Image Encryption Enabling Chaotic Ergodicity with Logistic and Sine Map

Mohammad Ahmar Khan[1]
College of Commerce and Business Administration
Dhofar University, Oman

Abdulrahman Abdullah Alghamdi[3]
College of Computing and Information Technology
Shaqra University, Shaqra 11961, Saudi Arabia

Jalaluddin Khan[2]*
School of Computer Science and Engineering
University of Electronic Science and Technology of China
Chengdu, 611731, China

Sarah Mohammed Awadh Bait Saidan[4]
College of Commerce and Business Administration
Dhofar University, Oman

***Abstract*—Chaotic systems with complicated characteristics of ergodicity, impredictability as well as sensitivity to beginning stages are commonly utilized in the world of cryptography. A 2D logistic-adjusted-sine (LS) map is implemented in this article. Performance assessments reveal superior ergodicity as well as unpredictable and even a broader spectrum of chaotics than numerous previous chaotic maps. This research also develops a 2D-LS-based image encryption system and proposed LS-IES. The notion of diffusion as well as confusion is properly complied with enabled encryption functions. Research outcomes as well as security analyses demonstrate that LS-IES can swiftly encrypting different parameters in various images with a great resistance towards security threats.**

Keywords*—Image encryption; ergodicity; logistic sine map; security; privacy

I. Introduction

Nowadays the advancement within digital technology as well as communications infrastructure, yet more digitized information is produced constantly communicated across networks, containing all sources of material in world [1]. Digital pictures include a common two-dimensional (2D) piece of content, typically contains a lot of information. The following are two illustrations: A image of a battleship can communicate not just about their dimensions as well as arms but rather about its geographical position as well as combat operation: a personalized photograph may sometimes indicate how it appears corresponding, and therefore its estimated physical state. As the digital image can hold significant indistinguishable content, image cybersecurity is becoming increasingly attractive. Picture encrypted among many types of image security methods is a visible means of changing a valuable actual image into something like an encrypted image that is not known as well as noise-less[2]–[4].

A digitized image is treated as dichotomous sequence as well as encrypted to most established systems including cryptographic benchmark as well as enhanced cryptography specification, as that of best technique among the encryption algorithm. Therefore, pixel consists usually 8 or even additional bits but there can be considerable association amongst consecutive frames. The significant correlation can persist while encoding a digital file in terms of binary sequence despite incorporating pixel characteristic as well as encryption effectiveness can still be relatively low. Consequently, various image-encoding systems were offered by numerous sorts of approaches, including magical cube [5], wavelet transform [6], [7], wave disturbance [8]and chaotic maps [9]–[12], in view of specific features of digitized images. As several scholars have indicated highlighted, although since mid-nineties numerous characteristics of chaos theory comparable to those encryption [13]–[16], analytical solutions were frequently utilized in image-based encryption but were extremely appropriate towards cryptography [17]–[19]. Whenever chaotic schemes are utilized in visual cryptography, the trustworthiness of privacy preservation depends heavily heavily onto performance of chaotic classifications implemented. For certain chaotic 1D processes, its chaotic cycles are very basic as well as completely predictable. After some data is collected, certain strategies can be used to approximate individual starting states [20]–[23].

The chaotic classification that has a straightforward nonlinear characteristic makes it easy to exploit appropriate image encryption technique [24]–[28]. A high-dynamic chaotic scheme feature complex chaotic conduct then are hard to anticipate future unpredictable orbits. Furthermore, technologies even have certain drawbacks, including difficult identification of problems as well as significant installation costs [5]. This study presents a novel, chaotic characteristics two dimensional map, with incorporation of logistics as well as sine map in terms of 2D LS-IES. Logistic map is used to regulate entrance of Sine map then afterwards expands their amplitude level between one dimensional to two dimensional. The assessments of efficiency demonstrate 2D-LS to be more chaotic, more ergodic as well as unpredictable than other current chaotic maps. This work also uses 2D-LS to create a 2D-LS image encryption technique (LS-IES). The confusion as well as diffusion are performed around pixel level. Simulation findings as well as security analyses demonstrate the LS-IES can randomly encrypted numerous photographic files (image) thus it is strongly able to prevent malicious activities.

