The Nucleus ***55***, *No.4 (2018) 219-225*

www.thenucleuspak.org.pk

The Nucleus
ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

A Novel Technique for the Generation and Application of Substitution Boxes (s-box) for the Image Encryption

S. Bukhari[1*], A. Yousaf[2], S. Niazi[1] and M. R. Anjum[1]

[1]*Department of Electronic Engineering, University College of Engineering & Technology, The Islamia University of Bahawalpur, Bahawalpur, Pakistan*

[2]*Department of Mathematics, The Islamia University of Bahawalpur, Bahawalpur, Pakistan*

ARTICLE INFO

Article history:
Received : 21 November, 2017
Accepted : 09 April, 2019
Published : 17 April, 2019

Keywords:
Substitution box,
Galois field,
Linear fraction transformation,
Non-linearity,
Strict avalanche criteria,
Statistical analysis

ABSTRACT

The increasing applications of image processing have shifted the focus to the security of images during their transmission. In this work, the main focus is on the security of gray scale images against cryptanalysis attacks. A new model for encryption algorithm of the grayscale image is presented through substitution boxes (s-box). The proposed technique contains two parts; in the first part six different substitution boxes are generated from Galois field and linear fractional transformations. In the second part, the generated substitution boxes are used for the encryption process of message image. For the estimation of the strength of the proposed technique; nonlinearity and strict avalanche criteria, statistical tests (contrast, correlation, energy and homogeneity) and histogram analysis were performed on the substitution boxes and on the encrypted images respectively to check its resistance. The proposed algorithm is found to be more robust as compared to other encryption techniques against attacks in insecure transmission paths.

1. Introduction

Image encryption technique is employed to protect the contents of image by transforming the confidential image into a noise-like image [1]. The information carried by images has very critical applications in the field of telemedicine, broadcasting, scientific research, government affairs and in the telecommunication field. As the transmitting media is open and insecure, it is very necessary to keep our data confidential from eaves droppers. It faces different threats during transmission on insecure channel like fabrication (middle person (attacker) makes the information false and sends it to the person), interruption (the transmitted information is blocked by the third persons and the intended receiver cannot receive the information), modification (the confidential data is eavesdropped by the attackers who send the data to the recipients by changing it), and interception (the confidential data are not only received by the intentional receiver, but also by the invader). These problems can be overcome using strong and complex cryptographic algorithms.

Image contains bulky information consisting of matrices of two or three dimensions, so its encryption and decryption processes are different than text files [2]. The values in these matrices which show the intensity and brightness of the images are called pixels. In image encryption techniques, the pixel values are transformed from the original values. Image security which is based on cryptography is divided into three major classes; permutation algorithms, pixel conversion dependent methodologies and visual change dependent algorithms [3]. In the work by Pareek and Patidar [4] and Enayatifar et al. [5] images are permuted by the Bakers map, logistic map, genetic algorithms, DNA sequence, Chen method, and column-row permutation. Encryption by permutation is also carried out either using pixels or bits. The bit planes are widely used in encryption of images.

In the study by Teng et al. [6] a chaos based bit level permutation was used in the encryption process for the image by first converting into three bit level and afterwards converted message image to one-bit level image. Xu et al. [7] presented an encryption method in which the message image was converted into two equal binary sequences that was diffused under the action of the piecewise linear chaotic map. There is another presented encryption algorithm in which multiple images are used in which encryption is done by xoring the chaotic permuted segmented image with scrambled image [8]. In the study by Tian and Lu [9] image is encrypted using both diffusion and confusion methods, in which confusion is done by chaotic dynamic substitution box and diffusion by DNA sequence.

In most of the research, the authors used two or more techniques step by step to increase the privacy of images. Pan et al. [10] presented a multiple image encryption technique which used the discrete wavelet transformation and nonlinear fractional mellin transformation. Arnold transformation was also used to scramble the secret images and discrete fractional angular transformation was applied to encrypt the scrambled image with phase information as a key in an iterative manner [11]. Chaotic time series is also used for scrambling of image for the encryption process [12]. Yuan et al. [13] enhanced image secrecy in both time domain and frequency domain by employing hyper digital chaos. Image steganography is another technique used for cover

*Corresponding author : sadafbukhari02@gmail.com

image to provide security to the message image. In the paper by Bukhari et al. [14] gray level image was first encrypted using double random phase encoding.

