Image Encryption Based on 5-Neighbor Programmable Cellular Automata

Sung Won Kang
Department of Artificial Intelligence Convergence,
Pukyong National University
Busan, South Korea
e-mail : jsm2371@hanmail.net

Un Sook Choi
School of Artificial Intelligence,
Tongmyong University
Busan, South Korea
e-mail: choies@tu.ac.kr

Abstract— **With the rapid development and spread of non-face-to-face digital technologies and services due to the spread of COVID-19, real-time non-face-to-face online meetings, education, telemedicine, online collaboration, telecommuting, various non-face-to-face tasks in the financial sector, and the sharing economy are frequent. As a result, network traffic increases and the demand for real-time security of multimedia is increasing. Security of information, including image content, is an essential part of today's communication technology and is very important for safe transmission. In this paper, we design a 5-neighbor programmable cellular automata (FNPCA) based ROI (region of interest) image encryption system that can effectively reduce computational cost and maintain an appropriate level of security.**

Keywords— color image encryption; programmable cellular automata; ROI (region of interest); five-neighbor CA; high speed encryption;YOLO;

I. INTRODUCTION

The remarkable development of the IT field in the era of the 4th industrial revolution has brought about many changes in various fields of our society. Information can be collected and used quickly and conveniently using computers and mobile devices. And through social networking service (SNS), opportunities for social participation have increased. In particular, as non-face-to-face digital technologies and services are rapidly developing and spreading due to the spread of COVID-19, the demand for real-time data transmission is increasing not only in the military but also in various application fields such as medicine, finance, and education. As real-time non-face-to-face online meetings, education, telemedicine, online collaboration, telecommuting, various non-face-to-face tasks in the financial sector, and the sharing economy such as shared cars occur frequently, network traffic increases and the demand for real-time security of multimedia is increasing. In such an environment, problems related to information protection such as personal information leakage and cyber terrorism also occur frequently.

Multimedia data, including video, audio and image content, is large and highly correlated between image pixels. Therefore, traditional encryption algorithms such as DES (Data Encryption Standard), AES (Advanced Encryption Standard), and IDEA (International Data Encryption Algorithm) designed for text encryption are not suitable for image encryption of real-time applications.

Many techniques have been developed to protect images [1]. Among these technologies, image encryption is the most intuitive and effective way to convert an original image into an unrecognizable image. It is possible to prevent theft and illegal viewing of personal images, also to keep back leakage of personal information during image transmission.

Chaos theory is a dynamic system that is very sensitive to time changes and initial conditions. It can effectively generate random sequences because logical laws exist even in seemingly disordered chaos. With these advantages, chaos-based encryption systems are often applied to image encryption. The chaos-based image encryption algorithm was introduced by Fridrich [2] and many research results have been proposed over the past 20 years [2-5].

The chaos-based encryption algorithm consists of two stages: diffusion and confusion. The first step is a process of randomly changing pixel values using a random sequence generated based on a chaos function. In this process, in order to obtain a high security and reliable encryption image, an encryption system that is very sensitive to the key must be used. Many literatures have used mathematical model functions such as logistic maps, chaotic cat maps, and sine maps in this step [1]. Another step is to effectively change the position of the pixel. This step is necessary to protect the image from unexpected noise generation or deletion attacks.

In this paper, we design a five-neighbor programmable cellular automata (FNPCA) based ROI (region of interest) image encryption system that can effectively reduce computational cost and maintain an appropriate level of security. The proposed image encryption system consists of the following steps: (a) extraction of the region of interest using deep learning, (b) encryption using the Chen system with high security for the extracted ROI, (c) whole image encryption using hardware-friendly FNPCA. The proposed encryption system aims to increase the security strength for the main part of the image, maintain an appropriate security strength for the rest, and increase the encryption speed. The image pixel shuffling process uses MLCA, which can already perform chaotic steps at high speed. To this end, we first design and analyze FNPCA. Next, FNPCA is applied to deep learning-based ROI image encryption. To evaluate the safety of the designed cryptographic system, the results are analyzed through various statistical experiments.

