혼돈함수와 기본 행렬 연산을 이용한 영상의 암호화

(Image Encryption using the chaos function and elementary matrix operations)

김 태 식*
(Tae Sik Kim)

요 약 오늘날 컴퓨터 네트워크의 발전과 휴대통신의 광범위한 보급으로 연예 오락, 영상 문화콘텐츠, 전자상거래 또는 의료분야에 이르기 까지 멀티미디어 자료의 응용은 매우 중요한 위치를 차지하고 있다. 그러나 실제 이들 자료들이 발달된 통신망을 통하여 효율적으로 전파, 활용되기 위해서는 무엇보다도 이들을 저장하거나 전송하는 과정에서 충분한 안정성이 전제되어야 할 것이다. 이를 위하여 오늘날 많은 암호화 방법들이 개발되어 응용되고 있다. 그러나 대부분 원문에 대한 자료를 텍스트에 기반으로 하게 됨으로, 영상과 같이 자료의 양이 방대하고 실시간 처리하는데 제약이 존재하는 멀티미디어 자료에 직접 적용하기는 문제점이 많다. 이에 본 논문에서는 먼저 복잡성과 초기 조건에 대한 민감성 등 카오스적 특성을 지닌 Logistic 함수를 이용한 암호화 기법을 도입하고 다음으로 비트평면상에서 Boolean 행렬의 기본 연산을 이용한 대수적 암호화 알고리즘을 수행함으로써 효과적인 영상 암호화 방법을 제시하였다.

Abstract Due to the spread of mobile communication with the development of computer network, nowadays various types of multimedia data play an important role in many areas such as entertainments, culture contents, e-commerce or medical science. But for the real application of these data, the security in the course of saving or transferring them through the public network should be assured. In this sense, many encryption algorithm have been developed and utilized. Nonetheless, most of them have focused on the text data. So they may not be suitable to the multimedia application because of their large size and real time constraint.

In this paper, a chaotic map has been employed to create a symmetric stream type of encryption scheme which may be applied to the digital images with a large amounts of data. Then an efficient algebraic encryption algorithm based on the elementary operations of the Boolean matrix and image data characteristics.

Key Words : cryptography, chaos, logistic 함수, 기본행렬연산(elementary matrix operation)

1. 서 론

IT관련 산업의 발달과 네트워크 기술의 폭넓은 보급으로 많은 컴퓨터들이 서로 결합되어 사용자들 간에 시·공간을 초월한 자료 교환 및 자원 공유가 용이해지는 등 컴퓨터 관련 개발환경이 유기적으로 발전되고 있다. 이에 따라 보다 적은 비용으로 지역적으로 분산되어 있는 많은 컴퓨터와 단말기들로부터 종합 정보시스템을 구축하거나, 데이터베이스에 저장된 광대한 정보를 효과적으로 분산 처리하는 것이 가능하게 되었다. 그리하여 오늘날 많은 사람들이 웹과 같은 인터넷 매체를 통해 전자메일을 주고받거

* 경주대학교 컴퓨터멀티미디어 공학부

나 전자게시판, 웹 하드 등을 통해 자료를 공유 또는 저장하기도 하고, 전자상거래와 같은 상행위를 하기도 한다. 그러나 이러한 자원의 공유가 불안전한 통신채널을 통해 이루어지기 때문에, 불시에 정보가 도청되어 불법적으로 사용되거나 변형되는 등 보안상 취약점을 지니게 된다. 그러므로 중요한 자료의 안전한 보관이나 전송을 위해 충분한 보안체계가 필요하다. 이러한 까닭으로 특히 인터넷 망을 통해서 중요한 자료를 전송해야 할 경우 우선적으로 웹 보안 프로토콜이 사용되고 필요에 따라서는 데이터의 암·복호화를 위한 알고리즘이 추가되기도 한다. 또 서버와 클라이언트 사이에 신뢰성과 안정성을 확보하기 위해 인증서버(Certificate Authority)를 통한 공개키 기반 인증과정이 사용되기도 한다 [1]. 대표적인 인증서 형식으로는 ITU-T의 X.509 등이 있다 [2]. 인증 과정이 종료된 후 암호화 채널을 통하여 실질적인 데이터를 주고받을 때 주로 비밀키 기반 암호화 알고리즘이 사용된다 [3]. 키 분배를 위해 사용되는 공개키 방식으로는 RSA 알고리즘이 많이 이용되나 최근에는 타원곡선기반 알고리즘도 많이 연구되고 있다 [4],[5]. 비밀키 방식으로는 초기 미국 표준 DES와 최근의 AES 알고리즘 [6],[7]이 있고, 국내에서는 한국전자통신연구원과 한국정보보호진흥원(KISA)에서 공동 개발한 SEED [8]를 들 수가 있다. 한편 최근에 이르러 다양한 멀티미디어 매체의 발달로, 영상자료와 같은 특정 영역의 자료가 높은 사회적 관심과 함께 상업적 이해와 결부되어, 불법적으로 채취되고 공중망을 통해 유통되고 이로 인해 많은 사회적 폐해가 나타나기도 한다. 그럼에도 무선 휴대 통신 매체를 중심으로 제공되는 여러 가지 콘텐츠기반 산업의 영향으로 영상자료는 날로 발전하고 있다. 영상 산업의 발달과 함께 관련 자료들에 대한 보안 대비가 더욱 강조될 것이다. 반면 개발된 많은 암호화 방법들은 주로 텍스트를 기반으로 한 원문을 다루므로, 이를 영상 자료와 같이 크기가 방대하고 실시간 처리에 제약이 있는 멀티미디어 자료에 직접 적용하기에 많은 제약이 따른다. 최근에 카오스 이론이 활발히 연구되어 이를 암호화 기법에 적용하려는 시도가 많이 이루어지고 있다 [9][10].

