Journal of Korea Multimedia Society Vol. 18, No. 12, December 2015(pp. 1462-1467)
http://dx.doi.org/10.9717/kmms.2015.18.12.1462

1차원 비선형 그룹 셀룰라 오토마타 기반의 영상 암호

최언숙[†], 조성진[††], 김태홍[†††]

Image Encryption Based on One Dimensional Nonlinear Group Cellular Automata

Un-Sook Choi[†], Sung-Jin Cho[††], Tae-Hong Kim[†††]

ABSTRACT

Pixel values of original image can be changed by XORing pixel values of original image and pixel values of the basis image obtained by pseudo random sequences. This is a simple method for image encryption. This method is an effect method for easy hardware implementation and image encryption with high speed. In this paper we propose a method to obtain basis image with pseudo random sequences with large nonlinearity using nonlinear cellular automata and maximum length linear cellular automata. And experimental results showed that the proposed image encryption scheme has large key space and low correlation of adjacent cipher pixel values.

Key words: Image Encryption, Group Cellular Automata, Nonlinear Cellular Automata, Pseudo Random Sequences, Basis Image

1. 서 론

멀티미디어 기술은 최근 몇 년 동안 상당한 발전이 있었다. 인터넷을 통해 오디오, 동영상, 이미지와 같은 멀티미디어를 전송하는 것이 이제 아주 보편화 되었다. 그러나 인터넷은 안전하지 못한 채널로 보안적인 측면에서 많은 문제들을 가지고 있다. 또한 데이터 복제를 할 수 있는 기기가 보편화 된 이후 멀티미디어 콘텐츠 이용자의 저작권에 대한 인식부족으로 인해 멀티미디어 콘텐츠의 불법복제 문제는 날이 갈수록 심각해지고 있다[1].

인터넷과 같은 비보안 채널 상에서 멀티미디어 데이터의 안전성과 기밀성을 획득하기 위해 많은 암호기술이 제안되어왔다. 특히 영상을 암호화하기 위한 가장 간단한 방법은 의사 난수열을 이용하여 기저영상을 만든 후 기저영상과 원 영상의 픽셀값을 XOR 연산을 취해 원 영상의 픽셀값을 변화시키는 것이다. 이러한 방법으로 영상을 암호화하는 경우, 하드웨어의 구현이 용이하고 암호화 속도가 빠른 장점이 있다[2].

셀룰라 오토마타(Cellular Automata, 이하 CA)란 이산 시간의 동적 시스템으로 셀이라는 기본 단위 메모리의 배열로 이루어진다. 이 시스템에서 셀의 다음 상태는 자기 자신과 인접한 두 셀의 상태에 의해 정해진 규칙에 의해 갱신된다. 이러한 CA는 간단하고, 규칙적이며, 작은 단위로 확장 연결할 수 있는 구조이기 때문에 VLSI 하드웨어 구현에 알맞다[3]. 가장 간단한 구조를 가지는 1차원 CA는 모든 셀이 선형으로 배열되어 있고, CA의 상태전이에 적용되는 규칙의 종류에 따라 선형 CA와 비선형 CA로 나뉜다. 또한 CA의 모든 상태에 대하여 이전상태가 존재하는 CA를 그룹 CA라 하고 그룹CA는 셀들이 일

※ Corresponding Author : Sung-Jin Cho, Address: (608-737) 45, Yongso-ro, Nam-gu, Busan, Korea, TEL : +82-51-629-5527, FAX : +82-51-629-5519, E-mail : sjcho@pknu.ac.kr
Receipt date : Aug. 3, 2015, Approval date : Oct. 1, 2015

[†] Dept. of Information & Communications Eng., Tongmyong Univ. (E-mail : choies@tu.ac.kr)
[††] Dept. of Applied Mathematics, Pukyong National Univ.
[†††] Dept. of Information Sequrity, Tongmyong Univ. (E-mail : rlaxoghd91@gmail.com)

정한 주기 이후 원래의 상태로 반복되는 특징을 가지고 있다. 크기가 n인 그룹 CA의 주기가 2^n-1인 경우 이러한 CA를 MLCA(maximum Length CA)라 한다. MLCA는 의사 난수열 생성기로 적합하여 테스트 패턴 생성기로 응용되며 암호시스템에 적용이 가능하다[4,5]. CA를 이용한 영상암호화는 대부분 그룹 CA를 적용한다[2,6-10]. 특히 최대 길이를 갖는 선형 MLCA 또는 여원 MLCA를 이용하여 영상을 암호화하는 방법은 먼저 CA에 의해 생성된 의사 난수열을 이용하여 기저영상을 생성한다. 영상암호를 위해 원영상과 CA를 이용하여 생성한 기저영상을 XOR 연산하여 원 영상의 모든 픽셀 값을 무질서하게 변환시켜 영상을 암호화 한다[2,6].

