# 진폭 마스크와 2D 카오스 함수를 이용한 다중 이미지 광학 암호화

# Optical encryption of multiple images using amplitude mask and 2D chaos function

김활*, 전성빈*, 김도형**, 박노철†, 박영필*

Hwal Kim, Sungbin Jeon, Do-Hyung Kim, No-Cheol Park and Young-Pil Park

(2014 년 9 월 18 일 접수; 2014 년 9 월 22 일 심사완료; 2014 년 9 월 23 일 게재확정)

**Abstract**

Object image using DRPE(Double Random Phase Encryption) in 4f system is encrypted by space-division method using amplitude mask. However, this method has the weakness for the case of having partial data of amplitude mask which can access the original image. To improve the security, we propose the method using the 2-dimension logistic chaos function which shuffles the encrypted data. It is shown in simulation results that the proposed method is highly sensitive to chaos function parameters. To properly decrypt from shuffled encryption data, below 1e-5 % errors of each parameter should be required. Thus compared with conventional method the proposed shows the higher security level.

**Key Words :** 홀로그래피(Holography), 디지털 홀로그래피(Digital holography), 광학 암호화 (Optical Encryption), 카오스 함수(Chaos function)

## 1. 서 론

홀로그래피는 홀로(holo) 전체라는 뜻과 그래피(graphy) 기록 혹은 그림이라는 뜻이 합성된 말로 전체를 기록한다는 것을 의미한다. 빛의 정보 전체를 저장한다는 것은 빛의 진폭(Amplitude)과 위상(phase)를 동시에 기록한다는 것이다. 홀로그래피는 물체의 표면에서 반사된 빛의 위상 변화를 간섭 무늬 형태로 기록한 것이다. 물체에 투사된 후에 반사 또는 투과하여 홀로그래피 저장 매체에 입사되는 물체파(object wave)와 저장 매체에 직접 입사되는 기준파(reference wave)의 2 개의 파가 서로 간섭 현상을 일으키며, 일반적으로 이 두 파는 서로 간섭할 수 있는 코히런트(coherent)한 빛을 사용한다.

홀로그래피는 크게 아날로그 방식과 디지털 방식으로 나뉜다. 광학 시스템을 구축하여 홀로그래픽 필름에 간섭 무늬 패턴을 저장하는 방식을 아날로그 홀로그래피라고 하고, 홀로그래픽 필름 대신에 CCD, CMOS 와 같은 디지털 장비를 이용해서 간섭 패턴을 기록 (디지털 홀로그램)하여 처리, 전송하여 재생하는 방식을 디지털 홀로그래피라고 한다. 홀로그래피 장치에서 기록되는 간섭 패턴은 아래 식과 같이 나타난다.

$$I = |E_R + E_O|^2 = |E_R|^2 + |E_O|^2 + E_R^* E_O + E_R E_O^* \quad (1)$$

위와 같은 디지털 홀로그래피를 사용하는 기술 중에는 홀로그래픽 디스플레이, 홀로그래픽 프린터, 홀로그래픽 메모리, 홀로그래픽 현미경, 홀로그래피를 이용한 광 암호화 등 다양하다. 이 중

† School of Mechanical Engineering, Yonsei Univ.
E-mail : pnch@yonsei.ac.kr
TEL : (02)2123-4530
* School of Mechanical Engineering, Yonsei Univ.
** Center for Information Storage Device, Yonsei Univ.

홀로그래피 광 암호화는 국방, 멀티미디어 방송, 원격의료, 원격교육, 기상예보 등 이미지의 전송과 보안에 관한 요구가 높아지면서 더욱 각광 받는 분야가 되고 있다.

1995 년 Refregier 와 Javidi 가 이중 랜덤 위상 암호화 방법을 제안한 이후 광 암호화는 광 정보 처리 분야에서 떠오르는 주제가 됐다. 이중 랜덤 위상 암호화 방법은 입력 면과 푸리에 면에 각각 랜덤 마스크를 사용하여 이미지를 백색 잡음 형태로 암호화하여 저장한다.[1]

광 암호화의 주요한 응용 방법은 다중 이미지를 하나의 암호화된 정보 속에 담는 다중 암호화 방법이다. 다중 각도[2], 다중 파장[3], 측면 이동(lateral shifting)[4]등의 다중 암호화 방법들이 있다.

