Regular paper

Journal of the KIECS. pp. 439-446, vol. 14, no. 2, Apr. 30. 2019, t. 94, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2019.14.2.439

C-MLCA와 1차원 CAT를 이용한 의료 영상 암호화

정현수* · 조성진** · 김석태***

Medical Image Encryption based on C-MLCA and 1D CAT

Hyun-Soo Jeong* · Sung-Jin Cho** · Seok-Tae Kim***

요 약

본 논문에서는 효율적으로 의료 영상을 보호하기 위하여 C-MLCA와 1차원 CAT를 이용한 암호화 방법을 제안한다. 먼저, Wolfram 규칙으로 상태 전이 행렬을 생성한 후 최대 길이의 수열을 만든다. 다음으로 여원 벡터를 곱하여 복잡한 수열로 변환한다. 그리고 두 수열을 행과 열로 곱하여 원 의료 영상 크기의 기저 영상을 생성한 후 XOR 연산을 한다. 마지막으로 게이트 웨이값을 설정하여 만들어진 1차원 CAT 기저함수와 CAT 변형 계수가 적용된 영상을 연산하면, 최종적으로 암호화된 영상을 얻을 수 있다. 암호화된 영상은 원 의료 영상과 비교하기 위해 히스토그램과 PSNR을 사용하여 평가한다. 또한 NPCR과 키 공간 분석을 통하여 제안한 방법의 안정성을 검증한다.

ABSTRACT

In this paper, we propose a encryption method using C-MLCA and 1D CAT to secure medical image for efficiently. First, we generate a state transition matrix using a Wolfram rule and create a sequence of maximum length. By operating the complemented vector, it converts an existing sequence to a more complex sequence. Then, we multiply the two sequences by rows and columns to generate C-MLCA basis images of the original image size and go through a XOR operation. Finally, we will get the encrypted image to operate the 1D CAT basis function created by setting the gateway values and the image which is calculated by transform coefficients. By comparing the encrypted image with the original image, we evaluate to analyze the histogram and PSNR. Also, by analyzing NPCR and key space, we confirmed that the proposed encryption method has a high level of stability and security.

키워드

C-MLCA, Cellular Automata Transform, Medical Image, Encryption Method
여원 MLCA, 셀룰러 오토마타 변환, 의료 영상, 암호화 방법

Ⅰ. 서 론

최근 의료계에서 사용되는 디지털 의료장비의 수가 증가하고 있다. 필름으로 대표되던 기존의 아날로그 영상 방식에서 디지털 방식으로 발전되어지고 있다. 디지털 의료 영상들을 효율적으로 관리하는 의료 영상 저장 전송 시스템(PACS, Picture Archiving and Communication System)은 진료의 질적 향상을 가져왔다. 이는 환자의 대기 시간 단축, 의료진의 진료 환경 개선, 진단의 정확성 및 효율성을 높여준다. 또한, 데이터베이스에 저장된 영상을 병원이 아닌 외부 무선통신망을 통하여 조회, 저장, 전송 등이 가능하며

* 부경대학교 정보통신공학과(s2oohj@gmail.com)
** 부경대학교 응용수학과(sjcho@pknu.ac.kr)
*** 교신저자 : 부경대학교 정보통신공학과
· 접 수 일 : 2019. 01. 15
· 수정완료일 : 2019. 03. 01
· 게재확정일 : 2019. 04. 15
· Received : Jan. 15, 2019, Revised : Mar. 01, 2019, Accepted : Apr. 15, 2019
· Corresponding Author : Seok-Tae Kim
Dept. : Information and communications Engineering, Pukyong National University
Email : setakim@pknu.ac.kr

영상의 편집 또한 가능해졌다[1-2].

하지만 정보화 시대가 데이터의 변형, 복사, 위조 등과 같은 심각한 문제들을 일으키고 있다. 이처럼 디지털 의료 영상 또한 불법적인 정보 유출 및 도용으로 인한 환자 개인 프라이버시 침해 문제의 위험이 있다. 시간이 지날수록 의료기관의 PACS 의존도는 높아지기에, 의료 영상 정보를 암호화하여 안전하게 전송하는 기술은 개인 정보보호 차원에서 꼭 필요하다.

