카오스 함수와 기본 행렬변환을 통한 영상의 암호화

김태식*

*경주대학교

Image encryption through the chaos function and elementary row column operations

Tae Sik Kim*

*Gyeongju University

E-mail : tskim@gju.ac.kr

요 약

영상 데이터의 효과적인 암호화를 위하여 logistic 함수를 이용한 chaos 암호화 알고리즘을 구축하였다. 이 방식은 블록기반 암호화 기법에 비해 빠른 계산을 할 수가 있고 비밀 키로서 두개의 초기 변수를 수신자에게 보내면 된다. 그렇지만 실수 연산을 하는 관계로 회수를 높여 암호의 안정성을 높이는 대신 행렬 기본 연산을 이용한 합성암호화 알고리즘을 구성하였다. 제안된 알고리즘에서는 송신자에게 logist 함수로부터 생성된 비밀 키와 이를 기반으로 만들어 진 반복 회수 키 열을 그대로 사용한다.

ABSTRACT

For the efficient image encryption, we proposed the encryption algorithm using the chaotic function and elementary matrix operation defined on the bit plane decomposition. Though the chaotic encryption algorithm is faster than block encryption, it uses a real number computation. In this sense, we use the row and column operations on the bit-plane decomposed images combined with logistic function for the recursive rounding number, too.

키워드

암호화 알고리즘, 카오스 함수, 기본행렬연산, 비트평면 분할

Ⅰ. 서 론(휴먼고딕10, 중간정열)

인터넷 관련 기술의 일반화와 컴퓨터 사양의 고급화로 멀티미디어 자료의 이용이 활발해지고 있다. 또한 많은 자료들이 인터넷 매체를 통해 전달되거나 공유되고 전자상거래를 통해 유통되기도 한다. 그러나 이 과정에서 불법적으로 취득된 정보가 인터넷 망을 통해 확산되어 사회, 경제적으로 손실을 주거나 개인의 사생활에 폐해를 끼치기도 한다. 그러므로 중요한 자료를 저장하거나 전송하는 과정에서 보안문제를 심각히 고려할 필요가 있다. 이를 위한 여러 가지 웹 보안장치 또는 데이터의 암·복호화 알고리즘이 개발되고 있다 [1][2]. 그중 공개키 기반의 보안시스템을 이용한 인증 과정을 수행한 뒤 비밀키 기반 암호화과정을 통해 실제 데이터를 주고받는 방법이 많이 이용되고 있다 [3][4]. 본 논문에서는 특히 영상자료의 보다 효율적 암호화 방법으로 카오스 함수를 이용하는 방법과 영상의 비트 평면 분리를 통한 기본 변환을 이용하는 방법을 제안하였다.

Ⅱ. 본 론

카오스 이론을 통해 난류현상에서와 같이 무작위성이 내재되어 그 추이를 예측하기 힘든 여러 가지 복잡계를 조사할 수 있다. 이를 바탕으로 결

정적 동역학 모델에서 출발하지만 초기값의 결정 조건에 매우 민감하게 반응하는 복잡계 모델을 바탕으로 카오스기반 암호화 알고리즘을 구축하고자 한다. 이를 위한 카오스 모델로 인구증가 모델 함수로 표현되는logistic 함수 $f_\lambda(x)=\lambda x(1-x)$를 조사하고 이의 카오스적 특성을 파악해 보기로 한다. $\lambda>2+\sqrt{5}$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 $s_1(x)=\frac{1}{2}-\sqrt{\frac{1}{4}-\frac{x}{\lambda}}$로 정의된 역함수 $s_1:[0,1]\to[0,a]$와 $s_2(x)=\frac{1}{2}-\sqrt{\frac{1}{4}-\frac{x}{\lambda}}$로 정의된 역함수 $s_2:[0,1]\to[1-a,1]$를 가진다. 이 때 각 역함수의 미분계수는 $|s_i'|=\frac{1}{2\lambda}(\frac{1}{4}-\frac{x}{\lambda})^{-1/2}$, $i=1,2$ 을 만족하고 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_λ의 유일불변 조밀집합 F는 $f_\lambda(F)=F$ 와 $F=\bigcup_{i=1}^{2}s_i(F)$를 만족하고 f_λ는 F 위에서 chaotic 운동을 하게 된다. 또한 F의 프랙탈 차원은 부등식 $\frac{\log 2}{\log\lambda}\le\dim_H(F)\le\frac{\log 2}{\log(\lambda(1-4/\lambda)^{1/2})}$을 만족한다. f_λ는 $0<\lambda\le 1$ 범위에서 attractive 고정점(fixed point) 0을 가지지만 $1<\lambda<3$에서는 unstable 고정점(fixed point) 0 과 stable 고정점 $1-\frac{1}{\lambda}$을 가진다. λ가 점점 증가하여 3을 지나게 되면 stable 고정점 $1-\frac{1}{\lambda}$은 unstable로 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 주기 2^q인 stable 궤도는 unstable로 바뀌면서 주기가 2^{q+1}인 stable 궤도로 분기되어 가산개의 점을 제외한 $(0,1)$의 모든 점들을 끌어 들이게 된다. 특히 $3.570<\lambda<4$ 사이에서는 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.

