Image Encryption Using a Novel Chaotic Map

Saeed Norouzi Davoodkhani, Leili Farzinvash, and Leyli Mohammad Khanli

***Abstract*—A new image encryption algorithm is proposed, in which a novel chaotic map is introduced to generate the random sequence. The mentioned sequence is employed to produce gray level values. The original image is encrypted by applying the XOR operator to every pixel using the mentioned values. Our chaotic map provides a large degree of randomization compared to existing approaches and therefore, the correlation between adjacent pixels in the encrypted image is reduced substantially. The security analysis demonstrates that the new algorithm is highly secure. As it is shown in the experimental results, our algorithm improves entropy, key sensitivity, and correlation. Specifically, the amounts of entropy and correlation measures are very close to the optimal values. It is also very robust against the noise. The PSNR of decrypted images are degraded slightly with the increasing noise strength. Additionally, the suggested approach leads to smoother histograms in comparison to the previous algorithms.**

***Index Terms*— Image Encryption, Chaotic Map, Noise**

I. Introduction

THE demand for digital image applications has been increased rapidly in recent years. Along with the growing need for image transmission, preserving its confidentiality has become an important research issue [1-12]. Most of the traditional encryption algorithms are not appropriate for multimedia applications. These algorithms cannot deal with unique features of images, such as high redundancy and correlation among adjacent pixels. Therefore, there is a need to develop novel encryption approaches which take into account the properties of digital images [1-2].

Recently, a large number of new image encryption algorithms have been proposed [6-12]. Many researchers have adopted chaotic map to develop effective methods [3-16, 17-28]. In these algorithms, the chaotic system is employed to generate pseudo-random sequences, which will be utilized in encryption process. The advantages of chaotic maps, including sensitivity to the value of secret key and other initial conditions, mixing property, aperiodicity, and pseudo-randomness, make them suitable for designing robust encryption algorithms. In this paper, we have proposed a new image encryption algorithm. In the suggested scheme, a novel chaotic map is developed to generate a pseudo-random sequence, which is utilized to produce gray level values. The encrypted image is obtained by applying the XOR operator to the original image using these values. The main advantages of our algorithm are listed in the following:

- In this work we have designed a new chaotic map. As it is shown in Section 3, it yields to more randomness compared to previous research. Our method improves the variance of generated sequence by 100%.
- Due to the high randomness of the pseudo-random sequence, gray-level values will have a large degree of randomization. Using these pseudo-random values in generating the encrypted image diminishes the correlation between the adjacent pixels.
- Each pixel of the encrypted image is generated by applying XOR operation to the corresponded pixel in the plain image and a pseudo-random number. Therefore, the corruption of each pixel in the encrypted image only affects the corresponded pixel in the plain image. As a result, the proposed algorithm is highly robust against noisy transmission channels.

The rest of the paper is organized as follows: Section 2 reviews the related work addressing image encryption algorithms. In Section 3, we present our algorithm. This section includes the analysis of the proposed chaotic map. The simulation results are reported in Section 4. Finally, we conclude our paper in Section 5.

II. Related Work

Most of the classical encryption algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), are not proper for multimedia applications. Therefore, other encryption techniques are developed. One of the most common solutions is to employ chaotic maps. Recently, other approaches, such as DNA encoding is used for image encryption [1-6]. In this approach, the encrypted image is obtained by the substitution of plain image with DNA sequences.

Jain and Raipal have proposed a new image encryption algorithm based on DNA encoding [8]. In this work, each pixel is transformed to a DNA sequence. In the proposed algorithm in [9], every pixel is substituted with another pixel which is chosen by the Logistic map. In the following, the pixels are replaced with the corresponded DNA sequences.

The combination of Logistic map and DNS encoding for image encryption is also used in [10]. The authors have utilized Logistic map for replacing bits of pixels with DNA sequences. This sequence will be substituted with other sequences to increase security. DNA encoding is time-consuming to some

Manuscript received May 19, 2016; accepted July 25, 2016
The authars are with the Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, 29 Bahman Blvd, Iran.

extent. Therefore, this approach is not so appropriate for multimedia applications due to their sensitivity to delay and high data rate.

The algorithm in [11] has used an s-box, which is based on Logistic map. Here, each pixel is divided into two parts. Then, the s-box is used for replacing these parts with pseudo-random numbers. In the following, the obtained numbers are considered as the coordinates of the pixel that will be substituted with the mentioned pixel.

