디지털망에서의 4-step 위상 천이 간섭계를 이용한 이진 데이터의 쌍방향 광 암호화 및 전송

Bi-directional encryption and transmission of binary data with 4-step phase-shifting interferometry in digital network

이현진, 길상근, 전석희*, 김남**
수원대학교 전자공학과, *인천대학교 전자공학과, **충북대학교 정보통신공학부
leehj@suwon.ac.kr

We present a new binary data encryption and transmission technique based on 4-step phase-shifting interferometry for a security system. Phase-shifting interferometry is used for recording phase and amplitude information on CCD device. 4-step phase-shifting is implemented by moving the PZT mirror with equidistant phase steps of $\pi/2$. The basic idea is that we reuse a 256 gray-level digital hologram to encrypt binary data with 4-step phase-shifting interferometry.

인터넷, LAN, 무선통신 같은 통신망이 발전하면서 보안의 중요성이 커지고 있으나 통신망의 개방성과 보안 장치의 결점 때문에 ID와 password 같은 중요한 개인정보가 누출될 위험이 있다. 본 논문에서는 위상 천이 디지털 간섭계를 이용하여 이진 데이터를 광학적으로 암호화하는 기법을 소개하고, 디지털 통신망에서 연속적인 암호화/전송/복호화 과정을 제안한다.

이진 데이터에 랜덤 위상을 준 함수 $f(x,y)$를 입력으로 하고, 이를 푸리에 변환한 값을 $F(\alpha,\beta)$라 한다. $G(\alpha,\beta)$는 데이터를 복원할 때 이용할 암호키 함수 $g(x,y)$를 푸리에 변환한 것이다. $G(\alpha,\beta)$를 PZT 거울로 $\pi/2$씩 위상을 이동하여 $F(\alpha,\beta)$와의 간섭무늬 디지털 홀로그램을 4개 얻고, 얻어진 4개의 디지털 홀로그램으로부터 $F(\alpha,\beta)$와 $G(\alpha,\beta)$의 위상차와 크기 곱을 구한다.[1]

$$I_i(\alpha,\beta) = |F(\alpha,\beta)|^2 + |G(\alpha,\beta)|^2 + 2\sqrt{F(\alpha,\beta)G(\alpha,\beta)}\cos(\Delta\phi_{FG} + \phi_i) \tag{1}$$

여기서, i=1, 2, 3, 4에 대해서 각각 ϕ_i=0, $\pi/2$, π, $3\pi/2$이다.

$$\Delta\phi_{FG} = \phi_F - \phi_G = \tan^{-1}\frac{I_2 - I_4}{I_1 - I_3}, \qquad A_{FG} = |F(\alpha,\beta)||G(\alpha,\beta)| = \frac{1}{4}\sqrt{(I_1 - I_3)^2 + (I_2 - I_4)^2} \tag{2}$$

식 (2)의 값으로부터 복소 홀로그램을 표현하면 $H(\alpha,\beta) = A_{FG}e^{j\Delta\phi_{FG}}$이다. 이미 알고 있는 암호키 함수 $G(\alpha,\beta)$를 이용하여 다음과 같이 $f(x,y)$를 복원할 수 있다.

$$D(\alpha,\beta) = \frac{H(\alpha,\beta)G(\alpha,\beta)}{|G(\alpha,\beta|^2} = |F(\alpha,\beta)|e^{j\phi_F}, \qquad F^{-1}\{D(\alpha,\beta)\} = f(x,y) \tag{3}$$

그림 1은 본 논문에서 제안한 이진 데이터의 쌍방향 광 암호화 및 전송 시스템을 보여준다. 제안한 방법은 처음에 사용자A가 이진 데이터와 암호키로 4-step 위상 천이 디지털 홀로그램을 만들어 사용자B에 전송을 한다. 사용자B는 알고 있는 암호키로 이진 데이터를 복원한다. 사용자B가 다른 암호키를 사용자A에게 보내려 한다면 새로운 암호키 데이터와 처음에 전송된 디지털 홀로그램을 각각 물체광과 참조광으로 하고, 4-step 위상 천이 간섭계를 이용하여 암호키를 암호화하여 사용자A에 전송한다. 사용자A는 처음에 보낸 암호화된 디지털 홀로그램을 이용하여 사용자B가 전송한 암호키를 복원할 수 있게 된다. 자신이 전송한 암호화된 디지털 홀로그램을 반복하여 이용하면서 연속적인 데이터 암호화/전송/복호화를 가능하게 한다.

