ISSN: 2277-3061
Volume: 17 Issue: 1
International Journal of Computers and Technology

Chaos Baker-based Image Encryption in Operation Modes

Mohammed A. AlZain

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

Email: m.alzain@tu.edu.sa

Abstract

This research paper study the application of chaos baker map for digital image encryption in different operation modes. The employed modes include the electronic code book (ECB), cipher block chaining (CBC), output feedback chaining (OFB), and cipher feedback chaining (CFB). The proposed method works by applying the chaos baker map in different operation modes for encrypting digital images. A group of tests were carried out to examine the impact of operation modes on chaos baker-based encryption. This is done using several encryption metrics like visual inspection, statistical measures, entropy measure, encryption quality measures, and noise resistance measures. Simulation results demonstrated the effectively of baker-based encryption in CBC mode.

Indexing terms/Keywords: Image encryption, Chaos Baker map, ECB, CBC, OFB, CFB.

1. Introduction

Images, as one of most famous media types, are widespread over various networks. How to prevent images from illegal copying and distribution in the era of the Internet is a critical issue. Therefore, image encryption has become recently a hot research topics in information security. Although there exist some classical schemes like the Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), and the Advanced Encryption Standard (AES) for information security [1], they usually cannot be directly applied to image encryption to yield satisfactory results since intrinsic features of images like bulky capacity, high correlation, and large redundancy [2–4]. In contrast, the chaos-based image encryption has attracted much attention for research purposes and has been demonstrated to be effective and secure in recent years [5–9]. Chaotic systems have the following properties: pseudo randomness, extreme initial values sensitivity and system parameters, and ergodicity, which make it very desirable in image encryption [10]. Typically, chaos based image ciphering framework includes chaotic sequence generation, pixel position permutation, and pixel value diffusion. One-dimensional (1D) chaos maps have easy forms and are simple to apply, and thus some researchers used them to encrypt images. For example, the authors used two 1D chaotic Logistic maps to generate the pseudorandom sequence for image encryption in [11]. Boriga et al. presented a 1D chaos map for real-time image ciphering [12]. However, since the 1D chaotic systems usually have only one variable and few parameters, along with relatively simple structures and chaotic orbits, it is easy to estimate the orbits and to predict the initial values and/or parameters by little information extracted from them [13]. Therefore, in order to improve image encryption security, chaotic systems with two or more dimensions have been applied to image encryption. Fridrich put forward symmetric ciphers with two-dimensional (2D) chaotic maps and the experimental results demonstrated good diffusion features regarding the key and the plain image [14]. Using the chaotic three-dimensional (3D) cat map extended from 2D Arnold's cat map [15] and 3D Chen's chaotic system [16], Chen et al. presented a symmetric image cipher method for alternative permutation and diffusion [5]. The Lyapunov exponent (LE) is a type of measurement methodology for chaotic level, and a chaotic system is said to be hyperchaotic if it has two or more positive LEs [17]. Since hyperchaotic systems have more advantages such as richer dynamic phenomena and higher randomness than common chaotic systems, lots of hyperchaotic systems have been employed to encrypt images [18–21]. For example, Norouzi et al. used the key stream generated by a hyperchaotic system to perform one round diffusion on the image to attain good results [20]. Yuan et al. presented a parallel image cryptosystem using the Logistic map and a five-dimensional

(5D) hyperchaotic system [21]. Most of the above-mentioned literature uses integral-order chaotic systems for image encryption. It has been reported that fractional-order hyperchaotic systems, as a counterpart of integral-order chaos, show higher nonlinearity and degrees owing to the complex geometrical interpretation of fractional derivatives for the nonlocal effects either in time or in space [22, 23]. Therefore, the fractional-order hyperchaotic systems have great potential in information security. Wang et al. applied a fractional order hyperchaotic Lorenz to color image encryption. To enhance the security of images, both system parameters and derivative order were hidden in scheme [23]. The 3D fractional-order Lorenz system and Chen chaotic systems were employed to encrypt images by Wu et al. and Zhao et al., respectively [3, 24]. Huang et al. used a four-dimensional (4D) fractional-order hyperchaotic neural network system to cipher color images, and the experiments demonstrated the effectiveness of the system [25].

