A Novel Image Encryption Scheme Based on Reversible Cellular Automata and Chaos

Zeinab Mehrnahad
Computer Engineering Department, Yazd, Iran
E-mail: zmehrnahad@gmail.com

AliMohammad Latif
Computer Engineering Department, Yazd, Iran
E-mail: alatif@yazd.ac.ir

Abstract—In this paper, a new scheme for image encryption is presented. The scheme is based on a chaotic map and cellular automata (CA). CA is a collection of cells arranged in a grid, such that each cell changes state as a function of time according to a defined set of rules that includes the states of neighboring cells. The major disadvantages of cellular automata in cryptography include limited number of reversal rules and inability to produce long sequences of states by these rules. In this paper, reversible cellular automaton is presented and used to solve this problem. The presented scheme is applied in three individual steps. Firstly, the image is blocked and the pixels are substituted by a reversible cellular automaton. Then, image pixels are scrambled by a chaos map that is produced by an elementary cellular automata and finally the blocks are attached and pixels are substituted by an individual reversible cellular automaton. Due to reversibility of used cellular automata, decryption scheme can reversely be applied. The experimental results show that encrypted image is suitable visually and this scheme has satisfied quantitative performance.

Index Terms—Cryptography, Cellular Automata, Reversible Cellular Automata, Image Encryption, Image Scrambling, Image Substituting.

I. Introduction

With development of communication, computer networks and digital multimedia, information security has become important. This development has some problems such as illegal copy and distribution of digital media. To solve this problem, some methods have been proposed [1,2].

Cryptography is one of the most common methods for information security. It derived from reversible mathematical operation and a set of rule-based calculations called algorithms for generating key of cryptography. Mathematical operations and keys are used to transform multimedia contents in ways that are hard to decryption. The encryption key is considered as the main element in cryptography, so that without the key, even

with knowing the algorithm, decryption is impossible [3].

Digital images are greatly used in multimedia applications recently. These images contain private information in business, military, political, medical and the privacy of visual information is also important [2].

Text encryption algorithms are not suitable for images since these methods require a long computational time and power. Also, images are different from text due to dependency of its pixels. Therefore, special encryption methods are presented for image encryption [4].

Substitution and scrambling are main image encryption methods. Scrambling changes, the arrangement of pixels in the image. In this method, the position of the pixels changed and the encrypted image is obtained. At the destination, according to a recursive process, the initial arrangement of the pixels is obtained [5-7].

In substitution, the value of the pixels is changed by logical and computational operations and then in destination reverse encryption method is performed to retrieve pixel values [8-10].

Cellular Automata (CA) with its inherent characteristics such as the possibility of parallel processing, uniformity, unpredictability of behavior and simple implementation is suitable for image encryption. CA were introduced in 1940's by Von Newmann [11]. After introducing of CA, extensive studies have been done on it. In recent years, CA have been used in cryptography [12-14], image processing [15] and information security [16,17].

The disadvantage of CA includes that it is not inherently reversible, so that only a limited number of rules are reversible. So cryptography using these limited rules does not have the complement security [25,26]. Therefore, we propose a reversible CA in this study. In reversible CA, the new state of a cell is determined not only by the cell itself and its neighbors one step back but also by the cell itself two steps back.

In this paper, image cryptography is provided using both elementary CA and a reversible CA. In this method the combination of substitution and scrambling has been used. We use two reversible CA for substitution and an elementary CA for scrambling; so the proposed structure

consists of three automata and image cryptography is performed in three steps. It should be noted that the proposed structure is reversible and by applying each step reversely, decryption is performed.

II. RELATED WORK

In 2008, Ruisong introduced a method for image encryption using CA. He first generated a sequence of random numbers using CA. Then, he scrambled the image using these [18].

In 2013, Fasel-Qadir et al. proposed digital image scrambling based on two dimensional cellular automata. He used CA for random number generator [19]. It should be noted that image scrambling techniques do not have high security due to the lack of histogram changes.

In 2012, Jin introduced a method for image cryptography using CA [20]. It was a simple image encryption method based on Elementary Cellular Automata (ECA). State attractors generated by ECAs under certain evolution rules perform the encryption function to transform pixel values of image, and the encrypted image is obtained. This method has a periodic behavior. Periodicity means a series of successive rules can be used in rotational way to achieve the original image.

