An Image Encryption Technique based on Chaotic S-Box and Arnold Transform

Shabieh Farwa*, Tariq Shah†, Nazeer Muhammad*, Nargis Bibi‡, Adnan Jahangir*, and Sidra Arshad†
*Department of Mathematics, COMSATS Institute of Information Technology, 47040, Wah Cantt, Pakistan
†Department of Mathematics,Quaid-i-Azam University, Islamabad, Pakistan
‡Department of Computer Science, Fatima Jinnah Women University, Rawalpindi, Pakistan

***Abstract*—In recent years, chaos has been extensively used in cryptographic systems. In this regard, one dimensional chaotic maps gained increased attention because of their intrinsic simplicity and ease in application. Many image encryption algorithms that are based on chaotic substitution boxes (S-boxes) have been studied in the last few years but some of them appear to be vulnerable to robustness. We, in this paper, propose an efficient scheme for image encryption that utilizes a composition of chaotic substitution based on tent map with the scrambling effect of the Arnold transform. The proposed construction algorithm for substitution box is, on one hand, straightforward and saves computational labour, while on the other, it provides highly efficient performance outcomes. The understudy scheme uses an S-box, that is based on 1-D chaotic tent map. We partially encrypt the image using this S-box and then apply certain number of iterations of the Arnold transform to attain the fully encrypted image. For decryption we apply the reverse process. The strength of the proposed method is determined through the most significant techniques used for the statistical analysis and it is proved that the anticipated algorithm shows coherent results.**

***Keywords*—Chaos; image encryption; tent map; S-box; Arnold transform; statistical analyses**

I. Introduction

Transmitting large amount of confidential information over the communication media has raised the security challenges. The growing demand for comparatively safer and more reliable crypto-systems has created new research problems in the field of cryptography and has engaged scientists from relevant backgrounds to design improved encryption algorithms. In recent years, it has been developed that the chaotic systems exhibit the most legitimate features to fit for cryptographic applications therefore chaos based algorithms have been widely used in digital multimedia applications including image ciphering, data hiding, watermarking and steganography [1]-[12].

Edward Lorenz in 1960's introduced the study of chaotic dynamics [13], [14]. The development of chaotic theory proved that the chaos based systems have capability to produce high level of confusion and diffusion in substitution-permutation networks. The basic characteristics of the chaotic maps such as ergodicity, broadband spectrum and high sensitivity to the initial conditions attracted the attention of researchers to incorporate them in high-security encryption algorithms used in modern communication. In the last few years many chaotic-encryption algorithms have been studied [15]-[18].

Substitution box, the most indispensable component in block ciphers, is widely used in image encryption applications [19]-[24]. However, many recent researchers ignore the encryption option in communication process of image and signal processing [25]-[31]. Recently Zhang, *et al*. [32] studied an S-box-only image cipher based on chaotic map and proposed that the S-box-only image encryption algorithms are vulnerable against cryptographic robustness. Keeping this in view, we in this paper, propose an image encryption scheme that is not just based on the chaotic S-box but further utilizes a composition of the chaotic substitution with the Arnold transform's scrambling effect. The scheme is as follows, we apply the chaotic tent map to synthesize an S-box. Firstly the plain image is encrypted using the chaotic S-box, then the Arnold transform is applied on this encrypted image in order to attain high level of perplexity and randomness. For decryption purposes we first apply the inverse Arnold transform and then the inverse S-box. The proposed method is tested and we prove that it can be used to produce required security level in the internet applications for safe handling of the confidential information.

The material presented in this paper is organized as: In Section 2 we explain in detail the major properties of the tent map and its use in the construction of a substitution box. In Section 3 the concepts regarding the Arnold transform are presented. Section 4 presents the detailed algorithm used for the image encryption. In Section 5 we test the strength of the proposed scheme using statistical analyses and lastly Section 6 presents the conclusion.

II. Chaos-based S-Box

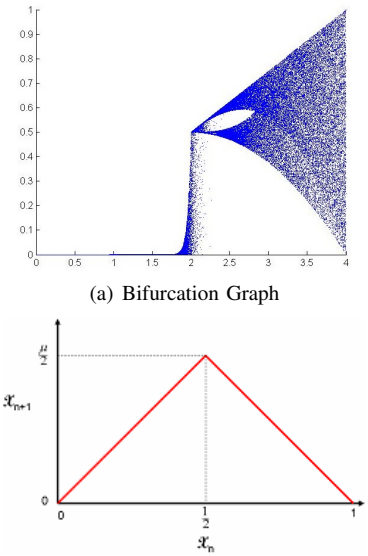
The intent of this section is to present the main algorithm used to design the chaotic S-box. We use the tent map to construct the substitution box. In the following subsections we discuss in detail, the properties of the underlying map and the detailed algorithm used to form the chaotic S-box.

