랜덤 위상 키와 Fresnel 전파를 이용한 디지털 홀로그램의 암호화

Encryption of Digital Hologram by Random phase key and Fresnel propagation

김도형*, 김 현, 문인규, 이연호
성균관대학교 정보통신공학부
hyuney92@skku.edu

최근의 초고속 광대역 통신망 및 인터넷의 발달은 대용량의 정보를 매우 빠른 시간에 전송 및 수신하도록 하여준다. 그러나 컴퓨터의 발달로 인하여 이러한 정보에 대한 불법 복제 및 악용이 그 어느 때보다 손쉽게 이루어 질 수 있으므로 정보 보안에 대한 관심이 매우 높아지고 있다. 특별히 광학 분야에서 디지털 홀로그래피를 이용한 2차원 혹은 3차원 정보의 암호화[1,2], 그리고 컴퓨터상에서 가상의 광학 이미징 시스템을 이용한 디지털 정보의 암호화[3,4] 등이 최근에 보고됐다.

본 논문에서는 랜덤 위상 키와 Fresnel 전파를 이용한 디지털 홀로그램의 새로운 암호화 기법을 제안한다. 실험적으로 구한 디지털 홀로그램 그 자체는 암호화 돼 있다고 볼 수 없다. 왜냐하면 기록시 사용된 파장, 2차원 혹은 3차원 정보가 위치했던 거리, 그리고 기록 매체인 CCD의 픽셀 개수와 픽셀 크기를 정확히 모르더라도 컴퓨터 상에서 여러번의 시행 착오를 거치면 디지털 홀로그램으로부터 원래 정보를 추출하는 것이 충분히 가능하기 때문이다. 따라서 본 논문에서는 그림 1에서 보듯이 랜덤 위상 키 $\exp(j\phi_k(x, y))$ 를 원래의 디지털 홀로그램 $U_H(x, y)$에 부착시킨 후 임의의 거리 d_e 만큼 Fresnel 전파를 시킴으로써 디지털 홀로그램 그 자체를 암호화시키게 된다. 이 경우 새로운 홀로그램 평면 (x_e, y_e)에서 얻게 되는 field $U_e(x_e, y_e)$는 다음과 같이 주어진다.

$$U_e(x_e, y_e) = \frac{exp(j2\pi d_e/\lambda)}{j\lambda d_e}\exp\left(j\frac{\pi}{\lambda d_e}(x_e^2 + y_e^2)\right)\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} U_H(x, y)exp(j\phi_k(x, y)) \times \exp\left(j\frac{\pi}{\lambda d_e}(x^2 + y^2)\right)\exp\left(-j\frac{2\pi}{\lambda d_e}(xx_e + yy_e)\right)dx\,dy$$

여기서 적분 기호 밖의 상수 항 $\exp(j2\pi d_e) / j\lambda d_e$ 은 일반적으로 무시할 수 있다. 이러한 Fresnel 회절 적분식은 대개 컴퓨터 상에서 FFT(Fast Fourier Transform) 알고리듬을 이용해 2차원 discrete Fourier transform을 함으로써 계산되어진다. 이와 같은 방법으로 새로이 얻은 디지털 홀로그램은 부착된 랜덤 위상 키로 인해 전파 거리에 상관없이 백색 잡음(white noise) 형태로 나타나게 된다.

그림 2는 새로이 제안된 디지털 홀로그램 암호화 기법에서 복호화 과정을 나타낸다. 새로이 제안된 암호화 기법에서는 암호화 과정에서 쓰인 Fresnel 전파 거리 d_e 와 CCD 평면 (x, y)에서 랜덤 위상 키의 정확한 정보를 아는 사람만이 암호화된 디지털 홀로그램으로부터 두 번의 역 Fresnel 전파와 랜덤 위상 키의 복호화 과정을 거쳐 원래의 정보를 정확히 추출할 수 있을 것이다. 실험에서 사용된 디지털 홀로그램은 대표적인 4단계 위상 천이 디지털 홀로그래피로부터 구해졌으며 사용된 3차원 물체의 크기는 3.5cm × 7.0 cm × 3.0 cm, CCD로부터 물체까지의 거리 d_o는 250cm, 그리고 파장 λ 는 514.5nm 였다. 또한 실험에서 사용된 CCD의 픽셀 개수는 640 × 480, 픽셀 크기는 8.4μm × 9.8μm 였다. 그리고 암호화를 위한 Fresnel 전파 거리 d_e 는 100cm로 선택했고

랜덤 위상 키는 구간 [0, 1] 에서 균일한 분포를 갖는 랜덤 숫자 발생기로부터 생성되어졌다.

그림 3은 실험 결과를 보여준다. 암호화된 홀로그램은 백색 잡음 형태였으며 정확한 거리 정보 및 랜덤 위상 키 정보를 알고 있는 경우에만 원래의 정보를 복원할 수 있다는 것이 실험에서 보여졌다.

