and diffusion process. The pseudo-random key streams are formed utilizing CFI, and that each colour pixel's bits are then rotated in a circle based on the key-stream. Key-stream and color pixels are combined to encrypt the permuted bits. By incorporating embedded process in lift wavelet transform, Kanso and Ghebleh [9] made a contribution to the field of visual image encryption. It improves both the output image resolution as well as the protection of encryption methods. Rawat et al. [14] developed an enhanced encryption scheme using Arnold transform, structurally random patterns, and compressive sensing (CS). The proposed method has a powerful computational performance and enhanced the quality of the encrypted image. The authors encourage the readers to have a look at the following review articles for more information [6, 10, 19] .

The rest of the paper is organized as follows. In Section 2, the main parts of the proposed technique, namely the chaotic automorphism transformation (CAT), and a linear shuffling Chirikov transformation, will be discussed in detail. Section 3 is dedicated to presenting the obtained results and corresponding discussions. Finally, the paper is concluded in Section 4.

2. Materials and methods

In this section, the chaotic automorphism transformation and a linear shuffling Chirikov transformation will be introduced as main parts of the proposed algorithm.

2.1. Arnold's CAT map (ACM)

Arnold's continuous automorphism on the torus map is a discrete-time dynamic system governing by the following generalized matrix,

$$\mathbf{A} = \begin{bmatrix} a & b \\ b & c \end{bmatrix}.$$

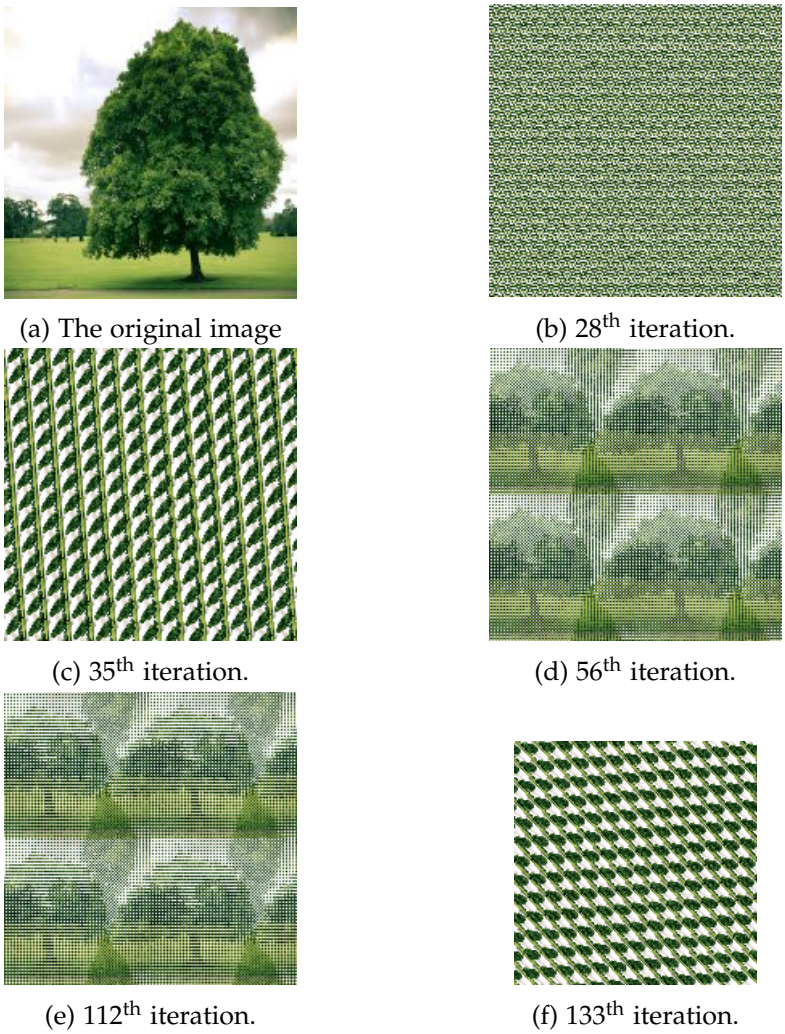
In order to preserve the size of the image, $\det(\mathbf{A})$ must be 1. Thereafter, the entries of the matrix $\mathbf{A}$ can be chosen from Fibonacci series of $(1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \dots)$ such as

$$\mathbf{A} = \begin{bmatrix} F_{2n-1} & F_{2n} \\ F_{2n} & F_{2n+1} \end{bmatrix}.$$

Considering an $N \times N$ grayscale image, Arnold's CAT map iteration can be calculated as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \mathbf{A} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N} + \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

