카오스에 기반을 둔 암호화 알고리즘의 구현

이 윤 수*, 이 기 철**, 김 동 준**, 박 정 남**,이 종 혁**

*경성대학교 멀티미디어정보예술대학원 정보공학과

**경성대학교 컴퓨터공학과

An Implementation of Encryption Algorithm based on Chaos

Yun-Soo Lee, Ki-Chul Lee, Dong-Jun Kim, Jung-Nam Park, Jong-Hyeok Lee

Kyungsung University

요 약

최근 해킹으로 인한 개인정보유출이 사회적으로 큰 문제가 되고 있다. 이러한 해킹의 강력한 대응 방법중의 하나인 암호화를 통해 개인의 정보유출을 방지하거나 안전도를 높일 수 있다.

이에 본 연구에서는 카오스 알고리즘을 이용한 암호화 방법을 제안한다. 이 카오스 알고리즘은 기존의 암호화 알고리즘인 DES, RSA와 비교되는 알고리즘으로 초기조건에 따라 완전히 다른 결과를 내는 카오스의 특징을 이용하였다.

주요어 : 카오스, 암호, 복호, 로지스틱, 멀티미디어,

I. 서 론

컴퓨터의 보급이 확대되고 정보통신 기술이 발달함에 따라 일반가정에선 초고속통신이, 각종 기관 및 단체에서는 LAN이 활발히 보급되고 있으며 이런 통신망을 통한 개인 및 공공기관의 주요 정보에 대한 위협이 증가되고 있다. 따라서 정보의 불법 유출, 삭제, 수정 등에 대한 적절한 보호 조치가 없다면 이런 불법적인 사고로 인하여 개인 사생활 침해뿐만 아니라 막대한 경제적 손실을 가져올 수 있다. 정보의 위조나 불법수정 및 탈취에 대한 정보 보호 기술 중에는 여러 가지가 있으나 대표적으로 암호 시스템을 통한 정보의 안전한 전달이 가장 대표적이라 할 수 있다.

암호시스템의 구현을 위한 암호 알고리즘, 즉, 제 삼자가 알 수 없도록 우리가 주고받는 정보를 암호화하는 연구가 활발히 진행되고 있다. 이러한 암호알고리즘과 운영방식은 시대에 따라 변화하고 있으며 다음과 같이 분류할 수 있다. 암호시스템은 암호화 복호화 시에 쓰이는 키가 같은지 다른지 여부에 따라 동일한 키를 사용하는 관용키 암호 시스템이 있으며 일명 비밀키 암호시스템이라고도 불린다. 비밀키 암호시스템방식인 DES(Data Encryption Standards) 알고리즘 같은 경우는 아주 효과적인 해독법인 LC(Linear Cryptoanalysis)나 DC(Differential Cryptoanalysis)로 인해 적정한 암호화 정도를 유지하기 위해선 상당히 높은 비트수의 키를 필요로 하므로 시간이 어느 정도 걸린다.[10] 두 번째는 서로 다른 키를 사용하는 공개키 암호시스템이다. 기존의 공개키 암호시스템 방식중 대표적인 RSA(Rivest, Shamir, Adleman)는 DES에 비하여 강력한 보안정도를 유지하나 암호문의 크기가 평문에 비해 대략 9배정도 커지며, 속도가 아주 느리다는 단점이 있다.[1]

공학에서의 카오스 응용은 한정된 영역에서 비선형적인 현상을 규명하고자 하는 결정론적 비선형 동역학 시스템(Deterministic Nonlinear Dynamic System)이나 불안정한 비주기적 운동을 정성적으로 해석하는 연구, 카오스 통신이나 회로등의 공학응용에 활발한 연구가 진행되고 있다. 카오스 알고리즘은 초기조건에 민감한 의존성을 보이고 있으며 시간에 따라 그 값이 달라지는 특성으로 인하여 많은 사람들이 암호화에 이용하려고 하고 있다.[2]

그러나 대부분의 연구는 텍스트의 암호화에만 적용되고 있으므로 현재 많이 사용되고 있는 멀티 미디어 정보에는 적용할 수 없는 문제가 있다.

본 연구에서는 기존의 암호화 기법으로 알려진 DES나 RSA보다 변화의 정도가 상대적으로 큰 ELM(Expanding Logistic Map)을 제안하고 이를 이용하여 텍스트뿐만 아니라 멀티미디어 정보에서도 암호화가 될 수 있음을 보이고자 한다.

