

Efficient Image Cipher using 2D Logistic Mapping and Singular Value Decomposition

Mohammed A. AlZain

Department of Information Technology
College of Computers and Information Technology, Taif University
P.O. Box 888, Al-Hawiya-Taif, 21974, KSA

Abstract—The research paper proposes an efficient image cryptosystem that depends on the utilization of two dimensional (2D) chaotic logistic map (CLM) and singular value decomposition (SVD). The encryption process starts by a confusion stage through applying the 2D-CLM to the input plainimage. Then, the resulted logistic transformed image is then decomposed using the SVD technique into three ciphered components; the horizontal, vertical, and diagonal components. The ciphered horizontal, vertical, and diagonal components are then transmitted to the destination which applies a reverse procedure to reconstruct the original plainimage. A matrix of encryption quality tests are performed for investigating the proposed 2D-CLM based SVD image cipher. The obtained test results confirmed and ensured the efficiency of the proposed 2D-CLM based SVD image cipher.

Keywords—Image cipher; 2D-CL; SVD

I. INTRODUCTION

Recently, the unexpected growing in digital technology field witnessed a lot of attention. And this raises and makes the security issues of the data a critical important task especially during the transmission of sensitive data like images, audios, and videos [1-4]. Images may be utilized in different fields like medical, military, and communication fields, the images may carry important valuable information and may be shared over communication networks, so; it becomes a serious issue to maintain them secured as possible against all probable potential attacks. Plenty of works have been done in recent years and resulted in a many studies on image encryption [5-10].

Several image encoding methods were done and founded in literature like ones that depends on classical encryption like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Double-DES, TDES, and International Data Encryption Algorithm (IDEA) [11-15]. Such techniques do not provide a satisfactory outcome because of image intrinsic characteristics like huge bulky capacity, high correlation, and redundancy [16-19].

On contrast, many reported methods in literature uses different transformations like Fractional Fourier Transform (FrFT) for image encoding which may be considered as a generalization of FT [20]. Other transformations that are actually utilized in image encryption include Discrete Wavelet transform (DWT) [21], Fractional Wavelet packet (FWP) [22],

and 2D-CLM [23-24]. An image cryptosystem that utilizes a multi-channel/multi-stage FrFT is given in [25]. In [26], the authors presented a proposed an image cipher that performs encryption using an iterative FrFT. A color image cipher which applies FWP is presented in [22]. In [27], a color image cipher is proposed that employed encryption in dual FrFT-WT using random phases. In [28], a color image cipher that employed FrFT in conjunction with DWT is presented. In [29], a secure color image cipher which employed a DWT and SVD is proposed. In [30], an image encoding which utilizes SVD and AT in FrFT is presented. This method works as follows; the plainimage is firstly transformed with FrFT and the transformed image is decomposed with SVD into three components. The three components are AT transformed with different iterations, which resulted in the three ciphered images. In decryption procedure, the three ciphered images are inverse AT transformed using the iterations number and the three components are correctly multiplied. Also, uses the inverse FrFT with corrected parameters to achieve the correct decrypted image.

The 2D-CLM can be employed for pixel shuffling for several many image encryption methods [23]. The other method that may be utilized for improving security is the SVD in which the plainimage is decomposed into three components. Such components with the multiplication order are required during decryption and hence may serve as an additional key.

The main objective of this study is to present an efficient and secure image cipher method for transmitting over secure/unsecure communication network. At encoder end, the encryption process starts by a confusion stage through applying the 2D-CLM to the input plainimage. Then, the resulted logistic transformed image is then decomposed using the SVD technique into three ciphered components; the horizontal, vertical, and diagonal components. At destination, with the knowledge of parameters value, it is easy to retrieve the plainimage from the three ciphered images.

The paper reminder is marshaled as follows: Sect. II provides necessary background regarding the 2D-CLM and the SVD. Sect. III is dedicated for describing in details the proposed 2D-CLM based SVD image cipher. Experimental test results and the analysis of 2D-CLM based SVD image cipher are given in Sect. IV, Sect. V concludes the proposed 2D-CLM based SVD image cipher.

II. BACKGROUND

This section presents the fundamental tools which the proposed image cryptosystem depends on. These tools include the 2D-CLM and the SVD.

