International Journal of Civil Engineering and Technology (IJCIET)
Volume 9, Issue 13, December 2018, pp.318–327, Article ID: IJCIET_09_13_032
Available online at http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=9&IType=13
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

A NEW BLOCK CIPHER ALGORITHM FOR IMAGE ENCRYPTION BASED ON CHAOTIC SYSTEM AND S-BOX

Amal AbdulBaqi Maryoosh
Department of Computer Science
Mustansiriyah University, collage of Education
Baghdad, Iraq

ABSTRACT

A new image encryption scheme based on Lorenz system, logistic map and s-box is proposed in this paper. The proposed algorithm encrypts and decrypts 128 bit block. At first the plain image will permuted by use permutation algorithm, after that input block by block to substitution by variable s-box and adding key stages. The resulted image XORed with another encrypted key that generated by logistic map, and then confused the resulted image again. The experiment results such as histogram, UACI, NPCR, entropy, correlation and key space showed that this algorithm achieved high level of security for image encryption.

Keyword: Chaotic, Image encryption, Lorenz system, Logistic map, S-box.

Cite this Article: Amal AbdulBaqi Maryoosh, A New Block Cipher Algorithm For Image Encryption Based On Chaotic System and S-Box, *International Journal of Civil Engineering and Technology (IJCIET)* 9(13), 2018, pp. 318–327.
http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=9&IType=13

1. INTRODUCTION

In the last years, a variety chaotic based image encryption algorithms designed and implemented. Chaotic systems have many features make them appropriate for image encryption such as pseudorandomness, arbitrary behavior, and sensitive to initial condition and control parameters [1, 2]. The values that generated by the chaotic systems are deterministic but unpredictable to a large extent provide a tremendous advantage for encryption systems. So, the chaotic systems have been accepted significantly for diffusion and confusion operations in image cryptography [2, 3].

Many of the current image encryption schemes such as [4, 5,6, 7] employ the permutation process to assure the diffusion of the plain image pixels in the entire encrypted image, while they employ the confusion process by substituting pixels values by using a deterministic algorithm [8]. Several studies are related with this work, for example, Ünal Çavuşoğluet al. [1] proposed new 3D chaotic system then use this system as a key and to generate s-box. The

plain image xored with chaotic key and then permuted by the generated s-box. S. N. Lagmiri et al. [9] proposed new 3D and 4D chaotic system to permute the pixel position for image encryption. R. Sridevi et al. [10] use a couple of logistic and standard maps for pre and post image shuffling and xored with 256 bit key for confuse the image. Xiuli Chai et al. [11] combining 2D logistic map, DNA, and SHA 256 hash, the plain image encoded to DNA and the logistic map used to rows and columns permutation and for image confusion. SHA 256 used for generate the initial value of logistic map. Hongjun Liu et al. [12] generate three s-box by using complex chen system each s-box used to encrypt one band of color image. The initial value of chen system is generated by 256 hash value and random noise. Ali Soleymani et al. [13] use Arnold cat map with variable parameter in each round to permute the plain image and use henon map to create secret image and to generate the parameters of cat map. And then xored permuted image with secret image. Zhi-liang Zhu et al. [14] propose image encryption system using Arnold cat map for bit level permutation and Logistic map for diffusion. Dragan Lambić [15] proposed a new special case of discrete chaotic map based on the composition of permutations. This special case can be considered as improvement of chaotic map presented in paper Lambić [16].

In this paper, we proposed a new algorithm for color image encryption by combining chaotic system with s-box. This algorithm increase the security and efficient of image encryption via high confusion that provided by chaotic system and S-box and high diffusion that provided by permutation method. This paper results are compared with AES algorithm by information entropy, correlation, histogram, NPCR,UACI and key space. The experimental results show that the proposed scheme efficient and more secure for image encryption.

The remainder of this paper is arranged as follows. In Section 2 the methods that used in proposed algorithm will introduced. In Section 3 the proposed system described in details. The security analysis is shown in Section 4. Finally, the conclusions are shown in Section 5.

2. CHAOTIC SYSTEMS

This paper used two chaotic systems, which are, Lorenz system [17] and 1D Logistic map [18] are employed in proposed system for keys generation.

