자기환원적 사상함수를 이용한 이미지 암호화

이근무*
*위덕대학교 정보통신공학부

e-mail:kmrhee@uu.ac.kr

Image Encryption Using Self Restoration Mapping Function

Keun-Moo Rhee
*School of Information & Communication Ui-Duk University

통신에서 이미지의 보안을 유지하는 일이 점점 중요한 이슈가 되고 있다. 그러나 기존의 여러 암호화 기법 통신상의 다양한 보안요구를 충족하지 못하고 있는 것이 현실이다. 이 논문에서는 새로운 암호화 전략이 제안되고 구현된다. 이는 통상적으로 카오스라 하는 암화 이미지와 원 이미지 간에 관계가 카오스적인, 패턴이 없는 무질서와 혼합적 구조를 가지고 있으나 그럼에도 불구하고 원래의 이미지로 돌아 올 수 있다. 여기에서는 이러한 카오스적 형태의 암호화 전략을 제안하고 구현하여 향후 나아간 연구를 자극하고자 한다.

*Keywords:*Self Restoration; Mapping Function ; Image encryption; Arnold map
..

1. 서론

급속하게 멀티미디어 저작시스템과 전자출판 디지털 멀티미디어 데이터의 이용이 인터넷상에서 폭발적으로 증가하면서 이들 저작물들이 쉽게 불법으로 유통되고 거래되어 심각한 문제로 대두되고 있다. 이런 현안에 대해서 이를 보호하기 위한 다양한 저통적인 암호화 전략들이 제안되고 구현되어 이용되고 있다. [1-2] 이러한 연구들이 그 타당성과 적응성 경제성 등에서 다양한 제한을 가지고 있다. 여기에서 카오스 이론이 빠르게 발달되어 가고 이를 이용한 카오스 기반의 암호화 연구들이 시작되고 있다. [3-7] 카오스 시스템은 여러 중요한 특성을 지닌다. 예른 들어 카오스 시스템에서 초기조건에 대한 민감성, 즉 초기 조건에 민감하다는 것은 초기상태의 차이가 아주 작은 두 계가 위상공간에서 전혀 다른 궤적을 따라 움직일 수 있다는 것이다.

2. 관련연구

통신에서 이미지의 보안을 유지하는 일이 점점 중요한 이슈가 되고 있다. 그러나 기조의 여러 암호화 기법 통신상의 다양한 보안요구를 충족하지 못하고 있는 것이 현실이다.

수학자 아놀드는 1960 년대 원래의 이미지로 돌아 올 수 있으며 서 카오스적인패턴이 없는 무질서와 혼합적 구조를 가지고 있으며 원래의 이미지로 돌아 올 수 있는 구조를 제안하였다. 이를 고양이의 그림 예증하여 이를 아놀드의 고양이 지도(Arnold' cat map) 이라 부른다. [8]

이는 다음과 같은$\Gamma : R^2 \rightarrow R^2$ 사상 함수이다.

$\Gamma : (x,y) \rightarrow (x+y, x+2y) \bmod 1$

이를 행렬의 형태로 표시하면

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1$$

여기에서

. $x' = (x+y) \bmod 1$
$y' = (x+2y) \bmod 1$

이 2차원 평면은 다양면체인 원환체(torus)의 표면으로 설명되고 있다. x.y는 원환체 표면의 경도와 위도를 나타내는 변수이다.

이 맵핑에서는 그 영역(고양이의 얼굴)이 유지되는 특징을 가지고 있다.

이는 ansov에 의해 카오스 동역학적인 특성을 가진다는 것이 이미 증명되었다. [9] 그리고 아놀드 맵은 두 개의 Lyapunov 지수함수들로 표시 될 수 있다. [10]

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod} 1$$

위의 식에서 x',y' 가 모듈라 연산 1 로 계산되었으며 그 행렬식(determinant) 이 1 이므로 영역보존 자기환원적 성질을 가지고 있으며 Lyapunov 특성방정식(Lyapunov characteristic equation) 는 다음과 같다. [11][12]

$$\left| \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} - \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \right| = 0$$

즉

$$\begin{vmatrix} 1-\lambda & 1 \\ 1 & 2-\lambda \end{vmatrix} = \lambda^2 - 3\lambda + 1 = 0$$

이 특성방정식에서 고유치(eigenvalue) 는 다음과 같다.

$$\lambda_{\pm} = \frac{1}{2}(3 \pm \sqrt{5})$$

이 고유치를 이용하여 고유벡터(eigenvector)를 구하자.

