Journal of Korea Multimedia Society Vol. 24, No. 3, March 2021(pp. 406-415)
https://doi.org/10.9717/kmms.2020.24.3.406

1차원 FN-MLCA와 3차원 카오틱 캣 맵 기반의 컬러 이미지 암호화

최 언 숙†

1D FN-MLCA and 3D Chaotic Cat Map Based Color Image Encryption

Un Sook Choi†

ABSTRACT

The worldwide spread of the Internet and the digital information revolution have resulted in a rapid increase in the use and transmission of multimedia information due to the rapid development of communication technologies. It is important to protect images in order to prevent problems such as piracy and illegal distribution. To solve this problem, I propose a new digital color image encryption algorithm in this paper. I design a new pseudo-random number generator based on 1D five-neighborhood maximum length cellular automata (FN-MLCA) to change the pixel values of the plain image into unpredictable values. And then I use a 3D chaotic cat map to effectively shuffle the positions of the image pixel. In this paper, I propose a method to construct a new MLCA by modeling 1D FN-MLCA. This result is an extension of 1D 3-neighborhood CA and shows that more 1D MLCAs can be synthesized. The safety of the proposed algorithm is verified through various statistical analyses.

Key words: Color Image Encryption, Symmetric Key Cryptography, Cellular Automata, Characteristic Polynomial, Chaotic Cat Map

1. 서 론

클라우드, 인공 지능, 빅 데이터와 같은 다양한 기술의 발전으로 데이터양이 폭발적으로 증가하고 있다. 이와 함께 5세대 이동 통신과 같은 무선 네트워크 기술, 멀티미디어 디스플레이 장치 기술의 급속한 발전으로 수많은 멀티미디어 정보가 인터넷을 통해 전송 및 공유된다. 따라서 불법 복제 및 불법 배포와 같은 문제로부터 이미지를 보호하는 것은 매우 중요하다. 특히 군사, 의료, 금융 등의 시스템에서 개인 정보 또는 기밀 정보를 보호하기 위해서는 안정적이고 강력한 보안 시스템이 필요하다. 암호화는 정보를 효과적으로 보호할 수 있는 기술 중 하나이다. 암호화는 군사 이미지, 의료 이미지 및 개인의 정보를 포함한 이미지와 같은 중요하고 민감한 원본 이미지를 알아볼 수 없는 이미지로 만들어 이미지에 대한 권한이 없는 자들로부터 이미지를 안전하게 보호할 수 있다[1]. 암호의 표준으로 잘 알려진 AES(Advanced Encryption Standard), DES(Data Encryption Standard) 등과 같은 기존 암호화 기술은 이미지를 암호화하는데 충분하지 못하다는 것이 잘 알려져 있다[2, 3]. 이는 이미지 데이터는 텍스트 데이터와 달리 데이터의 용량이 크고 인접한 이미지 픽셀 사이의 높은 중복도와 강한 상관관계를 갖기 때문이다. 따라서 기

※ Corresponding Author : Un Sook Choi, Address: (48520) 428 Sinseon-ro, Nam-gu, Busan, Korea, TEL : +82-51-629-2824, FAX : +82-51- 629-1519, E-mail : choies@tu.ac.kr
Receipt date : Jan. 28, 2021, Revision date : Mar. 8, 2021
Approval date : Mar. 10, 2021
† Dept. of Information, Communications & Software Engineering, Tongmyong University

존 암호화 기술보다 더 나은 성능을 제공하는 이미지 암호화 알고리즘이 필요하다. 이미지 암호를 위한 여러 가지 기법 중 카오스 함수 기반의 이미지 암호 기술이 연구자들에 의해 활발히 연구되고 있다[3-11]. 카오스 이론은 여러 과학 및 기술 분야에서 광범위하게 연구되는 복잡한 비선형 역학 분야이다. 카오스 함수는 초기 조건에 대한 민감도, 조밀한 주기적 궤도와 같은 특징을 가지고 있기 때문에 이미지 암호화 영역에서 널리 사용된다.

셀룰라 오토마타(Cellular automata, 이하 CA)는 단순한 규칙 구조, 국소적 상호 작용, 임의의 유사한 동작 및 대규모 병렬 처리의 장점을 가지고 있는 동역학계이다. 이러한 CA 중 최대길이를 가지는 CA는 훌륭한 랜덤수열을 생성할 수 있어 이미지 암호에 도입되었다[12-16].

본 논문에서는 CA와 카오틱 함수 기반의 새로운 컬러 이미지 암호화 알고리즘을 제안한다. 키 공간을 효과적으로 확장하기 위해 1차원 5이웃 최대길이 CA (five-neighbour maximum length CA, 이하 FN-MLCA)를 설계하고, 1차원 FN-MLCA에 의해 생성된 수열을 이용하여 원 이미지의 픽셀값을 예측할 수 없는 값으로 변경한다. 이 후 노이즈 및 삭제공격에 강한 암호시스템을 위해 이미지 픽셀의 위치를 효과적으로 섞는다. 이를 위해 3차원 카오틱 캣 맵을 사용한다. 제안된 새로운 이미지 암호 알고리즘의 보안성과 신뢰성을 입증하기 위해 실험을 통한 상세한 분석을 수행한다. 본 논문의 구성은 다음과 같다. 2절에서 관련 연구로 카오틱 함수 기반의 암호알고리즘과 CA 기반의 이미지 암호에 대해 정리하고 3절에서 1차원 FN-MLCA의 설계와 새로운 이미지 암호알고리즘을 제안한다. 4절에서는 제안된 암호 알고리즘의 실험 및 분석과 기존 연구와의 비교를 통해 새로운 암호알고리즘의 성능을 평가하고 5절에서 결론을 맺는다.

