

논문 2004-41SD-11-7

# 컴퓨터 홀로그래피와 프레넬 회절을 이용한 위상 영상 광 암호화 시스템

(Fully Phase-based Optical Encryption System Using Computer  
Holography and Fresnel Diffraction)

윤 경 효\*, 신 창 목\*\*, 조 규 보\*\*, 김 수 중\*\*, 김 철 수\*\*\*, 서 동 환\*\*\*\*

(Kyung-Hyo Yoon, Chang-Mok Shin, Kyu-Bo Cho, Soo-Joong Kim,  
Cheol-Soo Kim, and Dong-Hoan Seo)

## 요 약

본 논문에서는 원 영상의 컴퓨터 생성 홀로그램(computer generated hologram; CGH) 패턴을 위상 변조한 후, 위상 부호화한 무작위 키 영상들의 프레넬 회절(Fresnel diffraction) 위상 패턴과 곱하여 암호화함으로써 외부 교란이나 절단에 강하고, 암호화 수준이 높은 광 암호화 방법을 제안하였다. 암호화시 원 영상의 이진 CGH패턴을 위상 변조한 후, 이를 위상 키 영상들의 프레넬 회절 공역 위상정보와 곱하며, 복호화시 암호화 영상에 위상 키 영상들의 프레넬 회절 위상 정보를 다시 곱한 후 푸리에 변화시켜 원 영상 정보를 얻는다. 암호화 영상은 CGH 패턴 특성을 가지므로, 절단이나 외부 잡음에 강하며 프레넬 회절 정보를 이용하여 암호화함으로써 높은 암호화 수준을 가진다. 컴퓨터 모의 실험을 통해 제안한 방법의 타당성을 확인하였으며 절단과 잡음에 대한 영향을 분석하였고, 위상 변조 특성이 있는 LCD를 사용하여 광학적으로 구현하였다.

## Abstract

In this paper, we propose a high-level optical encryption system, which is tolerant with noises and cropping, by encrypting the phase-encoded CGH pattern of original image with the phase-encoded Fresnel diffraction pattern of random key images. For encryption, the phase-encoded CGH pattern of original image is multiplied by conjugate components which are the phase-encoded Fresnel diffraction patterns of random key images. The original information can be reconstructed by multiplying encrypted image by phase-encoded Fresnel diffraction pattern of random key images and performing Fourier transform of the multiplication result. The proposed system is robust to noises and cropping due to characteristics of CGH pattern and can guarantee high-level encryption by using Fresnel diffraction information. We verified the validity of proposed system by computer simulations, numerical analysis of noises and cropping effect and optical experiment.

**Keywords :** 광 암호화(optical security), 컴퓨터 홀로그래피(computer holography), 프레넬 회절(Fresnel diffraction)

\* 정회원, LG전자 디지털 영상사업부 영상제품연구소  
(Display Product Research Lab, LG Electronics Inc.)

\*\* 정회원, 경북대학교 전자전기컴퓨터공학부  
(Optical Signal Processing Lab, School of  
Electrical Engineering and Computer Science,  
Kyungpook Nat'l University)

\*\*\* 정회원, 경주대학교 컴퓨터전자공학부  
(School of Computer & Electronic Engineering,  
Kyongju University)

\*\*\*\* 정회원, 한국해양대학교 전기전자공학부  
(Division of Electrical and Electronics Engineering,  
Korea Maritime University)

접수일자: 2004년2월 일, 수정완료일: 2004년10월18일

## I. 서 론

현대사회는 정보화 사회이며 이에 따라 개인의 신원을 확인할 수 있는 신분증의 사용이 늘어나고 있다. 신분증의 위조 여부를 확인하기 위한 수단으로 사진, 얼굴, 지문 등이 사용되고 있으나 기술의 발달은 위조 및 복제를 가능하게 하였고, 각종 범죄의 수단으로 사용되어 국내외적으로 심각한 사회 문제로 대두되고 있다. 따라서 전 세계적으로 복제나 위조 방지에 관한 연구와

여러 가지 암호화 시스템 개발에 대한 연구가 활발히 진행되고 있다. 최근에는 CCD와 같은 기존의 세기 검출기로는 볼 수도 복제할 수도 없는 복소 함수 형태의 무작위 위상 마스크를 사용하는 광학적 보안 기법이 제시되고 있다<sup>[1-8]</sup>.

그러나 이러한 시스템에서 암호화된 영상은 진폭과 위상의 복소 함수이므로 암호화된 영상을 저장하기 위해서는 간섭을 이용하여 홀로그램 형태로 저장해야 한다. 간섭 현상은 진동이나 공기의 흐름, 온도의 차이 등에 의한 외부 교란에 쉽게 영향을 받기 때문에 정밀한 시스템이 요구된다<sup>[4,5]</sup>. 암호화된 영상을 홀로그램을 사용하지 않고 저장하기 위해서는 암호화된 영상이 진폭 또는 위상 정보만으로 구성되어야 하며 암호화 수준을 높이고 잡음의 영향을 줄이기 위해서 위상 정보만으로 구성되어야 한다. 그러나 키 영상과 암호화된 영상이 모두 위상만의 정보라고 하더라도 암호화와 복호화 과정에서 진폭성분이 생성되기 때문에 진폭성분과 위상성분을 분리해야 한다. 그리고 원 영상을 위상 변조하여 암호화하는 방법<sup>[2,4-6]</sup>에서는 복호된 영상이 위상만의 함수이므로 간섭계 등을 이용한 위상측정방법(phase measurement technique)으로 위상 정보를 진폭 정보로 변환해야 진위 여부를 판별할 수 있기 때문에 외부 교란에 약하며, 위상 연속화(phase unwrapping)가 필요하기 때문에 오차가 수반한다. Mogensen 등이 제안한 위상 암호화 방법<sup>[6]</sup>은 두 개의 위상 변조기를 이용하여 복원 영상의 위상정보를 얻고 위상 대조차 여파기(phase-contrast filter)를 사용하여 위상정보를 진폭 정보로 변환하여 원 영상을 복원하기 때문에 위상측정방법을 이용하지 않으나 복호화 과정에서 위상 대조차 방법이 사용되어야하고, 암호화된 영상이나 키 영상이 절단되었을 때 정확한 원 영상을 복호화할 수 없다.

