

論文2001-38SD-1-5

위상 카드와 간섭계를 이용한 광학적 보안 시스템 (Optical Security System Using Phase Mask and Interferometer)

金鍾允*, 金杞貞**, 朴世駿*, 金喆洙***, 裊長根****,
金正雨*****, 金秀重*

(Jong-Yun Kim, Ki-Jung Kim, Se-Joon Park, Cheol-Su Kim, Jang-Keun Bae, Jeong-Woo Kim, and Soo-Joong Kim)

요 약

본 논문에서는 컴퓨터와 리소그라피를 이용하여 암호화된 두 개의 위상카드를 제작하고, 마흐-젠더 간섭계를 이용하여 암호화된 이진영상을 복호화하는 방법을 제안하였다. 이때 두 위상카드 중 하나는 기준 영상으로 사용되고 다른 하나는 암호 영상으로 사용된다. 하나의 랜덤 위상 카드를 기준 영상으로 두고 암호화하고자 하는 영상에 맞게 빛의 간섭 현상을 이용하여 암호 영상으로 사용될 위상 카드를 제작하였다. 원 영상의 복원은 경로차가 같도록 구성한 마흐-젠더 간섭계의 두 경로에 기준 영상과 암호 영상을 위치시켜 간섭 시킴으로써 영상을 복원할 수 있다. 위상 카드는 광세기 검출기로 볼 수 없을 뿐만 아니라 복제할 수도 없어서 개인 정보보호 및 인증시스템에 매우 유용하게 사용될 수 있다. 간단한 영상에 대한 광실험을 통하여 제안한 시스템의 타당성을 확인하였다.

Abstract

In this paper, we propose a new optical security technique using two phase masks based on interferometer. A binary random phase image is used as a reference image and the encrypted image is generated according to the phase difference between the reference image and the original image. If there is no phase difference of a same pixel position in two phase masks, interference intensity of the pixel has minimum value and if phase difference of a same pixel position in two phase masks is π , its interference intensity has maximum value. We can decrypt the original image by putting two phase masks on each of the two optical paths of the Mach-Zehnder interferometer. Computer simulation and the optical experiments show a good performance of the proposed optical security system.

* 正會員, 慶北大學校 電子工學科
(Dept. of Electronics Eng., Kyungpook Nat'l University)
** 正會員, 三星重工業 조선플랜트연구소
(Shipbuilding & plant R & D Center, Samsung Heavy industries)
*** 正會員, 慶州大學校 컴퓨터·電子工學部
(School of Computer and Electronics Eng., Kyongju

University)
**** 正會員, 구미1大學 電子情報課
(Dept. of Electronics and Information, Kumi College)
***** 正會員, 東洋大學校 電子工學部
(Dept. of Electronics Eng., Dongyang University)
※ 본 연구는 정보통신부에서 지원하는 대학기초 연구
지원사업(C1-1999-4049-00)으로 수행하였습니다.
接受日字:2000年1月13日, 수정완료일:2000年12月13日

I. 서론

현대 정보화 사회에서는 컴퓨터 시스템 및 통신 시스템의 결합으로 시공간을 초월하여 엄청난 양의 정보 교환이 신속히 이루어지고 있고, 다양한 형태의 서비스 환경이 창출되어 빠르게 확산됨으로써 경제, 사회 등 전 분야에 큰 변화를 일으키고 있다. 이러한 사회는 우리생활을 보다 편리하게 만들어 주고 있지만 때로는 정보의 유출로 인한 막대한 피해를 주기도 하여 정보 보호가 매우 중요한 문제로 대두된다. 또한 정보화 진전에 따라 개인의 정보와 신용이 중요시되고, 여권, 신용카드, 은행카드 등과 같은 개인의 신원을 증명할 수 있는 신분증의 사용이 늘어나고 있으나 프린터, 스캐너, 복사기, 컴퓨터 관련 장치들의 발달로 인해 복제기술의 수준이 높아져 이에 대한 대책으로 최첨단 컴퓨터, 디지털 및 광학 기술들을 이용하여 위조 방지 시스템에 관한 연구가 활발히 이루어지고 있다. 현재 신용카드와 여권 등의 신분증의 복제 방지용으로 부착된 엠보스(embossed) 홀로그램은 광세기 검출기를 이용하여 마스터 홀로그램을 합성하고, 이를 이용해 대량복제가 가능해짐에 따라 기존의 광세기 검출기를 이용하더라도 복제할 수 없는 새로운 광학적 정보보호 기술이 차세대 기술로서 연구되고 있다^[1-5].

