비선형 FSR과 2D CAT을 이용한 영상 암호화

정회원 남 태 희*, 조 성 진***, 종신회원 김 석 태**°

Image Encryption using Non-linear FSR and 2D CAT

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

요 약

본 논문에서는 NFSR(Non-linear Feedback Shift Register)과 2D CAT(Two-Dimensional Cellular Automata Transform)를 단계적으로 이용하여 영상을 암호화하는 방법을 제안한다. 암호화 방법은 먼저, NFSR을 이용해서 원 영상의 크기만큼 PN(pseudo noise) 수열을 생성한다. 그리고 생성된 수열을 원 영상과 XOR 연산하여 암호화를 한다. 그 후, 게이트웨이 값을 설정하여 2D CAT 기저함수를 생성한다. 생성된 기저함수를 변환된 암호화 영상에 곱하여 2D CAT 암호화를 한다. 마지막으로, 키 공간 분석, 엔트로피 분석 및 민감도 분석을 통해 제안한 방법이 효율적이고 매우 안전함을 검증한다.

Key Words : NFSR; CAT; PN(pseudo noise) sequences; Image Encryption

ABSTRACT

In this paper, we propose the image encryption method which gradually uses NFSR(Non-linear Feedback Shift Register) and 2D CAT(Two-Dimensional Cellular Automata Transform). The encryption method is processed in the following order. First, NFSR is used to create a PN(pseudo noise) sequence, which matches the size of the original image. Then, the created sequence goes through a XOR operation with the original image and process the encipherment. Next, the gateway value is set to produce a 2D CAT basis function. The produced basis function is multiplied by encryption image that has been converted to process the 2D CAT encipherment. Lastly, the results of the experiment which are key space analysis, entropy analysis, and sensitivity analysis verify that the proposed method is efficient and very secure.

Ⅰ. 서 론

오늘날 정보통신 기술의 비약적인 발전은 다양한 정보에 대한 접근을 용이하게 해주고 그 활용 가치로 인해 개개인 생활의 질도 향상시켜주고 있다. 특히 정보 통신의 발전으로 많은 디지털 영상 제작물들이 시공을 넘어 유통되면서 유용한 멀티미디어 정보를 제공하고 있다. 최근 이러한 디지털 영상 제작물 활용을 위해 유비쿼터스 환경이 새로운 관심의 대상이 되고 있다. 유비쿼터스 환경은 다양한 기능 및 멀티미디어 방식으로 인해 사용자가 편리하게 정보를 활용할 수 있게 해준다. 그러나 유비쿼터스 환경은 광범위한 정보를 활용할 수 있다는 장점은 있지만 정보 보호 차원에서 심각한 문제가 발생할 수 있다. 즉 정보 컨텐츠의 활용은 자칫 외부 침입자에 의해 불법으로 중요 정보가 유출될 가능성이 있으며, 이러한 불법적인 정보 유출과 도용은 저작권 및 개인 프라이버시 침해, 해킹 등과 같은 문제와 맞물려 심각한 사회적인 문제가 되고 있다.[1]-[4].

* 동주대학 의료기공학과(thnam1@hanmail.net), ** 부경대학교 전자컴퓨터정보통신공학부 (setakim@pknu.ac.kr) (°:교신저자)
*** 부경대학교 수리과학부(sjcho@pknu.ac.kr)
논문번호 : KICS2009-05-204, 접수일자 : 2009년 5월 15일, 최종논문접수일자 : 2009년 7월 8일

이와 같이 정보 보호에 대한 사회적 관심이 높아지면서 정보 유출을 예방하고 보호하기 위한 하나의 방안으로 많은 연구들이 영상을 암호화하는 방법들을 제안하고 있다[5]-[12].

