PLCM을 이용한 카오스 블록 암호화 기법

Chaotic Block Encryption Scheme using a PLCM

이민구, 이성우, 신재호 · 동국대학교 전자공학과
Min-Goo Lee, Sung-Woo Lee, Jaeho Shin · Dept. of Electronics Engineering., Dongguk University

Abstract

In this paper, we propose 128bits chaotic bloc k encryption scheme using a PLCM(Piece-wise Li near Chaotic Map) having a good dynamical pro perty. The proposed scheme has a block size of 128 bits and a key size of 128 bits. In proposed scheme we use four 32bits sub-keys of session ke y and four 32bit sub-blocks of block to decide th e initial value and the number of iteration of PL CM. The encrypted code is generated from the o utput of PLCM.

With results of test and analyses of security we show the proposed scheme is very secure aga inst statistical attacks and have very good Avalan che Effect and Randomness properties.

Keywords

Chaos, Chaotic Maps, PLCM, Chaotic-Block Encryption

I. 서 론

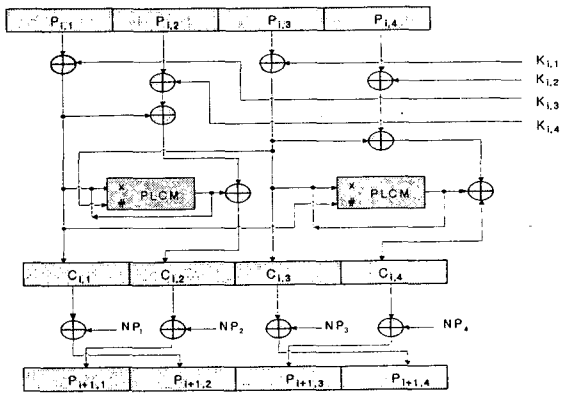
복잡계(Complex) 비선형 동역학 분야로서 카오스(Chaos)이론은 많은 과학과 기술영역에서 오래전부터 폭 넓게 연구되어 왔다. 카오스는 나비효과(Butterfly Effect)라고 알려진 초기조건에 민감한 특성과 혼합(Mixing)특성으로 인해 암호분야와도 밀접한 관계를 가지며 연구되어 왔다. 카오스의 대표적인 특성인 초기조건에 민감성은 매우 근접한 초기상태에서 출발한 두 개의 궤도(Trajectory)가 시간이 지남에 따라 매우 빠르게 갈라지는 것을 의미한다. 또한 다른 카오스의 특징인 혼합(Mixing) 특성은 상태 공간의 아주 작은 일부분이 전 상태 공간으로 빠르게 뿔뿔이 흩어져가는 특성을 말한다. 위의 두 가지 카오스의 대표적인 특성은 일반 암호에서 요구하는 혼동(Confusion)과 확산(Diffusion)특성과 깊은 관계를 가지고 있다. 여기서 혼동특성이란 암호문과 평문간의 통계적인(Statistical)특성을 아주 복잡하게 하여 암호문과 평문 또는 키와의 관계를 알 수 없도록 하는 특성을 말하는데 이는 카오스의 첫 번째 특성인 초기조건의 민감성과 관계가 있다. 그리고 확산 특성은 평문의 하나의 비트가 암호문의 많은 비트에 영향을 주는 특성을 말하는데 이는 카오스의 혼합특성 및 초기조건의 민감성에 깊은 연관성이 있다. 이러한 카오스와 암호와의 밀접한 관계로 새로운 암호 알고리즘과 시스템 개발에 카오스를 이용한 연구가 많이 진행되고 있다.

본 논문에서는 카오스 특성이 뛰어난 PLCM(Piecewise Linear Chaotic Map)을 이용한 128비트 길이의 키와 128비트 길이의 데이터 블록을 갖는 카오스 블록 암호화 기법을 제안한다.