*Corresponding Author

The remaining article proceeded at the section-based descriptions such as: Section II provides preliminaries about complex chaotic functions. Section III described the proposed concept about 2D LS-IES. Section IV is discussed with incorporated simulation and experimental setup of 2D LS-IES. Section V is illustrated with security analysis and comparative study of 2D LS-IES and at last concludes with Section VI.

II. Preliminaries about Chaotic Functions

The preliminaries about the chaotic functions in terms of one dimensional and two-dimensional functions including logistic as well as sine map represented as following:

A. Logistic Maps

The logistic function is a discreet analogue of something like logistic equation involving increasing population [29]. A logistic map is expressed quantitatively as following Eq. (1),

$$X_{i+1} = 4Kx_i(1 - x_i) \quad (1)$$

where K is well inside [0, 1] domain and logistic function is K [0.89,1], the logistic function declared within this rage is chaotic in nature.

B. Sine Maps

If function of sine has intakes that lie inside [0, π] region, their outcomes occur inside [0, 1] target area. Sine map is constructed through translating their parameters at [0, 1] as generating sine function. It has been characterized as following Eq. (2),

$$X_{i+1} = \mathrm{D}\,Sin(\pi x_i) \quad (2)$$

Here variable D is set to factor D [0, 1]. The complex chaotic sequence of Sine map is formally noticeable in nature such as D [0.87, 1].

C. Logistic Adjusted Sine Map

Here incorporating the 2D-LS algebraic formulation including each two well-known chaotic function such as logistic as well as sine as following Eq. (3):

$$\begin{cases} X_{i+1} = \{\ Sin\left(\pi\zeta\left(y_i+2\right)x_i\left(1-x_i\right)\right) \\ Y_{i+1} = \{\ Sin\left(\pi\zeta\left(x_i+2\right)y_i\left(1-y_i\right)\right) \end{cases} \quad (3)$$

When variable ζ [0, 1] is assigned to [0, 1]. 2D-LS is constructed using logistic as well as sinus mapping. The logistic polynomial x_i $(1 - x_i)$ is initially normalized by something like a coefficient of ζ as well as supplied through Sine map insight. The frequency field is again stretched between 1-diamention and 2-diamention. 2D-LS simultaneously affects two parameters as well as outcome couples (x_i+1, y_i+1) spread over the 2D phase plane. That has an additional significant action thus its results are harder to gauge comparing other Sine as well as Logistic Mapping.

III. 2D LS-IES Image Encryption

Employing 2D-LS, this part establishes a different LS-IES image encryption system, wherein cryptographic keys are being utilized to establish a minimum 2D-LS configuration to produce chaotic S matrix. Confusion as well as diffusion algorithms are useful to periodically adjust pixel placements as well as to alter number of pixels. The confusion as well as dispersion activities a single image can be encoded in a bunch of high randomized encrypted images. Fig. 1 shows the entire design of LS-IES.

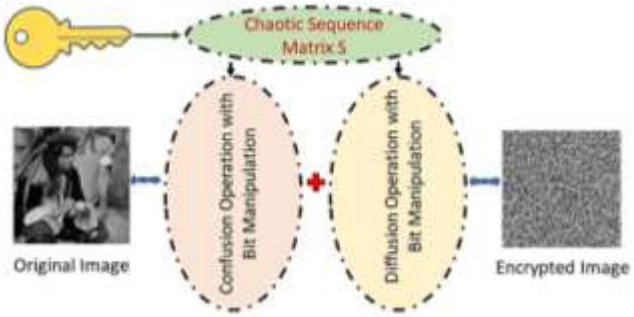

Fig. 1. The Concrete of 2D LS-IES Image Encryption.

A. Generation of Key

The generalization ability among the chaos-oriented encryption technique must ≥ 2^{100} to withstand the assault by brute force [30]. We have a cryptographic key of 232 bits, K = {X_0, Y_0, α, m, β, £} to meet this criterion as well as adjust it to the construction of the LS-IES. It comprises of four pieces, whereas β, £ are two interfering intensities (X_0, Y_0, α) as well as m are the interfering parameters. The activities of confusion as well as diffusion are adjusted onto pixel level. These protected findings seem to have the same formatting as both the actual pictures. LS-IES can therefore be used to digitized photos about any source.