2.1. Lorenz System

In the end of 1950s, Edward Lorenz developed Lorenz system which is the first numerical study on chaotic system. It is developed in order to atmosphere model [17]. The system equations are as follows in eqs. (1):

$$x' = \alpha(y - x)$$

$$y' = (\beta x - y - xz) \qquad (1)$$

$$z' = (xy - \gamma z)$$

The intervals that are used in the states of the system are $-20 \leq x \leq 20$, $-50 \leq y \leq 50$, and $-50 \leq z \leq 50$. As shown in fig.1 the system exhibits periodic behavior for parameters values $\alpha = 10, \beta = 28$, and $\gamma = 8/3$

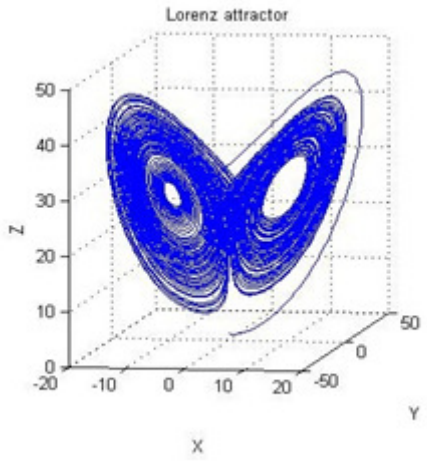


Fig. 1 The plot of Lorenz system along x–y–z axis, for α = 10,β = 28, γ = 8/3

2.2. Logistic map

A one dimensional logistic map is described in the following eq.:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (2)$$

Where x_n refer to the n*th* output and μis the map's parameter that the range of it must be between the interval (3.56,4]. The initial valuex_0 and μ can be used as encryption key [18]. By reason of its simplicity and high efficiency, this paper employed the chaotic systems times in its algorithm.

3. PROPOSED SCHEME

The encryption scheme contain four main operations that are: complement, permutation, substitution and add chaotic keys. At first the plain image will input to permutation step. And then the permuted image will divided to 4x4 blocks to enter to *n* iterations of substitution and add Lorenz key. After the end of iterations the resulting image will XO Red with Logistic map key to increase the confusion. Finally, implement the complement step which provide extra confusion process and it's done by subtract each pixel value from 255.The general structure diagram of proposed system shown in fig. 2.

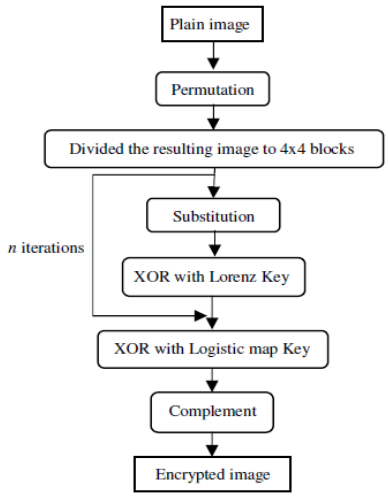


Fig. 2 The general structure of proposed system

A. Permutation method

Permutation is very important step in this algorithm. It's suitable to hinder the high correlation among the pixels of image to increment the security of encrypted images. It's provide high level of diffusion by swap the location of two pixels randomly and mark each pixel that has been swapped in which it will not swapped again. In this method the random number generator will reset each time, for this reason the same method is used for retrieve permuted image. These steps are performed until nearly all image pixels are swapped. Table 1 shown the random swap of 10x10 sub image pixels. Fig. 3 shown the plain bird image and the resulting image after permutation.

B. Substitution

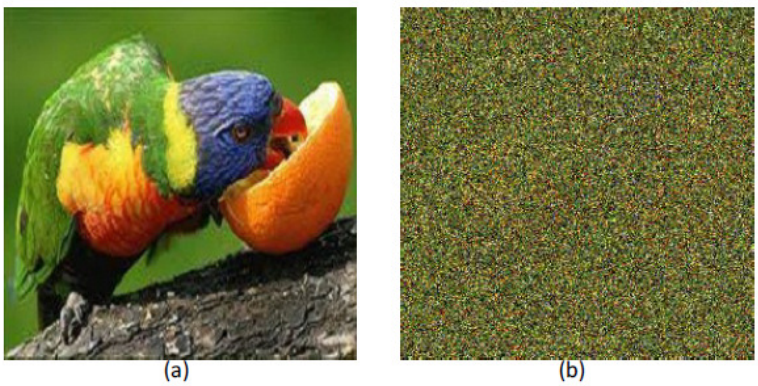
In this process, this paper used the S-box of AES algorithm with some changes to get rid from the weakness in the fixed S-box and improve the key sensitivity by implement 15 byte circular shift on the S-box in each round, where each block will be substituted with a new s-box, this operation will provide one time pad property. Fig.4 shown the result of encryption horse image by using shifted S-box only.