따라서 본 논문에서는 원 영상의 컴퓨터 형성 홀로그램을 위상 변조한 후 암호화에 이용함으로써 외부교란이나 절단에 강하고 위상 정보를 진폭 정보로 변환할 필요가 없으며 암호화된 영상의 저장이 간편한 암호화 방법을 제안하였다. 그리고 암호화 수준을 높이고 잡음에 강한 시스템을 위해 무작위 위상 키의 자유 공간 이동에 따른 프레넬 회절 패턴의 위상 정보만을 이용한 시스템을 제안하였다. 홀로그래피의 기록과 복원의 2단계 과정 중에서 어느 한 단계라도 디지털로 이루어지면 컴퓨터 홀로그래피(computer holography)라고 한다<sup>[7]</sup>. 제안한 시스템은 CGH와 디지털 홀로그래피(digital holography)를 이용하였다. 원 영상을 컴퓨터 형성 홀

로그램으로 변환하여 위상 변조한 영상을 암호화에 이용한다면 복호화된 영상이 위상 변조된 CGH이기 때문에 푸리에 변환을 하게 되면 진폭성분은 영차(zero-order)에 위치하게 되고 위상 변조된 CGH는 1차(first-order)에 위치하게 된다. 따라서 진폭성분과 위상성분이 분리될 수 있고 원 영상이 1차 위치에 나타나게 되므로<sup>[8]</sup> 위상을 진폭 정보로 변환할 필요가 없다. 디지털 홀로그래피의 기록과 재생 과정을 이용한다면 진폭 정보를 수치적으로 제거할 수 있어 영상의 해상도를 향상시킬 수 있다. 그리고 CGH의 특성으로 인하여 암호화된 영상이 절단되었을 때에도 원 영상을 재생시킬 수 있고 원 영상의 위상 변조된 CGH를 암호화에 이용했기 때문에 이진 무작위 영상에 준 하는 영상을 암호화한 것과 같은 효과가 있다. 그리고 어떤 영상이 자유 공간상에서 일정거리 만큼 전파된다면 프레넬 회절 현상이 나타난다<sup>[9]</sup>. 따라서 거리 정보를 영상 암호화에 이용하면 암호화 수준을 높일 수 있다<sup>[10]</sup>. 두 개의 키에 의한 프레넬 회절 패턴의 위상 성분을 복소공역을 취한 후 위상 변조된 CGH와 곱하여 암호화된 영상을 얻었다. 복호화 과정은 키 영상과 암호화된 영상간의 일정한 거리를 유지하여 생성된 정보를 푸리에 변환하여 원 영상을 복원하였다.

## II. 제안한 암호화 및 복호화 방법

### 1. 암호화 방법

원 영상  $f(\xi, \eta)$ 를 이진 CGH 패턴  $h_{cgh}(x, y)$ 로 생성하여 위상 변조하고, 컴퓨터로 발생시킨 무작위 키 영상  $r_1(x, y), r_2(x, y)$ 을 위상 변조하여 두 개의 키 영상을 구한다. 이때  $h_{cgh}(x, y)$ 는 0과 1의 값을 가지며,  $r_1(x, y), r_2(x, y)$ 는 [0, 1]의 값을 가진다. 위상 변조된 각각의 영상  $h_p(x, y), k_1(x, y), k_2(x, y)$ 는

$$\begin{aligned} h_p(x, y) &= \exp[j\pi h_{cgh}(x, y)] \\ k_1(x, y) &= \exp[j2\pi r_1(x, y)] \\ k_2(x, y) &= \exp[j2\pi r_2(x, y)] \end{aligned} \quad (1)$$

와 같이 표현된다. 위상 변조된 영상의 세기는 다음과 같이 세기가 '1'인 값을 가지므로 세기검출기나 인간의 시각으로는 복사나 구별이 불가능하다.

$$|h_p(x, y)|^2 = |k_1(x, y)|^2 = |k_2(x, y)|^2 = 1 \quad (2)$$

암호화 과정은 먼저 위상 키 영상  $k_1(x, y)$ 와  $k_2(x, y)$ 를 각각 서로 다른 일정한 거리  $d_1$ 과  $d_2$ 만큼 프레넬 회절시켜 복소함수  $k_{fre_1}(x, y)$ 와  $k_{fre_2}(x, y)$ 를 구한다. 그리고 각각을 복소공액한 함수들과 위상 변조된 CGH 영상  $h_p(x, y)$ 를 곱한다. 여기서 생성된 복소함수에서 위상 정보를 취하여 암호화된 영상  $e(x, y)$ 를 구한다.

어떤 영상이 다음 그림 1과 같이 자유공간에서 일정 거리만큼 전파한다면 프레넬 회절 패턴은

$$\begin{aligned} k_{fre}(x, y) &= A_k(x, y) \exp[j\phi_k(x, y)] \\ &= k(x, y) \otimes h(x, y; z) \\ &= k(x, y) \otimes \frac{\exp[jkz]}{j\lambda z} \exp\left[\frac{jk}{2z}(x^2 + y^2)\right] \end{aligned} \quad (3)$$

와 같고, 여기서  $A_k(x, y)$ 는 회절 패턴의 진폭,  $\phi_k(x, y)$ 는 위상,  $z$ 는 거리 정보,  $h(x, y; z)$ 는 프레넬 회절의 컨볼루션 핵(convolution kernel),  $\otimes$ 는 컨볼루션 연산자를 나타낸다<sup>[9]</sup>.