II. 기존 암호화 알고리즘

2.1 DES

DES는 미국 IBM에서 1974년 전치 및 대치암호

화 방식을 혼합한 형태로 개발되었으며 1977년에는 미국정부의 표준 암호화 방식으로 채택된 이후 ANSI(American National Standards Institute), ISO(International Standards Organization)에서도 표준안으로 채택되어 널리 사용되고 있는 암호화 알고리즘으로 1라운드를 16번 반복하는 구조로 구성되어 있으며, 암호화는 라운드의 동일한 동작 과정의 반복으로 이루어진다. 복호화는 암호화 과정과 동일하나 사용되는 키만 역순으로 적용하면 된다. DES는 운영, 관리가 쉽고 Key의 설정이 용이하여 규칙적으로 변경해도 암호문에는 영향이 나타나지 않으며, 암호화와 복호화과 쉽다는 장점도 있지만 Key의 관리 및 전송이 어려운 단점이 있다.

2.2 RSA

RSA 전자서명 알고리즘은 1978년 Rivest, Shamir, Adleman이 제안한 RSA 공개키 암호 시스템을 이용한 전자서명 방식으로 공용키/비밀키를 가지는, 비대칭 키 암호화 알고리즘의 대표주자격인 알고리즘이다. 입력방식은, 블록 단위로 이루어지는데 블록 사이즈는 2^k 이고, 알고리즘에서 중요한 역할을 하는 n 이라는 숫자의 범위는 $2^k < n < 2^{k+1}$ 이다. RSA 에서는, 입력을 숫자로 본다. 일반적으로 RSA 공개키 암호의 안전성은 두 개의 큰 소수 p 와 q의 합성수 n = p*q을 소인수 분해 하는 문제의 어려움에 의존한다. 즉, 공격자가 공개키 {e, n}으로부터 개인키 d를 도출해 내기 위해서는 n을 p와 q로 소인수 분해하여야 한다. 일단 개인키가 노출이 되면 그 개인키 소유자에게 보내어지는 모든 메시지들은 복호화 될 수가 있게 된다. RSA는 강력한 암호화를 지원하고 DES의 가장 큰 문제점중 하나였던 키 관리 문제를 해결하였다. 그러나 기본 연산알고리즘이 곱셈이기 때문에 DES에 비하여 약 100배 이상 느리다는 문제점이 있다.[3]

III. ELM(Expanding Logistic Map)

3.1 카오스이론의 개요

카오스 이론은 1960년대 등장한 이후 계속적인 연구를 통해 현대과학의 새로운 장을 열어가고 있다. 카오스 이론은 자연계에 존재하는 일정한 규칙을 가진 불규칙해 보이는 현상을 연구하는 학문으로서 카오스의 일반적인 정의는 다음과 같다.[4]

1.어떤 동력학계의 복잡하고 비주기적이며 유인적인 궤도
2.주기성이 없는 일종의 질서
3.새롭게 인식된 보편적인 자연현상
4.결정론적인 비선형 동력학계에 나타나는 불규칙적이고 예측불가능한 형태

로버트 메이(Robert May)는 1975년에 생물의 개체수 변동을 수학적으로 처리함으로서 카오스 공학을 가전제품이나 전기기기 등에 이용하기 시작하였다[5].

카오스 시스템은 랜덤행위(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 분야의 하나가 되고 있다.[7] 특히 초기조건에의 민감한 의존성(Sensitive Dependence on Initial Condition)으로 대표되는 카오스 이론은 주기성(Periodicity), 프랙탈(Fractal), 바이퍼케이션(Bifercation), 간헐성(Internittency), 등의 새로운 용어를 만들어 냈다.

최근 컴퓨터의 처리 능력 향상과 인공지능의 학문적인 이론과 응용기술의 발달로 카오스 이론이 전산학 분야에 새로운 관심으로 등장하기 시작하였다. 즉, 자연 속에서 일어나는 어떤 현상에서 일정한 규칙을 찾기 위한 수많은 자료를 컴퓨터는 쉽게 처리할 수 있으며, 그 속에서 규칙을 찾아 함수로 만들고 시간의 변화에 따라 변하는 함수 값을 이용하게 하는 것이다.

3.2 Logistic map

로버트 메이(Robert May)는 시간의 변화에 따른 동물의 개체수 변화를 구하는 간단한 식을 통하여 구체적인 연구결과를 발표하였다.