A. Chaotic tent map

Tent map is a 1-D chaotic map $\phi : [0,1] \to [0,1]$ defined by:

$$\phi(x_n) : \begin{cases} \mu x_{n-1} & ; \ 0 \leq x < \frac{1}{2} \\ \mu(1 - x_{n-1}) & ; \ \frac{1}{2} \leq x \leq 1, \end{cases}$$

Where, $\mu \in \mathbb{R}^+$ and ϕ has chaotic behaviour when $\mu = 2$. For the desired purpose regarding construction of S-box, we assume $\mu = 2$. One can observe through Fig. 1 that the graph of the bifurcation diagram of tent map is in tent shape, representing chaotic behaviour.



(a) Bifurcation Graph

(b) Tent-shape Diagram

Fig. 1. Bifurcation graph of Tent map.

B. Algorithm for S-box

The formation of the S-box is then subsequent to the following steps:

- Partition the output interval $I = [0, 1]$ into 256 subintervals $I_m = [m\Delta, (m + 1)\Delta)$; $0 \leq m \leq 255$, where $\Delta = \frac{1-0}{256}$.
- Set the initial condition. Her we choose $x_0 = 1$.
- Apply ϕ for 256 times and assign the output interval number by using ψ, i.e. if $\phi(x_n) \in I_m$ then $\psi(n) = m$.
- If a region is repeated then definitely some region is missed also. Remove this error by assigning the leftover regions (in ascending order) to keep $\psi : GF(2^n) \rightarrow GF(2^n)$ bijective.
- The images of ψ produce the required S-box (see Table I).
  The performance parameters of the newly developed S-box are shown in the Table II, which clearly show that our proposed S-box exhibits extra-ordinary properties. It is worth-mentioning at this stage, that if we compare our algorithm with some of well-prevailing chaotic S-boxes as presented in [33]-[35], it is crystal clear that the performance indices such as nonlinearity, strict avalanche, bit independence, linear and differential approximation probabailities of our S-box are much better than the models discussed in [33]-[35]. However our scheme is very simple and direct as compared to the aforementioned methods.

III. Arnold Transform

Arnold transform is used for encryption of digital images to increase the spread of pixel intensities [36]. For any square image of size $M \times M$, encryption of the Arnold transform can be given as:

$$\begin{bmatrix} \acute{a} \\ \acute{b} \end{bmatrix} = \begin{bmatrix} \vartheta & \vartheta \\ \vartheta & \tau \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} (mod\, M), \tag{1}$$

Where, (a, b) and $(\acute{a}, \acute{b})$ represent the pixel coordinates of the input image and encrypted data respectively, such that $(\vartheta, \tau) = (1, 2)$. Fig. 2 shows the effect of 10 iterations of the Arnold Transform's application on the test image "House".

The Arnold transform encryption is worked on periodic boundary treatment. The image encryption using k number of iterations of Arnold transform may be written as:

$$I(\acute{a}, \acute{b})^k = I\Lambda(a, b)^{k-1} (mod\, M), \tag{2}$$

Where, Λ is the Arnold transform matrix given in (1) and I is an $M \times M$ encrypted image data for k number of iterations: $k = 1, 2, ..., n$, such that $I(\acute{a}, \acute{b})^0 = I(a, b)$. Periodicity of encryption is dependent on the size of a given image. The encrypted image data can be reversed on application of the inverse Arnold transform to I with same number of iterations k as follows:

$$I(a, b)^k = I\Lambda^{-1}(\acute{a}, \acute{b})^{k-1} (mod\, M). \tag{3}$$

IV. Image Encryption Scheme

In this section we present the scheme used for the image encryption. It comprises of the following two steps:

- Use chaotic substitution box to partially encrypt the plain image.
- Apply 10 iterations of the Arnold transform on this partially encrypted image to obtain the fully encrypted image.

We selected three benchmark images, house (256×256), cameraman (256×256) and Lena (512×512). By following the above stated scheme the images are encrypted. We obtain the decrypted images by applying the inverse Arnold transform and inverse S-box, respectively. Fig. 3 to 5 show the results obtained from encryption and decryption of images.

