情報保護學會論文誌
第 21 卷 第 6 號, 2011. 12

산업용 디지털 이미지 보안을 위한 이미지 암호화 기법 구현 및 검증

홍 영 식[†], 정 장 영[‡]
동국대학교

Implementation and Verification of the Image Encryption Scheme for Industrial Digital Image Security

Young Sik Hong[†], Jang Young Chung[‡]
Dongguk University

요 약

오늘날 디지털 이미지의 사용범위는 웹, 산업, 의료분야 까지 많은 분야에서 사용되고 있다. 웹과 온라인 저작권의 경우 많은 연구가 진행되어왔지만, 산업용 디지털 이미지 보안에 관한 연구는 미비한 실정이다. 본 논문에서는 산업용 필름에서 사용되는 디지털 이미지 암호화 기법을 제안한다. 산업용 지적 재산권 및 산업기밀 유출을 막기 위한 산업용 이미지 보안에 적합한 이미지 암호화 기법을 구현 및 검증 한다.

ABSTRACT

Nowadays, digital-images are widely used at Web, industrial and medical applications. There have been many studies on online and Web copyright. But there are a few studies on industrial digital-image. In this paper, we propose the image encryption scheme for digital image in the industrial film. We implement and verify the proposed digital image encryption scheme for prevention of industrial secrets and intellectual property right outflow.

Keywords: Industry Security, Image encryption, Logistic map

I. 서 론

오늘날 네트워크의 발달과 디지털 이미지 제작기법의 발달로 다양한 디지털 콘텐츠 이미지와 온라인과 각종 디바이스를 통해 불법적인 유출이 문제가 되고 있다. 이로 인하여 지적재산권과 관련된 DRM과 이미지 암호화 기법에 대해 많은 연구가 진행되었다.

그러나, 산업용 디지털 이미지의 경우 기밀성이 첨가된 도면과 같은 이미지가 대부분이어서 일반적인 저작권의 경우보다 더 큰 피해가 될 수 있다. 이에 본 논문에서는 산업용 디지털 이미지를 위한 지적 재산권 및 산업기밀 유출을 막기 위해 이에 적합한 이미지 암호화 기법을 제안하고자 한다.

기존의 기법들은 주로 웹에서 이용되는 이미지 암호화 기법들로 저작권보호를 위한 워터마킹기법이나 사용권한을 다양하게 제어하기위한 DRM기법들이 주를 이룬다. 반면 기밀성을 요구하는 문서나 이미지들은 직접적인 암호화 알고리즘을 이용하여 문서나 이미지가 서비스되지 않게 하고 있다. 이러한 문서나 이미지들은 암호화 과정에서 실시간성을 요구하지 않으며 적법한 사용자인가를 판별하는 인증과 암호화의 강성에 주목함으로 인해 암·복호화의 시간복잡도가 증가한

접수일(2011년 1월 28일), 수정일(2011년 7월13일), 게재확정일(2011년 7월 28일)
† 주저자, hongys@dongguk.edu
‡ 교신저자, sd109@dongguk.edu

다.

반면 산업용의 경우 생산라인에서의 특정 이미지정보를 장치 간 또는 관리 컴퓨터와 카메라간의 통신에 있어 실시간성을 필요로 하기 때문에 암·복호화 단계에서 빠른 동작 속도를 보장하여야 한다. 그리고 암호화에 대한 강성도 필요로 하게 된다. 따라서 이러한 trade-off의 해결책으로 산업용에 적합하게 빠르면서도 허용할 수 있는 암호화강성을 갖는 디지털 이미지 암호화 기법을 필요로 하게 된다.

본 논문에서는 ARIA에서 사용된 2개의 S-Box와 Logistic Map을 이용하여 암호화를 적용한 기법을 제안하고자한다[1][2][3][4][5][6][7].

II. 관련연구

De Wang[1]이 제안한 기법은 AES의 S-Box를 이용한 기법이다. 이 기법은 다중 라운드를 사용하여 보안성을 높인 기법으로써, 절차는 다음과 같다. 이 기법은 Logistic Map인 함수 $x_{n+1}=\lambda x_n(1-x_n)$을 이용한 것으로, 이때 λ ($3.57 < \lambda < 4$)와 x_0 ($0 < x_0 < 1$)를 사용하여 카오스 영역에서의 값을 이용한다. 이 정보를 이용하여 [표 1]과 같이 $GF(2^8)$에서의 기약함수를 선택하게 되며, 선택된 기약함수와 초기화된 S-Box의 정보를 사용하여 곱셈에 대한 역원으로 맵핑하여 만들게 된다.[1]

Li Chuanmu등[2]이 제안한 기법은 Hyper-chaotic Sequences를 사용한 것으로서 Hyper-chaotic Logistic Map함수는 식(1)과 같다.