광 다중 암호화 방법은 두 개의 중요한 도전 과제가 있다. 첫 번째는 암호화 될 수 있는 다중 이미지의 양이 제한적이기 때문에 크로스톡(cross talk)과 노이즈(noise)의 영향을 최소화 시켜야 한다. 두 번째는 암호화된 정보가 부분적인 암호화나 노이즈가 추가 되는 등 정보 전송 중의 공격이나 왜곡에 간겅성을 가져야 한다.

최근에 Barrera 등이 이미지 정보를 암호화 하는 과정에서 몇 개의 다른 진폭 마스크를 사용하는 다중 어퍼쳐[aperture] 기술[5]을 제안했다. 이를 이용하면 크로스톡 없이 일치하는 어퍼쳐 마스크에 맞는 이미지가 복원된다. 하지만 부분적으로 일치하는 마스크를 사용하여 복원할 경우에도 이미지 정보가 복원될 수 있다는 단점이 있다. 이러한 현상은 컴퓨터를 통한 반복적인 알고리듬을 통해서 부분적인 진폭 마스크를 얻는 경우 암호화된 정보가 노출될 위험이 있다는 것을 의미한다. 이러한 단점을 보완하기 위해서 향상된 다중 이미지 암호화 방법을 제안한다. 진폭 마스크를 통한 공간 분할이 사용된다. 복호화 과정에서 얻게 되는 이미지의 질과 보안성을 위해서 이중 랜덤 위상 암호화 방법에 수치적 처리를 더할 것이다. 다음 장에서 시뮬레이션을 통해서 이 방법을 검증한다.

## 2. 이론적 배경

### 2.1 이중 랜덤 위상 암호화 방법(double random phase mask encoding)

1995 년 Refregier 와 Javidi 는 4f 광학계를 이용하여 입력 평면과 푸리에 평면에 랜덤 위상 마스크를 놓아서 영상의 정보를 암호화 하는 방법을 제안했다. 이 방법을 통해서 암호화된 영상은 백색 잡음 형태로 변환된다.

f(x)가 암호화 될 영상이라고 하고, ψ(x)가 암호화된 영상이라고 놓자. n(x)와 b(x)는 각각 독립적으로 [0,1] 사이의 값이 분포된 수의 나열이라고 한다. 입력 평면에서의 위상 암호화 마스크는 exp[i2πn(x)]이고, 푸리에 평면에서의 위상 암호화 마스크는 exp[i2πb(x)] 이다. 입력 평면에서 위상 암호화 마스크를 씌운 영상 정보는 아래와 같이 나타낸다.

$$f(x)\exp[i2\pi n(x)] \tag{2}$$

푸리에 렌즈를 통해서 푸리에 평면으로 진행하면 푸리에 변환에 의해서 다음과 같이 변한다.

$$F[f(x)\exp[i2\pi n(x)]] \tag{3}$$

푸리에 평면에서 위상 암호화 마스크가 씌워져서 $F[f(x)\exp[i2\pi n(x)]]\times F[h(x)]$로 바뀌게 되고, 또 한 번 푸리에 렌즈에 의해 출력 평면에 암호화된 정보로 나타난다.

$$\psi(x)=f(x)\exp[i2\pi n(x)]*h(x) \tag{4}$$

이렇게 암호화된 정보는 백색잡음 형태로 변환되어, 암호화 마스크의 정보 없이는 영상을 복원할 수 없게 된다.

암호화 마스크의 정보를 알고 있는 경우 복호화하는 방법은 암호화된 정보 (4)식을 푸리에면으로 역전사 시킨다.

$$F[f(x)\exp[i2\pi n(x)]]\times F[h(x)] \tag{5}$$

이와 같은 식을 얻어서 두 번째 랜덤 위상 마스크의 공액 복소를 곱해서 F[f(x)exp[i2πn(x)]를 구한다. 그 다음 푸리에 평면에서 재생 평면으로 역전사 시켜서 얻은 푸리에 변환 f(x)exp[i2πn(x)]에 첫 번째 랜덤 위상 마스크의 공액 복소를 곱하면 처음에 암호화했던 영상이 복원된다.