본 논문에서 제안한 기법은 128비트의 키를 PLCM을 이용해서 4개의 32비트 서브키를 가진 128비트 세션 키(Session Key)를 생성하는 키 생성부분

과 키 생성 알고리즘에서 생성된 4개의 32비트 서브 키와 128비트 평문 블록을 4개로 나눈 32비트 서브 블록들과 XOR(Exclusive-OR)된 값을 카오스 사상(Map)인 PLCM의 초기 값과 반복 회수로 사용해서 암호문을 생성하는 암/복호화 부분으로 크게 구성되어 있다. 그리고 생성된 128비트 암호문은 다음 평문 블록 128비트와 XOR(Exclusive-OR)되어져 다음 암호화과정의 입력으로 사용된다.

본 논문의 2장에서는 카오스의 특성과 본 제안 암호기법에 사용된 PLCM에 대해 기술하고 3장에서는 본 제안 카오스 암호기법의 구조와 암/복호화 과정 그리고 세션 키 생성과정에 대해 기술한다.



[그림 1] 제안 기법의 전체 구조
[Fig. 1] The whole structure of proposed technique

본 논문의 4장에서는 실험 영상을 가지고 본 제안 기법의 암호화 결과와 여러 가지 안전성에 관련된 시뮬레이션 결과를 보여주고 또한 여러 가지 통계적 분석과 Avalanche Effect 그리고 Randomness 분석을 현재 잘 알려진 대칭키 암호인 DES, AES 그리고 SEED등과 비교하여 본 제안 기법의 안전성에 대해 살펴보고 마지막 5장에서 결론을 맺는다.

II. 카오스 암호 개요

이 장에서는 비선형 동력학 시스템으로서의 카오스의 특성에 대해서 간략하게 설명하고 본 제안 기법에 사용되는 PLCM에 대해서 기술한다.

2.1 카오스 특성

식(1)과 같이 표현되는 1차원 동력학 시스템이 아래와 같은 조건을 만족하면 카오스 특성을 가지고 있다고 한다.[1]

$$x_{k+1} = f(x_k),\ f: I \to I,\ x_0 \in I \qquad (1)$$

여기서, f는 연속적인(Continuous) 사상이며, $I = [0,1]$ 이다.

① 초기조건에 대한 민감성(Sensitivity)

$$|x_0 - y_0| < \varepsilon \Rightarrow |f^n(x_0) - f^n(y_0)| > \delta,$$
$$\exists \delta > 0, \forall x_0 \in I, \varepsilon > 0, \exists n \in N, y_0 \in I$$

② 위상 이행성(Topological transitivity)

$$f^n(x_0) \in I_2,\ \forall I_1,\ I_2 \subset I, \exists x_0 \in I_1, n \in N$$

③ 주기점이 집합I에 밀집(Density)

$$p = \{p \in I | \exists n \in N: f^n(p) = p\},\ \bar{p} = I$$

위의 카오스 특성은 좋은 암호시스템이 지녀야 하는 조건인, '평문이나 키에 대해 민감성 그리고 평문과 암호문 사이에 어떤 패턴도 존재하지 않아야 한다.'는 조건과 일치한다.

2.2 PLCM(Piecewise Linear Chaotic Map)

본 제안 기법에 사용되는 PLCM은 [2]에서 소개되었고 식(2)과 같다.

$$F(x,q) = \begin{cases} x/q, & 0 \le x \le q \\ (x-q)/(\frac{1}{2}-q), & q \le x \le \frac{1}{2} \\ F(1-x,q), & \frac{1}{2} \le x \le 1 \end{cases} \qquad (2)$$

여기서 q는 $0 < q < \frac{1}{2}$.

식(2)에서 보는 것처럼, PLCM은 가장 간단한 카오스 사상 중에 하나이며 다음과 같은 매우 완벽한 동력학적 특성을 가지고 있다.[3]

① 에르고딕성(Ergodic), 혼합성(Mixing).

② 균일한 불변밀도함수(invariant density function).

③ δ-like한 자기상관성(auto-correlation).

이와 같이, PLCM이 균일한(Uniform) 불변밀도와 좋은 상관성을 가지고 있기 때문에, 카오스 암호기법을 설계할 때 많이 사용되고 있다.