The Logistic map has been used in some other algorithms such as [14]. The algorithms have encrypted the image in multiple rounds. The key of each round is generated using the round-keys of previous rounds. In the proposed algorithm, firstly the plain image is processed. Then, the XOR operation is applied to each pixel and a pseudo-random number that is generated by Logistic map. In [18], the authors have discussed the disadvantages of substation techniques. To overcome these shortcomings, they have employed a 3-dimentional matrix for in image encryption.

The main disadvantage of algorithms in [9-11] is that in the generated sequences by Logistic map, some of the successive numbers are very close. This leads to increasing the correlation between adjacent pixels of the encrypted image.

III. The Proposed Encryption Algorithm

In this section we explain our proposed method. The steps of our scheme are as follows:

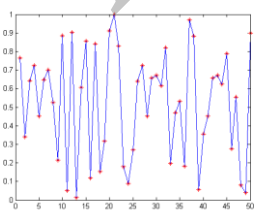
Step 1: A pseudo-random sequence is generated by means of the suggested chaotic map. The procedure is expounded in Section 3.1.

Step 2: The gray-level values are produced using (1). In this equation, g_k stands for the k[th] gray-level value, and x_k shows the k[th] random number. As the pixels are represented by one byte, the produced gray-level values should be in the range [0,255]. Therefore, x_k, which is between 0 and 1, should be scaled up to fit in this range.

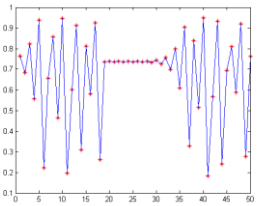
$$g_k = ceil\left(255.x_k\right) \tag{1}$$

Next, x_k is modified as it is shown in the following:

$$x_k = x_k\left(\frac{g_k}{256}\right) \tag{2}$$



a) The proposed approach



b) The Logistic map

Fig. 1: The distribution of generated pseudo-number numbers

Each pixel value of the original image, which is denoted by p_k, will be enciphered as follows:

$$e_k = p_k \oplus g_k \tag{3}$$

where $\oplus$ denotes bitwise XOR operation, and the k[th] pixel of encrypted image is presented by e_k.

The disadvantage of this approach is that it is vulnerable to key reuse attack. Suppose we have two plain images P_1 and P_2, and the same secret key is used for encrypting them. The k[th] pixel of encrypted images will be computed as follows:

$$e_{1k} = p_{1k} \oplus g_k \tag{4}$$

$$e_{2k} = p_{2k} \oplus g_k \tag{5}$$

where p_{1k}, e_{1k}, p_{2k}, and e_{2k}, stands for the k[th] pixel of P_1, encrypted P_1, P_2, and encrypted P_2, respectively.

The random part of the encrypted images can be omitted by simply applying XOR operation to (4) and (5).

The common approach to mitigate this attack is to append a random sequence, namely Initial Vector, to the secret key. In this way, the keys of images will differ.

In the rest of this section, the suggested chaotic map is described.

A. The Proposed Chaotic Map

Recently, many encryption algorithms based on chaotic systems have been developed [7-12]. These systems are employed due to their desirable properties including sensitivity to initial condition, ergodicity, and pseudo randomness. In this work, we have designed a new chaotic map, which is defined in the following:

$$x_{k+1} = \mathrm{mod}\left(\frac{r}{4}\frac{\cot\left(x_k\right)}{\tan\left(2/\pi\right)},1\right) \tag{6}$$

where r is a constant value in the range [3.6, 4). The initial pseudo-random number, x_0, is generated based on the secret key.

Many of the previous works have used the Logistic map for image encryption [6-12], which is defined as follows:

$$x_{k+1} = r\,x_k\left(1-x_k\right) \tag{7}$$

As it is shown in [11], Logistic map behaves like a chaotic system if parameter r is in the range [3.6, 4).

TABLE I
VARIANCES OF PSEUDO-RANDOM SEQUENCES

Random-generator scheme	The amount of variance
The proposed algorithm	**0.1028**
The Logistic map	0.05

To demonstrate the superiority of the proposed map over this method, we have studied the randomness of their generated sequences. The length of these sequences is set to 50. The values of r and x_0 are set to 3.8 and 0.7647, respectively. Fig. 1 displays the generated numbers by our scheme and Logistic map. It is obvious from this figure that our approach leads to more randomness.

