JTC 구조를 이용한 광학적 영상 암호화 시스템

박세준, 서동환, *이응대, **김종윤, ***김정우, ****이하운, 김수중
경북대학교 전자공학과, *국립과학수사연구소, **경동대학교 정보통신공학부,
*** 동양대학교 전자공학과, **** 동양대학교 정보통신학과
전화 : 053-940-8611 / 핸드폰 : 016-784-0675

An optical encryption system for Joint transform correlator

Se Joon Park, Eung Dae Lee, Dong Hoan Seo, Jong Yun Kim,
Jeong Woo Kim, Ha Woon Lee, Soo Joong Kim
School of Electronic & Electrical Engineering, Kyungpook Natl' University
E-mail : psj@palgong.kyungpook.ac.kr

Abstract

In this paper a binary image encryption technique and decryption system based on a joint transform correlator (JTC) are proposed. In this method, a Fourier transform of the encrypted image is used as the encrypted data and a Fourier transform of the random phase is used as the key code. The original binary image can be reconstructed on a square law device, such as a CCD camera after the joint input is inverse Fourier transformed. The proposed encryption technique does not suffer from strong auto-correlation terms appearing in the output plane. Based on computer simulations, the proposed encryption technique and decoding system were demonstrated as adequate for optical security applications.

I. 서론

정보화 사회의 진전에 따른 여권, 신용카드, 은행카드 등과 같은 개인의 신원을 인증하는 신분증의 사용이 늘어나고 있다. 광신호 처리를 이용한 정보 보호 방법에서는 무작위 위상(phase)을 발생시켜 원래 영상을 암호화 한 후 위상 마스크(phase mask), 컴퓨터 형성 홀로그램(CGH) 또는 SLM(spatial light modulator)에 기록하는데 이는 세기 검출기로는 추출이 불가능하여 복제나 위조가 불가능하며, 무작위 특성에 의해서 원래의 패턴을 역추적하기 어렵다는 장점이 있다.

현재 사용되는 광정보보호 시스템은 주로 4-f 광 상관시스템[1]이나 Mach-Zehnder 간섭계 구조[2]를 이용하고 있으며 이 중 4-f 상관시스템은 광축정렬 문제, 복소 위상마스크 제작등의 어려움이 있으며, 간섭계를 이용한 시스템은 화소대화소 정합의 어려움과 정밀한 실험 setup을 필요로 하며 외부 교란에 많은 영향을 받는다. 이러한 문제점들은 결합 변환 상관기(Joint transform correlator) 구조를 이용하면 해결이 가능하며, 또한 JTC는 현재 널리 사용되는 디지털 장비와 직접적인 결합을 통하여 실시간 처리에도 적합하다는 장점을 가진다. 그러나 JTC 구조는 출력 평면에 항상 큰 세기의 자기상관 성분을 가지는 문제점 때문에 광정보 보호시스템에 적용하기 어렵다[3].

본 논문에서는 새로운 암호화 방법으로 영상을 암호화 하고, 이를 JTC 구조를 이용하여 영상을 재생하는 시스템을 제안하고자 한다. 제안한 암호화 방법을 이용하면 복호화시 JTC 시스템이 가지는 자기상관 성분은 영상 재생에 필요한 신호로 이용되므로 JTC 시스템의 문제점을 해결하고 JTC 시스템이 가지는 장점을 그대로 광정보 보안 시스템에 이용할 수 있다. 컴퓨터 모의 실험을 통하여 제안한 방법의 타당성과 성능을 확인하였다.

II. Conventional JTC system

JTC 시스템은 4-f 상관시스템의 광축정렬문제를 해결하기 위하여 입력평면에 기준영상과 입력영상을 함께 두어 푸리에 변환한 후 제곱법칙 검출기(square-law detector)를 거친 후 물체를 인식하는 시스템이며, 그 시스템 블럭도를 그림 1에 나타내었다. 여기에서 SLM은 입력영상이 올라가는 결합입력평면을, 렌즈 L1은 푸리에 변환렌즈를, P1은 출력평면을 나타내며, f 는 렌즈의 촛점거리이다.

