A Review on Encryption Techniques based on Cellular Automata

Eakta Kumari and Saurabh Mukherjee

Department of Computer Science, Banasthali Vidyapith, Banasthali, Rajasthan, India

Corresponding author: Eakta Kumari, Email: eaktayadav19@gmail.com

In this digital world, images are an important part of communication and while communicating security is a crucial problem. And to deal with security various image encryption techniques are based on the cellular automata. The study gives a basic introduction to cryptography and cellular automata and various encryption scheme based on cellular automata. Various performance measures related to the analysis of encryption techniques have been studied. And a comparison of encryption techniques based on the performance matrices is presented. The paper gives a concluding remark on the advancement in the field of image encryption.

Keywords: Cellular automata, Image encryption, Image encoding, Scrambling

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 225–234. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-24

1 Introduction

Now a days, Digital images have been extensively used in various fields Due to advancement in distributed computer networks, storage devices, and imaging tools[1], [2].and due to the communication over public networks, the data/ images are prone to various security threats such as, illegal modification, eavesdropping and duplication etc. Therefore, image security has received more attention from the past decade. The security of data can be done by two ways either by hiding the data termed as information hiding or by encrypting the data i.e., cryptography. The information hiding has further two branches i.e., watermarking and steganography and the two deals with hiding the existence of actual data from the intruders and the original information is available only to the intended recipient. But in case of cryptography, the original data is encoded into a form which seems to be meaningless before it is communicated over the network for transmission and after receiving at the recipient side it is again decoded back to the original form before the use. And various image encryption algorithms are used for this protection of data[3]–[5]. Encryption and decryption can be performed in two ways- symmetric key cryptography and asymmetric key cryptography. Encryption may be achieved by two types of ciphering schemes—stream cipher and block cipher as mentioned in[6].

General Model of Cryptography: A general procedure for any encryption technique is illustrated in figure 1. An input image or the plain image(P) that the sender needs to transmit over the network and encrypted image or ciphered image(C) is the encoded image obtained after applying the encryption algorithm on the plain image. The encryption process is carried out and demonstrated as:

$$C = EF_{EK}(P) \quad (1)$$

Here, C is the ciphered image obtained after applying the encryption function (EF) on the P using the encryption key (EK). And in the same manner the reverse process is carried at the receiver end to decrypt the ciphered image by the use of the decryption function (DF) using the decryption key (DK) as depicted in equation 2.

$$D = DF_{DK}(C) \quad (2)$$

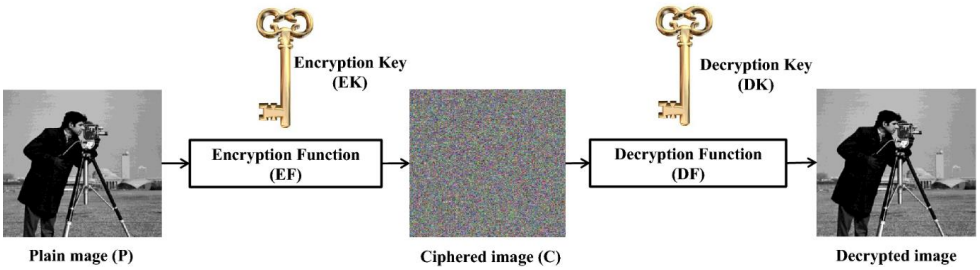

Figure 1 General Framework of Cryptography

In order to fulfill the security requirements, many encryption schemes have been proposed and analyzed as possible solution systems which include chaos[7]–[9], Scan[10], [11] and some other methods are available[12]–[15]. Each technique has their own merits and demerits in terms of pixel randomness of encoded image, key size, strength, security and size of input data. Nowadays, encryption using cellular automata is getting focus due to its parallel processing and easy implementation in hardware. There are some techniques that use cellular automata to encrypt images[16]–[19].

The basic idea behind image encryption can be divided into three broad categories: position permutation, value transformation and the combination of the two[16]. For the three categories cellular automata can be used in image encryption due to its robust nature it is inherently implemented in hardware. And it is computationally infeasible to find the exact key for generating the original information by the intruder due to large number of rules used to generate the secret key. Recursive cellular automata substitution demands only arithmetic and/or logic operations. Here in this article, we try to cover all the major techniques which uses the cellular automata as the base for image encryption. The full article is organised as section 2 is about the literature survey related to the cellular automata, section 3 gives the basic idea of cellular automata and its rules and section 4 consists of the various performance metrices used to check the applicability of an encryption technique and the comparison of various techniques is listed in section 5 and section 6 gives the conclusion of the article.