After the first step it was steganographed by employing least significant bit technique. However, the traditional cryptographic techniques were not fully utilized, instead some basic ideas and techniques were used in the encryption of image as a building block of ciphering technique [15]. Image security is also achieved by the substitution boxes. From review, permuted images are more vulnerable than substituted images. Substitution boxes are the nonlinear part of the symmetric cryptographic algorithm. It is the main part of the standard cryptographic algorithms like DES (data encryption standard) and AES (advanced encryption standard) etc. [16].

Substitution boxes fulfill the condition of confusion of secret communication presented by Claude Shannon against frequency analysis attack, words and phrases analysis attacks which were used to cryptanalyze the block ciphers. Substitution box is defined as a function in which the series of length *x* is an input and it outputs the series of length y. The main property of s-box is its size as DES used 6×4 size s-boxes and blowfish used 8×32 size s-boxes. S-box of larger size is more resistant to linear and differential attacks [17]. The main standardized encryption algorithms such as Data encryption standard (DES), advanced encryption standard (AES), Triple data encryption standard (TDES) and Chinese ZUC used the s-boxes for non-linearity purposes [18]. The construction of substitution box also depended on the three-D four wing autonomous chaotic system. In which the parameters a= 0.2, b= 0.01, c =1, d= -0.04, e= -1, f= -1 for the chaotic system equation were used. In previous study 16*16 substitution box was generated with nonlinearity 105.8 and strict avalanche criteria value 0.4976 [19]. In another method Mobius transformation and invertible equation were used to generate the substitution box. From that process, substitution box showed nonlinearity 108 with strict avalanche criteria value 0.476 [20]. Alkhaldi et al. [21] presented the algorithm for the generation of substitution box. It was based on the tderc sequence which is two dimensional chaotic sequences. The analysis tests showed the nonlinearity 104 and strict avalanche criteria 0.4609.

For the design of s-boxes random, man-made and mathematical approaches are used. In this paper, we focus on the generation of s-box through math made approach. In math made approach, mathematical principles are used for the generation of s-boxes [22]. The encryption process of gray scale image was carried out by the AES Gray substitution boxes and the phase embedding technique [23]. Some are generated using the finite fields. In the study by Azam [24] 40320 s-boxes were generated by employing symmetric permutation group on Galois field with non-linearity of 104. S-boxes generated from the heuristic algorithm and hill climbing techniques were also efficient against differential attacks. Some security algorithms employed arlond transformation to increase the strength of substitution boxes by certain number of iterations [25]. In the work by Zhang et al. [26] substitution box is designed using chaotic properties of the Lorenz equation for image encryption.

The linear fractional transformation was also used in the construction of substitution boxes to produce non-linearity in them. Substitution boxes which are made from chaotic maps for the advanced encryption standard (AES) also showed non-linearity 106 [27]. The main emphasis of this paper is the encryption of a gray level image through substitution boxes, which are generated by finite field and different orders of linear fractional transformation. The resultant substituted images are tested by statistical tests to evaluate the robustness of designed encryption technique against attacks.

2. Linear Fractional Transformation

Linear Fraction Transformation (LFT) is also known as the Mobius transformation and is expressed as:

$$Z(x) = (a)\,(x) + (b)/(c)\,(x) + (d) \quad (1)$$

Where *a, b, c* and *d* belong to the given fields and it satisfies the condition ad-bc≠0.

LFT contains one or two specific elements and gives the symmetry.

3. Galois Field

Evariste Galois gave the idea of Galois field that contains a fixed number of elements. It is also known as the finite field. In a finite field GF (M^n) mathematical operations are applied to the data which is represented as a vector. A field has two operations, additions and multiplications. In the Galois field, prime integer is used (M). The prime integer (n) is greater than or equal to zero [28]. In this way Galois field, becomes a unique field containing M^n Elements. In the encryption field, M is chosen as 2. Advanced encryption standard (AES) used the GF (2^8) in its block cipher. In this field, the elements are represented by bytes (8 bits). These 8-bit elements are referred as a polynomial with coefficients. The polynomial of each element has degree n^{-1}.

GF (2^8) is expressed in the form of irreducible polynomial as:

$$a^8 + a^4 + a^3 + a^2 + 1 \quad (2)$$

The elements of the Galois field GF (P^n) are represented as:

$$GF(M^n) = (0,1,2,\dots,M-1)\ U\ (M, M+1, M+2, \dots M+M-1)\ U\ (M^2, M^2+1, M^2+1, \dots M^2+M-1)\ U \dots U (M^{n-1}, M^{n-1}+1, \dots M^{n-1}+M-1) \quad (3)$$

4. Methodology

This paper has focused on the security of grayscale image with the help of encryption by substitution boxes (s-boxes). In image encryption, the input is a message image and we get the output as a cipher image. A grayscale image is represented by the matrix which contains the specific range of intensities of the pixels.