V. Statistical Analysis of the Proposed Method

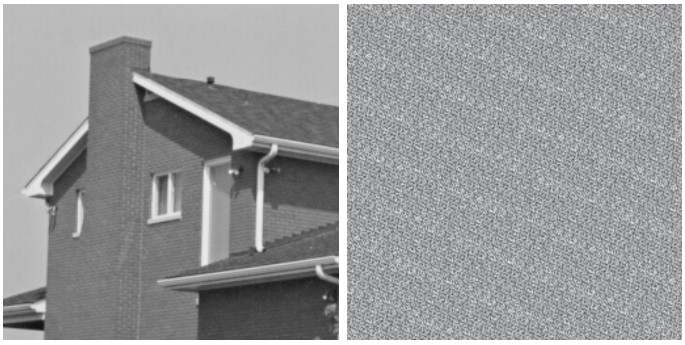
In this section we evaluate the forte of our method by some useful analysis such as contrast Table III, correlation Table IV, homogeneity Table V, number of pixels change rate (NPCR) and unified average change intensity (UACI) Table VI. We discuss these security parameters one by one and present the numerical results also.

A. Contrast

Contrast is a measure used to identify objects in an image. A strong encryption technique produces high level of contrast. Table III shows that our encryption scheme is quite efficient to attain acceptably high level of contrast.

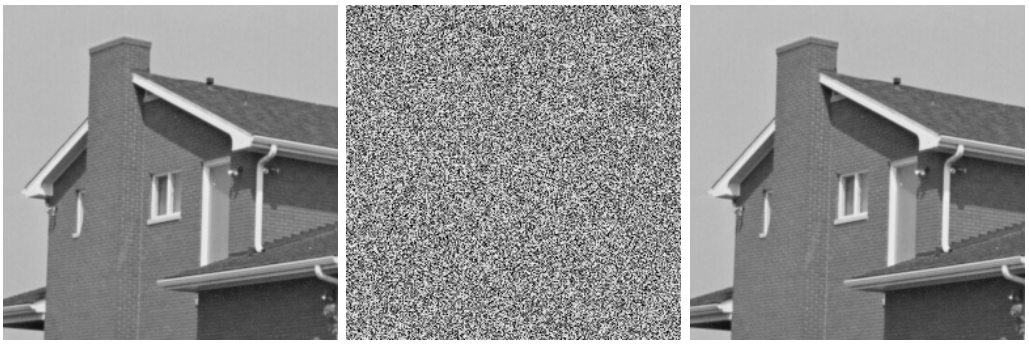
TABLE I. CHAOTIC S-BOX

79	159	193	124	249	12	24	49	99	199	112	224	62	125	251	9
18	36	72	144	222	67	134	243	25	51	103	206	98	196	119	238
34	68	136	239	32	65	130	248	8	16	33	89	137	242	26	52
104	209	93	187	148	230	50	66	132	247	22	60	95	150	236	19
38	77	155	100	200	55	110	221	69	138	235	40	80	160	191	128
255	1	2	5	11	23	46	115	197	152	223	39	78	157	203	139
232	54	90	135	241	27	56	113	226	58	117	234	42	84	169	172
166	179	153	205	101	202	107	214	82	165	180	151	212	92	185	141
229	75	105	211	88	176	181	192	127	250	0	3	10	4	17	29
57	91	145	240	31	63	126	252	6	13	45	53	121	216	83	167
190	158	195	120	233	30	61	122	244	44	47	94	189	133	245	20
41	111	164	182	147	217	76	178	210	116	207	123	218	97	177	220
71	109	161	188	146	237	28	86	131	219	59	118	227	70	108	156
204	129	225	87	142	246	43	73	81	163	194	140	231	48	96	201
143	253	254	7	14	15	21	35	37	74	149	213	85	170	184	186
171	168	174	162	198	173	228	64	102	154	208	106	215	114	183	175



(a) Plain image (b) Encrypted image

Fig. 2. 10 iterations of Arnold transform's application on the test image (House)



(a) Plain image (b) Encrypted (c) Decrypted

Fig. 3. House: Plain, encrypted and decrypted images

TABLE II. PERFORMANCE INDICES FOR S-BOX

Analysis	**Max**.	**Min**.	**Average**	**Square deviation**		
Nonlinearity	106	102	**104.5**			
SAC	0.609375	0.421875	**0.514648**	0.0191304		
LP	162					**0.132813**
DP					**0.046875**	
BIC		94	**103.214**	3.17757		

