LCI 카오스 암호화 기법

김대영*, 김태식**
*안동정보대학 인터넷정보과
**계명대학교 공과대학 컴퓨터전자공학부
e-mail: dykim@www.ait.ac.kr

Encryption Method Based on a Chaos LCI

Kim, dae young*, Kim, tae sik**
*Dept. of Internet & Information, Andong Info Tech
**Dept. of Computer Engineering, Keimyung University

요 약

본 연구에서는 카오스이론을 기초로하여 이미지를 암호화 할 수 있도록 하는 LCI(Logistic Chaos Cryptosystem Image)를 제안한다. 로지스틱맵을 이용한 이미지 암호화 기법은 초기 조건에 민감한 카오스의 특징을 이용하였다.

실험결과 제안된 LCI(Logistic Chaos Cryptosystem Image) 기법을 통해 이미지는 카오스적으로 표현되었으며, 소스이미지와 암호 이미지 사이는 관련성이 없었다. 향후 안전성이나 처리속도에 대한 검증과 표준화 문제 및 멀티미디어 자료 등에 대한 암호화 기법을 계속 연구해야 할 것이다.

실험결과 제안된 LCI 기법을 통해 암호문은 카오스적으로 표현되었으며, 소스이미지와 암호이미지 사이에 어떠한 동질성도 찾아 볼 수 없었다. 향후 안전성이나 처리속도에 대한 검증과 표준화 문제 및 멀티미디어 자료에 대한 암호화 기법을 계속 연구해야 할 것이다.

1. 서 론

카오스란 말은 혼돈이라는 뜻으로 번역되는 단어로 사전적 의미로는 천지창조 이전의 혼란스러움 또는 무질서, 대 혼란이란 뜻으로 쓰이며, 카오스란 말의 근원은 그리스어에서 기원하며 그 뜻 은 세상의 여러 가지 무질서한 상태, 즉 우주가 생성되는 과정 중 최초의 단계로 천지의 구별과 질서가 없는 영망진창의 상태를 말한다. 그러나 이 단어의 내면에는 창조의 근원이라는 이미지가 포함되어 있다.

카오스라는 존재의 의미는 이 세상에서 일상적으로 낭연히 일어나는 현상으로서 지금까지의 공학세계라는 것이 대부분 선형 세계의 모습을 나타내지만 우리가 속해 있는 자연계의 현상은 선형시스템과는 달리 비선형적인 모습이다. 예를 들어 공기의 흐름이나 뇌의 활동, 물의 흐름 등이 모두 비선형의 모습을 지닌다. 혹자는 미분방정식이나 차분방정식 등으로 표시되는 결정론적 역학계에서 생성하는 카오스는 상대론, 양자역학과 더불어 20세기 과학의 3대 발견이라고 까지 말하는 학자가 있을 정도로 과학적으로 중요한 개념을 지닌다. 현재 전세계의 연구원들은 지금까지의 공학분야에서의 학문의 틀인 선형세계를 넘어서 비선형시스템으로 문제를 해결하려는 움직임을 보이고 있다.

대기의 흐름이나 물의 흐름, 뇌의 활동 등이 모두 비선형의 한 모습이다. 이 비선형시스템에서도 가장 일반적으로 일어나는 현상이 카오스다. 이러한 의미에서 카오스는 세계의 모든 시스템과 밀접한 관계가 있다고 말할 수 있다.

공학에서의 카오스 응용은 한정된 영역에서 비선형적인 현상을 규명하고자 하는 시도로서 어느 정도 예측이 가능한 결정론적 카오스(deterministic chaos)를 다루게 된다. 이러한 연구를 바탕으로 카오스 이론을 결정론적 비선형 동역학 시스템 (Deterministic Nonlinear Dynamic System)을 다루고, 불안정한 비주기적 운동을 정성적으로 연구하는 학문으로 정의하고 있다[1].

카오스이론은 그 복잡한 현상중 일정한 규칙과 단순한 행동에 따라 움직인다는 뜻이다. 즉 카오스에는 일정한 규칙이 있어 그 규칙에 따라 진행하는 것이 카오스 이론이라 한다.

