Optica Applicata, Vol. XLIX, No. 2, 2019
DOI: 10.5277/oa190212

Image encryption based on Chebyshev chaotic map and S_8 S-boxes

Iqtadar HUSSAIN[1, 2], Amir ANEES[3], Ali Hussain ALKHALDI[4], Muhammad ASLAM[5], Nasir SIDDIQUI[6], Rehan AHMED[7]

[1]Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia; ihkhudad@kku.edu.sa

[2]Department of Mathematics, Statistics and Physics, Qatar University, Doha 2713, Qatar; iqtadarqau@qu.edu.qa

[3]Department of Electrical Engineering, HITEC University, Pakistan; amir.anees@hitecuni.edu.pk

[4]Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

[5]Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia; aslamq@qau.edu.pk

[6]Department of Basic Sciences, University of Engineering and Technology, Taxila, Pakistan

[7]Department of Meteorology, Comsats Institute of Information Technology, Islamabad, Pakistan

The encryption of image data is artful as compare to others due to some special characteristics such as entropy, contrast, the correlation between the pixels, intensity, and homogeneity. During encryption process, it is conventionally not easy to manage these characteristics with non-chaotic cryptosystems. Therefore for the sake of strong encryption algorithms, in last decades many cryptographers have presented invulnerable schemes for image encryption based on the chaotic maps. This manuscript aims to propose a strong encryption scheme based on a symmetric group of permutation advanced encryption standard (AES) substitution boxes and modified Chebyshev map. Principally, the secret key depends upon the parameters of Chebyshev map to create confusion in the main image and is encrypted by the scheme made from the S_8 AES S-boxes and chaotic map. By this procedure, one can obtain an encrypted image that is entirely twisted. The results of analyses showed that the presented image encryption is strong and invulnerable.

Keywords: image encryption, chaos, noise-resistant, statistical analysis, key sensitivity.

1. Introduction

Nowadays, secret data is conveyed through insecure channels, such as the Internet. For the security of the data, various kinds of cryptosystems have proposed, especially for

images [1–7]. Moreover, numerous features should be focused in the images cryptosystems, specifically: the primary feature is the complexity of the presented algorithm, and the secondary feature, it is critical to do not carry out uncertainty analyses on cryptosystems such as entropy, contrast, the correlation between the pixels, intensity, and homogeneity.

Last decade is considered as a remarkable era for secure communication and image processing. In wireless communication, protection of digital data such as text, sound, image, and video has got more importance because multimedia kind of stuff has taken hold on many important fields like electronic commerce, banking industry, law enforcement agencies requirements and personal data. The performance of old cryptosystems for image is poor in encryption of bulk-sized data [8–16]. To tackle this problem, new schemes based on chaos for image encryption have been developed [17–20]. AMIGÓ *et al*. [10], and JAKIMOSKI and KOCAREV [13] have shown a link between secure communication and chaos theory. They said some basic requirements of secure communication such as randomness, robustness, and sensitivity to initial conditions could be achieved by chaotic maps. OTT [14], and ALVAREZ and LI [15] have observed that values obtained by chaotic maps can be regained based on initial conditions but extremely erratic, and this kind of behavior is valuable for cryptosystems. Based on these properties, some cryptographers have proposed novel cryptosystems [16, 21]. Pseudorandom number generator based on chaotic maps is one of the emerging fields nowadays and can be utilized in different cryptosystems to get more security [22, 23].

Moreover, the combination of symmetric group of permutation and Chebyshev chaotic map is used to propose an image encryption [24]. In that work, the private keys are the initial conditions and parameters of chaotic Chebyshev map. Using this method, the ciphertext is completely different and random with respect to the plaintext. The decryption algorithm is just the inverse of the encryption algorithm. The converted image can be deciphered well when the handler gets the exact keys. Finally, the outcomes of numerous investigates illustrates that the scheme of image encryption is successful, and some safety analyses are offered to display it's high security for image encryption and transmission.

The manuscript is planned as follows. Section 2 presents the preliminaries of the proposed image encryption algorithm, Section 3 describes the proposed encryption algorithm in detail, Section 4 presents the simulation results and security analysis, and, finally, Section 5 concludes the paper.

2. Preliminaries

In this section, we will present the basic of chaotic map and its significance in secure communication. The S_8 S-boxes and motivation of the proposed work are given later.

2.1. Modified chaotic map and its randomness

It is a well known that Chebyshev polynomial can produce chaotic behavior for particular initial conditions [16]. The Chebyshev polynomials are as follows:

$$C_y(d) : [-1, 1] \to [-1, 1] \tag{1}$$

$$C_y(d) = \cos(y \cos^{-1} d) \tag{2}$$

where y is the degree of polynomial $C_y(d)$.

The above polynomials fulfill the following conditions:

$$C_0(d) = 1 \tag{3}$$

$$C_1(d) = d \tag{4}$$

$$C_y(d) \equiv 2dC_{y-1}(d) - C_{y-2}(d), \quad y \geq 2 \tag{5}$$

$$C_{y_1}(C_{y_2}(d)) = C_{y_2}(C_{y_1}(d)) = C_{y_1 y_2}(d), \quad y_1, y_2 = 0, 1, 2, \ldots \tag{6}$$

The modified map is as follows:

$$y(i + i) = \text{mod}(\text{floor}(y(i) \cdot 1000 \cdot n), 256) + 1 \tag{7}$$

where, n is the number of S-boxes involved in the experiment. To test the randomness of the modified map, we are going to use renown built in "runs test" function of Matlab, $[h, p, \text{stats}] = \text{runstest}(x)$. The results of modified Chebyshev chaotic map are very good such as $h = 0$, $P = 0.2436$, number of runs is 384, values above mean of $x = 397$, values below mean of $x = 403$ and test statistic is –1.1659. It means modified Chebyshev map is random.

