임의 위상판에 의한 광학상 암호화의 분석

The analysis of optical image encryption using random phase mask

김병철, 차성도, 신승호
강원대학교 물리학과
shinsh@kangwon.ac.kr

Ⅰ. 서론

대용량 정보의 보안이 매우 중요해짐에 따라 활발히 진행 중인 광정보의 보안에 대한 연구[1,2]중에서 광학적 위상암호화는 많은 양의 정보를 한번에 암호화하고 해독할 수 있다[3]. 특히 Javidi[4] 등이 제안한 Fresnal 영역 임의 위상판(random phase mask; RPM)을 이용한 암호화 방법은 3차원 위치 정보를 암호화 키로 사용한다. 이와 같은 암호화 방법에 회전에 의한 위상변화를 추가하면 암호화 수준을 높일 수 있다[5]. 디지털 입력의 경우에는 BER(bit error rate)를 이용하여 암호화 수준을 측정하지만 아날로그 입력상의 경우는 적절한 방법이 제시되지 못하였다. 본 논문에서는 회전형 임의 위상판을 이용한 암호화 시스템에서 정확한 암호화 수준을 측정하기 위하여 아날로그 입력에 대한 암호화 수준을 평가하는 방법을 제시하고 비교하였다.

Ⅱ. 실험장치

실험 장치도(그림 1)에서 광원은 파장 514.5 nm의 Ar$^+$레이저를 사용하였고 기록 매질은 Fe가 0.02-mol.% 첨가된 $LiNbO_3$:Fe를 사용하였다. 입력 이미지는 렌즈 L1에 의해 점선으로 표현된 푸리에 평면에 푸리에 변환 후 렌즈 L2에 의해 기록매질에 입사되어 기준빔과 간섭하여 홀로그램을 형성한다. 위상 변조를 위한 두 개의 위상판 RPM1 과 RPM2는 각각 입사이미지와 렌즈 L1 사이 그리고 렌즈 L1과 푸리에 평면 사이에 위치한다. 실험에 사용한 RPM은 지름 26 mm의 원형 엠보싱 필름이다. 기록이 끝난 후 암호화된 상은 위상공액파에 의해 재생되고 렌즈 L3에 의해 역 푸리에 변환 된 후 CCD2로 관측한다.

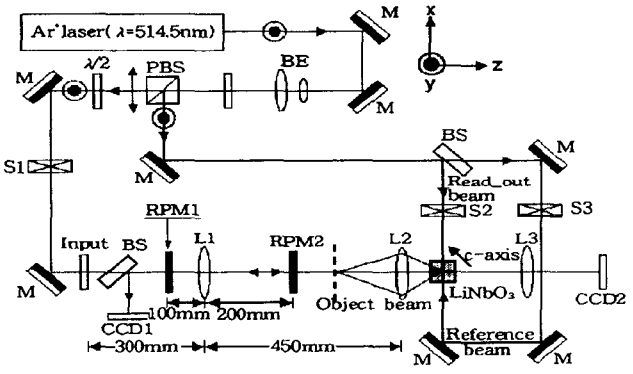
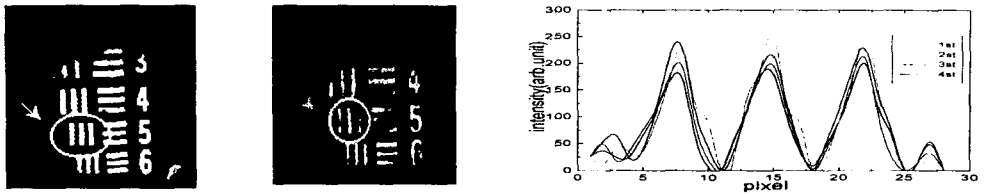


그림 1. 실험장치 구성도.