따라서 두 개의 위상 키에 의한 프레넬 회절 정보의 공액과 위상 변조된 CGH의 곱은

$$\begin{aligned} \tilde{e}(x, y) &= \{ [k_1(x, y) \otimes h(x, y; d_1)] \\ &\quad \times [k_2(x, y) \otimes h(x, y; d_2)] \}^* h_p(x, y) \\ &= \{ k_{fre_1}(x, y) k_{fre_2}(x, y) \}^* h_p(x, y) \\ &= A_{k_1}(x, y) A_{k_2}(x, y) \\ &\quad \times \exp[-j\{\phi_{k_1}(x, y) + \phi_{k_2}(x, y)\}] h_p(x, y) \\ &= A_k(x, y) \exp[j\pi h(x, y) - \phi_k(x, y)] \end{aligned} \quad (4)$$

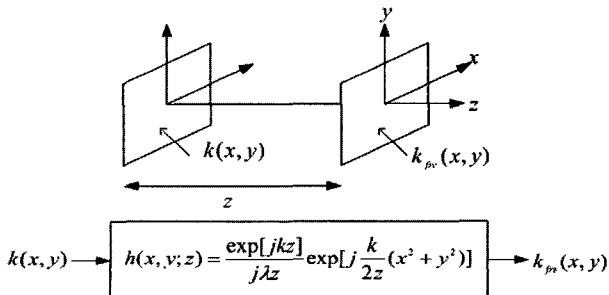


그림 1. 자유 공간 이동에 따른 프레넬 회절  
Fig. 1. Fresnel diffraction of the free space propagation.

와 같이 표현되며, 기호 \*는 복소공액(conjugate)을 나타낸다. 식 (4)에서  $A_k$ 는  $A_{k_1}A_{k_2}$ 를,  $\phi_k$ 는  $\phi_{k_1} + \phi_{k_2}$ 를 나타낸다. 위상 정보만으로 이루어진 암호화된 영상  $e(x, y)$ 는

$$\begin{aligned} e(x, y) &= \frac{1}{|A_k(x, y)|} \tilde{e}(x, y) \\ &= \exp[j\{\pi h(x, y) - \phi_k(x, y)\}] \end{aligned} \quad (5)$$

와 같이 표현되며, 그림 2에 블록 다이어그램으로 암호화 과정을 나타내었다.

### 2. 복호화 방법

암호화된 영상은 그림 3과 같은 시스템을 통하여 두 개의 키 영상, 정확한 거리 정보와 순서를 알고 있을 경우에만 원 영상에 대한 CGH의 위상 성분을 복원할 수 있고, 이를 푸리에 변환하여 원 영상을 재생할 수 있다.

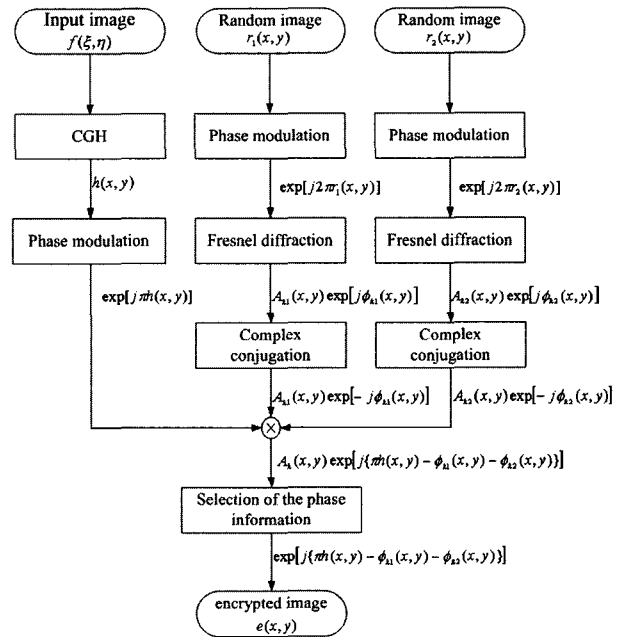


그림 2. 제안한 암호화 방법의 블록 다이어그램  
Fig. 2. The block diagram of proposed encryption method.

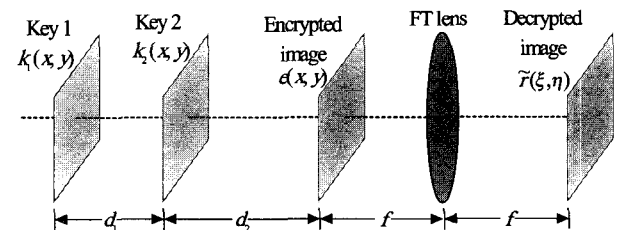


그림 3. 복호화 시스템  
Fig. 3. Decrypting system.

복호화된 정보는

$$\begin{aligned} \tilde{d}(x, y) &= [k_1(x, y) \otimes h(x, y, d_1)] \\ &\quad \times [k_2(x, y) \otimes h(x, y, d_2)] e(x, y) \\ &= A_k(x, y) \exp[j\phi_k(x, y)] \\ &\quad \times \exp[j\{\pi h(x, y) - \phi_k(x, y)\}] \\ &= A_k(x, y) \exp[j\pi h(x, y)] \end{aligned} \tag{6}$$

와 같다. 이 정보를 푸리에 변환하면

$$\begin{aligned} \tilde{r}(\xi, \eta) &= \mathcal{T}\{\tilde{d}(x, y)\} \\ &= \mathcal{T}\{A_k(x, y)\} \otimes \mathcal{T}\{\exp[j\pi h(x, y)]\} \end{aligned} \tag{7}$$

와 같다. 여기서 재생된 영상은 위상 키들의 프레넬 회절 패턴에 의한 진폭성분이 푸리에 변환된 성분과 재생된 원 영상이 함께 나타나게 된다. 그러나 본 논문에서는 1차 위치에서만 원 영상이 재생되도록 SA 알고리즘을 이용한 비축 홀로그램 형태의 CGH를 설계하고, 원 영상 재생 시 영차성분 즉 DC성분의 영향을 최소화하기 위해 CGH를 위상 변조하였기 때문에 CGH에 의한 재생 영상은 식 (8)과 같이 Zernike의 위상차 기술(phase contrast technique)의 수학적 근사화 방법[9]을 이용해 근사화하여 표현할 수 있다.

$$\begin{aligned} &\mathcal{T}\{\exp[j\pi h(x, y)]\} \\ &= \mathcal{T}\left\{1 + j[\pi h(x, y)] - \frac{1}{2!}[\pi h(x, y)]^2 \right. \\ &\quad \left. - \frac{j}{3!}[\pi h(x, y)]^3 + \dots\right\} \\ &\approx \mathcal{T}[1 + j\pi h(x, y)] \\ &\approx j\pi \mathcal{T}[h(x, y)] \\ &\approx j\pi [f(\xi - \xi_0, \eta - \eta_0) + f(-\xi - \xi_0, -\eta - \eta_0)] \end{aligned} \tag{8}$$

이 때  $\xi_0$ 와  $\eta_0$ 는 CGH 생성시 원 영상의 위치를 나타낸다.

