《연구논문》 Hankook Kwanghak Hoeji, Volume 17, Number 5, October 2006

# 2-단계 위상 천이 디지털 홀로그래피를 이용한 이진 정보 광 암호화 기법

변현중 · 길상근†

수원대학교 전자공학과

㉾ 445-743 경기도 화성시 봉담읍 와우리 수원대학교 산 2-2

(2006년 9월 1일 받음, 2006년 10월 12일 수정본 받음)

보안 시스템에서 2-단계 위상 천이 홀로그래피를 이용하여 이진 정보 광 암호화 기법을 제안하였다. 위상 천이 디지털 간섭계는 CCD 카메라를 이용하여 위상과 크기 정보를 기록할 수 있는 기법이다. 2-단계 위상 천이는 0과 π/2의 위상 천이 각을 갖도록 PZT 거울을 움직여서 구현하였다. 이진 정보와 암호키는 랜덤 코드와 랜덤 위상으로 표현하였고, 디지털 홀로그램은 푸리에변환 홀로그램으로 간섭무늬는 CCD를 이용하여 256 레벨의 양자화 된 광세기로 획득되었다. 데이터 복원 시 DC 성분 제거 방법을 사용하였다. 컴퓨터 모의실험을 통하여 데이터 복원과 양자화 과정에서의 양자화 레벨 변화량과 디지털 홀로그램 간섭무늬의 오차 픽셀수에 따른 오차 분석을 수행하였다. 이 결과를 이용하여 정보의 광학적 암호화에 적용이 가능함을 확인하였다.

주제어 : Optical encryption, Digital holography, Phase-shifting holography.

## I. 서 론

1990년대에 들어서 멀티미디어 시대의 도래와 함께 사회 전반에 인터넷과 무선 네트워크 같은 정보통신망이 확산되었다. 네트워크 이용자들은 개인정보 유출 및 악용 문제와 네트워크 무단 사용에 대해서 우려하면서 시스템의 보안 문제가 중요시되었다. 하지만 현재 사용하는 디지털 처리(digital processing) 암호화 방법은 보안성에 한계를 갖고 있다. 이러한 문제를 해결하기 위해 1990년대 초부터 Bahram Javidi를 중심으로 디지털 처리가 아닌 아날로그 처리를 하기 위한 암호화/복호화 기법들이 연구되고 있는 가운데 홀로그래피(holography)의 관심이 증가하였다.[1,2] 정보 보안을 위한 여러 가지 시스템이 있겠지만 디지털 홀로그램(digital hologram)을 이용하면 광학적 정보 암호화와 복호화를 컴퓨터 프로세스로 쉽게 처리할 수 있다.[3-5]

두 개의 광이 렌즈를 통해 푸리에 변환(Fourier Transform)되어 간섭된 홀로그램은 복소수로 표현된다. 이러한 복소수 신호는 컴퓨터 프로세스에 많은 어려움을 있으므로 디지털 신호로 바꾸기 위해서 CCD(Charged Coupled Devices) 카메라를 사용한다. CCD 카메라를 사용하면 필름과 같은 저장매질이 불필요하고 아날로그 신호를 디지털 신호로 바꿔 컴퓨터 프로세스를 용이하게 할 수 있다. 반면 제한된 픽셀수와 양자화 과정에서 일부 정보를 잃어버리기 때문에 간섭무늬의 해상도는 떨어지는 단점이 있다. 이러한 단점을 최소화하기 위해서 Skarman이 제안한 신호의 세기와 위상 정보를 모두 알 수 있는 위상 천이 디지털 간섭계(phase-shifting digital holography)를 이용한다. 후에 Javidi 그룹과 Yamaguchi 등에 의해 보완 개선된 위상 천이 디지털 홀로그래피를 이요한 정보 암호화가 연구되었다.[6,7]

본 논문에서는 마흐-젠더 간섭계를 기본으로 Kreis가 발전시킨 DC 성분 제거(DC-term removal) 방법[8]으로 영 차수(zero order) 또는 DC 성분 때문에 이미지를 제대로 복원하지 못하는 점을 보안한 2-단계 위상 천이 디지털 홀로그래피를 이용하여 이진(binary) 정보를 광학적으로 암호화 하는 기법을 제안한다. 2절에서는 디지털 홀로그램의 이론적 배경을 설명하고, 3절에서는 본 논문에서 사용한 암호화에 쓰인 광학적 장치도를 설명한다. 4절에서는 컴퓨터 모의실험을 통해 제안한 기법의 성능을 보이고, 5절에서는 제안한 시스템에서 발생할 수 있는 오차를 분석한 후, 6절에서 결론을 맺도록 하겠다.

