NBCA에 기초한 여원 MLCA와 2D CAT를 이용한 새로운 영상 암호화

정회원 김 하 경*, 남 태 희**, 조 성 진***, 종신회원 김 석 태*°

A Novel Image Encryption using Complemented MLCA based on NBCA and 2D CAT

Ha-Kyung Kim*, Tae-Hee Nam**, Sung-Jin Cho*** *Regular Members*,
Seok-Tae Kim*° *Lifelong Member*

요 약

본 논문에서는 효율적인 영상 암호화를 위해 NBCA(Null Boundary CA)에 기초한 여원 MLCA(Maximum Length Cellular Automata)와 2D CAT(Two-Dimensional Cellular Automata Transform)를 이용한 암호화 방법을 제안한다. 암호화 방법은 먼저, Wolfram Rule 행렬에 의해 전이행렬 T를 생성한다. 그 후, 암호화하려는 원 영상에 생성된 전이 행렬 T를 곱하여 원 영상의 픽셀 값을 변환한다. 또한 변환된 원 영상을 여원 벡터 F와 XOR 연산하여 여원 MLCA가 적용된 영상으로 변환한다. 다음, 게이트웨이 값을 설정하여 2D CAT 기저함수를 생성한다. 그리고, 여원 MLCA가 적용된 영상에 생성된 기저함수를 곱하여 2D CAT 암호화를 한다. 마지막으로 안정성 분석을 통하여 제안한 방법이 높은 암호화 수준의 성질을 가졌음을 검증한다.

Key Words : Complemented MLCA(Maximum Length Cellular Automata), CAT(Cellular Automata Transform), Wolfram Rule, Image Encryption

ABSTRACT

In this paper, we propose encryption method to using complemented MLCA(Maximum Length Cellular Automata) based on NBCA(Null Boundary CA) and 2D CAT(Two-Dimensional Cellular Automata Transform) for efficient image encryption. The encryption method is processed in the following order. First, a transition matrix T is created using the Wolfram Rule matrix. Then, the transition matrix T is multiplied to the original image that is intended to be encrypted, which transfers the pixel values of the original image. Furthermore, the converted original image goes through a XOR operation with complemented vector F to convert into a complemented MLCA applied image. Then, the gateway value is set and 2D CAT basis function is created. Also, the 2D CAT is encrypted by multiplying the created basis function to the complemented MLCA applied image. Lastly, the stability analysis verifies that proposed method holds a high encryption quality status.

Ⅰ. 서 론

오늘날 정보통신 기술의 발전은 사회 전 분야에 걸쳐 다양한 양질의 정보를 신속하게 제공받을 수 있다. 즉 정보 통신 기술의 발전으로 인해 경제적 사회적 부가 막대하게 창출되고 있다. 하지만 빠른 속도의 정보

* 부경대학교 전자컴퓨터정보통신공학부 (kyankees@hanmail.net, setakim@pknu.ac.kr), (° : 교신저자)
** 동주대학 의료기공학과 (thnam1@hanmail.net), *** 부경대학교 수리과학부 (sjcho@pknu.ac.kr)
논문번호 : KICS2011-01-073, 접수일자 : 2011년 1월 31일, 최종논문접수일자 : 2011년 5월 25일

통신 기술은 제도적 기술적 장치의 미비로 인해 주요 정보가 불법으로 유출되거나 도용되는 등 사회적인 문제가 되고 있다. 특히 인터넷상에서 영상 정보, 컨텐츠 등 저작권 보호를 받아야 할 주요 정보들이 해킹에 의해 유출되면서 사실상 관리 어려움에 직면해 있다[1,2].

이와 같이 정보 보호에 대한 사회적 관심이 높아지면서 정보 유출을 예방하고 보호하기 위한 하나의 방안으로 영상 분야에서 암호화하는 방법들을 제안하고 있다[3-9].

제안 방법 중 Scharinger는 Kolmogorov flow map을 이용한 영상 암호화 기법을 제안하였다[3]. 또한 Wong은 chaotic standard map을 기반으로 한 방법[4], Chen은 3D chaotic cat maps를 기반으로 하는 영상 암호화 방법[5]을 제안하였다. 그리고 Pareek은 두 개의 chaotic logistic maps와 긴 키를 이용하여 영상을 암호화하는 방법을 제안하였다[6].

