다중변수 혼돈계를 이용한 이미지 암호화 방법의 설계 및 구현

임 거 수*

요 약

컴퓨터성능의 향상과 인터넷의 발달로 인하여 디지털 이미지의 보안에 대한 중요성이 계속 증가 하고 있고, 이런 현상때문에 혼돈신호를 이용한 암호화 알고리즘은 새롭고 효과적인 이미지 암호화 방법중의 하나로 제시되고 있다. 본 논문에서 우리는 기존의 혼돈신호를 이용한 암호화 방법의 혼돈신호가 특정 값에 변중된 분포로 생성되는 현상에 대한 암호화의 문제점을 보이고 우리가 설계한 다중변수 혼돈계를 이용한 암호화 알고리즘은 혼돈신호의 분포가 생성되는 신호의 전체 영역에 일정한 분포로 발생되는 것을 보인다. 우리는 이미지를 암호화하고 복호화한 결과값으로 우리가 제시한 다중변수 혼돈계를 이용한 암호화 방법의 타당성을 제시한다.

Design and Implementation of Image Encryption Method for Multi-Parameter Chaotic System

Geo Su Yim*

ABSTRACT

The Security of digital images has become increasingly more important in highly computerized and interconnected world. Therefore, The chaos-based encryption algorithms have suggested some new and efficient ways to develop secure image encryption method. This paper is described for the point at issue in all chaos-based encryption method for distribution of a chaotic signals. It has a method for generation of uniformly distributed chaotic signals that we designed secure algorithm of multi-parameter chaotic systems. So we are present validity of the theoretical models for results of image encryption and decryption for proposed method.

Key words : Chaos, Chaotic Signal, Encryption, Decryption

* 배재대학교 과학기술학부

1. 서 론

최근 들어 컴퓨터의 성능과 인터넷통신이 고도로 발달되면서 정보를 보다 빠르고 안전하게 전달하는 방법에 대한 문제점이 계속 발생되고 있고 이에 대한 대책 또한 필요하게 되었다. 이런 문제점을 보완하기 위한 대책으로 새로운 암호화 방법의 필요성이 요구되었고 일부 연구자들은 새로운 방법으로 혼돈계를 이용한 암호화 방법을 선택하게 되었다[1, 2, 10, 11].

혼돈계를 이용한 암호화방법은 일반적으로 잡음을 이용한 암호화방법과 같은 구조로 암호화가 이루어진다. 암호화 하려는 데이터에 잡음신호를 XOR 비트연산이나 그 외의 연산으로 처리하게 되면 잡음신호는 예측할 수 없기 때문에 암호화된 데이터 역시 그 내용을 파악할 수 없게 되어 완벽한 암호화가 되는 것이다[1]. 그러나 이 방법은 암호화한 사람도 결국 복호화 할 수 없는 문제점이 있다. 잡음을 이용한 방법은 암호화 정도는 강하지만 재생산이 불가능해 복호화를 할 수 없는 결정적인 단점이 있기 때문에 암호화방법으로 아무런 효용 가치가 없게 되는 것이다. 그러나 혼돈신호는 잡음과 유사한 특성을 가지고 있지만 초기값만 알고 있으면 발생되는 신호를 똑같이 재생할 수 있는 특성을 가지고 있으므로 암호화에 적당하다고 할 수 있다. 그래서 이런 혼돈신호를 미리 결정된 잡음이라고 말하고 있는 것이다. 혼돈신호가 잡음신호와 시계열적으로 유사한 특성을 지니고 있기는 하지만 발생신호의 모든 영역에 일정한 분포로 나타나지는 않는다. 이와 같이 특정 신호에 편중된 신호는 암호화 처리 이후 암호화된 자료가 무단 복호화방법으로 복호화 될 수 있는 위험성을 지니게 된다. 우리는 이런 문제점에 대한 내용을 제 2장에서 보이고 이러한 문제점을 보완 하는 방법에 대한 결과를 제 3장에서 다중변수 혼돈계의 응용으로 보인다.