B. Confusion through Bit Manipulation

The characteristics of confusion which demonstrates the number of outcomes would vary sensibly mostly on confidential key [31], [32]. The confusion of bit arbitrarily shifts pixel coordinates inside the image based on current chaotic binary sequence.

TABLE I. Bit Manipulation Algorithm

Confusion through Bit manipulation algorithm	
Input	Image I with chaotic sequence S and size of element K×L
Output	G operated result
	H initiated matrix of size K×L
	f=$\mathbf{log_2(KL)}$
	for i =1: K
	for j=1: L
	a= (i-1) L+ j
	ab=Bin (a, f)
	Hi,j =Joint(Si,j, ab,Ii,j)
	end
	end
	H=SortH(H)
	H=SortC(H)
	G=FetEnd ($H_{1:K\ 1:L}$, p)

Table I is explained about the processing algorithm in the certain steps, initially it takes input parameter in terms of original image with complex chaotic sequences S with the size of K×L. The whole algorithm is incorporated and generated with the confusion outcomes from the optimized bit manipulation process from the algorithm.

C. Diffusion through Bit Manipulation

The diffusion possessions showed that perhaps encrypted message must be highly responsive to unencrypted changes, meaning where each bit inside encrypted data can be altered with about fifty percent likelihood of occurrence [31], [32]. LAS-IES employs earlier pixel as well as a chaotic complex matrices S component to modify within contemporary pixel. The alteration through one pixel can be extended throughout the image sequence during computations within the proposed setup. Assume complex chaotic matrices S as well as confusion outcome G for bit manipulation algorithm are K × L, so that diffusion for bit manipulating is defined as following Eq. (4):

$$U_{i,j} = \begin{cases} G_{i,j} \oplus G_{K,L} \oplus S_{i,j}; \text{ for i=1; j=1;} \\ G_{i,j} \oplus U_{\text{i}-1,L} \oplus S_{i,j}; \text{ for j=1; i} \neq 1; \\ G_{i,j} \oplus U_{i,j-1} \oplus S_{i,j}; \text{ for j} \neq 1; \end{cases} \quad (4)$$

Whereas U recognizes as a consequence of bit diffusion manipulating, sign of $\oplus$ is bitwise XOR function. The methodology of decryption of whole portion is to perform reverse procedure stated as following Eq (5):

$$G_{i,j} = \begin{cases} U_{i,j} \oplus U_{\text{i,j}-1} \oplus S_{i,j}, \text{ for j} \neq 1; \\ U_{i,j} \oplus U_{\text{i}-1,L} \oplus S_{i,j}, \text{ for i} \neq 1, \text{j=1;} \\ U_{i,j} \oplus G_{\text{K,L}} \oplus S_{i,j}, \text{ for i=1 , j=1;} \end{cases} \quad (5)$$

After the confusion as well as diffusion of bit manipulating with separate complex chaotic vectors, a single original image can indeed be scrambled into an unidentifiable cipher-image matrix. The proposed concept at the entire setup recognizes that excellent diffusion as well as confusion effects can be achieved because premise of diffusion as well as confusion has been achieved. A high encrypted communications performance may be achieved as LS-IES requires only bit-level confusion in addition broadcast techniques. This has strong noise resistance or information leakage assault dependability. LAS-IES can indeed capture entire image having good graphical fidelity whenever an encrypted image contains turbulence or certain loss of data.

IV. Simulation and Discussion

We estimate the benefits of image encryption and it is supposed to encrypt various aspects of digital photos (Image data) using unpredictable cipher images. Mostly with the encryption credentials (key) can such a cipher picture to be deciphered successfully. This report outlines the LS-IES measured data as well as evaluates their dependability. We utilize R2018a MATLAB to construct LS-IES as well as deploy it to several digital image formats hereunder. Fig. 2 and Fig. 3 demonstrated the grayscale image simulated results. Using Fig. 2, we can also see that LS-IES may encrypted images (as mentioned A to C and A' to C') with a uniformly distributed to randomized cryptographic images. With the right equipment (Keys), the actual pictures can also be totally reconstructed. As illustrated in Fig. 2(A' to C') and Fig. 3(E' to G') the histograms of the underlying gray image as well as it is distributed randomly. In such scenarios, the intruders have difficulties accessing statistical data. The simulation work organized in the ecosystem which is Intel (R) Core (TM) i3-4030U CPU @ 1.90 GHz personal computer, Microsoft Windows 10 pro with 8GB RAM. Since individually encryption procedure is equally composite towards diverse undisclosed keys, LS-IES is technically more robust in contradiction of adversarial attack.