Processing of the grayscale image is less complicated because it requires the least amount of information. In the encryption process, substitution box is used for the replacement of pixels in the plain text image and generates the substituted image. S-box elements are created from mathematical formulas. Its elements are not randomly selected or permuted but are balanced by mathematical formulas.

4.1 Construction of s-box

The construction of substitution box (m×n) is carried out with the Galois field elements and linear fractional transformation. In this methodology, primitive polynomial is generated from the Galois field (2^8). In the Galois field, each element is represented by a vector. So that each element is converted into a binary vector containing 1s and 0s. Substitution box consists of a finite number of elements 2^n. Each element of the substitution box consists of n bits, for example, in the case of GF (2^8), each element of s-box has 8 bits. These elements are generated from the irreducible primitive polynomial, and used in LFT. The elements of Galois field are used in different orders LFT formula to generate different substitution boxes. These orders of LFTs are used as secret keys. In the proposed methodology the algorithm should satisfy the LFT condition that the determinant of the LFT function does not equal to zero. For the calculation of elements of substitution box or to find $s_i = (\frac{a_i+b_i}{c_i+d_i})$, each element in binary form of the finite field is individually passing through s_i (transformation).

Table 1: Values of a, b, c, d in s_i.

No.	S-box	i	a	b	c	d
1	S_1	1	14	50	0	60
2	S_2	2	29	201	29	39
3	S_3	3	3	67	9	3
4	S_4	4	10	197	102	216
5	S_5	5	147	155	1	200
6	S_6	6	54	1	200	1

Indexes are calculated from the numerator and denominator of the transformation. These indexes are used to find the values of the elements of field and elements of s-box is the resultant of the subtraction of the indexes of numerator and denominator of transformation. The LFTs are $s_i = (\frac{a_i+b_i}{c_i+d_i})$ where *i, a, b, c, d* are given in Table 1. From this process six substitution boxes of size 16×16 are generated.

4.2 Image Encryption

In this process, the pixels of the original image are taken and converted into the binary form (8 bits). Then these bits are divided into two equal parts (4 bits each) and each parts is converted into a decimal number which is used to locate the elements from substitution box to substitute in message image. In this way, the iteration number depends on the number of pixels of message image. The proposed methodology is shown in Fig. 1.

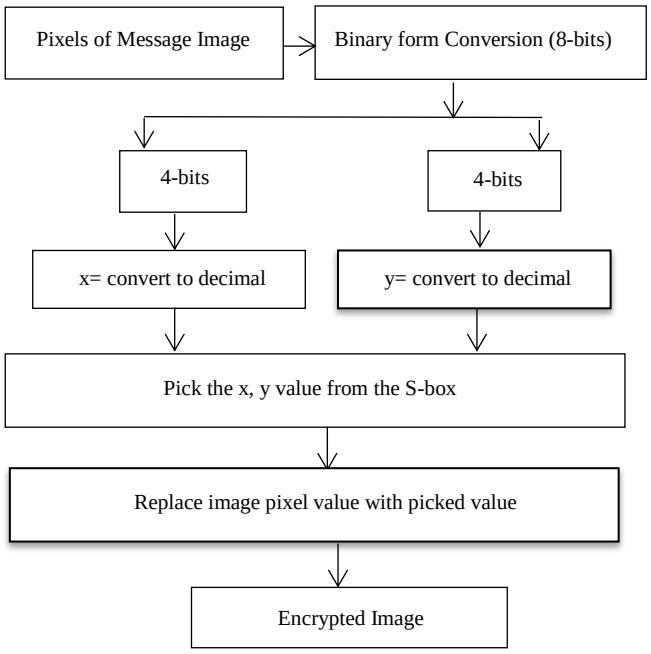

Fig. 1: Proposed methodology

5. Results and Discussion

In this section, the outcomes of the proposed technique for encryption of images are presented. In the section below, visual results show the encrypted images. The second section discusses the tests that are used to analyze the generated substitution boxes by nonlinearity (NL) and strict avalanche criteria (SAC). It also discusses results by applying statistical tests on message image and substituted or encrypted images.

