논문 2009-46SP-4-5

IBCA에 기초한 여원 MLCA와 2D CAT를 이용한 영상 암호화

(Image Encryption using Complemented MLCA based on IBCA and 2D CAT)

남 태 희*, 김 석 태**, 조 성 진***

(Tae-Hee Nam, Seok-Tae Kim, and Sung-Jin Cho)

요 약

본 논문에서는 IBCA(Intermediate Boundary Cellular Automata)에 기반을 둔 여원 MLCA(Maximum Length Cellular Automata)와 2D CAT(Cellular Automata Transform)를 단계적으로 이용하여 영상을 암호화하는 방법을 제안한다. 암호화 방법은 먼저, 여원 MLCA를 이용하여 원 영상의 크기만큼 PN(pseudo noise) 수열을 생성한다. 그리고, 원 영상과 생성된 수열을 XOR 연산하여 여원 MLCA 영상으로 변환한다. 그 후, 게이트웨이 값을 설정하여 2D CAT 기저함수를 생성한다. 생성된 기저 함수를 변환된 여원 MLCA 영상에 곱하여 암호화를 한다. 마지막으로 PSNR(Peak Signal to Noise Ratio) 및 안정성 분석을 통하여 제안한 방법이 높은 암호화 수준의 성질을 가졌음을 검증한다.

Abstract

In this paper we propose a new image encryption method which utilizes Complemented MLCA(Complemented Maximum Length Cellular Automata) based on IBCA(Intermediate Boundary CA) and 2D CAT(Cellular Automata Transform). The encryption method is processed in the following order. First, Complemented MLCA is used to create a PN (pseudo noise) sequence, which matches the size of the original image. And, the original image goes through a XOR operation with the created sequence to convert the image into Complemented MLCA image. Then, the gateway value is set to produce a 2D CAT basis function. The produced basis function is multiplied by the encrypted MLCA image that has been converted to process the encipherment. Lastly, the stability analysis and PSNR(Peak Signal to Noise Ratio) verifies that the proposed method holds a high encryption quality status.

Keywords : Maximum Length, CAT(Cellular Automata Transform), IBCA(Intermediate Boundary Cellular Automata), Gateway values, Complemented MLCA(Maximum Length Cellular Automata)

Ⅰ. 서 론

최근 컴퓨터 및 인터넷의 발전으로 인해 다양한 정보들이 폭발적으로 늘어나고 있다. 정보 홍수의 시대라고 할 만큼 매일 같이 최신의 정보들이 업데이터 되고 있다. 특히 인터넷상에서 큰 비중을 차지하는 정보들 중에는 시각적으로 이해하기 쉬우며, 함축적인 정보를 포함하는 영상 관련 컨텐츠에 대한 선호도가 매우 증가하고 있다[1]. 그러나 영상 관련 컨텐츠는 인터넷상에서 누구나 쉽게 응용할 수 있는 문제로 인해 개인 및 단체의 주요 저작권에 많은 피해를 주고 있다. 따라서 오늘날 영상 정보 보호는 개인 및 단체의 저작권 문제로서 중요한 화두로 대두되고 있다. 즉 비밀 보장 및 보호를 위한 새로운 연구과제의 대상이 되고 있다. 최근 이러한 영상을 보호하는 주요 연구 방향 중 하나로 영상 암호화 방법이 있다[2~3].

* 정회원, 동주대학 의료기공학과
(Dept. of Biomedical Engineering, Dongju College University)
** 정회원, 부경대학교 전자컴퓨터정보통신공학부
(Division of Electronic, Computer and Telecommunication Engineering, Pukyung National University)
*** 정회원, 부경대학교 수리과학부
(Division of Mathematical Sciences, Pukyung National University)
※ 본 연구는 2008년 동주대학 교내 학술 연구 조성비 지원에 의해 연구되었습니다.
접수일자: 2009년4월20일, 수정완료일: 2009년6월9일

영상 암호화 방법에는 시각적 암호작성(Visual Cryptography), Kolmogorov flow map, chaotic standard map, chaotic logistic map, 푸리에 변환 기법, 압축 기술 등을 이용한 영상 암호화 연구가 제시되고 있다[4~6].

