International Journal of Computer Networks and Communications Security

VOL. 5, NO. 3, MARCH 2017, 60–65
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Novel Image Encryption Algorithm Based on Chaotic Map and Encoding

SAEED NOROUZI DAVOODKHANI[1] and LEILI FARZINVASH[2]

[1, 2] Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

[1]*s.norouzi93@ms.tabrizu.ac.ir*, [2]*l.farzinvash@tabrizu.ac.ir*

ABSTRACT

In this paper we have designed a new image encryption algorithm, which includes a novel chaotic map and coding scheme. In the suggested approach, the coding algorithm is based on Gray code. Each pixel in the encrypted image is generated by applying XOR operation to two items: the first item is the coded form of the corresponded pixel in the original image. The second one is a pixel in the original image which is selected by the chaotic map. Experimental results shows that our chaotic map leads more randomness in comparison with the existing approaches. To evaluate the effectiveness of our algorithm, we have performed some security analysis. The results have demonstrated that the proposed approach improves entropy, correlation, and key sensitivity. Moreover, it generates smoother histograms in comparison with the existing algorithms.

Keywords: *Image Encryption, Chaotic Map, Coding, Gray Code, Secure Image Transmission*.

1 INTRODUCTION

With the rapid growth of the digital image applications, designing effective encryption algorithms for secure image transmission becomes a critical demand. The traditional encryption algorithms, such as DES [1] and AES [2] cannot be applied to images due to their distinctive features, such as high correlation between the adjacent pixels. Considering the inefficiency of the traditional schemes, many image encryption algorithms have been developed recently. These algorithms have typically employed chaotic maps to generate pseudo-random sequences, which is utilized to confuse the pixels [3-18]. The popularity of these maps is due to their desirable features, including high sensitivity to initial conditions and small variations in the secret key, aperiodicity, and pseudo-randomness.

One of the widely-used chaotic maps is the Logistic map. As it is shown in [3], this map becomes chaotic under certain conditions. The disadvantage of this map is that in some situations, the adjacent numbers are close to each other in the generated sequences. This problem degrades the confusing property, and as a consequence, the correlation of the encrypted image increases. To tackle this problem, in this paper we have designed a new map, which provides more randomness in comparison with the Logistic map. As it is shown in Section 3, our proposed map improves the randomness of the sequences by 70%. As a result, the correlation of the encrypted image degrades through utilizing the suggested map.

The other contribution of our work is the design of a novel coding scheme, which is based on Gray code [19]. Our proposed approach changes the structure of the pixels and therefore, it enhances the quality of encrypted images. To encipher each pixel of the plain image, the XOR operation is applied to its coded form using the chosen pixel by the chaotic map.

The rest of this paper is organized as follows: Section 2 discusses the related work to our research. We have expounded our work in Section 3, where the suggested chaotic map and coding approach are introduced. The proposed algorithm is evaluated in Section 4 through extensive simulations. Finally, in Section 5 we have concluded the paper.

2 RELATED WORK

The traditional encryption algorithms have followed blocking approach, in which the plain data is divided into fixed size partitions, and each partition is considered separately. The main challenge of this scheme is that, breaking of an encrypted block leads the disclosure of all the data. Considering the shortcomings of the blocking approach, the streaming algorithms, in which the

whole data is enciphered together, have drawn attention. These algorithms have employed chaotic maps to generate pseudo random sequences. The streaming approach is also well suited for image encryption, and has been extensively considered to provide effective solutions [3-18]. Murillo-Escobar and et al. [4] have used Logistic map to generate pseudo random sequences. Moreover, a s-box is employed to perform substitution process. The given algorithm in [5] has also utilized Logistic map and s-boxes for image encryption. In this work, the image is encrypted in multiple rounds. The key of each round is generated considering the outcome of the previous round.

In the suggested algorithm in [6], each pixel is substituted for another pixel, which is determined as follows. First, the original pixel is divided into two parts. In the following, a s-box, which is based on Logistic map, is utilized to generate a random number per half. These numbers are employed as the coordinates of the latter pixel. In the proposed algorithm by Zheng and et al. [7], a circular s-box, which contains a header, is employed. Each pixel is substituted by an element of the s-box, considering the pixel value and the element of the s-box which is pointed by the header. In the following, each pixel is enciphered using the outcome of the s-box and previous encrypted pixel. Ref. [8] has investigated the disadvantages of substitution-based encryption algorithms. Then, it has proposed an algorithm which utilized a three-dimensional matrix for permutation.