Table 1: Original pixel location on the left and their new position on the right

										125 91 119 175 183 225 100 92 155 153
										120 116 137 80 208 135 161 176 159 113
										60 138 168 155 178 138 80 116 118 109
116	159	162	183	175	190	145	110	119	145	119 125 190 181 172 210 110 42 91 64
81	42	168	162	155	190	109	135	118	121	158 83 166 135 100 107 107 136 135 142
132	120	137	208	210	189	116	100	159	161	185 189 218 110 187 137 116 191 138 100
187	191	225	181	192	178	92	116	120	137	99 120 108 192 226 129 132 162 81 113
158	218	136	176	203	175	98	166	150	110	159 177 158 98 120 125 57 119 100 96
226	138	83	177	119	64	125	125	169	116	162 137 145 120 175 190 133 67 137 145
125	91	67	172	185	77	60	119	120	113	83 203 116 169 121 110 150 42 77 131
91	110	96	107	138	99	42	155	100	158	
80	133	100	131	107	135	137	108	137	153	
83	100	80	138	113	142	135	57	129	120	

3.1. Encryption Algorithm

Input: plain image (m), Lorenz_key, Logistic_key, Sbox



(a) (b)

Fig.3 (a) Plain bird image (b) Permuted bird image

Output: encrypted image (c)

Step1: read colored image (m)

Step2: generate index vector (iv)

for i→ 1: length of (m)

find two unswapped pixels

p→ Swap (m)

Store the location of p in iv

end.

Step3: for j→ 1:n

sub_byte→ circular_shift (Sbox)

s→ sub_byte (p)

k1 → xor (Lorenz_key, s)

end

Step4: k2→ xor (Logistic_key, k1)

Step5: c→ imcomplement (k2)

3.2. Decryption Algorithm

Input: encrypted image (*c*), *Lorenz_key*, *Logistic_key, InvSbox*
Output: plain image (*m*)
Step1: read encrypted image (*c*)

Step2: *r*→ imcomplement (*c*)

Step3: *k1*→ xor (*Logistic_key*, *r*)

Step4:for *j*→ 1:*n*

*k*2 → xor (*Lorenz_key*, *k1*)

Inv_sub_byte→ circular_shift (*InvSbox*)

s→ Inv_sub_byte (*k2*)

end

Step5:generate index vector (*iv*)

for *i*→ 1: length of (*s*)

find two unswapped pixels

m→ Swap (*s*)

Store the location of *d* in *iv*

end.

4. SECURITY ANALYSIS

In this section we review the results of the series of tests to proof the efficiency of the proposed method and compare the results with AES. The evaluation consist of many practical experiments. The experiments are performed via Matlab R2013a on a computer with Intel Core i3 CPU 2.10 GHz, 3 GB of RAM.