In 2013, Abdo proposed a method based on pixel substitution. In this method, a linearly array of cells with a periodic behavior are generated by CA [21]. In this method loops of recursive rules are formed, and it used to encrypt and decrypt image periodically. In both of above methods, due to the periodicity of the algorithm, there is the possibility of attack and image decryption.

In 2013, Wang proposed a method based on pixel scrambling and substitution [22]. In the scrambling section, reversible CA were used. Substitution was performed only on low-value 4 bits. Therefore, the chance of randomness in this method is less and not suitable for encryption.

In 2014, Mohamed presented a blocking method for cryptography of the image using recursive CA [23]. In this method by using reversible CA, a pseudorandom permutation is first constructed, and then it injected into a parallelizable encryption schema that act on the different blocks of a digital image independently. This method performs well on multi-processor platforms and need powerful hardware implementation.

III. CELLULAR AUTOMAMTA

CA is a mathematical model for discrete dynamic systems consisting of a number of cells. These cells form a network that can have different dimensions. CA has four components in the form of $CA = \{C, S, V, F\}$. The component C indicates the automata cell and S indicates the cell state. In most applications, the cells have two states of zero and one. The component V indicates the dimensions of the automata and the type of neighborhood. The component F indicates the rules for the transfer of CA [24].

A sample of CA including one-dimensional neighborhoods and a periodic boundary state with the transfer rule 30 is shown in Table 1. The first column shows eight possible states for cells with radius neighborhood 1 and second column shows the next state of each cell. The rule number 30 is placed binary in the second column.

Table 1. Elementary CA with Rule = 30

$S_{i,j-1}^{t-1} S_{i,j}^{t-1} S_{i,j+1}^{t-1}$	$S_{i,j}^{t}$
000	0
001	1
010	1
011	1
100	1
101	0
110	0
111	0

In Table 2, the initial input vector of the automata is considered as [0 1 1 0 1 0 1 1]. To apply rule number 30 and 1-D neighborhood to determine the next state, the following procedure is applied. Given the 1-D neighborhood, the first three pixels [0 1 1] are selected. According to the rule 30, the next state is considered 1. Similarly, for the next three pixels, the rule [1 1 0] is applied and the next state of the cell becomes 0. This process continues for the other pixels. For the first and last pixels, the periodic boundary state is considered. The general trend up to 2 steps is shown in Table 2.

Table 2. Example of Elementary CA with Rule = 30

Input vector	01101011							
1-d neighborhood	101	011	110	101	010	101	011	100
Next state	0	1	0	0	1	0	1	0
Output vector Of step 1	01101011 01001010							
1-d neighborhood	001	010	100	001	010	101	010	100
Next state	1	1	1	1	1	0	1	1
Output vector Of step 2	01101011 01001010 11111011							

IV. REVERSIBLE CELLULAR AUTOMAMTA

CA are not inherently reversible, so that only a limited number of rules are reversible. In order to have a proper cryptography algorithm, the mathematical operation should be reversible. Cryptography using these limited rules does not have the complement security [25,26]. Therefore, we decided to use a reversible CA in this study.

In reversible CA, the new state of a cell is determined not only by the cell itself and its neighbors one step back but also by the cell itself two steps back (time(t-1) and (t-2)) [27,28].

For each cell of two step back (time (t-2)), there are two states of zero and one. In addition, for each cell and its neighbors one step back (time (t-1)) for 1-D neighborhoods, eight states can be defined. These two times are shown in Table 3. According to the rule number, we can determine the cell state for time t. In this method, two rules are considered for automata (R_1 and $R_2 = 2^n - R_1 - 1$). This is shown in the second column of table 3 for two rules of 30 and 225.

Table 3. Reversible CA with $R_1 = 30$ and $R_2 = 225$

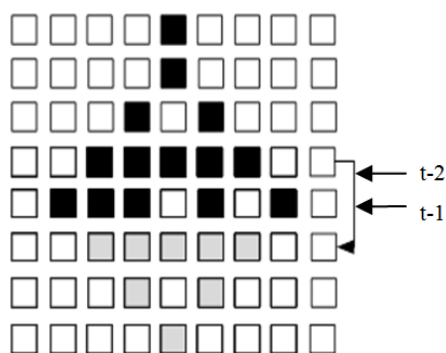| $S_{i,j-1}^{t-1} S_{i,j}^{t-1} S_{i,j+1}^{t-1}$	$S_{i,j}^{t}$	
	$S_{i,j}^{t-2} = 1$ (R$_1$=30)	$S_{i,j}^{t-2} = 0$ (R$_2$=225)
000	0	1
001	1	0
010	1	0
011	0	1
100	1	0
101	0	1
110	0	1
111	0	1