An illustrative example of CAT Map image encryption is shown in Figure 1. The original image shown in Figure 1a is a 182×182 RGB image. After 28^{th} iteration, a sample of encrypted image is obtained. It is almost impossible to predict the original image just looking at Figure 1b without any additional information. However, after 35^{th} iteration or 133^{th} iteration, many of smaller size of the original images appear, which is called miniature effect. Moreover, somehow blurry version of the original image will come out as depicted in Figure 1c and 1f. It is known as ghost effect. In addition of these types of weaknesses, after a certain number of iterations, the original image might appear but up side down depending on the size of the image and the chosen transformation matrix, $\mathbf{A}$ [16].



(a) The original image

(b) 28^{th} iteration.

(c) 35^{th} iteration.

(d) 56^{th} iteration.

(e) 112^{th} iteration.

(f) 133^{th} iteration.

Figure 1: An illustrative example for CAT Map algorithm.

2.2. Discrete Chirikov map (DCM)

Discrete Chirikov map (DCM) is a dynamic transformation which maps the inputs from $(N \times N)$ domain onto the $(N \times N)$ range as one-by-one operator. Therefore, DCM not only preserves the area of the image but also it has an inverse operation [4]. The DCM iterative can be calculated using the following equation [5]:

$$x_{i+1} = (x_i + y_i) \text{Mod}(N) + 1, \quad y_{i+1} = \lambda \text{ round} \left(\sin \left(\frac{2\pi x_i}{N} \right) \right) \text{Mod}(N) + y_i + 1,$$

where (x_{i+1}, y_{i+1}) defines the new position of the related pixel, N is the size of the square image, and λ is the permutation key, which is a positive integer.

The inverse Chirikov transform is carried out by means of equation (2.1) as

$$\begin{aligned} x_{i+1} &= \left(x_i - y_i + \lambda \text{ round} \left(\sin \left(\frac{2\pi x_i}{N} \right) \right) \right) \text{Mod}(N) + 1, \\ y_{i+1} &= \left(y_i - \lambda \text{ round} \left(\sin \left(\frac{2\pi x_i}{N} \right) \right) \right) \text{Mod}(N) + 1. \end{aligned} \tag{2.1}$$

An illustration purpose example of application of Chirikov mapping is shown in Figure 2. The algorithm was applied for a 128×128 and 256×256 images. As one can easily check from the figures, it is impossible to guess the original figures from their encrypted versions.

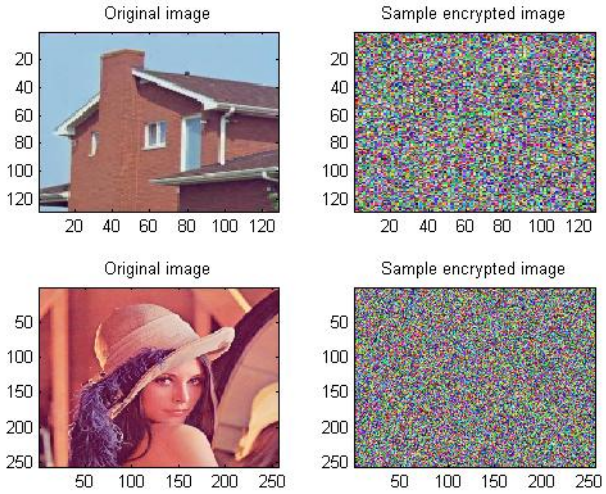


Figure 2: Example graphs of Chirikov mapping.

In order to enhance and then to check the effectiveness of the proposed method, the following analysis techniques will be employed accompanying with the main algorithm.

2.2.1. Normalized pixel change rate (NPCR)

NPCR is a number $\in [0, 1]$, which indicates the discrepancy between two digital images. It can be calculated as

$$\text{NPCR} = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} D(i,j), \quad D(i,j) = \begin{cases} 0, & \text{if } O(i,j) = E(i,j), \\ 1, & \text{if } O(i,j) \neq E(i,j), \end{cases}$$

where $O(i,j)$ and $E(i,j)$ are represented for the original image and the encrypted image, respectively. While NPCR value increases, the similarity rate between two images decreases. Therefore, in theory, NPCR value should approach to the unity.

2.2.2. Correlation coefficient

The percentage of the number of pixels at any edge, where the intensity level of the adjacent pixels change dramatically, over the total number of pixels is relatively small for a digital image. Therefore, the intensity levels of the neighbor pixels are highly correlated. In general, the correlation coefficient can be calculated as [1]

$$\rho_{xy} = \frac{C_{xy}}{\sigma_x \sigma_y},$$

where C_{xy} is the covariance and σ_x and σ_y are the standard deviations of each data set.