III. 제안한 카오스 블록 암호화 기법

본 논문에서 제안한 블록 암호화 기법은 동력학적 특성이 좋은 PLCM을 사용하고 128비트 길이의 암호 키와 128비트 길이의 데이터 블록을 사용하는 대칭키 암호기법이다.

3.1 제안 기법의 암/복호화 과정

본 제안 암호기법의 전체 구조는 그림 1과 같다. 본 제안 기법은 128비트의 평문 블록(P)이 4개의 32비트 서브 블록(P_1, P_2, P_3, P_4)으로 나누어져서 암호화된다. 암호화 될 입력 평문의 처음 128비트 평문은 4개의 초기 상수(IC1, IC2, IC3, IC4)와 XOR 된 후 암호화 과정을 거친다. 그 다음에 암호화 될 128비트 입력 평문(NP)는 그 전단계의 암호문과 XOR(Exclusive-OR)되어 암호화 과정을 수행된다.

본 제안 암호기법에 사용된 4개의 초기 상수는 아래와 같다.

IC1 = 0x3c6ef373

IC2 = 0x9e3779b9

IC3 = 0xde6e678d

IC4 = 0x78dde6eb

4개의 32비트 평문 블록($P_{i,1}, P_{i,2}, P_{i,3}, P_{i,4}$)은 키 생성 알고리즘에서 생성된 4개의 32비트 서브 키 ($K_{i,1} K_{i,2}, K_{i,3}, K_{i,4}$)와 XOR된 후 PLCM의 초기 값과 반복 회수로 사용된다. PLCM의 출력은 두 번째와 네 번째 평문 블록과 XOR되어져 암호문의 두 번째와 네 번째 블록을 생성한다. 암호화 과정은 아래와 같다.

① 입력 평문 128비트 블록은 4개의 32비트 평문 블록($P_{i,1}, P_{i,2}, P_{i,3}, P_{i,4}$, $i = 0,1,2,\cdots$)는 나누어진다. 입력 평문블록이 평문의 처음 블록($i = 0$)이면 초기 상수(IC)와 XOR되고 처음 블록이 아니면 그 전의 암호문 블록과 XOR 된다.

$$PP_{0,1} = P_{0,1} \oplus IC1,$$

$$PP_{0,2} = P_{0,2} \oplus IC2,$$

$$PP_{0,3} = P_{0,3} \oplus IC3,$$

$$PP_{0,4} = P_{0,4} \oplus IC4$$

$$PP_{i,1} = P_{i,1} \oplus C_{i-1,2}, \quad (i = 1,2,3,\cdots)$$

$$PP_{i,2} = P_{i,2} \oplus C_{i-1,1}, \quad (i = 1,2,3,\cdots)$$

$$PP_{i,3} = P_{i,3} \oplus C_{i-1,4}, \quad (i = 1,2,3,\cdots)$$

$$PP_{i,4} = P_{i,4} \oplus C_{i-1,3}, \quad (i = 1,2,3,\cdots)$$

첫 번째 32비트 평문 블록은 그 전단계의 암호문의 두 번째 블록과 두 번째 평문 블록은 암호문의 첫 번째 블록과 XOR되며, 세 번째 평문 블록과 네 번째 평문 블록은 각각 전 단계 암호문의 네 번째와 세 번째 블록과 XOR된다.

② 4개의 32비트 평문 블록은 먼저 4개의 32비트의 서브키($K_{i,1}, K_{i,2}, K_{i,3}, K_{i,4}$)와 XOR된다.

$$TP_{i,1} = PP_{i,1} \oplus K_{i,3}, \quad (i = 0,1,2,\cdots)$$
$$TP_{i,2} = PP_{i,2} \oplus K_{i,4}, \quad (i = 0,1,2,\cdots)$$
$$TP_{i,3} = PP_{i,3} \oplus K_{i,1}, \quad (i = 0,1,2,\cdots)$$
$$TP_{i,4} = PP_{i,4} \oplus K_{i,2}, \quad (i = 0,1,2,\cdots)$$

그리고 두 번째와 네 번째 32비트 입력 블록은 다시 서브키와 XOR된 첫 번째와 세 번째 블록과 XOR된다.

$$XP_{i,2} = TP_{i,2} \oplus TP_{i,1}, \quad (i = 0,1,2,\cdots)$$
$$XP_{i,4} = TP_{i,4} \oplus TP_{i,3}, \quad (i = 0,1,2,\cdots)$$

$TP_{i,1}$과 $TP_{i,3}$ 각각 두 개의 PLCM의 초기 값과 반복 회수로 사용된다.