본 논문에서는 비선형 그룹 CA와 선형 90/150 MLCA를 이용하여 비선형성이 매우 높은 의사난수열을 생성하여 기저영상을 만드는 방법을 제안하고 제안된 영상암호의 안전성에 대해 분석한다. 제안된 방법은 기존의 선형 의사 난수열을 생성하여 기저영상을 만드는 방법에 비해 훨씬 랜덤성이 강하므로 암호체계의 보안수준을 높일 수 있으리라 사료된다.

2. 관련연구

세 개의 이웃을 가지는 CA에 대한 다음 상태 전이 함수는 3개의 변수를 가지는 부울 함수로 f:{000, 001, … , 111}→{0,1}이다. 그러므로 다음 상태 전이 함수 f는 256개가 있으며 이것을 CA의 규칙이라고 한다. Table 1은 CA의 전이규칙의 몇 가지 예이다. 전이규칙 150이라는 것은 현재 이웃상태에 대한 다음 상태 값 '10010110'을 십진수로 나타낸 것이다.

n개의 셀로 이루어진 n-셀 CA의 각 셀에 사용되는 규칙이 90과 150만 사용되는 CA를 90/150 CA라 하고 Table 2는 전이규칙 90, 150을 부울식으로 나타낸 것이다.

Table 2. Boolean representation of the transition rules 90 and 150

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

Table 2와 같이 전이규칙을 부울식으로 표현했을 때 XOR함수로만 이루어진 CA를 선형 CA라 한다. 이러한 CA는 상태전이 함수를 $n \times n$ 행렬로 나타낼 수 있으며, 이를 상태전이행렬(state-transition matrix) T 라고 한다[5]. 본 논문에서 이용하는 90/150 CA는 특성다항식과 최소다항식이 같으며, 모든 크기의 CA에 대하여 MLCA가 존재한다[11]. 비선형 CA는 셀에 선형이 아닌 규칙을 적용한 CA이며, 그룹 CA는 주어진 상태에 대한 이전상태가 존재하는 CA이다[5]. 예를 들어 전이 규칙 141은 식 (1)과 같이 표현 된다.

$$q_i(t+1) = q_i(t)q_{i+1}(t) \oplus q_{i-1}(t)q_{i+1}(t) \oplus q_{i-1}(t) \oplus q_{i+1}(t) \oplus 1 \quad (1)$$

식(1)과 같이 전이규칙이 선형이 아닌 경우는 다음상태를 나타내는 함수가 자신과 이웃한 셀의 상태의 곱의 항이 반드시 나타나게 된다. 따라서 생성되는 수열은 비선형 수열이 된다. 비선형 수열은 선형 수열에 비하여 렌덤성이 강하므로 본 논문에서는 영상암호를 위하여 비선형 수열을 생성하는 크기가 작은 비선형 그룹 CA와 최대주기를 갖는 선형 MLCA를 이용한다.

3. 제안 방법

본 논문에서는 그룹 성질을 가지는 두 개의 비선형 CA와 선형 MLCA를 이용하여 기저영상을 만드

Table 1. State transition rules of CA

Neighborhood	111	110	101	100	011	010	001	000	Rule
Next state	0	1	0	1	1	0	1	0	90
Next state	1	0	0	0	1	1	0	1	141
Next state	1	0	0	1	0	1	1	0	150
Next state	1	0	1	0	0	1	0	1	165
Next state	1	0	1	0	1	1	0	0	172

는 방법을 제안한다. 제안 방법은 식 (2)와 같이 나타낼 수 있다.

$$B_{i,j} = Nf_2(Nf_1(S_0))(i=1\cdots 255,\ j=1\cdots 255) \quad (2)$$

식 (2)에서 S_0는 키의 일부인 상태의 초깃값을 의미하며 비선형 함수 Nf_1을 통해 생성된 값이 영상의 첫 번째 행의 값으로 생성되며 비선형 함수 Nf_2을 통해 두 번째 행부터의 픽셀 값이 생성되게 된다. $Nf_i(i=1,2)$를 통해 생성된 영상을 $B_{i,j}$로 표현 한 후 기저영상을 생성한다. Fig. 1은 $Nf_i(i=1,2)$를 통해 기저영상을 얻는 과정이다.

