韓國 컴퓨터情報學會 論文誌
第13卷 第5號, 2008. 9.

2008-13-5-3-9

잡음으로 동기화된 혼돈신호를 이용한 이미지 암호화 방법

임 거 수*, 김 홍 섭**

Chaos-based Image Encryption Scheme using Noise-induced Synchronization

Geo-Su Yim*, Hong-Sop Kim**

요 약

컴퓨터의 성능과 인터넷의 발달로 디지털 이미지의 보안에 대한 중요성이 더욱더 증가하고 있고, 그 결과로 혼돈 신호를 이용한 암호화 알고리즘은 이미지를 암호화하는 기술 중 새로운 방법으로 그 내용이 부각되고 있다. 이 논문에서 서로 다른 두 개의 혼돈계를 잡음을 이용하여 동기화 시키는 방법에 대한 연구의 수행 결과를 보인다. 이 동기화 방법으로 이미지 암호화 시스템을 구축하고 석가탑 이미지를 사용하여 구축된 암호화 시스템의 성능을 증명하였다. 연구 결과로 제시한 이미지 암호화 방법은 잡음이 복호화의 키값으로 사용되는 암호화 방법으로 기존의 방법보다 암호화 정도가 강하게 된다. 본 연구에서는 우리는 이 암호화 방법이 효과적이면서 쉽게 적용될 수 있는 새로운 알고리즘이라고 제안한다.

Abstract

The security of digital image has become increasingly important with the development of the computing performance and internet. Therefore, the encryption algorithms exploiting chaos signal have recently attracted considerable attentions as a new method of image-encryption techniques. In this paper, it is demonstrated that two different chaotic systems are synchronized by the methods of noise-induced synchronization. Based on this synchronization method, an image-encryption system is implemented and an image of Seok-Ga-Tap is encrypted as a verification of the performance of our system. The method suggested in this paper in which the noise is used as the key of decryption is superior to the existing methods in the aspect of the degree of encryption. In this paper, we propose that the method is a new effective encryption algorithm as well as an easily applicable one.

▸ Keyword : CKBA(Chaotic key-based algorithm), CBFSC(Chaos-Based Feedback Stream Cipher), 동기화(Synchronization), 혼돈(Chaos), 암호화(Encryption), 복호화(Decryption), 잡음(Noise)

• 제1저자 : 임거수
• 접수일 : 2008. 7. 22, 심사일 : 2008. 8. 21, 심사완료일 : 2008. 9. 25.
* 배재대학교 전임강사 ** 오산대학 교수

Ⅰ. 서 론

정보통신의 발전과 산업이 고도화 되면서 데이터 전송의 고속화와 대량화가 사회 발전의 기본이 되었고 전송되는 데이터의 보안 또한 그 중요성이 증가되고 있다. 자료를 보다 안전하고 빠르게 원하는 목적지로 전송하는 새로운 방법에 대한 필요성이 계속 증가하고 있어 이런 일들에 대한 연구 또한 많은 연구자들로부터 다양하게 이루어지고 있다. 연구자들은 자료를 안전하게 전송하기 위해 기존에 사용되고 있는 암호화 방법들을 통신방법에 적용하고 그 내용의 타당성을 연구하고 있다. 여기서 우리는 기존의 암호화 방법과 다른 비선형 신호를 이용한 암호화 방법에 대한 내용과 그 응용성을 제시한다. 비선형 신호를 이용한 암호화 방법은 혼돈계라는 비선형계를 이용한 방법으로 기본 개념은 정보신호에 잡음과 비슷한 혼돈신호를 첨가하면 정보신호를 잡음과 같은 신호로 바꾸어 감청자가 정보신호를 획득할 수 없게 하는 방법이다. 만약 암호화 방법으로 혼돈신호가 아닌 잡음신호를 사용하여 암호화 한다면 같은 효과를 얻을 수 있지만, 암호화를 시킨 쪽에서도 복호화할 수 없는 문제점이 발생하게 된다. 그 원인은 암호화 할 때 사용된 잡음신호와 같은 신호를 다시 만들 수 없기 때문이다. 그러나 혼돈신호는 잡음신호와 그 특성이 비슷하지만 초기 값을 찾아낸다면 혼돈신호를 재 발생 시킬 수 있는 특징을 가지고 있기 때문에 암호화 방법으로 사용하기 적절한 것이다. 현재 이런 혼돈신호의 초기 값을 키 값으로 하는 암호화 방법을 CKBA(Chaotic key-based algorithm)라 하고 이 방법에 대한 이론 및 응용 결과물이 많이 발표되고 있다. [1] 본 연구에서 CKBA 방법을 기본 모델로 설정하고 키 값으로 사용되는 초기 값을 없애는 방법에 대한 연구를 수행하고 그 결과로 동기화를 이용하여 키 값을 잡음으로 대체하는 방법에 대한 결과를 다음과 같이 제시한다.