## II. 이론적 배경

### 2.1. 디지털 홀로그래피

홀로그램은 물체광(object beam)과 기준광(reference beam)의 간섭으로 표현한다. 본 논문에 사용된 물체광의 함수는 다음과 같다.

$$s(x,y)=|s(x,y)|e^{j\theta_s(x,y)} \tag{1}$$

위 식에서 $|s(x,y)|$는 암호화될 입력의 이진 정보이고, $e^{j\theta_s(x,y)}$는 랜덤 위상 마스크 정보이다. 여기서 $x,y$는 입력 공간 좌표이다. $s(x,y)$를 푸리에 변환하면 다음 식과 같이 표현되고,

$$S(\alpha,\beta)=F\{s(x,y)\}=|S(\alpha,\beta)|e^{j\phi_S(\alpha,\beta)} \tag{2}$$

† E-mail: skgil@suwon.ac.kr

여기서 $\alpha,\beta$는 공간 주파수 좌표이다.

암호화와 복호화에 암호키(key)로 사용될 기준광의 함수는 다음과 같다.

$$r(x,y)=1\cdot\ e^{j\theta_r(x,y)} \tag{3}$$

$|r(x,y)|$가 보안 시스템에서 0과 1로 표현되는 키의 이진 정보이고, 만약 랜덤 이진 코드 $|r(x,y)|$에 $\pi$가 곱해진 $\theta_r(x,y)=\pi\cdot\ |r(x,y)|$가 이진 위상 패턴이 된다면, (3)식에서의 위상함수 $\exp[j\theta_r(x,y)]$는 키 코드 위상 패턴을 나타낸다. 여기서 크기 1은 참조광에서 광학적으로 평행광이 입사됨을 의미한다. $r(x,y)$를 푸리에 변환하면 다음과 같이 표현된다.

$$R(\alpha,\beta)=F\{r(x,y)\}=|R(\alpha,\beta)|e^{j\phi_R(\alpha,\beta)} \tag{4}$$

신호광과 기준광의 간섭으로 CCD 카메라로 획득되는 간섭무늬의 세기는

$$\begin{aligned} I(\alpha,\beta)&=|S(\alpha,\beta)+R(\alpha,\beta)|^2\\ &=|S(\alpha,\beta)|^2+|R(\alpha,\beta)|^2\\ &\quad+2\sqrt{|S(\alpha,\beta)||R(\alpha,\beta)|}\cos\Delta\phi \end{aligned} \tag{5}$$

이며, 여기서 $\Delta\phi=\phi_S-\phi_R$이다.

### 2.2. 2-단계 위상 천이 간섭계

(5)식으로부터 얻은 정보를 가지고는 입력 신호의 크기만 알 수 있고, 위상 정보를 알 수 없기에 정확한 입력 신호를 복원할 수 없다. 위상과 크기의 정보를 모두 구하기 위하여 위상 천이 간섭계를 사용한다.. 위상 천이 간섭계는

$$\begin{aligned} &I_i(\alpha,\beta)=|S(\alpha,\beta)|^2+|R(\alpha,\beta)|^2\\ &+2\sqrt{|S(\alpha,\beta)||R(\alpha,\beta)|}(\cos\Delta\phi+\phi_i) \end{aligned} \tag{6}$$

$i=2,3,4,...$로 표현 되며, 2-단계 위상 천이 간섭계는 $i=2$인 경우이다.

