2-step 위상 천이 디지털 간섭계를 이용한 이진 데이터 암호화 및 복호화

Encryption and decryption of binary data with 2-step phase-shifting digital interferometry

변현중, 길상근, 하승호*
수원대학교 전자공학과, *수원대학교 TIC
hjbyun@suwon.ac.kr

We propose a method of encryption and decryption of binary data using 2-step phase-shifting digital interferometry. This technique reduces the number of interferograms in the phase-shifting interferometry. The binary data has been expressed with random code and random phase. We remove the dc-term of the phase-shifting digital interferogram to restore the original binary data. Simulation results shows that the proposed technique can be used for binary data encryption and decryption.

정보통신기술의 발달로 초고속 대용량 데이터 전송 시스템이 중요시되지만 그에 못지않게 데이터의 정보보안 역시 중요한 요소이다. 여러 정보보안 시스템이 있지만 본 논문에서는 위상 천이 디지털 간섭계를 이용한 광학적 정보 암호화와 컴퓨터 처리에 의한 복호화를 기술한다. 디지털 홀로그램을 얻는 방법은 여러 가지가 있지만 원 정보의 위상과 크기를 모두 알 수 있는 4-step 위상 천이 디지털 간섭계가 대표적이다. 본 논문에서는 4-step 위상 천이 디지털 간섭계를 이용한 것보다 간섭무늬의 획득 수를 줄일 수 있는 2-step 위상 천이 디지털 간섭계 이용한 이진 데이터 암호화 및 복호화 방법을 제안한다.

이진 데이타의 정보 $s(x,y)$를 푸리에 변환한 것을 $S(\alpha,\beta)$라 하고, $R(\alpha,\beta)$는 데이터를 복원할 때 이용할 암호키 함수 $r(x,y)$를 푸리에 변환한 것이라 할 때, CCD로 받은 두 개의 위상천이 간섭무늬 디지털 홀로그램 식은 다음과 같다.

$$I_1(\alpha,\beta) = |S(\alpha,\beta)|^2 + |R(\alpha,\beta)|^2 + 2\sqrt{|S(\alpha,\beta)||R(\alpha,\beta)|}\cos\Delta\phi \quad (1)$$

$$I_2(\alpha,\beta) = |S(\alpha,\beta)|^2 + |R(\alpha,\beta)|^2 + 2\sqrt{|S(\alpha,\beta)||R(\alpha,\beta)|}\cos(\Delta\phi + \frac{\pi}{2})$$

여기서 $\Delta\phi = \phi_S - \phi_R$ 로 물체광 $S(\alpha,\beta)$와 참조광 $R(\alpha,\beta)$의 위상차를 나타낸다.

식 (1)에서 $A(\alpha,\beta) = |S(\alpha,\beta)|^2 + |R(\alpha,\beta)|^2$, $B(\alpha,\beta) = 2\sqrt{|S(\alpha,\beta)||R(\alpha,\beta)|}$라 하고, dc-term인 $A(\alpha,\beta)$를 제거 한 후 다시 쓰면,

$$I_1' = I_1 - A(\alpha,\beta) = B(\alpha,\beta)\cos\Delta\phi, \qquad I_2' = I_2 - A(\alpha,\beta) = B(\alpha,\beta)\cos(\Delta\phi + \frac{\pi}{2}) \quad (2)$$

이다. 식 (2)로부터 복소 홀로그램 $H_1(\alpha,\beta)$의 위상과 크기는 다음과 같이 구해진다.

$$\Delta\phi = \phi_S - \phi_R = \tan^{-1}\left(\frac{I_2'}{I_1'}\right), \quad |S(\alpha,\beta)||R(\alpha,\beta)| = \frac{1}{2}\sqrt{(I_1')^2 + (I_2')^2} \quad (3)$$

원 이진 데이터는 복소 홀로그램 $H_1(\alpha,\beta)$과 암호키 함수 $R(\alpha,\beta)$를 이용하여 복원할 수 있다.