Recently, other techniques, such as DNA encoding, have been employed to encipher images. In this approach, the pixels of plain image are substituted for DNA sequences. Jain and Rajpal [11] have proposed an image encryption algorithm based on DNA encoding, in which the corresponding DNA sequence to each pixel is determined according to its binary presentation. In [12], Liu and Wang have merged DNA encoding and Logistic map. In this work, each pixel of the plain image is substituted for another pixel, where the coordinates of the latter is determined using the generated numbers by the chaotic map. Next, the pixels are substituted for the equivalent DNA sequences. The proposed algorithms in [15-16] have also combined DNA encoding and chaotic map. The main disadvantage of DNA encoding is its high time complexity. Moreover, in some DNA-based algorithms the data is enlarged. Therefore, this approach is not appropriate to encrypt images.

One critical issue in the considered works is the low degree of randomization of the generated sequences by the Logistic map. In some situations, the successive numbers in these sequences are very close to each other, which increases the correlation of the encrypted image.

3 THE PROPOSED ALGORITHM

In this section we have explained the proposed algorithm for image encryption. The steps of enciphering pixel $p_{i,j}$ are given in the following:

1. In the first step, a random pixel of the image is chosen. The coordinates of this pixel is determined using the generated numbers by the proposed chaotic map. Since these numbers are in the range of [0,1], they should be scaled up to present the height and width of the pixel. Therefore, the coordinates of $p_{l,k}$ is calculated as follows:

$$\begin{aligned} k &= ceil\left(x_n H\right) \\ l &= ceil\left(x_{n+1} W\right) \end{aligned} \quad (1)$$

where x_n presents the nth random number, and H and W stand for the number of rows and columns of the image.

2. Next, the coding algorithm is applied to $p_{i,j}$. The coded form of this pixel is named as $c_{i,j}$. To generate the encrypted pixel, namely $e_{i,j}$, the XOR operator is applied to the outcomes of the previous steps. So we have:

$$e_{i,j} = p_{k,l} \oplus c_{i,j} \quad (2)$$

3.1 The Chaotic Map

Recently, chaotic maps have drawn significant attention in image encryption algorithms. These maps are so popular due to their unique features, such as pseudo randomness and ergodicity. The most commonly used variation of chaotic map is the Logistic map, which is defined as follows:

$$x_{n+1} = r\, x_n \left(1 - x_n\right) \quad (3)$$

It has been proved in [3] that the Logistic map displays chaotic behavior, if r is chosen within the range of [3.6, 4).

The other method to generate random sequences is the Charkovsky map [20], which is presented in the following:

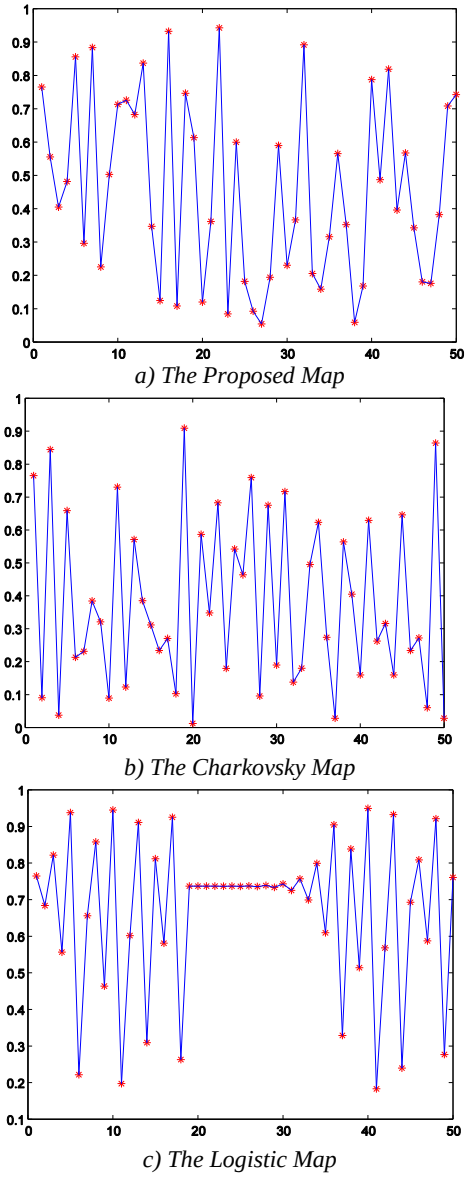
$$x_{n+1} = \mathrm{mod}\left(\cot^2\left(x_n\right), 1\right) \quad (4)$$

As it is shown in the experiments, this map outperforms the Logistic map. In this work, we have designed a novel chaotic map based on the Charkovsky map. Our proposed map is formulated as:

$$x_{n+1} = \mathrm{mod}\left(\frac{\pi}{2}\frac{r}{4}\cot\left(x_n\right), 1\right) \quad (5)$$

where r is a constant parameter in the range of [3.6,4).