II. RELATED WORKS AND BACKGROUNDS

A. Related works

An encryption method for data and images using two-dimensional periodic boundary cellular automata (CA) was proposed in [6]. However, the two-dimensional CA has a complex structure and it is very difficult to analyze the behavior change. This makes it difficult to find a suitable CA for crypto implementation. A method of dividing an image into several blocks and encrypting the divided blocks using CA was proposed in [7]. To increase complexity, they used a logistic map to generate a sequence of pseudo-

random numbers and, based on this sequence, determined the transition rules applied to the CA. However, their proposed method reduced the efficiency of high-speed implementation, which is one of the advantages of CA, because CA is designed to be controlled by logistic maps. A cryptographic system combining Bernoulli map and logistic map was proposed in [8]. The proposed method applied CA to the cryptosystem to improve the sensitivity of the cryptosystem. However, since most encryption processes use chaos maps based on mathematical operations, it is difficult to encrypt at high speed.

Choi et al. [9] proposed a color image encryption algorithm based on programmable complemented maximum length CA (PCMLCA) and 90/150 MLCA. Their method improved the image encryption algorithm based on C-MLCA and 2-D chaotic cat map proposed in [10]. A method for synthesizing 1-D symmetric 5-neighbor MLCA, which can generate a more effective key sequence than 1-D 90/150 MLCA, was proposed in [11], and an image encryption system based on it was proposed.

In this paper, we design a 5-neighbor programmable CA based ROI image encryption system that can increase the security strength for the main part of the image, maintain the appropriate security strength for the rest, and increase the encryption speed.

B. YOLO

Redmon et al. proposed a method to quickly find which object is located in an image by redefining the procedures from pixels of the image to finding the coordinates and class probabilities of the bounding box into a single regression problem[12].This method is named YOLO (you only look once) because it is possible to detect an object by looking at the image once. YOLO is composed of one neural network, so it predicts the class probability of the class to which the object belongs and the bounding box surrounding the object by one calculation for the entire image. Compared to the existing object detection model based on R-CNN, YOLO is simpler and faster to configure. In addition, the background error is small and the detection accuracy is high. In this paper, we use YOLO to extract the ROI of the original image.

C. Cellular Automata

A CA is known as an excellent pseudo-random number sequence generator because of its simple structure, easy expansion and connection in small units, and superior randomness than LFSR. It has been widely applied in various fields such as error correcting code, test pattern generation, pattern classification, and encryption system [1].

In particular, the MLCA has been proven to be an excellent PRNG when applied to the image encryption system [9,10,13]. Maiti et al. [13] performed a NIST statistical test consisting of 15 checks using a 24-bit symmetric 5-neighbor maximum length linear CA to verify the randomness of binary sequences generated by one-dimensional 5-neighbor CAs. It was confirmed that the binary sequence generated by the 5-neighbor CA has high randomness.

The CA used in this paper is a 5-neighbor CA. When c_i^t is the state of the i-th cell at time t, the next state c_i^{t+1} of the i-th cell is the same as Equation (1), where f_i is the transition rule applied to the i-th cell.

$$c_i^{t+1} = f_i(c_{i-2}^t, c_{i-1}^t, c_i^t, c_{i+1}^t, c_{i+2}^t) \quad (1)$$

Figure 1 shows the i-th cell structure of a 5-neighbor linear CA.

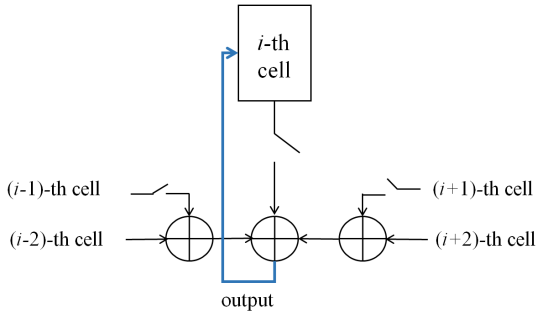


Fig. 1. Cell structure of 5-neighbor linear CA.

