通信情報保護論文誌
第9券 第4號, 1999. 12

# 이산 카오스 함수와 Permutation Algorithm을 결합한 고신뢰도 광영상 암호시스템

홍 진근*, 박 종호*, 황 찬식**

# A high reliable optical image encryption system which combined discrete chaos function with permutation algorithm

Jin-keun Hong*, Jong-ho Park*, Chan-sik Hwang**

요 약

현대 암호 방식은 종래의 선형 대수와 수리이론을 적용한 암호통신을 벗어난 유사 잡음성을 띠는 카오스 신호를 이용한 암호통신을 적용해 오고 있다[1-2]. 본 논문은 1차 permutation 알고리즘을 이용하여 변환된 정보를 2차 이산 카오스 변환 함수를 이용해 암호화하는 광영상 암호시스템을 제안하였다. 제안된 시스템은 키수열 발생기의 출력을 통해 영상정보를 permutation 하는 알고리즘을 설계하였고, 이에 대한 검정을 수행하였다. 또한 본 논문에서는 permutation 알고리즘을 통해 제한적인 카오스 함수의 적용시 발생하는 문제점을 해결하고, 비도를 증가시킴으로써 광영상 암호시스템에 적용시 그 타당성을 검정하였다.

ABSTRACT

Current encryption methods have been applied to secure communication using discrete chaotic system whose output is a noise-like signal, which differs from the conventional encryption methods that employ algebra and number theory[1-2].

* 경북대학교 전자공학과 데이터통신시스템 연구실(hjk@palgong.knu.ac.kr)(sleeper@palgong.knu.ac.kr)
** 경북대학교 전자전기공학부(cshwang@ee.knu.ac.kr)

We propose an optical encryption method that transforms the primary pattern into the image pattern of discrete chaotic function, first a primary pattern is encoded using permutation algorithm. In the proposed system, we suggest the permutation algorithm using the output of key stream generator and its security level is analyzed. In this paper, we worked out problem of the application about few discrete chaos function through a permutation algorithm and enhanced the security level. Experimental results with image, signal demonstrate the proper operation of the implemented optical encryption system.

## I. 서 론

다양한 유형의 정보에 대한 효율적인 암호화 방식에 대한 연구가 진행되고 있다[3-6]. 그 가운데 영상정보에 대한 암호화 방식은 종래에 개발된 전자회로적인 방식과 새로운 개념의 광학을 이용한 암호화 방식 등으로 분류해 볼 수 있다. 전자회로적인 방식은 암호 시스템으로 구현시 고속성과 대용량화가 요구되는 현실에 만족할만한 결과를 얻을 수 없다. 따라서 기존의 전자회로적인 방식에 한계를 벗어나 이에 대한 보완적인 광학을 이용한 암호화 시스템이 부각되고 있다. 광학을 이용한 영상 암호시스템은 고속성과 병렬처리가 가능한 특성을 가지고 있으므로 방대한 양의 정보를 갖는 영상정보 암호화에 적합한 방식으로 고려되고 있다. 이러한 광영상 암호시스템의 유형에는 신용카드, 현금카드에 이용되는 홀로그램 방법, *Refregier*[7], *Javidi*[8] 등에 의해 연구된 위상정보를 이용한 암호화 방법, 편광 특성을 이용한 암호화 방법 등으로 분류할 수 있다.

본 논문은 다양한 광영상 암호시스템 가운데 *Philippe Refregier*가 제안한 위상정보를 이용한 암호시스템 방식에 대한 연구로서 입력 평면과 주파수 평면에 사용되는 두 종류의 난수를 이용하여 원영상의 위상을 변환함으로써 암호화하는 방식에 관한 것이다. 이때 암호시스템에 사용되는 암호키가 되는 두 종류의 난수는 초기조건이 민감한 성질을 갖는 이산 카오스 함수에 의해 발생된다. 통신중에 만약 인허가되지 않은 제3자가 정보를 복호하고자 한다면 두 종류의 정확한 난수 값에 대한 예측이 요구되고, 본 논문에서는 영상 암호시스템에서 키가 되는 난수를 이산 카오스 함수를 이용하여 발생하였다. 이산 카오스 시스템[9-11]은 그 특성상 불결정적이고 불예측성을 갖는 시스템(nonlinear deterministic system)으로 그 신호는 비주기적인 불규칙성을 가지면서 상태공간의 어떤 영역 내부로 제한되어 있다. 또한 카오스 신호는 극히 근접한 초기 조건을 가지는 시스템으로부터 발생하더라도 일정 시간이 경과하면 전혀 다른 궤적을 나타내므로 초기조건에 매우 민감한 특성을 가진다. 실제 암호통신에서 사용되는 이산 카오스 시스템에서 발생하는 신호는 비주기적인 랜덤한 수의 연속이므로 잡음과 유사하게 나타난다. 그리고 카오스 함수는 초기값, 파라미터 등의 모든 조건이 완전히 일치하지 않으면 전혀 다른 난수를 발생시킨다. 이러한 카오스 신호의 특성은 정보의 은닉을 위한 암호통신에 적합하다[12-13]. 카오스 사상(chaos map)은 다양한 시스템에 적용가능한 특징을 가지고 있으나 암호통신에 적용시 카오스 함수의 유형이 제한되어 있으므로 제3자에 의한 도청 및 변조 가능성이 있다. 따라서 본 논문에서는 1차적으로 permutation 알고리즘을 통해 정보를 변환한 후 2차 카오스 함수에 의해 위상정보를 변환함으로써 해당되는 정보의 식별, 유무 판별, 카오스 함수 유형 판별이 불가능하도록 암호시스템을 설계하였으며 permutation 알고리즘, 카오스 함수에 의해 발생되는 난수의 비도 검사를 통해 그 적합성을 평가하였다.

## II. Permutation 알고리즘 설계

### 1. 키수열 발생기

1차 Permutation 알고리즘을 수행하기 위해서는 비도 수준을 만족하는 난수의 랜덤성을 갖는 키수열 발생기가 요구된다. 본 논문은 비도 수준을 만족하는 설계된 키수열 발생기를 이용하여 Permutation을 수행하였다. LFSR(Linear Feedback Shift Register)로 구성된 암호 체계의 비도 수준은 키수열 발생기의 설계에 결정된다. 따라서 키수열의 주기, 난수성, 상관면역도, 선형복잡도 등을 평가하여 만족할만한 비도 수준을 갖는 키수열 발생기의 설계가 요구된다.