To evaluate the effectiveness of the proposed map, we have generated a sequence of 50 random numbers by each of the maps, and compare the randomness of these sequences. In these set of experiments, r and x_0 are set to 3.8 and 0.7674, respectively. The distribution of the sequences is depicted in Figure 1. From this figure we can conclude that our map provides more randomness.



a) The Proposed Map

b) The Charkovsky Map

c) The Logistic Map

Fig 1. The Distribution of the Generated Sequences

We have also calculated the variances of the sequences to quantify the results. The variance of a sequence presents the degree of its spreading. The results are gathered in Table 1. From these results we can see that our map improves the variance by 0.0333 and 0.005 in comparison with the Logistic map and Charkovsky map, respectively.

Table 1. The Variances of the Generated Sequences

The Random Generator Scheme	Variance
The proposed algorithm	0.080
The Charkovsky map	0.075
The Logistic map	0.050

3.2 The Coding Algorithm

In the proposed algorithm, we have coded the pixels to confuse them. Our scheme is based on Gray code [19], which is defined as follows:

$$gb_{i,j}^{k} = \begin{cases} pb_{i,j}^{k} & k = 1 \\ pb_{i,j}^{k-1} \oplus pb_{i,j}^{k} & 1 < k \le 8 \end{cases} \quad (6)$$

In this formulation, the Gray code of $p_{i,j}$ is denoted by $g_{i,j}$. In addition, the k^{th} bit of $p_{i,j}$ and $g_{i,j}$ are presented by $pb_{i,j}^{k}$ and $gb_{i,j}^{k}$, respectively. According to (6), the first bit of the coded and original pixels are equal. In the following, each bit of the coded pixel is derived by applying XOR operator to the corresponded bit in the plain pixel and its preceding bit.

The proposed coding algorithm has been extended the Gray code considering the way of data representation in the images. A pixel is represented using one byte, where the stored value determines its gray level. For example, black and white colors are presented by 0 and 255, respectively. The most significant bit (MSB) of a pixel contains the most information about its gray level. Therefore, the modification of this bit changes the gray level of the pixel significantly. Other bits are not as effective as MSB. According to the above discussion, in the coding algorithm, the MSB of the pixel is complemented. The other bits are coded as the same as the Gray code. The formula of calculating $c_{i,j}$ is formally stated in the following:

$$cb_{i,j}^{k} = \begin{cases} \tilde{pb}_{i,j}^{k} & k = 1 \\ pb_{i,j}^{k-1} \oplus pb_{i,j}^{k} & 1 < k \le 8 \end{cases} \quad (7)$$

where $cb_{i,j}^{k}$ shows the k^{th} pixel of $c_{i,j}$.

We have presented an example in Figure 2 to illustrate our coding scheme. In this figure, the pixel with the binary representation of 10101001 is coded using (7).

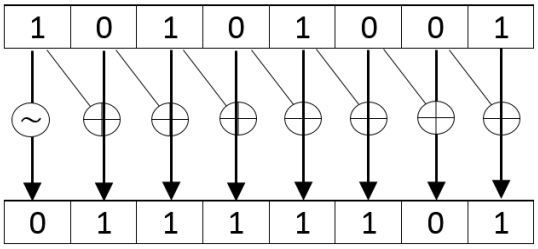


Fig 2. Applying Coding Algorithm to 10101001

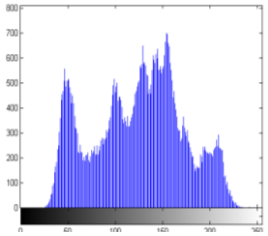
4 EXPERIMENTAL RESULTS

In this section, we have studied the effectiveness of the proposed algorithm. The considered criteria are the smoothness of the histogram, entropy, correlation, and key sensitivity. The proposed algorithm has been compared with [6,11-12], where the gray image "Lena" with the size of 256 × 256 is used for evaluation. The algorithms are implemented using Matlab.