5.1 Visual Results

In MATLAB, the implementation of image encryption technique through generated substitution boxes is taken. Visual results contain the eight types of images; first two are the colored message image and the grayscale message image respectively, and the others are the ciphered images which are encrypted through the generated substitution boxes as shown in Fig. 2. After getting the visual results, statistical tests (contrast, correlation, energy and homogeneity) are performed on the encrypted images for the evaluation of its immunity against cryptanalysis. In addition to this, the resultant ciphered images and the plain image are analyzed by histograms. For substitution-box (s-box) evaluation tests; two tests nonlinearity and the strict avalanche criteria are applied on the proposed substitution boxes. Afterwards, the

calculated values of non-linearity and strict avalanche criteria of generated substitution boxes are compared with the references [19-21] in which substitution boxes are generated by using different techniques.

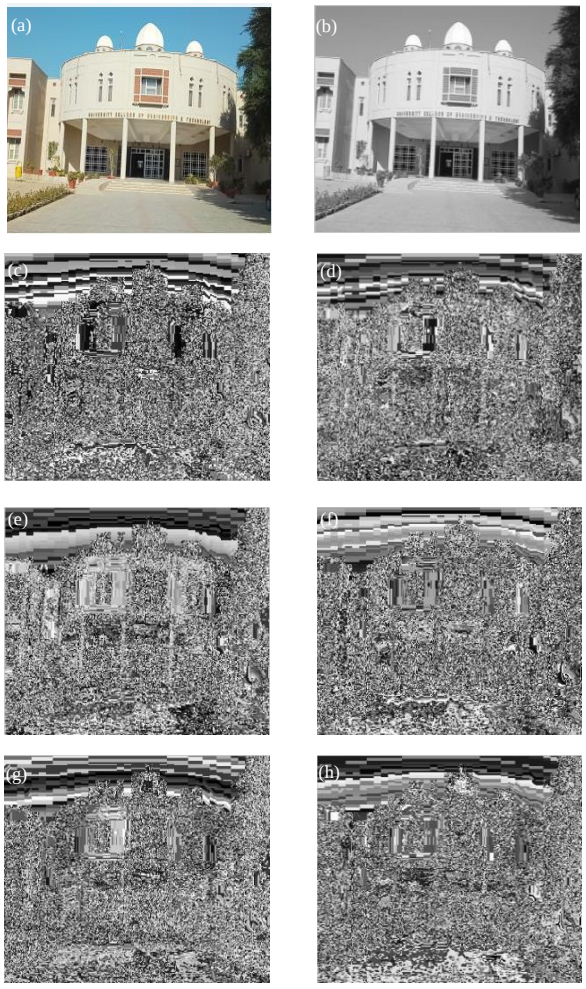

Fig. 2: (a) Plain image, (b) Grayscale image, (c) Encrypted image with S_1, (d) Encrypted image with S_2, (e) Encrypted image with S_3, (f) Encrypted image with S_4, (g) Encrypted image with S_5, (h) Encrypted image with S_6.

5.2 Analysis Tests on s-box

5.2.1 Nonlinearity

The definition of nonlinearity of the substitution box is dependent on the hamming distance between the given function and the linear function. For the linearity criteria, the hamming distance should be minimum. It is also defined as there is no linear mapping of the substitution box between the input and output vector [29]. For the boolean functions, Walsh Hadamard transformation Matrix is very useful. The nonlinearity of the s-box is calculated by making the boolean functions (*f*) and then applying Walsh Hadamard transformation on it to check the correlation between linear functions and the boolean functions [30]. It is difficult to compute the non-linearity when *n* is large. The nonlinearty of six different s-boxes are depicted graphically in Fig. 3 which shows that there is no linear mapping between elements of s-box (output) and Galois field elements (Input).