이에 본 논문에서는 영상자료에 대한 암호화를 위해 카오스 이론에 근거한 해석학적 암호화 방법과 행렬연산에 근거한 대수적인 암호화 방법을 동시에 시도하므로 효과적인 영상 암호화가 이루어지도록 했다.

2. 암호화 방법의 종류

자료를 암호화 하는 방법으로 암호키의 분배 방식에 따라 비밀키 암호계(private key cryptosystems)와 공개키 암호계(public key cryptosystems)를 들 수가 있다. 비밀키 암호 방식에서는 암호화 키와 복호화 키가 근본적으로 동일하며 송신자와 수신자가 비밀키(secrete key)를 함께 공유하게 된다. 공개키 암호 방식에서는 암호화 키와 복호화 키가 서로 다른데 암호화 키는 공개하나 복호화 키는 비밀로 보존하는 것이 보통이다. 이 때 송신자는 수신자의 공개키를 이용하여 암호화한 비문을 전달하게 되고 송신자는 자신의 비밀키로 이를 복호화하게 된다. 따라서 전송 중 제 3자에 의해 공개키가 도청되더라도 이를 통한 암호문의 해독은 불가능하게 된다. 뿐만 아니라 송신자가 자신의 비밀키로 서명하면 수신자는 송신자의 공개키를 이용해 이를 복원해 수신자가 진짜 서명자 인지 인증할 수가 있다. 이와 같이 공개키 암호계에서는 비밀키의 분배가 불필요하고 인증 수순이 용이하지만 암호화 처리 속도가 느린 면이 있다. 이러한 공개키 방식의 암호기로는 RSA 와 타원곡선 암호를 들 수가 있다. 비밀키 암호로 데이터를 처리하는 데에는 블록 암호화 방식과 스트림 암호화 방식이 있다. 블록암호는 평문을 일정길이의 블록으로 세분하여 블록마다 동일키를 사용하여 암호화 한다. 이러한 블록암호계로는 Hill 암호와 DES를 들 수가 있다. 최근까지 미국표준으로 채택했던 IBM의 DES 알고리즘은 64비트의 평문과 56비트의 키가 치환과 순열 및 모듈러 2 연산의 조합으로 16라운드를 거친 대표적인 블록암호이다. NTT가 개발한 일본의 FEAL(Fast Data Encipherment Algorithm)은 DES를 개량해 암호화 속도를 향상한 암호기라 하겠다. 스트림 암호는 같은 길이의 키 수열

(key bit sequence)을 평문과 비트단위로 암호화 해서 동일한 길이의 암호문을 만든다. 주기성을 보유한 LFSR(Linear feedback shift register)를 키 생성기로 사용하는 경우 주기 스트림 암호계라 부르는데 예로서 Hagelin 암호기와 Roto 암호기를 들 수가 있다. 이에 반해 비주기 스트림 암호계로는 Vernam 암호기가 있다. 스트림기반 암호화 방식은 블록기반 암호화 방식에 비교해 안정성면에서 뛰어나나 데이터의 오류 발생 등으로 인해 송·수신 과정에서 문제점이 야기될 수 있다. 이에 반해 블록기반 암호화 방식은 데이터 오류를 예방할 수 있으나 안정성을 높이기 위하여 블록의 크기 및 라운드 회수를 크게 해야 하는 문제점이 있다. 그러므로 오늘 날 데이터를 주고받을 때에 먼저 공개키를 통해 수신자를 호출하고 공개키를 통해 전달된 대칭키를 중심으로 암호화된 데이터를 가지고 통신을 하게 된다.