We have also measure the variances of generated sequences to quantify our results, which are reported in Table 1. The more is the amount of variance, the more is the randomness of generated sequence. As it is show in this table, our method increases the variance by 100%.

IV. Experimental results

A practical encryption algorithm should resist against various attacks. To validate the effectiveness of the proposed algorithm, we perform some security analysis including histogram, correlation, entropy, and key sensitivity. We compare our method with the algorithms in [8-9, 11]. The algorithms are implemented by Matlab [29]. The gray image "Lena" with the size of 256 × 256 is used for measuring the performance of the proposed algorithm.

B. Histogram of Cipher Image

The histogram displays the number of pixels at each gray level. Fig. 2 shows the histograms of the plain and the encrypted images of Lena. From this figure we can see that the distribution of the generated histogram by our algorithm is close to the uniform distribution. It is difficult for the attacker to obtain statistical information from this histogram. Therefore, we can conclude that the algorithm is robust against statistical attacks.

C. Entropy Analysis

The entropy of a system presents the amount of its randomness. This concept was introduced by Claude E. Shannon in 1948 [16]. The entropy $H(m)$ of source m is defined as follows:

$$H(m) = -\sum_{i=1}^{n} p(m_i)\log_2\left(p(m_i)\right) \tag{8}$$

where p(.) presents the probability mass function. The entropy of an image is calculated on its histogram counts.

The entropies of original and encrypted Lena are gathered in Table 2. From this table it is obvious that our algorithm improves the entropy of the encrypted image.

D. Correlation Analysis

The other important criterion in evaluating an image encryption algorithm is correlation. The correlation of an image is given as:

$$Corr = \frac{\mathrm{cov}(x,y)}{\sigma_x\sigma_y} = \frac{E\left[\left(X - E[x]\right)\left(Y - E[y]\right)\right]}{\sigma_x\sigma_y} \tag{9}$$

where x and y are two adjacent pixels. Moreover, μ and σ denotes the expected value and standard deviation, respectively.

TABLE II
COMPARISON OF ENTROPIES

Encryption scheme	Entropy
The plain image	7.5889
The proposed algorithm	**7.9974**
Ref. [8]	7.994
Ref. [9]	7.987
Ref. [11]	7.8523

TABLE III
COMPARISON OF CORRELATIONS

Encryption scheme	Correlation
The plain image	0.9575
The proposed algorithm	**-0.000385**
Ref. [8]	0.0032
Ref. [9]	0.0021
Ref. [11]	0.0201

Table 3 shows the resultant correlations of the proposed algorithm and Refs. [8-9, 11]. From these results, it can be seen that the reported correlation by our algorithm is close to zero. This means that it approximately eliminates the correlation between adjacent pixels in the image.

E. Key Sensitivity Analysis

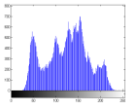
One important aspect of an effective image encryption algorithm is its sensitivity to small modifications in the secret key. This means that a slight change in the key, such as modifying one of its bits, should lead to worthy change in the cipher image. To study the impact of a one-bit change of the key on the whole encrypted image, we have employed two measures: the Number of Pixels Change Rate (NPCR) and the Unified Average Change Intensity (UACI). These measures calculate the number of different pixels of two images, and the difference of two images, respectively. Given two images $x = \{x_1, x_2, \cdots, x_n\}$ and $y = \{y_1, y_2, \cdots, y_n\}$, these criteria are defined as follows:

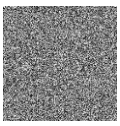
$$NPCR = \frac{1}{n}\sum_{i=1}^{n} D(x_i, y_i) \times 100\% \tag{10}$$

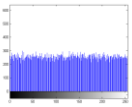
$$UACI = \frac{1}{n}\sum_{i=1}^{n} \frac{|x_i - y_i|}{255} \tag{11}$$

In our experiments, Lena has been encrypted using two different keys with only one-bit difference. The obtained NPCR and UACI of encrypted images are tabulated in Table 4. According to the results, we can conclude our algorithm is more sensitive to the modifications of the secret key in compare to existing approaches

