Regular paper | Journal of the KIECS. pp. 1187-1196, vol. 14, no. 6, Dec. 31. 2019, t. 98, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2019.14.6.1187

C-MLCA와 Laplace 전개를 이용한 3차원 카오스 캣맵에 의한 영상 암호

조성진* · 김한두** · 최언숙*** · 강성원****

Image Encryption by C-MLCA and 3-dimensional Chaotic Cat Map using Laplace Expansions

Sung-Jin Cho* · Han-Doo Kim** · Un-Sook Choi*** · Sung-Won Kang****

요 약

정보 보안은 클라우드 및 소셜 네트워킹 사이트의 출현으로 주요 과제가 되었다. 기존의 암호화 알고리즘은 디지털 영상의 큰 데이터 크기와 원시 픽셀 간에 높은 중복성으로 인해 영상 암호화에 적합하지 않을 수 있다. 본 논문에서는 Jeong 등이 제안한 컬러 영상의 암호화 방법을 C-MLCA와 Laplace 전개를 이용한 매개변수식 3차원 카오스 캣맵을 사용하여 일반화한다. 제안된 새로운 영상 암호시스템이 높은 보안성과 신뢰성을 제공한다는 것을 엄격한 실험을 통해 입증한다.

ABSTRACT

Information security has become a major challenge with the advent of cloud and social networking sites. Conventional encryption algorithms might not be suitable for image encryption because of the large data size and high redundancy among the raw pixels of a digital image. In this paper, we generalize the encryption method for of color image proposed by Jeong et al. to color image encryption using parametric 3-dimensional chaotic cat map using Laplace expansion and C-MLCA. Through rigorous experiments, we demonstrate that the proposed new image encryption system provides high security and reliability.

키워드

Image Encryption, Chaotic Cat Map, Laplace Expansion, C-MLCA
영상 암호, 카오스 캣맵, Laplace 전개, C-MLCA

Ⅰ. Introduction

With the rapid advancements of digital image processing and network technologies over the past two decades, a vast number of digital images are now transmitted over the Internet and through wireless networks for convenient accessing and sharing. As a result, protection of digital images

* 부경대학교 응용수학과(sjcho@pknu.ac.kr)
** 교신저자 : 인제대학교 컴퓨터공학부
*** 동명대학교 정보통신공학과(choies@tu.ac.kr)
**** 부경대학교 응용수학과(jsm2371@hanmail.net)
• 접 수 일 : 2019. 08. 10
• 수정완료일 : 2019. 10. 12
• 게재확정일 : 2019. 12. 15
• Received : Aug. 10, 2019, Revised : Oct. 12, 2019, Accepted : Dec. 15, 2019
• Corresponding Author : Han-Doo Kim
Dept. of Computer Engineering, Inje University,
Email : mathkhd@inje.ac.kr

against illegal copying and distribution has become an important challenge. To prevent the loss of image information, a large number of encryption algorithms have been proposed. Among them the image encryption based on the chaotic map is being widely used. Because chaos has generous characteristics, such as sensitivity to initial conditions, pseudo-randomness, ergodicity and reproduction, chaos is widely used in image encryption area. Chen et al.[1] proposed a symmetric image encryption scheme that generalizes a two-dimensional chaos map in three dimensions in order to design a real-time secure image encryption scheme. Many researchers have studied several cryptosystems based on CA. Jeong et al.[2] proposed a color medical image encryption algorithm based on a two-dimensional chaotic cat map and C-MLCA for medical image encryption. The two-dimensional chaotic cat map was used to effectively shuffle the positions of each pixel without changing the pixel values. C-MLCA was used to generate a PN sequence of maximum period to perform XOR operation with plain image.

In this paper, we generalize the encryption method for color image proposed by Jeong et al.[2] to color image encryption using parametric 3-dimensional chaotic cat map using Laplace expansion and C-MLCA. We also propose a generalized 3-D chaotic cat map for reliable and secure image encryption that can change the position of pixels in each R, G and B channels of a color image at the same time without the reconstruction of plain image. We generate the key image using C-MLCA, and then perform the XOR operation on the generated key image with the plain color image. We then use a generalized 3-D chaotic cat map to effectively shuffle the positions of the image pixels. Since C-MLCA is nonlinear, it increases randomness. We conduct thorough experimental testing with detailed analysis to demonstrate the high security and reliability of the proposed new image encryption system.