우리가 제시한 새로운 암호화 혼돈계인 다중변수 혼돈계에 대한 결과물을 제 4장에서 이미지 암호화와 복호화의 결과로 보이고 암호화 이후 생성된 데이터의 분포가 일정한 분포를 갖고 있다는 것으로 제시한 암호화 방법의 안정성을 보인다.

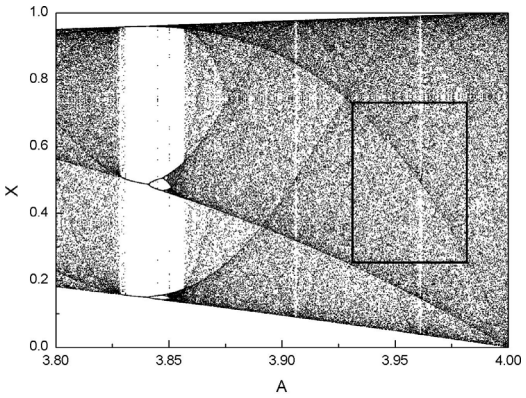
2. 혼돈계를 이용한 암호화 방법

2.1 혼돈계 신호의 구조

혼돈계에 대한 연구는 이학계와 공학계에 상당한 변화의 물결을 일으키고 있고 또한 새로운 연구분야로 부각되고 있다. 혼돈계의 이론은 기존의 과학이 연구하지 않았던 불규칙한 현상을 이론이나 실험을 통해 현상론적으로 연구하고 그 결과로 혼돈계의 지배적인 규칙성을 찾는데 중점을 두고 발전하였다. 그러나 지금은 과학의 전반적인 분야에 응용되고 있고 과학자들 또한 이 현상을 새로운 시각으로 보게 되었다[3, 4].

$$X_{n+1} = aX_n(1-X_n) \tag{1}$$

우리는 이런 혼돈계의 특징을 응용하여 암호화 방법에 적용하려 한다. 혼돈계의 신호는 잡음과 유사하여 시스템을 파악하지 못하면 그 값을 예측할 수 없는 특징을 갖고 있다. 이것이 혼돈계가 암호계에 사용될 수 있는 가장 큰 이유이다. 혼돈신호를 발생하는 대표적인 혼돈계는 Map 구조의 시스템으로 Logistic, Henon, Ikeda 등이 있고, ODE (Ordinary Differential Equation)시스템으로는 Lorenz, Rossler, Duffing, Chua 등이 있다[6]. 여기서 우리는 가장 대표적인 Map 구조인 Logistic 시스템을 식 (1)에 보이고 컴퓨터 시뮬레이션 결과를 (그림 1)에 보인다. (그림 1)은 혼돈계의 특징 중 하나인 갈래질 모양으로 식 (1)에서 a값을 3.80에서 4.00까지 변화 시키면서 획득한 X_{n+1}값을 a축에서 중복해서 그린 결과값이다.



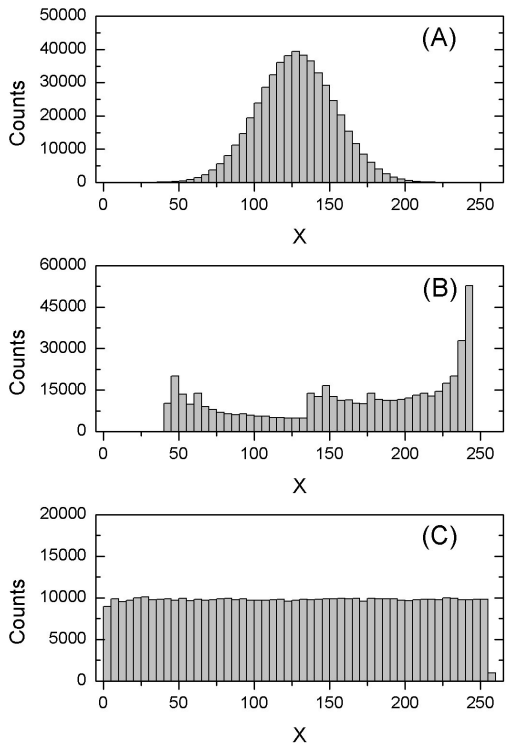
(그림 1) 혼돈계의 갈래질 모양

우리는 이 결과값에서 곡선으로 나타나고 있는 진한 부분들로 혼돈신호가 특정 값에서 반복적으로 많이 나타나고 있다는 것을 확인할 수 있고 이와 같은 분포로 인하여 암호화에 문제점이 발생할 수 있다는 것을 예측한다[7, 8].