Fig. 2는 Nf_i의 구조이다. 먼저 8 비트 초깃값(S_0)을 4 비트로 나눈 후 비선형 그룹 CA를 통해 상태전이를 한 후 선형 MLCA를 통해 다시 상태전이를 한다. 이때 90/150 MLCA를 통해 최대주기까지 생성할 수 있다. 90/150 MLCA를 통해 상태 전이된 결과를 다시 비선형 그룹 CA의 역함수를 통해 최종 상태전이를 함으로써 행의 픽셀값을 생성 하게 된다. 다음으로 두 번째 비선형 함수를 이용하여 기저 영상의 나머지 픽셀값을 생성하는데, 첫 번째 비선형 함수와 달리 초깃값이 첫 행에 의해 이미 정해진 상태이고 이 값을 이용하여 동일한 절차에 의해 픽셀값이 생성된다. 식 (3)은 식 (2)에 의해 생성된 기저영상을 이용하여 주어진 영상을 암호화하는 과정이다.

$$E_{i,j} = (B_{i,j} \oplus I_{i,j})\ (i=1,\ 2,\cdots 255,\ j=1,\ 2,\cdots\ 255) \quad (3)$$

여기서 $I_{i,j}$는 원 영상의 픽셀값이다.

Fig. 3은 본 논문에서 제안하고 있는 암호화 과정 및 복호화 과정을 나타낸다.

4. 실험결과 및 안정성 분석

본 논문에서는 영상들의 변화를 고찰하기 위해 영상처리에서 대표적으로 사용되어지는 이미지인 256 × 256 크기의 8 비트 그레이 레벨 'lena' 영상을 사용하여 고찰하였다. Fig. 4는 기저영상과 XOR 연산을 통해 생성된 암호화 영상이다.

r / c	1	2	3	4	5	·····	253	254	255	256
1	176	43	48	235	160	·····	39	57	1	176
2	4	78	132	14	52	·····	71	175	242	4
3	30	80	222	240	166	·····	111	59	193	30
4	208	177	96	196	200	·····	171	174	146	208
5	97	10	164	190	184	·····	206	53	20	97
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
252	145	31	155	241	130	·····	80	182	125	145
253	18	211	246	202	36	·····	177	232	64	18
254	212	106	56	185	70	·····	10	13	81	212
255	94	140	173	239	109	·····	25	245	178	94
256	176	43	48	235	160	·····	39	57	1	176

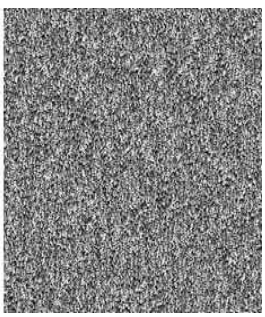


Fig. 1. The process of obtaining a basis image using $Nf_i(i=1,2)$.

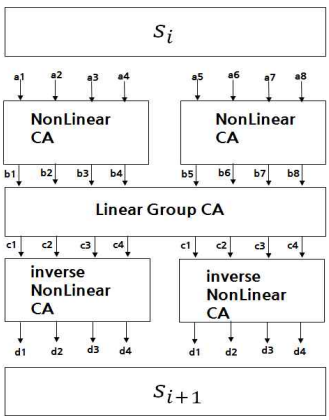


Fig. 2. Structure of Nf_i.

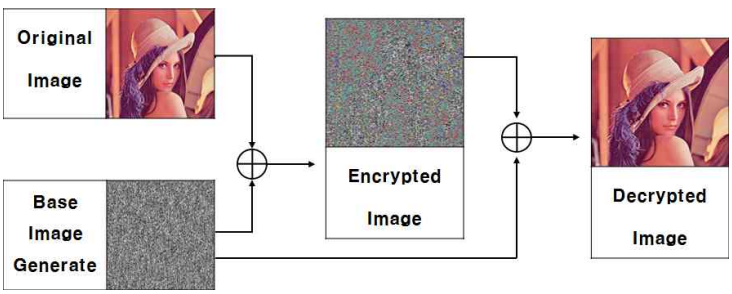


Fig. 3. Encryption and decryption process.

(a) (b)

Fig. 4. The original image(a) and the encrypted image (b).

