90/150 NBCA 구조를 이용한 영상 암호화

남태희* · 김석태1)** · 조성진***

*동주대학 **부경대학교 ***부경대학교

Image Encryption using 90/150 NBCA structure

Tae-Hee Nam* · Seok-Tae Kim** · Sung-Jin Cho***

*Dongju College University **Pukyong National University ***Pukyong National University

E-mail : thnam1@hanmail.net setakim@pknu.ac.kr sjcho@pknu.ac.kr

요 약

본 논문은 90/150 NBCA(Null Boundary Cellular Automata)에 기반한 여원 MLCA(Maximum Length Cellular Automata)를 이용하여 영상을 암호화하는 방법을 제안한다. 암호화 방법은 먼저 선형 MLCA에서 유도된 여원 MLCA를 이용하여 원 영상의 크기만큼 PN(pseudo noise) 수열을 생성한다. 그 후 생성된 여원 MLCA 수열을 원 영상과 XOR 연산하여 암호화를 한다. 마지막으로 실험을 통하여 본 방법의 유효성을 검증한다.

ABSTRACT

In this paper, we propose the image encryption method using complemented MLCA based on 90/150 NBCA(Null Boundary Cellular Automata). The encryption method is processed in the following order. First, complemented MLCA, which is derived from linear LFSR, is used to produce a PN(pseudo noise) sequence, which matches the size of the original image. Then, the created complemented MLCA sequence goes through a XOR operation with the original image to become encrypted. Lastly, an experiment is processed to verify the effectiveness of this method.

키워드

Cellular Automata, PN(pseudo noise) sequences, MLCA(Maximum Length Cellular Automata), NBCA(Null Boundary Cellular Automata), Complemented MLCA

Ⅰ. 서 론

오늘날 영상 정보들은 새로운 정보 컨텐츠로서 희소의 가치를 가진다. 그러나 컨텐츠는 인터넷상에서 누구나 쉽게 응용하는 문제로 인해 개인 및 단체의 주요 저작권에 많은 피해를 주고 있다. 따라서 오늘날 영상 정보 보호는 저작권 문제로서 중요한 화두로 대두되고 있다. 즉 비밀 보장 및 개인의 정보 보호를 위한 새로운 연구과제의 대상이 되고 있다. 최근 이러한 정보를 보호하는 주요 연구 방향 중 하나로 영상 정보를 암호화하는 방법들이 연구되고 있다[1,2].

영상 암호화 방법들 중에는 시각적 암호작성(Visual Cryptography), Kolmogorov flow map, chaotic standard map, chaotic logistic map 등의 기술을 이용한 연구가 제시되고 있다[3,4,5,6].

제시된 방법들 중 Ateniese는 시각적 암호작성을 이용하여 암호화하는 방법을 제안하였으며[3], Scharinger는 Kolmogorov flow map을 이용한 영상 암호화 방법을 제안 하였다[4]. 또한 Wong은 chaotic standard map을 기반으로 한 영상 암호화 방법을 제안하였으며[5], Pareek은 chaotic logistic map을 이용하여 영상 암호화 방법을 제안하였다[6].

제안 방법 중 시각적 암호 작성은 원 영상을 픽셀단위로 분할하여 암호화함으로서 결합 시 무손실 복원이 되지 않는 단점이 있다[3]. 또한 map을 이용한 방법들은 영상의 픽셀 위치를 discredited chaotic map을 이용하여 변환 시킨 다음, CBC(Cipher Block Chain) 모드로 픽셀 값을 변환하기 때문에 암호화 효과가 떨어지는 단점이 있다.

본 논문에서는 기존 방법과 달리 랜덤성이 강한 CA(Cellular Automata) 원리를 이용한 영상 암호화 방법을 제안한다. 암호화 방법은 90/150 NBCA(Null Boundary Cellular Automata)에 기초하여 원 영상의 크기만큼 여원 MLCA 수열을 생성한다. 그 후, 생성된 여원 MLCA(Maximum Length Cellular Automata) 수열을 원 영상과 XOR 연산하여 영상을 암호화 한다. 또한 복호화

**1) 교신저자

는 암호화된 영상과 여원 MLCA 수열을 XOR 연산하여 원 영상으로 복원한다. 마지막으로 실험을 통하여 본 암호화 방법의 유효성을 검증한다.

II. 제안 방법

CA 원리는 시간과 공간을 이산적으로 다루는 시스템이다.