II. Cellular Automata and Generalized 3-D Chaotic Cat Map

2.1 Cellular Automata

Cellular Automata(CA) are deterministic mathematical idealizations of physical systems in which space and time are discrete and each cell can assume the value either zero or one[3]. Although CA is a simple structure, it can generate complex and random patterns[4]. Of particular importance is the 2-state, 3-neighborhood CA with cells arranged linearly in one dimension, where the next state of a particular cell is assumed to depend on itself and on its two neighbors. The state of the ith cell at time $(t+1)$ is denoted as

$$s_i^{t+1} = f_i\left(s_{i-1}^t, s_i^t, s_{i+1}^t\right) \tag{1}$$

where s_i^t denotes the state of the ith cell at the time of instant t. When $f_i\left(s_{i-1}^t, s_i^t, s_{i+1}^t\right)$ is expressed as a Boolean function, the rules expressed only by XOR logic and XNOR logic are called *additive rules*. If the next state generating logic employs only XOR logic, then it is called a *linear rule*. And a CA with all the cells having linear rules is called a *linear CA*. And CA with one or more rules of XNOR logic is called *complemented CA*. Table 1 shows the Boolean expressions for the transition rules 90, 165, 150 and 105 to be used in this paper. The state transition function of linear n-cell CA can be expressed as an $n \times n$ matrix T. T is called a *state transition matrix*. When the state of CA at time t is S^t, the next state S^{t+1} is given as follows[5]:

$$S^{t+1} = TS^t \tag{2}$$

Table 1. The Boolean expressions of additive transition rules 90, 165, 150 and 105

Rule	Expression	Rule	Expression
90	$s_i^{t+1}=s_{i-1}^t \oplus s_{i+1}^t$	150	$s_i^{t+1}=s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t$
165	$s_i^{t+1}=\overline{s_{i-1}^t \oplus s_{i+1}^t}$	105	$s_i^{t+1}=\overline{s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t}$

Generally, a complemented CA can be expressed as a linear CA and a complement vector. When the state transition function of the complemented CA is $\overline{T}$, the next state of the complemented CA can be expressed as Eq. (3) using T and complement vector F as follows:

$$S^{t+1}=\overline{T}S^t=TS^t \oplus F \tag{3}$$

The smallest positive integer k that satisfies $\overline{T}^k S=S$ for an arbitrary state S of CA is called the *period* of the CA. If the period of an n-cell CA is 2^n-1, then it will be called *complemented maximum length CA*(*C-MLCA*)[6, 7]. The complemented CA where the characteristic polynomial $c(x)=|T \oplus xI_n|$ for T corresponding to $\overline{T}$ is the primitive polynomial is C-MLCA, where I_n is the $n \times n$ identity matrix[5]. C-MLCA generates several maximum-length PN sequences according to the choice of complement vector. We can create a basis image using the C-MLCA sequence. The basis image consists of a pseudo noise sequence that is hard to find regularity. This basis image is bitwise XORed with the original image.

2.2 Generalized 3-D Chaotic Cat Map

The classical chaotic cat map is a 2-D reversible chaotic map described by Eq. (4)[1].

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N \tag{4}$$

where N is the width or length of a square image. This function preserves the area because the determinant of the linear transformation matrix is 1. The above 2-D cat map is generalized by introducing two control parameters a and b as follows:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N \tag{5}$$

where a and b are positive integers and $x_n, y_n \in \{0,1,\cdots,N-1\}$. The parameters a, b and the number of iterations l all can be used as the secret keys. To enhance the security level of the cat map based cryptography and other applications, several 3-D cat map generation methods were developed[8]. A 2-D cat matrix $\boldsymbol{C}^{2D}$ can be generated in a parametric way, where the parameters consist of a given 1-D cat matrix $\boldsymbol{C}^{1D}=[1]$, the location of the element a_{ij} associated with $\boldsymbol{C}^{1D}$, and 2 additional matrix elements. A 3-D cat matrix $\boldsymbol{C}^{3D}$ can be generated in a parametric way, where the parameters consist of a given 2-D cat matrix $\boldsymbol{C}^{2D}$, the location of the element a_{ij} associated with $\boldsymbol{C}^{2D}$, and 2×2 additional matrix elements. There are four 2-dimensional cat matrices, and there are nine 3-dimensional cat matrices constructed for each 2-dimensional cat matrix as follows. In particular, there are nine 3-dimensional cat matrices for matrix $\begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix}$.

