濟州大學校 尖端技術硏究所 論文集, 第14卷, 1號, pp.40-47, 2003. 6
Cheju Nat'l Univ. Res. Inst. Adv. Tech. Jour., Vol.14, No.1, pp.40-47, 2003. 6

주파수 영역 결합변환 상관기를 이용한 광 암호화 시스템

도 양 회* · 박 세 준**

Optical Security System Using the Frequency-domain Joint Transform Correlator

Yang-Hoi Doh* · Se-Joon Park**

ABSTRACT

In this paper an optical encryption system, which can decrypt the original image by using the autocorrelation terms of a JTC, is proposed. Unlike the conventional JTC, the joint input plane of the proposed system is composed in a frequency-domain not a spatial-domain, thus it is sufficient only one Fourier transformation operation. An original image is encrypted to a complex-valued random image and the original image is reconstructed by using the autocorrelation terms which is the main drawback of conventional JTC. Therefore the proposed system is more suitable for JTC and real time processing. Computer simulations and optical experiments show that the proposed system is very useful for a JTC architecture.

Key Words : Encryption, Decryption, Phase modulation, JTC

Ⅰ. 서 론

영상신호처리 장비들은 대개 영상신호의 밝고 어두움 즉 세기를 검출해서 대량 복제나 위조를 가능하게 한다. 이를 예방하는 기술로 영상신호처리에 사용되는 여러 가지 방법[1]과 홀로그램 등이 응용되고 있으나 이러한 방법들은 궁극적으로 세기검출기(intensity detector)에 의한 복제 가능성에서 벗어날 수 없는 실정이다. 광신호처리를 이용한 보안 시스템[2-4]에서는 무작위 위상을 발생시켜 원래 영상을 암호화한 후 위상 마스크, 컴퓨터 형성 홀로그램(CGH: computer generated hologram) 또는 공간광변조기(SLM: spatial light modulator)에 기록을 한다. 이렇게 기록되어진 암호화 영상은 기존의 세기 검출기로는 추출이 불가능하므로 복제나 위조가 어렵고, 무작위 특성에 의해서 원래의 패턴을 역추적하기 어렵다는 장점이 있다.

현재 사용되는 광 보안 시스템 중에서 결합변환상관기(JTC: joint transform correlator)[5]는 광축정렬이 필요없고 복소공액 마스크를 제작할 필요가 없으며 외부교란에도 거의 영향을 받지 않는 장점이 있다. 또한 JTC는 현재 널리 사용되는 디지털 장비와

* 제주대학교 전기전자공학부, 첨단기술연구소
Department of Electrical & Electronic Eng., Cheju Nat'l Univ., Res. Inst. of Adv. Tech.
** 구미1대학 전자정보과
Department of Electronics Information, Kumi 1 College.

직접적인 결합을 통하여 실시간 처리에도 적합하다는 장점을 가진다. 그러나 JTC는 그 구조적인 특성 때문에 출력 평면에 큰 세기의 자기상관 성분이 나타나는데, 이는 JTC를 광 상관 시스템이나 광 보안 시스템에 이용하기 어렵게 만드는 주원인이 된다.

본 논문에서는 JTC의 문제점인 자기상관성분을 이용하여 원 영상을 재생하며 전통적인 JTC[6]와는 달리 결합입력평면을 주파수영역으로 사용하는 광 암호화 시스템을 제안하였다. 암호화 방법[7]은 이진영상을 위상변조 시키고 무작위 위상영상과 곱한 후 푸리에 변환하여 원 영상을 수치적으로 암호화하며, 암호화에 사용된 무작위 위상영상의 푸리에 변환된 영상을 진위 여부를 판별하는 키 코드로 사용한다. 이렇게 암호화된 영상은 두번의 암호화 과정을 거치므로 쉽게 역 추적되기 어려우며 복소함수 값을 가지므로 세기검출기로는 복사가 불가능하다는 광 보안 시스템의 장점을 그대로 이용할 수 있다. 또한 JTC로 재생되는 영상은 가장 큰 문제로 작용하는 자기상관성분을 이용하여 재생되므로 실시간 처리에 보다 유리하다. 컴퓨터 모의실험과 광 실험을 통하여 제안한 암호화 방법의 성능을 확인하였다.