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

식 (1)은 1D CA의 상태전이 함수로서 모든 셀들이 선형으로 배열되어 있는 3-이웃 구조이다. 여기서 f는 결합논리를 가지는 국소전이 함수이다. 3-이웃 CA는 서로 다른 2^3 개 이웃의 배열상태가 있다. 또한 CA는 Wolfram Rule에 의해서 그 원리가 인접한 이웃과 결합 논리로 서로 연결되어 있고, 그 형태가 규칙적인 배열로 구성되기 때문에 랜덤성이 강한 특성을 가진다.

제안된 방법에서 그림 1은 8셀의 90/150 NBCA 에 의하여 주기가 255인 고품질의 PN 수열을 생성하는 구조이며, 식 (2)는 계산 방법이다.

본 논문의 암호화 방법은 90/150 NBCA에 기초하여 선형 MLCA 수열을 구한 다음, 선형 MLCA에서 유도된 여원 MLCA 수열을 구한다.

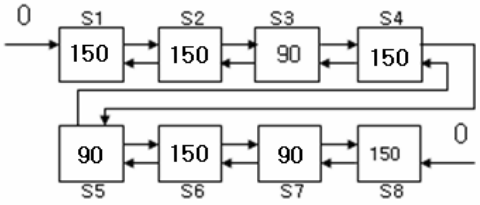


그림 1. 90/150 NBCA structure

$$\begin{aligned}
s_1^+ &= 0 \oplus s_1 \oplus s_2 \\
s_2^+ &= s_1 \oplus s_2 \oplus s_3 \\
s_3^+ &= s_2 \oplus s_4 \\
s_4^+ &= s_3 \oplus s_4 \oplus s_5 \\
s_5^+ &= s_4 \oplus s_6 \\
s_6^+ &= s_5 \oplus s_6 \oplus s_7 \\
s_7^+ &= s_6 \oplus s_8 \\
s_8^+ &= s_7 \oplus s_8 \oplus 0
\end{aligned} \quad (2)$$

식 (2)에서, s_i는 i셀의 현재 상태이며, s_i^+는 다음 상태를 표시한다.

n개의 셀을 가지는 선형 3-이웃 90/150 NBCA에서는 현재 상태를 다음 상태로 전이시키는 전이함수를 $n \times n$ 행렬로 나타낸다. n 셀 90/150 NBCA의 상태전이 행렬(transition matrix) T는 식 (3)과 같이 삼중 대각 행렬로 나타낸다[7,8].

$$T = \begin{pmatrix} a_1 & 1 & 0 & \dots & 0 & 0 \\ 1 & a_2 & 1 & \dots & 0 & 0 \\ 0 & 1 & a_3 & \dots & 0 & 0 \\ & & & \dots & & 1 \\ 0 & 0 & 0 & \dots & 1 & a_n \end{pmatrix} \quad (3)$$
$$(a_1, a_2, \dots, a_n \in \{0,1\})$$

a_n는 n번째 셀에 적용된 전이규칙이 90인 경우는 0이고, 150인 경우는 1이다. 이것은 상태전이 행렬 T에서 n번째 행은 n번째 셀에 적용되는 CA 규칙이며, 그 셀의 다음 상태가 현재 상태에 의존하면 1, 그렇지 않으면 0으로 한다는 의미이다. 즉 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. $R = < a_1, a_2, \dots, a_n >$를 CA 전이 규칙이라 한다.

표 1. Linear and complemented rule

선형 규칙	$x_i(t+1)$	여원 규칙	$\overline{x_i(t+1)}$
90	$x_{i-1}^t \oplus x_{i+1}^t$	165	$\overline{x_{i-1}^t \oplus x_{i+1}^t}$
150	$x_{i-1}^t \oplus x_i^t \oplus x_{i+1}^t$	105	$\overline{x_{i-1}^t \oplus x_i^t \oplus x_{i+1}^t}$

전이 행렬 T에서 n번째 행은 n번째 셀에 적용되는 규칙이며, $f_t(x)$가 시간 t에서 CA의 상태를 나타내면 시간 $t+1$에서의 상태는 식 (4)와 같다.

$$f_{t+1}(x) = T \bullet f_t(x) \quad (4)$$

여기서 p단계 시간은

$$f_{t+p}(x) = T^p \bullet f_t(x) \quad (5)$$

이다. 90/150 MLCA로부터 유도된 여원 MLCA의 p단계 후 상태는 식 (6)과 같다.

$$\begin{aligned} f_{t+p}(x) &= \overline{T}^p \bullet f_t(x) \\ &= T^p \bullet f_t(x) \oplus (I \oplus T \oplus \dots \oplus T^{p-1}) F \end{aligned} \quad (6)$$

여기서 F는 여원벡터이다.