2 Literature Review

Cellular automata (CA) are discrete models of time and space which are capable of generating chaos. Cellular automaton was introduced by Ulam [20] and Von Neumann and came to the fore by S. Wolfram[21].CA evolution is governed by very simple rules. The benefits of parallel processing and direct implementation in hardware of CA make them an ideal choice for image encryption and are preferred over the use of chaotic maps in encryption systems[22]. An encryption technique based on Logistic map and chaotic cellular automata was proposed by Zhang and Luo (2012). Wang and Luan [23] proposed a new scheme for image encryption using the combination of chaotic map and reversible CA. In the two-stage technique of confusion and diffusion, the first stage makes use of chaotic map for key generation by dividing the image into units and 4 bits are used for each unit and the later diffusion stage considers only the higher bits which stores all the information about an image. For the second stage reversible CA is applied. Another encryption technique was proposed by Rey, Sanchez, and Cuenca [24] on cat chaotic map and cellular automata which makes the use of 2D chaotic map to implement the confusion phase and the reversible memory CA is used to implement the diffusion phase. In another study by Bakhshandeh and Eslami [25] a new technique for image encryption based on chaotic maps, CA, and permutation-diffusion architecture A piecewise linear chaotic map is used to permute the image in permutation phase. A secure image is obtained in the diffusion phase by diffusing the permuted image using logistic map and reversible memory CA. Ping et al.[26] proposed an image encryption scheme which uses the concept of diffusion and confusion with the help of CA. But here a random sequence is generated by CA for creating a scrambled image. Interaction between the local cells is used for diffusion process while confusion process is achieved by applying CA rules on these cells. An image encryption algorithm using chaotic map and ant cellular automata was proposed by Wang and Xu [27]. The integral imaging-based schemes have the ability to implement secure and strong cryptography and was proved by Li et al. [28] which makes the use of Hybrid Cellular Automata (HCA). Mohamed [29] uses CA to show parallelization in image cryptography. Here, the input image is decomposed into blocks and then each block is encrypted independently by the secret key and hence which makes it computationally fast as compared to other techniques. A hybrid model for image encryption which contains chaotic map, DNA, and CA was proposed by Enayatifar et al.[30]. In this algorithm chaotic map is used to select the rule number and the computational speed is poor. In another study quantum CA was used by Yang et al. [19] for image encryption and reported the less time complexity than the traditional quantum encryption technique. Li et al. [31] reported the use of CA and depth- conversion integral imaging for encryption. But this technique degrades the reconstruction process. A scheme which makes the use of Rule 30 is [32], and it can be applied in cryptography due to the randomness of numbers generated using rule 30 of CA. Chai et al.[33] proposed another encryption technique where the use of CA and DNA sequence are introduced and which generates the initial values of chaotic system and secret key using SHA-256 hash function. This scheme has the ability to resist noise and Known plaintext attacks (KPA). In the technique proposed by Yaghouti Niyat et al. [34] non-uniform CA is used to create the key-image and then random numbers are selected by hyper-chaotic mapping. But the encrypted results are only in horizontal patterns. Li et al. [22] tried to overcome this issue which uses CA pixel permutation methods to break the order of pixels and provide large key space and sensitive

towards secret keys. A novel image encryption algorithm based on cellular automata was proposed [35]. The scheme works on two phase permutation and diffusion phase. The scheme is robust against noise and KPA attacks. Another scheme which uses 2D cellular automata to encrypt the grayscale images was proposed [36] which uses Arnold's cat map for the image scrambling. In a recent scheme proposed by Zubair Jeelani [37] reported the use of two dimensional outer totalistic cellular automata (2D-OTCA) for the image encryption. The scheme [38] uses the RSA algorithm for key generation and quantum logistic map, CA for image encryption. A recent reported scheme [39] for the encryption of color images was implemented in three stages. First rule 30 of CA is used to generate the encryption key then permutation if performed in the second stage using S-box and in the last stage Lorenz map is used to generate the second encryption key. The security and robustness of the encrypted image is enhanced by the three-stage scheme. A brief comparison between CA based encryption techniques is presented in the table 2. Various performance measures are used to represent the efficacy and security of the scheme.

