한국광학회지 Hankook Kwanghak Hoeji, Volume 14, Number 5, October 2003

Binary CGH를 사용한 JTC 광암호화 시스템 연구

주성현 · 정만호†

청주대학교 레이저 광정보공학과

㉾ 360-764 충북 청주시 상당구 내덕동 36

(2003년 2월 5일 받음, 2003년 8월 12일 수정본 받음)

Joint transform correlator(JTC)를 기반으로 이진 암호화 키를 사용하는 광 암호화 시스템을 제시하였다. 이진 암호화 키는 pixel-oriented CGH의 설계방법을 이용하여 제작하였고, 컴퓨터 모의 실험결과를 통하여 구현된 이진 암호화 키의 독립성 및 효능을 조사하였다. CGH방법으로 구현된 이진 암호화 키의 효능을 검증하기 위하여 홀로그래픽 메모리 기반의 광 암호화 장치를 구성하여 실험을 하였으며 그 결과 높은 암호화 가능성을 나타내었다.

주제어 : optical encryption, binary key code, holographic encryption system, joint transform correlator.

I. 서 론

사회의 정보화가 진전됨에 따라 개인 정보의 보안이 중요한 문제로 대두되고 있고, 이를 위한 보안 시스템들이 활발하게 연구되고 있다. 이 중에서 지문인식이나 얼굴인식과 같은 생체 인식을 이용한 시스템들이 차세대 보안시스템으로 채택되는 것은 거스를 수 없는 대세로 받아들여지고 있다. 또한 이러한 보안시스템들이 정상적으로 운영되기 위해서는 외부로 노출되는 생체패턴을 반드시 보호하기 위한 방법이 필요하게 된다. 그동안 생체패턴 및 영상정보의 보호를 위하여 랜덤패턴을 기준파로 사용하는 홀로그램의 제작과 같은 방법이 이용되어 왔고, 그 중에서 가장 대표적인 방법이 이중 랜덤 위상 암호화(Double Random Phase Encryption) 방법[1-3]이다. 이 암호화 방법은 암호화된 데이터가 복소값을 가지므로 광학적인 구현시 약간의 문제점이 발생할 수 있고, 특히 해독 알고리즘에 의해 해독될 가능성이 크다는 것이 단점이다. 따라서 이를 보완하기 위해서 Joint Transform Correlator(JTC) 구조를 사용하는 이중 랜덤 암호화 방법이 제안되었다.[4-6]

본 논문에서는 생체인증과 같은 실제 보안시스템에 적용하기 위하여 기존에 알려진 JTC 구조를 사용하는 이중 랜덤 위상 암호화 방법에 대하여 실제 컴퓨터 모의 실험과 광학 실험을 통하여 그 실현 가능성을 검증하였다. 암호화 과정에서 사용되는 이진 암호화 키는 Pixel-Oriented CGH 기법[7,8]을 이용하여 설계하였고, 설계된 이진 암호화 키가 실제로 암호화 키로서의 역할을 수행할 수 있는지 컴퓨터 모의 실험을 통하여 독립성 및 효능을 제시하였다. 특히 CGH 방법으로 제작된 이진 암호화 키의 컴퓨터 모의 실험 결과를 검증하기 위하여 홀로그래픽 메모리 기반의 광학실험을 수행하였으며 그 결과 홀로그래픽 광암호화 장치의 실제 적용 가능성을 나타내었다.

†E-mail: manho@chongju.ac.kr

II. Pixel-oriented CGH 이진 암호화 키의 구현

그림 1은 JTC 구조를 기반으로 하는 암호화 및 복호화 과정을 나타낸다.

그림 1-(a)는 입력영상을 암호화하기 위한 과정으로 입력 영상 $f(x,y)$와 암호화 키코드 $h(x,y)$가 동일한 입력 평면상에서 각각 좌표 $x=a$와 $x=b$에 위치되고 후리어 변환 렌즈에 조명하여 후리어 변환된다. 이 때, 입력영상은 입력 랜덤 위상마스크 $\alpha(x,y)$와 붙여져서 입력면에 위치된다. 즉, $\alpha(x,y)$ $f(x,y)$가 암호화될 입력 영상으로 사용된다. $h(x,y)$는 암호화 키로 역할을 하며 후리어 랜덤 위상마스크 $H(u,v)$의 역후리어 변환이다. 결과적으로, 후리어 면에 형성되는 Joint Power Spectrum (JPS)은 다음과 같다.

$$
\begin{aligned}
&E(u,v)\\
&=\Im\{\alpha(x-a,y)f(x-a,y)+h(x-b,y)\}^2\\
&=[A(u,v)*F(u,v)\exp(-j2\pi ua)]+H(u,v)\exp(-j2\pi ub)]^2\\
&=|A(u,v)*F(u,v)|^2+|H(u,v)|^2\\
&+[A(u,v)*F(u,v)]+H^*(u,v)\exp[-j2\pi(a-b)u]\\
&+[A(u,v)*F(u,v)]^*H(u,v)\exp[-j2\pi(b-a)u] \qquad (
\end{aligned}
$$

여기서, $*$은 convolution 연산자이다. $A(u,v)$와 $F(u,v)$는 각각 $\alpha(x,y)$와 $f(x,y)$의 후리어 변환을 나타내고, $H(u,v)$는 위상 정보만을 가지고 있으므로 $|H(u,v)|^2=1$이다. 식 (1)로 주어지는 간섭무늬 세기 분포, 즉 JPS가 암호화된 데이터로 저장된다. 따라서, 이 방법으로 암호화된 데이터는 양의 실수 값을 갖는다. 그림 1-(b)에서처럼, 암호화된 데이터의 복호화는 입력면에 암호화 당시에 사용된 암호화 키를 좌표 $x=b$에 위치시킴으로써 수행될 수 있다. 이 때, 암호화된 영상 $E(u,v)$는 후리어 랜덤 위상 마스크, $H(u,v)\exp(-j2\pi ub)$에 의해 조명된다. 즉, 입력 영상을 랜덤 기준파와의 간섭을 통해 후리어 변환 홀로그램으로 기록하고 재생하는 방법과 동일하다고 할