[표 1] De Wang의 제안기법의 기약함수

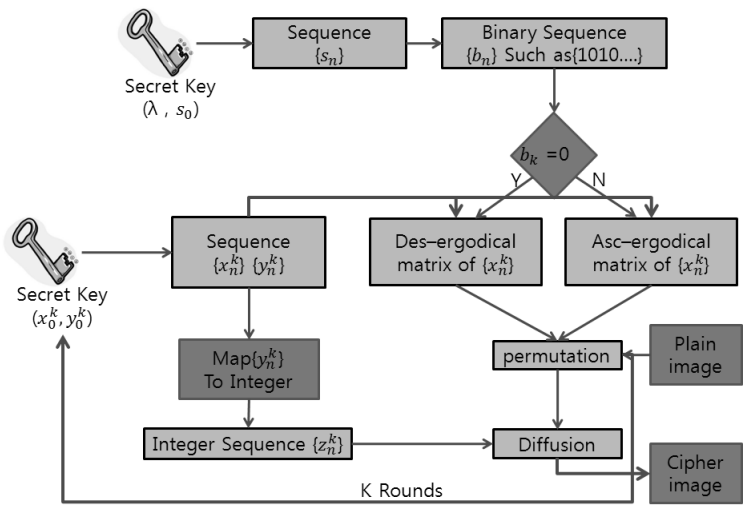
no	기약 함수
1	$x^8+x^4+x^3+x+1$
2	$x^8+x^4+x^3+x^2+1$
3	$x^8+x^5+x^3+x+1$
. . .	
28	$x^8+x^7+x^6+x^5+x^4+x+1$
29	$x^8+x^7+x^6+x^5+x^4+x^2+1$
30	$x^8+x^7+x^6+x^5+x^4+x^3+1$

$$\begin{cases} x_{n+1}=a_1y_n+a_2y_n^2 \\ y_{n+1}=a_3x_n+a_4y_n \end{cases} \quad (1)$$

Hyper-Chaotic Logistic Map을 사용한 이유는 기존 기법과 달리 혼돈의 특징을 가지고 빠르게 작동하고자 사용된 기법이며 전체적으로는 확산과 혼돈의 기능을 빠르게 적용시키고자 사용되었다. 절차는 [그림 1]과 같다.

Xin Zhang[4]가 제안한 이미지 암호화 기법의 경우 Henon Chaotic Map을 이용한 기법으로서, 식(2)와 같다.

$$\begin{cases} x_{i+1}=1-a_x^2+y_i \\ y_{i+1}=b_{x\,i}\,, i=0,1,2 \end{cases} \quad (2)$$



[그림 1] Li Chuanmu의 제안 기법

Henon Chaotic Map을 사용한 이유는, 많은 양의 계산의 경우 기존 사용된 Logistic Map의 경우와 비교해서 간결하기 때문에 빠르게 계산되는 장점이 있기 때문이다. 이 기법의 경우 2단계의 절차를 가지며 Henon Chaotic Map을 이용하여 빠르게 계산되지만, 기존 Logistic Map에 비해 랜덤한 결과를 보여주지는 못한다.

그리고 문광석[15]가 제안한 CAD 데이터에 관한 기법의 경우 실제 산업현장에서 사용되는 CAD 데이터에 대한 저작권을 위한 보호기법이다. CAD의 경우 산업현장의 설계 데이터와 핵심부품 기술, 디자인등의 내용이 첨가된 경우가 대부분이어서 이에 대한 보안 기법을 제안하게 되었다. 이 기법의 경우 CAD 데이터 종류 중 DXF 파일에 대한 포맷을 분석하고 CAD 성분중 Arc 성분, Circle 성분, Polyline 성분 등을 파악하고 저작권을 위한 워터마크 삽입할 지점과 그 알고리즘을 정립하였다. 제안된 기법은 [그림 2]와 같으며, 절차는 다음과 같다. 워터마크 은닉을 위해서 CAD 데이터를 분석하고, 은닉하는 워터마크는 적응적인 알고리즘을 이용해 비 가시성을 가지게 한다. 적응적 알고리즘은 Line이나 Arc정보에서 구성요소로 추출한 후 각각의 정보들 사이 워터마크정보를 삽입하게 된다[15].