2. 관련연구

2.1 카오틱 맵 기반의 이미지 암호 알고리즘

카오틱 시스템은 초기 조건 및 제어 매개 변수에 대한 높은 민감도, 에르고딕성, 순환성, 의사 난수 동작 등 우수한 고유 특성을 가진다. 전형적인 카오틱 맵 기반의 이미지 암호는 순열과 확산의 두 단계를 거쳐 최종적으로 암호화 이미지를 얻는다. [4]에서는 실시간 이미지 암호화 체계를 설계하기 위해 2차원 카오틱 캣 맵을 선형대수 이론을 이용하여 3차원으로 일반화 하였다. 그들은 3차원 카오틱 캣 맵을 사용하여 이미지 픽셀의 위치를 섞고 또 다른 카오틱 맵을 사용하여 픽셀의 위치가 뒤섞인 이미지를 암호화하였다. [5]에서는 두 개의 카오틱 로지스틱 맵을 이용한 이미지 암호화 알고리즘이 제안되었다. [6]에서는 순열과 확산을 결합한 빠른 이미지 암호화 알고리즘이 제안되었다. 제안된 방법은 이미지를 픽셀 블록으로 분할한 다음 카오스 함수를 이용하여 픽셀 블록을 섞으면서 동시에 픽셀 값을 변경하여 이미지 암호화의 성능을 향상시켰다. 또한 [7]에서는 카오틱 함수를 사용하여 컬러 이미지의 R, G, B 구성 요소를 동시에 암호화 하고 이 세 구성 요소가 서로 상호작용할 수 있는 방법을 제안하였다. [8]에서는 순환이동, 스와핑 및 부분 선형 카오스 맵 기반의 새로운 비트 레벨 이미지 암호화 기법이 제안되었다. 그러나 로지스틱 맵, 삼각함수와 같은 수학적 연산을 기반으로 하고 있는 카오틱 맵을 기반의 암호 시스템은 실시간 암호화가 이루어져야 하는 시스템에서 사용하기 어렵다. [9]에서는 PWLCM 카오스 함수와 해시 알고리즘을 기반의 이미지 암호화 기법이 제안되었다. [9]에서 제안된 알고리즘은 비트 수준에서 암호화를 수행하는 방법을 제안하였으며, SHA-1 해시함수를 사용하였다.

2.2 CA기반의 이미지 암호 알고리즘

CA는 다양한 과학 분야에서 비선형 동역학을 보다 구체적으로 표현할 수 있는 이산적이고 추상적인 계산 시스템이다. CA는 셀이라 불리는 기억소자의 배열 형태에 따라 1차원, 2차원, 3차원 등으로 나뉜다. 그리고 하나의 셀이 다음 상태로 전이될 때 영향을 주는 이웃의 수에 따라 3-이웃 CA, 5-이웃 CA, 9-이웃 CA 등으로 분류된다. CA의 각 셀의 다음 상태는 이전 시간 단계에서 인접한 셀의 상태에 따라 주어진 전이 규칙에 의해 업데이트된다. 이러한 CA의 구조적 특성은 시스템에 랜덤성을 제공할 수 있기 때문에, CA는 암호체계에 응용되고 있다. 특히 수학적 연산을 기반으로 하는 카오틱 맵과 달리 CA는 하드웨어 친화적 연산으로 구현할 수 있으며 병렬처리가 가능하다는 장점을 가지고 있다. [12]에서는 비

선형 CA를 이용하여 원 이미지의 픽셀 값을 대체하는 이미지 암호 시스템이 제안되었다. CA는 훌륭한 난수열을 생성할 수 있기 때문에 효과적으로 이미지를 암호화 할 수 있다. [13]에서는 가역 및 비가역 CA를 기반으로 하는 이미지 암호화 방식이 제안되었다. 가역 CA는 혼동 및 확산 과정에서 사용되었고, 비가역 CA는 의사 랜덤 키 스트림을 생성하는 데 사용되었다. [14]에서는 2차원 CA를 암호화에 응용하였으며, 픽셀 분리기법을 사용하여 이미지를 암호화 방법이 제안되었다. 이 방법은 키 이미지를 생성하기 위해 2차원 CA를 이용하였는데, 상태를 전이시키는 과정에서 하나의 셀의 상태전이에 영향을 주는 셀의 수가 5개(위, 아래, 왼쪽, 오른쪽, 자신)인 Moore 이웃의 균형 잡힌 2차원 CA를 적용하였다. [15]에서는 의료 영상 암호화를 위해 2차원 카오틱 캣 맵과 1차원 여원 MLCA를 기반으로 한 컬러 이미지 암호알고리즘이 제안되었다. 그들은 여원 MLCA를 이용하여 원 이미지의 픽셀 값을 예측할 수 없는 값으로 변경하였고, 픽셀의 위치를 변경하기 위해 2차원 카오틱 캣 맵을 이용하였다. 그러나 [15]에서 제안된 2차원 카오틱 캣 맵은 아놀드 캣 맵의 일반화 형태가 아닌 특별한 2차 선형변환으로 특수한 몇몇의 경우를 제외하고 행렬식의 크기가 1을 유지하지 않기 때문에 픽셀 위치를 변경에 있어 암호화 이미지를 정확하게 얻을 수 없다는 문제가 있다.