### 2.2 2D 카오스 함수

다중 이미지 암호화에 대한 관심과 요구가 많아짐에 따라 다양한 방법의 다중 이미지 암호화 방

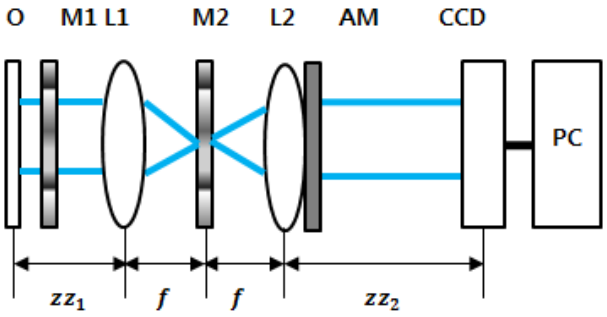


**Fig. 1** Schematic description of proposed method. O: object; M: random phase mask; L: lens; AM: amplitude mask.

법들이 고안되고 있다. 연구자들과 학자들은 다중 파장(wavelength multiplexing), 랜덤 위상 마스크, 다중 위치(position multiplexing), 이중 랜덤 위상 암호화, 다중 채널 암호화 등의 광학적인 암호화 방법을 제안했다. 여기서는 암호화의 보안성을 높이기 위해서 정보를 섞는 과정 중에서 2 D 의 논리적 함수를 사용한다. 가장 간단하고 일반적인 비선형 카오스 함수는 다음과 같이 정의 된다. [6]

$$x(i+1) = \mu_1 x(i)(1-x(i)) + \gamma_1 y^2(i)$$
$$y(i+1) = \mu_2\, y(i)(1-y(i)) + \gamma_2 (x^2(i) + x(i)y(i)) \quad (5)$$

여기서 $x(i), y(i) \in (0,1)$ 이란 조건을 만족시킨다. 카오스 랜덤 수열을 만들기 위해서 식(5)은 다음과 같은 조건을 만족시켜야 한다.

$$2.75 < \mu_1 \le 3.4,\ 2.7 < \mu_2 \le 3.45,$$
$$0.15 < \gamma_1 \le 0.21,\ 0.13 < \gamma_2 \le 0.15.$$

$$x = x \times 10^5 - floor(x(i) \times 10^5)$$
$$y = y \times 10^5 - floor(y(i) \times 10^5) \quad (6)$$

다중 암호화 영상 정보를 임의로 섞기 위해서 랜덤 좌표계로 사용되는 카오스 함수를 만들고, 이 두 수열은 영상과 같은 길이, 높이와 너비를 갖는다. 논리적 카오스 함수는 초기 변수의 미세한 변화에도 큰 차이를 보여준다고 입증됐다. 또한 암호화된 정보를 뒤섞기 위해서 몇 개의 추가적인 연산이 필요할 뿐이어서 기존의 광학 시스템의 큰 변경 없이 더 높은 수준의 보안성을 얻을 수 있다.

## 3. 실험 결과

Fig.1 은 제안된 광학 암호화 방법을 표현한다. 물체 이미지는 4f 시스템에서 DRPE 에 의해서 암호화된다. 이미지 센서에 기록되기 전에 진폭 마스크가 데이터를 부분적으로 차단한다. 이 방법을 이용해서 각각의 암호화된 이미지 중첩을 통해 다중 이미지 암호화가 가능하다. 이 논문에서 제안된 방법을 검증하기 위해서 시뮬레이션을 해봤다. 그 전에 Fig.2 는 기존에 사용하던 공간 분할 암호화 결과를 나타낸다. 두 개의 이미지는 DRPE 에 의해서 암호화 되었는데, 이 때 사용한 변수는 $zz_1 = 0.2m$, $zz_2 = 0.2m$, $\lambda = 532\text{nm}$ 이다. 간단한 직교 진폭 마스크를 적용시켰다. 해독 과정에서 올바른 위상 마스크와 진폭 마스크를 사용 하면 크로스톡없이 해독이 가능하다. 하지만 원래의 것과 부분적으로 일치하는 마스크를 사용하더라도 Fig.3 에서 보는 것과 같이 물체의 정보를 복원할 수 있다. 공간 분할 방법이 다른 물체의 효과 없이 이미지의 질을 보장하지만 상대적으로 낮은 보안성을 갖는다.