III. 암호화 방법 및 실험 결과

본 논문에서 제안한 영상 암호화 방법은 먼저 선형 MLCA에서 유도된 여원 MLCA를 이용하여 원 영상의 크기만큼 고품질의 PN 수열을 생성한다. 생성된 여원 MLCA 수열을 이용하여 여원 MLCA 기저 영상으로 변환한다. 그 후 변환된 여원 MLCA 기저영상을 원 영상과 XOR 연산하여 영상을 암호화한다. 또한 복원 영상은 암호화된

영상과 여원 MLCA 기저영상을 XOR 연산하여 원 영상으로 복원한다.

본 논문에서 실험된 영상은 256X256 크기의 8 비트 그레이 레벨 영상을 사용하였다. 영상은 저주파 성분과 고주파 성분이 균일하게 잘 분포되어 있는 영상을 암호화 대상으로 하였다.

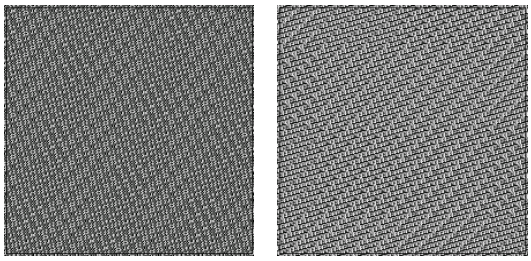


그림 2. Complemented MLCA basis image and linear MLCA using based on 90/150 NBCA

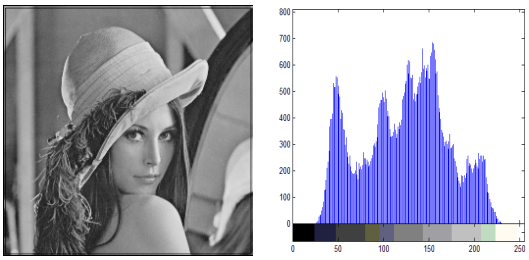
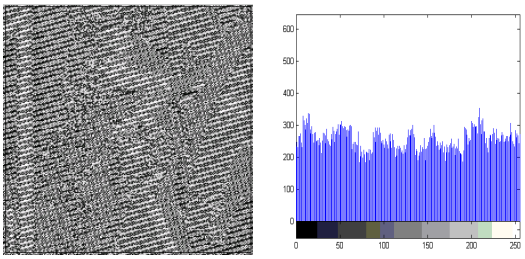
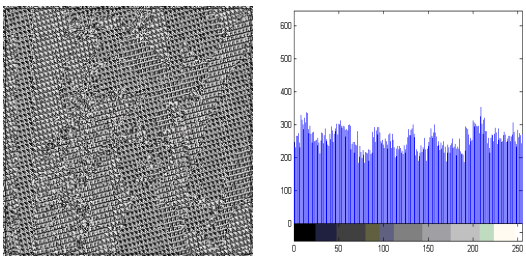


그림 3. Original image "lena" and Histogram



PSNR of encrypted image(PSNR=+27.3148 dB)
그림 4. Image encryption and Histogram by Linear MLCA



PSNR of encrypted image(PSNR=+25.5098 dB)
그림 5. Image encryption and Histogram by Complemented MLCA

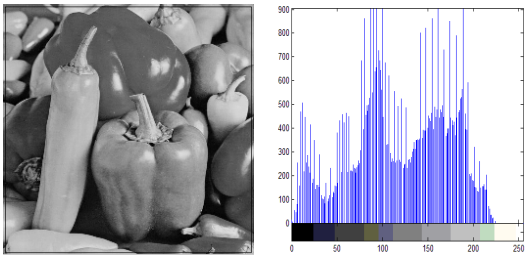
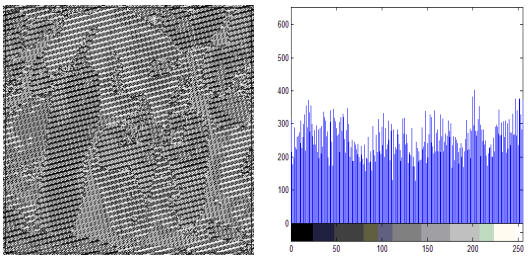
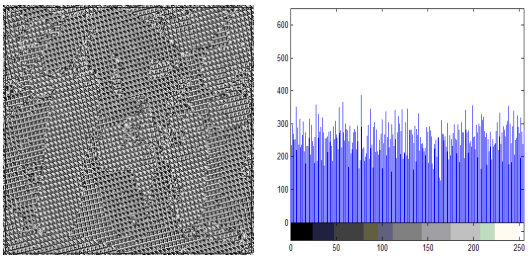