이들 방법 중 시각적 암호 작성은 원 영상을 픽셀단위로 분할하여 암호화함으로서 결합 시 무 손실 복원이 되지 않는 단점이 있다[7]. 또한 Scharinger[8]는 Kolmogorov flow map을 이용한 영상 암호화로서 픽셀 값을 변환하는 암호화 기법을 제안 하였으며, Wong[9]은 chaotic standard map을 기반으로 한 영상 암호화 방법을 제안하였다. 이들 방법 또한 영상의 픽셀 위치를 discredited chaotic map을 이용하여 변환 시킨 다음, CBC(Cipher Block Chain) 모드로 픽셀 값을 변환하기 때문에 암호화 효과가 떨어지는 단점이 있다.

또한 Tong[10]은 두 개의 1D chaotic functions을 이용해서 새로운 chaotic function의 수열을 생성하고 이를 원 영상과 XOR 연산하여 암호화하는 복잡한 기법을 제안하였으며 Pareek[11]는 두 개의 chaotic logistic maps와 긴 키를 이용하여 영상을 암호화하는 방법을 제안하였다.

본 논문에서는 기존 방법과 달리 CA(Cellular Automata) 성질을 적용하여 영상을 암호화하는 방법을 제안한다. 암호화 방법은 먼저 여원 MLCA (Maximum Length Cellular Automata)를 이용하여 각 원 영상의 크기만큼 PN(pseudo noise) 수열을 생성하고, 이를 원 영상과 XOR 연산하여 여원 MLCA 변환 영상을 구한다. 그 후, 생성된 여원 MLCA 변환 영상에 2D CAT(Cellular Automata Transform) 기저함수를 곱하여 CAT 영상 암호화를 한다. 즉 IBCA (Intermediate Boundary Cellular Automata)에 기초한 여원 MLCA 원리와 2D CAT를 단계별로 적용하여 영상의 암호화 수준을 높인다. 본 실험은 PSNR 및 안정성 분석을 통하여 제안한 방법이 높은 암호화 수준의 성질을 가졌음을 확인한다.

II. 여원 MLCA와 2D CAT

1. 여원 MLCA

CA는 시간과 공간을 이산적으로 다루는 시스템으로서 복잡한 자연현상을 시뮬레이션 하는데 유용한 도구이다.

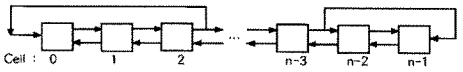

그림 1. IBCA 구조
Fig. 1. IBCA structure.

표 1. 선형과 여원 규칙
Table 1. Linear and complemented rule.

선형 규칙	$x_i(t+1)$	여원 규칙	$\overline{x_i(t+1)}$
90	$x_{i-1}^t \oplus x_{i+1}^t$	165	$\overline{x_{i-1}^t \oplus x_{i+1}^t}$
150	$x_{i-1}^t \oplus x_i^t \oplus x_{i+1}^t$	105	$\overline{x_{i-1}^t \oplus x_i^t \oplus x_{i+1}^t}$

CA를 실행할 때 중요하게 다루는 것이 경계조건이다. 본 논문에서는 경계조건이 그림 1과 같은 IBCA를 기초로 한다. IBCA는 PN 수열을 생성하는데 매우 유용한 경계조건이다[12].

그 원리는 양 끝 셀의 다음 상태가 그 자신과 그것의 오른쪽 및 왼쪽 이웃 그리고 두 번째 오른쪽 및 왼쪽 이웃의 상태에 의존하는 경우를 의미한다. 또한 IBCA는 n 개의 셀을 가지는 선형 3-이웃에서는 현재 상태를 다음 상태로 전이시키는 전이함수를 $n \times n$ 행렬로 나타낼 수 있으며, 이것을 상태전이 행렬(state transition matrix)이라 한다.

90/150 IBCA의 상태전이 행렬 T에서 i번째 행은 i번째 셀에 적용되는 규칙이며, 그 셀의 다음 상태가 현재 상태에 의존하면 1, 그렇지 않으면 0으로 한다. 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.

식 (1)은 n 셀 90/150 IBCA의 상태전이 행렬 T이다. 90/150 IBCA의 상태전이 행렬은 첫 번째 행의 왼쪽으로부터 세 번째 원소와 마지막 행의 오른 쪽부터 세 번째 원소가 항상 1이다.