이 문제점을 처리하기 위해 (그림 1)에서 사각형으로 선택된 부분의 혼돈신호를 암호화에 사용하면 신호가 반복적으로 많이 나타나는 곡선 부분이 사각형에 대각선으로 포함되어 있기 때문에 X 축에서 보았을 때 일정한 분포의 신호가 발생 되어 혼돈신호가 특성부분에 편중되어 분포되는 문제점을 처리할 수 있게 된다.

2.2 CKBA(Chaotic key-based algorithm)

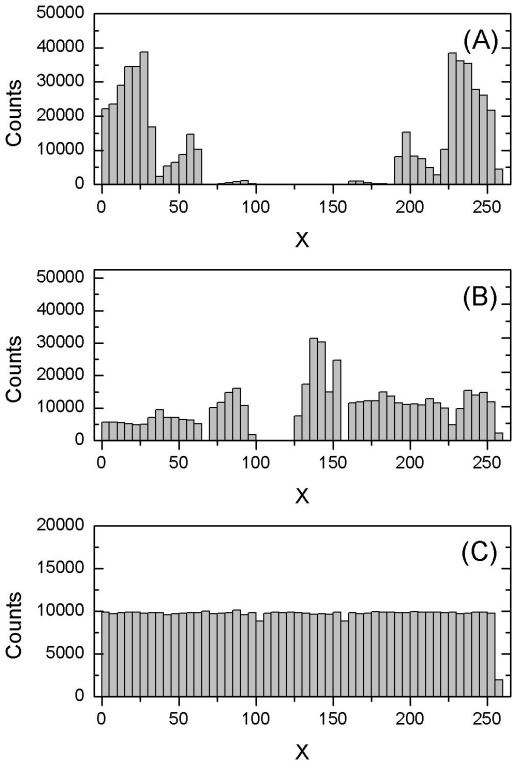
혼돈신호를 이용한 암호화 알고리즘중 가장 대표적인 방법이 CKBA(Chaotic key-based algorithm)으로 원래의 데이터에 혼돈계에서 발생된 신호를 XOR 이나 그 외의 암호화 방법으로 암호화하고 같은 방법으로 복호화 하는 방법이 사용되고 있다[1]. 이 방법이 가능한 이유는 혼돈신호는 결정론적 잡음이라할 수 있기 때문이다. 초기값을 알고 있으면 같은 혼돈신호를 발생시킬 수 있기 때문에 암호화 할 때 사용한 초기값을 암호화의 비밀번호로 사용하고 복호화 할 때 그 비밀번호를 초기값으로 사용하여 원래의 신호로 복귀시키는 것이다[2]. 우리는 이와 같은 혼돈신호를 이용한 암호화 방법의 충실도를 확인하기 위해 임의의 3종류 잡음을 생성하여 컴퓨터 시뮬레이션으로 실험을 하였다. 우리가 사용한 임의의 잡음은 가우시안 분포의 잡음, 혼돈계의 신호 그리고 균일한 분포의 잡음이고 이것의 분포를 나타내는 히스토그램을 (그림 2)에 보인다.