그 중 Ateniese는 시각적 암호작성(Visual Cryptography)법으로 암호화하는 방법을 제안하였다[6]. 또한 Scharinger의 Kolmogorov flow map을 이용한 암호화 기법[7], Wong의 chaotic standard map을 기반으로 한 방법[8] Chen의 3D chaotic cat maps를 기반으로 하는 영상 암호화 방법[9]을 제안하였다. 그리고 Pareek은 두 개의 chaotic logistic maps와 긴 키를 이용하여 영상을 암호화하는 방법을 제안하였다[10]. 그 외 Zhang은 chaotic maps을, Zhou는 discretized chaotic map을 이용하여 영상 암호화 방법을 제안하였다[11][12].

제시된 시각적 암호 작성 방법은 원 영상을 픽셀 단위로 분할하여 암호화함으로서 결합 시 무 손실 복원이 되지 않는 단점이 있다[6]. 또한 Map을 이용한 암호화 방법들은 Map을 생성하는 방법이 복잡하던가[9][10], 완벽한 복원이 안된다던가[7][12], 암호화 수준이 떨어지는 등[7][8][11][12]의 문제점이 있었다.

본 논문에서는 기존 방법이 갖는 방법의 복잡성, 복원상의 문제, 낮은 암호화 수준 등을 보완하기 위한 방법으로 NFSR(Non-linear Feedback Shift Register)과 2D CAT(Two-Dimensional Cellular Automata Transform)를 이용한 새로운 영상 암호화 방법을 제안한다. 암호화 방법은 먼저, NFSR을 원 영상의 크기만큼 PN(pseudo noise) 수열을 생성하고, 이를 원 영상과 XOR 연산하여 1단계 암호화된 영상으로 변환한다. 그 후, 게이트웨이 값을 설정하여 2D CAT 기저함수를 생성한다. 그리고 생성된 기저함수를 변환된 NFSR 변환 영상에 곱하여 2D CAT 암호화를 한다. 마지막으로, 실험 및 안정성 분석을 통하여 타 논문에서 제시된 성능과 비교하여 제안한 방법이 높은 암호화 수준의 성질이 있음을 검증한다.

Ⅱ. NFSR과 2D CAT

NFSR은 스트림 암호화로서 2진 평문과 2진 비밀 키를 각 비트마다 XOR 연산하여 암호문을 얻고, 복호화는 암호문의 각 비트마다 비밀 키의 각 비트를 XOR 연산으로 평문을 구하는 암호 시스템이다. 이 방법은 비트 단위로 단순히 XOR 연산하므로 오류 확산 현상이 없고 블록 암호 알고리듬에 비해 빠르고 구현이 쉽다. 또한 NFSR은 선형 귀환 시프트 레지스트 보다 알려진 평문 공격에 개선된 기능을 가지며, 향상된 주기를 갖는다.

CAT의 기본은 1D CA로서, 모든 셀들이 선형으로 배열되어 있는 3-이웃 구조이다[13][14].

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

식 (1)은 상태전이 함수로서, f는 결합논리를 가지는 국소전이 함수이며, 서로 다른 2^3개 이웃의 배열상태가 있다. CA는 $2^{2^3} = 256$개의 상태전이 함수가 있다. 이것을 CA 규칙이라 한다. 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 기저함수 A_{ik}로부터 식 (2)와 같이 2D 기저함수 식을 생성한다.

$$A_{ijkl} = A_{ik} \cdot A_{jl} \tag{2}$$

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 (3)과 같다[15].

$$f_{ij} = \sum_{k=0}^{N-1}\sum_{l=0}^{N-1} c_{kl} A_{ijkl} \quad (i,j = 0,1,2,....,N-1) \tag{3}$$

c_{kl}는 2D CAT 계수이다. 식 (4)을 이용하여 영상을 암호화한다.

$$c_{kl} = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f_{ij} A_{ijkl} \ (k,l = 0,1,2,...,N-1) \tag{4}$$

2D CAT 기저함수를 구하는 절차는 그림 1에 나타내었다.