Fig.1. Performance of Reversible CA

An example of reversible CA with rule 30 is shown in Fig. 1. The first row is the input vector and the second row is repetition of first row. As shown in Fig. 1, the next state of cells is determined with two rows above this state. For reversibility of automata, the row at time (t-2) can be

placed after row at time (t-1) and the rules of the reversible automata are applied according to Table 3. The reversible operation is applied and then the initial states is obtained. In Fig. 1, the reversible steps are shown in gray color.

V. PROPOSED IMAGE CRYPTOGRAPHY

The proposed method for image cryptography is based on reversible CA. In this method, two one-dimensional reversible CA and one elementary CA are used. The cryptography algorithm is described below:

Step 1: Two rows of input image are read and m (determined by user) number of pixels are selected from two rows. (In Table 2 m is set 2).

Step 2: These pixels in each row are placed in binary way according to its values.

Step 3: According to K that was determined by user binary string in step 2 is divided into k parts. (In table 2 with k=2 the string is divided in 2 parts.)

Step 4: Two produced binary strings are considered as input of reversible CA, and cryptography of numbers is performed by the CA. The output of this step consists of numbers in two times of t and (t-1).

Step 5: In step 4 substituted procedure is performed. Then, in this step the scrambling procedure is applied on the output of previous step by elementary CA for random value generation. Binary strings are connected to each other as output.

Step 6: Generated data in step 5 feeds as input of another reversible CA and encryption is done.

Step 7: In last step, two outputs are generated for two times of (t) and (t-1), which are the encrypted values of pixels. These values are stored in the encrypted matrix, as shown in Table 4.

In the decryption step, the above steps are applied reversely. Using the encrypted image and the key given as encrypted matrix in time (t-1), the image can be decrypted reversely according to the algorithm. One example of an iteration of 7 steps is shown in Table 4.

Table 4. Values of the Correlation of Cameraman with Rule 98.

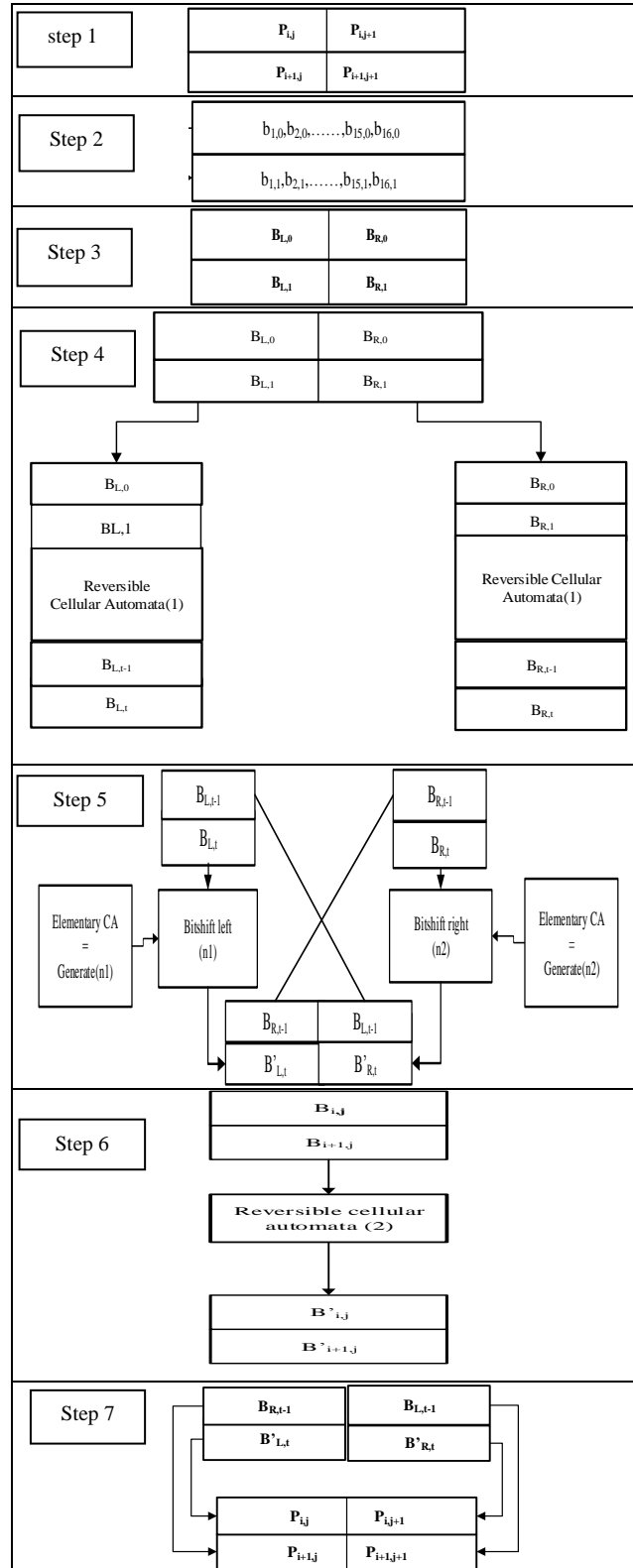| Correlation	diagonal	vertical	horizontal
Original image	0.9373	0.9546	0.9562
[20]	0.0114	-0.0383	-0.0369
[21]	-0.0178	0.0149	0.0122
[22]	0.0068	-0.0176	-0.0116
[23]	0.0113	0.0337	-0..204
Proposed method	-0.000067	-0.0015	0.0012