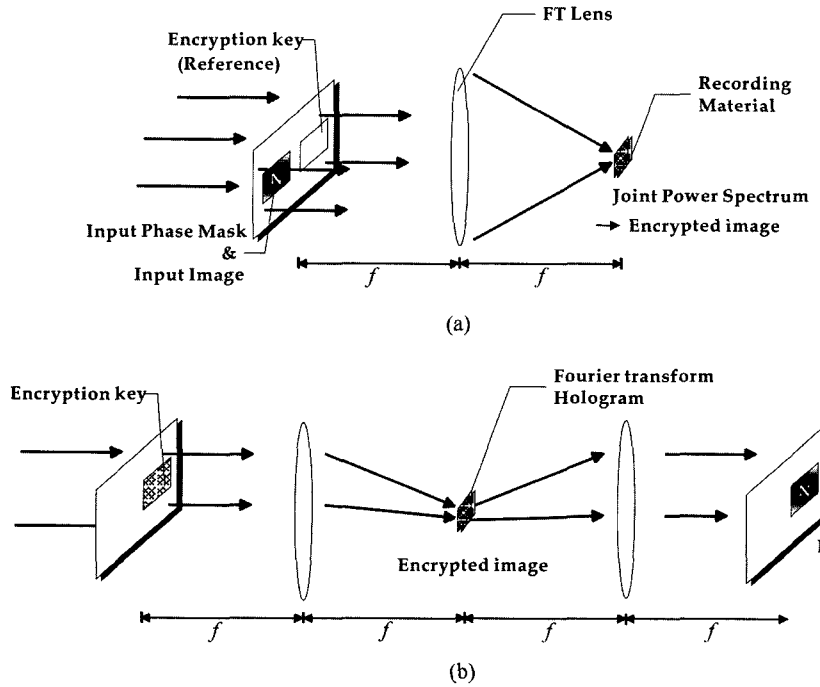


그림 1. JTC 구조를 사용하는 광암호화 시스템. (a) 암호화 과정, (b) 복호화 과정.

있다. 따라서, 후리어 변환 홀로그램을 재생하면 원 영상의 정보를 얻어낼 수 있다. 즉,

$$
\begin{aligned}
&d(x,y)= \\
&[\alpha(x,y)f(x,y)]^{*}\star[\alpha(x,y)]*\delta(x+b,y) \\
&+h(x,y)\ d(x+b,y) \\
&+\alpha(x,y)f(x,y)*\delta(x+a,y) \\
&+[\alpha(x,y)f(x,y)]^{*}*h(x,y)h(x,y)*\delta[x-(2b-a),y]
\end{aligned}
\tag{2}
$$

여기서 ★는 correlation 연산자이다. 식 (2)의 우항에서 첫 번째 항과 두 번째 항은 각각 입력 함수와 암호화 키의 자기 상관에 의한 DC항으로서, 원 영상을 복원하는데 도움을 주지 않는 항이다. 따라서 출력면에서 $x=-b$인 위치를 공간적으로 필터링 함으로써 원 영상을 복호화 하는데 필요한 항들만 추출할 수 있다. 세 번째 항은 초기 입력 영상을 복원해 낼 수 있는 항이다. $f(x,y)$는 양의 실수 함수이고, 위상 함수 $a(x,y)$는 순수한 위상 성분만으로 이루어진 함수이기 때문에, CCD와 같은 세기 검출기를 사용하면 원 영상을 복원해 낼 수 있다. 복호화 영상은 출력면의 좌표 $x=-a$에서 검출되며, 출력면 좌표 $x=2b-a$에서 잡음과 같은 원치 않는 항이 복원된 영상과 공간적으로 분리되어 나타난다. 따라서, 복원된 영상만을 검출해 낼 수 있다.

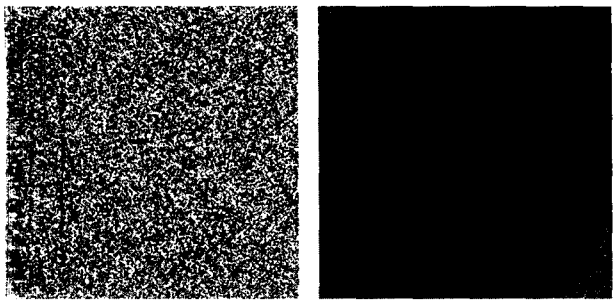
JTC구조의 암호화 방법에서 사용되는 암호화 키는 후리어 랜덤 위상마스크의 역후리어 변환으로 정의된다. 이중 랜덤 위상 암호화 방법에서는 랜덤 위상마스크가 가장 핵심적인 암호화 소자이다. 전자적인(electrical) 암호화 시스템의 경우에 랜덤 위상마스크는 상대적으로 쉽게 구현될 수 있으나 광학적인(optical) 암호화 시스템의 경우에 랜덤 위상마스크의 구현은 그리 간단한 문제만은 아니다. 특히 후리어 랜덤 위상마스크는 물리적으로 존재하지 않으며, 순수한 위상 성분만을 갖는 복소함수이므로 이를 구현하기 위해서는 컴퓨터 형성 홀로그램(Computer Generated Holograms, CGH)의 설계 기법[7,8]과 같이 이진 데이터로부터 복소함수를 재생시킬 수 있는 방법이 사용되어야 한다. 또한, 랜덤 위상은 물리적으로 표현하기는 힘들지만 수학적으로 충분히 나타낼 수 있는 함수이므로 후리어 변환 CGH를 이용하여 합성될 수 있다. 따라서 본 논문에서는 JTC 구조의 암호화 시스템에 사용하기 위한 암호화 키를 구현하기 위하여 pixel-oriented CGH의 설계 방법을 사용하였다. 후리어 면에서 랜덤한 위상분포를 재생시킬 수 있는 암호화 키의 구현을 위해서 다음과 같이 에러함수를 정의하여 그 값이 최소가 되도록 하는 조건으로 CGH 패턴을 얻어내었다.