2-단계 위상 천이 간섭계의 위상 천이 각을 각각 $0,\pi/2$라 하고, (6)식을 표현하면

$$\begin{aligned} I_1(\alpha,\beta)&=|S(\alpha,\beta)|^2+|R(\alpha,\beta)|^2\\ &\quad+2\sqrt{|S(\alpha,\beta)||R(\alpha,\beta)|}\cos\Delta\phi\\ I_2(\alpha,\beta)&=|S(\alpha,\beta)|^2+|R(\alpha,\beta)|^2\\ &\quad+2\sqrt{|S(\alpha,\beta)||R(\alpha,\beta)|}\cos(\Delta\phi+\frac{\pi}{2}) \end{aligned} \tag{7}$$

과 같이 기술된다. 이는 암호화 하고자 하는 이진 입력 정보의 암호화된 두 개의 광세기를 나타내며 암호화된 정보는 전송되거나 저장될 수 있다. 여기서 DC 성분을 나타내는 $|S(\alpha,\beta)|^2+|R(\alpha,\beta)|^2$을 $A(\alpha,\beta)$로, AC 성분의 크기를 나타내는 $2\sqrt{|S(\alpha,\beta)||R(\alpha,\beta)|}$를 $B(\alpha,\beta)$라 놓으면 다음과 같이 다시 표현할 수 있다.

$$\begin{aligned} I_1(\alpha,\beta)&=A(\alpha,\beta)+B(\alpha,\beta)\cos\Delta\phi\\ I_2(\alpha,\beta)&=A(\alpha,\beta)+B(\alpha,\beta)\cos(\Delta\phi+\frac{\pi}{2})\\ &=A(\alpha,\beta)+B(\alpha,\beta)\sin\Delta\phi \end{aligned} \tag{8}$$

CCD 카메라에 획득된 두 개의 간섭무늬 세기를 나타내는 (8)식에서 DC 성분인 $A(\alpha,\beta)$를 제거하여 수정된 간섭무늬의 세기를 구하면

$$\begin{aligned} I_1'&=I_1-A(\alpha,\beta)=B(\alpha,\beta)\cos\Delta\phi\\ I_2'&=I_2-A(\alpha,\beta)=B(\alpha,\beta)\sin\Delta\phi \end{aligned} \tag{9}$$

이다. 이 식을 이용하여 신호광과 기준광의 위상차를 구할 수 있고,

$$\begin{aligned} &\frac{I_1'}{I_2'}=\frac{\sin\Delta\phi}{\cos\Delta\phi}=\tan\Delta\phi\\ &\Delta\phi=\phi_S-\phi_R=\tan^{-1}\left(\frac{I_1'}{I_2'}\right) \end{aligned} \tag{10}$$

이다. 위 식으로부터 우리가 사용한 알고리즘에서 간섭무늬의 위상정보를 알기 위해서는 DC 성분을 꼭 제거해야만 한다는 것을 알 수 있다.

위의 (8), (9)식을 활용하여 AC 성분의 크기를 구하면 다음과 같다.

$$\sqrt{|S(\alpha,\beta)||R(\alpha,\beta)|}=\frac{1}{2}\sqrt{(I_1')^2+(I_2')^2} \tag{11}$$

지금까지 구한 위상과 크기로부터 복소 홀로그램은 아래와 같이

$$H(\alpha,\beta)=|S(\alpha,\beta)||R(\alpha,\beta)|e^{j\Delta\phi} \tag{12}$$

로 나타낼 수 있으며, 이 복소 홀로그램과 우리가 알고 있는 키 정보를 이용하면 원래의 이진 입력 정보의 복소 분포를 복원할 수 있다.

$$\begin{aligned} D(\alpha,\beta)&=\frac{H(\alpha,\beta)R(\alpha,\beta)}{|R(\alpha,\beta)|^2}\\ &=\frac{|S(\alpha,\beta)||R(\alpha,\beta)|e^{j(\phi_S-\phi_R)}|R(\alpha,\beta)|e^{j\phi_R}}{|R(\alpha,\beta)|^2}\\ &=S(\alpha,\beta)e^{j\phi_S} \end{aligned} \tag{13}$$

(13)식을 역 푸리에변환을 하면 복원된 데이터 $d(x,y)$는 본래의 입력 정보 $s(x,y)$와 같다.