$\exp(j\pi)$  함수로 위상 변조된 CGH의 화소값은 1 또는 -1로서, 전 영역에 고르게 분포하므로 식 (9)와 같이 전 영역의 대한 적분값은 0으로 근사화된다.

$$\int \int \exp[j\pi h(x, y)] dx dy = 0 \tag{9}$$

이는 위상 변조된 CGH의 재생 영상의 영차 성분이 억제되는 것을 의미하므로 위상 변조된 CGH의 재생 영상은 회절 효율이 향상된다. 이때 진폭 정보  $A_k(x, y)$ 는 푸리에 변환되어 저주파 영역으로 모이게 되고 강한 영차 성분을 가지게 되므로 CGH가 재생될 1차 위치와는 중첩되지 않는다<sup>[8]</sup>.

그러나 진폭 정보는 1차 위치에서 재생 영상에 잡음으로 작용하기 때문에 재생된 원 영상의 해상도는 낮아진다. 그러므로 진폭성분은 원 영상에 잡음으로 작용하므로 이를 제거할 필요가 있다. 디지털 홀로그래피는 어떤 파의 위상과 진폭을 기록하고 수치적으로 복원하기 때문에 그림 4와 같이 디지털 홀로그래피 기록과 재생 과정을 복호화 과정에 추가하면 진폭 성분을 수치적으로 제거할 수 있고, 위상 잡음에 의한 위상 왜곡을 감소시킬 수 있다. 위상천이 디지털 홀로그래피는 마흐젠더(Mach-Zehnder) 간섭계 구조로 이루어져 있다<sup>[11]</sup>.

물체의 복소 진폭 분포  $U_0(x, y; z)$ 는 프레넬 회절되어 CCD 평면에서 참조파와 간섭한다. 물체와 거리  $z$ 만큼 떨어져 있는 CCD 평면에서의 프레넬 회절 패턴은

$$\begin{aligned} H_o(x', y') &= A_H(x', y') \exp[j\phi_H(x', y')] \\ &= \frac{1}{j\lambda} \iiint_{-\infty}^{\infty} U_o(x, y, z) \frac{1}{z} \exp(j\frac{2\pi}{\lambda} z) \\ &\quad \times \exp\left\{j\frac{\pi}{\lambda z} [(x'-x)^2 + (y'-y)^2]\right\} dx dy dz \end{aligned} \tag{10}$$

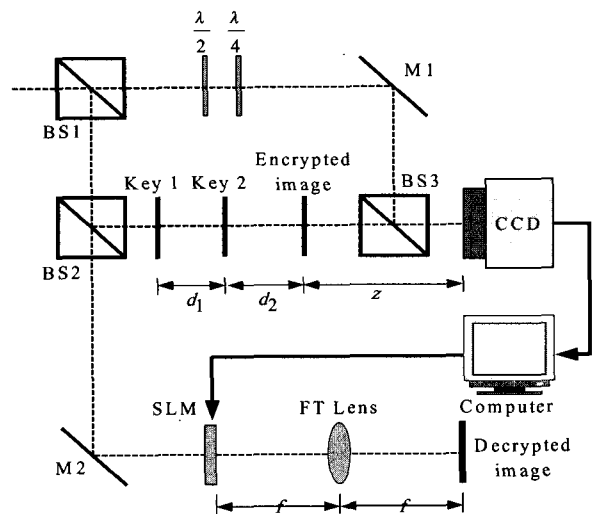


그림 4. 디지털 홀로그래피 방법을 이용한 복호화 시스템  
Fig. 4. Decrypting system using digital holography method.

으로 기록되고 참조파에 의해 생성되는 복소필드는

$$R(x', y' ; \alpha) = A_R(x', y') \exp\{j[\psi(x', y') + \alpha]\} \quad (11)$$

이다. 여기서  $A_R(x', y')$ 은 일정한 진폭,  $\psi(x', y')$ 는 두 위상지연기의 빠른 축(fast axis)이 편광방향에 일직선일 때의 일정한 위상,  $\alpha$ 는 위상천이를 나타내는 인자이다.  $\alpha$ 는 두 위상지연기의 빠른 축(fast axis)과 느린 축(slow axis)을 적절히 배열함으로써  $A_R(x', y')$ 는 바꾸지 않으면서 위상천이를  $\alpha = 0, \pi/2, \pi, 3\pi/2$ 가 되게 한다. 식 (10)과 식 (11)을 사용한 4개의 간섭패턴  $I(x', y' ; \alpha)$ 는

$$I(x', y' ; \alpha) = H_o(x', y') + R(x', y' ; \alpha)^2 \quad (12)$$

이다. 위 식의 4개의 간섭패턴으로부터 다음 식 (13)와 식 (14)을 이용하여 프레넬 회절 패턴  $H_o(x', y')$ 의 위상과 진폭을 구하고, 이를 역 프레넬 회절 적분을 취하면 물체 파를 재생할 수 있다.

$$\begin{aligned} & \phi_H(x', y') - \psi \\ &= \tan^{-1} \frac{I(x', y'; -3\pi/2) - I(x', y'; -\pi/2)}{I(x', y'; 0) - I(x', y'; -\pi)} \end{aligned} \quad (13)$$

$$A_H(x', y') A_R = \frac{1}{4} \frac{I(x', y'; 0) - I(x', y'; -\pi)}{\cos[\phi_H(x', y') - \psi]} \quad (14)$$

여기서  $\psi$ 와  $A_R$ 은 일정한 인자이므로 각각 0과 1로 둔다. 또한 디지털 홀로그래피는 기록 평면인 CCD평면과 기록할 정보와의 거리가 재생과정의 역 프레넬 회절 적분의 거리 인자와 동일해야 기록한 정보를 정확하게 재생할 수 있으므로 암호화 수준을 높일 수 있다. 따라서 식 (10)에서 구한 복호화된 영상이 일정거리  $z$ 만큼 프레넬 회절된 패턴은 식 (10)과 같고, 식 (13)과 식 (14)을 이용하여 복호화된 영상의 프레넬 회절 패턴의 진폭과 위상 성분을 수치적으로 구할 수 있다. 따라서 프레넬 회절 패턴을 다음 식 (15)를 이용하여 역 프레넬 회절 적분을 취하면 식 (6)을 수치적으로 구할 수 있고 다음 식 (16)을 이용하여 수치적으로 진폭 성분을 제거하여 위상 성분을 구할 수 있다.