환자의 의료 영상 정보를 보호하기 위해 다양한 암호화에 관한 연구들이 진행 중이다. Ashtiyani은 대칭형 알고리즘을 이용한 방법을 제안하였으나 픽셀 값의 분포가 고르지 못하여 외부 공격으로부터 정보가 쉽게 노출될 수 있는 단점이 있다[3]. Dai는 Logistic Maps과 Chebyshev Maps를 이용한 방법을 제안하였으나 반복적인 공격에 대해 안정성이 낮은 단점이 있다[4]. Dagadu는 Arnold Map과 Logistic Map을 이용한 방법을 제안하였으나 초기 키 생성을 위한 알고리즘이 복잡하다는 단점이 있다[5].

본 논문에서는 기존의 의료 영상 암호화 방법들의 문제점을 보완하기 위한 새로운 암호화 방법을 제안한다. 먼저, Wolfram 규칙으로 상태 전이 행렬을 생성한 후 최대 길이의 수열을 만든다. 다음으로 여원 벡터를 곱하여 복잡한 수열로 변환한다. 그리고 두 수열을 행과 열로 곱하여 원 의료 영상 크기의 기저 영상을 생성한 후 XOR 연산을 한다. 마지막으로 게이트웨이값을 설정하여 만들어진 1차원 CAT(Cellular Automata Transform) 기저함수와 CAT 변형 계수가 적용된 영상을 연산하면, 최종적으로 암호화된 영상을 얻을 수 있다. 암호화된 영상은 원 의료 영상과의 픽셀 값의 분포를 비교하기 위해 히스토그램과 PSNR(Peak Signal to Noise Ratio)을 사용하여 평가한다. 또한 NPCR(Number of Pixels Change Rate)과 키 공간 분석을 통하여 제안한 방법의 반복적인 공격에 대한 안정성을 검증한다.

II. 관련 이론

2.1 CA

CA(Cellular Automata)는 이산 시간의 동적 시스템이며, 구성 요소 중 셀(Cell)은 기본 단위 메모리로 일정하게 배열된 공간 격자의 점이다. 셀이 가질 수 있는 변수는 0과 1, 두 가지이다[6].

Wolfram은 자기 자신의 셀과 이웃한 두 셀의 값에 의해 다음 상태를 결정하는 시스템을 제안하였으며 식 (1)과 같다.

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

s_i^t는 시간 t에서의 i번째 셀의 상태를 의미하며, f는 국소적인 상호작용에 의한 함수이다. f는 3개의 변수를 가지는 부울(Boole) 함수이며, 다음 상태 전이 함수 f는 2^{2^3}개, 즉 256개의 경우의 수가 존재한다.

Wolfram은 각각 256가지의 결과 값을 이용하여 규칙으로 표현하였다[7]. 전이규칙을 부울 식으로 나타냈을 때, XOR 함수로 이루어질 수 있는 CA를 선형 CA(Linear CA)라 한다. 대표적으로 규칙 90과 규칙 150이 있으며 부울 식은 표 1과 같다[8-9].

표 1. 규칙 90과 규칙 150의 부울 식
Table 1. Boole function of rule 90 and rule 150

Rule	Boole function
90	$q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$
150	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$

본 논문에서는 규칙 90과 규칙 150으로 구성된 상태 전이 행렬을 사용하였으며, 경계 조건으로는 IBCA 방식을 채택하였다. IBCA는 첫 번째 셀의 왼쪽 성분을 세 번째 셀로, 마지막 셀의 오른쪽 성분을 끝에서 세 번째 셀로 정의한 CA이며, 이는 그림 1과 같다.

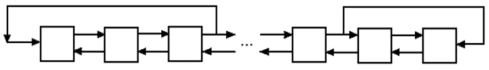

그림 1. IBCA 경계조건
Fig. 1 IBCA(Intermediate Boundary Cellular Automata)

2.2 C-MLCA

세 개의 이웃을 가지는 CA에 1을 XOR 연산한 번째 셀의 상태 전이함수는 식 (2)와 같다.

$$\overline{s_i^{t+1}} = f(s_{i-1}^t, s_i^t, s_{i+1}^t) \oplus 1 \tag{2}$$

CA가 가질 수 있는 변수는 0 또는 1이므로, 1을 여원(Complement)이라 한다. 1을 XOR 연산함으로 CA의 다음 상태는 여원 규칙에 따라 변화하게 된다. 여원을 벡터로 표현하면 여러 비트의 성분을 바꿀 수 있다. 기존 값에서 역으로 바꿀 위치의 성분을 나타내는 벡터를 여원 벡터(Complemented Vector)라 한다.