$$E=\sum(\Im\{h(x,y)\}-C)^{2} \tag{3}$$

여기서, $h(x,y)$는 후리어 랜덤 위상마스크 함수 $H(u,v)$의 역후리어 변환으로써 암호화 키, 즉 CGH의 투과도 함수를 나타내며 C는 목표값으로 균일한 단위진폭 분포를 갖는 함수이다. CGH 패턴을 얻기 위한 입력영상으로는 균일한 단위진폭(unity amplitude)을 갖고 균일한 랜덤위상을 갖는 복소함수를 사용하였고, 후리어 면에서 aliasing효과를 제어하기 위하여 물체크기의 4배 만큼 오버 샘플링(over sampling)하였다.[7,8] 또한, 계산된 홀로그램의 투과도 함수를 직접양자화에 의한 이진 처리하여 이진값을 갖도록 하였다. 그림 2는 본 논문에서 구현된 이진 암호화 키와 그 재생상을 나타낸다.

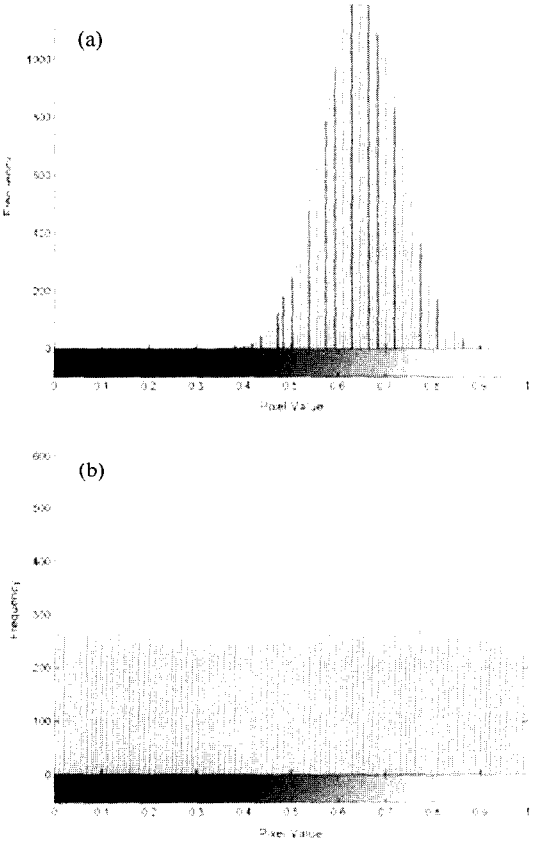
암호화 키가 정확하게 재생되는지 확인하기 위해서 재생된 영상의 1차 회절만을 추출하여 진폭과 위상에 대한 히스토그램을 계산하여 보았다. 그림 3은 이진 암호화 키로부터 재생된 후리어 랜덤 위상마스크의 진폭과 위상에 대한 히스토그램이다.

그림 3-(a)에서 진폭분포는 균일한 단위진폭이 아님을 확인할 수 있고 이 효과에 의해 암호화 과정에서 암호화된 영상의



(a) (b)

그림 2. (a) 이진 암호화 키, (b) 암호화 키의 재생상.



림 3. 이진 암호화 키의 재생상의 히스토그램. (a) 진폭분포, (b) 위상분포.

폭이 변조될 것이다. 그러나 그림 3-(b)의 위상분포는 서로 관계가 존재하지 않고 균일하게 분포되어 있으므로 암호는 성공적으로 수행된다는 것을 예상할 수 있다.

다음으로 암호화 키의 상호 독립성에 대하여 고려하여 본다. 암호화 키의 후리어 변환이 균일한 단위진폭과 균일한 랜 위상을 가진다는 것이 밝혀졌을 때 똑같은 암호화 키의 복 기능성에 대한 고찰이다. 구현된 이진 CGH가 암호화 키 서의 역할을 수행하기 위해서는 어떠한 상황에서도 다음과 은 조건이 만족되어야 한다.

$$\arg[H_i(u,v)] \neq \arg[H_j(u,v)] \quad \text{for } i \neq j \tag{4}$$

기서, arg[ ]는 괄호내의 함수에서 위상성분만을 추출하는 연

표 1. 이진 암호화 키의 독립성 조사

	key 1	key 2	key 3	key 4	key 5
key 1	0	1.8098	1.8188	1.8196	1.8127
key 2	1.8098	0	1.8109	1.8123	1.8176
key 3	1.8188	1.8109	0	1.8182	1.8036
key 4	1.8196	1.8123	1.8182	0	1.8143
key 5	1.8127	1.8176	1.8036	1.8143	0

산을 나타낸다. 이를 위하여, 5개의 서로 다른 암호화 키를 각 구현하여 다음과 같은 연산을 수행하였다.

