1999년도 대한전기학회 정기총회 및 추계학술대회 논문집 1999. 11. 20

랜덤 위상 마스크를 이용한 광 메모리에서의 암호화 특성

최진산*, 양병춘, 이병호
서울대학교 전기공학부 국가 지정 홀로그래피 기술 연구실

Characteristics of encryption in optical memory using random phase mask

Jinsan Choi*, Byungchoon Yang, and Byoungho Lee
NRL of Holotech, School of Electrical Engineering, Seoul National University

Abstract - Opical encoding method of images using random-phase encoding in both input and Fourier planes was proposed by Javidi and his group, and the method was realized experimentally by Singh and his group with use of a photorefractive crystal and a phase conjugate wave.[1-2] Recently various techniques have been proposed theorically and experimentally. These include the method using one random-phase mask in the Fourier plane or two random-phase masks in the input and the Fresnel planes.[3] We demonstrate the difference and the problem of the methods using one or two random-phase masks in the Fourier or Fresnel plane. We perform the encoding and decoding in $LiNbO_3$ crystal using degenerate four-wave mixing.

1. 서 론

현대 사회가 점차 고도의 정보화 사회로 발전해 감에 따라 음성, 화상, 데이터 등의 다양한 종류의 정보를 교환하고 저장하는 대용량 정보 처리 시스템이 구축되어 가고 있다.이러한 정보 시스템이 일반화 되기 위해서는 신뢰성과 안정성이 필수적인 요소이다. 현재까지 정보를 보호하기 위해 개발된 정보 보호 시스템은 전자 회로적인 기술로 이루어져 있다. 그러나 시스템이 고속화 및 대용량화 되어 가는 현재의 상태에서 전자 회로적인 기술은 속도와 집적도에 한계를 가지고 있으므로 이를 대신 할 수 있는 고속 및 대용량 정보 처리 기술이 필요하다. 또한 기존의 1차원 데이터에 편중 되어 있는 정보 보호 방식을 화상과 같은 2차원 데이타에 적용하는 데에도 한계가 있다. 그러므로 고속과 대용량 및 2차원 정보 처리 특성을 동시에 가지고 있는 광 정보 처리 기술이 미래의 정보 보호 시스템에 적합한 기술이라고 생각할 수 있다. 본 논문에서는 양의 실수 값을 갖는 2차원 이미지를 랜덤 위상 마스크를 이용하여 광 메모리에 암호화해서 저장하고 degenerate four-wave mixing을 이용해서 복호화하는 실험을 하였고 랜덤 위상 마스크의 위치와 사용 개수가 암호화에 미치는 영향을 실험을 통해서 알아 보았다.

2. 본 론

2.1 광 메모리 암호화의 원리

2차원 영상 신호는 푸리에 변환에 의해서 주파수 영역에서 해석될 수 있다. 푸리에 변환된 신호는 위상과 크기를 갖는 복소수로 표현되는데 이중에서 위상 성분이 크기 성분보다 훨씬 더 중요함이 연구된 바 있다. 원래의 영상은 푸리에 변환된 신호를 역 푸리에 변환을 함으로써 얻어 지는데, 위상에 대한 정보가 임의로 바뀌었다면 역 푸리에 변환에 의해서 원래의 영상을 얻을 수 없게 된다. 이러한 사실은 2차원 영상의 암호화에 응용될 수 있다.

2.1.1 암호화 과정

푸리에 변환된 신호의 위상을 0에서 2π까지 랜덤하게 변화시킴으로써 암호화된 영상을 얻을 수 있다. 이러한 암호화 과정은 그림 1과 같이 나타낼 수 있다.

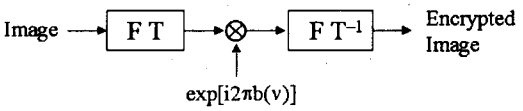

그림 1. 암호화의 개념도

여기서 FT와 FT^{-1}은 각각 푸리에 변환과 역 푸리에 변환을 나타내며 $b(\nu)$는 0과 1사이에 균일하게 분포한 랜덤한 값이다. 이것을 식으로 표현하면 다음과 같다. 2차원 영상을 f(x), $\exp[i2\pi b(\nu)]$의 역 푸리에 변환을 h(x), 암호화된 영상을 $\psi(x)$라 하면(편의상 1차원 기호를 쓰고 x좌표의 부호의 뒤집힘을 무시한다.)

$$\psi(x) = FT^{-1}[FT[f(x)] \times e^{i2\pi b(\nu)}] = f(x) \otimes h(x) \quad (1)$$

과 같이 된다. 여기서 ⊗는 컨벌루션을 의미한다.

2.1.2 복호화 과정

암호화된 신호를 복호화하기 위해서는 암호화에 사용된 랜덤 위상 성분의 복소 공액을 곱해야 한다. 이 과정은 그림 2와 같다.