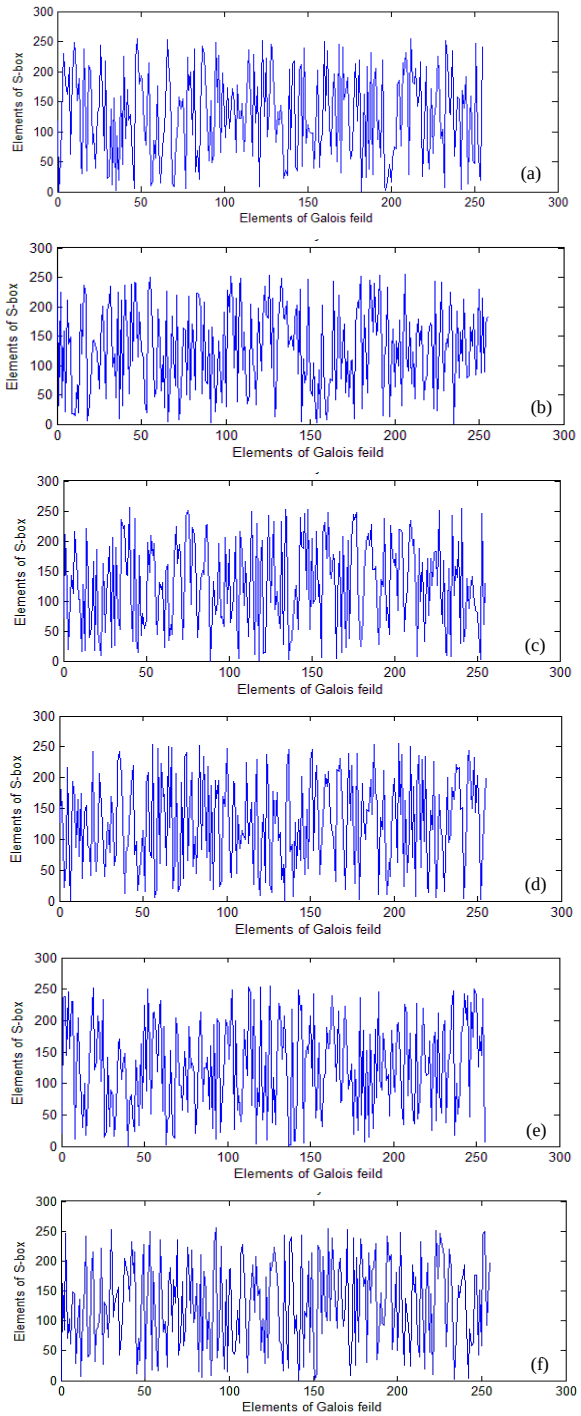

Fig. 3: (a) Non linearity behaviour of S_1, (b) Non linearity behaviour of S_2, (c) Non linearity behaviour of S_3, (d) Non linearity behaviour of S_4, (e) Non linearity behaviour of S_5, (f) Non linearity behaviour of S_6.

The nonlinearity is formulated as:

$$NL = \frac{1}{2}\left(2^n - WHT\left(max(f)\right)\right) \quad (4)$$

Good substitution box tries to reach its ideal nonlinear value. The ideal value for the non-linearity of s-box in GF(2^8) is 120, which is calculated through the given formula:

$$NL \leq \frac{2^n - 2^{n/2}}{2} \quad (5)$$

Where n= 8.

5.2.2 Strict Avalanche Criteria (SAC)

For the effective design of substitution box, it should satisfy the strict avalanche criteria (SAC). In the designing of the substitution box, our requirement is to get balanced s-box in which, when the input vector is changed in all possible combination then every output should appear on that amount of time [31]. Through this criteria, only 50 percent bits change in the output. It means that when only one bit is changed in the input, the output result depicts change in bits of 0.5. In Table 2 both calculated values of non-linearity (NL) and strict avalanche criteria (SAC) of proposed substitution boxes (s-boxes) are tabulated. From the results, it is clear that proposed substitution boxes have shown good values of non-linearity and strict avalanche criteria than the compared ones.

Table 2: Non-linearity (NL and SAC for substitution boxes).

S-box	NL	SAC
[19]	105.8	0.4976
[20]	108	0.46
[21]	104	0.4609
S_1	112	0.5156
S_2	102.3750	0.4854
S_3	105.75	0.5215
S_4	108.125	0.5029
S_5	104	0.5000
S_6	107.25	0.5117

5.3 Statistical Tests

In this section statistical tests have been performed to prove the robustness of the proposed methodology used for encryption, which describes its confusion property against statistical attacks.

From literature review, it is clear that many encryption algorithms have been broken with the assistance of statistical properties. These statistical tests are explained below.

5.3.1 Contrast

In image processing brightness and contrast of the image are properly adjusted for easy viewing. Contrast is defined as the difference in the object's brightness. In encryption process, the contrast value is directly proportional to the randomness of the image [32]. The constant image has zero contrast value. It is formulated as:

$$C = \sum_{k,r}^{n-1,m-1} |k - r|^2 P(k,r) \quad (6)$$

Where *P (k, r)* represents the position of pixels in gray level co-occurrence matrices.

Table 3: Contrast Analysis between plain image and encrypted image.

Contrast Analysis		
S-box	Plain Image	Encrypted Image
S_1	0.5834	8.2718
S_2		7.7263
S_3		6.8759
S_4		7.4659
S_5		7.2074
S_6		7.1113

Table 3 shows the contrast analysis of plain image and encrypted images which showed that contrast value of encrypted image with substitution box S_1 has higher value than plain image contrast value.

