情報保護學會論文誌
第14券 第4號, 2004. 8

다중 카오스 사상을 이용한 영상 암호시스템 설계

이 성 우†, 신 재 호‡
동국대학교

Design of image encryption system using multiple chaotic maps

Sung-Woo Lee†, Jaeho Shin‡
Dongguk University

요 약

인터넷 이용의 폭발적인 증가와 유무선 통신기술의 발달로 인해 디지털 영상의 교환이 매우 빈번하게 일어나고 있는 현실에서 개인 사생활과 기업 및 기관의 기밀에 관련된 영상에 대한 보안이 매우 중요시 되어가고 있다. 또한 최근 카오스 이론과 암호와의 밀접한 관련성으로 인해 카오스 사상(Map)에 기반 한 새로운 암호기술 개발에 많은 연구가 진행되고 있다. 본 논문에서는 1차원 카오스 사상(Map)인 PLCM(Piecewise Linear Chaotic Map)과 2차원 카오스 사상인 Baker 사상을 이용한 정지영상 암호 시스템을 제안한다. 본 제안 시스템은 1차원 PLCM을 기반으로 한 섭동(Perturbance)기반 카오스 스트림(Stream)암호 기법과 2차원 Baker 사상을 기반으로 한 카오스 블록(Block)암호 기법이 결합된 구조로서 좋은 혼동(Confusion)특성과 확산(Diffusion)특성을 지닌 매우 안전하고 구현이 쉬운 암호시스템이다. 또한 본 논문에서는 실험 결과를 통해 통계적(Statistical) 공격에도 매우 강함을 보여주었다.

ABSTRACT

The proliferation of the Internet and the rapid progress of wire/wireless communication technology makes security of digital images more and more important since the exchanges of digital images occur more and more frequently. And as the tight relationship between chaos theory and cryptography, many researches for development of new encryption systems based on chaotic maps have been widely progressed recently. In this paper, we propose a digital image encryption system based on both one-dimensional PLCM(Piecewise Linear Chaotic Map) and two-dimensional baker map. This proposed system is a product cipher that contains a perturbance-based chaotic stream cipher based on 1D PLCM and a chaotic block cipher based on 2D baker map and is very high secure and easily implementable cipher having both a good confusion property and a good diffusion property. And with test results, we showed this system is very secure against statistical attacks.

Keywords : *Chaos, Chaotic image encryption, Chaotic maps, PLCM, Baker map*

Ⅰ. 서 론

복잡계(Complex) 비선형 동력학 분야로서 카오스(Chaos)이론은 많은 과학영역에서 오래전부터 폭넓게 연구되어 왔고 나비효과라고 알려진 초기조건에 민감한 특성과 혼합(Mixing) 특성으로 인해 암호(Cryptography)분야와도 밀접한 관계를 가지며 연구되어 왔다. 카오스의 대표적인 특성인 초기조건에 민감성(Sensitivity)은 매우 근접한 초기상태에서 출발한 두 개의 궤도(Trajectories)가 시간이 지남에 따라 매우 빠르게 갈라지는 것을 의미한다.

접수일 : 2004년 6월 2일 ; 채택일 : 2004년 8월 5일
† 주저자 : niceisw@dgu.ac.kr
‡ 교신저자 : jhshin@dgu.ac.kr

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 혼동(Confusion) 특성이란 암호문과 평문간의 통계적인(Statistical) 특성을 아주 복잡하게 해서 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 시스템 개발에 카오스를 이용한 연구가 많이 진행되고 있다.[1,2][4-13] 또한 이러한 카오스 특성으로 인해 특히 높은 안전성과 빠른 처리를 요구하는 영상 암호에 효과적인 방법으로 카오스 암호가 새롭게 제안되고 있다.[1,5,8] 또한 최근에는 카오스 사상(Maps)을 이용한 카오스 암호에 대한 연구에 특히 많은 관심이 두고 있다. 카오스 암호에는 주로 비밀 통신(Communication)을 위해 하드웨어 기반의 동기화 기법을 이용한 아날로그(Analog) 카오스 암호와 동기화 기법에 기반을 두지 않고 컴퓨터에서 실현될 수 있는 소프트웨어 기반의 데이터 암호로 이산(Discrete) 또는 디지털(Digital) 카오스 암호로 나누어 질 수 있는데 아날로그 카오스 암호는 여러 가지 보안 취약점 때문에 안전하지 않은 것으로 알려져 있다.[2]

본 논문에서는 다루는 카오스 암호는 이산 또는 디지털 카오스 암호에 대해서만 다룬다. 최근 인터넷 이용의 폭발적인 증가와 디지털 기술의 발달로 인터넷 상에서의 디지털 영상에 대한 교환이 빈번하게 일어나고 있어 디지털 영상에 대한 보안이 점점 더 중요하게 되어 가고 있다. 특히 유료 케이블 방송, 의료 영상 및 군사용 영상 그리고 개인 및 회사의 비밀 영상에 있어서 안전한 저장과 전송이 요구되고 있다.

본 논문에서는 1차원 카오스 사상(Map)인 PLCM (Piecewise Linear Chaotic Map)과 2차원 카오스 사상인 Baker 사상을 이용한 정지영상 암호 시스템을 제안한다. 본 제안 시스템은 1차원 PLCM을 기반으로 한 섭동(Perturbance)기반 카오스 스트림(Stream) 암호 기법과 2차원 Baker 사상을 기반으로 한 카오스 블록(Block) 암호 기법이 결합된 암호 시스템이다. 본 제안 시스템의 섭동기반 카오스 스트림 암호 기법은 1차원 PLCM 기반의 카오스 스트림 암호가 생성하는 키 스트림의 주기(Cycle)의 길이(Length)를 확장시키기 위해 섭동을 발생시키는 LFSR(Linear Feedback Shift Register)가 포함된 카오스 스트림 암호이다.