Ⅱ. 관련연구

2.1 혼돈신호의 특징

혼돈에 대한 연구는 지난 30여 년 동안 이학 및 공학 계에 상당한 변화의 물결을 일으켰고 또한 새로운 연구 분야로 부각되고 있다. 혼돈의 이론은 기존의 과학이 연구 하지 않았던 불규칙한 현상을 실험이나 이론을 통해 현상론적으로 연구하고 그 배후에 감추어져 있는 혼돈계의 지배적인 규칙성을 연구하는데 중점을 두고 발전하였다. 그러나 지금은 이런 연구가 암호학, 통신학, 생물학, 물리학 및 화학 등의 과학의 전반적인 분야에 응용되고 있고 연구자들 또한 이 불규칙한 현상을 새로운 시각으로 보고 있다.

본 연구에서는 이런 혼돈현상을 암호학의 응용방법 중 하나인 이미지 암호화에 적용하려고 한다. 혼돈신호가 암호화에 사용 되고 있는 이유는 혼돈계에서 발생된 신호가 잡음신호와 형태가 유사하기 때문이다. [3] [4] [5]

혼돈신호와 잡음신호를 시계열 분석 방법으로 분석해 보면 확률분포나 상관관계의 결과 값이 서로 유사한 것을 확인할 수 있고 이런 결과로 혼돈신호가 암호화에 잡음을 대신하여 사용되고 있는 것이다. 이런 암호화 방법으로 사용되고 있는 혼돈계는 Logistic Map, Henon Map 과 Lorenz Equation, Rossler Equation 등이 있고 그 중 대표적인 혼돈계인 Logistic Map을 식(1)에 보인다. [2] [3]

$$x_{n+1} = \mu x_n (1 - x_n) \quad \cdots\cdots (1)$$

x_n은 바로 이전 단계의 혼돈신호이고 x_{n+1}은 계산 이후에 발생되는 혼돈신호이다. 식에서 μ 값은 혼돈계의 매개변수로 μ에 따라 신호가 주기적으로 발생하기도 하고 또는 혼돈신호를 발생하기도 한다. [3] [4] [5]

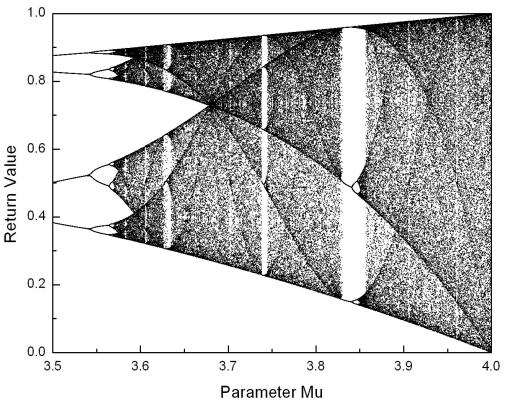

그림 1. 로지스틱 맵의 갈래질 모양
Fig 1. Bifurcation Diagram of Logistic Map

이런 현상을 <그림 1>에 보이고 계산된 결과 값은 혼돈계의 갈래질 모양이라고 부른다. 또 이런 모양의 신호는 간헐성이라는 특성과 같이 일반신호에서 혼돈신호로 넘어가는 혼돈 특성의 하나이다. [3] [5]

〈그림 1〉에서 보인 결과 값 중 우리가 암호화에 사용하려는 혼돈신호는 매개변수 μ의 값이 3.98 부분으로 x_{n+1}의 계산 값이 0 과 1사이에 일정하게 분포되어 있는 값으로 일반적인 잡음과 유사한 분포를 나타내고 있다. 그렇기 때문에 잡음을 대신하여 암호화에 사용하기 적당한 신호라고 할 수 있다.