5.3.2 Correlation

Correlation analysis measures the closeness of pixel values to its neighboring values. It gives the linear relationship between two pixel values of the image. Correlation is measured in vertical, horizontal, diagonal formats. Its range is between -1 and +1. If the value of correlation is +1 then the image is positively correlated and if it is -1 then the image is negatively correlated [33]. The correlation between the neighboring pixels in the plain image is strong. The encrypted image which has less correlated values is more robust in insecure channel.

The mathematical formula of correlation analysis is as follows:

$$K = \sum_{k,r} \frac{(k-\mu k)(r-\mu r)p(k,r)}{\sigma_k \sigma_r} \quad (7)$$

Where μ and σ are the variance and the mean of the glcm (gray level co-occurrence matrix), respectively.

Table 4 provides the correlation analysis of the message image and ciphered images with different generated substitution boxes. The calculated outcomes clarifies that the encrypted image has lower value of correlation than the plain image when used S_1.

Table 4: Analysis of correlation values of message image and the ciphered image.

Correlation Analysis		
S-box	Plain image	Encrypted image
S_1	0.9226	0.2761
S_2		0.2664
S_3		0.3123
S_4		0.2587
S_5		0.2902
S_6		0.3176

5.3.3 Energy

In energy analysis, the sum of the squared elements of gray level co-occurrence is measured [34]. In the plain image, the observed energy value is high because in glcm (gray level co-occurrence matrix) high valued pixels are found in some specific place. In ciphered image, energy values are distributed and show low energy. That is why the energy of the encrypted image is small as compared to the original message image.

The energy analysis is mathematically defined as:

$$E = \sum_{k,r} p(k,r)^2 \quad (8)$$

Table 5 contains the energy analysis values between the message image and the encrypted images with different substitution boxes which illustrates that the encrypted image has lesser energy value than the plain image that used the substitution box S_1 during encryption.

Table 5: Energy analysis between the plain image and the encrypted image.

Energy Analysis		
S-box	Plain image	Encrypted image
S_1	0.1025	0.0246
S_2		0.0241
S_3		0.0255
S_4		0.0241
S_5		0.0246
S_6		0.0254

5.3.4 Homogeneity

In homogeneity analysis, the familiarity of the distribution of components of gray level co-occurrence and diagonal gray level co-occurrence is measured [35]. Its value is highly dependent on the elements present on the diagonal of glcm (gray level co-occurrence matrix). Its range is between zero and one. In encryption process, the homogeneity value is small which reveals the strength of the encryption algorithm.

Homogeneity analysis is mathematically defined as:

$$M = \sum_{k,r} \frac{p(k,r)}{1+|k-r|} \quad (9)$$

Table 6: Analysis of Message image and encrypted image.

Homogeneity Analysis		
S-box	Plain Image	Encrypted Image
S_1	0.8674	0.5463
S_2		0.5508
S_3		0.5598
S_4		0.5516
S_5		0.5500
S_6		0.5579

Table 6 shows the homogeneity analysis of the message image and the ciphered images with different substitution boxes. It represents that the encrypted image has a small homogeneity value when substitution box S_1 is used in the encryption process.

6. Histrogram Analysis

In histogram analysis, the distribution of intensities of the color values of the pixels is illustrated. It is used to find the difference between the intensities of colours between non-ciphered and ciphered image [36]. The histogram of the encrypted image is mainly different from the histogram of the plain image and shows no statistical similarity to the plain image.

Fig. 4 depicts the histogram analysis of the proposed technique outcomes. It consists of histograms of message image and encrypted images. These results make clear that the histograms of encrypted image are different from the message image histogram and give no evidence of the message image.