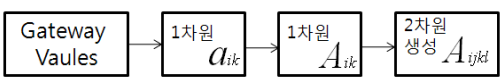


그림 1. 2D 기저함수 생성과정
Fig. 1. 2D basis function generation process

Ⅲ. 제안 방법

본 논문에서는 NFSR과 2D CAT를 단계적으로 이용하여 영상 암호화 방법을 제안한다. 제안 과정은

먼저 NFSR을 이용하여 PN 수열을 생성한다. 생성된 수열을 이용하여 기저영상을 만든다. 그리고 생성된 기저영상과 원 영상을 XOR 연산으로 1단계 암호화된 변환 영상을 구한다. 그 다음 게이트웨이 값을 이용해서 2D CAT 기저함수를 생성하여 1단계 암호화된 영상을 마지막 암호화 영상으로 변환한다. 제안하는 암호화 과정의 흐름도는 그림 2와 같다

본 논문에서 제안하는 NFSR 구조는 그림 3과 같다. NFSR 구조는 8비트와 비선형 귀환회로 XOR과 NOT 연산자로 구성된다. 비선형 귀환함수 f를 식 (5)에 나타내며, F는 여원 벡터를 표시한다.

$$f(x_1,x_2,...,x_8) = x_8 \oplus x_6 \oplus x_5 \oplus x_4 \oplus (x_1 \oplus F) \quad (5)$$

NFSR 기저영상의 생성은 식 (5)를 이용한다. 즉 생성된 기저영상과 원 영상을 XOR 연산으로 1단계 암호화된 변환 영상을 구한다. NFSR 기저영상은 그림 4에 나타내었다.

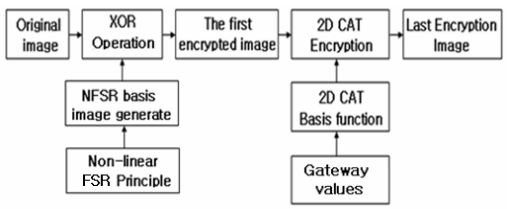


그림. 2. 제안된 암호화 방법의 흐름도
Fig. 2. Flowchart of proposed encryption method

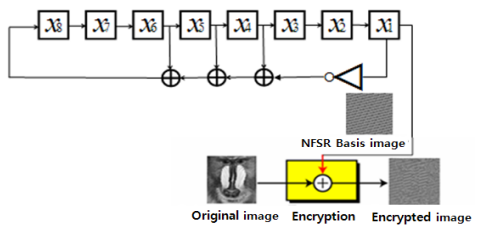


그림 3. 제안된 NFSR 구조
Fig. 3. Proposed NFSR structure

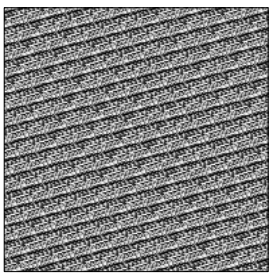


그림 4. NFSR 기저영상
Fig. 4. NFSR basis image

다음은 1단계로 암호화된 영상에 2D CAT 게이트웨이 값에 의해 생성된 기저함수를 곱하여 마지막 암호화 영상을 얻는다. 이때에 이용하는 암호화는 식 (4)를 이용한다. 게이트웨이 값은 2D CAT 기저함수를 만드는 값으로서 CA 규칙, 셀의 개수, 셀의 초기상태, 경계조건, 기저함수 타입 등에 의해서 생성된다. 표 1에 나타낸 게이트웨이 값에 따라 갱신되는 셀들의 상태전이 함수식은 식 (6)과 같다.

$$a_{(r)(t+1)} = \left(\sum_{j=0}^{2^m-2} W_j \alpha_j + W_{2^m-1} \right)^{W_{2^m}} \bmod K$$
$$a_{(1)(t+1)} = (W_0 a_{0t} + W_1 a_{1t} + W_2 a_{2t} + W_3 a_{0t} a_{1t} + W_4 a_{1t} a_{2t} + W_5 a_{2t} a_{0t} + W_6 a_{0t} a_{1t} a_{2t} + W_7)^{W_{2^3}} \bmod K \quad (6)$$

식 (6)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. a_{ik}는 $t=k$ 일 때 i번째 셀의 상태를 의미한다.

