Color Medical Image Encryption Using Two-dimensional Chaotic Map and C-MLCA

Hyun-soo Jeong
Department of Information and Communications Engineering, Pukyong National University
Busan, Korea
s2oohj@gmail.com

Kyu-chil Park
Department of Information and Communications Engineering, Pukyong National University
Busan, Korea
kcpark@pknu.ac.kr

Sung-jin Cho
Department of Applied Mathematics, Pukyong National University
Busan, Korea
sjcho@pknu.ac.kr

Seok-tae Kim
Department of Information and Communications Engineering, Pukyong National University
Busan, Korea
setakim@pknu.ac.kr

***Abstract*—** In this paper, we propose a new color medical image encryption method using two-dimensional chaotic map and C-MLCA. The two-dimensional chaotic map is a structure with self-preserving properties, which moves the position of the pixel and encrypts the image. C-MLCA uses a maximum length PN sequence based on the properties of CA. The sequences with unpredictably complex rules create a basis image and the basis image is XOR-computed with the original image. That is, C-MLCA encrypts the image by changing the eigenvalues of the pixels through the computation process. Using these two features, we introduce an effective encryption method to overcome the limitations of the existing encryption methods. By comparing and analyzing the encrypted image with the original image, we were able to confirm that the proposed encryption method has a high level of stability and security.

Keywords*— *Image Encryption; Chaotic Map; C-MLCA; Color Medical Image; Wolfram Rule

I. INTRODUCTION

With the rapid change of the digital age, the number of digital medical devices used in the medical industry is increasing [1]. The introduction of PACS (Picture Archiving and Communication System) also made editing, searching, viewing, and sending of medical images much easier [2]. However, in the information age, digital medical images are exposed to various risks such as illegal copying, leakage and theft. As the dependence of PACS is getting higher, the encryption technology of medical image is essential for protecting the patients' privacy.

Many researchers have been studying on various image encryption methods. Widely practiced image encryption methods use random characteristics of the chaotic property. For example, there is a method based on 3D chaotic Maps developed by Chen [3] and Chaotic Logistic Map created by Pareek [4].

Also, there is ongoing research related to the encryption of medical images such as MRI, X-ray and PET images. Dagadu proposed an encryption method using Arnold map and logistic map; however, it has a weakness in that the encryption takes long due to the complex algorithms [5]. Dai suggests an encryption method based on composition of logistic maps and Chebyshev maps. Yet, it exhibits a low security level under continuous attacks [6]. Nam. T. H. applied the encryption method of non-linear cycle and CAT. But it fails to restore the original image without any loss and results in a low confidence level [7].

This paper attempts to overcome the problems of existing medical image encryption methods using two-dimensional chaotic map and C-MLCA. By analyzing the histogram and PSNR, we confirmed that this encryption method has been successfully performed. Also, we were able to confirm that the proposed encryption method has a high level of stability and security by analyzing correlation coefficient, entropy and NPCR. Finally, through the deletion attack experiment, we confirmed the robustness of the encrypted image against external attacks.

II. THEORETICAL ANALYSIS

A. Two-dimensional Chaotic Map

Various cryptographic studies based on chaotic properties are underway. The proposed two-dimensional chaotic map in this paper deforms the image by shearing and then rearranges such pieces into a newly generated image. It is mathematically given as:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & S_k \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \quad (1)$$

$$S_k = 2(1 + \sum_{n=2}^{k} 2^{n-1}) \, (k \geq 2) \quad (2)$$

S_k has a certain rule and it shows the degree of distortion of the image. It is an important factor for transforming the original shape of the image. The two-dimensional chaotic map has a self-preserving property and is able to realize the shearing effect of the image through the process of rotating n times [8]. Also, it can recover the original image without loss through the iterative calculation.

