A Novel Method for Image Encryption Using Modified Logistic Map

Ardalan Ghasemzadeh*
Computer Engineering & Information Technology Department, Urmia University of Technology, Urmia, Iran
a.ghasemzadeh@uut.ac.ir
Omid R.B. Speily
Computer Engineering & Information Technology Department, Urmia University of Technology, Urmia, Iran
speily@uut.ac.ir

Received: 19/Nov/2018 Revised: 19/Mar/2019 Accepted: 07/May/2019

Abstract

With the development of the internet and social networks, the multimedia data, particularly digital images, has been of increasing interest to scientists. Due to their advantages including high speed, high security, and complexity, chaotic functions have been broadly employed in image encryption. The present paper proposed a modified logistic map function which resulted in higher scattering in the obtained results. Confusion and diffusion functions, as the two main actions in cryptography, are not necessarily performed in order, i.e. each of these two functions can be applied on the image in either order, provided that the sum of total functions does not exceed 10. So, to calculate the sum of functions, confusion has the factor of 1 and diffusion has the factor of 2. To simulate this method, a binary stack was used. Application of binary stack and pseudo-random numbers obtained from the modified chaotic function increased the complexity of the proposed encryption algorithm. The security key length, entropy value, NPCR and UACI values, and correlation coefficient represented in the analytical results revealed the capability and validity of the proposed method. Analyzing the obtained results and comparing the algorithm to other investigated methods clearly verified high efficiency of the proposed method.

Keywords: Encryption; Decryption; Logistic Map; Confusion; Diffusion.

1. Introduction

With widespread use of the Internet, especially after the advent of online communities such as social networks, millions of bytes of information are being transmitted every day [1]. This information is transmitted through text, audio, image and video between different users [2]. Encryption is a traditional technique for the secure transmission of this information. However, the traditional text encryption techniques cannot protect images efficiently due to the big difference between images and texts. Image Encryption is a serious challenge in governmental (military, medical) digital services, multimedia systems, and Internet-based communications. On the other hand, the recent advances in information and communication technology and e-commerce have provided potential markets for distributing digital content such as image over the Internet [3]. A big challenge is how to protect the intellectual property of multimedia content, namely image, in multimedia networks. Accordingly, development of efficient methods for the storage and transfer of digital data has become an attractive topic for researchers. It is highly

Necessary for these data to be transformed to a template preventing the access of invalid users to them.

Therefore, ensuring the security of image messages is a dramatically important topic today [4]. In the last decade, different encryption algorithms have been introduced based on various principles in the literature, such pixel adaptive diffusion [5], fractional wavelet transform [6], image filtering [7], elliptic curve [8], and reversible cellular automata [9]. 2D cellular automatic machines [10, 11], collusion function-based methods [12], domain phase-based algorithms [13], and chaos theory [14-16] are more popular in image encryption. Due to the properties of chaotic systems such as acceptable speed, security, and high complexity, chaos-based encryption algorithms can be useful in many applications.

An ideal encryption method is expected to address some of the fundamental requirements of encryption including chaos, distribution, and randomness. Due to their random behavior and high sensitivity to primary parameters and conditions, chaotic systems provide great potential to resist the attack of invalid users. Natiq et al. proposed a new hyperchaotic map based on Sine map and two-dimensional Henon map. They indicated that their proposed method could encrypt digital images with high complexity performance and low implementation cost [17]. Huang and Ye used an image encryption algorithm based on irregular wave representation [18]. Although the method's NPCR and UACI were higher than 0.9 and 0.33, respectively, it was time-consuming. In [19], a synchronous permutation-diffusion technique was used for image encryption. In that paper, in order to reduce the sending process time, permutation and diffusion steps for any pixel are performed in the same time. An image encryption scheme based on chaotic tent map is proposed by Li et al. [20]. They show that, image encryption systems based on such map show some better performances. A new cryptographic method was proposed based on Henon chaotic map in [21]. Color image encryption using random

* Corresponding Author

transforms, phase retrieval, chaotic maps, and diffusion was presented in [22]. A combination of several encryption tools is used in that paper.

Chaotic functions are generally employed in the encryption of text and image files. Basic logistic map chaos function has some disadvantages such as short alternation period, undesirable uniformity, and low independence from the generated data [23].

In this paper, a modified basic logistic map function is introduced to overcome the disadvantages such as undesirable uniformity and low independence. Then the modified logistic map function is employed in the encryption of images to efficiently apply diffusion and confusion functions on images using a stack structure and favorably performed encryption.

The rest of this paper is organized as follows. Section 2 introduces the theoretical foundations of the proposed algorithm. Section 3 investigates the implementation of the proposed algorithm and its effect on some sample images. The experimental results along with their analysis are presented in section 4. Conclusions are represented in section 5.