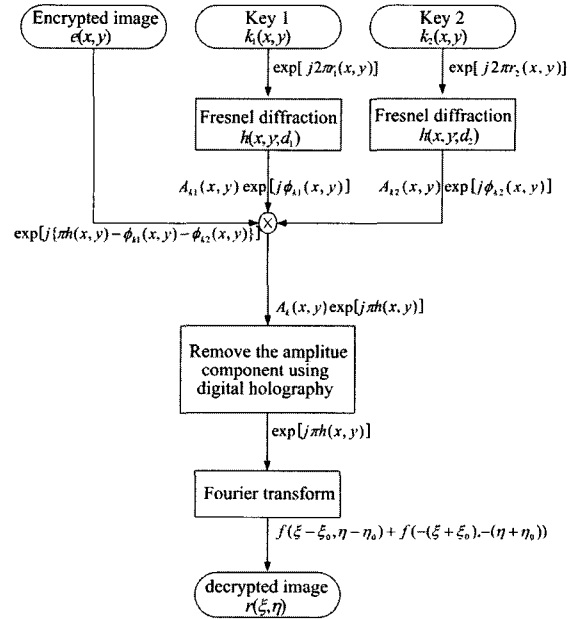


그림 5. 제안한 복호화 방법의 블록 다이어그램  
Fig. 5. The block diagram of the proposed decryption method.

$$\begin{aligned} & \tilde{d}(x, y) \\ &= -\frac{1}{j\lambda} \iint_{-\infty}^{\infty} H_o(x', y') \frac{1}{z} \exp(-j\frac{2\pi}{\lambda}z) \end{aligned} \quad (15)$$

$$\begin{aligned} & \times \exp\left\{-j\frac{\pi}{\lambda z} [(x-x')^2 + (y-y')^2]\right\} dx' dy \\ & A_k(x, y) = \sqrt{[\text{Re}\{\tilde{d}(x, y)\}]^2 + [\text{Im}\{\tilde{d}(x, y)\}]^2} \quad (16) \\ & \phi_k(x, y) = \text{atan}[\text{Im}\{\tilde{d}(x, y)\} / \text{Re}\{\tilde{d}\}] \end{aligned}$$

디지털 홀로그래피 방법을 이용하여 구한 위상 성분을 공간 광 변조기를 사용하여 푸리에 변환하면 재생된 원 영상은

$$\begin{aligned} & r(\xi, \eta) \\ &= \mathcal{J}\left\{\frac{1}{A_k(x, y)} \tilde{d}(x, y)\right\} \quad (17) \\ &= \mathcal{J}\{\exp[j\pi h(x, y)]\} \\ &\approx j[f(\xi - \xi_0, \eta - \eta_0) + f(-\xi - \xi_0, -\eta - \eta_0)] \end{aligned}$$

와 같이 나타나게 된다. 제안한 복호화 과정은 그림 5의 블록 다이어그램과 같다.

### III. 컴퓨터 모의 실험 결과 및 고찰

1. SA 알고리즘을 이용한 컴퓨터 형성 홀로그램  
본 논문에서는 SA(simulated annealing) 알고리즘을 이용하여 CGH를 설계 및 제작하였다. SA 알고리즘을

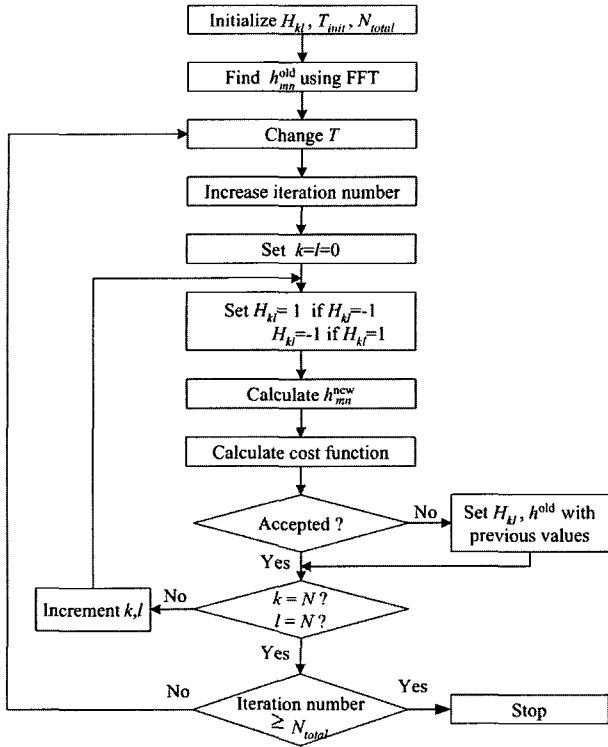


그림 6. 이진 위상 홀로그램의 설계를 위한 SA 알고리즘의 순서도  
 Fig. 6. Flowchart for generation of binary phase hologram using SA algorithm.

