

# 랜덤 위상 마스크와 2-단계 위상 천이 디지털 홀로그래피를 이용한 이진 영상 이중 암호화

김 철 수<sup>†</sup>

## Double Encryption of Binary Image using a Random Phase Mask and Two-step Phase-shifting Digital Holography

Cheolsu Kim<sup>†</sup>

### ABSTRACT

In this paper, double encryption technique of binary image using random phase mask and 2-step phase-shifting digital holography is proposed. After phase modulating of binary image, firstly, random phase mask to be used as key image is generated through the XOR operation with the binary phase image. And the first encrypted image is encrypted again through the fresnel transform and 2-step phase-shifting digital holography. In the decryption, simple arithmetic operation and inverse Fresnel transform are used to get the first decryption image, and second decryption image is generated through XOR operation between first decryption image and key image. Finally, the original binary image is recovered through phase modulation.

**Key words:** Double Encryption, Random Phase Mask, Phase-shifting Digital Holography, Key Image, Decryption, XOR Operation

### 서 론

현재 인터넷과 무선통신을 통해 전송되는 영상데이터와 같은 디지털 정보는 쉽게 복제가 가능하기 때문에 이러한 불법 정보 복제 및 도난을 방지하기 위한 많은 정보보호 방법들이 제안되어 오고 있으며, 이를 방법에는 이중 랜덤 위상 부호화, 디지털 홀로그래피, 편광암호화 등이 있다[1,2]. 이를 중 위상 천이 디지털 홀로그래피는 복잡한 물체파를 2개 이상의 간섭세기를 이용하여 재생할 수 있는 기법으로 정보 보호 분야뿐만 아니라 계측학, 3차원 디스플레이 및 홀로그래피 현미경 등의 응용분야에도 널리 사용되고 있다[3-9].

일반적으로 디지털 홀로그래피에서 간섭무늬는

CCD카메라와 같은 전자 장비를 이용하여 얻고, 단일 간섭무늬에서는 0차 항 및 역영상이 항상 존재하기 때문에 이를 제거하기 위한 노력이 필요하다[10-11]. 이를 해결하기 위한 방법 중의 하나가 기준빔의 위상을 천이시켜 가면서 여러 개의 간섭 세기를 구하고 이로부터 물체빔을 복원하는 위상 천이 디지털 홀로그래피 방법(phase-shifting digital holography; PSDH)이며, 여기에는 4개의 간섭세기를 필요로 하는 4-단계 PSDH[3], 3개의 간섭세기를 필요로 하는 3-단계 PSDH[5], 그리고 2개의 간섭세기를 필요로 하는 2-단계 PSDH 방법[4,6,7,8]이 있다. 본 논문에서는 2개의 간섭세기 만으로 복잡한 물체파를 재생할 수 있는 2-단계 PSDH 방법을 이용하고자 한다. 이때 재생되는 물체파의 질(quality)은 간섭패턴의

\* Corresponding Author : Cheolsu Kim, Address: (38065) Taejongro 188, Gyeongju-City, Kyungpook Korea, TEL : +82-54-770-5178, FAX : +82-54-748-5364, E-mail : kimcs@gju.ac.kr

Receipt date : Mar. 29, 2016, Revision date : May 17, 2016

Approval date : May 30, 2016

<sup>†</sup> Dept. of Electrical Energy & Computer Engineering,  
Gyeongju University

시각성(visibility) 및 물체빔과 기준빔 사이의 세기비에 의해 결정이 된다. 그러나 이 두 인자는 입력영상의 형태에 따라 달라질 수 있기 때문에 입력영상에 따라 물체빔과 기준빔 사이의 세기 비를 적절히 조절해 주어야 한다.

본 논문에서는 2-단계 PSDH에서의 이러한 문제점을 해결하고, 이를 이진 영상의 암호화 및 복호화하는데 활용하는 방법을 제안하였다. 암호화 과정에서는 이진 영상정보를 위상 변조하여 이진 위상 형태로 만든 후, 키 정보로 사용할 랜덤하게 발생시킨 이진 위상 정보와 XOR연산을 통해 1차 암호화를 하고, 이를 2-단계 PSDH의 입력영상으로 사용하였다. 1차 암호화된 영상은 이진 영상정보의 형태에 상관없이 항상 랜덤한 이진 위상 정보로 되어, 입력 영상의 형태와 상관없이 항상 일정한 형태의 물체빔을 생성하므로 기준빔과의 세기 비와 간섭패턴의 시각성을 일정하게 할 수 있는 장점이 있다. 그리고 2-단계 PSDH 기법을 2차 암호화 과정에 적용함으로써 보안이 좀 더 강화된 이중 암호화된 영상 정보를 얻을 수 있다.

복호화 과정은 암호화과정의 역순으로 진행되며, 2-단계 PSDH 기법으로 암호화된 두 간섭세기 정보를 이용하여 디지털 처리 및 역프레즈넬 변환을 통해 1차 복호화 정보를 얻고, 다시 키 정보와의 XOR연산 및 위상정보 복조를 통해 원래의 물체파를 완전히 재생하게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 디지털 홀로그래피와 위상 천이 디지털 홀로그래피의 이론적인 설명을 하고, 3장에서는 제안한 암호화 및 복호화 방법과 광학적 구성도에 대해 설명한다. 4장에서는 컴퓨터 모의실험을 통해 제안한 방법의 성능과 장점을 설명하고, 마지막 5장에서 결론을 맺도록 한다.

## 2. 이론적 배경

### 2.1 디지털 홀로그래피

- 디지털 홀로그래피는 물체빔과 기준빔 사이의 간섭세기를 화학적인 처리 방법 대신에 CCD 또는 CMOS와 같은 디지털 영상 장치를 이용하여 전자적으로 획득하고, 이를 수치적인 계산을 통해 2차원 또는 3차원 영상을 재생하는 기술로써 최근 들

어 반도체 집적기술 발달로 인한 디지털 영상 장치의 성능 개선과 병렬 컴퓨팅 처리로 인한 연산 속도 개선 등으로 인해 그 기술의 활용도가 점점 증대되고 있다. 디지털 홀로그래피와 관련된 파면 해석을 이론적으로 설명하기 위한 좌표계는 Fig. 1과 같다.