2. Theoretical Foundations of the Proposed Algorithm

General procedure of image encryption algorithms using chaotic functions is as follows:

i. First, the input image is transformed into a 2D arrangement of constituent pixel values.
ii. A chaotic map function is chosen to generate pseudo-random numbers. In this step, parameters and primary values of the chaotic function are chosen in order for the signal to have chaotic behaviour in the considered interval.
iii. All parameters and values required for the encryption of the image in the destination are included in the encryption key.
iv. The procedure of confusion is applied. In this step, matrix values of the image are relocated to random positions using random numbers generated by the chaotic function. This relocation takes place according to box, row-column, singular, or other methods. Method selection affects the operational speed of the algorithm.
v. The procedure of diffusion is applied. In this step, every single pixel in the image matrix is changed. In fact, the value of each pixel is added to the random value obtained from chaotic function and other parameters (depending on the used algorithm considering speed and security) were balanced within the valid interval of pixel values.

Depending on the type of the algorithm, each of the two above steps could be repeated until the algorithm reached the required resistance to different attacks. The order of repeat was included in the encryption key. Decryption of the image was done at the destination with the encryption key with the reverse order of the above steps.

2.1 Algorithm Description

In the proposed algorithm, the modified linear logistic chaotic map was used. Logistic map function is defined by Eq. (1) [24]:

$$x_{n+1} = r.x_n(1 - x_n) \quad n = 1, 2, 3, \ldots \tag{1}$$

Fig. (1) shows the behavior of this function over time.

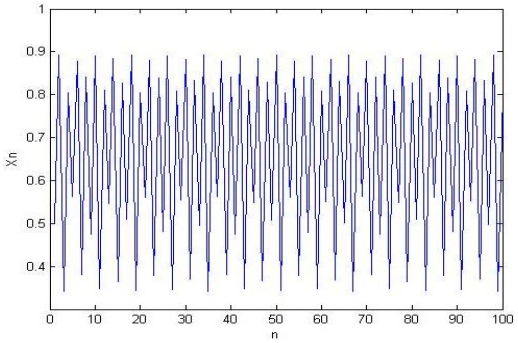

Fig. 1. Behavior of logistic map function

The main problem of logistic map function is that the scattering of numbers generated in the random interval is low, especially in the beginning and end of the interval. By introducing some changes in the basic logistic map function, as shown below, more chaotic and random behavior was observed:

```
Logistic(x0,r)
Begin
   pow←1
   t←(r * x0 * (1 - x0))
   if ((t * 100) Mod 2) = 0 then
  pow ← 2
   p ← t + Math.Pow(-1, pow) * (t /100)
   if (0 < p and p < 1) then
      return p
   else
return Logistic(t, r)
end.
```

Algorithm 1. Modified Logistic Map algorithm

In this algorithm, t stands for the value obtained from basic logistic map function. If t is even it increases by $t/100$, otherwise $t/100$ is subtracted from its value.

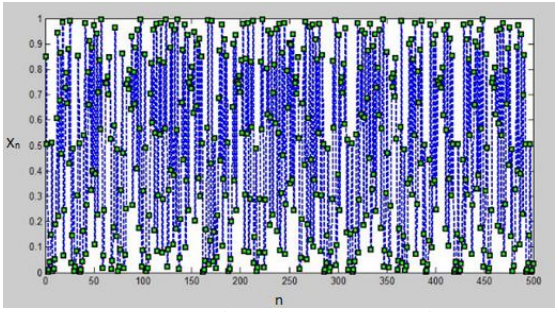

Fig. 2. Behavior of modified logistic map function

Only values between 0 and 1 were used as random values. The behavior of the modified function for the primary value of $x_0 = 0.3$ and parameter of $r = 3.988$ is shown in Fig. 2. The values obtained from the algorithm were arranged in a linear array and sorted in an ascending

order. After sorting, the primary array index was used as the values for encryption. The scattering of basic and modified logistic map in the interval of [0,1] for 500 repeats is given in Table 1.

Table 1. Results for logistic map and modified logistic map

Primary values	$x_0 = 0.5$ r = 3.988 n = 500
Main Algorithm	79,59,36,27,35,40,40,27,43,114
Modified Algorithm	86 ,49,34,43,21,52,36,41,53,85
Primary values	$x_0 = 0.8$ r = 3.978 n = 500
Main Algorithm	80,45,33,38,42,36,33,30,56,107
Modified Algorithm	33 ,44,42,40,25,33,39,86,53,105

As it is clear in the results, the scattering of the modified mapping is better for primary similar values.

2.2 Stack Structure

The proposed algorithm is not sensitive to the order of confusion and diffusion applied on the image provided that the sum of the applied procedure does not exceed 10. To calculate the sum of procedures, confusion procedure has the factor of 1 and diffusion procedure has the factor of 2. For the simulation of this method, the binary stack was used so as to make it possible to perform the procedures in the reverse order in the decryption step and obtain the original image. During encryption, the stack status is included in the encryption key and the stack structure is restored at the destination according to the values of encryption key.