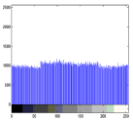

a) Plain Lena

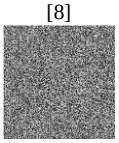

b) Histogram of plain Lena

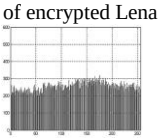

c) Encrypted Lena by the proposed algorithm

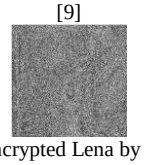

d) Histogram of encrypted Lena by the proposed algorithm


e) Encrypted Lena by Ref. [8]


f) Histogram of encrypted Lena by Ref. [8]


i) Encrypted Lena by Ref. [9]


j) Histogram of encrypted Lena by Ref. [9]


g) Encrypted Lena by Ref. [11]

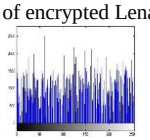

h) Histogram of encrypted Lena by Ref. [11]

Fig. 2. The histograms of plain and encrypted Lena

F. he Effect of Noise

The presence of noise in the transmission stage can degrade the quality of the decrypted image. In this section, the impact of noise on the performance of the proposed algorithm has been studied. Suppose that the Gaussian white noise with zero-mean and unit standard deviation is added to the sent encrypted image. The received encrypted image will be computed as:

$$E_r = E_s + kG \qquad (12)$$

where E_s and E_r presents the sent and received encrypted image, and G stands for Gaussian noise.

Fig. 3 presents the decrypted image with different values of k. As it is shown in this figure, the quality of decrypted image is acceptable for various amounts of the noise level. This is due o that, each pixel in the decrypted pixel is only related to the corresponded pixel in the encrypted image. This leads to high robustness of our algorithm against noise.

The PSNR of decrypted Lena with different values of k is gathered in Table 5. From this table we can see that by increasing the noise strength, the PSNR of decrypted Lena is reduced slightly. This result indicates the robustness of the proposed algorithm against noise.

TABLE IV
COMPARISON OF KEY SENSITIVITY OF DIFFERENT ALGORITHMS

Encryption scheme	NPCR	UACI
The proposed algorithm	**99.621**	**33.37**
Ref. [8]	99.62	33.06
Ref. [9]	99.5376	32.57
Ref. [11]	-	-

TABLE V
: PSNR OF DECRYPTED LENA

k	PSNR
0.5	29.39
1	28.82
1.5	28.67
2	28.51
3	28.39
4	28.25

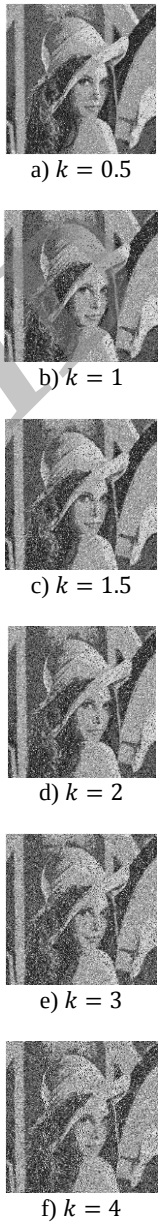

a) $k = 0.5$
b) $k = 1$
c) $k = 1.5$
d) $k = 2$
e) $k = 3$
f) $k = 4$

Fig. 3: Decrypted Lena with different noise strengths

V. CONCLUSION

The importance of secure image transmission necessitates designing efficient image encryption algorithms. In this paper

we have presented a novel image encryption approach, which employs a new chaotic map for generating random sequences. Each pixel in the encrypted image is produced by applying XOR operation to two pixels: the corresponded pixel in the original image, and a pseudo-random number that is generated by the chaotic map. The security analysis demonstrates that our algorithm can provide more security in compare to the existing approaches. Therefore, it is a practical algorithm for image encryption.

REFERENCES

[1] V. Rijmen and J. Daemen, "Advanced encryption standard" Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology, 2001, pp. 19-22.

[2] D. Coppersmith, C. Holloway, S. M. Matyas, and N. Zunic, "The data encryption standard" Information Security Technical Report, 2(2), 1997, pp. 22-24.

[3] W. S. Yap, R. C. W. Phan, W. C. Yau, and S. H. Heng, "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map" Nonlinear Dynamics, 80(3), 2015, pp. 1483-1491.