(그림 2) 암호화에 사용될 신호의 히스토그램 분석 결과 (A) 가우시안 분포의 잡음 (B) 혼돈계의 신호 (C) 균일한 분포의 잡음

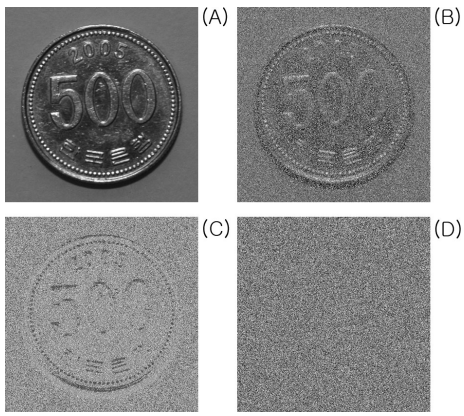
(그림 2)의 (B)는 혼돈신호의 히스토그램으로 계산에 사용된 a값은 3.97값이다. 식 (1) 그림에서 X의 값이 50, 150, 240 부분에서 신호의 분포가 많은 것을 볼 수 있다. 이것은 같은 신호의 갈래질 결과 그림인 (그림 1)에서도 a값이 3.97에서 3부분

의 신호 분포가 많은 곳을 관측할 수 있다. (그림 2)의 (A)와 (C)는 각각 가우신안 분포의 잡음과 일정분포의 잡음을 히스토그램으로 나타낸 결과값이다[9].



(그림 3) XOR을 사용한 암호화 연산 이후의 히스토그램 분석 결과 (A) 가우시안 분포의 잡음 (B) 혼돈계의신호 (C) 일정한 분포의 잡음

(그림 2)에서 보인 두 종류의 잡음과 혼돈신호를 이용하여 일정색(회색)의 이미지 데이타를 XOR 비트연산을 이용하여 암호화시킨 데이터의 분포를 계산하여 (그림 3)에 보인다. 그림에서 나타난 결과값으로 특정 분포의 신호는 암호화 방법을 거친 이후에도 암호화된 데이터가 특정 분포에 같은 비율로 나타난다는 것을 확인 할 수 있다. 이런 현상은 암호화된 이미지가 외형적으로 원본의 이미지와 같은 윤곽을 나타내고 있다는 것을 예측할 수 있게 한다. 우리는 이런 현상을 가시화하기 위해 시험(동전이미지) 데이터를 사용하여 위에서 설명한바와 같이 암호화 방법을 프로그램으로 구현하여 그 결과값을 (그림 4)에 보인다.



(그림 4) 신호로 암호화 시킨 이미지 (A) 원본이미지 (B) 가우시안분포 잡음 이미지 (C) 혼돈신호 이미지 (D) 일정분포 잡음 이미지

(그림 4)의 (A)는 원본이미지이고 이것을 가우시안 분포(그림 2)의 (A)를 갖는 잡음으로 암호화한 결과값을 (B)에 보이고, 혼돈신호((그림 2)의 (B))로 암호화 결과를 (C)에 보이고 일정한 분포((그림 2)의 (C))의 잡음으로 암호화한 결과를 (D)에 보인다.

위의 실험결과로 혼돈신호보다 일정한 분포의 잡음이 암호화 방법으로 효과적인 것을 확인할 수 있다. 그러나 잡음은 암호화에 사용할 수 없는 단점이 있다. 한번 발생된 잡음을 다시 발생 시킬 수 없기 때문이다. 결국 암화에 사용된 다량의 잡음을 다시 재발생 할 수 없기 때문에 복호화 할 수 없는 것이다. 그러나 혼돈신호는 초기 값만 알고 있으면 다시 같은신호를 발생 할수 있는 특징을 가지고 있다. 결론적으로 우리가 원하는 신호는 혼돈계 신호이면서 일정한 분포의 잡음과 같은 분

포를 갖는 혼돈계를 만드는 것이다. 우리는 (그림 1)의 혼돈 갈래질에서 a값을 고정해서 사용하는 기존의 암호화 방법을 변형하여 일정범위를 가변으로 움직이게 하는 혼돈계를 구성하고 그 시스템에 대한 내용을 다음에 보인다.