카오스이론을 가전제품이나 전기기기등에 이용하기 시작한 것은 1975년에 로버트 메이라는 수리생물학자에 의해서 생물의 개체수 변동을 수학적으로 처리하는 데서부터 기원을 잡을 수 있다. 네이쳐지에 발표된 로버트 메이의 논문에서 그는 매우 복잡한 동적 시스템을 간단한 수학적 모델로 제한하였고 이 간단하고 단순한 방정식에서 나온 해답이 카오스적인 의미를 갖는다고 표시하였다. 이러한 표현은 상당히 충격적인 의미를 지닌다. 왜냐하면 일반적으로 대부분의 사람들은 복잡한 현상을 나타내는 것으로 되어 있다고 생각했는데 카오스이론은 아주 단순한 장치에서 복잡한 것을 도출할 수 있기 때문이다. 또한 1975년에 라이와 요크스는 "Period Three Implies Chaos"라는 제목의 논문을 발표하였고, 이 논문에서 카오스는 "결정적 비선형 동적시스템에서의 복잡한 현상" 이라고 정의하고 있다.[1]

본 연구에서는 생물의 개체수 변동에서 주기배가 분기(Period Doubling Bifurcation)는 결국 카오스 상태에 도달하는 것을 발견한 로버트 메이의 논리차이방정식(Logistic difference equation)을 이용한 LCI(Logistic Chaos Cryptosystrm Image)를 제안하고 블랜

드사의 델파이4.0의 프로그램을 이용하였다.

2. 이론적 배경

카오스 이론의 창시자는 프랑스 수학자 포앵카레(H. Poincaré)로, (1854~1912) 맨 처음 카오스이론을 이해한 과학 자 중 한사람이었다. 그는 카오스이론을 3개의 몸체문제에 제한하였고 이 시스템을 가지고 완전한 시스템을 구성할 수 없다는 것을 발견하였다. 그는 또한 호모클리닉 포인트, 포앙카레 맵, 연속 방정식, 고정점 이론, 바이퍼케이션이론 등과 같은 카오스현상 을 이해하기 위한 기본적 상황을 고려한 다양하고 중요한 개념들을 발견하였다. 특별히 그는 동적시스템의 시작점 이론을 가진 비선형시스템의 정성적 연구를 제안하였다. 포앙카레의 연구는 G.D.버크호프 (1884~1944)에 의해 계속 이어져 발진하였고 동적시스템에서 그의 이론이 큰 공헌을 하였다. 한편 카오스이론을 듣는 것으로부터 보는 형태로 시도를 한 사람은 반더폴 이다. 그는 진공관을 포함한 전기회로를 연구하였고 그 연구에서 주기적 더블링과 카오스로부터 기원된 이미 들은 소리를 스피커의 일 종인 전기회로의 출력으로 들을 수 있는 제품을 만들었다. 후에 M. L.카트라이트와 J.E리틀우드는 강제 항을 가진 2차계 비 선형 미분방정식의 해를 관찰할 수 있는 복잡한 행위를 발견하였다. L.레빈슨은 이들 방정식을 단순화하고 부분선형 모델을 제한 하였으며 그의 모델방정식을 결정적 2차계 부분선형 상미분방정식의 해로 해석하는 것을 보여주었다.

카오스 이론은 자연계에 존재하는 일정한 규칙을 가진 불규칙해 보이는 현상을 연구하는 학문으로서 카오스의 일반적인 정의는 첫째, 어떤 동력학계의 복잡하고 비주기적이며 유인적인 궤도이고 둘째, 주기성이 없는 일종의 질서이며 셋째, 새롭게 인식된 보편적인 자연현상 으로 넷째, 결정론적인 비선형 동력학계에 나타나는 불규칙적이고 예측 불가능한 형태 이다