III. THE PROPOESD ROI IMAGE ENCRYPTION SCHEME

A. 5-neighbor Progammable CA

In [9], an n-bit keystream was generated using n-cell MLCA, m-cell MLCA which controls complement vectors according to time, and several fixed complement vectors. The n-bit stream is finally output by determining the complement vector according to the output from the controller, and XORing the determined complement vector with the sequence output from the n-cell MLCA. Since the output nonlinear sequence can be generated using a programmable CA, the randomness is higher than that of C-MLCA using a fixed complement vector. Figure 2 shows the structure of PC-MLCA used in [9].

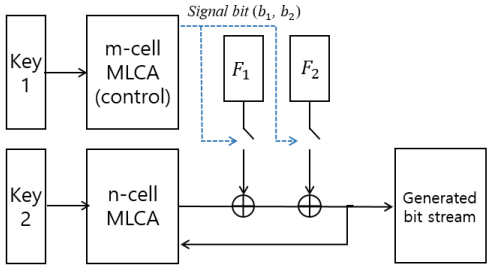


Fig. 2. Structure of PC-MLCA.

The FNPCA proposed in this paper is an integrated PRNG that has a wider range of neighbors than the existing PC-MLCA, and can compose all of the control unit, complement vector, and m-bit output stream with a single CA. We design FNPCA with greater randomness of output sequences than PC-MLCA with extended neighbor range.

Let the state transition matrix $P_n = (u_{ij})_{n\times n}$ of n-cell FNPCA whose transition rule $< r_1 r_2 \cdots r_n >, r_i \in \{0,1\}$ is be as Equation (2).

$$u_{ij} = \begin{cases} r_i, & i = j \\ 1, & |i-j| = 2 \\ 0, & otherwise \end{cases} \quad (2)$$

The state transition matrix P_n is simply denoted as $P_n =< r_1 r_2 \cdots r_n >$. Then, the characteristic polynomial ϕ_n for $P_n =< r_1 r_2 \cdots r_n >$ satisfies the following recurrence relation.

$$\phi_n = (x + r_n)\phi_{n-1} + (x + r_{n-1})\phi_{n-3} + \phi_{n-4} \quad (n \geq 3) \quad (3)$$

where, $\phi_1 = x + r_1$, $\phi_2 = (x + r_2)(x + r_1)$, $\phi_0 = 1$, $\phi_{-1} = 0$, and ϕ_i are characteristic polynomials of FNPCA whose transition rule is $< r_1 r_2 \cdots r_i >$.

ϕ_n is a reducible polynomial and is decomposed as follows.

$$\phi_n = \begin{cases} \Theta_m \mathrm{E}_{m-1}, & n = 2m-1 \\ \Theta_m \mathrm{E}_m, & n = 2m \end{cases} \quad (4)$$

Where, Θ_m is the characteristic polynomial of 90/50 CA composed of the odd-numbered rule $< r_1 r_3 \cdots >$ among the rules $P_n =< r_1 r_2 \cdots r_n >$of FNPCA, and E_{m-1} or E_m is the characteristic polynomial of the 90/50 CA composed of the even-numbered rule $< r_2 r_4 \cdots >$.

To output an effective nonlinear m-bit random number sequence, FNPCA of (2m+1)-cell is used. FNPCA whose transition rule is $< o_1 e_1 o_2 e_2 \cdots o_m e_m o_{m+1} >$ is synthesized using the transition rule $< e_1 e_2 \cdots e_m >$ of the m-cell 90/150 MLCA and the transition rule $< o_1 o_2 \cdots o_{m+1} >$ of the (m+1)-cell 90/150 MLCA. After the state of FNPCA is transferred according to the given rule, the final m-bit random number sequence $S = (s_1 s_2 \cdots s_m)$ is obtained by controlling the complement vector using the bitstream c_{2m+1} output from the (2m+1)-th cell. When c_{2m+1} is 0, $s_i = c_{2i}$, and when c_{2m+1} is 1, $s_i = c_{2i-1} \oplus c_{2i}$. Here, c_j is the bit output from the j-th cell.

Figure 3 shows the structure of FNPCA proposed in this paper.