$(x,y)$  평면의 임의의 물체로부터 반사된 물체빔 함수를  $o(x,y)$ 라 하면, 물체로부터  $d$ 만큼 떨어진 위치에서의 물체빔은 프레즈넬 변환에 의해  $O(u,v)$ 로 표현되며 다음 식과 같다.

$$O(u,v) = \frac{\exp(ikd)}{i\lambda d} \iint o(x,y) \times \exp[i\pi \frac{(x-u)^2 + (y-v)^2}{d\lambda}] dx dy \quad (1)$$

여기서  $i = \sqrt{-1}$ 이고,  $\lambda$ 는 사용된 광원의 파장이며,  $k$ 는 파수(wave number)를 의미하며,  $d$ 는 프레즈넬 변환 거리이다.

홀로그램 평면에서의 물체빔 함수  $O(u,v)$ 와 기준빔 함수  $R(u,v)$ 는 복소함수 형태인 다음 식으로 표현된다.

$$O(u,v) = |O(u,v)| \exp[i\phi_O(u,v)] \quad (2)$$

$$R(u,v) = |R(u,v)| \exp[i\phi_R(u,v)] \quad (3)$$

홀로그램 평면에서 물체빔과 기준빔이 서로 간섭을 일으키고, 그 간섭세기는 CCD 카메라에 기록되며, 다음 식으로 표현된다.

$$\begin{aligned} I(u,v) &= |O(u,v) + R(u,v)| |O(u,v) + R(u,v)|^* \\ &= |O(u,v)|^2 + |R(u,v)|^2 + O(u,v)R(u,v)^* + O(u,v)^*R(u,v) \end{aligned} \quad (4)$$

식 (4)에서 간섭 세기  $I(u,v)$ 의 첫 번째 항과 두 번째 항은 물체빔 및 기준빔 함수의 DC 성분을 나타내고, 세 번째 항에는 물체빔 함수 항이 있으며, 네 번째 항에는 물체빔 함수의 복소공액 항이 들어 있다.

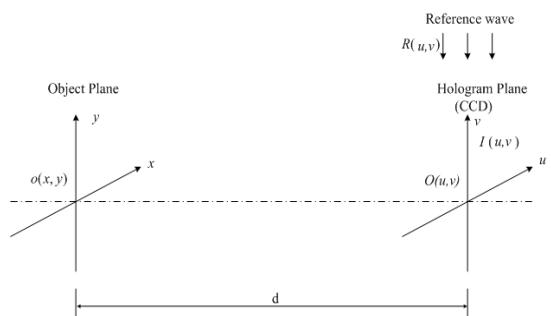


Fig. 1. Coordinate system in digital holography.

다. 원래의 물체빔 함수를 복원하기 위해서는 세 번째 항만을 구한 후, 디지털처리와 역프레즈넬 변환을 수행하면 된다.

기준빔과 물체빔이 평행하게 입사하는 on-axis 홀로그래피 시스템의 경우에는 재생 시에 DC 성분과 물체빔의 복소공액 항이 잡음 역할을 하기 때문에 이 항들을 억제하거나 제거할 수 있는 방법이 필요하다.

## 2.2 위상 천이 디지털 홀로그래피

기존의 단일 노출(single exposure) on-axis 디지털 홀로그래피 시스템을 그대로 이용하면서 재생 시에 깨끗한 원래의 물체파를 얻기 위해서는 식 (4)에서  $O(u,v)$ 만을 구할 수 있는 방법이 필요하다. On-axis 디지털 홀로그래피 시스템에서 기준빔의 경로에 위상 지연기(phase retarder)나 위상 제어기를 설치하여 기준빔의 위상 값( $\theta=0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ )을 제어하면 서 간섭 세기를 구하고, 이를 세기 값을 이용하여 정리하면 홀로그램 평면에서의 물체빔 함수  $O(u,v)$ 만을 얻을 수 있다. 이 방법을 위상 천이 디지털 홀로그래피 기술이라고 한다.

위상 천이기를 통과한 기준빔  $R(u,v)\exp(i\theta)$ 과 물체빔  $O(u,v)$ 사이의 간섭 세기는 다음 식으로 표현된다.

$$\begin{aligned} I(u,v;\theta) &= |O(u,v) + R(u,v)\exp(i\theta)| |O(u,v) + R(u,v)\exp(i\theta)|^* \\ &= I_O(u,v) + I_R(u,v) + 2|O(u,v)|R(u,v)| \times \cos[\phi_O(u,v) - \phi_R(u,v) - \theta] \end{aligned} \quad (5)$$

여기서  $I_O(u,v) = |O(u,v)|^2$ 이고,  $I_R(u,v) = |R(u,v)|^2$ 이다.

위상 천이 값  $\theta$ 의 변화에 따른 각각의 간섭세기를 간략히 표현하면 다음과 같이 쓸 수 있다.

$$I_1 = I(u,v;0) \quad (6)$$

$$I_2 = I(u,v;\frac{\pi}{2}) \quad (7)$$

$$I_3 = I(u,v;\pi) \quad (8)$$

$$I_4 = I(u,v;\frac{3\pi}{2}) \quad (9)$$

간섭세기  $I_1, I_2, I_3$  그리고  $I_4$ 에서 좌표  $(u,v)$ 는 모두 생략되었다. 위의 식들로부터 복소값을 갖는 물체빔 함수  $O(u,v)$ 를 구할 수 있는데, 4개의 간섭세기를 이용할 경우를 4-단계 PSDH, 3개의 간섭세기를 이용하면 3-단계 PSDH 그리고 2개의 간섭세기를 이용하면 2-단계 PSDH라 부른다. 그들의 식들은 각각

다음과 같다.