3 Cellular Automata Basics

A mathematical model of a system where only discrete values of inputs and outputs is considered is termed as cellular automata. It studies the sequential behavior of the interconnected cells (neighboring cells) arranged in a regular manner having a finite set of values is shown by CA. It grows in discrete time steps and the value taken by a particular cell for the next state is affected by the neighboring cell values at the current state using to a function known as the CA rule.

The value of each CA cell is computed by the local transition function denoted by the δ symbol. The transition function also known as CA rule considers the current cell state and state of neighboring cells at time t as an input and computes the value for the current cell for next step. Mathematically, a cellular automaton C can be expressed as a quintuple [40] as shown below:

$$C = (\Sigma, N, \delta, A, G\delta) \quad (3)$$

where, Σ is the finite set of states a CA cell may assume at any given time; N is the local neighborhood of a cell, where $N = \{c1, \ldots, ck\}$ is a CA lattice finite subset; δ: is the transition function to determine the next state of the cell; A is the configuration set; and, $G\delta$ is the global mapping.

Transition function (δ) to for computing the state of a current cell for the next step in elementary cellular automata (ECA) is defined as in Eq. (4).

$$C(i)_{t+1} = \delta\,(C(i-1)_t, C(i)_t, C(i+1)_t) \quad (4)$$

Every cell in ECA can assume either a 0 or 1 state at any given time and three stage CA. Therefore, there are 2^3 possible configurations and $2^8 = 256$ distinct next states. Each mapping represents a CA rule. There are a total of 256 rules [6].-A three variable Boolean function is used to represent Each number from 0-255 [41].

The most commonly used rule of CA is rule 30. The calculation of next state in rule 30 in 1D cellular automata is denoted by below equation:

$$S(i)_{t+1} = XOR\,[S(i-1), OR(S(i), S(i+1))] \quad (5)$$

current pattern	111	110	101	100	011	010	001	000
new state for centre cell	0	0	0	1	1	1	1	0

It is called Rule 30 because in binary, $00011110_2 = 30$.

Various other rules are also there like rule 90, rule 102, rule 110 which are represented in figure 2

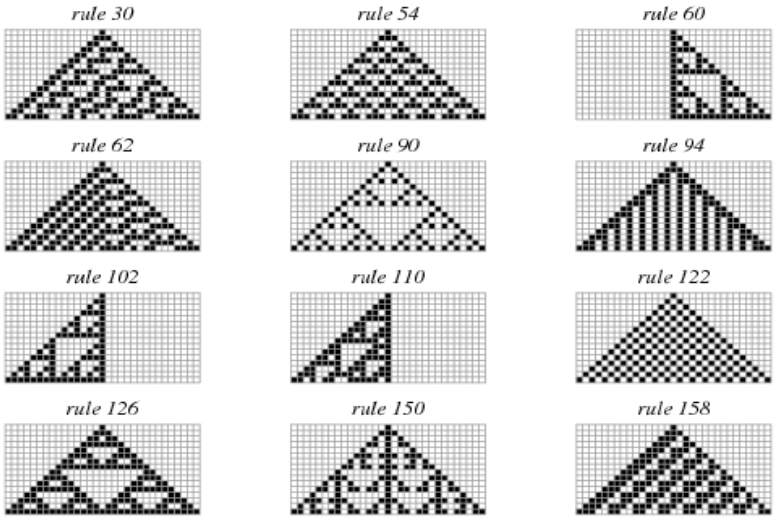

Figure 2 Various rules of Elementary Cellular Automata

4 Performance Metrices

The efficacy of a particular encryption techniques is confirmed by the analysis of various performance metrices which are listed in this section.

4.1 Number of Pixel Change Rate (NPCR): It is defined as the no of pixels change in the two encrypted images obtained from the original image and one pixel changed image from the original image. Higher the value of NPCR better is the encryption technique [42].