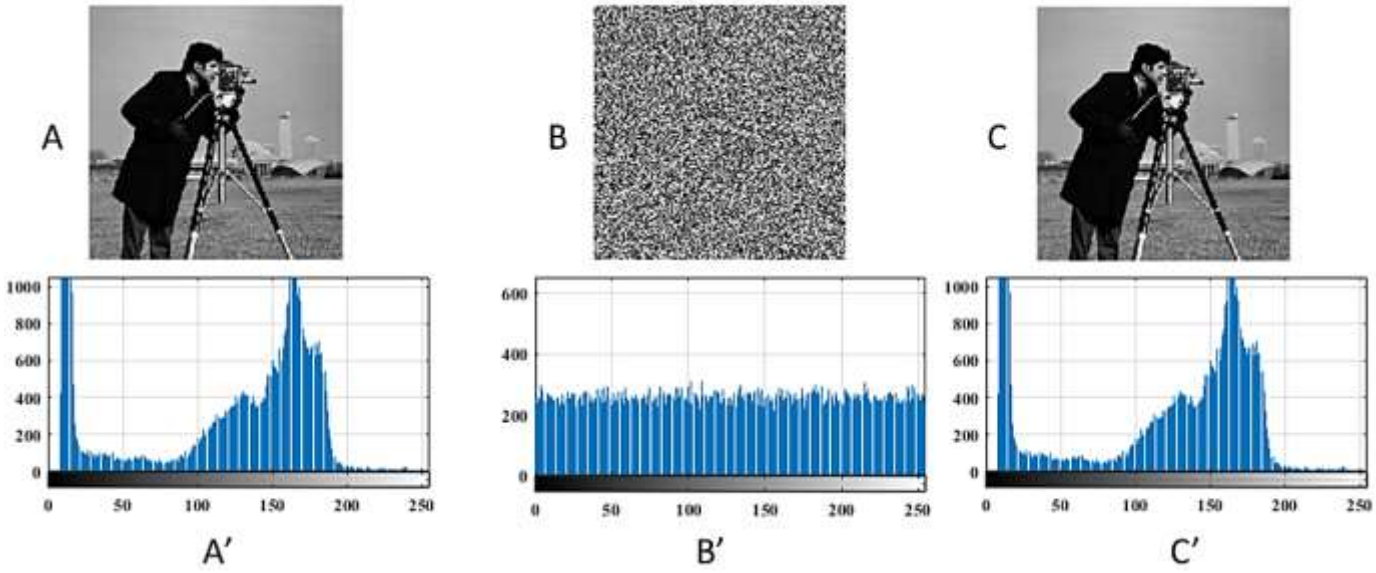

Fig. 2. Image Encryption Outcomes for the Cameramen Image.