3. 제안하는 알고리즘

이 절에서는 1차원 FN-MLCA와 3차원 카오틱 캣 맵을 이용하여 효과적으로 이미지를 암호화 하는 방법을 제안한다. 이 알고리즘의 장점은 CA를 기반으로 하는 암호 시스템으로 하드웨어 구현이 가능하다는 것이다. 또한 키 수열을 생성하는 데 있어 CA의 차원을 높이지 않고 이웃의 수를 증가시키면서 효과적으로 랜덤성을 높일 수 있다. 그리고 다양한 매개변수를 사용으로 인한 견고성 과 구현의 용이성이다. 제안하는 암호 시스템은 두 가지 주요 단계로 구성된다. 첫 번째 단계는 원 이미지의 픽셀 값의 조작이고 다른 단계는 픽셀 위치 셔플링이다.

3.1 1차원 FN-MLCA를 이용한 원이미지의 픽셀 값 대체단계

대체단계에서는 원 이미지가 가지고 있는 강한 상관관계와 높은 중복성을 제거하기 위해 의사 랜덤 수열 수열생성기를 이용하여 생성한 키 수열과 원 이미지의 각 픽셀값을 XOR연산 하여 원 이미지의 픽셀 값을 예측할 수 없는 값으로 조작한다. 1차원 FN-MLCA가 키 수열을 생성하는 생성기로 본 논문에서 설계된다. CA는 일정한 방식으로 배열된 여러 개의 셀이 상호 연결되어 구성되며 각 셀의 상태 전이는 인접 셀의 상태에 따라 달라진다. CA는 단순한 구조이지만 복잡하고 무작위적인 패턴을 생성 할 수 있다[16]. 본 논문에서는 키 공간의 확장과 복잡한 상태 전이 행동을 위해 1차원 CA의 이웃의 반경을 1에서 2로 확장한다. 이는 2차원 CA의 분석의 어려움을 해소하면서 1차원 MLCA보다 키 공간을 넓히고, 랜덤성을 높이기 위함이다. 각 셀의 이웃의 반경이 2로 넓어진 CA는 5개의 이웃을 가지므로 1차원 FN-CA(five-neighbour CA)가 된다. 시간 $(t+1)$에서 1차원 선형 FN-CA의 i번 째 셀의 상태는 식 (1)과 같다.

$$s_i^{t+1} = a \cdot s_{i-2}^t \oplus b \cdot s_{i-1}^t \oplus c \cdot s_i^t \oplus d \cdot s_{i+1}^t \oplus e \cdot s_{i+2}^t \quad (1)$$

여기서 s_i^t는 시간 t에서 i번째 셀의 상태를 나타내며, $a, b, c, d, e \in \{0, 1\}$이다. 1차원 선형 n-셀 FN-CA의 상태전이함수는 $n \times n$ 행렬 T로 표현되며, T를 상태전이행렬이라고 한다. n-셀 CA의 임의 상태 S에 대하여 $T^k S = S$를 만족하는 가장 작은 양의 정수 k가 $2^n - 1$이면 주어진 CA는 MLCA(maximum length CA)이다. 선형 n-셀 1차원 FN-MLCA의 상태전이행렬 T에 대한 특성 다항식 $c(x) = |T - xI|$은 원시다항식이다. 식 (1)에서 $a = e = 0, b = d = 1$이고 $c = R_i$이면, 1차원 FN-CA는 1차원 3-이웃 90/150 CA이다. 여기서 $R_i = 0$이면 전이규칙이 90이고, $R_i = 1$이면 전이규칙이 150이다. Table 1은 이웃 연결 유형에 따른 n-셀 1차원 FN-MLCA의 수를 나타낸다. 1차원 3-이웃 90/150 MLCA는 1차원 FN-MLCA에 포함되므로 1차원 FN-MLCA가 1차원 3-이웃 90/150 MLCA가 더 많다는 것은 당연하다.

Table 1에서 유형 II는 $i-2$번째 이웃과 $i+2$번째 이웃에 대해 의존도가 없으므로 3-이웃 90/150 CA와 같은 구조이다. 유형 II의 n-셀 CA의 특성다항식의 점화관계는 식 (2)를 만족한다[16].

유형 II :

Table 1. The number of 1D FN-MLCAs according to the connection types of neighbors a, b, c, d, and e of FN-CA.

Type	(a,b,c,d,e)	Number of n-cell ID FN-MLCAs						
		$n=6$	$n=7$	$n=8$	$n=9$	$n=10$	$n=11$	$n=12$
Ⅰ	(1,0,*,0,1)	-	-	-	-	-	-	-
Ⅱ	(0,1,*,1,0)	12	36	32	96	120	352	288
Ⅲ	(1,1,*,1,1)	8	20	6	52	66	188	174
Ⅳ	(0,1,*,1,1)	18	10	18	57	106	242	206
Ⅴ	(1,1,*,1,0)	18	10	18	57	106	242	206
Ⅵ	(1,0,*,1,1)	2	10	2	49	46	160	102
Ⅶ	(1,1,*,0,1)	2	10	2	49	46	160	102
Ⅷ	(1,0,*,1,0)	8	18	2	101	88	160	210
Ⅸ	(0,1,*,0,1)	8	18	2	101	88	160	210
Total		76	132	82	562	666	1,664	1,498

$$\Delta_n = (x + R_n)\Delta_{n-1} + \Delta_{n-2} \ (n \geq 1, \Delta_0 = 1, \Delta_{-1} = 0) \quad (2)$$

여기서 Δ_i는 여기서는 셀 1부터 셀 i까지 구성된 부분 CA의 특성 다항식이다. 유형 Ⅳ의 상태전이행렬 중 $n=1, n=2$일 때는 유형 Ⅱ와 동일하므로 유형 Ⅳ의 CA 특성Δ_1, Δ_2는 식 (2)에 의해 구한다. 유형 Ⅳ의 CA의 특성다항식에 대하여 $\Delta_0 = 1, \Delta_{-1} = \Delta_{-2} = 0$라 두면 유형 Ⅳ의 CA의 특성다항식의 점화관계는 식 (3)과 같다.