2.2. S_8 AES S-boxes

In [24], HUSSAIN *et al*. presented a scheme for the construction of S_8 AES S-boxes. The authors used the definition of group action which is as follows. If M is a group and S is a set, then a (left) group action φ of M on S is a function

$$\varphi : M \times S \to S : (m, s) \to \varphi(m, s) \tag{8}$$

where, $s \cdot e = s$ and $s \cdot (m \cdot h) = (s \cdot m) \cdot h$ for all $g, h, e \in G$ and for all s in S. For the construction of S_8 AES S-boxes, HUSSAIN *et al*. [24], replaced M with S_8 symmetric group of permutation and S with GF(2^8) Galois field of order 256 to construct 40320 S-boxes with same properties as AES S-box. The mathematical expression of S_8 AES S-boxes is as follows:

$$\varphi : S_8 \times \text{GF}(2^8) \to \text{GF}(2^8) : (\alpha, f) \to \varphi(\alpha, f) \tag{9}$$

where $\alpha \cdot e_{\text{GF}(2^8)} = \alpha$ and $\alpha \cdot (f_1 \cdot f_2) = (\alpha \cdot f_1) \cdot f_2$ for all $f_1, f_2 \in GF(2^8)$ and for all α in S_8.

2.3. Motivation

We have three inspirations in the wake of a presented algorithm such as:

1. To assemble a new and well-organized S-P network from various S-boxes and the applications of chaos. The S-boxes will create fruitful results to reduce the correlation among the pixels of the encrypted image in few rounds be based on the number of S-boxes utilized in the scheme. Figure 1 presents an example of an image with sixteen pixels in the form of a row vector and the correlation among the pixels of part A is ideally high that is one due to the same (white) color of every pixel. In part B, it can be seen that correlation is still one because one S-box will not reduce the correlation among the pixels because the color of every pixel is black. When we will use multiple different S-boxes the probability that two pixels will have same correlation will be very low as can be seen in part C. With the help of multiple S-box transformations method, we can get the desired confusion in fewer rounds as compare to single transformation.

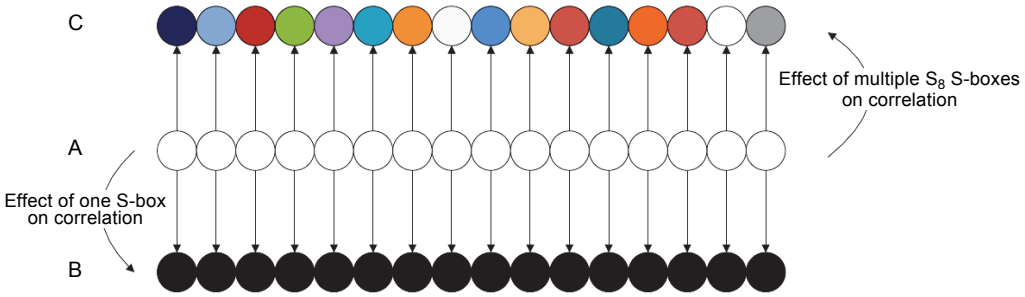

Fig. 1. Effect of multiple S-boxes transformations on an image with correlation 1. Sixteen pixels plaintext image in row vector with correlation 1, *i.e.* all the pixels have same color (A). Transformed row vector image corresponding to single S-box substitution, it can be observed that color of all pixels are same, *i.e.* correlation is 1 (B). Transformed image corresponding to sixteen different S-boxes, it can be observe that color of all pixels are different, *i.e.* correlation is better as compared to single S-box substitution (C).

2. Proposed algorithm should be good against all known attacks.
3. Proposed algorithm should be noise tolerant, *i.e.*, the decryption can be possible even with the presence of channel noise.

3. Proposed algorithm

The proposed algorithm is a combination of confusion-diffusion network. The confusion is gained using the symmetric group of permutation S-boxes [24] and diffusion is achieved with the help of permutation of a particular type. The proposed algorithm is a novel chaotic S-P network explained in Fig. 2. The proposed S-P network is as follows.

3.1. Substitution process

The substitution process is defined as follows. The substitution is done in blocks of data having eight bits in each block. The application of data is image which has pixels