II. 전통적인 JTC

결합변환 상관기[6]는 광축정렬 문제를 해결할 수 있는 광 상관 시스템이며 이는 입력영상과 기준영상을 JTC의 결합입력평면에 동시에 두기 때문에 가능하다. 전통적인 JTC의 시스템 블럭도는 Fig. 1과 같다. 여기에서 SLM은 입력영상이 올라가는 결합입력평면(joint input plane)을, 렌즈 L1은 푸리에 변환렌즈를, P1은 출력평면을 나타내며, f 는 렌즈의 촛점거리이다. 그림 1에서 $r(x,y)$는 중심이 $(-x_0,0)$에 배치되는 기준영상이고 $h(x,y)$는 중심이 $(x_0,0)$에 배치되는 입력영상이다. 따라서 결합입력평면은

$$e(x,y) = h(x-x_0,y) + r(x+x_0,y) \qquad (1)$$

로 주어지며, 결합입력평면은 L1에 의해서 푸리에변환되는데 이는

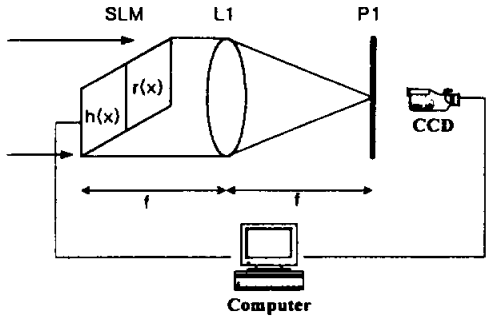


Fig. 1. Conventional JTC

$$E(u,v) = H(u,v)\exp(-j2\pi x_0 u) + R(u,v)\exp(j2\pi x_0 u) \qquad (2)$$

와 같이 표현된다. 출력평면 P1에 놓인 세기 검출기의 광세기 함수는

$$|E(u,v)|^2 = |H(u,v)|^2 + |R(u,v)|^2 + H(u,v)R^*(u,v)\exp(-j4\pi x_0 u) + H^*(u,v)R(u,v)\exp(j4\pi x_0 u) \qquad (3)$$

와 같이 표현된다. CCD로 검출된 광세기 함수는 다시 SLM으로 올려지게 되며, L1에 의해서 푸리에 역변환된다. 이때 출력 상관평면에서의 광분포 함수는

$$g(x,y) = h\star h + r\star r + h\star r * \delta(x+2x_0,y) + r\star h * \delta(x-2x_0,y) \qquad (4)$$

와 같다. 여기서 ★는 상관자(correlation operator)를, *는 상승자(convolution operator)를 뜻한다. 식 (1)에서 결합입력평면에 놓여진 각각의 영상은 공간영역에서 원래에 중심에 대해 $\pm x_0$ 만큼 이동한 결과가 되며 이는 주파수영역에서 식 (2)의 위상성분 $\exp[j2\pi x_0 u]$으로 나타나게 된다. 식 (3)과 식 (4)에서 앞의 두 항은 각각의 입력영상의 자기상관성분이며, 뒤의 두 항은 각 입력영상간의 상호상관 성분이다. 자기상관의 세기는 상호상관의 세기에 비해 아주 크므로 광 상관

시스템에서는 오인식을 유발시키며, 광 암호화 시스템에서는 원 영상의 복원을 어렵게 만든다.