NPCR is computed using the below equation:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \quad (6)$$

$$D(i.j) = \begin{cases} 0, if\ E(i,j) = E1(i,j) \\ 1, if\ E(i,j) \neq E1(i,j) \end{cases} \quad (7)$$

$D(i,j)$ indicates the deviation of values of corresponding pixels of encrypted images of original image and changed original image. The changed image and original image have only one pixel difference. The range of NPCR is $[0, 100]$.

4.2 Unified Average Changing Intensity (UACI): As the name implies it measures the average of intensity difference between two encrypted images, obtained from the input images that have one pixel difference [43] and is computed as:

$$UACI = \frac{\sum_{i,j} E(i,j) - E1(i,j)}{255 \times W \times H} \times 100 \quad (8)$$

where $E(i,j)$ and $E1(i,j)$ are the encrypted images corresponding to original and changed images respectively. For an encryption scheme to produce better results the UACI has to be maximized.

4.3 Histogram Analysis (HA): To judge the quality of any encryption algorithm histogram analysis is done. If the histogram of encrypted image appears to be uniform in nature and is totally different

from the histogram of input image then that schemes is considered to perform better because it protects the leakage of information. Histogram of original image is always non- uniform in nature while the histogram of encrypted image is uniform which can also be observed from the figure 3 which represents the histogram of grayscale input image and encrypted image of cameraman.

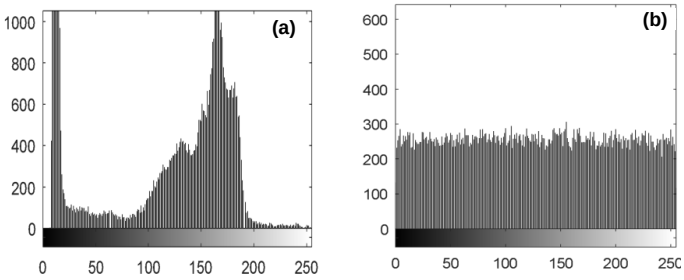

Figure 3 Histogram of grayscale image of cameraman (a) Input image; (b) Encrypted image.

4.4 Correlation Coefficient (CC) and Distribution: To check the similarity between the corresponding pixels of an original and encrypted image, correlation coefficient is computed. A strong correlation is there between the adjacent pixels of an original image in three directions, i.e., horizontal, vertical and diagonal while the correlation must be reduced in the encrypted image for a scheme to be considered good. Correlation coefficient can be computed as follows:

$$CC = \frac{cov(I(x,y), \mathrm{E}(x,y))}{\sigma(I(x,y))\sigma(\mathrm{E}(x,y))} \tag{9}$$

$$MSE = \frac{1}{N \times N} \sum_{x=1}^{N} \sum_{y=1}^{N} |f(x,y) - f'(x,y)|^2 \tag{10}$$

$$PSNR = 10 \times \frac{255^2}{MSE} \tag{11}$$

Peak Signal to Noise ratio (PSNR) and Mean square Error (MSE) are also used to check the performance of an encryption scheme which are defines by equation 10 and 11. For an efficient scheme the PSNR should be high and MSE should be minimum.

4.5 Information Entropy (IE): To measure the randomness of pixels in any image information entropy is used. High value of information entropy represents more randomness of pixels and the encryption techniques is assumed to be good to implement. To calculate the information entropy, the given below equation is used.

$$H(k) = \sum -p(k_i) log\ log\ p(k\_i\,) \tag{12}$$

where k is used to represent the information source and for representing the information entropy of k information source $H(k)$ notation is used and probability for every symbol k_i. is represented by $p(k_i)$. The value of IE tends to 8 for a good encryption technique.