A. 2D-CLM

The chaotic logistic is based on several control parameters and this makes it commonly applied in chaos based encryption applications. This is because it is sensitive regarding to initial conditions. The 2D-CLM is derived from the 1D-CLM.

The 1D-CLM can be considered as a simple model that provides a chaotic manner and it can be represented mathematically as [31]:

$$Y_{n+1} = rY_n (1 - Y_n) \quad (1)$$

Where Y_n values are in the range [0,1], the r parameter is defined as positive and it allows values in the range [0,4]. Its utilized value controls and gives the manner of how logistic map can work.

The 2D-CLM is more complicated than the 1D-CLM since it has a complex chaotic manner which makes it efficiently sufficient for data encryption. The 2D-CLM can be mathematically described as [23-24]:

$$\text{2D Logistic map: } \begin{cases} x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = r(3x_i + 1)y_i(1 - y_i) \end{cases} \quad (2)$$

Where r defines system control parameter and (x_i, y_i) represents pair-wise point at iteration i^{th} .

B. The SVD

The Singular value decomposition (SVD) is a commonly famous method in linear algebra, and it has many mathematical applications with respect to matrix inversion. The SVD can be considered as a powerful tool in numerical analysis that can be utilized in matrix analysis. The SVD transformation method works by splitting the matrix into three equivalent sized matrices like the input matrix. So, any image may be considered like an array of positive scalar like a matrix. If Z is a square image, defined like $Z \in \mathbb{R}$ with size of $n \times n$, where \mathbb{R} defines the domain of real numbers, then SVD of Z can be mathematically described as [32]:

$$Z = USV^T \quad (3)$$

Where U and V define the orthogonal vertical and horizontal matrices with condition $U^T U = I$, $V^T V = I$, where I defines the identity matrix. $S = \text{diagonal}(\sigma_1, \dots, \sigma_p)$, $p = \min(m, n)$, $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_p$ represent Z singular values. Diagonal entries may be considered as Z matrix singular values. The U columns and V columns are the Z left and right singular vectors. The SVD of Z is mathematically defined like given above in Eq. 3, where S , U and V are the diagonal, orthogonal vertical and horizontal matrices.

III. THE PROPOSED 2D-CLM BASED SVD IMAGE CIPHER

The proposed 2D-CLM based SVD image cipher is based on the utilization of 2D-CLM and SVD. The encryption procedure of 2D-CLM based SVD image cipher works through

applying the 2D-CLM to the input plainimage. The logistic transformed image is then decomposed with the SVD into the final ciphered diagonal, vertical, and Horizontal orthogonal matrixes which then transmitted to the receiving end. The decryption procedure follows the inverse procedure of the encryption. It starts by applying the inverse SVD transformation to the received ciphered diagonal, vertical, and Horizontal orthogonal matrixes then followed by applying the inverse 2D-CLM to retrieve the final decrypted image. Figs. 1-2 show the encryption/decryption procedures of 2D-CLM based SVD image cipher, respectively.

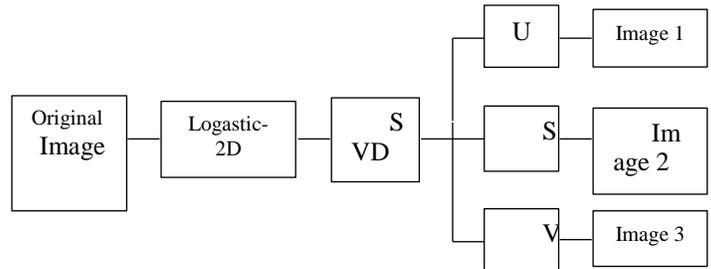


Fig. 1. Encryption Procedure of 2D-CLM based SVD Image Cipher.

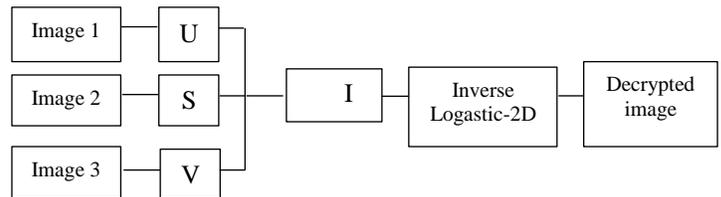


Fig. 2. Decryption Procedure of 2D-CLM based SVD Image Cipher.