2.3 Encryption Key Definition

In the introduced algorithm, key consists of two parts and has a length of 128 bits. The first part keeps parameters and primary values of the chaotic function and the second part is used for mapping the stack status. At the beginning and for each image, the part associated with the parameters and primary values in the encryption key is generated randomly. Furthermoer, according to these 0-1 strings, primary value and parameter of chaotic function is generated.

3. Implementation of the Proposed Algorithm

The proposed algorithm is implemented based on the following steps:

a. First, the values of three elements of color image, namely red, green, and blue, are separated and put into separate matrices, i.e. if the dimensions of the input image are in the form of $L = [h * W]$ then matrices will be in the form of $L_2 = [h * 3W]$.

b. The encryption key is generated as a sequence of random binary numbers, as shown in Fig. 3.

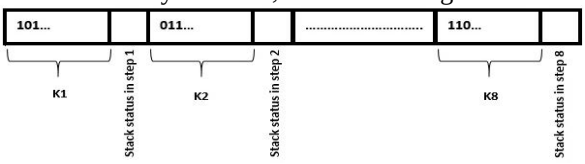

Fig. 3. key structure

According to the generated key, parameter R and primary value X_0 are obtained by the following equations:

$$K = K_1, K_2, \dots, K_8 \quad (2)$$

$$K' = (K_1 \oplus K_2), \dots, (K_7 \oplus K_8) \quad (3)$$

$$K'' = (K'_1 \oplus K'_2), (K'_3 \oplus K'_4) \quad (4)$$

$$\text{Sum} = K'_1 + K'_2 + K'_3 + K'_4 \quad (5)$$

$$K''' = K''_1 \oplus K''_2 \quad (6)$$

$$X_0 = [(\text{float})(K''' + \text{Sum})\%256]/256 \quad (7)$$

$$r = 3.97 + [(\text{float})\ \text{Sum}\ \%\ 299]/10000 \quad (8)$$

According to Fig. 3, each K_i includes 14 bit-containers of encryption key. Applying these equations, parameters and primary values are obtained randomly within the following intervals:

$$x \in [0, 0.9999] \quad r \in [3.97, 3.9999]$$

In order to apply confusion, the two following steps are taken:

a. Linear array I_1 with length h is created and filled with decimal values obtained from chaotic function. The sorted values of I_1 are put into array I_2. Then, values of I_2 are searched in I_1 and their index is input into another array with the name of Index, whose length is equal to I_1 and I_2. This way, column indices of the image are randomly placed in the Index array. Then, each column of L_2 matrix is relocated according to the Index array, as well illustrated in Fig. 4.

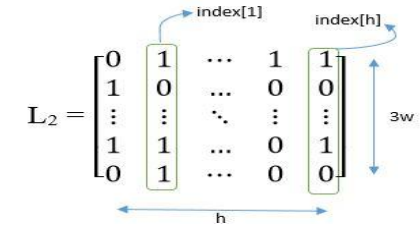

Fig. 4. First step in applying confusion

b. Now, according to Fig. 5, the procedure of step c is applied to rows in order to relocate 3w dimension.

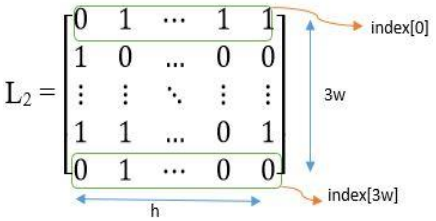

Fig. 5. Second step in applying confusion

Moreover, the following steps are taken for applying diffusion algorithm.

c. First, in linear chaotic matrix with the length of $h * w_2$, random numbers from the interval $[0, (h * w) - 1]$ are located. The parameter X_0 is divided by 3, i.e. $X'_0 = X_0/3$.

d. In this step, the parameter sum is added to each element of a pixel. Here, the sum includes the value of red element associated with the previous pixel and the random number generated for the current pixel. The red color element of the previous pixel is added so that if a small variation takes place in the decryption of the image, the original image cannot be restored even if the correct key is available. Then, the value of each color element of the pixel is added with sum and balanced into the interval [0,255]. This step is applied on every pixel of the image.
e. Finally, all three matrix elements of the image are integrated.

At last, having the parameter and primary value as well as the employed logistic function, random numbers used during encryption can be restored to decrypt the image. That is to say, using the above-mentioned steps in the reverse order, the original image is obtained. In the Fig. 6, the proposed method is shown in the flowchart format.