그림 1에서 주어진 초기값 x=0.4 와 0과 4사이에 있는 λ 값들에 매번 1000번의 반복한 궤도 값의 분포를 보여주므로 위에서 언급한 내용을 나타내주고 있음을 알 수가 있다.

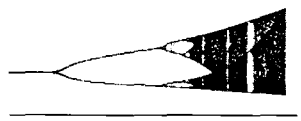

그림 1. Logistic의 분기에 대한 카오스분포

그림에서와 같이 $3.9905<\lambda<4$ 처럼 λ가 4에 극히 가까이 있는 경우 f_λ의 궤도는 $[0,1]$사이에 균등분포하며 이 영역에서 f_λ 는 카오스 움직임을 보여준다. 그리하여 주어진 초기값 x_0와 λ에 대해 f_λ는 매우 민감하게 대응하고 이 때 생성하는 궤도는 수렴하거나 주기적이지 않고 chaotic하게 된다. 이를 바탕으로 주어진 λ에 대해 f_λ를 통해 초기값 x_0를 255회 반복하고 구해진 255개의 궤도값을 크기순으로 재배치하여 대응하는 번호를 처음 번호값과 대치하는 암호화 방법으로서 암호화된 영상을 구한다. 즉 (x_0,λ)를 비밀키로하여 궤도 $\{a_k=f_\lambda^k(x_0)\}_{k=0}^{255}$을 구하고 이를 크기 순으로 재배치한 $\{b_k=a_{s(k)}\}_{k=0}^{255}$를 생성한다. 이로부터 영상 $\boldsymbol{Q}$의 한 픽셀 값 k를 새로운 픽셀 값 $s(k)$로 대치하므로 암호화 된 영상 $\boldsymbol{P}=L(\boldsymbol{Q})$를 구하는 알고리즘이 수행되게 된다. 수신측에서 복호화 또한 암호화와 동일한 과정을 수행하여 $s(k)$에 대해 k값을 환원 함으로 복호화된 영상 $\boldsymbol{Q}=L^{-1}(\boldsymbol{P})$를 구하게 된다. 이와 같은 카오스기반 암호화는 수행속도가 우수하므로 알고리즘 수행과정의 반복 회수를 높여 복잡도를 높을 수 있으나 실수 연산의 사용으로 인한 반올림 오차 등을 고려해 본 논문에서는 한 번만 수행하기로 하였다.

한편 행렬 A에 대한 기본 행 변환 (elementary row operation)으로 다음의 세 가지 변환이 정의된다.

(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 한다 (A_{kR_i}).