그 외에도 Rijindal의 S-Box에 기반 하는 기법과 Celluar 기법에 기반 하는 기법들이 소개 되었다[3][4][5][6][7][8][9].

III. 제안기법

제안 기법에서 사용하는 ARIA의 경우 국내에서 개발된 암호 알고리즘으로서 AES와 일본의 국가 암호인 Camellia와 비교하여 하드웨어로 구현 하였을 경우 성능 면에서 동등하거나 그 이상의 빠른 작동을 보이는 암호알고리즘이다[11].

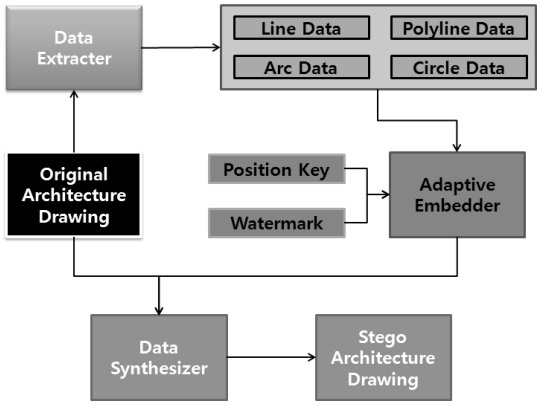
ARIA의 경우 $GF(2^8)$ 유한체 원소로 해석될 수 있는 구조이며 2개의 S-Box를 가진다[11][12][13][14].

본 논문에서는 ARIA에서 사용되는 2개의 S-Box를 선택 사용하였다. S-Box의 기능은 이미지 위치벡터(x, y) 치환에 사용하기위해 사용되며, 2개 S-Box를 사용하게 되면 악의적인 사용자에게 암호화된 이미지가 유출이 되었을 경우에 원 이미지의 위치벡터 정보를 예측하는 어려움을 주기 위해서 이다. 이미지 암호화 기법에서 사용하고 있는 카오스 기법은 생물의 개체수의 변동을 수학적으로 처리하였다. 카오스 공학은 다양한 분야에 적용되어져 왔으며, 제안된 카오스 공식의 의미는 다음과 같다.

다음 개체 수 = 증가율×(1-현재의 개체 수)×현재의 개체 수로 표현되며, 이러한 개체 수를 모델화한 때에는 개체의 상태를 0과 1사이로 나타내며 1은 개체의 최대, 0은 전멸을 의미하며 증가율에 따른 모양이 매우 예측할 수 없는 결과를 보여주기도 하며 식(3)과 같은 범위조정으로 그 결과를 확인할 수 있다.

[그림 4]는 Logistic Map을 그래프로 표현한 것이며, Logistic Map을 통해 3.5699~4의 값을 가지는 경우에는 개체수를 예측하기 어려운 매우 혼란한 상태로 표시되어 진다. 기존의 제안된 기법에서는 Logistic Map을 기약함수로 선택 하는 알고리즘대신 사상함수를 통한 기법을 사용하고자 한다.

사용된 Logistic Map인 함수 $x_{n+1} = \lambda x_n (1 - x_n)$



[그림 2] 디지털 워터마킹의 블록 다이어그램[15]

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	e2	4e	54	fc	94	c2	4a	cc	62	0d	6a	46	3c	4d	8b	d1
1	5e	fa	64	cb	b4	97	be	2b	bc	77	2e	03	d3	19	59	c1
2	1d	06	41	6b	55	f0	99	69	ea	9c	18	ae	63	df	e7	bb
3	00	73	66	fb	96	4c	85	e4	3a	09	45	aa	0f	ee	10	eb
4	2d	7f	f4	29	ac	cf	ad	91	8d	78	c8	95	f9	2f	ce	cd
5	08	7a	88	38	5c	83	2a	28	47	db	b8	c7	93	a4	12	53
6	ff	87	0e	31	36	21	58	48	01	8e	37	74	32	ca	e9	b1
7	b7	ab	0c	d7	c4	56	42	26	07	98	60	d9	b6	b9	11	40
8	ec	20	8c	bd	a0	c9	84	04	49	23	f1	4f	50	1f	13	dc
9	d8	c0	9e	57	e3	c3	7b	65	3b	02	8f	3e	e8	25	92	e5
a	15	dd	fd	17	a9	bf	d4	9a	7e	c5	39	67	fe	76	9d	43
b	a7	e1	d0	f5	68	f2	1b	34	70	05	a3	8a	d5	79	86	a8
c	30	c6	51	4b	1e	a6	27	f6	35	d2	6e	24	16	82	5f	da
d	e6	75	a2	ef	2c	b2	1c	9f	5d	6f	80	0a	72	44	9b	6c
e	90	0b	5b	33	7d	5a	52	f3	61	a1	f7	b0	d6	3f	7c	6d
f	ed	14	e0	a5	3d	22	b3	f8	89	de	71	1a	af	ba	b5	81

