카오스 이론을 이용한 암호화 기법

정성용[O], 김태식[1]
[O] 계명대학교 대학원 전자계산학과
[1] 계명대학교 컴퓨터전자공학부 교수

Encrytion Method Based on the Chaos Technique

Jung, sung-yong, Kim, Tae-sik
Dept. of Computer Engineering, Keimyung University

요 약

본 연구에서는 로버트 메이의 논리차이방정식(Logistic difference equation)을 이용하여 ASCII 코드로 만들어진 문서를 암호화 할 수 있도록 하는 카오스 LCC(Logistic Chaos Cryptosystem)을 제안한다. 카오스를 이용한 암호화 기법은 기존의 암호화 기법으로 알려진 DES(Data Encrypion Standard)나 RSA(Rivest,Shamir,Adleman)등과는 비교되는 기법으로 초기 조건에 민감한 카오스의 특징을 이용하였다.

실험결과 제안된 LCC 기법을 통해 암호문은 카오스적으로 표현되었으며, 원문과 암호문 사이에 어떠한 관련성도 찾아 볼수 없었다. 향후 안전성이나 처리속도에 대한 검증과 표준화 문제 및 멀티미디어 자료등에 대한 암호화 기법을 계속 연구해야 할 것이다

1. 서 론

최근 카오스 이론의 등장으로 다양한 분야에서 새로운 관점의 문제 해결법을 제시하여 주고 있다. 기존의 공학적인 문제 해결은 결정론적인 사고에 지배를 받아왔으나 이러한 문제 해결법은 비결정론적인 사고와는 괴리가 있다 이것은 태양계의 운동 법칙으로 수백년 후의 일식과 월식의 시간은 정확히 계산하면서도 1미터 위에서 떨어지는 나뭇잎의 운동 방향은 계산하지 못하는 것을 통해 알 수 있게 된다 비결정론에 의해 일어나는 여러 현상을 결정론에 의해 일어나는 현상으로 생각하고 그 속에서 일정한 규칙을 찾아 응용하는 것이 카오스 연구의 목적이라 할 수 있다

자연현상에서 흔히 관찰되는 여러가지 현상들이 오랜 노력에도 불구하고 규명하기 곤란했었으나, 로렌츠(Lolenz)의 연구이후 자연의 복잡성속에 숨어 있는 규칙성 및 질서를 찾아 내고자 하는 노력이 매우 활발해 지고 있다 1963년 로렌츠는 '결정론적인 비주기성 흐름'이란 논문에서는 '초기조건에 민감한 의존성'을 표현하는 비주기성 개념을 발전하여 로렌츠 어트랙트(Atractor)라 불리는 나비효과와 같이 겉으로는 무질서해 보이지만 내면에는 놀라운 규칙성을 갖고 있는 현상이 존재하고 있음을 밝혔다.

공학에서의 카오스 응용은 한정된 영역에서 비선형적인 현상을 규명하고자 하는 시도로서 결정론적 카오스(deterministic chaos)에 기반한 연구를 바탕으로 결정론적 비선형 동역학 시스템(Deterministic Nonlinear Dynamic System)이나 불안정한 비주기적 운동을 정성적으로 해석하는 연구, 음성인식, 패턴인식, 카오스 통신이나 회로등의 공학응용에 활발한 연구가 진행되고 있다

본 연구에서는 초기 조건에 민감한 의존성을 보이고 있는 카오스 이론을 이용한 응용분야의 하나로 최근 국내외의 연구가 활발한 카오스 암호화 기법을 제시하고자 한다 카오스를 이용한 암호화 기법은 기존의 암호화 기법으로 알려진 DES(Data Encrypion Standard)나 RSA(Rivest, Shamir, Adleman)과는 비교되는 기법으로 초기 조건에 민감한 카오스의 특징을 이용함으로서, 어떤 형태의 공격에도 안전할 것으로 기대된다[2].

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 LCC(Logistic Chaos Cryptosystem)을 제안한다

2. 카오스 이론

2.1. 카오스 이론의 개요

공학적 측면에서볼 때 카오스 이론은 결정론적 비선형 동역학 시스템(deterministic nonlinear dynamic system)을 다루는 학문이다 카오스 이론의 창시자는 프랑스 수학자 포앵카레(H. Poincaré)로, 그는 간단한 결정론적 방정식에서 예측 불가능한 비결정론적 해를 얻어냄으로써 결정론적 시스템은 예측 가능하다는 고전적인 개념을 뒤집어 놓았다. 카오스 이론은 1960년대에 등장한 이후 계속적인 연구를 통해 현대과학의 새로운 장을 열어가고 있다.