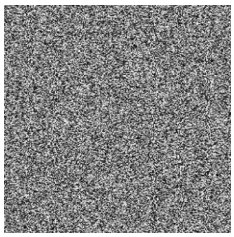
4.1 The Histogram

The histograms of plain and encrypted Lena are depicted in Figure 3. From this figure it is clear that the proposed algorithm provides a very smooth histogram for the encrypted image. As this diagram presents the number of pixels in each gray level, its smoothness means that the number of pixels in different levels are close to each other. This result demonstrates the effectiveness of our algorithm against statistical attacks.

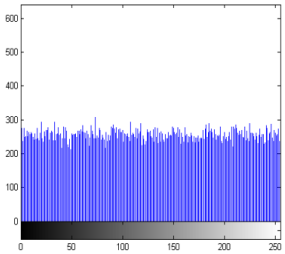
a) Plain Lena



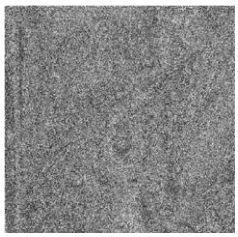
b) The Histogram of (a)



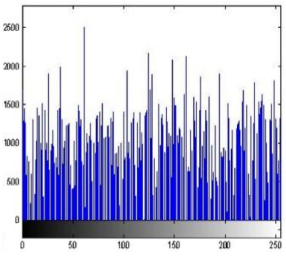
c) The Encrypted Image by Our Algorithm



d) The Histogram of (c)

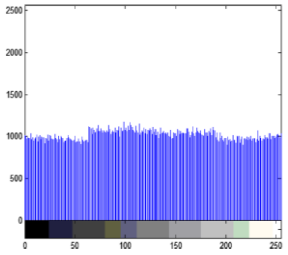


e) The Encrypted Image by [6]

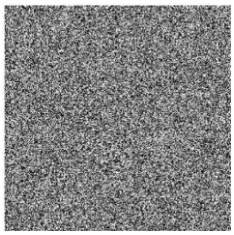


f) The Histogram of (e)

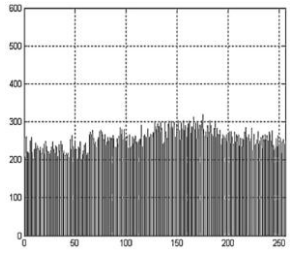
g) The Encrypted Image by [11]



h) The Histogram of (g)



i) The Encrypted Image by [12]



j) The Histogram of (i)

Figure 3. The Histograms of Plain and Encrypted Lena

4.2 Entropy

The entropy of a source is a criteria to measure the degree of its randomness. The entropy of the gray image *I*, which includes 255 gray levels, is given as:

$$H(I) = -\sum_{i=1}^{255} p(l_i)\log_2\left(p(l_i)\right) \qquad (8)$$

where $p(.)$ and l_i denote the probability function and the number of the pixels in the i^{th} gray level, respectively.

Table 2 shows the entropies of plain and encrypted Lena. The results demonstrate that the proposed algorithm improves entropy in comparison with [6,11-12]. Moreover, the outcome of our algorithm is close to the optimal value, which is equal to 8.

Table 2: Comparison of Entropies

Encryption Algorithm	Entropy
The plain image	7.5889
The proposed algorithm	7.9973
Ref. [6]	7.857
Ref. [11]	7.994
Ref. [12]	7.987

4.3 Correlation

The correlation of an image determines the degree of similarity between its adjacent pixels, which is defined as the following:

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

In this formulation, $E[.]$ and σ denote average and standard deviation, respectively.

The correlations of plain and encrypted Lena are tabulated in Table 3. From this table we can see that the proposed algorithm degrades correlation substantially. This criterion is reduced at least by 50% in comparison with the other approaches.

Table 3: Comparison of Correlations

Encryption Algorithm	Correlation
The plain image	0.9597
The proposed algorithm	0.0014
Ref. [6]	0.021
Ref. [11]	0.0032
Ref. [12]	0.0021

4.4 Key Sensitivity

The other important measure for evaluating image encryption algorithms is the key sensitivity. This criterion shows the amount of adaption of the encrypted image against small variations of the secret key. Two measure are employed to quantify the key sensitivity: Number of Pixels Change Rate (NPCR) and Unified Average Change Intensity (UACI). These criteria present the number of different pixels, and the difference of two images, respectively. For two images x and y with n pixels, NPCR and UACI are formally defined as:

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

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

where x_i and y_i are the nth pixel of x and y, respectively.