첫 번째 PLCM의 초기 값(x_1)은 $TP_{i,1}$이 사용되고 첫 번째 PLCM의 반복회수($\#_1$)는 $TP_{i,3}$이 사용된다. 두 번째 PLCM의 초기 값(x_2)은 $TP_{i,3}$이 사용되고 두 번째 PLCM의 반복 회수($\#_2$)는 $TP_{i,1}$이 사용된다.

$$x_1 = P_{i,1} \pmod 1, \quad 0 < x_1 < 1$$
$$\#_1 = P_{i,3} \pmod{255}$$
$$x_2 = P_{i,3} \pmod 1, \quad 0 < x_2 < 1$$
$$\#_2 = P_{i,1} \pmod{255}$$

③ 4개의 32비트 암호문 블록($C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4}$)을 생성한다.

첫 번째 32비트 암호문 블록($C_{i,1}$)은 $TP_{i,1}$이 되고 두 번째 암호문 블록($C_{i,2}$)은 $XP_{i,2}$와 첫 번째 PLCM의 출력($Y_{i,1}$)과 XOR된 값으로 생성된다. 세 번째 암호문 블록($C_{i,3}$)은 $TP_{i,3}$이 되고 네 번째 암호문 블록($C_{i,4}$)은 $XP_{i,4}$와 두 번째 PLCM에서 얻어진 결과($Y_{i,2}$)를 XOR해서 생성한다.

$$C_{i,1} = TP_{i,1}$$
$$C_{i,2} = XP_{i,2} \oplus Y_{i,1}$$
$$C_{i,3} = TP_{i,3}$$
$$C_{i,4} = XP_{i,4} \oplus Y_{i,2}$$

128비트 입력 평문에 대한 128비트 암호문(C_i)은 4개의 32비트 암호문 블록을 결합해서 생성된다.

$$C_i = C_{i,1} \| C_{i,2} \| C_{i,3} \| C_{i,4}$$

복호화과정은 암호화과정의 역순으로 수행하면 평문을 얻을 수 있다.

3.2 서브키 생성 과정

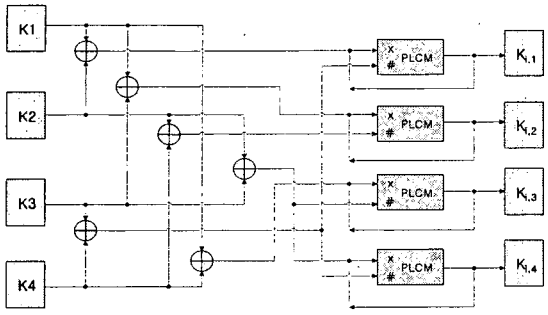
128비트 키에서 암호화에 사용될 4개의 32비트 서브 키($K_{i,1}, K_{i,2}, K_{i,3}, K_{i,4}$)를 생성하는 과정은 그림2와 같다.

128비트 비밀 키는 32비트씩 4개($K1, K2, K3, K4$)로 나눈 후 서브키를 생성한다. 서브 키 생성과정에는 4개의 PLCM(PLCM1, PLCM2, PLCM3, PLCM4)이 사용되며 각 PLCM에서 나온 출력 값이 서브키로서 사용된다.

서브키를 생성하는 과정은 아래와 같다.