$$\begin{pmatrix} C_{1,1}^{3D} & c & d \\ e & 1 & a \\ f & b & C_{2,2}^{2D} \end{pmatrix}, \begin{pmatrix} g & C_{1,2}^{3D} & h \\ 1 & i & a \\ b & j & C_{2,2}^{2D} \end{pmatrix}, \cdots, \begin{pmatrix} 1 & a & k \\ b & C_{2,2}^{2D} & l \\ m & n & C_{3,3}^{3D} \end{pmatrix}$$

where $C_{1,1}^{3D}=abce+ce+df-acf-bde+1$, $C_{1,2}^{3D}=abgi+hj-agj-bhi-1$ and $C_{3,3}^{3D}=abkm+km+ln-alm-bkn+1$.

Let $L_1=\begin{pmatrix} abce+ce+df-acf-bde+1 & c & d \\ e & 1 & a \\ f & b & C_{2,2}^{2D} \end{pmatrix}$,

$$L_2=\begin{pmatrix} g & abgi+gi+hj-agj-bhi-1 & h \\ 1 & i & a \\ b & j & C_{2,2}^{2D} \end{pmatrix},$$

$$L_3=\begin{pmatrix} 1 & a & k \\ b & C_{2,2}^{2D} & l \\ m & n & abkm+km+ln-alm-bkn+1 \end{pmatrix}.$$

The 3-dimensional cat matrix we use to encrypt is the product of three generalized cat matrices of pairwise-coupled dynamics as $L=L_3L_2L_1$ where $a,b,\cdots,m$ and n are fourteen integer control parameters. Since $\det(L_i)=1$ for each $i=1,2,3$, $\det(L)=1$. For example, for the generalized cat matrix $L=\begin{pmatrix} 29 & 23 & 35 \\ 64 & 51 & 75 \\ 146 & 115 & 184 \end{pmatrix}$, three eigenvalues of L are:

$$\lambda_1=3.80957(>1),\ \lambda_2=260.187(>1),\ \lambda_3=0.00302663 \quad (6)$$

, which are actually the three Lyapunov exponents of the matrix L. Since the leading Lyapunov exponent is strictly larger than 1, the map has chaotic behavior. The 3-D cat matrices generated by Wu's methods[8] have the largest parameter space of M^{14}(M is the number of possible values of each matrix parameter) attained by L. Taking $M=256$ as an example, then $(256)^{14}=2^{112}<2^{128}$, which is smaller than the required size to resist brute-force attacks. We use C-MLCA to expand the key space. This implies that applications directly using these parametric 3-D cat matrices are insecure. Consequently, these 3-D cat matrices are commonly used with additional components.

III. The Proposed Algorithm

In this section, we describe the image cryptosystem proposed in this paper in two phases.

3.1 Generation of the Key Image

In this section, we give a C-MLCA for the generation of the key image which consists of n-cell MLCA ($n\geq 8$), complement vectors F. The color image having the size of $N\times N$ is divided into three images with R, G and B channels respectively, and then the three images are connected to a grayscale image having the size of $N\times 3N$. The generated grayscale image is converted into a one-dimensional image pixel matrix, and then converted into a one-dimensional image bit matrix. In order to change the pixel value of the plain image to an unpredictable value, the XOR operation is performed on the key image generated by the C-MLCA and the plain image. The basis image generated by a C-MLCA is bitwise XORed with the one-dimensional image bit matrix.

3.2 Generalized 3-D Chaotic Cat Map Method

Each pixel value of a gray image whose size is $N\times N$ has a value between 0 and 255. The unit pixel of color image is represented by R, G and B components of 256 steps, respectively, so that the size of one color image is $N\times N\times 8\times 3$ bits. The 3-D chaotic cat map based cryptosystem proposed by Chen et al.[1] requires the reconstruction of the plain image into several 3-D cubic arrays.