3. 제안한 암호화 방법

평문의 집합을 P, 키 집합을 K라 할 때 주어진 평문 $P\in$ P와 키 $K\in$ K에 대해 암호함수 E_K 와 복호함수 D_K 가 존재하여 $D_K(E_K(P))=P$ 를 만족하는 암호계(cryptosystem)를 기본으로 암호 키 열 $K=\langle K_i\rangle$를 평문열 $P=\langle P_i\rangle$에 적용하여 $E_K(P)=E_{K_1}(P_1)E_{K_2}(P_2)\cdots$로 암호화 하는 스트림 형식의 암호계를 생각하기로 한다. 특히 스트림 암호계에서 키 열이 $K_i=K_j=K$ 을 만족할 때, 즉 $E_K(P)=E_K(P_1)E_K(P_2)\cdots$ 일 때 이 암호계는 블록기반 암호계로 말 할 수 있다. 보통 암호를 위한 키 열을 미리 제공하는 대신 초기에 제공되는 키 값 K_0 를 기반으로 키 생성 함수를 통해 키 열을 만드는 암호계를 스트림 동기화 암호계 (synchronous cryptosystem)라 한다. 또 두개의 암호계가 서로 결합하여 $E_{K_1\times K_2}(P)=E_{K_2}E_{K_1}(P)$ 와 $D_{K_1\times K_2}(C)=D_{K_1}D_{K_2}(C)$ 을 만족하도록 하는 암호계를 곱 암호계(product cryptosystem)라 한다. 오늘날 많은 블록기반 암호계는 동기화에 기반한 키 열과 특정 반복함수 (round function)을 이용하여 개발되고 있다.

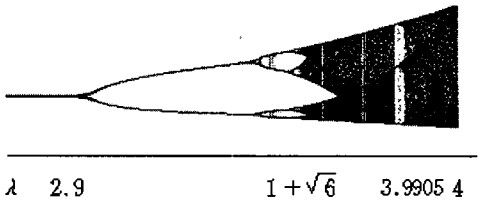
일반적으로 카오스 현상은 난류(turbulence)와 같이 무작위성을 가진 비선형적 동역학계(nonlinear dynamics)식으로 표현되며, 흐름에 대한 예측이 어려운 다양한 복잡계(complex systems)를 설명하기도 한다. 이러한 카오스 모델은 특히 초기 조건에 대단히 민감하게 반응하여 전체적으로 매우 불규칙한 궤적을 지니고 또한 프랙탈적 모습을 띠게 된다. 따라서 기존의 기하학적 적용이나 통계적 접근이 원활하지 못하다. 이러한 카오스 현상을 계산적 어려움과 충분한 혼돈성 및 복잡도를 근거로 암호화에 적용하고자 한다. 이를 위한 카오스 모델로 종에 있어서 인구 증가 현상의 동역학적 모델로 이용되는 Logistic 함수 $f_\lambda(x)=\lambda x(1-x)$를 도입하기로 한다. 이 함수는 특히 매개변수 λ에 따라 초기변수의 궤적이 달라진다. $\lambda>2+\sqrt{5}$에 대해 $f_\lambda(x)=1$을 만족하는 두 근을 $a=\frac{1}{2}-\sqrt{\frac{1}{4}-\frac{1}{\lambda}}$와 $1-a=\frac{1}{2}+\sqrt{\frac{1}{4}-\frac{1}{\lambda}}$라 둘 때 $f_\lambda(x)$는 $s_1:[0,1]\to[0,a]$, $s_1(x)=\frac{1}{2}-\sqrt{\frac{1}{4}-\frac{x}{\lambda}}$로 정의된 역함수와 $s_2:[0,1]\to[1-a,1]$, $s_2(x)=\frac{1}{2}-\sqrt{\frac{1}{4}-\frac{x}{\lambda}}$로 정의된 역함수를 가지게 된다. 이 때 각 역함수의 미분계수를 구해보면 $|s_i'|=\frac{1}{2\lambda}(\frac{1}{4}-\frac{x}{\lambda})^{-1/2}$, $i=1,2$ 을 만족하게 되고 따라서 평균값 정리로부터 $0\le x\le 1$에 대해 다음 등식

$$\frac{1}{\lambda}|x-y|\le|s_i(x)-s_i(y)|\le\frac{1}{2}(\frac{\lambda^2}{4}-\lambda)^{-1/2}|x-y|$$

이 성립하게 된다. 그러므로 $\lambda>2+\sqrt{5}$에 대해 s_i, $i=1,2$ 는 축소함수로서 함수 f_λ에 대해 유일 불변인 조밀집합 F를 가지게 된다. 즉 $f_\lambda(F)=F$ 와 $F=\bigcup_{i=1}^{2}s_i(F)$이 성립한다 [10]. 또한 집합 F는 repeller로서 F위에서 f_λ는 chaotic한 운동을 하게 된다. 한편 위 등식으로부터 프랙탈 차원은 부등식