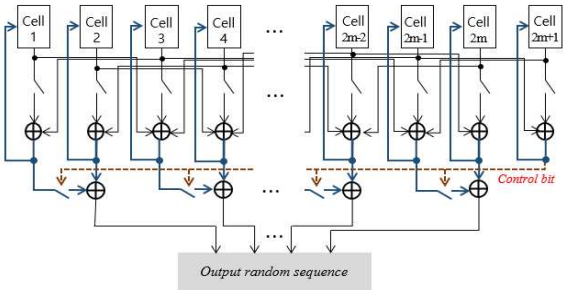


Fig. 3. Structure of (2m+1)-cell FNPCA.

We synthesize the (2m+1)-cell FNPCA, an integrated PRNG that can compose both a control unit that can control complemented vectors and the m-bit output stream. Table 1 shows the FNPCA synthesis algorithm.

TABLE I. ALGORITHM FOR THE 1-D FNPCA SYNTHESIS

Input: primitive polynomial $c(x) = x^n + c_{n-1}x^{n-1} + \cdots + 1$
Output: 1-D symmetric 5-neighbor MLCA $F_n =< r_1, r_2, \cdots, r_n >$.
Step1. Synthesize 1-D 90/150 MLCA by $T_n =< d_1, d_2, \cdots, d_n >$ corresponding to c(x) using the algorithm proposed in [12]
Step2. Choose $F_n =< r_1, \cdots, r_n >$ satisfying $\sum_{i=1}^{n} r_i = c_{n-1}$
Step3. Calculate $\lvert F_n \rvert$ and $\lvert F_n + I_n \rvert$ using Eq. (3).
Step4. If $\lvert F_n \rvert \times \lvert F_n + I_n \rvert = 0$ Goto Step2.
Step5. Construct B_F in Eq. (4) with F_n and T_n.
Step6. Construct row echelon form of B_F.
Step7. Find the number of rows (K) where all components of row in B_F are 0.
Step8. If K = n Stop else Goto Step2.

B. Proposed ROI image encryption scheme using FNPCA

When an image is divided into several regions, it is a common fact that the divided regions do not contain important information of equal intensity. Efficiently extract the ROI from the image to enhance the security of the ROI image and enable adaptive encryption. This has the advantage of saving time by performing low-computational encryption on the non-ROI portion of the input source image while maintaining the security level of the system. Table 2 shows the proposed ROI encryption algorithm.

Figure 4 shows the main procedure of the encryption system. The proposed ROI image encryption system consists of three steps as follows.

1) ROI detection process for the original image: Using YOLO, an object is detected in the original image, and the ROI is extracted by obtaining the minimum rectangular coordinates including all the detected objects.

2) ROI image encryption: ROI encryption consists of shuffling the pixel position of the ROI image using FNPCA, and then changing the pixel value using the sequence generated by the Chen system.

3) Encryption of entire image: For the entire image including the ROI encrypted image, the final encrypted image is obtained through pixel shuffling and pixel value change using FNPCA.

TABLE II. ALGORITHM FOR PROPOSED ROI ENCRYPTION SYSTEM

Input: An original image.
Output: The encrypted image.

//Object detection
Step 1. Find ROI index of the original image using YOLO.
//Setting
Step 2-1. Divide the key into Key1 and Key2.
Step 2-2. Construct shuffling index (1) and key image (1) using the key1 and the ROI index by FNPCA and the Chen system.
Step 2-3. Construct shuffling index (2) and key image (2) using the key2 and the size of the original image by FNPCA.
//Encryption
Step3-1. Shuffle the ROI image by shuffling index (1).
Step3-2. XOR the shuffled ROI image with key image(1).
Step3-3. Shuffle the image of the step3-2 by shuffling index (2).
Step3-4. XOR the image of the step3-3 with key image(2).
Step3-5. Return the image of the step 3-4.