Fig.2. Proposed Method.

VI. EXPERIMENTAL RESULTS

The results of implementation on cameraman and boats images at sizes of 256×256 with different keys are shown. Fig. 3 to 5 illustrate the original, encrypted and decrypted image of cameraman with rules 30, 98, and 153, respectively.

To illustrate the sensitivity of the algorithm to keys in Fig. 6, we tried to decrypt the encrypted image with rule 98 with another key. As it is seen, decryption was not done correctly and the image is completely inaccurate. In

Fig.7 to 9, this algorithm has been applied to the image of   boats and the results are shown.
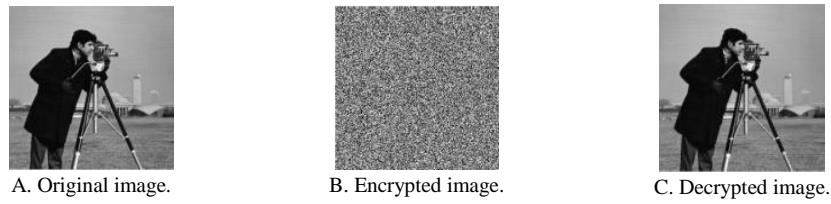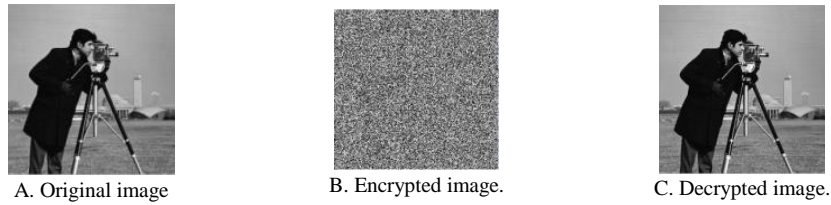
A. Original image.   B. Encrypted image.   C. Decrypted image.

Fig.3. Output Results of Proposed Algorithm With Rule 30.

A. Original image   B. Encrypted image.   C. Decrypted image.

Fig.4. Output Results of Proposed Algorithm With Rule 98.

A. Original image.   B. Encrypted image.   C. Decrypted image.

Fig.5. Output results of proposed algorithm with rule 153.
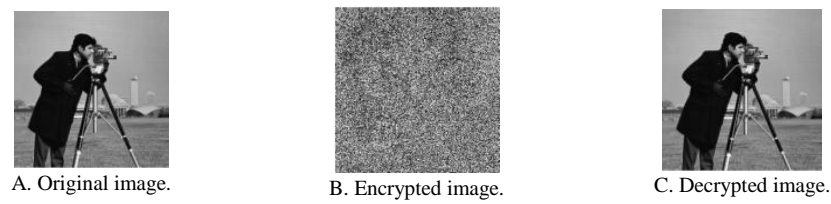
A. Encrypted image with rule 98.   B. Decrypted image with rule 153.