IV. SECURITY STUDY

The security investigation of 2D-CLM based SVD image cipher is examined with a matrix of encryption measures and with the visual inspection. The proposed 2D-CLM based SVD image cipher is tested with a group of tests for investigating the performance of the proposed 2D-CLM based SVD image cipher for ciphering gray scale. These tests have been done using a set of different test images; such as Brabra, Boat and Pirate images as shown in Fig. 3.

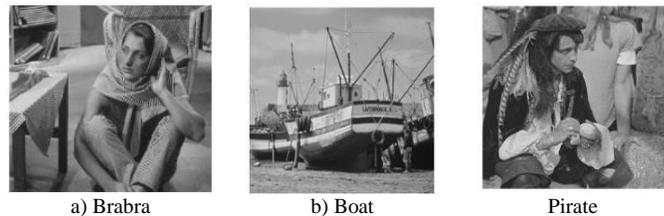


Fig. 3. Different Samples of Original Images.

A. Visual Inspecting Results

The visual inspecting results of encrypting different test images; such as Brabra, Boat and Pirate images using the proposed 2D-CLM based SVD image cipher are in Fig. 4. The visual inspection results show that the proposed 2D-CLM based SVD image cipher can successfully hide all the details of the tested plainimages. These visually inspected results have verified and proved the efficiency of 2D-CLM based SVD image cipher.

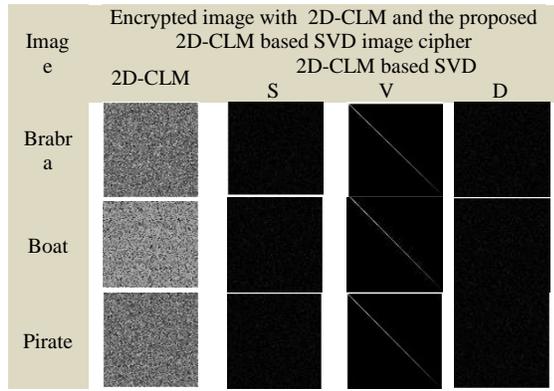


Fig. 4. Obtained Encryption Test Results of using the Proposed the Proposed 2D-CLM based SVD Image Cipher.

B. Histogram Test

The histogram results of examined plainimages and their corresponding cipherimages using the 2D-CLM and the proposed 2D-CLM based SVD image cipher are shown in Fig. 5. The cipherimages histogram results using the proposed 2D-CLM based SVD image cipher are completely different from their corresponding plainimages histogram results. On the other hand, it is noticed that the cipherimages histogram results using the 2D-CLM image cipher are equivalent to their corresponding plainimages histogram results. This is expected since the 2D-CLM just changes the location of pixels.

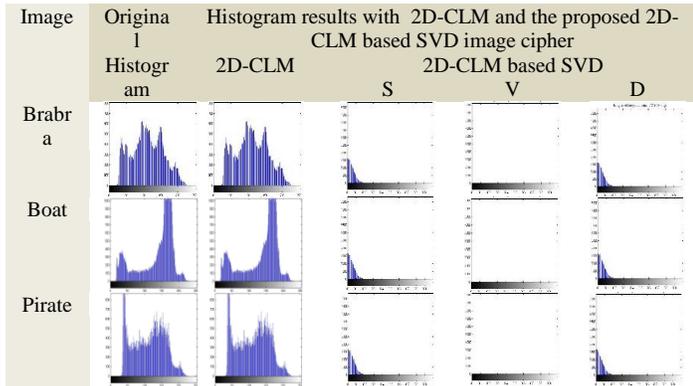


Fig. 5. Histogram test Results of Original/Encrypted Images using the Proposed 2D-CLM based SVD Image Cipher.

C. Entropy Metric

The entropy metric is performed for examining the cipherimages produced using the proposed 2D-CLM based SVD image cipher. The entropy metric can be defined as follows [33]:

$$E = -\sum_{i=1}^n P_r(x_i) \log P_r(x_i) \tag{4}$$

Where x_i defines the i^{th} point intensity. High entropy values indicate a best ciphering. The obtained entropy test results using the proposed 2D-CLM based SVD image cipher are given in Table I. The entropy test results indicate that entropy of encrypted images with 2D-CLM is higher compared with their corresponding results using the proposed 2D-CLM

based SVD image cipher. But this is expected due to the decomposition nature of the SVD.