이러한 Map을 이용한 암호화 방법들은 Map을 생성하는 방법이 복잡하던가[5,6], 완벽한 복원이 안된다던가[3], 암호화 수준이 떨어지는 등[3,4,7]의 문제점이 있었다.

본 논문에서는 기존 방법을 보완하기 위해 CA (Cellular Automata)성질[10]을 이용하여 영상을 암호화하는 방법을 제안한다. 암호화 방법은 먼저, Wolfram Rule에 의해 전이행렬(transition matrix) T를 생성한다. 그 후, 암호화 하려는 원 영상에 생성된 전이 행렬 T를 곱하여 원 영상의 픽셀 값을 변환한다. 또한 변환된 원 영상에 여원 벡터 F와 XOR 연산하여 여원 MLCA가 적용된 영상으로 변환한다. 다음, 여원 MLCA 변환 영상에 2D CAT 기저함수를 곱하여 영상을 암호화 한다. 또한 복호화는 암호화의 역 과정으로 2D CAT 식과 여원 벡터 F를 이용하여 선형 MLCA가 적용된 영상을 생성한다. 선형 MLCA 변환 영상에 전이 행렬 T의 역행렬을 곱하여 원 영상으로 무 손실 복원한다. 마지막으로 실험 및 안정성 분석을 통하여 타 논문에서 제시된 성능에 비해 제안한 방법이 높은 암호화 수준의 성질이 있음을 검증한다.

Ⅱ. 여원 MLCA

CA는 시간과 공간을 이산적으로 다루는 시스템이다.

$$\overline{x_i(t+1)} = f[x_{i-1}(t), x_i(t), x_{i+1}(t)] \oplus F(x) \tag{1}$$

식 (1)은 여원규칙을 나타내는 상태 전이 함수이다. 여기서 f는 결합논리를 가지는 국소전이 함수이며, 서로 다른 2^3 개 이웃의 배열상태가 있다. $F(x)$는 여원 벡터를 의미한다.

본 논문에서 제안한 여원 MLCA는 선형 MLCA에서 유도된 방법이며, 그 구조는 NBCA를 기초로 한다. NBCA는 경계조건으로서 첫 번째와 마지막 셀이 0의 상태로 연결된 것을 의미한다.

n개의 셀을 가지는 선형 3-이웃 NBCA에서는 현재 상태를 다음 상태로 전이시키는 전이함수를 $n \times n$ 행렬로 나타낸다. n 셀 CA의 상태전이 행렬 T는 식 (2)와 같이 삼중 대각 행렬로 나타낸다[11,15].

$$T = \begin{pmatrix} a_1 & 1 & 0 & \dots & 0 & 0 \\ 1 & a_2 & 1 & \dots & 0 & 0 \\ 0 & 1 & a_3 & \dots & 0 & 0 \\ & & & \dots & & 1 \\ 0 & 0 & 0 & \dots & 1 & a_n \end{pmatrix} \tag{2}$$
$$(a_1, a_2, \dots, a_n \in \{0,1\})$$

a_n는 n번째 셀에 적용된 전이규칙이 90인 경우는 0이고, 150인 경우는 1이다. 이것은 상태전이 행렬 T에서 n번째 행은 n번째 셀에 적용되는 규칙이다. $R = < a_1, a_2, \dots, a_n >$를 CA 전이 규칙이라 한다.

$f_t(x)$가 시간 t에서 CA 상태를 나타내면 시간 $t+1$에서의 유도된 여원 CA는 식 (3)과 같다.

$$f_{t+1}(x) = \overline{T} \bullet f_t(x) = F(x) \oplus T \bullet f_t(x) \tag{3}$$

여기서 $F(x)$는 n차원 여원 벡터로서 n은 셀의 개수를 의미한다. $\overline{T}^p$가 $\overline{T}$를 p번 적용한 것이라면 식 (4)와 같다.

$$\begin{aligned} f_{t+p}(x) &= \overline{T}^p \bullet f_t(x) \\ &= T^p \bullet f_t(x) \oplus (I \oplus T \oplus T^2 \oplus \dots \oplus T^{p-1}) F(x) \end{aligned} \tag{4}$$

선형 NBCA의 상태전이 행렬을 T라 하면 $\det(T) = 1$이며, 모든 셀들이 $2^n - 1$개의 사이클 구조를 이룬다. 이러한 선형 그룹 NBCA의 상태전이 행렬은 역 행렬이 존재한다. 따라서 상태전이 행렬 T의 역 행렬을 구하면 현재 상태의 바로 직전 상태를 구할 수 있다.