① PLCM1에 사용되는 초기 값(x_1)은 $K1$과 $K2$을 XOR 값이 사용되며 반복회수($\#_1$)는 $K3$과 $K4$을 XOR값이 사용되며 PLCM1의 출력 값이 첫 번째 32비트 서브키($K_{i,1}$)가 된다.

$$x_1 = K1 \oplus K2, \quad 0 < x_1 < 1$$
$$\#_1 = K3 \oplus K4 \pmod{255}$$
$$K_{i,1} = \text{PLCM1}(x_1, \#_1), \quad i = 0,1,2,\cdots$$



[그림 2] 서브키 생성 과정
[Fig. 2] Sub-key generation processing

② PLCM2에 사용되는 초기 값(x_2)은 $K1$과 $K3$을 XOR값이 사용되며 반복회수($\#_2$)는 $K2$과 $K4$을 XOR 값이 사용되며 PLCM2의 출력 값이 두 번째 32비트 서브키($K_{i,2}$)가 된다.

$x_2 = K1 \oplus K3 \ , \ 0 < x_2 < 1$

$\#_2 = K2 \oplus K4 \ (\mathrm{mod}\ 255)$

$K_{i,2} = \mathrm{PLCM2}(x_2, \#_2), \ i = 0,1,2,\cdots$

③ PLCM3에 사용되는 초기 값(x_3)은 $K1$과 $K4$을 XOR값이 사용되며 반복회수($\#_3$)는 $K2$과 $K3$을 XOR 값이 사용되며 PLCM3의 출력 값이 세 번째 32비트 서브키($K_{i,3}$)가 된다.

$x_3 = K1 \oplus K4 \ , \ 0 < x_3 < 1$

$\#_3 = K2 \oplus K3 \ (\mathrm{mod}\ 255)$

$K_{i,3} = \mathrm{PLCM3}(x_3, \#_3), \ i = 0,1,2,\cdots$

④ PLCM4에 사용되는 초기 값(x_4)은 $K2$과 $K3$을 XOR값이 사용되며 반복회수($\#_4$)는 $K3$과 $K4$을 XOR 값이 사용되며 PLCM4의 출력 값이 네 번째 32비트 서브키($K_{i,4}$)가 된다.

$x_4 = K2 \oplus K3 \ , \ 0 < x_4 < 1$

$\#_4 = K3 \oplus K4 \ (\mathrm{mod}\ 255)$

$K_{i,4} = \mathrm{PLCM4}(x_4, \#_4), \ i = 0,1,2,\cdots$

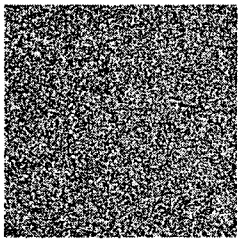
⑤ 생성된 4개의 서브키($K_{i,1}, K_{i,2}, K_{i,3}, K_{i,4}$)는 다음 (Next) 평문 블록 암호화에 사용될 다음 서브키 ($K_{i+1,1}, K_{i+1,2}, K_{i+1,3}, K_{i+1,4}$)생성에 사용된다.

IV. 실험 및 안전성 분석

4.1 시뮬레이션 결과 고찰

본 제안 암호기법의 실험 데이터로 [그림 3]의 Lena 256x256 크기의 256그레이(Gray)레벨 영상을 사용하였다.

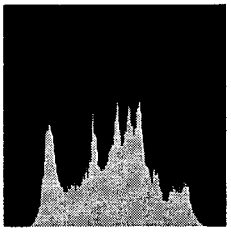
[그림 3] Lena 원 영상
[Fig. 3] Lena origin-al image



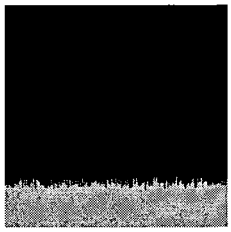
[그림 4] 암호화 된 Len a 영상
[Fig. 4] The Encrypte d Lena image

실험에 사용된 암호 키(K)는 128비트의 "#helloChaosblock"을 사용하였고 PLCM에 사용되는 q파라미터는 0.3597815497로 설정하였다.

[그림 4]는 본 제안기법으로 Lena 영상을 암호화한 영상이다. [그림 4]에서 보는 것처럼 암호화된 영상은 거의 아무 형태도 보이지 않는 매우 Random 한 영상으로 보인다.



