디지털산업정보학회 논문지 제7권 제4호-2011년 12월

선형구조 혼돈계를 이용한 이미지 암호화 방법 연구

조 창 호*·임 거 수**

Research on the Image Encryption Method using a Linear-structure Chaos System

Cho, Chang Ho · Yim, Geo Su

〈Abstract〉

With the rapid growth of digital communication and the internet, the importance of conducting research on data encryption methods is increasing. Some of the pertinent researches that have been conducted so far introduced data encryption methods using chaos systems, and numerous researches are currently being conducted on such methods. The signals produced by the chaos systems are called "determined noise," and if this is applied to data encryption, very effective results can be obtained. Using the Henon map, the relationship between the non-linearity of the chaos system and the strength of encryption was analyzed, and a linear-structure chaos system that uses non-linearity as a variable for encryption strength was constructed. Using the constructed chaos system, an image was encrypted and decoded, and the correlation coefficient of the linear-structure chaos system's performance was calculated and then analyzed.

Key Words : Linear-structure, Encryption, Decryption, Chaos

Ⅰ. 서론

전자기기와 통신의 발달로 컴퓨터나 스마트기기들 간의 통신이 많아 졌고, 전송되는 데이터의 크기 또한 급격히 증가되고 있다. 이러한 현상은 사회가 발전하면서 계속 가중될 것으로 예측된다. 이렇게 많은 양의 데이터가 움직이다 보면 상대적으로 보안에 대한 문제점이 발생하게 되고, 이런 문제점을 처리하기 위해 기존의 암호화 방법을 적용 하게 되었다. 그러나 이러한 기존의 암호화 방법은 암호화의 구조와 내용 그리고 구현방법이 많이 공개 되었고, 더욱이 컴퓨터의 성능이 발달하면서 무단 복호화의 가능성이 높아지고 있다. 이런 문제점을 보완하기 위해 새로운 암호화 방법에 대한 연구가 많이 이루어지고 있고, 그 중 혼돈계를 이용한 암호화 방법 또한 많은 관심을 얻고 있다[1-4].

혼돈계를 이용한 암호화 방법은 잡음을 이용한 암호화 방법과 그 구조가 유사하다. 잡음을 이용한 암호화 방법은 정보신호에 잡음신호를 첨가하여 암호화를 시키는 형태로 구성되고 잡음신호가 충분히 크다면 암호화된 신호는 잡음신호와 같은 특성을 보이게 된다. 이렇게 생성된 신호에서 원본의 정보를 추출하는 것은 거의 불가능한 일이 된다. 그러나 정상적인 상태로 정보를 복원해야

* 배재대학교 물리융합 전기공학과 교수
** 배재대학교 물리융합 전기공학과 전임강사(교신저자)

하는 경우에도 원본 정보신호를 복원할 수 없는 결정적인 단점을 갖게 된다.

혼돈신호는 잡음신호와 유사하지만 혼돈계의 초기값이나 설정값과 같은 매개변수만 다시 설정해 주면 같은 신호를 재생산 할 수 있는 특징이 있어 잡음을 이용한 암호화 방법의 결점을 제거 할 수 있는 효율적인 암호화 방법이라고 할 수 있다[5-6].

Ⅱ. 관련연구

2.1 혼돈신호를 이용한 암호화 방법

혼돈계의 신호를 이용한 암호화 방법중 가장 일반적인 방법은 CKBA(Chaotic key-based algorithm) 방법으로 원본의 정보신호에 혼돈계에서 발생된 신호를 디지털화 시켜 정보신호와 혼돈신호를 논리연산(XOR) 으로 암호화 시키는 방법이다[1].

CBFSC(Chaos-based Feedback Stream Cipher) 방법은 혼돈신호를 이용하여 스트림신호를 암호화 하는 방법이고, ECBFSC(Efficient Chaos-based Feedback Stream Cipher) 방법은 기존의 방법의 문제점을 보완한 방법으로 2007년에 발표 되었다[2]. ECBFS 방법은 혼돈신호로 데이터를 암호화 하는 것이 아니라 혼돈신호에 대응되는 외부 256-Bit 데이터 테이블을 참조하여 암호화 하는 방법이다. 이 방법은 혼돈계의 특성 까지 숨기는 방법으로 기존의 혼돈계 암호화 방법보다 암호화 강도가 높다고 할 수 있다.