### 1.1 주기(Period)

키수열 발생기 가운데 1973년 *Geffe*가 제안한 비선형 시스템은 3개의 *m-LFSR (Maximum Length Feedback Shift Register)* 로 구성되고, 각 레지스터의 초기치가 0이 아닌 출력 수열을 갖는다[14]. 이때 *m-LFSR1*~*m-LFSR3*의 각 쉬프터 레지스터의 차수가 *m, n, k*이면 각 쌍마다 서로 소의 조건에서 발생되는 출력 수열의 주기는 $(2^m - 1)(2^n - 1)(2^k - 1)$값으로 결정된다[15-16].

### 1.2 선형복잡도(Linear Complexity)

*Massey*[17]의 LFSR 합성법에 의해 얻을 수 있는 선형복잡도는 임의의 키수열 발생기가 발생시키는 난수와 동일한 난수를 발생하는 최단의 LFSR로 나타낼 수 있고 이때 선형복잡도를 증가하기 위해서는 후단에 비선형 결합기를 추가한다. *m-LFSR1*~*m-LFSR3*의 각 쉬프터 레지스터의 차수가 *m, n, k*을 갖는 *Geffe* 발생기는 랜덤 특성이 양호하며 선형복잡도는 $m \cdot n + n \cdot k + k$로 결정된다.

### 1.3 상관면역도(Correlation Immunity)

이진 수열이 *m*차 상관면역을 가지는 것은 *m*개의 어떤 입력과도 생성자에 의한 출력사이에는 통계적인 종속성이 존재하지 않음을 의미한다. 상관성 공격은 입출력 조합을 함수적으로 분리한 후 키수열의 각개 공격을 통해 키를 검출해낸다. 만일 상관성 공격에 취약할 경우 LFSR탭과 단수를 알고 있으면 LFSR 초기 키를 찾기 위한 계산복잡도는 크게 낮아진다. *R.A.Rueppel*[18]은 메모리를 갖는 생성자를 제안하였고 *J.Siegenthaler*[19]은 키수열의 분리정복에 의한 상관공격에 대응 가능한 방법을 제안하였다. 이때 메모리가 없는 함수의 비선형 차수($k$)와 상관 면역도($m$) 사이에는 $k+1 \le N-1$, $1 \le m \le N-2$와 같은 *trade off* 특성을 갖는다.

본 논문에서는 키수열 발생기의 각 LFSR 주기의 단수가 31, 59, 91단의 서로소로서 전가산기를 이용하여 구성하였다. 구성된 키수열 함수의 1차 출력 $X_i$ 는 LFSR1의 출력 수열 $a_i$와 LFSR의 출력 수열 $b_i$, 이전 carry $c_{i-1}$(carry의 초기 값은 0), 이전 feedback 메모리 비트 $D_{i-1}$의 전가산기를 통해 구해지고 구해진 출력은 다음과 같다.

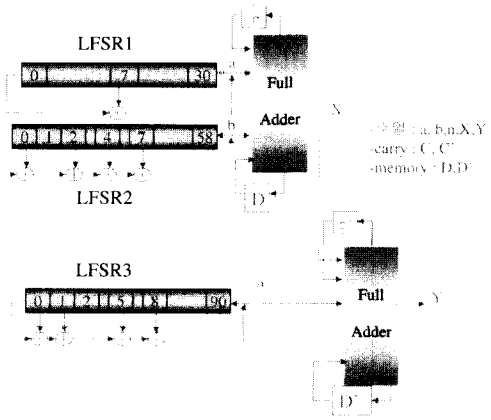



그림 1. 키수열 발생기의 구조
Fig. 1. The structure of keystream generator.

$$X_i = (a_i \oplus b_i \oplus C_{i-1}) \oplus D_{i-1} \quad (1)$$

$$C_i = a_i \cdot b_i \oplus (a_i \oplus b_i) \cdot C_{i-1} \quad (2)$$

$$D_i = b_i \oplus (a_i \oplus b_i) D_{i-1} \quad (3)$$

2차 출력 $Y_i$는 $X_i$의 1차 출력과 $n_i$의 출력의 전가산기를 통해 얻어진다. 이때 $i=0, 1, \ldots$ 이다.

$$Y_i = (X_i \oplus n_i \oplus C'_{i-1}) \oplus D'_{i-1} \quad (4)$$

$$C'_i = X_i \cdot n_i \oplus (X_i \oplus n_i) \cdot C'_{i-1} \quad (5)$$

$$D'_i = n_i \oplus (X_i \oplus n_i) D'_{i-1} \quad (6)$$

본 논문은 비도 수준을 고려하여 키수열 발생기를 설계하였으며 설계된 키수열 발생기는 제안된 permutation 알고리즘의 난수를 발생시키는데 사용하였다. 제안된 비선형 키수열 발생기의 주기는 $(2^{31}-1)(2^{59}-1)(2^{91}-1)$으로 $\simeq 2.85 \times 10^{45}$로 설계하였으며, 선형복잡도는 주기에 근접하며 상관면역도는 최고 차수를 갖도록 설계되었다. 키수열 발생기의 전체 주기로부터 발생된 키수열에 대한 랜덤성 검정을 불가능하므로 유효 비트를 검출하여 국부적인 랜덤성을 검정을 실시하였다. 이때 사용된 비트는 16만비트의 수집된 샘플로 검정을 실시하였으며 검정방안에 대한 적합도 평가는 카이제곱검정 *(Chi-square test)*를 사용하였다[20]. 일반적으로 사용되는 난수성 검사는 문턱치를 결정하는 유의수준(significance level)으로 0.05의 값을 선택하였으며, 일반적으로 많이 사용하는 Frequency test, Serial test, Generalized serial test,

Poker test를 실시하여 검정하였다. 제안된 키수열 발생기는 해당 검정 항목에 대해 난수의 랜덤성을 만족하므로 사용하기에 적합하다.

표 1. 키수열 발생기의 난수성
Table 1. Randomness of Key stream generator.

| Test Items | | 자유도 ($\nu$) | Threshold value ($\alpha \leq 0.05$) | Results |
|---|---|---|---|---|
| Frequency test | | 1 | 3.841 | 1.021 |
| Serial test | | 2 | 5.991 | 1.034 |
| Generalized Serial test | 3-serial | 4 | 9.488 | 1.506 |
| | 4-serial | 8 | 15.507 | 4.981 |
| | 5-serial | 16 | 26.296 | 8.934 |
| Poker test | m=3 | 7 | 14.067 | 8.566 |
| | m=4 | 15 | 24.996 | 13.380 |
| | m=5 | 31 | 44.654 | 22.862 |

## 2. 제안된 Permutation 알고리즘

제안된 permutation 알고리즘은 그림2에서와 같이 구성되고 다수 개의 Block으로 구성된다. 각 Block을 살펴보면 키수열 발생기에서 발생되는 전체 난수열에서 SKey를 사용하여 영상정보의 permutation을 위해 요구되는 8bit의 난수열을 얻는다. 이때 사용되는 SKey는 전체 난수열에서 특정 비트 위치를 결정하여 8bit에 해당되는 값을 선택하도록 하는데 사용된다.