TABLE I. ENCRYPTED IMAGES ENTROPY USING THE PROPOSED 2D-CLM BASED SVD IMAGE CIPHER

Image	Entropy values with 2D-CLM and the proposed 2D-CLM based SVD image cipher			
	2D-CLM	2D-CLM based SVD		
		S	V	D
Brabra	7.43567	3.439830	44.3808*10 ⁻³	3.44555
Boat	7.09441	3.44494	43.71455*10 ⁻³	3.43681
Pirate	7.2966	3.43596	44.76*10 ⁻³	3.43

D. Encryption Quality Tests

A set of encryption quality tests are performed for investigating the quality of encryption for the obtained cipherimages using the proposed 2D-CLM based SVD image cipher. This set of encryption quality tests may contain correlation coefficients test (Cr), irregular deviation test (I_d) and histogram deviation test (H_d).

D1. Correlation Coefficients Metric (Cr)

The correlation coefficients test (Cr) is estimated among plainimage/cipherimage as follows [34]:

$$C_r = \frac{\text{cov}(P,C)}{\sqrt{D(P)}\sqrt{D(C)}} \tag{5}$$

Small Cr values shows high encryption quality.

TABLE II. CORRELATION COEFFICIENT TEST RESULTS USING THE PROPOSED 2D-CLM BASED SVD IMAGE CIPHER

Image	Entropy values with 2D-CLM and the proposed 2D-CLM based SVD image cipher			
	2D-CLM	2D-CLM		
		S	V	D
Brabra	4.8728*10 ⁻³	-11.786*10 ⁻³	4.9116*10 ⁻³	-2.93400*10 ⁻³
Boat	-1.4715	796.61*10 ⁻⁶	8.443*10 ⁻³	-4.85415
Pirate	-919*10 ⁻⁶	-1.95*10 ⁻³	-2.73*10 ⁻³	979.65*10 ⁻⁶

The achieved correlation coefficients test results for the 2D-CLM and the proposed 2D-CLM based SVD image cipher are given in Table II. The obtained test results show that Cr among plainimage/cipherimage pairs is very small and close to the ideal value of zero that demonstrate high encryption quality.

D2. Irregular Deviation Metric (ID)

The ID metric estimate the encryption quality through computing the abnormality resulted by encryption using the proposed 2D-CLM based SVD image cipher. The IR Metric can be calculated as follows [35]:

$$I_D = \frac{\left| \sum_{i=0}^{255} |h(i) - M_h| \right|}{M \times N} \tag{6}$$

TABLE III. IRREGULAR DEVIATION TEST RESULTS USING THE PROPOSED 2D-CLM BASED SVD IMAGE CIPHER

Image	Irregular deviation values with 2D-CLM and the proposed 2D-CLM based SVD image cipher			
	2D-CLM	2D-CLM		
		S	V	D
Brabra	232.231*10 ⁻³	168.86*10 ⁻³	168.800*10 ⁻³	168.861*10 ⁻³
Boat	203.3*10 ⁻³	220.92*10 ⁻³	220.90*10 ⁻³	220.924*10 ⁻³
Pirate	234.3*10 ⁻³	191.68*10 ⁻³	191.67*10 ⁻³	191.68*10 ⁻³

Where h(i) is cipherimage histogram at the i intensity value, and M_h is the ideal encrypted histogram. Small ID values demonstrate a good encryption quality.

The ID test results of both the 2D-CLM and the proposed 2D-CLM based SVD image cipher are given in Table III. The achieved testing results showed that the ID values using the proposed 2D-CLM based SVD image cipher are good when compared to their corresponding ID values using the 2D-CLM image cipher. This confirmed the efficiency of the proposed 2D-CLM based SVD compared with the 2D-CLM.

