International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 25 No. 1 Jun. 2016, pp. 299-307

http://www.ijisr.issr-journals.org/

A Novel Image Encryption Scheme Using Chaos and Hybrid Cellular Automata

S. Hanis and R. Amutha

ECE, SSN College of Engineering, Chennai, India

ABSTRACT: This paper presents a novel image encryption scheme based on cellular automata (CA) and chaotic logistic mapping. The logistic chaotic mapping is used for shuffling the pixels which results in permutation. This permuted image is converted into a binary stream image where each rows of the image are converted into binary streams. Then a hybrid cellular automata (HCA) is used to provide diffusion by local interaction of the adjacent bits by applying various CA rules in the permuted image and confusion is brought by the cellular automata rules and keys from pseudo random number generator. In this scheme both reversible and irreversible cellular automata are used where irreversible cellular automata are used as a Pseudo Random Number Generator (PRNG) and reversible CA is used for diffusion. The properties of the encrypted image such as entropy, correlation coefficients, histogram, key space and key sensitivity prove that the encryption scheme is highly robust against attacks and also reliable in transmission loss scenarios.

KEYWORDS: Diffusion, Encryption, Decryption, Logistic Mapping, Cellular Automata.

1 INTRODUCTION

Due to transmission or storage of images in internet the security of such data from impostors and online intruders is necessary. Thus various image encryption scheme have been used in the history where scan based methods, transform based methods and chaos based methods are predominant. In recent years, cellular automata have been in use for encrypting 1D, 2D and 3D data due to its simple linear structure and chaotic behavior. Cellular automata based encryption schemes have shown better performance in terms of robustness and information security due to its confusion and diffusion property. There are two types of cellular automata namely reversible and irreversible. In reversible CA, it is possible to retrieve back to the original state from the updated state by backward iteration whereas in irreversible CA we cannot get back to the original state after updating by the forward iteration. It also provides data integrity due to its reversible behavior. Further logistic mapping based permutation essentially reduces the correlation of the permuted binary stream image which is given to CA for encryption which results in better performance characteristics.

In this paper the basic overview of cellular automata in image encryption is discussed in section II followed by introduction to chaotic logistic mapping in section III and in section IV the proposed encryption and decryption scheme is explained and followed by various performance analysis of the cipher image in Section V.

2 CELLULAR AUTOMATA

Cellular automata is a rectangular grid of cells where both time and space are discrete i.e. the states and the size of the cells are finite. The relationship between the adjacent cells is defined locally by a rule. A new generation of the cells is updated according to a fixed rule depending on the current state of the cell and the states of its neighborhood.

In this paper, reversible CA is used in order to preserve the information during the forward iteration. Irreversible CA is used in the key generation phase. This cryptosystem uses 1-D CA and chaotic logistic mapping so that features such as high speed and large key space are obtained.

Corresponding Author: S. Hanis

3 CHAOTIC LOGISTIC MAPPING

The logistic map exhibits complex chaotic behaviour and can be expressed mathematically as given in equation (1).

$$Xn+1 = \mu\, Xn\, (1-Xn) \quad (1)$$

Here X_n is a number between zero and one. The $\mu=4$ case of the logistic map is a nonlinear transformation of both the bit-shift map and the $\mu=2$ case of the map. The behavior of the logistic map is dependent on μ which is a constant, the map produces complex relationship between the present and next state when $3.5699456<\mu<4$.

4 ENCRYPTION SCHEME

The proposed encryption scheme uses chaotic Logistic mapping as a tool for pixel shuffling, irreversible CA for key generation and reversible CA during diffusion process.

4.1 CHAOTIC LOGISTIC MAPPING

In this paper, initially we use the logistic chaotic mapping for permutation of original image's pixel locations. Thus the adjacent pixels have no relationship between them bringing down their correlation. The scheme can be explained as follows:

Step 1: Get the size of the input grayscale image i.e., number of rows and columns.
Step 2: Convert these row and column index to floating point values (K_r, K_c) by dividing the index by their maximum values.
Step 3: Subtract a constant value (0.007 & 0.003 for row & column index in our algorithm) from these floating values to break the symmetric property obtained due to logistic mapping technique.
Step 4: Let μrow=3.712381 & μcol=3.579703 be the constants which produces chaotic behavior between the next state and the present of a pixel location.
Step 5: Iterate the row and column index according to the rule given in (1) to get K'_r and K'_c. Let iteration number be a prime number greater than 256 for the result to be chaotic.
Step 6: Sort the values K'_r& K'_c and find their index and match them.