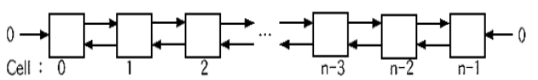

그림 1. NBCA 구조
Fig. 1. NBCA structure

$$f_{i,t-1} = T^{-1} f_{i,t} \tag{5}$$

Ⅲ. Cellular Automata Transform

2D CAT 기저함수는 2D CA 공간 $a \equiv a_{ijt}(i,j,t=0, a \equiv a_{ijt}(i,j,t=0,1,2,...,N-1)$에서 2D 기저함수 A_{ijkl}을 생성한다. 이것은 1D 기저함수 A_{ik}로부터 식 (6)과 같이 2D CAT 기저함수 식을 생성한다.

$$A_{ijkl} = A_{ik} A_{jl} \tag{6}$$

2D 영상 공간 $n \times n$ 셀일 경우, f는 공간영역 i,j에서 정의된 함수일 때 $f_{ij}(i,j=0,1,2,...,N-1)$의 2D CAT 식은 (7)과 같다[10,11,13,14].

$$f_{ij} = \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} c_{kl} A_{ijkl} \quad (i,j=0,1,2,....,N-1) \tag{7}$$

c_{kl}는 2D CAT 계수이다. 식 (8)을 이용하여 영상을 암호화한다.

$$c_{kl} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f_{ij} A_{ijkl} \ (k,l=0,1,2,...,N-1) \tag{8}$$

2D CAT 기저함수를 구하는 절차는 그림 2에 나타내었다.

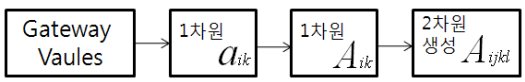

그림 2. 2D 기저함수 생성과정
Fig. 2. 2D basis function generation process

Ⅳ. 제안 방법

본 논문에서 제안한 방법에 대한 흐름은 그림 3과 같이 나타내었다.

암호화 방법은 여원 MLCA로 영상을 변환한 다음, 2D CAT 암호화하는 두 가지 단계를 거친다. 먼저, Wolfram Rule이 정의된 선형 NBCA 기반은 선형 MLCA 수열을 생성하는 원리이며, 그림 4에 나타내었다.

식 (9)는 선형 NBCA 기반에서 여원 MLCA를 계산하는 수식이다.

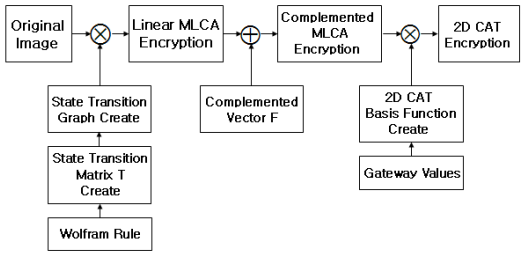

그림 3. 제안된 암호화 방법의 흐름도
Fig. 3. Flowchart of proposed encryption method

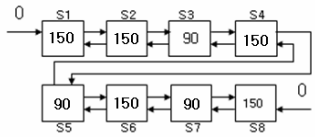

그림 4. 제안된 선형 NBCA 구조
Fig. 4. Proposed Linear NBCA structure

$$\begin{aligned}
\bar{s}_1^+ &= (0 \oplus s_1 \oplus s_2) \oplus F \\
\bar{s}_2^+ &= (s_1 \oplus s_2 \oplus s_3) \oplus F \\
\bar{s}_3^+ &= (s_2 \oplus s_4) \oplus F \\
\bar{s}_4^+ &= (s_3 \oplus s_4 \oplus s_5) \oplus F \\
\bar{s}_5^+ &= (s_4 \oplus s_6) \oplus F \\
\bar{s}_6^+ &= (s_5 \oplus s_6 \oplus s_7) \oplus F \\
\bar{s}_7^+ &= (s_6 \oplus s_8) \oplus F \\
\bar{s}_8^+ &= (s_7 \oplus s_8 \oplus 0) \oplus F
\end{aligned} \tag{9}$$

식 (9)에서, F는 여원 벡터를 의미하며, $\bar{s}_i$는 여원 MLCA가 적용된 i셀의 현재 상태를 의미한다. 또한 $\bar{s}_i^+$는 다음 상태를 의미한다. NBCA 기반의 여원 MLCA 구조는 기존 남태희[14]가 제안한 IBCA 기반의 여원 MLCA 구조보다 최대 주기가 255인 고품질의 PN 수열을 생성한다.