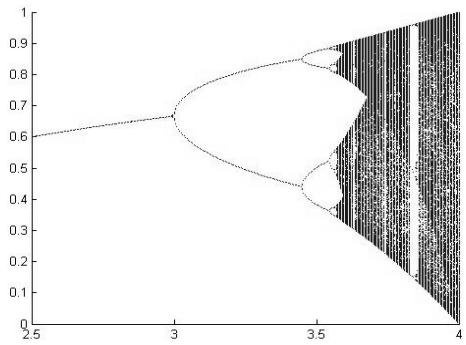
[그림 3] ARIA 의 S1-Box와 S2-Box

0 〈 증가율 ≦ 1
다음 개체 수는 0으로 수렴
1 〈 증가율 ≦ 2
다음 개체 수는 1 - (1 / α)로 수렴
2 〈 증가율 ≦ 3.5699
다음 개체 수는 주기배가 상태
3.5699 〈 증가율 〈 4
다음 개체 수는 혼돈 상태 (3)

을 이용한 것으로, 이때 λ(3.57 〈 λ 〈 4)와 x_0(0 〈 x_0 〈 1)를 2개의 키로 이용한다.

제안 기법은 〔그림 5〕와 〔그림 6〕과 같다. 우선 디지털 이미지를 위한 암호기법의 경우 Logistic Map에서 결과를 얻기 위한 키 2개를 선택하게 된다. 키2개를 사용하여 랜덤한 결과를 얻고 이결과를 사상함수를 통하여 이미지 색 정보와 XOR 할 수 있도록 한다. 그리고 치환과정에서 사용되는 S-Box의 경우 선택적으로 사용하여 기존 1개의 S-Box를 사용하던 기법에서 보안성을 높이고자 하였다.

제안 기법에서 2개의 키를 사용하며, 2개의 키를 사용할 경우 악의적인 사용자에게 이미지가 유출이 되었을 경우에 1개의 키만 유출이 되었다면 해당 이미지에 대한 보안성을 높일 수 있기 때문이다. 또한 키 관리를 독립적으로 하게 된다면 1개의 키가 유출이 되었더라도 나머지 키를 예측하는데 어려움이 있다. 그리고 ARIA의 S-Box를 통하여 픽셀의 위치정보를 변경하게 된다.



〔그림 4〕 Logistic Map 그래프

그리고 제안된 기법의 사상 함수는 다음과 같다.

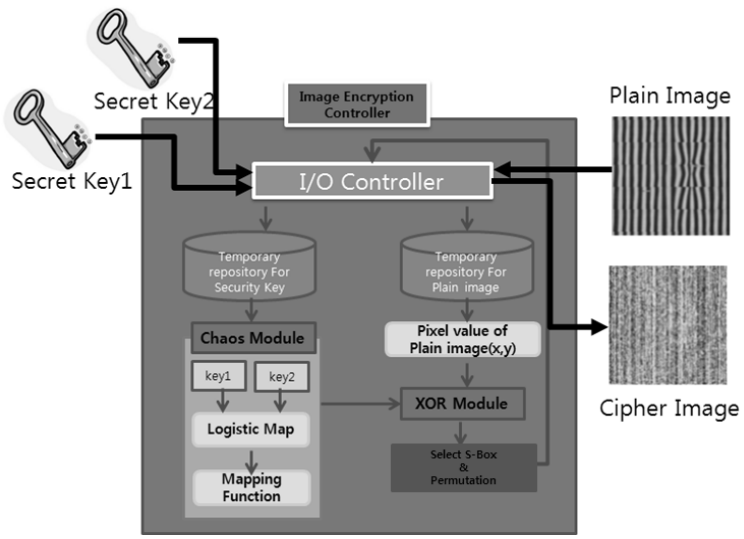
$$k = -x_n \bmod 255$$
$$P(i,j) = P(i,j)\ XOR\ k \quad (4)$$

Logistic Map 을 통한 정보를 위의 식으로 값을 얻어낸 후 위치 픽셀정보와 XOR연산을 하게 된다.