$\frac{\log 2}{\log \lambda} \le \dim_H(F) \le \frac{\log 2}{\log(\lambda(1-4/\lambda)^{1/2})}$을 만족하게 되고 충분히 큰 λ에 대해 $\frac{\log 2}{\log \lambda}$에 가까이 간다. $0<\lambda\le 1$에 대해 f_λ는 $x=0$에서 $f_\lambda(0)=0$, $|f'(0)|<1$을 만족하게 되고 따라서 attractive 고정점(fixed point) 0을 가지게 된다. 그리하여 모든 $x\in[0,1]$는 0에 수렴 ($f_\lambda^k(x)\to 0$, $k\to\infty$)하게 된다. $1<\lambda<3$에 대해 f_λ는 unstable 고정점(fixed point) 0 과 stable 고정점 $1-\frac{1}{\lambda}$을 가지게 되고 따라서 모든 $x\in(0,1)$는 $1-\frac{1}{\lambda}$에 수렴, 즉 $f_\lambda^k(x)\to 1-\frac{1}{\lambda}$, $k\to\infty$이 성립하게 된다. λ가 점점 증가하여 3을 지나게 되면 stable 고정점 $1-\frac{1}{\lambda}$은 오히려 unstable로 바뀌면서 주기가 2인 stable 궤도(orbit)로 분리되어 가산개의 점을 제외한 $(0,1)$의 모든 점들을 끌어들인다. λ가 증가하여 $1+\sqrt{6}$을 지나면 주기 2인 궤도는 다시 unstable로 바뀌면서 주기가 4인 stable 궤도로 분기되게 된다. 이와 같이 λ가 3.570까지 증가하는 동안 충분히 큰 q에 대해 주기 2^q인 stable 궤도는 unstable로 바뀌면서 다시 주기가 2^{q+1}인 stable 궤도로 분기되어 가산개의 점을 제외한 $(0,1)$의 모든 점들을 끌어 들이게 된다. $3.570<\lambda<4$ 사이에서는 여러 유형의 운동이 관찰된다. 이 때 양측도(positive Lebesgue measure)를 가지는 적당한 집합 K가 있어서 모든 $\lambda\in K$에 대해 f_λ가 chaotic 한 끌개(attractor)를 가지게 된다. 그럼에도 중간에 간극이 생겨 이 부분에서 주기를 배가시키는 stable 궤도가 나타나기도 한다. 예로서 $\lambda\approx 3.83$에서는 주기 3인 궤도가 나타나기 시작하여 주기가 6, 12등으로 분기하게 된다.

그림 1 에서 주어진 초기값 x=0.4 와 0과 4 사이에 있는 λ 값들에 매번 1000번의 반복한 궤도 값의 분포를 보여주는 데 위에서 언급한 바와 같은 분기점의 분포를 나타내고 있다.



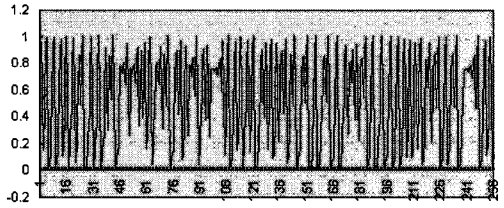
<그림 1> Logistic의 분기에 대한 카오스분포

특히 $3.9905<\lambda$ 처럼 λ가 4에 극히 가까이 있는 경우 f_λ의 궤도는 $[0,1]$사이에 거의 균등하게 분포하게 되고 f_λ 또한 이 영역에서 chaotic 하게 움직이게 된다. 이와 같이 f_λ는 주어진 초기값 x와 λ에 대해 매우 민감하게 움직이고 이 때 생성하는 궤도는 수렴하거나 주기적이지 않고 chaotic 한 복잡계를 보임에 따라 이를 바탕으로 일차 암호화 알고리즘을 다음과 같이 구축한다. 주어진 λ에 대해 초기값 x를 취해 f_λ를 통해 255회 반복함으로 구해진 256개의 궤도 값을 크기 순으로 재배치하여 대응하는 부분수열의 번호를 처음 대응하는 수열의 번호와 대치하는 암호화 방법으로 주어진 영상에 새로운 픽셀 값을 부여하기로 한다. 이 때 그림 2 에서 보여주는 바와 같이 chaotic 한 영역부분에 대해 픽셀 값 변환을 취함으로 인접한 영상 값이라도 서로 멀리 떨어지게 되고 따라서 원 영상과 전혀 다른 암호화된 영상을 얻을 수가 있다. 또한 수신자에게는 암호화 된 자료를 전송할 때 초기값과 λ를 비밀키로 하여 따로 전달하므로, 수신측에서도 동일한 방법으로 암호화와 동일한 과정으로 궤도를 추출하여 원 픽셀 값으로 환원 할 수가 있다.

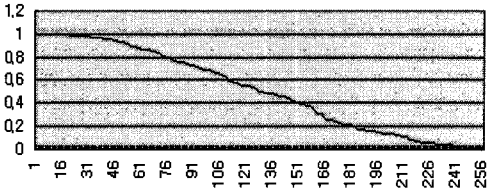
한편 임의의 행렬 A에 대해 다음의 세 가지 기본 행 변환 (elementary row operation)을 도입하기로 한다.