유형 Ⅳ(Ⅴ) :

$$\Delta_n = (x + R_n)\Delta_{n-1} + \Delta_{n-2} + \Delta_{n-3} \ (n \geq 1) \quad (3)$$

여기서 $\Delta_2 = (x + R_2)\Delta_1 + \Delta_0$, $\Delta_1 = (x + R_1)$, 이다. 유형 Ⅴ의 특성다항식은 유형 Ⅳ의 특성다항식과 같으므로 식 (3)의 점화관계를 만족한다. 식 (2)와 (3)은 주어진 FN-CA에 대한 특성 다항식을 효과적으로 계산할 수 있는 알고리즘을 제공한다.

N × N 크기의 컬러 이미지의 픽셀 값을 변경하기 위해 컬러 이미지를 각각 R, G, B 색상별로 분할한다. 키 이미지의 첫 번째 행은 임의의 초기 값과 1차원 FN-MLCA $\mathbb{C}_1$을 사용하여 N개의 의사 랜덤 수열을 생성한다. 다음으로, 1차원 FN-MLCA $\mathbb{C}_2$를 사용하여 각 열에 대해 N개의 의사 랜덤 수열을 생성한다. 각 열의 초기 값은 이전 단계에서 생성 된 각 열의 첫 번째 행 값이다. 이 과정을 세 번 반복하여 키 이미지를 생성 한 다음 생성 된 세 개의 키 이미지와 원 이미지의 R, G, B 색상별 이미지와 XOR 연산한다.

3.2 3차원 카오틱 캣 맵을 이용한 픽셀 셔플링 단계

이미지가 전송되는 과정에서 부분적으로 심각한 데이터 손실이 발생할 경우 복호 알고리즘을 이용해 암호 이미지를 복호화 하였을 때 원 이미지의 주요 부분이 손상되는 경우가 생길 수 있다. 암호 이미지의 집중된 손상이 복호화 과정에서 원이미지의 전체에 고루 퍼지도록 하여 원 이미지를 알아 볼 수 있도록 암호화 과정에서 이미지의 픽셀 위치를 섞는다. 원 이미지의 픽셀 값이 변경된 암호 이미지의 픽셀 위치를 효과적으로 변경하기 위해 [4]에서 제안한 3차원 카오틱 캣 맵을 사용한다. 이 과정을 결합함으로써 제안 된 컬러 이미지 암호화 기법은 데이터 손실 및 노이즈 공격에 강한 저항력을 갖는다. 크기가 N × N 인 이미지의 각 픽셀 값은 컬러 별로 0에서 255단계의 값을 갖는다. 3차원 카오틱 캣 맵 사용을 위해 이미지를 $n_1^3, n_2^3, \cdots$ 크기로 분할한다. 분할 된 큐브 이미지의 각 픽셀의 위치는 3차원 카오틱 캣 맵을 통해 새롭게 변경된다. 재 정렬된 각 큐브 이미지를 원 이미지의 크기대로 결합시킨다. 보안 수준을 높이기 위해 3차원 카오틱 캣 맵을 반복하여 픽셀 위치를 섞는다. Fig. 1은 제안 된 이미지 암호화 시스템의 블록 다이어그램이다.

4. 실험 결과 및 보안 분석

Lena를 포함한 다수의 255 × 255 컬러 이미지가 원 이미지로 사용된다. 임의의 공격으로부터 이미지

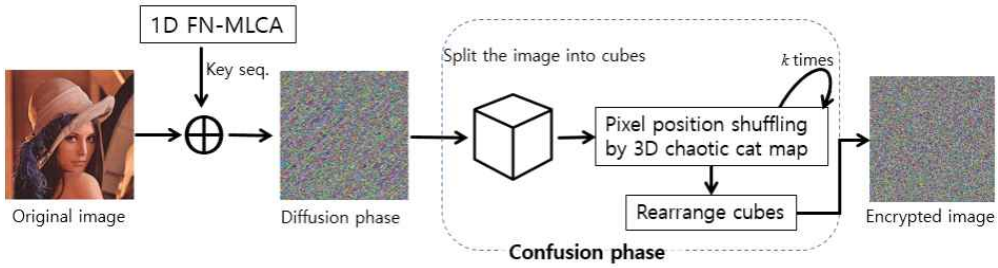

Fig. 1. Block diagram of the proposed color image encryption scheme.

를 보호하려면 원 이미지와 암호화 된 이미지 사이에 통계적 유사성이 없어야 한다. Fig. 2는 Lena 원 이미지를 제안 된 알고리즘에 따라 암호화 하고 복호한 이미지를 보여준다. Fig. 2(c)는 원 이미지와 동일하며 동일한 히스토그램을 갖는다. 이러한 결과는 제안된 알고리즘이 원 이미지를 올바르게 암호화 및 복호화 할 수 있음을 보여준다.

Fig. 3은 실험에 사용된 여러 장의 원 이미지에 대하여 제안된 알고리즘에 의해 암호화된 이미지와 각각의 이미지에 대한 히스토그램을 보여준다. 암호화된 이미지(Fig. 3(b))는 육안으로 암호 이미지를 예측하기에는 불가능함을 알 수 있다. 또한 Fig. 3(d)의 암호화된 이미지의 히스토그램들을 보면 원 이미지의 히스토그램(Fig. 3(c))과 달리 암호 이미지의 히스토그램이 상당히 균일하다는 것을 알 수 있다. 따라서 제안된 알고리즘은 통계적 공격에 내성이 있음을 보여준다.