4-단계 PSDH:

$$O(u,v) = \frac{1}{4|R(u,v)|} [(I_1 - I_3) + j(I_2 - I_4)] \quad (10)$$

3-단계 PSDH:

$$O(u,v) = \frac{1}{4|R(u,v)|} [(I_1 - I_2)(1+j) + j(I_2 - I_3)(1-j)] \quad (11)$$

2-단계 PSDH:

$$O(u,v) = \frac{1}{2R(u,v)} [(I_1 - I_O - I_R) + j(I_2 - I_O - I_R)] \quad (12)$$

이렇게 구해진 복소함수  $O(u,v)$ 는 컴퓨터를 이용하여 디지털적으로 역프레즈넬 변환하면 물체빔 함수의 복원 영상  $o'(x,y)$ 가 구해진다. 이를 식으로 나타내면 다음과 같다.

$$\begin{aligned} o'(x,y) &= \frac{\exp(ik(-d))}{i\lambda(-d)} \iint O(u,v) \exp[i\pi \frac{(u-x)^2 + (v-y)^2}{d\lambda}] du dv \\ &= \frac{\exp(ik(-d))}{i\lambda(-d)} \exp[ik \frac{1}{2d}(x^2 + y^2)] \times FFT2D \left\{ O(u,v) \exp \left[ \frac{ik}{2(-d)} (u^2 + v^2) \right] \right\} \end{aligned} \quad (13)$$

여기서  $FFT2D$ 는 2차원 푸리에 변환 연산을 의미한다. 즉 2차원 푸리에 변환 및 간단한 곱셈 연산을 통해 프레즈넬 역변환을 수행할 수 있음을 보여준다.

PSDH에 대한 지금까지의 연구는 가급적 적은 수의 간섭세기를 이용하여 물체빔 함수를 완벽하게 복원할 수 있는 방법을 찾는 방향으로 진행되어오고 있다. 3-단계 및 4-단계 PSDH를 이용하게 되면 기준빔과 물체빔 사이의 세기 비에 상관없이 원래의 물체파를 복원할 수 있지만, 2-단계 PSDH를 이용하게 되면 복원되는 물체파가 기준빔과 물체빔 사이의 세기비에 영향을 받게 된다. 이를 확인하기 위해 PSDH 기술에서 기준빔과 물체빔 사이의 세기 비 변화에 따라 복원되는 영상의 성능을 컴퓨터 시뮬레이션을 통해 평가하였다. 성능평가에 사용된 비용함수는 원래의 물체빔 함수  $o(x,y)$ 와 복원된 물체빔 함수  $o'(x,y)$  사이의 RMSE(root mean square error)이며, 다음 식으로 표현된다.

$$RMSE = \sqrt{\frac{1}{MN} \sum_{m=1}^M \sum_{n=1}^N [o(m,n) - o'(m,n)]^2} \quad (14)$$

여기서  $o(m,n)$ 과  $o'(m,n)$ 은  $o(x,y)$ 와  $o'(x,y)$ 를 이산적으로 표현한 함수이다. Fig. 2에서는 기준빔과 물체빔 사이의 세기 비 변화에 따른 4-단계, 3-단계

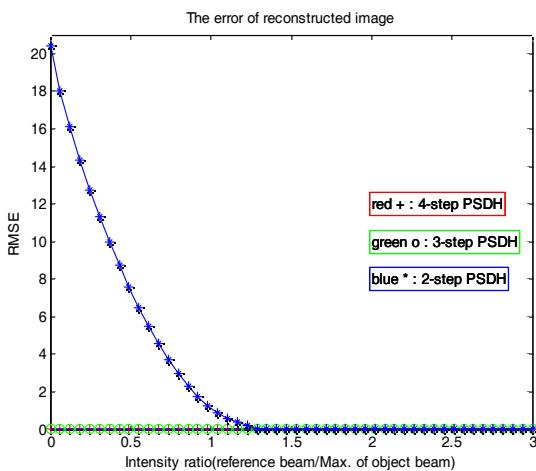


Fig. 2. Comparison of the performance two, three and four step PSDH according to the intensity ratios (reference beam/Max. of object beam).

및 2-단계 PSDH 방법의 RMSE 성능을 비교하였다. 시뮬레이션 결과 3-단계 및 4-단계 PSDH 방법에서는 기준빔과 물체빔 사이의 세기 비에 영향을 받지 않지만, 2-단계 PSDH 방법에서는 기준빔의 세기가 물체빔 세기의 최대값보다 어느 정도 클 경우에만 RMSE가 최소값에 가까워짐을 알 수 있다. 그러나 2-단계 PSDH 방법에서는 필요한 간섭패턴의 수는 가장 작지만 입력되는 물체의 형태가 바뀌게 되면 물체빔의 세기도 변하게 되는 단점이 있으므로 이에 대한 보완이 필요하다. 만약 기준빔의 세기를 물체빔 세기의 최대값보다 훨씬 크게 한다면 수치적으로는 RMSE가 최소가 되는 복원 영상을 얻을 수 있겠지만, 기준빔과 물체빔의 간섭세기의 가시성(visibility)이 떨어져서 CCD 카메라로 간섭패턴을 정확하게 얻기 힘든 문제점을 가진다. 그러므로 입력되는 물체빔의 형태에 상관없이 일정한 물체빔 세기를 얻을 수 있는 방법이 필요하며, 물체빔 세기가 일정하면 기준빔 세기도 항상 일정하게 할 수 있다.