먼저 $\lambda_{+} = \frac{1}{2}(3+\sqrt{5})$ 를 이용하여 계산된 고유벡터를 v1 이라하자

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} v1 = \frac{3+\sqrt{5}}{2} v1$$
$$= \left(\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} - \frac{3+\sqrt{5}}{2} I \right) v1 = 0$$
$$= \begin{bmatrix} -\frac{1+\sqrt{5}}{2} & 1 \\ 1 & \frac{1-\sqrt{5}}{2} \end{bmatrix} v1 = 0$$

2 행의 첫 원소를 제거하기 위하여 1 행의 첫 번째 원소의 역수 $-\frac{2}{1+\sqrt{5}}$ 를 2 행에 곱한후 그를 1 행과 곱한후 그 결과를 2 행에서 빼준다.

2 행에 첫행을 빼서 2 행에 첫행을 곱하면

$$\begin{bmatrix} -\frac{1+\sqrt{5}}{2} & 1 \\ 1-\frac{-(1+\sqrt{5}}{2}(-\frac{2}{1+\sqrt{5}} & \frac{1-\sqrt{5}}{2} - 1(-\frac{2}{1+\sqrt{5}}) \end{bmatrix} v1 = 0$$

따라서 첫번째 고유벡터는

$$0 = -\frac{1+\sqrt{5}}{2}x + y$$
$$y = \frac{1+\sqrt{5}}{2}x = \Phi x \,(\Phi \text{는 } golden\, ration)$$

이를 풀면 고유벡터 $v1 = \begin{bmatrix} 1 \\ \frac{1+\sqrt{5}}{2} \end{bmatrix}$

같은 방법으로 $\lambda_{-} = \frac{1}{2}(3-\sqrt{5})$ 를 이용하여 풀면

λ_{-} 에서 고유벡터는

$$y = -\frac{1}{2}(1-\sqrt{5})x = \Phi^{-1}x \,(\Phi \text{ 는 } golden\, ratio)$$

$$v2 = \begin{pmatrix} 1 \\ \frac{1-\sqrt{5}}{2} \end{pmatrix}$$

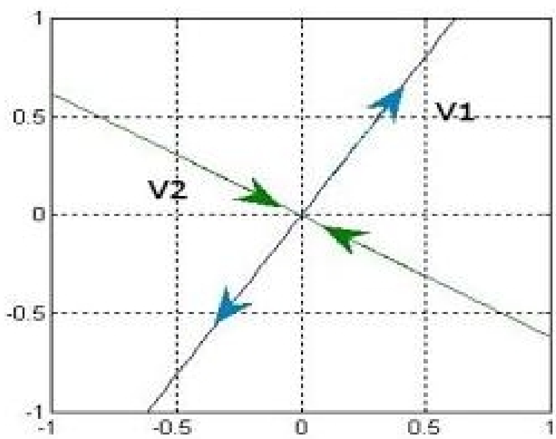

그림 1 고유벡터 plot

따라서 행렬에 대한 $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$

$$\lambda_+ = \frac{1}{2}(3+\sqrt{5}) \approx 2.6180..., v1 = \begin{bmatrix} 1 \\ \frac{1+\sqrt{5}}{2} \end{bmatrix} \approx \begin{bmatrix} 1 \\ 1.6180 \end{bmatrix}$$

$$\lambda_- = \frac{1}{2}(3-\sqrt{5}) \approx 0.38196..., v2 = \begin{bmatrix} 1 \\ \frac{1-\sqrt{5}}{2} \end{bmatrix} \approx \begin{bmatrix} 1 \\ -0.6180 \end{bmatrix}$$

3. 실험

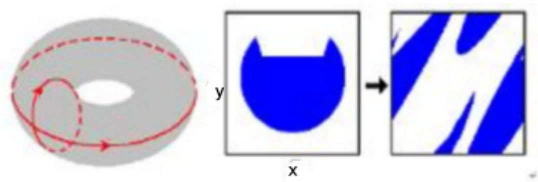

그림 2 cat 이미지

$$\Gamma\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod 1$$

위의 식은 그림의 토르스(torus) 와 같이 x,y 방향으로 비틀림(shear)이 일어난다. 그림은 이 현상을 보여주고 있다. 그리고 위의 식에서 x',y' 가 모듈라 연산 1 로 계산되었으124×124며 그 행렬식(determinant) 이 1 이므로 영역보존 자기환원적 성질을 가진다. 예를들어보자 행렬의 크기가 같은 (a/n, b/n) 좌표평면에서 그림의 한 픽셀을 예를 들어보자. 여기에서 a,b , n은 정수이다. 그리고 $0 \le a < n$, $0 \le b < n$.