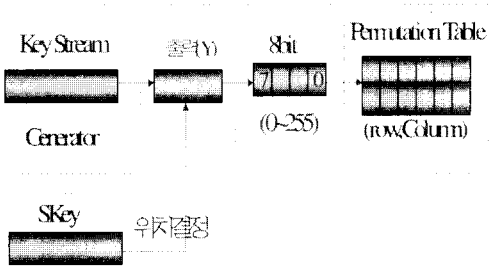



그림 2. permutation 알고리즘을 수행 과정
Fig. 2. Process of permutation algorithm.

원시 다항식 $P_1(x)$이 $x^{31} + x^3 + 1$의 값을 갖는다고 가정하면 이때 LFSR을 이용한 키수열 발생기는 각 Register를 좌측으로 쉬프트를 수행하면서 조합에 의해 키수열을 발생한다. LFSR의 특정 위치의 8비트(1,7,16,20,23,29,31,11)의 값을 초기에 선택했다고 하면 출력 값은 0~255사이의 값을 갖게되고 이 출력 값이 row, column 방향으로 permutation 위치를 결정하는 인자가 된다. permutation 알고리즘은 주어진 원시 다항식으로부터 임의의 8비트를 선택하고, LFSR의 초기 값은 Non all zero의 값을 선택하여 256개의 랜덤한 값을 갖도록 선택할 때 각 LFSR의 Shift 상태에 따른 결과 값을 다음 그림 3에서와 다음 표2를 통해 제시하였다.

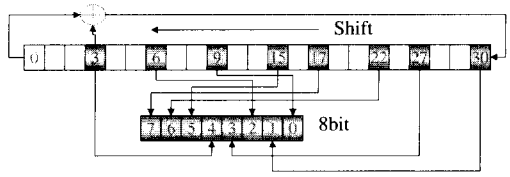



그림 3. SKey를 이용한 특정 8비트를 결정
Fig. 3. decision of selected 8bits using SKey.

위치를 결정하는 8비트를 선택할 때 permutation에 이용되는 값은 31비트중 몇번째 비트에 위치할 것인가를 결정할 비트 위치와 몇 번째 위치한 비트가 언제 선택될 것인가를 결정하는 순서에 랜덤하므로 8비트를 어떤 순서에 어떤 비트를 선택할 것인가에 대한 여부가 row, column 방향으로 영상정보의 permutation 위치를 결정한다.

본 논문에서는 permutation 위치를 결정하는 인자인 특정 8비트의 위치와 순서를 랜덤하게 발생하도록 SKey를 설계하였고, 키수열 발생기를 이용해 출력되는 난수열 가운데 특정 8비트를 결정하도록 하였다. 그림 3에서 LFSR이 31bits의 1010101010101010101010101010101의 초기 값을 갖는다고 가정하였다. 이때 LFSR의 특정 8비트의 순서와 위치를 17, 22, 15, 3, 27, 6, 30, 9와 같이 선택한다면 LFSR 좌측 쉬프트 레지스터와 조합에 의해 난수를 생성시킬 때, 반복되는 횟수 i가 0일 때 해당되는 비트의 결과는 01000110(70)의 값을 갖는다. 수행한 결과는 표2에서 나타내었다. 반복 횟수 i가 1일 경우 선택된 8bits의 결과 값은 10111011(187)의 값을 갖게되며 이 값이 permutation에 이용되는 위치 값이다. 이와 동일한 방법을 이용하여 반복 횟수 i가 255까지 수행되고 각 row, column 방향에 대해 permutation을 수행하면 영상정보에 대해 1차 변형된 결과정보를

표 2. 특정 8비트를 이용한 permutation 테이블
Table 2. Permutation Table using selected 8bits of LFSR.

| 반복 (i) | 순서 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 초기값 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 초기값 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 2 | 초기값 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| 3 | 초기값 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 4 | 초기값 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| ... | | ... | | ... | | ... | | ... | | ... | | ... | | ... | | ... | | ... | | ... | | ... | | ... | | ... | | ... | | ... | | |
| 250 | 초기값 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| 251 | 초기값 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 252 | 초기값 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| 253 | 초기값 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| 254 | 초기값 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 255 | 초기값 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |

얻게된다. row, column 방향에 대한 permutation을 수행할 때 영상정보의 permutation 과정은 주어진 키수열 발생기의 결정이나 특정 8비트의 위치와 순서의 결정 등에 의해 수행된다. 역 permutation 과정에서는 permutation 과정에서 위치를 변환시 역과정을 통해 원래의 영상정보를 검출할 수 있다. permutation 과정은 다음 그림 4에서 제시하였다. 이 테이블은 먼저 반복 횟수 i가 0에서부터 255까지 수행하고 row, column 방향으로 수행한다. 이때 수행 초기에는 permutation 테이블을 초기화하고 permutation 순서는 permutation 테이블을 이용하여 permutation 및 역 permutation이 수행된다.

본 논문에서는 비도 수준을 만족하는 키수열 발생기의 출력 수열을 permutation에 적용하였다. 적용된 출력 수열은 임의의 특정 위치를 결정하는 SKey를 사용하여 특정 8비트를 랜덤하게 결정하고 이로부터 출력되는 8비트의 값을 permutation에 사용되는 값으로 결정했다. 이때 출력되는 8비트 (0~255)사이의 값을 row, column 방향으로 permutation을 수행하였다.

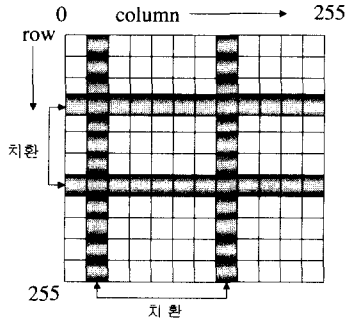



그림 4. Permutation(row, column 방향) 수행
Fig. 4. Process of Permutation(at direction of row, column).