The reminder of this research is marshaled as follows: In section 2, fundamental knowledge regarding 2D chaos baker map and operation modes are presented. Section 3 explains the chaos baker-based encryption/decryption with operation modes. Section 4 presents the performance of proposed chaos baker-based encryption/decryption with operation modes. Section 5 concludes this research.

2. Fundamental Knowledge

2.1 2D Chaos Baker map

The chaos 2D baker map, BM is represented as [14]:

$$\begin{aligned} &BM(m,n) = (2m,\ n/2), && 0 =< m < 0.5 \\ &BM(m,n) = (2m-1,\ n/2 + 1/2), && 0.5 =< m <= 1 \end{aligned} \tag{1}$$

2.2 Modes of Operation

This subsection explores and summarizes the different operation modes. These operation modes may include ECB, CBC, OFB, and CFB.

2.2.1 ECB Operation Mode

With the ECB operation mode , the plainimage is split into equal size blocks of n-bits for each block. Every block is individually encrypted and decrypted using same key k as given by Eqs. 2 and 3, respectively [26]:

$$CI_i = E_K(PI_i) \tag{2}$$

$$PI_i = D_K(CI_i) \tag{3}$$

2.2.2 CBC Operation Mode

With the CBC operation mode , a fixed length Initialization Vector (IV) is firstly initialized. The CBC operation mode individually encrypts and decrypts each block as given by Eqs. 5 and 6, respectively [27].

$$CI_0 = IV \tag{4}$$

$$CI_j = E_K(CI_{j-1} \oplus PI_j) \tag{5}$$

$$PI_j = D_K(CI_j) \oplus CI_{j-1}, \quad j = 1,2,3,..... \tag{6}$$

ISSN: 2277-3061
Volume: 17 Issue: 2
International Journal of Computers and Technology

2.2.3 CFB Operation Mode

With the CFB operation mode , a fixed length Initialization Vector (IV) is firstly initialized like in CBC. The CFB mode XORs the input block with the previously ciphered block to produce the new encrypted block. The encryption/decryption in CFB can be described using Eqs. 9 and 10, respectively [28].

$$CI_j = PI_j \oplus V_j \tag{9}$$

$$PI_j = CI_j \oplus V_j \tag{10}$$

$$V_j = E_K(CI_{j-1}), \quad j = 1,2,3,..... \tag{11}$$

$$CI_0 = IV \tag{12}$$

2.2.4 OFB Operation Mode

The OFB operation mode as CBC and CFB employs also a fixed length Initialization Vector (IV). The encryption/decryption in OFB can be described using Eqs. 13 and 14, respectively [29].

$$CI_j = PI_j \oplus V_j \tag{13}$$

$$PI_j = CI_j \oplus V_j \tag{14}$$

$$V_j = E_K(V_{j-1}), \quad j = 1,2,3,..... \tag{15}$$

3. The Chaos Baker-Based Encryption/Decryption with Operation Modes

The chaos baker-based encryption/decryption with operation modes uses chaos baker map in different operation modes. Fig. 1 depicts encryption/decryption modules, respectively. The encryption module begins with reading the plainimage. Then, employ the chaos baker map encryption using EBC or CBC or CFB or OFB operation modes. The decryption module is the inverse of encryption module.