$$\Gamma\left(\begin{bmatrix} a/n \\ b/n \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} a/n \\ b/n \end{bmatrix} \bmod 1$$
$$= \begin{bmatrix} (a+b)/n \\ (a+2b)/n \end{bmatrix} \bmod 1$$
$$= \begin{bmatrix} (a+b)/n \bmod 1 \\ (a+2b)/n \bmod 1 \end{bmatrix}$$

예를들어보자 행렬의 크기가 124×124 같은 그림의 좌표평면에서 한 픽셀을 예를 들어보자

좌표 $\begin{bmatrix} 32 \\ 13 \end{bmatrix}$을 예를들어 보자.

$$\Gamma\begin{bmatrix} 32/124 \\ 13/124 \end{bmatrix} \Rightarrow \begin{bmatrix} (32+13)/124 \\ (13+2*32)/124 \end{bmatrix} \bmod 1 = \begin{bmatrix} 45/124 \\ 58/124 \end{bmatrix} \Rightarrow$$
$$\begin{bmatrix} 103/124 \\ 37/124 \end{bmatrix} \Rightarrow \begin{bmatrix} 16/124 \\ 53/124 \end{bmatrix} \Rightarrow \begin{bmatrix} 69/124 \\ 122/124 \end{bmatrix} \Rightarrow \begin{bmatrix} 67/124 \\ 65/124 \end{bmatrix} \Rightarrow$$
$$\begin{bmatrix} 8/124 \\ 73/124 \end{bmatrix} \Rightarrow \begin{bmatrix} 81/124 \\ 30/124 \end{bmatrix} \Rightarrow \begin{bmatrix} 111/124 \\ 17/124 \end{bmatrix} \Rightarrow \begin{bmatrix} 4/124 \\ 21/124 \end{bmatrix} \Rightarrow$$
$$\begin{bmatrix} 25/124 \\ 46/124 \end{bmatrix} \Rightarrow \begin{bmatrix} 71/124 \\ 117/124 \end{bmatrix} \Rightarrow \begin{bmatrix} 64/124 \\ 57/124 \end{bmatrix} \Rightarrow \begin{bmatrix} 121/124 \\ 54/124 \end{bmatrix} \Rightarrow$$
$$\begin{bmatrix} 51/124 \\ 105/124 \end{bmatrix} \Rightarrow \begin{bmatrix} 32/124 \\ 13/124 \end{bmatrix}$$

위와 같이 15 회의 반복 연산 후에는 원래의 좌표로 복귀하게 된다.

4. 결과

자기환원적 사상함수를 이용한 이미지 암호화 복호화 과정은 다음과 같다.
제안된 암호화 기법은 암호화 과정이 곧 복호화 과정이 되는 카오스적이고 자가환원적인 특징을 가지고 있다. 이런 특징으로 간단하고 효율적으로 이미지의 보안을 유지 할 수 있다는 것이 특징이다