혼돈신호가 암호화에 사용될 수 있는 또 하나의 특징은 초기치 민감성이다. 두 개의 혼돈계에서 매개변수 μ의 값이 일치 하더라도 서로 약간 다른 초기 값 x_0과 x'_0으로 계산을 수행하면 계산된 결과 값은 시간이 지날수록 큰 차이를 갖는 혼돈의 궤적을 그리게 되는 것이다. 이것 또한 암호화된 데이터를 복원할 때 정확한 초기 값을 대입하지 못하면 궤적이 예측할 수 없는 방향으로 진행되기 때문에 기존의 데이터를 복원할 수 없게 되는 것이다. 이런 특징들로 인해 혼돈신호가 암호화 방법의 한 예로 발전하고 있고 이것에 대한 응용의 필요성 또한 증대되고 있는 것이다. [11][12][13][14]

2.2 혼돈신호를 이용한 암호화 알고리즘

현재까지도 혼돈계를 이용한 암호화 방법은 상당히 많은 저널에 발표 되고 있다. 그 중 가장 대표적인 방법은 Yen 과 Guo 에 의해 발표된 CKBA(Chaotic key-based al- gorithm)방법이다.[1] 이 방법 이후 CKBA를 기초로 하여 스트림 데이터를 암호화하는 방법인 CBFSC (Chaos-Based Feedback Stream Cipher) 방법이 발표됐고 이 방법을 보완한 ECBFSC (Efficient Chaos-Based Feedback Stream Cipher) 방법이 2007년에 발표되었다.[6] ECBFSC은 초기 값으로 발생된 혼돈신호로 이미지 신호를 암호화하는 것이 아니라 외부에서 발생된 256-Bit의 비밀 키 값을 혼돈신호에 대응시켜 그 값으로 데이터를 암호화하는 방법이다. 앞에서 제시한 일련의 암호화 방법의 공통점은 혼돈신호로 데이터를 암호화하기 때문에 암호화하는 부분과 복호화하는 부분에서 모두 동일한 초기 값을 가지고 계산을 해야 한다는 것이다. 여기서 우리는 혼돈신호 시계열 분석을 수행하던 중 이런 초기 값을 잡음신호로 동기화 시킨 이후에 발생하게 하는 방법을 찾아내었고, 이 방법을 이용하면 이미지나 그 외의 정보를 암호화할 수 있는 새로운 방법이 될 수 있음을 확인하고 그 결과를 다음과 같이 제시한다.[9]

2.3 혼돈의 동기화

주기적인 신호의 동기화에 관한 현상은 C.Huygens(1673)가 진자시계를 연구하던 중에 처음으로 관측하였다. 벽에 걸려있는 여러 개의 진자시계가 처음에는 서로 다른 주기로 움직이다가 일정 시간이 지나면 벽으로 진동이 전파 되면서 모든 진자시계의 진자 주기가 같아지게 되는 현상이다.

C. Huygens가 동기화에 관한 현상을 관측한 이후에 많은 과학자와 기술자들에 의해 동기화에 대한 여러 가지 연구가 이루어 졌고 이런 동기화의 종류를 크게 2가지 정도로 나누어 정리해 보면 다음과 같다.[7][8]

① **완전 동기화** (Identical Synchronization)
연결된 두 개의 혼돈계가 $t\to\infty$ 에서 위상 변수들의 차이가 점차적으로 0 으로 수렴해 가는 형태의 동기화를 말한다.

② **위상 동기화** (Phase Synchronization)
위상 동기화는 1996년 Rosenblum등에 의해서 혼돈계에 처음 관측된 현상이다.[7] 여기서 위상이란 위상공간에서 새롭게 정의된 좌표를 의미하며 연결된 두 개의 혼돈계의 위상을 각각 ϕ_1과 ϕ_2라고 정의했을 때 $|\phi_1-\phi_2|=C$ 인 상태로 동기화되는 것을 말한다.

위에서 설명한 바와 같이 혼돈의 동기화 방법 중 위상 동기화는 진폭의 동기는 무관하고 위상의 동기만 관찰하기 때문에 완전 동기화와 같은 모양의 동기화는 일어나지 않는다.[10] 우리가 구현하려는 이미지 암호화 방법은 위상의 값으로 데이터를 암호화하는 것이 아니고 진폭의 값으로 암호화하는 방법이므로 위에 설명한 동기화중 완전 동기화 방법을 사용한다.