III. 제안한 광 암호화 시스템

3.1. 암호화 방법

본 논문에서 제안한 암호화 시스템은 Fig. 2와 같다. 먼저 암호화 할 이진영상 $f(x,y)$를 위상 변조 시키고, 컴퓨터에서 발생한 이진 무작위 영상 $r(x,y)$을 위상변조한다. 위상변조된 각각의 영상 $f_p(x,y)$, $r_p(x,y)$는

$$f_p(x,y) = \exp[j\pi f(x,y)]$$
$$r_p(x,y) = \exp[j\pi r(x,y)] \quad (5)$$

와 같이 표현된다. 이때 위상 변조된 영상의 세기는 '1' 이므로 $|f_p(x,y)|^2 = |r_p(x,y)|^2 = 1$ 이다. 두 위상변조된 영상을 곱한 암호화 영상을 $h(x,y)$라 두면

$$h(x,y) = f_p(x,y)\, r_p(x,y)$$
$$= \exp[j\pi\{f(x,y) + r(x,y)\}] \quad (6)$$

와 같고 암호화된 영상의 세기도 '1'이 된다. 이때 암호화된 위상영상 $h(x,y)$를 푸리에변환한 복소함수 $H(u,v)$를 최종 암호화된 영상으로 사용하며, 진위를 판별하는 키 코드(key-code)는 위상변조된 무작위 영상 $r_p(x,y)$를 푸리에변환한 $R_p(u,v)$를 사용한다. 이는

$$H(u,v) = \mathcal{F}\{h(x,y)\}$$
$$R_p(u,v) = \mathcal{F}\{r_p(x,y)\} \quad (7)$$

와 같고, 여기서 $\mathcal{F}$는 푸리에변환을 나타낸다.

제안한 방법으로 암호화된 영상은 원 영상을 위상변조한 후 위상변조된 무작위 영상과 곱해진 후 푸리에변환을 하므로 두 번의 암호화 과정을 거친 것과 동일한 결과를 가지게 되며, 암호화에 사용된 키 코드 없이는 원 영상을 복원할 수 없다. 또한 제안한

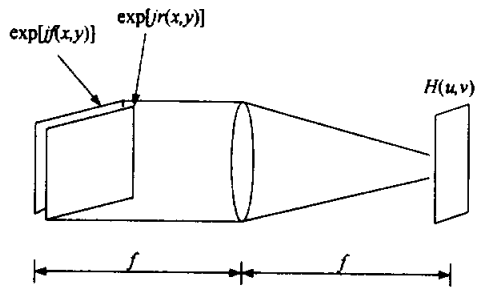


Fig. 2 Proposed encryption system

암호화 방법은 위상마스크를 제작한 후 단순히 푸리에 변환 과정을 통하여 구현이 가능하므로 기존의 4-f 광 상관기 시스템이 가지는 광축정렬이 필요 없으며 외부교란에 거의 영향을 받지 않으며 복소함수 값을 가지므로 세기검출기로 복사되지 않는 광 보안 시스템의 장점을 그대로 가지게 된다.

3.2. JTC를 이용한 복호화

복호화에 사용되는 JTC 시스템 구성도는 Fig. 1과 동일하다. Fig. 1의 결합입력평면의 좌반 평면에는 암호화된 영상 $H(u,v)$를 놓고, 우반평면에는 진위를 판별하는 키 코드 $R_p(u,v)$를 놓는다. 따라서 결합입력평면 $E(u,v)$는

$$E(u,v) = H(u-u_0, v) + R_p(u+u_0, v) \quad (8)$$

과 같다. 결합입력평면은 렌즈 L1에 의해서 푸리에 역변환 되어지며 이는

$$e(x,y) = h(x,y)\exp(j2\pi u_0 x)$$
$$+ r_p(x,y)\exp(-j2\pi u_0 x) \quad (9)$$

로 주어진다. 여기서 $\exp(\pm j2\pi u_0 x)$는 주파수영역에서 중심의 이동에 의해 생기는 출력평면에서의 위상성분이다.