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

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

여기서 $R=<a_1,a_2,\ldots,a_n>$를 IBCA의 전이 규칙이라 한다. 전이 행렬 T는 현재 상태 $f_t(x)$가 시간 t에서 CA의 상태를 나타내면 시간 $t+1$에서의 상태는 식 (2)와 같다.

$$f_{t+1}(x) = T \cdot f_t(x) \tag{2}$$

여기서 p단계 시간은

$$f_{t+p}(x) = T^p \cdot f_t(x) \tag{3}$$

이다. IBCA에 기초로 유도된 여원 MLCA의 p단계 후 상태는 식 (4)와 같다.

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

식 (4)에서 $f_t(x)$는 현재 상태의 값이며, F는 여원 벡터를 표시한다. 여원 MLCA는 비선형이므로 XOR 논리만을 사용하는 선형 CA에 비해 분석이 어렵다. 또한 선형 MLCA와 이로부터 유도된 여원 MLCA의 사이클이 다르다. 그러나 최대길이를 갖는 90/150 선형 CA로부터 유도된 여원 MLCA 또한 최대길이를 갖는 CA가 되어 대응되는 선형 MLCA와 사이클 구조가 같다는 것을 밝혔다[13]. 최대 길이를 갖는 n 셀 90/150 IBCA의 사이클 구조는 0-벡터를 제외한 모든 셀의 상태들이 주기가 2^n-1인 하나의 사이클을 이룬다.

2. 2D CAT

CAT의 기본은 1D CA로서, 모든 셀들이 선형으로 배열되어 있는 3-이웃 구조이다.

$$a_{i,t+1} = f[a_{i,t}, a_{i+1,t}, a_{i-1,t}] \tag{5}$$

식(5)은 상태전이 함수로서, f는 결합논리를 가지는 국소전이함수이며, 서로 다른 2^3개 이웃의 배열상태가 있다. CA는$2^{2^3}=256$개의 상태전이함수가 있다. 이것을 CA의 규칙이라고 한다. CAT로서, f는 공간영역 i에서 정의된 함수일 때 1D CAT 식은 (6)과 같다.

$$f_i = \sum_{k=0}^{N-1} c_k A_{ik} \quad (i = 0,1,2,...N-1) \tag{6}$$

A_{ik}는 CAT 기저함수, c_k는 CAT 계수를 나타내며, c_k는 식 (7)로 부터 구할 수 있다.

$$c_k = \frac{1}{\lambda_k} \sum_{i=0}^{N-1} f_i A_{ik} \quad \lambda_k = \sum_{i=0}^{N-1} A_{ik}^2 \tag{7}$$

2D 영상의 공간 $n \times n$ 셀일 경우, 기저함수는 $A_k \equiv A_{ijkl}, (i,j,k,l = 0,1,....,N-1)$이다.

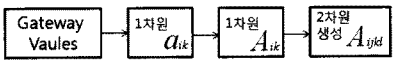

그림 2. 2D 기저함수 생성과정
Fig. 2. 2D basis function generation process.

$f_{ij}(i,j = 0,1,2,...,N-1)$의 2D CAT는 식(8)과 같다.

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

여기서 c_{kl}는 2D CAT 기저함수이다. 2D 기저함수는 2D CA 공간 $a \equiv a_{ijt}(i,j,t = 0,1,2,...,N-1)$에서 2D 기저함수 A_{ijkl}을 생성한다. 이것은 1D 기저함수로부터 식 (9)와 같이 2D 기저함수 식을 생성한다[14~15].

$$A_{ijkl} = A_{ik} A_{jl} \tag{9}$$

2D CAT의 기저함수를 구하는 절차는 그림 2에 나타내었다.

III. 제안 방법

본 논문에서 제안된 방법은 여원 MLCA를 구하기 위해 먼저, 90/150 IBCA에 기초한 선형 MLCA의 최대길이를 갖는 특성다항식에서 고품질의 PN 수열을 생성한다.

$$x^8 + x^6 + x^5 + x + 1 \tag{10}$$

식 (10)은 그림 3과 같이 제안된 90/150 IBCA의 상태전이 행렬의 특성 다항식을 나타낸다. 식 (10)의 특성다항식은 원시다항식(primitive polynomial)이므로 제안된 8셀 90/150 IBCA에 의하여 주기가 255인 PN 수열을 생성할 수 있다.

여기서 IBCA에 기초한 선형 MLCA를 분석하고 선형 MLCA에 의하여 유도된 여원 MLCA를 이용하여 고품질의 PN 수열을 생성한다.