그림3 원 이미지

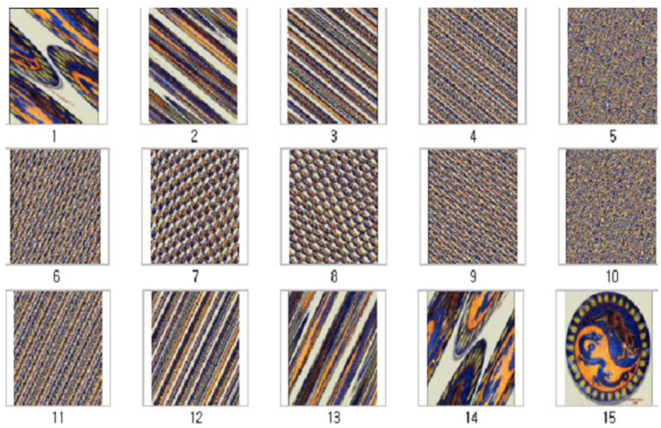

그림 4. 15 단계를 거쳐 원래의 이미지로 복귀한 원 이미지

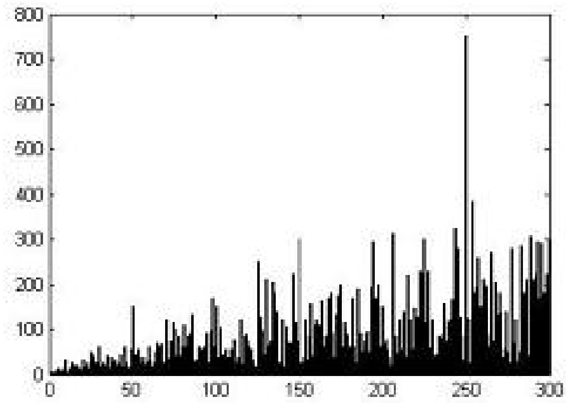

그림 5 이미지 크기와 반복회수 그래프

위의 그래프는 픽셀 단위의 이미지의 크기와 반복 횟수 간 빈도 분포를 보여주고 있다. 여기에서 이미지의 크기에 따른 정규적인 분포 특성을 보이지는 않고 있으나 대략 이미지 크기와 분포간의 관계는 다음과 같이 추측할 수 있다.

1. $\prod(n) = 3n$ if and only if $n = 2 \bullet 5^k$ for $k = 1, 2, \ldots$
2. $\prod(n) = 2n$ if and only if $n = 5^k$ or $n = 6 \bullet 5^k$ for $k = 1, 2, \ldots$
3. $\prod(n) \le \frac{12n}{7}$ for all other choices of n

그림 6 추측된 이미지 크기와 반복회수

5 . 결론

제안된 암호화 기법은 암호화 과정이 곧 복호화 과정이 되는 카오스적이고 자기 환원적인 특징을 가지고 있다. 이런 특징으로 간단하고 효율적으로 이미지의 보안을 유지 할 수 있다는 것이 특징이다. 그러나 적용된 사상함수 자체가 정방 행렬적 구조를 가지는 제한적 응용과 적용에 한계가 있다. 이후 이를 다양한 이미지에 간단하고 효율적으로 적용될 수 있는 방법들이 제안되기를 기대한다.

참고문헌

[1] 강혁 외 2인, 이동통신환경에서의 타원곡선 암호 알고리즘을 이용한 이미지 분배에 대한 지불 프로토콜, 2002 년, 한국멀티미디어 학회 추계학술 발표논문집.

[2] S.S. Maniccam, N.G. Bourbakis, Pattern Recognition 37 (2004) 725.

[3] S. Li, X. Zheng,, Cryptanalysis of a Chaotic Image Encryption Method, Scottsdale, AZ, USA, 2002, in: Proceedings IEEE International Symposium on Circuits and Systems, vol. 2, 2002, pp. 708--711.

[4] F. Beldhouche, U. Qidwai, Binary Image Encoding Using 1D , Chaotic Maps, in: IEEE Annual Technical Conference, 11 April 2003, pp. 39--43.

[5] Y. Mao, G. Chen, Chaos-Based Image Encryption, Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics, Springer-Verlag, Berlin, 2003.

[6] G. Chen, Y. Mao, C.K. Chui, Chaos Solitons Fractals 21 (2004) 749.

[7]A. Uhl and A. Pommer, Image and Video Encryption: From Digital Rights Management to Secured Personal ,Communication. Boston: Springer Science + Business Media Inc., 2005.

[8]. Kyle Shw, Arnold' at map , 2006: -- http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/fall2005/kshaw/catmappres.pdf

[9]http://www.scholarpedia.org/article/Arnold's_cat_map

[10] J. Andries 외 3 인, The dynamical entropy of the quantum Arnold cat map , Letters in Mathematical Physics Volume 35, Number 4 / 1995년 12월, pp.375-383.

[11] Gabriel Peterson , Arnold' catr map - http://online.redwoods.cc.ca.us/instruct/darnold/maw/catmap.htm

[12]. Wong Kw. 외 2 인, A Fast Image Encryption Scheme based on Chaotic Standard Map:http://arxiv.org/ftp/cs/papers/0609/0609158.pdf

[13] X Y Yu,Chaotic Image Scrambling Algorithm Based on S-DES, Journal of Physics: Conference Series 48 (2006) 349.353

[14]Linhua Zhang 외2 인, An image encryption approach based on chaotic maps, Chaos, Solitons and Fractals 24 (2005) 759-.765