내년의 개체수 = 번식률×(1 - 금년의 개체수) ×금년의 개체수

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.[6]

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

α는 개체수의 증가량이며, X_n은 금년의 개체수, X_{n-1}은 내년의 개체수이다. 위의 로지스틱 방정식에서 X_n에서 X_{n-1}로의 변화를 논리사상(Logistic map)이라 한다. α의 값이 크다면 개체수가 적을 때는 빠른 속도로 증가하고 작다면 빠른 속도로 감소함을 나타낸다.[5] 다음 그림 2는 $X_1 = 1$ 일 때 매개변수 α에 따른 개체수의 변화를 쉽게 알 수 있도록 나타낸 Feigenbaum

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

(1) $0 < \alpha \leq 1$ X_n은 0으로 수렴
(2) $1 < \alpha \leq 2$ X_n은 1 -(1 / a)로 수렴
(3) $2 < \alpha \leq 3.5699$ X_n는 주기배가 상태
(4) $3.5699 < \alpha$ X_n는 혼돈 상태

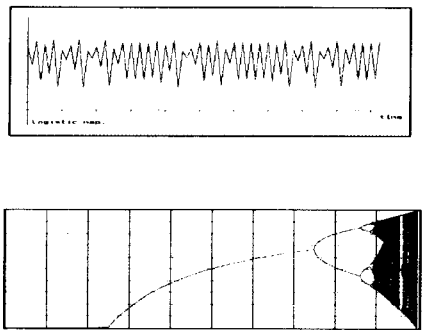


그림 2. 개체수의 변화와 Feigenbaum분기도

3.3 ELM

우리가 카오스 신호를 만들어내기 위해 사용한 방법은 로지스틱 방정식보다 넓은 진동 범위를 가지는 3차 함수를 이용한 것이다. 본 연구에서 제안한 ELM의 일반형은 다음과 같다.

$$X_{n+1} = a\,X_n^3 + b\,X_n^2 + cX_n + d \quad (a \neq 0) \quad \text{----- (2)}$$

ELM의 특징은 바로 최대값과 최소값을 갖는다는 사실이다. 이차함수 $X_{n+1} = a\,X_n^2 + bX_n + c\ (a \neq 0)$는 a의 값에 따라 최소값 또는 최대값 중 하나만 갖게 되지만, 삼차함수는 a가 0이 아니라면 언제나 최대값과 최소값을 다 가지게 되기 때문에, 그만큼 암호화에 사용할 수 있는 키의 범위가 넓어지게 된다. 이 최대값과 최소값을 기점으로 암호화에 이용되는 키 값의 범위가 정해진다. a의 값은 그래프의 폭을 결정한다. a의 값이 0에 가까울수록 폭이 넓어지고 최대값과 최소값의 차이가 커지며, 0에서 멀어질수록 폭이 좁아지고 최대값과 최소값의 차이가 작아지므로 구하고자 하는 a의 값에는 제한이 있다. 그러므로 a의 조건은, 0에 가장 가까운 0이 아닌 수가 가장 최적이다. 이는 a의 값만을 생각했을 때고 나머지 b, c의 값을 고려하면 키 값의 범위가 달라질 수 있다. 그리고 c와 a의 부호가 같다면 b의 값이 월등하게 크지 않은 이상, 그래프는 최대점과 최소점을 가지지 않기 때문에 c는 a와 같은 부호 값을 가지지 않는 경우가 일반적이다.

식 2에서 초기 값을 0.5, 적당한 키 값을 입력하였을 시 ELM의 출력 값의 변화를 그림 3에 나타내었다. 출력 값이 불규칙하게 진동함을 알 수 있었다. (X_2, Y_2)

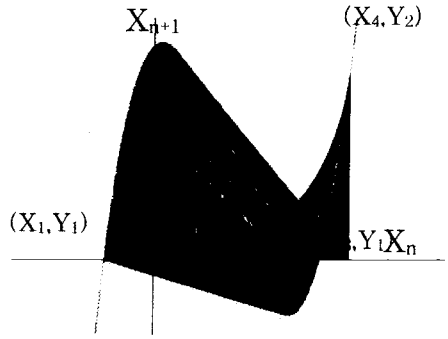


그림 3. 초기 값에 따른 카오스 신호 값의 변화

그림 4는 본 연구에서 제안한 ELM을 이용하여 그 출력 카오스 신호값을 그래프로 나타내었을 때 초기 값의 변화가 0.01임에도 불구하고 두 그래프의 그림이 완전히 다르다.

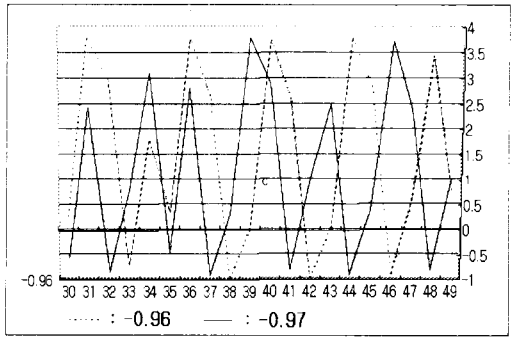
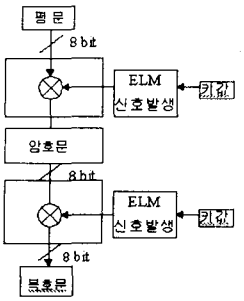


그림 4. 초기값에 따른 카오스 신호값의 변화

IV. ELM의 구현

본 연구에서는 앞서 제시한 ELM을 이용하여 파일을 암호화한다. 본 연구에서의 암호화 과정을 그림 5에 나타내었다. 암호문의 크기와 평문의 크기를 같게 하기 위하여 평문과 ELM의 출력을 XOR연산하였다.