본 논문에서는 컴퓨터와 리소그래피를 이용하여 암호화된 두 개의 위상카드를 제작하고, 마흐-젠더 간섭계를 이용하여 암호화된 이진영상을 복호화하는 방법을 제안하였다. 이때 두 위상카드 중 하나는 기준 영상으로 사용되고 다른 하나는 암호 영상으로 사용된다. 하나의 랜덤 위상 카드를 기준 영상으로 두고 암호화하고자 하는 영상에 맞게 빛의 간섭 현상을 이용하여 암호 영상으로 사용될 위상 카드를 제작하였다. 원 영상의 복원은 경로차가 같도록 구성된 마흐-젠더 간섭계의 두 경로에 기준 영상과 암호 영상을 위치시켜 간섭시킴으로써 영상을 복원할 수 있다. 위상 카드는 광세기 검출기로 볼 수 없을 뿐만 아니라 복제할 수도 없어서 개인 정보보호 및 인증시스템에 매우 유용하게 사용될 수 있다. 간단한 영상에 대한 광실험을 통하여 제안한 시스템의 타당성을 확인하였다.

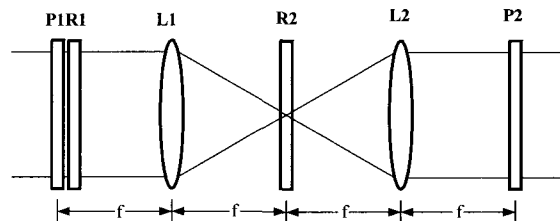
II. 기존의 광학적 영상 암호화 방법

Han 등은 256 그레이 레벨을 가지는 원 영상을 각

비트 평면으로 나누어 8개의 이진 영상들을 얻은 후 이들을 각각 암호화 키와 XOR 연산을 수행함으로써 영상을 암호화하는 방법을 제시하였다^[1]. 그러나 이 방법은 영상을 이진 비트평면 영상으로 변환하기 위해 디지털적인 처리가 필요하므로 시스템이 복잡하고, 광학적 장치만으로는 구현이 불가능한 단점이 있다.

Stepien 등과 Kim 등은 위상 CGH(computer generated hologram)를 이용하여 영상을 암호화하였는데^[2,3], 이 방법들은 영상을 CGH로 변환시킬 때의 샘플링 오차 등에 의해 영상의 왜곡이 생기고 반복 알고리즘에 의한 시간 소모가 많다.

그리고 Neto 등은 4f 광상관기의 푸리에 평면에 중심이 유전체로 코팅된 유리판을 사용하고, 원 영상을 진폭값에 비례하는 위상값으로 바꾸어 랜덤 위상 마스크와 함께 암호화하고, 영상을 복원하기 위해 암호화 과정에 사용된 랜덤 위상 마스크의 복소 공액값을 가진 마스크를 입력마스크에 사용하는 위상-세기(Phase-Contrast) 방법을 제안하였다^[4]. 이 방법 역시 세기에 비례하는 위상값의 근사식에 대한 에러가 복원영상의 왜곡으로 나타나게 된다.



P1 : Input Image

R1, R2 : Phase Mask

P2 : Encrypted Image

L1, L2 : Fourier Lens

그림 1. Refregier가 제안한 영상 암호화 시스템

Fig. 1. The image encryption system proposed by Refregier.