To investigate the key sensitivity of the proposed algorithm, we have changed a bit of the secret key randomly and compute NPCR and UACI of the encrypted Lena with these keys. The results are given in Table 4. As it is shown in this table, The NPCR is degraded by 0.02. On the other hand, UACI is improved by 0.38.

Table 4: Comparison of NPCR and UACI

Encryption Algorithm	NPCR	UACI
The proposed algorithm	99.60	33.44
Ref. [6]	-	-
Ref. [11]	99.62	33.06
Ref. [12]	99.53	32.57

5 CONCLUSION

In this paper we have proposed a novel image encryption algorithm. In this scheme, we have designed a new chaotic map to generate pseudo random sequences. This map increases the degree of randomization of the generated sequences in comparison with the previous approaches. Moreover, we have developed a coding scheme through extending the Gray code. This algorithm enhances the confusion of the pixels and consequently, the performance of the encryption procedure is improved. The security analysis has demonstrated the superiority of our algorithm in comparison with the previous approaches.

6 REFERENCES

[1] D. Coppersmith, C. Holloway, S.M. Matyas, and N. Zunic, "The Data Encryption Standard. Information Security Technical Report", Vol. 2, No. 2, 1997, pp. 22-24.

[2] 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.

[3] Z. Yisheng, L. Shuyun, and L. Dequn, "A New Chaotic Algorithm for Image Encryption", Chaos, Solitons & Fractals, Vol. 29. No. 2, 2006, pp. 393-399.

[4] 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, Vol. 109, 2015, pp. 119-131.

[5] M. Rani, and S. Kumar, "A Novel and Efficient Approach to Encrypt Images Using Chaotic Logistic Map and Stream Cipher", Proceedings of IEEE International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 1442-1447.

[6] 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, Vol. 19, No. 9, 2014, pp. 3106-3118.

[7] 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, No. 8, 2014, pp. 902-913.

[8] W. Zhang, H. Yu, Y.L. Zhao, and Z.L. Zhu, "Image Encryption Based on Three-

Dimensional Bit Matrix Permutation", Signal Processing, Vol. 118, 2016, pp. 36-50.

[9] L. Habibpour, S. Yousefi, M. Zolfi Lighvan, and H. Aghdasi, "1D Chaos-based Image Encryption Acceleration by using GPU", Indian Journal of Science & Technology, Vol. 9, No. 6, 2016, doi: 10.17485/ijst/2016/v9i6/72651.

[10] 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, Vo. 127, No. 7, 2016, pp. 3541-3545.

[11] A. Jain, and N. Rajpal, "A Robust Image Encryption Algorithm Resistant to Attacks Using DNA and Chaotic Logistic Maps", Multimedia Tools and Applications, Vol. 75, No. 10, 2016, pp. 5455-5472.

[12] H. Liu, and X. Wang, "Image Encryption Using DNA Complementary Rule and Chaotic Maps", Applied Soft Computing, Vol. 12, No. 5, 2012, pp. 1457-1466.

[13] A. Bakhshandeh, and Z. Eslami, "An Authenticated Image Encryption Scheme Based on Chaotic Maps and Memory Cellular Automata", Optics and Lasers in Engineering, Vol. 51, N. 6, 2013, pp. 665-673.

[14] Z. Tang, X. Zhang, and W. Lan, "Efficient Image Encryption with Block Shuffling and Chaotic Map", Multimedia Tools and Applications, Vol. 74, No. 15, 2015, pp. 5429-5448.

[15] A. Abirami, and R. Amutha, "Image Encryption Based on DNA Sequence Coding and Logistic Map", Advances in Natural and Applied Sciences, Vol. 9, No. 9, 2015, pp. 55-63.

[16] 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, Vol. 75, No. 1, 2016, pp. 1-23.

[17] 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, Vol. 66, 2015, pp. 10-18.

[18] 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, Vol. 80, No. 3, 2015, pp. 1483-1491.

[19] C. Savage, "A Survey of Combinatorial Gray Codes", SIAM Review, Vol. 39, No. 4, 1997, p. 605-629.

[20] N. Mondal, and P.P. Ghosh, "A Pseudo Random Number Generator from Chaos", 2012, arXiv:1203.5731v7.