LFSR과 CAT을 이용한 영상 암호화

남태희* · 김석태1)** · 조성진***

*동주대학 **부경대학교 ***부경대학교

Image Encryption using LFSR and CAT

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 논문에서는 LFSR(Linear Feedback Shift Register)과 2D CAT(Two-Dimensional Cellular Automata Transform)를 이용한 영상 암호화법을 제안한다. 먼저 LFSR을 이용하여 원 영상의 크기만큼 PN(pseudo noise) 수열을 생성한다. 그런 다음, 생성된 수열을 원 영상과 XOR 연산하여 원 영상을 변환한다. 그리고, 게이트웨이 값을 설정하여 2D CAT 기저함수를 생성한다. 생성된 기저함수를 변환된 원 영상에 곱하여 2D CAT 영상 암호화를 한다. 마지막으로, 안정성 분석을 통하여 제안한 방법이 높은 암호화 수준의 성질을 가졌음을 검증한다.

ABSTRACT

In this paper, we propose the image encryption using LFSR(Linear Feedback Shift Register) and 2D CAT(Two-Dimensional Cellular Automata Transform). First, a LFSR is used to create a PN(pseudo noise) sequence, which is identical to the size of the original image. Then, the created sequence goes through a XOR operation with the original image to convert the original image. Next, the gateway value is set to produce a 2D CAT basis function. Using the created basis function, multiplication is done with the converted original image to process 2D CAT image encipherment. Lastly, the stability analysis verifies that the proposed method holds a high encryption quality status.

키워드

CAT(Cellular Automata Transform), PN(pseudo noise) sequences, LFSR(Linear Feedback Shift Register), encryption, Gateway Values

Ⅰ. 서 론

최근 인터넷의 발전으로 인해 다양한 정보들이 폭발적으로 늘어나고 있다. 정보 홍수의 시대라고 할 만큼 매일 같이 최신의 정보들이 업데이트 되고 있다. 특히 인터넷상에서 큰 비중을 차지하는 정보들 중 영상 관련 컨텐츠에 대한 선호도가 매우 높다. 영상 관련 컨텐츠는 누구나 쉽게 내려 받아 자유롭게 활용한다. 이로 인해 개인 및 단체가 제작한 영상물에 대한 저작권에 많은 피해를 주고 있다. 따라서 오늘날 영상 보호는 개인 및 단체의 저작권 문제로서 중요한 화두로 대두되고 있다. 최근 이러한 영상을 보호하는 주요 연구 방향 중 하나로 영상 암호화 방법이 있다[1,2].

영상 암호화 방법에는 Kolmogorov flow map, chaotic standard map, chaotic logistic map 등의 기술을 이용한 영상 암호화 연구가 제시되고 있다[3,4,5].

이들 방법 중 Scharinger는 Kolmogorov flow map을 이용한 영상 암호화 기법을 제안 하였으며[3], Wong은 chaotic standard map을 기반으로 한 영상 암호화 방법을 제안하였다[4]. 제안한 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 최대 주기를 갖는 LFSR(Linear Feedback Shift Register)[6]과 2D CAT(Two-Dimensional Cellular Automata Transform)[7]를 이용한 새로운 영상 암호화 방법을 제안한다. 암호화 방법은 먼저, LFSR을 이용하여 원 영상의 크기만큼 PN(pseudo noise) 수열을 생성한다. 생성된 PN 수열을 이용하여 LFSR 기저 영상을 만든다. 그 후 생성된 LFSR 기저 영상과 원 영상을 XOR 연산하여 LFSR이 적용된 변환 영상을 구한다. 그 다음, 2D CAT의 게이트

**1) 교신저자

웨이 값을 설정하고 이를 이용한 2D 기저함수를 생성한다. 마지막으로, 이미 생성된 LFSR 변환 영상에 2D 기저함수를 곱하여 2D CAT 영상 암호화를 한다. 또한 영상의 복호화 방법은 생성된 2D 기저함수가 직교성질을 갖고 있기 때문에 역 CAT로서 암호화된 영상은 LFSR 변환 영상으로 복원된다. 복원된 LFSR 변환 영상을 LFSR 기저 영상과 XOR 연산하여 무 손실 복원한다. 본 논문에서는 키 공간 및 히스토그램 분석을 통하여 제안한 방법이 높은 암호화 수준의 성질을 가졌음이 실험을 통하여 확인한다.