$$\text{std}\{\arg[H_i(u,v)\,H_j^*(u,v)]\} \tag{5}$$

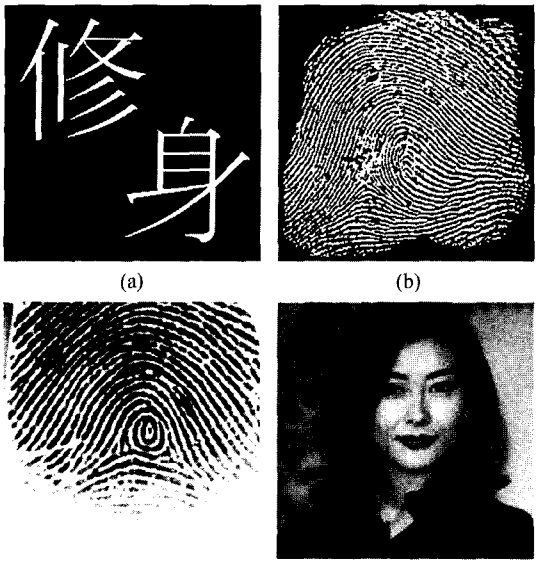
여기서, std{ }는 괄호내의 함수에 대한 표준편차를 구하는 연산을 의미한다. 만약 임의의 두 암호화 키가 서로 동일하다면, 두 암호화 키의 후리어 변환의 위상성분이 완전히 같을 것이므로 식 (5)에서 $H_i(u,v)\,H_j^*(u,v)$의 연산 결과는 연산 도중 위상 성분이 소거되어 진폭 성분만 남게된다. 그러나 두 위상분포가 조금이라도 다르게되면, 곱의 결과는 진폭과 위상이 모두 존재하는 복소함수가 될 것이다. 따라서 곱의 결과에서 위상 성분만을 취하면, 전자의 경우에는 0이 되고 후자의 경우에는 0이 아닌 어떤 값을 가지게 될 것이다. 이 실험에 대한 결과를 표 1에 나타내었다.

표 1로부터 식 (4)의 조건이 잘 만족되는 것을 확인할 수 있다. 따라서, 구현된 암호화 키는 서로 완전히 독립적이라는 것을 알 수 있고, 암호화 키의 구현 방법을 알아냈다고 하더라도 그와 동일한 암호화 키를 복제할 수 있는 가능성은 존재하겠지만, 그 확률은 매우 미미하다고 할 수 있다. 그 이유는 N개의 레벨을 갖는 M 픽셀 크기의 영상에서 무려 N^M에 해당하는 개수의 패턴이 생길 수 있기 때문이다. 예를 들어 0과 1의 2레벨을 갖는 256×256 크기의 영상이라면, $2^{65536} \approx 10^{19}$개의 패턴이 생길 수 있다. 즉 무한개의 암호화 키가 만들어지므로 그 중에서 똑같은 암호화 키를 찾아낸다는 것은 거의 불가능하다고 보아야 할 것이다.

III. 전산모의 및 실험결과

3.1. 전산 모의 실험

암호화 시스템에서 사용하는 암호화 키의 정의가 후리어 변환 위상마스크의 역후리어 변환이므로 다음과 같이 두 가지 경우로 암호화 키를 구현하여 암호화 및 복호화의 전산 모의실험을 수행하였다. 첫 번째는 암호화 키의 정의를 그대로 사용한 경우로, 암호화 키는 복소함수의 형태를 가지며 입력영상의 크기와 동일한 크기를 갖는다. 두 번째는 앞절에서 논의한 pixel-oriented CGH로 암호화 키를 구현한 경우이다. 첫 번째 구현 방식의 암호화 키는 복호화되어 출력되는 영상의 질이 상대적으로 우수하고 비교적 간단하게 구현할 수 있지만 광학 시스템으로 구성하기에는 여전히 부적절하다. 그 이유는 암호화된 영상은 양의 실수 값을 갖지만, 암호화 키가 여전히 복소함수이기 때문이다. 두 번째 방식의 암호화 키를 사용하는 경우는 암호화 키가 이진 데이터의 형식을 가지고 있으므로



(a) (b) (c) (d)

그림 4. 암호화 시스템을 테스트하기 위한 입력영상. (a) Case 1: 이진 문자영상, (b) Case 2: 이진 지문영상, (c) 256그레이 지문영상, (d) 256그레이 인물영상.

광학적으로 구현하는데 있어서 큰 이점을 가지고 있고 상대적으로 향상된 암호화 수준으로 영상을 암호화할 수 있으나 이진화 과정에서 영상정보의 부족으로 인하여 복호화 되어 출력되는 영상의 질이 다소 저하되는 단점이 있다. 따라서 이를 보완하기 위해서는 반드시 최적화 과정이 병행되어야 한다.[12]

본 논문에서 암호화 키는 이진 데이터의 형태를 가지며 입력영상의 4배의 크기를 갖는다. 또한 설계된 CGH는 비축상에 ±1차 회절광으로 재생되므로 암호화 및 복호화 과정에서는 +1차 회절만 사용하였다. 암호화 및 복호화를 테스트하기 위한 입력영상으로 그림 4에 나타낸 네 가지 샘플을 사용하였다. 이 입력영상들은 이진 지문영상에서부터 256그레이 레벨의 인물영상까지 일반적인 보안시스템에서 사용자의 정보를 나타내는 데이터의 형식을 갖추고 있다.

