두 개의 최대 주기를 갖는 셀룰라 오토마타 수열을 이용한 영상 암호화

남태희* · 조성진** · 김석태***

Image Encryption using Cellular Automata Sequence with Two Maximum Cycle

Tae-Hee Nam* · Sung-Jin Cho** · Seok-Tae Kim***

요 약

본 논문에서는 두 개의 선형 MLCA(Maximum Length Cellular Automata)을 이용한 영상 암호화 방법을 제안한다. 암호화 방법은 먼저 8 비트 초기 값을 임의로 설정한다. 그 다음, 설정된 초기 값을 이용하여 행과 열을 단계적으로 변화시켜 고품질의 PN(pseudo noise) 수열을 생성한다. 생성된 수열을 이용하여 기저영상을 생성한다. 마지막으로 기저영상을 원 영상과 XOR 연산함으로서 암호화 수준이 높은 결과 영상을 얻는다. 히스토그램 및 안정성 분석을 통하여 제안한 방법이 높은 암호화 수준의 성질을 가졌음을 검증한다.

ABSTRACT

In this paper, we propose an image encryption method using two linear MLCA(Maximum Length Cellular Automata). The encryption method first sets arbitrary 8 bit initial values. Next, we create high quality PN(pseudo noise) sequences by converting rows and columns with the set initial values. Then we generate a basis image using the set PN sequences. Lastly, the final image with high encryption level is produced by XOR operation of the basis image and the original image. In order to verify that the proposed method has the high encryption level, we performed histogram and stability analysis.

키워드

셀룰라 오토마타, PN 수열, 최대 길이를 갖는 셀룰라 오토마타, 영상 암호화

Key word

Cellular Automata, PN(pseudo noise) sequences, MLCA(Maximum Length Cellular Automata), Image encryption

* 동주대학 의료기공학과 교수 (책임연구원, thnam1@hanmail.net)
** 부경대학교 수리과학부 교수
*** 부경대학교 전자컴퓨터정보통신공학부 교수 (교신저자)

접수일자 : 2010. 01. 21
심사완료일자 : 2010. 02. 16

I. 서 론

인터넷은 영상 정보를 활용하기 위한 중요한 도구이다. 누구든 자유롭게 최신의 정보를 이용하기 위해 인터넷을 활용한다. 인터넷은 보이지 않는 정보 제공의 통로로서 필요한 다수의 사용자들에게 자유롭게 제공하고 있다. 이러한 정보들은 개인 및 기관의 주요 저작권이 있는 정보일 수 있으며, 이로 인해 다수의 저작권자들에게 많은 피해를 주고 있다. 오늘날 영상 정보는 비밀 보장 및 개인의 정보 보호를 위한 새로운 연구과제의 대상이 되고 있다[1,2]. 최근 이러한 정보를 보호하는 주요 연구 방향 중 하나로 영상 정보를 암호화하는 방법들이 연구되고 있다[3-6].

영상 암호화 방법들 중 Scharinger는 Kolmogorov flow map을 이용한 영상 암호화 방법을 제안하였다[3]. 또한 Wong은 chaotic standard map[4]을, Pareek은 chaotic logistic map을 이용하여 영상 암호화 방법을 제안하였다[5]. 또한 Tong은 두 개의 1D chaotic functions을 이용해서 새로운 chaotic function의 수열을 생성하고 이를 원 영상과 XOR 연산하여 암호화하는 복잡한 기법을 제안하였으며[6], 또한 남태희는 IBCA를 기반으로 한 여원 MLCA와 2D CAT를 단계적으로 이용하여 암호화하는 방법을 제안하였다[7].

제시된 암호화 방법들 중, 공통의 문제점은 기저 영상 생성의 복잡성[3-7]과 영상의 복원에 대한 문제점[3,4] 등이 있었다.

본 논문에서는 기존 방법이 갖는 방법의 복잡성, 복원상의 문제를 보완하기 위한 방법으로 간단히 두 개의 선형 MLCA(Maximum Length Cellular Automata)를 이용하여 영상을 암호화하는 방법을 제안한다. 암호화 방법은 임의 초기 값을 행으로 하여 단계적으로 열의 값을 변화시킴으로서 고품질의 수열을 생성한다.

이와 같은 방법으로 원 영상의 크기만큼 PN(pseudo noise) 수열을 생성하여 이를 기저영상으로 만든다. 생성된 기저 영상을 원 영상과 XOR 연산함으로서 고효율의 암호화 영상을 얻는다.