다음으로, 2D CAT를 이용하여 영상을 암호화한다. 표 1을 이용하여 2D CAT 기저함수를 생성한다.

2-상태, 8-셀을 가지는 CA에서 표 1에 나타낸 게이

표 1. 게이트웨이 값
Table 1. Gateway Values

Gateway	Values
Wolfram Rule	234
Number of Cells per Neighborhood	3
Number of Cells in Lattice	8
Initial Configuration	01100101
Boundary Configuration	Cyclic
Basis Function Type 2	$A_{ik} = 2a_{ik}a_{ki} - 1$

트웨이 값의 조건하에 갱신되는 셀들의 상태전이 함수는 식 (10)과 같다. 여기서 셀들의 상태들은 시간 t $(t=k)$에서 a_{0k}, a_{1k}, a_{2k} 순으로 정의된다.

$$a_{(1)(t+1)} = (W_0 a_{0t} + W_1 a_{1t} + W_2 a_{2t} + W_3 a_{0t} a_{1t} + W_4 a_{1t} a_{2t} + W_5 a_{2t} a_{0t} + W_6 a_{0t} a_{1t} a_{2t} + W_7)^{W_2} \bmod K \quad (10)$$

a_{ik}는 $t=k$ 일 때 i번째 셀의 상태를 의미한다. 또한 2D 기저함수 A_{ijkl}는 1D 기저 함수로부터 구할 수 있으며, 2D CAT 암호화는 식 (8)과 같다.

2D CAT 게이트웨이 값에 의해 생성된 2D CAT 기저함수는 그림 5에 나타내었다.

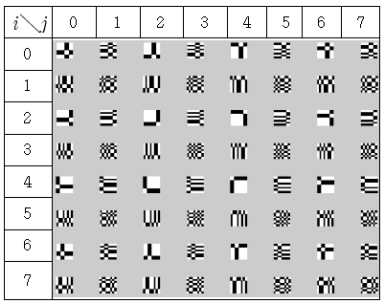

그림 5. 2D 기저 함수
Fig. 5. 2D basis function

V. 암호화 방법 및 실험 결과

암호화 방법은 먼저, Wolfram Rule에 의해 선형 MLCA의 상태 전이 행렬 T를 생성한다. 그 후, 암호화하려는 원 영상의 픽셀 위치에 생성된 전이 행렬 T를 곱하여 원 영상의 픽셀 값을 변환한다. 또한 변환된 원 영상의 픽셀 위치에 여원 벡터 F와 XOR 연산하여 여원 MLCA가 적용된 영상으로 변환한다. 다음, 여원 MLCA 변환 영상에 생성된 2D CAT 기저함수를 곱하여 영상 암호화를 한다.

본 논문에서 실험된 영상은 256×256 크기의 8비트 그레이 레벨 영상을 사용하여 고찰하였다.

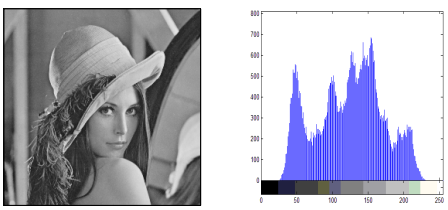

그림 6. 원 영상과 히스토그램
Fig. 6. Original image "lena" and Histogram

원 영상에 대한 여원 MLCA가 적용된 영상은 그림 7에 보였으며, 여원 MLCA가 적용된 영상에 2D CAT 기저함수를 곱한 결과는 그림 8에 나타내었다. 영상 암호화 결과는 원 영상과 비교해서 각 픽셀간의 연관성이 전혀 알 수 없게 고르게 출력됨이 히스토그램에 의해 확인되었다.