2.4 잡음을 이용한 혼돈의 동기화

암호화와 복호화를 하는 두 개의 혼돈계는 일반적으로 서로 다른 시간과 다른 장소에서 계산이 수행되게 된다. 그러나 두 개의 혼돈계가 같은 초기 값으로 계산된다면 두 개의 혼돈계는 동일한 궤적을 그리며 움직이게 될 것이다. 서로 다른 두 개의 혼돈계가 서로 다른 초기 값으로 궤적을 그리고 있어도 같은 양의 잡음신호로 외부에서 궤적을 흔들어 주면 일정 시간 이후 두 개의 혼돈계는 같은 궤적으로 움직이게 된다는 것을 확인 하였다.[7][11]

식(2) 와 식(3)에서 보인 바와 같이 f_1과 f_2 두 개의 혼돈계를 구성하고 초기 값 $x1_0$과 $x2_0$을 서로 다르게 주고 계산했을 때 서로 다른 궤적을 그린다는 것을 그림 2의 (B), (C)에서 보인다. 시계열 그림에서 앞부분은 서로 다른 궤적을 그리고 있는 그림이다. 그림 2의 (D)는 $x1$과 $x2$의 차이값을 그린 시계열 그림으로 앞부분의 신호가 0 이 아닌 것은 두 혼돈계가 서로 다른 궤적을 그리고 있다는 것을 보여준다.

$$x1_{n+1}=f_1(\mu,\ \alpha\xi_n+x1_n-\alpha x1_n) \quad \cdots\cdots (2)$$

$$x2_{n+1}=f_2(\mu,\ \alpha\xi_n+x2_n-\alpha x2_n) \quad \cdots\cdots (3)$$

혼돈계 시스템을 $f(\mu,x)=\mu x(1-x)$ 로 정의하고 두 개의

혼돈신호 $x1$과$x2$ 를 식(2), (3)과 같이 구성하고 잡음의 비율을 0부터 1까지의 값으로 하고 그 값을 α로 정의하였다.

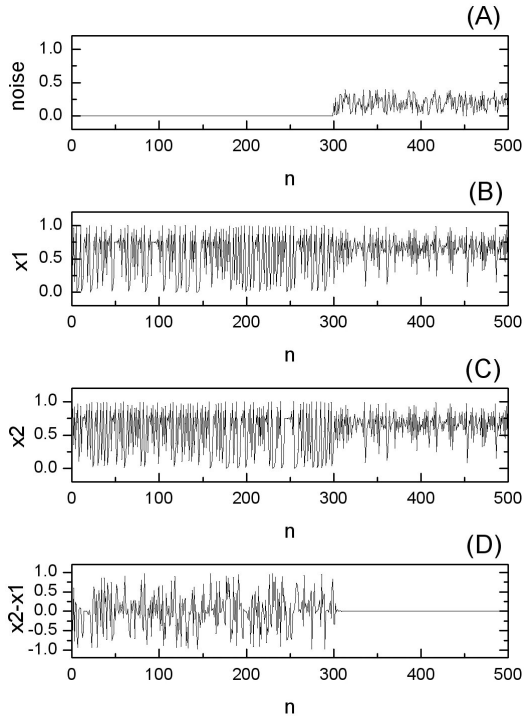

그림 2. 잡음을 이용한 혼돈 동기화의 시계열 그림. 그림(A)는 잡음신호, 그림(B)(C) 혼돈신호, 그림(C)는 두 혼돈신호의 차이
Fig 2. Temporal behaviors of Synchronization with noise (A) noise signal (B)(C) Chaotic signal (D) Difference of Chaotic signal

정의된 값으로 계산한 결과 값을 그림 2에 보인다. 그림 2의 (A)는 $\alpha\xi_n$ 의 값이고 n 값이 300인 지점부터 α값이 0에서 0.4로 식(2), (3)에서 보인 바와 같이 혼돈계에 잡음이 첨가된다. n 값이 350인 지점부터 두 개의 혼돈계가 동기화되기 시작 하는 것을 확인할 수 있다. 그림 2의 (D)를 보면 같은 n 값에서 $x2-x1$ 의 값이 0 이 된 것을 확인할 수 있고 서로 다른 궤적을 그리고 있는 혼돈계는 초기값이 서로 다른 상태에서도 잡음을 이용하여 동기화된 것을 확인할 수 있다. 이런 동기화의 특성을 이용하여 동기화된 두 혼돈계를 한쪽은 암호화용 혼돈계로 사용하고 다른 한쪽은 복호화용 혼돈계로 사용한다면 이 방법이 암호화에 새로운 결과를 줄 수 있을 것이다.

식(2), (3)에서 보인 잡음 ξ 는 0부터 1 사이에 난수가 일정하게 분포되어 있는 잡음이다.

