MLCA와 CAT를 이용한 새로운 영상 암호화 방법

박영일* · 조성진** · 김석태***

A Novel Image Encryption using MLCA and CAT

Yongri Piao* · Sung-Jin Cho** · Seok-Tae Kim***

이 논문은 2008학년도 부경대학교의 지원을 받아 수행된 연구임(PK-2008-026)

요 약

본 논문에서는 MLCA (Maximum Length Cellular Automata)와 CAT (Cellular Automata Transform)을 이용한 새로운 영상 암호화 방법을 제안한다. 먼저 Wolfram 규칙을 선택하여 규칙행렬을 구성하고 규칙행렬에 의하여 MLCA의 상태 전이행렬 T를 만든 후 암호화 하려는 영상의 픽셀 위치에 따라 전이행렬을 곱하여 픽셀의 값을 변환한다. 다음 게이트웨이 값의 설정에 따라 2D CAT 기저함수를 생성하여 MLCA 암호화한 영상을 CAT 암호화를 한다. 실험결과와 안정성 분석을 통하여 제안한 방법은 높은 암호화 수준과 무손실 암호화의 성질을 가졌음을 확인한다.

ABSTRACT

In this paper, we propose a novel Image Encryption using MLCA (Maximum Length Cellular Automata) and CAT (Cellular Automata Transform). Firstly, we use the Wolfram rule matrix to generate MLCA state transition matrix T. Then the state transition matrix T changes pixel value of original image according to pixel position. Next, we obtain Gateway Values to generate 2D CAT basis function. Lastly, the basis function encrypts the MLCA encrypted image into cellular automata space. The experimental results and security analysis show that the proposed method guarantees better security and non-lossy encryption.

키워드

MLCA, CAT, Gateway Values, Basis Function, Image Encryption

* 광운대학교 전자공학과, 3DRC
** 부경대학교 수리과학부 교수
*** 부경대학교 전자컴퓨터정보통신공학부 교수(교신저자)

접수일자 : 2009. 03. 23
심사완료일자 : 2009. 04. 23

Ⅰ. 서 론

최근 통신과 컴퓨터의 결합으로 멀티미디어 콘텐츠의 디지털화가 급속하게 진행되고 있으며 많은 정보가 고속으로 교환되고 있다. 하지만 개인 및 단체의 소중한 콘텐츠가 해커의 표적이 되고 있어 국가 및 기업뿐만 아니라 개인에게도 중요한 문제가 되고 있다. 최근 들어 각국에서 콘텐츠의 복제와 위조 방지에 관한 연구가 활발히 진행되고 있지만 우리나라는 인터넷 및 관련 기술의 발달에 비해 콘텐츠 정보보호에 대하나 인식과 연구가 상대적으로 미흡한 상태이다.

디지털 멀티미디어 콘텐츠를 보호하는 방법에는 콘텐츠가 불법적으로 유통되었을 때 배포자가 누구인지 또는 원 소유자가 누구인지를 구분하기 위한 워터마크 방법과 불법적인 형태의 멀티미디어 콘텐츠에 대한 접근 자체를 원천적으로 막을 수 있는 암호화 방법이 있다. 그 중 암호화는 군사적, 상업적으로 많이 이용되면서 콘텐츠의 신뢰성, 비밀성을 제공하는 방법으로 활용되고 있다. Pichler 와 Scharinger [1-2]는 Kolmogorov flow map을 기반으로 하여 영상의 픽셀 값을 변환하는 암호화 기법을 제안하였고 Chen [3]은 3D maps를 기반으로 하는 영상 암호화 방법을 제안하였으며 Lian [4]은 standard map 을 기반으로 한 영상 암호화 방법을 제안하였다. 이 방법들은 암호화하려는 영상의 픽셀위치를 discredited chaotic map을 이용하여 변환 시킨 다음 cipher block chain (CBC) mode로 픽셀 값을 변환 한다. 하지만 이러한 방법들은 동일한 framework 으로 영상의 암호화를 하였기 때문에 암호화 효과가 떨어지는 문제점이 생기는 동시에, 암호화된 영상이 복원할 때에 어느 정도의 화질 손실이 발생하는 단점이 있다.