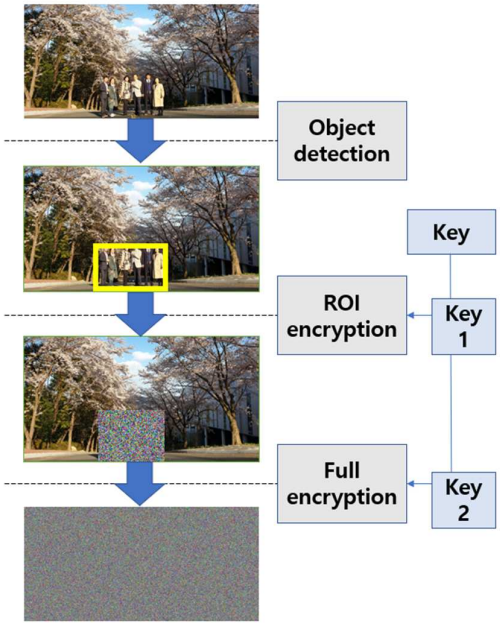


Fig. 4. The main procedure of the encryption system.

In the ROI image pixel shuffling and entire image pixel shuffling process, shuffling is not performed in units of pixels, but repeats shuffling in units of rows and columns an appropriate number of times. As one of the chaotic dynamic system mathematical models, the Chen system can generate chaotic sequences sensitive to initial values. The Chen system is expressed as a system of third-order nonlinear differential equations as shown in (5).

$$\begin{cases} dx/dt = 35(y - x) \\ dy/dt = -7x + 28y - xz \\ dz/dt = -3z + xy \end{cases} \quad (5)$$

The sequence generated by the Chen system is highly random. We use the Chen system to generate a sequence for changing the pixel values of the ROI image considering the encryption execution time.

IV. Experimental Results and Security Analysis

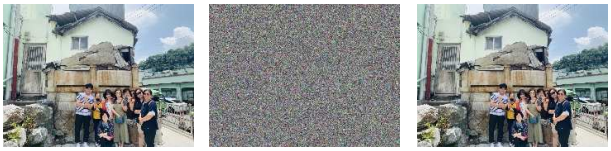
Various types of portraits were used as original images for the simulation. The original image in Figure 5 is one of the original image samples of various sizes used in the experiment. And the rest of the images are images as a result of performing encryption/decryption according to the method of proposing the original image.

It is impossible to obtain information about the original image with the naked eye with respect to the encrypted image. Also, the decrypted image matches the original image. The size of the original image is 960(W)×720(H), and the size of the ROI image is 460(W)×320(H).

A. Statistical Analysis

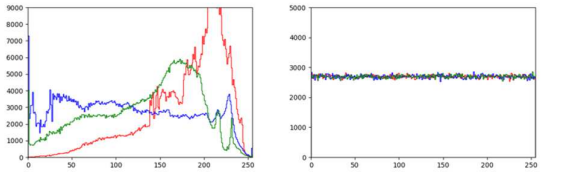
To protect an image from random attacks, there should be no statistical similarity between the original image and the encrypted image.

The histogram of an image represents the distribution of pixel values within the image. The constant histogram of the encrypted image means that the attacker cannot obtain useful statistical information for the attack. Figure 6 is a histogram of the original image and the encrypted image in Figure 5. The histogram of the encrypted image shows a uniform distribution, unlike the original image. It can be seen that the statistical characteristics of the original image are lost in the process of performing the encryption process.



(a) Original image (b) Encrypted image (c) Decrypted image

Fig. 5. Original image and encryped/decrypted image.



(a) Histogram of the original image (b) Histogram of the encrypted image

Fig. 6. Histograms of the original image and the encrypted image. .

In general, images have a strong correlation between adjacent cells and a high redundancy. Through the histogram analysis, it was confirmed that the low redundancy appears in the encrypted image. It is confirmed that the strong correlation between adjacent pixels of the original image does not appear in the encrypted image. The correlation coefficient is calculated by selecting 2000 pairs of two adjacent pixels (vertical, horizontal and diagonal directions) from the original image and the encrypted image. Table III shows the results of calculating the correlation coefficient between the original image and the encrypted image. According to Table III, it can be seen that the very high correlation seen in each direction of each color plane in the original image, but little correlation in the encrypted image. Figure 7 shows the correlation between the original image and the encrypted image in the vertical direction of the R,G and B color channels. The image encryption

algorithm should be designed to be resistant to differential attacks in which the encrypted image must be changed significantly even if the original image is slightly changed.