4.2 CELLULAR AUTOMATA DIFFUSION

A reversible CA can be regarded as an information processing unit. Here, R_i R_j {00; 01; 10; 11} are control bits which determine the selection of cellular automata rules as shown in Table 1. Two initial configurations of the reversible CA C(0), C(1) are viewed as the inputs, while the outputs are the two final configurations C(d), C(d+1), which are obtained after d times forward iteration of the reversible CA. We refer to this processing unit as an elementary block of our image cryptosystem.

Initially we convert the permuted image I'_{MxN} into rows of binary sequences to obtain the binary stream image B_{MxN}. Here, N is even. If not, a random row of pixels could be added at the end of the image. The length of each binary sequence is L =M X T bits, where T is the number of bits per pixel. In our encryption scheme there are two rounds of encryption. The key K_1 and rule selectors r_1 are used for first round while key K_2 and rules r_2 are selected for second round. We obtain a good performance by the encryption scheme. The encryption scheme is shown in Fig.1.

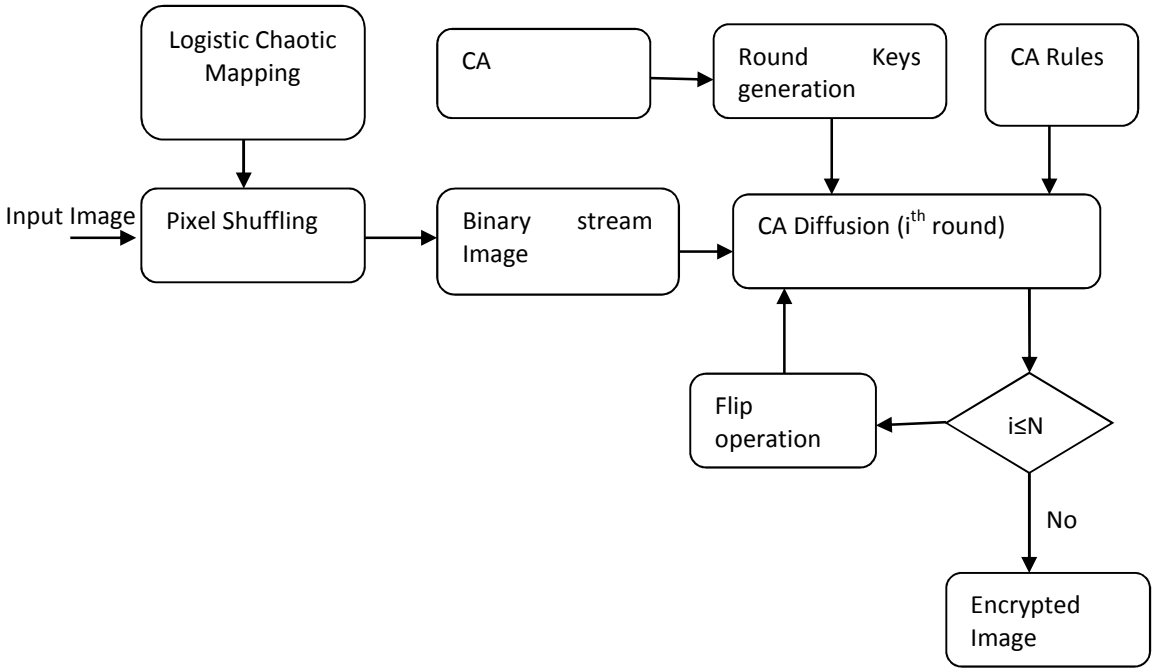


Fig.1. Block Diagram of Encryption Scheme

Table 1 Cellular Automata Diffusion Rules

Group	CA Rule	R_iR_j
Group 1	$e_j^{t+1}=e_{j-1}\oplus e_j\oplus e_{j+1}$	00
	$e_j^{t+1}=e_{j+1}\oplus e_j\oplus e_{j-1}$	01
	$e_j^{t+1}=e_{j-1}\oplus e_j\oplus e_{j+1}$	10
	$e_j^{t+1}=e_{j-1}\oplus e_j\oplus e_{j+1}$	11
Group 2	$e_j^{t+1}=e_{j-1}\oplus e_j\oplus e_{j+1}$	00
	$e_j^{t+1}=e_{j-1}\oplus e_j\oplus e_{j+1}$	01
	$e_j^{t+1}=e_{j-1}\oplus e_j\oplus e_{j+1}$	10
	$e_j^{t+1}=e_{j-1}\oplus e_j\oplus e_{j+1}$	11

The first round:

Step 1: Take first two rows of binary stream image and key K1 and XOR them to get C1 and C2. Iteratively apply the CA diffusion rule selected according to first two rows values of r1 to obtain C`1 & C`2. Then again XOR C`1 & C`2 with first two rows of key K1.