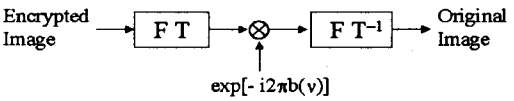

그림 2. 복호화의 개념도

암호화된 영상이 $\psi(x)$라면 복원된 영상 r(x)는

$$r(x) = FT^{-1}[FT[\psi(x)] \times e^{-i2\pi b(\nu)}]$$
$$= FT^{-1}[[FT[f(x)] \times e^{i2\pi b(\nu)}] \times e^{-i2\pi b(\nu)}] = f(x) \quad (2)$$

와 같이 되어서 원래의 영상 f(x)와 같아 진다.(편의상 x 좌표의 부호의 뒤집힘을 무시한다.)

2.2 광학적 구현

푸리에 변환 및 역 푸리에 변환은 광학적으로 렌즈를 통해서 이루어지며, $\exp[i2\pi b(\nu)]$로 표현되는 랜덤한

위상 변화는 랜덤 위상 마스크를 이용하여 광학적으로 구현될 수 있다. 랜덤 위상 마스크로는 위상을 변화시키는 공간 광 변조기(SLM), ground glass, 또는 젤라틴을 바른 투명 유리 등이 사용될 수 있다. 한편, 복호화를 할 때는 일반적으로 복소 공액 위상 마스크가 필요한데 degenerate four-wave mixing을 이용할 경우에는 이것이 필요하지 않다.

2.3 실험 및 결과

2.3.1 Degenerate four-wave mixing을 이용한 광 메모리 암호화

본 실험의 구성도는 그림 3과 같다.

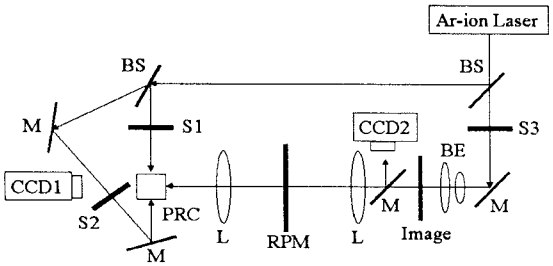

그림 3. 광 메모리 암호화에 사용된 실험 setup
BS: beam splitter, BE: beam expander, M: mirror, S: shutter, L: lens, RPM: random phase mask, PRC: photorefractive crystal

광굴절 물질로는 Fe이온이 0.03% 도핑된 10 × 10× 10 mm^3 크기의 $LiNbO_3$ 결정을 사용하였으며, Ar-ion 레이저의 파장은 514.5nm이다. 랜덤 위상 마스크로는 투명 라커를 분사한 투명 필름을 사용했다. 입력 이미지를 암호화하고 암호화된 이미지를 저장할 때에는 S1과 S3를 열고 S2는 닫는다. 입력 이미지를 가지고 있는 목적빔과 S1을 통과하는 기록빔이 크리스탈에 체적 회절 격자를 만들면서 목적빔을 저장한다. CCD1을 통해서 이미지가 암호화 된 것을 확인한다. 크리스탈에 저장된 이미지를 재생하여 원래의 입력 이미지로 복호화 할 때에는 S1과 S3를 닫고 S2를 연다. 그러면 degenerate four-wave mixing을 통해서 생성된 재생빔이 랜덤 위상 마스크를 지난 후 CCD2에서 관측된다. 이때 방향이 서로 반대인 두 기록빔은 이론적으로는 평면파이어야 degenerate four-wave mixing이 있어나지만 실험에서는 빔의 강도를 크게 하기 위해서 레이저에서 나오는 가우시안 빔을 그대로 이용하였다. 이 실험에서 사용된 입력 이미지와 암호화된 이미지는 각각 그림 4와 그림 5이고, 올바른 마스크와 다른 마스크를 써서 복호화된 이미지는 각각 그림 6, 그림 7과 같다. 그림 6에서는 입력 이미지가 복원되었고 그림 7에서는 그렇지 않음을 볼 수 있다.

2.3.2 랜덤 위상 마스크의 위치에 따른 영향

일반적으로 랜덤 위상 마스크가 사용되는 위치는 입력 이미지가 렌즈에 의해서 모이는 초점이다. 이곳은 푸리에 변환이 일어나는 점이기 때문에 이론적으로도 타당하다. 한편, 렌즈와 초점 사이의 프레넬 영역에 랜덤 위상 마스크를 놓아서 암호화하는 방법이 제안되기도 한다.[3]

본 실험에서는 그림 8과 같이 구성하였다. 랜덤 위상 마스크를 초점 평면(위치 1)의 앞 뒤(위치 2,3)로 이동시키면서 CCD도 적당하게 이동시켜서 이미지를 촬영했다. 이렇게 해서 얻어진 이미지는 그림 9와 같다. 따라서 이러한 방식을 사용해서 이미지가 암호화되었다고 말하기 힘들다.