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

기본 행 변환과 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 수 있다. 또 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 행 동치 (row equivalence)라 는 동치관계를 만족하고 $A \sim_R B$로 나타낸다. 동일한 방법으로 열 동치 (column equivalence) $A \sim_C B$ 가 정의된다. 또 단위행렬 I 에 기본 행 변환을 한번 행하여 얻어진 행렬을 기본행렬 (elementary matrix)이라 한다. 또 Boolean 연산

$$a \oplus b = \begin{cases} 1 & \text{if } a \neq b \\ 0 & \text{otherwise} \end{cases}, \quad a \wedge b = \begin{cases} 1 & \text{if } a = 1 = b \\ 0 & \text{otherwise} \end{cases}$$

로 정의된 Galois체 $GF(2) = (\{0,1\}, \oplus, \wedge)$ 위에 정의된 두 $N \times N$ Boolean 행렬 $A = (a_{i,j})$ 와 $B = (b_{i,j})$에 대해 Boolean 행렬 연산 합을 $A \oplus B = (a_{i,j} \oplus b_{i,j})$로 정의하고 Boolean 행렬 연산 곱을 $AB = (\oplus_{k=1}^{m} a_{i,k} \wedge b_{k,j})$ 로 정의하기로 한다. 그러면 $A \oplus A = I$ 이 만족됨을 쉽게 알 수 있다. 또한 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 고려할 필요가 없다. 마찬가지로 세 번째 변환 $A_{kR_i+R_j}$도 $A_{R_i \oplus R_j}$만 고려하면 되겠다. 그러면 행렬의 변환과 기본행렬과의 관계를 살펴보기로 한다. 만약 행렬 A에 기본 행 변환 $A_{R_i \leftrightarrow R_j}$을 통하여 B가 얻어졌다면 B의 i 행 벡터 $B_{i.}$는 A의 j 행 벡터 $A_{j.}$으로, B의 j 행 벡터 $B_{j.}$는 A의 i 행 벡터 $A_{i.}$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 행 벡터 $B_{j.}$는 A의 i 행 벡터 $A_{i.}$를 A의 j 행 벡터 $A_{j.}$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. 이를 이용하여 만약 A가 I와 행 동치, 즉 $A \sim_R I$, 이라고 하면 유한개의 적당한 기본행렬 $E_1, E_2, \cdots, E_n$ 이 있어서 $A = E_n E_{n-1} \cdots E_1 I$ 이 되게 된다. 이 때 $B \sim_C I$를 만족하는 $B = I E_1 E_2 \cdots E_n$에 대해 $AB = E_n E_{n-1} \cdots I I E_1 E_2 \cdots E_n = I$이 성립하므로 B는 A의 역행렬이 된다. 이러한 관계를 이용한 암호 알고리즘을 앞에서 제시한 카오스 암호화 영상 P에 적용고자 한다. 보통 암호화의 안정성을 위하여 DES 에서처럼 블록기반 암호화 하고 회수를 16회 반복하는 암호화 알고리즘 사용하지만 본 논문에서는 영상을 비트평면으로 분할하여 유효층에 대해 키를 생성하여 반복 암호화하여 복잡도를 높이도록 했다. 이를 위해 먼저 logistic 함수에 의해 생성된 케도 $\{a_k\}_{k=n_0}^{n_0+N/2}$를 크기 순으로 재구성한 $\{b_k = a_{s(k)}\}_{k=n_0}^{n_0+N/2}$와 기본 행렬 $E_{i,j} = I_{R_i \leftrightarrow R_j}$ 및 $E'_{i,j} = I_{R_i \oplus R_j}$ 로부터 $K = E_{s(n_0+N/2-1), s(n_0+N/2)} \cdots E_{s(n_0), s(n_0+1)} I$ 와 $K^{-1} = I E_{s(n_0), s(n_0+1)} \cdots E_{s(n_0+N/2-1), s(n_0+N/2)}$ 를 생성한다. $K_0 = K$라 둘 때 유효 회수 의 암호키 평면 열을 $K_i = E'_{i,N} K_{i-1}$ 로, 복호화 키 평면 열을 $K_i^{-1} = K_{i-1}^{-1} E'_{i,N}$ 로 생성하였다. 따라서 반복키 열 $\langle K_i \rangle$는 logistic 함수의 비밀 키로서의 초기값 λ 와 x_0에 의해 결정한다. 한편 logistic 함수에 의한 암호화된 영상을 비트 평면 분할하여 $P = (P_7, P_6, \cdots, P_0)$로 나타낼 때 LSB평면 P_0는 난수 분포를 보인다. 따라서 이를 초기 난수 평면 V로 두고 보안을 위해 $V^* = K P_0 K$로 변환된 V^*를 λ 및 x_0와 함께 전송하므로 수신자는 K를 생성하고 이로부터 $V = K^{-1} V^* K^{-1}$를 복원하게 된다. 이상의 암호키 열로부터 제기된 대수적 암호화 알고리즘은 기존의 DES 구조와 비슷한 블록기반 횟수 반복 알고리즘에 기반을 둔다. 각 비트 평면 P_i를 암호화 하기위하여 다음의 세 단계 연산을 취한다.