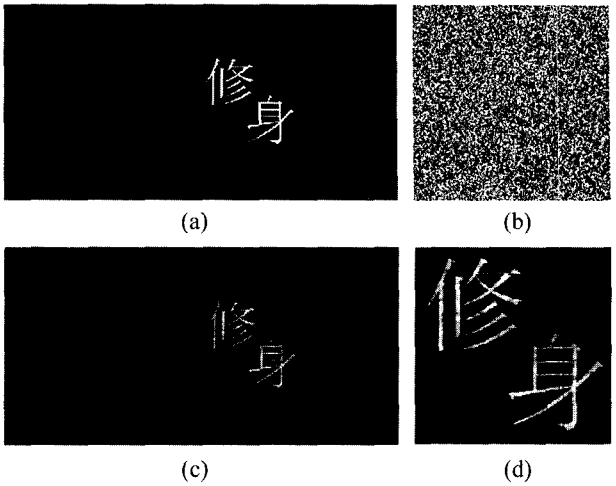
이때 복호화된 영상의 질을 정량적으로 비교하기 위한 척도로서 다음과 같이 정의된 Mean Squared Error(MSE)와 Signal to Noise Ratio(SNR)[9,10]을 사용하였다.

$$\mathrm{MSE}=\frac{1}{NM}\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}[f(x,y)-f_r(x,y)^2] \tag{6}$$

$$\mathrm{SNR(dB)}=10\log_{10}\frac{\sigma_u^2}{\mathrm{MSE}} \tag{7}$$

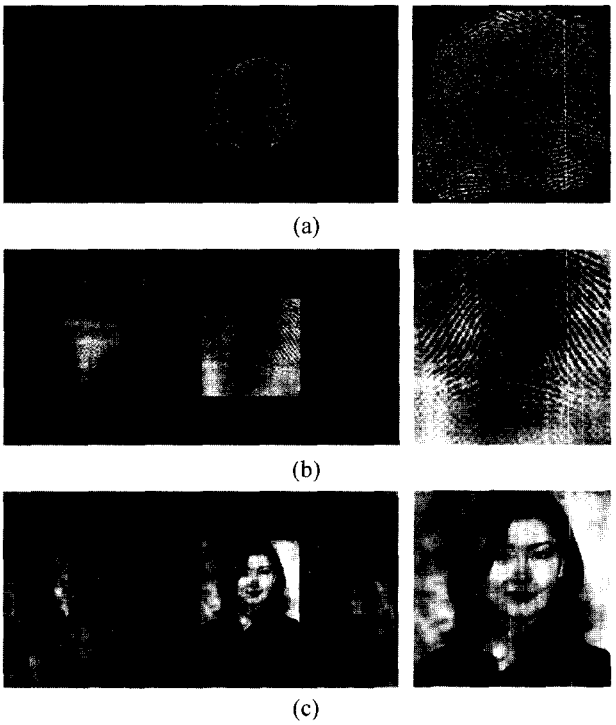
여기서, $N\times M$은 영상의 픽셀 수를 나타내고, $f(x,y)$와 $f_r(x,y)$는 각각 초기 입력영상과 복호화된 영상을 나타낸다. 그리고 σ_u^2은 원 영상의 분산값을 나타낸다. 따라서 복호화된 영상이 원 영상하고 비슷할수록 MSE는 0으로 향하고, SNR은 무한대로 향하게 된다.

그림 5와 그림6은 첫 번째 경우의 암호화 키를 사용하여 암호화 및 복호화를 수행한 결과이다.



(a) (b) (c) (d)

그림 5. 단순한 정의를 이용하여 구현된 암호화 키를 사용하여 얻어진 결과 중 이진 문자영상에 대한 경우. (a) 입력면에서의 영상, (b) 암호화된 영상의 일부분, (c) 출력면에서의 영상, (d) 복호화된 영상.



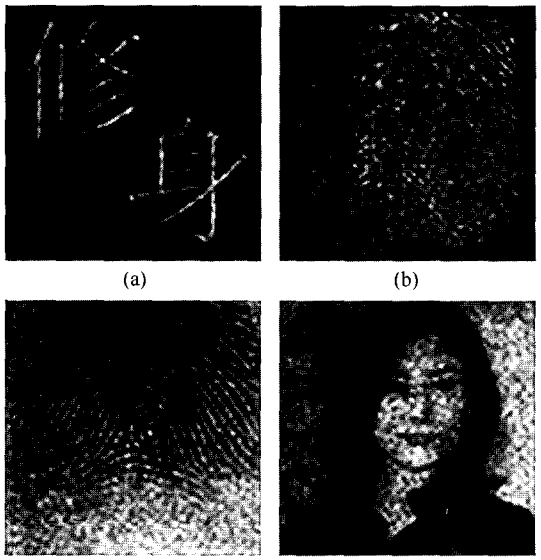
(a) (b) (c)

그림 6. 단순한 정의를 이용하여 구현된 암호화 키를 구현한 경우, 암호화 및 복호화 결과. (a) 이진 지문영상의 경우, (b) 256그레이 지문영상의 경우, (c) 256그레이 인물영상의 경우.

그림 5-(a)는 JTC의 입력면을 나타내며 암호화 키와 암호화할 입력영상을 입력면의 중심으로부터 각각 128픽셀씩 이동시켜 위치시켰다. 따라서 그림 5-(c)에서처럼 복호화되어 출력되는 영상 또한 같은 간격만큼 이동되어 출력된다. 출력면의 좌표는 입력면 좌표에 대하여 180° 회전되기 때문에 입력면의 좌표를 기준으로 유도한 식 (2)의 결과와 그림 5-(c)의 결과는 동일하다. 그림 5-(b)는 암호화된 JPS의 일부분을 나타낸 것이며, 그림 5-(d)는 복호화된 영상만 추출한 것이다. 그림 6은 나머지

표 2. 단순한 암호화 키를 사용한 경우, 복호화된 영상의 MSE와 SNR

	Use Correct Key				
	Case 1	Case 2	Case 3	Case 4	Mean
MSE	0.0184	0.1087	0.0098	0.1010	0.059475
SNR(dB)	6.3841	2.3639	6.0982	2.4683	4.328625
	Use Incorrect Key				
	Case 1	Case 2	Case 3	Case 4	Mean
MSE	0.1278	0.2655	0.2263	0.08168	0.17532
SNR(dB)	−0.8077	−0.2249	−0.572	−1.416	−0.75515