## III. 카오스 함수

카오스 함수는 *Shannon*의 고전 암호 통신으로 거슬러 올라 갈 수 있다[21]. 또한 *Sloane*는 카오스 함수를 통한 랜덤한 permutation에 대한 중요성을 언급했다[22]. 암호 및 통신분야에서는 동기화된 카오스 회로를 근거로 하는 응용이 증가하고 있다[23]. *Oppenheim*은 카오스 신호를 정보신호에

실어 전송하는 마스킹 방법을 제안했다[24]. 이는 카오스 신호에 삽입된 정보신호는 카오스적인 성질을 가지게 되므로 송신측이 사용한 카오스 시스템과 동일한 시스템을 사용할 경우 동기가 가능하고 수신측에서는 *Pecora*가 제안한 동기화 방법을 이용하여 수신된 신호에서 마스킹된 카오스 신호를 제거함으로써 정보신호를 복호한다[25]. 이 방식은 카오스신호와 동일한 레벨의 정보신호를 사용할 때 정확한 검출이 불가능한 것으로 알려지고 있다. 또다른 방식으로는 *Parlitz*가 제안한 카오스 시스템의 파라미터를 변화시켜 이진 정보를 카오스적인 아날로그 신호로 변조하는 파라미터 변조 방식이다[26]. 이는 상이한 파라미터를 갖는 두 개의 카오스 신호를 전송하고 각각의 시스템을 배타적인 동기 특성에 의해 복호한다. 그러나 이 방식은 연속적인 카오스신호를 사용하여 이진정보를 변조하므로 동기화가 어려운 것으로 알려지고 있다. 카오스 함수는 암호, 통신 등 다양한 곳에 다양한 유형으로 응용되어 오고 있으며 그 중 스트림 암호시스템에서 평문을 암호화하기 위해 사용되는 키수열 발생기를 대치하여 사용되기도 한다[27].

본 논문에서는 광영상 정보를 암호화하는데 요구되는 난수를 이산 카오스 함수를 적용했는데 이는 이산 카오스 시스템이 그 특성상 미소한 불확실성이 지속적으로 증폭되어 일정 시간이후에는 커다란 차이를 갖기 때문이다. 사용자가 외부에서 세션 키를 이용해서 암호시스템에 적용가능한 적합한 카오스 함수의 초기 값을 구하고 그 초기 값에서 발생된 난수를 이용하여 정보를 암호화한다. 이때 카오스 함수는 비가역적이므로 초기 값을 알지 못하는 경우 원신호를 복원할 수 없다. 일반적으로 사용되는 대표적인 이산 카오스 사상인 로지스틱 함수는 식 (7)에서 제시한 바와 같다[28].

$$x_{n+1} = \alpha x_n(1-x_n) \qquad (7)$$

이때 파라미터 $\alpha$는 $0 \le \alpha \le 4$의 범위를 가지고, 초기값 $x_0$의 범위가 $0 \le x_0 \le 1$일 때 $x_{n+1}$은 바로 이전 상태값인 $x_n$으로부터 결정된다. 그러나 이에 역으로 $x_{n+1}$이 주어질 때 가능한 $x_n$은 2차 방정식의 해가 되므로 두개의 값을 가진다. 로지스틱 사상(logistic map)은 비가역적인 특성을 갖는다. 이때 $\alpha$는 초기 값에 대한 다음 값의 의존성을 나타내는 감도 파라미터(sensitivity parameter)로서, $\alpha$가 클수록 초기 값의 미소한 변화가 반복된 계산에 의해 현저한 차이를 갖게된다. $\alpha$값에 따른 반복 수행 후의 $x_n$상태에 대해 표3에서 제시하였다. 1보다 작은 $\alpha$의 값에 대해 $x_n$이 반복 수행할 때 0으로 수렴하게 되고, 1과 3사이의 범위에서는 $1-1/\alpha$로, 3보다 클 경우 분기과정을, $\alpha$의 값이 증가함에 따라 정상상태에서의 로지스틱 사상은 안정한 주기 상태에서 무한대의 주기성을 갖는 카오스 영역으로 들어가게 된다.

카오스 사상의 역함수로부터 생성되는 신호를 복호하기 위해서는 이산 카오스 함수의 암호화 과정에서 사용된 초기 값을 복호화 과정에서도 사용하여 동기를 일치시킨다. 이는 수신측에서 암호화된 정보를 복호하기 위해 긴 주기의 펄스열인 제어용 신호를 사용하여 역추정 방법에 의해 역함수로부터 원신호를 복호한다. 제어용 신호에 사용되는 펄스열 신호는 역함수로부터 나오는 신호와 원신호사이의 동기 에러를 0으로 수렴시키기 위해 카오스 사상이 최대가 되는 $x_n$의 값을 선택해야 하고 사용되는 카오스 함수로부터 얻어지는 난수열은 실수 난수 검정을 통과하여야 한다.

표 3. $\alpha$값에 따른 상태 값 $x_n$

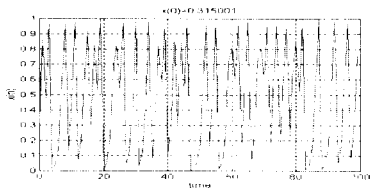
Table. 3. state value $x_n$ at $\alpha$.

| $SP$ \ $x_n$ | 반복 수행 후의 $x_n$ |
|---|---|
| $\alpha<1$ | 0 으로 수렴 |
| $1<\alpha<3$ | $1-\frac{1}{\alpha}$ 으로 수렴 |
| $\alpha>3$ | 분기과정 시작 |
| $\alpha>3.56$ | 비주기의 카오스 성질 |

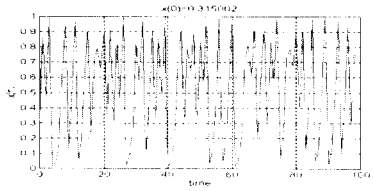
다음 그림 5에서는 이산 카오스 함수의 미세한 초기 값의 변화 영향에 대해 살펴본다. 초기 값 $x_0$ = 0.315001과 미소한 초기 오차를 갖는 $x_0$ = 0.315002의 100회 반복 수행시, 로지스틱 사상은 초기 값의 미소한 변화로 반복수행의 초기 시작 부분에서는 유사하나, 수행 횟수가 증가할 수록 전혀 다른 궤적을 갖는 $x_n$을 출력한다. 본 논문은 또다른 이산 카오스 함수 사상으로 $k$차의 *Chevbyshev* 함수를 사용하였다.

$$x_{n+1} = \cos(k\cos^{-1}x_n), \quad -1 < x_n < 1 \qquad (8)$$

상기 함수로부터 적용된 카오스 난수는 생성된 $x_n$의 절대 값을 이용하여 [0 , 1] 범위에 존재하는 난수를 발생시켰고 사용된 $\alpha$는 4, $k$는 2의 값으로 설정했다.