3. 다중변수 혼돈계 시스템

3.1 다중변수 혼돈시스템 설계

기존의 혼돈신호를 이용한 암호화방법에 사용되고 있는 혼돈계는 고정된 변수 a로 혼돈신호를 발생시켜 그 값으로 데이터를 암호화하는 방법을 사용하고 있다. 그러나 암호화에 사용된 혼돈신호가 특정값에 분포가 되어 있는 신호라면 그 결과는 (그림 4)와 같이 암호화에 문제점을 발생시키게 된다. 우리는 이 문제점을 해결하기 위해 다중변수 혼돈 시스템을 설계하게 되었다. 다중변수 혼돈시스템은 변수 a의 값을 고정하지 않고 변화시키면서 혼돈신호값의 분포를 일정하게 만드는 시스템으로 그 결과값은 (그림 4)의 (D)와 같을 것으로 예측한다.

$$A^{(i)} = [a^1, a^2, a^3, \cdots, a^i] \tag{2}$$

혼돈계의 변수 a를 (그림 1)의 갈래질 모양중 선택된 사각형의 값으로 식 (2)와 같이 설정하고 그 값을 식 (3)의 혼돈계에 적용 한다.

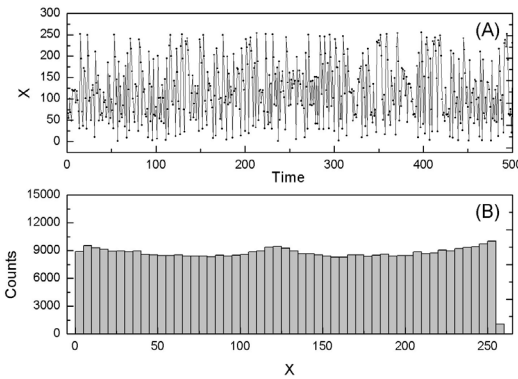
$$X_{n+1} = A^{(j)} X_n (1 - X_n) \tag{3}$$

식 (3)에서 $A^{(j)}$에서 j값은 n *MOD* i값으로 혼돈신호 발생시 변수 a의 값이 일정한 범위로 변하게 만들어 혼돈신호의 분포값이 일정하게 발생하도록 한다.

이렇게 구성된 혼돈신호는 일정분포 잡음과 그 결과값이 같지만 잡음과 달리 초기값만 대입 시키면 다시 같은 신호를 발생시킬 수 있게 된다. 결국 재생산이 가능한 일정분포 잡음을 만들 수 있게 된 것이다.

3.2 다중변수 혼돈 시스템 구현

다중변수 혼돈시스템의 설계방법에 따라 컴퓨터 시뮬레이션 결과 그 값이 제 3.1절 다중변수 혼돈시스템 설계에서 설명한 바와 같이 일정 분포 잡음과 유사함을 (그림 5)에서 결과값으로 보인다.



(그림 5) 다중변수 혼돈계의 결과 (A) 혼돈신호의 시계열 (B) 혼돈신호의 히스토그램

(그림 5)의 (A)값은 다중변수 혼돈시스템에서 발생된 혼돈신호를 시간축에서 본 결과값이고, (B)는 그 결과값의 분포를 히스토그램으로 그린 결과값이다. 실험 결과값이 (그림 2)의 (D)와 같음을 확인하고 우리가 제시한 혼돈계가 일정분포 혼돈계임 보인다.

4. 다중변수 혼돈계의 암호화 방법

4.1 암호화 방법의 설계 및 구현

제 3장의 다중변수 혼돈계 시스템에서 구성한 혼돈계를 사용하여 이미지를 암화하고 복호화하는

프로그램을 구성하고 그 프로그램의 의사코드를 (그림 6)과 (그림 7)에 보인다.

```
 LET array = array(-3.95, -3.96, -3.97, -3.98)

READ original_image_file TO Image(x, y)

SET v = Image(x, y) vertical lines
SET h = Image(x, y) horizontal lines

FOR y = 1 TO v STEP 1 DO
    FOR x = 1 TO h STEP 1 DO
        SET n = n + 1
        SET I = mod(n, size of array)
        A = array(I)
        CALL Logistic_Map with A, xn RETURN xn
        SET seed = digit xn value
        SET image(x, y) = image(y, x) XOR seed
    END DO
END DO

WRITE encrypt_image_file FROM Image(x, y)
```