S_t가 시간 t에서 CA의 상태를 나타낼 때, 여원 벡터 F를 XOR 연산한 시간 $t+p$에서 CA 상태 $t+p$는 식 (3)과 같다[10-11].

$$S_{t+p} = \overline{T^p} \bullet S_t \tag{3}$$

행렬 T는 S_t의 다음 상태를 결정하기 때문에 이를 상태 전이 행렬이라 한다. 여원 규칙이 적용된 상태 전이 행렬은 $\overline{T}$로 표현하였다. $\overline{T}$를 p번 적용한 것을 $\overline{T^p}$라 할 때, 이는 식 (4)와 같다.

$$\overline{T^p} = T^p S_t \oplus (I \oplus T \oplus \cdots \oplus T^{p-1}) \bullet F \tag{4}$$

상태 전이 행렬을 반복 연산하였을 때, 모든 상태들이 일정한 주기를 이룬다. CA의 최소다항식이 원시다항식인 경우에 최대 길이의 주기를 가지게 되는데 이를 MLCA(Maximum Length CA)라 한다. 최대 길이를 갖는 CA에 여원 벡터를 연산함으로 C-MLCA를 만들 수 있다.

C-MLCA(Complemented-MLCA)는 각 셀에 적용되는 규칙이 XNOR 논리와 XOR 논리의 조합으로 이루어진 MLCA를 말한다. 임의의 원시다항식에 대응되는 최대 길이를 갖는 선형 CA는 2개 존재하지만, 이러한 제약을 극복하고 보다 많은 MLCA를 찾을 수 있다. 이는 더 많은 키 공간을 확보할 수 있다는 것을 의미한다.

2.3 1D CAT

CAT(Cellular Automata Transform)는 CA 규칙을 활용하여 만들어진 기저함수를 이용한 변환법이다. 먼저 CA 변환은 식 (5)와 같다[12].

$$f_i = \sum_k c_k A_{ik} \tag{5}$$

A는 CAT의 기저함수, k는 음의 정수가 아닌 공간 벡터, c는 변환 계수를 나타낸다. CAT 기저함수는 Wolfram 규칙, 셀의 개수, 초기 값, 경계 구성, 그리고 기저 함수 타입에 의해 생성되는데, 이를 게이트웨이(Gateway) 값이라 한다. 이 게이트웨이값으로 갱신되는 셀들의 상태 전이 함수식은 식 (6)과 같다.

$$a_{(r)(t+1)} = \left(\sum_{j=0}^{2^m-2} W_j \alpha_j + W_{2^m-1}\right)^{W_{2^m}} \bmod K \tag{6}$$

W_j는 CA 규칙에 의해 결정되며, 2진으로 표현하여 8비트로 나타낼 수 있다. α_j는 이웃 셀 상태조합으로 시간 t에서 a_{0k}, a_{1k}, a_{2k} 순으로 정의한다. 위 식에서 구한 a_{ik}를 통해 1차원 기저함수를 구하는 식은 식 (7)과 같다.

$$A_{ik} = 2a_{ik}a_{ki} - 1 \tag{7}$$

예를 들어 규칙이 172이고, 셀의 초기 값이 10101101일 때의 CA의 상태는 표 2와 같으며 t=8일 때 원 상태로 돌아오는 것을 알 수 있다. 식 (7)을 이용하여 1차원 기저함수 A_{ik}를 계산하였을 때의 결과는 식 (8)과 같다.

표 2. 게이트웨이값의 예시
Table 2. Example of gateway values

t=1	1	1	0	1	0	1	1	0
t=2	0	1	1	0	1	0	1	1
t=3	1	0	1	1	0	1	0	1
t=4	1	1	0	1	1	0	1	0
t=5	0	1	1	0	1	1	0	1
t=6	1	0	1	1	0	1	1	0
t=7	0	1	0	1	1	0	1	1
t=8	1	0	1	0	1	1	0	1

$$A_{ik}=\begin{pmatrix}+1-1-1+1-1+1-1-1\\-1+1-1-1+1-1+1-1\\-1-1+1-1-1+1-1+1\\+1-1-1+1-1-1+1-1\\-1+1-1-1+1-1-1+1\\+1-1+1-1-1+1-1-1\\-1+1-1+1-1-1+1-1\\-1-1+1-1+1-1-1+1\end{pmatrix} \quad (8)$$

CA는 단순 경계 조건과 규칙에 따라 영상을 변환시키지만, CAT는 셀들의 초기 값, 경계 조건, 셀 공간 및 구조의 형태, 셀 공간 차원 등을 이용한 새로운 영상 변환법이다.