본 논문에서는 이러한 문제점을 해결하기 위하여 MLCA(Maximum Length Cellular Automata)와 CAT (Cellular Automata Transform)를 이용한 새로운 영상 암호화 방법을 제안한다. CA (Cellular automata) 는 Von Neumann [5-6]에 의해 스스로 조직화 하고 재생산할 수 있는 모델로 처음 소개되었으며 그 후 Wolfram [7-8]은 셀의 상태가 자기 자신 및 인접한 셀 상태의 국소적인 상호작용에 의해서 동시에 갱신되는 시스템으로 발전시켰다. 특히 CA가운데 다음 상태를 결정하는 함수가 선형적인 CA는 LFSR(Linear Feedback Shift Register)의 대안으로 제안되고, 지금껏 오류정정부호, 신호분석, 영상처리[9-12] 등의 분야에서 응용되고 있으나 아직 영상의 암호화 연구에는 이용되고 있지 않다.

본 논문에서는 최대길이를 생성하는 MLCA와 무손실 CAT를 이용하여 새로운 영상 암호화 방법을 제안한다. 제안한 방법은 암호화 수준을 높이기 위하여 먼저 Wolfram규칙을 선택하여 규칙행렬을 구성하고 규칙행렬에 의하여 MLCA의 전이행렬을 만든다. 그리고 암호화 하려는 영상의 픽셀 위치에 따라 전이행렬을 곱하여 픽셀의 값을 변환한다.

그 후, 게이트웨이 값의 설정에 따라 2D CAT 기저함수를 생성해 MLCA 암호화한 영상을 다시 한번 CAT를 이용해 암호화한다.

실험결과와 안정성 분석을 통하여 제안한 방법은 높은 암호화 수준과 무손실 암호화의 성질을 가졌음을 확인한다.

Ⅱ. Cellular Automata (CA)

CA는 동역학계(dynamical system)를 해석하는 한 방법이다. 공간과 시간을 이산적으로 다루고, 이산적인 공간의 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다.

2.1 Cellular Automata의 기본성질

가장 간단한 구조를 가지는 1D CA (one dimensional CA)에서는 모든 셀들이 선형으로 배열되어 있다. 본 논문에서 사용하는 CA는 3이웃 (3-neighbourhood) CA로서 현재의 상태가 국소적 상호 작용에 의해 3개의 셀, 즉 자기 자신과 인접한 셀에 의해 다음 상태로 갱신되는 CA이다. 3-이웃 CA에 대한 상태전이 함수 (state-transition function)은 다음과 같다.

$$a_{i,t+1} = f[a_{i,t}, a_{i+1,t}, a_{i-1,t}] \quad (1)$$

여기서 $a_{i,t+1}$ 은 현재상태 $a_{i,t}$ 의 갱신되는 다음 상태이며, $a_{i-1,t}$ 와 $a_{i+1,t}$ 는 각각 $a_{i,t}$ 의 왼쪽 이웃 상태와 오른쪽 이웃 상태들이며 f 는 결합 논리를 가지는 국소전이 함수이다.

GF(2)={0, 1} 상에서 3-이웃 CA에는 서로 다른 23개의 이웃의 배열상태가 있으며 그러한 CA에는 2^{2^3} 개의

상태전이함수가 있다. 이것을 CA의 규칙이라고 한다.

3-이웃 CA에서의 맨 외쪽 셀의 왼쪽 이웃이 없고 맨 오른쪽 셀의 오른쪽 이웃이 없기 때문에 맨 왼쪽 셀의 왼쪽 이웃을 0으로 주고 또한 맨 오른쪽 셀의 오른쪽 이웃도 0으로 준다. 이러한 CA를 NBCA (Null Boundary CA)라고 한다.