통상 기존 영상 암호화 방법에서는 두 단계를 거쳐서 암호화를 한다. 그것은 한 번에 영상의 픽셀을 무질서하게 변환하는 것이 암호화의 수준을 떨어뜨리는 결과가 초래되기 때문이다. 그러나 본 논문에서는 한 번의 변환으로 영상의 암호화 수준을 높였다.

또한 복호화는 암호화된 영상과 기저 영상을 XOR 연산하여 원 영상으로 무 손실 복원한다. 마지막으로, 실험 및 안정성 분석을 통하여 타 논문에서 제시된 성능과 비교하여 제안한 방법이 높은 암호화 수준의 성질이 있음을 검증한다.

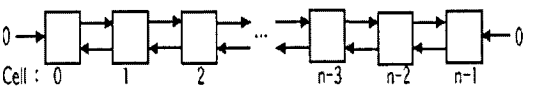
II. MLCA

CA 원리는 시간과 공간을 이산적으로 다루는 시스템이다.

$$x_i(t+1) = f[x_{i-1}(t), x_i(t), x_{i+1}(t)] \qquad (1)$$

식 (1)은 1D CA의 상태전이 함수로서 모든 셀들이 선형으로 배열되어 있는 3-이웃 구조이다. 여기서 f는 결합 논리를 가지는 국소전이 함수이다. 3-이웃 CA는 서로 다른 23 개 이웃의 배열상태가 있다. 또한 CA는 Wolfram Rule에 의해서 그 원리가 인접한 이웃과 결합 논리로 서로 연결되어 있고, 그 형태가 규칙적인 배열로 구성되기 때문에 랜덤성이 강한 특성을 가진다[8,9].

본 논문에서 제안한 선형 MLCA 구조는 NBCA(Null Boundary CA)를 기초로 한다. NBCA는 경계조건으로서 첫 번째와 마지막 셀이 0의 상태로 연결된 것을 의미한다.



$$x_i^{(t)} = 0 \Leftrightarrow i < 1 \text{ or } i > n$$

그림 1. NBCA 구조
Fig. 1 NBCA structure

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[9-13].

$$T=\begin{pmatrix} a_1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & a_2 & 1 & \cdots & 0 & 0 \\ 0 & 1 & a_3 & \cdots & 0 & 0 \\ & & & \cdots & & 1 \\ 0 & 0 & 0 & \cdots & 1 & a_n \end{pmatrix} \quad (2)$$

$(a_1,a_2,\ldots,a_n \in \{0,1\})$

a_n는 n번째 셀에 적용된 전이규칙이 90인 경우는 0이고, 150인 경우는 1이다. 이것은 상태전이 행렬 T에서 n번째 행은 n번째 셀에 적용되는 CA 규칙이며, 그 셀의 다음 상태가 현재 상태에 의존하면 1, 그렇지 않으면 0으로 한다는 의미이다. 즉 현재 상태가 자기 자신과 두 이웃에 의존하여 다음 상태로 갱신될 때, 규칙 150이라 하고, 현재 상태가 두 이웃에만 의존하여 다음 상태로 갱신될 때, 규칙 90이라 한다. $R=<a_1,a_2,\ldots,a_{n-1},a_n>$를 CA 전이 규칙이라 한다.

규칙 90 :

$$x_i^{(t+1)}=f(x_{i-1}^{(t)},x_i^{(t)},x_{i+1}^{(t)})=x_{i-1}^{(t)}\oplus x_{i+1}^{(t)} \quad (3)$$

규칙 150 :

$$x_i^{(t+1)}=f(x_{i-1}^{(t)},x_i^{(t)},x_{i+1}^{(t)})=x_{i-1}^{(t)}\oplus x_i^{(t)}\oplus x_{i+1}^{(t)} \quad (4)$$

상태 전이 행렬 T는 현재 상태 $f_i^{(t)}$가 시간 t에서 CA의 상태를 나타내면 시간 $t+1$에서의 상태는 식 (5)와 같다.

$$f_i^{(t+1)}=T\cdot f_i^{(t)} \quad (5)$$

또한 시간 $t+2$에서 CA의 상태는 식 (6)과 같이 표현된다.

$$\begin{aligned} f_i^{(t+2)} &= T\cdot f_i^{(t+1)} \\ &= T(T\cdot f_i^{(t)}) \\ &= T^2\cdot f_i^{(t)} \end{aligned} \quad (6)$$

같은 방법으로 p단계 시간은 식 (7)과 같다.

$$f_i^{(t+p)}=T^p\cdot f_i^{(t)} \quad (7)$$

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

$$f_i^{(t-1)}=T^{-1}f_i^{(t)} \quad (8)$$

식 (8)에서, T^{-1}은 상태 전이 행렬 T의 역행렬이며, $f_i^{(t)}$는 i번째 셀이 t시간 일 때의 상태를 나타낸다.