그림 2는 역 전송 되는 새로운 암호키와 수신된 암호화된 첫 번째 디지털 홀로그램을 보여주고, 그림 3은 디지털 홀로그램이 일치할 때와 일치하지 않을 때 복원된 암호키와 threshold하여 복원된 암호키의 컴퓨터 시뮬레이션 결과를 보여준다.

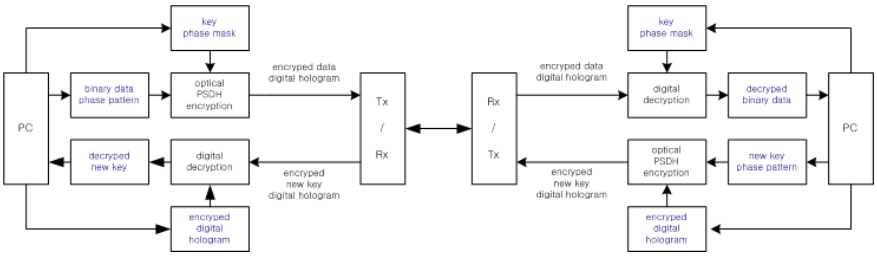
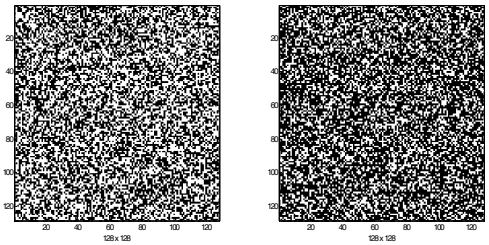
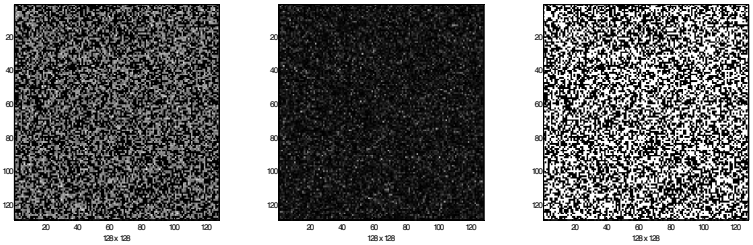


그림 1. 디지털 통신망에서의 이진 데이터의 쌍방향 광 암호화 및 전송 시스템



(a) (b)

그림 2. (a) 랜덤 생성한 새로운 암호키: 물체광, (b) 암호화되어 수신된 첫 번째 디지털 홀로그램: 참조광



(a) (b) (c)

그림 3. 컴퓨터 시뮬레이션 결과 : (a) 암호화된 디지털 홀로그램에 의해 복원된 암호키, (b) 디지털 홀로그램이 일치하지 않을 때 복원된 암호키, (c) thresholding 한 후 복원된 암호키의 원 이진 데이터

참고문헌

[1] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry", Appl. Opt., vol. 39, pp. 2313-2320, 2000.

[2] B. Javidi and T. Nomura, "Securing information by means of digital holography", Opt. Lett., vol. 25, pp. 28-30, 2000.

[3] 길상근, 이현진, 변현중, “위상천이 디지털 홀로그래피를 이용한 정보 암호화와 복호화”, 한국광학회 2005년도 하계학술발표대회, 7월(2005).

*본 연구는 한국과학재단 목적기초연구(R01-2003-000-10528-0(2005)) 지원으로 수행되었습니다.