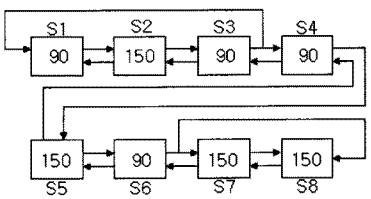

그림 3. 제안된 90/150 IBCA 구조
Fig. 3. Proposed 90/150 IBCA structure.

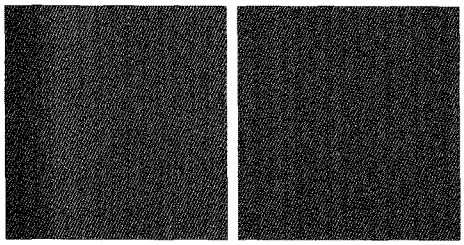

그림 4. 선형 MLCA와 여원 MLCA 기저 영상
Fig. 4. Linear MLCA and complemented MLCA basis image.

$$\begin{aligned}
\bar{s}_1^+ &= (s_3 \oplus s_2) \oplus F \\
\bar{s}_2^+ &= (s_1 \oplus s_2 \oplus s_3) \oplus F \\
\bar{s}_3^+ &= (s_2 \oplus s_4) \oplus F \\
\bar{s}_4^+ &= (s_3 \oplus s_5) \oplus F \\
\bar{s}_5^+ &= (s_4 \oplus s_5 \oplus s_6) \oplus F \\
\bar{s}_6^+ &= (s_5 \oplus s_7) \oplus F \\
\bar{s}_7^+ &= (s_6 \oplus s_7 \oplus s_8) \oplus F \\
\bar{s}_8^+ &= (s_7 \oplus s_8 \oplus s_6) \oplus F
\end{aligned} \tag{11}$$

식 (11)에서, F는 여원 벡터를 의미하며, $\bar{s}_i$는 여원 MLCA가 적용된 i셀의 현재 상태를 의미한다. 또한 $\bar{s}_i^+$는 다음 상태를 의미한다.

90/150 IBCA에 기초하여 생성된 선형 MLCA와 여원 MLCA 기저 영상은 그림 4와 같이 나타내었다. 즉 식 (11)에 의해 생성된 수열을 영상으로 표시한 것이다. 다음 단계로, 2D CAT를 이용한 영상 암호화를 하기 위해, 먼저 표 2를 이용하여 기저함수를 생성한다.

2-상태, 8-셀을 가지는 CA에서 표 2에 나타낸 게이트 웨이 값의 조건하에 갱신되는 셀들의 상태전이 함수식은 (12)와 같다.

$$\begin{aligned}
a_{(r)(t+1)} &= \left(\sum_{j=0}^{2^m-2} W_j \alpha_j + W_{2^m-1} \right)^{W_{2^m}} \bmod K \\
a_{(1)(t+1)} &= (W_0 a_{0t} + W_1 a_{1t} + W_2 a_{2t} + W_3 a_{0t} a_{1t} + \\
& W_4 a_{1t} a_{2t} + W_5 a_{2t} a_{0t} + W_6 a_{0t} a_{1t} a_{2t} + W_7)^{W_{2^3}} \bmod K
\end{aligned} \tag{12}$$

식 (12)에서 $r=1$이고 $t+1$일 경우, 조건은 $0 \le W_j \le 2$이다. α_j는 이웃 셀 상태들의 조합으로 이루어진다. 이것은 1D 3-이웃이다. 따라서 m=3으로 $W_{2^3} = W_8$의 값을 가진다. 여기서 셀들의 상태는 시간 t $(t=k)$에서 a_{0k}, a_{1k}, a_{2k}순으로 정의된다. 다음 식 (13)을 이용해서 1D 기저함수를 구한다.

$$A_{ik} = 2a_{ik}a_{ki} - 1 \tag{13}$$

표 2. 게이트웨이 값
Table 2. 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 Type2	$A_{ik} = 2a_{ik}a_{ki} - 1$

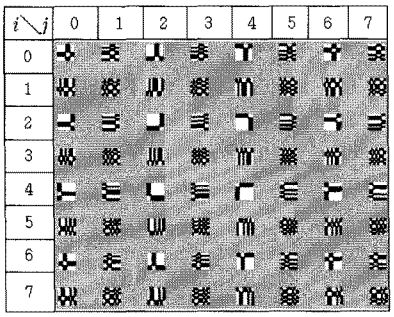

그림 5. 2D 기저 함수
Fig. 5. Two-dimensional basis function.

a_{ik}는 $t=k$ 일 때 i번째 셀의 상태를 의미하며, 식 (13)과 같은 1D 기저함수를 구한다. 또한 2D 기저함수 A_{ijkl}는 1D 기저 함수로부터 구할 수 있으며, 2D CAT 암호화는 식(14)와 같다.

$$c_{kl} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f_{ij} A_{ijkl} \quad (k,l = 0,1,2,...,N-1) \tag{14}$$

식 (14)를 이용하여 영상을 암호화한다. 표 2에 의해 생성된 2D 기저함수는 그림 5와 같이 나타내었다.