(i) 행렬 A의 i번째 행과 j번째 행을 서로 교환하는 변환 : $A_{R_i \leftrightarrow R_j}$

(ii) 행렬 A의 i번째 행의 각 원소를 $k(\neq 0)$배 하는 변환 : A_{kR_i}



(a) 정렬하기 전 분포



(b) 정렬한 후 분포

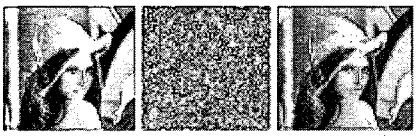
<그림 2> 정렬하기 전, 후의 원 궤도 값 분포

(iii) 행렬 A의 i번째 행의 각 원소를 k배 하여 j번째 행의 대응하는 각각의 원소에 더하는 변환 : $A_{kR_i+R_j}$

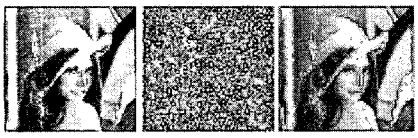
또한 동일한 방법으로 행렬 A에 대한 기본 열 변환 (elementary column operation) $A_{C_i \leftrightarrow C_j}$, A_{kC_i} 및 $A_{kC_i+C_j}$ 를 정의 할 수가 있다. 위의 기본 행 변환과 열 변환을 합쳐서 기본 변환으로 부르기로 한다. 또 행렬 A에 유한번의 기본 행 변환을 하여 B 행렬이 만들어 질 때 A와 B는 서로 행동치 (row equivalence)라 는 동치관계를 만족하고 $A \sim_R B$로 나타낸다. 동일한 방법으로 열 동치 (column equivalence) $A \sim_C B$ 가 정의된다. 또한 행렬 A에 유한번의 기본 변환을 통하여 B 행렬이 만들어 질 때 A와 B를 단순히 동치라 하고 $A \sim B$로 나타내기로 한다. 또 단위행렬 I 에 기본 행 변환을 한번 행하여 얻어진 행렬을 기본행렬 (elementary matrix)이라 한다. 이제 Boolean 연산 $a \oplus b = \begin{cases} 1 & \text{if } a \neq b \\ 0 & \text{otherwise} \end{cases}$ 와 $a \wedge b = \begin{cases} 1 \text{ if } a = 1 = b \\ 0 \text{ otherwise} \end{cases}$ 로 정의된 Galois 체 $GF(2) = (\{0,1\}, \oplus, \wedge)$ 위에 정의된 두 $N \times N$ Boolean 행렬 $A = (a_{i,j})$ 와 $B = (b_{i,j})$에 대해 Boolean 합 연산 $A \oplus B = (a_{i,j} \oplus b_{i,j})$와 Boolean 곱 연산 $AB = (\oplus_{k=1}^{m} a_{i,k} \wedge b_{k,j})$ 를 정의한다. 이때 $A \oplus A = I$ 이 만족됨을 쉽게 알 수 있다. 그러면 Galois 체 상에 정의된 Boolean 행렬에 대해 위에서 정의된 기본(행, 열) 변환을 생각할 수 있으나 두 번째 변환 A_{kR_i}은 오로지 $k=1$일 때 뿐 이므로 여기에서는 고려하지 않기로 한다. 세 번째 변환 $A_{kR_i+R_j}$도 $k=1$일 경우로 단순히 $A_{R_i \oplus R_j}$ 만 고려하기로 한다. 그러면 Boolean 행렬에 대해 E 가 앞에서 정의된 기본 행렬일 경우 $EE = I$ 을 만족함을 쉽게 알 수 있다. 이때 행렬 변환과 기본행렬과의 관계를 살펴보기로 한다. 만약 행렬 A에 기본 행 변환 $A_{R_i \leftrightarrow R_j}$을 통하여 B가 얻어졌다면 B의 i 행벡터 $B_{i.}$는 A의 j 행벡터 $A_{j.}$으로, B의 j 행벡터 $B_{j.}$는 A의 i 행벡터 $A_{i.}$으로 이는 항등행렬의 i 행과 j 행을 서로 교환한 기본행렬 $E = I_{R_i \leftrightarrow R_j}$에 A를 우측에 곱한 것과 같다. 같은 방법으로 행렬 A에 기본 행 변환 $A_{R_i \oplus R_j}$을 통하여 B가 얻어졌다면 B의 j 행벡터 $B_{j.}$는 A의 i 행벡터 $A_{i.}$를 A의 j 행벡터 $A_{j.}$에 Boolean 합 한 것으로 이는 항등행렬의 I의 i 행과 j 행을 서로 Boolean 합한 기본행렬 $E = I_{R_i \oplus R_j}$ 우측에 A를 곱한 것과 같다. 마찬가지로 B가 행렬 A에 기본 열 변환 한번을 취함으로 얻어진 행렬이면, B는 항등행렬의 I에 B를 얻을 때와 동일한 과정으로 기본 열 변환을 취해 얻은 기본행렬 E 좌측에 A를 곱한 것과 같다. 이를 이용하여 만약 A가 I와 행동치, 즉 $A \sim_R I$, 이라고 하면 유한개의 적당한 기본 행렬 $E_1, E_2, \cdots, E_n$ 이 있어서 $A = E_n E_{n-1} \cdots E_1 I$ 이 되게 된다. 이 때 인 I와 열 동치 $B_{\mathrm{C}}\mathrm{I}$ 를 만족하는 $B = IE_1 E_2 \cdots E_n$에 대해 $AB = E_n E_{n-1} \cdots IE_1 E_2 \cdots E_n = I$ 이 성립하게 된다. 따라서 B는 A의 역행렬이 되게 된다. 이를 이용하여 우리는 Boolean 행렬의 역 행렬을 쉽게 생성하는 암호 키 행렬을 만

들 수가 있다.