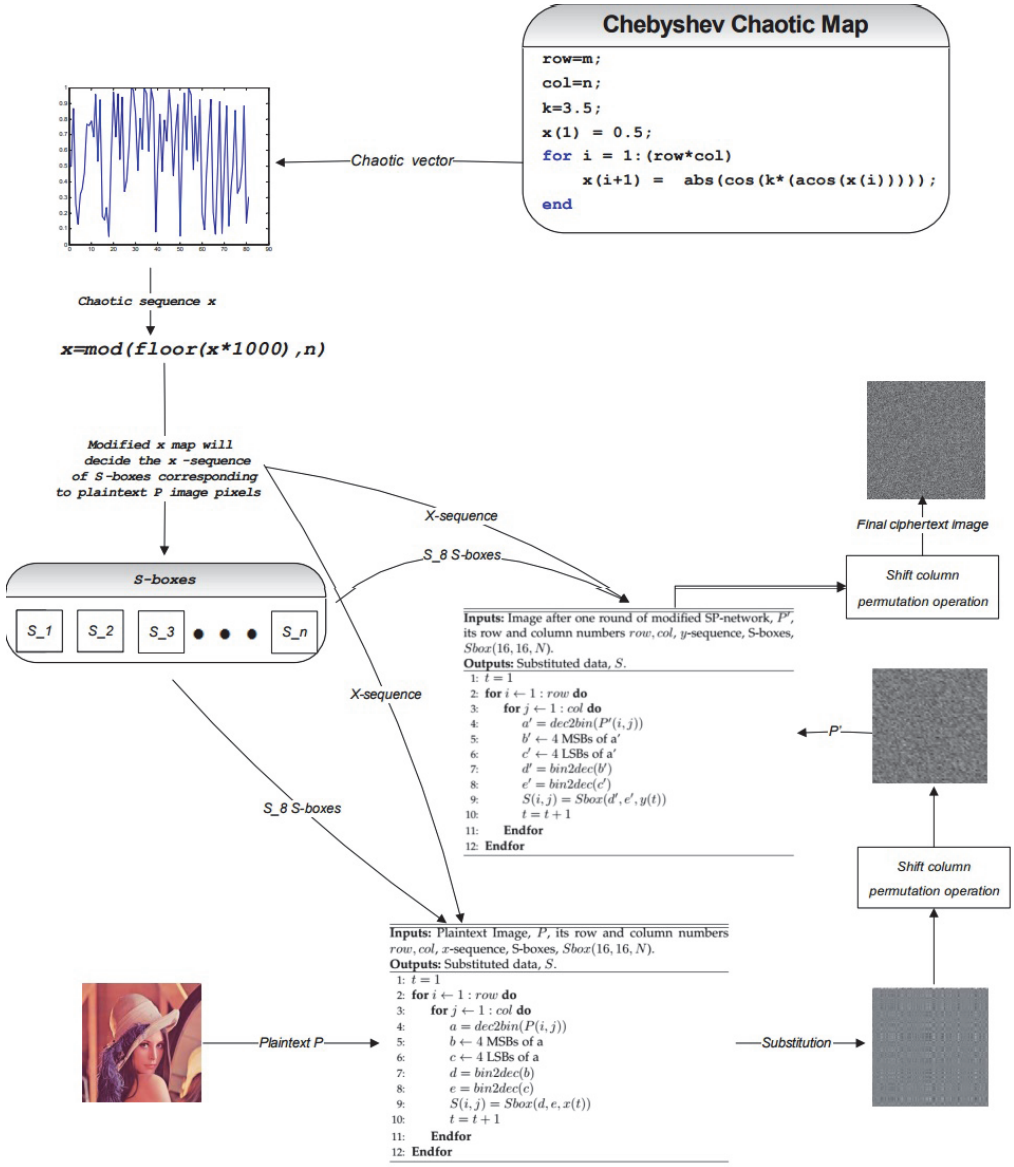

Fig. 2. The proposed image encryption algorithm.

values between 0 and 255 and therefore can be represented in eight bits. For a color image, there are three frames: red, green and blue, respectively. Let take a single image pixel from a single frame, denoted as I. This pixel is converted into binary of eight bits, represented as I_b. The eight bits are then divided into two sections, having four binary bits each, labeled as I_{lsb} and I_{msb}. These two sections of binary bits are converted into decimal values having the range between 0 and 15. These decimal values of I_{lsb} and I_{msb} corresponds to the row and column position of a substitution box. The element at

that position will be replaced with I. This step will be performed for all the image pixels using different substitution boxes which are proposed earlier. The decision of substituting image pixel with one of the S-box from the group of 256 S_8 AES S-boxes is done by the chaotic values corresponding to chaotic trajectories x of Chebyshev chaotic map. The chaotic value of Eq. (5) does the decision of substituting image pixel with one of the S-box from the group of S_8 AES S-boxes. One based on Chebyshev chaotic map

$$x = \mathrm{mod}(\mathrm{floor}(x \cdot 1000), N) \tag{10}$$

where N represents the total number of substitution boxes than can be employed. More the substitution boxes, the more data get random. However, it will also increase the computational complexity and therefore may not require for a low profile application. If we consider an image as a plaintext, the first image pixel of that image is substituted by the substitution box defined by x_1, the second image pixel will be substituted by the substitution box defined by x_2 and so on. Also, the sequence of substitution boxes is random defined by the initial condition and parameters of the chaotic map. By changing the values of these initial condition, the sequence of substitution boxes can also be changed.

3.2. Permutation process

Once the data is substituted with the multiple substitution boxes, the next step is to diffuse the data using the permutation which is defined as the shuffling of rows and columns given as follows:

$$\begin{cases} M_{\mathrm{s}}(:, k(i)) = M_{\mathrm{sp}}(:, i) & \forall i \in n \\ M_{\mathrm{s}}(k(i), :) = M_{\mathrm{sp}}(i, :) & \forall i \in n \end{cases} \tag{11}$$

where, M_{s} and M_{sp} are those images achieved after the processes of substitution and permutation, respectively. In the above equation, consists of two sub-equations first