본 제안 시스템은 혼동(Confusion)특성이 뛰어난 카오스 스트림 암호기법과 확산(Diffusion)특성이 좋은 카오스 블록 암호기법이 결합된 구조이기 때문에 매우 안전한 암호시스템이며 또한 본 제안 시스템에 사용되는 PLCM과 Baker 사상은 매우 간단한 구조로 이루어져 있기 때문에 소프트웨어나 하드웨어로 구현이 쉬운 암호시스템이다. 그리고 암호화 과정을 수행하기 전에 원 영상을 같은 크기의 블록 영상들로 분할시킨 후에 각 블록 영상에 대해 CBC (Cipher Block Chaining)암호화 운영모드로 암호화를 수행하기 때문에 선택평문공격(Chosen Plain Text Attack)에도 매우 강한 암호시스템이다.

본 논문은 2장에서 카오스 암호에 대해 간략히 살펴보고 또한 카오스 암호가 이산화(Discrete)될 때 발생될 수 있는 문제점과 해결방안에 대해서 기술하고 3장에서는 본 논문에서 제안하는 다중 카오스 사상을 이용한 영상 암호화 시스템에 대해서 기술한다. 4장에서는 실험 결과 및 시스템 안전성에 대해서 논하고 마지막 5장에서 결론을 맺는다.

II. 카오스 암호 개요

이 장에서는 비선형 동력학 시스템으로서 카오스의 특성에 대해서 간략하게 설명하고 카오스 암호기법과 카오스 암호 설계 시 고려사항에 대해 기술한다.

2.1 카오스의 특성(Property)

식(1)과 같이 표현되는 1차원 동력학 시스템이 다음의 3가지 조건을 만족하면 카오스 특성을 가지고 있다고 한다.[3,4]

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

(i) 초기조건에 대한 민감성(Sensitivity)

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

(ii) 위상 이행성(Topological transitivity)

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

(iii) 주기점(Periodic points)이 집합 I에 밀집(Denseness)

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

위의 카오스 특성은 좋은 암호시스템이 지녀야 하는 조건인, '평문이나 키에 대해 민감성 그리고 평문과 암호문사이에 어떤 패턴도 존재하지 않아야 한다'는 조건과 일치한다.[5]

2.2 카오스 암호

카오스 암호는 크게 의사난수 키 스트림을 생성해서 평문을 암호화하는 카오스 스트림(Stream) 암호와 평문 또는 초기 조건 및 제어 매개변수 등을 이용해서 카오스 시스템의 반복 수행을 통해 암호문을 생성하는 카오스 블록(Block) 암호로 나눌 수 있다.

2.2.1 카오스 스트림 암호

키 스트림 발생기(Generator)로 카오스 시스템을 사용하는 일반적인 방법은 다음과 같다.[4] 카오스 시스템이 아래 식(2)와 같다고 가정하자.

$$x_{k+1} = f(x_k) \tag{2}$$

여기서 $f: I \rightarrow I$가 I 나 I x I 에서 카오스 특성을 가지고 있고 $x_0 \in I$ 을 비밀리 유지한다. x_k로부터 키 시퀀스를 생성하는 두 가지 방법이 있다. 첫 번째 방법은 비트 시퀀스 $(\theta_c(x_k)) = (\theta_c(f^k(x_0)))$을 생성하기 위해 아래 식(3)과 같은 경계(Thre-shold)함수를 사용한 것이다.

$$\theta_c(x) = \begin{cases} 0 & \text{if } x < c, \\ 1 & \text{if } x \geq c, \end{cases} \tag{3}$$

다른 두 번째 방법은 $|x_k|$에서 i번째 비트인 b_i를 취해서 $b_i(x_k)$인 비트 시퀀스로 생성하는 것이다. 위 두 가지 방법 모두 x_0를 비밀 키로 하여 비트 시퀀스를 생성한다.

2.2.2 카오스 블록 암호

블록 암호로 카오스 시스템을 사용하는 일반적인 방법은 다음 식(4)과 같은 카오스 사상을 이용하는 것이다.[4]

$$f_\alpha: I \rightarrow I \text{ 또는 } f_\alpha: I \text{ x } I \rightarrow I \text{x } I. \tag{4}$$

여기서 매개변수 α는 비밀 키 그리고 x_0는 평문.

그리고 카오스 사상을 정해진 회수 n만큼 반복 수행함으로써 암호문 $f_\alpha^n(x_0)$을 생성한다. 카오스 사상을 이용한 블록 암호시스템은 Habutsu et.al 에 의해 처음으로 제안되었다.[6] 이 시스템은 Tent 사상을 변형한 다음 식(5)(6)을 이용해서 암호시스템을 설계하였다.

$$f: \begin{cases} x_{k+1} = \dfrac{x_k}{\alpha} & 0 \leq x_k < \alpha \\ x_{k+1} = \dfrac{x_k - 1}{\alpha - 1} & \alpha < x_k \leq 1 \end{cases} \tag{5}$$

$$f^{-1}: \ x_{k-1} = \alpha x_k \text{ 또는 } (\alpha - 1)x_k + 1 \tag{6}$$

이 시스템은 메시지 블록 M을 암호하기 위해 M을 0과 1사이의 실수 m으로 변경한 후 역함수 f^{-1}을 n번 반복 수행해서 암호문 $C = f_\alpha^{-n}(m)$을 생성한다. 그리고 식(6)에서와 같이 두 개의 f^{-1} 중에 하나를 선택하기 위해서 n개의 임의의 비트를 사용한다. 평문 블록 m은 $f_\alpha^n(C) = f_\alpha^n(f_\alpha^{-n}(m))$을 통해 복호화 된다. 그러나 이 시스템은 곧바로 Biham에 의해 선택암호문공격(Known-Cipher-text attack)방법으로 깨졌다.[7] 그러나 이 시스템이 발표된 이후 다른 여러 카오스 사상을 이용한 많은 카오스 블록 암호시스템이 제안되어 왔다.