Step 2: Take the third and fourth rows of the binary stream image and XOR with next two rows of key K1 and previous two encrypted rows. Then similarly apply iterative CA rule depending on third and fourth rows of rule selector r1. Then again XOR with key and previous two rows if the encrypted matrix. Repeat the step 2 until step N/2.

The second round:

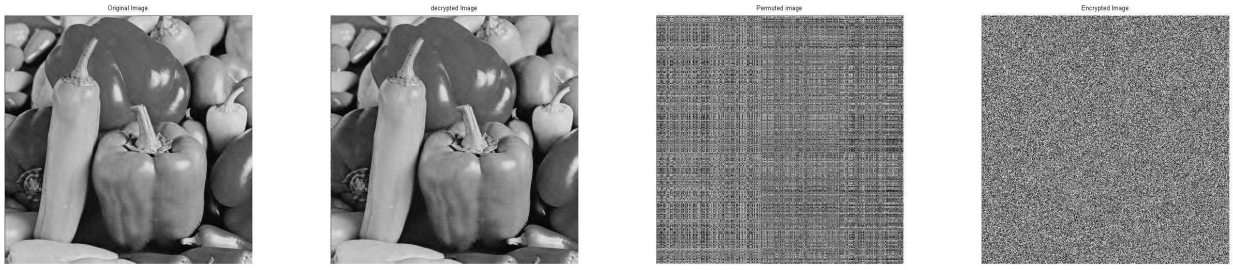
Then flip the first round encrypted matrix upside down and perform the steps similar to first round with key K2 and rule selector r2. The encrypted matrix is converted back to decimal values ENC_{MxN} from binary streams.

4.3 DECRYPTION SCHEME

This scheme is a symmetric encryption algorithm thus the keys and rule selectors have to be known at the decryption side. The decryption is the exact reverse procedure of encryption which also has two rounds. The key K_2 and rule selector r_2 for first round while key K_1 and r_1 for the second round. Initially convert the encrypted image ENC_{MxN}.

Step 1: Take the last two rows of the encrypted matrix and key K2 along with previous two rows of encrypted matrix and XOR them. Then apply the iterative CA rule selected based on r2. Then again XOR the iterated value with key K2 last two rows and previous two rows of the encrypted matrix. Repeat this step similarly for all rows.

Step 2: Flip the matrix after first round of decryption and apply key K1 and rule selector r1 similar to the first round to obtain the decrypted matrix DEC_{MxN}. The original image peppers 512 x 512 encrypted by our scheme are shown in Fig.2.



(a) (b) (c) (d)

Fig.2. (a) Original image Peppers 512 x 512, (b) Permuted image, (c) Encrypted image, (d) Decrypted image

5 PERFORMANCE ANALYSES

Any encryption algorithm is graded based on its certain performance parameters. To test the security, complexity and chaotic nature of the encrypted image, analyses such as entropy analysis, histogram analysis, correlation coefficient analysis, key space analysis, statistical analysis, key sensitivity analysis and robustness analysis are performed.

5.1 KEY SPACE ANALYSIS

The key space refers to the set of all possible keys that can be used in the cipher system. In our proposed encryption algorithm, the relatively short key (secret seed) shared by the transmitter and receiver is expanded to form the sufficient long keys (reversible CA rules) by a secure PRNG. This would make different non-affine and balanced rules are used in each sub-round encryption, which greatly enhance the security of the algorithm.

The length of the secret seed adopted in our key expansion algorithm is 256-bit, so the key space is 2^{256} is expanded using reversible CA so the key space becomes $2^{256x256x2}$ which is sufficient large to prohibit exhaustive search of the key space. Further the iteration number, CA rules used, logistic mapping μ values increase the key space.

5.2 INFORMATION ENTROPY ANALYSIS

Information entropy is regarded as the most important feature of randomness. The information entropy H (m) of a source is calculated by the following formula:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad (2)$$

$p(m_i)$ is the probability of symbol m [14]. The entropy was calculated for different images with different sizes. For peppers image of size 512 x 512, the cipher image had entropy of 7.9993 which means it is less possible for our cryptosystem to divulge information. The entropy was also calculated different low frequency and high frequency images in Table 2. The entropy is compared with ping method [14] and Wang method [17] as given in Table 3.