n개의 셀을 가지는 선형 3-이웃 NBCA에서는 현재 상태를 다음 상태로 전이시키는 전이함수를 $n \times n$ 행렬로 나타낼 수 있으며, 이것을 상태전이 행렬(state- transition matrix)이라 한다. 상태전이 행렬 T에서 I번째 행은 I번째 셀에 적용되는 규칙이며 그 셀의 다음 상태가 현재 상태에 의존하면 1, 그렇지 않으면 0으로 한다. 현재 상태가 자기 자신과 두 이웃에 의존하여 다음 상태로 갱신될 때, 규칙 150이라 하고 현재 상태가 두 이웃에만 의존하여 다음 상태로 갱신될 때, 규칙 90이라 한다. 예를 들어 규칙 (150, 90, 150, 150)인 4개 셀로 구성된 CA의 상태전이 행렬은 식(2)과 같다.

$$T = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \tag{2}$$

3-이웃 CA의 전이행렬은 정방 행렬 (Square matrix)의 주 대각선과 그 바로 위의 대각선과 아래 대각선을 제외한 나머지가 0인 삼중대각 행렬(tridiagonal matrix)이다. $f_t(x)$ 가 시간 t에서 CA의 상태를 나타내면 시간 t+1에서의 다음과 같다.

$$f_{t+1}(x) = T \cdot f_t(x) \tag{3}$$

여기서 T는 전이행렬이다.

2.2 Maximum LengthCA(MLCA)

선형 NBCA는 그룹 (Group) NBCA와 비그룹 (nongroup) NBCA로 분류되는데 그룹 NBCA는 상태전이 행렬의 행렬식(determinant)이 1인 CA이다. 즉, 그룹 NBCA의 상태전이 행렬을 T라 하면 det(T)=1이며 상태들이 사이클(cycle)을 이룬다. 그러므로 이러한 그룹 NBCA의 상태전이 행렬은 역 행렬이 반드시 존재한다. 따라서 상태전이 행렬 T의 역행렬을 구하여 현재 상태의 바로 직전 상태 (immediate state)를 식(4)를 이용해 구할 수 있다.

$$S_{i,t-1} = T^{-1} S_{i,t} \tag{4}$$

여기서는 S_t i번째 셀이 t시간 일 때 상태를 나타 낸다. 그룹 NBCA는 최대 길이를 갖는 CA와 최대 길이를 갖지 않는 CA로 구별할 수 있다. 최대 길이를 갖는 NBCA를 MLCA (Maximum Length CA)라 한다. n셀 CA의 상태전이 행렬 T의 특성 다항식을 $p(x)$ 라하면 $p(x) = \det(T - xI_n)$ 이다. 여기서 I_n 은 n 차 단위행렬이다. f(x)가 $\min\{m : f(x) \mid x^m - 1\} = 2^n - 1$ 을 만족할 때, f(x)를 원시 다항식이라 한다. 따라서 MLCA의 상태전이 행렬의 특성다항식은 원시다항식이 된다. 예를 들어 NBCA <90, 90, 90, 90>의 상태전이 행렬은

$$T = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{5}$$

이며 특성 다항식은 $(x^2 + x + 1)^2$ 이며 최대길이를 갖지 못한다. 그러나 2.1절의 상태전이 행렬 T의 특성 다항식은 $x^4 + x^3 + 1$ 이며 따라서 주기가 15(=24-1)이다. 그러므로 <150, 90, 150, 150>은 MLCA이며 상태전이 그래프는 그림 1과 같다.

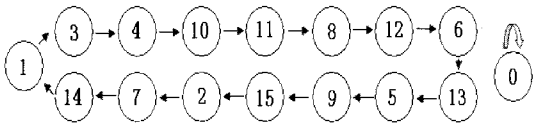


그림.1 상태전이 그래프
Fig. 1 State transition graph

2.3 Cellular Automata Transform (CAT)

함수 f는 영역 i의 함수일 때 1D CAT 변환은 식(6)과 같이 정의 한다[13].

$$f_i = \sum_{k=0}^{N-1} c_k A_{ik} \quad i = 0,1,2,\cdots,N-1 \tag{6}$$

여기서 A는 CAT 기저함수, k는 CA 공간벡터, c_k는 CAT 계수를 나타내고 식(7)으로 구할 수 있다.

$$c_k = \frac{1}{\lambda_k} \sum_{i=0}^{N-1} f_i A_{ik} \tag{7}$$

여기서 λ_k 는 식 (8)과 같다.

$$\lambda_k = \sum_{i=0}^{N-1} A_{ik}^2 \tag{8}$$

f_{ij} 의 2D CAT는 식 (9)과 같다.

$$f_{ij} = \sum_{k=0}^{N-1}\sum_{l=0}^{N-1} c_{kl} A_{ijkl} \quad (i,j = 0,1,\cdots,N-1) \tag{9}$$

여기서c_{kl} 는 2D CAT 기저함수이다.