2.3 카오스 암호 설계 시 고려사항

컴퓨터는 유한한 메모리와 유한한 정밀도(Precision)를 가지고 있기 때문에 컴퓨터상에서 카오스 암호를 설계할 때 가장 중요하게 고려되어야 할 사항은 동력학적(Dynamical) 기능저하(Degradation)이다.[4,8] 기능저하와 관련된 문제로 짧은 주기 길이와 비이상적인(non-ideal) 분산(Distribution) 그리고 상관관계(Correlation) 문제가 있다. 그 원인으로, 유한 정밀도를 L 비트라고 가정하면 카오스

시스템은 2^L개의 값으로만 표현되기 때문에 카오스 시스템의 주기 길이는 2^L보다 클 수가 없으며 실제 대부분의 주기 길이는 2^L 보다 매우 작다. 또한 카오스 시스템은 초기조건에 매우 민감하기 때문에 반복 수행될 때 발생하는 라운딩 에러와 양자화(Quantization) 에러가 발생되는 경우가 생긴다. 이러한 원인으로 해서 카오스의 동력학적 특성이 컴퓨터상에서 구현될 때 사라져버리는 경우가 발생하게 된다. 이러한 기능저하에 대한 보완책으로 더 높은 유한 정밀도를 사용하거나 의사난수(Pseudo-Random)를 통한 섭동(Perturbance)기반의 알고리즘을 이용하거나 또는 다수의 카오스 시스템을 연결시키는 방법이 제안되고 있다.[8]

Ⅲ. 다중 카오스 사상을 이용한 영상 암호화 시스템

본 논문에서 제안한 다중 카오스 사상을 이용한 영상 암호 시스템은 1차원 PLCM을 이용한 카오스 스트림 암호 기법과 2차원 Baker 사상을 이용한 카오스 블록 암호 기법이 결합된 암호화 시스템이다. 본 제안 시스템은 암호화 처리를 하기 전에 원 영상을 몇 개의 서브 블록들로 먼저 나눈 후에 나눠진 각 블록에 대해서 암호화 처리를 수행한다. 본 시스템의 암호화 운영 모드로 CBC(Cipher Feedback Chaining)를 적용함으로써, 즉 암호화 된 서브 블록이 다음에 암호화 될 서브 블록과 XOR되어져서 선택 평문 공격(Chosen plaintext attack)에 저항성을 갖도록 했다. 임의로 나누어진 각 블록은 먼저 한 개의 1차원 PLCM과 한 개의 m-LFSR로 구성된 섭동(Perturbance)기반의 카오스 스트림 암호 기법으로 암호화 된다. 이렇게 암호화된 블록은 다시 2차원 Baker 사상으로 구성된 카오스 블록 암호 기법으로 암호화 된다. 본 제안 시스템은 두 개의 카오스 암호 알고리즘을 결합시킴으로써 카오스 스트림 암호나 카오스 블록 암호에 각기 내재된 보안상의 취약점을 극복할 수 있도록 설계되었다. 또한 본 제안 시스템은 1차원 PLCM에 바탕을 둔 카오스 스트림 암호알고리즘을 통해 좋은 혼동(Confusion)특성과 2차원 Baker 사상(Map)에 바탕을 둔 카오스 블록 암호알고리즘을 통해서는 좋은 확산(Diffusion) 특성을 지니도록 설계하였다. 본 제안 시스템의 블록 다이어그램은 그림 1과 같다.

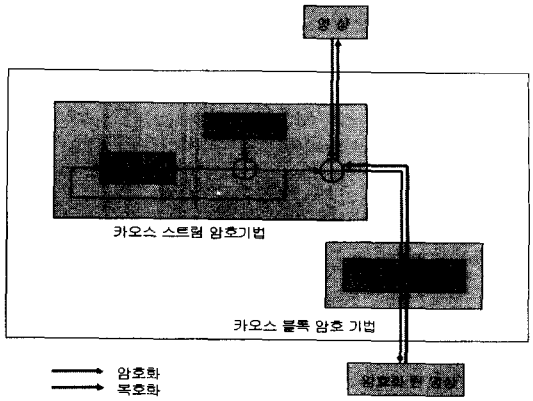


그림 1. 제안시스템의 블록 다이어그램
Fig. 1. Block diagram of proposed system.

3.1 시스템 구성요소

본 제안 시스템에서는 1차원 PLCM과 m-LFSR으로 구성된 섭동기반 카오스 스트림 암호기법과 2차원 Baker 사상(Map)을 이용한 카오스 블록 암호기법으로 구성되어 있다.

3.1.1 섭동기반 카오스 스트림 암호 기법

본 제안 시스템에서는 그림 2와 같이 1차원 PLCM과 m-LFSR으로 구성된 섭동기반 카오스 스트림 암호기법을 이용한다.

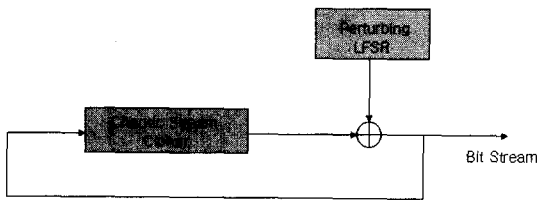


그림 2. 섭동(Perturbance)기반 카오스 스트림 암호
Fig. 2. Perturbance-based Chaotic Stream Cipher.

본 시스템에서는 식(7)과 같은 간단한 1차원 카오스 사상을 고려한다.

$$x_{t+1} = F(x_t) \in [0,1), \text{ 여기서 } x_t \in [0, 1), \quad t = 0, 1, 2, \cdots \tag{7}$$

컴퓨터에서 수치로 표현할 수 있는 정밀도를 P라고 하면, x_t는 식(8)과 같이 표시할 수 있다.[9]

$$x_t = 0.x_{t,1}x_{t,2}\ldots x_{t,i}\ldots x_{t,p},\ x_{t,i} \in \{0,1\},$$
$$i = 1, 2, \cdots, P \tag{8}$$

의사난수(Pseudo Random) 비트 스트림 $BS_i = \{x_{1,i}, x_{2,i}, x_{3,i}, \ldots\}$는 $x_t(t = 1,2,3\ldots)$에서 i번째 비트를 추출한 시퀀스로 구성된다. 본 시스템에서는 카오스 사상 F으로 [10]에서 제안된 PLCM (Piecewise Linear Chaotic Maps)을 사용한다. PLCM은 다음 식(9)과 같다.

$$F(x,q) = \begin{cases} x/q & 0 \le x \le q, \\ (x-q)/(\frac{1}{2}-q) & q \le x \le \frac{1}{2}, \\ F(1-x,q) & \frac{1}{2} \le x \le 1, \end{cases} \tag{9}$$

여기서 q는 $0 < q < \frac{1}{2}$.