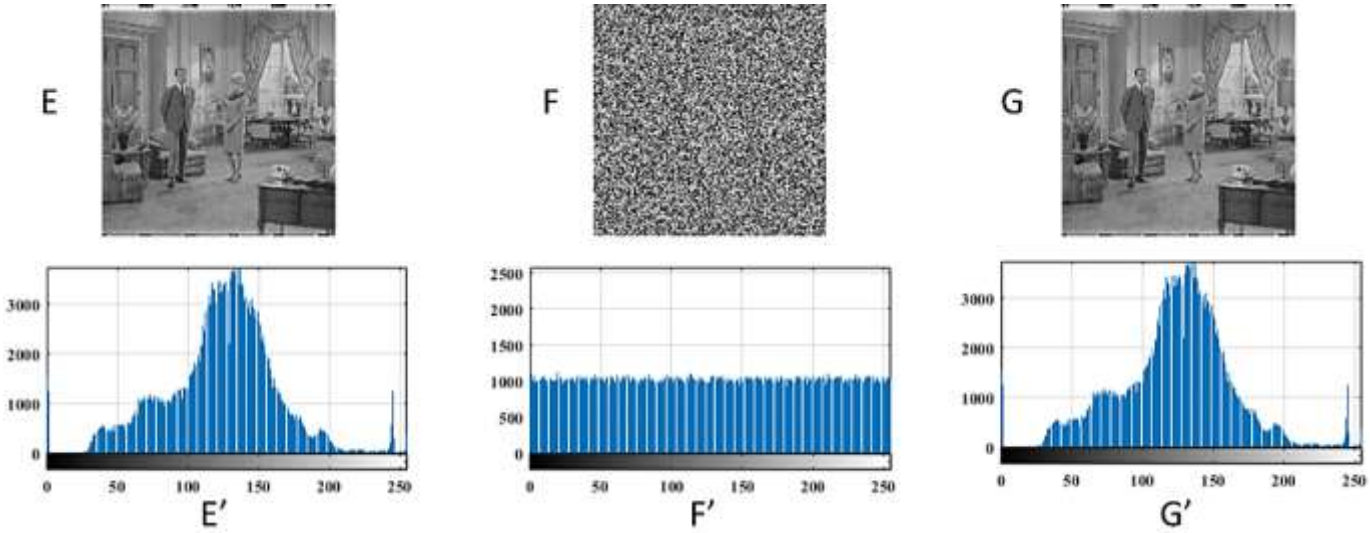

Fig. 3. Image Encryption Outcomes for the Meeting Image.

V. Security Analysis

This subsection shows effectiveness of its encryption algorithm to examine secure communication of LS-IES as well as its capacity to withstand conventional safety threats. The entire experimental setup is used gray scale test image from 'Miscellaneous' image dataset of USC-SIPI [33]. We compared this with other published state-of-the-art mechanism in the similar field of image encryption to highlight its benefits of LS-IES. Several simulation findings were used for the comparison of published data and cited that article with the references as mentioned at the reference section for the more clarity.

A. Histogram Analysis

Histogram is a homogenous as well as significantly separate histogram diagram only for idealized encrypted images, therefore prevents the adversary from getting significant evidence in the epidemiology including its encrypted images. This experiment showed histograms of the actual picture as well as encrypted image in Fig. 2(A', B' and C') and Fig. 3(E', F' and G'). Fig. 2 (B') and Fig. 3(F') demonstrates how cipher image histograms are consistent; those are unique histograms of actual pictures. These contains uniformly characteristics as a flat representation of cipher images. This encryption algorithm suggested about the enhanced and successfully avoidable any kind of statistical attacks.

B. Correlation Analysis

Throughout this investigation the actual as well as encrypted images have been picked by random means for the correlation testing of 1000 combinations of consecutive frames and afterwards coefficient of correlation have been computed in terms of directional such as horizontal (H), vertical (V) and diagonal (D). The coefficient of determination computation procedure incorporated from Eq. 6-11, whereas x and y indicate the gray values of consecutive frames.

$$CC_{xy} = \frac{\text{Covariance}(x,y)}{\sqrt{K(x)L(y)}} \tag{6}$$

$$\text{Covariance}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - A(x)\right)\left(y_i - B(y)\right) \tag{7}$$

$$K(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - A(x)\right)^2 \tag{8}$$

$$L(y) = \frac{1}{N}\sum_{i=1}^{N}\left(y_i - E(y)\right)^2 \tag{9}$$

$$A(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{10}$$

$$B(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{11}$$

Table II reveals that perhaps the correlations of unencrypted images are near 1; the encrypted images are near 0 that further confirms that the methodology implemented removes the interaction amongst neighboring pixels of unencrypted images.

TABLE II. Correlation Coefficient on Experimented Images

Image	Plain Images			Encrypted Images		
	H	V	D	H	V	D
5.1.14	0.8890	0.9186	0.8730	0.0040	0.0031	-0.0048
5.1.12	0.9649	0.9423	0.9289	0.0060	-0.0020	-0.0040
5.1.09	0.9280	0.9081	0.9121	-0.0049	-0.0030	0.0018

C. Differential Attacks

The demonstration of the differential attack is based on two premium criteria such as number of pixels change rate (NPCR) as well as unified average changing intensity (UACI). These two are key factor to distinguishing about the differential attacks exist at any image during the image encryption methods. These two are mythically demonstrated on Eq. 12 to 14 as following:

$$NPCR = \frac{\sum_{i,j} H(i,j)}{M \times N} \times 100\% \tag{12}$$

$$H(i,j) = \begin{cases} 0 & if\ C_1(i,j) = C_2(i,j) \\ 1 & if\ C_1(i,j) \neq C_2(i,j) \end{cases} \tag{13}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{14}$$

in which $C_1(i, j)$ signifies cipher picture value of each pixel. C_2 (i j) indicates encrypted image value of the pixel where actual picture modifies its pixel values.