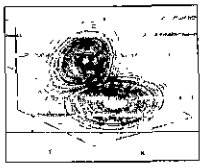
카오스 이론은 자연계에 존재하는 일정한 규칙을 가진 불규칙해 보이는 현상을 연구하는 학문으로서 카오스의 일반적인 성의는 다음과 같다

① 어떤 동력학계의 복잡하고 비주기적이며 유인적인 궤도
② 주기성이 없는 일종의 질서
③ 새롭게 인식된 보편적인 지연현상
④ 결정론적인 비선형 동력학계에 나타나는 불규칙적이고 예측 불가능한 형태

미국의 기상학자인 로렌츠는 <그림 1>의 '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 가진제품이나 전기기기 등에 이용하기 시작하였다[3]. 그 예로 비선형 회로에서의 카오스, 유체와 기체의 진동에서 발견되는 카오스(Acoustic Chaos), 광학

에서의 카오스, 맥파, 뇌파, 심전도 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

$$x_1 = \alpha(x_2 - x_1)$$
$$x_2 = \Gamma x_1 - x_2 - x_1 x_3$$
$$x_3 = -\beta x_3 + x_1 x_2$$



<그림 1> 로렌츠 방적식과 로렌츠 어트렉트

카오스 시스템은 랜덤 행위(Random Behavior)를 나타내는 결정론적 시스템(Deterministic System)이라고 할 수 있다 또한 이상 행동(Strange behavior) 이라고도 불리는 카오스는 최근에 비선형 시스템 연구분야의 가장 흥미있는 것 분야의 하나가 되고 있다[11].

특히 초기조건에의 민감한 의존성(Sensitive Dependence on Initial Condition)으로 대표되는 카오스 이론은 주기성(Periodicity), 프랙탈(Fractal), 바이퍼케이션(Bifurcation), 간헐성(Intermittency) 등의 새로운 용어를 만들어 냈다

카오스 이론은 짧은 역사 속에서 편력된 분야의 학자들이 많은 연구를 하였지만 이론에 많은 비중을 두어 실제적인 응용분야는 거의 발달하지 못하였다. 그러나 최근 컴퓨터의 처리 능력 향상과 인공지능의 학문적인 이론과 응용기술의 발달로 카오스 이론이 신산학 분야에 새로운 관심사로 등장하기 시작하였다 즉 자연속에서 일어나는 어떤 현상에서 일정한 규칙을 찾기위한 수 많은 자료를 컴퓨터는 쉽게 처리할 수 있으며, 그 속에서 규칙을 찾아 함수로 만들고 시간의 변화에 따라 변하는 함수값을 이용하게 하는 것이다.

2.2. Logistic map

자연에서 발생하고 있는 현상들은 어떠한 동일한 법칙을 따라 발생과 변화를 거듭하고 있다 이천암과 요크는 로렌츠의 3연립 미분방정식을 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]. 로비트 메이는 시간의 변화에 따른 동물의 개체수 변화를 구하는 간단한 식을 통하여 이천암과 요크의 논문의 구체적인 연구결과를 발표하였다

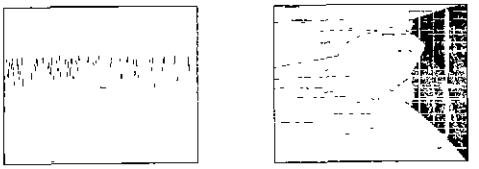
내년의개체수 = 번식률×(1-금년의 개체수)×금년의개체수

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 나타낸다 [1] 다음 <그림 2>는 X_1=0.04일 때 매개변수 α에 따른 개체수의 변화를 쉽게 알 수 있도록 나타낸 Feigenbaum 분기도이다



<그림 2> 개체수의 변화와 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 정보의 의미를 당사자 이외에는 알지 못하게 정보를 변환시키는 것이다 암호화는 암호화키(Encryption Key)라는 파라미타에 의존한 변환이다 당사자가 암호화키에 대응하는 복호화키(Decryption Key)를 이용하여 암호문을 본래의 평문으로 변환시키는 것은 복호화(Decryption, Deciphering)라 한다 암호과와 복호화의 전과정을 총칭하여 암호 시스템(Cryptosystem)이라 하고, 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 그 분류의 관점도 여러 가지가 있으며, 가장 일반적으로 알려진 알고리즘으로는 DES(Data Encryption Standard)나 RSA(Rivest, Shamir, Adleman)등이 있다

3.1. DES

현재 가장 널리 사용되는 암호 기법은 1977년 미국 표준국(NBS : National Bureau of Satandard, 현 NIST의 전신)에 의해 미 연방정보처리표준46(FIPS PUB46)으로 채택된 DES에 기초를 두고 있다 비밀키 암호의 대명사인 DES는 64비트 입력을, 56비트 키를 이용하여 64비트 출력으로 변환한다. 복호화에는 동일한 키를 사용하여 동일한 단계가 암호화의 역순으로 사용된다

DES는 암호화 단계가 세단계로 진행된다[6]

(1) 64비트 평문의 치환된 입력을 생성하기 의해 미드열와 순서를 재조정하는 초기순열(IP Initial Permutation)단계를 통과한다.