3.1 Results of Applying Algorithm on Some Sample Images

The proposed algorithm was applied on some standard images including Figs. 7, 8, and 9 as primary, encrypted, and decrypted images, respectively. Moreover, the color histogram of each image is shown within three main color channels. The color histograms clearly shows the performance of the proposed algorithm for Baboon and Lena images.

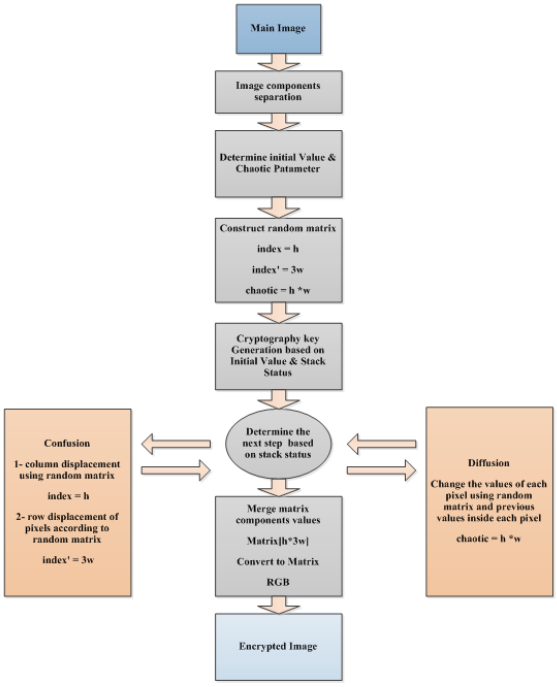

Fig. 6. The flowchart of the proposed method

4. Results and Discussions

An optimal encryption algorithm mush have enough security and efficiency against different types of decryption attacks, statistical attacks, comprehensive operation of key space, and brute-force. In what follows, the performance of the proposed algorithm in these tests is described.

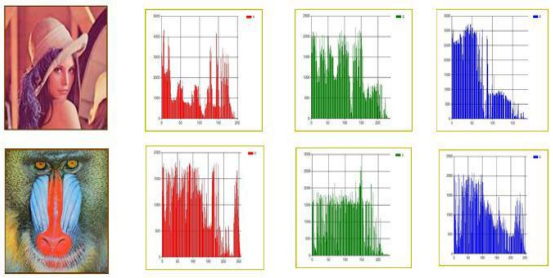

Fig. 7. Primary images and color histograms

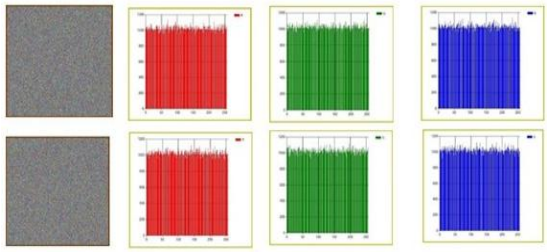

Fig. 8. Ciphered images and color histograms

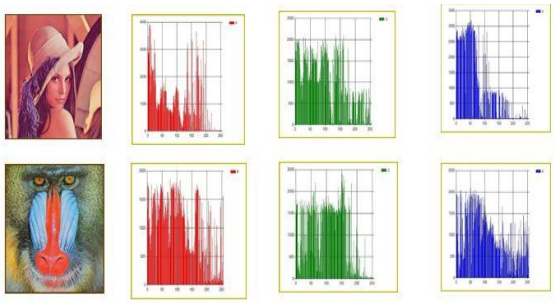

Fig. 9. Decrypted images and color histograms

4.1 Key Space Analysis

In an encryption algorithm, key space has to be big enough to be resistant against brute-force attacks. NIST organization has predicted the minimum required length of encryption key to be 80 bits [25]. The key space of the proposed method is 2^128 which is much bigger than 2^80, therefore it is safe against comprehensive key search attacks.

4.2 Histogram Analysis

Histogram shows the number of pixels at each gray level of an image. If the distribution of gray levels is not uniform in an image, the original image can be restored merely with attack by having the encrypted image and not needing the key. Therefore, a good encryption algorithm has to act in order for the histogram of the encrypted image to have random and uniform appearance and the attackers cannot get any information from this aspect of the image.

In Figs. 7, 8, 9, the histograms of two standard images of Lena and Baboon are shown in three states including original, encrypted, and decrypted, respectively. Histogram of the image in encrypted state was perfectly uniform and different from the histogram of the original image. That is to say that the attackers cannot obtain any

information on the original image by analyzing the histograms of encrypted images.

4.3 Correlation Coefficient Analysis

The correlation between two adjacent pixels is known as the correlation coefficient which is one of the most important features in image encryption area [16]. To investigate the correlation between two adjacent pixels in an image, first 4069 couples of adjacent pixels were chosen totally randomly. Later, the correlation coefficient of each couple was calculated using Eq. (9) [26].

$$r_{xy} = \frac{\mathrm{Cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (9)$$

where x and y are the gray levels of two adjacent pixels. Eqs. (10)-(12) define parameters used in Eq. (9).