III. 동기화를 이용한 이미지 암호화

3.1 이미지 암호화 방법

혼돈의 동기화를 이용한 이미지 암호화 방법에 대한 알고리즘을 수치계산 도구인 Matlab 으로 구현하고 그 내용의 의사코드를 그림 3에서 보인다. 동기화를 이용한 암호화 방법의 처리 과정은 크게 3부분으로 구분되어 지고 그 내용을 정리해 보면 다음과 같다.

① 두 개의 서로 다른 혼돈계를 암호화시키기 위해 가상의 혼돈계를 구성하고 그림 3의 변수 noise_length에서 보인 바와 같이 잡음을 생성한다. 여기서 생성된 잡음은 0과 1사이의 일정한 분포를 갖는 일반 적인 잡음이다. 이렇게 생성된 잡음을 혼돈계에서 발생된 xn에 0.4 비율로 첨가한다. 이렇게 계속 혼돈신호를 발생시키면서 특정 궤적으로 혼돈계를 동기화시킨다.

② 이렇게 동기화 된 순간의 마지막 xn 을 이용하여 이미지 파일의 픽셀과 계속 발생되는 xn을 8비트로 변환한 값을 XOR로 암호화시키고 암호화된 파일을 이미지파일로 저장한다.

③ 동기화에 사용된 잡음을 파일로 저장한다. 추후 응용 프로그램을 개발할 때 이 잡음을 이미지 파일에 첨가하여 저장한다.

```
LET noise_length = 200
LET n_rate = 0.4
LET s_rate = 0.6
LET mu = 3.98

FOR  n = 1 TO noise_length STEP 1 DO
    CALL Noise_Generator RETURNING noise_value
    SET noise(n) = noise_value
END DO
SET x0 = random value
```

```
FOR  n = 1 TO noise_length STEP 1 DO
    CALL Logistic_Map with mu, x0 RETURNING xn
    CALL Mixed_Signal with noise, xn, n_rate,
        s_rate RETURNING x0
END DO
READ Original_image_file TO img(x, y)
SET ver = img(x, y) vertical lines
SET hor = img(x, y) horizontal lines
FOR y = 1 TO ver STEP 1 DO
    FOR x = 1 TO hor STEP 1 DO
        CALL Logistic_Map with mu, xn
            RETURNING xn
        SET seed = quantization xn value
        SET img(x,y) = img(y, x) XOR seed
    END DO
END DO
WRITE Encrypted_image_file FROM img(x, y)
WRITE Noise_file FROM noise(n)
```

그림 3. 이미지 암호화 의사코드
Fig 3. Pseudo code of Image Encryption

3.2 이미지 복호화 방법

이미지 암호화 방법으로 암호화된 이미지를 원래의 이미지로 복호화하는 방법은 암호화 방법의 역순으로 진행되지만 먼저 저장된 잡음신호를 이용하여 가상의 혼돈계 시스템을 암호화에 사용됐던 초기 xn으로 동기화 시킨 이후에 처리되어야 한다. 이런 내용에 대한 의사코드를 그림 5에 보이고 상세 내용은 다음과 같다.

① 암호화에 사용된 후 저장 되었던 잡음신호를 읽어 들여 혼돈계에 잡음비율 0.4로 첨가 하여 가상으로 동기화를 시켜 암호화 시켰을 때의 초기 xn 값을 찾아낸다.

② 위의 단계로 찾아 낸 xn 값을 초기 값으로 하여 암호화된 이미지의 픽셀 값에 발생된 혼돈 값을 8Bit로 변환한 값을 다시 XOR 하여 원래의 이미지를 복호화한다. 이렇게 복원된 픽셀 이미지를 이미지 파일로 저장한다.

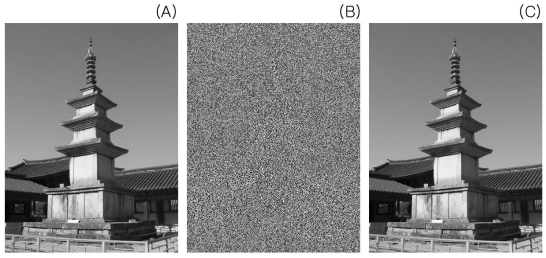

그림 4. 혼돈동기화로 만들어낸 이미지의 암호화 및 복호화
A) 원본이미지 B) 암호화된 이미지 C) 복호화된 이미지
Fig 4. Application of Chaos-Based Synchronization Algorithm
A) Original image B)Encrypted image C) Decrypted image