(a)



(b)

그림 5. 로지스틱 함수의 초기 값에 따른 $x_n$
(a) 초기 값 = 0.315001
(b) 초기 값 = 0.315002

Fig. 5. $X_n$ for initial value of logistic function.
(a) initial value = 0.315001
(b) initial value = 0.315002

## IV. 제안된 모델을 이용한 광영상 암호시스템

### 1. 제안한 모델을 이용한 광영상 암호시스템

본 논문은 1995년 *Philippe Refregier*[7]가 제안한 광영상 암호시스템에 근거한다. 암호시스템은 원영상 정보를 stationary한 white noise의 특성을 갖는 난수를 이용하여 암호화하기 때문에 정확한 키를 알지 못하는 제3자에 의한 복호시 해독되기가 가장 어려운 형태의 정보이다. 제안한 모델을 이용한 암호시스템은 그림 6에서 제시한 바와 같이 비도 수준을 만족하는 난수열을 사용하여 permutation 알고리즘을 통해 1차 암호화를 수행한 후 2차 광영상 암호처리를 수행한다.

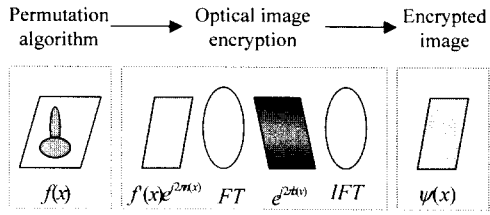



그림 6. 제안된 광영상 암호시스템
Fig. 6. the proposed optical image encryption system.

이때 2차 광영상 암호화를 수행할 때 비주기성을 지니는 카오스 함수를 이용하여 고신뢰도를 갖는 암호화를 수행한다. 제안한 모델의 복호화 과정은 암호화 과정을 역순과정으로 수행한다. 그림6에서 $f'(x)$는 원영상에서 permutation된 영상정보이고, $\psi(x)$는 암호화된 영상정보이다. $n(x)$, $b(x)$는 각각의 독립적인 [0,1] 범위에서 균일한 분포를 갖는 white sequence이다. 만일 permutation을 수행한 영상정보 $f'(x)$를 stationary한 white noise를 갖는 정보로 암호화하려면 먼저, 영상정보 $f'(x)$를 랜덤한 위상 마스크(phase mask)인 $e^{i2\pi n(x)}$ 값을 곱한 후 주파수 평면에서 $h(x)$의 푸리에 변환(Fourier Transform)인 $\hat{h} = e^{i2\pi b(\nu)}$ 정보를 입력 영상정보의 푸리에 변환(FT) 결과 값과 곱한다. 따라서 이 과정은 입력 영상정보와 랜덤 값을 갖는 위상마스크를 곱한 후 푸리에 변환(FT)을 수행하고 또 다른 랜덤 값을 갖는 위상 마스크와 한번 더 곱하는 과정을 수행한다. 수행 결과를 다시 역 푸리에 변환(IFT)을 시키면 암호화된 영상정보 $\psi(x)$를 얻을 수 있다. 암호화된 영상정보 $\psi(x)$는 복소수 형태를 가지며 진폭과 위상으로 표현된다. 전 암호시스템을 수식으로 표현하면 다음 식 (9)으로 나타낼 수 있다. 이때 *은 컨볼루션 연산자를 나타낸다.

$$\begin{aligned}\psi(x) &= IFT\{\ FT\{f(x)\, e^{i2\pi n(x)}\} \times h(\nu)\ \} \\ &= \{f(x)\, e^{i2\pi n(x)}\} * h(x) \end{aligned} \qquad (9)$$

식 (9)에서 첫 번째 과정을 통과한 $f(x)\, e^{i2\pi n(x)}$는 white noise의 특성은 있으나 stationary하지 않다. 첫 번째 과정을 통과한 정보를 두 번째 과정인 주파수 평면에 존재하는 $f(x)\, e^{i2\pi n(x)}$ 정보를 위상마스크인 $e^{i2\pi b(\nu)}$ 과정을 통과하므로써 입력 영상정보를 stationary성을 갖는 white noise로 암호

화하는 것이 된다.

복호화 과정은 상기 암호화 과정을 역순으로 수행하게 된다. 복호화시 암호화된 영상 $\phi(x)$를 푸리에 변환(FT)를 수행하고 암호화에서 사용된 위상마스크와 역수관계를 갖는 $e^{-i2\pi b(\nu)}$를 곱하고, 역 푸리에 변환(IFT)를 수행하면 $f(x)\,e^{i2\pi n(x)}$ 를 얻게 된다. 이때 $|f(x)|^2$ 통해서 양수인 $f(x)$을 선택하고 복호화 과정은 식 (10)에서 제시했다.

$$f(x) = IFT\{ FT\{\phi(x)\} \times e^{-i2\pi b(\nu)} \} \times e^{-i2\pi n(x)} \quad (10)$$

식 (10)에서 $n(x)$와 $b(\nu)$는 암호시스템에서 복호화를 수행할 때 중요한 키의 기능을 갖는다. 정확한 영상정보 $f(x)$를 복호화하거나 암호화된 영상정보의 비도는 $n(x)$와 $b(\nu)$ 값에 의해 결정된다.

본 논문에서는 암호시스템의 중요 파라미터 $n(x)$와 $b(\nu)$를 비주기적인 성질을 갖는 두 개의 카오스 함수를 이용하여 난수를 발생시켰다. 이때 $n(x)$와 $b(\nu)$는 0과 1사이 범위에서 균일한 랜덤 분포를 갖도록 하였으며, 사용자가 입력하는 세션 키를 이용하여 카오스 함수의 초기 값을 생성하였으므로 입력된 세션키 값의 미세한 변화에 따라 상이한 난수를 발생하도록 하였고, 복호 시 정확한 세션 키의 입력이 이루어지지 않으면 원영상 정보를 복호가 불가능하다.

## V. 제안된 암호시스템의 시뮬레이션 및 결과

### 1. 난수성 검정

난수성 검정은 Frequency test, Permutation test, Gap test, Run test를 수행하였으며 실수의 난수성 검정은 0과 1사이 범위에서 발생되는 실수 값을 갖는 난수열 $\langle U_n \rangle$ 이라고 가정하고 식 (11)에서 정의하였다.

$$\langle U_n \rangle = U_0, U_1, U_2, \cdots \quad (11)$$

먼저 난수성 검정을 위해 주어진 실수 값을 정수 값을 갖는 수열 $Y_n$ 으로 변환한 후 검정을 수행하였으며 식 (12)을 사용하였다.

$$Y_n = \lfloor dU_n \rfloor, \langle Y_n \rangle = Y_0, Y_1, Y_2, \cdots \quad (12)$$

이때 $Y_n$ 은 임의로 선택되고 0과 d-1사이 범위에서 독립적이고 uniform(indepedently and uniformly)한 분포를 갖는 정수열로 이루어진다. 제안된 모델을 이용한 암호시스템의 난수성을 검정한 결과는 다음 표4에서 제시하였다.