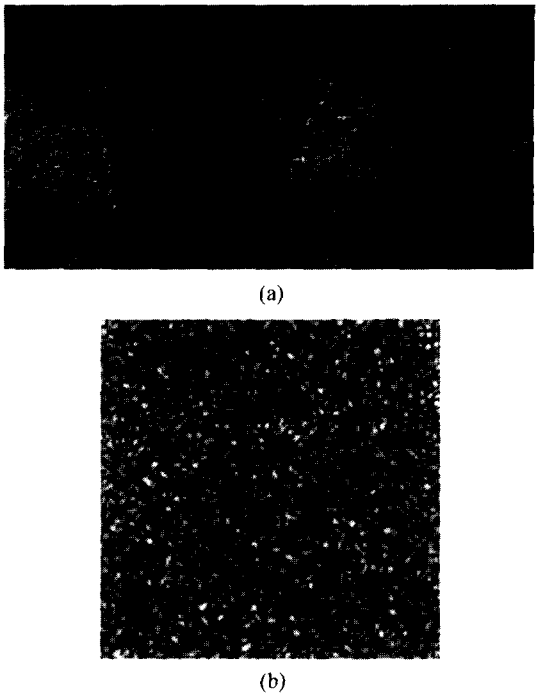
(a) (b) (c) (d)

그림 7. CGH를 사용하여 이진 암호화 키를 구현한 경우, 암호화 및 복호화 결과. (a) 이진 문자영상의 경우, (b) 이진 지문영상의 경우, (c) 256그레이 지문영상의 경우, (d) 256 그레이 인물영상의 경우.

개의 입력영상에 대한 결과 중 출력면에서 복호화되어 나타나는 영상만 표시한 것이다. 복호화된 영상에서 나타나는 잡음은 식 (2)의 잡음 항에 의해 기인한 것으로 판단되며, 실제 응용 시스템으로 응용될 때에는 반드시 해결되어야 할 문제이다. 표 2는 첫 번째 경우의 암호화 키를 사용하여 복호화한 영상의 MSE와 SNR을 계산한 결과이다. 표 2로부터, 올바른 암호화가 그렇지 않은 경우에 대하여 MSE는 약 2.94배 낮고 SNR은 약 5.73배 정도 크게 나타났다.

그림 7과 그림 8은 CGH방법으로 제작된 두 번째 경우의 이진 암호화 키를 사용하여 복호화를 수행한 결과이다.

그림 7을 통하여 살펴볼 때 첫번째 방법에 의한 결과 보다 육안으로 간신히 구별할 수 있을 정도로 복호화된 영상의 질이 상당히 저하되었다는 것을 알 수 있다. 이렇게 이진 암호화 키를 사용한 경우 복호화된 영상의 질이 저하되는 이유는 암호화 키로부터 재생되는 랜덤 위상마스크의 진폭분포가 그림 3-(a)와 같이 균일한 단위진폭이 아니기 때문에 암호화된 영상의 진폭을 변조시키기 때문이다. 이 암호화된 영상의 진폭변조 효과는 암호화된 영상에 잡음이 섞여 왜곡된 경우와 유사한 영향을 복호화에 미치게 된다. 그러나 그림 8의 결과를 통하여 알 수



(a) (b)

그림 8. 옳지 않은 암호화 키를 사용하여 복호화를 시도한 결과. (a) 단순한 암호화 키를 사용한 경우, (c) CGH에 의한 이진 암호화 키를 사용한 경우.

표 3. 이진 암호화 키를 사용한 경우, 복호화된 영상의 MSE와 SNR

	Use Correct Key				
	Case 1	Case 2	Case 3	Case 4	Mean
MSE	0.0275	0.1969	0.1507	0.0134	0.097125
SNR(dB)	4.7350	6.9759	4.4387	7.4967	5.911575
	Use Incorrect Key				
	Case 1	Case 2	Case 3	Case 4	Mean
MSE	0.1377	0.2701	0.2967	0.0782	0.195675
SNR(dB)	−0.9219	−0.4742	−0.8805	−1.2116	−0.8720

있듯이 옳지 않은 암호화 키를 사용한 경우와 비교해보면 암호화 및 복호화 자체는 성공적으로 이루어 졌다고 할 수 있다. 수치적으로도 표 3의 복호화 결과를 살펴보면 올바른 암호화 키를 사용한 경우가 옳지 않은 암호화 키를 사용한 경우 보다 MSE는 약 2.01배 낮고, SNR은 약 6.78배 높은 것으로 나타나 암호화 및 복호화에는 문제가 없는 것을 나타내고 있다.

3.2. 광학 실험

이진 암호화 키를 사용하는 홀로그래픽 광암호화 시스템을 실험적으로 제시하기 위하여 그림 9와 같은 구조를 사용하였다.