III. 실험 방법

본 논문에서는 C-MLCA와 1차원 CAT를 이용한 새로운 영상 암호화 방법을 제안한다. 제안한 영상 암호화 방법은 그림 2와 같이 먼저 C-MLCA 암호화한 다음 1차원 CAT 암호화하는 두 가지 절차를 거친다.

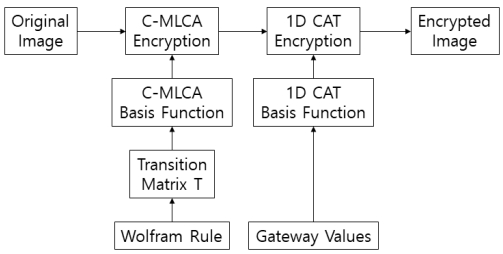

그림 2. 영상 암호화 과정
Fig. 2 Block diagram of the image encryption

먼저, Wolfram 규칙으로 상태 전이 행렬 T를 생성한 후 최대 길이의 수열을 만든다. 다음으로 여원 벡터를 곱하여 조금 더 복잡한 수열로 변환한다. 그리고 두 수열을 행과 열로 곱하여 원 의료 영상 크기의 기저 영상을 생성한 후 XOR 연산을 한다. 마지막으로 게이트웨이값을 설정하여 만들어진 1차원 CAT 기저함수와 CAT 변형 계수가 적용된 영상을 연산하면 최종적으로 암호화된 영상을 얻을 수 있다.

표 2. C-MLCA 파라미터
Table 2. C-MLCA Parameter

Initial Configuration	01101011
Transition matrix T_1	<90,150,150,150, 150,90,90,150>
Complemented vector F_1	10100100
Transition matrix T_2	<90,150,150,150, 150,90,90,150>
Complemented vector F_2	00101111
Boundary Configuration	IBCA

제안한 암호화 과정에서 사용되는 상태 전이 행렬은 규칙 90과 규칙 150으로 구성된 8×8 행렬이며, 표 2의 파라미터 값으로 C-MLCA 수열을 생성하였다.

생성된 두 개의 C-MLCA 수열은 식 (9)와 식 (10), 식 (11)과 같이 행과 열을 서로 곱하여 기저 영상을 생성할 수 있다.

$$I=\sum_{r=1}^{256}(\sum_{c=1}^{256}I_{r,c})=(I_{1,1},I_{1,2},\cdots,I_{256,256}) \quad (9)$$

$$S_{r,c}^{(t)}=\sum_{r=1}^{N}\sum_{t=1}^{N}(a_{r,1}^{(t)})\cdot\sum_{t=1}^{N}(\sum_{r=1}^{N}(\sum_{c=1}^{N}b_{r,c}^{(t)})) \quad (10)$$

$$E=I_{1,1}\oplus S_{1,1}^{(1)},I_{1,2}\oplus S_{1,2}^{(1)},\cdots, I_{1,256}\oplus S_{1,256}^{(1)},\cdots,I_{256,256}\oplus S_{256,256}^{(256)} \quad (11)$$

다음으로, 1차원 CAT를 이용하여 영상을 암호화한다. 표 3의 게이트웨이값을 이용하여 1차원 CAT 기저 함수를 생성할 수 있으며, 이를 그림 3으로 나타내었다.