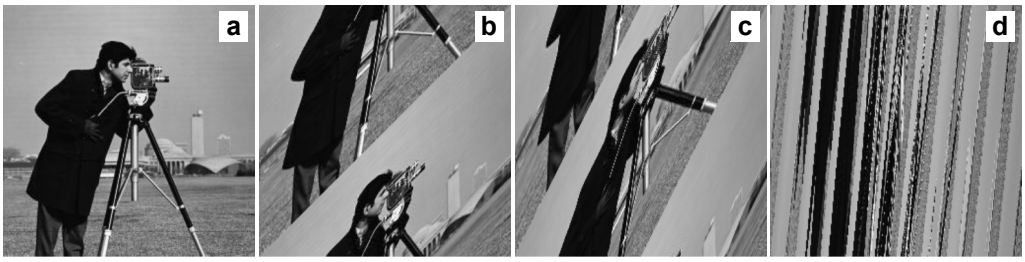

Fig. 3. Illustration of the proposed permutation effect on the image. Plaintext *Cameraman* image (**a**), image after one round of the proposed permutation (**b**), image after two rounds of the proposed permutation (**c**), and image after ten rounds of the proposed permutation (**d**).

sub-equation will swap the columns and the second sub-equation will swap the rows of the image, such as in the first step, the first column will be swap with the last column and after this step first row will be swap with last row and then second column with second last column and second row with second last row and so on. Figure 3 illustrates the results of permutation applied on a *Cameraman* image. To get back to the original *Cameraman* from the permuted image, the inverse should be applied.

4. Simulation results and analyses

The proposed algorithm is applied to a *Cameraman* image having 256 rows and 256 columns. The initial values of chaotic sequence are taken as $x_0 = 0.34243$ and $n = 3$. There are 256 S-boxes generated from different permutations of S_8. The simulation results of the proposed image encryption algorithm are shown in Fig. 4. Figure 4**a** shows the plain image of *Cameraman* and the encrypted *Cameraman* image resulted from applying proposed encryption algorithm is shown in Fig. 4**b**. The strength of proposed algorithm can be seen from the encrypted image which is completely random and not

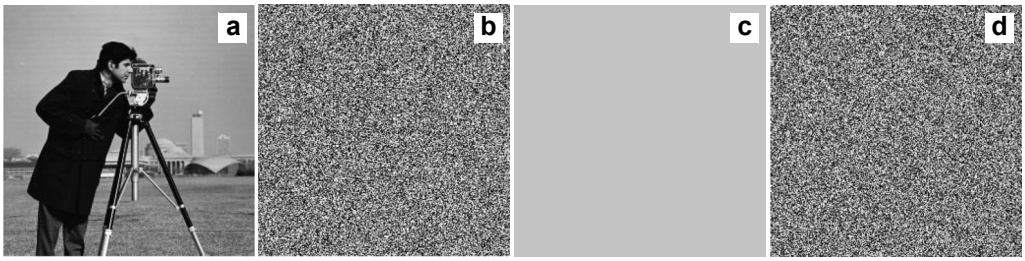

Fig. 4. Simulated results of the proposed algorithm. *Cameraman* image as plain image having 256 rows and 256 columns (**a**), encrypted image of *Cameraman* (**b**), one gray scale image as plain image having 256 rows and 256 columns (**c**), and encrypted image of one gray scale image (**d**).

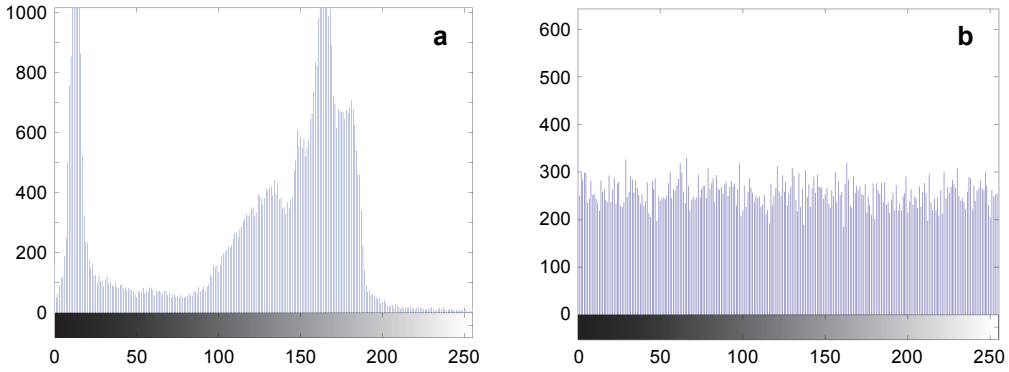

Fig. 5. Illustration of the histograms of plain (**a**) and cipher (**b**) *Cameraman* image.

giving any information regarding plain image. Moreover, to demonstrate the strength of proposed algorithm, we have taken a case for plain image having perfect correlation. It means that the pixel values for each image pixel are same, specifically 195. This image with perfect correlation is shown in Fig. 4**c** and the encrypted image resulted from applying proposed encryption algorithm is shown in Fig. 4**d**. Again, it can be visualized that the proposed algorithm has good cryptographic properties. The visual results can also be seen by plotting the histograms of plain images and cipher images. The histogram of a cipher image should be flat demonstrating that the distribution of image pixels is even throughout the image. Figure 5**a** shows the histogram of *Cameraman* image used as plain image and Fig. 5**b** shows the histogram of cipher image obtained after applying the proposed encryption algorithm demonstrating the strong results of the algorithm.

Moreover, to see the distribution of pixels in each frame of plain and encrypted color images, we have plotted the correlation as can be seen in Figs. 6 and 7. These figures show the distribution of horizontally adjacent pixels, and it can be seen that the performance of proposed image encryption is excellent.