2D CAT의 기저함수는 다음 두 가지 방법으로 생성할 수 있다.

1. 2D CA 공간 $a \equiv a_{ijt}, (i,j,t = 0,1,\cdots,N-1)$ 에서 직접 2D기 저저함수 A_{ijkl}을 생성한다.
2. 1D CAT 기저함수로부터 2D CAT기저함수를 생성한다. 즉 $A_{ijkl} = A_{ik}A_{jl}$

Ⅲ. 제안한 영상 암호화 방법

본 논문에서는 MLCA와 CAT를 이용한 새로운 영상 암호화 방법을 제안한다. 제안한 영상암호화 방법은 그림 2과 같이 먼저 MLCA 암호화 한 다음 2D CAT 암호화 하는 두 가지 절차를 거친다.

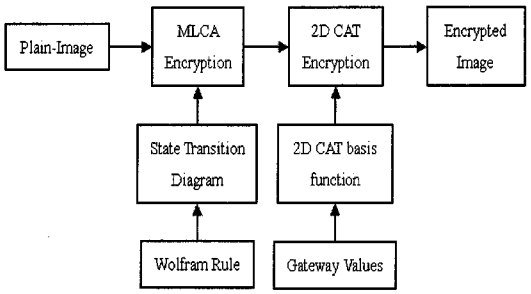


그림2. 영상 암호화의 블록 다이어그램
Fig. 2 Block diagram of the image encryption

3.1 MLCA 암호화

본 논문에서는 영상의 암호화 정도를 높이기 위해 먼저 원 영상에 MLCA 암호화를 적용한다.

Step 1: Wolfram 규칙을 선택한다.
Step 2: 선택한 규칙을 사용하여 규칙행렬 R을 생성한다.
Step 3: 규칙행렬 R로부터 전이행렬 T를 만들어낸다.

전이행렬을 생성하는 순서를 그림 3 에 나타낸다.

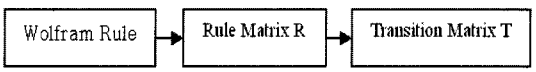


그림3. 전이행렬의 생성
Fig. 3 Generation of Transition Matrix

Step 4: 원 영상의 픽셀 위치 값이 짝수인 경우 전이행렬 T를 픽셀 값에 곱하고, 픽셀 의 위치값이 홀수인 경우에 전이행렬 T 제곱을 픽셀 값에 곱한다.
Step 5: MLCA로 암호화 된 영상을 얻는다.

3.2 CAT 암호화

본 절에서는 CAT 기저함수를 생성하는 방법과 CAT 암호화를 설명한다. 그림4에 2D 기저함수를 구하는 과정을 나타낸다.

Gateway Values ▷ 1D a_{ik} ▷ 1D A_{ik} ▷ Generate 2D A_{ikjl}

그림4. 2D 기저함수의 생성
Fig. 4 Generation of 2D basis function

Step 1: 2-상태, 8-셀, 3-이웃, 2-D CA 기저함수는 게이트웨이 값(룰, 셀의 개수, 셀의 초기상태, 경계조건, 기저함수 타입 등)에 의해 생성되는데 표1은 게이트웨이 값 296개의 경우 중 한 가지 경우를 나타낸다.

표1. 게이트웨이 값
Table 1. Gateway Values

Wolfram Rule Number	158
Number of Cells per Neighborhood	3
Number of Cells in Lattice	8
Initial Configuration	01100101
Boundary Configuration	Cyclic
Basis Function Type 2	$A_{ik}=2_{aikaki}-1$

Step 2: 2-상태, 8-셀을 가지는CA에서 표 1에 나타낸 게이트웨이 값의 조건하에서 갱신되는 셀들의 상태전이 함수식은 식(11)과 같다.

$$a_{(1)(t+1)} = (W_0 a_{0t} + W_1 a_{1t} + W_2 a_{2t} + W_3 a_{0t} a_{1t} + W_4 a_{0t} a_{2t} + W_5 a_{1t} a_{2t} + W_6 a_{0t} a_{1t} a_{2t} + W_7)^{W_3} \quad (11)$$

여기서 $0 \le W_j < 2$ 고, α_j는 이웃 셀 상태조합으로 정해진다.