암호화된 영상을 육안으로 보았을 때 원 영상을 알아보기 어려웠으며 PSNR(Peak Signal-to- Noise Ratio)에 대한 계산 결과는 8.5592로 암호화된 결과가 원 영상에 대한 왜곡이 심하다는 것을 알 수 있다. 본 논문에서 제안한 영상 암호 체계의 안전성을 평가하기 위해 통계적 분석인 히스토그램, 픽셀값 간의 상관관계 분석결과를 제시한 후 키공간을 분석한다.

4.1 통계적 분석

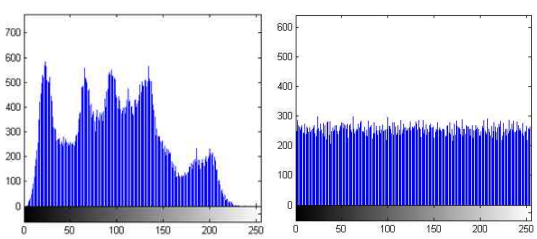
4.1.1 히스토그램 분석

Fig. 5는 원래 영상, 암호화된 영상의 히스토그램이다. 암호화된 영상의 히스토그램을 보면 모든 픽셀값이 균등하게 분포되어 있으므로 통계적인 공격(빈도수 분석)에 강하다는 것을 알 수 있다[12].

4.1.2 이미지 상관관계 분석

일반적으로 원 영상의 인접한 픽셀값은 높은 상관관계를 갖는다. 반면 효과적인 영상암호 기법에 의해 암호화된 영상은 인접한 픽셀값 사이의 상관관계가 낮다. x와 y를 인접한 두 픽셀의 그레이 레벨 값이라고 할 때 x, y 사이의 상관계수 C_{xy}는 식 (4)와 같다.

$$C_{xy} = \frac{Cov(x,y)}{\sigma_x \cdot \sigma_y} \tag{4}$$



(a) (b)

Fig. 5. Histogram distribution of the original image(a) and the encrypted image(b).

여기서 $Cov(x,y)$는 x와 y의 공분산이며, σ_x는 x의 표준편차이다. $Cov(x,y)$와 σ_x는 식 (5)와 (6)과 같다.

$$\sigma_x = \sqrt{Var(x)} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2} \tag{5}$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{6}$$

Fig. 6은 원 영상과 암호화된 영상의 세로 픽셀간의 상관관계에 대한 그래프이다. 암호화 된 영상의 세로 픽셀에 대한 상관관계를 보면 원 영상에 비해 인접한 픽셀값들 간의 유사성이 매우 낮다. 이는 암호화된 영상에서 원래의 영상 혹은 기저영상을 추출 하는 것이 어렵다는 것을 의미한다[12]. 이러한 결과는 가로 픽셀과 대각선 픽셀 사이에 대해서도 유사하다.

4.2 키 공간 분석

Nf_i를 이용하여 기저영상을 생성 할 수 있는 주요 키는 CA 규칙, 셀의 최대 상태의 수, 비선형 CA f의 개수, f^{-1}의 개수, 이웃 셀의 수, 초기 구성 등이 있다. 큰 범위의 키 공간은 영상의 암호화 수준을 높인다. 따라서 셀의 상태 수를 k, m은 이웃 셀의 수, n은 셀의 수라 할 때 키 공간은 식 (7)과 같다.

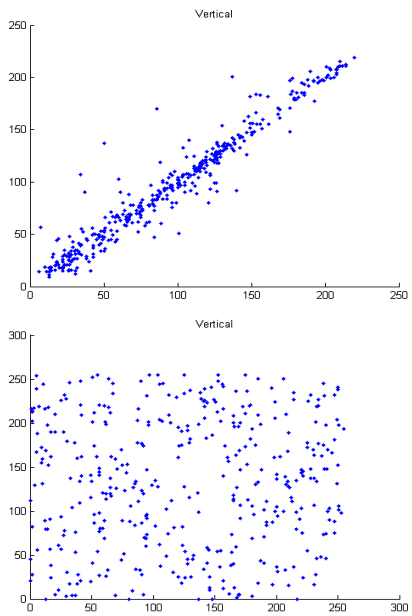


Fig. 6. Correlation of vertically adjacent pixels. (a) the original image (b) the encrypted image.