The strength of the proposed algorithm is further verified by examining some of the statistical and security analysis. These analyses are then compared with the advanced

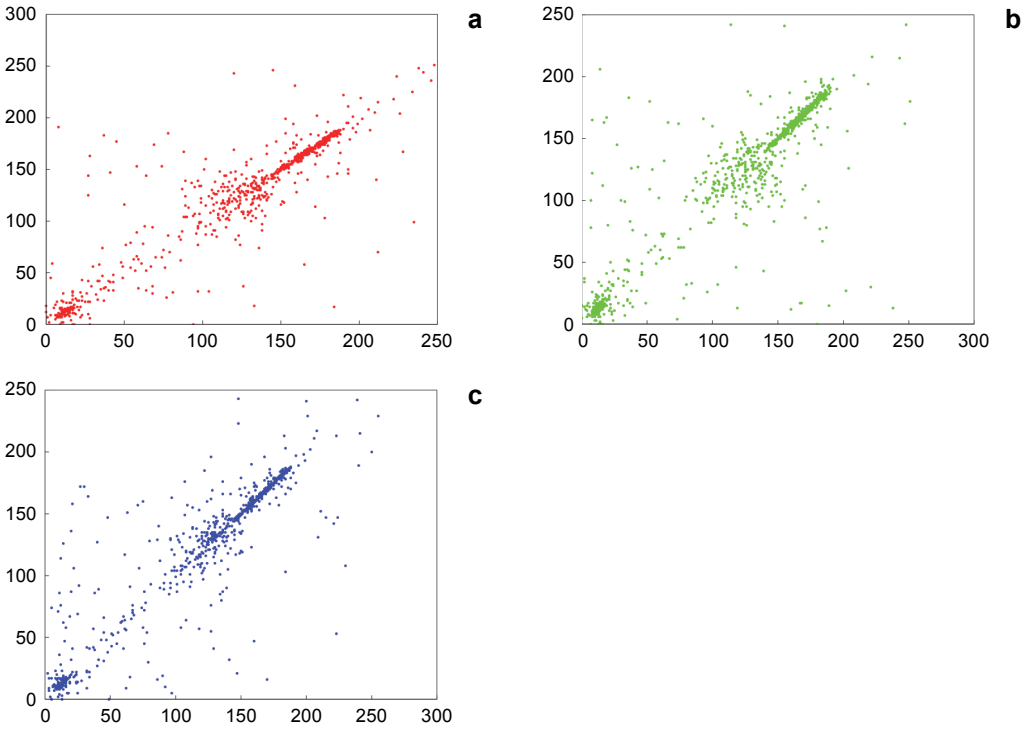

Fig. 6. The distribution of horizontally adjacent pixels of first layer (red), second layer (green) and third layer (blue) channel in the plain *Lena* image. To explain the figure according to RGB, figures are colored as red (**a**), green (**b**), and blue (**c**).

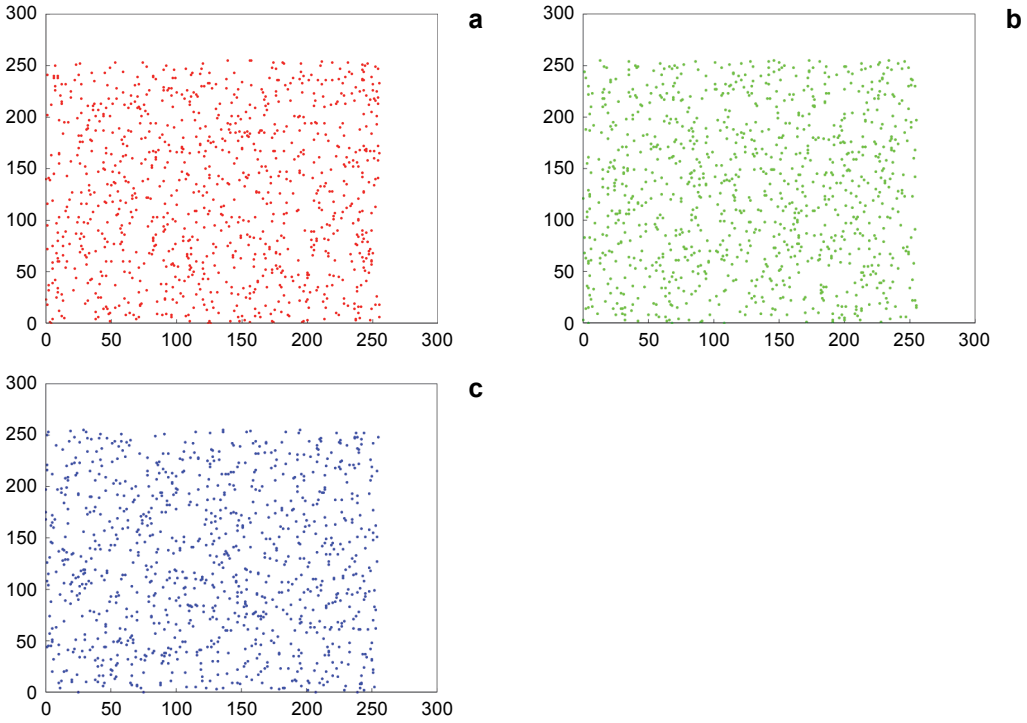

Fig. 7. The distribution of horizontally adjacent pixels of first layer (red), second layer (green) and third layer (blue) channel in the ciphered *Lena* image. To explain the figure according to RGB, figures are colored as red (**a**), green (**b**), and blue (**c**).

encryption standard (AES) that will demonstrate that the presented work is the optimum choice.