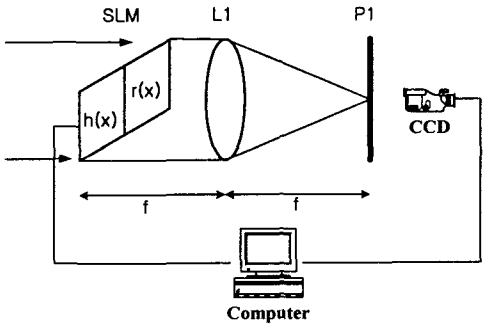

그림 1 결합변환 상관기(JTC)의 구조도

그림 1에서 $r(x+x_0, y)$는 중심이 $(x_0, 0)$에 배치되는 기준영상이고 $s(x-x_0, y)$는 중심이 $(-x_0, 0)$에 배치되는 입력영상이다. 입력평면의 영상들은 L1에 의해서 푸리에 변환되며 이는

$$E(u,v) = S(u,v)e^{-j2\pi x_0 u} + R(u,v)e^{j2\pi x_0 u} \quad (1)$$

와 같이 표현되고, 출력평면 P1에 놓인 square-law 검출기 출력단의 광세기 함수는

$$\begin{aligned} |E(u,v)|^2 &= |S(u,v)|^2 + |R(u,v)|^2 \\ &+ S(u,v)R^*(u,v)e^{-j4\pi x_0 u} \\ &+ S^*(u,v)R(u,v)e^{j4\pi x_0 u} \end{aligned} \quad (2)$$

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

$$\begin{aligned} g(x,y) &= s\star s + r\star r \\ &+ s\star r * \delta(x+2x_0, y) + r\star s * \delta(x-2x_0, y) \end{aligned} \quad (3)$$

와 같다. 여기서 ★는 상관자(correlation operator)를, *는 상승자(convolution operator)를 뜻한다. 식 (3)에서와 같이 출력상관평면의 중심에 입력영상과 기준영상의 자기상관성분이 존재하여 오인식이 유발될 수 있다. JTC를 광정보 보호 시스템에 적용시, 입력영상 s(x,y)가 원래영상 f(x,y) 와 키 위상마스크 r(x,y)로 암호화된 영상이라면

$$\begin{aligned} &s(x,y) = f(x,y) * r(x,y) \\ &\Leftrightarrow S(u,v) = F(u,v)R^*(u,v) \end{aligned} \quad (4)$$

여기서 $R(u,v) = \exp[j\pi(u,v)]$ 로 주어지는 위상함수이다. 암호화된 영상 s(x,y)와 키 위상 마스크 r(x,y)를 결합입력평면에 두게 되면 식 (3)은

$$\begin{aligned} g(x,y) &= s\star s + r\star r \\ &+ f(x,y) * \delta(x+2x_0, y) + f(x,y) * \delta(x-2x_0, y) \end{aligned} \quad (5)$$

로 주어진다. 여기서 전통적인 4-f 시스템에서 복원시 복소공액 키 마스크를 사용하는 것과는 달리 원래의 키 마스크로 원 영상이 출력평면에 대칭적으로 나옴을 알 수 있어 복소 공액마스크의 제작이 필요 없음을 알 수 있다. 그러나 중앙에 나타나는 두 입력영상의 자기상관성분 때문에 원래의 영상을 복원하기는 어렵다.