[4] A. Abirami and R. Amutha, "Image encryption based on DNA sequence coding and Logistic map" Advances in Natural and Applied Sciences, 9(9 SE), 2015, pp.55-63.

[5] B. Wang, Y. Xie, C. Zhou, S. Zhou, and X. Zheng, "Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps" Optik-International Journal for Light and Electron Optics, 127(7), 2016, pp. 3541-3545.

[6] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique" Optics and Lasers in Engineering, 66, 2015, pp. 10-18.

[7] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2" Nonlinear Dynamics, 83(3), 2016, pp. 1123-1136.

[8] A. Jain and N. Rajpal, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps" Multimedia Tools and Applications, DOI 10.1007/s11042-015-2515-7.

[9] H. Liu and X. Wang, "Image encryption using DNA complementary rule and chaotic maps" Applied Soft Computing, 12(5), 2012, pp. 1457-1466.

[10] S. Chakraborty, A. Seal, M. Roy, and K. Mali, "A novel lossless image encryption method using DNA substitution and chaotic Logistic map" International Journal of Security and Its Applications, 10(2), 2016, pp. 205-216.

[11] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly auto-correlated data in encryption algorithm" Communications in Nonlinear Science and Numerical Simulation, 19(9), 2014, pp. 3106-3118.

[12] A. Kulsoom, D. Xiao, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules" Multimedia Tools and Applications, 75(1), 2016, pp. 1-23.

[13] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos" Signal Processing, 109, 2015, pp. 119-131.

[14] M. Rani and S. Kumar, "A novel and efficient approach to encrypt images using chaotic Logistic map and tream cipher" In Proceedings of IEEE International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 1442-1447.

[15] C. Savage, "A survey of combinatorial Gray codes" SIAM Review, 39(4), 1997, pp. 605–629.

[16] C. Shannon, "Communication Theory of Secrecy Systems" Bell System Technical Journal, 28(4), 1949, pp. 656-715.

[17] H. S. Kwok and W. K. S. Tang, "A Fast Image Encryption System Based on Chaotic Maps with Finite Precision Representation" Chaos, Solitons and Fractals, 32, 2007, p. 1518-1529.

[18] W. Zhang, H. Yu, Y. L. Zhao, and Z. L. Zhu, "Image encryption based on three-dimensional bit matrix permutation" Signal Processing, 118, 2016, pp. 36-50.

[19] X. Zhang, Z. Zhao, and J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer" Signal Processing: Image Communication, 29(8), 2014, pp. 902-913.

[20] Z. Tang, X. Zhang, and W. Lan, "Efficient image encryption with block shuffling and chaotic map", Multimedia Tools and Applications, 74(15), 2015, pp. 5429-5448.

[21] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, "Image encryption using the two-dimensional Logistic chaotic map" Journal of Electronic Imaging, 21(1), 2012, DOI doi:10.1117/1.JEI.21.1.013014.

[22] H. Cheng, C. Huang, Q. Ding, and S. C. Chu, "An efficient image encryption scheme based on ZUC stream cipher and chaotic logistic map" In Proceedings of the First Euro-China Conference on Intelligent Data Analysis and Applications, Intelligent Data analysis and its Applications, 2014, pp. 301-310.

[23] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata" Optics and Lasers in Engineering, 51(6), 2013, pp. 665-673.

[24] X. Wang and K. Guo, "A new image alternate encryption algorithm based on chaotic map" Nonlinear Dynamics, 76(4), 2014, pp. 1943-1950.

[25] X. J. Tong, Z. Wang, M. Zhang, and Y. Liu, "A new algorithm of the combination of image compression and encryption technology based on cross chaotic map" Nonlinear Dynamics, 72(1-2), 2013, pp. 229-241.

[26] Q. Zhang, L. Guo, and X. Wei, "A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system" Optik-International Journal for Light and Electron Optics, 124(18), 2013, pp. 3596-3600.

[27] I. Hussain and M. A. Gondal, "An extended image encryption using chaotic coupled map and S-box transformation" Nonlinear Dynamics, 76(2), 2014, pp. 1355-1363.

[28] Z. Yisheng, L. Shuyun, and L. Dequn, "A new chaotic algorithm for image encryption" Chaos Solitons & Fractals, 29(2), 2006, pp. 393-399.

[29] www.mathworks.com