In this paper, we design an efficient and generalized 3-D chaotic cat map that can change the position of each pixel of the original image at the same time without changing the size of the original image. Using the proposed 3-D chaotic cat map, the position $(i,j,k)(0\leq i<N, 0\leq j<N, 0\leq k<N)$ of a given plain color image pixel is mapped to a new position. Let $L(r_i)(i=1,2,3)$ be each row of $L=L_3L_2L_1$. And let (i',j',k') be the new position of (i,j,k) determined by the 3-D chaotic cat map, then Eq. (7) is the mathematical expression of a generalized 3-D chaotic cat map for a given color image.

$$\begin{pmatrix} i' \\ j' \\ k' \end{pmatrix}=L\begin{pmatrix} i \\ j \\ k \end{pmatrix} \bmod N \quad (7)$$

where $i' = L(r_1)(i,j,k)^t \bmod N$, $j' = L(r_2)(i,j,k)^t \bmod N$, and $k' = L(r_3)(i,j,k)^t \bmod N$. $L^l(i,j,k)^t$ be the l-times application of L to $(i,j,k)^t$. To increase the security level, the chaotic cat map is repeated to shuffle the pixel positions. The block diagram of the proposed image encryption system is shown in Fig. 1.

3.3 Key Scheming

The variables available as keys in the proposed algorithm are: (1) Components of n-cell C-MLCA needed to generate key images in the generating phase of the key image : rules, initial values and complement vectors. (2) Control parameters of the generalized 3-D chaotic cat map used in the suffling phase of the pixel positions.

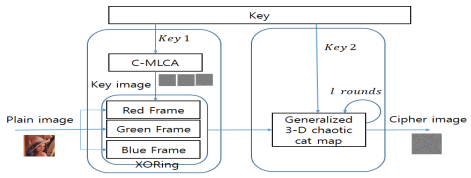


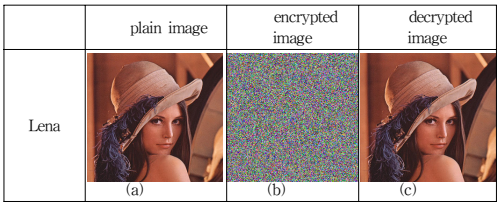
Fig. 1 Block diagram of the proposed image encryption scheme

Ⅳ. Experimental Results and Security Analysis

In this section, several experiments are employed to evaluate the proposed algorithm. We have used Matlab 9.0 to run encryption and decryption programs in a personal computer. The crucial measure for the quality of a cryptosystem is its capability to withstand the attempts of an unauthorized opponent. Color image "Lena" with 256×256 size was used for experimental purposes. Some security analysis has been performed on the proposed algorithm, including the most important ones like statistical analysis (including histogram, information entropy, and correlation of adjacent pixels), key space analysis and key sensitivity analysis, which has demonstrated the satisfactory security of the new scheme, as discussed in the following. Fig. 2 shows that the proposed algorithm can correctly encrypt and decrypt an image. The decoded image(c) is the same as the original image(a) and has the same histogram.

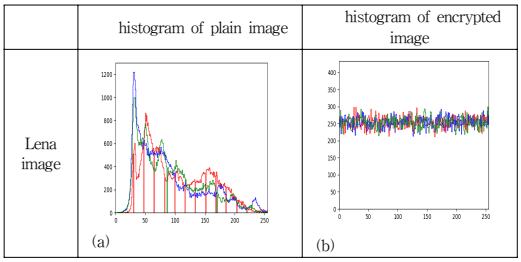
4.1. Histogram Analysis

A constant histogram of an encrypted image means that an opponent cannot obtain statistical information about the relation between plain image and encrypted image. The histogram for plain image and their encrypted image generated by the proposed algorithm is shown in Fig. 3. It's clear from Fig. 3(b) that the histogram of the encrypted image is fairly uniform and significantly different from that of the plain image. It follows from this result that the proposed algorithm yielded the encrypted image which had no histogram similarity to the original Lena image. Therefore the proposed encryption algorithm is resistant against statistical attacks.