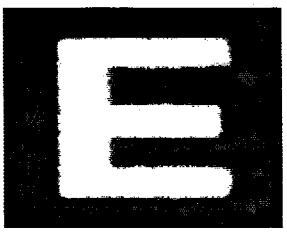

그림 4. 입력 이미지

그림 5.
암호화된 이미지

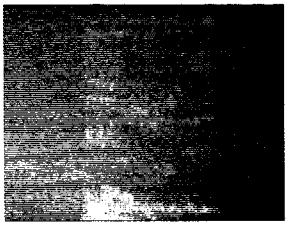

그림 6. 바르게 복호화된 이미지

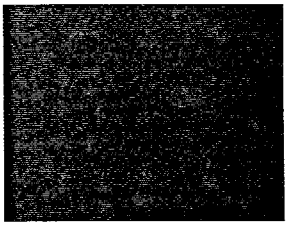

그림 7. 다른 마스크로 복호화된 이미지

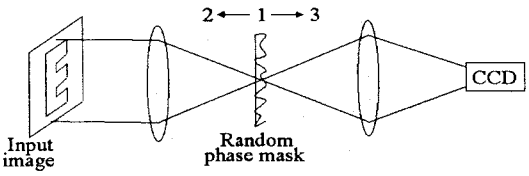

그림 8. 프레넬 영역에서의 암호화 실험 개념도

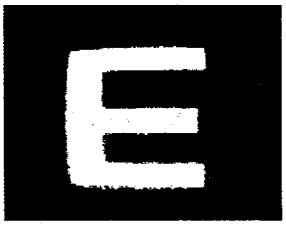

그림 9. 프레넬 영역을
이용해서 얻어진
이미지

2.3.3 랜덤 위상 마스크의 사용개수에 따른 영향

암호화에 사용되는 랜덤 위상 마스크는 1개 또는 2개이다. 1개를 사용할 경우에는 푸리에 평면(초점 평면)에 위치시키고, 2개를 사용할 경우에는 입력 이미지의 바로 뒤(입력 평면)와 푸리에 평면에 위치시킨다. 만일 1개의 랜덤 위상 마스크만 이용할 경우에는 그림 4는 그림 10과 같이 암호화된다. 또 입력 평면에 1개를 추가해서 모두 2개의 랜덤 위상 마스크를 사용해서 암호화한 이미지는 그림 11와 같다.두 그림 모두 암호화가 되었지만 그림 11이 그림 10에 비해서 광도 분포가 더 고르게 분산되어 있는 것을 알 수 있다. 그리고 1개의 랜덤 위상 마스크를 입력 평면에 놓아서 얻어진 이미지는 그림 12과 같은데 이것은 입력 이미지와 같다. 따라서 입력 평면에 추가되는 랜덤 위상 마스크는 암호화 자체와는 상관 없이 에너지 밀도를 고르게 해 주어서 암호화된 이미지의 통계적 성질을 향상시킨다. 반면에 두 개의 랜덤 위상 마스크를 사용하면 효율이 낮아지는 단점이 있다. 따라서 실제적으로 1개의 랜덤 위상 마스크를 쓰는 것이 더 효율적일 수 있다.

그림 10. 한 개의 마스크를
푸리에 평면에 사용하여
암호화된 이미지

그림 11. 두 개의 마스크를
이용하여 암호화된 이미지

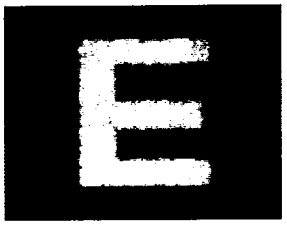

그림 12. 한 개의 마스크를
입력 평면에 사용해서 얻은
이미지

3. 결 론

본 논문에서는 랜덤 위상 마스크와 $LiNbO_3$ 크리스탈을 이용하여 광 메모리 암호화 실험을 수행하였고 암호화 및 복호화가 됨을 확인하였다. 여기서 degenerate four-wave mixing을 이용해서 한 개의 랜덤 위상 마스크만으로 암호화 및 복호화를 하였다. 또한 랜덤 위상 마스크의 위치가 푸리에 평면에서 벗어나서 프레넬 영역에 놓일 때는 암호화가 덜 이루어 진다는 것과 두 개의 랜덤 위상 마스크를 사용할 경우의 장,단점을 논의했다. 랜덤 위상 마스크의 투과 효율이 개선된다면 두 개의 마스크를 쓰는 것도 좋을 것이다.

[참 고 문 헌]

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett, 20, 767-769, 1995

[2] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," Appl. Opt, 37, 8181-8186, 1998

[3] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett, 24, 762-764, 1999