PLCM은 다음과 같은 매우 완벽한 동력학적(dynamical) 특성을 가지고 있다.[11]

(i) 에르고딕성(Ergodic), 혼합성(Mixing).
(ii) 균일한 불변밀도함수(invariant density function).
(iii) δlike한 자기상관성(auto-correlation).

PLCM에 의해 생성되는 키 스트림의 주기를 확장시키기 위해서 PLCM에 섭동을 발생시킨다. 이는 PLCM이 안정된(Stable) 주기상태로 진입하는 것을 막음으로써 주기를 확장시키는 방법이다. 섭동(Pert-urbance)은 아래와 같은 조건을 만족하는 것을 선택한다.[9]

(i) 제어할 수 있는 긴 주기와 균일한 분포(Distribution)를 가지고 있어야 한다.
(ii) 카오스 시스템이 지닌 본래의 특성(Property)을 약화시키지 않아야 한다. 그렇게 하기위해 섭동 신호의 크기는 카오스 신호의 크기에 비해 매우 작아야 한다.
(iii) 섭동 시간은 전체 시스템 동작 시간에 비해 매우 작어야 한다.

위의 조건을 만족하는 섭동 신호발생기로는 최대 길이 LFSR이다. LFSR에 의해 발생된 시퀀스는 다음과 같은 장점을 가지고 있다.[9]

(i) 주기 길이가 2^L-1 (여기서 L은 차수(Degree))로 명확하다.
(ii) 균일한 분포(Distribution)를 가지고 있다.
(iii) δ-like한 자기상관성(auto-correlation)을 가지고 있다.
(iv) P-precision 시스템에서 제어할 수 최대 신호 크기는 $2^{-p}(2^L-1)$개다.

섭동신호 시퀀스는 아래 식(10)에 의해서 생성된다.

$$a_{L+k} = c_1 a_{L+k-1} \oplus c_2 a_{L+k-2} \oplus \ldots \oplus c_L a_k$$
$$k = 0, 1, 2, \cdots \tag{10}$$

여기서 $\{c_1, c_2, \ldots, c_L\}$은 탭(Tap) 시퀀스이고 $\{a_0, a_1, \ldots, a_{L-1}\}$은 모두 0이 아닌 초기 값이다.

섭동은 $t = 0$에서 시작해서 매 $\triangle$만큼의 반복수행(Iteration)후에 다음 섭동이 발생하는데 섭동은 현재의 카오스 신호와 섭동 신호와의 비트 간 XOR (Exclusive-or)로 수행된다. XOR되는 각 신호의 비트는 다음 식(11)에 의해서 결정된다.

$t = k\triangle$ ($k = 0, 1, 2, \cdots$) 일 때

$$x_{t+1,i} = \begin{cases} [F(x_t)]_i & 1 \le i \le P-L \\ [F(x_t)]_i \oplus a_{k+P+1-i} & P-L+1 \le i \le P \end{cases} \tag{11}$$

여기서 P는 유효정밀도, L은 차수(Degree) 그리고 $[F(x_t)]_i$은 $F(x_t)$의 i번째 비트.

$t \neq k\triangle$ 일 때는 섭동이 발생하지 않는다. 즉 $x_{t+1} = F(x_t)$.

위의 섭동기반 스트림암호에서 발생된 비트 스트림과 영상의 각 픽셀의 그레이 값과 XOR을 통해 암호화 된 영상을 생성한다.

3.1.2 2차원 Baker 사상(Map) 기반 카오스 블록 암호 기법

2차원 Baker 사상을 이용한 카오스 블록 암호기법에서 사용되는 연속 Baker 사상 B는 다음 식(12)과 같다.

$$B(x,y)=\begin{cases}(2x,\frac{y}{2}) & 0\le x<\frac{1}{2}\\ (2x-1,\frac{y}{2}+\frac{1}{2}) & \frac{1}{2}\le x\le 1\end{cases} \quad (12)$$

Baker 사상은 그림 3과 같이 단위 평방(Square)위에서 동작한다.

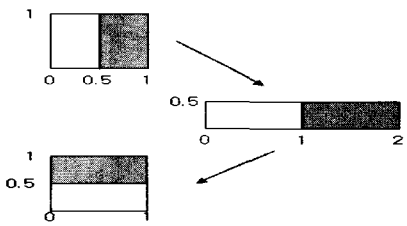


그림 3. Baker 사상
Fig. 3. Baker Map.

왼쪽에 수직으로 있는 열[0,1/2) x [0,1)은 수평으로 늘어진 후 다시 수직 [0,1) x [0,1/2) 으로 줄어든다. 오른쪽에 수직으로 있는 열[1/2,1) x [0,1)도 똑같은 과정을 통해 [0,1) x [1/2,1) 으로 사상(Mapping)된다. Baker 사상은 단위 평방으로의 전단사 카오스 사상이다. 그리고 암호화 될 영상이 유한한 픽셀로 구성되어 있기 때문에 Baker 사상도 그에 따라 이산화(Discrete) 되어야한다. 즉, 단위 평방(I x I)에서 격자 M_0^M x M_0^M으로 사상(Map)의 범위와 영역이 바뀌어야한다. 여기서 $M_0^M=\{0,\cdots,M-1\}$이고 M은 픽셀의 열(Row)수와 같다. 기본적으로 이산화 된 사상은 아래의 식(13)의 조건을 만족해야 한다.[5]

$$\lim_{M\to\infty}\max_{0\le i,j<M}|f(i/M,j/M)-F(i,j)|=0 \quad (13)$$

여기서 f는 연속(Continuous)사상이고 F는 이산화 된 사상이다.