[그림 5] Lena 영상의 히스토그램
[Fig. 5] Histogram of the Lena image



[그림 6] 암호화 된 Le na 영상의 히스토그램
[Fig. 6] Histogram of the Encrypted Le na image

[그림 5]은 Lena 원 영상의 히스토그램을 보여주고 있다. [그림 6]은 제안 기법으로 암호화 된 영상의 히스토그램이다. [그림 6]에서 보는 것처럼 암호화 된 영상이 모두 균일한 히스토그램을 보여주고 있는데 이는 통계적 공격에 매우 저항성을 가지고 있음을 보여주고 있다.

4.2 안전성 분석

이 절에서는 암호 키에 대한 분석, 통계적(Statistical) 분석, Avalanche Effect 분석 그리고 Randomness 분석을 여러 다른 기존의 암호 기법과 비교를 통해 본 시스템에 대한 안전성을 분석한다.

4.2.1 암호 키에 대한 분석

암호 기법은 기본적으로 암호 키에 매우 민감해야 하고 암호 키의 수가 전사공격(Brute force attack)에 대응할 수 있도록 커야 한다. 본 제안 기법에 사용된 PLCM은 거의 완벽한 동력학 특성을 가지고 있기 때문에 암호 키에 매우 민감하고 또한 본 제안 기법에 사용되는 키의 길이가 128비트이기 때문에 전사공격에 충분히 대응할 수 있는 키 공간을 가지고 있다.

4.2.2 통계적(Statistical) 분석

본 제안 기법의 통계적 분석은 암호화 된 영상의 히스토그램과 암호화 된 영상의 인접한 픽셀간의 상관관계를 통해 분석한다. 통계적 공격에 저항성을 갖기 위해서는, 좋은 혼동(Confusion)과 좋은 확산(Diffusion)을 보여줌으로써 평문과 암호문 사이에 어떠한 통계적 특성을 찾을 수 없도록 해야 한다.

본 제안 기법은 암호화 된 영상의 히스토그램은 4.1의 실험 결과에서 보는 것처럼 매우 균일한 히스토그램을 가지고 있다. 히스토그램이 균일하다는 것은 통계적 특성을 찾기가 매우 어려운 좋은 혼동특성을 가지고 있음을 보여주는 것이다.

통계적 특성을 정량적으로 분석하는 방식으로 암호화 된 영상에서 인접한 픽셀간의 상관관계를 분석하는 방법이 있다.

상관관계(Correlation)의 상관계수는 식 (3)과 같은 방식으로 구한다.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad (3)$$

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

여기서, x,y는 영상에서 두 개의 인접한 픽셀의 그레이 값이다.

[표 1]은 Lena 영상을 DES, SEED, AES와 본 제안 기법으로 암호화 한 영상에서 임의로 수직 방향, 수평 방향 그리고 대각선 방향으로 각 1000개씩 인접한 두 개의 픽셀을 선택한 후 식(3)으로 계산한 평균 상관 계수 값을 보여주고 있다.

표 1. Lena 영상의 상관계수 분석 결과.
Table 1. Correlation coefficient of Lena image.

	Lena	DES	SEED	AES	제안 기법
수평	0.9695	0.0084	-0.0171	-0.0274	0.0272
수직	0.9479	0.0276	0.0034	0.0174	0.0607
대각선	0.9240	-0.0482	0.3311	0.0205	0.0211

[표 1]에서 보는 바와 같이 제안 기법으로 암호화 된 영상의 상관계수 값은 DES, SEED 그리고 AES로

암호화 된 영상의 상관계수 값과 비슷한 결과를 보여주고 있다. 이는 본 제안 기법으로 암호화 된 영상에서 인접한 픽셀간의 상관관계는 거의 없음을 보여주는 것이다.

4.2.3 Avalanche Effect 분석

Avalanche Effect는 평문의 한 비트가 바뀌면 암호문의 변하는 비트 수가 1/2이어야 한다는 개념이다.