### 3. 제안한 이진 영상 암호화 및 복호화 방법

본 논문에서 제안하는 랜덤 위상 마스크와 2단계 PSDH 방법을 이용한 이진영상의 이중 암호화 및 복호화 과정은 Fig. 3과 같다. 암호화 과정은 이진 입력 영상 함수인  $s(x,y)$ 를 위상변조 한 후, 랜덤 발생 이진 위상 키 정보인  $key(x,y)$ 와의 XOR 연산을 통해 1차

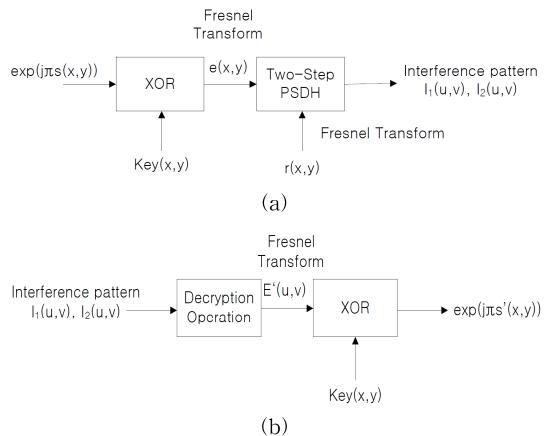


Fig. 3. Block diagrams for (a) image encryption and (b) decryption process.

암호화 영상  $e(x,y)$ 을 생성한다. 이 영상의 프레즈넬 변환된 물체파와 기준파 및  $\frac{\pi}{2}$  위상천이 된 기준파와의 간섭에 의해 각각 두 간섭세기  $I_1(u,v)$ 와  $I_2(u,v)$ 가 생성된다. 이 두 간섭세기가 이진영상의 2차 암호화 영상정보가 되는 것이다. 암호화된 정보는 기준영상과는 형태가 전혀 다른 값을 가지며, 암호화 과정에 사용된 인자는 키영상 정보뿐만 아니라 간섭무늬 획득과정에서 사용된 많은 변수들(CCD 카메라의 화소길이, 프레즈넬 변환 거리)의 값을 정확히 알지 못하면 원래의 영상을 복원할 수 없다.

복호화 과정은 암호화 과정의 역으로서, 식 (12)와 같은 복호화 연산과 프레즈넬 역변환을 통해 간섭전의 물체파  $e'(x,y)$ 를 재생한 후, 다시 암호화 시 사용한 키 정보와의 XOR 연산을 통해 원래의 위상 영상을 재생한다. 그리고 마지막으로 위상성분의 복조를 통해 이진 입력영상을 복원한다.

제안한 방법의 구현을 위한 광학적 구성도는 Fig. 4와 같다. Ar 레이저 광원으로부터 나온 빔이 SF (spatial filter)와 CL(collimating lens)를 거쳐 시준화된(collimated) 후, 빔분할기(BS1)에 의해 물체빔과 기준빔으로 나누어진 진다. 물체빔은 XOR 연산에 의해 암호화된  $e(x,y)$ 가 로딩/loading)된 LCD를 통과하고, PZT(piezoelectric transducer) mirror에 의해 위상이 제어된 기준빔( $0, \frac{\pi}{2}$ )이 빔분할기(BS2)에서 간섭을 일으키고, 그 간섭 세기가 CCD에 기록된다. 이때 기준빔의 세기는 ND를 이용하여 제어한다. 두 간섭세기는 다음 식으로 표현된다.

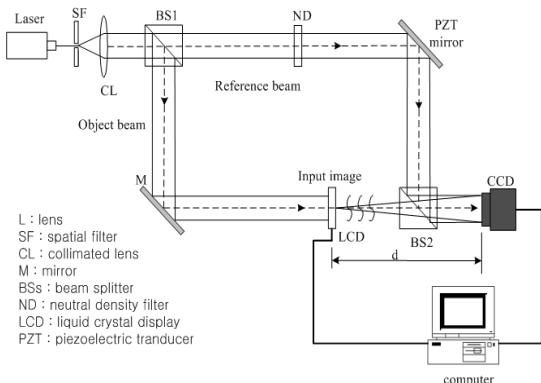


Fig. 4. Optical schematic diagram for implementing the proposed 2-step PSDH.

$$I_i = I_E + I_R + E \cdot R^* e^{-j\theta_i} + E^* \cdot R e^{j\theta_i}, \text{ for } i=1,2 \quad (15)$$

여기서  $E$ 는 1차 암호화된  $e(x,y)$ 의 프레즈넬 변환된 물체파 함수  $E(u,v) = |E|e^{j\phi_E}$ 를 간략하게 나타낸 함수이고,  $R$ 은 기준파 함수  $R(u,v) = |R|e^{j\phi_R}$ 를 간략하게 나타낸 함수이다. 그리고 기준빔에서의 위상 값  $\theta_1$ 은 0이고,  $\theta_2$ 는  $\frac{\pi}{2}$ 이다. 또한  $(x,y)$ 는 공간영역의 좌표이고,  $(u,v)$ 는 프레즈넬 영역의 좌표를 나타내며, 수식 간략화를 위해 가급적 생략했다. 입력과 CCD 사이의 프레즈넬 변환 거리는  $d = 300mm$ 이다.  $I_E$ 와  $I_R$ 은 각각 물체파와 기준파의 세기함수이고,  $\phi_E$ 와  $\phi_R$ 은 각각 물체파와 기준파의 위상 함수이다. 2단계 PSDH를 위해 기준빔의 위상이 PZT mirror에 의해 제어되어 각각  $\theta_1 = 0$ ,  $\theta_2 = \frac{\pi}{2}$  값을 가진다. 즉 2-단계 PSDH에 의해 최종 암호화된 간섭세기 함수  $I_1$ 과  $I_2$ 를 얻을 수 있다.

그리고 복호화를 위해서는 식 (15)의 표현을 약간 변형하고, 두 간섭세기 함수를 더한 후, 제곱을 하면 다음과 같은  $I_E + I_R$ 에 대한 2차 함수식을 얻을 수 있다.

$$2(I_E + I_R)^2 - (2I_R + I_1 + I_2)(I_E + I_R) + (I_1^2 + I_2^2 + 4I_R^2) = 0 \quad (16)$$

그러므로 간섭세기의 0차(zero order)항인  $I_E + I_R$ 는 식 (16)으로부터 쉽게 구해질 수 있다.

$$I_E + I_R = \frac{2I_R + I_1 + I_2}{2} - \frac{\sqrt{(2I_R + I_1 + I_2)^2 - 2(I_1^2 + I_2^2 + 4I_R^2)}}{2} \quad (17)$$

식 (17)로부터, 물체파  $E(u,v)$ 의 세기함수  $I_E$ 는 두

간섭세기  $I_1$ ,  $I_2$  그리고 기준빔의 세기  $I_R$ 로부터 구할 수 있음을 알 수 있다. 즉  $I_1$ 과  $I_2$ 는 측정을 통해 구할 수 있고,  $I_R$ 은 간섭무늬에서 가시성이 좋도록 물체빔의 세기를 고려하여 결정하면 된다. 특히 물체빔은 입력 이진영상이 키 정보에 의해 1차 암호화 되고, 그 세기분포가 랜덤한 잡음 형태를 가진다. 즉, 어떠한 이진영상의 형태에 상관없이 항상 랜덤한 세기분포를 가지므로 간섭무늬의 가시성을 좋게 하도록 기준빔의 세기를 쉽게 결정할 수 있다.