Ⅲ. 제안 방법

본 논문에서는 두 개의 선형 MLCA을 이용하여 영상을 암호화하는 방법을 제안한다. 제안 방법은 식 (9)와 같은 수식으로 나타낼 수 있다.

$$S_{r,c}^{(t)}=\sum_{r=1}^{256}\sum_{t=1}^{256}(a_{r,1}^{(t)})\cdot\sum_{t=1}^{256}(\sum_{r=1}^{256}(\sum_{c=1}^{256}b_{r,c}^{(t)})) \quad (9)$$

식 (9)에서, a, b는 각각 행과 열로서 최대 256의 사이클을 갖는 수열을 의미하며, S로 표현한다.

표 1. 두 개의 선형 MLCA 응용 결과
Table. 1 Two Linear MLCA application results

t / r	1	2	3	4	5	.....	252	253	254	255	256
1	63	67	165	184	140	.....	133	200	116	242	63
2	188	134	205	124	230	.....	81	138	211	77	188
3	46	105	198	109	204	.....	49	90	155	249	46
4	147	237	12	30	49	.....	157	244	50	95	147
5	106	195	101	216	92	.....	131	197	104	196	106
6	105	198	109	204	126	.....	90	155	249	46	105
7	187	137	214	69	168	.....	43	97	210	79	187
:	:	:	:	:	:	:	:	:	:	:	:
255	177	154	251	41	102	.....	158	241	58	75	177
256	63	67	165	184	140	.....	133	200	116	242	63

생성된 표 1을 이용하여 그림 2와 같은 기저영상을 생성하고, 이를 원 영상과 XOR 연산함으로서 고효율의 암호화 영상을 얻는다.

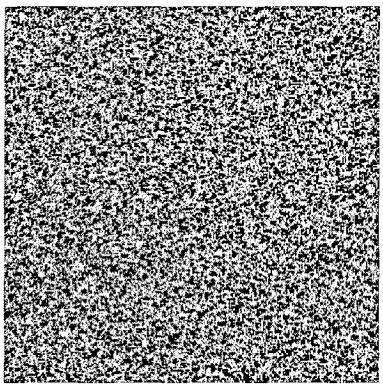


그림 2. 선형 MLCA 기저 영상
Fig. 2 Linear MLCA basis image

$$I_{r,c}=\sum_{r=1}^{256}(\sum_{c=1}^{256}I_{r,c})=(I_{1,1},I_{1,2},..,I_{256,256}) \tag{10}$$

$$E=(I_{1,1}\oplus S_{1,1}^{(1)},I_{1,2}\oplus S_{1,2}^{(1)},..,I_{1,256}\oplus S_{1,256}^{(1)} \tag{11}$$

$$...,I_{256,256}\oplus S_{256,256}^{(256)})$$

식 (10)과 (11)에서 I는 원 영상을 의미하며, E는 원 영상과 생성된 수열을 XOR 연산하는 과정으로, 암호화 영상을 얻는 수식이다.

제안하는 암호화 과정의 흐름도는 그림 3과 같다

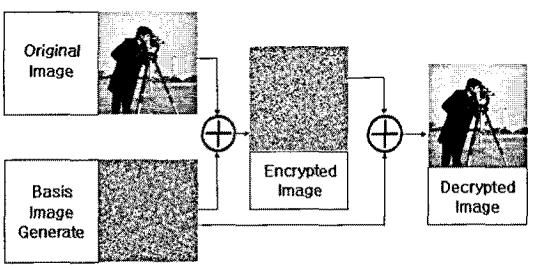


그림 3. 암호화 및 복호화 과정
Fig. 3 Encryption and decryption process

또한 제안된 방법에서 그림 4와 그림 5는 8셀의 90/150 NBCA에 의하여 주기가 256인 고품질의 PN 수열을 생성하는 구조이며, 응용 식은 표 2와 같이 표현한다.