Refregier 등은 4f 광상관기를 이용하여 입력 평면과 푸리에 평면에 랜덤 위상 마스크를 사용하여 영상을 암호화하고, 동일한 시스템을 이용하여 원영상을 복원하는 방법을 제안하였다^[5]. 즉, 암호화시스템에서는 그림 1에서와 같이 입력 평면과 푸리에 평면에 두 개의 랜덤 위상 마스크를 이용하여 원 영상을 정상적(stationary) 백색잡음으로 변환시키고, 영상 복원 시스

템에서는 그림 2에서와 같이 암호키 카드로 영상 암호화시 사용한 푸리에 영역에서의 랜덤 위상 마스크의 공액 복소값을 가진 마스크를 푸리에 평면에 놓아 암호 영상과의 곱한 후 광세기 검출기를 통해 원영상을 복원하게 된다. 이 방법은 기존의 영상 암호화 방법 중 응용 가능성이 가장 높고, 많이 연구되어지고 있다. 그러나 이 방법은 암호화된 영상이 복소수 값이므로 카드를 제작하기 어려울 뿐 아니라 복소값을 나타낼 수 있는 실시간 공간 광 변조기(SLM : spatial light modulator)가 요구되는 문제점이 있다.

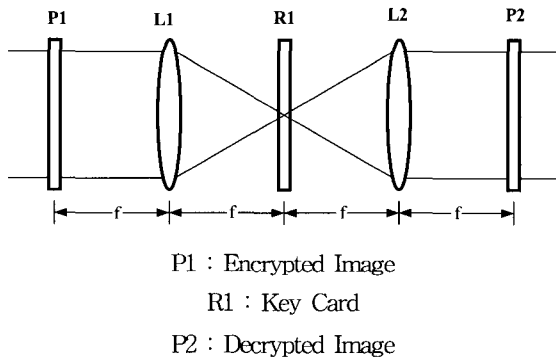


그림 2. Refregier가 제안한 영상 복원 시스템
Fig. 2. The image decryption system proposed by Refregier.

III. 제안한 암호화 시스템

본 논문에서는 빛의 간섭 현상^{6,7)}을 기초로 하여 광학적 암호화 시스템을 제안하였으며, 이 시스템에서는 암호키 자체는 원 영상의 정보를 전혀 가지고 있지 않고, 단지 위상만을 이용하므로 복소함수 형태를 가지는 기존의 방법들보다 제작이 간단하며 광세기 검출기로는 측정이 불가능한 장점을 가지고 있다.

1. 이진 영상 생성

z 방향으로 진행하고 주파수(ω)와 파장(λ), 진폭(E_0), 그리고 편광 방향(수직 방향)이 같은 두 개의 평면파 E_1 과 E_2 를

$$\begin{aligned} E_1(z, t) &= E_0 \cos(kz - \omega t) \\ E_2(z, t) &= E_0 \cos(kz - \omega t + \delta) \end{aligned} \quad (1)$$

라고 하자. 여기서 δ 는 두 파의 위상차이다. 이때 어느 주어진 시각에서 두 파를 합성하면 합성파는

$$\begin{aligned} E &= E_1 + E_2 \\ &= E_0 \cos(kz - \omega t) + E_0 \cos(kz - \omega t + \delta) \end{aligned} \quad (2)$$

가 되고, 그 세기는

$$\begin{aligned} I &= \langle E^2 \rangle \\ &= \langle (E_1 + E_2)(\overline{E_1 + E_2}) \rangle \\ &= \langle E_1^2 \rangle + \langle E_2^2 \rangle + 2\langle E_1 E_2 \rangle \\ &= 2E_0^2 + 2E_0^2 \cos \delta \end{aligned} \quad (3)$$

과 같다. 여기서 $\langle \cdot \rangle$ 는 시간평균을 의미한다. 합성파의 세기는 $\cos \delta = -1$ 즉 두 파의 위상차가 π 의 홀수배가 될 때 최소($I=0$)가 되고, $\cos \delta = 1$ 일 때(최대($I=4E_0^2$))가 된다.