식(13)은 이산화 된 사상의 픽셀의 수를 무한대로 증가시키면 연속 사상에 가깝게 될 수 있어야 함을 의미한다. 이산화 된 Baker 사상은 $B_{(m_1,\ldots,m_k)}$으로 표기될 수 있다. 여기서 k개의 정수 시퀀스 $m_1,\cdots,m_k$를 선택한다. 선택된 정수 m_i는 M을 나눌 수 있고 $m_1+\cdots+m_k=M$을 만족해야 한다. $M_i=m_1+\cdots+m_i$이라고 하면, $M_i\le x<M_i+m_i$ 이고 $0\le y<M$ 인 픽셀 (x,y)은 식(14)과 같이 사상된다.[5]

$$B_{(m_1,\ldots m_k)}(x,y)=\left(\frac{M}{m_i}(x-M_i)+y \bmod \frac{M}{m_i},\ \frac{m_i}{M}(y-y\bmod\frac{M}{m_i})+M_i\right) \quad (14)$$

다음 그림 4는 이산화 된 Baker 사상을 보여준다.

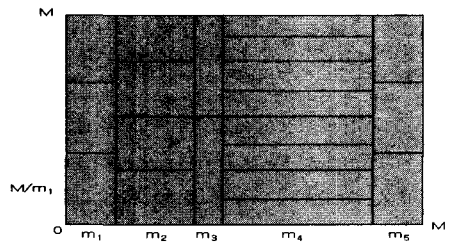


그림 4. 이산화 된 Baker 사상
Fig. 4. Discretized Baker map

그림 5에서는 8픽셀 영상을 3개의 세그먼트 값 4, 2, 2 (4+2+2=8)로 나누어서 치환(Permutation)시키는 예를 보여주고 있다.

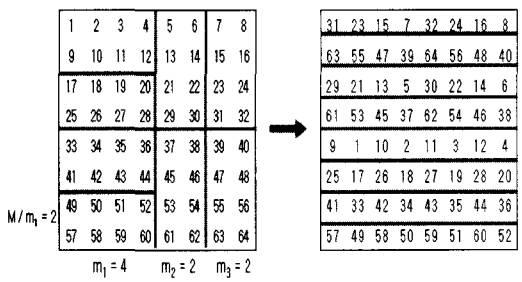


그림 5. 이산화 된 Baker 사상 치환 예
Fig. 5 Example of the permutation of the discretized Baker map.

영상은 위의 방법과 같이 세그먼트 값을 암호 키로 하여 식(14)과 같은 치환을 통해 암호화 된다.

3.2 암호화 과정

암호화 과정을 수행하기 하기 전에 원 영상을 임의의 작은 정사각형 크기의 블록(Block)들로 분할한다. 영상을 L 그레이(Gray) 레벨을 가진 M x M 픽셀로 구성된 정사각형(Square)의 영상 OP라고 하고, 작은 정사각형 블록 영상 S는 b x b의 크기를 갖는다고 가정하자. $M = n * b$이면 원 영상은 n^2개의 블록 영상 S로 나누어지고 n^2개의 블록 영상에 대한 암호화가 수행되며 CBC (Cipher block chaining) 암호화 운영모드로 동작한다.

암호화 과정은 크게 2단계로 구성되어 있다. 첫 단계에서는 섭동(Perturbance)기반 카오스 스트림 암호기법으로 영상에 대한 대치(Substitution)를 수행하고 두 번째 단계에서는 카오스 블록 암호기법으로 영상에 대한 치환(Permutation)을 수행한다. 첫 번째 단계와 두 번째 단계의 반복 수행(Iteration) 횟수는 요구되는 암호강도(level of security)에 따라 결정된다. 그리고 일반적으로 카오스 암호 시스템에서는 초기 조건과 제어 파라미터가 암호 키로서 동작을 한다. 본 제안 시스템에서도 첫 번째 단계의 PLCM에 사용하는 초기조건과 초기 파라미터, 두 번째 단계에서 사용되는 영상의 세그먼트(Segment)들의 값 그리고 반복 수행 회수가 암호 키 및 비밀 키로서의 역할을 하며 사용되는 암호 키는 다음과 같다.

(i) x_0 : PLCM의 초기 값.

(ii) q : PLCM의 초기 파라미터.

(iii) $K_{seg} = \{ b_{1,} b_{2} \ldots b_m \}$ (여기서 $b_1 + b_2 + \cdots + b_m = b$) : 영상의 세그먼트들의 값.

(iv) K_{ter} : 반복 수행 회수

첫 번째 단계: 섭동기반 카오스 스트림 암호기법을 통한 암호화 수행.

섭동기반 카오스 스트림암호에서 x_0와 q을 키로 해서 발생된 비트 스트림 BS와 블록 영상 S의 각 픽셀의 그레이 값과 XOR을 통해 암호화 된 블록 영상 S'을 생성한다.

두 번째 단계: 2차원 Baker 사상(Map) 기반 카오스 블록 암호기법을 통한 암호화 수행.

두 번째 단계에서는 2차원 Baker 사상을 이용한 카오스 블록 암호기법을 통해 첫 번째 단계에서 암호화된 블록에 좋은 확산(Diffusion)특성을 부여하는 것이다. 블록 영상 S'을 세그먼트 값 K_{seg}을 암호 키로 하여 치환(Permutation)과정을 통해 암호화 된 영상 S''을 얻는다.

반복 수행: 반복 수행 회수 K_{er}만큼 첫 번째단계와 두 번째 단계를 반복 수행한다.

CBC 암호화 운영 모드: 암호화 된 블록 영상은 다음 처리될 블록 영상과 XOR되며 그 결과로 나온 영상이 새로운 입력 블록 영상으로 암호화가 수행된다.

$$S''_i = E_k(S_i \oplus S''_{i-1})$$

여기서 S_i는 영상, S''_i는 암호화 된 영상, i =1,…

복호화 과정: 복호화는 암호화과정의 역순으로 수행된다. 먼저 마지막 암호화 된 블록 영상을 두 번째 암호화 단계를 거쳐 복호화를 수행하고 나온 결과 영상을 다시 첫 번째 암호화 단계로 복호화를 수행한다. 이러한 과정은 반복 수행 회수 만큼 각기 두 번째와 첫 번째 단계를 반복 수행하며 나온 복호화 된 블록 영상은 CBC 암호화 운영모드로 다음 복호화 처리될 블록 영상과 XOR된다. 이러한 과정을 나머지 블록 영상들에 모두 똑같이 적용하여 복호화 된 영상을 얻는다.