$$D(\alpha,\beta) = \frac{H_1(\alpha,\beta)R(\alpha,\beta)}{|R(\alpha,\beta)|^2} = \frac{|S(\alpha,\beta)||R(\alpha,\beta)|e^{j(\phi_S-\phi_R)}|R(\alpha,\beta)|e^{j(\phi_R)}}{|R(\alpha,\beta)|^2} = |S(\alpha,\beta)|e^{j\phi_S} \quad (4)$$

$$F^{-1}[D(\alpha,\beta)] = F^{-1}[S(\alpha,\beta)] = s(x,y) \quad (5)$$

그림 1은 마흐-젠더 간섭계를 기본으로 하는 위상천이 디지털 홀로그래피 장치이다.
그림 2는 128×128 화소로 랜덤 생성한 이진 데이터와 랜덤 생성한 암호키를 보여주고 있고, 그림 3과 4는 dc-term을 제거 안한 경우와 제거한 경우의 원 데이터의 복원상태를 보여준다.

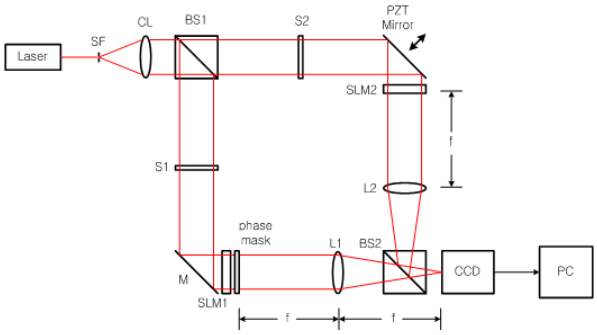
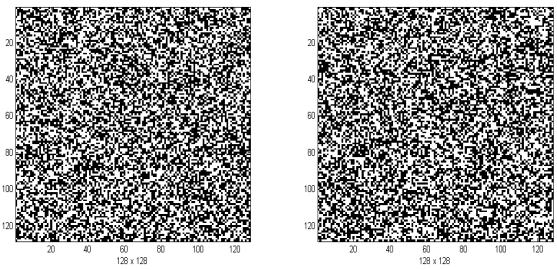
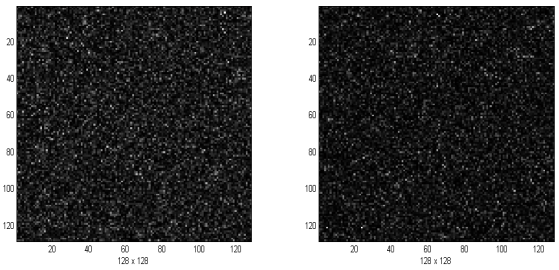


그림 1. 마흐-젠더 간섭계를 기본으로 하는 위상천이 디지털 홀로그래피 장치



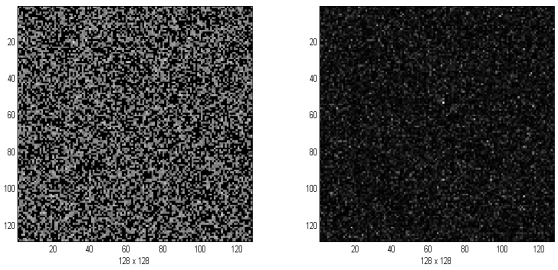
(a) (b)

그림 2. (a) 랜덤 생성한 이진 데이터
(b) 랜덤 생성한 암호키



(a) (b)

그림 3. dc-term을 제거하지 않고
(a) 암호키가 일치하는 경우
(b) 암호키가 일치하지 않은 경우



(a) (b)

그림 4. dc-term을 제거하고
(a) 암호키가 일치하는 경우
(b) 암호키가 일치하지 않은 경우

참고문헌

[1] B. Javidi, T. Nomura, “Securing information by use of digital holography”, Opt. Lett. 25, No.1, Jan.(2000).

[2] T. Tajahuerce, O. Matoba, S. Verral, B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry, Appl Opt. 39(14), 2000

[3] 길상근, 이현진, 변현중, “2-steps 위상천이 간섭기법을 이용한 정보 암호화”, 한국광학회 2005년도 광정보처리분과 워크샵.

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