Ⅳ. 암호화 방법

암호화 방법은 90/150 IBCA에 기초한 선형 MLCA를 이용하여 원 영상의 크기만큼 PN 수열을 생성한다. 생성된 선형 MLCA를 이용하여 선형 MLCA 및 여원 MLCA 기저 영상을 생성한다. 여기서 선형 MLCA 기저 영상을 생성하는 것은 원 영상을 적용하여 여원 MLCA가 선형 MLCA보다 우월함을 검증하기 위함이다. 생성된 선형 MLCA 및 여원 MLCA 기저 영상을 원 영상과 XOR 연산하여 각각의 변환 영상을 얻는다. 변환된 영상

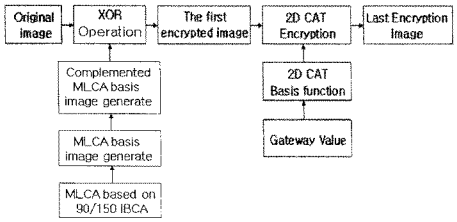

그림 6. 제안된 암호화 방법의 흐름도
Fig. 6. Flowchart of the proposed encryption method.

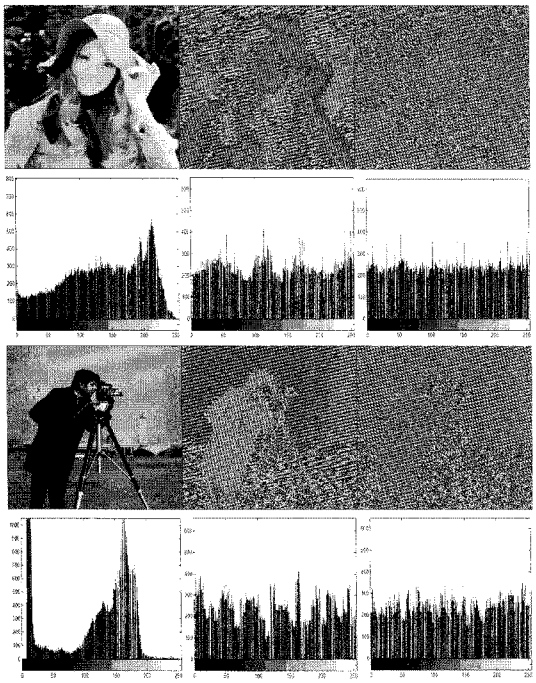

그림 7. 원 영상, 선형 MLCA, 여원 MLCA 변환 결과와 히스토그램
Fig. 7. Original image, linear MLCA, complemented MLCA conversion result and histogram.

에 게이트웨이 값을 적용하여 2D CAT 암호화를 한다. 암호화된 영상을 복호화 하는 방법은 표 2의 게이트웨이 값에 의해 생성된 기저함수 A_{ijkl}이 직교 성질을 갖고 있기 때문에 역 CAT로서 암호화 된 영상은 완전 복원될 수 있다. 원 영상을 암호화하는 과정을 그림 6에 나타내었다.

여원 MLCA의 안정성을 검증하기 위해, 선형 MLCA에 의하여 생성된 영상과 비교 분석하였다. 원 영상과 선형 MLCA 및 여원 MLCA 기저 영상을 각각 XOR 연산하여 변환된 암호화 영상은 그림 7과 같다.

단계적인 변환 영상에 대해 히스토그램을 이용하여 영상의 변화를 관찰하였다. 이것은 선형 MLCA에서 여원 MLCA로 영상 변환을 보여주는 것으로, 히스토그램 상에서 여원 MLCA가 적용된 영상이 선형 MLCA 보다 전체적으로 안정되고 고르게 분포되는 현상을 확인하였다. 따라서 본 논문에서는 선형 MLCA보다 안정성이 강한 여원 MLCA를 기본적인 영상 변환 방법으로 선택했다.