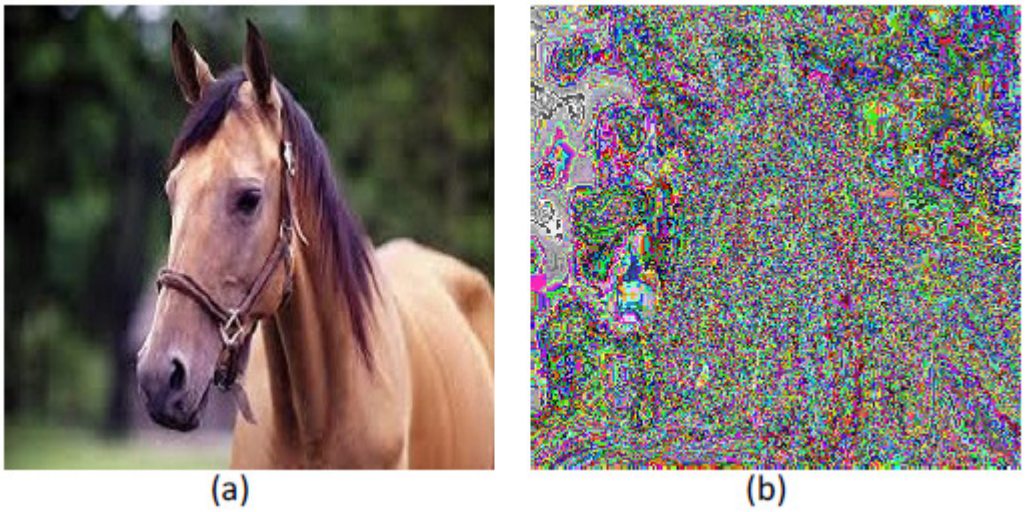


Fig.4 (a) Plain horse image (b) the image after substitution process

4.1. Histogram Analysis

Histogram analysis is used to explain the confusion and diffusion characteristic of the encryption algorithm. Fig. 5 shown the difference in image distribution among plain horse image, its permutation and encryption.

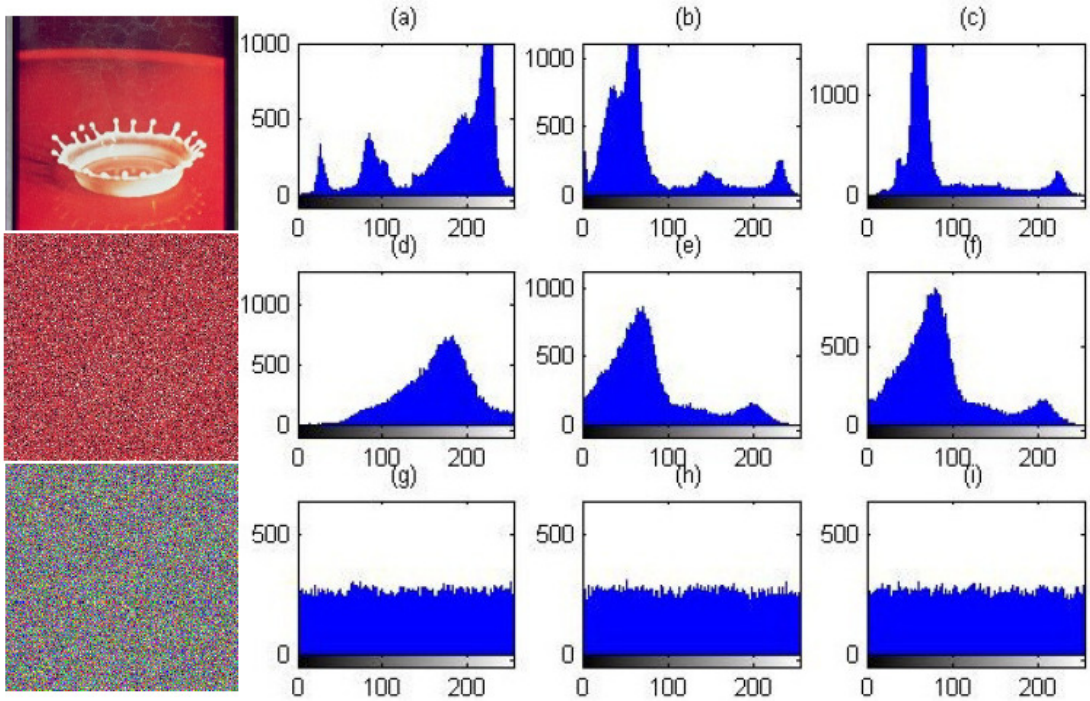


Fig. 5 Histogram Analysis: (a), (b) and (c) are the histogram of (Red, Green and Blue) of the plain splash image, (d),(e) and (f) are the histogram of (Red, Green and Blue) of permutedimage, (g),(h) and (i) are the histogram of (Red, Green and Blue) of encryptedimage.