B. C-MLCA

Cellular Automata (CA) is a discrete-time dynamic system that can implement a transition function determining the next state by its own cell and the two neighborhood cells. It is defined by:

$$s_i^{t+1} = f(s_{i-1}^t, s_i^t, s_{i+1}^t) \tag{3}$$

s_i^t means the state of the i^{th} cell at time t and f is a function due to local interaction. Since the function f is a Boole function with three variables, the following state transition functions exist in 2^{2^3} cases. Wolfram proposed the system and it is expressed as Rules using each of 256 cases [9]. In this paper, we use Rule 90 and Rule 150, which are suitable for generating patterns that have linear characteristics and are difficult to predict.

Rule 90 and Rule 150 can be used to generate a state transition matrix which can create a CA sequence with the maximum period, and this is called Maximum Length CA (MLCA). MLCA has a feature that the minimum polynomial is the primitive polynomial. In order to convert the sequence into a more complex sequence, we perform XOR operation on the complemented vector. This is defined as:

$$\begin{aligned} S_{t+p} &= S_t \cdot \overline{T^p} \\ &= S_t \cdot (I \oplus T \oplus T^2 \oplus \cdots \oplus T^{p-1}) \cdot F \end{aligned} \tag{4}$$

The state transition matrix to which the complemented vector is applied can be expressed as $\overline{T}$ and it is written as $\overline{T^p}$ to express the vector applying p times. The complemented vector represents the component of the position to be reversed from the existing value. Even if the same state transition matrix is used, the state transition graph is different depending on which complemented vector is calculated. This results in an increased key space and can be an advantage.

C-MLCA (Complemented MLCA) is the MLCA which is a combination of XNOR logic and XOR logic [10]. The more complex the rules and the longer the cycle, the more effective the image encryption can be. Therefore, we can generate the C-MLCA by computing the complemented vector on the CA having the maximum length.

We can make the basis image using the C-MLCA sequence. The basis image is composed of a pseudo noise (PN) sequence which is hard to find a regularity. And it is created for XOR operation with the original image. Making the basis image can be implemented as shown in the following equation:

$$S_{r,c}^{(t)} = \sum_{r=1}^{N}\left(\sum_{t=1}^{N}(a_{r,1}^{(t)})\right) \cdot \sum_{t=1}^{N}\left(\sum_{r=1}^{N}\left(\sum_{c=1}^{N}(b_{r,c}^{(t)})\right)\right) \tag{5}$$

In the equation, a and b are rows and columns. First, initial values are set and then the sequence of rows is generated according to the change of the initial value. Afterwards, we can use the equation (5) to generate the basis image.

III. Experimental Result

A block diagram of the proposed image encryption is depicted in Fig. 1.

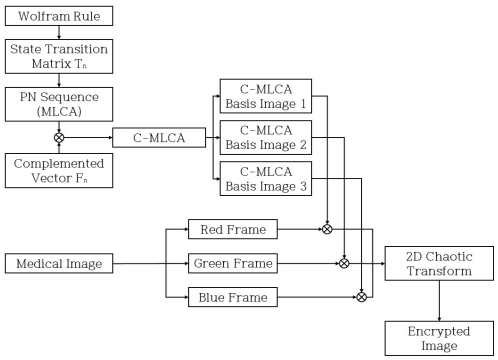
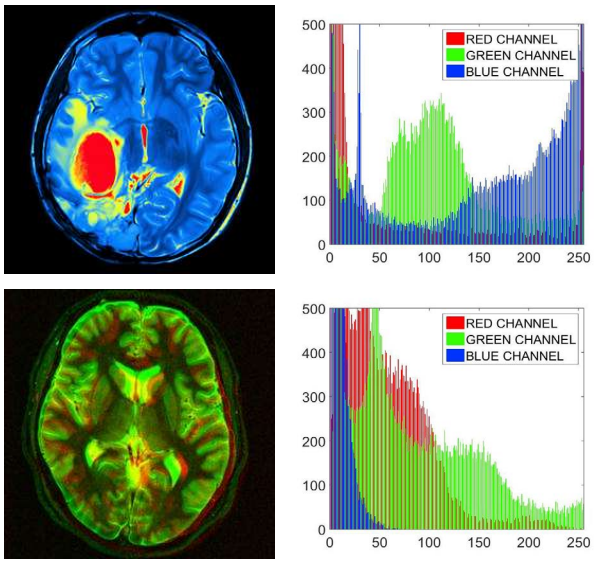