그러므로 두 파의 위상차를 조정하여 간섭 세기를 조절할 수 있고, 특히 E_1 과 E_2 가 π 의 짝수배 또는 홀수배의 위상차만 갖도록 하면 각 화소의 간섭 위치에서 이진 영상을 만들 수 있음을 알 수 있다.

2. 간섭 원리를 기초로 한 영상 암호화

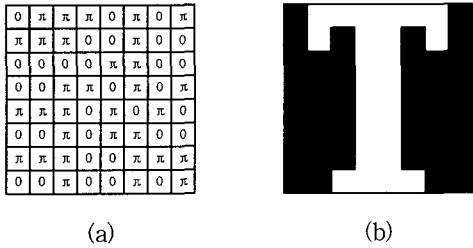
본 논문에서는 두 파의 경로차가 동일한 광경로를 가지는 두 지점에 위상값 0과 π 로 이루어진 위상 마스크를 각각 놓아서 이들의 합성파가 이진 영상을 표현할 수 있게 하였다. 이때 사용한 위상 마스크를 각각 기준 영상, 암호 영상이라 하고 암호 영상을 생성하는 과정은 다음과 같다. 먼저 기준 영상은 랜덤 잡음 발생기를 사용해서 구하고, 이와 원 영상에 따라 표 1에서 제안한 암호규칙을 이용하여 암호 영상을 생성한다. 이들은 0과 π 로 구성된 위상 마스크로 제작할 수 있다. 예를 들어 랜덤한 기준 영상과 원 영상이 각각 그림 3(a), 그림 3(b)와 같다고 할때, 표 1을 이용하여 구한 암호 영상은 그림 3(c)와 같이 된다. 기준 영상과 암호 영상은 위상값이 '0'인 부분은 흰 색으로, 위상값이 ' π '인 부분은 검은색으로 대치한 이진 영상 패턴이다. 그리고 제안한 방법을 이용하면 하나의 기준 영상에 대해 다른 여러 영상들을 암호화시킬 수 있다. 예를 들어 그림 4(a)와 같은 기준 영상을 사용하여 그림 4(b), 4(d), 4(f) 및 4(h)의 영상들을 암호화한 영상은 각각 그림 4(c), 4(e), 4(g) 및 4(i)와 같다. 또 제안한 방법을 확장하여 0과 π 사이의 임의의 위상값을 가진 마스크를 사용함으로써 그레이 레벨의 영상도 암호화가 가능하다. 즉 간섭 세기의 최대값과 최소값 사이의 세기인 cosine값을 이용하여 암호 영상과 기준 영상의 위상을

조절함으로써 그레이 레벨 영상을 생성할 수 있다.

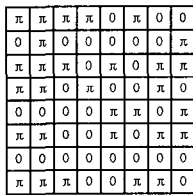
표 1. 원 영상에 대한 기준 영상과 암호 영상의 위상값

Table 1. Phase values of reference image and encrypted image for the original image.

Original image	Reference image	Encrypted image
0	0	π
	π	0
1	0	0
	π	π



(a) (b)

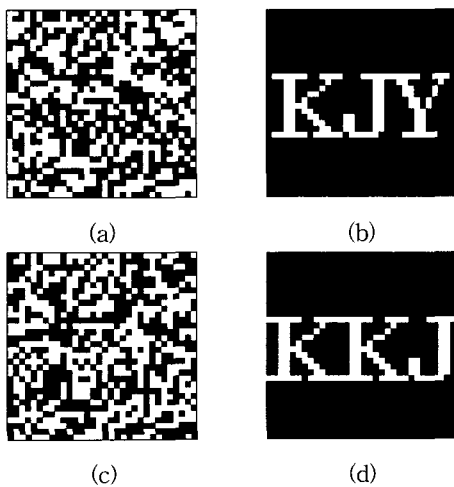


(c)