4.2. Correlation Analysis

The correlation between adjacent pixels in the normal image is always strongly, and the correlation coefficient values are so close to 1. For this reason, the correlation must be decreased significantly in an efficient encryption algorithm and the value extremely close to 0

[8, 19].We can compute the correlation coefficients for three directions horizontal, vertical, and diagonal, according to the following equations.

$$\text{cov}(x, y) = E\{(x - E(x))(y - E(y))\} \quad (3)$$

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (4)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (5)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (6)$$

In equation (3), x and y are the values of two neighboring pixels in the image, D(x) and E(x)are the variance and the expectation of x. N in the equations (5) and (6) is the number of image pixels. Fig 6 shown the horizontal, vertical and diagonal correlation coefficient in plain and encrypted horse image, and Table2 display the results of correlation for the various plain images and encrypted images and compared it with AES algorithm.

Table2: Comparing Correlation coefficients of two neighboring pixels in the plain and encrypted images between proposed system and AES algorithm.

Images	Correlation of proposed system			Correlation of AES		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
House	0.0018	-0.00009	-0.00004	0.0021	0.0017	0.0031
Flower	-0.0041	-0.0038	0.0034	-0.0028	0.0015	-0.0027
Pepper	0.0016	0.0035	-0.00003	0.0022	-0.0014	0.00008
Lion	0.00004	0.0016	-0.0013	0.0107	0.004	-0.0026
Bird	-0.0069	-0.0046	-0.0053	0.0028	0.0037	0.001
Garden	-0.0032	-0.00005	-0.00006	-0.0019	-0.00051	-0.007
Horse	-0.0000006	-0.0016	0.00009	0.0068	-0.0021	-0.0019
Tree	-0.001	-0.0048	0.0033	-0.0029	-0.0039	0.0051
Sky	0.0018	-0.0028	0.0026	0.0031	-0.0023	-0.00007
Ladybug	0.005	0.0081	0.004	0.0034	0.0053	-0.00003
splash	0.0016	-0.00009	0.002	-0.00007	0.0024	0.0015

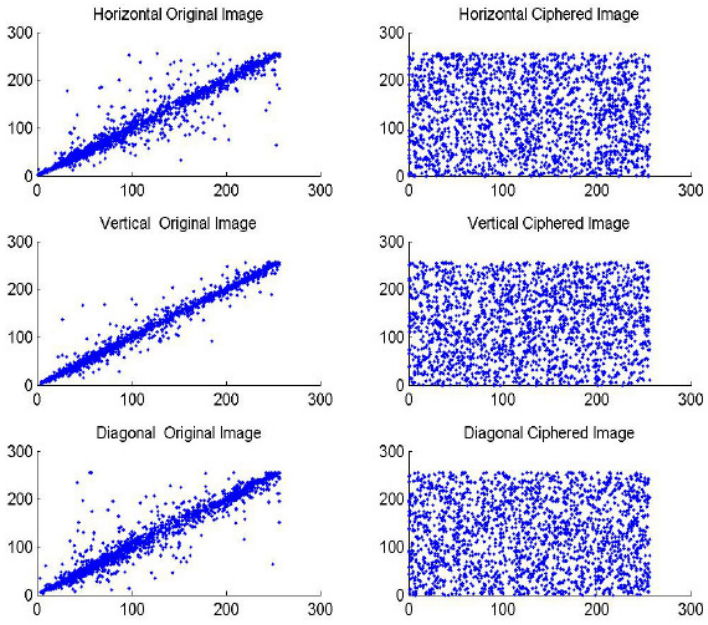


Fig. 6 Correlation of two neighboring pixels in plain and encrypted horse image

4.3. Information entropy analysis

One of the very important measure to compute the randomness is information entropy.It can be computed by:

$$H(m)=\sum_{i=0}^{2^n-1} p(m_i)\log_2\frac{1}{p(m_i)} \quad (7)$$

Table3 Comparing Information Entropy of plain and encrypted image between proposed method and AES algorithm

Images	Entropy of plain images	Entropy of proposed system	Entropy of AES
House	7.7871	7.9991	7.9992
Flower	7.7666	7.9983	7.9991
Pepper	7.7124	7.9984	7.9990
Lion	7.8794	7.9990	7.9980
Bird	7.6741	7.9991	7.9990
Garden	7.7955	7.9991	7.9990
Horse	7.6143	7.9990	7.9990
Tree	7.6659	7.9976	7.9990
Sky	7.9339	7.9990	7.9992
Ladybug	7.5706	7.9987	7.9990
splash	7.3795	7.9989	7.9988