4.1. Statistical analysis

Statistical analysis of an image deal with the manipulation of quantitative values of image pixels. These analyses assist in examining the visual and quantitative qualities of plain and encrypted images. The analysis considered in this work are correlation, entropy, homogeneity, contrast, and energy of the plaintext and ciphertext images. These analyses are given as [20]:

$$\text{Correlation} = \sum_{i,j} \frac{(i-\mu i)(j-\mu j)p(i,j)}{\sigma_i \sigma_j} \tag{12}$$

$$\text{Entropy} = -\sum_{i,j} p(x_{i,j}) \log_2 p(x_{i,j}) \tag{13}$$

$$\text{Contrast} = \sum_{i,j} |i-j|^2 p(i,j) \tag{14}$$

T a b l e. Comparative statistical analysis of the images of *Cameraman* and *Baboon* resulted from AES and the proposed algorithm.

Analysis	Images	Correlation	Entropy	Homogeneity	Contrast	Energy
AES	*Cameraman*	0.014	7.9975	0.2641	7.4585	0.0081
	Baboon	0.0112	7.9973	0.2315	7.8651	0.0101
Proposed	*Cameraman*	0.0472	7.7351	0.3478	6.5018	0.0131
	Baboon	0.0315	7.8704	0.3342	6.8705	0.0117

$$\text{Homogeneity} = \sum_{i,j} \frac{p(i,j)}{1+|i-j|} \tag{15}$$

$$\text{Energy} = \sum_{i,j} p(i,j)^2 \tag{16}$$

where, the value of image pixel is denoted as $p(i,j)$, i denotes the row position and j denotes the column position for image pixel, the variance is denoted as μ, standard deviation is denoted as σ and the probability of image pixel is denoted as $p(x_{i,j})$.

The correlation analysis determines the similarity between two images having a range between –1 and 1 with 1 showing the perfect correlation. Entropy shows the randomness of the digital image having a range between 0 and 8 for a digital image having 256 gray scales. A greater value of entropy shows the greater amount of randomness in the digital image. The contrast analysis of the image enables the viewer to vividly identify the objects in the texture of an image. The contrast values ranges between 0 and $(\text{size(Image)} - 1)^2$. The contrast value of a constant image is 0. The greater value of the contrast shows greater variation in image pixels. The homogeneity analysis processes the closeness of the distribution in the gray level co-occurrence matrix (GLCM) to GLCM diagonal. The range of homogeneity and energy is between 0 and 1. These analyses are applied on the plain, and encrypted images resulted from the proposed and AES encryption algorithms. The comparative results are listed in the Table.

4.2. Key space and key sensitivity

The total number of private and secure keys that can be used in the encryption algorithm corresponds to key space. With the keys represented in binary bits k, the total keys are 10^k. AES uses a key of 128, 192 or 256 bits making a very large key space. A large key space assists in resisting all types of brute force attacks. In the proposed algorithm, the key is the combination of initial values of x and n in the Chebyshev chaotic map making the key space large enough that a modern computer will take more than 10^{20} years to check all combinations.

The exhaustiveness of key space will only be effective when the encryption results of each key is different and unique from the results of all the other keys. The encrypted data should not be successfully decrypted regardless of the fact that there is just a little contrast of even a single bit between the encryption and decryption keys. This effect

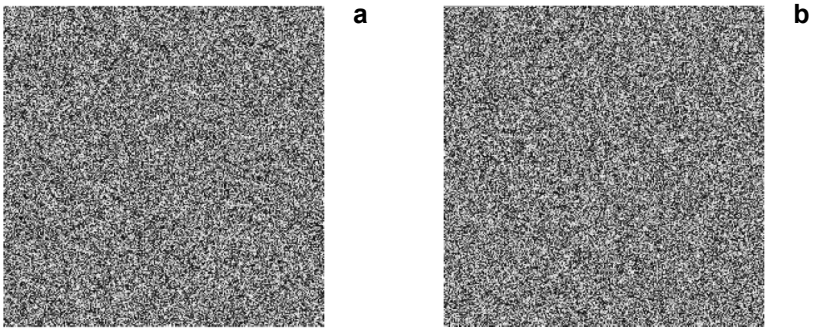

Fig. 8. Encrypted *Cameraman* image with the key having initial values of x_0 = 0.721546321451, p = 0.2 (**a**), and decrypted *Cameraman* image with the key having initial values of x_0 = 0.721546321452, p = 0.2 (only one bit change in x) (**b**).

is known as key sensitivity. To demonstrate the key sensitivity of presented work, the *Cameraman* image is encrypted with the key having initial values of x_0 = 0.721546321451, n = 0.2 and encrypted image is shown in Fig. 8**a**. The encrypted image is then decrypted with the key having values of x_0 = 0.721546321452, n = 0.2 (only one bit change in x) and decrypted image is shown in Fig. 8**b**. It can be seen that the decryption is not successfully done despite the difference of only one bit between the encryption and decryption keys.