미국의 기상학자인 로렌츠는 '초기값의 민감한 의존성' 즉 '나비효과'를 발견하였고 1975년에 요크(York)와 이천암은 처음으로 '카오스'를 결정적 비선형 동적시스템에서의 복잡한 현상이라고 정의하였다. 로버트 메이(Robert May)는 1975년에 생물의 개체수 변동을 수학적으로 처리함으로서 카오스 공학을 가전제품이나 진기기기 등에 이용하기 시작하였다[3]. 그 예로 비선형 회로에서의 카오스, 유체와 기체의 진동에서 발견되는 카오스(Acoustic Chaos), 광학에서의 카오스, 맥파, 뇌파, 심진도 등과 같은 생체 카오스, 주가지수와 같은 경제학에서의 카오스 등이 있다. 공학적인 응용 또한 활발히 이루어지고 있는데, 카오스 뉴럴 네트웍, 패턴 인식, 데이터 압축, 이미지 처리, 광학 시스템, Chaotic System 등이 있다.

자연속에서 일어나는 어떤 현상에서 일정한 규칙을 찾기위한 수많은 자료를 컴퓨터는 쉽게 처리할 수 있으며, 그 속에서 규칙을 찾아 함수로 만들고 시간의 변화에 따라 변하는 함수값을 이용하게 하는 것이다.

2.1. Logistic map

자연 현상들은 어떠한 동일한 법칙을 따라 발생과 변화를 거듭하고 있다. 이천암과 요크는 로렌츠의 3연립 미분 방정식을 사용한 연구에서 3개의 변수 중 하나의 변수의 움직임에만 주목하여 보았을 때 증가와 감소를 반복하며 복잡한 양상으로 변화하고 있는 그 변수의 최대값의 변동이 실제는 1차원 사상에 의해 생성된다는 사실을 밝혀냈다[4]. 로버트 메이는 시간의 변화에 따른 동물의 개체수 변화를 구하는 간단한 식을 통하여 이천암과 요크의 논문의 구체적인 연구결과를 발표하였다.

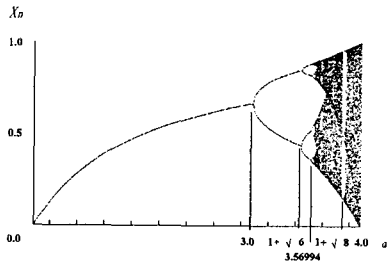
내년의개체수 = 번식률×(1-금년의 개체수)×금년의개체수

이러한 개체수를 모델화할 때에는 개의 상태를 0과 1사이로 나타내는데 1은 개체수의 최대수를 나타내고 0은 진멸을 나타낸다.

이 공식에서 (1 - 금년의 개체수) 라는 새로운 항을 통하여 개체수의 변화법칙에 있어서 비선형성이 있음을 알 수 있다. 즉, 단순히 '내년의 개체수 = 번식률 × 금년의 개체수' 라고 한다면, 번식률이 1보다 클 경우에는 개체수가 무제한으로 증가할 것이고, 1보다 작은 경우는 개체수가 0으로 수렴하는 극단적인 결과가 나타나게 된다. 그러므로 '번식률 × (1- 금년의 개체수)'를 곱함으로써, 내년의 개체수는 금년의 개체수에 의존하여 결정된다는 것을 알 수 있다. 이것을 다음의 로지스틱 방정식으로 나타낼 수 있다[5].

$$X_{n+1} = \alpha X_n(1-X_n)$$

α는 개체수의 증가량이며, Xn은 금년의 개체수, X_{n+1} 은 내년의 개체수이다. 위의 로지스틱 방정식에서 X_n 에서 X_{n+1} 로의 변화를 논리사상 (logistic map)이라 한다. α의 값이 크다면 개체수가 적을 때는 빠른 속도로 증가하고 작다면 빠른 속도로 감소함을 나타낸다. 이러한 값의 변화는 매개변수 α의 값에 따라 다른 양상을 타나낸다. <그림 1>는 X_1=0.04일 때 매개변수 α에 따른 개체수의 변화를 쉽게 알 수 있도록 나타낸 Feigenbaum 분기도이다.