$$K = \left(\frac{(k^k)^m}{2} \cdot k^n \right)^2 \cdot k^n \quad (7)$$

본 논문에서 제안된 조건은 행과 열이 각각 8-셀, 2-상태, 3-이웃, 각각 두 개의 f, f^{-1}으로 구성된다. 먼저 f, f^{-1}의 개수를 구하면 $\frac{(2^{2^3})^8}{2} = 2^{64-1} = 2^{63}$ 이고, 상태전이행렬 T의 개수를 구하면 2^8, 초깃값의 개수는 2^8이다. 그러므로 키 공간은 $(2^{63} \times 2^8)^2 \times 2^8 = = 2^{142} \times 2^8 = 2^{150}$가지의 일정한 키를 생성 할 수 있기 때문에 충분한 암호화 수준을 확보 할 수 있다[12].

5. 결 론

본 논문에서는 원 영상을 암호화하기 위해 비선형 그룹 CA와 선형 MLCA를 이용하였다. 즉, 영상을 암호화하기 위해 두 개의 비선형 함수와 그것의 역함수들 및 두 개의 상태 전이행렬를 행과 열에 각각 적용하여 비선형 수열을 생성시켜 랜덤성이 높은 효과적인 기저영상을 생성하였다. 여기서 생성된 기저영상을 통해 원 영상을 암호화 하였다. 암호화된 영상의 안전성을 평가하기 위하여 통계적 분석과 키공간 분석을 하였다. 본 논문에서 제안한 암호화 방법이 통계적인 공격에 강하고 인접한 픽셀 간의 상관관계가 현저히 낮음을 볼 수 있었고, 충분한 암호화 수준을 확보 할 수 있었다.

REFERENCE

[1] Korea Federation of Copyright Organizations, *Annual Report on Copyright Protection in Korea*, 2014.

[2] 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, pp. 1279-1285, 2014.

[3] J.V. Neumann, *Theory of Self-reproducing Automata*, University of Illinois Press, Urbana and London, 1966.

[4] S. Wolfram, "Statistical Mechanics of Cellular Automata," *Reviews of Modern Physics*, Vol. 55, No. 3, pp. 601-644, 1983.

[5] P.P. Chaudhuri, D.R. Choudhury, S. Nandi, and S. Chattopadhyay, *Additive Cellular Automata Theory and Applications*, IEEE Computer Society Press, USA, 1997.

[6] T.H. Nam, S.T. Kim, and S.J. Cho, "Image Encryption using Complemented MLCA based on IBCA and 2D CAT," *Journal of The Institute of Electronics and Information Engineers*, Vol. 46-SP, No. 4, pp. 34-41, 2009.

[7] P. Ping, F. Xu, and Z.J. Wang, "Image Encryption based on Non-affine and Balanced Cellular Automata," *Signal Processing*, Vol. 105, No. 12, pp. 419-429, 2014.

[8] J. Jin, "An Image Encryption Method based on Elementary Cellular Automata," *Optics and Lasers in Engineering*, Vol. 50, No. 12, pp. 1836-1843, 2012.

[9] S. Roy, S. Nandi, J. Dansana, and P.K. Pattnaik, "Application of Cellular Automata in Symmetric Key Cryptography," *Proceeding of IEEE International Conference on Communication amd Signal Processing*, pp. 572-576, 2014.

[10] S. Nandi, S. Roy, S. Nath, S. Chakraborty, W.B.A. Karaa, and N. Dey, "1-D Group Cellular Automata based Image Encryption Technique," *Proceeding of IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies*, pp. 521-526, 2014.

[11] S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim, and S.H. Heo, "New Synthesis of One-dimensional 90/150 Linear Hybrid Group Cellular Automata," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 26, No. 9, pp. 1720-1724, 2007.

[12] J. Ahmad and F. Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes," *International Journal of Video & Image Processing and Network Security*, Vol. 12, No. 4, pp. 18-31, 2012.

최 언 숙

1992년 성균관대학교 산업공학과 졸업(공학사)
2000년 부경대학교 응용수학과 석사졸업(이학석사)
2004년 부경대학교 응용수학과 박사졸업(이학박사)
2009년 부경대학교 정보보호학과 박사졸업(공학박사)
2006년~현재 동명대학교 정보통신공학과 교수
관심분야 : 정보보호 및 암호이론/ 셀룰라 오토마타 및 그 응용

조 성 진

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

김 태 홍

2010년~현재 동명대학교 정보보호학과 학과과정
2015년 차세대보안리더양성프로그램 이수중
관심분야 : 디지털포렌식, 네트워크보안