Fig.6. Output results of proposed algorithm with rule 98.
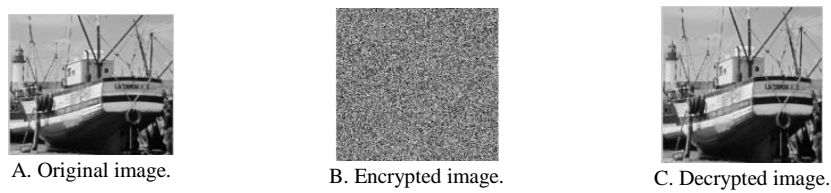
A. Original image.   B. Encrypted image.   C. Decrypted image.

Fig.7. Output results of proposed algorithm with rule 30.

A. Original image.   B. Encrypted image.   C. Decrypted image.

Fig.8. Output results of proposed algorithm with rule 98.

A. Original image.   B. Encrypted image.   C. Decrypted image.
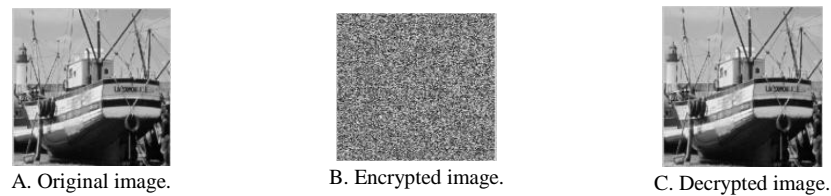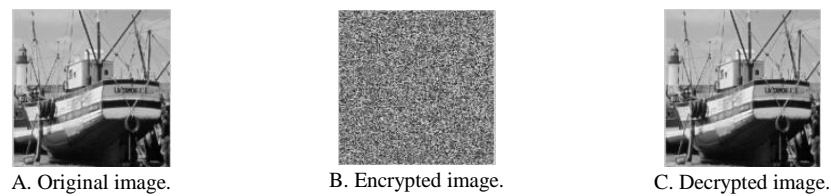
Fig.9. Output results of proposed algorithm with rule 153.

VII. ANALYSIS AND EVALUATION OF PROPOSED METHOD

In this paper, we examined the proposed scheme with [20-23]. In the following, you will see the evaluation of our method in comparison with those methods.

A. Statistical Analysis

According to Shannon's theory, attackers can decrypt encrypted image by using statistical analysis. The cryptography algorithm should be such that it will increase the difficulty of statistical analysis. Histogram analysis and correlation coefficients are used to evaluate statistical analysis [22].

A. Original image.   B. Histogram.

C. Encrypted image by rule 98.   D. Histogram.

C. Encrypted image by rule 153.   F. Histogram.

Fig.10. Output Results of Proposed Algorithm with Rule 153.

A. Original Image.   B. Histogram.

C. Encrypted image by rule 98.   D. Histogram.
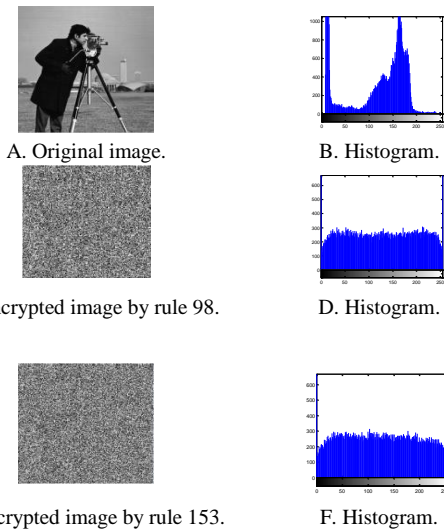
E. Encrypted image by rule 153.   F. Histogram.
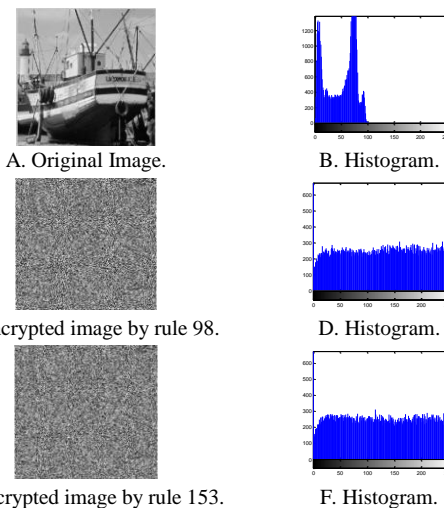
Fig.11. Output Results of Proposed Algorithm With Rule 153.