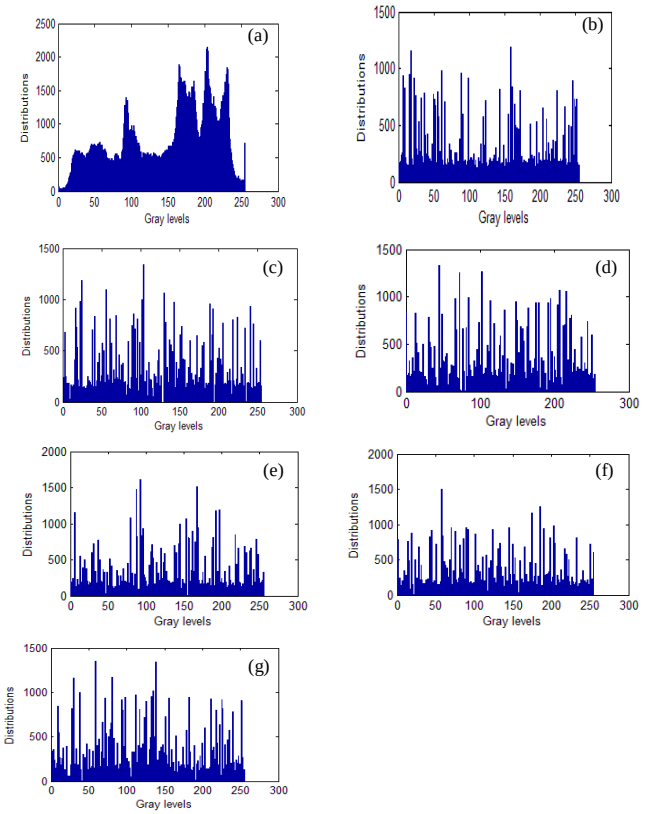

Fig. 4: (a) Histogram of original image, (b) Histogram of encrypted image with S_1, (c) Histogram of encrypted image with S_2, (d) Histogram of encrypted image with S_3, (e) Histogram of encrypted image with S_4, (f) Histogram of encrypted image with S_5, (g) Histogram of encrypted image with S_6.

7. Conclusions

It is concluded from the experimental results and analysis tests that the proposed encryption algorithm for a grayscale image has fulfilled the main objective of cryptography, i.e., confidentiality. It is based on the generation of substitution boxes through linear fraction transformation and elements of Galois field and implementation of these substitution boxes for ciphering the plain image. The message image showed

more randomness and immunity against attacks when encrypted with S_1 (substitution-box) which has a high nonlinearity value and satisfies the strict avalanche criteria as compared to the other substitution boxes (S_2, S_3, S_4, S_5, and S_6).

References

[1] Q. Jiang, W. Zeng, W. Ou and R. Xu, "A scrambling and encryption algorithm for selective block of identification photo", IEEE 8th International Conference on Wireless Communications & Signal Processing, WCSP, Yangzhou, China, pp. 1-5, October 13-15, 2016,

[2] J. Mondal and D. Swain, "A Contemplator on topical image encryption measures: Security breaches and threat prevention in the internet of things, India", IGI Global, pp. 189-212, 2017.

[3] L. Bao and Y. Zhou, "Image encryption: generating visually meaningful encrypted images", Information Sciences, vol. 324, pp. 197-207, 2015.

[4] N.K. Pareek and V. Patidar, "Medical image protection using genetic algorithm operations", Soft Computing, vol. 20, pp.763-772, 2016.

[5] R. Enayatifar, A.H. Abdullah, I.F. Isnin, A. Altameem and M. Lee, "Image encryption using a synchronous permutation-diffusion technique", Optics and Lasers in Engineering, vol. 90, pp. 146-154, 2017.

[6] L. Teng, X. Wang and J. Meng, "A chaotic color image encryption using integrated bit-level permutation", Multimedia Tools and Applications, vol. 24, pp. 1-14, 2018.

[7] 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.

[8] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and permutation", Optics and Lasers in Engineering, vol. 92, pp. 6-16, 2017.

[9] Y. Tian and Z. Lu, "Novel permutation-diffusion image encryption algorithm with chaotic dynamic S-box and DNA sequence operation", AIP Advances, vol. 7, pp. 085008, 2017.

[10] S.M. Pan, R.H. Wen, Z.H. Zhou and N.R. Zhou, "Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform", Multimedia Tools and Applications, vol. 76, pp. 2933-2953, 2017.

[11] Z. Liu, M. Gong, Y. Dou, F. Liu, S. Lin, M.A. Ahmad, J. Dai and S. Liu, "Double image encryption by using Arnold transform and discrete fractional angular transform", Optics and Lasers in Engineering, vol. 50, pp. 248-255, 2012.

[12] G.C. Wu, D. Baleanu and Z.X. Lin, "Image encryption technique based on fractional chaotic time series", Journal of Vibration and Control, vol. 22, pp. 2092-2099, 2016.

[13] W. Yuan, X. Yang, W. Guo, and W. Hu, "A double-domain image encryption using hyper chaos", IEEE 19th International Conference on Transparent Optical Networks, ICTON, 2017, Gerona, Spain, pp. 1-4, July 2-6, 2017.

[14] S. Bukhari, M. S. Arif, M. R. Anjum, and S. Dilbar, "Enhancing security of images by Steganography and Cryptography techniques", IEEE Sixth international Conference on Innovative Computing Technology, INTECH, Dublin, Ireland, pp. 531-534, August 24-26, 2016.