<그림 1> Feigenbaum 분기도

위의 Feigenbaum 분기도를 통하여 매개변수 α에 따르는 몇 가지 특징을 발견할 수 있다.

(1) $0 < \alpha <= 1$ Xn은 0으로 수렴
(2) $1 < \alpha <= 2$ Xn은 1 -(1 / a)로 수렴
(3) $2 < \alpha <= 3.5699$ Xn는 주기배가 상태
(4) $3.5699 < \alpha$ Xn 는 혼돈 상태

3. 암호화

암호(Cryptography)라는 것은 전자상거래를 안전하고 효율적으로 이루어지도록 해주며 확실한 믿음을 갖도록 한다. 정보의 의미를 당사자 이외에는 알지 못하게 정보를 변환시키는 것이다. 암호화를 수행하는 방법은 대치암호시스템(substitution cryptosystem)과 진치암호시스템(transposition cryptosystem)의 전통적인 암호화 방법, 암호키와 복호키가 같은 대칭키 암호화 방법과 서로 다른 공개키 암호화 방법이 있다.

암호화키와 복호화키를 총칭하여 암호키(Cryptographic Key) 혹은 키(Key)라 한다[6].

현대 암호는 암호의 안전성을 암호키에 귀착시키고 있기 때문에 그 키를 알지 못하면 암호 알고리즘을 알고 있다 하더라도 평문을 얻기가 어렵다. 현재 많은 암호 알고리즘이 있으며, 평문을 암호문으로 변환하는 여러 가지 알고리즘 중에서 전통적인 암호알고리즘. DES(Data Encrypion Standard) 암호알고리즘, ECC(Elliptic Curve Cryptography) 암호알고리즘, RSA(Rivest, Shamir, Adleman) 암호알고리즘 ,LUC 수열 기반 암호알고리즘, Knapsack 암호알고리즘 등이 있다.

오래전 부터 사용되어온 전통적인 암호 시스템으로 대치암호 시스템, 진치암호시스템 등이 있다. 이러한 시스템은 암호화의 속도가 빠르고, 알고리즘기법이 간단하다는 장점이 있지만 해독이 쉽기 때문에 안전성에 문제가 있다[12][13].

대치 암호 시스템은 1차 대진낭시 사용되던 영국의 Lyon Playfair와 C. Wheatston 이 1854년 에 발표한 Playfair 암호시스템이 있다. 이시스템은 원문과 암호문의 구성요소를 1:1로 대응시켜 치환시키는 방법으로서 임의의 키를 첨가하고 알파벳을 재배치하여 만드는 방법과 알파벳 순서를 n 자리씩 이동시켜 만드는 방법이 있다. 진치 암호 시스템은 평문의 문자를 재배열하여 암호문을 만드는 방법으로 암호문의 문자 출현빈도가 평문의 문자 출현빈도와 같으며, 평문의 문자가 암호문에 그대로 사용하게 된다.

DES 암호 기법은 1977년 IBM의 Water Tuchman 과 Carl Me미국 상무성의 표준국(NBS : National Bureau of Satandards)에 의해 미 연방정보처리표준46(FIPS PUB46)으로 채택되었으며. 1983년

ISO(International Standardization Organization)에서 표준안으로 채택되었다. 이 표준안은 재검토 과정을 거치면서 현재의 알고리즘이 되었으며 특히 금융분야에 많이 사용되고 있다.
DES는 56비트의 키를 사용하며 16단계의 단일 반복 과정을 거쳐 64비트의 암호문 출력을 내는 Feistel 구조를 갖는다. 복호화 시에는 동일한 키를 사용하여 암호화의 역순으로 수행된다. 초기의 128비트의 키 길이로 설계되었던 DBS는 NSA에 의해 56비트로 키 길이가 줄어든 이후 꾸준히 키 길이에 대한 논쟁이 있어 왔으며 컴퓨팅 파워가 증가하고 네트워크 기술이 발달 하면서 DBS에 대한 다양한 공격이 시도되어 왔다.