V. 실험 결과

본 실험에서는 256×256 크기의 8비트 그레이 레벨 영상을 사용하였으며, 그 변화를 고찰하였다. 히스토그램과 PSNR를 이용하여 원 영상과 암호화된 영상에 대한 변화를 분석하였다.

본 논문에서는 200개 이상의 영상들을 가지고 실험하

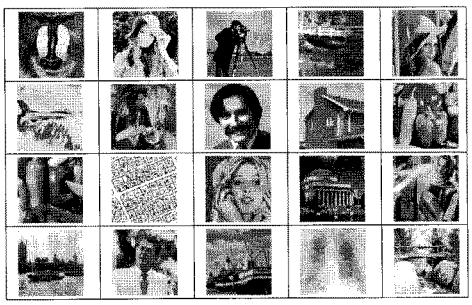

그림 8. 실험 영상들
Fig. 8. Experimental images.

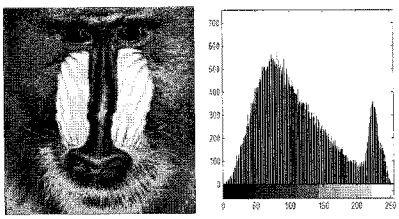

그림 9. 원 영상 "baboon" 과 히스토그램
Fig. 9. Original image "baboon" and Histogram.

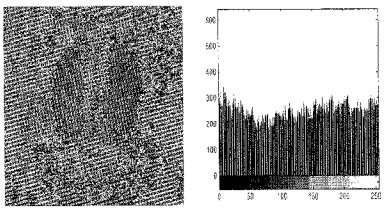

그림 10. 선형 MLCA를 적용한 영상과 히스토그램
Fig. 10. The image using linear MLCA and Histogram (PSNR=+28.2740 dB).

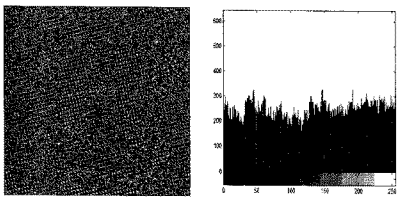

그림 11. 여원 MLCA를 적용한 영상과 히스토그램
Fig. 11. The image using complemented MLCA and Histogram(PSNR=+27.6609 dB).

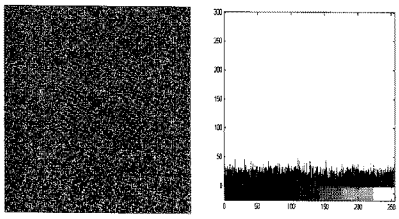

그림 12. 여원 MLCA와 2D CAT에 의한 암호화 영상과 히스토그램
Fig. 12. Encrypted image by 2D CAT and Complemented MLCA, Histogram. (PSNR=+24.3823 dB).

였으며, 그 중 일부 영상들을 그림 8에 나타내었다.

원 영상에 대한 선형 MLCA 및 여원 MLCA가 적용된 영상을 그림 10과 그림 11에 나타내었다. 또한 여원 MLCA가 적용된 변환 영상에 2D CAT 기저함수를 곱하여 영상을 암호화한 결과는 그림 12에 나타내었다. 여기서 암호화된 영상을 분석하기 위해 PSNR을 사용하였다. PSNR은 원 영상과 잡음 영상의 비로서, 암호화된 그림 12는 +24.3823 dB로서 영상의 왜곡이 크다는 것을 확인하였다. PSNR은 그 값이 낮을수록 영상의 왜곡이 크다는 것을 의미하는데, 보통 PSNR<35 dB이면, 시각적으로 영상의 왜곡을 느낄 수 있다.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)[dB] \tag{15}$$

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(I_{ij} - K_{ij})^2$$

식(15)에서 255는 픽셀의 최대 값으로 8비트 잡음 또는 밝기를 나타내며 dB로 표현한다. 또한 MSE는 오차제곱평균으로 i 와 j 값은 가로와 세로 영상을 의미하며, 두 개의 같은 양의 영상 데이터에 대해 동일한 위치의 분산을 계산한다.