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (10)$$

$$\mathrm{Cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (11)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (12)$$

Below, the results of this test for adjacent pixels in diagonal state for two images of Lena and Baboon are represented. Figs. 10 and 11 display the diagonal correlation for the two images.

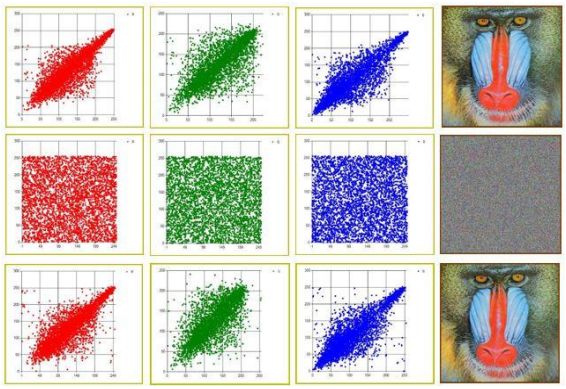

Fig. 10. Diagonal correlation test for original, encrypted, and decrypted images

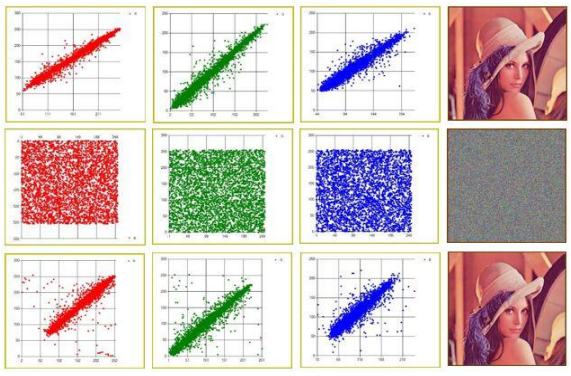

Fig. 11. Diagonal correlation test for original, encrypted, and decrypted images

As shown in Table 2, all three diagonal, horizontal, and vertical correlations are calculated for the image of Lena.

Table 2. Correlation of Lena image

Correlation type	Plain image	Cipher image
Horizontal correlation	0.97028249	0.0079959
Vertical correlation	0.9628058	0.0096502
Diagonal correlation	0.985534	0.0109409

According to the results and figures, it is clear thatthe correlation of pixels is significantly reduced in the encrypted state .

4.4 Analysis of the Sensitivity of the Algorithm

In addition to the key sensitivity, plaintext sensitivity is also an important rule to evaluate the efficiency of a designed image encryption algorithm. In other words, the algorithm should be very sensitive to the plain-image even just for one-bit change [18]. To analyze the sensitivity of the algorithm, the original image was encrypted at first. Then, one pixel of the original image was changed in a completely random way. The obtained image was encrypted one more time and finally the two encrypted images were compared based on the following equations. The effect of changing one pixel in the original image on the encrypted image was investigated with two measurement criteria, namely NPCR and UACI [27].

NPCR is the average number of pixels in the encrypted image varied due to the change of one pixel in the original image. For two encrypted images $C1$ and $C2$ whose original images were different only in one pixel, a 2D arrangement of $D(i,j)$ was first calculated according to the following equation:

$$D(i,j) = \begin{cases} 0 & ; C1(i,j) = C2(i,j) \\ 1 & ; C1(i,j) \neq C2(i,j) \end{cases} \quad (13)$$

Where $C1(i,j)$ and $C2(i,j)$ stand for the value of gray level of pixels in encrypted images of $C1$ and $C2$, respectively. Based on [27], NPCR is the absolute number of pixels which changes value in differential attacks, can be evaluated by Equation (14).

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} * 100 \quad (14)$$

Where M and N are the dimensions of the original image.

UACI is the average of lightness intensity difference between two images which is calculated as follows [27]:

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\frac{\sum_{i,j}|C1(i,j) - C2(i,j)|}{2^L - 1}\right] * 100 \quad (15)$$

Where L is the number of bits used for displaying the image, which was 8 in the present study.

To design an acceptable encryption method, the NPCR should be greater than 0.99 and the UACI is about 0.33 [28]. Average NPCR and UACI for this algorithm were 0.993454 and 0.334267, respectively.

4.5 Analysis of Entropy

Entropy or irregularity is a criterion for describing the randomness of information source which was first introduced by Shanon in 1949. Moreover, it is calculated as follows and the theoretical value is 8 for a message in gray level [15].

$$H(s) = -\sum_{i=0}^{N-1} P(S_i).\log\left(\frac{1}{P(S_i)}\right) \quad (16)$$

where N is the number of gray levels used in the image which was $2^8 = 256$ here and $P(S_i)$ shows the probability of occurrence of the i-th gray level in the image. Table 3 shows the results of entropy test for original and encrypted images of Lena.