II. 제안 방법

LFSR은 주기적 스트림 암호화에 이용되는 기법으로 주로 의사 난수를 발생시킨다. 이것은 비트 단위로 암호화하므로 오류 확산 현상이 없고 블록 암호 알고리듬에 비해 빠르고 구현이 쉽다.
본 논문에서 제안된 LFSR 구조는 그림 1과 같다.

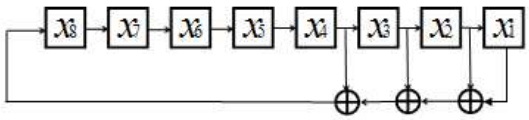

그림 1. Proposed LFSR structure

제안된 방법은 8비트와 귀환회로 XOR 연산자로서 최대 길이 사이클을 보여주며, 8,4,3,2에 탭을 가지고 있다. 이것은 식 (1)과 같이 특성다항식[8]으로 표현된다.

$$x^8+x^4+x^3+x^2+1 \tag{1}$$

CAT는 동역학계를 해석하는 한 방법으로 시간과 공간을 이산적으로 다루는 시스템으로서 복잡한 자연현상을 시뮬레이션 하는데 유용한 도구이다. 그 기본은 1D CA로서, 모든 셀들이 선형으로 배열되어 있는 3-이웃 CA이다.

$$a_{i,t+1}=f[a_{i,t},a_{i+1,t},a_{i-1,t}] \tag{2}$$

식 (2)는 상태전이 함수로서, f는 결합논리를 가지는 국소전이함수이며, 서로 다른 2^3 개 이웃의 배열상태가 있다. CAT는 2D 영상 공간 $n\times n$ 셀일 경우, 기저함수는 $A_k\equiv A_{ijkl},(i,j,k,l=0,1,....,N-1)$이다. 또한 $f_{ij}(i,j=0,1,2,...,N-1)$의 2D CAT는 식(3)과 같다.

$$f_{ij}=\sum_{k=0}^{N-1}\sum_{l=0}^{N-1}c_{kl}Aijkl \quad (i,j=0,1,2,....,N-1) \tag{3}$$

본 논문에서는 영상 암호화를 위해 2D 기저함수를 생성한다. 2D 기저함수는 먼저 2D CA공간 $a\equiv a_{ijt}(i,j,t=0,1,2,...,N-1)$에서 2D 기저함수 A_{ijkl}을 생성한다. 이것은 1D 기저함수 A_{ik}로부터 생성한다. 식 (4)는 2D 기저 함수식이다.

$$A_{ijkl}=A_{ik}A_{jl} \tag{4}$$

2D 기저함수는 표 1을 이용하여 생성한다.

표 1. Gateway Values

Gateway	Values
Wolfram Rule	14
Number of Cells per Neighborhood	3
Number of Cells in Lattice	8
Initial Configuration	01001101
Boundary Configuration	Cyclic
Basis Function Type2	$A_{ik}=2a_{ik}a_{ki}-1$

게이트웨이 값의 조건하에서 갱신되는 셀들의 상태 전이함수식은 (5)와 같다.

$$\begin{aligned}a_{(r)(t+1)}&=\left(\sum_{j=0}^{2^m-2}W_j\alpha_j+W_{2^m-1}\right)^{W_{2^m}}\bmod K\\ a_{(1)(t+1)}&=(W_0a_{0t}+W_1a_{1t}+W_2a_{2t}+W_3a_{0t}a_{1t}+\\ &W_4a_{1t}a_{2t}+W_5a_{2t}a_{0t}+W_6a_{0t}a_{1t}a_{2t}+W_7)^{W_{2^3}}\bmod K\end{aligned} \tag{5}$$