이용하여 제작한 CGH는 다른 CGH 제작 방법에 비해 제작 시간은 다소 오래 걸리지만, 회절효율이 높아 원래 영상을 충실히 재생할 수 있다<sup>[12]</sup>. 생성하려는 원 영상 함수  $h(x,y)$ 는 SA 알고리즘을 통해 설계된 위상 홀로그램  $H(u,v)$ 를 푸리에 변환함으로써 얻을 수 있으며 각 함수는  $N \times N$  화소로 구성되어 있다. 이들의 이산적인 표현은

$$h_{mn} = \frac{1}{N^2} \sum_{k=-N/2}^{N/2-1} \sum_{l=-N/2}^{N/2-1} H_{kl} \exp j2\pi \left( \frac{km}{N} + \frac{ln}{N} \right) \quad (18)$$

과 같고, 여기서  $H_{kl}$ 은  $H(u, v)$ 의  $(k,l)$ 번째 표본 값이며  $h_{mn}$ 은  $h(x,y)$ 의  $(m,n)$ 번째 표본의 값이다. 이진 위상 홀로그램의 최적 설계를 위한 SA 알고리즘의 순서도는 그림 6과 같다.

원 영상을 이용하여 CGH를 생성하기 위해 그림 7(a)와 같이 128×128픽셀 크기의 그레이(gray) 레벨 'Lena' 영상을 256×256 픽셀 크기의 홀로그램 평면에  $\xi_0, \eta_0$ 만큼 이동시켜 비축 홀로그램이 되도록 배치하였다. 그림 7(b)는 원 영상의 CGH를 나타내며, 그림 7(c)는 CGH를 재생한 영상을 나타낸다.

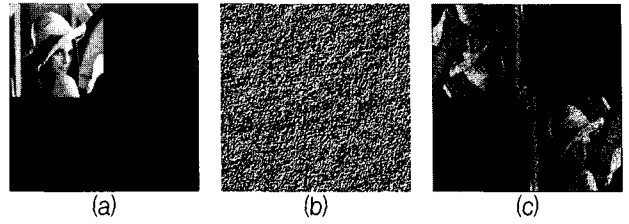


그림 7. SA 알고리즘을 이용한 CGH 생성과 재생: (a) 원 영상, (b) (a)의 CGH, (c) (b)의 재생 영상  
 Fig. 7. Generation and reconstruction of CGH using SA algorithm: (a) Original image, (b) CGH of (a), (c) reconstructed image of (b).

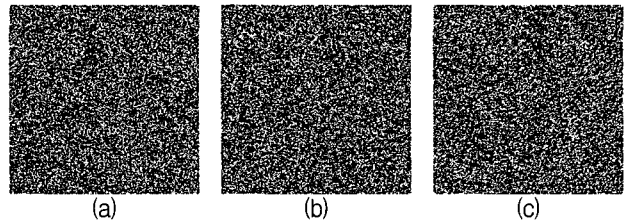


그림 8. 키 영상과 암호화된 영상: (a) 키1 영상, (b) 키2 영상, (c) 암호화된 영상  
 Fig. 8. Key images and encrypted image: (a) Key 1 image, (b) key 2 image, (c) encrypted image.

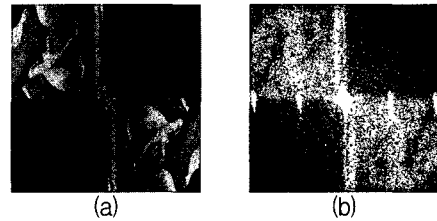


그림 9. 컴퓨터 모의 실험과 광 실험에 의해 재생된 영상: (a)컴퓨터 모의 실험 결과, (b)광 실험 결과  
 Fig. 9. Reconstructed images of computer simulation and optical experiment: (a)result of the computer simulation, (b)result of the optical experiment.

## 2. 컴퓨터 모의 실험 및 광 실험

그림 8(a)와 8(b)는 컴퓨터에서 제공하는 랜덤 발생기를 이용하여 생성한 두 개의 무작위 키 영상이다. 그림 8(c)는 CGH를 위상 변조한 후 두 개의 키로부터 거리  $d_1, d_2$ 의 거리와 순서를 지켜 암호화된 영상을 나타낸다.

그림 9(a)는 복호화된 CGH를 푸리에 변환하여 원 영상을 재생한 것이다. 복호화되어 재생된 영상은 원점에 대칭적으로 비축 홀로그래피의 특성에 따라 가상 영상과 실 영상이 서로 분리되어 나타남을 알 수 있고, 복화된 CGH는 0과  $\pi$ 의 위상만을 가지고 그 개수가 동일하므로 식 (9)에 의해 영차 성분이 제거됨을 알 수 있다. 그림 9(b)는 광 실험을 통해 복호화되어 재생된 원 영상을 나타낸다.

위상 변조된 두 개의 키 영상과 암호화된 영상을 공간 광 변조기(spatial light modulator; SLM)에 올려서 실험하였다. SLM은 한쪽 면에만 편광기가 부착되어 있어서 투사기(projector)용으로 제작된 모듈이며, 미리 위상 변조 특성을 정밀하게 조사한 후 그 결과에 따라서 입력 전압을 인가하였다. 실험에 사용된 He-Ne 레이저 빔은 파장이 632.8 nm인 선형빔이며, 위상 변조 특성이 있는 공간 광 변조기는 EPSON사의 P13SM015 LCD panel과 BE13S010 driver를 사용하였다. CCD는 픽셀 크기가 1300×1030이고 각각의 셀 크기가 6.7 μm × 6.7 μm 인 PULIX사의 TM-1320-15CL CCD를 사용하였다. 복호화되어 재생된 원 영상인 그림 9(b)는 그림 9(a)의 컴퓨터 모의 실험 결과와 같음을 확인할 수 있다. 광 실험을 통해 재생된 원 영상은 광학장비의 성능과 서로 다른 LCD의 위상 변조 특성 등의 오차로 인해 왜곡이 발생한 것으로 생각되며, 결과 영상에서 나타나는 밝은 점들은 LCD의 각 픽셀 격자에 의해 나타나는 것들이다.