Table 3. Entropy test results for Lena image

	Red element	Green element	Blue element
Plain image	7.2530845	7.5951533	6.968516
Cipher image	7.999302	7.999353	7.999269

4.6 Performance Analysis

To provide more evaluations, the proposed method was compared with several methods including hyper chaotic map [7], irregular wave representation [15], synchronous permutation-diffusion technique [19], chaotic tent map [20], chaos-based fast image encryption algorithm [28], hybrid genetic algorithm and chaotic function model [29], chaos-based symmetric image encryption using a bit-level permutation [30], DNA sequence operation and hyper-chaotic system [31], quantum logistic map [32], and coupled two-dimensional piecewise chaotic map [33] , Total Chaotic Shuffling Scheme [34].

First, this comparison was made based on the correlation of adjacent pixels, shown in.Table 4.

The results show that the correlation in the proposed method is smaller than that in many other methods.

Table 5 summarizes the sensitivity of the algorithm to the original image and compares it with other algorithms.

Table 4. Correlation comparison between the proposed method and other related methods

	Horizontal	Vertical	Diagonal
Proposed algorithm	0.0009995	0.006650	0.00109
Ref. [18]	0.0172	0.0277	0.0039
Ref. [19]	0.0008	0.0021	0.0005
Ref. [20]	0.0016	0.0025	0.0003
Ref. [28]	0.0009	-0.0022	0.0149
Ref. [29]	-0.0054	0.0093	-0.00009
Ref. [30]	0.002	0.0009	0.0016
Ref. [31]	-0.0002	0.0038	0.0009
Ref. [32]	0.0065	0.0055	0.0082
Ref. [34]	0.00235	0.001235	0.00036

As can be seen in Table 5, after encryption of both images, the values of NPCR and UACI exceed 99% and 33%, respectively, outperforming other comparable methods and proving that the proposed method has the capability to resist differential attacks.

Table 5. The performance of the proposed scheme and other comparable methods based on NPCR and UACI

Algorithm	UACI	NPCR
Proposed algorithm	0.334267	0.993454
Ref. [10]	0.3327	0.9941
Ref. [19]	0.335989	0.996304
Ref. [28]	0.335615	0.996427
Ref. [29]	0.331084	0.971394
Ref. [30]	0.334815	0.996473
Ref. [31]	0.335989	0.996304
Ref. [34]	0.334627	0.996086

In Table 6, the entropies of the original and encrypted images at three states are shown and compared with other algorithms.

The results show that the entropy of the proposed method is very close to the ideal entropy value, higher than that of many other existing algorithms.

Table 6. Entropy Comparison

Algorithm	Entropy
Proposed Algorithm	7.999308
Ref. [10]	7.9965
Ref. [19]	7.9994
Ref.[20]	7.9998
Ref. [28]	7.9994
Ref. [29]	7.9978
Ref.[30]	7.9993
Ref.[31]	7.9975
Ref.[33]	7.9992
Ref.[34]	7.9993

4.7 Resistance to Noise Analysis

The resistance of an encryption system to noise in real-world communication technologies is one of the most important issues. When an image is transferred through a communication channel, it can be exposed to destructive noise. A good encryption algorithm needs to have the potential of preventing severe destruction of the decrypted image on receiver's side when the encrypted images are subjected to noise by being transferred through a communication channel [25,35].

The results obtained by tests on the images show that the proposed algorithm has the required resistance to salt and pepper noise and Gaussian noise. Figs. 12 and 13 present the results obtained by applying salt and pepper noise on sample images. Fig. 12 depicts the results obtained by testing the image after applying 15% salt and pepper noise on the encrypted Baboon image which can be observed after decryption on the right side of the figure.

Fig. 12. Applying Salt and pepper noise with 15% density on encrypted image

Fig. 13 shows the application of 40% noise on an image of an airplane.

Noise can have a great destructive effect on the key such that decryption becomes impossible even by small changes in the key. Transferring key through a safe channel, independent from the channel through which the image is transferred, can prevent this problem.

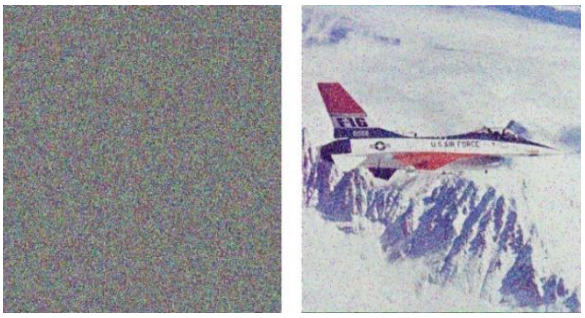

Fig. 13. Applying Salt and pepper noise with 40% density on encrypted image

5. Conclusion

Different patterns have proposed for image encryption among which those based on chaos theory have gained special popularity. The present paper proposed a novel algorithm based on chaos theory and modified logistic map. Pseudo-random numbers obtained from the modified function had higher distribution than those obtained from the basic logistic mapping function.