Table 1 Comparison of Various Cellular Automata Encryption Techniques

Scheme/ performance metric	NPCR	UACI	KA	HA	CC	IE	NA	Speed
Chai et.el. [33]	Y	Y	Y	Y	Y	Y	Y	Good
Li et.el. [28]	N	N	N	N	N	N	Y	Good
Bakhshandeh A, Eslami Z [25]	Y	Y	Y	Y	Y	Y	N	Average
Wang X, Luan D [23]	Y	Y	Y	Y	Y	Y	N	Poor
Ping et. Al. [26]	Y	Y	Y	Y	Y	Y	N	Good
Mohamed [29]	N	N	Y	Y	Y	Y	N	Average
Enayatifar et. Al. [30]	Y	Y	Y	Y	Y	Y	N	Average
Yang et al. [19]	Y	Y	Y	Y	Y	Y	Y	Good
Li et al. [31]	N	N	Y	Y	Y	N	Y	Good
Yaghouti Niyat et al., [34]	Y	Y	Y	Y	Y	Y	Y	Average
Li et al. [22]	N	N	Y	Y	N	N	Y	Good
Bhardwaj & Bhagat [36]	Y	Y	Y	Y	Y	Y	Y	Good
Z. Jeelani [37]	Y	Y	Y	Y	Y	Y	Y	Average
Jiao et al. [38]	Y	Y	Y	Y	Y	N	Y	Good
Alexan et al. [39]	Y	Y	Y	Y	Y	N	Y	Good

4.6 Key Analysis (KA): The key analysis is considered to be the main part of any encryption technique because the strength of any encryption technique is measured by its security keys. The keys should be strong enough to provide resistance to all types of attacks. And any encryption technique must be sensitive to its secret keys and having long key space. Because larger is the key space, it is difficult for an attacker to estimate the same key. And if a single bit is modified in the secret key, then it is difficult to know the information about the original image.

4.7 Noise Attack (NA): Sometimes attacker tries to remove the useful information by introducing the noise in the encrypted image so it cannot be reproduced at the receiver's end. Noise may be Gaussian, Poisson noise, additive noise etc. A good encryption scheme should be resistant to noise attacks.

4.8 Execution Time (ET): The time required to execute an encryption technique is known as encryption time which is a aggregation of compile time and run time. Minimal is the ET, good is the encryption scheme and it is normally measured in milliseconds and microseconds.

5 Comparison of Various Cellular Automata based Encryption Schemes

The different scheme studied so far in the literature are now compared on the basis of various performance metrices described in section 4 and the comparison is listed in table 2.

6 Conclusion

The paper presents a concise and effective view of various existing encryption schemes using CA. But due to continuous expansion of calculating power of machines, almost all the encryption schemes are a back step in terms of security and speed. And as images require more space and demands more bandwidth than text while communicating. And due to scarcity of image encryption techniques along with compression, we can work in that direction which gives best results in terms of security, speed and space.

7 References

[1] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps," *Signal Processing: Image Communication*, vol. 29, no. 5, pp. 618–627, May 2014, doi: 10.1016/j.image.2013.09.009.

[2] H. M. Furqan, M. S. J. Solaija, H. Türkmen, and H. Arslan, "Wireless Communication, Sensing, and REM: A Security Perspective," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 287–321, 2021, doi: 10.1109/OJCOMS.2021.3054066.

[3] Archana, Sachin, and P. Singh, "Cryptosystem Based on Triple Random Phase Encoding with Chaotic Henon Map," in *Proceedings of International Conference on Data Science and Applications*, Singapore, 2021, pp. 73–84. doi: 10.1007/978-981-15-7561-7_5.

[4] E. Kumari, P. Singh, S. Mukherjee, and G. N. Purohit, "Analysis of triple random phase encoding cryptosystem in Fresnel domain," *Results in Optics*, vol. 1, p. 100009, Nov. 2020, doi: 10.1016/j.rio.2020.100009.

[5] P. Rakheja, R. Vig, and P. Singh, "Asymmetric hybrid encryption scheme based on modified equal modulus decomposition in hybrid multi-resolution wavelet domain," *Journal of Modern Optics*, vol. 66, no. 7, pp. 799–811, Apr. 2019, doi: 10.1080/09500340.2019.1574037.

[6] S. Nandi, B. K. Kar, and P. Pal Chaudhuri, "Theory and applications of cellular automata in cryptography," *IEEE Trans. Comput.*, vol. 43, no. 12, pp. 1346–1357, Dec. 1994, doi: 10.1109/12.338094.

[7] A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *AEU - International Journal of Electronics and Communications*, vol. 66, no. 10, pp. 806–816, Oct. 2012, doi: 10.1016/j.aeue.2012.01.015.