Table 2 Entropy Analysis

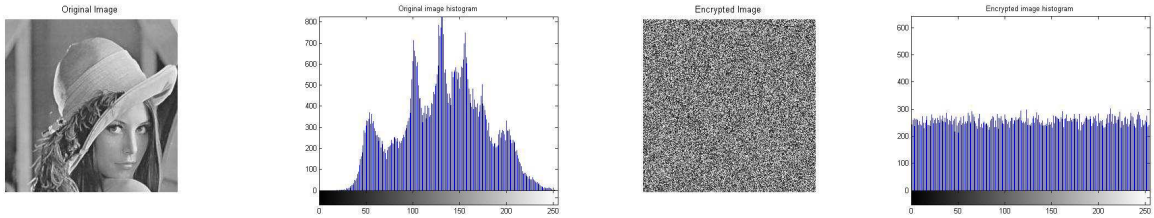
Image	Entropy Values	
	Original Image	Encrypted Image
Lena 256x256	7.4328	7.9974
Baboon 256x256	6.6962	7.9972
Peppers 512x512	7.5867	7.9994
Cameraman 512x512	7.0480	7.9994

Table 3 Entropy Comparison

Method	Entropy	
	Lena (256 x 256)	Peppers(512 x 512)
Our Method	7.4328	7.9994
Ping Method [14]	7.9970	7.9994
Wang Method [17]	7.9969	7.9993

5.3 HISTOGRAM ANALYSIS

The histogram plot is the graphical representation of the distribution of the gray values of an image where the x-axis represents the gray values while the y-axis corresponds to its frequency. The histogram of the original grayscale image Lena of size 256 x 256 and its encrypted image are shown in Fig 3 from which we can see that the histogram of the encrypted image is flat where there is equal probability of occurrences of all gray values. Thus our encryption scheme can be robust against brute force attack and dictionary attacks.



(a) (b) (c) (d)

Fig. 3. (a) Original image, (b) Original image histogram, (c) Encrypted image, (d) Encrypted image histogram

5.4 NIST STATISTICAL ANALYSIS

The randomness of the output sequence is one of the criteria to evaluate the security of cryptographic algorithms. Although various kind of randomness tests have been proposed so far, there is no known sequences generated by an algorithm which pass all the randomness tests. One of the most popular randomness tests is the SP800-22 published by the National Institute of Standards and Technology (NIST).

The SP800-22 provided a statistical test suite (STS) consisting of 15 tests. These tests focus on a variety of different types of non- randomness that could exist in one sequence. For each test, the default significance level α=0.01 was used for the analysis of P-value obtained from various tests. For P-value$_T \geq 0.0001$, the sequences are considered to be uniformly distributed. NIST statistical test results prove that the results of this scheme have passed all the 15 tests as shown in Table 4. Thus the encryption scheme is statistically highly random which is highly tedious for any impostor to decrypt the information without knowing the keys by exhaustive search and brute force attack.

Table 4 NIST Statistical Analysis

Statistical Test	P-value	Proportion
Frequency	0.657933	.99
Block Frequency	0.514124	.99
Runs	0.366918	1
Longest runs of ones	0.637119	.96
Rank	0.202268	.98
Spectral DFT	0.897763	1
Non-overlapping templates	0.419021	.99
Overlapping templates	0.171867	.98
Maurer's Universal	0.075719	1
Linear Complexity	0.637119	1
Serial	0.719747	1
Approximate entropy	0.494392	.97
Cumulative ums(Forward)	0.350485	.99
Random excursions	0.213309	1
Random excursions variant	0.911413	1

5.5 CORRELATION OF TWO ADJACENT PIXELS

In general, adjacent pixels of most natural images are highly correlated. An effective encryption scheme should produce the cipher image with sufficiently low correlation of adjacent pixels. To test the correlation between horizontally, vertically, and diagonally adjacent pixels in the image the following procedure is carried out. First, we select N pairs of two adjacent pixels from an image. Then, we calculate the correlation coefficient by using the standard formulas.

The horizontal, vertical and diagonal correlation coefficients of the original and encrypted image are shown in Table 5 from which we can see that the correlation coefficients of the encrypted image are very low. Thus adjacent pixels in the encrypted image are highly uncorrelated.

The correlation coefficients plot of the original and encrypted image is shown in fig. 4. from which we can see that the coefficients are spread throughout the pixel range for the encrypted image.