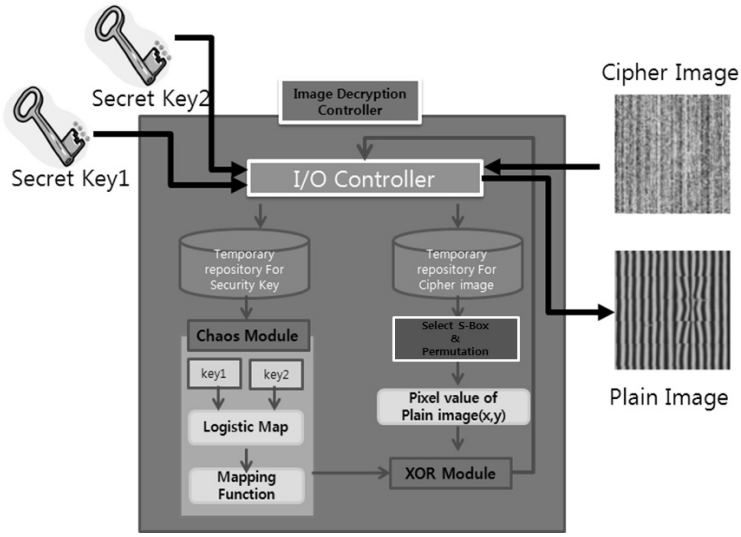
IV. 결과 및 분석

제안 기법의 구현환경은〔표 2〕와 같다.

제안기법을 구현하여 모의 테스트한 결과는 다음 〔그림 7〕과 〔그림 8〕과 같다. 10개의 이미지를 암호



〔그림 5〕 제안된 암호화 기법



〔그림 6〕 제안된 복호화 기법

화 하였을 경우 픽셀의 원본 이미지와 암호화된 픽셀 변화율 *NPCR*(Number of Pixel Change Rate)이 평균 99.63%로 나왔다.

이 같은 결과는 암호화된 이미지에서 평문 이미지를 유추하기가 어려울 것으로 예상된다. *NPCR*의 경우 아래 식5를 이용하였다. 평문이미지 *P(i,j)*와 암호화된 이미지 *E(i,j)*와 픽셀 정보를 이용하여 같 으면 *D(i,j)*를 0으로 하고, 다르면 1로 하여 총 픽셀 수에서 같은 색 정보를 가진 픽셀 수를 나누었다.

또한 원본이미지와 복호화 된 이미지의 픽셀의 색 정보 일치율이 100%로 나왔기에 복호화 된 이미지와 원본을 비교하여 왜곡이 없음을 보였다.

그리고 암호화된 이미지가 유출이 되었을 경우 〔그림 7〕의 암호화 이미지처럼 왜곡이 심하게 되었다. 또한 잘못된 키를 입력하여 복호화 하였을 경우 암호화 이미지와 잘못된 키의 이미지의 픽셀의 값 일치 율이 약 0.0085%로 낮게 나와서 잘못된 이미지에서 원본이미

〔표 2〕 구현환경

CPU	Pentium4 3.06Ghz
RAM	512MB
HDD	200GB
OS	RED HAT ENTERPRISE 3
Language	GCC 3.4.6
Image size	128×128
Color Depth	8Bit

$$
\begin{aligned}
&if\ (P(ij) = E(ij)) \\
&D(ij) = 1 \\
&else \\
&D(ij) = 0
\end{aligned}
\tag{5}
$$