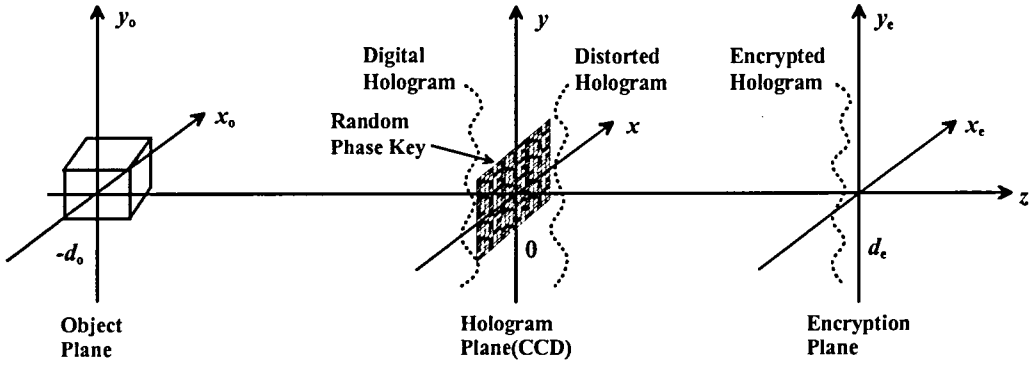


그림 1. 랜덤 위상 키와 Fresnel 전파를 이용한 디지털 홀로그램의 암호화 과정을 설명하는 구조도.

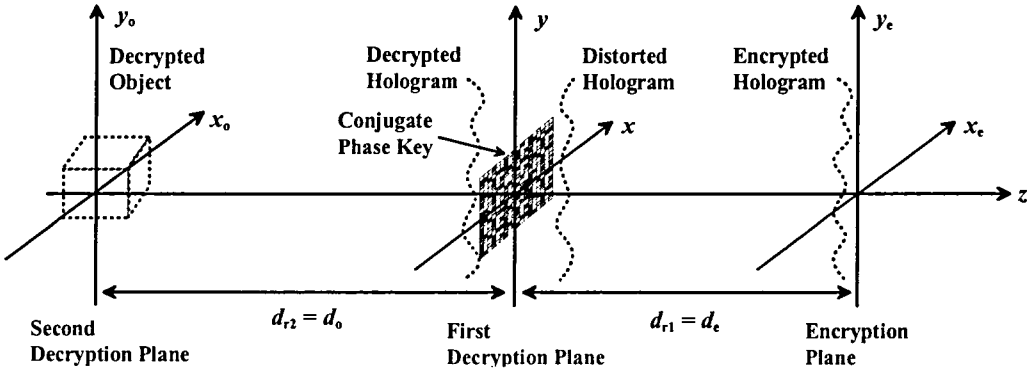
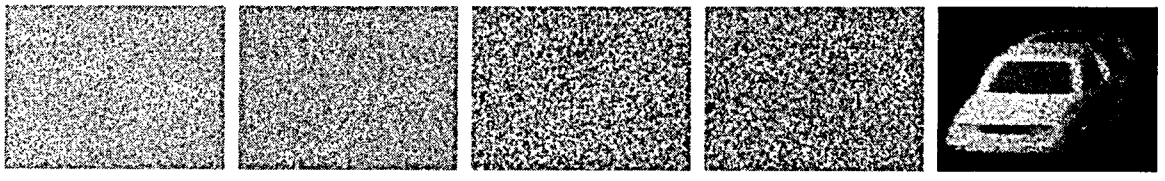


그림 2. 암호화된 디지털 홀로그램으로부터 복호화 과정을 설명하는 구조도.



(a) (b) (c) (d) (e)

그림 3. 암호화 및 복호화 결과. (a) 암호화된 홀로그램의 실수부, (b) 암호화된 홀로그램의 허수부, (c) 정확한 거리 정보(d_o, d_e) 및 위상 키 정보를 모르는 경우 d_r = 350cm에서 직접 복원한 결과, (d) 정확한 거리 정보는 알고 있지만 위상 키 정보를 모르는 경우 두 번(d_{r1} = 100cm, d_{r2} = 250cm)의 역 Fresnel 전파를 거쳐 복원한 결과, (e) 모든 암호화 정보를 정확히 알고 있는 경우 두 번의 역 Fresnel 전파와 위상 키 복호화 과정을 거친 후 복원한 결과.

F
D

References

1. B. Javidi and T. Nomura, Opt. Lett. **25**, 28 (2000).
2. E. Tajahuerce and B. Javidi, Appl. Opt. **39**, 6595 (2000).
3. L. Yu, X. Peng, and L. Cai, Opt. Comm. **203**, 67 (2002).
4. X. Peng, Z. Cui, and T. Tan, Opt. Comm. **212**, 235 (2002).