Ⅲ. 선형구조 혼돈계의 이미지 암호화

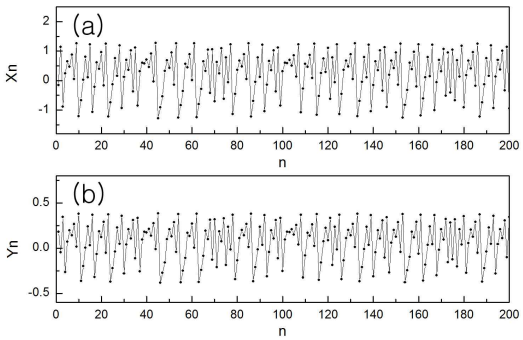
3.1 선형구조 혼돈계

혼돈계를 이용한 암호화 방법에 사용되는 혼돈 시스템은 맵 형태의 혼돈계를 많이 사용한다. 맵 형태의 혼돈계 이면서 복잡도가 높은 혼돈계를 사용하는 것이 암호화된 데이터의 무단 복호화를 막을 수 있는 최선의 방법이 되는 것이다.

우리는 맵 형태의 혼돈계중 암호화에 적용시키기 위해 식 (1)에 보인 Henon-Map 혼돈계를 사용하였다[9].

$$x_{n+1} = y_n + 1 - a\,xn^2 \qquad \text{(식 1)}$$
$$y_{n+1} = b\,x_n$$

식 (1)의 Henon 혼돈계에서 매개변수 a와 b의 값을 각각 1.4와 0.3 으로 설정하고 계산된 시계열 결과 값을 그림 (1)에 보인다.



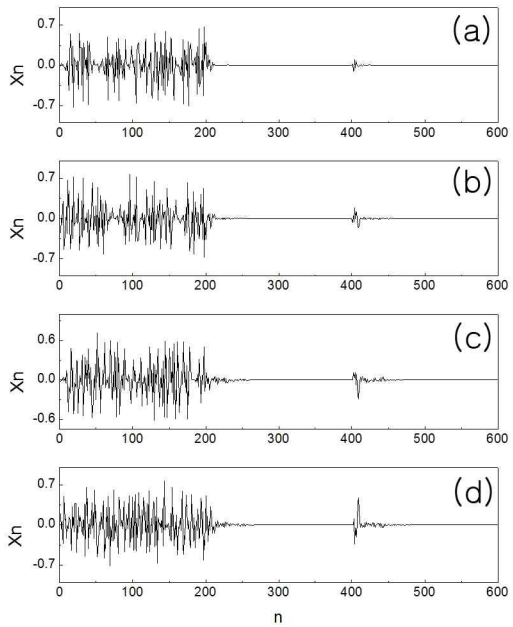
<그림 1> Henon 혼돈계의 시계열

이렇게 발생된 혼돈신호는 잡음과 유사하여 혼돈신호에 이미지 정보를 비트연산(XOR)으로 처리하면 이미지 데이터가 암호화 된다[7-10].

우리는 이런 기존의 암호화 방법을 기초로 하여 암호화 강도를 개선하기 위해 Henon 혼돈계를 선형으로 연결하여 n개를 구성하였다. 그리고 i번째 $x_n^{(i)}$ 값에 $i+1$번째 $x_n^{(i+1)}$ 값의 차이 값을 α의 비율로 더해주면 선형구조에 포함된 혼돈계는 더욱더 복잡해지면서 모두 같은 신호를 발생 하게 구성하였다. 이렇게 구성된 선형구조 혼돈계를 식 (2)에 보인다.

$$z_n^{(i)} = \alpha(x_n^{(i+1)} - x_n^{(i)})$$
$$x_{n+1}^{(i)} = y_n^{(i)} + 1 - a\,(x_n^{(i)} + z_n^{(i)}))$$
$$y_{n+1}^{(i)} = b\,x_n^{(i)} \qquad \text{(식 2)}$$

식 (2)에 보인 혼돈계는 단일 혼돈계보다 복잡한 구조를 갖지만 일정시간 이후에 같은 신호를 발생하기 때문에 각각 암호화와 복호화에 효과 적으로 사용될 수 있다. 그림 (2)에 선형구조 혼돈계의 시계열을 보인다.