3. 복호화에 대한 고찰

그림 10(a)는 암호화된 영상을 키1 영상과 키2 영상의 순서를 서로 바꾸었을 때의 재생된 결과 영상을 나타낸다. 그림 10(b)는 암호화된 영상과 키1, 키2 영상

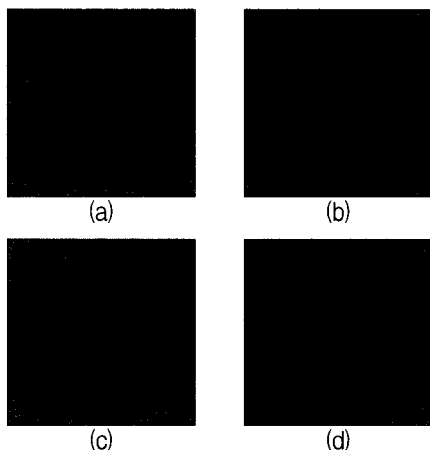


그림 10. 키 영상들의 순서와 거리가 다를 때와 거짓 키를 사용했을 때의 결과 영상: (a)키 영상들의 순서가 다를 때, (b)키 영상들의 거리가 다를 때, (c)키1 영상 대신에 거짓 키 영상을 사용했을 때, (d)키2 영상 대신에 거짓 키 영상을 사용했을 때.

Fig. 10. Reconstructed images with incorrect order and incorrect distance parameter of key images: (a) incorrect order of key images, (b)incorrect distance parameter of key images, (c)using the incorrect key1 image, (d)using incorrect key2 image.

사이의 거리가 암호화에 사용된 거리와 다를 경우의 결과 영상이다. 그림 10(c)는 키1 영상을 거짓 키 영상으로 대치했을 때이고, 그림 10(d)는 키2 영상을 거짓 키 영상으로 사용했을 때의 결과 영상이다.

그림 11(a), (b), (c)는 암호화된 영상을 각각 25%, 50%, 75% 절단했을 때의 영상이고, 그림 11(d), (e), (f)는 재생된 결과 영상이다.

암호화된 영상이 절단된 후 재생된 영상들은 절단되기 전의 영상에 비해 해상도는 낮아졌지만 여전히 식별 가능하므로 제안한 암호화 영상은 절단에 강인하다. 재생된 영상의 식별 가능 정도를 알아보기 위해 절단된 각각의 암호화된 영상으로부터 재생한 영상이 가지는 오차의 정량적 지표로 평균 자승 오차(mean squared error; MSE)를 다음 식 (19)와 같이 정의하고, PSNR (peak signal-to-noise ratio)은 다음 식 (20)과 같이 정의하였다<sup>[7,8]</sup>.

$$MSE[d_r(\xi, \eta)] = E \left\{ \frac{1}{M \times N} \sum_{\xi=0}^{M-1} \sum_{\eta=0}^{N-1} [ |d(\xi, \eta) - d_r(\xi, \eta)|^2 ] \right\} \quad (19)$$

$$PSNR = 20 \log_{10} \left\{ \frac{255}{\sqrt{MSE[d_r(\xi, \eta)]}} \right\} \quad (20)$$

여기서  $d_r(\xi, \eta)$ 는 절단된 영상으로부터 재생된 영

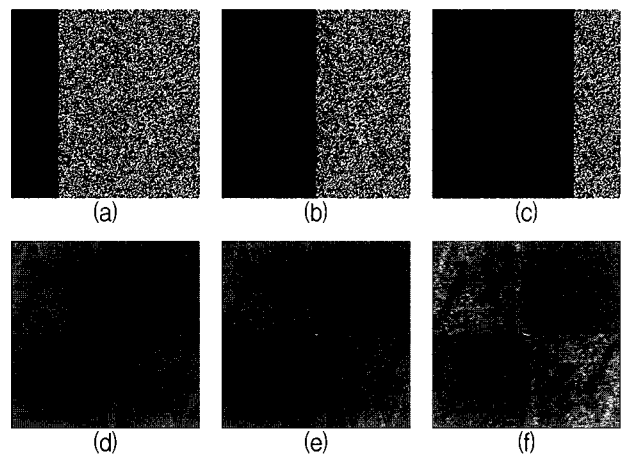


그림 11. 절단된 암호화 영상과 재생 영상: (a) 25% 절단, (b) 50% 절단, (c) 75% 절단, (d) (a)에 의해 재생된 영상, (e) (b)에 의해 재생된 영상, (f) (c)에 의해 재생된 영상

Fig. 11. Cropped encrypted images and reconstructed images (a) 25% cropped encrypted image, (b) 50% cropped encrypted image, (c) 75% cropped encrypted image, (d) reconstructed image by (a), (e) reconstructed image by (b), (f) reconstructed image by (c).

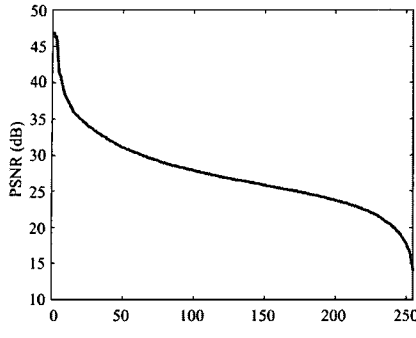


그림 12. 암호화 영상의 픽셀 줄 차단에 따른 PSNR  
 Fig. 12. PSNR for reconstructed image by blocking the pixel lines of encrypted image.

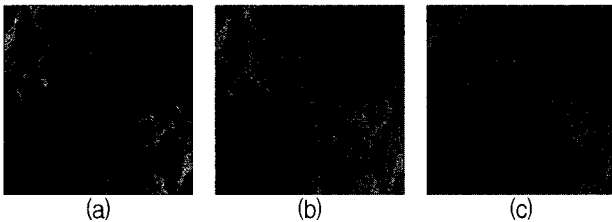


그림 13. 위상 잡음의 표준편차 변화에 의한 재생 영상:  
 (a)표준편차 0.1, (b)표준편차 0.2, (c)표준편차0.3  
 Fig. 13. Reconstructed image in presence of phase noises which are (a) standard deviation 0.1, (b) standard deviation 0.2, (c) standard deviation 0.3.