Ⅳ. 실험 결과 및 안전성 분석

4.1 실험 결과

본 실험에서는 실험 영상으로 그림 6의 그레이 레벨 Lena 256 x 256 영상을 사용하였다. 영상을 암호화하기 전에 임의의 크기로 영상을 분할하는데 본 실험에서는 128 x 128 크기의 블록 4개로 분할하였다. 첫 번째 암호화 단계에서 암호 키로 사용되는 PLCM의 초기 값과 초기 파라미터는 다음과 같다.

x_0 = 0.7159814937

q = 0.3597815497

그리고 첫 번째 암호화 단계의 카오스 스트림 암호에서 발생되는 키 스트림 주기의 길이를 확장하기 위해 사용되는 섭동 신호 발생기 LFSR는 $x^{32}+x^7+x^5+x^3+x^2+x+1$로 표현되는 32비트 원시다항식을 사용하며 초기 값(x_{seed})은 0x15를 선택하고 $\triangle = 10^4$ 마다 섭동을 발생시켰다. 두 번째 암호화 단계에서 암호 키로 사용되는 영상 세그먼트 크기 값인 K_{seg}는 {8, 16, 32, 8, 32, 8, 16, 4, 4}로 설정하여 암호화를 수행했다. 위의 두 단계의 암호화는 CBC 암호화 운영모드로 반복 수행 회수(K_{er})만큼 암호화가 수행된다. 그림 7은 1번 반복 수행된 암호화된 영상이며 그림 8은 9번 반복 수행된 암호화된 영상이다.

그림 6. 실험 원 영상
Fig. 6. The test original image.

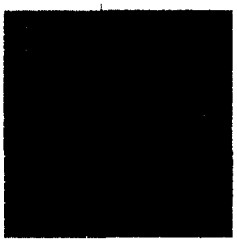


그림 7. 1번 반복 수행된 암호화 된 영상
Fig. 7. The encrypted image after 1 iteration.

그림 9는 원 영상의 히스토그램이고 그림 10 그리고 그림 11은 각각 그림 7과 그림 8 영상에 대한 히스토그램을 보여주고 있다. 그림 7과 그림 8에서 보이는 것처럼 암호화 된 영상은 거의 무작의적인 (Random) 영상처럼 보인다. 그리고 암호화된 영상의 히스토그램은 그림 10과 그림 11에서 보이는 것처럼 균일한 히스토그램을 보여주고 있다. 그림 12는 PLCM의 초기값 x_0=0.7159814937로 암호화 된 영상을 같은 PLCM의 초기값 x_0 값으로 복호화 한 영상이고 그림 13은 PLCM의 초기값 x_0 = 0.7159814 938로 복호화 한 영상이다. 그림 12와 그림 13에서 보는 것처럼 초기 값의 조그마한 차이가 결과적으로 아주 큰 차이로 나타난다. 그림 14는 두 번째 암호화 단계에서 사용되는 영상 세그먼트 크기 값 K_{seg}= {8, 16, 32, 8, 32, 8, 16, 4, 4}로 암호화 된 영상을 같은 K_{seg}으로 복호화 한 영상이고 그림 15는 영상 세그먼트 크기 값을 K_{seg}={8, 16, 4, 8, 32, 8, 16, 4, 32}로 하였을 때 복호화 된 영상이다. 그림 14와 그림 15에서 보는 바와 같이 단지 세그먼트 값들의 순서만 바꾸어도 결과적으로 아주 다른 영상이 나오게 된다.

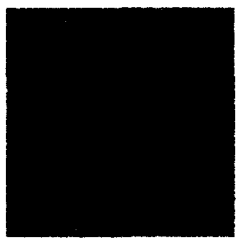


그림 8. 9번 반복 수행된 암호화 된 영상
Fig. 8. The encrypted image after 9 iterations

그림 9. 원 영상의 히스토그램
Fig. 9. Histogram of the original image.

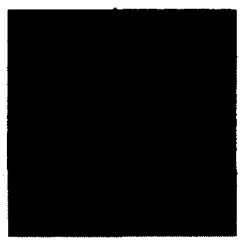


그림 10. 그림 7의 히스토그램
Fig. 10. Histogram of the Pic. 7.

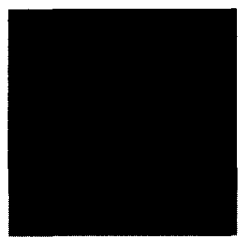


그림 11. 그림 8의 히스토그램
Fig. 11. Histogram of the Pic. 8.

4.2 안전성 분석

암호 시스템은 기본적으로 암호 키에 민감해야 하고 사용되는 암호 키의 수가 전사공격(Brute force attack)에 대응할 수 있도록 충분히 커야 한다. 본 시스템에 사용되는 PLCM과 Baker 사상은 거의 완벽한 카오스 동력학 특성을 가지고 있기 때문에 암호 키에 매우 민감하다. 위의 그림 13에서 보는 바와 같이 초기 조건에 미세한 차이가 발생해도 정확하

게 복호화가 되지 않는다. 그리고 첫 번째 암호화 단계인 섭동기반 카오스 스트림 암호에서 L 차수(Degree)의 LFSR를 사용하는 경우에 키 스트림 주기 길이(Cycle Length) T는 $\sigma\triangle(2^L-1)$ (여기서 σ는 양의 정수)이다.[9] 그래서 최소 키 스트림 주기 길이 T는 $\triangle(2^L-1)$가 된다. 이 T값은 암호학적으로 충분히 큰 값이다.

그림 12. x_0= 0.7159814937 으로 복호화 한 영상
Fig. 12. Decrypted image with x_0= 0.7159814937.