암호화 방법은 그림 4를 이용하여 임의로 설정된 8비트 초기 값을 변환시킨다. 또한 변환된 초기 값을 그림 5를 이용하여 주기가 256인 행의 수열을 생성한다. 이와 같은 방법으로 초기 값의 변화에 따라서 행의 수열을 생성한다.

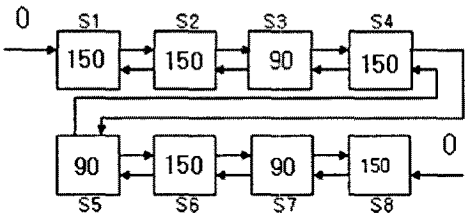


그림 4. 초기 값을 생성하기 위한 90/150 NBCA 구조
Fig. 4 90/150 NBCA structure to generate initial value

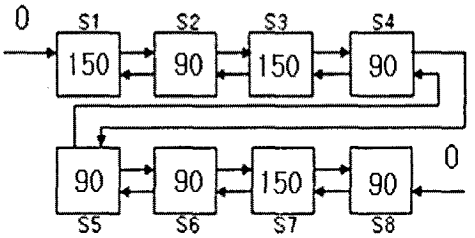


그림 5. 행의 수열을 생성하기 위한 90/150 NBCA 구조
Fig. 5 90/150 NBCA structure to create sequences of row

표2의 수식 1은 그림 4의 구조에서, 수식 2는 그림 5의 구조에서 각각 최대 사이클을 갖는 수식이다. 식에서 s_i는 i셀의 현재 상태이며, s_i^+는 다음 상태를 표시한다.

표 2. 응용 식 1,2
Table. 2 Application formula 1,2

수식 1	수식 2
$s_1^+ = 0 \oplus s_1 \oplus s_2$	$s_1^+ = 0 \oplus s_1 \oplus s_2$
$s_2^+ = s_1 \oplus s_2 \oplus s_3$	$s_2^+ = s_1 \oplus s_3$
$s_3^+ = s_2 \oplus s_4$	$s_3^+ = s_2 \oplus s_3 \oplus s_4$
$s_4^+ = s_3 \oplus s_4 \oplus s_5$	$s_4^+ = s_3 \oplus s_5$
$s_5^+ = s_4 \oplus s_6$	$s_5^+ = s_4 \oplus s_6$
$s_6^+ = s_5 \oplus s_6 \oplus s_7$	$s_6^+ = s_5 \oplus s_7$
$s_7^+ = s_6 \oplus s_8$	$s_7^+ = s_6 \oplus s_7 \oplus s_8$
$s_8^+ = s_7 \oplus s_8 \oplus 0$	$s_8^+ = s_7 \oplus 0$

Ⅳ. 암호화 방법 및 실험 결과

본 논문에서 제안한 영상 암호화 방법은 NBCA에 기초하여 서로 다른 규칙이 적용된 두 개의 선형 MLCA(Maximum Length Cellular Automata)을 이용하여 영상을 암호화하는 방법을 제안한다. 암호화 방법은 8비트 초기치를 행의 값으로 하여 열의 수열을 생성하며, 이를 기저영상으로 생성한다. 생성된 기저 영상을 원 영상과 XOR 연산함으로서 간단히 암호화 영상을 생성한다.

본 논문에서 실험된 영상은 256×256 크기의 8비트 그레이 레벨 영상을 사용하여 고찰하였다. 이러한 영상들의 변화를 고찰하기 위해 100개의 영상들을 가지고 실험하였으며, 그 중 일부 영상들을 그림 6에 나타내었다.