<그림 2> 링-구조 혼돈계의 동기화

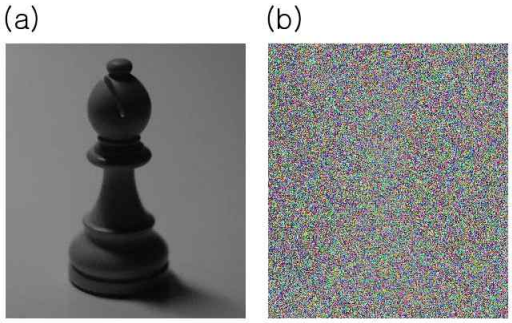
그림 (2)에서 (a)는 혼돈계 $x_n^{(1)}$ 과 $x_n^{(2)}$의 차이 값을 나타낸 것이고, (b)는 $x_n^{(2)}$와 $x_n^{(3)}$, (c) 는 $x_n^{(3)}$과 $x_n^{(4)}$ 그리고 (d)는 $x_n^{(4)}$와 $x_n^{(5)}$의 차이 값을 나타낸 것이다.

x축의 n값이 200이 되는 지점부터 동기화가 시작되어 일정 시간 이후 모든 시스템이 동기화 된 것을 확인 할 수 있다. 그리고 n 이 400 인 지점은 동기화의 강도를 측정하기 위해 $x_n^{(1)}$에 외부의 잡음을 첨가한 것이다. 이런 잡음도 일정시간 이후 모든 혼돈계가 동기화 되는 것을 확인 할 수 있다.

실험 결과로 5개의 혼돈계중 이미지 데이터를 암호화 시키거나 복호화 시키는 혼돈계가 선형구조에 포함된 혼돈계라며 임의의 혼돈계를 사용해도 무방하다는 것을 확인 할 수 있다.

3.2 이미지 암호화 및 복호화

혼돈신호를 이용하여 데이터가 암호화 및 복호화 되는 것을 가시화하기 위해 선형구조 혼돈계에서 $x_n^{(2)}$ 와 $x_n^{(4)}$의 혼돈신호를 사용하여 암호화와 복호화를 실험하였다. 실험에 사용되는 이미지는 실험용으로 제작된 이미지로 0~255의 흑백이미지를 사용하였다. 그리고 실험 결과를 그림 (3) 에 보인다.



<그림 3> 이미지 암호화 결과

그림 (3)의 (b)는 혼돈계 $x_n^{(2)}$의 신호를 0 ~255 디지털 신호로 양자화 시킨 이후 원본이미지 신호화 논리연산(XOR) 시킨 이후의 이미지이다. 육안으로는 원본이미지를 예측할 수 없는 결과를 보이고 있다.

그림(3)의 (a)는 암호화된 (b) 이미지를 $x_n^{(4)}$ 혼돈계의 신호를 0~255 디지털 신호로 양자화 된 신호로 다시 XOR 시킨 결과 값이다. 원본 이미지가 복원된 것을 확인 할 수 있다. 그림 (3)의 암호화 결과는ECBFSC 방법과 같이 혼돈신호의 결과 값과 난수로 구성된 테이블을 참조하여 암호화 시켰다[2].

3.3 암호화 결과의 상관계수 측정

이미지 암호화 방법을 이용하여 암호화된 이미지의 암호화 정도를 측정하는 방법 중 가장 많이 사용되고 있는 것이 암호화된 결과 이미지의 상관계수를 측정 하는 것이다. 상관계수는 특정 위치의 이미지 값과 이웃한 이미지 값의 관계를 나타내는 척도이다. 결과 값이 1에 가까울수록 관계가 있다고 볼 수 있다. 그러므로 암호화된 이미지의 상관계수는 0에 가까울수록 암호화 강도가 높다고 볼 수 있는 것이다[10].

$$\rho_{xy} = \frac{cov(r_x\,,\,r_y)}{\sigma_x \sigma_y} \qquad \text{(식 3)}$$

상관관계를 측정 하기위해 우리는 가로, 세로, 대각선의 이웃한 픽셀의 이미지 값을 사용하였다. 상관계수 계산에 사용된 수식은 식 (3) 과 같다.

$$Cov(r_x,r_y) = \frac{1}{N}\sum(x_i-\overline{x})(y_i-\overline{y}) \qquad \text{(식 4)}$$

$$\sigma_x = \sqrt{\frac{1}{N}\sum(x_i-\overline{x})^2} \qquad \text{(식 5)}$$

$$\sigma_y = \sqrt{\frac{1}{N}\sum(y_i-\overline{y})^2} \qquad \text{(식 6)}$$

식 (3) 의 공분산 $Cov(r_x\,,\,r_y)$는 식 (4)에 보이고 표준편자 σ_x와 σ_y는 식 (5) 와 식 (6) 에 보인다.

암호화된 그림 (3)의 (b) 이미지의 상관계수를 측정한 결과값을 표 <1> 에 보인다.

<표 1> 이미지의 상관계수

상관계수 측정 방향	그림 (3) 이미지	
	(a)	(b)
가로 방향	0.9970	0.0099
세로 방향	0.9963	0.0141
대각선 방향	0.9954	0.0093

계산 결과 암호화된 이미지의 상관계수가 원본 이미지의 상관계수 보다 작은 것을 확인 할 수 있다. 이것은 특정 픽셀의 이미지가 이웃하는 이미지와의 관계가 적다는 것을 나타내고 암호화가 잘 이루어 졌다는 것을 확인 할 수 있는 것이다.