이진 암호화 키는 앞 절에서 논의된 pixel-oriented CGH의 설계방법으로 구현하였고, 계산된 CGH 패턴의 크기는 공간광 변조기(Spatial Light Modulator, SLM)의 픽셀 크게에 맞추어 640×480 픽셀로 하였다. 본 실험에서 사용된 SLM은 EPSON 사의 VGA급 투과형 LCD로 한 픽셀이 약 42 μ 크기를 갖는다. 암호화 할 영상은 알파벳 'E'의 이진 영상을

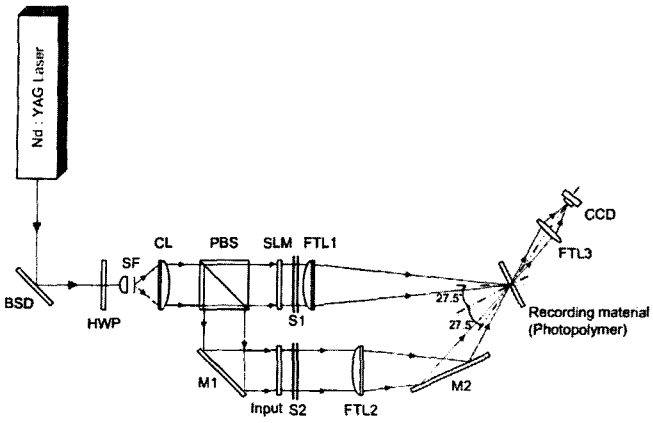


그림 9. 광학 실험 장치도.

프린트하여 투명 마스크의 형태로 제작하였고, 입력 랜덤 위상 마스크로는 확산판(diffuser)을 사용하였다. 따라서 암호화 시스템의 입력 물체는 두 마스크가 붙여져서 그림 9의 Input에 위치된다. CGH와 입력 물체를 조명하기 위한 가간섭성 광원으로 Coherent사의 CW형 Nd:YAG 레이저(532nm에서 150 mW)를 사용하였고, 홀로그램을 기록하기 위한 매질로는 Dupont 사의 포토폴리머 HRF-150-38을 사용하였다. 그림 9를 참고하여, 입력 물체를 암호화하기 위해서 셔터 S1과 S2가 모두 열린다. 평행광이 SLM을 조명하면 암호화 키가 FTL1에 의해 재생되어 기록면에 랜덤 위상을 분포시킨다. 이와 동시에 물체 경로에서는 입력 영상이 조명되고 FTL2에 의해 후리어 변환되어 기록면에 입력 물체의 스펙트럼이 형성된다. 따라서 기록면에서는 랜덤 위상의 기준빔과 입력 물체 스펙트럼의 물체빔이 간섭되어 간섭무늬가 포토폴리머에 기록되며, 이 포토폴리머에 기록된 정보를 암호화된 영상으로 이용하게 된다.

그림 10-(a)는 셔터 S1만 열고 암호화 키코드를 재생한 영상, 즉 기준빔을 CCD로 획득한 영상이다. 컴퓨터 모의 실험 결과에서처럼 재생된 후리어 랜덤 위상 분포의 진폭이 변조된 것을 확인할 수 있다. 그림 10-(b)는 셔터 S2만 열고 입력 영상을 CCD로 획득한 영상이다. 암호화된 영상을 복호화하기 위해서 S2는 닫고 S1은 연다. 그러면 암호화 키로부터 재생되는 랜덤 위상 패턴이 홀로그램을 조명하고 홀로그램에 기록된 정보가 재생된다. 그 다음 FTL3에 의해 역후리어 변환되어 CCD에 복호화된 상이 형성된다. 본 실험에서는 두 개의 암호

표 4. 광학 실험의 결과로 복호화된 영상의 MSE와 SNR

Mean Squared Error, MSE		
Encryption \ Decryption	Key 1	Key 2
Key 1	0.0051	0.0250
Key 2	0.0724	0.0094
Signal to Noise Ratio, SNR (dB)		
Encryption \ Decryption	Key 1	Key 2
Key 1	8.5475	0.9249
Key 2	0.7362	7.3527

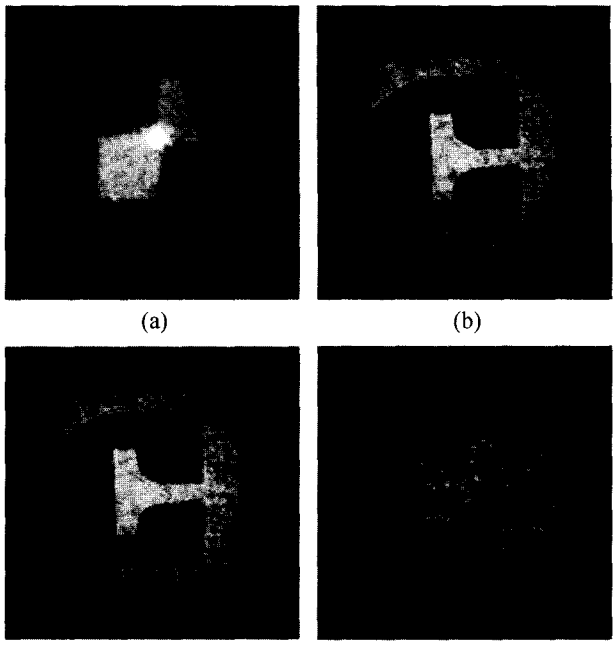


그림 10. 광학 실험 결과. (a) 암호화키의 재생상(홀로그램의 기준빔), (b) 입력영상, (c) 올바른 키에 의해 복호화된 영상, (d) 옳지 않은 키로 복호화를 시도한 경우의 출력영상.

화 키를 제작하여 각각의 경우에 대한 암호화 및 복호화를 수행하여 보았다. 그림 10-(c)는 올바른 키에 의해 복호화된 영상을 나타내고, 그림 10-(d)는 옳지 않은 키를 사용하여 복호화를 시도한 경우에 해당한다. 정량적인 비교를 위해서 입력 영상 기준으로 복호화된 영상의 MSE와 SNR을 계산하여 표 2에 나타내었다. 표 2로부터, 올바른 키를 사용하여 복호화한 결과가 그렇지 않은 경우에 비하여 SNR은 약 9.57배 정도 크며, MSE는 약 6.71배 차이가 발생하였다. 따라서 이 결과는 이진 키코드를 사용한 홀로그래픽 광 암호화 및 복호화의 가능성을 충분히 증명해 주었다고 할 수 있다.