4.3. Noise tolerant analysis

One of the requirements in a modern image encryption algorithm is the noise resistant feature. This feature is not required in a case where the plaintext is considered as text. In that scenario, if some of the bits are corrupted, then the whole text will be changed completely. However, this is contrast to the case of image, in which, if the values of image pixels are corrupted or changed by some margin, the overall visual appearance of those image pixels almost remain same. Therefore, the noise resistant feature can be used in the case of images and those images can tolerate noise to some level. To understand this, consider a scenario in which an image after encryption is transmitted on a wireless noisy transmission medium and the encrypted image is corrupted by some noise. At the receiver, after receiving the noisy encrypted image, the receiver has to decrypt this image. However, the traditional cryptosystems, like AES do not have the ability to decrypt these kinds of corrupted noisy encrypted images. To remove or correct the noises, receiver uses the forward error correction codes which generally adds to the computational complexity of overall system and may be not required in some low profile applications. In order to solve this, our proposed encryption algorithm has the capacity of successfully decrypting the corrupted noisy encrypted images. Although, after decrypting, there will be some noise in the decrypted image, however, as mentioned earlier, the images can tolerate the noise at certain level keeping the visual meaning intact. To demonstrate this effect, we have intentionally inserted some kinds of noises in the encrypted *Cameraman* images and then try to decrypt those images using the

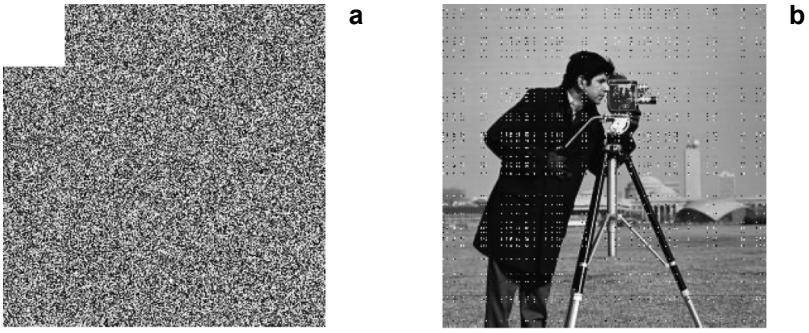

Fig. 9. Encrypted *Cameraman* image cropped with 50 × 50 image pixels (**a**) and successfully decrypted *Cameraman* image with some distortion (**b**).

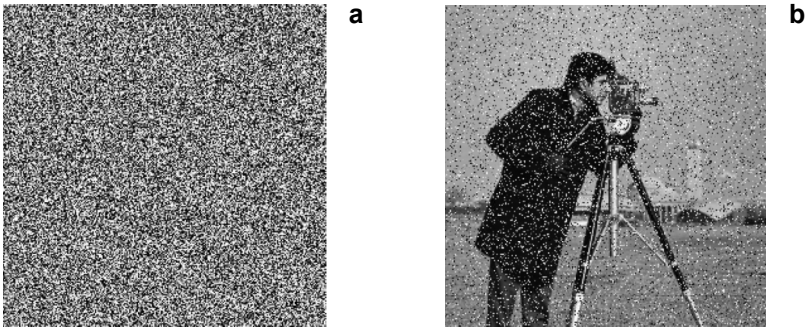

Fig. 10. Encrypted *Cameraman* image exposed to channel noise of salt and pepper having noise level of 0.2 density (**a**) and successfully decrypted *Cameraman* image with some distortion (**b**).

proposed decryption algorithm. Figure 9**a** shows the *Cameraman* encrypted image which is corrupted by the cropping effect. The cropping is done at the top left side of the encrypted image. This corrupted image is then fed into decryption algorithm and results are shown in the Fig. 9**b**. It can be seen that the decryption is possible with some noise but keeping the visual meaning of the image intact. The other example is shown in Fig. 10. Figure 10**a** demonstrates an image which is corrupted by the salt and pepper noise at a certain level. Again this corrupted image is fed into decryption algorithm and results are shown in the Fig. 10**b**. It can be seen that the decryption is possible with some noise but keeping the visual meaning of the image intact.

5. Conclusion

In this paper, an image encryption algorithm is proposed. The proposed algorithm is based on the network of the combination of confusion and diffusion. The confusion block is performed with the help of multiple substitution boxes. The choice of substi-

tution boxes for different data depends upon the values of chaotic maps which are generated using specific initial values and parameters. By using multiple substitution boxes instead of a single substitution box provides more randomness resulting in difficult cryptanalysis. The diffusion process is performed using permutation of a particular type.

Moreover, the cryptanalysis of the cipher demonstrated the robustness of proposed work. The proposed algorithm is applied on $N \times N$ images, N is the number of rows and N is the number of columns as well; though the original image could be of any magnitude, say $N \times M$ as the presented work is multidimensional size compatible. Furthermore, the proposed scheme has only two rounds of substitution and permutation having much low computational complexity than the traditional cryptosystems. It is concluded that with good cryptographic features, low processing complexity and resistant to the channel noise make it suitable for low profile mobile applications.

Acknowledgments – The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under grant number R.G.P-1/5/38.

References

[1] Nanrun Zhou, Haolin Li, Di Wang, Shumin Pan, Zhihong Zhou, *Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform*, Optics Communications **343**, 2015, pp. 10–21, DOI: 10.1016/j.optcom.2014.12.084.

[2] Lihua Gong, Xingbin Liu, Fen Zheng, Nanrun Zhou, *Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique*, Journal of Modern Optics **60**(13), 2013, pp. 1074–1082, DOI: 10.1080/09500340.2013.831139.

[3] Anees A., Khan W.A., Gondal M.A., Hussain I., *Application of mean of absolute deviation method for the selection of best nonlinear component based on video encryption*, Zeitschrift für Naturforschung A **68**(6–7), 2013, pp. 479–482, DOI: 10.5560/zna.2013-0022.

[4] Anees A., Ahmed Z., *A technique for designing substitution box based on Van der Pol oscillator*, Wireless Personal Communications **82**(3), 2015, pp. 1497–1503, DOI: 10.1007/s11277-015-2295-4.