표 1의 게이트웨이 값에 의해서 생성된 2D CAT 기저함수는 그림 5와 같다.

표 1. 게이트웨이 값
Table 1. Gateway Values

Gateway	Values
Wolfram Rule	46
Number of Cells per Neighborhood	3
Number of Cells in Lattice	8
Initial Configuration	00001001
Boundary Configuration	Cyclic
Basis Function Type	$A_{ik} = 2a_{ik}a_{ki} - 1$

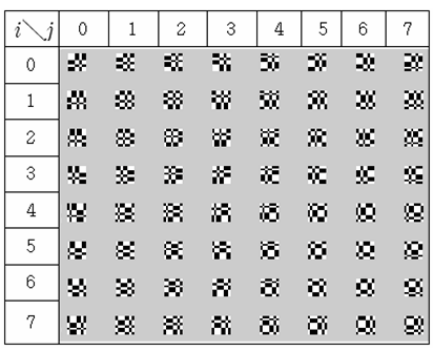


그림 5. 2D CAT 기저함수
Fig. 5. 2D CAT basis function

Ⅳ. 실험 및 성능 평가

본 암호화 방법에 대한 성능 평가는 256×256 크기의 8비트 그레이 레벨 영상을 사용하였다. 성능 평가 방법은 본 논문에서 제안하는 NFSR과 2D CAT를 각기 원 영상에 적용하여 영상의 변화를 고찰하였다. 이러한 영상들의 다양한 변화를 고찰하기 위해 100개의 영상들을 가지고 실험하였으며, 그 중 일부 영상들을 그림 6에 나타내었다.

암호화 및 복호화 실행 시간은 비트 스트림 단위로 암호화하므로 maps 알고리듬[7]-[12]을 이용하는 것보다 빠르고 구현이 쉽다. 본 논문에서는 Intel Core2 Duo CPU E4500, 2G 메모리의 윈도우 XP 환경에서 Java와 matlab을 이용하여 실험하였다. 그 결과 평균 암호화 및 복호화 시간은 0.56~2.3초 걸렸다.

본 절에서 제안한 성능 평가는 각 NFSR, 2D CAT, 그리고 NFSR과 2D CAT를 단계적으로 적용하는 세 가지 방법을 비교 분석하였다. 평가 척도로는 히스토그램과 PSNR(Peak Signal to Noise Ratio) 값을 이용하였다. 식 (7)은 PSNR로서 영상의 식별 가능 또는 불가능 정도를 수치적으로 표현하기 위해 이용한다.

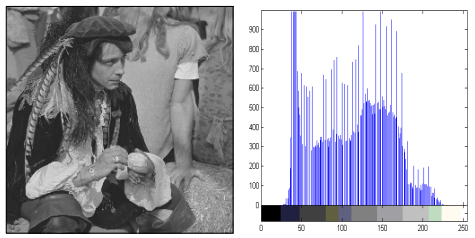
$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)[dB] \tag{7}$$

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

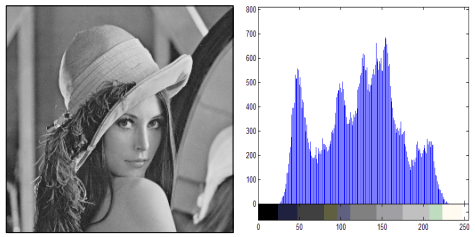
식 (7)에서 255는 픽셀의 최대값으로 8비트 잡음 또는 밝기를 나타내며 dB로 표현한다. 또한 MSE는 오차제곱평균으로 i 와 j 값은 가로와 세로 영상을 의미하며, 두 개의 같은 양의 영상 데이터에 대해 동일한 위치의 분산을 계산한다.