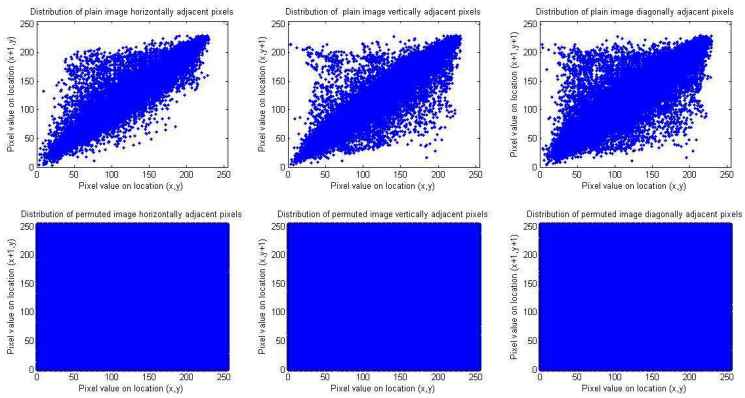


Fig .4. Correlation Coefficient Plot of original & encrypted image

Table 5 Correlation Coefficients Analysis

	Correlation Coefficient(Original Image)			Correlation Coefficient(Encrypted) Image)		
Image	Hori.	Vert.	Diag.	Hori.	Vert.	Diag.
Lena	0.9654	0.9354	0.8995	0.0012	0.0041	0.0008
Baboon	0.8368	0.8710	0.7841	0.0030	0.0007	0.0045
Peppers	0.9870	0.9834	0.9715	0.0008	0.0013	0.0021
Cameraman 512x512	0.9900	0.9832	0.9733	0.0021	0.0009	0.0019

5.6 DIFFERENTIAL ATTACK ANALYSIS

Generally the attacker can make as light change of the plain image and then observes the change of the result. Thus he may find out a meaningful relationship between the plain image and the cipher image. If one minor change in the plain image can cause a significant change in the cipher image with respect to diffusion and confusion then this differential attack would become very inefficient and practically useless. To test the influence of one image pixel change on the whole image encrypted by the proposed scheme two common measures were used: NPCR (number of pixels change rate) and UACI (unified average changing intensity).

Table 6 Differential Analysis

Image Name	NPCR (%)	UACI (%)
Lena	95.22	16.41
Mandril	89.41	14.67
Peppers	89.09	14.83
Cameraman	90.39	15.37

5.7 KEY SENSITIVITY ANALYSIS

An outstanding cryptosystem should not only be sensitive to plain text but also be sensitive to key. To evaluate the key sensitivity of our scheme, two tests have been performed. For the first key sensitivity test, the plain image is encrypted by using a 256 size seed key. Next, the seed key is changed by one bit and encrypts the same input image and then we compute the correlation coefficient between two cipher images. It is seen that original image can be well recovered with a correct key while a random-like image is obtained with a wrong key as shown in fig 5. This means that the proposed scheme has a high degree of sensitivity to the key.

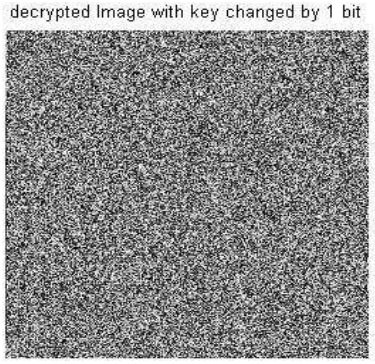
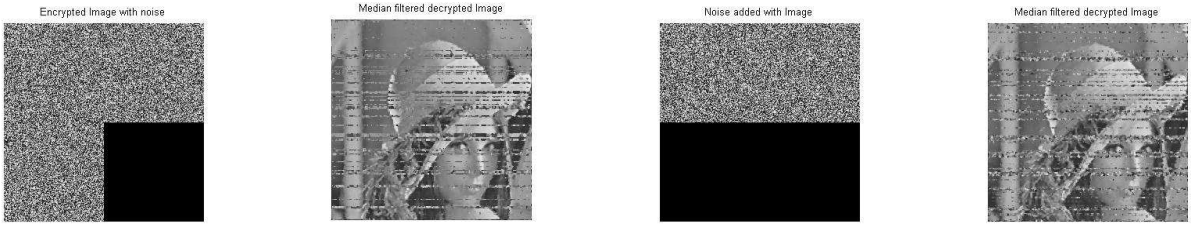


Fig.5 Key Sensitivity Analysis

5.8 ROBUSTNESS ANALYSIS

To testify the robustness of such image encryption scheme, we occlude i.e., replace some portion of the encrypted image with zeros and use the correct decryption key. Then we see the extent to which we can decrypt the image and the amount of information loss both visually and mathematically from Peak Signal to Noise Ratio (PSNR) between the original and the decrypted image. The ½ occluded and ¼ occluded encrypted images and their corresponding decrypted images are shown in fig .6. From the figure we can see that the information is not fully lost due to occlusion and we can obtain visually less information loss image with acceptable PSNR.