혼돈의 동기화를 이용한 이미지 암호호방법의 구현을 위해 Matlab을 이용하여 석가탑의 이미지를 그림 3의 암호화 의사코드로 계산한 결과 값을 그림 4의 (B)에 보이고 그림 5의 복호화 의사코드로 계산한 이미지를 그림 4의 (C)에 보인다.

```
LET noise_length = 200
LET n_rate = 0.4
LET s_rate = 0.6
LET mu = 3.98

READ Noise_file TO noise(n)
FOR  n = 1 TO noise_length STEP 1 DO
    CALL Logistic_Map with mu, x0 RETURNING xn
    CALL Mixed_Signal with noise(n), xn, n_rate,
        s_rate RETURNING x0
END DO
READ Encrypted_image_file TO img(x, y)
SET ver = img(x, y) vertical lines
SET hor = img(x, y) horizontal lines
FOR y = 1 TO ver STEP 1 DO
    FOR x = 1 TO hor STEP 1 DO
        CALL Logistic_Map with mu, xn
            RETURNING xn
        SET seed = quantization xn value
        SET img(x,y) = img(y, x) XOR seed
    END DO
END DO
WRITE Decrypted_image_file FROM img(x, y)
```

그림 5. 이미지 복호화 의사코드
Fig 5. Pseudo code of Image Decryption

복호화된 그림 4의 (C)와 (A)가 서로 동일하게 원본 이미지로 복호화된 이미지를 볼 수 있다. 암호화된 이미지 그림 4의 (B)는 원본이미지를 예측할 수 없을 만큼 혼돈신호가 첨가된 이미지를 볼 수 있다.

IV. 성능 평가

4.1 잡음의 비율에 따른 동기화 분석

혼돈의 동기화를 이용한 이미지 암호화 방법은 잡음을 첨가 했을 때 완전 동기화되는 시간이 암호화 성능의 중요한 요인이 된다. 그림 6은 동기화 혼돈식에 잡음의 비율을 바꾸어 가면서 두 혼돈계의 차이 값이 0 으로 수렴하는 길이를 나타낸 결과값이다.

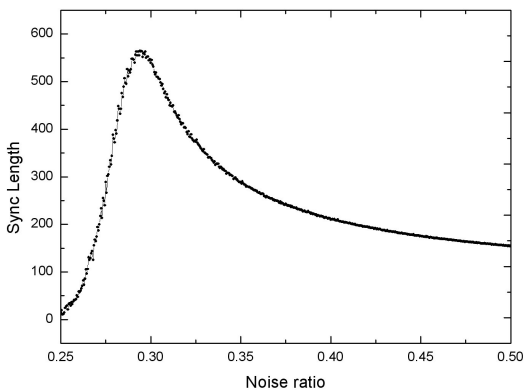

그림 6. 잡음 비율에 따른 동기화 길이
Fig 6. Synchronization Length vs. noise ratio

x축은 잡음의 비율을 나타낸 것이고 y축은 잡음을 첨가했을 때 두 개의 혼돈계가 완전 동기화되는 길이를 나타낸 것이다. 그림에서 보이는 것과 같이 잡음의 비율이 0.3일 때 동기화되는 길이가 가장 긴 것을 확인 할 수 있다. 이것은 혼돈계를 동기화 시킬 때 보다 많은 양의 잡음 정보가 필요하게 되는 것으로 효율성에서 떨어지는 것을 알 수 있다. 우리가 그림 4의 이미지 암호화를 검증하기 위해 사용한 잡음의 비율은 0.4 이고, 대략적으로 동기화가 되기 위한 시간 값은 200 정도 이다. 그림 3과 그림 4에 보인 암호화와 복호화 프로그램의 잡음의 길이 역시 위에서 보인 바와 같이 200으로 설정하여 계산을 수행하였다.

4.2 이미지의 히스토그램 분석

원이미지와 암호화된 이미지의 특성 중 8 Bit 로 이루어진 색의 밝기별 히스토그램으로 암호화된 정도를 측정 하였다. 원이미지의 히스토그램 결과 값인 그림 7의 (B)를 보면 색의 밝기 별로 분포 되어 있는 것을 확인할 수 있다. 이것은 석가탑 사진의 하늘이나 탑의 면부분의 색이 특정 밝기로 분포 되어 있기 때문에 나타나는 결과 값이다.