(a) (b) (c)

Fig. 2. (a) Original image, (b) Encrypted image, and (c) Decrypted image.

정보 엔트로피는 이미지의 불확실성과 모호성의 정도를 나타내는 측도이다. 한 픽셀 값의 범위가 0~255일 때, 엔트로피 값의 범위는 0~8이다. 암호화 된 이미지의 엔트로피 값이 최대값에 가까우면 불확실성이 최대이며 이는 랜덤 속성이 우수하다는 것을 의미한다. m이 정보 소스 일 때, 암호화 된 이미지의 정보 엔트로피는 식 (4)에 의해 계산된다.

$$H(m) = -\sum_{i=0}^{L-1} p(m_i)\log_2 p(m_i) \tag{4}$$

여기서 $p(m_i)$는 이산 확률 밀도함수, m_i는 0에서 255까지의 픽셀 값, L은 그레이 레벨로 8비트 이미지일 때 $L=256$이다. Table 2는 제안된 알고리즘에 의해 암호화 된 Fig. 3(b)의 여러 이미지에 대한 엔트로피를 보인다. Table 2에 의하면 암호화된 이미지의 엔트로피 값은 이상적인 값 8에 매우 가까움을 알 수 있다. 이는 제안 된 암호화 시스템이 안전하다는 것을 의미한다. Table 3은 제안된 알고리즘 및 기타 알고리즘을 사용하여 암호화 된 이미지의 엔트로피를 보여준다.

이미지의 특성 중 하나는 인접한 셀 간의 강한 상관관계이다. 효과적인 암호 알고리즘은 이미지를 암호화 하였을 때 원 이미지가 가지고 있는 상관관계가 사라져야 한다. Fig. 4은 원 이미지 Fig. 2 (a)와 암호화된 이미지 Fig. 2(b)에 대해 R, G, B 채널의 수직,

Table 2. The entropy of images encrypted by the proposed algorithm.

Image	Entropy			
	R	G	B	Average
Lena	7.9972	7.9970	7.9972	7.9971
Pepper	7.9970	7.9971	7.9968	7.9970
Chimpanzee	7.9971	7.9967	7.9971	7.9970
Organic food	7.9974	7.9974	7.9972	7.9973

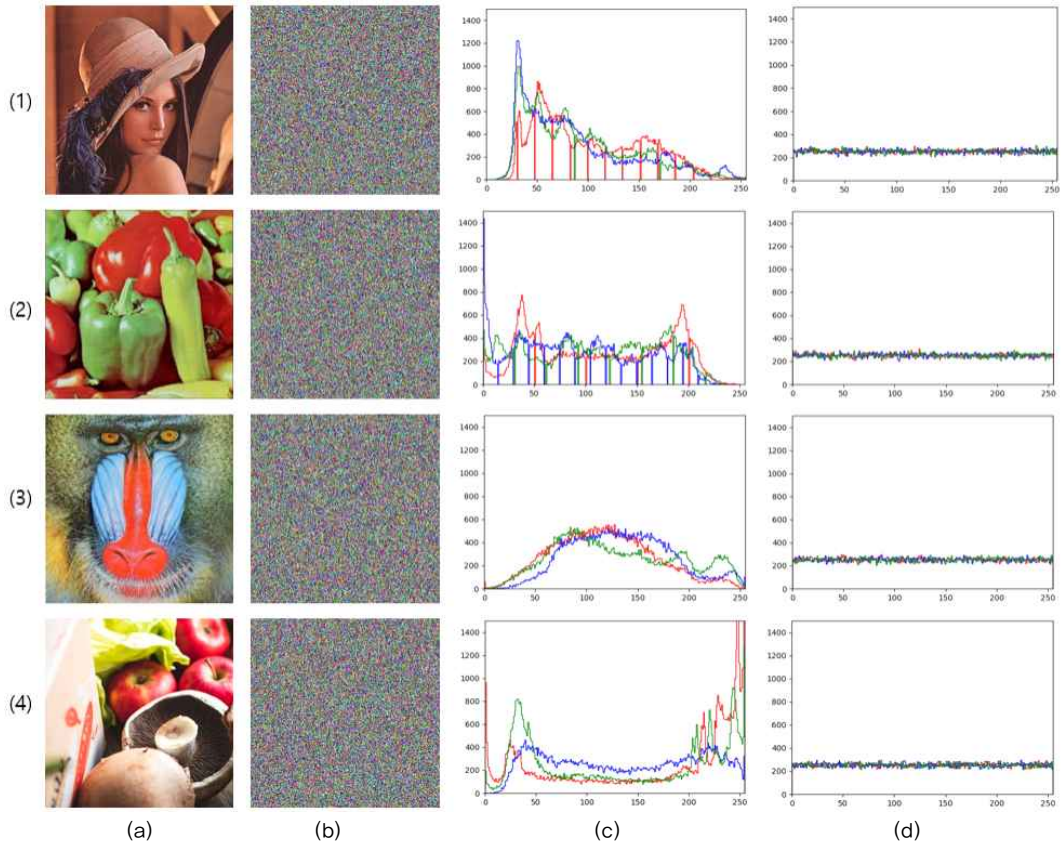

Fig. 3. The histograms corresponding to original images and encrypted images. (a) Original image, (b) Encrypted image,(c) Histogram of original image, and (d) Histogram of encrypted image.