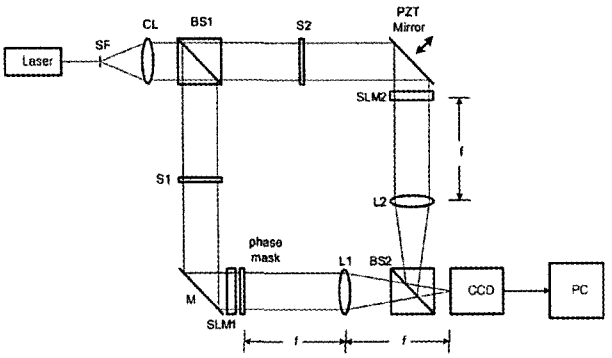



그림 1. 광학적 암호화 장치도.
SF: spatial filter, CL: collimating lens,
BSs: beam splitter, S: shutter, M: mirror,
Ls: lenses.

$$d(x,y)=F^{-1}\{D(\alpha,\beta)\}=F^{-1}\{S(\alpha,\beta)\}=s(x,y) \tag{14}$$

## III. 암호화를 위한 광학적 장치도

그림 1은 본 논문에서 마흐-젠더 간섭계의 2-단계 위상천이 디지털 홀로그래피를 이용한광학적 암호화 장치도이다.

빔 분리기(beam splitter) BS1는 시준광을 물체광과 기준광으로 나눈다. 셔터 S1을 열면 물체광은 거울 M에서 반사되어 이진 데이터가 표현될 SLM(spatial light modulator)1과 랜덤 위상 마스크(random phase mask)로 조사된다. SLM1에 표현된 이진 입력 정보와 랜덤 위상 마스크가 곱해진 형태는 푸리에 렌즈 L1을 거쳐 푸리에 변환된다. 셔터 S2를 열면 기준광은 위상 천이 각을 전기적으로 조절할 수 있는 PZT거울에서 반사되어 위상 타입의 SLM2로 조사된다. 이것은 푸리에 렌즈 L2을 거쳐 푸리에 변환된다. 물체광과 기준광이 렌즈를 거쳐 푸리에 변환되는 초점거리 $f$에 CCD 카메라를 설치하여 간섭무늬를 얻고, 이 간섭무늬는 입력 정보의 암호화한 형태를 지니게 되며 컴퓨터에 저장되거나 다른 컴퓨터로 전송되어진다. 두 개의 렌즈를 직렬로 두어 4개의 초점거리를 갖는 $4f$ 시스템에서는 입력 공간 영역과 푸리에 공간 주파수 영역에 두 개의 위상 마스크를 사용하였지만 본 논문에서 제안한 광학 시스템에서는 입력 공간 영역에 하나의 랜덤 마스크를 두고 위상 타입의 SLM을 사용하였고, 푸리에 공간 주파수 영역에 위상 마스크 패턴을 위치시키지 않았기 때문에 광학적 정렬구조를 쉽게 하였다.

입력 데이터 정보의 암호화하는 과정은 다음과 같다. 셔터 S1과 S2 모두 열고, PZT 거울을 조정하여 두 개의 간섭무늬 $I_1$과 $I_2$을 얻는다. 두 개의 간섭무늬에서 DC 성분을 제거해야 위상 정보를 구할 수 있기 때문에 DC 성분을 나타내는 신호광과 기준광의 크기 정보를 얻어야 한다. 그러므로 S1은 열고 S2는 닫아 물체광만 크기 정보를 얻고, S1은 닫고 S2는 열어 신호광만 세기 정보를 얻는다. 이렇게 얻은 4개의 광세기 정보를 가지고 앞 절의 이론적 배경에서 구한 수식을 이용하면 원래의 입력 정보를 복원할 수 있다.