The received outcomes of Table III, the NPCR and UACI from the image dataset demonstrated about the efficacy of the used encryption methodology. It is acknowledging that the output of the NPCR is approaching towards hundred and UACI is reaching one-third of the hundred. This is also justifying about the withstand of any type of differential attacks with the utilization of 2D LS-IES mechanism.

D. Entropy Analysis

The entropy of any image is fundamentally recognized towards reflecting picture information uncertainty. Basically, the entropy quality of information is determined via formula 15. The highest entropy value is 8 if probability among gray levels is precisely same. Entropy can be computationally obtained through Eq. (15) which is as followed:

$$Z(r) = -\sum_{i=1}^{255} P(r_i) \log_2 P(r_i) \tag{15}$$

Whereas Z(r) is the calculated information entropy of experimented images and its probability as shown by P(r). Table IV is illustrated optimize setup with the produced information entropy which are experimentally comes through dataset images.

E. Key Analysis

The generalization ability among the chaos-oriented encryption technique must $\geq 2^{100}$ to withstand the assault by brute force [30]. We have a cryptographic key of 232 bits, K = $\{X_0, Y_0, \alpha, m, \beta, £\}$ to meet this criterion as well as adjust it to the construction of the LS-IES.

F. Comparative Study

This section is illustrated efficiently of proposed outcomes and compared with earlier well-known published state-of-art methods on Table V. After comparison, we found that our proposed 2D LS-IES method is comparatively satisfactory in terms of result generated by 2D LS-IES methodology.

TABLE III. NPCR AND UACI VALUES OF ENCRYPTED IMAGES

Images	NPCR	UACI
5.1.14	99.59	33.30
5.1.12	99.49	33.31
5.1.09	99.60	33.32

TABLE IV. ENTROPY OF THE EXPERIMENTED IMAGES

Images	5.1.14	5.1.12	5.1.09
Plain image	7.3321	6.6050	6.6027
Encrypted	7.9985	7.9945	7.9956

TABLE V. COMPARATIVE STUDY OF 2D LS-IES

Methods	Image	Key	Entropy	NPCR	Correlation Coefficient	UACI
Proposed	5.1.14	2^{232}	7.9985	99.59	0.0031	33.30
[34]	5.1.09	2^{232}	7.9971	99.66	-0.0017	33.30
[35]	512×512 [3]	2^{256}	7.9991	99.6212	0.0015	33.4406
[36]	Lena	2^{279}	7.9969	99.62	NA	33.50
[37]	512×512 [3]	2^{256}	7.9996	99.6383	0.0010	33.3516
[38]	Lena	2^{312}	7.9993	99.60	0.0020	33.4754
[39]	Lena	2^{262}	7.9993	99.62	0.0023	33.46
[40]	5.1.09	2^{512}	NA	99.6185	0.0593	33.45
[41]	5.1.09	2^{224}	7.997	99.60	-0.00033	33.45
[42]	5.1.09	2^{256}	7.9026	99.6094	NA	33.5253

VI. CONCLUSION

This research initiated a unique 2D-LS chaotic. The logistical map's outcome is used to alter associated sine map insight, and after that transition period is extended to one dimension to two dimensions. A variety of empirical techniques and its examination have been offered to indicate why 2D-LS has greater ergodicity as well as chaotic spectrum compare to all those current one dimension as well as two-dimensional cryptosystems. This research is also suggested an innovative image encryption system named LS-IES utilizing 2D-LS. It has two fundamental characteristics, including misunderstanding over bit manipulation as well as diffusion through bit manipulation. Uncertainty as well as dispersion are accomplished at bit scale to reach the confusion as well as diffusion premise. Research outcomes as well as security concern have shown that LS-IES can easily encrypts many picture formats with producing high security randomized cryptographic images. For the future work, this work can carry with different types of images and some improved encryption methods in terms of critical security with medical healthcare systems.