Step 3: 1-D CA 기저함수는 식(12)으로 구할 수 있다.

$$A_{ik} = 2a_{ik}a_{ki} - 1 \quad (12)$$

여기서 a_{ik} 는 t=k 일 때 i번째 셀의 상태이다.

Step 4: 2-D 기저함수는 1-D 기저함수로부터 구할 수 있고 식(13)과 같다.

$$A_{ijkl} = A_{ik}A_{jl} \quad (13)$$

Step 5: 2-D 기저함수 A_{ijkl} 를 이용한 2-D CAT 암호화는 식(14)를 이용한다.

$$c_{kl} = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f_{ij}A_{ijkl} \quad k,l = 0,1,2,\cdots,N-1 \quad (14)$$

Step 6: 식 (14)을 이용하여 최종 암호화 된 영상을 얻는다.

그림 5는 표1의 게이트웨이 값에 의해 생성된 2-D 기저함수를 나타낸다. 여기서 하얀 점은 1을 나타내고 검은 점은 -1을 나타낸다. A_{00kl}는 i=0, j=0인 Block을 나타내고 A_{ij00}는 매개 Block 오른 쪽 위의 첫 번째 점을 나타낸다.

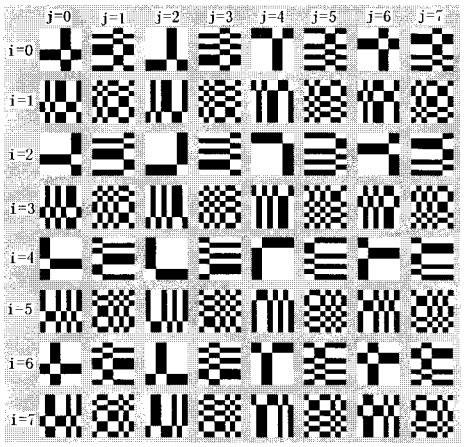


그림5. 2차원 기저함수
Fig. 5 Two-dimensional basis functions

3.3 복호화

영상의 복호화는 암호화의 역 과정이고 다음 순서에 따라 복호화 한다.

Step 1: 게이트웨이 값을 선택하여 2D CAT기저함수를 생성한다.

Step 2: 생성된 2D CAT 기저함수로 암호화 된 영상을 식 (9)을 이용하여 MLCA로 암호화 된 영상을 얻는다.

Step 3: Wolfram 규칙을 선택하여 전이행렬 T를 생성한다.

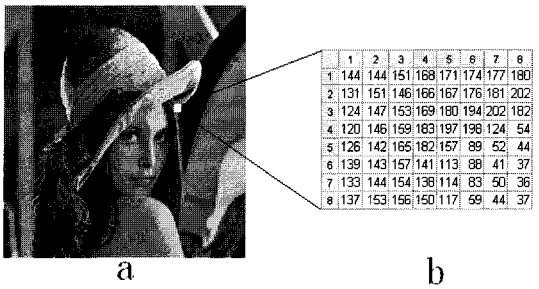
Step 4: MLCA 암호화 된 영상의 픽셀 위치에 따라 픽셀 위치 값이 짝수인 경우 전이행렬T 제곱의 역 행렬을 곱하고, 픽셀 위치 값이 홀수 인 경우 전이 행렬 T의 역 행렬을 곱한다.

Step 5: 원 영상을 얻는다.

