두 개의 선형 MLCA을 이용한 영상 암호화

남태희* · 조성진** · 김석태1)***

*동주대학 **부경대학교 ***부경대학교

Image Encryption Using Two Linear MLCA

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

*Dongju College University **Pukyong National University ***Pukyong National University

E-mail : thnam1@hanmail.net sjcho@pknu.ac.kr setakim@pknu.ac.kr

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 operating 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

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

Ⅰ. 서 론

인터넷은 보이지 않는 정보 제공의 통로로서 다수의 사용자에게 필요한 정보를 편리하게 제공하고 있다. 그러나 이러한 정보들은 개인 및 기관의 주요 저작권이 있는 정보일 수 있지만 무단도용, 해손, 변질 등으로 인해 다수의 저작권자들에게 많은 피해를 주고 있는 것이 현실이다. 최근 이러한 문제점을 해결하기 위한 수단으로 영상 정보를 암호화하는 방법들이 연구되고 있다[1-5].

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

제시된 암호화 방법들 중, 공통의 문제점은 기저 영상 생성의 복잡성[2-5]과 영상의 복원에 대한 문제점[2,3] 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 초기 값에 의해 단계적인 행과 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 높은 수준의 암호화 영상을 얻는다.

본 방법의 장점은 한 번의 변환으로 영상의 암호화 수준을 높일 수 있다는 점이다.

Ⅱ. 제안 방법

***1) 교신저자

본 방법의 8셀의 90/150 NBCA에 의한 주기가 256인 PN 수열을 생성하는 구조를 그림 1과 2에서 나타내고, 응용 수식을 표 1과 같이 표현한다.

암호화 방법은 그림 1을 이용하여 임의로 설정된 8비트 초기 값을 변환시킨다. 또한 변환된 초기 값을 그림 2를 이용하여 주기가 256인 행의 수열을 생성한다.

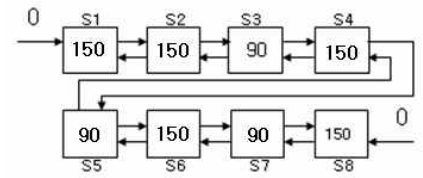

그림 1. 초기 값을 생성하기 위한 90/150 NBCA 구조

Fig. 1 90/150 NBCA structure to generate initial value

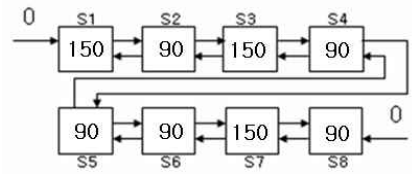

그림 2. 행의 수열을 생성하기 위한 90/150 NBCA 구조

Fig. 2 90/150 NBCA structure to generate sequences of row

표 1. 응용 수식 1,2

Table 1. Application formula 1,2

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

표1의 수식 1은 그림 1의 구조에서, 수식 2는 그림 2의 구조에서 각각 최대 사이클을 갖는 수식이다. 여기서 s_i는 i셀의 현재 상태이며, s_i^+는 다음 상태를 표시한다.

본 논문에서 제안한 기저 영상 생성 방법은 식 (1)과 같이 나타낼 수 있다.

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

식 (1)에서, a, b는 각각 행과 열로서 최대 256의 사이클을 갖는 수열을 의미하며, S로 표현한다. 또한 식 (1)에 의해 생성된 결과는 표 2로 나타낼 수 있으며, 이를 그림 3과 같은 기저영상으로 생성한다.

표 2. 두 개의 선형 MLCA 응용 결과

Table 2. Two Linear MLCA application results

c / 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

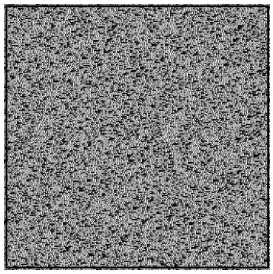

그림 3. 선형 MLCA 기저 영상

Fig. 3. Linear MLCA basis image

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

$$E = (I_{1,1} \oplus S_{1,1}^{(1)}, I_{1,2} \oplus S_{1,2}^{(1)}, .., I_{1,256} \oplus S_{1,256}^{(1)} \ldots, I_{256,256} \oplus S_{256,256}^{(256)}) \quad (3)$$

식 (2)와 (3)에서 I는 원 영상을 의미하며, E는 원 영상과 생성된 수열을 XOR 연산하는 과정으로, 암호화 영상을 얻는 식이다.

Ⅲ. 실험 결과

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

원 영상을 기저영상과 XOR 연산에 의해 생성

된 암호화 영상은 그림 5에 보였다. 여기서 암호화된 영상은 잡음의 패턴과 유사하게 출력된 것을 확인 할 수 있으며, 각 픽셀간의 연관성도 전혀 알 수 없게 출력됨을 볼 수 있었다.

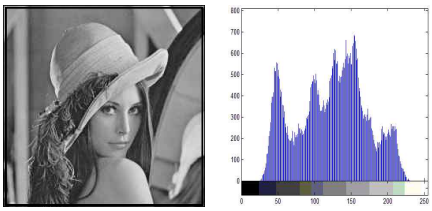

그림 4. 원 영상 "lena"와 히스토그램
Fig. 4 Original image "lena" and Histogram

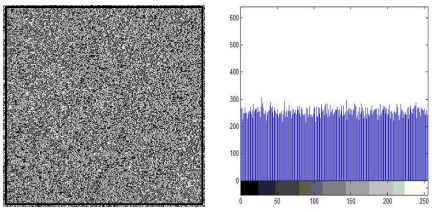

그림 5. 암호화된 영상 "lena"와 히스토그램
Fig. 5 Encrypted image "lena" and Histogram

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

test images		test results
Pareek [4]	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 [5]	lena	0.0031624999(73/23083)
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)

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

암호화 키에 대한 민감도 분석은 표 3과 같은 결과를 나타내었다.

본 논문에서는 Pareek[4]이나 Tong[5]에 의하여 제시된 실험 결과보다 향상되며 안정된 암호화 수준을 갖는 결과를 얻었다.

또한 키 공간 분석 결과, 서로 다른 규칙을 적용한 두 개의 MLCA 키 공간 분석은 $N_T^1 = K^{k^m+N+2T} = K^{2^3+8+2\times 8} = 2^{32}$의 두 배이다. (여기서 K^{k^m}=규칙, K^{2T}=시간 T와 좌우 경계 구성, K^N=셀 공간) 따라서 제안된 영상 암호화 방법은 총 $2^{32+32} = 2^{64}$가지의 키를 생성할 수 있기 때문에 충분한 암호화 수준을 확보할 수 있다. 이것은 일반 CA 키를 이용한 영상 암호화 수준보다 훨씬 향상된 결과이다.

Ⅳ. 결 론

본 논문에서는 원 영상을 암호화하기 위해 두 개의 선형 MLCA 수열을 이용하였다. 실험 결과 통상 2단계를 거쳐 높은 암호화 수준을 얻는 기존 방법보다 월등히 암호화 수준이 향상되는 것을 키 공간 및 민감도 분석에서 확인 할 수 있었다. 특히 한 번에 영상을 암호화 할 수 있기 때문에 단순하면서 고효율의 암호화를 실현 할 수 있었다.

차후에는 더 많은 양의 실험 데이터를 이용한 결과의 비교, 새로운 최대길이를 갖는 수열의 생성법 등에 관한 연구가 필요하다고 생각된다.

참고문헌

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

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

[3] 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.

[4] N.K. Pareek, V. Patidar, and K.K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing, Feb. 2006.

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