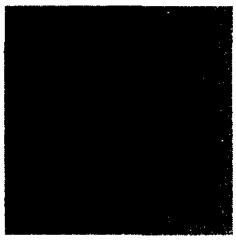


그림 13. x_0= 0.7159814938 으로 복호화 한 영상
Fig. 13. Decrypted image with x_0= 0.7159814938.

그림 14 K_{seg}= {8, 16, 32, 8, 32, 8, 16, 4, 4}로 복호화 한 영상
Fig. 14. Decrypted image with K_{seg} = {8, 16, 32, 8, 32, 8, 16, 4, 4}.

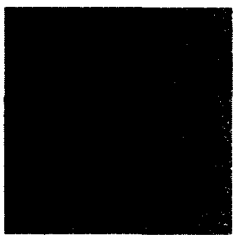


그림 15. K_{seg}= {8, 16, 4, 8, 32, 8, 16, 4, 32}로 복호화 한 영상
Fig. 15. Decrypted image with K_{seg}= {8, 16, 4, 8, 32, 8, 4, 32}.

위의 4.1의 실험의 경우에 $\triangle$이 10^4이고 L의 차수가 32이기 때문에 최소 키 스트림 주기 길이 $T_{\min}$는 4.294 x 10^{14} 이 된다. 본 시스템에서의 사용되는 키 Key는 식(15)과 같이 표현될 수 있다.

$$Key = \{I,\ S_{x0},\ S_p,\ n_1,\ldots,n_k\} \qquad (15)$$

여기서 I는 반복 회수, S_{x0}는 PLCM에 사용되는 초기 값, S_p는 PLCM에서 사용되는 초기 파라미터 그리고 $n_1,\ldots,n_k$는 Baker 사상에 사용되는 파라미터 값이다.

암호에 사용되는 영상이 그레이 레벨의 N x N 크기의 영상이라고 가정하자. 우선 Baker 사상에서 사용되는 파라미터 $n_1,\ldots,n_k$에 의해 생성되는 암호 키의 수는 영상의 크기 N과 제수들의 합이 N, 즉 $n_1+\ldots+n_k=N$, 이 되는 얼마나 많은 제수들의 조합이 존재하는 가에 달려있다.[5] 영상의 크기 N이 64, 128, 256, 512 인 경우의 암호 키의 수는 각기 대략 10^{15}, 10^{31}, 10^{63}, 10^{126} 이 됨이 알려져 있다.[5] 그리고 유효 정밀도 P가 64비트인 시스템에서 PLCM의 S_{x0}와 S_p는 각기 2^{64}개를 가진다. 그래서 본 제안 시스템의 암호 키의 수는 I x $K(S_{x0})$ x $K(S_p)$ x $K(N_k)$ 된다. 여기서 $K(S_{x0})$, $K(S_p)$ 그리고 $K(N_k)$는 각기 S_{x0}의 암호 키의 수, S_p의 암호 키의 수 그리고 Baker 사상에 사용되는 암호 키의 수를 나타낸다. 본 제안 시스템의 암호 키의 수는 전사공격에 대응할 만큼 충분한 암호 키의 수를 가지고 있다. 표 1은 반복 회수에 따른 원 영상(그레이 레벨의 256x256 Lena 영상)과 암호화 된 영상간의 픽셀 값의 차이가 생기는 픽셀의 백분율을 보여주고 있다.

표 1. 원 영상과 암호화 된 영상과의 반복 회수에 따른 픽셀 값의 변화율
Table 1. Percentage of different pixel numbers between the original image and the encrypted image by iteration number.

반복 회수	1번	3번	5번	9번
백분율	99.577%	99.623%	99.638%	99.620%

표 1에서 보는 것처럼 1번의 반복 회수만으로도 거의 모든 원 영상의 픽셀 값이 변하게 됨을 알 수 있다.

또한 표 2는 PLCM의 초기 값 x_0에 미세한 변화를 주었을 때의 차이가 생기는 픽셀의 백분율을 보여주고 있다. x_0 = 0.7159814937로 암호화 된 영상과 x_0 = 0.7159814938로 암호화 된 영상 사

이에 반복 회수에 따른 차이가 있는 픽셀의 백분율을 보여준다. 표 2에서 보는 것처럼 암호 키의 1비트 차이도 거의 모든 영상의 픽셀에 영향을 준다

표 2. 초기 값의 미세한 차이로 인한 영상간의 반복 회수에 따른 픽셀의 변화율
Table 2. Percentage of different pixel numbers between the two images have slight different of initial value by iteration number.

반복 회수	1번	3번	5번	9번
백분율	99.168%	99.230%	99.203%	99.176%

또한 원 영상과 1번 반복 수행된 암호화 된 영상에서 임의로 각각 1000개씩 수직방향, 수평방향 그리고 대각선방향으로 인접한 두 개의 픽셀을 선택한 후 아래 식(16)을 이용해서 상관계수(Correlation coefficient)를 계산하면 표 3과 같다.

$$r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{16}$$

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

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

여기서 x, y는 영상에서 두 개의 인접한 픽셀의 그레이 값이다.

표 3. 원 영상과 암호화 된 영상에서 인접한 픽셀간의 상관계수(Correlation coefficient) 분석
Table 3. Correlation coefficients of two adjacent pixels both in original image and encrypted image.

	원 영상 (Lena 256 x 256)	암호화 된 영상
수평방향	0.99368558	0.01140810
수직방향	0.95553439	0.00536324
대각선방향	0.94722958	-0.018230303

영상 암호시스템이 통계적(Statistical) 공격에 매우 강하기 위해서는 매우 좋은 혼동(Confusion) 특성과 확산(Diffusion)특성을 가지고 있어야 하는데 혼동 특성은 암호화 된 영상의 히스토그램으로 확산 특성은 영상의 인접한 픽셀간의 상관계수로 정량적으로 확인 할 수 있다. 본 제안 시스템은 표 3에서 보는 바와 같이 암호화 된 영상에서의 인접한 픽셀간의 상관계수가 거의 0에 가까운 값을 가지고 있고 또한 그림 10과 그림 11에서 보는 바와 같이 암호화 된 영상이 매우 균일한 히스토그램을 가지고 있기 때문에 통계적인(Statistical) 공격에 매우 강한 특성을 가지고 있다.