In equation above, m is a sample, n is the number of samples, and p(m) is the probability of symbol m. the ideal value of H(m) we can get according to Eq. (7) is 8,this indicates that random information in image [20]. The values of information entropy that we obtained from proposed system are closer to eight, this show that the proposed scheme has good random. Table3 shown the values of information entropy for the various plain images and encrypted images and compared it with AES algorithm.4.4 Resisting differential attack analysis

The attackers usually make a tiny changes on the selected plain image and then notes the changes in the encrypted image. Thus, they may be able to find a significant relationship between the plain and encrypted image [4]. In order to know the effect of changing a tiny portion of pixels in the normal image on the encrypted image, in this paper we used the number of pixels change rate (NPCR) and unified averaged changed intensity (UACI). The NPCR indicator can be used to know the number of different pixels that have the same location in the original image and in its encrypted image, and it is defined as follows:

$$NPCR=\frac{\sum_{i,j} D(i,j)}{wxh}x100\% \quad (8)$$

Where, *w* and *h* are the width and height of the image, $C_1(i, j)$ and $C_2(i, j)$ are the two encrypted images whose corresponding plainimages$I_1(i, j)$ and $I_2(i, j)$ have only one-pixel value difference. $D(i, j) = 0$, if $C_1(i, j) = C_2(i, j)$; else $D(i, j) = 1$.

The UACI indicator is used to know the effect on encrypted image if one pixel is changed in plain image, and it is defined as follows:

$$UACI=\frac{1}{w\ x\ h}\left(\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right)x\ 100\% \quad (9)$$

The ideal value of NPCR and UACI are 99.61 and 33.46 [21]. In this paper we implement NPCR and UACI measures on ten color images and the results of the two indicator are close to ideal value. Table4 shown the results of NPCR and UACI in proposed scheme and compare it with AES algorithm.

4.5. key space

The key space must be large enough to resist against robust attack, that make the find of key is very hard for attacker. In the systems that based on chaotic systems the key space increases

by increasing the number of parameters and the size of chaotic system. In this scheme the key space is$(10^{14})^5$ which is nearly equal to 2^{224}. Comparing the key space of this scheme with AES algorithm which has 2^{128} bit key space, it is note that the value of the chaos system key space is much larger.

5. CONCLUSION

In this paper, a new image encryption algorithm has been introduced to provide high level of security for image encryption based on the combination of permutation method, chaotic system and dynamic s-box. Whereas the random permutation method provide high level of diffusion, and the substitution process provide high confusion and improve the key sensitivity by implement some circular shift on S-box. Also the use of chaotic system offer high randomness, key sensitivity, and confusion. The efficiency of this method has been confirmed through above experiment results. According to these results the proposed scheme offers high resistance against differential and statistical attacks.Table4: Comparing UACI and NPCR indicator of plain and encrypted image between proposed scheme and AES algorithm

Table4: Comparing UACI and NPCR indicator of plain and encrypted image between proposed scheme and AES algorithm

Images	Proposed system		AES	
	UACI	**NPCR**	**UACI**	**NPCR**
House	32.02	99.62	32.08	99.62
Flower	33.49	99.62	34.65	99.60
Pepper	33.61	99.60	34.25	99.62
Lion	33.41	99.61	33.59	99.60
Bird	33.68	99.60	33.73	99.60
Garden	33.43	99.61	33.39	99.60
Horse	33.47	99.63	33.43	66.62
Tree	33.79	99.60	34.01	99.62
Sky	33.74	99.60	33.78	99.63
Ladybug	33.57	99.59	34.07	99.62
splash	33.73	99.60	33.87	99.59

ACKNOWLEDGEMENTS

I would like to thank Mustansiriyah university (www.uomustansiriyah.edu.iq) Baghdad – Iraq for its support in the present work.