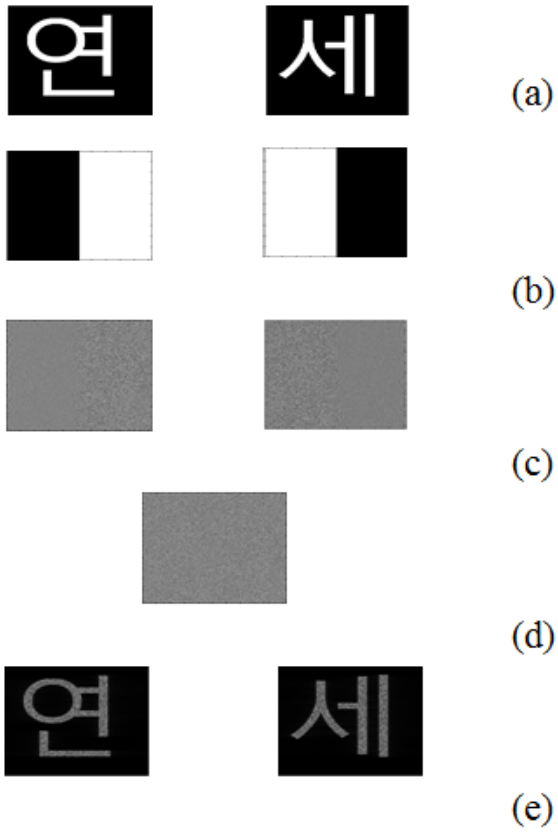


**Fig. 2** Result of conventional space-division multiplexing encryption method. (a) object images, (b) amplitude masks next to the exit pupil, (c) encrypted image of each object, (d) multiplexed data, and (e) decrypted image with proper amplitude mask.

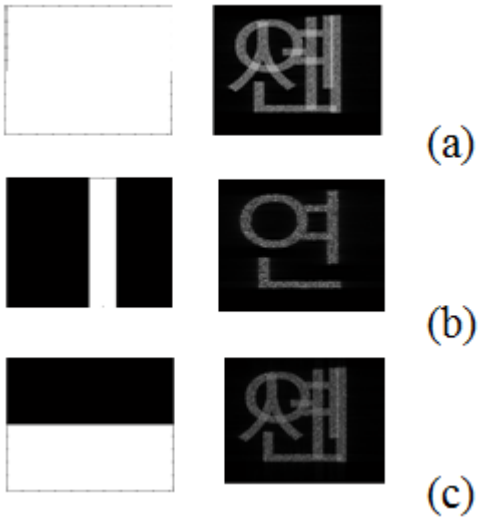


**Fig. 3** Wrong amplitude masks and decrypted image. (a) no amplitude mask and image (b) , (c) partial amplitude mask and image.

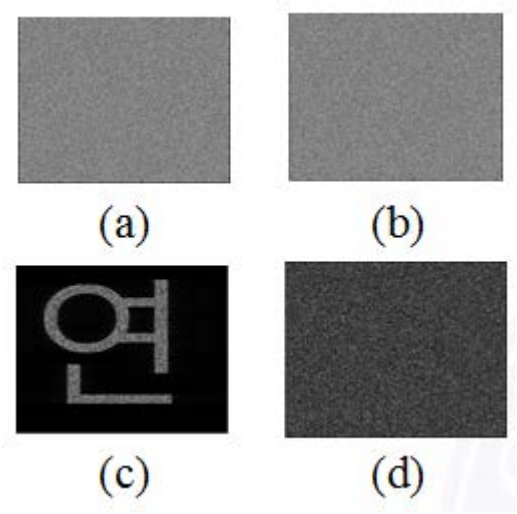


**Fig. 4** (a) encrypted image using conventional space-division method, and (b) shuffled image applying proposed 2D chaos map, (c) decrypted image with proper parameters, and (d) decrypted image with wrong parameters.

이는 광학 암호화에서 중요한 이슈이다.