## IV. 오차 분석

이상적인 경우 (14)식과 같이 복원된 데이터의 정보 $d(x,y)$와 입력 정보 $s(x,y)$는 일치한다. 이 절에서는 데이터 복호화 과정에서 오차가 발생하였을 경우 $d(x,y)$와 $s(x,y)$가 어느 정도 일치하는지에 대한 복호화 성능을 분석한다. 아날로그 신호인 간섭무늬를 CCD로 받기 위해서는 CCD가 허용하는 양자화 레벨(gray level)의 디지털 신호로 바뀌어야 한다. 본 논문에서는 256 레벨의 CCD를 사용하였기에 모든 간섭무늬는 256 양자화 레벨로 표현하였다. 이 과정에서 CCD 상에 작은 세기 변화량 $\Delta_g$로 인해 CCD 상에서의 간섭무늬 세기는 $\Delta_g$만큼 크거나 작게 인식되어 256 양자화 레벨 오차가 발생할 수 있고, 이 때문에 데이터 복원 시 입력과 다른 신호를 복원하는 원인이 될 수 있다. 또 다른 오차 발생 경우는 복원 시 사용할 암호키 데이터의 작은 오차가 발생하였음에도 불구하고 원래의 입력 정보가 제대로 복원되는 경우이다.

복원된 데이터와 입력 정보와의 픽셀 오차 개수 $N_E$는 다음과 같은 표현식으로 나타낼 수 있다.

$$N_E=\sum_{x=1}^{N_X}\sum_{y=1}^{N_Y}|d(x,y)-s(x,y)|^2 \tag{15}$$

여기서 $N_X$와 $N_Y$는 데이터의 가로와 세로 픽셀 사이즈를 나타낸다.

$$MSE=\frac{1}{N_X}\frac{1}{N_Y}\sum_{x=1}^{N_X}\sum_{y=1}^{N_Y}|d(x,y)-s(x,y)|^2 \tag{16}$$

MSE(Mean Square Error)는 (15)식을 전체 픽셀 개수로 나눈 것으로 복원 데이터의 오차 확률을 뜻한다.

위에서 언급한 오차 발생 두 경우 중 양자화 과정에서 오차가 발생한 경우를 수식적으로 살펴보기 위하여 복소 홀로그램을 표시하면,

$$H_1=|S_g(\alpha,\beta)||R_g(\alpha,\beta)|e^{j\Delta\phi_g} \tag{17}$$

이다, 여기서 $|S_g(\alpha,\beta)||R_g(\alpha,\beta)|$는 오차를 가지고 CCD에 획득되어 256 그레이 레벨로 양자화 된 간섭무늬로부터 계산된 크기를 말하며 $|S_g(\alpha,\beta)||R_g(\alpha,\beta)|=|S(\alpha,\beta)||R(\alpha,\beta)|+A_e$로 다시 표현된다. 여기서, $A_e$는 추가된 오차 크기를 말한다. $\Delta\phi_g$는 마찬가지로 256 그레이 레벨로 양자화 된 간섭무늬로부터 계산된 위상을 말하며 $\Delta\phi_g=(\phi_S-\phi_R)+\phi_e$로 다시 표현된다. 여기서, $\phi_e$는 추가된 오차 위상을 말한다. 이로부터 복원된 복소 분포를 계산하면,