(a) (b) (c)

[그림 7] Avalanche Effect 실험 데이터 영상
[Fig. 7] Avalanche Effect Simulation data image
(a) 모든 비트 값이 0인 영상
(b) 처음 한 비트 값만 1인 영상
(c) 두 번째 비트 값만 1인 영상

Avalanche Effect 분석의 실험 데이터로 모든 비트 값인 0인 256x256 영상[그림 7.(a)]과 첫 번째 비트만 1인 영상[그림 7.(b)] 그리고 두 번째 비트 값만 1인 영상[그림 7.(c)]을 기존의 DES, SEED, AES 그리고 본 제안 기법으로 암호화 한 영상들을 사용하였다. Avalanche Effect 분석도 다른 분석과 마찬가지고 기존의 암호 기법의 결과와 비교 분석했다.

Avalanche Effect 분석은 표준 정규 분포로 유의수준 0.3%로 검정을 해서 전체 비트 수(524288 bits)에서 변하는 비트수가 261376과 262912 사이에 있으면 Avalanche Effect를 만족한다고 한다.

[표 2]는 [그림 7.(a)]를 암호화 한 영상과 [그림 7.(b)]를 암호화 한 영상에 대한 Avalanche Effect 결과를 보여준다.

표 2. Avalanche Effect test1 분석 결과.
Table 2. Avalanche Effect test1 analysis result.

	바뀐 비트 수	결 과
DES	261595	통 과
AES	261890	통 과
SEED	262075	통 과
제안 기법	262009	통 과

표 3. Avalanche Effect test2 분석 결과.
Table 3. Avalanche Effect test2 analysis result.

	바뀐 비트 수	결 과
DES	261595	통 과
AES	261735	통 과
SEED	261790	통 과
제안 기법	261855	통 과

[표 3]은 [그림 7.(a)]를 암호화 한 영상과 [그림 7.(c)]를 암호화 한 영상에 대한 Avalanche Effect 결과를 보여준다.

[표 2]와 [표 3]의 결과에서 보는 바와 같이 본 제안 기법도 기존의 다른 암호 기법과 마찬가지로 Avalanche Effect를 만족함을 보여주고 있다.

4.2.4 Randomness 분석

일반적으로 블록 암호기법의 Randomness 테스트 방법으로 랜덤(Random)하지 않는 비트 스트림을 알고리즘에 평문으로 입력할 경우, 만일 평문과 암호문이 독립성을 가지고 있다면, 암호문은 랜덤한 비트 스트림일 될 것이다. 따라서 이 암호문에 대해 Randomness 통계 특성을 수행하는 방법을 취한다. 본 논문에서는 Randomness 분석의 입력으로 비교 테스트 대상 암호 기법으로 암호화 된 Lena 영상을 사용했다.

Randomness 평가는 유의 수준 1%로 해서 산출된 유의 확률(P-value)을 통해 Randomness를 검증했다.

유의 확률(P-value)이란 가설이 맞다고 가정하는 경우에 가설을 검증하기 위해 사용되는 검정통계량의 값이 표본에서 나올 확률로서 유의 확률 값이 작으면 작을수록 주어진 가설 하에서 나오기 어렵다는 의미를 지니고 있다. 가설 검증에서는 이를 주어진 유의 수준과 비교하여 검정하는데, 유의 확률이 유의 수준보다 작으면 가설을 기각하게 된다. 즉, 유의 확률이 유의 수준(유의 확률 > 유의 수준)보다 크면 귀무가설을 채택하는 것이고 유의 확률이 유의 수준(유의 확률 < 유의 수준)보다 작으면 귀무가설을 기각하게 된다.

표 6. Serial Test 결과.
Table 6. Serial Test result.

암호화 된 Lena 영상		
	유의확률	결과
DES	0.219831	통과
AES	0.920116	통과
SEED	0.623865	통과
제안 기법	0.292539	통과

표 5. Frequency Test 결과.
Table 5. Frequency Test result.