TABLE III. CONTRAST ANALYSIS

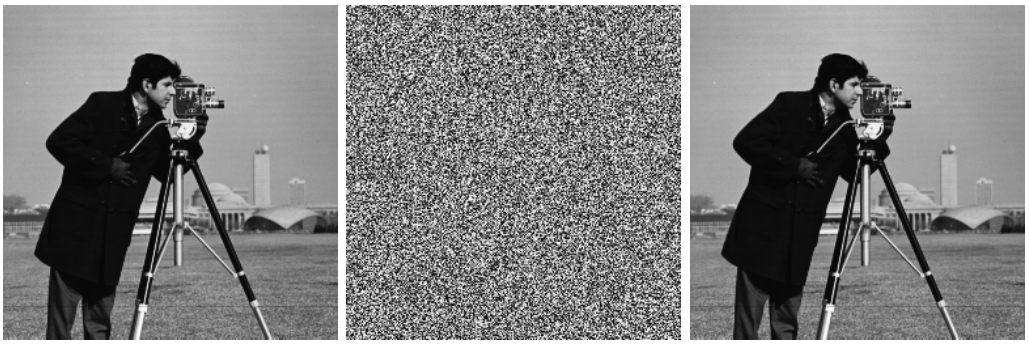
	Contrast	
Test images	Plain	Encrypted
House (256 × 256)	0.1826	8.0021
Cameraman (256 × 256)	0.5871	11.2393
Lena (512 × 512)	0.2287	10.8693

B. Correaltion

In order to examine the encryption effect of the proposed method we perform correlation analysis on both the plain and the encrypted images. It is quite clear that for an efficient encryption, the correlation of the encrypted image should be reduced as compared to the plain image. The correlation coefficient is given by,

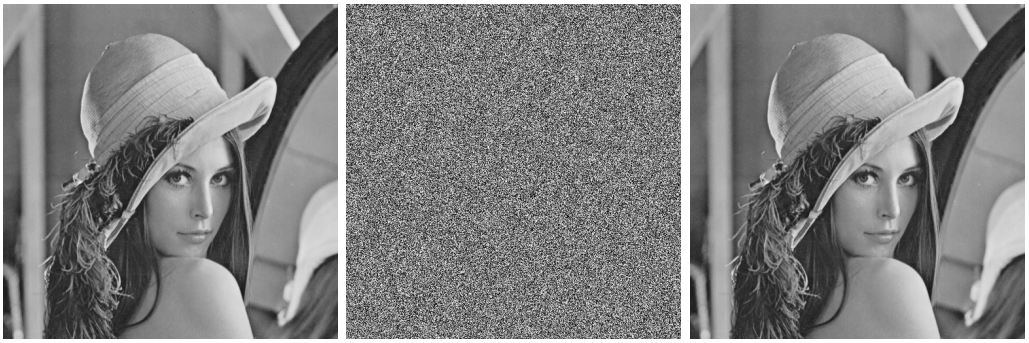
$$r_{xy} = \frac{E((x-\mu_x)(y-\mu_y))}{\sqrt{\delta_x \delta_y}},$$

Where, μ and δ represent the expected value and variance. The value of correlation coefficient close to zero guarantees better



(a) Plain image (b) Encrypted (c) Decrypted

Fig. 4. Cameraman: Plain, encrypted and decrypted images



(a) Plain image (b) Encrypted (c) Decrypted

Fig. 5. Lena: Plain, encrypted and decrypted images

encryption quality. The analysis is performed on three images, house (256×256), cameraman (256×256) and Lena (512×512). Results arranged in Table IV witness the effectiveness of the proposed method.

TABLE IV. CORRELATION ANALYSIS

	Correlation Coefficient	
Test images	Plain	Encrypted
House (256×256)	0.9497	-0.0166
Cameraman (256×256)	0.9227	0.0034
Lena (512×512)	0.9505	-0.0033

C. Homogeneity

Gray level co-occurrence matrix (GLCM) depicts the ability of combinations of pixel brightness results in tabular form. The closeness of the distribution in the (GLCM) to its diagonal is measured through the homogeneity analysis. The smaller is the homogeneity measure, the better is encryption. The numerical results shown in the following table witness the effectiveness of the proposed method.