Fig. 1. Block diagram of the proposed image encryption

First, we create various state transition matrix T based on Wolfram rules. Using the transition matrix, we generate PN sequence with the maximum length and set a random initial value. Then we convert rows and columns with the set initial value and compute the complemented vector F to generate various C-MLCA sequences. Using the generated sequences, we can create three C-MLCA basis images. Each of the C-MLCA basis images is XOR-computed with red frame, green frame and blue frame of the original medical image for encryption. Lastly, we perform a conversion process using a two-dimensional chaotic map for more robust encrypted image.

For experiments, we used 100 different color medical images registered on Google website. Among them, we selected three color medical images (PET, MRI and X-ray images) with different color components. We recorded the results of the experiments in this paper.

The encrypted images are represented by a histogram for comparison with the original image, which are shown in Fig. 2 and Fig. 3.



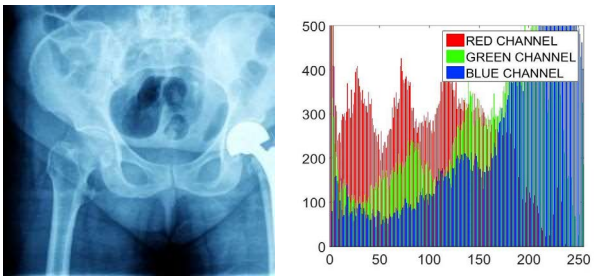


Fig. 2. Original medical images and their histogram

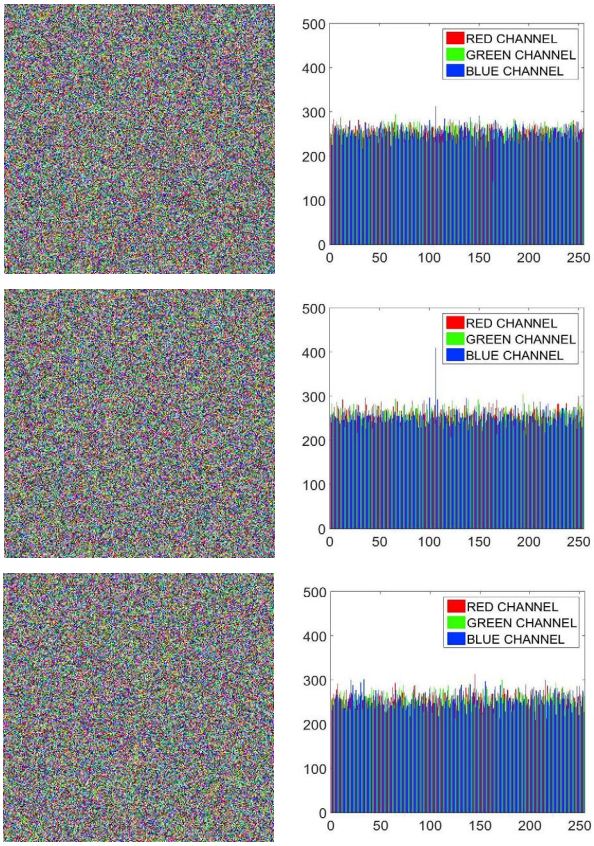


Fig. 3. Encrypted images and their histogram

The pixel distribution of the original medical images varies for each of the red, green, and blue channel. But, the encrypted images' distribution of the three channels is uniform. It means that the encrypted images are more secure against external attacks.

Lastly, we analyzed the computation time for 256×256 sized medical images on CPU 3.4 GHz with 8GB RAM computer. The average time taken to generate a C-MLCA basis image is 0.46 seconds by XOR operation with the PN sequence and the complemented vector. And the average time taken to process two- dimensional chaotic map is 1.06 seconds.