Ⅳ. 실험결과

본 논문에서는 제안한 알고리즘의 유용성을 검증하기 위하여 256×256 크기의 8bit 그레이 레벨을 갖는100 가지 영상을 사용하여 실험하였으며 그 중에서 저주파 성분과 고주파 성분이 균일하게 잘 분포된 Lena 영상으로 실험한 결과를 가지고 제안한 알고리즘의 성능을 검증한다. 그림 6에서 (a)는 Lena 원 영상을 나타내고 (b)는 Lena 영상에서 8×8 크기인 영역의 픽셀 값을 나타낸다. 그림 7과 그림 8은 MLCA 암호화된 영상과 2D CAT 암호화된 영상, 그리고 원 Lena 영상에서 8×8 크기인 영역의 픽셀 값이 암호화된 후 픽셀 값을 나타낸다. 그림9에서 (a)-(d)는 원 영상으로부터 두 단계의 암호화 과정과 올바른 키로 복호화 된 영상을 나타내고 (e)-(f)는 (a)-(d)에 대응하는 히스토그램을 나타낸다.

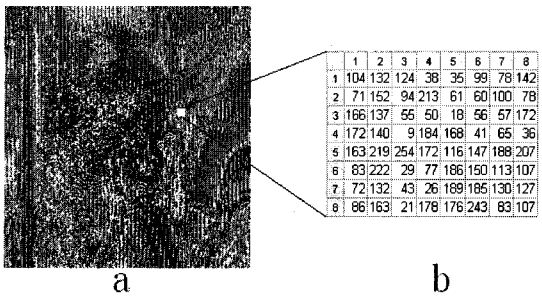
그림 9에서 암호화된 영상과 히스토그램은 원 영상과 상관성이 없을 뿐만 아니라 암호화된 영상은 잡음의 패턴과 유사하여 각 픽셀간의 연관성도 없음을 알 수 있다. 그리고 그림 9(d)에서 복원된 영상은 MLCA와 CAT를 기반으로 영상 암호화 하였기 때문에 복호화 할 때에 화질의 손실이 없이 완전 회복되었음을 알 수 있다.



	1	2	3	4	5	6	7	8
1	144	144	151	168	171	174	177	180
2	131	151	146	166	167	176	181	202
3	124	147	153	169	180	194	202	182
4	120	146	159	183	197	198	124	54
5	126	142	165	182	157	89	52	44
6	139	143	157	141	113	88	41	37
7	133	144	154	138	114	83	50	36
8	137	153	156	150	117	59	44	37

a b

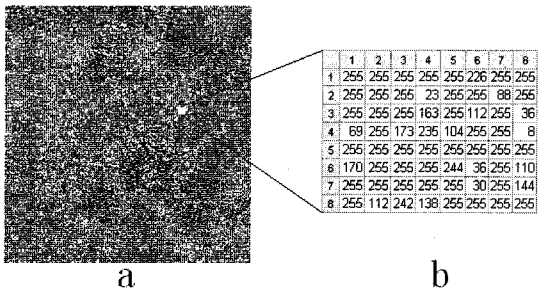
그림6. (a) 원영상 (b) 원영상의 데이터 집합
Fig. 6 (a) Original Image (b) Original data set



	1	2	3	4	5	6	7	8
1	104	132	124	38	35	99	78	142
2	71	152	94	213	61	60	100	78
3	166	137	55	50	18	56	57	172
4	172	140	9	184	168	41	65	36
5	163	219	254	172	116	147	188	207
6	83	222	29	77	186	150	113	107
7	72	132	43	26	189	185	130	127
8	86	163	21	178	176	243	83	107

a b

그림7. (a) MLCA암호화 영상 (b)MLCA 데이터집합
Fig. 7 (a) MLCA encrypted image (b) MLCA encrypted data set



	1	2	3	4	5	6	7	8
1	255	255	255	255	255	226	255	255
2	255	255	255	23	255	255	88	255
3	255	255	255	163	255	112	255	36
4	69	255	173	235	104	255	255	8
5	255	255	255	255	255	255	255	255
6	170	255	255	255	244	36	255	110
7	255	255	255	255	255	30	255	144
8	255	112	242	138	255	255	255	255

a b

그림8. (a) CAT 암호화 영상 (b) CAT 데이터 집합
Fig. 8 (a) CAT encrypted image (b) CAT encrypted data set