TABLE V. HOMOGENEITY ANALYSIS

	Homogeneity	
Test images	Plain	Encrypted
House (256×256)	0.9250	0.4210
Cameraman (256×256)	0.8952	0.3849
Lena (512×512)	0.9050	0.3876

D. Differential analysis

A desirable feature of a cryptosystem is to show high sensitivity to single-bit change in the plain image. For this purpose two measures, NPCR and UACI, are commonly used. NPCR stands for the number of pixels change rate of encrypted image as a result of one pixel change in the plain image. NPCR can be defined as the variance rate of pixels in the encrypted image that occurs through the change of a single pixel in original image. However UACI means unified average intensity of differences between the plain and encrypted images. The percentage values for both these measures are given by the following formulae.

$$NPCR = \frac{\sum_{i,j} D_{ij}}{W \times H} \times 100, \tag{4}$$

$$UACI = \frac{1}{W \times H}\left[\frac{\sum_{i,j} C_{ij} - \acute{C}_{ij}}{255}\right] \times 100. \tag{5}$$

In above C and $\acute{C}$ represent the encrypted images obtained as a result of single bit change in the original image. In (4) and (5), W and H represent the width and the height of the images C and $\acute{C}$.

An efficient encryption scheme is one that produces higher values of both NPCR and UACI. The results obtained in our case are shown in Table VI.

TABLE VI. DIFFERENTIAL ANALYSIS

Test images	NPCR%	UACI%
House (256 × 256)	0.9958	0.3347
Cameraman (256 × 256)	0.9960	0.3346
Lena (512 × 512)	0.9959	0.3345

VI. CONCLUSION

In this work, an image encryption scheme is proposed that is extremely simple and highly effective. It has been established in some recent research work that the S-box only encryption techniques are not secured enough to resist cryptographic robustness therefore we introduced the combination of the chaotic S-box with certain iterations of the Arnold transform. The strength of the proposed method is then analyzed through several techniques that proves high effectiveness of our scheme as shown in listed tables.

REFERENCES

[1] Ghebleh, M., Kanso, A.: A robust chaotic algorithm for digital image steganography. Commun. Nonlinear Sci. Numer. Simul. 19(6), 1898-1907 (2014)

[2] Zhou, Y., Bao, L., Chen, C.L.P.: A new $1-D$ chaotic system for image encryption. Signal Processing 97, 172-184 (2014)

[3] Aziz, M., Tayarani-N, M.H., Afsar, M.: A cycling chaos-based cryptic-free algorithm for image steganography. Nonlinear Dyn. 80(3), 1271-1290 (2015)

[4] Cavusoglu, U., Kacar, S., Pehlivan, I., Zengin, A.: Secure image encryption algorithm using a novel chaos based S-box, Chaos, Solitions and Fractals, 95, 92-101 (2017)

[5] Muhammad, N., Bibi, N., Qasim, I., Jahangir, A., Mahmood, Z. Digital watermarking using Hall property image decomposition method. Pattern Analysis and Applications, 1–16, (2017)

[6] Muhammad, N., Bibi, N., Zahid M, Dai-Gyoung K. Blind data hiding technique using the Fresnelet transform. SpringerPlus, 4(1), 1–15, (2015)

[7] Muhammad, N., Bibi, N., Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain. IET Image Processing, 9(9), 795–803, (2015)

[8] Muhammad, N., and D. G. Kim, A novel Fresnlet based robust data hiding algorithm for medical images, 2012 IEEE International Conference on Imaging Systems and Techniques Proceedings, Manchester, 213-216, (2012)

[9] Muhammad, N., and Dai-Gyoung Kim. An Efficient Data Hiding Technique in Frequency domain by using Fresnelet Basis. Proceedings of the World Congress on Engineering. Imperial College London, UK.Vol. 2. (2012)

[10] Muhammad, N., Bibi, N., Zahid, M., Tallha, A., Syed, R-N., Reversible Integer Wavelet Transform for Blind Image Hiding Method 10.1371/journal.pone.0176979, (2017)

[11] Muhammad, N., Bibi, N., Zahid, M., Tallha, A., Syed, R-N.: Reversible Integer Wavelet Transform for Blind Image Hiding Method, PLOS ONE, (2017)

[12] Jamal, S.S., Shah, T., Hussain, I.: An efficient scheme for digital watermarking using chaotic map, Nonlinear Dyn. 73(3), 14691474 (2013)

[13] Edward, N. L. Deterministic Nonperiodic Flow, Journal of the Atmospheric Sciences, 20(2), 130141, (1963)