1. Histogram analysis

A cryptography algorithm is suitable when the image is encrypted in a way that no information is seen from the original image. In other words, the image must not be visually recognizable in cryptography. As the result of the visual test varies from one viewer to another, a histogram analysis can be used. Histogram analysis describes the distribution of the pixels in the image by plotting the number of observations at brightness intensity.

Histogram of original and encrypted images of two cameraman and boats images is shown in Fig. 10 and Fig. 11, respectively. As seen in the figures, the histogram of the encrypted images is uniform and then it is suitable.

2. Correlation coefficients analysis

Another evaluation criterion for statistical analysis is correlation. As the correlation of adjacent pixels in the encrypted image is less, the performance of the algorithm would be more suitable [22].

To evaluate the correlation of pixels in horizontal, vertical and diagonal direction, we use (1). In this equations, x and y are brightness of two adjacent pixels in image and N is the number of pixels selected from image. The values of the correlation in three vertical, horizontal and diagonal directions for the cameraman image and its encrypted images with rules 98 and 153 with four algorithms introduced by [20-23] and the proposed algorithm are shown in Tables 4 and 5, respectively. Based on values, as expected, the pixel correlation of the original image is high. In the encrypted images, this value is reduced and the pixels are less dependent on each other. In the proposed method, this value is less than the other methods, indicating that the proposed method has better performance than others.

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{1}$$

$$\text{cov}(x, y) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))(y_j - E(y)) \tag{2}$$

$$E(x) = \frac{1}{N}\sum_{j=1}^{N}x_j \tag{3}$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))^2 \tag{4}$$

Table 5. Values of the Correlation of Cameraman with Rule 153.

Correlation	diagonal	vertical	horizontal
Original image	0.9212	0.9536	0.9489
[20]	0.0410	-0.0641	-0.0632
[21]	0.0432	-0.0635	-0.0604
[22]	0.0017	-0.0227	-0.0219
[23]	0.1368	0.2562	0.1541
Proposed method	-0.0015	-0.0052	-0.0166

B. Sensitivity analysis

An ideal property for an encrypted algorithm is sensitivity to small changes in the original image and keys. Three criteria of UACI, MAE, and NPCR are used to test the effect of changing an input pixel on the encrypted image. As these three criteria are higher, the cryptography algorithm would have more efficiency (Kanso and Ghebleh 2012).

Equation 5 introduced mean absolute error [1]. In this equation, $C(i, j)$ and $P(i, j)$ are the pixel values of the encrypted image and the original image, respectively.

Equation 6 shows the calculation of NPCR, which measures the percentage of different pixels between two cipher images whose plane images have only one pixel difference. C_1 and C_2 are two different cipher images whose corresponding plaintext images differ by only one bit [8,20].

The *UACI* is illustrated in 8. It measures the average intensity of differences between two cipher images.

Table 6 shows the values of the evaluation criteria for the algorithms introduced by [20-23] and proposed algorithm with rule 153. From table, we can see that the values for the proposed method have the highest value compared to others; that is, the tiny change of pixel in the original image causes great change in encrypted image.

$$MAE = \frac{1}{M \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} \left| C(i, j) - P(i, j) \right|. \quad (5)$$

$$NPCR = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} D(i, j)}{M \times N}. \quad (6)$$

$$D(i, j) = \begin{cases} 0 & if \quad C_1(i, j) \equiv C_2(i, j) \\ 1 & if \quad C_1(i, j) \neq C_2(i, j) \end{cases} \quad (7)$$

$$UACI = \frac{1}{M \times N} \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} C_1(i, j) - C_2(i, j)}{255} \quad (8)$$

Table 6. Values of the MAE, NPCR and UACI

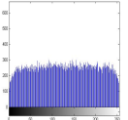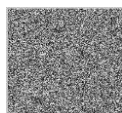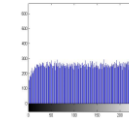| Ref.	MAE	NPCR	UACI
[20]	39.572	49.3057	15.0151
[21]	38.6359	49.4232	13.8246
[22]	74.4251	49.2706	9.6542
[23]	40.8497	50.0253	15.0241
Proposed method	44.7147	50.2045	17.3348