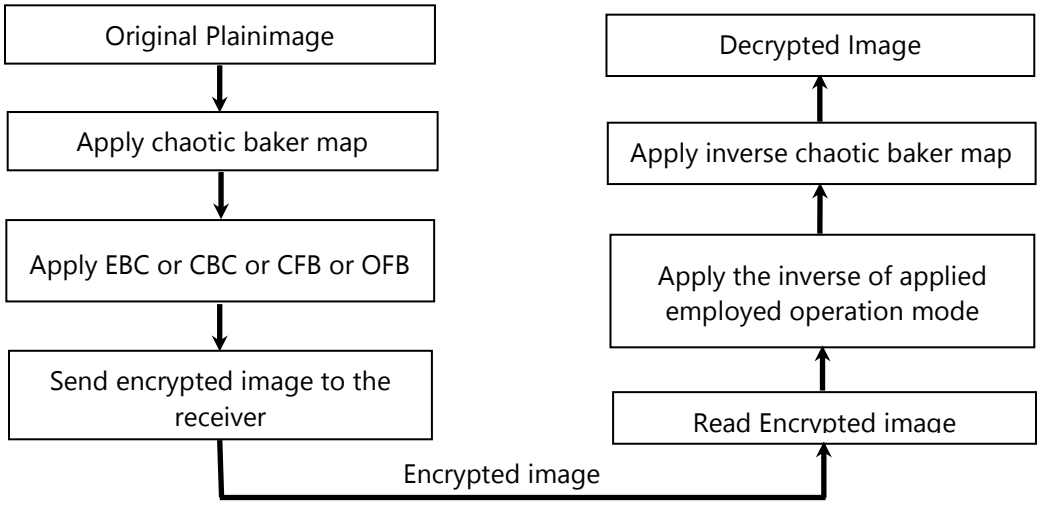

Fig. 1. Encryption/decryption modules of Chaos Baker-Based with Modes of Operation

ISSN: 2277-3061
Volume: 17 Issue: 2
International Journal of Computers and Technology

4. Security Study

The security study of chaos baker-based encryption/decryption with operation modes is tested using a set of encryption key metrics along with addition to the visual test. The chaos baker-based encryption is tested using a set of experiments to examine the impact using various operation modes like ECB, CBC, CFB, and OFB on the performance of chaos baker-based encryption on encrypting gray level images. Such experiments may include various encryption/decryption quality measures on different test images; like Fruits, peppers and Water lilies images illustrated in Fig. 2.

a) Fruits b) Peppers c) Water lilies

Fig. 2. Test Images

4.1 Visual Test

The impact of using chaos baker-based with operation modes in encrypting images is explored. The results of chaos baker-based with operation modes are depicted Fig. 3. Using visual test, it is realized that the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes gives good results. In addition, the details of encrypted images by chaos baker-based with ECB, CBC, CFB, OFB operation modes are completely vanished which indicates good quality.

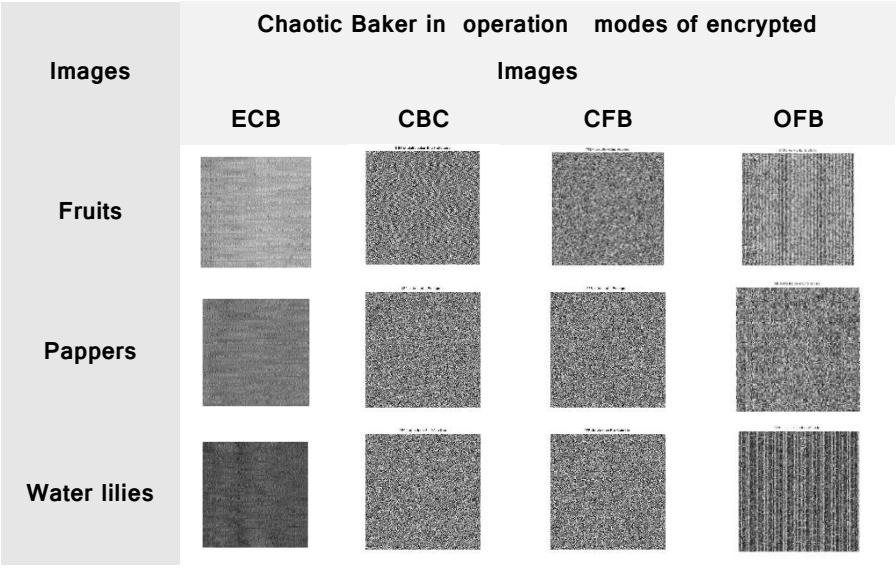

Fig. 3. Encryption results using chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes

4.2 Histogram Test

The histogram of original tested plainimages and their respected encrypted images using the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes are given in Fig. 4. It is noted that histograms of all tested images using the chaos baker-based encryption with CBC, CFB, OFB are uniform and completely distinguished from the histograms of plainimages. Such results reveal the capability of the chaos baker-based encryption with CBC, CFB, OFB operation modes to efficiently encrypt images. But, it is seen that histograms of encrypted images using the chaos baker-based encryption with ECB are not uniform and look like the histogram of original plainimages which indicates inefficiency of ECB mode in encrypting information.