[8] H. Chen, L. Zhu, Z. Liu, C. Tanougast, F. Liu, and W. Blondel, "Optical single-channel color image asymmetric cryptosystem based on hyperchaotic system and random modulus decomposition in Gyrator domains," *Optics and Lasers in Engineering*, vol. 124, p. 105809, Jan. 2020, doi: 10.1016/j.optlaseng.2019.105809.

[9] E. Kumari, P. Singh, S. Mukherjee, and G. Purohit, "Optical Chaotic Cryptosystem for Phase Images Using Random Amplitude and Phase Masks with Lorenz Map in Fresnel Domain," 2020, pp. 1–13. doi: 10.1007/978-981-15-5414-8_1.

[10] S. Sachin, R. Kumar, and P. Singh, "Unequal modulus decomposition and modified Gerchberg Saxton algorithm based asymmetric cryptosystem in Chirp-Z transform domain," *Opt Quant Electron*, vol. 53, no. 5, p. 254, Apr. 2021, doi: 10.1007/s11082-021-02908-w.

[11] J. Cai and X. Shen, "Modified optical asymmetric image cryptosystem based on coherent superposition and equal modulus decomposition," *Optics & Laser Technology*, vol. 95, pp. 105–112, Oct. 2017, doi: 10.1016/j.optlastec.2017.04.018.

[12] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Lett.*, vol. 35, no. 2, p. 118, Jan. 2010, doi: 10.1364/OL.35.000118.

[13] H. Xu, W. Xu, S. Wang, and S. Wu, "Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain," *Optics Communications*, vol. 402, pp. 302–310, Nov. 2017, doi: 10.1016/j.optcom.2017.05.035.

[14] J. Wang, X. Chen, J. Zeng, Q.-H. Wang, and Y. Hu, "Asymmetric Cryptosystem Using Improved Equal Modulus Decomposition in Cylindrical Diffraction Domain," *IEEE Access*, vol. 7, pp. 66234–66241, 2019, doi: 10.1109/ACCESS.2019.2917994.

[15] H. Li *et al.*, "Asymmetric multiparameter encryption of hyperspectral images based on hybrid chaotic mapping and an equal modulus decomposition tree," *Appl. Opt., AO*, vol. 60, no. 22, pp. 6511–6519, Aug. 2021, doi: 10.1364/AO.425776.

[16] Jin Jun, "Image encryption method based on Elementary Cellular Automata," in *IEEE Southeastcon 2009*, Atlanta, GA, USA, Mar. 2009, pp. 345–349. doi: 10.1109/SECON.2009.5174103.

[17] O. Lafe, *Cellular Automata Transforms: Theory and Applications in Multimedia Compression, Encryption, and Modeling*. Springer Science & Business Media, 2012.

[18] Y. Wang, Y. Zhao, Q. Zhou, and Z. Lin, "Image encryption using partitioned cellular automata," *Neurocomputing*, vol. 275, pp. 1318–1332, Jan. 2018, doi: 10.1016/j.neucom.2017.09.068.

[19] Y.-G. Yang, J. Tian, H. Lei, Y.-H. Zhou, and W.-M. Shi, "Novel quantum image encryption using one-dimensional quantum cellular automata," *Information Sciences*, vol. 345, pp. 257–270, Jun. 2016, doi: 10.1016/j.ins.2016.01.078.

[20] S. Ulam, "Random processes and transformations," in *In Sets, Numbers, and Universes*, 1974, pp. 326–337.

[21] N. Ganguly, B. K. Sikdar, and P. P. Chaudhuri, "Theory of Additive Cellular Automata," p. 21.

[22] X. Li, D. Xiao, and Q.-H. Wang, "Error-free holographic frames encryption with CA pixel-permutation encoding algorithm," *Optics and Lasers in Engineering*, vol. 100, pp. 200–207, Jan. 2018, doi: 10.1016/j.optlaseng.2017.08.018.

[23] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, Nov. 2013, doi: 10.1016/j.cnsns.2013.04.008.

[24] A. M. del Rey, G. R. Sanchez, and A. de la Villa Cuenca, "A protocol to encrypt digital images using chaotic maps and memory cellular automata," *Logic Journal of IGPL*, vol. 23, no. 3, pp. 485–494, Jun. 2015, doi: 10.1093/jigpal/jzv013.