(a) The plain image (b) The encrypted image (c) The decrypted image

Fig. 2 The color plain image and cipher image



(a) The histogram of plain image (b) The histogram of the encrypted image

Fig. 3 The histogram of the plain image Lena and the encrypted image

4.2 Information Entropy Analysis

Information entropy is the most important mathematical feature that measures the unpredictability of a source. When m is an information source, the information entropy is defined as Eq. (8).

$$H(m)=-\sum_{i=0}^{2^n-1} p(m_i)\log_2 p(m_i) \tag{8}$$

where n is the number of bits to represent a symbol $m_i \in m$ and $p(m_i)$ represents the probability of symbols m_i so that the entropy is expressed in bits. If the probability of occurrence of each pixel value of the information source is the same, then the information entropy value should be 8. This will be the maximum information entropy for an encrypted image that has true uniform pixel distribution. If the information entropy value of the encrypted image is close to the ideal maximum value 8, then it means that it has excellent random property against decipher attacks. Table 2 shows the entropy of the three color components (R, G, B). The entropy value obtained is very close to 8. Table 3 shows the entropy of images encrypted using the proposed algorithm and other algorithms. From the results in Table 3, it can be seen that the proposed image encryption algorithm has strong ability of resisting statistical attack.

4.3 Correlation Coefficient Analysis

The correlation coefficients between adjacent pixels should be significantly reduced in the ciphered image. An ideal algorithm should generate encrypted images with low correlation between its pixels. To test the correlation coefficients of plain image and ciphered image, the following procedures are carried out. First, randomly select 3000 pairs of two adjacent pixels from an image. Then, the correlation coefficients of adjacent pixels in vertical, horizontal and diagonal directions are evaluated using the following Eq. (9).

Table 2. Information entropies of plain images and encrypted images with the proposed algorithm

Image		Plain Image	Encrypted Image
Lena	R	6.8352	7.9972
	G	7.1195	7.9973
	B	7.5776	7.9974

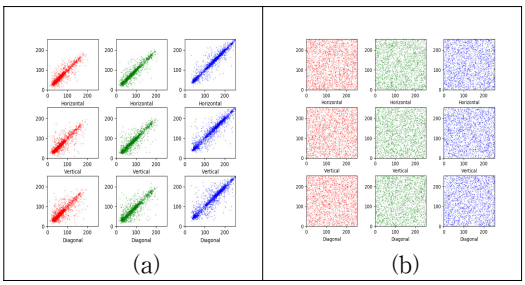
Table 3. The comparison of information entropy of encrypted images using several algorithms

	R	G	B
proposed algorithm	7.9972	7.9973	7.9974
Jeong et al.[2]		7.999	
Liu et al. [9]	7.9877	7.9881	7.9877
Niyat et al. [10]	7.9972	7.9973	7.9972
Mohamed et al. [11]	7.9899	7.9979	7.9979
Wang et al. [12]	7.9926	7.9934	7.9923

$$\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \\ cov(x,y) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \\ r_{xy} &= \frac{cov(x,y)}{\sqrt{D(x)}\ \sqrt{D(y)}}, \end{aligned} \tag{9}$$

where x and y are grayscale values of two adjacent pixels in the images and N is the number of selected adjacent pixels of the image in order to calculate the correlation. Table 4 shows the correlation coefficients of the encrypted images by the proposed algorithm. Table 5 shows the correlation coefficients (in vertical, horizontal and diagonal direction) of the encrypted images for selected plain images by the proposed algorithm and several algorithms. From Table 5, it can be seen that the correlation between two adjacent pixels of the cipher image is very close to zero and we can confirm that the proposed algorithm is more effective. Fig. 4 shows the correlation

diagram between adjacent pixels in the vertical, horizontal, and diagonal directions of the R, G, B channels of the plain Lena image and the encrypted Lena image.



(a) R, G, B channels of the plain Lena image (b) R, G, B channels of the encrypted Lena image

Fig. 4 Correlation distribution diagram of the plain Lena image and the encrypted Lena image.