ISSN: 2277-3061
Volume: 17 Issue: 2
International Journal of Computers and Technology

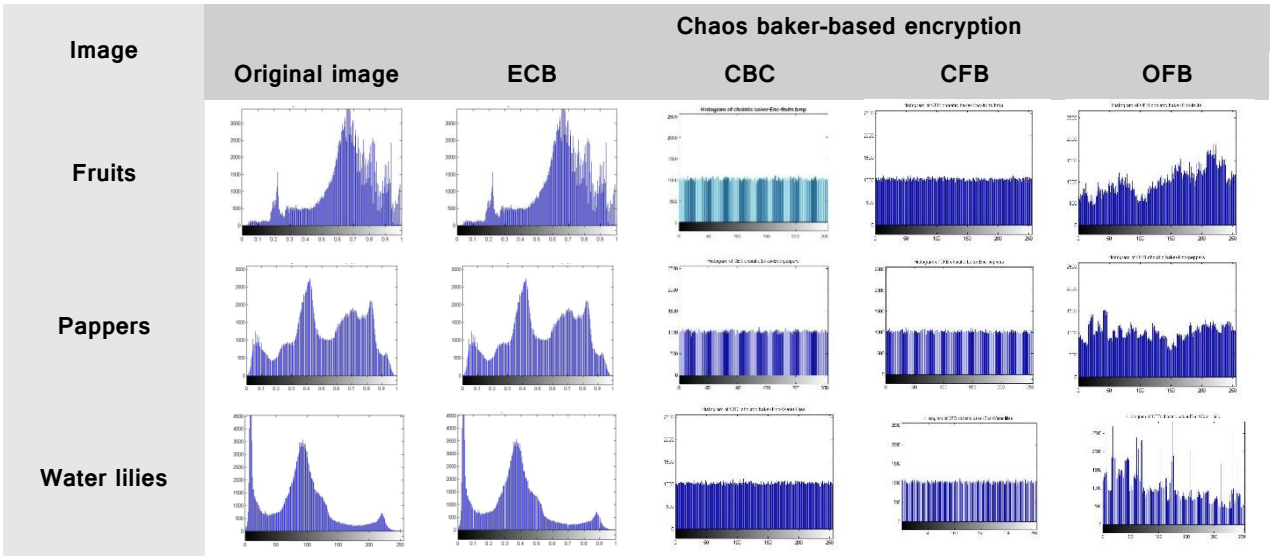

Fig. 4. Histogram results of plainimages/cipherimages using chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes

4.3 Entropy Measure

The entropy measure is employed to test the encrypted images resulted by chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes The entropy as encryption quality indicator can is defined in Eq. 16 as follows [30]:

$$ET = -\sum_{i=1}^{n} P_r(x_i) \log P_r(x_i) \quad (16)$$

Where xi is the intensity value for ith point. So, large entropy means that the ciphering is good.

The entropy results by the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes are depicted in Table 1. The results demonstrated that entropy values for encrypted images using the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes are higher than entropy values of plainimages. Also, the entropy values of encrypted images by chaos baker-based encryption with CBC, CFB, OFB operation modes are good . Also, the entropy values of encrypted images by chaos baker-based encryption with ECB operation mode the smallest compared to CBC, CFB, OFB operation modes.

Table 1: Entropy of encrypted images using chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes

Images	Chaos baker-based encryption			
	ECB	CBC	CFB	OFB
Fruits	7.4515	7.9994	7.9992	7.9327
Pappers	7.5937	7.9992	7.9993	7.9780
Water lilies	7.1722	7.9993	7.9993	7.8620

4.4 Encryption Quality Measures

The encryption quality measures are employed to examine, test and compare the encryption quality of the produced encrypted images. The encryption quality measures include correlation coefficients (Cr), irregular deviation (Id) and histogram deviation (Hd).

4.4.1 Correlation Coefficients (Cr)

The correlation coefficients (Cr) is measured between the plainimage and its corresponding cipherimage using the formula [31]:

$$C_r = \frac{\text{cov}(P,C)}{\sqrt{D(P)}\sqrt{D(C)}}, \tag{17}$$

Low values of Cr among plainimage (P) and cipherimage (C) indicates good encryption quality.