출력평면 P1에 놓인 CCD 카메라에 의해서 검출되어지는 세기함수는

$$
\begin{aligned}
|e(x,y)|^2 &= |h(x,y)|^2 + |r_p(x,y)|^2 \\
&\quad + h(x,y)r_p^*(x,y)\exp(j4\pi u_0 x) \\
&\quad + h^*(x,y)r_p(x,y)\exp(-j4\pi u_0 x) \\
&= 1+1 \\
&\quad + \exp[j\pi f(x,y)]\exp(j4\pi u_0 x) \\
&\quad + \exp[-j\pi f(x,y)]\exp(-j4\pi u_0 x)
\end{aligned} \tag{10}
$$

과 같고 이는 이진 값으로 구성되는 원 영상의 각 화소 값에 따라

$$
e(x,y) = \begin{cases} 2+2\cos(4\pi u_0 x), & \text{if } f(x,y)=0 \\ 2-2\cos(4\pi u_0 x), & \text{if } f(x,y)=1 \end{cases} \tag{11}
$$

과 같이 정리된다. 식 (11)에서 재생된 영상의 세기에 영향을 미치는 u_0는 결합입력평면의 중심에서 입력영상과 기준영상의 각각의 중심의 위치이며 이의 영향이 없다면, 즉 $\cos(4\pi u_0 x) = 1$로 두면

$$
e(x,y) = \begin{cases} 4, & \text{if } f(x,y)=0 \\ 0, & \text{if } f(x,y)=1 \end{cases} \tag{12}
$$

와 같이 나타나게 되어 원래 영상의 명암이 반전된 영상이 나타나게 된다. 식 (10)의 앞의 두 항은 결합입력평면을 구성하는 각 입력 영상의 자기상관 성분이며 뒤의 두 항은 상호상관 성분이다. 식 (10)에서 자기상관 성분이 있어야 원 영상의 재생이 가능하므로 JTC의 가장 큰 어려움인 자기상관 성분을 제거시킬 필요가 없다는 것을 알 수 있다. 따라서 제안한 암호화 방법은 JTC 구조에 보다 적합한 방법이라 할 수 있다. 만약 암호화할 때 원 영상의 명암을 반전시켜 위상변조한 후 암호화 한다면 JTC의 출력평면에 원 영상이 재생된다.

위의 결과는 위상성분의 영향을 배제하였을 경우이나, 실제 재생된 영상은 u_0의 값에 따라 그 세기 값이 변하게 된다. 따라서 u_0의 값에 따라 복원된 영상이 어떤 영향을 받는 지를 분석하여야 하고 그 영향을 제거하는 방법을 찾아야 제안한 암호화 방법이 JTC로 구현될 수 있다.

IV. 실험결과 및 고찰

4.1. 컴퓨터 모의 실험

Fig. 3은 제안한 암호화 방법을 컴퓨터 모의실험하기 위하여 제작된 영상이다. Fig. 3(a)는 암호화될 원 영상이며, Fig. 3(b)는 컴퓨터로 발생된 무작위 영상이며 이를 위상 변조한 후 푸리에 변환한 영상을 키 코드로 사용한다. Fig. 3(c)는 암호화된 영상인데 Fig. 3(a)의 영상을 위상 변조하고 Fig. 3(b)의 무작위 영상을 위상 변조하여 서로 곱한 후 푸리에 변환하여 제작하였다. 그림에서 보듯이 암호화된 영상은 원래의 영상과는 전혀 관계없는 무작위 패턴으로 나타남을 확인할 수 있다. Fig. 3(d)는 거짓 키 코드로 사용되는 무작위 영상이며 이는 암호화에 사용된 키 코드와는 다른 키 코드를 사용하였을 때 영상이 재생되지 않음을 확인하기 위해서 사용하였다. Fig. 3의 모든 영상들은 64×64의 크기를 가진다.