C. Entropy analysis
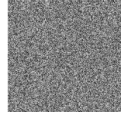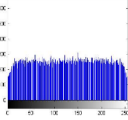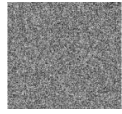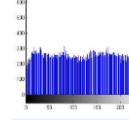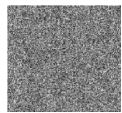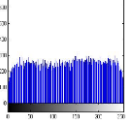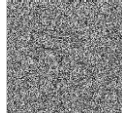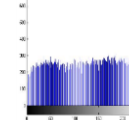
Entropy is another important characteristics of the randomness of the algorithm. Entropy is calculated according to 9., where $P(m_i)$ is the number of occurrences of m_i. In an ideal state, for an encrypted image, which each pixel of it is 8 bits, this value should be about 8 [22]. Table 7 shows entropy values for mentioned methods.

$$H(m) = \sum_{i=0}^{2^N - 1} P(m_i) \times \log_2 \left[\frac{1}{P(m_i)} \right] \quad (9)$$

Table 7. Values of Entropy.

Methods	Proposed method	[20]	[21]	[22]	[23]
Entropy	7.9892	7.9322	7.4259	7.2992	7.9253

Table 8. Key Sensitivity Analysis.

Original key		Slightly changed keys	
Encrypted image	Histogram	Encrypted image	Histogram

D. Key sensitivity analysis

Key sensitivity is one of the essential characteristics for a cryptography algorithm. This means that changing a bit in the private key should produce a completely different encrypted image. The high sensitivity to the key guarantees the security of the cryptography system against Brute-force attack. To evaluate the characteristics of sensitivity to the key, the original image is encrypted with the one secret key, then, the key is slightly changed and the original image is re-encrypted. If the comparison of these two encrypted images is not possible visually, the encryption algorithm would have high sensitivity to the key.

Table 8 shows the result of the sensitivity to key test. In order to detect the difference of encrypted images, histogram of the images has been plotted to make their comparison easier.

E. Key space analysis

In order to prevent brute-force attack, the key space of the cryptography algorithm should be large enough. The key space of the algorithm contains the total number of available keys in the cryptography algorithm. As the key space of cryptography is larger, the time to test all keys would increase, so it would be resistant to brute-force attack. In the proposed algorithm, four automata are used. Due to the fact that in each automaton, 2^8 rules can be used, the key space is $2^8 \times 2^8 \times 2^8 \times 2^8 = 2^{32} = 4294967296$, so proposed structure is immune to brute-force attack.

F. Implementation analysis

The performance of a cryptography system is evaluated based on various factors such as reliability against various attacks, computational complexity and cryptography time. In the previous sections, it was observed that the proposed algorithm had a good performance against various attacks. In this section, computational complexity and algorithm implementation time are discussed. The proposed algorithm is performed in three steps and includes various operations, including production of random numbers, linear calculations of CA, shifting, and bit XOR. All of these operations have direct implementation. Therefore, the proposed algorithm is efficient computationally.

VIII. CONCLUCION

CA is a useful tool for cryptography. Due to the randomness of the CA, the image can be encrypted with high quality. The reversible CA also has the capability to introduce reversible cryptography techniques on the image. The proposed method uses reversible CA to encrypt the image. In this article, a new structure for image cryptography is introduced, which encrypts the image in three steps. The results of the application of this algorithm on the image compared with the methods introduced in [20-23] by evaluation criteria such as UACI, MAE, and NPCR. The results show that this method has better performance.

REFERENCES

[1] Jolfaei, A. Mirghadri, "A novel chaotic image encryption scheme using chaotic maps," *ADST Journal*, vol. 2, 2011, pp. 111-124.

[2] T.Kumar, S. Chauhan, "Image cryptography with matrix array symmetric key using chaos based approach" *International Journal of Computer Network and Information Security*, vol. 11,2018, p.60.

[3] D.Mewada, N. Dave, and R.K. Prajapati, "A Survey: Prospects of Internet of Things Using Cryptography Based on its Subsequent Challenges," *Australian Journal of Wireless Technologies, Mobility and Security*, vol. 1, 2019, pp.28-30.

[4] S.S. Moafimadani, Y. Chen, and C. Tang, "A New Algorithm for Medical Color Images Encryption Using Chaotic Systems," *Entropy*, vol. 21,2019, pp. 577.

[5] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons & Fractals*, vol. 29, 2006, pp. 393-399.

[6] X. Xian, J. Liu, "Application of Chaos Theory in Incomplete Randomized Financial Analysis," vol. *2*, 2019, pp.3-5.

[7] A. Ding, W.Q. Yan, and D.X. Qi, "Digital image scrambling technology based on Arnold transformation" *Journal of Computer-aided design & Computer Graphics*, vol.4, 2001, pp. 338-341.