식 (5)에서 $r=1$이고 $t+1$일 경우, 조건은 $0\le W_j\le 2$이다. α_j는 이웃 셀 상태들의 조합으로 이루어진다. 이것은 1D 3-이웃이다. 따라서 m=3으로 $W_{2^3}=W_8$의 값을 가진다. 여기서 셀들의 상태는 시간 $t(t=k)$에서 a_{0k},a_{1k},a_{2k}순으로 정의된다. 2D 기저함수는 1D 기저함수로부터 구할 수 있다. 기저 함수 타입 2를 이용하여 2D CAT 식 (6)을 구한다[9].

$$c_{kl}=\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}f_{ij}A_{ijkl}\ (k,l=0,1,2,...,N-1) \tag{6}$$

식 (6)을 이용하여 영상을 암호화한다. 게이트웨이 값에 의해 생성된 2D 기저함수는 그림 2와 같이 나타내었다.

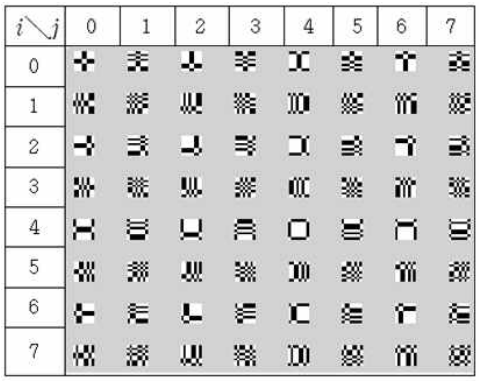

그림 2. 2D basis function

III. 암호화 방법 및 실험 결과

암호화 방법은 최대길이를 갖는 LFSR을 이용하여 원 영상의 크기만큼 PN 수열을 생성한다. 생성된 PN 수열을 이용하여 LFSR 기저 영상을 만든다. 그 후 생성된 LFSR 기저 영상과 원 영상을 XOR 연산하여 LFSR이 적용된 변환 영상을 구한다. 그 다음, 2D CAT의 게이트웨이 값을 설정하고 이를 이용하여 2D 기저함수를 생성한다. 이미 생성된 LFSR 변환 영상에 2D 기저함수를 곱하여 2D CAT 암호화된 영상을 얻는다. 또한 복호화 방법은 생성된 2D 기저함수가 직교 성질을 갖고 있기 때문에 역 CAT로서 암호화된 영상은 LFSR 변환 영상으로 복원되고, 이를 LFSR 기저 영상과 XOR 연산하여 복호화 영상을 얻는다.

실험된 영상은 256X256 크기의 8비트 그레이 레벨 영상을 이용하여 그 변화를 고찰 하였다.