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

이로부터 암호영상 $C_i = K_i(P_i \oplus C_{i-1}) K_i \oplus P_{i-1}$ 를 생성하게 된다. 복호화과정은 근본적으로 암호화 알고리즘과 동일한 형태로 구성되게 된다. 이렇게 복호화된 영상 $P = (P_7, P_6, \cdots, P_0)$에 대해 logistic 복호화 과정 $L^{-1}(P)$ 를 한번 더 취하므로 원 영상을 구하게 된다. 그림 2에서 제안된 알고리즘을 실제 Lenna 영상에 적용하여 암호화하고 복호화 한 영상을 나타낸다. 또 그림 3은 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 관찰 할 수가 있다. 실제 계산을

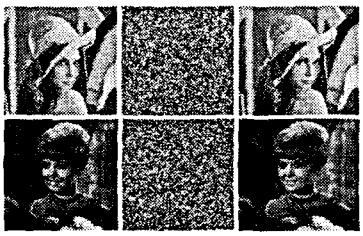

그림 2. (위) Lenna영상, (아래) Girl영상 : (a)원영상 (b)암호영상 (c)복호영상

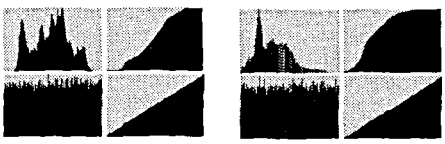

그림 3. (좌) Lenna영상, (우) Girl영상 : (a) 원영상분포도, (b) 원영상 누적분포도, (c) 암호영상 분포도, (d) 암호영상 누적분포도

해보면 Lenna 영상에 대해 원영상의 평균값은 123.47이고 편차는 47.89임에 비해 보기에서 암호화된 영상의 평균값은 73.57 이고 편차는 74.10이 된다. 또한 Girl 영상에 대해서도 원영상의 평균값은 123.47이고 편차는 42.62임에 비해 암호화된 영상의 평균값은 127.29이고 편차는 73.60이 된다.

III. 결 론

일반적으로 텍스트 데이터와 달리 영상데이터는 저장된 자료의 양이 방대하고 따라서 이의 원활한 암호화를 위하여 먼저 영상의 특성을 파악하여 암호화 할 필요가 있다. 이를 위하여 본 논문에서는 logistic 함수를 이용한 chaos 암호화 기법을 이용하여 일 단계 암호화 알고리즘을 구축했다. 이러한 암호화 방식은 블록기반 암호화 기법과 달리 빠른 계산을 할 수가 있고 비밀 키로서 두개의 초기변수를 수신자에게 보내면 된다. 그렇지만 실수 연산을 수행하는 관계로 회수를 높여 암호의 안정성을 높이는 대신 행렬의 기본 변환을 이용한 새 암호화기법을 추가하여 구하였다. 이러한 2단계 암호화 알고리즘에서는 송신자에 정보 전달없이 1단계에서 사용된 logist 함수를 이용하여 생성된 비밀 키와 이를 기반으로 반복 회수 키열을 만들었다. 대신 영상의 LSB 비트 평면 영상을 초기 난수 영상의 킷값으로 사용하였다. 이렇게 두 단계를 통하여 암호화하므로 암호화의 효율성을 높일 수가 있음을 실제 영상에 적용하므로 보일 수가 있었다.

참고문헌

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

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

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

[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] K. Muralii, "Hetrogeneous chaotic systems based on cryptography" , *Phys. Lett. A*, 272, 184-192, 2000

[6] X. Yi, C. K. Tan, C. K. Siew and M. R. Syed, "Fast encryption for multimedia", *IEEE Trans. Consumer Electronics*, 47, 101-107, 2001.