TABLE III. CORRELATION COEFFICIENTS OF THE ORIGINAL IMAGE AND THE ENCRYPTED IMAGE BY THE PROPOSED ALGORITHM

Image		Horizontal	Vertical	Diagonal
Original image	R	0.92061	0.86531	0.83701
	G	0.93501	0.88912	0.86439
	B	0.91687	0.85701	0.82629
Encrypted image (Proposed)	R	0.00027	0.00083	0.00869
	G	0.00566	-0.00025	-0.00421
	B	-0.01186	-0.00915	-0.00370

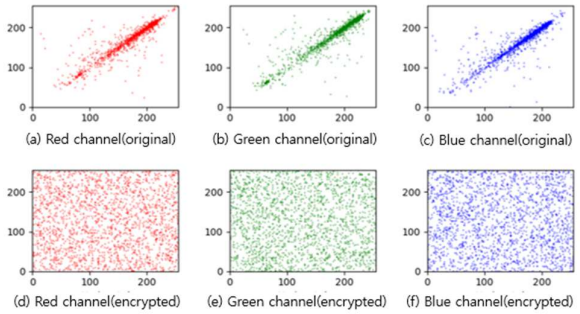


Fig. 7. The correlation scatter plots of pixels adjacent to each channel in for the original/encrypted image.

To substantiate that the proposed cryptosystem is safe against various brute force attacks, various statistical experiments and analyzes are performed. The entropy range is 0-8. Entropy is a measure of the uncertainty of information. Therefore, the closer to 8, the more difficult it is to predict the information. As a result of calculating the entropy of the encrypted image for the original image samples of various sizes, the average is 7.999, very close to the maximum value of 8.

B. *Differential Analysis*

A cryptosystem should not be able to decrypt an encrypted data using a different key. Differential analysis is performed to analyze whether the cryptosystem satisfies these characteristics. For example, if the encryption is performed using two keys, then the two encrypted images must obtain completely different results. Figure 8 shows two images encrypted using two keys with different 1-bits.

The differential attack is used to analyze the sensitivity of the key, and there are measures for the differential analysis; NPCR, UACI and PSNR. NPCR and UACI measure the difference between the encrypted image obtained after changing one pixel in the original image and the encrypted image obtained before the change[14]. NPCR is the rate of pixel change between two encrypted images, and UACI is the average of the difference in pixel change intensity between two encrypted images. The famous measure PSNR, the Peak Signal-to-noise ratio, can be able to use in differential analysis. The PSNR of images of figure 8 is 7.7. It means that images are almost different. NPCR and UACI obtained by the proposed encryption algorithm are 99.627% and 33.478%, respectively. For the perfectly different images, the NPCR is over 99%, and the UACI is about 33.4%. It is verifying that they are designed to have sufficient resistance to differential attacks.

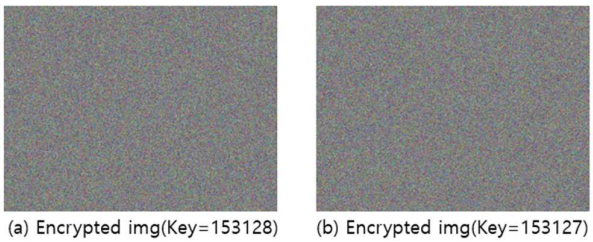


Fig. 8. The encrypted images using differential keys.

TABLE IV. DIFFERENTIAL ANALYSIS OF THE ENCRYPTED IMAGES BY THE PROPOSED ALGORITHM

	Red	Blue	Green
NPCR	99.6200	99.6148	99.6278
UACI	33.4275	33.5004	33.4789
PSNR	7.7555	7.7425	7.7443

C. *Date Loss and delete Attack*

The purpose of image shuffling is to design an encryption system that is resistant to noise and partial erasure attacks by changing the location of the pixels. Figure 9 shows that the proposed encryption algorithm is resistant to data loss and noise attacks. Therefore, it can be confirmed that image shuffling has been effectively performed. Furthermore, as you can see in the figure 9-(c), if only a part of the key is used, the ROI cannot be decrypted. In other words, if attackers didn't get the complete key, they can't decrypt correctly.