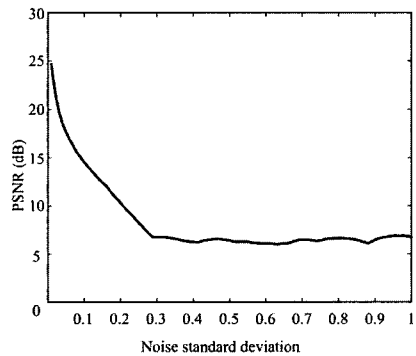


그림 14. 위상 잡음의 표준편차 변화에 따른 PSNR  
 Fig. 14. PSNR for reconstructed image by the variation with standard deviation of phase noise.

상이고,  $d(\xi, \eta)$ 는 재생된 영상이다.  $M$ 과  $N$ 은 재생된 영상의 픽셀 크기이며,  $E\{\cdot\}$ 는 기대값을 나타낸다. 그림 12는 암호화된 영상을 한 라인씩 절단했을 때의 PSNR를 나타낸다. 절단된 라인 수가 증가할수록 PSNR은 낮아지며, 75%의 절단에 대해서도 재생 영상이 원 영상과 유사하게 나타남을 알 수 있다.

제안된 복호화 방법으로 재생된 영상은 SLM 위의 먼지, 진동, SLM에 인가되는 전압 변화에 영향을 받는다. 본 논문에서 세기 정보는 디지털 홀로그래피로 제거할 수 있으므로 위상 잡음만을 고려하며, 위상 변조된 CGH에 위상 잡음의 평균이 0인 백색 가우스 잡음

이 첨가되었다고 가정한다. 그림 13(a), (b), (c)는 위상 잡음의 표준편차가 각각 0.1, 0.2, 0.3 일 때의 재생 영상이고, 그림 14는 위상 잡음의 표준편차 변화에 따른 PSNR을 나타낸다. 표준편차가 0.3인 경우 PSNR값이 급격하게 떨어지며, 그림 13에서와 같이 재생영상의 질이 상대적으로 많이 낮아짐을 확인할 수 있다.

#### IV. 결 론

본 논문에서는 원 영상이 아니라 원 영상의 위상 변조된 CGH와 위상 정보에 기반한 암호화 방법과 키 영상들의 프레넬 회절을 이용하여 암호화 수준을 높일 수 있는 방법을 제안하였다. 제안한 암호화 방법에서의 암호화된 정보는 위상 성분만으로 구성되어 있기 때문에 위상 잡음에 강하며 위상 마스크 형태로 저장할 수 있어 간섭을 이용한 홀로그램이 필요 없다. 또한 위상 변조된 CGH를 이용하기 때문에 절단에 강하며, 복호화 과정에서 위상측정방법이나 위상 대조차 여파기 등을 이용하지 않는다. 그리고 키 영상들에 의한 일정한 거리에서의 프레넬 회절 정보의 위상 성분을 이용하기 때문에 암호화 시에 사용된 키 영상 정보뿐만 아니라 키 영상들간의 거리와 순서 정보를 알고 있어야 복호화할 수 있다. 따라서 기존의 방법들보다 암호화 수준을 상당히 높였다. 컴퓨터 모의실험과 광 실험을 통하여 제안한 암호화 방법이 광 암호화 시스템에 적용 가능함을 확인하였다. 현재 사용되는 광학장비의 성능개선과 위상 정보를 정확히 표현할 수 있는 SLM이나 식각 기술의 개발 등을 통하여 제안한 암호화 방법의 성능은 더 나아질 것이라 생각된다.

#### 참 고 문 헌

- [1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letter*, vol. 20, no. 7, pp. 767-769, April, 1995.
- [2] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *J. Opt. Soc. Am. A*, vol. 16, no. 8, pp. 1915-1927, August, 1999.
- [3] B. Javidi, N. Towghi, N. Maghzi, and S. C. Verrall, "Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption," *Applied Optics*, vol. 39, no. 23, pp. 4117-4130, August, 2000.
- [4] J. Y. Kim, S. J. Park, C. S. Kim, J. G. Bae, and



- S. J. Kim, "Optical image encryption using interferometry-based phase masks," *Electron Letters*, vol. 36, no. 10, pp. 874-875, June, 2000.
- [5] D. H. Seo and S. J. Kim, "Interferometric phase-only optical encryption system that uses a reference wave," *Optics Letters*, vol. 28, no. 5, pp. 304-306, March, 2003.
- [6] P. C. Mogensen and J. Gluckstad, "Phase-only optical encryption," *Optics Letters*, vol. 25, no. 8, pp. 566-568, April, 2000.
- [7] T. J. Naughton, Y. Frauel, B. Javidi, and E. Tajahuerce, "Compression of digital holograms for three-dimensional object reconstruction and recognition," *Applied Optics*, vol. 41, no. 20, pp. 4124-4132, July, 2002.
- [8] G. R. Fowles, Introduction to Mordern Optics, 2nd ed., Dover Publications, New York, 1975.
- [9] J. W. Goodman, Introduction to Fourier Optics, 2nd ed., McGraw-Hill, New York, 1996.
- [10] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Optics Letters*, vol. 24, no. 11, pp. 762-764, June, 1999.
- [11] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," *Applied Optics*, vol. 39, no. 14, pp. 2313-2320, May, 2000.
- [12] M. S. Kim, M. R. Feldman, and C. C. Guest, "Optimum encoding of binary phase-only filters with a simulated annealing algorithm," *Optics Letters*, vol. 14, no. 11, pp. 545-547, June, 1989.

---

 저 자 소 개
 

---



윤 경 호(정회원)  
2002년 경북 대학교 전자공학과  
학사 졸업.  
2004년 경북 대학교 대학원  
전자공학과 석사 졸업.  
2004년~현재 LG전자 영상제품  
연구소

<주관심분야: DTV, 광 영상처리, 홀로그램 및 광  
메모리>

조 규 보(정회원)  
제40권 SD편 3호 참조

김 철 수(정회원)  
제33권 B편 11호 참조  
현재 경주대학교 컴퓨터 전자공학부 부교수

신 창 목(정회원)  
제41권 SD편 6호 참조

김 수 중(정회원)  
제33권 B편 7호 참조  
현재 : 경북대학교 전자전기컴퓨터학부 정교수

서 동 환(정회원)  
제38권 SD편 11호 참조  
현재 한국해양대학교 전기전자공학부 교수