표 3. 1차원 CAT 게이트웨이값
Table 3. 1D CAT Gateway values

Wolfram Rule Number	172
N	8
Initial Configuration	10101101
Boundary Configuration	Cyclic
Basis Function Type	2

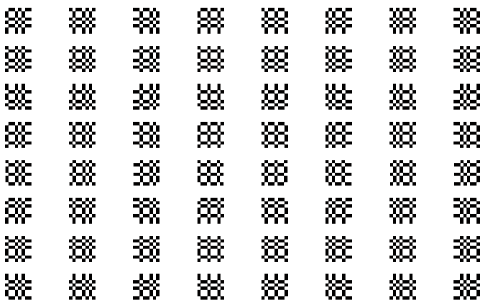

그림 3. 1차원 CAT 기저 함수
Fig. 3 1D CAT basis function

생성된 1차원 CAT 기저함수와 CAT 변형 계수가 적용된 영상을 최종적으로 연산을 하였을 때 암호화된 영상을 획득하게 된다. 본 논문에서 제안하는 암호화 방법을 평가하기 위해 256×256 크기의 8bit 그레이 의료 영상으로 실험하였다.

Ⅳ. 실험 결과 및 분석

본 논문에서는 다양한 8bit 그레이 의료 영상들 중 3개의 의료 영상에 대한 데이터를 기재하였으며, 실험 결과는 그림 4, 그림 5, 그림 6과 같다.

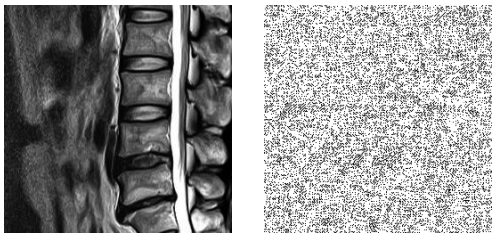

그림 4. 원 영상과 암호화된 영상 (1)
Fig. 4 Original image and encrypted image (1)

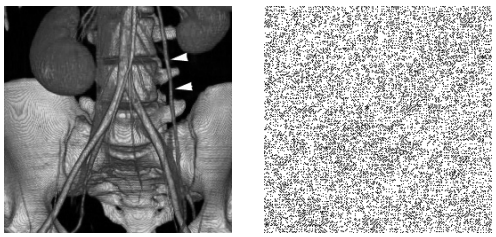

그림 5. 원 영상과 암호화된 영상 (2)
Fig. 5 Original image and encrypted image (2)

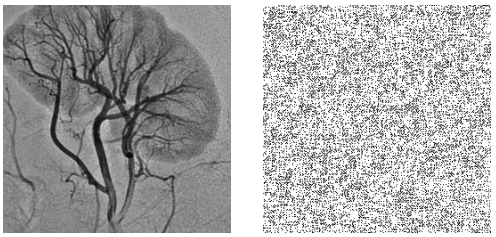

그림 6. 원 영상과 암호화된 영상 (3)
Fig. 6 Original image and encrypted image (3)

PSNR(Peak Signal to Noise Ratio)은 원 영상에 대한 암호화된 영상의 노이즈 비율을 수치로 표현하는 파라미터이다. 두 영상 간의 PSNR을 구하는 방법은 식 (12)와 식 (13)과 같다.

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (I_{ij} - K_{ij})^2 \tag{12}$$

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{13}$$

영상 정보일 경우 평균 35dB 이하일 때 육안으로 원 영상의 형태를 알아보기 어렵다. 원 의료 영상과 암호화된 영상을 서로 비교한 PSNR 값은 다음 표 4와 같으며, 암호화된 영상이 수치적으로 영상의 왜곡이 있음을 알 수 있다.

표 4. PSNR 값
Table 4. PSNR Value

Medical image	PSNR[dB]
Image 1	31.4255
Image 2	31.8983
Image 3	31.1580

히스토그램(Histogram)은 픽셀 값을 막대 모양으로 표시하여 영상을 분석하는 파라미터이다. 원 의료 영상과 암호화된 영상의 픽셀(Pixel)의 분포도를 비교한 결과는 그림 7, 그림 8, 그림 9와 같다.