Since, a digital image is a 2-D data, the correlation coefficient has to be calculated in three directions, namely diagonal, horizontal, and vertical. The range of the correlation coefficient is

$$-1 \leqslant \rho_{xy} \leqslant 1.$$

If ρ_{xy} approaches zero, then it can be stated that x and y are less correlated variables, while the magnitude of the ρ_{xy} approaches one it is said that x and y are highly correlated variables.

Hence, having ρ_{xy} around zero is a good indicator to validate the quality of the image encryption process.

2.2.3. Histogram analysis

The image histogram shows the distribution of the intensity values of the pixels. In general, the histogram of a digital image is intrinsically non-uniform. On the other hand, the histogram of an encrypted image should almost be uniformly distributed.

3. Results and Discussion

In this paper a novel image encryption technique is discussed. The proposed algorithm is based on chaotic transformation, and dynamic linear shifting of a digital image of RGB, or gray scale. The encryption steps are summarized Algorithm 1.

Require: $I \Leftarrow$: Load the input image (the original image)
Ensure: Check the size of I, if it is not a square image, resize the image.
1: **CAT Map**
2: Randomly select an F_{2n} from the set of Fibonacci series, then create the transformation matrix, **A**
3: $T \Leftarrow$: Find the period of the iteration
4: Run ACM till $k = \frac{T}{2}$
5: Check *NPCR* fro each iteration step
6: $k \Leftarrow$: Select k at which *NPCR* is at its maximum
7: $E_1 \Leftarrow$: Assign the encrypted image by means of running ACM k times. $E_1 = ACM_k\{I\}$
8: **DCM**
9: $\lambda \Leftarrow$: Randomly select the permutation key
10: $E_2 \Leftarrow$: Run DCM to get the encrypted image. $E_2 = DCM\{E_1\}$
11: **Results**
12: Display correlations between I and E_2
13: Display histograms of I and E_2

Algorithm 1: The Encryption Steps.

The original data, that is a digital image in this context, is encrypted by following the steps described in Algorithm 1. The encrypted data might be stored at any appropriate device and/or it might be sent to another side, receiver party. The encrypted data obtained by the receiver side should be decrypted following the steps described in Algorithm 2.

Require: $E_2 \Leftarrow$: Load the input image (the decrypted image)
Ensure: Check the size of E_2
1: **DCM**
2: $E_1 \Leftarrow$: Apply inverse DCM
3: $I \Leftarrow$: Run CAT map $T - k$ times on E_1 to get the original image
4: Display the original image I

Algorithm 2: The Decryption Steps.

In Figure 3, histogram analysis of the original image and the corresponding encrypted image are depicted. As expected from the theory, histogram of the original image is not uniformly distributed. On the other hand, histogram of the encrypted image is almost uniformly distributed shaped. Therefore, the proposed algorithm shows its resilience against to the attacks based on statistical analysis.

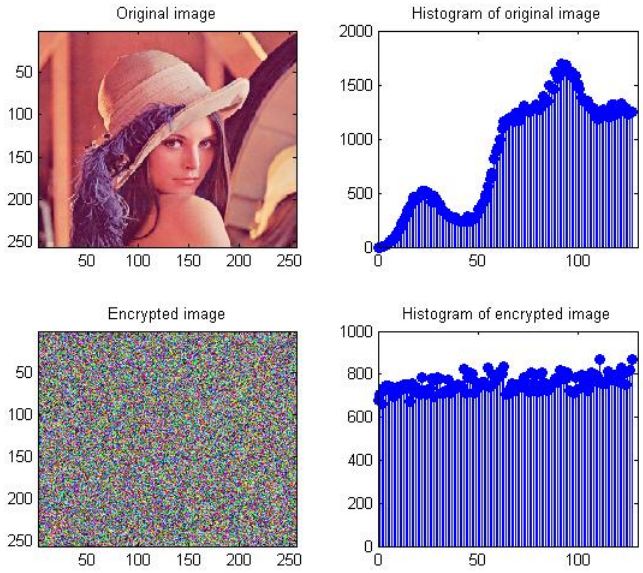


Figure 3: Histogram analysis of the original image and the encrypted image.

The correlation analysis of the original image is given in Figure 4. In all cases, the pixels are highly correlated within the original image. The correlation coefficients are listed as 0.9385, 0.8916, 0.8562 for horizontal, vertical, and diagonal correlations, respectively.