(2) 다음에 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 에비 출력을 생성하기 위해 좌우로교환된다

(3) 이 에비출력은 64비트 암호문 생성을 위해 초기 순열의 역인 역초기 순열(IP-1)을 통과한다

3.2. RSA

공개키 암호는 비밀키 암호에서의 문제점들을 해결하고자 하는 시도로부터 발전된 개념이다 RSA암호는 MIT의 R.Rivest, A.Shamir, 그리고 L Adleman에 의해 1977년에 개발되었다 RSA 암호는 이후 널리 사용되게 되었고 공개키 암호를 위한 접근 방법에 응용되었다. RSA 암호의 구조는 지수승을 가진 수식을 사용하도록 만들고 있다 공개키 암호화 과정은 다음과 같다[6]

(1) 네크워크상에서 각 시스템들은 수신할 메시지의 암호화와 복호화에 사용되는 한 쌍의 키를 생성한다

(2) 시스템은 공개 기록집 또는 공개 파일에 암호키를 공개한다 이것이 공개키이다 또 다른 키는 비밀키로 개인이 가지고있는다

(3) 만일 A가 메시지를 B에게 보내길 원한다면 B의 공개키를 사용해 메시지를 암호화하여 보낸다

(4) B가 비밀키를 알지 못하기 때문에 암호문을 복호할 수가 없다

4. LCC(Logistic Chaos Cryptosystem)

4.1. Chaos Cryptosystem

카오스 암호기술은 카오스 신호를 이용하여 정보를 암호화 하는 기술로서 암호화 및 복호화 단계가 카오스적이라는 본질적 이유 때문에 수학적 방식으로는 절대로 풀리지 않는다고 알려져 있으며, 이 같은 연구가 미국, 일본, 중국 등에서 계속되고 있으며, 지금까지 알려진 어떤 암호 기술 보다도 완벽하고, 안전하다는 결론을 얻어 놓고 있으며, 일본등에서는 카오스 암호기술을 이용한 상품이 소개되고 있는 실정이다[7].

일본 통상 산제 국제 정보 과학 연구소(IISI. 중국), 일본 고오찌대학, 미해군연구소의 조지아공대등에서 카오스 이론에 근거한 통신 및 암호화 기술에 관한 연구가 진행되어 왔으며, 상용화 제품도 제공하고 있다 그러나, 국내에서는 이와 관련된 연구가 거의 전무한 실정이며, 하루빨리 이 분야에 대한 연구가 활발히 이루어지야 할 것이다

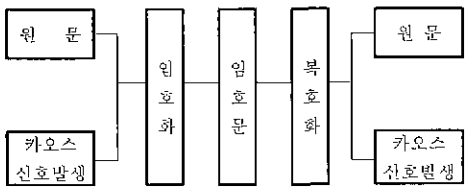
일반적으로 미국은 카오스 통신분야에서, 일본과 중국은 카오스 암호 분야에서 기술적 우위를 보이고 있으며, 국내의 기술수준은 아직 이들과는 비교할 수 없는 초보 단계로 매우 열악한 상태이다. IISI의 GCC 암호기술과 이를 응용한 Chaos-mail, Chaos-inforguard, Chaos- remocon등의 제품이 발표되어 있으며, 이들 제품은 일반적으로 다음과 같은 매우 강력한 기능을 제공하고 있다.