Ⅳ. 결론

정보통신 기술이 발달하고 정보의 양의 기하급수적으로 늘어나고 있는 사회에서 정보의 보안은 상당히 중요한 비중을 차지하고 있다. 그 중 동영상이나 이미지에 대한 암호화는 많은 사람들에게 관심을 받고 있는 분야이다. 이런 시점에서 기존의 암호화 방법을 적용하는 것도 좋은 연구의 목적이 될 수 있지만, 미래지향적으로 새로운 암호화 방법을 연구하고 개발하여 적용하는 것도 간과 할 수 없는 새로운 연구의 방향인 것 같다. 우리는 이미지를 암호화시키기 위해 기존의 암호화 방법이 아닌 혼돈계의 동기화 특성을 이용한 방법을 구성하고, 단일 혼돈계가 아닌 선형으로 연결된 다중 혼돈계를 이용하여 복잡도를 증가 시킨 암호화 방법을 제시하고 그 결과를 실험적으로 보였다. 그리고 그 결과의 타당성을 이미지 암호화 결과와 결과 이미지의 상관계수로 보였다. 우리가 보인 이미지 암호화 방법은 다소 이론적인 부분이 있을지는 모르지만 계속 연구하고 발전시킨다면 추후 기존의 암호화 방법을 대체 할 수 있는 새로운 암호화 분야의 좋은 예가 될 것으로 생각된다[11-12].

참고문헌

[1] J. -C. Yen and J. -I. Guo, “A New chaotic key-based design for image encryption and decryption,” ISACS 2000, Vol 4, 2000.

[2] H. E. Ahmed, H. M. Kalash, and O. S. Farag

Allah, "An Efficient Chaos-Based Feed backs Stream Cipher for Image Encryption and Decryption," Information, Vol. 31. 2007.

[3] F. Fu, Z. Zhang, Y. Chen, and X. Wang, "An Improved Chaos-Based Image Encryption Scheme," LNCS 4487, 2007.

[4] S. BanerJee, G. Ghosh, A. Ray and A. Roy Chowdhury, "Synchronization between two difference time-delayed systems and image encryption," EPL, Vol. 81, 2008.

[5] 문희태, "카오스와 비선형동역학", 서울대학교 출판부, 2007.

[6] 김명훈, "혼돈 진자의 동기화 분석," 서강대학교 대학원, 2000.

[7] 임거수, 김홍섭, "잡음으로 동기화된 혼돈신호를 이용한 이미지 암호화 방법," 한국컴퓨터정보학회논문집, 제13권, 제5호, 2008, pp. 155-162.

[8] 임거수, "다중변수 혼돈계를 이용한 이미지 암호화 방법의 설계 및 구현," 정보보안논문지, Vol 8, No. 3, 2008, pp. 57-64.

[9] 임거수, "혼돈신호에 따른 암호화 정도 분석," 한국정보기술학회 논문지, 제7권, 제6호, 2009. pp. 167-171.

[10] 김홍섭, 임거수, "혼돈신호의 동기화를 이용한 근거리 전자액자 설계," 한국컴퓨터정보학회논문집, 제16권, 제2호, 2011, pp. 201-206.

[11] 노시춘, "네트워크보안 인프라의 차단구조 설계방법," 디지털산업정보학회 논문지, 제2권, 제2호, 2006.

[12] 박영호, "352-비트 암호 알고리즘의 하드웨어 설계," 디지털산업정보학회 논문지, 제5권, 제1호, 2009.

■ 저자소개 ■

조 창 호
Cho, Chang Ho

1985년 3월~현재
배재대학교 (물리융합)전기공학과 교수
1988년 2월 서울대학교 물리학과(이학박사)
1982년 2월 서울대학교 물리학과(이학석사)

관심분야 : 광학의료기기, 자동화장비, 임베디드
E-mail : cho51111@pcu.ac.kr

임 거 수
Yim, Geo Su

2008년 3월~현재
배재대학교 (물리융합)전기공학과 전임강사
2006년 10월 ㈜ 로콜넷 연구소장
2004년 2월 서강대학교 물리학과(이학박사)

관심분야 : 시계열분석, 암호통신, 임베디드
E-mail : lomac@pcu.ac.kr

논문접수일 : 2011년 11월 30일
수 정 일 : 2011년 12월 05일
게재확정일 : 2011년 12월 08일