III. 제안한 암호화 방법과 영상재생

2.1 암호화 방법

본 논문에서 제안한 암호화 방법은 다음과 같다. 먼저 원래의 이진영상을 위상 변조 시키고, 컴퓨터에서 발생한 이진 무작위 영상을 위상변조 시킨다. 두 위상변조된 영상을 곱하여 암호화 시키면

$$\begin{aligned} &e(x,y) = f_1(x,y)f_2(x,y) \\ &f_1(x,y) = \exp[j\pi f(x,y)],\ f_2(x,y) = \exp[j\pi r(x,y)] \end{aligned} \quad (6)$$

와 같다. 여기서 e(x,y)는 암호화된 위상영상이고, f(x,y)는 원영상이며, r(x,y)는 이진 무작위 영상이다. 각각의 이진영상의 0은 "0" 위상을,1은 "π"위상으로 할당된다. 본 논문에서는 암호화된 위상영상을 푸리에 변환시킨 복소함수 E(u,v)를 최종 암호화된 영상으로 사용하며, 위상변조된 무작위 영상을 푸리에 변환한 R(u,v)를 진위를 판별하는 키 코드로 사용한다.

$$\begin{aligned} &E(u,v) = F\{e(x,y)\}, \\ &R(u,v) = F\{\exp[j\pi r(x,y)]\} \end{aligned} \quad (7)$$

여기서 F 는 푸리에 변환을 나타낸다. 제안한 방법으로 암호화된 영상은 원래 영상을 위상변조 시킨후 위상변조된 무작위 영상과 곱해져 푸리에 변환을 하게되므로 두번의 암호화 과정을 거친것과 동일한 결과를 가지게 되며, 복소 함수 값을 가지므로 세기검출기로 복사 되지 않는 광보안 시스템의 장점을 그대로 가지게 된다.

2.2 JTC를 이용한 암호화된 영상의 복원

제안한 암호화 방법을 이용하여 암호화된 영상은 그림1의 좌반 평면에, 진위를 판별하는 키 코드는 우반

평면에 각각 놓여지며 렌즈 1에 의해서 푸리에 역변환 된다. 이는

$$JTC(u,v) = H(u-u_0,v) + R(u+u_0,v) \Leftrightarrow \quad (8)$$

$$jtc(x,y) = h(x,y)\exp[j2\pi u_0 x] + r(x,y)\exp[-j2\pi u_0 x]$$

로 주어지며 CCD 카메라에 의해서 검출되어지는 영상은

$$\begin{aligned} |jtc(x,y)|^2 &= |h(x,y)|^2 + |r(x,y)|^2 \\ &+ h(x,y)r(x,y)^* e^{j4\pi(u_{0x},y)} + h(x,y)^* r(x,y) e^{-j4\pi(u_0 x,y)} \\ &= 1+1+e^{j\pi f(x,y)} e^{j4\pi(u_0 x,y)} + e^{-j\pi f(x,y)} e^{-j4\pi(u_0 x,y)} \\ &= \begin{cases} 2+2\cos[4\pi(u_0 x,y)], & f(x,y)=0 \\ 2-2\cos[4\pi(u_0 x,y)], & f(x,y)=1 \end{cases} \end{aligned} \quad (9)$$

와 같다. 여기서 위상 성분 cosine 항을 1로 두면 식 (9)는

$$\begin{cases} 4, & f(x,y)=0 \\ 0, & f(x,y)=1 \end{cases} \quad (10)$$

로 주어지며 원래의 영상이 명암이 반전되어 재생됨을 알 수 있다. 식 (9)에서 출력평면에서 원영상 복원을 어렵게 하는 자기 상관 성분이 제안한 암호화 방법에서는 원영상 재생에 필요한 성분이 되므로 JTC 구조에서 가장 큰 문제점인 자기상관성분을 제거해야 하는 문제를 해결 할 수 잇음을 알 수 있다.