[15] T. Cipresso and M. Stamp, "Software reverse engineering": Handbook of Information and Communication Security, 2nd ed., Berlin Heidelberg: Springer, pp. 659-696, 2010.

[16] C. Paar and J. Pelzl, "Understanding cryptography: A textbook for students and practitioners, Germany: Springer Science & Business Media, pp. 30-40, 2009.

[17] A. Biryukov, L. Perrin and A. Udovenko, "Reverse-engineering the S-box of Streebog, Kuznyechik and STRIBOBr", Advaces in cryptology eurocrypt: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2nd ed., vol. 003, M. Fichlin and S.J. Coron, Ed. Austria: Springer, pp. 372-402, 2016.

[18] M.N.A. Wahid, A. Ali, B. Esparham and M. Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention", JCSIT., vol. 3, pp. 1-7, 2018.

[19] G. Liu, W. Yang, W. Liu and Y. Dai, "Designing S-boxes based on 3-D four-wing autonomous chaotic system", Nonlinear Dynamics, vol. 4, pp. 1867-1877, 2015.

[20] M. Sarfraz, I. Hussain and F. Ali, "Construction of S-box based on mobius transformation and increasing its confusion creating ability through invertible function", IJCSS, vol. 14, pp. 187, 2016.

[21] A.H. Alkhaldi, I. Hussain and M.A. Gondal, "A novel design for the construction of safe S-boxes based on TDERC sequence", Alexandria Engineering Journal, vol. 54, pp. 65-69, 2015.

[22] N.R. Zhou, T.X. Hua, L.H. Gong, D.J. Pei and Q.H. Liao, "Quantum image encryption based on generalized Arnold transform and double random-phase encoding", Quantum Information Processing, vol. 14, pp. 1193-1213, 2015.

[23] M. Juhani and O. Saarinen, "Cryptographic analysis of all 4×4-bit s-boxes", International Workshop on Selected Areas in Cryptography, Berlin Heidelberg, Springer, vol. 7118, pp. 118-133, 2011.

[24] N.A. Azam, "A Novel Fuzzy Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding", Security and Communication Networks, vol. 2017, pp-1-9, 2017.

[25] S. Farwa, N. Muhammad, T. Shah and S. Ahmad, "A novel image encryption based on algebraic S-box and Arnold transform", 3D Research, vol. 8, no. 3, pp. 26, 2017.

[26] X. Zhang, Z. Zhao and J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer", Signal Processing: Image Communication, vol. 29, pp. 902-913, 2014.

[27] V.M.S. Garcia, R.F. Carapia, C.R. Marquez, B.L. Benoso and M.A. Perez, "Substitution box generation using Chaos: An image encryption application", Applied Mathematics and Computation, vol. 332, pp. 123-135, 2018.

[28] I. Hussain, T. Shah, H. Mahmood and M.A. Gondal, "Construction of S 8 Liu J S-boxes and their applications", Computers & Mathematics with Applications, vol. 64, pp. 2450-2458, 2012.

[29] F.A. Khan, J. Ahmed, J.S. Khan, J. Ahmad and M.A. Khan, "A novel substitution box for encryption based on Lorenz equations", IEEE International Conference on Circuits, System and Simulation, pp. 32-36, July 14, 2017, London, UK.

[30] W. Wen, Y. Zhang, Y. Fang, and Z. Fang "Image salient regions encryption for generating visually meaningful cipher text image", Neural Computing and Applications, vol. 29, no. 3, pp. 653-663, 2018.

[31] C.J. Benvenuto, "Galois Field in Cryptography", University of Washington, pp. 56, 2012.

[32] C. Adams, and S. Tavares, "The structured design of cryptographically good S-boxes", Journal of Cryptology, vol. 3, pp. 27-41, 1990.

[33] O. Kazymyrov, V. Kazymyrova and R. Oliynykov, "A Method for Generation of High-Nonlinear S-Boxes Based on Gradient Descent", IACR Cryptology ePrint Archive, vol. 23, pp. 578, 2013.

[34] R. Forre, "The strict avalanche criterion: spectral properties of Boolean functions and an extended definition", Lecture notes in computer science: Advances in cryptology, Ed. 1, vol. 403, New York, Springer-Verlag, pp. 450-468, 1990.

[35] S.A.K.E. Hafiz, A.G. Radwan, S.H.A. Haleem and M.L. Barakat, "A fractal-based image encryption system", IET Image Processing, vol. 8, pp. 742-752, 2014.

[36] S. Som and S. Sen, "A non-adaptive partial encryption of grayscale images based on chaos". Procedia Technology, vol. 10, pp. 663-671, 2013.