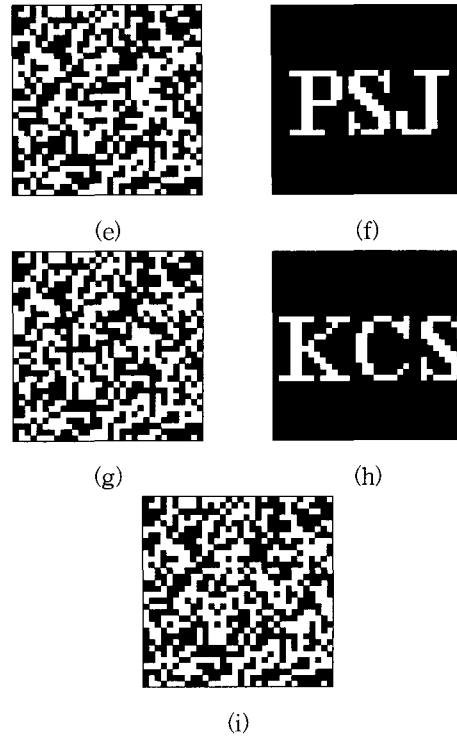
그림 3. 암호 영상 생성

Fig. 3. The generation of encrypted image:

- (a) Reference image;
- (b) original image;
- (c) encrypted image.



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



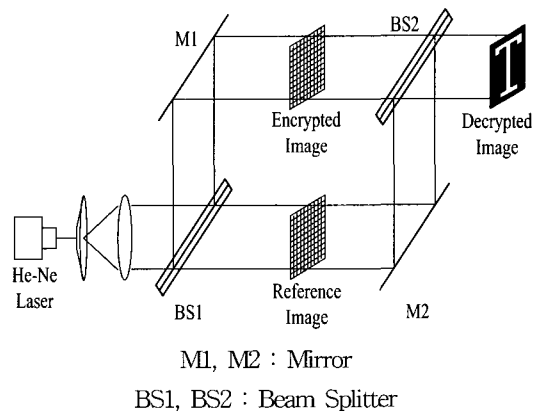
(e) (f) (g) (h) (i)

그림 4. 동일한 (a)기준 영상에 대한 다양한 원 영상들 (b), (d), (f) 및 (h)와 이들의 암호 영상 (c), (e), (g), 그리고 (i)

Fig. 4. Various original images (b), (d), (f), and (h) and their encrypted images (c), (e), (g), and (i) to the same reference image (a).

3. 영상 복원 시스템

암호화된 두 개의 위상 카드로 원 영상을 복원하기 위한 영상 복원 시스템 구성도는 그림 5에서와 같이 마흐-젠더 간섭계와 그 구조가 유사하다. 기준 영상을



ML, M2 : Mirror

BS1, BS2 : Beam Splitter

그림 5. 제안한 영상 암호화 시스템

Fig. 5. The proposed image security system.

마호-젠더 간섭계의 두 경로 중 한 경로에 두고 원 영상에 따른 암호 영상을 경로차가 같은 다른 하나의 경로에 두면 원 영상을 복원할 수 있다.

IV. 광실험 및 고찰

광학적 실험에서는 먼저 기준 영상과 암호 영상에 대한 위상 마스크를 컴퓨터와 광 리소그래피를 이용해 제작한 후, 이들을 마호-젠더 간섭계를 이용한 광 시스템에 사용하여 영상을 복원하였다.

1. 위상 마스크 제작

영상 암호화를 위해서는 위상 마스크 형태로 사용되는 기준 영상과 암호 영상의 정확한 제작이 중요하다. 본 논문에서는 그림 3(b)와 같은 영문자 'T'를 원 영상으로 사용하였고, 컴퓨터를 이용하여 구한 원 영상에 대한 기준 영상과 암호 영상은 각각 그림 3(a) 및 3(c)와 같다. 그리고 기준 영상과 암호 영상에서 위상값이 '0'인 부분은 흰색으로, 위상값이 ' π '인 부분은 검은색으로 대치한 이진 영상 패턴을 구한다. 그림 3(a)와 3(c)의 영상에 대한 이진 영상의 패턴은 각각 그림 6(a)와 6(b)와 같다. 기준 영상과 암호 영상에 대한 이진 영상 패턴들을 플로터(plotter)로 그린 후 축소하여 마스크를 제작하였다.