Ⅲ. 실험결과

암호화수준을 측정하기 위하여 USAF resolution Target을 입력 이미지로 사용하였다. 그림 2-(a)는 두 개의 RPM을 사용하여 암호된 광학상을 재생한 것으로 원으로 표시된 이미지의 선폭은 0.039 mm이다. 그림 2-(b)는 RPM1은 고정시키고 RPM2를 x축으로 5 μm 이동하였을 때의 재생상이고 (c)는 동일 조건하에서 4차례 실험하여 얻은 재생상의 세기분포이다. 선명도변조가 $\gamma = I_{max} - I_{min} / I_{max} + I_{min}$ 로 정의 될 때, 그림 3에서 보듯이 RPM2를 x축으로 11 μm 이상 이동시키면 γ가 급격히 줄어들고 18



(a) (b) (c)

그림 2. (a) 두 개의 RPM으로 암호화된 광학상의 재생상, (b) RPM2를 x축으로 5 μm이동시 재생상, (c) 동일 조건하에서 4회 반복한 재생상들의 세기 분포.

μm 이상이면 γ가 20 %이하로 재생상의 판별이 불가능하다. 그림 4는 RPM2를 회전시켰을 때의 재생상의 선명도변조로 RPM2를 0.23 °이상 회전시키면 γ가 현저히 작아지며 0.3 °이상이면 판별이 불가능하다. 그림 5와 같이 RPM2를 z축으로 1.0 mm 이상 이동시키면 γ의 변화가 일어나고 2.4 mm 이상

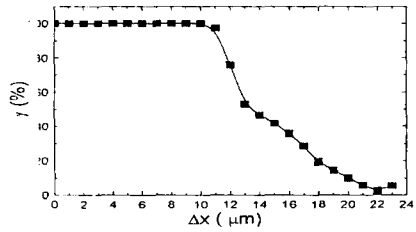


그림 3. RPM2를 x축으로 이동시 γ의 변화.

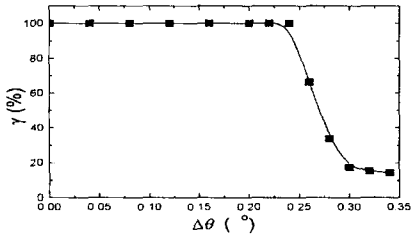


그림 4. RPM2를 회전시 γ의 변화.

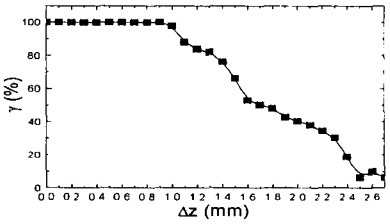


그림 5. RPM2를 z축으로 이동시 γ의 변화.

이면 판독이 불가능하다. 이와 같은 실험결과로 부터 계산한 입력상의 해독 가능한 경우의 수는 ~ 6 x 10^{21} 이었다. 회전형 임의 위상판을 추가하여 사용한 경우의 암호화 수준은 병진 이동만 고려한 경우의 수 ~ 4 x 10^{15} 보다 ~10^{6} 정도 향상되었다.

IV 결론

광굴절 결정인 $LiNbO_3$:Fe에 기록된 광학상을 두 개의 RPM을 사용하여 광학적으로 암호화하여 기록하고 위상공액파를 이용하여 해독시킬 수 있었으며, RPM의 위치와 각도 변화에 따른 선명도변조의 변화를 측정하여 암호화 수준을 분석하였다. RPM의 위치 정보를 이용한 광학상의 암호화 방법은 기록시의 RPM의 정확한 위치 정보를 알지 못하면 암호의 해독이 거의 불가능하므로 홀로그램 광 기억장치의 보안에 매우 유용한 암호화 방법임을 알 수 있다.

이 연구는 한국과학재단 목적기초연구 (2000-2-11100-003-3)지원으로 수행되었음.

V 참고문헌

[1] F. H. Mok, Opt. Lett. 11, 915(1993).
[2] X. An, D. Psaltis, and G. W. Burr, Appl. Opt. 38, 386(1999).
[3] Bahram Javidi, Physics Today, March 27(1997).
[4] B. Javidi, G. Zhang, and J. Li, Opt. Eng. 35, 2506(1996).
[5] 김병철, 차성도, 신승호, 제5회 광정보처리 학술발표회 논문집. Vol. 6, No. 1. 203(2000).