본 논문에서는 임의의 랜덤한 이진 위상 함수의 프레즈넬 변환을 한 후, 그 복소 값의 최대크기를 기준빔의 세기로 결정하였다. 기준빔의 세기  $I_R$ 이 결정되면, 다음 식을 이용하여 물체파 함수  $E'(u,v)$ 를 왜곡 없이 재생할 수 있다.

$$H_{2-PSDH} = \frac{(I_1 - I_E - I_R) + j(I_2 - I_E - I_R)}{2R^*} = E' \quad (18)$$

위 식은 식 (12)와 동일하며, 재생된 함수  $E'(u,v)$ 는 역프레즈넬 변환에 의해  $e'(x,y)$ 가 구해지고, 키정보  $k(x,y)$ 와 다시 XOR 연산을 하면 위상 이진 영상 함수  $e^{js'(x,y)}$ 를 얻을 수 있다. 여기서 위상 정보만을 취하면  $s'(x,y)$ 는 원래의 이진 입력 영상과 정확히 같은 왜곡 없는 영상을 복원할 수 있게 된다. 프레즈넬 변환 시 거리 정보 또한 복호화에 반드시 필요한 요소정보라고 할 수 있다. 그러므로 키 정보 함수뿐만 아니라 프레즈넬 변환 시 사용된 거리 정보를 반드시 알아야만 원래의 이진 영상을 복원할 수 있게 되는 것이다. 제안한 암호화 및 복호화 방법에서는 3개 및 4개의 홀로그램을 필요로 하는 3단계 및 4단계 PSDH방법보다 적은 2개의 홀로그램만을 이용하여 원래의 영상을 재생하는 2단계 PSDH 방법을 암호화 및 복호화 과정에 사용하였으므로, 3단계 및 4단계 PSDH방법보다 암호화 및 복호화를 수행하는 시간도 단축시킬 수 있을 뿐만 아니라 계산의 복잡도도 훨씬 낮다고 할 수 있다.

#### 4. 컴퓨터 모의실험 결과 및 고찰

컴퓨터 모의실험에 사용된 조건은 광원으로 514nm의 파장을 갖는 Ar레이저이며, 간섭세기를 획득하는 CCD 카메라의 화소 크기는  $15.6\mu\text{m} \times 15.6\mu\text{m}$ 이며, 입력영상과 CCD 카메라 사이의 거리( $d$ )는 300mm로 하였다. 먼저 on-axis 기반 디지털 홀로그

래피 시스템을 이용하여 간섭무늬를 CCD 카메라를 통해 얻고, 이를 디지털 프레즈넬 변환을 통해 원래의 물체과 영상을 복원하는 실험을 하였다. 실험에 사용된 입력 이진영상은  $256 \times 256$  크기의 영문 학교 명으로써 Fig. 5(a)와 같고, Fig. 5(a)의 물체빔 함수와 기준빔 함수의 간섭 세기 무늬는 Fig. 5(b)와 같으며, Fig. 5(b)를 디지털 프레즈넬 변환하여 구한 복원 영상은 Fig. 5(c)와 같다. 디지털처리를 통해 복원된 영상을 보면 식 (4)의 첫 번째와 두 번째 항인 DC의 성분의 세기와, 네 번째 항인 복소 공액 영상이 동시에

재생되어 원하는 물체빔 함수를 제대로 복원할 수 없음을 알 수 있다. 그러므로 잡음처럼 보이는 이들 두 성분들을 억제하거나 제거하는 방법이 필요하며, 본 논문에서는 2-단계 PSDH 방법을 이용하여 해결하고자 하였다.

2-단계 PSDH 방법은 두 개의 간섭 세기 패턴만을 이용하여 원래의 물체빔 함수를 복원할 수 있으나, 물체빔 세기와 기준빔 세기의 비에 따라 복원되는 물체빔 함수의 성능이 달라진다. Fig. 6에서 보는 바와 같이 기준빔의 세기가 물체빔 세기의 최대값보다

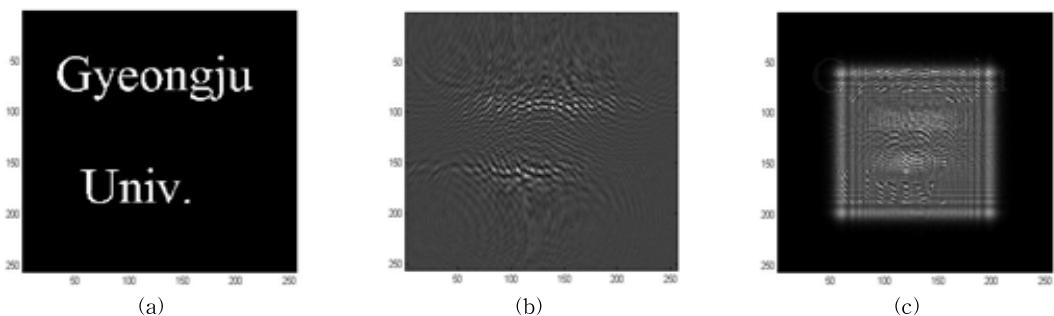


Fig. 5. Simulation results in on-axis digital holography system; (a) original binary image, (b) Interference pattern, and (c) reconstructed image.