VI. 안정성 분석

1. 키 민감도 분석

암호화 키의 민감도 분석은 식(16)을 이용한다.

$$C_r = \frac{N\sum_{i=1}^{N}(x_i \times y_i) - \sum_{i=1}^{N}x_i \times \sum_{i=1}^{N}y_i}{\sqrt{(N\sum_{i=1}^{N}x_i^2 - (\sum_{i=1}^{N}x_i)^2) \times (N\sum_{i=1}^{N}y_i^2 - (\sum_{i=1}^{N}y_i)^2)}} \tag{16}$$

식 (16)에서 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
Tong [10]	lena	0.0031624999(73/23083)
Pareek [11]	moon surface	0.000779(33/42362)
	aerial	0.007672(93/12122)
	airplane	0.004110(55/13382)
	clock	0.011780(145/12309)
	chemical plant	0.008989(85/9456)
제안 방법	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)

본 논문에서는 Tong[10]이나 Pareek[11]에 의하여 제시된 실험 결과보다 전체적으로 향상된 민감도를 갖는 결과를 얻었다. 따라서 본 논문에서 제시한 여원 MLCA와 2D CAT를 이용한 새로운 암호화 방법이 외부 공격에 대해서 강건함을 확인하였다.

2. 키 공간 분석

2D CAT를 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 8-셀, 2-상태, 5-이웃이다. 따라서 2D CA는 $N_T^2 = K^{k^m + 3(N+M)+2T} = 2^{96}$ $(2^{2^5+3(8+8)+2\times8})$가지의 키를 생성한다. 결국 본 논문에서 제안된 영상 암호화 방법은 총 2^{96}가지의 일정한 키를 생성할 수 있기 때문에 충분히 암호화 수준을 확보할 수 있다. 그러나 일반적인 CA 적용은 일정한 규칙에 의

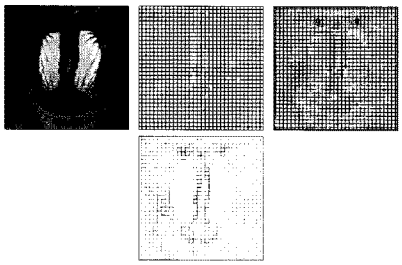

그림 13. 정상적인 복원 영상과 허용되지 않는 외부 키에 의한 복원 영상들

Fig. 13. Restoration images by impermissible external key with normal restoration image.

해 변환되기 때문에 영상이 매우 민감하게 반응한다. 따라서 허용되지 않는 일반적인 외부 키를 적용하면, 원 영상으로 전혀 복원할 수 없음을 그림 13에서 보여준다.

3. 엔트로피 분석

원 영상에 대한 암호화 영상이 얼마만큼 균등하게 분포되어 있는가를 분석한다.

$$H(S)=\sum_{i=1}^{N}P(s_i)\log\frac{1}{P(s_i)} \tag{17}$$

식 (17)에서 영상을 분석하기 위한 엔트로피로서 $H(S)$로 나타낸다. 식 (17)에서 $P(s_i)$는 확률을 의미하며 밑수가 2인 log를 사용한다. 원 영상의 엔트로피와 암호화된 엔트로피를 수치로 표 4에 나타내었다. 제안된 원 영상 "baboon"에 대한 엔트로피 측정 결과는 7.1170이며, 암호화 된 영상에서의 엔트로피는 Giesl과 제안 방법에서 각각 7.9960과 7.9988로 측정되었다.

256×256 영상에서 모든 비트가 동등한 확률로 발생한다면 엔트로피는 가장 높은 8이 된다.

본 논문에서 제안된 영상 암호화 엔트로피 수치가 Giesl의 논문에서 실험한 결과에 비해 보다 향상된 결과를 얻었다.

표 4. 영상에 대한 엔트로피

Table 4. Entropy values for images.

baboon image	Entropy of Original image	Entropy of encrypted image
Giesl[16]	7.1170	7.9960
제안 방법		7.9988

Ⅶ. 결 론

본 논문에서는 원 영상을 암호화하기 위해 90/150 IBCA에 기초한 여원 MLCA와 2D CAT를 단계별로 적용하여 영상을 암호화 하였다. 암호화 방법은 여원 MLCA를 이용하여 각 원 영상의 크기만큼 PN 수열을 생성한다. 다음, 생성된 PN 수열을 원 영상과 XOR 연산하여 여원 MLCA가 적용된 변환 영상을 구한다. 여원 MLCA는 선형 MLCA보다 그 구조가 복잡하다는 것을 본 논문의 실험에서 보였다. 따라서 여원 MLCA는 선형 MLCA 보다 영상 암호화에 대한 강한 안정성이 있음이 확인되어 영상 변환을 위해 적용하였다. 그리고 생성된 여원 MLCA 변환 영상에 2D CAT 기저함수를 곱하여 새로운 높은 수준의 암호화 영상을 얻었다.