A. Correlation Coefficient

The higher the correlation coefficient between two adjacent pixels, the easier it is to extract information from the image. Hence, we assure a high level of stability when the correlation coefficient is low.

We randomly selected 3000 pairs of adjacent pixels. And the horizontal correlation coefficients from the original images and the encrypted images are plotted in graphs in Fig. 4.

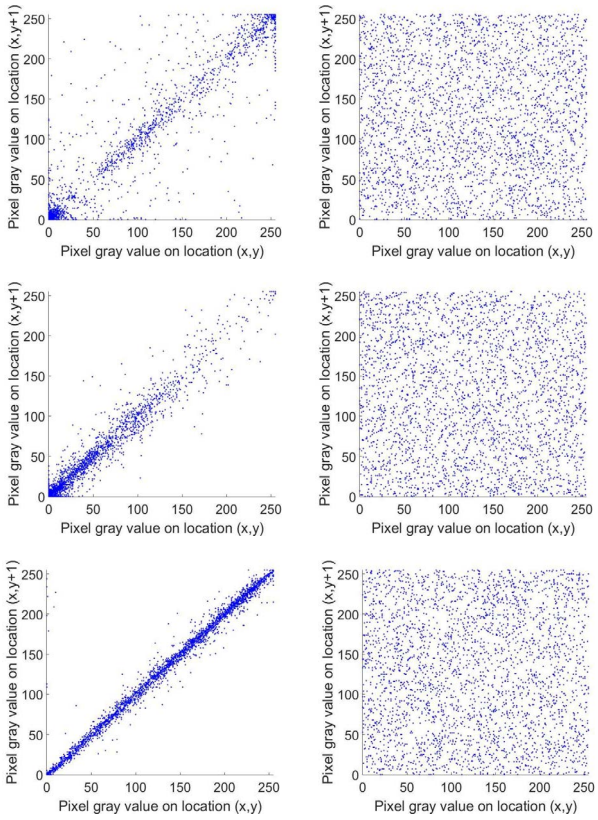


Fig. 4. Correlation coefficient of original medical images and encrypted images

The encrypted images are uniformly distributed on the x and y axes without regularity of the pixel positions. Therefore, the correlation coefficient is low. This means that the proposed image encryption is strong against statistical attacks and is difficult to extract the original image from the encrypted image.

B. Entropy and NPCR

Entropy represents the degree of how evenly distributed the original medical image and the encrypted image are. The closer to the numerical value 8, the more difficult it is to predict and the higher the randomness is. It means there is almost no duplication of information. It is mathematically given as:

$$H(S) = \sum_{i=0}^{N} P(s_i) \log_2 \frac{1}{P(s_i)} \tag{6}$$

The number of pixels change rate (NPCR) is used to evaluate the strength of the image encryption against attacks. A high NPCR score is generally highly resistant to differential attacks. This is defined by:

$$D(i,j) = \begin{cases} 0, & A(i,j) = B(i,j) \\ 1, & A(i,j) \neq B(i,j) \end{cases} \quad (7)$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (8)$$

In order to verify the superiority of the proposed encryption method, we compared entropy and NPCR with other encryption methods. The following Table 1 shows the results.

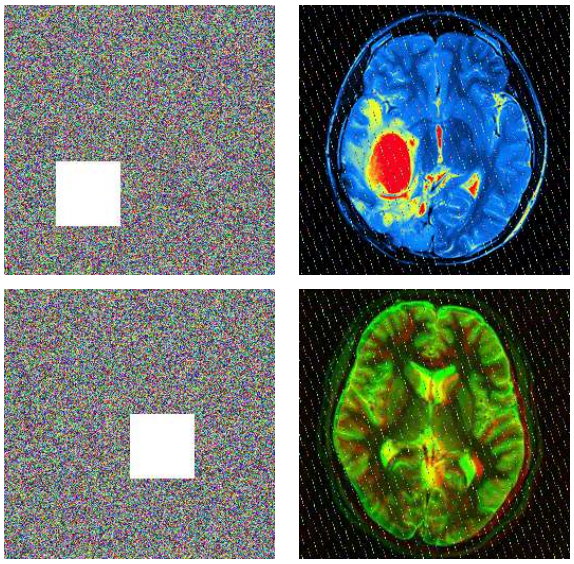
TABLE I. COMPARED WITH OTHER ENCRYPTION METHODS

Encryption Method	Parameter	
	Entropy	***NPCR***
Chen [3]	7.997	99.66%
Dagadu [5]	7.997	93.12%
Nam [7]	7.998	99.72%
Jeong	7.999	99.85%

We show that the proposed encryption method is more stable and superior to other encryption methods.