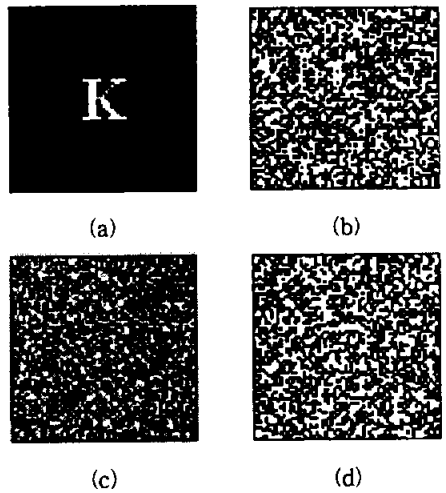
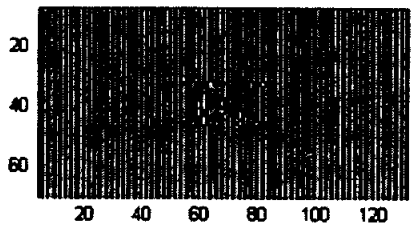
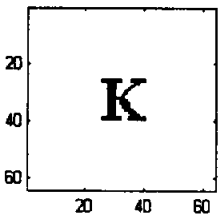


Fig. 3. Used image for computer simulation testing proposed encryption system: (a) original binary image, (b) random binary image used for key code, (c) encrypted data, and (d) another random binary image used for false key code.

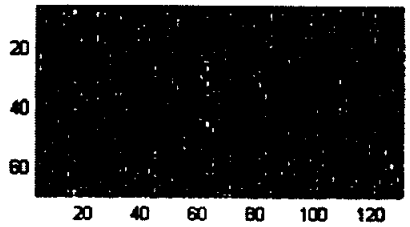
Fig. 4는 JTC의 좌반 평면에 Fig. 3(c)의 암호화된 영상을 놓고, 우반 평면에는 키 코드를 놓아 복원한 영상이다. 키 코드는 암호화에 사용된 Fig. 3(b)의 무작위 영상을 위상 변조시킨 후 푸리에 변환하여 사용하였다. Fig. 4(a)에서 보듯이 재생된 영상은 원래 영상에 비해서 x축 방향으로만 두 배 커져 있으며 위



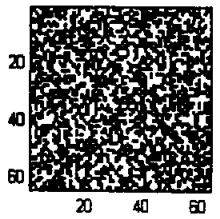
(a)



(b)



(c)



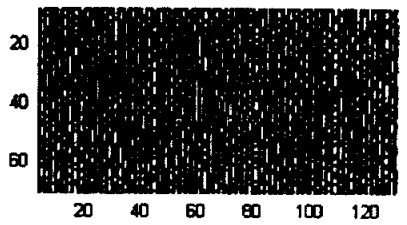
(d)

Fig. 4. Computer simulation results: (a) reconstructed image with correct key code, (b) extracting the even pixels of (a) in x-axis, (c) reconstructed image with false key code, and (d) extracting the even pixels of (c) in x-axis.

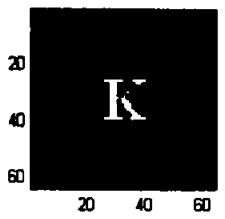
상성분의 영향이 일정하게 나타남을 눈으로 확인할 수 있다. Fig. 4(b)는 Fig. 4(a) 영상의 x축의 짝수화소만 추출한 영상이다. 원래의 영상이 같은 크기로 명암이 반전되어 재생됨을 확인할 수 있다. Fig. 4(c)는 결합 입력평면의 우반 평면에 Fig. 4(d)의 거짓 키 코드를 두고 재생 영상이며, Fig. 4(d)는 Fig. 4(c)에서 짝수 화소만 추출한 영상이다. 명확하게 거짓 키 코드로는 원래의 영상을 복원할 수 없음을 확인할 수 있다. 따라서 본 논문에서 제안한 암호화 방법의 성능을 확인할 수 있다.