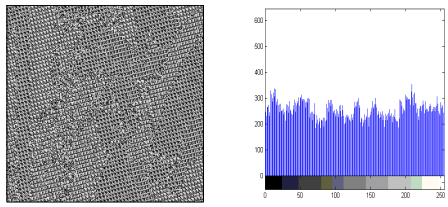

그림 7. 여원 MLCA를 적용한 영상과 히스토그램
Fig. 7. Image which apply Complemented MLCA and Histogram

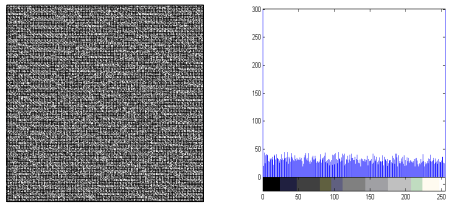

그림 8. 여원 MLCA와 2D CAT에 의한 암호화된 영상, 히스토그램
Fig. 8. Encrypted image by Complemented MLCA and 2D CAT, Histogram

VI. 안정성 분석

5.1 키 민감도 분석

식 (11)에서 x_i 와 y_i는 인접한 픽셀 값을 나타내고, N은 총 픽셀 수를 나타낸다. 키 민감도 분석에 대한 결과는 표 2에 나타내었다.

$$C_r = \frac{N\sum_{i=1}^{N}(x_i \times y_i) - \sum_{i=1}^{N} x_i \times \sum_{i=1}^{N} y_i}{\sqrt{(N\sum_{i=1}^{N} x_i^2 - (\sum_{i=1}^{N} x_i)^2) \times (N\sum_{i=1}^{N} y_i^2 - (\sum_{i=1}^{N} y_i)^2)}} \quad (11)$$

본 논문에서는 Pareek[6]이나 Tong[8], Ahmed[12], 남태희[14]에서 제시된 실험 결과보다 향상되며 안정된 암호화 수준을 갖는 결과를 얻었다. 특히 초기 암호화 단계에서 제시된 NBCA 기반의 여원 MLCA 구조는 기존 남태희[14]가 제안한 IBCA 기반의 여원 MLCA 구조를 적용한 방법보다 최대 주기가 255인 고품질의 PN 수열을 생성하기에 외부공격에 대해 좀 더 강인하다.

5.2 키 공간 분석

본 논문에서 제안된 조건은 각각 8-셀, 2-상태, 3-이웃(여원 MLCA)과 8-셀, 2-상태, 5-이웃(2D CAT)이다. 여원 MLCA는 $N_T^1 = K^{k^m+N+2T} = K^{2^3+8+2\times 8} = 2^{32}$ 가지의 키를 생성하며, 2D CAT는 $N_T^2 = K^{k^m+3(N+M)+2T} = 2^{96}(2^{2^5+3(8+8)+2\times 8})$가지의 키를 생성한다. 따라서 본 논문에 제안된 영상 암호화 방법은 총 $2^{32+96} = 2^{128}$가지의 일정한 키를 생성할 수 있기 때문에 충분한 암호화 수준을 확보할 수 있다. 이것은 일반 CA 키를 이용한 영상 암호화 수준보다 훨씬 향상된 결과이다.

5.3 픽셀의 민감도 분석

픽셀의 민감도 분석은 NPCR(number of pixels change rate)과 UACI(unified average changing intensity)을 이용한다. 조건 $D(i,j)$는 식 (12)와 같이 정의한다. 식 (13), (14)에서 W와 H는 영상의 폭과 높이를 의미하며, $A(i,j)$ 또는 $B(i,j)$는 영상의 i번째 행과 j번째 열의 픽셀을 의미한다.

$$D(i,j) = \begin{cases} 0, & A(i,j) = B(i,j) \\ 1, & A(i,j) \neq B(i,j) \end{cases} \tag{12}$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{13}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|A(i,j) - B(i,j)|}{255}\right] \times 100\% \tag{14}$$

암호화 영상의 민감도를 측정한 결과는 표 3과 같다. 본 논문에서 제안된 암호화 영상의 평균 변화와 픽셀 수에 대한 변화율은 각각 33.23%와 99.72%를 얻었다. 즉 낮은 평균 변화에 비해 높은 픽셀 수에 대한 변화율을 보였다. 따라서 Wong[4], Chen[5], Zhang[7], Giesl[9]에 비해 본 논문의 암호화 방법이 외부 공격에 강건함이 있음을 확인하였다.