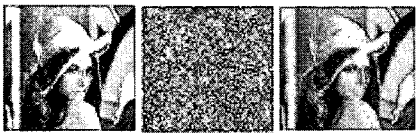
한편 앞에서 언급한 바와 같이 Logistic 함수 f_λ에 대해 초기 $\lambda \in [3.9905, 4)$에 대해 함수 f_λ는 $(0,1)$에서 chaotic 한 움직임을 보이고 또 초기 변수 λ 와 x_0에 매우 민감하게 움직임을 알아보았다. $f^k(x) = f \circ f \circ \cdots f(x)$라 둘 때 0과 512 사이에 있는 임의의 정수 $k \neq \ell$ 에 대해 $f_\lambda^k(x) \neq f_\lambda^\ell(x)$이 만족됨을 위에서 관찰 할 수 있다. 따라서 (x_0, λ)를 비밀키로 정하고 이로부터 먼저 궤도 $\{a_k = f_\lambda^k(x_0)\}_{k=0}^{255}$을 구하고 이 수열 $\{a_k\}$을 크기 순으로 재구성한 $\{b_k = a_{s(k)}\}_{k=0}^{255}$를 생성하기로 한다. 이로부터 주어진 영상 $\boldsymbol{Q}$의 한 픽셀 값이 k이면 이를 새로운 픽셀 값 $s(k)$로 대치함으로 암호화 된 영상 $\boldsymbol{P} = L(\boldsymbol{Q})$를 Logistic 함수에 기반한 일 단계 카오스 암호화 알고리즘으로 얻을 수 있게 된다. 수신측에서 복호화 또한 암호화와 동일한 과정을 수행함으로서 $s(k)$에 대해 k값을 환원하여 복호화된 영상 $\boldsymbol{Q} = L^{-1}(\boldsymbol{P})$를 구할 수가 있는 것이다. 그림 3 에서 여러 가지 초기값에 대한 암호화된 영상과 이를 복호화한 영상을 보여준다.



(a) λ=3.991567, x_0=0.489845



(b) λ=3.991567, x_0=0.789845



(c) λ=3.999567, x_0=0.789845.

<그림 3> Logistic 함수에서 초기값에 따른 암호화 영상 및 복호화 영상

이와 같은 카오스 함수에 기반한 암호 방법은 수행속도가 매우 빠르다. 그러므로 이러한 암호화 알고리즘을 수행함에 있어서 과정의 회수를 높여 여러 번 암호화 알고리즘을 수행함으로 암호화 된 영상의 복잡도를 높을 수는 있으나 카오스 연산 자체가 실수 연산을 사용하므로 반올림 오차 등을 고려할 때 본 논문에서는 한번만 수행하는 것으로 제한하였다.

추가적으로 복잡도를 높이는 방법으로 앞서 카오스 암호화 된 영상 $\boldsymbol{P}$ 에 대해 언급한 행, 열 변환을 이용한 암호화를 회수반복법을 사용하여 수행하기로 한다. 보통 암호화의 안정성을 위하여 DES에서 처럼 블록기반 암호화 하고 회수를 16회 반복하는 알고리즘을 사용기도 하지만 제기한 방법에서는 앞서 카오스 암호화한 영상을 비트평면으로 분할하여 유효층에 대해서만 키를 생성하여 반복화 암호 알고리즘을 적용하였다.

이를 위해 Logistic 함수에 의해 생성된 수열 $\{a_k\}_{k=n_0}^{n_0+N/2}$와 이를 크기 순으로 재구성한 $\{b_k = a_{s(k)}\}_{k=n_0}^{n_0+N/2}$ 를 가져온다. 기본 행렬 $E_{i,j}$를 $E_{i,j} = I_{R_i \leftrightarrow R_j}$, $E'_{i,j}$를 $E'_{i,j} = I_{R_i \oplus R_j}$ 라 둘 때 $N \times N$ 항등행렬 I 에 대해 행, 열 변환을 통해 $K = E_{s(n_0+N/2-1),s(n_0+N/2)} \cdots E_{s(n_0),s(n_0+1)} I$ 와 열 변환을 통하여 $K^{-1} = I E_{s(n_0),s(n_0+1)} \cdots E_{s(n_0+N/2-1),s(n_0+N/2)}$ 를 생성한다. $K_0 = K$라 둘 때 유효 회수의 암호 키 평면 열로 $K_i = E'_{i,N} K_{i-1}$ 와, 복호화 키 평면 열로 $K_i^{-1} = K_{i-1}^{-1} E'_{i,N}$ 을 생성하였다. k-비트 평면 영상을 P_k라 할 때 Logistic 함수에 의한 일차 암호화 영상을 비트 평면벡터 $\boldsymbol{P} = (P_7, P_6, \cdots, P_0)$로 비트평면으로 분해할 때 LSB 비트 평면은 매우 난수적 분포를 보이므로, 이를 초기 암호화한 영상에 대한 초기 난수 평면으로 $V = P_0$로 두기로 한다. 따라서 반복 키열 $\langle K_i \rangle$는 Logistic 함수의 비밀 키로서의 초기값 λ 와 x_0 에 의해 결정됨을 알 수 있다. 또한 초기 난수 평면 V 를 보호하기 위하여 송신자는 수신자에게 $V^* = K P_0 K$ 로 변환된 V^*를 λ 및 x_0와 함께 보낸다. 그러면 송신자는 K를 생성하고 $V = K^{-1} K^* K^{-1}$ 을 통해

V를 구할 수 있게 된다. 이상의 암호키 열로부터 제기된 대수적 암호화 알고리즘을 구성하기로 한다. 원 비트 평면 영상 P_i를 암호화 하기 위하여 다음의 세 단계 연산을 취하기로 한다.