위상 성분 cosine 항의 영향을 살펴 보면 주파수 평면에서 이동 $-u_0$ 와 $+u_0$ 의 위치는 JTC 구조의 특성상 입력평면의 1/4, 3/4 지점이 된다. 따라서 식 (9)에서

$$\begin{aligned} \cos[4\pi(u_0 x,y)] &= \cos(\pi x, 4\pi y) \\ &= \begin{cases} -1, & x=2n+1 \\ 1, & x=2n \end{cases} \end{aligned} \quad (11)$$

로 주어지며 n 은 정수이다. 식 (11)에서 위상성분에 영향을 받는 것은 출력평면의 x 축에서 홀수 항이란것을 알 수 있으며 이는 CCD 카메라의 홀수 픽셀이 된다. 따라서 CCD 카메라에 재생된 영상에서 홀수 픽셀을 단순히 제거함으로써 페이즈 영향을 없앨 수 잇으며, 제안한 암호화 방법이 주파수 평면을 이용하므로 원래의 주파수 성분의 크기는 변하지 않지만 u축이 두배로 늘어나게 되고 이는 각 암호화 영상의 주파수 스펙트럼 크기가 줄어든 결과가 되므로 재생 영상의 크기가 두배로 커지는 문제도 동시에 해결한다.

Ⅳ. 모의실험

먼저 전통적인 JTC를 이용하여 모의 실험 하였다. 모의 실험에 사용된 영상은 그림 2의 영문자 K 이며 암호화된 영상은 그림 3과 같다. 각각의 영상은 64×64 크기를 가진다. 암호화된 영상과 암호화에 사용된 키 마스크를 JTC 입력평면에 두고 재생된 영상은 그림 4와 같고 크기는 64×128 이다. 중앙에서 발생하는 자기 상관성분의 세기가 재생영상의 세기보다 훨씬 커므로 원래 영상을 복원할 수 없음을 알 수 있다. 그림 5는 중앙의 자기 상관 성분을 디지탈 적으로 감산 연산을 실행하여 재생한 영상이다. 출력평면에 좌우에 원래 영상이 대칭으로 나옴을 알 수 잇다. 자기 상관 성분을 디지탈로 제거 시키기 위해서는 Cuo 등이 제안한 FS-JTC (frequency selecte-JTC)[4]를 이용하는데 이 방법은 결합 입력평면을 구성하기 전에 각각의 입력 영상을 따로 SLM에 올린후 각각을 푸리에 변환시켜 그 주파수 성분을 CCD 카메라로 획득하여 컴퓨터에 저장해 두어야 한다. 그 후에 결합 입력 평면을 구성한 후 푸리엔 변환을 시키고 그 주파수 성분을 CCD로 획득한 후 컴퓨터에서 기록된 성분들을 빼주게 된다. 이는 실시간 처리를 어렵게 하는 요소이다.

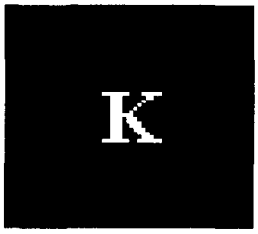

그림 2 원영상

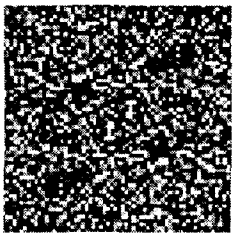

그림 3. 암호화된영상

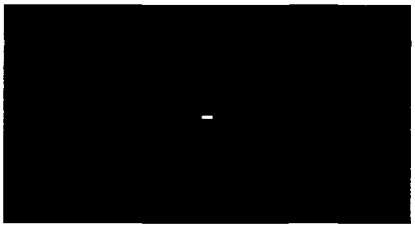

그림 4. 재생영상

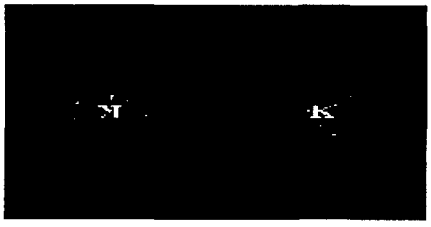

그림 5. 자기상관성분이 제거된 재생영상

제안한 방법에 사용된 원래 영상은 그림 6의 영문자

T 이며, 암호화된 영상은 그림 7과 같다. 각각의 영상은 64×64의 크기를 가지는 이진영상이다. 그림 8은 암호화에 사용된 무작위 영상이며 카드의 진위를 판별하는 키코드영상에 사용되어진다. 그림 9는 키 코드와 다른 무작위 영상을 사용하엿을때 원래 영상이 재생되지 않음을 확인하기 위해서 사용된 또 다른 무작위 영상이다.