D3. Histogram Deviation Metric (HD)

The HD Metric estimate computes the encryption quality through measuring the variation increase between plainimage (P)/ cipherimage (C) pairs. The HD metric can be estimated as follows [36]:

$$H_D = \frac{\sum_{i=0}^{255} d(i)}{M \times N}, \tag{7}$$

Where d(i) defines the difference between plainimage/cipherimage pairs at pixel intensity ith. M and N represent the image height and width. Higher ID values demonstrate good quality for encryption. The HD test results for both the 2D-CLM and the proposed 2D-CLM based SVD image cipher are given in Table IV. It is noticed that the obtained HD values using the 2D-CLM image cipher is zero. This can be interpreted since the 2D-CLM image cipher is just shuffle pixels position and does not change the histogram after employing the encryption. So, it is expected theoretically that the HD values using the 2D-CLM image cipher is zero. Also, results demonstrated that the values of HD using the proposed 2D-CLM based SVD image cipher are high compared with the obtained ID values using the 2D-CLM image cipher. This again confirmed the efficiency of the proposed 2D-CLM based SVD compared with the 2D-CLM.

TABLE IV. HISTOGRAM DEVIATION TEST RESULTS USING THE PROPOSED 2D-CLM BASED SVD IMAGE CIPHER

Image	Irregular deviation values with 2D-CLM and the proposed 2D-CLM based SVD image cipher			
	2D-CLM	2D-CLM		
		S	V	D
Brabra	0	415.884*10 ⁻³	372.537*10 ⁻³	416.072*10 ⁻³
Boat	0	396.661*10 ⁻³	374.782*10 ⁻³	396.657*10 ⁻³
Pirate	0	427.85*10 ⁻³	374.78*10 ⁻³	428.04*10 ⁻³

E. Differential Metrics

Differential metrics are employed for testing the effect of one pixel modification in the input plainimage on the resulted cipherimage using 2D-CLM based SVD image cipher. Differential metrics may include both the Unified Average Changing Intensity (UACI) and the Number of Pixels Change Rate (NPCR) metrics. The NPCR calculates the percentage of unequal pixels in two ciphered images E1 and E2. The NPCR can be computed as follows [37-39]:

$$NPCR(E_1, E_2) = \frac{\sum_{i,j} D(x_i, y_j)}{M \times N} \times 100\%, \tag{8}$$

$$D(x_i, y_j) = \begin{cases} 1 & \text{if } E_1(x_i, y_j) \neq E_2(x_i, y_j) \\ 0 & \text{Otherwise} \end{cases} \tag{9}$$

Where M, N represent both the E1 and E2 height and width.

The UACI evaluates the variance average intensity among two encrypted images, CE1 and CE2. The UACI can be computed as [37-39]:

$$UACI(CE_1, CE_2) = \frac{1}{M \times N} \left[\sum_{x_i, y_j} \frac{CE_1(x_i, y_j) - CE_2(x_i, y_j)}{255} \right] \times 100\%, \tag{10}$$

The results of NPCR and UACI between two cipherimages with a modification in one-pixel in their respected plainimages using the proposed 2D-CLM based SVD image cipher are given in Table V. The NPCR and UACI evaluations prove that the proposed 2D-CLM based SVD image cipher is sensitive to tiny changes in the tested images which indicate a good encryption.

TABLE V. NPCR/UACI TEST RESULTS USING THE PROPOSED 2D-CLM BASED SVD IMAGE CIPHER

Image	Irregular deviation values with 2D-CLM and the proposed 2D-CLM based SVD image cipher				
		2D-CLM	2D-CLM		
			S	V	D
Brabra	NPCR	99.3606	100	100	100
	UACI	0	0	0	0
Boat	NPCR	99.0112	100	100	100
	UACI	0	0	0	0
Pirate	NPCR	99.2935	100	100	100
	UACI	0	0	0	0

V. CONCLUSIONS

The paper presented an efficient and secure 2D-CLM based SVD image cipher. The proposed 2D-CLM based SVD image cipher is inspected, examined and investigated with a group of different encryption quality metrics such as visual inspecting, histogram examination, entropy testing, encryption quality measures and differential testing. The obtained test outcomes proved the superiority and affectivity of 2D-CLM based SVD image cipher in terms of different encryption quality metrics.