(i) $P_i^1 = P_i \oplus C_{i-1}$, (단 $C_0 = V$).

(ii) $P_i^2 = K_i P_i^1 K_i$.

(iii) $C_i = P_i^2 \oplus P_{i-1}$.

따라서 암호 영상 C_i 는 $C_i = K_i(P_i \oplus C_{i-1})K_i \oplus P_{i-1}$ 로 표현된다. 수신측에서 복호화를 행할 때 암호화 과정과 비슷한 다음의 과정을 이용하게 된다.

(i) $C_i^1 = C_i \oplus P_{i-1}$, (단 $P_0 = V$),

(ii) $C_i^2 = K_i^{-1} C_i^1 K_i^{-1}$,

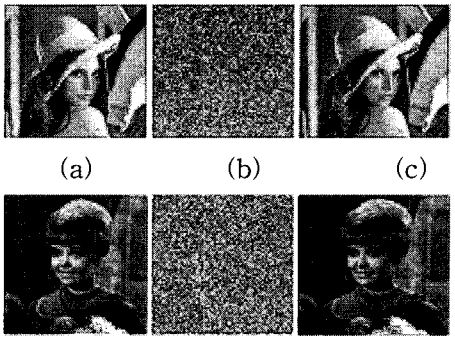
(iii) $P_i = C_i^2 \oplus C_{i-1}$, (단 $C_0 = V$).

따라서 복호화 연산을 하나의 식으로 표현하면 $P_i = K_i^{-1}(C_i \oplus P_{i-1})K_i^{-1} \oplus C_{i-1}$ 이 된다.

그러면 주어진 암, 복호화 알고리즘의 정당성은 다음의 연산에서 유효함을 알 수가 있다.

$$
\begin{aligned}
& K_i^{-1}(C_i \oplus P_{i-1})K_i^{-1} \oplus C_{i-1} \\
&= K_i^{-1}(K_i(P_i \oplus C_{i-1})K_i \oplus P_{i-1} \oplus P_{i-1})K_i^{-1} \oplus C_{i-1} \\
&= (P_i \oplus C_{i-1})K_i K_i^{-1} \oplus C_{i-1} \\
&= (P_i \oplus C_{i-1}) \oplus C_{i-1} \\
&= P_i
\end{aligned}
$$

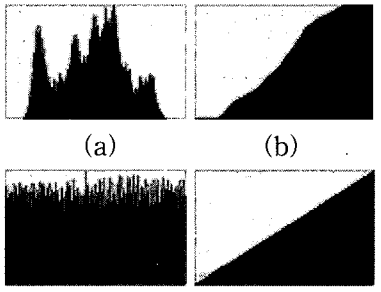
이러한 복호화 과정을 통하여 구해진 영상 $\boldsymbol{P} = (P_7, P_6, \cdots, P_0)$에 대해 logistic 복호화 과정 $L^{-1}(\boldsymbol{P})$ 를 통해 원 영상을 구할 수가 있다. 그림 4 에서 제안된 알고리즘을 실제 Lenna 영상과 Girl 영상에 직접 적용하여 암호화하고 복호화 한 영상을 나타낸다.



(a) (b) (c)

(c) (d) (e)

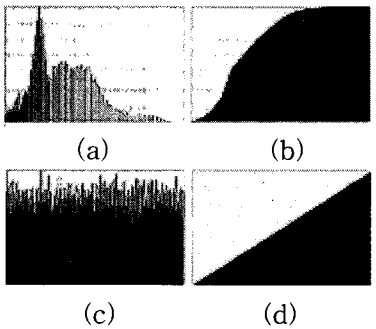
<그림 4> (a) Lenna 원영상 (b) 암호화된 영상 (c) 복호화된 영상 (d) Girl 원영상 (e) 암호화된 영상 (f) 복호화된 영상 ($\lambda = 3.999567, x_0 = 0.789845$)



(a) (b)

(c) (d)

<그림 5> Lenna 원영상과 암호화 영상의 분포 비교 (a) 원영상의 확률분포 (b)원영상의 누적 확률분포 (c) 암호영상의 확률분포 (d)암호영상의 누적확률분포 ($\lambda = 3.999567, x_0 = 0.789845$)



(a) (b)

(c) (d)

<그림 6> Girl 원영상과 암호화 영상의 분포 비교 (a) 원영상의 확률분포 (b)원영상의 누적 확률분포 (c) 암호영상의 확률분포 (d)암호영상의 누적확률분포 ($\lambda = 3.999567, x_0 = 0.789845$)