실험에는 픽셀의 주기가 불균등한 "man"과 "lena" 영상을 대상으로 변화를 고찰하였다. 실험 대상 영상 및 히스토그램은 그림 7에 나타내었다.

그림. 6. 실험 영상들
Fig. 6. Experimental images



(a) Image "man" and Histogram

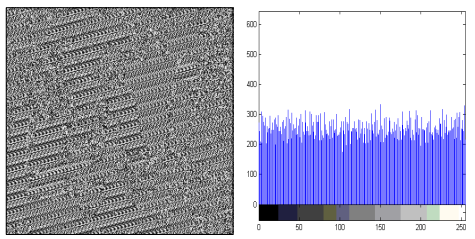


(b) Image "lena" and Histogram

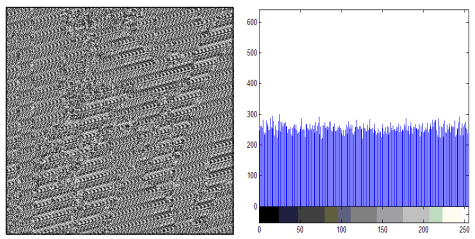
그림 7. 원 영상들과 히스토그램
Fig. 7. Original images and its Histogram

먼저, NFSR은 스트림 암호화 방식으로 주기적인 특성을 가진 암호 시스템이다. 암호화 방식은 주기적인 수열을 생성하여, 그림 4와 같은 기저영상을 생성한다. 생성한 기저영상을 원 영상과 XOR 연산하여 NFSR이 적용된 암호화 변환 영상을 얻는다. 그림 8은 NFSR 기저영상을 원 영상과 XOR 연산한 결과이다.

다음으로, 2D CAT는 이산적이며 랜덤성이 강한



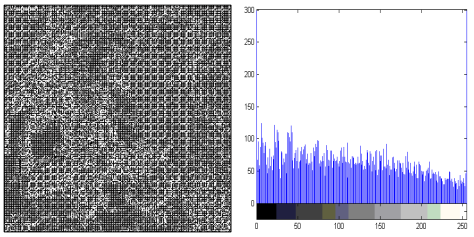
PSNR of encrypted image(PSNR=+24.2390 dB)
(a) Encrypted image "man" and Histogram



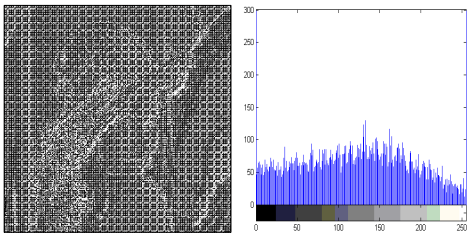
PSNR of encrypted image(PSNR=+24.2279 dB)
(b) Encrypted image "lena" and Histogram

그림 8. NFSR에 의한 암호화된 영상과 히스토그램
Fig. 8. Encrypted image and Histogram by NFSR

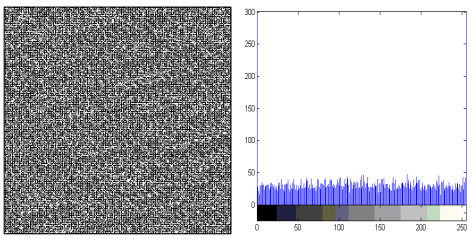
방식으로 모든 셀들이 국소적 상호작용에 의해서 복잡한 수열을 생성하는 방식이다. 암호화 방식은 그림 5와 같은 2D CAT 기저함수를 생성하여 원 영상에 곱함으로서 영상을 변환한다. 그림 9는 원 영상을 대상으로 2D CAT를 적용한 결과이다. 마지막으로, 원 영상을 대상으로 NFSR과 2D CAT를 함께 적용한 영상 변환은 그림 10과 같이 나타내었다.