REFERENCES

- [1] A. A. A. El-Latif, L. Li, and X. Niu, "A new image encryption scheme based on cyclic elliptic curve and chaotic system," *Multimedia Tools and Applications*, vol. 70, no. 3, pp. 1559–1584, 2014.
- [2] Osama S. Faragallah, "Secure Audio Cryptosystem Using Hashed Image LSB watermarking and Encryption," *Wireless Personal Communication*, vol. 98(2), pp. 2009–2023, 2018, Springer (ISI JCR IF 2016: 0.951).
- [3] Fuwen Liu, Hartmut Koenig, "A Survey of Video Encryption Algorithms," *Journal of Computers & Security*, Vol. 19, No. 1, 2010, pp. 3–15.
- [4] Esam Elsheh and Ben Hamza "Secret Sharing Approaches for 3D Object Encryption," *Journal of Expert Systems with Applications*, Vol. 38 , No. 11, 2011, pp. 13906–13911.
- [5] X. Zhang, X. Fan, J. Wang, and Z. Zhao, "A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution," *Multimedia Tools and Applications*, vol. 75, no. 4, pp. 1745–1763, 2016.
- [6] Xiaofeng Chen, Xinyi Huang, Jin Li, Jianfeng Ma, Wenjing Lou and Duncan Wong "New Algorithms for Secure Outsourcing of Large-scale Systems of Linear Equations," *IEEE Transactions on Information and Forensics Security*, Vol. 10, No. 1, 2015, pp. 69–78.
- [7] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.
- [8] Ibrahim F. Elashry, Osama S. Faragallah, Alaa M. Abbas , S. El-Rabaie, Fathi E. Abd El-Samie, "Homomorphic image encryption," *Journal of Electronic Imaging* 18(3), 033002, 2009.
- [9] Heba M. Elhoseny, Hossam E. H. Ahmed, Alaa M. Abbas, Hassan B. Kazemian, Osama S. Faragallah, Sayed M. El-Rabaie, Fathi E. Abd El-Samie, "Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation," *Signal, Image and Video Processing Journal*, vol. 9(3), pp. 611–622, 2015.
- [10] Fuyan Sun, Shutang Liu, Zhongqin Li, and Zongwang Lü, "A novel image encryption algorithm based on spatial chaos map," *Chaos, Solitons and Fractals* vol. 38, pp. 631–640, 2008.
- [11] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," John Wiley and Sons, Indianapolis, IN, USA, 2015.
- [12] S. Contini, R. L. Rivest, M. J. B. Robshaw, and Y. L. Yin, "The Security of The RC6TM Block Cipher", RSA Laboratories, M. I. T Laboratory for Computer Science, Version 1.0 - August 20, 1998.
- [13] A. H. M. Ragab, N. A. Ismail, and O. S. FaragAllah, "Enhancements and Implementation of RC6 Block Cipher for Data Security", *Proceedings of International Conference on Electrical and Electronic Technology*, Vol. 1, pp. 133–137, 2001.
- [14] Luanlan, "The AES Encryption and Decryption Realization Based on FPGA", *Seventh International Conference on Computational Intelligence and Security (CIS)*, pp. 603 – 607, 2011.
- [15] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES implementation on a grain of sand," *IEEE Proceedings of Information Security*, vol. 152, no. 1, pp. 13–20, 2005.
- [16] Yuling Luo, Minghui Du, "A Novel Digital Image Encryption Scheme Based on Spatial-chaos", *Journal of Convergence Information Technology (JCIT)*, Vol. 7, N. 3, February 2012.
- [17] Shan Gai, Guowei Yang, Sheng Zhang, "Multiscale texture classification using reduced quaternion wavelet transform. *International Journal of Electronics and Communications*, 2013,67(3):233–241.
- [18] Majid Khan, and Tariq Shah, "A Literature Review on Image Encryption Techniques", *3D Res*, vol. 29(5), 2014.
- [19] G. A. Sathishkumar, K. Bhoopathybagan, N. Sriraam, S. P. Venkatachalam, R. Vignesh, "A Novel Image Encryption Algorithm Using Two Chaotic Maps for Medical Application", *Advanced Computing Communication in Computer and Information Science*, Berlin-Heidelberg: Springer-Verlag, vol.133, pp. 290–299, 2011.