그림 5와 그림 6은 원 영상과 암호화 된 영상의 픽셀 값 분포를 비교하여 보여준다. 여기에서 알 수 있는 것과 같이 원 영상에 비해 암호화된 영상의 픽셀 값 분포는 전체 범위에 걸쳐 매우 균질하게 퍼져있어 엔트로피가 향상됨을 알 수가 있다. 실제 계산을 해보면 Lenna 영상에 대해 원영상의 평균값은 123.47이고 표준편차는 47.89임에 비해 보기에서와 같이 매개변수 $\lambda = 3.999567$과 초기값 $x_0 = 0.789845$에서 암호화된 영상의 평균값은 127.43 이고 편차는 73.92가 된다. 또한 Girl 영상에 대해서도 원영상의 평균값은 73.57이고 편차는 42.62임에 비해 보기에서처럼 암호화된 영상의 평균값은 127.47 이고 표준편차는 74.25가 된다. 아래 표는 두 실험 영상에 대해 매개변수 값과 초기값을 달리할 때 분포하는 평균값과 표준편차를 나타낸다.

<표 1> 실험영상에 대한 원영상과 암호영상에 대한 통계량 비교

λ	x_0	Lenna 영상		Girl 영상	
		평균	표준편차	평균	표준편차
3.999567	0.789845	127.43	73.92	127.47	74.25
3.999567	0.089845	127.70	73.91	127.72	74.23
3.991567	0.089845	127.44	73.98	127.77	74.10
원 영상		123.47	47.89	73.57	42.62

4. 결 론

일반적으로 텍스트 데이터와 달리 영상데이터는 요구하는 자료의 양이 방대하고 구조가 복잡하다. 따라서 이러한 자료의 원활한 암호화를 위해서 영상의 특성을 이용하는 암호화가 더 효용성이 있을 것이다. 이를 위하여 본 논문에서는 먼저 카오스 모델로서 Logistic 함수를 도입하고 이 함수의 복잡성을 이용한 chaos 암호화를 통해 일 단계 암호화 알고리즘을 구축했다. 이러한 암호화 방식은 블록기반 암호화 기법과 달리 빠른 계산을 할 수가 있고 비밀 키로서 두 개의 초기변수를 수신자에게 보내면 된다. 그렇지만 카오스 함수가 실수 연산을 수행하는 관계로, 반복 회수를 높여 암호의 안정성을 높이는 방법으로 카오스 함수를 이용하는 대신 행렬의 기본 변환을 이용한 2차 암호화기법을 추가하였다. 이러한 2단계 암호화 알고리즘에서는 송신자에 추가 정보 전달 없이 1단계에서 사용된 Logist 함수를 이용하여 생성된 비밀 키와 이를 기반으로 반복 회수 키 열을 만들어 사용하였다. 대신 영상의 LSB 비트평면 영상을 초기 난수 영상의 초기값으로 사용하였다. 이렇게 1, 2차 단계를 통하여 암호화하므로 암호화 된 영상의 픽셀 값들이 균등 분포에 근접하게 하여 엔트로피를 증대 시킬 수 있음을 확인하였다.

참 고 문 헌

[1] E. Okamoto and K. Tanaka, "Key distribution system based on identification information", *IEEE Selected Areas in Communications,* 7, 482-485, 1989.

[2] ITU-T Rec. X509, Information technology-Open Systems Interconnection-The Directory : Public-key and attribute certificate frameworks, March.2000.

[3] X. Lai, "On the design and security of block cipher", Konstanz, Germany: Jartung-Gorre, 1992.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystem", *Communication of ACM*, Feb. 1978.

[5] N.Koblitz,"Elliptic Curve Cryptosystems", *Mathematics of Computation,* 48, 203-209, (1987).

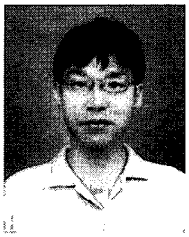
[6] "Data encryption standard", FIPS PUB 46, National Breau of Standards,Washington, D.C., Jan. 1997.

[7] J. Daenen and V. Rijmen, "AES Proposal: Rijndael",June, 1998. AES submission.

[8] KISA, "128비트 블록암호화알고리즘(SEED) 개발 및 분석보고서", 1998.

[9] K. Falconer, "Fractal geometry", Brisbane: John Wiley & Sons, 1990.

[10] L. Kocarev and G. Jakimoski, "Pseudorandom bits generated by chaotic maps", *IEEE Trans. Circuits Systems I Fund. Theory Appl.* 50, 123-126, (2003)



김 태 식 (Tae Sik Kim)

- 1982. 2. 경북대학교 수학과 졸업(학사)
- 1984. 2. 경북대학교 대학원 수학과 졸업(해석학, 이학석사)
- 1996. 2. 경북대학교 대학원 수학과 졸업(응용수학, 이학박사)
- 2002. 8. 경북대학교 대학원 전자공학과 수료(정보통신 : 영상통신)
- 2002. - 2003. 경북대학교 전자공학과 교수
- 2004. 3. - 현 경주대학교 컴퓨터멀티미디어공학부 교수
- 관심분야 : 영상통신, 영상처리, 암호론, 프랙탈, 비선형동역학