The correlation coefficients results Cr by the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes are depicted in Table 2. The results demonstrated that Cr values beteen plainimage and its corresponding cipherimage using the chaos baker-based encryption with ECB, CBC, CFB and OFB are close to zero which indicate good encryption. Also, the results demonstrated that Cr values using the chaos baker-based encryption with CBC, CFB, OFB operation modes are better than the chaos baker-based encryption with ECB.

Table 2: Correlation coefficient results using chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes

Images	Chaos baker-based encryption			
	ECB	CBC	CFB	OFB
Fruits	-0.0298	-0.0027	0.00065	0.0025
Pappers	0.0080	-0.0013	0.0025	8.2698e-004
Water lilies	0.0048	0.0033	0.0019	0.0049

4.4.2 Irregular Deviation (ID)

The ID computes encryption efficiency by how much abnormal caused by encryption. The IR is computed using the formula [32]:

$$I_D = \frac{\left|\sum_{i=0}^{255}|h(i) - M_h|\right|}{MxN}, \tag{18}$$

where h(i) defines cipherimage histogram at intensity level i, and M_h is the average histogram of ideal encrypted. Low values of ID indicates good encryption quality.

The Irregular Deviation (ID) results using the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes are depicted in Table 3. The results demonstrated that ID values using the chaos baker-based encryption with CBC, CFB and OFB are better (low) compared to ID values produced using the chaos baker-based encryption with ECB. This ensures the superiority of the chaos baker-based encryption with CBC, CFB and OFB compared to ECB.

ISSN: 2277-3061
Volume: 17 Issue: 2
International Journal of Computers and Technology

Table 3: Irregular Deviation results using chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes

Images	Chaos baker-based encryption			
	ECB	CBC	CFB	OFB
Fruits	0.8769	0.5695	0.5746	0.6578
Pappers	0.8296	0.6330	0.6370	0.6191
Water lilies	0.8574	0.5426	0.8227	0.6519

4.4.3 Histogram Deviation (HD)

The HD computes encryption quality by how much it increases the variation among plainimage (P) and cipherimage (C). The HD is computed using the formula [33]:

$$H_D = \frac{\left|\sum_{i=0}^{255} d(i)\right|}{MxN}, \quad (19)$$

where $d(i)$ is difference value among the plainimage (P) and cipherimage (C) at pixel level ith. M and N are image height and width. High ID values indicates good encryption quality.

The Histogram Deviation (HD) results using the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes are illustrated in Table 4. The obtained results show that HD values using chaos baker-based encryption with CBC, CFB and OFB are better (high) compared to HD values produced using the chaos baker-based encryption with ECB. This again ensures the superiority of the chaos baker-based encryption with CBC, CFB and OFB compared to ECB.

Table 4: Histogram Deviation results using chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes

Images	Chaos baker-based encryption			
	ECB	CBC	CFB	OFB
Fruits	0	0.7245	0.7257	0.5803
Pappers	0	0.5521	0.5521	0.6353
Water lilies	0	0.8231	0.8227	0.8106

4.5 Differential measures

Differential measures examines the impact of modifying just only one pixel on cipherimage using the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes. The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) measures are utilized in investigating the chaos baker-based encryption with ECB, CBC, CFB, OFB. The NPCR evaluates unalike pixel numbers percentage in two encrypted images CE1 and CE2. The NPCR can be computed as [30, 34]:

$$NPCR(CE_1, CE_2) = \frac{\sum_{i,j} D(x_i, y_j)}{M \times N} \times 100\%, \quad (20)$$

$$D(x_i, y_j) = \begin{cases} 1 & if \quad CE_1(x_i, y_j) = CE_2(x_i, y_j) \\ 0 & \text{Otherwise} \end{cases} \tag{21}$$

where M, N are the height and width of CE1 and CE2. The UACI evaluates the variance average intensity among two encrypted images, CE1 and CE2 The UACI can be computed as [30]:

$$UACI(CE_1, CE_2) = \frac{1}{M \times N}\left[\sum_{x_i y_j} \frac{CE_1(x_i, y_j) - CE_1(x_i, y_j)}{255}\right] \times 100\%, \tag{22}$$

Table 5: NPCR and UACI results using chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes