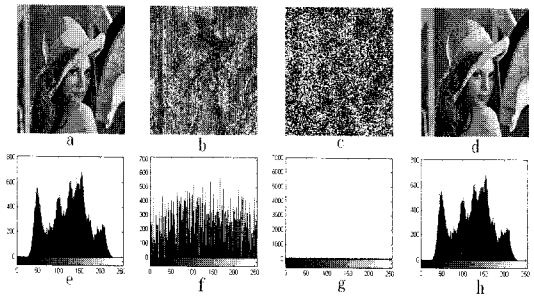


그림9. (a) 원영상 (b) MLCA로 암호화된 영상
(c) CAT로 암호화된 영상 (d) 복원된 영상 (e)-(h)
(a)-(d)의 그레이 스케일 히스토그램
Fig. 9 (a) Original image (b) MLCA encrypted image
(c) CAT encrypted image (d) decrypted image (e)-(h)
Gray-scale histogram of (a)-(d)

V. 안정성 분석

본 논문에서는 제안한 방법의 성능을 고찰하기 위하여 키 공간, 민감도, 손실 정도의 세 가지 측면에서 분석하였다.

5.1 암호화 키 공간 분석

충분히 큰 범위의 키 공간은 암호화 된 영상의 암호화 수준을 높인다고 알려져 있다. 본 논문에서 제안한 방법은 N-셀, 2-상태, M-이웃, 2D CA는 $2^{2^m+3(N+M)+2T}=2^{96}$ 가지의 키공간을 생성하며 동일한 CA구조를 갖는 MLCA는 $2^{2^m+N+2N}=2^{32}$ 가지의 키를 생성한다. 따라서 본 방법은 총 2^{128} 가지의 서로 다른 키를 생성할 수 있어 높은 암호화 수준을 확보할 수 있다.

5.2 암호화 키의 민감도 분석

암호화 키의 민감도 분석(Sensitivity Analysis)을 하기 위하여 식(15)을 도입한다.

$$C_r=\frac{N\sum_{i=1}^{N}(x_i\times y_i)-\sum_{i=1}^{N}x_i\times\sum_{i=1}^{N}y_i}{\sqrt{(N\sum_{i=1}^{N}x_i^2-(\sum_{i=1}^{N}x_i)^2)\times(N\sum_{i=1}^{N}y_i^2-(\sum_{i=1}^{N}y_i)^2)}} \quad (15)$$

여기서 x_i 와 y_i 는 인접한 픽셀 값을 나타내고 N은 총 픽셀 수이다.

표2 는 거짓 키에 대한 민감도 분석(sensitivity analysis) 결과를 나타낸다. 표2에서 알 수 있듯이 제안한 방법은 암호 키의 변화에 매우 민감하며 잘못된 키는 원 영상을 복원할 수 없음을 그림10에 그 예를 보인다.

표2. 민감도 분석
Table 2. Sensitivity analysis

Test item	Test Results
Sensitive for cipher to key(different key 10^{-36})	0.000000296045377

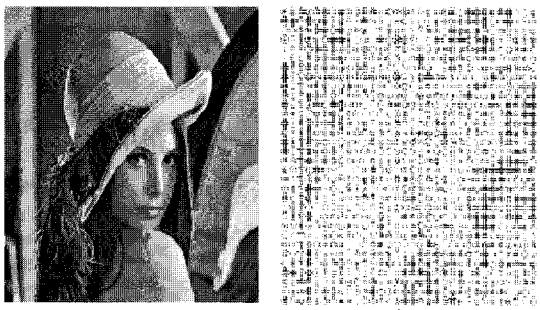


그림10. (a) 바른 키에 의해 복원된 영상 (b)거짓 키에 의해 복원된 영상
Fig 10 (a) Decrypted image with encryption key
(b) Decrypted image with wrong key

5.3 무손실 영상 암호화

본 논문에서 먼저 MLCA 암호화를 통하여 원 영상에 전이행렬 T를 곱하여 픽셀 값을 변환하였다. MLCA는 그룹 CA에 속하며 전이행렬 T는 정칙이기 때문에 전이행렬 T는 역행렬이 존재하며 변화된 픽셀 값은 원 픽셀 값으로 돌아올 수 있다.