$$
\frac{\sum_{ij} D(ij)}{WidthPixel \times heightPixel} \times 100\%
$$

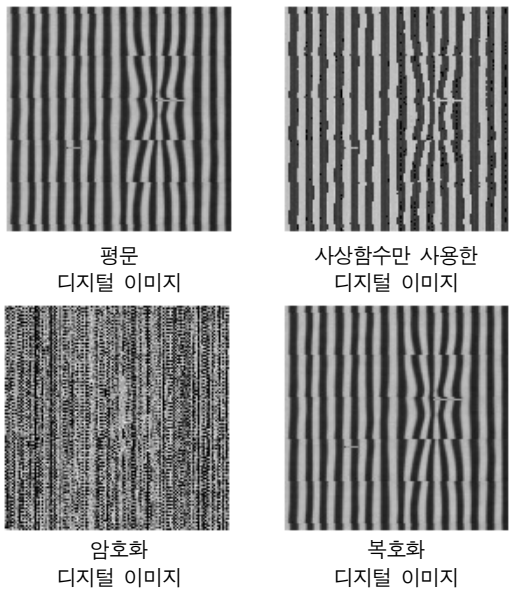
〔표 3〕 평균 처리시간

구 분	암호화	복호화
시간(평균)	$1.250723ms$	$1.287794ms$

지를 유추하기 어렵다.

〔표 3〕은 평균 처리 속도에 대한 결과이다. 약 1,000,000번 시행횟수에 대한 평균 처리 속도를 측정한 것이다. 암호화 시간은 약 $1.250723ms$로 측정되었으며, 복호화 시간은 약 $1.287794ms$로 측정이 되었다. 이를 측정한 이유는 산업현장에서 빠른 실시간 처리를 요하기 때문이며, 암·복호화에 따른 지연 문제를 위하여 제안기법의 처리속도를 측정한 것이다.

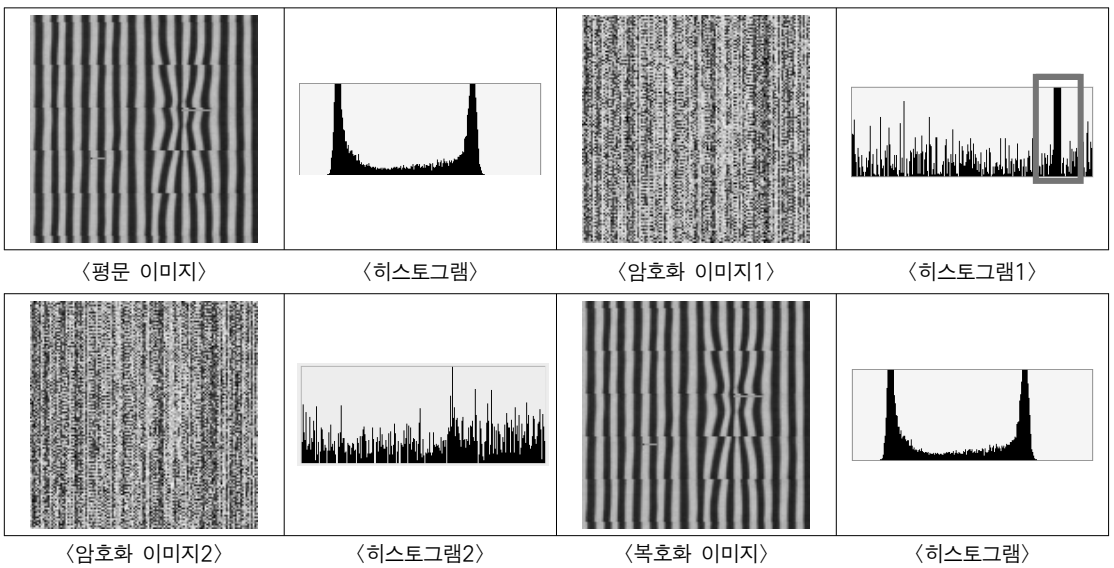
그러나 〔그림 8〕에서와 같이 히스토그램의 일정 부분의 비율이 높은 결과를 보여주게 되며, 이는 특정 키 값에서 발생하는 문제이다. 만약 악의적인 사용자가 이를 이용하여 평문 이미지의 일정 색의 분포를 예측할 수 있기 때문에 암호이미지에 대한 평문이미지의 일부 정보를 예측 할 가능성이 있다.



〔그림 7〕 구현 디지털 이미지 보안기술의 모의 테스트 결과

V. 결론 및 향후 연구

이미지 및 디지털 이미지 보안 기법의 경우 다양한 방법이 존재 한다. 하지만 산업용 보안의 경우 그 연구가 미비했다. 본 연구에서 산업용 디지털 이미지에 대한 암호화 기법을 제안하고 구현 하였다. 이를 이용한 산업용 디지털 이미지의 보안 응용에서 적용이 가능할 것으로 예상 된다. 그리고 구현이 되었을 경우 산업 기밀이 유출 되었더라도 원본과 암호화된 디지털 이미지의 일치율이 1% 미만으로 나왔기 때문에 암호화된 이미지에서 원본 이미지의 예측의 어렵다. 그러나 특정 키 값에 따른 보안상의 취약성은 향후 연구를 통해서 해결하고자 한다.