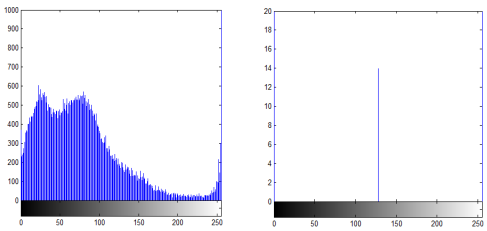

그림 7. 원 영상과 암호화된 영상의 히스토그램 (1)
Fig. 7 Original medical image's and encrypted image's histogram (1)

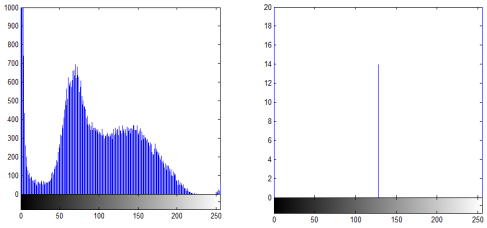

그림 8. 원 영상과 암호화된 영상의 히스토그램 (2)
Fig. 8 Original medical image's and encrypted image's histogram (2)

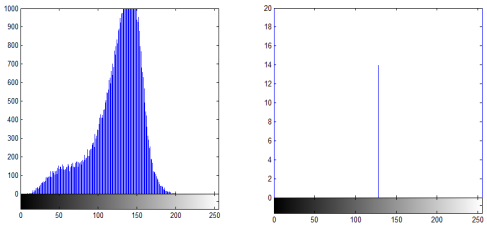

그림 9. 원 영상과 암호화된 영상의 히스토그램 (3)
Fig. 9 Original medical image's and encrypted image's histogram (3)

원 영상과 달리 암호화된 영상의 히스토그램은 0과 128, 그리고 255의 성분으로 출력됨을 확인할 수 있다. 이는 외부 공격으로부터 강하다는 것을 의미하며, 암호화가 잘 되었다고 평가할 수 있다.

4.1 키 공간 분석

CA의 키 공간을 구하는 방법은 식 (14)와 같다.

$$N_T = K^{k^m + N + 2T} \tag{14}$$

k는 셀의 상태, m은 자기 자신과 이웃 셀들의 합, N과 T는 셀의 공간을 의미한다. 표 2의 파라미터로 구성된 C-MLCA는 여원 벡터의 경우의 수까지 포함하여 2^{80}의 일정한 키를 생성할 수 있다. 또한, 표 3의 파라미터로 구성된 1차원 CAT는 2^{32}의 키 공간을 가진다. 따라서 총 2^{112} 가지의 서로 다른 키를 생성할 수 있어 높은 암호화 수준을 확보할 수 있다.

4.2 NPCR 분석

NPCR(Number of Pixels Change Rate)은 인접한 두 픽셀간의 민감도를 분석하는 데 주로 사용되는 안정성 분석법이며, 식 (15)와 식 (16)과 같다.

$$D(i,j) = \begin{cases} 0, A(i,j) = B(i,j) \\ 1, A(i,j) \neq B(i,j) \end{cases} \tag{15}$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{16}$$

암호화된 영상의 NPCR은 표 5와 같으며, 차등 공격과 같은 암호 해독에 대한 저항이 높다고 평가할 수 있다. 또한, 표 6과 같이 타 암호화 방법과 비교하였을 때, 제안한 방법이 우수하다는 사실을 알 수 있다. 타 암호화 방법의 NPCR은 각 논문에 나와 있는 수치를 참고하였다.

표 5. NPCR 값
Table 5. NPCR Value

Medical image	NPCR[%]
Image 1	99.97
Image 2	99.97
Image 3	99.96

표 6. 타 암호화 방법과 비교
Table 6. Compared with other encryption methods

Methods	NPCR[%]
Dagadu[5]	93.12
Wong[13]	99.62
Zhou[14]	99.64
Zhang[15]	98.67
Proposed	99.97

Ⅴ. 결 론

본 논문에서는 기존의 의료 영상 암호화 방법들의 문제점을 극복하기 위하여 두 가지의 CA 성질을 이용한 암호화 방법을 제안하였다. 제안한 암호화 방법을 평가하기 위해 그레이 의료 영상으로 실험하였다.

원 영상과 암호화된 영상의 PSNR과 히스토그램 분석을 통해 외부 공격으로부터 강하다는 것을 확인하였다. 또한 NPCR은 평균 99.97%로 타 암호화 방법과의 비교를 통해 제안한 암호화 방법의 우수함을 확인하였다.

향후 환자의 의료 영상 보호를 위한 연구에 도움이 되고, 제안한 방법을 기반으로 한 다양한 분야에서 실생활에 적용이 되길 기대한다.