그림. 6 실험 영상들
Fig. 6. Experimental images

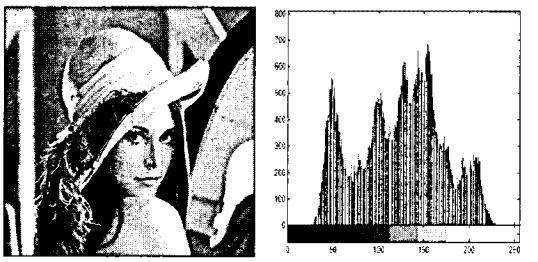


그림 7. 원 영상 "lena"와 히스토그램
Fig. 7 Original image "lena" and Histogram

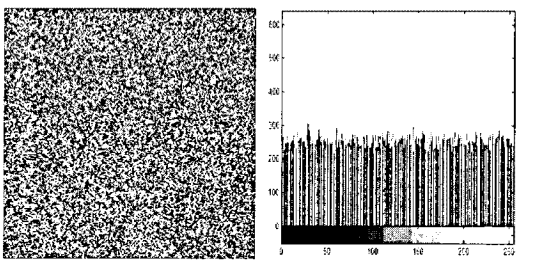
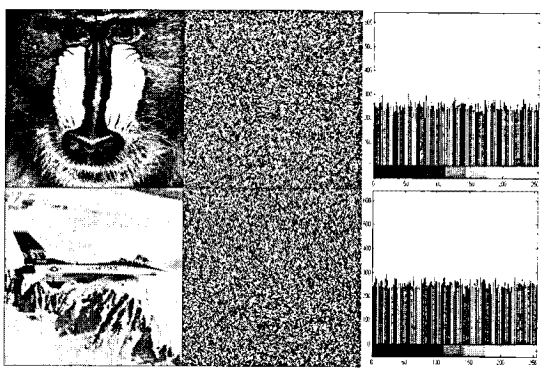


그림 8. 암호화된 영상 "lena"와 히스토그램
Fig. 8 Encrypted image "lena" and Histogram

원 영상을 기저영상과 XOR 연산에 의해 생성된 암호화 영상은 그림 8에 보였다. 여기서 암호화된 영상은 잡음의 패턴과 유사하게 출력된 것을 확인 할 수 있으며, 각 픽셀간의 연관성도 전혀 알 수 없게 출력됨을 볼 수 있었다.

또한 영상의 암호화 평가 기준으로 히스토그램을 사용하여 영상의 픽셀 분포를 분석한 결과, 고르고 안정되게 출력됨을 볼 수 있다.



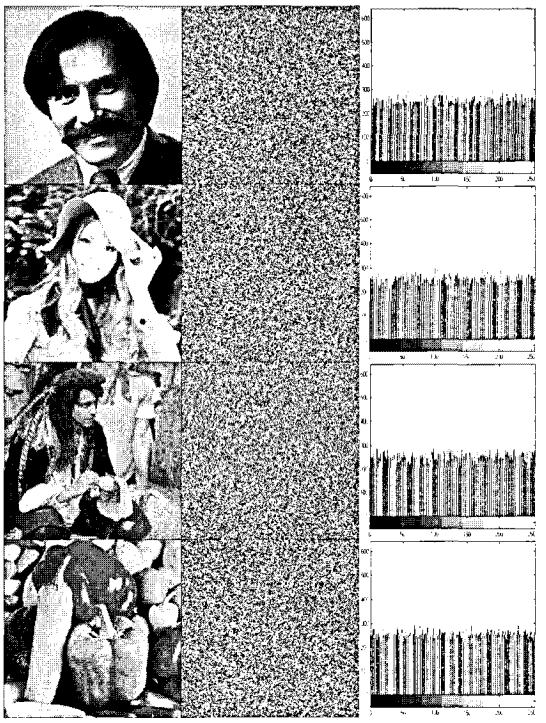


그림 9. 원 영상들과 암호화된 영상들
Fig. 9 Original images and encrypted images

V. 안정성 분석

1. 키 민감도 분석

암호화 키의 민감도 분석은 식(12)를 이용한다.

$$C_r = \frac{N\sum_{i=1}^{N}(x_i \times y_i) - \sum_{i=1}^{N} x_i \times \sum_{i=1}^{N} y_i}{\sqrt{(N\sum_{i=1}^{N} x_i^2 - (\sum_{i=1}^{N} x_i)^2) \times (N\sum_{i=1}^{N} y_i^2 - (\sum_{i=1}^{N} y_i)^2)}} \quad (12)$$

x_i 와 y_i는 인접한 픽셀 값을 나타내고 N은 총 픽셀 수를 나타낸다. 민감도 분석은 표 3과 같은 결과를 나타내었다.

표 3. 암호화 키를 위한 민감도 분석
Table. 3 Sensitivity analysis for the encryption key.

test images		test results
Pareek [5]	airplane	0.004110(55/13382)
	moon surface	0.000779(33/42362)
	aerial	0.007672(93/12122)
	clock	0.011780(145/12309)
	chemical plant	0.008989(85/9456)
Tong [6]	lena	0.0031624999(73/23083)
남태희 [7]	baboon	0.0000156594(5/319297)
	lena	0.0000128182(1/78014)
	airplane	0.0000086184(5/580154)
	man	0.0000148702(5/366243)
	girl	0.0000130124(4/307399)
제안 방법	baboon	0.0000142344(3/210757)
	lena	0.0000122153(2/163729)
	airplane	0.0000078911(1/126725)
	man	0.0000151234(3/198368)
	girl	0.0000112212(1/89117)

본 논문에서는 Pareek[5]이나 Tong[6], 남태희[7]에 의하여 제시된 실험 결과보다 전체적으로 향상되며 안정된 암호화 수준을 갖는 결과를 얻었다. 특히 남태희가 제시한 단계별 복잡한 방법과 거의 유사한 민감도로 나타났다.