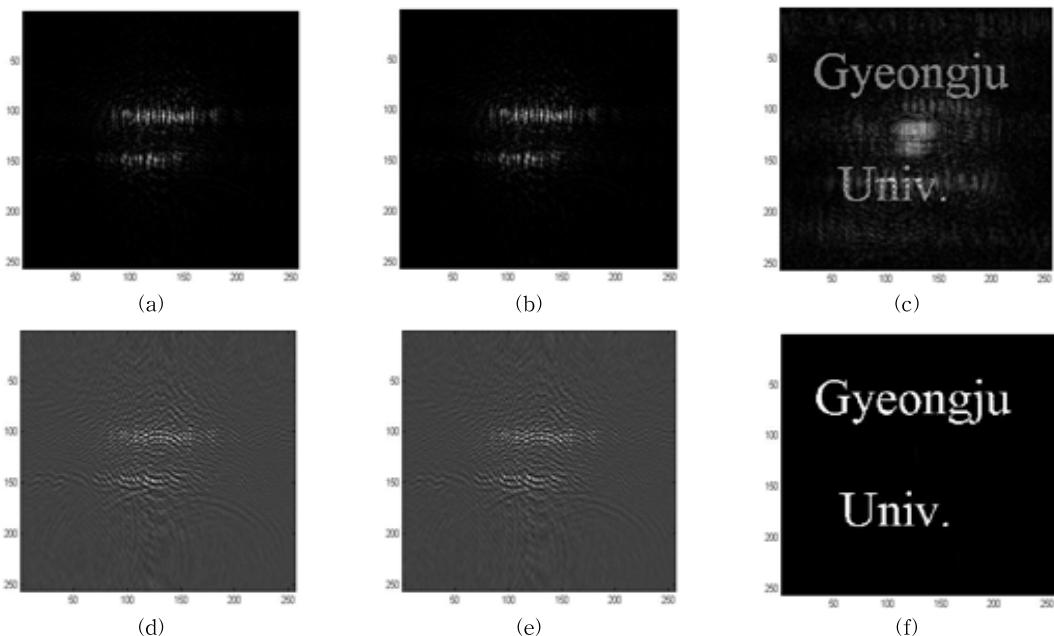


Fig. 6. Reconstructed images according to the intensity ratio(reference beam/Max. of object beam) in 2-step PSDH. (a) interference pattern 1, (b) interference pattern 2, and (c) reconstructed image when the intensity ratio is 0.1, (d) interference pattern 1, (e) interference pattern 2, and (f) reconstructed image when the intensity ratio is 1.3.

커야만 잡음이 없는 물체빔 할수를 복원할 수 있다. 물체빔과 기준빔 세기의 변화에 따른 재생영상의 성능 변화를 Fig. 6에 나타내었다.

Fig. 6(a)와 6(b)는 기준빔 세기와 물체빔 세기의 최대값과의 비가 0.1일 때 CCD카메라로 획득한 간섭무늬들이고, Fig. 6(c)는 식 (18)을 이용하여 재생한 영상이다. 마찬가지로 Fig. 6(d)와 6(e)는 기준빔 세기와 물체빔 세기의 최대값과의 비가 1.3일 때의 간섭무늬들이고, Fig. 6(e)는 이를 간섭무늬들로부터 재생된 영상이다.

Fig. 6(c)와 6(f)를 비교해 보면, 기준빔과 물체빔의 세기비가 클수록 깨끗한 재생 영상을 얻을 수 있음을 알 수 있다. 만약 기준빔의 세기를 무조건 크게 하면 이 잡음이 생기지 않게 할 수 있겠지만 Fig. 6(d)와 6(e)와 같이 간섭무늬의 시각성이 떨어져 CCD 카메라로 선명한 간섭패턴을 획득할 수 없게 된다. 그러므로 입력되는 물체빔 함수의 형태에 상관없이 항상 일정한 물체빔을 얻을 수 있다면 기준빔의 세기도 일정하게 할 수 있고, 재생되는 영상의 성능도 일정하게 유지할 수 있을 것이다. 그래서 본 논문에서는 물체빔 함수를 위상 변조한 후, 랜덤하게 발생시

킨 키 정보와 XOR 연산을 통해 1차 암호화한 영상을 2단계 DSPH의 입력영상으로 사용함으로써 이 문제를 해결할 수 있었다.

본 논문에서 제안한 랜덤위상 마스크와 2-단계 DSPH를 이용한 이진 영상의 이중 암호화 및 복호화 방법을 컴퓨터 모의실험을 통해 검증하였다. 실험에 사용된 입력 이진영상, 키 정보로 사용되는 랜덤 이진 위상 마스크, 그리고 XOR연산 및 2-단계 DSPH를 이용한 암호화 과정에서 도출된 결과들을 Fig. 7에 나타내었다. 입력 이진영상은 앞 실험에서 사용된  $256 \times 256$  학교 영문명 영상으로 Fig. 7(a)와 같고, 랜덤 이진 위상 영상인 키 정보는 Fig. 7(b), 그리고 이진 영상의 위상 정보와 키 정보와의 XOR 연산을 통해 얻은 1차 암호화 영상은 Fig. 7(c)와 같다. Fig. 7(d)와 7(e)는 1차 암호화 영상인 7(c)를 2-단계 PSDH의 입력으로 사용하여 얻은 간섭세기 패턴으로 우리가 구하고자 하는 2차 암호화 영상들이다. 암호화된 영상은 입력 이진영상과 전혀 형태가 다르며, 랜덤 잡음과 유사하다고 할 수 있다. 그리고 암호화 과정에서 사용된 키 정보 및 암호 인자(CCD화소 크기 및 프레즈넬 변환 거리)에 대한 정보를 정확히