Fig. 5(a)는 Fig. 3(a)의 원 영상의 명암을 반전시킨 후 이를 위상 변조시키고 Fig. 3(b)의 영상을 키 코드로 이용하여 암호화 한 영상을 JTC의 결합 입력평면에 두고 재생한 영상이다. Fig. 5(b)는 Fig. 5 (a)의 영상에서 x축의 짝수 화소만 추출한 영상이다. 명암을 반전시킨 영상을 위상변조하여 암호화하면 원래의 영상이 재생됨을 확인할 수 있다.

Fig. 6은 여러 개의 문자를 가지며 화소수가 증가한 입력영상에 대해 컴퓨터 모의 실험한 것이다. Fig. 6(a)는 암호화에 사용된 원 영상이며, Fig. 6(b)는 키 코드로 사용된 무작위 이진영상이다. Fig. 6(c)는 키



(a)



(b)

Fig. 5. Computer simulation results: (a) reconstructed image when using the negative image of Fig. 3(a) as the encrypted data and (b) extracting the even pixel of (a) in x-axis.

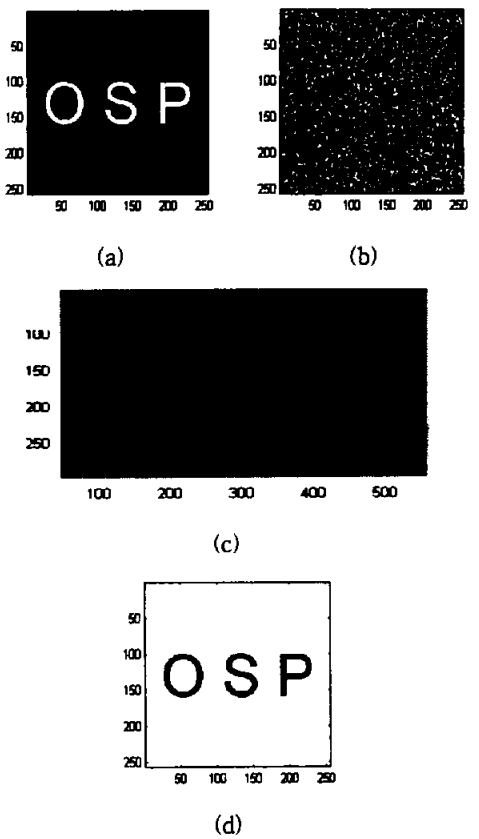


Fig. 6. Computer simulation results: (a) original image, (b) key code, (c) reconstructed image, and (d) extracting the even pixels of (c) in x-axis.

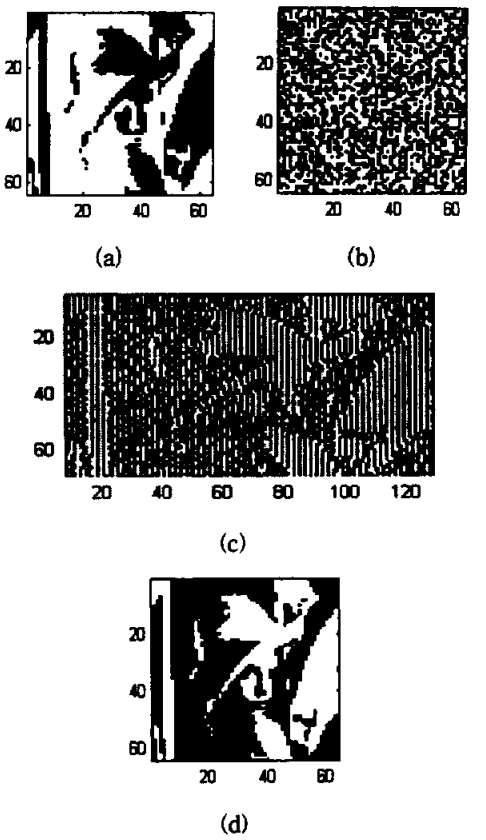


Fig. 7. Computer simulation results: (a) original image, (b) key code, (c) reconstructed image, and (d) extracting the even pixels of (c) in x-axis.

