# 원형 편광과 간섭계를 이용한 광 정보 보호 시스템

# Optical Encryption System based on Circular Polarization and Interferometer

조규보, 배효욱, 신창목, 서동환, 김수중
경북대학교 전자공학과
ckb10040@hanmail.net

We proposed an optical encryption system using circular polarization based on interferometer. The phase modulated input image, represented as orthogonal linearly polarized states respectively, is encrypted into circularly polarized states using polarization modulated masks. In the decryption we use the inverse matrix of polarization modulation mask and can recover the original polarization states.

현대 사회에서 개인의 신용 정보가 포함된 신분증의 사용이 늘어나면서 컴퓨터와 관련장비들도 급격히 발달하여 복제와 위조가 쉽게 일어나므로 이를 방지하기 위해 복사기나 스캐너 같은 기존의 광세기 검출기로는 복제 할 수 없는 복소 함수 형태의 패턴을 사용하는 광학적 보안 시스템[1] 및 위상만으로 영상을 암호화하는 기법[2]과 편광을 이용한 방법[3] 등이 연구되고 있다. 본 논문에서는 Mach-Zender 간섭계의 각각의 경로에 서로 직교하는 선형 편광파를 입사시키고 한 경로에 위상 변조된 이진 입력 영상을 두어 간섭에 의해 생기는 합성파가 45°혹은 -45°선형 편광 된 파로 표현이 되며 이를 원형편광 변조 마스크에 투사하여 원형 편광 상태로 암호화 시켜서 간섭 잡음에 민감하지 않고, 세기 검출기로도 영상의 정보를 알 수 없는 암호화 및 복호화 방법을 제안하였다. Mach-Zender 간섭계의 두 경로에 각각 수직, 수평으로 편광 된 파를 입사시키고, 한 쪽 경로에 0과 $\pi$로 위상 변조된 이진 입력 영상을 위치시킴으로써 생기는 위상 지연에 의해 두 직교 편광 된 파의 합은 입력 영상의 값에 의해 45°혹은 -45° 선형 편광 상태가 된다. 이진 입력 영상을 $f(x,y)$, 두 경로에서 각 파 성분의 전장을 $E_0$, 45°및 -45°선형 편광 된 합성파 $p(x,y)$을 존스 행렬로 각각 표시하면 다음과 같다.

$$p(x,y) = E_0\begin{bmatrix} 0 \\ \exp[i\pi\{f(x,y)\}] \end{bmatrix} + E_0\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$= E_0\begin{bmatrix} 1 \\ \exp[i\pi\{f(x,y)\}] \end{bmatrix} \quad (1)$$

암호화 키로 사용되는 원형 편광 변조 마스크는 $\pi/2$ 위상 지연기가 45°편광 된 파를 왼손 원형 편광 상태로, -45°편광 된 파를 오른손 원형 편광 상태로 바꾸어 주고 $-\pi/2$ 위상 지연기가 45°편광 된 파를 오른손 원형 편광 상태로, -45°편광 된 파를 왼손 원형 편광 상태로 바꾸어 주는 특성을 이용하여 제작한다. $\pi/2$ 위상 지연기의 존스 행렬을 $Q$, $-\pi/2$ 위상 지연기의 존스 행렬을 $T$, 원형 편광 변조 키의 변조 함수를 $M(x,y)$라고 각각 표현하면 다음 식이 성립된다.

$$M(x,y) = \text{random}[Q,T] \tag{2}$$

여기에서 $Q=\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix}$, $T=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$이다. 위와 같은 $M(x,y)$을 통과하게 되면 각 화소가 무작위로 왼손 혹은 오른손으로 편광 된 상태의 암호화 영상을 얻을 수 있게 된다. 선형 편광 된 합성파의 존스 벡터를 $p\blacksquare(x,y)$, 암호화 영상을 $e(x,y)$라 하면 암호화 영상은 다음 식으로 얻어지게 된다.

$$e(x,y) = M(x,y)p_{1\text{ or }2}(x,y) \tag{3}$$

여기서 $p\blacksquare_1(x,y)$과 $p_2\blacksquare(x,y)$는 각각 정규화된 45°와 -45°선형 편광의 존스 행렬을 나타낸다. 제안한 복호 영상의 편광 표현은 암호화 편광 변조함수의 역함수를 이용해서 간단히 얻을 수 있다. 이 때 $Q$와 $T$는 식(4)를 만족하므로 서로 역함수 관계가 성립되어 암호화 변조 함수가 $Q$이면 복호화 변조 함수는 $T$로, 암호화 변조 함수가 $T$이면, 복호화 변조함수가 $Q$가 되게 제작한다. 식(5)는 복호화 된 직교 편광성분을 나타낸다.

$$QT=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \tag{4}$$

$$p_{1\text{ or }2}(x,y) = M(x,y)^{-1}e(x,y) \tag{5}$$

복호화 영상은 암호화 된 영상을 복호화 선형 변조 마스크에 통과시키면 이진 입력 영상의 명도 값에 따라 45° 혹은 -45°로 편광 된 두 선형 편광으로 나타나며 두 선형 편광 중에서 영상의 정보를 가지고 있는 광(여기서는 -45°편광된 광에 정보를 포함시켰음)을 검광기에 투과시켜서 광세기 검출기로 세기 형태의 원영상으로 복구 할 수 있다. 세기 검출기를 통해서 복원된 영상의 식은 다음과 같다.

$$\begin{aligned} I(x,y) &= \left| E_0\left[\frac{1}{\exp[i\pi f(x,y)]}\right][1,-1]\right|^2 = |E_0(1-\exp i\pi f(x,y))|^2 \\ &= \begin{cases} 0, & f(x,y)=0 \\ 4{E_0}^2, & f(x,y)=1 \end{cases} \end{aligned} \tag{6}$$

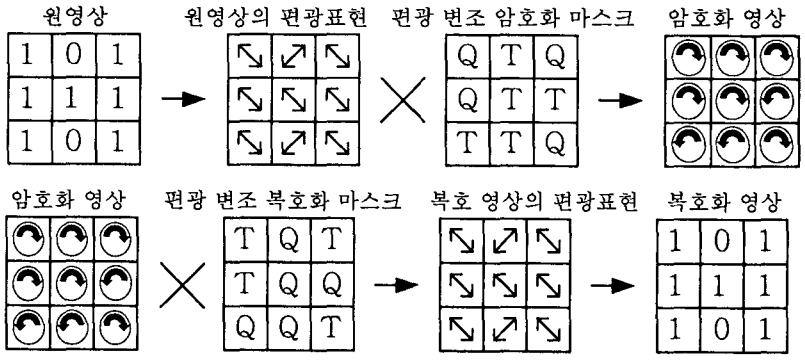


그림 1. 암호화/복호화 알고리즘

참고문헌

[1] J. Y. Kim, S. J. Park, C. S. Kim, J. K. Bae, S. J. Kim "Optical image encryption using interferometry-based phase mask", Electronics Lett., vol. 36, no. 10, 874-875, 2000.

[2] P. Stepien, R. Gajda, and T. Spoplik, "Distributed kinoforms in optical security application", Opt. Eng., vol. 35, no. 9, 2453-2458, 1996.

[3] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, "Secure optical memory with polarization encryption", Applied Optics, vol. 40, no. 14, 2310-2314, 2001.