Table 4. Correlation coefficients of the encrypted images by the proposed algorithm

	Direction	R	G	B
Encrypted Lena	Horizontal	0.0002	0.0010	-0.0007
	Vertical	-0.0025	-0.0007	-0.0023
	Diagonal	0.0002	-0.0025	0.0011

Table 5. Correlation coefficients of the encrypted images by the proposed algorithm and several algorithms

Image		Horizontal	Vertical	Diagonal
proposed algorithm	Lena	0.0002	-0.0025	0.0011
Niyat et al.[10]		0.0022	0.0001	0.0017
Mohamed[11]		0.0069	0.0023	0.0039

4.4 Sensitivity Analysis

As a general requirement for all the image encryption schemes, the encrypted image should be greatly different from its plain form. Such differences can be measured by means of two criteria namely, the NPCR and the UACI. NPCR represents the rate of pixel change between two cipher images after changing one pixel in the plain image. UACI is the intensity difference average between two encrypted images. NPCR and UACI are defined by Eq. (11) and Eq. (12) respectively.

$$D_{RGB}(i,j)=\begin{cases}0, & C_{RGB}(i,j)=C'_{RGB}(i,j)\\ 1, & C_{RGB}(i,j)\neq C'_{RGB}(i,j)\end{cases} \tag{10}$$

$$NPCR_{RGB}=\frac{\sum_{i,j} D_{RGB}(i,j)}{W\times H}\times 100\% \tag{11}$$

$$UACI_{RGB}=\frac{1}{W\times H}\left[\frac{\sum_{i,j}|C_{RGB}(i,j)-C'_{RGB}(i,j)|}{2^{L}-1}\right]\times 100\% \tag{12}$$

where W and H represent the width and height of the images, respectively, $C_{RGB}(i,j)$ and $C'_{RGB}(i,j)$ are the ith row and the jth column pixel values of the cipher images before and after one pixel of one plain image is changed respectively. The ideal value for NPCR is 100% while the ideal value for UACI is $33.\overline{33}\%$[13]. When the value of NPCR gets closer to 100%, the encryption algorithm is more sensitive to the changing of plain image, therefore the algorithm can effectively resist plaintext attack. Also when the value of NPCR gets closer to $33.\overline{33}\%$, the proposed algorithm can effectively resist differential attack. Table 6 shows $NPCR_{RGB}$ and $UACI_{RGB}$ performed for the selected images by the proposed algorithm and other algorithms. Table 6 shows the values of $NPCR(>99\%)$ and $UACI(\approx 33\%)$ for each color component image for three widely different nature images, showing thereby that the encryption scheme is very sensitive with respect to small changes in the plain image.

4.5 Key Space

The key space is the total number of different keys that can be used in the encryption/decryption process. To generate a key image, we need n-cell

MLCA and n-cell complement vector ($n \geq 8$). Since the number of rules applied to each cell is 2^8, the number of keys is 2^{8n}. The number of keys required for the initial values and complement vectors F is 2^{16}. The number of keys which are the control parameters in a generalized 3-D chaotic cat map is N^{14} where $N \times N$ is the size of a plain image. If $N=256$, then the size of key space is $2^{8n+16+112} > 2^{128}$. Therefore, the brute-force attack is not suitable for information eavesdroppers because the proposed color image encryption algorithm has a sufficiently large key space.

V. Conclusion

Conventional encryption algorithms might not be suitable for image encryption because of the large data size and high redundancy among the raw pixels of a digital image.

In this paper, we generalized the encryption method for color image proposed by Jeong et al.[2] to color image encryption using parametric 3-dimensional chaotic cat map using Laplace expansion and C-MLCA. Experimental results and security analysis showed that the correlation between the pixels of the image encrypted by the proposed encryption algorithm is reduced and the histogram of the encrypted image is uniformly distributed. Entropy values of encrypted images are more than 7.99 and very close to the ideal value.

Table 6. NPCR and UACI for encrypted images of selected images using proposed algorithm and other algorithms

Method		NPCR(%)			UACI(%)		
		R	G	B	R	G	B
proposed algorithm	Lena	99.9815	99.9800	99.9815	33.5476	33.6915	33.6615
Jeong et al.[2]			99.85				
Niyat et al.[10]		99.6357	99.6158	99.6247	33.4570	33.4705	33.4423
Wang et al.[12]		99.63	99.59	99.67	33.43	33.39	33.51

Our proposed encryption algorithm has a very good encryption effect and a sufficiently large key space. Experimental results also showed that the proposed algorithm can resist against noise with different intensity, differential attack and statistical analysis. All of these features demonstrate that the proposed method is suitable for encrypting digital images.