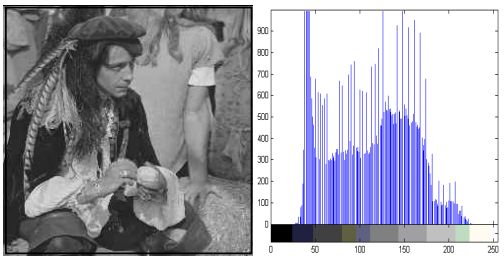

그림 3. Original image “man" and Histogram

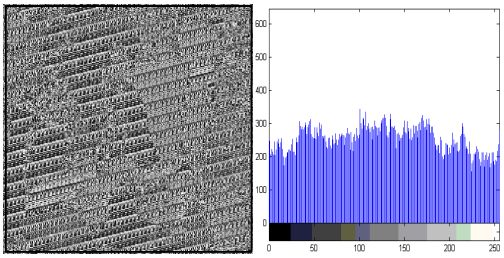

그림 4. Image and Histogram by XOR operation with LFSR and Original image

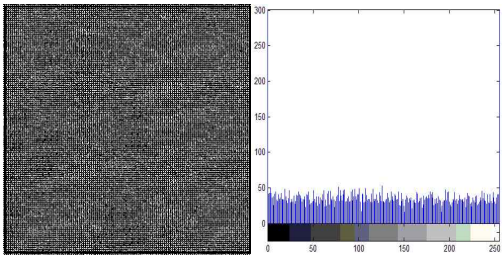

그림 5. Encrypted image and Histogram using LFSR and CAT

LFSR에 의해 생성된 PN 수열과 원 영상을 XOR 연산하여 생성된 LFSR 변환 영상은 그림 4에 보였다. 또한 LFSR 변환 영상에 2D CAT 기저 함수를 곱하여 2D CAT 영상 암호화에 대한 결과는 그림 5에 보였다. 영상 암호화 결과는 원 영상과 비교해서 각 픽셀간의 연관성이 전혀 알 수 없게 고르게 출력됨이 확인되었다.

암호화의 평가 기준은 주요 키 공간 및 히스토그램 분석에 의해 결정된다. 큰 범위의 키 공간은 영상의 암호화 수준을 높인다.

본 논문에서 2D CAT 이용에 대한 제안 방법은 8-셀, 2-상태, 5-이웃을 적용하였다. 이런 경우, K-상태는 K^{k^5} (5-이웃으로서 m=5) 규칙으로 발전된다. $M=T=N=8$일 때 5(m=5)개 셀의 폰 노이만(Von Neumann) 이웃과 2D CA가 발전하는 방법으로 $N_T^2 = K^{k^m+3(N+M)+2T} = 2^{96}(2^{2^5+3(8+8)+2\times 8})$ 가지의 키를 생성한다. 이것은 일반 CA 키를 이용한 영상 암호화 수준보다 훨씬 향상된 결과이다. 따라서 제안된 방법은 총 2^{96}가지의 일정한 키를 생성할 수 있기 때문에 충분히 암호화 수준을 확보할 수 있다.

IV. 결 론

본 논문에서는 원 영상을 암호화하기 위해 최대길이를 갖는 LFSR과 2D CAT를 적용하였다. 암호화 방법에서 LFSR 적용은 효과적인 난수 발생으로 영상 변환에 매우 유용하다. 또한 CAT는 시간과 공간을 이산적으로 다루는 시스템으로서 매우 랜덤성이 강한 성질을 가지고 있다. 이러한 두 단계를 거쳐 효과적으로 영상 암호화를 수행하였다. 또한 키 공간과 히스토그램 분석에 의해 암호화 결과를 평가하였다. 그 결과, 본 논문에 제안된 방법이 영상의 암호화 수준이 높음을 확인하였고, 또한 외부 공격에 대해 강인한 특성을 가졌음이 확인되었다.

참고 문헌

[1] 박진, 나철훈, “디지털 컨텐츠의 보호기술에 관한 기술동향 분석”, 한국해양정보통신학회 논문집, pp. 1094-1097, 2005.
[2] 송학현, 김윤호, 류광렬, “영상 콘텐츠 지적재산권 보호 워터마킹 기술”, 한국해양정보통신학회논문집, pp.144-148, 2004.
[3] J. Scharinger, “Fast encryption of image data using chaotic Kolmogorov Flows”, J. Electron Image, Vol. 2, No. 2, pp. 318-325, 1998.
[4] K.W. Wong, “Fast image encryption scheme based on chaotic standard map”, Physics Letters A, Dec 2007.
[5] N.K. Pareek, "Image encryption using chaotic logistic map", Image and Vision Computing, Feb 2006.
[6] H.Y. Song, "Feedback Shift Register Sequences", Encyclopedia of telecommunications, edited by G. J. Proakis, John Wiley & Sons, New York, Dec 2002.
[7] O. Lafe, “Cellular Automata Transforms: Theory and Application in Multimedia Compression, Encryption, and Modeling”, Kluwer Academic Publishers, Boston/Dordrecht/London, 2000.
[8] 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.
[9] 박영일, 김석태, “다해상도 특성을 갖는 2D 셀룰러 오토마타변환을 이용한 디지탈 워터마킹”, 한국통신학회 Vol. 34, No. 1, pp. 105-112, 2009.