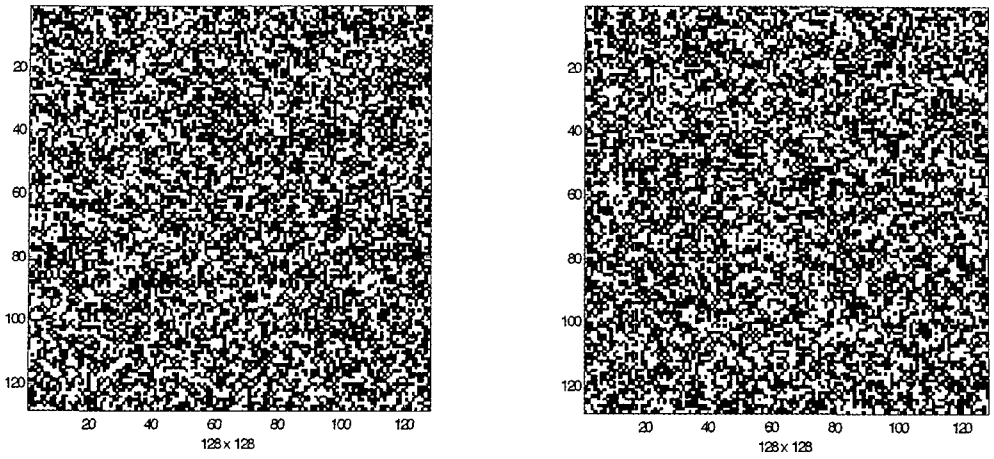



그림 2. (a)랜덤 생성한 이진 데이터,(b)랜덤 생성한 이진 암호키.

$$D(\alpha,\beta)=\frac{H_1 \bullet R(\alpha,\beta)}{|R(\alpha,\beta)|^2} \tag{18}$$
$$=\frac{|S_g(\alpha,\beta)\|R_g(\alpha,\beta)|e^{j\Delta\phi_g} \bullet |R(\alpha,\beta)|e^{j\phi_R}}{|R(\alpha,\beta)|^2}$$
$$=S(\alpha,\beta)e^{j(\phi_S+\phi_e)}+E_1(\alpha,\beta)$$

이다. 여기서 $E_1(\alpha,\beta)$은 발생한 오차의 복소 분포이며, $\frac{A_e e^{j(\phi_S+\phi_e)}}{|R(\alpha,\beta)|}$로 나타낼 수 있다.

(18)식을 역 푸리에변환을 하면,

$$d(x,y)=F^{-1}\{D(\alpha,\beta)\} \tag{19}$$
$$=F^{-1}\{|S(\alpha,\beta)|e^{j(\phi_S+\phi_e)}\}+F^{-1}\{E_1(\alpha,\beta)\}$$

이다. (18)식에서 $\phi_e=0$, $A_e=0$이면,

$$d(x,y)=F^{-1}\{S(\alpha,\beta)\}=s(x,y) \tag{20}$$

로 복원된 데이터와 입력 정보가 같고, 식 (18)에서 $\phi_e\neq 0$, $A_e\neq 0$이면,

$$d(x,y)=s(x,y)+e_1(x,y) \tag{21}$$

로 복원된 데이터는 원래 입력 정보에 오차 함수 $e_1(x,y)$가 추가된 형태로 나타난다.

다음은 복원 시 암호키의 오차가 발생한 경우를 수식적으로 살펴보기 위하여 복소 홀로그램을 표시하면,

$$H_1=|S(\alpha,\beta)\|R(\alpha,\beta)|e^{j\Delta\phi} \tag{22}$$

이다. 오차가 생긴 암호키 $r_f(x,y)$의 푸리에변환을 $R_f(\alpha,\beta)$라 하고 오차를 유발하는 복소 분포를 $R_e(\alpha,\beta)$라 하면, $R_f(\alpha,\beta)=R(\alpha,\beta)+R_e(\alpha,\beta)$가 된다. 여기서 $R(\alpha,\beta)$는 (3)식에 표현된 것과 같이 오차가 없는 암호키의 푸리에 변환된 복소 분포를 나타낸다. 이를 가지고 복원된 복소 분포를 계산하면 다음과 같다.

$$D(\alpha,\beta)=\frac{H_1 \bullet R_f(\alpha,\beta)}{|R(\alpha,\beta)|^2} \tag{23}$$
$$=\frac{|S(\alpha,\beta)\|R(\alpha,\beta)|e^{j\Delta\phi} \bullet R_f(\alpha,\beta)}{|R(\alpha,\beta)|^2}$$
$$=S(\alpha,\beta)e^{j(\phi_S+\phi_e)}+E_2(\alpha,\beta)$$

여기서 $E_2(\alpha,\beta)$는 발생한 오차이며, $\frac{|S(\alpha,\beta)\|R(\alpha,\beta)|e^{j(\phi_S-\phi_R)} \bullet R_e(\alpha,\beta)}{|R(\alpha,\beta)|^2}$로 나타낼 수 있다.