그림 6. Original image "peppers" and Histogram



PSNR of encrypted image(PSNR=+27.0438 dB)
그림 7. Image encryption and Histogram by Linear MLCA



PSNR of encrypted image(PSNR=+25.3825 dB)
그림 8. Image encryption and Histogram by Complemented MLCA

생성된 선형과 여원 MLCA 기저영상은 그림 2에 보였다. 또한 원 영상을 선형 MLCA 기저영상과 XOR 연산에 의해 생성된 선형 MLCA 영상 변환은 그림 4와 그림 7에서 보였다. 원 영상을 여원 MLCA 기저영상과 XOR 연산에 의해 생성된 영상 암호화의 결과는 그림 5와 그림 8에서 나타내었다. 여기서 여원 MLCA에 의해 암호화된 영상은 잡음의 패턴과 유사하게 출력된 것을 확인 할 수 있으며, 각 픽셀간의 연관성도 전혀 알 수 없게 출력됨을 볼 수 있었다. 영상의 암호화 평가 기준으로 히스토그램과 PSNR(Peak Signal to Noise Ratio)을 사용한다. 히스토그램은 원 영상에 선형 및 여원 MLCA 적용 결과, 공통적으로 픽셀의 분포가 고르고 안정되게 출력됨을 볼 수 있다. PSNR은 원 영상과 잡음 영상의 비를 측정하는데, 선형 MLCA 적용에 의한 영상 암호화는 각각 +27.3148 dB, +27.0438 dB 이었으며, 여원 MLCA 적용에 의한 영상 암호화는 각각 +25.5098 dB, +25.3825 dB로 나타났다. 즉 선형

MLCA를 적용하여 영상을 변환한 결과 보다 여원 MLCA가 보다 향상된 암호화 수준임을 알 수 있다.

본 논문에서 제시된 PSNR은 그 값이 낮을수록 영상의 왜곡이 크다는 것을 의미하는데, 보통 PSNR<35 dB이면, 시각적으로 영상의 왜곡을 느낄수 있다.

Ⅳ. 결 론

본 논문에서는 원 영상을 암호화하기 위해 90/150 NBCA에 기초하여 여원 MLCA를 적용하였다. 여원 MLCA는 선형 MLCA를 유도하여 여원 MLCA를 구한다. 여원 MLCA는 선형 MLCA보다 높은 복잡도를 가지므로 고품질의 PN 수열을 생성한다. 따라서 생성된 여원 MLCA를 원 영상과 XOR 연산에 의해 영상을 암호화 하였다.

결과적으로 제안된 여원 MLCA를 이용한 영상 암호화 방법은 기존 선형 MLCA보다 랜덤성이 강한 암호화 수준임을 알 수 있고, 암호화 방법으로 강한 안정성이 있음을 확인하였다.

참고문헌

[1] 박진, 나철훈, “디지털 컨텐츠의 보호기술에 관한 기술동향 분석”, 한국해양정보통신학회 논문집, pp. 1094-1097, 2005.

[2] A. Menezes, P. Van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997.

[3] G. Ateniese, C. Blundo, and A. Santis, “Extended Schemes for Visual Cryptography," Theoretical Computer Science, Vol. 250, pp. 143-161, 2001.

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

[5] K.W. Wong, “Fast image encryption scheme based on chaotic standard map”, Physics Letters A, Dec 2007.

[6] N.K. Pareek, "Image encryption using chaotic logistic map", Image and Vision Computing, Feb 2006.

[7] 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, Aug 2007.

[8] 박영일, 김석태, “다해상도 특성을 갖는 2D 셀룰러 오토마타변환을 이용한 디지탈 워터마킹”, 한국통신학회 Vol. 34, No. 1, pp. 105-112, 2009.