[25] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," *Optics and Lasers in Engineering*, vol. 51, pp. 665–673, Jun. 2013, doi: 10.1016/j.optlaseng.2013.01.001.

[26] P. Ping, F. Xu, and Z.-J. Wang, "Image encryption based on non-affine and balanced cellular automata," *Signal Processing*, vol. 105, pp. 419–429, Dec. 2014, doi: 10.1016/j.sigpro.2014.06.020.

[27] X. Wang and D. Xu, "A novel image encryption scheme using chaos and Langton's Ant cellular automaton," *Nonlinear Dyn*, vol. 79, no. 4, pp. 2449–2456, Mar. 2015, doi: 10.1007/s11071-014-1824-0.

[28] X. W. Li, S. J. Cho, and S. T. Kim, "A 3D image encryption technique using computer-generated integral imaging and cellular automata transform," *Optik*, vol. 125, no. 13, pp. 2983–2990, Jul. 2014, doi: 10.1016/j.ijleo.2013.12.036.

[29] F. Kamel Mohamed, "A parallel block-based encryption schema for digital images using reversible cellular automata," *Engineering Science and Technology, an International Journal*, vol. 17, no. 2, pp. 85–94, Jun. 2014, doi: 10.1016/j.jestch.2014.04.001.

[30] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata," *Optics and Lasers in Engineering*, vol. 71, pp. 33–41, Aug. 2015, doi: 10.1016/j.optlaseng.2015.03.007.

[31] X. Li, C. Li, and I.-K. Lee, "Chaotic image encryption using pseudo-random masks and pixel mapping," *Signal Processing*, vol. 125, pp. 48–63, Aug. 2016, doi: 10.1016/j.sigpro.2015.11.017.

[32] R. V. Yampolskiy, J. D. Rebolledo-Mendez, and M. M. Hindi, "Password Protected Visual Cryptography via Cellular Automaton Rule 30," in *Transactions on Data Hiding and Multimedia Security IX*, vol. 8363, Y. Q. Shi, F. Liu, and W. Yan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 57–67. doi: 10.1007/978-3-642-55046-1_4.

[33] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Processing: Image Communication*, vol. 52, pp. 6–19, Mar. 2017, doi: 10.1016/j.image.2016.12.007.

[34] A. Yaghouti Niyat, M. H. Moattar, and M. Niazi Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, Mar. 2017, doi: 10.1016/j.optlaseng.2016.10.019.

[35] B. Jeyaram, R. R, and R. Raghavan, "New cellular automata-based image cryptosystem and a novel non-parametric pixel randomness test: CA based Image Cryptosystem," *Security Comm. Networks*, vol. 9, no. 16, pp. 3365–3377, Nov. 2016, doi: 10.1002/sec.1542.

[36] R. Bhardwaj and D. Bhagat, "Two Level Encryption of Grey Scale Image through 2D Cellular Automata," *Procedia Computer Science*, vol. 125, pp. 855–861, 2018, doi: 10.1016/j.procs.2017.12.109.

[37] Z. Jeelani, "Digital Image Encryption Based on Chaotic Cellular Automata:," *International Journal of Computer Vision and Image Processing*, vol. 10, no. 4, pp. 29–42, Oct. 2020, doi: 10.4018/IJCVIP.2020100102.

[38] K. Jiao, G. Ye, and Q. Mei, "Image Encryption Scheme Based on Quantum Logistic Map and Cellular Automata," in *2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS)*, Apr. 2021, pp. 375–379. doi: 10.1109/ICCCS52626.2021.9449238.

[39] W. Alexan, M. ElBeltagy, and A. Aboshousha, "RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System," *Symmetry*, vol. 14, no. 3, Art. no. 3, Mar. 2022, doi: 10.3390/sym14030443.

[40] O. Lafe, "Cellular Automata Transforms," in *Cellular Automata Transforms*, Boston, MA: Springer US, 2000, pp. 23–44. doi: 10.1007/978-1-4615-4365-7_2.

[41] S. Wolfram, "Computation Theory of Cellular Automata," *Cellular Automata*, p. 43.

[42] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, Nov. 2016, doi: 10.1016/j.sigpro.2016.03.021.

[43] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, pp. 197–213, Jan. 2017, doi: 10.1016/j.optlaseng.2016.08.009.