또 본 방법은 MLCA 암호화 후에 CAT 암호화를 하였다. 표1의 게이트웨이 값에 의해 만들어진 기저함수는 직교성질을 갖고 있기 때문에 역CAT때에 암호화 된 영상은 완전 회복될 수 있다. 이로부터 본 논문에서 제안한 MLCA와 CAT를 이용한 방법은 무손실 암호화 방식이라는 것을 알 수 있다.

VI. 결론

CA는 공간과 시간을 이산적으로 다루고, 각 셀의 취할 수 있는 상태는 유한하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. 이러한 CA의 성질을 만족하는 새로운 개념인 MLCA와 CAT 을 이용하여 새로운 영상 암호화 방법을 제안하였다.

제안한 방법은 암호화 수준을 높이기 위하여 먼저 Wolfram 규칙을 선택하여 규칙행렬을 구성한다. 그리고 규칙 행렬에 의해MLCA 전이행렬 T을 만든 후, 암호화하려는 영상의 픽셀 위치에 따라 전이행렬을 곱하여 픽셀의 값을 변환하였다. 또 게이트웨이 값의 설정에 따른 2D CAT 기저함수를 생성하여 MLCA 암호화한 영상을 다시 한번 CAT를 이용해 암호화하였다.

실험결과와 분석을 통하여 본 방법은 총 2128 가지의 암호화 키 공간을 생성할 수 있어 높은 암호화 수준을 가짐을 확인하였으며 영상의 암호화 및 복원 시에 무손실 암호화를 실현할 수 있었다.

참고문헌

[1] F. Pichler, J. Scharinger, "Ciphering by Bernoulli shifts in finite Abelian groups", Contributions to general algebra. Proc. Linz-conference, pp. 465-476, 1994.

[2] J. Scharinger, "Fast encryption of image data using chaotic Kolmogorov Flows", J Electron Image, Vol. 2, No. 2, pp. 318-325, 1998.

[3] G. Chen, Y. Mao, C. Chui, "Symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons & Fractals, Vol.21, No. 3, pp. 749-761, 2004.

[4] S. Lian, "Efficient image or video encryption based on spatiotemporal chaos system", Chaos, Solitons & Fractals, Vol.34, pp. 851-859, 2007.

[5] J. Von Neumann, "The theory of self-reproducing Automata", A. W. Burksed. Univ. of Illinois Press, UrbanaandLondon,1966.

[6] J. Von Neumann, "The General and Logical Theory of Automata", Collected Works, A. H. Taub, Vol. 5, pp. 288, 1963.

[7] S. Wolfram, "Statical Mechanic of Cellular Automata", Review of Modern Physiscs, Vol. 55, pp. 601-644, 1983.

[8] S. Wolfram, "Computational Theory of Cellular Automata in Cellular Automata and Complexity", Addison-Wesley, pp. 150-202, 1984.

[9] M. Skolnick, S. Kim, and R. O'Bara, "Morphological algorithms for computing non-planar point neighborhoods on cellular automata", in Proc. 2ndInt. conf. Comput. Vision, pp.106-111, 1988.

[10] G. Hernandez and H. J. Herrmann, "Cellular automata for elementary image enhancement", Graphical Models and Image Processing, Vol. 58, No. 1, pp. 82-89, 1996.

[11] 박영일, 김석태, "다 해상도 특성을 갖는 2D 셀룰러 오토마타 변환을 이용한 디지털 워터마킹" 한국통신학회, Vol. 34, pp. 105-112, 2009.

[12] Yongri Piao, Seoktae Kim, Sungjin Cho, "Two-Dimensional Cellular Automata Transform for a Novel Edge Detection", Computability in Europe 2008, Logic and Theory of Algorithms, pp. 367-376, Greece, June 2008.

[13] Olu Lafe, "Cellular Automata Transforms: Theory and Application in Multimedia Compression, Encryption, and Modeling", Kluwer Academic Publishers, Boston/ Dordrecht/London, 2000.

저자소개

박영일(Yongri Piao)

해양정보통신학회 논문지 제13권 8호 참조

조성진(Sung-Jin Cho)

해양정보통신학회 논문지 제13권 6호 참조

김석태(Seok-Tae Kim)

해양정보통신학회 논문지 제13권 8호 참조