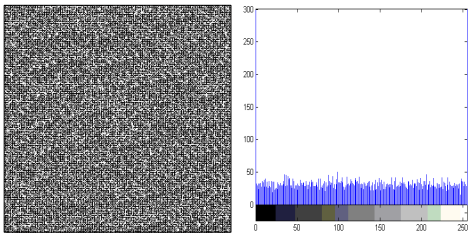
PSNR of encrypted image(PSNR=+26.6012 dB)
(a) Encrypted image “man” and Histogram



PSNR of encrypted image(PSNR=+26.6949 dB)
(b) Encrypted image “lena” and Histogram
그림 9. 2D CAT에 의한 암호화된 영상과 히스토그램
Fig. 9. Encrypted image and Histogram by 2D CAT



PSNR of encrypted image(PSNR=+23.4223 dB)
(a) Encrypted image “man” and Histogram



PSNR of encrypted image(PSNR=+23.0823 dB)
(b) Encrypted image “lena” and Histogram
그림 10. NFSR과 2D CAT에 의한 암호화된 영상과 히스토그램
Fig. 10. Encrypted image and Histogram by NFSR and 2D CAT

여기서, 각 방식에 대한 비교 평가는 히스토그램과 PSNR 값을 이용해 영상의 픽셀들이 어떠한 형태로 분포되어 있는가를 비교 분석하였다. 히스토그램을 살펴보면, NFSR과 2D CAT을 개별적으로 이용하여 변환된 영상들은 주기가 불규칙적이고, 픽셀에 대한 농도도 높게 출력되는 것을 볼 수 있었다(그림8, 그림9 참조). 그러나 NFSR과 2D CAT 방식을 단계적으로 적용한 본 방법은 각각의 방식을 따로 적용한 것에 비해 히스토그램이 상대적으로 고르고, 픽셀에 대한 농도도 낮게 출력되어 영상 암호화의 수준이 높음을 짐작할 수 있다(그림10 참조).

또한 영상의 왜곡을 측정하는 PSNR 값도 두 방법을 함께 적용한 방식은 각각 적용한 방식에 비해 그 값이 평균 $23dB$로서 낮게 출력되어 영상의 왜곡이 크다는 것을 그림 10에서 알 수 있다. 또한 이 방법은 픽셀 주기가 불균등한 영상에서도 100개의 영상을 실험한 결과 일정한 값으로 출력되는 것을 알았다. 통상적으로 PSNR<35 dB이면, 시각적으로 영상의 왜곡을 느낄 수 있다.

결과적으로 NFSR과 2D CAT를 단계적으로 함께 적용했을 경우, 원 영상과 비교하면 각 픽셀간의 연관성이 전혀 알 수 없게 고르게 출력되는 것을 PSNR과 히스토그램에 의해 확인하였다. 따라서 영상 암호화는 NFSR과 2D CAT 방식을 단계적으로 함께 적용하는 것이 영상의 암호화 수준을 높이는 것이며, 또한 외부 공격에 강함을 확인할 수 있었다. 복호화 할 때에는 2D CAT 기저함수 A_{ijkl}가 직교 성질을 갖고 있기 때문에 식 (3)을 이용하여 역 CAT를 한다. 다음으로 NFSR이 적용된 변환 영상에 NFSR 기저영상을 XOR 연산으로 정보의 손실 없이 완벽하게 복원할 수 있다.

Ⅴ. 안정성 분석

5.1 키 공간 분석

2D CAT를 이용하여 영상을 분석할 수 있는 주요 키는 CA 규칙, 셀 당 최대 상태의 수, 이웃 셀 수, 초기 구성, 경계 형상, 기저함수 타입 등이 있다. 큰 범위의 키 공간은 영상의 암호화 수준을 높인다.