- [20] Li Y, Zhang F, Li Y, Tao R., "Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform," *Opt. Lasers Eng.*, vol. 72, pp. 18–25, 2015.
- [21] Ensherah A. Naeem, Mustafa M. AbdElNaby, Hala S. El-sayed, Fathi E. Abd El-Samie, and Osama S. Faragallah, "Wavelet Fusion for Encrypting Images with a Few Details," *Computers and Electrical Engineering*, vol. 54, pp. 450–470, 2016.
- [22] Chen L, Zhao D., "Image encryption with fractional wavelet packet method," *Optik*, vol. 119, pp.286–291, 2008.
- [23] 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, Article ID 013014, 2012.
- [24] Sabry S. Nassar, Nabil M. Ayad, Hamdy M. Kelash, Hala S. El-sayed, Mohsen A. M. El-Bendary Fathi E. Abd El-Samie, Osama S. Faragallah, "Secure Wireless Image Communication Using LSB Steganography and Chaotic Baker Ciphering," *Wireless Personal Communication*, vol. 91(3), pp. 1023–1049, 2016.
- [25] Liu S, Mi Q, Zhu B., "Optical image encryption with multistage and multichannel fractional Fourier-domain filtering," *Opt. Lett.*, vol. 26, pp. 1242–1244, 2001.
- [26] Zhang Y, Zheng CH, Tanno N., "Optical encryption based on iterative fractional Fourier transform," *Opt. Commun.*, vol. 202, pp. 277–285, 2002.
- [27] Chen L, Zhao D., "Color image encoding in dual fractional Fourier-wavelet domain with random phases," *Opt. Commun.* vol. 282, pp. 3433–3438, 2009.
- [28] Prasad A, Kumar M, Choudhury DR., "Color image encoding using fractional Fourier transformation associated with wavelet transformation," *Opt. Commun.*, vol. 285, pp. 1005–1009, 2012.
- [29] Kumar M, Agrawal S., "Color image encoding in DOST domain using DWT and SVD," *Opt. Laser Technol.*, vol. 75, pp. 138–145, 2015.
- [30] Chen L, Zhao D, Ge F., "Image encryption based on singular value decomposition and Arnold transform in fractional domain," *Opt. Commun.* vol. 291, pp. 98–103, 2013.
- [31] Chai Wah Wu, Nikolai F. Rul kov, "Studying Chaos via 1-D Maps", *IEEE Transactions on Circuits and Systems: Fundamental Theory and Applications*, vol. 40(10), 1993.
- [32] B. Sarwar , G. Karypis, J. Konstan, J. Riedl, "Incremental Singular Value Decomposition Algorithms for Highly Scalable Recommender Systems," *Fifth International Conference on Computer and Information Science*, pp. 27–28, 2002.
- [33] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
- [34] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Optics and Lasers in Engineering*, vol. 91, pp. 41–52, 2017.
- [35] H. Elkamchouchi and M. A. Makar, "Measuring encryption quality of Bitmap images encrypted with Rijndael and KAMKAR block ciphers," in *Proceedings Twenty second National Radio Science Conference (NRSC 2005)*, pp. C11, Cairo, Egypt, Mar. 15,17, 2005.
- [36] I. Ziedan, M. Fouad, and D. H. Salem, "Application of Data encryption standard to bitmap and JPEG images," *Proceedings Twentieth National Radio Science Conference*, pp. C16, Egypt, Mar. 2003.
- [37] Osama S. Faragallah, Ashraf Afifi, "Optical Color Image Cryptosystem Using Chaotic Baker Mapping Based-Double Random Phase Encoding", *Optical and Quantum Electronics*, vol. 49(3):89, pp. 1–33, 2017.
- [38] Fatma Elgendy, Amany M. Sarhan, Tarek E. Eltobely, S. F. El-Zoghdy, Hala S. El-sayed, Osama S. Faragallah, "Chaos-based model for encryption and decryption of digital images," *Multimedia Tools and Applications*, vol. 75(18), pp. 11529–11553, 2016, Springer (ISI JCR IF 2016: 1.530).
- [39] Osama S. Faragallah, "Optical Double Color Image Encryption Scheme in the Fresnel-based Hartley Domain Using Arnold Transform and Chaotic Logistic Adjusted Sine Phase Masks," *Optical and Quantum Electronics*, vol. 50(3):118, pp. 1–27, 2018.