C. Deletion Attack

A deletion attack is a method which erases a part of the original image. The proposed encryption method can restore the original image as much as possible even if data loss occurs in the encrypted image. The test results are shown in Fig. 5.



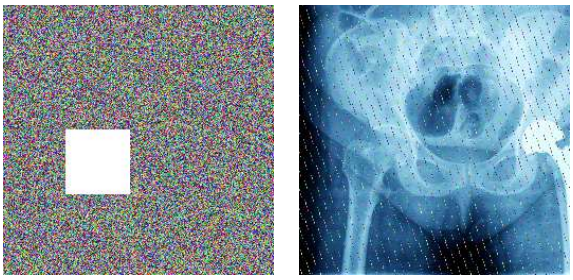


Fig. 5. Encrypted images with deletion attack and decrypted images

The PSNR between the original images and the decrypted images is 44.4691dB in average which is visually identifiable. We verify that the proposed encryption method is robust against deletion attacks.

IV. CONCLUSION

This paper proposes a new color medical image encryption method using two-dimensional chaotic map and C-MLCA. By analyzing the histogram and PSNR, we verify that the proposed encryption method has been successfully performed. We confirm its stability through various analysis and external attack experiments.

In the future, we are planning to work on simplifying the algorithm and shortening the encryption and decryption time. We will also commercialize the mobile PACS so that one can check his medical image records anytime and anywhere safely by applying the proposed encryption method.

REFERENCES

[1] S. A. Chowdhury, M. M. Saki Kowsar and K. Deb, "Human detection utilizing adaptive background mixture models and improved histogram of oriented gradients", ICT Express, 2017.

[2] G. T. Oh, Y. B. Lee and S. J. Yeom, "Security Mechanism for Medical Image Information on PACS Using Invisible Watermark," VECPAR 2004, 2005, pp. 315-324.

[3] G. Chen, Y. Mao and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons & Fractals, Vol. 21, Issue 3, 2004, pp. 749-761.

[4] N. K. Pareek, V. Patidar and K. K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing, Vol. 24, Issue 9, 2006, pp. 926-934.

[5] J. C. Dagadu, J. Li, E. O. Aboagye and X. Ge, "Chaotic Medical Image Encryption Based on Arnold Transformation and Pseudorandomly Enhanced Logistic Map," Journal of Multidisciplinary Engineering Science and Technology, Vol. 4, Issue 9, 2017, pp. 8096-8103.

[6] Y. Dai and X. Wang, "Medical image encryption based on composition of Logistic Maps and Chebyshev Maps," Proc. IEEE Int. Conf. Information and Automation, 2012, pp. 210-214.

[7] T. H. Nam, "Gradual Encryption of Medical Image using Non-linear Cycle and 2D Cellular Automata Transform," Journal of Korea Multimedia Society, Vol. 17, No. 11, 2014, pp. 1279-1285.

[8] H. S. Jeong, S. J. Cho and S. T. Kim, "A Novel Image Encryption Using Two-dimensional Chaotic Map," CEIC 2017, 2017, pp. 169-171.

[9] S. Wolfram, "Cryptography with cellular automata," In Advances in Cryptology Crypto '85 Proceedings, 1986, pp. 429-432.

[10] S. J. Cho, U. S. Choi and H. D. Kim, "Behavior of complemented CA which the complement vector is a cyclic in a linear TPMACA," Mathematical and Computer Modelling, 2002, pp. 979-986.