본 논문에서 제안된 조건은 8-셀, 2-상태, 5-이웃이다. 따라서 2D CA는 $N_T^2 = K^{k^m+3(N+M)+2T} = 2^{96}$ ($2^{2^5+3(8+8)+2\times 8}$)가지의 키를 생성한다. 이것은 일반 CA 키를 이용한 영상 암호화 수준보다 훨씬 향

상된 결과이다. 또한 NFSR은 1D 주기적 수열을 갖는 스트림 암호화 방법으로서 서로 다른 2^8가지를 가진다. 따라서 본 논문에 제안된 영상 암호화 방법은 총 $2^{8+96}=2^{104}$가지의 일정한 키를 생성할 수 있기 때문에 충분한 암호화 수준을 확보할 수 있다.

그러나 일반적인 CA 적용은 일정한 규칙에 의해 변환되기 때문에 영상이 매우 민감하게 반응한다. 따라서 허용되지 않는 일반적인 외부 키를 적용하면, 원 영상으로 전혀 복원할 수 없음을 그림 11에서 보여준다.

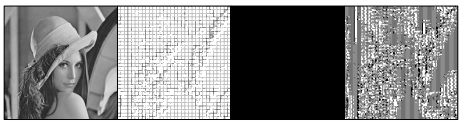


그림. 11. 정상적인 복원 영상과 허용되지 않는 키에 의한 복원 영상들
Fig. 11. Restoration images by impermissible key with normal restoration image

5.2 엔트로피 분석

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

$$H(S)=\sum_{i=0}^{N}P(s_i)\log_2\frac{1}{P(s_i)} \tag{8}$$

엔트로피 $H(S)$는 식 (8)과 같다. 여기서 $P(s_i)$는 확률을 의미하며 밑수가 2인 log를 사용한다. 표 2는 원 영상과 암호화된 영상을 엔트로피 수치로 나타내었다.

제안된 "lena" 원 영상의 측정값은 7.2010이며, 암호화된 영상의 값은 Chen[9]과 제안방법에서 각각 7.9970과 7.9981로 측정되었다. 256×256 영상에서 모든 비트가 동등한 확률로 발생한다면 엔트로피가 가장 높은 8이 된다.

본 논문에서 제안하는 영상 암호화 방법의 엔트로피 수치가 Chen에서 제시된 실험 결과에 비해 향상된 수치의 결과를 얻었다.

표 2. 영상에 대한 엔트로피
Table 2. Entropy values for images

test images		Entropy of Original image	Entropy of encrypted image
Chen[9]	lena	7.2010	7.9970
제안 방법			**7.9981**
	man	6.9747	**7.9984**

5.3 픽셀의 민감도 분석

픽셀의 민감도 분석은 NPCR(Number of Pixels Change Rate)과 UACI(Unified Average Changing Intensity)을 이용한다. $D(i,j)$는 식 (9)와 같이 정의한다. 식 (10), (11)에서 W와 H는 영상의 폭과 높이를 의미하며, $A(i,j)$ 또는 $B(i,j)$는 영상의 i번째 행과 j번째 열의 픽셀을 의미한다.

$$D(i,j)=\begin{cases}0, & A(i,j)=B(i,j)\\ 1, & A(i,j)\neq B(i,j)\end{cases} \tag{9}$$

$$NPCR=\frac{\sum_{i,j}D(i,j)}{W\times H}\times100\% \tag{10}$$

$$UACI=\frac{1}{W\times H}\left[\sum_{i,j}\frac{|A(i,j)-B(i,j)|}{255}\right]\times100\% \tag{11}$$

픽셀의 민감도를 측정한 결과는 표 3과 같다.

제안된 방법의 "lena" 영상 암호화의 평균 강도 변화와 픽셀 수에 대한 변화율은 각각 32.12%와 99.66%를 얻었다. 낮은 평균 변화에 비해 높은 픽셀 수의 변화율을 보였다. 따라서 Wong[8], Chen[9], Zhang[11], Zhou[12]에서 제안된 각 알고리듬에 비해 본 논문의 암호화 방법이 외부 공격에 강함을 확인하였다.