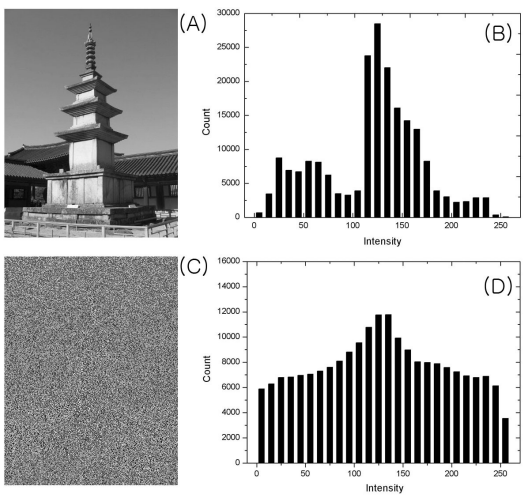

그림 7. 원본이미지와 암호화된 이미지의 히스토그램 분포도
A)원본 이미지 B) 원본 이미지의 히스토그램
C)암호화된 이미지 D)암호화된 이미지의 히스토그램
Fig 7. Histogram of the Original Image and Encrypted Image
A) Original image B) Histogram of Original image
C)Encrypted image E) Histogram of Encrypted image

반면에 암호화되어 있는 이미지는 혼돈신호로 암호화되어 있기 때문에 밝기의 정도에 따라 일정하게 분포 되어 있는 것을 확인할 수 있다. 이것은 암호화된 이미지가 특정 밝기에 대한 의존성이 거의 없음을 의미하고 사진의 외형상으로 원본 이미지를 확인할 수 없음을 알 수 있다.

4.3 혼돈동기화 암호화 방법의 특징

혼돈 신호를 이용한 이미지 암호화 방법은 2.2절에서 설명한 것처럼 현재 여러 방법으로 연구되어 지고 있고 그 결과 또한 새롭게 발표 되고 있다. 그러나 이 모든 방법의 공통점은 고정된 키값을 혼돈계의 초기값으로 설정하여 이후 계산된 혼돈값에 암호화 하고자 하는 정보를 매핑 시키는 방법으로 암호화가 이루어지고 있다. 연구자들 또한 이런 방법을 기초

로 하여 혼돈계를 더욱더 복잡하게 하는 방법으로 암호화의 정도를 강하게 하고 있다. 여기서 우리는 기존의 이런 암호화 방법과 달리 혼돈계의 동기화 방법을 적용하여 서로 다른 초기값으로 계산된 시스템을 특정 시간 이후에 같은 신호가 발생되게 하는 방법을 연구하여 암호화 시스템의 키값을 없애는 방법과 그 결과를 보였다. 우리가 제시한 방법을 기존의 암호화 방법에 적용 한다면 암호화 방법의 성능을 더욱더 향상 시킬 수 있을 것이다.

V. 결론 및 향후 연구

본 논문에서 제시한 잡음으로 동기화된 혼돈계를 이용한 암호화 방법은 이미 발표된 바 있는 CKBA(Chaotic key-based algorithm)방법 중의 한 방법으로 암호화하는 혼돈계의 초기 값을 키 값으로 사용하지 않고 잡음을 이용하여 혼돈계가 자체적으로 동기화가 되도록 유도한 후 발생되는 초기 값을 키 값으로 사용하는 암호화 방법이다.