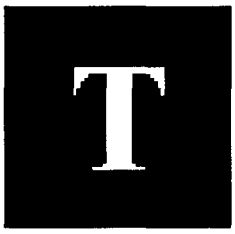

그림 6. 원영상

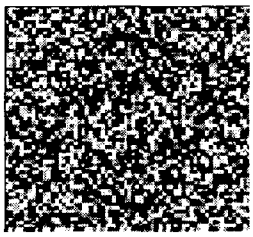

그림 7. 암호화된 영상

그림 8. 키 코드

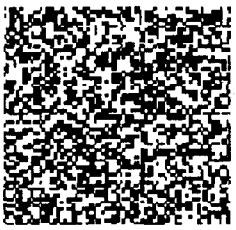

그림 9 거짓키코드

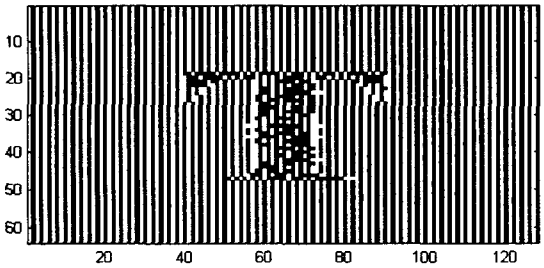

그림 10. 그림8의 키코드를 사용하여 재생한 영상

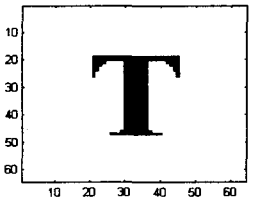

그림 11. 그림 10의 홀수 화소를 제거시킨 영상

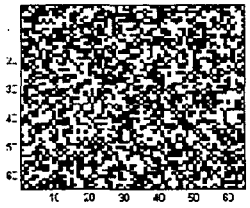

그림 12. 그림 9의 거짓키코드를 이용하여 재생한 후 홀수 화소를 제거 시킨 영상

그림 10은 그림 8의 키 코드를 사용하여 재생한 영상이다. 바탕과 영상안의 검고 힌 줄은 식 (11)의 위상의 영향에 의해서 발생한다는 것을 알 수 있다. 또한 원래 영상의 크기보다 x 축 방향으로 2배 커져 있음을 확인할 수 있다. 그림 11은 그림 10의 영상에서 홀수 픽셀을 제거하여 획득한 영상이며 원래의 영상의 명암이 반전하여 재생됨을 확인할 수 있다. 그림 12는 그림 9의 거짓 키코드를 입력평면에 두어 재생한 후 홀수 픽셀을 제거 시킨 영상이며 원래의 영상이 재생되지 않음을 확인 할 수 있다.

V. 결론

본 논문에서는 JTC 구조에 적합한 암호화 방법을 제안하고 컴퓨터 모의실험을 통하여 그 성능을 확인하였다. 제안한 암호화 방법은 JTC의 자기 상관성분을 영상 재생에 이용함으로써 JTC 구조가 가지는 여러 장점을 최대한 활용할 수 있으며, 또한 현재의 디지털 장비와 결합하여 실시간 처리에 보다 적합하리라 사료되어진다.

참고문헌(또는 Reference)

[1] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.*, vol. 33, No. 6, pp. 1752-1756, 1994.

[2] Jong-Yun Kim, "Optical image encryption using interferometry-based phase masks", *Electronics Letters*, vol. 36, no. 10, pp. 874-875, 2000. 5.

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

[4] C. J. Kuo, "Joint transform correlation improved by means of the frequency selective technique," *Opt. Eng.*, vol. 33, no. 2, pp. 522-527, 1994.