표 3. NPCR와 UACI을 이용하여 측정한 결과
Table 3. Result that measure using NPCR and UACI

lena image	UACI(%)	NPCR(%)
Wong[4]	33.49	99.62
Chen[5]	33.57	99.66
Zhang[7]	33.37	98.67
Giesl[9]	33.57	99.66
제안 방법	33.23	99.72

5.4 엔트로피 분석

엔트로피는 원 영상에 대한 암호화 영상이 얼마만큼 균등하게 분포되어 있는가를 나타낸다.

$$H(S) = \sum_{i=0}^{N} P(s_i)\log_2 \frac{1}{P(s_i)} \tag{15}$$

엔트로피 $H(S)$는 식 (15)와 같다. 여기서 $P(s_i)$는 확률을 의미하며 밑수가 2인 log를 사용한다. 표 4는 원 영상과 암호화된 영상을 엔트로피 수치로 나타내었다.

본 논문에서 제안하는 영상 암호화 방법의 엔트로피 수치가 Chen[5], Giesl[9]에서 제시된 실험 결과에 비해 향상된 결과를 얻었다. 그러나 남태희[14] 방법에서 lena 및 baboon 영상의 엔트로피는 각각 7.9967과 7.9988로서 baboon 영상은 본 논문에 제시된 실험 결과에 비해 다소 우월함을 보였지만, 저주파와 고주파 성분이 균등하게 분포된 lena 영상에서는 본 논문에서 제안한 방법이 좀 더 우수함을 보였다.

표 4. 영상에 대한 엔트로피
Table 4. Entropy values for images

test images		Entropy of Original image	Entropy of encrypted image
Chen[5]	lena	7.2010	7.9970
Giesl[9]	baboon	7.1170	7.9960
제안방법	lena	7.2010	7.9992
	baboon	7.1170	7.9980

Ⅶ. 결 론

본 논문에서는 원 영상을 암호화하기 위해 NBCA에 기초한 여원 MLCA와 2D CAT를 단계적으로 적용하여 영상을 암호화 하였다. 암호화 방법은 Wolfram Rule 행렬에 의해 선형 MLCA의 상태 전이 행렬 T를 생성한다. 그 후, 암호화하려는 원 영상의 픽셀 위치에 생성된 선형 MLCA의 전이 행렬 T를 곱하여 원 영상의 픽셀 값을 변환한다. 또한 변환된 원 영상의 픽셀 위치에 여원 벡터 F와 XOR 연산하여 여원 MLCA가 적용된 영상으로 변환한다. 다음, 게이트웨이 값의 설정에 따라 2D CAT 기저함수를 생성한다. 그리고 여원 MLCA 변환 영상에 생성된 2D CAT 기저함수를 곱하여 영상을 암호화 한다. 또한 복호화는 암호화의 역 과정으로 생성된 2D CAT 식 (7)를 이용

하여 여원 MLCA 변환 영상을 얻는다. 여원 MLCA 변환 영상에 여원 벡터 F와 XOR 연산하여 선형 MLCA가 적용된 영상을 생성한다. 또한 선형 MLCA 변환 영상에 전이 행렬 T의 역행렬을 곱하여 원 영상으로 무 손실 복원한다.

제안한 암호화 방법은 Java와 Matlab으로 실험을 수행하였으며, 대상은 약 100개의 영상을 대상으로 하였다. 또한 키 민감도 및 기타 안정성 분석을 통하여 타 논문과 비교 분석하였다. 비교 분석에서 타 논문에 비해 보다 높은 수준의 결과 값을 얻었다.

따라서 제안된 본 암호화 방법이 높은 암호화 수준의 성질을 가졌음을 안정성 분석에 의해 확인하였다. 향후 연구 과제로는 CAT 기저 함수의 성질을 분석하여 고효율의 영상 암호화 방법을 새롭게 규명함으로서 암호화 분야에 한 단계 진보된 연구로 진행해야 할 것으로 생각한다.

참 고 문 헌

〔1〕 박성욱, 이현우, "정보보호산업 동향 분석", 한국해양정보통신학회논문집, pp.522-525, May. 2003.