Permutation과정을 통해 변환된 영상정보는 이산 카오스 함수를 이용하여 2차 변환되었을 때 실수 난수 검정시 해당된 난수성 항목을 모두 만족하는 것으로 평가된다. 이때 transform(변환)과정은 카오스 함수의 난수성 자체가 0과 1사이 범위에서 non-uniform한 분포를 가지므로 이 정보에 대한 uniform한 분포를 가지도록 처리하였으며 이 uniform한 분포를 갖는 난수를 통해 랜덤성을 만족하도록 설계하였다. non-uniform한 분포를 가지는 이산 카오스 함수에 의해 발생된 난수가 랜덤성을 가지는 uniform한 분포를 가지기 위해서는 주어진 식 (12)에서 제시된 변환 함수가 요구된다. $x' = h(x)$가 [0,1]사이 범위일 때 이산 카오스함수의 비선형적인 값을 tent 변환 $T(x)$을 통해 uniform한 선형적인 값을 가지게 한다. 이때 $h$함수는 1 : 1 uniform한 분포를 가지도록 변환한다.

$$x' = h(x) = \sin^2(\pi x/2) \quad (13)$$

tent 변환하에서 초기 값 $x_0$ 이라 가정할 때 변환된 초기 값 $x'(0) = h(x_0)$ 을 갖는다.

$$x_1 = T(x_0), x_2 = T^2(x_0), \ldots, x_k = T^k(x_0), \ldots \quad (14)$$

$y_0 = x'_0$ 반복 값을 계산하기 위해 $y_1 = f(y_0), y_2 = f^2(y_0), \ldots, y_k = f^k(y_0)$ 식을 유도한다. 상기 $f$ 와 $T$의 함수로부터 다음 식 (15)를 유도하여 0과 1사이의 범위에 존재하는 모든 $x$에 대한 선형적인 값을 얻어낸다. 이때 $k$는 1, 2, .... 이다.

$$f^k(h(x)) = h(T^k(x)) \quad (15)$$

식 (12)에서 제시된 변환식은 카오스 함수의 난수성을 결정하며 이 식에 의해 전혀 다른 난수가 발생되므로 이 변환식이 또하나의 키가 된다. 그림 8에서

는 x'축의 비선형적인 값을 tent 변환식을 사용하여 x축의 선형적인 값으로 변환 처리하여 난수가 uniform한 분포를 갖도록 하였다.

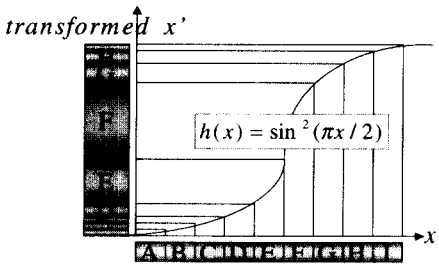



그림 8. 카오스 함수를 정규 분포화한 tent 변환 함수
Fig. 8. tent transformation function of uniform distributed chaotic function.

난수의 랜덤성 검정 결과는 표4에서 나타내었다. 검정항목으로는 Frequency test, Permutation test, Gap test, Run test를 수행하였다. 수행결과는 Permutation을 수행한 영상정보를 chaos와 transform 과정을 수행하였을 때 각 난수성 검정항목을 만족하는 것을 알 수 있다.

표 4. Permutation+Chaos+Transform(Uniform) 과정을 수행한 난수성 검사 결과
Table 4. The result of randomness about permutation+chaos+transform algorithm.

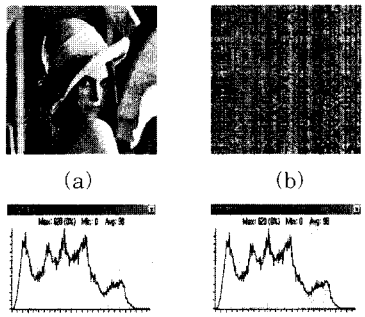
| Test Items | 자유도( $\nu$ ) | Threshold value ( $\alpha \leq 0.05$ ) | Results |
|---|---|---|---|
| Frequency | 29 | 42.557 | 25.623 |
| Permutation | 23 | 35.172 | 17.981 |
| Gap | 11 | 19.675 | 12.961 |
| Run | 6 | 12.591 | 3.953 |

## 2. 시뮬레이션 환경 및 결과

본 논문은 실험영상으로 Lena 영상, 'AB'문자 영상(256×256)을 사용하였다. 영상정보를 1차 permutation 알고리즘을 수행한 후 2차 이산 카오스 변환 함수로 암호화를 수행하였다. 이때 2차 이산 카오스 변환 함수의 주요 키가 되는 로지스틱 사상과 chevbyshev 함수를 사용하였으며 난수성을 만족시키기 위해 uniform 분포를 갖도록 변환 처리를 수행하였다. 1차 permutation 알고리즘 수행시 해당되는 영상정보의 비도 수준을 만족하기 위해 LFSR로 구성된 키수열 발생기를 이용하였고 해당 특정 8비트를 선택하여 추출된 8비트의 정보를 row, column 방향으로 permutation을 수행하였다. 1차 permutation 알고리즘에 사용되는 키수열 발생기를 비도 수준을 만족하도록 설계하였으므로 적용시 그 적합성을 검정하였다. 2차 카오스 함수를 사용할 때 카오스 함수의 특성을 분석하였으며 적용시 그 적합성을 난수성 검정을 통해 분석하였으며 또한 변환함수를 통해 카오스 난수가 갖는 non-uniform한 분포를 uniform한 분포의 난수로 변환하여 사용하였다. 또한 암호화 과정에서 사용되는 $n(x)$는 2차 *Chevbyshev* 함수를 사용하고, $b(\nu)$는 $\alpha=4$를 가지는 로지스틱 함수를 사용하여 실 난수를 발생시켰다. 그림 9에서는 원 영상정보를 permutation 알고리즘을 수행시 원 영상과 비교하였으며, 히스토그램을 함께 제시하였다. 1차 permutation 처리한 영상정보는 동일한 신호성분을 갖는 정보로 히스토그램을 통해 확인할 수 있다. 이것은 permutation 과정만으로는 영상정보가 암호된 영상으로 공격당하기가 쉽다. 또한 이산 카오스 함수를 이용한 방식도 암호화에 사용가능한 이산 카오스 사상이 제한되어 있으므로 자체적으로 사용할 때 문제점이 있다. 따라서 1차 구현이 쉬운 LFSR을 이용한 키수열 발생기의 출력으로부터 유도된 난수열을 통해 permutation 알고리즘을 수행한 후 2차 대표적으로 많이 사용되는 이산 카오스 함수를 사용하여 암호화를 수행할 경우에도 높은 신뢰성를 제공하는 암호시스템을 구축한다.