DES는 암호화 단계가 세 단계로 진행된다[6]. 첫 단계는 64비트 평문의 치환된 입력을 생성하기 의해 비트열의 순서를 재조정하는 초기순열(IP : Initial Permutation)단계를 통과한다. 두 번째 단계는 라운드 함수의 16회 반복 단계가 수행되는데 순열과 치환 모두가 포함된다. 마지막(16번째) 반복 처리의 출력은 입력 평문과 키의 함수 결과인 64비트로 구성된다. 이 64비트 출력의 좌우 절반은 예비 출력을 생성하기 위해 좌우로 교환된다. 세 번째 단계는 예비출력의 64비트 암호문 생성을 위해 초기 순열의 역인 역 초기 순열(IP-1)을 통과한다.

RSA 암호는 1978년 MIT의 R. Rivest, A. Shamir, 그리고 L. Adleman에 개발되었다. RSA 암호는 수년 동안에 제안된 모든 공개키 알고리즘 중에서 이해 및 구현하기가 가장 용이한 알고리즘으로 평가받고 있다. 또한 이 알고리즘은 가장 대중적으로 알려졌으며, 아직까지 수많은 암호분석을 이겨내고 있다. RSA 암호의 구조는 지수승을 가진 수식을 사용하도록 만들고 있다. 공개키 암호화 과정은 넷 가지 단계를 가진다.[6] 첫째 네크워크상에서 각 시스템들은 수신할 메시지의 암호화와 복호화에 사용되는 한 쌍의 키를 생성한다. 둘째 시스템은 공개 기록집 또는 공개 파일에 암호키를 공개한다. 이것이 공개키이다. 또 다른 키는 비밀키로 개인이 가지고 있다. 세째 만일 A가 메시지를 B에게 보내길 원한다면 B의 공개키를 사용해 메시지를 암호화하여 보낸다. 넷째 B가 비밀키를 알지 못하기 때문에 암호문을 복호화 할 수가 없다.

3.1. Chaos Cryptosystem

카오스 암호는 카오스 신호를 이용하여 정보를 암호화 하는 기술로서 암호화 및 복호화 단계가 카오스적이라는 본질적 이유 때문에 수학적 방식으로는 절대로 풀리지 않는다고 알려져 있다. 일본등에서는 카오스 암호기술을 이용한 상품이 소개되고 있는 실정이다[7].

일본 동경 소재 국제 정보 과학 연구소(IISI, 중국), 일본 고오찌대학, 미해군연구소와 조지아공대등에서 카오스 이론에 근거한 통신 및 암호화 기술에 관한 연구가 진행되어 왔으며, 상용화 제품도 제공하고 있다.

미국은 카오스 통신분야에서, 일본과 중국은 카오스 암호 분야에서 기술적 우위를 보이고 있으며, 국내의 기술수준은 아직 이들과는 비교할 수 없는 초보 단계로 매우 열악한 상태이다. IISI의 GCC 암호기술과 이를 응용한 Chaos-mail, Chaos-inforguard, Chaos- remocon등의 제품이 발표되어 있으며, 이들 제품은 일반적으로 몇 가지 매우 강력한 기능을 제공하고 있다.

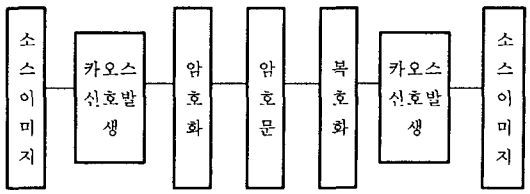
첫째, 공개키 방식과 대칭형 방식에 대한 대체 기술로서의 가능성을 가지고 있으며 둘째, 가변형 키와 카오스 신호를 이용함으로서 최고의 신뢰성 보장한다. 셋째, 암호화, 복호화에 따르는 Speed_Up 이고 넷째, 멀티미디어 데이터에 대한 암호화가 가능하며 통신에 적용할 수 도 있다.