Fig. 4 은 제안된 방법을 이용한 결과를 나타낸다. 초기 변수는 $\mu_1 = 2.84124$ , $\mu_2 = 3.41073$ , $\gamma_1 = 0.20052$ , $\gamma_2 = 0.14984$ , $x(1) = 0.95854$ , and $y(1) = 0.34563$ 이다. Fig. 4(b)는 셔플링(shuffling)된 이미지를 나타내고, 랜덤하게 분포된 데이터를 보여준다. 해독 과정에서 오직 정확한 변수 값을 가지고 다중 암호화된 이미지에서 원하는 이미지를 복원할 수 있다. Fig. 4(d)를 보면 $\mu_1$ 을 0.00001 바꾼 값을 대입해서 복원했을 때 결과를 보여준다. 보이는 것과 같이 미세한 값의 변화가 있을 뿐인데 정보가 전혀 복원되지 않는다. 이는 높은 보안성을 지니는 것을 의미한다.

올바른 변수 값을 가지고 복원했을 경우 MSE 와 SNR 값은 각각 0.2421, 2.5378 이다. 이와 비교하기 위해서 각각의 변수들을 1e-5 만큼 변화를 준 다음에 MSE, SNR 을 구했을 때 결과를 Tab. 1 에 정리해서 보여주고 있다. 결과를 보면 확실히 SNR 이 많이 감소했으며, MSE 가 증가함을 알 수 있는데 이는 이미지 질이 감소했음을 알려주는 결과이다. 또 한 Fig. 4 에서 본 것과 같은 결과가 모든 변수에서도 나타났다. 1e-5 만큼 변화를 줬음에도 복원되는 이미지가 원래 물체 이미 지의 정보를 전혀 알 수 없게 만들었다. 이는 셔 플링된 이미지를 복원할 때 원래 카오스 함수의 변수를 적용하지 않으면 매우 민감하기 때문에 복원이 어렵다는 것을 의미한다.

## 4. 결론

기존의 진폭 마스크를 이용한 공간 분할 방식의 다중이미지 암호화 방법의 보안성을 높이기 위해서 2 차원의 논리 카오스 함수를 사용하였다. 기존의 방식은 진폭 마스크의 부분적인 정보만 알더라도 정보의 복원이 가능하여 보안성에 문제점을 보였다. 하지만 제안된 방법을 사용하면 소수점 5 번째 자리의 변화 만으로도 정보가 전혀 복원되지 않음을 보여줬다. 이는 6 개의 변수 중에 하나의

**Table 1** MSE, SNR with the parameter change.

| Parameters | Δ | MSE | SNR |
|---|---|---|---|
| $\mu_1$ | 1e-5 | 0.3944 | 0.9560 |
| $\mu_2$ | 1e-5 | 0.3982 | 0.9378 |
| $\gamma_1$ | 1e-5 | 0.3941 | 0.9573 |
| $\gamma_2$ | 1e-5 | 0.3960 | 0.9482 |
| $x(1)$ | 1e-5 | 0.3964 | 0.9463 |
| $y(1)$ | 1e-5 | 0.3928 | 0.9640 |

변수라도 미세한 오차가 발생하면 정보를 복원하지 못함을 의미한다. 또한 제안한 방법은 기존의 광학 시스템의 변경 없이 사용 가능 하기 때문에 많은 이점을 지니고 있다.

## 후 기

이 논문은 2014 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2012-009378)

## REFERENCES

[1] Refregier, P., and Javidi, B., 1995, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, 30(7):767:769.
[2] Matoba, O., and Javidi, B., 1999, “Encrypted optical storage with angular multiplexing.,” *Appl. Opt.*, 38(35):7288-93.
[3] Situ, G., and Zhang, J., 2005, “Multiple-image encryption by wavelength multiplexing,” *Opt. Lett.*, 30(11):1306-1308.
[4] Fredy Barrera, J., Henao, R., Tebaldi, M., Torroba, R., and Bolognini, N., 2006, “Multiplexing encryption–decryption via lateral shifting of a random phase mask,” *Opt. Commun.*, 259(2):532–536.
[5] Barrera, J. F., Henao, R., Tebaldi, M., Torroba, R., and Bolognini, N., 2006, “Multiple image encryption using an aperture-modulated optical system,” *Opt. Commun.*, 261(1):29–33.
[6] Wang X. Y., and Shi, Q. J., 1998, “New type crisis, hysteresis and fractal in coupled logistic map,” *Chin J Appl Mech*, 23:501–506