(그림 6) 암호화 방법의 의사코드

암호화방법은 이미지의 픽셀값을 배열로 변환하여 컴퓨터에 적재하고 다중변수 혼돈계에서 발생되는 혼돈신호를 8Bit 신호로 양자화시켜 그 값을 이미지신호와 XOR 연산으로 암호화 시킨 후 그 이미지를 저장하는 방법으로 실행된다. 이 암호화 시스템에서 암호화의 키값은 변수값을 저장하고 있는 배열값이 암호화의 키값으로 사용되고 복호화 할 때 역시 같은 배열값을 사용해야 복호화 할 수 있게 된다. 키값에 포함된 배열의 개수나 또는 배열의 값이 하나라도 바뀌게 되면 혼돈계의 특성 중 하나인 초기치 민감성 때문에 전혀 다른 복호화 결과값이 나타 나게 되어 원하는 결과를 획득할 수 없게 된다. 이것이 우리가 제시한 암호화 방법의 충실도가 높다는 것을 확인 하게 해주는 내용이다. 복호화 방법의 내용은 (그림 7)에서 의사코드로 내용을 보이고 처리 순서는 암호화 방법의 역순으로 진행된다. 비트 연산자중 XOR 연산자로 데이터를 암호화 시켰기 때문에 암호화는 역순으로 실행시켜 원본의 데이터를 획득하게 한다.

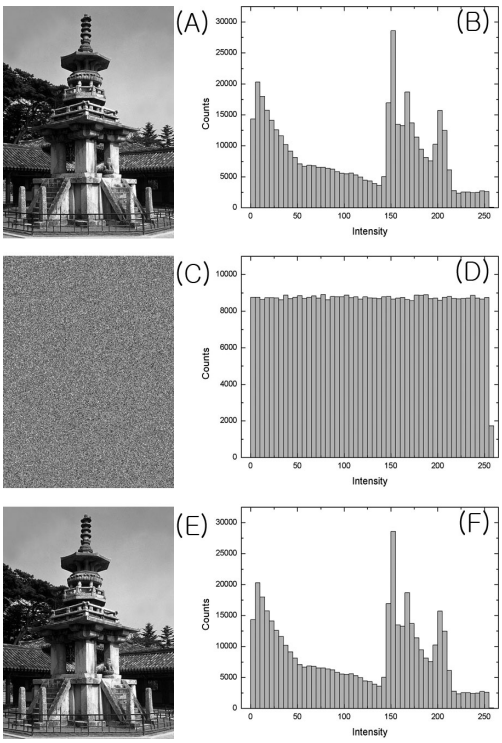
```
LET array = array(-3.95, -3.96, -3.97, -3.98)

READ encrypt_image_file TO Image(x, y)

SET v = Image(x, y) vertical lines
SET h = Image(x, y) horizontal lines

FOR y = 1 TO v STEP 1 DO
    FOR x = 1 TO h STEP 1 DO
        SET n = n + 1
        SET I = mod(n, size of array)
        A = array(I)
        CALL Logistic_Map with A, xn RETURN xn
        SET seed = digit xn value
        SET image(x, y) = image(y, x) XOR seed
    END DO
END DO

WRITE decrypt_image_file FROM Image(x, y)
```

(그림 7) 복호화 방법의 의사코드

위에서 제시한 암호화와 복호화하는 의사 코드에서 확인할 수 있듯이 키값으로 사용된 array 값이 서로 같음을 확인할 수 있다. 본 논문에는 실험결과를 제시하지 않았지만 키값이 바뀌었을 때 복호화 이미지는 원본 이미지를 두 번 암호화 한 이미지의 결과를 보이게 된다.

4.2 암호화 방법의 성능평가

다중변수 혼돈계을 구성하고 암호화와 복호화 프로그램을 수치계산 도구인 Matlab을 사용하여 프로그램을 구동시켜 결과값을 (그림 8)에 보인다. [5] 다보탑의 이미지를 기본이미지로 설정하고 우리가 구성한 다중변수 혼돈계를 이용한 암호화방법으로 이미지를 암호화하여 그 결과를 (그림 8)의 (C)에 보인다. 그림에서 다보탑의 외형을 확인할 수 없음을 보인다.