[8] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools and Applications,* 2019, pp.1-21.

[9] Z.H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, 2005, pp. 153-157.

[10] D.A. Guardeno, "Framework for the Analysis and Design of Encryption Strategies Based on Discrete-Time Chaotic Dynamical Systems," *Doctoral Thesis, Universidad Politecticnica De Madrid*, 2009.

[11] J. Von Neumann, "Theory of self-reproducing automata," *University of Illinois Press*, 1966.

[12] J. Jin, Z.H. Wu, "A secret image sharing based on neighborhood configurations of 2-D cellular automata," *Optics & Laser Technology*, vol.44, 2012, pp.538-548.

[13] M. Ahangaran, N. Taghizadeh, and H. Beigy, "Associative cellular learning automata and its applications," *Applied Soft Computing*, vol. 53, 2017, pp.1-18.

[14] Z. Eslami, S. Razzagh, and J. Zarepour Ahmadabadi, "Secret image sharing based on cellular automata and steganography," *Pattern Recognition,* vol. 43, 2010, pp. 397-404.

[15] P.L. Rosin, "Image processing using 3-state cellular automata," *Computer Vision and Image understanding,* vol. 114, 2010, pp. 790-802.

[16] Kauffmann, N. Piché, "Seeded ND medical image segmentation by cellular automaton on GPU," *International Journal of Computer Assisted Radiology and Surgery*, vol.5, 2010, pp.251-262.

[17] Z. Eslami, J. Zarepour Ahmadabadi, "A verifiable multi-secret sharing scheme based on cellular automata," *Information Sciences*, vol0180, 2010, pp. 2889-2894.

[18] Y. Ruisong, L. Huiliang, "A novel image scrambling and watermarking scheme based on cellular automata," *International Symposium on Electronic Commerce and Security*, 2008, pp.938-941.

[19] F. Qadir, M. Peer, and K. Khan, "Digital image scrambling based on two dimensional cellular automata,"

International Journal of Computer Network & Information Security, vol.5, 2013, pp. 36-41.

[20] J. Jin, "An image encryption based on elementary cellular automata" *Optics and Lasers in Engineering*, vol. 50, 2012, pp. 18396-1843.

[21] A. Abdo, S. Lian, L. Ismail, M. Amin, and H. Diab, "A cryptosystem based on elementary cellular automata" *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, 2013, pp. 136-147.

[22] X. Wang, D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol.18, 2013, pp. 3075-3085.

[23] F.K. Mohamed, "A parallel block-based encryption schema for digital images using reversible cellular automata," *an International Journal of Science and Technology*, vol. 17, 2014, pp. 85-94.

[24] S. Wolframe, "Theory and Application of Cellular Automata" *Singapore: World scientific Publishing*, 1986.

[25] M. Esnaashari, M. Meybodi, "A novel clustering algorithm for wireless sensor networks using irregular cellular learning automata*" in International Symposium on Telecommunications*, 2008, pp. 330-336.

[26] S. Roy, "A study on delay-sensitive cellular automata*," Physical A: Statistical Mechanics and its Applications,* vol. 515, 2019, pp.600-616*.

[27] M. Medenjak, V. Popkov, T. Prosen, E. Ragoucy, and M. Vanicat, "Two-species hardcore reversible cellular automaton: matrix ansatz for dynamics and no equilibrium stationary state," *arXiv preprint arXiv,* 2019, pp.1903.10590.

[28] S. Yingri, Y. Wo, and G. Han, "Reversible cellular automata image encryption for similarity search," *Signal Processing:Image Communication* 72, 2019, pp. 134-147.

Authors' Profiles

Alimohammad Latif obtained his first degree in electronic engineering from Isfahan University of Technology in 1993 and his M. Sc. in electronic engineering from Amirkabir University of Technology in 1996. In 2001, he joined the academic staff at electrical engineering department of Yazd University. He worked as a Ph. D. candidate at university of Isfahan where he obtained his Ph. D. in 2011, he joined the academic staff at computer department of Yazd University. His research interests are digital Image Processing, watermarking and cryptography.

Zeinab MEHRNAHAD receives her first degree in computer engineering from Yazd University in 2012. she graduated as M.Sc. of computer engineering from Yazd University, Iran in 2014. Now, she is PhD Student in Computer Science in Yazd University, Iran. Her research interests are Image processing and cryptography.