〔그림 8〕 이미지 암호화 복호화 및 히스토그램 결과

참고문헌

〔1〕 De Wang and Yuan-Biao Zhang, "Image encryption Algorithm Based on S-Boxes Substitution And Chaos Random Sequence," IEEE ICCMS'09, pp.110-113, Feb, 2009.

〔2〕 Li Chuanmu and Hong Lianxi, "New Image Encryption Scheme Based on Hyper-chaotic Sequences," 2007 IEEE International Workshop, pp.237-240, April, 2007.

〔3〕 Chen Wei-bin and Zhang Xin "Image encryption algorithm based on Henon chaotic system," ISAP 2009, pp94-97, April, 2009.

〔4〕 Yu Li, Li Yuanxiang and Xia Xuewen, "Image Encryption Algorithm Based on Self - adaptive Symmetrical-coupled Toggle Cellular-Automata," 2008 CISP'08, pp 32-36, May, 2008.

〔5〕 Ahmad M, Gupta C and Varshney A, "Digital Image Encryption Based on Chaotic Map for Secure Transmission," 2009. IMPACT '09, pp292-295, March, 2009.

〔6〕 Chen Wei-bin and Zhang Xin, "Image Encryption Algorithm Based on Henon Chaotic System," IASP2009, pp94-97, April, 2009.

〔7〕 Niu Jiping, "Image Encryption Algorithm Based on Rijindeal S-Boxes," CIS2008, pp.277-280. Dec, 2008.

〔8〕 Xin Zhang and Weibin Chen, "A New Chaotic Algorithm for Image Encryption," ICALIP2008, pp.889-892, July,2008.

〔9〕 Jin Jun, "Image Encryption Method based on Elementary Cellular automata," SOUTHEASTCON '09. IEEE, pp.345-349, March, 2009.

〔10〕 Fangchao Wang, Sen Bai, Guibin Zhu and Zhenghui Song, "An Image Encryption Algorithm Based on N-Dimension Affine Transformation," ICIS '09, pp.579-585, June, 2009

〔11〕 ARIA 개발팀, "민관겸용 블록 암호 알고리즘 ARIA 알고리즘 명세서," IT보안인증 사무국, MAY, 2004.

〔12〕 ARIA 개발팀, "블록 암호 알고리즘 ARIA," IT보안인증 사무국, May, 2004.

〔13〕 Daesung Kwon, Jaesung Kim, Sangwoo Park, Soo Hak Sung, Yaekwon Sohn, Jung Hwan Song, Yongjin Yeom, E-Joong Yoon, Sangjin Lee, Jaewon Lee, Seongtaek Chee, Daewan Han, and Jin Hong, "New Block Cipher: ARIA," LNCS 2971, pp. 432-445, 2004.

〔14〕 Alex Biryukov, Christophe De Canni, Joseph Lano, Siddika Berna Ors and Bart Preneel, "Security and Performance Analysis of Aria," LEUVEN UNIV COSIC, January, 2003.

〔15〕 문광석, "디지털 워터마킹을 이용한 건축설계도면의 저작권 보호에 관한 연구," 한국 과학재단, May, 2004.

〈著者紹介〉

홍 영 식 (Young Sik Hong) 정회원
1973년 2월: 서울대학교 응용수학과 졸업
1975년 8월: 한국과학기술원 전산학과 석사
1986년 8월: 서울대학교 컴퓨터공학과 박사
1976년 9월~현재: 동국대학교 컴퓨터공학과 교수
〈관심분야〉 분산처리, 분산/병렬알고리즘, 암호학, 정보보호시스템

정 장 영 (Jang-young Chung) 학생회원
2006년 8월: 대전대학교 전산정보보호학과 졸업
2009년 2월: 동국대학교 컴퓨터 공학과 석사
2009년 3월~현재: 동국대학교 컴퓨터 공학과 박사과정
〈관심분야〉 이미지 보안, 인증 프로토콜, 병렬 이미지 암호알고리즘, 생체보안