Acknowledgment

This paper is an extension of the 2019 Proceeding (KIECS) [Image Encryption by C-MLCA and 3-Dimensional Chaotic Cat Map].

References

[1] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Soliton Fract.,* vol. 21, no. 3, July 2004, pp. 749-761.

[2] H. Jeong, K. Park, S. Cho, and S. Kim, "Color medical image encryption using two-dimensional chaotic map and C-MLCA," In *Proc. of Int. Conf. on Ubiquitous and Future Networks,* Prague, Czech Republic, Aug. 2018, pp. 801-804.

[3] J. Von Neumann, *Theory of self-reproducing automata.* Urbana and London: University of Illinois Press, Urbana and London, 1966.

[4] S. Cho, U. Choi, H. Kim, Y. Hwang, J. Kim, and S. Heo, "New synthesis of one-dimensional 90/150 linear hybrid group cellular automata," *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems,* vol. 26, no. 9, Sept. 2007, pp. 1720-1724.

[5] P. P. Chaudhuri, D. R. Chowdhury, S. Nandi, and S. Chattopadhyay, *Additive cellular automata, Theory and applications, vol. 1.* Los Alamitos: California; IEEE Computer Society Press, 1997.

[6] H. Jeong, S. Cho, and S. Kim, "Medical image encryption based on C-MLCA and 1D CAT," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 14, no. 2, Apr. 2019, pp. 439-446.

[7] H. Kim, S. Cho, U. Choi, M. Kwon, and G. Kong, "Synthesis of uniform CA and 90/150 hybrid CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 3, Mar. 2016, pp. 293-302.

[8] Y. Wu, Z. Hua, and Y. Zhou, "*n*-dimensional discrete cat map generation using Laplace Expansions," *IEEE T Cybernetics,* vol. 46, no. 11, Nov. 2016, pp. 2622-2633.

[9] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.,* vol. 284, no. 16-17, Aug. 2011, pp. 3895-3903.

[10] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Laser Eng.,* vol. 90, Mar. 2017, pp. 225-237.

[11] F. K. Mohamed, "Fast encryption of RGB color digital images using a tweakable cellular automaton based schema," *Opt. Laser Technol.,* vol. 64, Dec. 2014, pp. 145-155.

[12] X. Wang, Y. Zhao, H. Zhang, and K. Guo, "A novel color image encryption scheme using alternate chaotic mapping structure," *Opt. Laser Eng.*, vol. 82, July 2016, pp. 79-86.

[13] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J.: Multidisciplinary J. in Science and Technology, J. of Selected Areas in Telecommunications (JSAT)*, Apr. 2011, pp. 31-38.

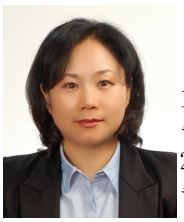
저자 소개

조성진(Sung-Jin Cho)

1979년 강원대학교 수학교육과 졸업(이학사)
1981년 고려대학교 대학원 수학과 졸업(이학석사)
1988년 고려대학교 대학원 수학과 졸업(이학박사)
1988년~ 현재 부경대학교 응용수학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

김한두(Han-Doo Kim)

1982년 고려대학교 수학과 졸업(이학사)
1984년 고려대학교 대학원 수학과 졸업(이학석사)
1988년 고려대학교 대학원 수학과 졸업(이학박사)
1989년~ 현재 인제대학교 컴퓨터공학부 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호



최언숙(Un-Sook Choi)

1992년 성균관대학교 산업공학과 졸업(공학사)
2000년 부경대학교 대학원 응용수학과 졸업(이학석사)
2004년 부경대학교 응용수학과 졸업(이학박사)
2009년 부경대학교 정보보호학과 졸업(공학박사)
2009년~ 현재 동명대학교 정보통신공학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

강성원(Sung-Won Kang)

2017년 부경대학교 응용수학과 졸업(이학사)
2019년 부경대학교 대학원 수학과 졸업(이학석사)
※ 관심분야 : 셀룰라 오토마타론, 정보보호