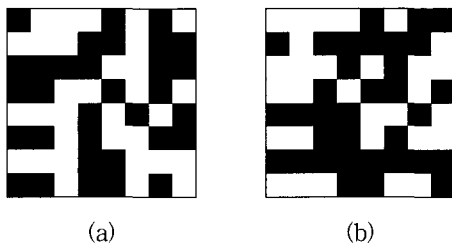


그림 6. 'T'자에 대한 마스크 패턴
(a) 기준 영상 패턴 (b) 암호 영상 패턴
Fig. 6. Mask Patterns for 'T': (a) Reference image pattern; (b) encrypted image pattern.

제작한 8×8 마스크의 전체 크기는 1.6×1.6 cm²이고 한 화소의 크기는 2×2 mm²이다. 이렇게 제작된 마스크 아래에 PR(photoresistor)을 바른 일반 유리판을 놓고 빛을 쬐어 주면 마스크의 π 부분의 패턴에 해당하는 부분의 PR만을 제거할 수 있다. 이를 BHF(buffered hydrofluoric acid)용액에 담그어 PR이 없는 부분을 화학적 식각을 통하여 유리판의 두께를 제어하였으며, 그

두께는

$$D = \frac{\lambda\phi}{2\pi(n-1)} \quad (4)$$

과 같다. 여기서 D는 식각하고자 하는 유리판의 두께이고, λ 는 사용 레이저(He-Ne)의 파장이며, n은 유리판의 굴절률이다. 그리고 ϕ 는 제어하고자 하는 위상을 나타내며, 본 실험에서는 λ 는 632.8nm, n은 1.52를 사용하였다. 또한 위상 마스크 제작시 식각 두께의 오차를 줄이기 위해 $\phi=5\pi$ 로 하여

$$D = \frac{632.8 \times 10^{-9} \times 5\pi}{2\pi(1.52-1)} \approx 3.0423\mu\text{m} \quad (5)$$

가 되도록 하였다. BHF 용액의 일반 유리 식각률은 용액에 담그어 놓는 시간에 따라 10초당 0.1 μm 로 측정되었고, 여러 번의 실험을 거쳐 계측기(α -step)로 식각 두께를 측정하면서 오차를 줄여 나갔다. 식각을 끝낸 후 유리판에 남아있는 PR을 다시 빛을 쬐어 제거하여 완전한 위상 마스크를 제작하였다.

2. 실험 구성도

제안한 방법을 이용하여 원 영상을 복원하기 위한 광 실험 구성도는 그림 7과 같다. 먼저 마호-젠더 간섭계의 경로차를 같게 하기 위하여 간섭무늬가 나타나지 않도록 간섭계를 구성하여 간섭영상이 그림 8(b)와 같은 패턴이 나오도록 하였다. 그림 8(a)는 간섭계를 정렬하기 위해 하나의 경로를 막고 다른 하나의 경로에

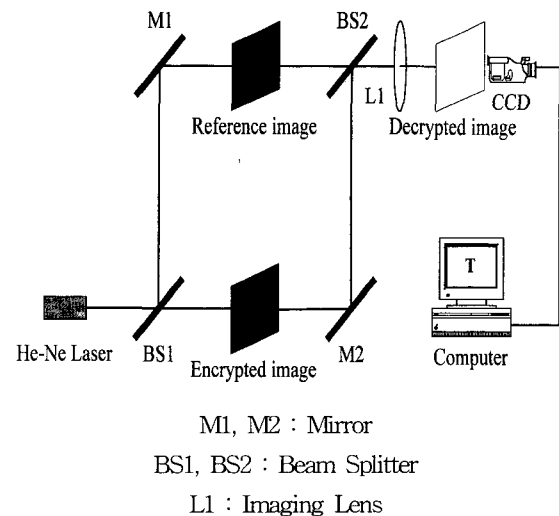


그림 7. 광학적 영상 암호화 시스템
Fig. 7. Optical image security system.