2. 키 공간 분석

선형 MLCA를 이용한 영상을 분석할 수 있는 주요 키는 CA 규칙, 셀 당 최대 상태의 수, 이웃 셀 수, 초기 구성, 경계 형상, 기저 함수 타입 등이 있다. 큰 범위의 키 공간은 영상의 암호화 수준을 높인다.

본 논문에서 제안된 조건은 행과 열이 각각 8-셀, 2-상태, 3-이웃으로 구성된다. 따라서 서로 다른 규칙을 적용한 두 개의 MLCA의 키 공간 분석은 $N_T^1 = K^{k''' + N + 2T} = K^{2^4 + 8 + 2 \times 8} = 2^{32}$의 두 배이다. 여기서 T와 N은 전체 셀 공간, K와 k는 셀의 상태, m은 자신의 셀과 이웃을 의미한다. 따라서 제안된 영상 암호화 방법은 총 $2^{32+32} = 2^{64}$가지의 일정한 키를 생성할 수 있기 때문에 충분한 암호화 수준을 확보할 수 있다.

이것은 일반 CA 키를 이용한 영상 암호화 수준보다 훨씬 향상된 결과이다.

VI. 결 론

본 논문에서는 원 영상을 암호화하기 위해 90/150 NBCA에 기초하여 두 개의 8비트 선형 MLCA를 이용하였다. 즉 영상을 암호화하기 위해 두 개의 최대 사이클을 갖는 선형 MLCA을 행과 열에 각각 적용하여 수열을 생성시켜 기저 영상을 생성한다. 생성된 기저 영상을 원 영상과 XOR 연산함으로서 고효율의 암호화 영상을 얻는다. 또한 복호화는 암호화된 영상과 기저 영상을 XOR 연산하여 원 영상으로 무 손실 복원한다.

여기서 생성된 기저 영상은 행과 열이 최대 사이클을 갖는 구조로서 우수한 선형 복잡도가 생성되는 것을 볼 수 있다. 특히 한 번에 암호화 할 수 있기 때문에 단순하면서 고효율의 암호화를 실현 할 수 있었다.

참고문헌

[1] 박진, 나철훈, "디지털 컨텐츠의 보호기술에 관한 기술동향 분석", 한국해양정보통신학회논문집, pp. 1094-1097, May. 2005.

[2] 박영일, 김석태, "다해상도 특성을 갖는 2D 셀룰러 오토마타변환을 이용한 디지탈 워터마킹", 한국통신학회논문지, Vol. 34, No. 1, pp. 105-112, Jan. 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] N.K. Pareek, V. Patidar, and K.K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing, Feb. 2006.

[6] X. Tong, "Image encryption with compound chaotic sequence cipher shifting dynamically", Image and Vision Computing, Sep. 2007.

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

[8] O. Lafe, "Cellular Automata Transforms: Theory and Application in Multimedia Compression, Encryption, and Modeling", Kluwer Academic Publishers, Jan. 2000.

[9] Q. Zhou, *"Parallel Image Encryption Algorithm based on discretized chaotic map"*, Chaos, Solitons and Fractals, Jan. 2007.

[10] A. Kaminsky, "Cellular Automata Based Stream Ciphers Lecture Notes", Department of Computer Science, Apr. 2004.

[11] K. Cattell and S. Zhang, "Minimal Cast One-Dimensional Linear Hybrid Cellular Automata of Degree through 500", Journal of Electronic Testing : Theory and Applications, pp. 255-258, Jun. 1995.

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

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

저자 소개

남태희(Tae-Hee Nam)

1996년~ 부경대학교 전자공학과 공학박사
1993년~ 현재 동주대학 의료기공학과 교수

※ 관심분야 : CA, 의료영상처리, 의료정보

조성진(Sung-Jin Cho)

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

김석태(Seok-Tae Kim)

1983년 2월 광운대학교 전자공학과 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