Image		Chaos baker-based encryption			
		ECB	CBC	CFB	OFB
Fruits	NPCR	99.2863	99.6128	99.6181	99.5415
	UACI	0	0	0	0
peppers	NPCR	99.4221	99.6117	99.6029	99.6223
	UACI	0	0	0	0
Water Lilies	NPCR	98.7061	99.6113	99.5953	99.5735
	UACI	0	0	0	0

The results of NPCR and UACI between two cipherimages with a modification in one-pixel in their respected plainimages using the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes are listed in Table 5. The NPCR and UACI evaluations prove that the chaos baker-based encryption with ECB, CBC, CFB, OFB different operation modes are sensitive to any small modification in the images which mean a powerful encryption.

4.6 Noise Resistance

The resistance of the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes regarding additive White Gaussian Noise (AWGN) is examined in decryption process. The PSNR measure is utilized to evaluate the decrypted image. The PSNR can be computed as [30]:

$$PSNR(I, D) = 10 \log \frac{(255)^2}{\sum_{i=0}^{W-1} \sum_{j=0}^{H-1} [DI(x_i, y_j) - PI(x_i, y_j)]^2} \tag{23}$$

where $PI(x_i, y_j)$ and $DI(x_i, y_j)$ are the plainimage and decrypted mage, respectively. Large PSNR values ensure good noise immunity.

The obtained PSNR using the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes in the presence of AWGN of different variances on decrypted images are depicted in Table 6. It is noticed that the PSNR for all decrypted images using the chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes increases as increasing the noise variances on the encrypted images. Also, it is noticed that, the maximum PSNR is achieved using the chaos baker-based encryption with ECB operation mode . The PSNR values attained using the chaos baker-based encryption with CBC, CFB, OFB operation modes are low compared to ECB. This results ensures the superiority of the chaos baker-based encryption with ECB operation mode in terms of noise immunity over CBC, CFB, OFB operation modes.

ISSN: 2277-3061
Volume: 17 Issue: 2
International Journal of Computers and Technology

Table 6: PSNR results using chaos baker-based encryption with ECB, CBC, CFB, OFB operation modes

Image name	Operation mode	Chaos baker-based encryption					
		AWGN			Salt & pappers		
		μ=0 $\sigma = 0.05$	μ=0 $\sigma = 0.1$	μ=0 $\sigma = 0.15$	0.01	0.05	0.1
Fruits	ECB	9.4468	9.4468	9.4468	10.8951	10.4254	9.9021
	CBC	8.4367	8.4251	8.4213	16.4454	10.8234	9.2140
	CFB	8.4284	8.4286	8.4198	16.5664	10.8116	9.2423
	OFB	8.4250	8.4080	8.4196	16.4281	10.7741	9.2325
Peppers	ECB	9.6192	9.6192	9.6192	9.6192	9.5192	9.2131
	CBC	8.8872	8.8684	8.8750	16.9032	11.2367	9.6553
	CFB	8.8751	8.8673	8.8761	19.9214	11.2305	9.6828
	OFB	8.858	8.8708	8.8806	16.9032	11.2367	9.6553
Water lilies	ECB	9.4736	9.4736	9.4736	10.3704	9.9501	9.4736
	CBC	7.9740	7.9910	7.9865	16.0972	10.3700	8.7878
	CFB	7.9958	7.9862	7.9938	16.0971	10.3669	8.7656
	OFB	7.9479	7.9992	7.9911	15.9176	10.3179	8.8050

5. Conclusion

The paper investigates the chaos baker-based encryption in different operation modes like ECB, CBC, CFB, OFB. The chaos baker-based encryption is tested using a large set of encryption quality measures in different operation modess. In terms of encryption efficiency measures, the experimental results demonstrated the efficiency of the chaos baker-based encryption with CBC, CFB, OFB operation modes over the chaos baker-based encryption with ECB operation mode . In terms of noise immunity measures, the experimental results show the efficiency and superiority of the chaos baker-based encryption with ECB operation mode compared with the chaos baker-based encryption with CBC, CFB, OFB operation modes.

References

[1] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," John Wiley and Sons, Indianapolis, IN, USA, 2015.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] Z. Zhu, W. Zhang, K. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," Information Sciences, vol. 181, no. 6, pp. 1171–1186, 2011.