본 논문에서는 permutation 알고리즘과 이산 카오스 함수를 결합한 고신뢰도를 갖는 광영상 암호시스템을 제안하며 결합된 암호시스템을 블록별로 나누어 비도를 검정하였으며 또한 전체 난수성을 검정하였을 때 난수성 항목을 모두 만족하는 것으로 판단할 수 있다. 원영상 정보가 암호화 과정을 거치면 실수부와 허수부로 구성된다. 암호화된 영상은 원 영상을 전혀 예측 할 수 없고, 정확한 n(x)와 $b(\nu)$의 정보를 통해 복호할 수 있다. 256 × 256개의 Lena 영상에 대한 65536개의 n(x) 정보와 65536개의 $b(\nu)$개의 정확한 난수 값을 요구하므로 임의적으로 복호하는 것은 거의 불가능하다. 원영상과 복호된 영상정보와의 객관적인 척도 PSNR(Peak Signal to Noise Ratio)는 52.1175[dB]를 나타내고, 주관적인 척도인 인간의

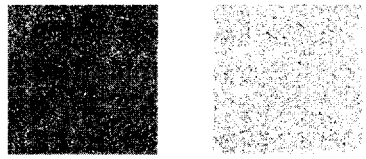
시각으로도 차이를 식별할 수 없으므로 원영상과 거의 동일한 영상이라 할수 있다. 그림 10에서는 암호화에 사용된 키 값과 아주 미세한 0.000001의 오차를 가진 키 값으로 복호를 수행하였다. 이때 암호화 키 값은 0.315001을 사용하였고 복호화 키 값은 0.315002를 사용하므로써 복호된 영상을 나타내었다. 0.000001의 미세한 초기 키 값의 차이가 복호된 영상을 원영상 정보와 비교할 때 전혀 식별할 수 없는 영상임을 알 수 있다. 즉 정확한 키 값을 알지 못하면 원 영상을 전혀 예측할 수 없다.



(a) (b) (c) (d)

그림 9. 원 영상정보와 permutation 처리한 영상정보
(a) 원영상 (b) Permutation 처리영상
(c) 원영상의 히스토그램
(d) Permutation 처리영상의 히스토그램

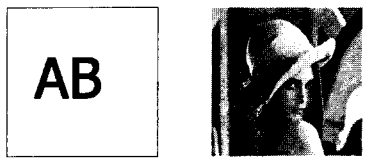
Fig. 10. Original image and permutation processing image
(a) Original image
(b) Permutation processing image
(c) Histogram of original image
(d) Histogram of permutation processing image



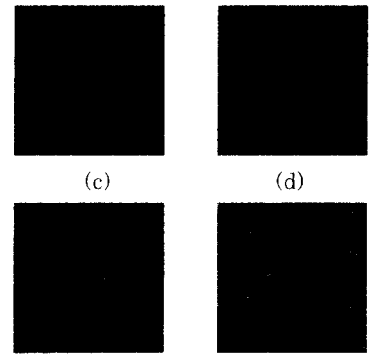
(a) (b)

그림 10. 카오스 함수의 초기 값에 따른 암호 및 복호영상
(a) 초기값 = 0.315001
(b) 복호용 초기 값 = 0.315002

Fig. 10. Encrypted and decrypted image of chaotic function given initial value
(a) initial seed = 0.315001
(b) initial seed for decryption = 0.315002




(a) (b)



(c) (d) (e) (f)

그림 11. 암호화된 영상
(a) Lena 영상 (b) 'AB' 문자 영상
(c) 암호화된 실수부영상(Lena)
(d) 암호화된 허수부 영상(Lena)
(e) 암호화된 실수부 영상(문자 AB)
(f) 암호화된 허수부 영상(문자 AB)

Fig. 11. Encrypted image
(a) Lena image (b) 'AB' character image
(c) encrypted real image(Lena)
(d) encrypted imaginary image(Lena)
(e) encrypted real image(character AB)
(f) encrypted imaginary image(character AB)

## VI. 결 론

본 논문에서는 1차적으로 permutation 알고리즘을 통해 정보를 변환한 후 2차 카오스 함수에 의해 위상정보를 변환하므로써 해당되는 정보의 식별, 유무 판별, 카오스 함수 유형 판별이 불가능하도록 암호시스템을 설계하였으며 permutation 알고리즘, 카오스 함수에 의해 발생되는 난수의 비도 검사를 통해 그 적합성을 평가하였다. 비도 수준을 고려하여 키수열 발생기를 설계하였으며 설계된 키수열 발생기는 제안된 permutation 알고리즘의 난수를 발생시키는데 사용하였다.

제안된 비선형 키수열 발생기의 주기는 $(2^{31}-1)(2^{59}-1)(2^{91}-1)$으로 $\cong 2.85\times10^{45}$로 설계하였으며, 선형복잡도는 주기에 근접하며 상관면역도는 최고 차수를 갖도록 설계되었다. 키수열 발생기의 전체 주기로부터 발생된 키수열에 대한 랜덤성 검정을 불가능하므로 유효 비트를 검출하여 국부적인 랜덤성을 검정을 실시하여 적합도를 평가하였다.

또한 본 논문에서는 암호시스템의 중요 파라미터 $n(x)$와 $b(\nu)$를 비주기적인 성질을 갖는 두 개의 카오스 함수를 이용하여 난수를 발생시켰다. 이때 $n(x)$와 $b(\nu)$는 0과 1사이 범위에서 균일한 랜덤 분포를 갖도록 하였으며, 이산 카오스함수의 비선

형적인 값을 tent 변환 $T(x)$을 통해 uniform한 선형적인 값을 가지도록 설계하였다.