For encryption, confusion and diffusion were applied on the pixels of the original image in a random order. Furthermore, the random order was managed based on a binary stack and a 128-bit key on both sender and receiver sides. The key consisted of two parts where the first part kept the parameter and primary value of chaotic function and the second part was used for mapping stock states. First, for each image, the part related to the parameter and primary value was randomly generated in the encryption key. Then, based on this 0-1 strings, primary value and the parameter of the chaotic function were created.

The proposed algorithm was tested on sample and standard images. Moreover, the parameters required for the analysis of the proposed algorithm were discussed and compared with other algorithms, verifying the efficiency and security of the proposed lagorithm to different attacks.

References

[1] Kardan, O. R. B. Speily. Increasing Information Reposting Behavior in Online Learning Community. Educational Technology & Society, 21(4), 100–110. 2018.

[2] Speily, O. R. B.. De-lurking in Online Communities Using Repost Behavior Prediction Method. Information Systems & Telecommunication, 192. 2017.

[3] Tarokh, M. J., Arian, H. S., & Speily, O. R. B.. Discovering Influential Users in Social Media to Enhance Effective Advertisement. Advances in Computer Science: An International Journal, 4(5), 23–28. 2015.

[4] H. Natiq,M. Said, & A. Kilicman. "A new hyperchaotic map and its application for image", https://doi.org/10.1140/epjp/i2018-11834-2. 2018.

[5] Z. Hua, S. Yi & Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion", Signal Processing. https://doi.org/10.1016/j.sigpro.2017.10.004, 2017.

[6] B. Gaurav, Q. M. Jonathan Wu & B. Raman. "Discrete fractional wavelet transforms and its application to multiple encryption." Inf. Sci. 223-297-316, 2013.

[7] Z. Hua & Y. Zhou. "Design of image cipher using block-based scrambling and image filtering". Information Sciences. https://doi.org/10.1016/j.ins.2017.02.036, 2017.

[8] L. D. Singh & K. M. Singh. 'Image Encryption using Elliptic Curve Cryptography", Procedia - Procedia Computer Science, 54, 472–481. https://doi.org/10.1016/j.procs.2015.06.054, 2015.

[9] X. Wang & D. Luan. "A novel image encryption algorithm using chaos and reversible cellular automata". Communications in Nonlinear Science and Numerical Simulation, 18(11), 3075–3085. https://doi.org/10.1016/j.cnsns.2013.04.008, 2013.

[10] O. Lafe, "Data Compression and Encryption using Cellular Automata Transform", Engineering Applications of Articial Intelligence, Vol. 10, No. 6, pp. 581–591, 1998.

[11] R. J. Chen and J. L. Lai, "Image Security System using Recursive Cellular Automata Substitution," Pattern Recognition , Vol. 40, pp. 1621–1631, 2007.

[12] A. Jolfaei and A. Mirghadri, "Survey: Image Encryption Using Salsa20", International Journal of Computer Science Issues, Vol. 7, Issue 5, pp. 213-220, September 2010.

[13] S. E. Borujeni and M. Eshghi, "Chaotic Image Encryption System using Phase-Magnitude Transformation and Pixel Substitution", J. Telecommun. Syst. DOI:10.1007/s11235-011-9458-8. 2011.

[14] C. Zhu, "A Novel Image Encryption Scheme based on Improved Hyperchaotic Sequences," Journal of Optics Communications, Vol. 285, pp 29–37, 2012.

[15] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, "A Simple,Sensitive and Secure Image Encryption Algorithm based on Hyper-Chaotic System with Only One Round Diffusion Process," The Journal of Multimedia Tools and Applications, DOI 10.1007/s11042-012-1292-9, 2012.

[16] X. Wang and L. Teng, "An Image Blocks Encryption Algorithm based on Spatiotemporal Chaos", J Nonlinear Dyn., Vol. 67, pp. 365–371, 2012.

[17] H. Natiq, M. R. M. Said & A. Kilicman. "A new hyperchaotic map and its application for image". https://doi.org/10.1140/epjp/i2018-11834-2, 2018.

[18] X. Huang, G. Ye, "An image encryption algorithm based on irregular wave representation". https://doi.org/10.1007/s11042-017-4455-x. 2017.

[19] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem & M. Lee, "Image encryption using a synchronous permutation diffusion technique". Optics and Lasers in Engineering, 90(June 2016), 146–154. https://doi.org/10.1016/j.optlaseng.2016.10.006. 2017.