ACKNOWLEDGMENT

We are thanking to the Dhofar University, Sultanate of Oman for constantly help and support.

REFERENCES

[1] W. D. Ferreira, C. B. R. Ferreira, G. da Cruz Júnior, and F. Soares, "A review of digital image forensics," Comput. Electr. Eng., vol. 85, p. 106685, Jul. 2020.

[2] M. Yu, "Film and television culture dissemination based on ZYNQ embedded digital image processing," Microprocess. Microsyst., vol. 82, p. 103921, Apr. 2021.

[3] Y. Zhang and L. Y. Zhang, "Exploiting random convolution and random subsampling for image encryption and compression," Electron. Lett., vol. 51, no. 20, pp. 1572–1574, 2015.

[4] Y. Zhang, D. Xiao, W. Wen, and K.-W. Wong, "On the security of symmetric ciphers based on DNA coding," Inf. Sci. (Ny)., vol. 289, pp. 254–261, Dec. 2014.

[5] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," Pattern Recognit. Lett., vol. 31, no. 5, pp. 347–354, Apr. 2010.

[6] J. Ramya, H. C. Vijaylakshmi, and H. Mirza Saifuddin, "Segmentation of skin lesion images using discrete wavelet transform," Biomed. Signal Process. Control, vol. 69, p. 102839, Aug. 2021.

[7] C. Ye, J. Peng, and S. Kong, "Implementation of wavelet transform on optical computer," Opt. Commun., vol. 486, p. 126761, May 2021.

[8] Y. Wu, Y. Zhou, S. Agaian, and J. P. Noonan, "A symmetric image cipher using wave perturbations," Signal Processing, vol. 102, pp. 122–131, Sep. 2014.

[9] A. Elghandour, A. Salah, and A. Karawia, "A new cryptographic algorithm via a two-dimensional chaotic map," Ain Shams Eng. J., May 2021.

[10] J. S. Muthu and P. Murali, "A new chaotic map with large chaotic band for a secured image cryptosystem," Optik (Stuttg)., vol. 242, p. 167300, Sep. 2021.

[11] M. Z. Talhaoui and X. Wang, "A new fractional one dimensional chaotic map and its application in high-speed image encryption," Inf. Sci. (Ny)., vol. 550, pp. 13–26, Mar. 2021.

[12] Y. Peng, S. He, and K. Sun, "A higher dimensional chaotic map with discrete memristor," AEU - Int. J. Electron. Commun., vol. 129, p. 153539, Feb. 2021.

[13] X. Wang, W. Zhang, W. Guo, and J. Zhang, "Secure chaotic system with application to chaotic ciphers," Inf. Sci. (Ny)., vol. 221, pp. 555–570, Feb. 2013.

[14] Yicong Zhou, Zhongyun Hua, Chi-Man Pun, and C. L. P. Chen, "Cascade Chaotic System With Applications," IEEE Trans. Cybern., vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[15] J. Khan, H. Abbas, and J. Al-Muhtadi, "Survey on Mobile User's Data Privacy Threats and Defense Mechanisms," Procedia Comput. Sci., vol. 56, pp. 376–383, 2015.

[16] J. Khan et al., "Medical Image Encryption Into Smart Healthcare IOT System," in 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, 2019, pp. 378–382.

[17] X. Wang, N. Guan, and J. Yang, "Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map," Chaos, Solitons & Fractals, vol. 150, p. 111117, Sep. 2021.

[18] C. Luo, B. Q. Liu, and H. S. Hou, "Fractional chaotic maps with q–deformation," Appl. Math. Comput., vol. 393, p. 125759, Mar. 2021.

[19] B. Khokhar, S. Dahiya, and K. P. S. Parmar, "Load frequency control of a microgrid employing a 2D Sine Logistic map based chaotic sine cosine algorithm," Appl. Soft Comput., vol. 109, p. 107564, Sep. 2021.

[20] Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain," Opt. Laser Technol., vol. 135, p. 106610, Mar. 2021.

[21] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," J. Inf. Secur. Appl., vol. 52, p. 102470, Jun. 2020.

[22] M. Alawida, A. Samsudin, and J. Sen Teh, "Enhanced digital chaotic maps based on bit reversal with applications in random bit generators," Inf. Sci. (Ny)., vol. 512, pp. 1155–1169, Feb. 2020.