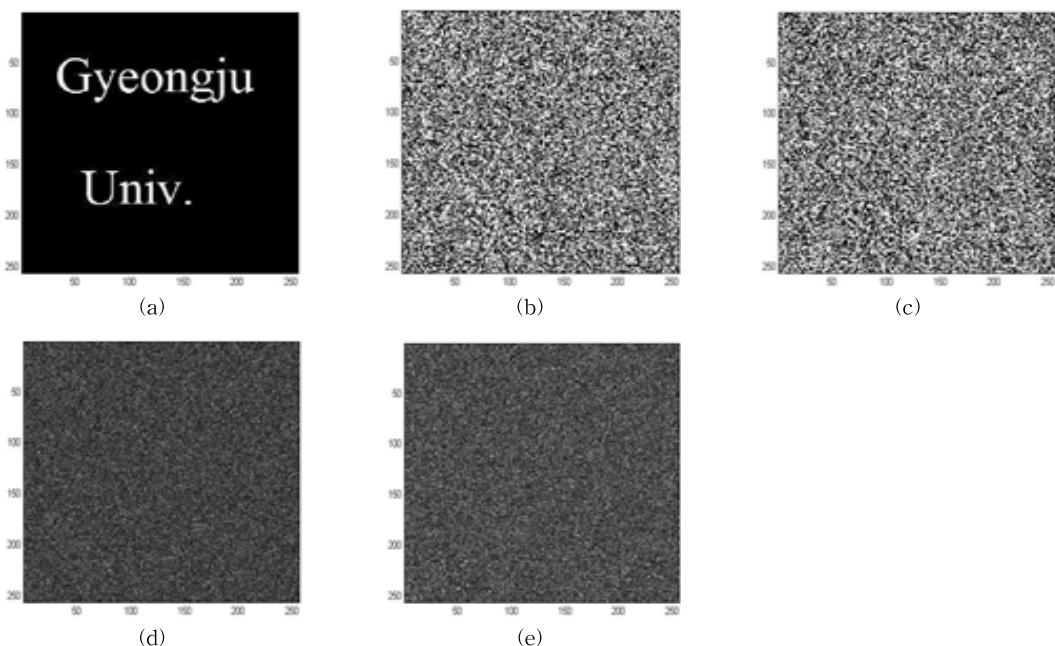


Fig. 7. (a) Original binary image, (b) key image, (c) 1st encrypted image that is generated XOR operation between binary phase image and key image, (d) 2nd encrypted image 1 and (e) 2nd encrypted image 2 that are generated through 2-step phase-shifting digital holography.

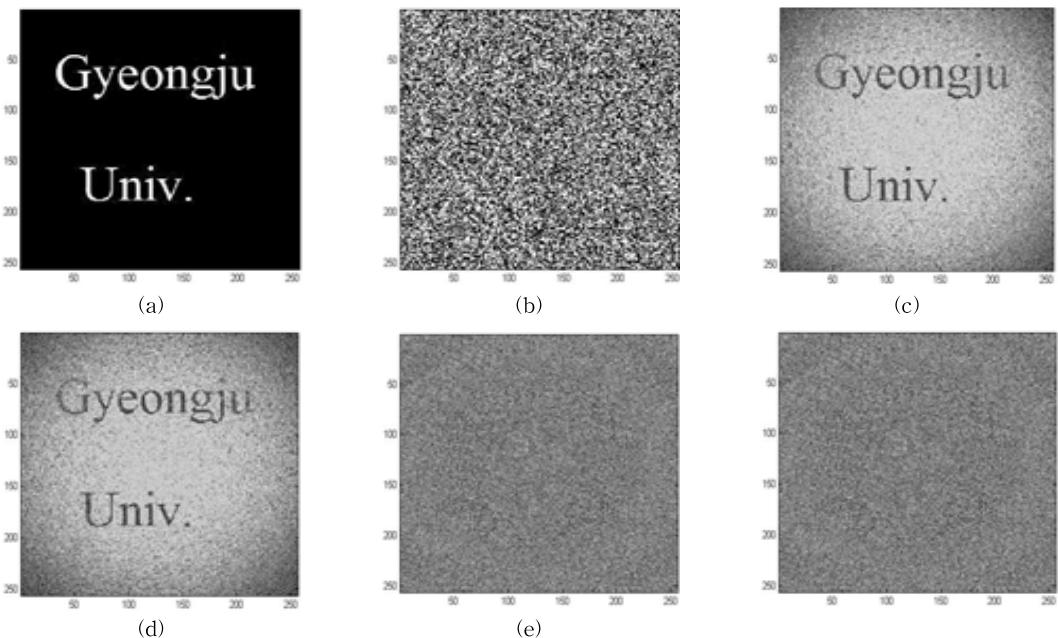


Fig. 8. Decrypted images; (a) correct key image and Fresnel distance( $d = -300\text{mm}$ ), (b) false key image and correct Fresnel distance( $d = -300\text{mm}$ ), (c) correct key image and false Fresnel distance( $d = -305\text{mm}$ )), (d) correct key image and false Fresnel distance( $d = -295\text{mm}$ ), (e) correct key image and false Fresnel distance( $d = -290\text{mm}$ ), and (f) correct key image and false Fresnel distance( $d = -280\text{mm}$ ).

알지 못하면 원래의 이진 영상을 복호화 할 수 없다. Fig. 8은 복호화 과정을 거쳐 복원된 결과 영상을 나타낸다. 시뮬레이션 과정에서 CCD카메라의 화소크기는 공개적으로 알려져 있다고 가정하고, 키 정보와 프레즈넬 변환의 거리 정보( $d = 300\text{mm}$ )만을 보안 요소로 설정하였다. Fig. 8(a)는 정확한 키 영상 정보와 프레즈넬 변환의 거리 정보( $d = 300\text{mm}$ )에서 구한 복원영상이다. 만약 암호화 시에 사용한 키 영상 정보를 모르거나 프레즈넬 거리 정보를 정확하게 모르게 되면 원하는 원래의 이진 영상 정보가 복원되지 않는다. 이를 Fig. 8(b), 8(c), 8(d), 8(e) 그리고 8(f)에 각각 나타내었다. Fig. 8(b)는 키 정보를 모르면 다른 모든 암호화 보안 요소들을 정확히 알아도 암호화된 정보를 복원할 수 없음을 보여주고 있으며, Fig. 8(c)와 8(d)와 같이 키 정보는 알고 있으면, 프레즈넬 거리 정보를 정확히 모르더라도 그 오차가 작으면 암호화된 영상이 어느 정도 복원되는 것으로 봐서 키 정보가 프레즈넬 변환의 거리 정보보다 더 중요함을 알 수 있다. Fig. 8(e)와 8(f)는 프레즈넬 변환의 거리 정보의 오차가 커지면 암호화된 정보를 복원할 수 없음을 보여준다. 시뮬레이션 결과들로부터 제안