(23)식을 역 푸리에변환을 하면,

$$d(x,y)=F^{-1}\{D(\alpha,\beta)\}=F^{-1}\{S(\alpha,\beta)\}+F^{-1}\{E_2(\alpha,\beta)\} \tag{24}$$

이다. (23)식에서 $R_e=0$이면,

$$d(x,y)=F^{-1}\{S(\alpha,\beta)\}=s(x,y) \tag{25}$$

로 복원된 데이터와 입력 정보가 같고, (23)식에서 $R_e\neq 0$이면,

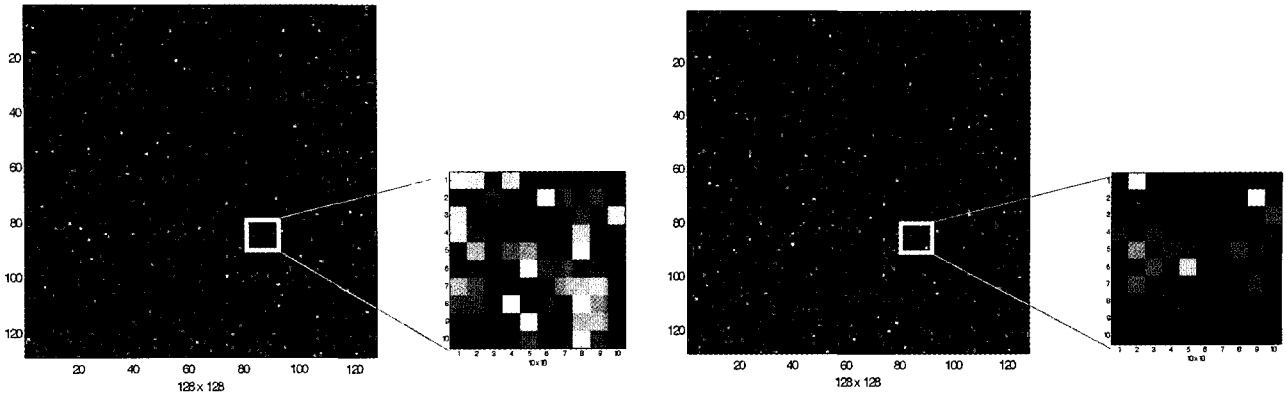
$$d(x,y)=s(x,y)+e_2(x,y) \tag{21}$$

로 복원된 데이터는 원래 입력 정보에 오차 함수 $e_2(x,y)$가 추가된 형태로 나타난다.

## V. 컴퓨터 모의실험

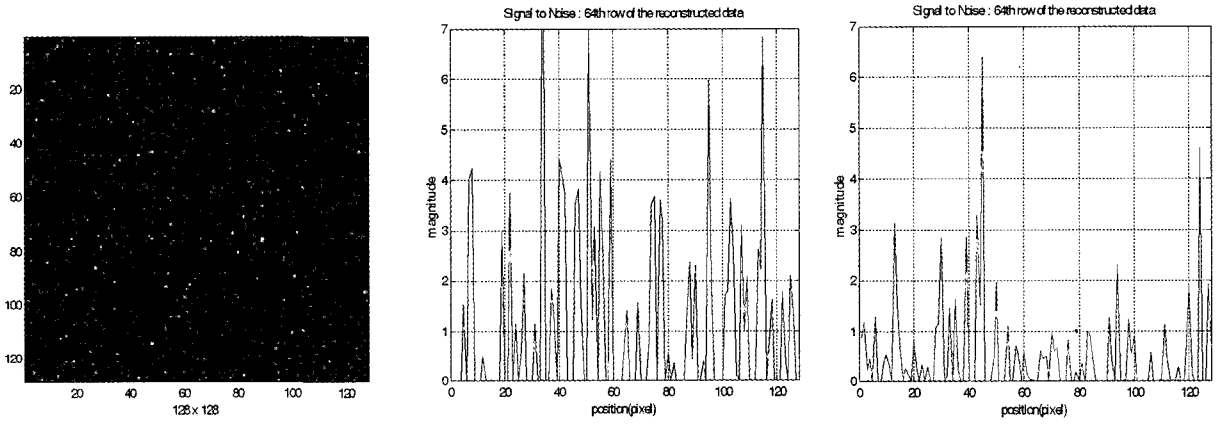
제안한 기법의 성능을 알아보기 위하여 이진 데이터와 이진 이미지로 컴퓨터 모의실험을 하였다.