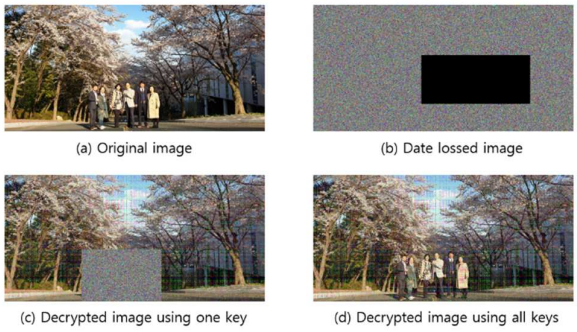


Fig. 9. Experiments on data loss and delete attack.

V. CONCLUSION

In this paper, we proposed a method for synthesizing a 5-neighbor programmable CA. The synthesized FNPCA is a PRNG that integrates PC-MLCA composed of two 90/150 MLCAs into one, and a nonlinear m-bit sequence can be generated. In addition, we proposed an ROI color image encryption algorithm using the designed FNPCA. Since the proposed algorithm can generate a key sequence with a hardware-friendly operation, it can be implemented at a

faster speed than other chaos-based encryption algorithms that require mathematical operations. The safety of the proposed algorithm was verified through various statistical analyzes.

REFERENCES

[1] H.M. Ghadirli, A. Nodehi and R. Enayatifar, "An overview of encryption algorithms in color images," Signal Processing, vol. 164, 2019, pp. 163–185.

[2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int J Bifurcation and Chaos, vol. 8, no. 6, 1998, pp.1259–1284.

[3] R. Enayatifar, A.H. Abdullah and I.F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," Opt. Laser Eng. vol.56, 2014, pp. 83–93.

[4] Y. Li, C. Wang and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," Opt. Lasers Eng. vol. 90, 2017, pp. 238–246.

[5] A. Broumandnia, "The 3D modular chaotic map to digital color image encryption," Future Generation Computer Systems, vol. 99, 2019, pp. 489-499.

[6] P.S. Kumar, C.S.U. Sampreeth and S.A.K. Reddy, "Image Encryption and Decryption Algorithm Using Two Dimensional Cellular Automata Rules In Cryptography," International Journal of Computer Science Engineering, vol. 6, no. 01, 2017, pp.1-9.

[7] Z. Eslami and S. Kabirirad, "A block-based image encryption scheme using cellular automata with authentication capability," Proc. of Third International Conference of Mathematical Sciences(ICMS 2019) AIP Conference Proceedings vol. 2183, 2019.

[8] W. Zhang, Z. Zhu and H. Yu, "A Symmetric Image Encryption Algorithm Based on a Coupled Logistic–Bernoulli Map and Cellular Automata Diffusion Strategy," Entropy, vol. 21, no. 5, 2019, 504.

[9] U.S. Choi, S.J. Cho, J.G. Kim, S.W. Kang, H.D. Kim and S.T. Kim, "Color Image Encryption Based on PC-MLCA and 3-D Chaotic Cat Map," Proc. of International Conference on Computer and Communication Systems (ICCCS), 2019

[10] H.S. Jeong, K.C. Park, S.J. Cho and S.T. Kim, "Color medical image encryption using two-dimensional chaotic map and C-MLCA," Proc. of the International Conference on Ubiquitous and Future Networks, 2018.

[11] U.S. Choi, S.J. Cho and S.W. Kang, "1-D Symmetric 5-Neighbor MLCA Based Color Image Encryption," Proc. of International Conference on Computer and Communication Systems (ICCCS), 2021.

[12] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: unified, real-time object detection," Proc. of Computer Vision and Pattern Recognition (CVPR), 2016.

[13] S. Maiti and D. R. Chowdhury, "Study of five-neighborhood linear hybrid cellular automata and their synthesis," Proc. of ICMC 2017, CCIS 655, 2017.

[14] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications(JSAT), 2011, pp 31–38.