[5] Lihua Gong, Chengzhi Deng, Shumin Pan, Nanrun Zhou, *Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform*, Optics and Laser Technology **103**, 2018, pp. 48–58, DOI: 10.1016/j.optlastec.2018.01.007.

[6] Jing Yu, Yuan Li, Xinwen Xie, Nanrun Zhou, Zhihong Zhou, *Image encryption algorithm by using the logistic map and discrete fractional angular transform*, Optica Applicata **47**(1), 2017, pp. 141–155, DOI: 10.5277/oa170113.

[7] Nan Run Zhou, Tian Xiang Hua, Li Hua Gong, Dong Ju Pei, Qing Hong Liao, *Quantum image encryption based on generalized Arnold transform and double random-phase encoding*, Quantum Information Processing **14**(4), 2015, pp. 1193–1213, DOI: 10.1007/s11128-015-0926-z.

[8] Huaqian Yang, Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang, Pengcheng Wei, *A fast image encryption and authentication scheme based on chaotic maps*, Communications in Nonlinear Science and Numerical Simulation **15**(11), 2010, pp. 3507–3517, DOI: 10.1016/j.cnsns.2010.01.004.

[9] Degang Yang, Xiaofeng Liao, Yong Wang, Huaqian Yang, Pengcheng Wei, *A novel chaotic block cryptosystem based on iterating map with output-feedback*, Chaos, Solitons and Fractals **41**(1), 2009, pp. 505–510, DOI: 10.1016/j.chaos.2008.02.017.

[10] AMIGÓ J. M., KOCAREV L., SZCZEPANSKI J., *Theory and practice of chaotic cryptography*, Physics Letters A **366**(3), 2007, pp. 211–216, DOI: 10.1016/j.physleta.2007.02.021.

[11] ANEES A., GONDAL M.A., *Construction of nonlinear component for block cipher based on one-dimensional chaotic map*, 3D Research **6**(2), 2015, article ID 17, DOI: 10.1007/s13319-015-0049-4.

[12] ANEES A., SIDDIQUI A.M., *A technique for digital watermarking in combined spatial and transform domains using chaotic maps*, IEEE 2nd National Conference on Information Assurance (NCIA), 2013, pp. 119–124, DOI: 10.1109/NCIA.2013.6725335.

[13] JAKIMOSKI G., KOCAREV L., *Chaos and cryptography: block encryption ciphers based on chaotic maps*, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications **48**(2), 2001, pp. 163–169, DOI: 10.1109/81.904880.

[14] OTT E., *Chaos in Dynamical Systems*, 2nd Ed., Cambridge University Press, 2001.

[15] ALVAREZ G., LI S., *Some basic cryptographic requirements for chaos-based cryptosystems*, International Journal of Bifurcation and Chaos **16**(8), 2006, pp. 2129–2151, DOI: 10.1142/S0218127-4060 15970.

[16] CICEK S., UYAROGLU Y., PEHLIVAN I., *Simulation and circuit implementation of sprott case h chaotic system and its synchronization application for secure communication systems*, Journal of Circuits, Systems and Computers **22**(4), 2013, article ID 1350022, DOI: 10.1142/S0218126613500229.

[17] AHMED F., ANEES A., ABBAS V.U., SIYAL M.Y., *A noisy channel tolerant image encryption scheme*, Wireless Personal Communications **77**(4), 2014, pp. 2771–2791, DOI: 10.1007/s11277-014-1667-5.

[18] AHMED F., ANEES A., *Hash-based authentication of digital images in noisy channels*, [In] *Robust Image Authentication in the Presence of Noise*, [Ed.] N. Zivic, Springer International Publishing, 2015, pp. 1–42, DOI: 10.1007/978-3-319-13156-6.

[19] ANEES A., SIDDIQUI A. M., AHMED J., HUSSAIN I., *A technique for digital steganography using chaotic maps*, Nonlinear Dynamics **75**(4), 2014, pp. 807–816, DOI: 10.1007/s11071-013-1105-3.

[20] ANEES A., SIDDIQUI A. M., AHMED F., *Chaotic substitution for highly autocorrelated data in encryption algorithm*, Communications in Nonlinear Science and Numerical Simulation **19**(9), 2014, pp. 3106 –3118, DOI: 10.1016/j.cnsns.2014.02.011.

[21] PEHLIVAN I., ZHOUCHAO WEI, *Analysis, nonlinear control, and chaos generator circuit of another strange chaotic system*, Turkish Journal of Electrical Engineering and Computer Sciences **20**, 2012, pp. 1229–1239, DOI: 10.3906/elk-1103-14.

[22] PARESCHI F., SETTI G., ROVATTI R., *Implementation and testing of high-speed CMOS true random number generators based on chaotic systems*, IEEE Transactions on Circuits and Systems I: Regular Papers **57**(12), 2010, pp. 3124–3137, DOI: 10.1109/TCSI.2010.2052515.

[23] OZKAYNAK F., *Cryptographically secure random number generator with chaotic additional input*, Nonlinear Dynamics **78**(3), 2014, pp. 2015–2020, DOI: 10.1007/s11071-014-1591-y.

[24] HUSSAIN I., SHAH T., MAHMOOD H., *A new algorithm to construct secure keys for AES*, International Journal of Contemporary Mathematical Sciences **5**(26), 2010, pp. 1263–1270.

Received March 2, 2018
in revised form April 14, 2019