[7] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," Optics & Laser Technology, vol. 82, pp. 121–133, 2016.

[8] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," Optics and Lasers in Engineering, vol. 78, pp. 17–25, 2016.

[9] 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.

[10] 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.

[11] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, no. 9, pp. 926–934, 2006.

[12] R. Boriga, A. C. Dascalescu, and A.-V. Diaconu, "A new one-dimensional chaotic map and its use in a novel real-time image encryption scheme," Advances in Multimedia, vol. 2014, Article ID 409586, 15 pages, 2014.

[13] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, and V. Fernandez, "On the security of a new image encryption scheme based on chaotic map lattices," Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 18, no. 3, Article ID 033112, 2008.

[14] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," International Journal of Bifurcation and Chaos, vol. 8, no. 6, pp. 1259–1284, 1998.

[15] G. Chen and X. Dong, "From Chaos to Order: Methodologies, Perspectives, and Applications," Series on Nonlinear Science, World Scientific, 1998.

[16] T. Ueta and G. Chen, "Bifurcation analysis of Chen's equation," International Journal of Bifurcation and Chaos, vol. 10, no. 8, pp. 1917-1931, 2000.

[17] Wolf, J. B. Swift, and H. L. A. Swinney, "Determining Lyapunov exponents from a time series," Physica D: Nonlinear Phenomena, vol. 16, no. 3, pp. 285–317, 1985.

[18] Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," Optics Communications, vol. 285, no. 1, pp. 29-37, 2012.

[19] Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," Multimedia Tools and Applications, vol. 71, no. 3, pp. 1469-1497, 2014.

[20] N. Zhou, Y. Hu, L. Gong, and G. Li, "Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations," Quantum Information Processing, vol. 16, no. 6, 2017.

[21] H.-M. Yuan, Y. Liu, T. Lin, T. Hu, and L.-H. Gong, "A new parallel image cryptosystem based on 5D hyper-chaotic system," Signal Processing: Image Communication, vol. 52, pp. 87–96, 2017.

[22] Podlubny, I. Petráš, B. M. Vinagre, and L. Dorcák, "Analogue realizations of fractional-order controllers," Nonlinear Dynamics, vol. 29, no. 1-4, pp. 281-296, 2002.

[23] Z. Wang, X. Huang, Y.-X. Li, and X.-N. Song, "A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system," Chinese Physics B, vol. 22, no. 1, Article ID 010504, 2013.

[24] Zhao, S. Wang, Y. Chang, and X. Li, "A novel image encryption scheme based on an improper fractional-order chaotic system," Nonlinear Dynamics, vol. 80, no. 4, pp. 1721-1729, 2015.

[25] X. Huang, T. Sun, Y. Li, and J. Liang, "A color image encryption algorithm based on a fractional-order hyperchaotic system," Entropy, vol. 17, no. 1, pp. 28–38, 2014.

[26] Kuo-Tsang Huang, Jung-Hui Chiu, and Sung-Shiou Shen, "A Novel Structure with Dynamic Operation Mode for Symmetric-Key Block Ciphers," International Journal of Network Security & Its Applications (IJNSA). vol. 5(1): 19, pp. 2-13, 2013.

[27] William F. Ehrsam, Carl H. W. Meyer, John L. Smith, Walter L. Tuchman, "Message verification and transmission error detection by block chaining," US Patent 4074066, 1976.

[28] Morris Dworkin "Recommendation for Block Cipher Modes of Operation: Methods and Techniques," NIST Special Publication 800-38A, 2001. http://dx.doi.org/10.6028/NIST.SP.800-38A

[29] Davies, D. W.; Parkin, G. I. P. (1983). "The average cycle size of the key stream in output feedback encipherment," Advances in Cryptology, Proceedings of CRYPTO 82. New York: Plenum Press. pp. 263–282. ISBN 0306413663.

[30] Ensherah A. Naeem, Mustafa M. Abd Elnaby, Hala S. El-sayed, Fathi E. Abd El-Samie, and Osama S. Faragallah, "Wavelet Fusion for Encrypting Images with Few Details," Computers and Electrical Engineering, vol. 60, pp. 450-470, 2016.

[31] 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.

[32] 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.

[33] 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.

[34] 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.