제안한 암호화 방법은 Matlab으로 구현하여 실험을 수행하였으며, 실험 대상은 200개 이상의 영상을 대상으로 하였다. 또한 키 민감도 및 기타 안정성을 분석하여 기존의 연구 결과[10~11, 16]에 비하여 본 연구 결과는 전체적으로 측정값이 높은 암호화 수준의 결과 값을 얻었다.

향후 연구 과제로는 CAT 기저 함수의 성질을 분석하여 다양한 영상 암호화 방법을 규명함으로서 영상 암호화 분야에 한 단계 진보된 연구로 진행해야 할 것으로 생각한다.

참 고 문 헌

[1] 홍도원, 장구영, 박태준, 정교일, "유비쿼터스 환경을 위한 암호 기술 동향",전자통신동향분석 제20권 제1호, Feb. 2005.

[2] 박성호, 최현준, 서영호, 김동욱, "DCT-기반 영상/비디오 보안을 위한 암호화 기법 및 하드웨어 구현", 전자공학회논문지, Vol. 42, SP No. 2, pp. 27-36, Mar. 2005.

[3] R. Want, and G. Borriello, "Survey on Information Appliances", IEEE Compute Graphics and Applications, Vol. 20 Issue 3, May-Jun. 2000.

[4] 서동환, 김수중, "가상 위상 영상을이용한 잡음 및 변이에 강한 암호화 시스템", 전자공학회 논문지, 제40권 SD 제9호, Sep. 2003.

[5] B. Schneier, "Applied Cryptography: Second Edition",Wiley Computer Publishing, John Wiley & Sons, Inc, 1996.

[6] A. Menezes, P. Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC

Press, 1997.
[7] C. Charles, "A Practical Approach to Using Visual Cryptography in Technical Drawing Environments", Masters Thesis, Florida State University, Dec. 1997.
[8] J. Scharinger, "Fast encryption of image data using chaotic Kolmogorov Flows", J. Electron Image, Vol. 2, No. 2, pp. 318-325, Apr. 1998.
[9] K.W. Wong, "Fast image encryption scheme based on chaotic standard map", Physics Letters A, Dec. 2007.
[10] X. Tong, "Image encryption with compound chaotic sequence cipher shifting dynamically", Image and Vision Computing, Sep. 2007.
[11] N.K. Pareek, "Image encryption using chaotic logistic map", Image and Vision Computing, Feb. 2006.
[12] A.K. Das, "Additive Cellular Automata : Theory and application as a built-in self-test structure", Ph D thesis, I.I.T., Kharagpur, India, 1990.
[13] 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.
[14] O. Lafe, "Cellular Automata Transforms: Theory and Application in Multimedia Compression, Encryption, and Modeling", Kluwer Academic Publishers, Boston/Dordrecht/London, 2000.
[15] 박영일, 김석태, "다해상도 특성을 갖는 2D 셀룰러 오토마타변환을 이용한 디지탈 워터마킹", 한국통신학회논문지, Vol. 34, No. 1, pp. 105-112, Jan. 2009.
[16] J. Giesl, "Image encryption based on strange attractor", ICGST-GVIP Journal, Vol. 9, Issue (II), Apr. 2009.

저 자 소 개

남 태 희(정회원)
1996년 부경대학교 전자공학과 박사수료
1993년 현재 동주대학 의료기공학과 교수
<주관심분야 : Cellular Automata, 영상처리, 의료정보>

조 성 진(정회원)
1979년 강원대학 수학교육과 이학사
1981년 고려대학교 수학과 대학원 이학석사
1988년 고려대학교 수학과 대학원 이학박사
1988년~현재 부경대학교 자연과학대학 수리과학부 교수
<주관심분야 : Cellular Automata론, ATM, Queueing론>

김 석 태(정회원)-교신저자
1983년 8월 광운대학교 전자공학과 공학사
1988년 8월 Kyoto Institute of Technology, 전자공학과 공학석사
1991년 8월 Osaka대학교 통신공학과 공학박사
1999년 Univ. of washington, USA 방문교수
2006년 Simon Fraser Univ., Canada 방문교수
1991년~현재 부경대학교 전자컴퓨터정보통신 공학부 교수
<주관심분야 : 영상처리, 패턴인식, 워터마킹, Cellular automata.>