의한 평면파의 영상이고, 그림 8(b)는 경로차가 동일하게 간섭계를 정렬한 후 두 경로를 따라 보강간섭된 평면파의 영상이다. 그리고 난 후 위상차가 동일한 두 경로에 제작된 기준 영상과 암호 영상을 각각 놓아서 이들을 간섭시켜 원 영상을 재생하였다. 이때 기준 영상과 암호 영상의 위상차가 π 의 홀수배만큼 나는 화소에서의 간섭의 세기는 최소가 되고, 2π 배가 나는 화소의 간섭 세기는 최대가 된다.

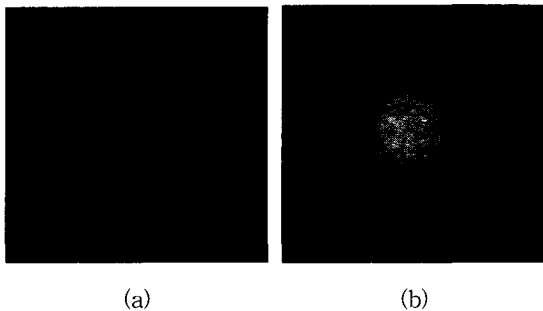


그림 8. 경로차가 같은 두 빛의 간섭
(a) 하나의 경로 광의 세기 (b) 두 빛의 간섭 광의 세기
Fig. 8. The interference of two beams with same path: (a) Intensity of one path; (b) intensity of two beams interference.

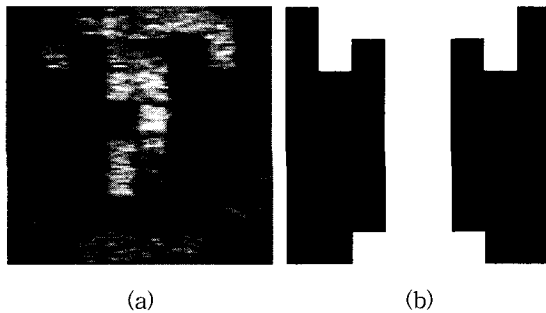


그림 9. 실험 영상과 이론적 영상의 비교:
(a) 광 실험 결과 영상; (b) 이론적 결과 영상
Fig. 9. The comparison of experimental image and original image:
(a) Experimental image; (b) original image.

그림 3(a)의 기준 영상과 그림 3(c)의 암호 영상에 대한 위상 마스크를 그림 7의 시스템에서 경로차가 동일한 광경로에 놓은 후 CCD 카메라로 얻은 간섭 영상은 그림 9에서와 같다. 그림 9에서 광 실험 결과와 그림 3(b)의 원 영상을 비교하면 오차 영역이 있음을 볼 수 있는데 이는 위상 마스크 제작시 식각되어진 두께

의 오차, 식각된 표면의 불균일성, 그리고 간섭계에서의 진동 등의 외부 잡음과 경로치의 오차 등에 의한 것이다.

더 발전된 리소그래피 기술을 이용하여 정확한 두께를 가지는 위상 마스크를 제작할 수 있고, 경로차가 정확히 같고 외부 잡음의 영향이 없는 마흐-젠더 간섭계를 구성한다면 원하는 결과와의 오차를 줄일 수 있을 것이다. 그리고 위상 마스크의 두께를 256 레벨로 제어할 수 있다면 그레이 레벨 영상에 대한 암호화도 구현할 수 있을 것이다.