REFERENCES

[1] Ünal Çavuşoğlu, et al., Secure image encryption algorithm design using a novel chaos based S-Box, Chaos, Solitons and Fractals, 95 (2017) 92–101, doi: 10.1016/j.chaos.2016.12.018.

[2] Ekhlas Abbas Albahrani, A New Audio Encryption Algorithm Based on Chaotic Block Cipher, Annual Conference on New Trends in Information & Communications Technology Applications, IEEE, 7 - 9 March 2017, doi: 10.1109/NTICT.2017.7976129.

[3] Guodong Ye and Xiaoling Huang, A secure image encryption algorithm based on chaotic maps and SHA-3, Security Comm. Networks 2016; 9:2015–2023, doi: 10.1002/sec.1458.

[4] Narendra K. Pareek, et al., Diffusion–substitution based gray image encryption scheme, (2013), doi:10.1016/j.dsp.2013.01.005.

[5] Alireza Jolfaei and Abdolrasoul Mirghadri, Image Encryption Using Chaos and Block Cipher, Computer and Information Science, Vol. 4, No. 1; January 2011.

[6] Iqtadar Hussain, et al., Application of S-box and chaotic map for image encryption, Mathematical and Computer Modelling 57 (2013) 2576–2579, doi:10.1016/j.mcm.2013.01.009.

[7] Yong Wang, et al., A new chaos-based fast image encryption algorithm, Applied Soft Computing 11 (2011) 514–522, doi:10.1016/j.asoc.2009.12.011.

[8] Ana Cristina Dăscălescu and Radu Eugen Boriga, A novel fast chaos-based algorithm for generating random permutations with high shift factor suitable for image scrambling, Nonlinear Dyn, (2013), doi: 10.1007/s11071-013-0969-6.

[9] S. N. Lagmiri, et al., Color and gray images encryption algorithm using chaotic systems of different dimensions, International Journal of Computer Science and Network Security, VOL.18 No.1, January 2018.

[10] R. Sridevi et al. Logistic and Standard Coupled Mapping on Pre and Post Shuffled Images: A Method of Image Encryption, Asian Journal of Scientific Research, 10(1): 10-23, 2017, doi: 10.3923/ajsr.2017.10.23.

[11] Xiuli Chai, YiranChen and LucieBroyde, A novel chaos-based image encryption algorithm using DNA sequence operations,

[12] Optics and Lasers in Engineering, 88(2017)197–213, doi: 10.1016/j.optlaseng.2016.08.009.

[13] Hongjun Liu, AbdurahmanKadir and PijuanGong, A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise, Optics Communications 338(2015)340–347, doi: 0.1016/j.optcom.2014.10.021.

[14] Ali Soleymani, Md Jan Nordin and Elankovan Sundararajan, A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map, The Scientific World Journal, Volume 2014, Article ID 536930, 21 pages, doi: 10.1155/2014/536930.

[15] Zhi-liang Zhu et al., A chaos-based symmetric image encryption scheme using a bit-level permutation, Information Sciences 181 (2011) 1171–1186, doi: 10.1016/j.ins.2010.11.009.

[16] Lambić, A new discrete chaotic map based on the composition of permutations, Chaos, Solitons & Fractals, 78, (2015). 245–248.

[17] Majid Khan et al, A novel technique for the construction of strong S-boxesbased on chaotic Lorenz systems, Nonlinear Dyn (2012) 70:2303–2311, doi: 10.1007/s11071-012-0621-x.

[18] Fatih Özkaynak and Ahmet Bedri Özer, A method for designing strong S-Boxes based on chaotic Lorenz system, Physics Letters A 374, (2010) 3733–3738, doi:10.1016/j.physleta.2010.07.019.

[19] W. Zhang, et al., Image encryption based on three-dimensional bit matrix permutation, Signal Processing (2015), doi: 10.1016/j.sigpro.2015.06.008i.

[20] Liu Hongjun and Wang Xingyuan, Color image encryption based on one-time keys and robust chaotic maps, Computers and Mathematics with Applications 59 (2010) 3320_3327, doi:10.1016/j.camwa.2010.03.017.

[21] Lingfeng Liu and Suoxia Miao, A new image encryption algorithm based on logistic chaotic map with varying parameter, SpringerPlus (2016) 5:289, doi: 10.1186/s40064-016-1959-1.