〔2〕 T.H. Nam, S.T. Kim, and S.J. Cho, "Image Encryption using Non-linear FSR and Complemented MLCA", 2009 International Conference of Maritime Information and Communication Sciences, Vol.2, No.1, pp.168-171, Jun. 2009.

〔3〕 J. Scharinger, "Fast encryption of image data using chaotic Kolmogorov Flows", J Electron Image, Vol.2, No.2, pp.318-325, Apr. 1998.

〔4〕 K.W. Wong, S.H. Kwok, and W.S. Law, "A fast image encryption scheme based on chaotic standard map", Physics Letters A, Dec. 2007.

〔5〕 G. Chen, Y. Mao, and C. Chui, "Symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons & Fractals, Vol.21, No.3, pp.749-761, Sep. 2004.

〔6〕 N.K. Pareek, V. Patidar, and K.K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing, Feb. 2006.

〔7〕 L. Zhang, X. Liao, and X. Wang, "An Image Encryption Approach based on chaotic maps", Chaos, Solitons and Fractals, Sep. 2004.

〔8〕 X. Tong and Minggen Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically", Image and Vision Computing, Sep. 2007.

〔9〕 J. Giesl, and K. Vlcek, "Image encryption based on strange attractor", ICGST-GVIP Journal, Vol.9, Issue No.2, Apr. 2009.

〔10〕 남태희, 김석태, 조성진, "LFSR과 2D CAT를 이용한 단계적 영상 암호화", 한국해양정보통신학회논문지, Vol.13, No.6, pp.1150-1156, Jun. 2009.

〔11〕 박영일, 김석태, "다해상도 특성을 갖는 2D 셀룰러 오토마타변환을 이용한 디지탈 워터마킹", 한국통신학회논문지, Vol.34, No.1, pp.105-112, Jan. 2009.

〔12〕 H. Ahmed, H. Kalash, and O. Allah, "Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images", International Journal of Computer, Information, and Systems Science, and Engineering 1;1 © www.waset.org Winter, 2007.

〔13〕 남태희, 조성진, 김석태, "비선형 FSR과 2D CAT을 이용한 영상 암호화", 한국통신학회논문지, Vol.34, No.7, pp.663-670, Jul. 2009.

〔14〕 남태희, 김석태, 조성진, "IBCA에 기초한 여원 MLCA와 2D CAT를 이용한 영상 암호화", 전자공학회논문지, Vol.46-SP, No.4, pp.34-41, Jul. 2009.

〔15〕 S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim, and S.H. Heo, "New synthesis of One-Dimensional 90/150 Linear Hybrid Group Cellular Automata", IEEE Transactions on computer-aided design of integrated circuits and systems, Vol.26, No.9, pp.1720-1724, Aug. 2007.

김 하 경 (Ha-Kyung Kim) 정회원

2005년 부경대학교 전자컴퓨터정보통신공학부 공학석사수료

2005년~2007년 부경대학교 정보전산원 직원

2007~2009년 부경대학교 산학협력단 직원

2010년~현재 한국발명진흥회 부산지회 컨설턴트

<관심분야> CA, 영상처리, 멀티미디어

남 태 희 (Tae-Hee Nam) 정회원

1996년 부경대학교 전자공학과 공학박사
1993년~현재 동주대학 의료기 공학과 교수
<관심분야> CAT, 의료영상처리, 워터마킹, 의료정보

조 성 진 (Sung-Jin Cho) 정회원

1979년 강원대학 수학교육과 이학사
1981년 고려대학교 수학과 대학원 이학석사
1988년 고려대학교 수학과 대학원 이학박사
1988년~현재 부경대학교 자연과학대학 수리과학부 교수
<관심분야> CA론, ATM, Queueing론>

김 석 태 (Seok-Tae Kim) 종신회원

1983년 2월 광운대학교 공학사
1988년 3월 Kyoto Institute of Technology, 전자공학과 공학석사
1991년 3월 Osaka대학교 통신공학과 공학박사
1999년 Univ. of washington, USA 방문교수
2006년 Simon Fraser Univ., Canada 방문교수
1991년~현재 부경대학교 전자컴퓨터정보통신공학부 교수
<관심분야> 영상처리, 패턴인식, 워터마킹, CA