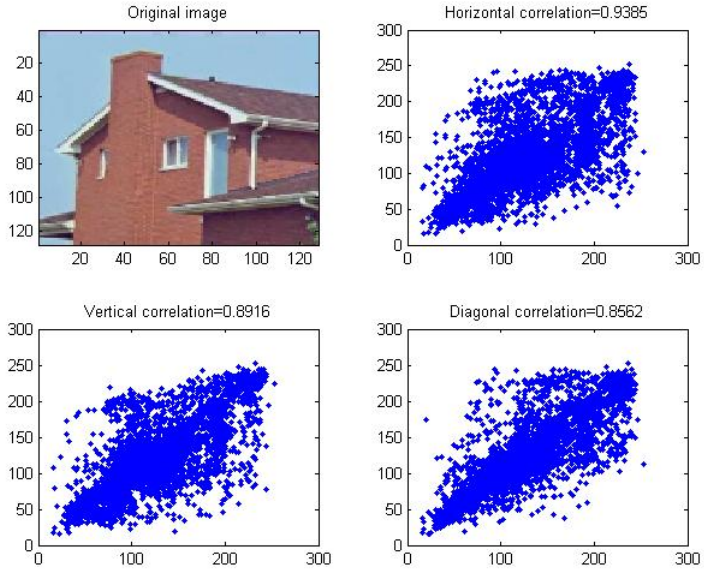


Figure 4: Correlation analysis of the original image.

In Figure 5 the correlation analysis of the encrypted image is illustrated. One can easily see that, the pixels are highly uncorrelated under all three possible cases. The correlation coefficients are dramatically

decreased comparing with the correlation coefficients of the original image. This is another significant sign proving that the efficiency of the proposed algorithm.

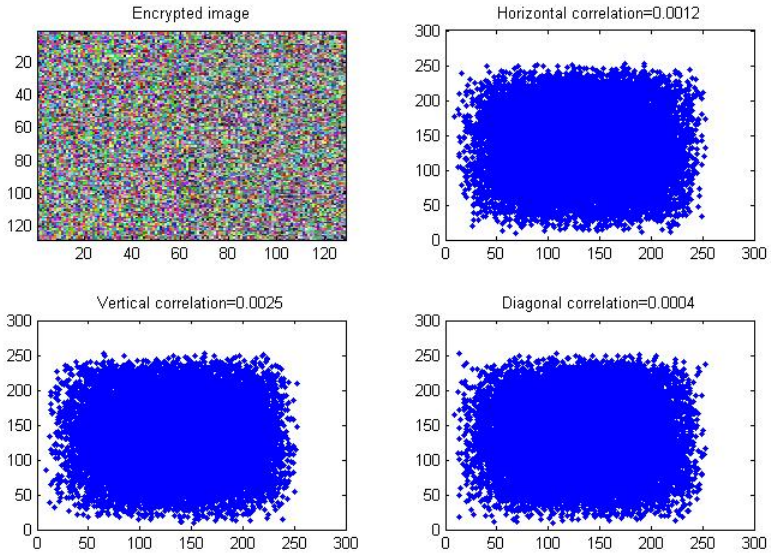


Figure 5: Correlation analysis of the encrypted image.

The comparison analysis of the proposed method with some other techniques are depicted in Table 1. The proposed algorithm shows one of the best records on NPCR percentages. Moreover, it supplies absolutely competent correlation coefficients for diagonal, vertical, and horizontal cases.

Table 1: Comparison of the proposed method with other techniques previously done.

References	NPCR	Diag. Corr.	Verti. Corr.	Hori. Corr.
[3]	99.629	0.0006	0.0019	0.0021
[24]	99.730	0.0012	0.0151	0.0044
[8]	99.609	-0.0193	-0.0226	-0.0245
[2]	99.620	0.0277	0.0039	0.0172
[13]	99.683	0.0009	0.0025	0.0030
[17]	99.589	0.0003	0.0002	0.0003
[11]	99.690	0.0043	0.0021	0.0042
[25]	93.790	0.0259	0.0232	0.0012
[22]	98.798	0.0007	0.0011	0.0021
Proposed	99.782	0.0004	0.0025	0.0012

4. Conclusion

The amount of the digitally created data keeps rapidly increasing. Therefore, data security is still an important topic in digital signal processing area. In this paper, a novel image encryption technique, which is based on chaotic automorphism and linear shuffling of the pixels of the image under study, is proposed. Some weak sides of the chaotic automorphism, such as miniature, ghost effects, are eliminated, and a more robust method is developed. It is shown that, the proposed algorithm is successful against the attacks especially based on statistical analysis. In addition, research into image encryption security vulnerabilities, parameter optimization, and computing performance is indeed active.