된 암호화 방법은 두 번의 암호화 와 key 정보뿐만 아니라 CCD의 사양과 프레즈넬 변환 거리정보를 알아야 정확한 입력 이진영상을 복원할 수 있으므로 보안능력이 한층 더 강화된 방법이라고 할 수 있다.

## 5. 결 론

본 논문에서 제안한 랜덤 위상 마스크와 2-단계 위상 천이 디지털 홀로그래피를 이용한 위상 영상 암호화 방법에서는 이진 영상을 위상 정보로 표현한 후, 키 영상 정보인 랜덤 이진 위상 정보와 XOR연산을 통해 1차 암호화를 하고, 다시 2-단계 PSDH 기법을 통해 2차 암호화를 하였다. 2단계 PSDH과정에서 프레즈넬 변환 거리정보와 CCD카메라 화소 크기 또한 보안 요소가 될 수 있기 때문에 한층 더 보완성이 강화된 새로운 방법이라고 할 수 있다. 그리고 2-단계 PSDH과정에서 랜덤한 이진 위상 값을 갖는 1차 암호화 영상을 물체빔으로 사용하기 때문에 입력 이진영상의 형태에 상관없이 항상 일정한 형태의 물체빔을 만들 수 있고, 이로 인해 물체빔과 기준빔 사이의 가시성과 세기 비를 일정하게 조정할 수 있는 장

점이 있었다. 그러므로 기존의 2-단계 PSDH과정에서 문제가 되는 입력영상에 따른 간섭패턴의 시각성이 변하는 문제와 이로 인해 재생되는 영상의 질(quality)이 떨어지는 문제를 동시에 해결할 수 있었다. 제안된 방법의 강화된 보완성은 다양한 컴퓨터시뮬레이션을 통해 검증하였으며, 이진 영상뿐만 아니라 명암도 영상으로까지 확대 적용이 가능할 것으로 판단되어 정보보호 분야뿐만 아니라 기존의 PSDH 기법이 사용되었던 다양한 응용분야에도 적용이 가능하리라고 예상 된다.

## REFERENCE

- [1] T.C. Poon, *Digital Holography and Three-Dimensional Display: Principles and Applications*, Springer, New York, USA, 2006.
- [2] C.S. Kim, "Digital Image Watermarking Technique using Scrambled Binary Phase Computer Generated Hologram in Discrete Cosine Transform Domain, *Journal of Korea Multimedia Society*, Vol. 14, No. 3, pp. 403-413, 2011.
- [3] I. Yamaguchi, "Phase-shifting Digital Holography," *Journal of Optics Letters*, Vol. 22, No. 16, pp. 1268-1270, 1997.
- [4] X.F. Meng, L.Z. Cai, X.F. Xu, X.L. Yang, X. Shen, G.Y. Dong, et al., "Two-step Phase-shifting Interferometry and Its Application in Image Encryption," *Journal of Optics Letters*, Vol. 31, No. 10, pp. 1414-1416, 2006.
- [5] L. Shen, J. Li, and H. Chang, "Double-image Encryption based on Joint Transform Correlation and Phase-shifting Interferometry," *Journal of Chinese Optics Letters*, Vol. 5, No. 12, pp. 687-689, 2007.
- [6] J.P. Liu and T.C. Poon, "Two-step-only Quadrature Phase-shifting Digital Holography," *Journal of Optics Letters*, Vol. 34, No. 3, pp. 250-252, 2009.
- [7] J.P. Liu, T.C. Poon, G.S. Jhou, and P.J. Chen, "Comparison of Two-, Three-, and Four-exposure Quadrature Phase-shifting Holography," *Journal of Optical Society of America*, Vol. 50, No. 16, pp. 2443-2450, 2011.
- [7] C.S. Kim and G.S. Kim, "Phase Image Encryption Using Random Phase Mask and Phase-shift Digital Holography," *Proceeding of the Fall Conference of the Korea Multimedia Society*, Vol. 18, No. 2, pp. 113-115, 2015.
- [9] S. Zhang and J. Zhou, "A New Estimation Method for Two-step-only Quadrature phase-shifting Digital Holography," *Journal of Optics Communication*, Vol. 335, No. 1, pp. 183-188, 2015.
- [10] T.M. Kreis and W.P.O. Juptner, "Suppression of the DC Term in Digital Holography," *Journal of Optical Engineering*, Vol. 36, No. 8, pp. 2357-2360, 1997.
- [11] G.L. Chen, C.Y. Lin, M.K. Kuo, and C.C. Chang, "Numerical Suppression of Zero-order Image in Digital Holography," *Journal of Optics Express*, Vol. 15, No. 14, pp. 8851-8856, 2007.



## 김 철 수

1985년 2월 ~ 1989년 2월 경북대학교 전자공학과 공학사  
 1989년 3월 ~ 1991년 2월 경북대학교 전자공학과 공학석사  
 1991년 3월 ~ 1997년 2월 경북대학교 전자공학과 공학박사  
 1995년 3월 ~ 1998년 2월 김천대학교 전자통신과 전임강사  
 2008년 2월 ~ 2009년 1월 미국 Univ. of Connecticut 방문 연구교수  
 1998년 3월 ~ 현재 경주대학교 전기에너지컴퓨터공학과 교수  
 관심분야 : 광신호처리, 3D 디스플레이, 광암호화, 워터마킹, 뉘-컴퓨터인터페이스 등