암호화 된 Lena 영상		
	유의확률	결과
DES	0.424721	통과
AES	0.709232	통과
SEED	0.861854	통과
제안 기법	0.339224	통과

본 Randomness 테스트 방법으로 잘 알려진 Frequency 테스트, Serial 테스트 그리고 Runs 테스트 방법을 사용했다.

표 7. Runs Test 결과.
Table 7. Runs Test result.

암호화 된 Lena 영상		
	유의확률	결과
DES	0.122124	통과
AES	0.868220	통과
SEED	0.339203	통과
제안 기법	0.213417	통과

위의 결과에선 보는 것처럼 본 제안 기법은 다른 암호 기법과 마찬가지로 여러 가지 Randomness 테스트에 좋은 결과로 통과된 것을 알 수 있다.

V. 결 론

본 논문에서는 동력학적 특성이 좋은 카오스 사상인 PLCM을 이용해서 128비트 길이의 카오스 블록 암호화 기법을 제안했다.

본 논문에서 제안한 기법은 4장의 실험 및 안전성 분석에서 살펴본 것처럼 통계적 공격에 매우 강하고 Avalanche Effect나 Randomness 특성을 모두 만족하고 있다. 또한 본 제안 기법은 매우 간단한 구조를 가지고 있는 PLCM을 사용하기 때문에 소프트웨어나 하드웨어로 구현이 쉽다는 장점이 있다. 또한 기존의 암호기법은 고정된 라운드 회수를 가지고 있는 반면에 본 논문에서 제시한 암호기법은 키와 평문 블록의 값에 의해 PLCM의 반복회수가 정해지는 키와 평문에 의존적인 암호기법이다. 그렇기 때문에 기존의 방법에 비해 속도가 늦다는 문제점을 가지고 있어서 향후 병렬처리 기법을 도입하거나 다른 방법을 통해 속도를 향상시켜야 하는 과제를 가지고 있다.

본 논문의 서론에서 기술한 것처럼 카오스 이론과 암호와는 매우 밀접한 관련성을 가지고 있기 때문에, 새로운 카오스 암호기법의 개발뿐만 아니라 기존의 암호 시스템의 안전성을 향상시키거나 기존의 암호시스템의 암호 응용 범위를 넓히는데 사용될 수 있도록 더욱 카오스 암호 이론에 대한 연구를 진척시켜야 할 것이다.

[참 고 문 헌]

[1] R. Devaney, An Introduction to Chao-tic Dynamical Systems, Addison-Wesley Publ

ishing Company, Inc, 1989.

[2] H. Zhou, and X. Ling, "*Problems with the chaotic inverse system encryption approac-h,*" I EEE transaction of Circuits and syste-ms, vol. 44, no. 3, pp. 268-271, 1997.

[3] R. Tenny, L. Tsimring, L. Larson, and H. Abarbanel, "*Using Distributed Nonlinear Dy namics for Public Key Encryption,*" Physi-cal Review Letters, vol. 90, no. 4, 2003.

[4] G. Tang, S. Wang, H. Lu and G. Hu, "Ch aos-based cryptograph incorporated with S-box algebraic operation," Physics Letters A, pp. 388-398, 2003.

요 약

본 논문에서는 동력학적 특성이 좋은 PLCM(Piecewise Linear Chaotic Map)을 이용한 128비트의 키와 128비트 평문 블록의 카오스 블록 암호화 기법을 제안한다. 본 논문에서 제안한 기법은 128비트의 키를 PLCM을 이용해서 4개의 32비트 서브키로 이루어진 세션 키 생성하는 키 생성과정과 128비트 평문을 4개로 나눈 32비트 서브 블록들과 4개의 서브키와의 XOR(Exclusive-OR)된 값을 PLCM의 초기 값과 반복회수로 사용해서 암호문을 생성하는 암/복호화 과정으로 이루어져 있다.

본 논문에서는 제안한 기법이 실험 결과와 안전성 분석을 통해 여러 가지 통계적 공격에 매우 강하고 Avalanche Effect와 Randomness 특성이 매우 좋음을 보여준다.