4. LCI(Logistic Chaos Cryptosystem Image)

4.1. LCI의 구현

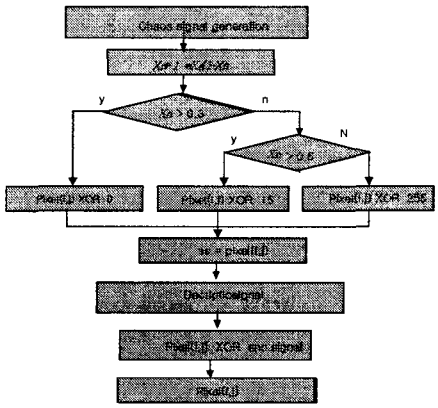
본 연구에서는 로버트메이의 논리차이방적식(Logistic difference equation)을 이용하여 특정한 이미지를 암호화 할 수 있도록 하는 LCI(Logistic Chaos Cryptosystem Image)을 제안한다.

본 연구에서의 암호화 과정을 그림으로 나타내면 다음과 같다.



<그림 2> LCI의 구조도

두 번의 카오스 신호의 발생으로 암호화와 복호화가 일어난다.

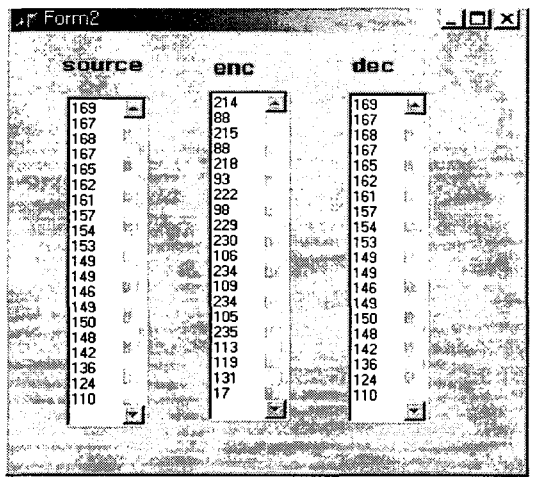


<그림3> 알고리즘

알고리즘은 로지스틱맵의 식에서 r=3.4일때, 카오스현상이 발생된다.

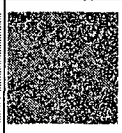
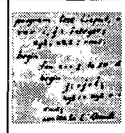
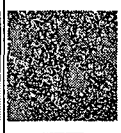
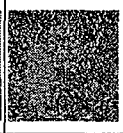
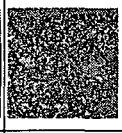
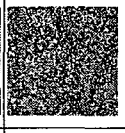
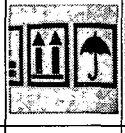
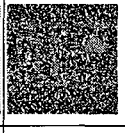
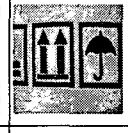
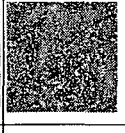
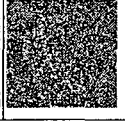
X_N 은 각 픽셀에 XOR시킬 값을 결정하기 위해 픽셀수 만큼 배열을 생성하고 pixel의 수는 여러 가지 형태로 구분된다.

만약 X_N 에 있는 값이 0.3 보다 클 경우에는 0 로 XOR시키고 0.6 보다 크면 15로 XOR 시키고 그렇지 않으면 255를 ss 에 저장한다. 복호화는 각 픽셀의 값을 구하고 ss 에 저장된 값을 XOR시켜서 이루어진다.



<그림 4> LCI를 이용한 Encrypting/Decrypting

<그림 4>에서 나타난 것은 이미지의 픽셀 수치를 특정한 부분을 잘라서 표현한 것인데, 전체의 픽셀값은 0 - 255 까지 표현이 되고 소스의 픽셀 값은 암호화 했을 때 전혀 다른 픽셀값을 가지며 다시 복호화 했을 때는 소스값과 100% 똑같은 값을 가진다.