이 방법은 위에 설명한 바와 같이 추가적인 키 값이 필요하지 않고 또 암호화된 정보 신호와 동기화에 사용된 잡음신호는 구별이 불가능하므로 두 신호를 적절히 섞어 놓으면 잡음신호를 추출할 수 없게 되어 완벽한 암호화 알고리즘으로 사용 될 수 있는 것이다. 본 논문에서 보인 컴퓨터 계산 결과값인 그림 4는 암호화 신호와 잡음신호를 구분하여 계산한 결과값이다. 실험적인 접근 이므로 실험의 확실성을 위해 구분을 지어 계산을 수행하였고 추후 이 방법으로 응용프로그램을 개발하게 된다면 잡음신호와 암호화 된 신호를 섞는 방법에 대한 추가 연구가 필요할 것으로 본다. 잡음으로 동기화된 혼돈계를 이용한 이미지 암호화 방법은 서로 다른 초기 값으로 구동되고 있는 혼돈계를 암호시스템으로 구축하기 위해 같은 잡음을 같은 비율로 각각의 혼돈계에 첨가하여 점차적으로 두 신호를 같게 만드는 방법이다. 위와 같은 방법으로 동기화가 되면 하나의 혼돈 시스템은 암호계로 사용되고, 다른 시스템은 복호계로 사용될 수 있는 것이다. 현재까지 우리가 연구한 결과는 컴퓨터에서 1차원 혼돈계인 Logistic Map 을 기초로 하여 컴퓨터 시뮬레이션으로 연구가 이루어졌지만 암호화의 성능을 향상시키기 위해 기존의 혼돈계보다 복잡한 3차원이상의 고차원 혼돈계를 사용하여 계속 연구를 진행한다면 암호화 효과를 극대화할 수 있는 성과를 얻을 수 있을 것으로 판단된다. 또한 그림 6에 보인 결과와 같이 잡음을 첨가했을 때 Logistic Map 보다 빠르게 동기화되는 혼돈계를 구성하는 것과 동기화에 사용되는 잡음의 종류를 일정 분포 잡음으로 사용하였으나 그 외의 특정 분포 잡음을 사용하면 더 효과적인 동기화 결과를 얻을 수 있을 것으로 보인다. 우리가 제시한 동기화를 이용한 암호화 방법은 저작권이나 지적재산에 대한 관심이 급증하고 있는 요즘에 개인의 소중한 지적 자산을 보호할 수 있는 방법으로 사용한다면 보다 효율적인 결과를 얻을 수 있을 것으로 판단된다.

참고문헌

〔1〕 J.-C. Yen and J.-I.Guo. "A new chaotic key-based design for image encryption and decryption", ISACS 2000, volume 4, pages 49-52, 2000.

〔2〕 K. M. Cuomo, A.V. Oppenheim, and S. H. Strogatz, " Synchronization of Lorenz-based chaotic circuits with applications to communication ", IEEE Trans, vol. 40, pp. 626-633, 1993.

〔3〕 Stephen Lynch, "Dynamics Systems with Applications Using Matlab", CA: Birkhauser, 2003.

〔4〕 Heinz G. Schuster, "Handbook of Chaos Control", Wiley-Vch, 1999.

〔5〕 Ali H. Nayfeh, "Applied Nonlinear Dynamics' CA: A Wiley-Interscience Publication, 1995.

〔6〕 H. E. Ahmed, H. M. Kalash, and O. S. Farag Allah, "An Efficient Chaos-Based Feedback Stream Cipher for Image Encryption and Decryption", Information 31, 121-129, 2007.

〔7〕 Xiao Song Yang, "Concepts of synchronization in dynamical systems", Phys. Lett. A. 260, 340-344(1999)

〔8〕 Thomas S. Parker, Leon O. Chua, "Practical Numerical Algorithms for Chaotic Systems", Springer-Verlag, 1998.

〔9〕 D. Socek, S. Li, Spyros S. Magliveras and B. Furtht "Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption", Security and Privacy for Emerging Areas in Communications Networks, 05-09 Setp. 2005 Page(s): 406-407

〔10〕 E.stanchez, M. A. Matias, and V. Perez-Munzuri, "Analysis of synchronization of chaotic systems by noise: An experimental study", Phys. Rev. E, 56, 4068(1997).

〔11〕 L. Rosier, R. Millerioux, G. Bloch, "Chaos Synchronization on the N-torus and cryptography", C. R.

Mecanique, 969-972, 2004.
〔12〕 G. Alvares, F. Montaya, M. Romera, G. Pastor, "Cr-yptanalyzing a discrete-time chaos synchronization s-ecure communication system", Chaos Solitons and Fractals, 21, 689-694, 2004.
〔13〕 C. Fu, Z. Zhang, Y. Chen, and X. Wang, "An Improved Chaos-Based Image Encryption Scheme", LNCS 4487, pp.575-582, 2007.
〔14〕 S. BanerJee, D. Ghosh, A. Ray and A. Roy Chowdh-ury, "Synchronization between two different time-del-ayed systems and image encryption", EPL, 81, 20006 (p6), 2008

저 자 소 개

임거수

2004년 2월 : 서강대학교 물리학과 이학박사
2004년 ~ 2006년 : 배재대학교 광혼돈제어현상연구단 연구교수
2008년 ~ 현재 : 배재대학교 과학기술학부 전임강사
관심분야 : 신호처리, 비선형 시계열 분석, 네트워크

김홍섭

2008년 2월 : 동국대학교 컴퓨터공학박사
1994년 ~ 현재 : 오산대학 컴퓨터정보계열 교수
관심분야 : 분산운영체제, 임베디드시스템, 유비쿼터스 컴퓨팅