(a) (b) (c) (d)

Fig.6. (a) ¼ occluded encrypted image, (b) Decrypted image, (c) ½ Occluded image, (d) Decrypted image

6 CONCLUSION

We conclude that this encryption method has many vital applications as it can be implemented in hardware at a minimal cost since it involves linear operations which don't involve complex integration or transforms and as the rules are linear the algorithm is simple to implement in hardware. We can also see better performance results in various tests and analyses such as entropy, correlation and key space. Also, our algorithm exhibits better reliability without compromising the security and robustness against attacks.

REFERENCES

[1] A.A. Abdo, Shiguo Lian, I.A. Ismail, M. Amin, H. Diab, "A cryptosystem based on elementary cellular automata" , Elsevier, Science Direct, Commun Nonlinear Sci Numer Simulat,2013, vol.18, pp. 136–147.

[2] Atieh Bakhshandeh; Ziba Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata", Elsevier, Science Direct, Optics and Lasers in Engineering, 2013, vol.51, pp. 665–673.

[3] Barakat, M.L., Mansingka, A.S., Radwan.A.G,Salama.K.N, "Hardware stream cipher with controllable chaos generator for colour image encryption," Image Processing, IET, 2014, vol.8, pp.33, 43.

[4] Cilardo, A., Barbareschi, M., Mazzeo, A., "Secure distribution infrastructure for hardware digital contents," Computers & Digital Techniques, IET, 2014, vol.8,issue no.6, pp.300-310.

[5] Dalhoum, A.L.A., Mahafzah, Awwad, Aldhamari, I. "Digital Image Scrambling Using 2D Cellular Automata", Multimedia, IEEE, 2012, vol.19, issue 4, ISSN: 1070-986X, pp 28-36.

[6] Faraoun Kamel Mohamed, "A parallel block-based encryption scheme for digital images using reversible cellular automata", Elsevier, Science Direct, Engineering Science and Technology, an International Journal, 2014, vol.17, issue 2, pp 85-94.

[7] http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

[8] Jeaneth Machicao; Anderson G. Marco; Odemir Martinez runo, "Chaotic encryption method based on life-like cellular automata", Elsevier, Science Direct, Expert Systems with Applications, 2012, vol.39, pp. 12626–12635.

[9] Jun Jin, "An image encryption based on elementary cellular automata", Elsevier, Science Direct, Optics and Lasers in Engineering, 2012, vol.50, pp. 1836–1843.

[10] Nanrun Zhou, Haolin Li, Di Wang, Shumin Pan, Zhihong Zhou,"Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform", Elsevier, Optics Communications, 2015, vol.343, pp. 10–21.

[11] V.Patidar, N.K.Pareek, G.Purohit, K.K.Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption", Elsevier, Optics Communication, 2011, vol.284, pp. 4331–4339.

[12] 12. Ping n, Feng Xu, Zhi-Jian Wang, "Image encryption based on non-affine and balanced cellular automata", Elsevier, Science Direct, Signal Processing, 2014, vol.105, pp. 419–429.

[13] Rong-Jian Chen; Shi-Jinn Horng, “Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata”, Elsevier, Science Direct, Signal Processing: Image Communication, 2010, vol.25, pp. 413–426.
[14] Rukhin, J. Soto, J. Nechvatal, S. Miles, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, 2010, NIST Special Publication 800-22 Revision 1a.
[15] Zefreh, E.Z., Rajaee, S., Farivary, M., “Image security system using recursive Cellular automata substitution and its parallelization”, Multimedia IEEE, 2011, vol.23, issue 2, ISSN: 978-1-61284-206-6, pp.77– 86.
[16] Zhang, Xuefeng; Fan, Jiulun, "Extended logistic chaotic sequence and its performance analysis," Tsinghua Science and Technology, 2007, vol.12, no.S1, pp.156-161.
[17] 17. Z.X. Wang, C. Jin “Image encryption using game of life permutation and PWLCM chaotic system”, Elsevier, Science direct, Optics Communication, 2012, vol. 285, pp. 412-417.