코드로 재생된 영상이다. 역시 분석과 동일한 결과를 가진다는 것을 확인할 수 있다. Fig. 6(d)는 Fig. 6(c)의 영상에서 짝수 화소만 추출한 영상이다.

원래 영상의 명암이 반전되어 나타나고 원 영상의 크기와 같다는 것을 확인할 수 있다. 제안한 방법이 화소수가 증가한 영상인 경우에도 위상성분의 영향을 받는 화소는 동일한 짝수화소임을 알 수 있으며 여러 문자를 가지는 입력영상인 경우에도 동일하게 적용이 가능함을 확인할 수 있다.

Fg. 7은 Lena 영상을 이진화 후 제안한 암호화 방법을 모의실험 하였다. Fig. 7(a)는 이진화된 레나 영상을 명암 반전시킨 영상이며 이 영상을 위상 변조하여 암호화하였다. Fig. 7(b)는 암호화에 사용된 키 코드 영상이다. Fig. 7(c)는 키 코드로 재생된 영상이다. 역시 분석과 동일한 결과를 가진다는 것을 확인할 수 있다. Fig. 7(d)는 Fig. 7(c)의 영상에서 짝수 화소만 추출한 영상이다. 원래 영상의 명암이 반전되어 나타나고 원 영상의 크기와 같다는 것을 확인할 수 있다. 따라서 제안한 방법은 일반적인 영상에도 적용이 가능하고, 명암도 영상의 경우 적절한 문턱치(threshold) 값을 통하여 이진화 하여 사용 가능함을 확인할 수 있다.

4.2. 광 실험 및 고찰

제안한 암호화 방법의 광 실험은 앞의 광 실험과 동일하게 이진 위상 CGH를 제작하고 이를 LCD에 올려 구현하였다. Fig. 8은 광 실험한 결과이다. 실험에 사용된 원 영상은 Fig. 3(a) 영상을 사용하였으며 암호화 한 후 제작한 CGH는 Fig. 8(a)와 같고, 키 코드

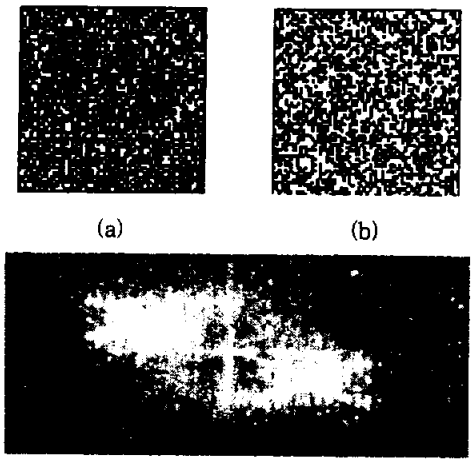


Fig. 8. Optical experiment results: (a) binary phase CGH of encrypted data, (b) binary phase CGH of key code, and (c) decrypted image with the key code.