① 공개키 방식과 대칭형 방식에 대한 대체 기술로서의 가능성
② 가변형 키와 카오스 신호를 이용함으로서 최고의 신화성 보장
③ 암호화, 복호화에 따르는 Speed_Up과 실용성 보장
④ 멀티미디어 데이터에 대한 암호화
⑤ 통신에 적용할 수 있는 표준화

4.2. LCC의 구현

본 연구에서는 로비트 메이의 논리차이방적식(Logistic difference equation)을 이용하여 ASCII 코드로 만들어진 문서를 암호화 할 수 있도록 하는 LCC(Logistic Chaos Cryptosystem)을 제안한다

본 연구에서의 암호화 과정을 그림으로 나타내면 다음과 같다



<그림 3> LCC의 구조도

제안된 암호화 기법을 이용하여 다음 문장을 암호화 한 과정을 보면 다음과 같다

(예문 - 원문)
This is the test of logistic chaos cryptosystem

(예문 - ASCII Code)
84 104 105 115 (32)
105 115 (32)
116 104 101 (32)
116 101 115 116 (32)
111 102 (32)
108 111 103 105 115 116 105 99 (32)
99 104 97 111 115 (32)
99 114 121 112 116 111 115 121 115 116 101 109

(암호문 - ASCII code)
103 165 226 140 (107)
223 150 (127)
208 202 187 (139)
183 222 139 190 (150)
145 196 (127)
200 208 191 209 219 190 223 132 (125)
195 195 196 196 223 (96)
220 137 193 231 146 197 222 188 236 140 175 227

(결과 - 복문)
This is the test of logistic chaos cryptosystem

<그림 4> LCC를 이용한 Encrypting/Decrypting

4.3. 결과

실험에서 로버트메이의 논리차이방적식(Logistic difference equation)을 이용한 LCC(Logistic Chaos Cryptosystem)은 Logistic map에서 보이는 것과 같은 혼돈 상태를 유지하는 코드로 Encrypting 되었으며, 암호화된 암호문은 평문으로 다시 Decrypting되었다

이때, Encrypting과정에서 원문은 카오스 신호에 의해 암호화되어 카오스 상태를 유지하고 있으며, 원문과 암호문과는 어떠한 관련성도 찾아 볼 수 없다 예를들어 원문에서 (32)로 나타나는 (Space)는 암호문에서 (107), (127), (139)등으로 나타 났으며, 이 값들은 다시 카오스 신호에 의해 정확히게 원문으로 Decrypting되었다.

5. 결론

본 연구에서 제시한 LCC 기법과 같이 카오스를 응용한 암호화 기술은 카오스 통신 기술과 함께 연구가 계속되고 있으며, 현재 일본등지에서는 일부 보안 시스템등에 상용화되어 사용되고 있다 이같은 변화는 카오스 암호기술이 대칭형 암호기술의 완벽한 대안으로 부각되는 것과 함께 공개키 암호기술의 대안이 될 수 있는 새로운 암호 기술임을 의미하는 것이다

국내에서도 카오스 신호 발생[8]에 관한 연구나 카오스를 이용한 암호의 특성분석[9]과 같은 카오스 응용 연구가 활발히 진행되고 있으나, 암호화에 관련된 만족할 만한 결과를 얻고 있지는 못하고 있다

일본, 미국등의 연구기관과 대학 또는 일부 외국기업들은 이미 우수한 기술을 확보하고, 상품화등에 응용하고 있는 것으로 알려지고 있으나, 암호화 기술이나 제품이 국가적인 규제에 묶여 공개되고 있지 않은 상황에서 본 연구는 암호화 연구에 대한 새로운 대안으로 기대를 줄수 있을 것으로 생각된다 또한, 이같은 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 신호의 발생과 암호화에 관한 기존의 연구[10]를 바탕으로 암호문의 안전성이나 키리속도등에 대한 검증이나 표준화 문제, 멀티미디어 자료등에 대한 암호화 기법도 함께 연구함으로서 카오스 암호기법이 실제 보안 시스템에 적용할 수 있도록 할 계획이다

참고문헌

[1] Stempen H Kellert, '카오스란 무엇인가', 범양사, p22-47, 1995
[2] IISI, 'Encryption for meultimedia age GCC Overview', http://www.iisi.co.jp/research/GCC-over.html, 1996
[3] 아이히라 키즈유키, '쉽게 읽는 카오스', 한빛출판사, p89-100,1995
[4] 도디 모리가즈, '카오스 혼돈속의 법칙', 대광서림, p90-99, 1993
[5] Hao Bai-lin 'Chaos II', World scientific, 1990
[6] 장재석, '보안의 암호화 기술', http://myhome.netsgo.com/xmulder/kfirst.html
[7] http://www.iisi.co.jp/kenkyuu.html
[8] 양일식, '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] http://bugs.wpi.edu:8080/ee535/hwk7cd95/alwesh/node5.html, 'Chaostic Digital encoding', 1995
[11] Thomas S Parker, Leon O Chua, "Chaos A Tutorial for Engineers", Proceedings of the IEEE Vol 75 No 8, pp 982, 1987