[20] C. Li, G. Luo & K. Qin. "An image encryption scheme based on chaotic tent map". Nonlinear Dynamics. https://doi.org/10.1007/s11071-016-3030-8.2016.

[21] K. Mishra, R. Saharan, & B. Rathor, "A new cryptographic method for image encryption", 32, 2885–2892. https://doi.org/10.3233/JIFS-169231. 2017.

[22] M. H. Annaby, M. A. Rushdi, & E. A. Nehary. “Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion”. Optics and Lasers in Engineering, 103, 9–23. https://doi.org/10.1016/j.optlaseng.2017.11.005. 2018.

[23] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian & M. F. Abu-elyazeed. “Generalized double-humped logistic map-based medical image encryption”. Journal of Advanced Research, 10, 85–98. https://doi.org/10.1016/j.jare.2018.01.009. 2018.

[24] L. Zhang, X. Liao, X. Wang, “An image encryption approach based on chaotic maps”, Chaos Solitons & Fractals, Vol. 24, pp. 759-765, 2005.

[25] Barker, E., Roginsky, A., & Barker, E. (n.d.). “Transitioning the Use of Cryptographic Algorithms and Key Lengths”, NIST Special Publication 800-131A Transitioning the Use of Cryptographic Algorithms and Key Lengths. July 2018.

[26] A. Kulsoom, D. Xiao, A. Rehman, S. A. Abbas, “An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules”, Multimed Tools Appl., DOI 10.1007/s11042-014-2221-x. 2014.

[27] Wu, Yue, Joseph P. Noonan, and Sos Agaian. "NPCR and UACI randomness tests for image encryption." Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) 1.2: 31-38, (2011).

[28] Y. Wang, K. Wong, X. Liao & G. Chen. “A new chaos-based fast image encryption algorithm”, 11, 514–522. https://doi.org/10.1016/j.asoc.2009.12.011. 2011.

[29] A. Hanan,R. Enayatifar & M. Lee., “A hybrid genetic algorithm and chaotic function model for image encryption. AEUE - International Journal of Electronics and Communications, 66(10), 806–816. https://doi.org/10.1016/j.aeue.2012.01.015. 2012.

[30] Z. Zhu, W. Zhang, K. Wong & H. Yu. “A chaos-based symmetric image encryption scheme using a bit-level permutation”. Information Sciences, 181(6), 1171–1186. https://doi.org/10.1016/j.ins.2010.11.009. 2011.

[31] G. Zhang & Q. Liu. “A novel image encryption method based on total shuffling scheme”. OPTICS, 284(12), 2775–2780. https://doi.org/10.1016/j.optcom.2011.02.039. 2011.

[32] A. Akhshani, A. Akhavan, S. C. Lim, Z. Hassan, “An image encryption scheme based on quantum logistic map”, Communications in Nonlinear Science and Numerical Simulation, Vol. 17, pp. 4653-4661, 2012.

[33] S. M. Seyedzadeh, S. Mirzakuchaki, “A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, “Signal Processing, Vol. 92, pp. 1202-1215, 2012.

[34] E. Vaferi, R. Sabbaghi-Nadooshan, “A New Encryption Algorithm for Color Images based on Total Chaotic Shuffling Scheme”, Optik - International Journal for Light and Electron Optics, Volume 126, Issue 20, Pages 2474–2480, October 2015.

[35] M. Mohammadizadeh, B. Pourabbas, K. Foroutani, M. Fallahian, “Conductive polythiophene nanoparticles deposition on transparent PET substrates: effect of modification with hybrid organic-inorganic coating”, International Journal of Engineering (IJE), TRANSACTIONS C: Aspects Vol. 28, No. 4, (April 2015) 567-572.

Ardalan Ghasemzadeh received the B.Sc. degree in software engineering from the Kharazmi University, Tehran, Iran, in 2001 and the M.Sc. degree in Artificial Intelligence and Robotics from Shiraz University, Shiraz, Iran, in 2003. He is currently Ph.D. Candidate in Department of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran. Since 2012, he served as a lecturer at Computer Engineering & Information Technology, Urmia University of Technology, Urmia, Iran. His research interests are Image & Audio processing, machine learning, deep learning & cryptography. His email address is: a.ghasemzadeh@uut.ac.ir.

Omid Reza Bolouki Speily received the B.Sc. degree in Computer Engineering from Urmia University, the M.Sc. & Ph.D. degrees in Information Technology from the AmirKabir University of Technology. He worked as a researcher at the Iran Telecommunication Research Center (ITRC). Since 2009 he joined the Urmia University of Technology as a faculty member of Information Technology & Computer Engineering Department. His research interest includes the dynamics complex networks, graph theory, intelligent system, e-Services. His email address is: speily@uut.ac.ir.