[14] Edward, N. L. Atmospheric predictability as revealed by naturally occurring analogues, Journal of the Atmospheric Sciences, 26(4), 636646, (1969)

[15] Zhu, Z., Leung, H. Optimal synchronization of chaotic systems in noise, IEEE Trans. Circ. Syst.-I: Fund. Th. Appl. 46, 1320-1329

[16] Chen, G. R., Mao, Y. B., Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Solitons Fract. 21(3), 749761, (2004)

[17] Wong, K.W., Kwok, B., Law, W. A fast image encryption scheme based on chaotic standard map, Phys. Lett. A 372(15), 26452652, (2008)

[18] Khan, M., Shah, T. An efficient chaotic image encryption scheme, Neural Computing and applications, 26(5), 1137-1148, (2015)

[19] Wang, D., Zhang, Y. B. Image encryption algorithm based on S-boxes substitution and chaos random sequence, International Conference on Computer Modeling and Simulation, Guangzhou, China 110113, (2009)

[20] Venkatachalam, S. P., Vignesh, R., Sathishkumar, G. A. An improved S-box based algorithm for efficient image encryption, International Conference on Electronics and Information Engineering, India 1, 428431, (2010)

[21] Xu, Z. H., Shen, G., Lin, S. Image encryption algorithm based on chaos and S-boxes scrambling, Adv. Mater. Res. 171172, 299304, (2011)

[22] Wang, Y., Lie, P., Wong, K. W. A Method for Constructing Bijective S-Box with High Nonlinearity Based on Chaos and Optimization, Int J. Bifurcation Chaos 25, 1550127, (2015)

[23] Xiao, D., Fu, Q., Xiang, T., Zhang, Y. Chaotic Image Encryption of Regions of Interest, Int J. Bifurcation Chaos 26, 11, (2016)

[24] Farwa, S., Shah, T., Idrees. L. A highly nonlinear S-box based on a fractional linear transformation, SpringerPlus. 5: 1658, (2016)

[25] Muhammad N, Bibi N, Jahangir A, Mahmood Z. Image denoising with norm weighted fusion estimators. Pattern Analysis and Applications. 2017:1-10.

[26] Mahmood Z, Muhammad N, Bibi N, Ali T. A Review on state-of-the-art Face Recognition Approaches. Fractals. 2017;25(02):1750025.

[27] Bushra M, Muhammad N, Muhammad S, Tanzila S, Amjad R. Extraction of breast border and removal of pectoral muscle in wavelet domain. Biomedical Research-ind 2017;28(10): 1-3.

[28] N. Muhammad, et al. Image de-noising with subband replacement and fusion process using bayes estimators, Computers and Electrical Engineering, 2017, http://dx.doi.org/10.1016/j.compeleceng.2017.05.023.

[29] Mughal, B., Sharif, M., Muhammad, N,. Bi-model processing for early detection of breast tumor in CAD system, The European Physical Journal Plus, 6(132), (2017), 10.1140/epjp/i2017-11523-8.

[30] Nargis, B., Nazeer M., Kleerekoper. A, and Cheetham, B. Equation Method for correcting clipping errors in OFDM signal, SpringerPlus, splus-016-0294. ,

[31] Nargis, B., Nazeer M., Kleerekoper. A, and Cheetham, B. Inverted Wrap-Around Limiting with Bussgang Noise Cancellation Receiver for OFDM Signals, Circuits, Systems, and Signal Processing, (2017), 10.1007/s00034-017-0585-7.

[32] Zhang, Y., Xiao, D. Cryptanalysis of S-box-only chaotic image ciphers against chosen plaintext attack, Nonlinear Dyn. 72(4): 751-756, (2013)

[33] zkayanak, F., zer, A. B.: A method for designin g stron S-boxes based on chaotic Lorenz system. Phys. Letters A, 374(36), 3733-3738 (2010)

[34] Khan, M., Shah, T., Mahmood, h., Gondal, M. A.: An efficient method for the construction of block cipher with multi-chaotic systems. Nonline ar Dynamics, 71(3), 489-492 (2013)

[35] Gondal, M. A., Raheem, A., Hussain, I.: A scheme for obtaining secure S-boxes based on chaotic Bakers map. 3D Res., 5-17 (2014).

[36] Muhammad, N., Bibi, N. Kim, D. G.: A Fresnelet-Based Encryption of Medical Images using Arnold Transform, International Journal of Advanced Computer Science and Applications. A 1(1), 131140, (2013)