References

[1] M. Catak, T. Allahviranloo, W. Pedrycz, *Probability and Random Variables for Electrical Engineering*, Springer, Cham, (2022). 2.2.2

[2] X. Chai, *An image encryption algorithm based on bit level Brownian motion and new chaotic systems*, Multimed. Tools Appl., **76** (2017), 1159–1175. 1

[3] X. Chai, Z. Gan, M. Zhang, *A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion*, Multimed. Tools Appl., **76** (2017), 15561–15585. 1

[4] B. V. Chirikov, *Research concerning the theory of non-linear resonance and stochasticity*, (1971). 2.2

[5] B. V. Chirikov, *A universal instability of many-dimensional oscillator systems*, Phys. Rep., **52** (1979), 264–379. 2.2

[6] L. Fransson, *Tribonacci Cat Map: A discrete chaotic mapping with Tribonacci matrix*, (2021). 1

[7] T. Gao, A. Chen, *A new image encryption algorithm based on hyper-chaos*, Phys. lett. A, **372** (2008), 394–400. 1

[8] X. Huang, G. Ye, *An image encryption algorithm based on irregular wave representation*, Multimed. Tools Appl., **77** (2018), 2611–2628. 1

[9] A. Kanso, M. Ghebleh, *An algorithm for encryption of secret images into meaningful images*, Opt. Lasers Eng., **90** (2017), 196–208. 1

[10] M. Kaur, V. Kumar, *A comprehensive review on image encryption techniques*, Arch. Comput. Methods Eng., **27** (2020), 15–43. 1

[11] L. Liu, S. Miao, *An image encryption algorithm based on Baker map with varying parameter*, Multimed. Tools Appl., **76** (2017), 16511–16527. 1

[12] B. Marr, *How Much Data Do We Create Every Day?*, Forbes, (2018). 1

[13] M. Mollaeefar, A. Sharif, M. Nazari, *A novel encryption scheme for colored image based on high level chaotic maps*, Multimed. Tools Appl., **76** (2017), 607–629. 1

[14] N. Rawat, B. Kim, R. Kumar, *Fast digital image encryption based on compressive sensing using structurally random matrices and Arnold transform technique*, Optik, **127** (2016), 2282–2286. 1

[15] S. M. Seyedzadeh, B. Norouzi, S. Mirzakuchaki, *RGB color image encryption based on Choquet fuzzy integral*, J. Syst. Softw., **97** (2014), 128–139. 1

[16] F. Svanström, *Properties of a generalized Arnold's discrete cat map*, (2014). 2.1

[17] Z. Tang, F. Wang, X. Zhang, *Image encryption based on random projection partition and chaotic system*, Multimed. Tools Appl., **76** (2017), 8257–8283. 1

[18] P. Taylor, *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025 (in zettabytes)*, Retrieved March, (2022). 1

[19] C. Tiken, R. Samli, *A Comprehensive Review About Image Encryption Methods*, Harran Univ. Eng. J., **7** (2022), 27–49. 1

[20] X. Wang, D. Luan, *A novel image encryption algorithm using chaos and reversible cellular automata*, Commun. Nonlinear Sci. Numer. Simul., **18** (2013), 3075–3085. 1

[21] X. Wu, H. Kan, J. Kurths, *A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps*, Appl. Soft Comput., **37** (2015), 24–39. 1

[22] J. Wu, M. Zhang, N. Zhou, *Image encryption scheme based on random fractional discrete cosine transform and dependent scrambling and diffusion*, J. Modern opt., **64** (2017), 334–346. 1

[23] M. Young, J. Soza-Parra, G. Circella, *The increase in online shopping during COVID-19: Who is responsible, will it last, and what does it mean for cities?*, Reg. Sci. Policy Pract., **14** (2022), 162–178. 1

[24] Y. Zhang, Y. Tang, *A plaintext-related image encryption algorithm based on chaos*, Multimed. Tools Appl., **77** (2018), 6647–6669. 1

[25] J. Zhu, X. Yang, X. Meng, Y. Wang, Y. Yin, X. Sun, G. Dong, *Optical image encryption scheme with multiple light paths based on compressive ghost imaging*, J. Modern Opt., **65** (2018), 306–313. 1

[26] Z. l. Zhu, W. Zhang, K. W. Wong, H. Yu, *A chaos-based symmetric image encryption scheme using a bit-level permutation*, Inf. sci., **181** (2011), 1171–1186. 1