본 논문은 permutation 알고리즘과 이산 카오스 함수를 결합한 고신뢰도를 갖는 광영상 암호시스템을 제안하며 결합된 암호시스템을 블록별로 나누어 비도를 검정하였으며 또한 전체 난수성을 검정하였을 때 난수성 항목을 모두 만족하는 것으로 판단할 수 있다. 원영상 정보와 복호된 영상정보와의 객관적인 척도 PSNR (Peak Signal to Noise Ratio) 는 52.1175[dB]를 나타내고, 주관적인 척도인 인간의 시각으로도 차이를 식별할 수 없으므로 원영상과 거의 동일한 영상이라고 판단할 수 있다. 향후 제안한 광영상 암호화 시스템을 통해 전자 결제, 전자 상거래 등에 적용되는 서명 영상이나 중요한 문서에 적용시 적합하다고 판단된다.

## 참고 문헌


[1] Brassard, G., Modern Cryptography, Chap 6. pp. 79, Springer-Verlag, New York, 1988.

[2] Douglas R. Frey, "chaotic Digital Encoding : An Approach to secure communication," Analog and Digital signal Processing, Vol. 40, No. 10 Oct., pp. 660-666, 1993.

[3] B. M. Macq., J. J. Quisquater, "Cryptology for digital TV broadcasting," Processings of the IEEE, pp. 944-957, June, 1995.

[4] N. Nikolaidis, I. Pitas, "Copyright protection of images using robust digital signatures," Proc.of ICASSP-96, pp. 2168-2171, May 7-10, Atlanta, GA, 1996.

[5] O. Bryngdahl and F. Wyrowski, "Digitalholography-computer generated holograms," in progress in Optics XXVIII, E. Wolf, Ed., North Holland, Amsterdam 1990.

[6] G. Colgate, "Document protection by holograms," in Optical Document Security, R. L. van Renesse, E., Chap. 8, pp. 149-167, Artech House, Boston 1994.

[7] Philippe Refregier, "Optical image encryption based on input plane and Fourier plane random encoding," Optical Letter, Vol. 20, No. 7, pp. 767-769, 1995.

[8] Baharm javidi, "Optical pattern recognition for validation and security verification," Optical Engineering, Vol. 33, No. 6, pp. 1752-1756, 1994.

[9] E. N. Lorenz, "Deterministic non-periodic flow," J. Atmospheric Sci., Vol. 20, pp. 130-141, Mar. 1963.

[10] L. Kocarev, K. Halle, K. Eckert, and L.Chua, "Experimental demonstration of secure communications via chaotic synchronization," Int. J. Bifurcation Chaos, Vol. 2, pp. 709-713, Sep. 1992.

[11] D. w. Jordon and P. Smith, Nonlinear Ordinary Differential Equations, New York, Oxford University Press, 1987, 2nd ed.

[12] K. S. Halle, C. W. Wu, M. Itoh, and L. O.Chua,"Spread spectrum communicat ion through modulation of chaos," Int. J. Bifurcation Chaos, Vol. 3, Apr. 1993.

[13] Henry D. I. Abarbanel and Paul S. Linsay, "Secure Communications and Unstable Periodic Orbits of Strange Attractors," IEEE Trans on circuits and system, Vol. 40, No. 10, Oct. 1993.

[14] P. R. Geffe, "How to Protect Data with Ciphers that are really hard to break," Electronics, pp. 99-101, Jan. 1973.

[15] H. J. Beker and F. C. Piper, Cipher systems: The Protection of Communica tions, Northwood Books, London, 1982.

[16] B. Schneier, Applied Cryptography : Protocols, Algorithms, and Source code in C, John Wiley & Sons, Inc., New York, USA, 1994.

[17] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," IEEE Trans. on Infor. Theory, Vol. IT-15, No. 1, pp. 122-127, Jan. 1969.

[18] R. A. Rueppel and O. J. Stafflebach, "Products of Linear Recurring Sequences with maximum Complexity "IEEE Trans. on Infor. theory, Vol. IT-33, No. 1, pp. 124-131, Jan. 1987.
[19] T.Siegen thaler,"Correlation-Immunity of Nonlinear Functions for Cryptograph ic Applications," IEEE Trans. on Infor. Theory, Vol. IT-30, No. 5, pp. 776-780, Sep.1984.
[20] Helen May gustalson, Statistical analysis of symmetric ciphers, Queensland Univ., July 1996.
[21] C. Shannon, "Communication theory of Secrecy Systems," Bell System Technical Journal, 28, pp. 656-715.
[22] N. J. Sloane, "Encrypting by Random Rotations," In: Proceedings of the workshop on Cryptography, LNCS edited by G. Goos and J. Hartmanis, Burg Feuerstein, Germany, March 29-April 2, 1982, pp. 71-128.
[23] G. M. Bernstein and M. A. Lieberman, "Secure Random Number Generator Using Chaotic Circuits," IEEE, May 1989, pp. 640-644.
[24] A. V. Oppenheim, G. W. Wornell, S. H. Isabelle, and K. M. Cuomo, "Signal processing in the context of chaotic signals," Proc. IEEE ICASSP, Vol. 4, pp. 117-120, 1992.
[25] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," Phys. Rev. A, Vol. 44, pp. 2374-2383, Aug. 1991.
[26] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," Int. J. Bifurcation chaos, Vol. 2, pp. 973-977, 1992.
[27] M. E. Bianco and D. A. Reed, Encryption System Based on Chaos Theory, US Patent No. 5, 048,086, Sep. 10, 1991.
[28] R. M. May, "Simple mathematical models with very complicated dynamics," Nature, Vol. 261, pp. 459-467, June 1976.
[29] H. O. Peitgen, H. Jurgens and D. Saupe, Chaos and Fractals, Springer -verlag, 1992.

著者紹介

**홍 진 근(Jin-keun Hong) 정회원**

1991년 2월 경북대학교 전자공학과 졸업(공학사)
1994년 2월 경북대학교 전자공학과 졸업(공학석사)
1996년 3월 ~현재 경북대학교 전자공학과 박사과정

**박 종 호(Jong-ho Park)**

1998년 2월 경북대학교 전자공학과 졸업(공학사)
1998년 3월 - 현재: 경북대학교 전자공학과 석사과정
〈관심분야〉 멀티미디어 검색, 영상처리

**황 찬 식(Chan-sik Hwang) 비회원**

1977년 2월 서강대학교 전자공학과 졸업(공학사)
1979년 8월 한국과학기술원 전기전자공학과 졸업 (공학석사)
1996년 2월 한국과학기술원 전기전자공학과 졸업(공학박사)
1991년 8월 - 1992년 8월 UTA 방문교수
1979년 9월 ~ 현재 경북대학교 전자전기공학부 교수