(그림 8) 다중변수 혼돈계의 결과값 (A) 원보이미지 (B) 원본이미지의 히스토그램 (C) 암호화된 이미지 (D) 암호화된 이미지의 히스토그램 (E) 복호화된 이미지 (F) 복호화된 이미지의 히스토그램

암호화된 이미지의 밝기 분포를 히스토그램으로 계산하여 (그림 8)의 (D)에 보인다. 분포도 또한 일정한 값을 유지하는 것을 확인할 수 있다. 이것은 일정분포 잡음으로 암호화한 결과 와 같다. 암호화된 이미지를 복호화방법으로 계산하여 그 결과값과 히스토그램을 (그림 8)의 (E)와 (F)에 보이고 결과값이 기본이미지와 같음을 보인다. 결론적으로 우리가 설계한 일정분포 혼돈신호를 이용한 이미지 암호화방법을 구현 하고 그 결과값이 우리가 설계한 내용과 같음을 실험적으로 보인다. 이 방법은 기존의 혼돈계를 이용한 암호화 방법에서 발생할 수 있는 혼돈신호의 분포에 따른 문제점을 보완한 새로운 방법으로 보여진다.

5. 결 론

본 논문에서 우리가 설계하고 구현한 다중변수 혼돈계를 이용한 이미지 암호화 방법은 기존의 혼돈신호를 그대로 사용하는 암호화 방법에서 나타나는 문제점을 해결하기 위해 혼돈신호가 발생하는 변수에 따른 모든 영역을 검토한 후 임의의 지역을 추출하여 분포가 일정한 혼돈신호를 암호화에 사용하는 방법으로, 기존방법에서 나타났던 암호화 이후의 데이터에서 보인 특정모양의 분포를 일정하게 하여 암호화를 강하게 만드는 방법이다.

우리가 보인 결과는 실험적인 측면에서 계산 되어 응용성은 고려되지 않았지만, 설계된 내용을 기존에 사용되고 있는 암호화방법 등의 혼돈신호발생기에 적용한다면 암호정도에 대한 충실도를 높일 수 있을 것으로 보인다.

이미지나 문서에 대한 저작권보호에 대한 관심이 급증하고 있는 요즘에 들어, 우리가 구현한 암호화방법은 기업 및 개인의 소중한 지적 재산을 보호하는 암호화 방법에 사용한다면 보다 효율적인 성과를 얻을 수 있을 것으로 본다.

참 고 문 헌

[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] 문희태, “카오스와 비선형동역학”, 서울대학교 출판부, 2003.

[4] 김명훈, “혼돈 진자의 동기화 분석”, 서강대학교 대학원, 2000.

[5] Stephen Lynch, “Dynamics Systems with Applications Using Matlab”, CA : Birkhanuser, 2003.

[6] G. L. Baker and J. P. Gollub, “Chaotic Dynamics : an introduction”, Cambridge University Press, 1996.

[7] Ali H. Nayfeh, “Applied Nonlinear Dynamics”, CA : A Wiley-Interscience Publications, 1995.

[8] Steven Henry Strogarz, “Nonlinear dynamics and chaos : With Applications to Physics, Biology, Chemistry, and Engineering”, Addison-Wesley, 1994.

[9] G. Alvarez, F. Montoya, M. Romera, G. Pastor, “Cryptanalyzing a discrete-time chaos synchronization secure communication system”, chaos solitons and fractals, Vol. 21, 2004.

[10] C. Fu, Z. Zhang, Y. Chen, and X. Wang, “An Improved Chaos-Based Image Encryption Scheme”, LNCS 4487, 2007.

[11] S. BanerJee, G. Ghosh, A. Ray and A. Roy Chowdhury, “Synchronization between two different time-delayed systems and image encryption”, EPL, Vol. 81, 2008.

임 거 수

2004년 서강대학교 물리학과 (이학박사)

2004년～2006년 배재대학교 광 혼돈현상연구단 연구교수

2006년～2008년 (주)로콜넷 연구실장

2008년～현재 배재대학교 과학 기술학부 전임강사