의 CGH 영상은 Fig. 8(b)와 같다. Fig. 3(b)의 CGH와는 달리 암호화된 영상과 키 마스크가 무작위 패턴이기 때문에 CGH 패턴 자체도 무작위 형태로 나타난다. 두 CGH를 x축으로 다운 샘플링한 후 결합 입력평면에 두고 CCD 카메라로 받은 결과는 Fig. 8(c)와 같다. 원래의 영상이 재생됨을 눈으로 확인할 수 있지만 앞 절의 모의실험과는 달리 정확하게 일치하지 않는다는 것을 볼 수 있다. 앞 절의 위상성분의 영향을 광 실험한 결과에 비해서 암호화 된 영상의 재생 실험이 더 결과가 나쁜 이유는 이진위상 CGH 제작시 양자화 과정에서의 정보손실로 인하여 암호화된 영상에 포함된 키 코드 성분과 CGH로 제작된 키 코드가 정확히 일치하지 않아서 더 많은 정보손실이 발생하여 나타나는 오차로 판단된다. 또한 실험에 사용한 LCD와 CCD 카메라의 해상도 차이에 따른 화소의 부정합도 영향을 미친다고 판단된다. 이는 다중위상을 구현할 수 있는 광 식각 기술의 발전이나 정확한 위상 제어를 할 수 있는 LCD 장비가 개발된다면 보다 나은 실험 결과를 얻을 수 있을 것이라 생각된다.

V. 결 론

본 논문에서는 JTC의 자기상관성분을 이용하여 원 영상을 재생할 수 있는 주파수영역에서의 암호화방법을 제안하였다. 제안한 암호화 과정은 먼저 암호화할 이진영상을 위상변조하고, 무작위 이진패턴을 컴퓨터로 발생시킨 후 위상변조한다. 두 위상변조된 영상을 공간영역에서 곱해서 원 영상을 순수한 위상 값만 가지는 무작위 패턴으로 만든 후 이를 푸리에 변환한 복소함수를 최종 암호화한 영상으로 사용하였다. 이 때 암호화에 사용된 무작위 위상영상의 푸리에 변환된 영상은 진위 여부를 판별하는 키 코드(key code)로 사용된다. 이렇게 암호화된 영상은 두 번의 암호화 과정을 거치므로 쉽게 역 추적되기 어렵고 복소 값을 가지므로 세기검출기로는 복사가 불가능하다는 광 보안 시스템의 장점을 그대로 이용할 수 있다. JTC를 이용하여 암호화된 영상을 복호하면 출력에 나타나는 암호화된 영상과 키 코드 영상은 위상변조된 영상이므로 이들의 자기상관 성분의 세기는 1이 되며 원 영상은 이 자기상관 성분을 이용하여 재생된다. 따라서 JTC의 가장 큰 문제점인 자기상관성분을 제거해야 하는 문제를 해결할 수 있고, 전통적인 JTC와는 달리 푸리에 역변환의 한 가지 과정만 거치므로 실시간 처리에 보다 유리하다

제안한 시스템에서 암호화된 영상은 두 번의 암호화 과정을 거치게 되며 복소함수 값을 가지므로 광 보안 시스템의 장점들을 그대로 가진다. 또한 JTC의 문제요소인 자기상관성분을 이용하여 영상이 재생되므로 JTC 구조에 보다 적합하며 실시간 처리에도 적합하다. 컴퓨터 모의실험과 광 실험을 통하여 제안한 암호화 방법의 성능을 확인하였다.

참고문헌

[1] H. Naor and A. Shamir, "Visual cryptography," *Advanced in Cryptography Eurocrypto '94*, vol. 950, no. 7, pp. 1-12, 1995.

[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier

plane random encoding," *Opt. Letters*, vol. 20, No. 7, pp. 767-769, 1995.

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

[4] J. Y. Kim, S. J. Park, C. S. Kim, J. K. Bae, and S. J. Kim, "Optical image encryption using interferometry-based phase masks," *Electron. Lett.*, vol. 36, no. 10, pp. 874-875, 2000.

[5] C. S. Weaver and J. W. Goodman, "Technique for optically convolving two functions," *Appl. Opt.*, vol. 5, pp. 1248-1249, 1966.

[6] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architectur e," *Opt. Eng.*, Vol. 39, No. 8, pp. 2031-2035, 2000.

[7] 이용대, 박세준, 이하운, 김수중, "세기검출기를 이용한 광 영상 암호화", *전자공학회논문지*, 제39권 SD편, 제3호, 34-40쪽, 2002년 3월.