V. 결 론

현재, 인터넷 및 무선 이동통신을 이용한 멀티미디어 정보교류가 활발히 이루어지고 있는 상황에서 개인의 사생활과 기업이나 기관의 기밀에 관련된 영상에 대한 보안이 더욱 중요시 되어 가고 있다.[14] 그런데 기존의 대칭키 및 공개키 암호시스템은 영상과 같이 큰 크기와 높은 중복특성(Redundancy)을 가진 데이터 형태의 암호에는 적합하지 않고 또한 앞으로 등장할 양자컴퓨터에 의해 안전성에도 의문이 제기되고 있다.[1,5] 그리고 최근 새로운 암호시스템의 원천으로 카오스 이론을 이용한 카오스 암호에 대한 연구가 활발히 진행되고 있다. 또한 카오스 이론을 이용한 영상 암호시스템에 대한 연구도 많은 관심을 가지고 연구되고 있고 안전성에 대한 분석도 함께 이루어지고 있다.[12] 이에 본 논문에서는 1차원 카오스 사상인 PLCM 과 2차원 카오스 사상인 Baker 사상을 이용한 영상 암호시스템을 제안했다. 제안된 시스템은 카오스 스트림 암호와 카오스 블록 암호가 결합된 구조로 되어있고 또한 CBC 운영모드를 사용해서 보다 좋은 혼동(Confusion)과 확산(Diffusion)특성을 지니도록 설계했다. 그리고 실험 결과를 통해 통계적인 공격에도 매우 안전함을 보여주었다. 그러나 원 영상이 여러 개의 서브 블록들로 나누져 CBC 운영모드로 암호화가 수행되기 때문에 몇 개의 블록으로 나누어지느냐에 따라 전체적으로 수행속도에 있어서 차이가 생길 수 있는 문제점이 있다. 앞으로 카오스 암호에 대한 연구를 더욱 진척시켜 보다 안전하고 그리고 많은 멀티미디어 서비스 응용에 쉽게 적용될 수 있는 카오스 암호 시스템을 개발해야 할 것이다.

참 고 문 헌

[1] G. Chen, Y. Mao, C. Chui, "A sym-

metric image encryption scheme based on 3D chaotic maps," Chaos, Solitons & Fractals, 21(3), pp. 749-761, July 2004.

[2] H. Zhou, X. Ling, J. Yu, "Secure communication via one-dimentional chaotic inverse systems," IEEE International Symposium on Circuits and Systems 97, 2, pp. 9-12, June 1997.

[3] R. Devaney, "An Introduction to Chaotic Dynamical Systems Second Edition," Addison-Wesley Publication Company, Reading MA, 1989.

[4] R. Schmitz, "Use of chaotic dynamical systems in cryptography," Journal of the Franklin Institute, 338, pp. 429-441, 2001.

[5] J. Fridrich, "Symmetric Ciphers based on two-dimensional chaotic maps," International Journal of Bifurcation and Chaos, 8(6), pp. 1259-1284, 1998.

[6] T. Habutsu, Y. Nishio, I. Sasase, S. Mori, "A secret key cryptosystem by iterating a chaotic map," In Advances in Cryptology EuroCrypt'91, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 0547, pp. 127-140, 1991.

[7] E. Biham, "Cryptoanalysis of the chaotic-map cryptosystem suggested at EuroCrypt'91," In Advances in Cryptology - EuroCrypt'91, Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 532-534, 1991.

[8] S. Li, X. Zheng, X. Mou, Y. Cai, "Chaotic encryption scheme for real-time digital video," In Real-Time Imaging VI, Proceedings of SPIE, 4666, pp. 149-160, 2002.

[9] S. Tao, W. Ruili, Y, Yixun, "Perturbance-based algorithm to expand cycle length of chaotic keystream," Electronics Letters, 4(9), pp. 873-874, April 1998.

[10] H. Zhou, X. Ling, "Problems with the chaotic inverse system encryption approach," IEEE Trans, Circuits and System-I, 44(3), pp 268-271, 1997.

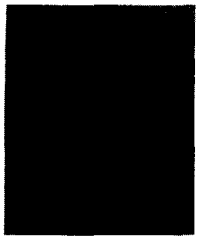
[11] R. Tenny.L.Tsimring, L. Larson, H. Abarbanel, "Using Distributed Nonlinear Dynamics for Public Key Encryption," Physical Review Letters, 90(4), pp.047903, January, 2003.

[12] S. Li, X. Zheng,"Cryptanalysis of a chaotic image encryption method," In 2002 IEEE Int. Sym. Circutis and Systems Proc. pp.708-711, 2002.

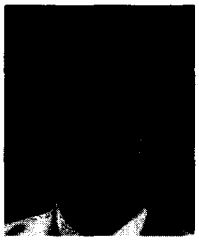
[13] 홍진근, 박종호, 황찬식, "이산 카오스 함수와 Permutation Algorithm을 결합한 고신뢰도 광영상 암호시스템," 통신정보보호논문지, 9(4), 1999.

[14] 정현수, 유은진, 전문석, 이철희, "고속 암호화 영상처리를 위한 대표성 병렬 시스템 개발," 통신정보보호논문지, 6(1), 1996.

〈著者紹介〉



이 성 우 (Sung-Woo Lee) 학생회원
1993년 2월 : 동국대학교 컴퓨터공학과 졸업
1998년 8월 : 동국대학교 전자공학과 석사
1998년 8월~현재 : 동국대학교 전자공학과 박사과정
〈관심분야〉 카오스암호, 멀티미디어 보안



신 재 호 (Jaeho Shin) 정회원
1979년 2월 : 서울대학교 전자공학과 졸업
1982년 2월 : 서울대학교 전자공학과 석사
1987년 2월 : 서울대학교 전자공학과 박사
1988년 3월~현재 : 동국대학교 전자공학과 정교수
〈관심분야〉 정보보호, 멀티미디어 보안, DSP