IV. 결 론

본 논문에서는 기존의 이중 랜덤 위상 암호화 방법을 광학적으로 구현하기 위한 방법으로 암호화된 영상의 세기(intensity)를 이용하는 JTC 구조의 암호화 시스템을 고려하였다. 이러한 시스템은 복소함수로 표시되는 랜덤 마스크를 실제적인 시스템에서 구현할 때 대두되었던 기존의 문제를 해결할 수 있으며, 또한 후리어 랜덤 위상분포를 만들어 내기 위해서 이진 암호화 키코드를 사용하였는데 이로 인하여 암호화가 높은 수준으로 향상되었다. 이진 암호화 키는 pixel-oriented CGH의 설계 방법을 이용하여 구현하였다. CGH로부터 재생되는 영상이 균일한 단위진폭과 랜덤 위상을 갖도록 CGH 패턴을 설계하였지만, 이진화로 인한 픽셀정보의 부족 때문에 재생영상의 진폭이 변조되었고 이에 따라서 복호화된 영상의 질을 저하시키는 결과를 초래하였다. 그러나 본 연구에서 구현된 이진 키코드가 암호화 키로서의 역할을 충분히 수행할 수 있다는 것과

암호화 키의 위·변조 및 복제가 거의 불가능하다는 것을 컴퓨터 모의 실험을 통하여 증명하였다. 따라서 이전에 대두되었던 암호화 시스템에서의 복소함수의 표현에 대한 문제와 높은 암호화 수준에 대한 문제는 암호화된 데이터의 세기 정보를 이용하는 JTC 방법으로 해결되고 이진 암호화 키를 사용하고 홀로그래픽 광 암호화 시스템에 대한 검증을 위하여 홀로그래픽 메모리 기반의 광학적 실험을 하였다. 실험결과 올바른 이진 암호화 키를 사용했을 경우에 옳지 않은 암호화 키를 사용했을 경우보다 SNR은 약 9.57배 그리고 MSE는 약 6.71배의 차이가 나서 이진 키코드를 사용한 홀로그래픽 광 암호화 및 복호화 시스템의 가능성을 충분히 증명해 주었다고 할 수 있다. 앞으로 본 논문을 통하여 검증된 홀로그래픽 이진 암호화 시스템을 생체 정보를 이용한 시스템에 응용하여 효율적인 사용자 인증을 위한 실험과 광학적 또는 전자적인 실제의 시스템으로 개발하기 위한 연구가 계속적으로 진행되어야 할 것이다.

감사의 글

본 연구는 2003학년도 청주대학교 학술연구조성비(일반과제)에 의하여 이루어진 연구입니다.

참고문헌

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767-769, 1995.

[2] B Javidi and E. Ahouzi, "Optical security system with Fourier plane encoding," *Appl. Opt.*, vol. 37, no. 26, pp. 6247-6255, 1998.

[3] B. Javidi, L. Bernard, and N. Towghi, "Noise performance of double-phase encryption compared to XOR encryption," *Opt. Eng.*, vol. 38, no. 1, pp. 9-19, 1999.

[4] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Opt. Eng.*, vol. 39, no. 8, pp. 2031-2035, 2000.

[5] T. Nomura and B. Javidi, "Optical encryption system with a binary key code," *Appl. Opt.*, vol. 39, no. 26, pp. 4783-4787, 2000.

[6] T. Nomura, S. Mikan, Y. Morimoto, and B. Javidi, "Optical image Encryption using an optimally designed encryption key," International workshop on optical display and information processing, pp. 34-42, Gyeongju, Korea, May 2002.

[7] E. Wolf, *Progress In Optics*, Vol. 28, North-Holland : Elsevier Science, 1990.

[8] J. W. Goodman, *Introduction to Fourier optics*, 2'nd Ed. McGraw-Hill, 1996.

[9] Anthony Vanderlgut, *Optical signal processing*, North Carolina : John Willey & Sons, 1992.

[10] B. V. K. Vijaya Kumar and L. Hassebrook, "Performance measure for correlation filters," *Appl. Opt.*, vol 29, no. 20, pp. 2997-3006, 1990.

[11] R. K. Battig, C. C. Guest, S. R. Schaefer, and D. J. Toms, "Simulated annealing of binary holograms for the interconnection of single-mode structures," *Appl. Opt.*, vol. 31, no. 8, pp. 1059-1066, 1992.

[12] M. Yamazaki and J. Ohtsubo, "Optimization of encrypted holograms in optical security systems," *Opt. Eng.*, vol. 40, no. 1, pp. 132-136, 2001.

[13] H. T. Chang, W. C. Lu, and C. J. Kuo, "Multiple-phase retrieval for optical security systems by use of random-phase encoding," *Appl. Opt.*, vol 41, no. 23, pp. 4825-4834, 2002.

A study on JTC optical encryption system using binary CGHs

Sung Hyun Joo and Man Ho Jeong†

Department of Laser and Optical Information Engineering, Chongju University, Chongju 360-764, KOREA

†*E-mail: manho@chongju.ac.kr*

(Received February 5, 2003, Revised manuscript August 12, 2003)

In this paper, an optical encryption system using binary key code based on the joint transform correlator (JTC) is considered. The binary key code is synthesized by using a design technique of the pixel-oriented Computer Generated Holograms (CGHs). The independence and efficiency of the binary encryption key are investigated through computer simulation. To test the efficiency of the encryption system using binary key code, a holographic encryption system is constructed, and the experimental results prove that our holographic encryption system has high ability.

OCIS Codes : 050.1380, 070.4550, 090.1760.