수평 및 대각선 방향의 인접한 픽셀 간의 상관관계 다이어그램을 보여준다. Fig. 3에서 원 이미지의 인접한 두 픽셀 간의 상관관계는 매우 강하지만 제안한 암호알고리즘에 의해 암호화 된 이미지는 인접한 픽셀 간의 상관관계가 거의 없음을 확인할 수 있다. 이러한 결과는 나머지 다른 원 이미지에 대해서도 같은 결과를 보였다. 상관 계수는 수직, 수평, 대각선으로 인접한 픽셀에 대한 원 이미지와 암호 이미지의 상관관계의 정도를 수치로 분석하기 위해 계산된다. 원 이미지(P)와 암호 이미지(C)에서 인접한 두 픽셀 간의 상관 계수를 테스트하기 위해 P와 C에서 두 개의 인접한 픽셀(수직, 수평 및 대각선 방향)을 무작위로 선택하여 식 (5)를 이용하여 상관 계수를 얻는다.

Table 3. The comparison of entropy of encrypted images using different algorithms.

Method	Entropy		
	R	G	B
Proposed Algorithm	7.9972	7.9970	7.9972
Ref.[17]	7.9877	7.9881	7.9877
Ref.[18]	7.9972	7.9973	7.9972
Ref.[19]	7.9896	7.9893	7.9896
Ref.[20]	7.9893	7.9897	7.9895
Ref.[21]	7.9971	7.9969	7.9962
Ref.[22]	7.9891	7.9900	7.9897

$$\rho_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5}$$

여기서

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i\,,\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2\,,$$

$$cov\,(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$$

이며 x, y는 이미지의 인접한 두 픽셀의 픽셀 값이다.

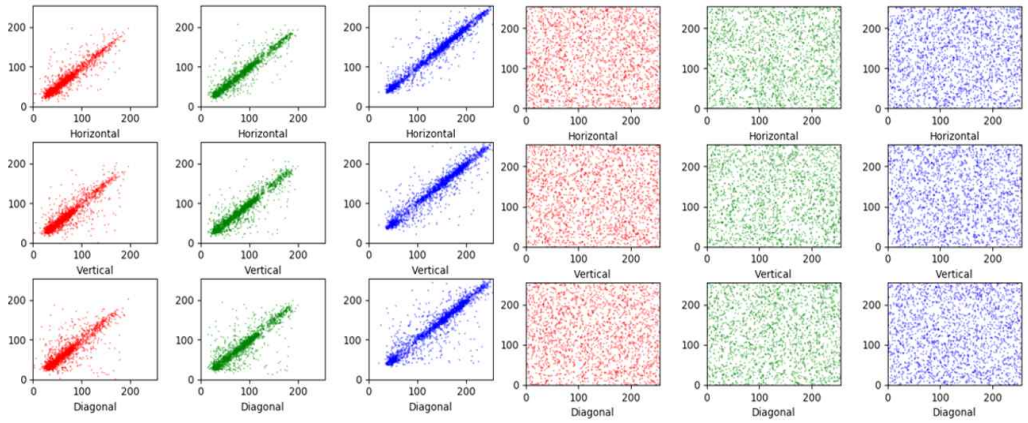

Fig. 4. Correlation analysis of (a) the original image (Lena) and (b) the encrypted image (Lena).

Table 4은 Fig. 3의 원 이미지와 암호화된 이미지에 대해 식(5)를 이용하여 계산한 상관계수를 계산한 결과이다. Table 4에서 수직(V), 수평(H), 대각선(D) 각 방향에 대해 원 이미지의 상관계수는 1의 값에 가깝고, 암호 이미지의 인접한 두 픽셀 사이의 상관 계수가 0에 매우 가깝다. 이는 원 이미지가 가지고 있는 인접한 픽셀간의 강한 상관관계가 암호화 되면서 상관관계가 거의 없음을 확인할 수 있다. 실험 결과는 2,000개의 샘플을 400회 반복하여 얻은 결과의 평균이다. Table 5는 제안된 알고리즘과 다른 알고리즘에 의해 암호화한 이미지의 상관 계수를 보여준다.

민감도 분석에는 NPCR과 UACI의 두 가지 측도가 이용된다. NPCR은 원 이미지에서 한 픽셀을 변경한 후 암호화 한 두 이미지 간의 픽셀 변경 비율을 나타낸다. UACI는 같은 방법으로 얻어진 두 암호화된 이미지 간의 픽셀 값의 변경 강도 차이의 평균이다. NPCR과 UACI는 식 (6)과 같다.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100(\%),$$
$$UACI = \left[\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{W \times H \times 255} \right] \times 100(\%) \quad (6)$$

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

Image	color	Original image			Encrypted image		
		H	V	D	H	V	D
Lena	R	0.9085	0.8955	0.8558	-0.0073	-0.0160	0.0531
	G	0.9372	0.9244	0.8964	-0.0398	-0.0105	-0.0279
	B	0.9589	0.9488	0.9217	-0.0099	-0.0186	-0.0005
Pepper	R	0.9675	0.9596	0.9390	-0.0173	0.0026	-0.0042
	G	0.9846	0.9783	0.9690	0.0111	0.0043	-0.01546
	B	0.9705	0.9602	0.9423	0.0021	0.0040	0.0067
Chimpanzee	R	0.9097	0.9251	0.8850	0.0332	-0.0194	-0.0270
	G	0.8444	0.8763	0.8041	-0.0163	-0.0307	-0.0119
	B	0.8994	0.9235	0.8777	0.0058	0.0037	0.0106
Organic food	R	0.9781	0.9808	0.9657	0.0131	-0.0207	-0.0139
	G	0.9808	0.9819	0.9673	0.0011	-0.0066	0.0086
	B	0.9806	0.9829	0.9689	0.0093	-0.0251	-0.0148

* H : Horizontal, V : Vertical, D : Diagonal

Table 5. Correlation coefficients of the encrypted image by the proposed algorithm and other algorithms.