VI. 결 론

본 논문에서는 광 리소그래피로 만든 두 개의 위상 마스크와 마흐-젠더 간섭계를 이용하여 원 영상이 랜덤한 기준 영상에 대한 암호 영상으로 변환되는 새로운 광학적 이진 영상 암호화 방법을 제안하였다. 0 과 π 의 위상값을 가지는 랜덤한 기준 영상과 파의 간섭 원리를 기초로 제안한 암호 규칙에 따라 암호 영상을 생성하였다. 그리고 기준 영상과 암호 영상을 경로차가 같은 마흐-젠더 간섭계의 두 개의 경로에 각각 놓아서 이들을 통과하는 두 빛의 간섭 패턴을 CCD 카메라로 획득함으로써 원 영상을 복원하였다.

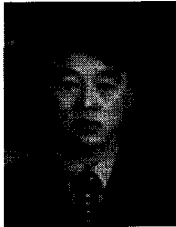
두 개의 위상 마스크는 일반 유리판을 화학적 식각을 통해 각 화소의 위상을 제어하였으며 광학적 실험을 통해 제안한 방법이 유효함을 확인하였다. 이러한 광학적 영상 암호화 방법에서 하나의 기준 영상으로 여러 개의 원 영상에 대한 암호 영상을 각각 만들고, 제안한 암호화 시스템을 광상관기와 결합시켜 사용하면 개인 인증 시스템에도 응용이 가능하다. 또한 제안한 방법은 그레이 레벨 영상에 대한 암호화 시스템에 적용 가능하다.

참 고 문 헌

- [1] J. W. Han, C. S. Park, D. H. Ryu, and E. S. Kim, "Optical image encryption based on XOR operations," *Optical Engineering*, vol. 38, no. 1, pp. 47-54, 1999.
- [2] P. Stepień, R. Gajda, and T. Szoplík, "Distributed kinoforms in optical security applications," *Optical Engineering*, vol. 35, no.

- 9, pp. 2453-2458, 1996.
- [3] J. Y. Kim, S. G. Park, J. W. Kim, Y. H. Doh, and S. J. Kim, "Image encryption and identification using computer generated hologram," *Proceedings of ITC-CSCC'99*, vol. 1, pp. 537-540, 1999.
- [4] L. G. Neto, "Implementation of image encryption using the phase-contrast technique," *Proceedings of SPIE*, vol. 3386, pp. 284-290, 1998.
- [5] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 32, no. 7, pp. 767-769, 1995.
- [6] 서울대학교 광학연구회, *현대광학*, 교문사, 1997
- [7] E. Hecht, *OPTICS*, Addison-Wesley, 1997.

저 자 소 개



金鍾允(正會員)

1971년 10월 11일생. 1995년 2월 경북대학교 전자공학과 졸업(공학사). 1997년 2월 경북대학교 대학원 전자공학과 졸업(공학석사). 2001년 2월 경북대학교 대학원 전자공학과 졸업예정(공학박사). 주관심분야는 광 보

안, 광 패턴인식, 홀로그램 및 광메모리



金杞貞(正會員)

1974년 9월 21일생. 1998년 2월 경북대학교 전자공학과 졸업(공학사). 2000년 2월 경북대학교 대학원 전자공학과 졸업(공학석사). 2000년 1월~현재 삼성중공업 조선플랜트 연구소 연구원. 주관심분야는 광 보안,

광 패턴인식, 컴퓨터형성홀로그램

朴世駿(正會員) 第 36券 T編 第 1號 參照
현재 경북대학교 대학원 전자공학과 박사과정 재학중

金喆洙(正會員) 第 36券D編 第 9號 參照
현재 경주대학교 컴퓨터·전자공학부 전임강사

裴長根(正會員) 第 36券 T編 第 1號 參照
현재 구미1대학 전자정보과 조교수

金正雨(正會員) 第 35券D編 第 3號 參照
현재 동양대학교 전자공학부 조교수

金秀重(正會員) 第 37券 SD編 第 8號 參照
현재 경북대학교 전자전기공학부 정교수