[23] A. A. Śliwiak, N. Chandramoorthy, and Q. Wang, "Ergodic sensitivity analysis of one-dimensional chaotic maps," Theor. Appl. Mech. Lett., vol. 10, no. 6, pp. 438–447, Nov. 2020.

[24] T. Zhao, L. Yuan, and Y. Chi, "Image encryption using linear weighted fractional-order transform," J. Vis. Commun. Image Represent., vol. 77, p. 103098, May 2021.

[25] Y. Zhang, L. Zhang, Z. Zhong, L. Yu, M. Shan, and Y. Zhao, "Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation," Opt. Lasers Eng., vol. 143, p. 106626, Aug. 2021.

[26] 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 Interdiscip. J. Nonlinear Sci., vol. 18, no. 3, p. 033112, Sep. 2008.

[27] C. Li, Y. Liu, L. Y. Zhang, And M. Z. Q. Chen, "Breaking A Chaotic Image Encryption Algorithm Based On Modulo Addition And Xor Operation," Int. J. Bifurc. Chaos, vol. 23, no. 04, p. 1350075, Apr. 2013.

[28] C. Li, D. Arroyo, And K.-T. Lo, "Breaking A Chaotic Cryptographic Scheme Based On Composition Maps," Int. J. Bifurc. Chaos, vol. 20, no. 08, pp. 2561–2568, Aug. 2010.

[29] R. M. May, "Simple mathematical models with very complicated dynamics," Nature, vol. 261, no. 5560, pp. 459–467, Jun. 1976.

[30] G. Alvarez And S. Li, "Some Basic Cryptographic Requirements For Chaos-Based Cryptosystems," Int. J. Bifurc. Chaos, vol. 16, no. 08, pp. 2129–2151, Aug. 2006.

[31] D. Xiao, X. Liao, and S. Deng, "One-way Hash function construction based on the chaotic map with changeable-parameter," Chaos, Solitons & Fractals, vol. 24, no. 1, pp. 65–71, Apr. 2005.

[32] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," Inf. Sci. (Ny)., vol. 339, pp. 237–253, Apr. 2016.

[33] Digital Test Image, "Usc-sipi image database for research in image processing, image analysis, and machine vision." [Online]. Available: http://sipi.usc.edu/database/. [Accessed: 29-Jun-2021].

[34] X. Gao, "Image encryption algorithm based on 2D hyperchaotic map," Opt. Laser Technol., vol. 142, p. 107252, Oct. 2021.

[35] J. Khan et al., "SMSH: Secure Surveillance Mechanism on Smart Healthcare IoT System With Probabilistic Image Encryption," IEEE Access, vol. 8, pp. 15747–15767, 2020.

[36] S. Zhang and L. Liu, "A novel image encryption algorithm based on SPWLCM and DNA coding," Math. Comput. Simul., vol. 190, pp. 723–744, Dec. 2021.

[37] J. Khan et al., "Efficient secure surveillance on smart healthcare IoT system through cosine-transform encryption," J. Intell. Fuzzy Syst., vol. 40, no. 1, pp. 1417–1442, Jan. 2021.

[38] Q. Cun, X. Tong, Z. Wang, and M. Zhang, "Selective image encryption method based on dynamic DNA coding and new chaotic map," Optik (Stuttg)., vol. 243, p. 167286, Oct. 2021.

[39] N. Khalil, A. Sarhan, and M. A. M. Alshewimy, "An efficient color/grayscale image encryption scheme based on hybrid chaotic maps," Opt. Laser Technol., vol. 143, p. 107326, Nov. 2021.

[40] X. Wang and M. Zhao, "An image encryption algorithm based on hyperchaotic system and DNA coding," Opt. Laser Technol., vol. 143, p. 107316, Nov. 2021.

[41] R. Wang, G.-Q. Deng, and X.-F. Duan, "An image encryption scheme based on double chaotic cyclic shift and Josephus problem," J. Inf. Secur. Appl., vol. 58, p. 102699, May 2021.

[42] H. Zhu, Y. Zhao, and Y. Song, "2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map for Image Encryption," IEEE Access, vol. 7, pp. 14081–14098, 2019.