감사의 글

본 논문은 부경대학교 자율창의학술연구비(2017년)에 의하여 연구되었음

References

[1] F. Cao, H. K. Huang, and X. Q. Zhou, “Medical image security in a HIPAA mandated PACS environment,” *Computerized Medical Imaging and Graphics 27*, vol. 23, issue 2-3, 2003, pp. 185-196.

[2] G. Oh, Y. Lee, and S. Yeom, “Security Mechanism for Medical Image Information on PACS Using invisible Watermark,” *High Performance Computing for Computational Science - VECPAR 2004*, Valencia, June, 2004, pp. 315-324.

[3] M. Ashtiyani, P. M. Birgani, and H. M. Hosseini, “Chaos-Based Medical Image Encryption Using Symmetric Cryptography,” *3rd International Conf. on Information and Communication Technologies: From Theory to Applications*, Damascus, Apr. 2008, pp. 1-5.

[4] Y. Dai and X. Wang, “Medical image encryption based on composition of Logistic Maps and Chebyshev Maps,” *Proc. IEEE Int. Conf. Information and Automation*, China, June, 2012, pp. 210-214.

[5] J. Dagadu, J. Li, E. Aboagye, and X. Ge, “Chaotic Medical Image Encryption Based on Arnold Transformation and Pseudorandomly Enhanced Logistic Map,” *J. of Multidisciplinary Engineering Science and Technology*, vol. 4, issue 9, 2017, pp. 8096-8103.

[6] J. Von Neumann, “The general and Logical Theory of Automata,” *Collected Works*, vol. 5, 1963, pp. 288-326.

[7] S. Wolfram, “Cryptography with cellular automata,” *In Advances in Cryptology Crypto ’85 Proc.*, Springer-Verlag, vol. 218, 1986, pp. 429-432.

[8] H. Ð.—Kim, S. J. Cho and U. S.—Choi, “On the Construction of the 90/150 State Transition Matrix Corresponding to the Trinomial x^(2^n-1)+x+1,“ *J. of the Korea Institute of Electronic Communication Sciences*, vol. 13, no. 2, Apr. 2018, pp. 383-390.

[9] 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.

[10] U. Shoi and S. Cho, “Generation of Maximum Length Cellular Automata,“ *J. of the Korea Institute of Information Security & Cryptology*, vol. 14, no. 6, 2004, pp. 25-30.

[11] H. Jeong, S. Cho, K. Park, and S. Tim, “Color Medical Image Encryption Using Two-dimensional Chaotic Map and C-MLCA,” *The 11th Int. Conference on Ubiquitous and Future Networks*, Prague, July, 2018, pp. 801-804.

[12] O. Lafe, *Cellular Automata Transform: Theory and Application in Multimedia Compression, Encryption, and Modeling*, Boston, MA : Kluwer Academic Publishers, 2000.

[13] K. Wong, B. Kwok, and W. Law, “A fast image encryption scheme based on chaotic standard map,” *Physics Letters A*, vol. 372, issue 15, 2008, pp. 2645-2652.

[14] Q. Zhou, K. Wong, X. Liao, T. Xiang, and Y. Hu, “Parallel Image Encryption Algorithm based on discretized chaotic map,” *Chaos, Solitons and Fractals*, vol. 38, issue 4, 2008, pp. 1081-1092.

[15] L. Zhang, X. Liao, and X. Wang, “An Image

Encryption Approach based on chaotic maps," *Chaos, Solitons and Fractals*, vol. 24, issue 3, 2005, pp. 759-765.

저자 소개

정현수(Hyun-Soo Jeong)

2016년 부경대학교 정보통신학과 졸업(공학사)
2018년 부경대학교 대학원 정보통신학과 졸업(공학석사)
2018년 ~현재 부경대학교 대학원 정보통신학과 박사과정
※ 관심분야 : 셀룰라 오토마타, 영상 처리

조성진(Sung-Jin Jo)

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

김석태(Seok-Tae Kim)

1983년 광운대학교 전자공학과 졸업(공학사)
1988년 Kyoto Institute of Technology 전자공학과 졸업(공학석사)
1991년 오사카대학교 통신공학과 졸업(공학박사)
1999년 Univ. of Washington, USA, 방문교수
2006년 Univ. of Simon Fraser, Canada, 방문교수
1991년 ~현재 부경대학교 정보통신공학과 교수
※ 관심분야 : 영상처리, 영상 암호화, Cellular Automata