그 림5. 암복호화 과정

운영체제는 윈도우즈 98, 펜티엄III 500MHz에서 JDK1.3과 kawa 5.0으로 ELM을 이용한 암호화알고리즘을 구현하였으며 이를 그림 6에 나타내었다. 구현한 프로그램은 간단한 데모를 보이기 위한 창과 텍스트뿐만 아니라 모든 파일을 암호화하여 저장할 수 있으며 저장된 암호화파일에서 복호화를 할수 있도록 구성되어져 있다.

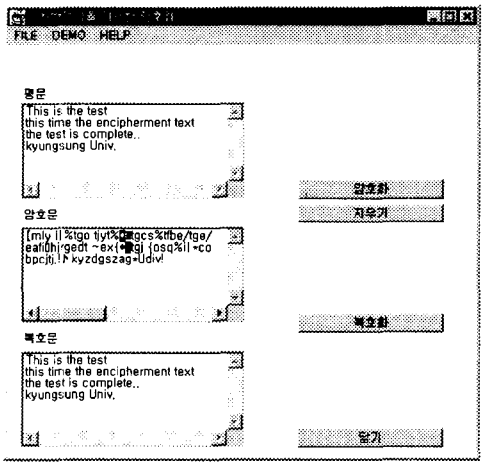


그림 6 실행한 데모화면

제안된 암호화 기법을 이용하여 filedfir.avi 파일을 암호화하여 암호화 정도를 비교하였다. 암호화 하기전의 파일과 암호화 한 후의 파일을 그림 7과 8에 각각 나타내었다.

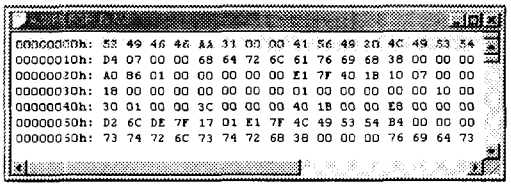


그림 7. 암호화 하기전 AVI 파일

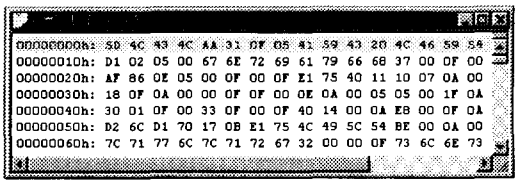


그림 8. 암호화 후 AVI파일

그림 7 과 8에서 보이는 것과 같이 원문에서 52 49 46 46..으로 나타나는 코드는 암호문에서 5D 4C 43 4C..으로 나타나 카오스신호에 의해 혼돈 상태를 가지는 코드로 암호화되었으며 암호화된 암호문은 원문으로 정확하게 다시 복호화 되었다.

V. 결 론

본 연구에서는 카오스 이론 기반의 3차 방정식을 이용한 암호화 알고리즘 ELM을 이용하여 텍스트 파일뿐만이 아니라 이미지 파일과 동영상 파일같은 멀티미디어 파일을, 혼동상태를 유지하는 값으로 암호화가 되었고 암호화된 파일은 원파일로 다시 복호화가 되었다.

본 암호화 알고리즘은 기본적으로 덧셈연산과 XOR연산이 주를 이루므로 속도가 빨라 웹에서의 디지털 서명이나 인터넷 뱅킹의 사용자 인증에서도 사용 가능하리라 생각된다.

앞으로 네트워크의 부하로 인한 패킷의 손실이나 패킷의 순서를 따지지 않는 UDP소켓 등의 동기화 문제만 해결된다면 실시간으로 영상이나 음성도 암복호화를 하여 인터넷 방송에서도 이용할 수 있을 것이다.

참고문헌

[1] 박정균, "RSA와 ECC암호화 방법의 비교분석", 명지대 산업대학원 석사학위 논문, 1999.

[2] IISI, 'Encryption for multimedia age GCC Overview',http://www.iisi.co.jp/research/GCCOverview.html, 1996.

[3] 김철, 암호학의 이해, 영풍문고, 1997.

[4] 정성용, 김태식, "카오스 이론을 이용한 암호화 기법", 한국정보과학회 가을 학술발표 논문집 Vol.25, pp.45-47, 1998.

[5] 이윤아, "DES알고리즘의 FPGA 구현", 한남대학교 석사학위 논문, 1999.

[6] 김용덕, "8비트 마이크로프로세서에 적합한 블록 암호 알고리즘의 설계",포항공과대학교 석사학위 논문, 1997.