번호	원문	암호화	복호화
1			
2			
3			
4			
5			
6			
7			
8			

<그림5> 이미지 암호화 복호화

4.2. 결과

실험에서 로버트메이의 논리차이방적식(Logistic difference equation)을 이용한 LCI(Logistic Chaos Cryptosystem Image)은 Logistic map 에서 보는 것과 같이 이미지로 Encrypting 되었으며, 암호화된 암호이미지는 다시 Decrypting되었다.

이때, Encrypting 과정에서 이미지는 카오스 신호에 의해 암호화되어 카오스 상태를 유지하고 있으며, 소스 이미지와 암호이미지 사이에는 어떠한 관련성도 찾아 볼 수 없었다.

픽셀	픽셀전체	바뀐픽셀	이미지와복호화
1	16384(128x128)	16384	100%
2	25600(160x160)	25600	100%
3	65025(255x255)	65025	100%
4	48400(220x220)	48400	100%
5	11025(105x105)	11025	100%
6	21025(145x145)	21025	100%
7	10404(102x102)	10404	100%
8	34596(186x186)	34596	100%

<표 1> 전체 픽셀 수치비교

예를 들어 소스 이미지의 각 픽셀 수치와 암호화된 이미지의 수치를 비교했을 때 100% 의 서로 다른 수치로 표현되었다.

5. 결론

본 연구에서 제시한 LCI 카오스 암호기법은 카오스를 응용한 암호화 기술과 함께 연구가 계속되고 있으며, 이 같은 변화는 카오스 암호기술이 대칭형 암호기술의 완벽한 대안으로 부각되는 것과 함께 공개키 암호기술의 대안이 될 수 있는 새로운 암호기술임을 의미하는 것이다.

국내에서도 카오스 신호 발생[8]에 관한 연구나 카오스를 이용한 암호의 특성분석[9]과 같은 카오스 응용 연구가 활발히 진행되고 있다.

미국, 일본등의 연구기관과 대학 또는 일부 외국기업들은 이미 우수한 기술을 확보하고, 상품화등에 응용하고 있는 것으로 알려지고 있다. 이 같은 연구가 지속적으로 계속되어, 카오스 암호의 안전성이 확보 된다면 현재 이용되고 있는 여러 암호기술들과도 충분히 경쟁 할 수 있는 여건이 충족될 수 있을 것이다.

앞으로 카오스 암호화에 관한 기존의 연구[10]를 바탕으로 암호화의 안전성이나 처리속도 등에 대한 검증이나 표준화 문제, 멀티미디어 자료 등에 대한 암호화 기법도 함께 연구함으로서 카오스 암호기법이 실제 보안 시스템에 적용될 것이다.

참고문헌

[1] Stempen H. Kellert, '카오스란 무엇인가', 범양사, p22-47, 1995

[2] 김철 : 암호학의 이해, 영풍문고 1996

[3] 아이하라 키즈유키, '쉽게 읽는 카오스', 한뜻출판사, p89-100,1995

[4] 도다 모리가즈, '카오스 혼돈속의 법칙', 대광서림, p90-99, 1993

[5] Hao Bai-lin, 'Chaos II', Worla secientific, 1990

[6] 강재석,보안과 암호화 기술, http://myhome.netsgo.com/xmulder/kfirst.html

[7] 원동호 암호학 한국정보과학회 정보통신연구회 학회지1권 p 72-81

[8] 양일석, '혼돈회로구현', 전자과학, p284-291, 1995,12

[9] won H. Lee, jong U. Choi, dae G. Kim, 'Fractal Analysis for Linearity on Cryptography Algorithms', http://www.knouk.co.kr/~wanna/cryptography/security.html

[10] D.R. Stinson : Cryptography Prentie Hall 1989.

[11] B.Schneir : Applied Cryptography, John & Sons, Inc.1996

[12] Thomas S. Parker, Leon O. Chua, "Chaos: A Tutorial for Engineers", Proceedings of the IEEE Vol.75 No.8, pp 982, 1987

[13]정성용, 김태식 카오스 특성을 이용한 스트림 암호 시스템의 키 수열 생성 기법, ' 99 추계공동학술대회 논문집, N/A, Vol. 0, pp. 113-119 , 한국정보진략학회, 1999