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

lena image	UACI(%)	NPCR(%)
Wong[8]	33.49	99.62
Chen[9]	33.57	99.66
Zhang[11]	33.37	98.67
Zhou[12]	33.43	99.64
제안 방법	**32.12**	**99.66**

Ⅵ. 결 론

본 논문에서는 영상을 암호화하기 위해 NFSR과 2D CAT를 단계적으로 이용하는 방법을 제안하였다. 본 암호화 방법은 먼저 NFSR을 이용하여 원 영상의 크기만큼 PN 수열을 생성한다. 생성된 NFSR 수열을 이용하여 NFSR 기저영상을 생성한다. 그리고 생성된 NFSR 기저영상을 원 영상과 XOR 연산하여 1단계 암호화된 영상을 얻는다. 그 후, 2D CAT의 기저함수를 1단계로 암호화된 영상에 곱하여 최종적으로 암호화된 결과를 얻었다. 이

와 같이 두 단계로 암호화함으로서 영상의 암호화 수준을 높일 수 있었다.

제안한 암호화 방법은 Java와 Matlab으로 구현하여 실험을 하였으며, 실험 대상은 약 100개의 영상을 대상으로 하였다. 또한 키 공간 및 기타 안정성을 분석하여 타 논문과 성능을 비교하였다. 측정값을 비교한 결과 본 방법이 타 논문에 비해 전체적으로 보다 높은 암호화 수준을 보였다.

향후 연구 과제로는 2D CAT 기저함수의 성질을 분석하여 이를 다른 분야에 응용하는 방법 혹은 고효율의 영상 암호화 방법 등을 개발해야 할 것으로 생각된다.

참 고 문 헌

〔1〕 서동환, 김수중, "가상 위상 영상을 이용한 잡음 및 변이에 강한 암호화 시스템", 전자공학회논문지, Vol.40, SD No.9, pp.28-35, Sep., 2003.

〔2〕 홍도원, 장구영, 박태준, 정교일, "유비쿼터스 환경을 위한 암호 기술 동향", 전자통신동향분석, Vol.20, No.1, Feb., 2005.

〔3〕 A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, Oct., 1996.

〔4〕 A. Uhl, Image and Video Encryption, Springer Science, 2005.

〔5〕 이지범, 고형화, "인터리빙과 랜덤 셔플링을 이용한 디지털 영상의 암호화 방법", 한국통신학회논문지. Vol.31, No. 5C, pp.497-502, May, 2006.

〔6〕 G. Ateniese, C. Blundo, and A. Santis, "Extended Schemes for Visual Cryptography," Theoretical Computer Science, Vol.250, pp.143-161, Feb., 2001.

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

〔8〕 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.

〔9〕 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.

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

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

〔12〕 Q. Zhou, K.W. Wong, X. Liao, T. Xiang, and Y. Hu, "Parallel Image Encryption Algorithm based on discretized chaotic map", Chaos, Solitons and Fractals, Jan., 2007.

〔13〕 S. Nandi, B.K. Kar, and P.P. Chaudhuri, "Theory and application of cellular automata in cryptography," IEEE Trans. Computer, Vol.43, Dec., 1994.

〔14〕 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.

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

남 태 희 (Tae-Hee Nam) 정회원

1996년 부경대학교 전자공학과 박사수료

1993년~ 현재 동주대학 의료기공학과 교수

<관심분야> CA, 영상처리, 의료정보

조 성 진 (Sung-Jin Cho) 정회원

1979년 강원대학 수학교육과 이학사

1981년 고려대학교 수학과 이학석사

1988년 고려대학교 수학과 이학박사

1988년~현재 부경대학교 자연과학대학 수리과학부 교수

<관심분야> CA론, ATM, Queueing론

김 석 태 (Seok-Tae Kim) 종신회원

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