Method	Horizontal	Vertical	Diagonal
Proposed Algorithm	0.0038	0.0036	-0.0177
Ref.[17]	-0.0028	-0.0351	0.0475
Ref.[18]	0.0022	0.0001	0.0017
Ref.[19]	0.0009	0.0009	0.0015
Ref.[20]	0.0045	0.0015	0.0015
Ref.[21]	0.0033	0.0042	0.0024
Ref.[22]	-0.0084	0.0004	-0.0015

여기서 W와 H는 각각 이미지의 너비와 높이를 나타내며, $C(i,j)$는 원이미지를 암호화하여 얻은 이미지의 i행 j열의 픽셀 값이고, $C'(i,j)$는 주어진 원이미지의 한 픽셀을 변경한 후 얻은 암호 이미지의 i행 j열의 픽셀 값이다. $D(i,j)$는 $C(i,j) = C'(i,j)$이면 0이고 그렇지 않으면 1이다. Table 6는 원 이미지 Lena에 대해 제안 된 알고리즘과 기존 알고리즘을 사용하여 얻은 NPCR과 UACI의 결과이다. Table 4에 의하면 원 이미지와 변경된 이미지에 대한 암호 이미지 간의 NPCR과 UACI의 결과는 NPCR>99%이고 UACI ≈ 33%이다. 이러한 실험 결과는 NPCR 및 UACI의 예상 기대치와 분산이 이론적 값에 매우 근접하여 이론적 값의 타당성을 정당화한다는 것을 보여준다[4]. 따라서 제안 된 암호화 체계는 차등 공격에 대해 내성이 있다.

암호 시스템의 키 공간은 암/복호화 과정에서 사용할 수 있는 서로 다른 키의 총 수이다. 이미지 암호화 알고리즘은 무차별 대입 공격에 저항 할 수 있을 만큼 충분히 큰 키 공간을 확보하는 것이 중요하다. 제안된 암호 시스템은 키 이미지를 생성하기 위해

Table 6. NPCR and UACI for encrypted image of using the proposed algorithm and other algorithms.

Algorithm	NPCR (%)	UACI (%)
Proposed algorithm	99.9982	33.7902
Ref. [18]	99.6254	33.4566
Ref. [19]	99.6165	33.5673
Ref. [20]	99.6161	33.4284
Ref. [21]	99.2171	33.4054
Ref. [22]	99.6084	33.4697

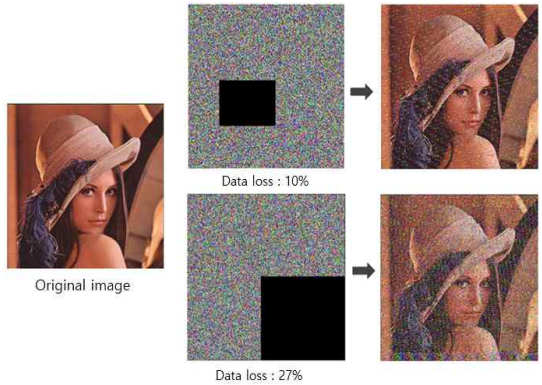

Fig. 5. Experiments on data loss and noise attack.

2개의 n-셀 1차원 FN-MLCA($n \geq 8$)와 3개의 n비트 크기의 초기 값이 필요하다. 각 셀에 적용되는 규칙의 수는 2^{32}이므로 초깃값과 2개의 1차원 FN-MLCA의 키공간은 $(2^{32})^n \cdot (2^{32})^n \cdot (2^n)^3 = 2^{67n}$이다. 또한 3차원 카오틱 캣 맵에서 제어 매개 변수인 키의 수는 N^9이며, 여기서 $N \times N$은 원이미지의 크기이다. $N = 256 (= 2^8)$이면 키 공간의 전체 크기는 2^{67n+72}이고 $n \geq 8$이므로 2^{128}보다 충분히 크다. 따라서 제안된 컬러 이미지 암호화 알고리즘은 키 공간은 무차별 대입 공격으로부터 안전하다.

디지털 이미지는 네트워크를 통한 전송 과정이나 물리적인 매체에 저장 중에 노이즈 및 데이터 손실이 있을 수 있다. 이미지 암호화 알고리즘은 이러한 비정상적인 현상에 저항 할 수 있어야한다. 공격에 대한 저항성을 테스트하기 위해 데이터 손실 및 노이즈 공격에 대한 실험이 수행되었다. Fig. 5는 제안 된 암호화 방법이 데이터 손실 및 노이즈 공격에 강함을 보여준다.

5. 결 론

본 논문에서는 1차원 FN-MLCA와 3차원 카오틱 캣 맵 기반의 컬러 이미지 암호 알고리즘을 제안하였다. 키 이미지를 생성하기 위한 의사난수열 생성기로 1차원 FN-MLCA를 모델링하였고, 특성다항식을 빠르게 계산할 수 있는 점화식을 구했다. 1차원 FN-MLCA는 병렬처리가 가능하며, 하드웨어 친화적인 연산을 통해 수열을 발생할 수 있으며 키 공간을 효과적으로 확장할 수 있다. 제안된 암호 알고리즘은 두 단계로 구성되어있다. 첫 번째 단계에서는 본 논문에

서 모델링 한 1차원 FN-MLCA를 사용하여 원 이미지의 픽셀 값을 예측할 수없는 값으로 효과적으로 조작했다. 그런 다음 제안 된 암호화 알고리즘의 두 번째 단계에서 데이터 손실 및 노이즈 공격에 저항할 수 있도록 3차원 카오틱 캣 맵을 사용하여 이미지의 픽셀 위치를 섞었다. 여러 실험과 키공간 분석을 통해 제안된 알고리즘이 다양한 통계 및 차분 공격, 데이터 손실 및 노이즈 공격에 대해 안전함 보였다.

REFERENCE

[1] G. Bhatnagar, Q.M.J. Wu, and B. Raman, "A New Fractional Random Wavelet Transform for Fingerprint Security," *IEEE Transactions on Systems, Man, and Cybernetics. Part A, Systems and Humans*, Vol. 42, No. 1, pp. 262-275, 2012.

[2] Y. Zhou, L. Bao, and C.L.P Chen, "A New 1D Chaotic System for Image Encryption," *Signal Processing*, Vol. 97, pp. 172-182, 2014.

[3] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A Color Image Cryptosystem Based on Dynamic DNA Encryption and Chaos," *Signal Processing*, Vol. 155, pp. 44-62, 2019.

[4] G. Chen, Y. Mao, and C.K. Chui, "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps," *Chaos, Solitons & Fractals*, Vol. 21, No. 3, pp. 749-761, 2004.

[5] N.K. Pareek, V. Patidar, and K.K. Sud, "Image Encryption Using Chaotic Logistic Map," *Image and Vision Computing*, Vol. 24, No. 9, pp. 926-934, 2006.

[6] Y. Wang, K.W. Wong, X. Liao, and G. Chen, "A New Chaos-Based Fast Image Encryption Algorithm," *Applied Soft Computing*, Vol. 11, No. 1, pp. 514-522, 2011.

[7] X. Wang, L. Teng, and X. Qin, "A Novel Colour Image Encryption Algorithm Based on Chaos," *Signal Processing*, Vol. 92, No. 4, pp. 1101-1108, 2012.

[8] L. Xu, Z. Jian, J. Li, and W. Hua, "A Novel Bit-Level Image Encryption Algorithm Based on Chaotic Maps," *Optics and Lasers in Engineering*, Vol. 78, pp. 17-25, 2016.

[9] A. Hasheminejad and M.J. Rostami, "A Novel Bit Level Multiphase Algorithm for Image Encryption Based on PWLCM Chaotic Map," *Optik*, Vol. 184, pp. 205-213, 2019.

[10] 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, No. 9, pp. 8096-8103, 2017.

[11] H.M. Ghadirli, A.Nodehi, and R. Enayatifar, "An Overview of Encryption Algorithms in Color Images," *Signal Processing*, Vol. 164, pp. 163-185, 2019.

[12] U.S. Choi, S.J. Cho, and T.H. Kim, "Image Encryption Based on One Dimensional Nonlinear Group Cellular Automata," *Journal of the Korean Multimedia Society,* Vol. 18, No. 12, pp. 1462-1467, 2015.

[13] P. Ping, F. Xu, and Z. Wang, "Image Encryption Based on Non-affine and Balanced Cellular Automata," *Signal Processing*, Vol. 105, pp. 419-429, 2014.

[14] D. Tralic and S Grgic, "Robust Image Encryption Based on Balanced Cellular Automaton and Pixel Separation," *Radioengineering,* Vol. 25, No. 3, pp. 548-555, 2016.

[15] 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," *Proceeding of International Conference Ubiquitous and Future Networks (ICUFN)*. pp. 801-804, 2018.

[16] K. Cattell and J.C. Muzio, "Synthesis of One-Dimensional Linear Hybrid Cellular Automata," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 15, No. 3, pp. 325-335, 1996.

[17] H. Liu and X. Wang, "Color Image Encryption Using Spatial Bit-Level Permutation and High-Dimension Chaotic System," *Optics Commu-*

nications, Vol. 284, No. 16-17, pp. 3895-3903, 2011.

[18] A.Y. Niyat, M.H. Moattar, and M.N. Torshiz, "Color Image Encryption Based on Hybrid Hyper-Chaotic System and Cellular Automata," *Optics and Lasers in Engineering,* Vol. 90, pp. 225-237, 2017.

[19] H. Liu and A. Kadir, "Asymmetric Color Image Encryption Scheme Using 2D Discrete-Time Map," *Signal Processing*, Vol. 113, pp. 104-112, 2015.

[20] C. Dong, "Color Image Encryption Using One-Time Keys and Coupled Chaotic Systems," *Signal Processing: Image Communication,* Vol. 29, No. 5, pp. 628-640, 2014.

[21] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A Novel Color Image Encryption Algorithm Based on DNA Sequence Operation and Hyper-Chaotic System," *Journal of Systems and Software,* Vol. 85, No. 2, pp. 290-299, 2012.

[22] X. Wu, H. Kan, and J. Kurths, "A New Color Image Encryption Scheme Based on DNA Sequences and Multiple Improved 1D Chaotic Maps," *Applied Soft Computing*, Vol. 37, pp. 24-39, 2015.

최 언 숙

1992년 성균관대학교 산업공학과 졸업(공학사)
2000년 부경대학교 대학원 응용수학과 졸업(이학석사)
2004년 부경대학교 응용수학과 졸업(이학박사)
2009년 부경대학교 정보보호학과 졸업(공학박사)
2006년~현재 동명대학교 정보통신소프트웨어공학과 교수
관심분야 : 셀룰라 오토마타론, 영상암호, 정보보호