그림 2.(a)는 랜덤 생성한 입력 데이터이고, (b)는 랜덤 생




(a) (b)

그림 3. 위상 천이 디지털 홀로그래피를 이용하여 얻은 홀로그램.
(a)위상 천이 각이 0일 때, (b)위상 천이 각이 $\pi/2$일 때




(a) (b) (c)

그림 4. 올바르지 않은 키로 복원하였을 때 (a)복원된 데이터 패턴, (b) (a)의 64번째 줄의 신호 비트, (c) (a)의 64번째 줄의 잡음 비트.

성한 암호키이다. 모두 이진 데이터이고 픽셀의 크기는 128×128 이다.

그림 3은 그림 2의 (a)와 (b)를 2-단계 위상 천이 디지털 홀로그래피에 적용하여 암호화된 디지털 홀로그램 간섭무늬이다. (a)는 위상 천이 각이 0일 때이고, (b)는 위상 천이 각이 $\pi/2$일 때이다. 각각 256 그레이 레벨로 양자화 되었다.

그림 4, 5, 6은 이진 데이터의 복호를 보여준다.

그림 4는 올바르지 않은 키 정보를 사용하여 복호 과정을 수행하였을 경우이다. 그림 4.(a)는 복원된 데이터 패턴으로 본래의 입력 데이터와 일치하지 않음을 보여준다. (b)와 (c)는 복원한 데이터 패턴의 64번째 줄을 분석한 결과이다. (b)에서 신호 비트란 입력 데이터에서 1인 부분이 올바르게 크기 성분을 갖는 부분이고, (c)에서 잡음 비트란 입력 데이터에서 0인 부분이 데이터 복원 시 0으로 복원되지 않고 일정 크기 성분을 가지고 있어 복원 과정에서 에러를 유발하는 부분이다. 그림에서 알 수 있듯이 (c)의 잡음 비트가 일부 신호 비트보다 크므로 올바른 복원이 되지 않는다. 홀로그래피의 특성상 기준광이 올바르지 않으면 물체광이 재생되지 않음을 보여준다.

올바른 복원과정에서 올바른 키를 사용하였으나, 복호 과정 중 두 개의 간섭무늬에서 DC 성분 제거를 하지 않은 경우의 결과를 그림 5가 보여준다. 2-단계 위성 천이 간섭계에서는 4-단계 위상 천이 간섭계와 달리 DC 성분을 제거 하지 않으면 간섭무늬에서 가운데의 DC 성분의 너무 강하여 주변의 작은 AC성분들의 위상 정보를 잃어버려 크기와 위상이 제대로 복원되지 않는다. 그림에서 보듯이 일부 그림 5.(c)의 잡음 비트가 (b)의 신호 비트보다 커서 (a)와 같이 원 데이터와 같이 복원되지 않았다.

올바른 키를 사용하고, 복호 과정 중 두 개의 간섭무늬에서 DC 성분을 제거한 경우가 그림 6이다. DC 성분을 제거해야 식 (9),(10)같이 광 정보의 위상성분까지 정확히 알 수 있다. 그림 6.(a)는 복원된 패턴으로 입력 데이터와 거의 비슷한 패턴을 나타내고 있다. (c)의 신호 비트의 크기를 보면 크기가 약 1이고 (d)의 잡음 비트의 크기를 보면 약 0.1 이하이므로 이 경우 신호 대 잡음비는 약 10이다. (d)의 잡음 비트를 모두 제거하기 위해 0.5의 문턱 값으로 (a)를 후처리하면 (b)과 같은 본래의 입력 데이터와 똑같은 패턴을 복원할 수 있다.

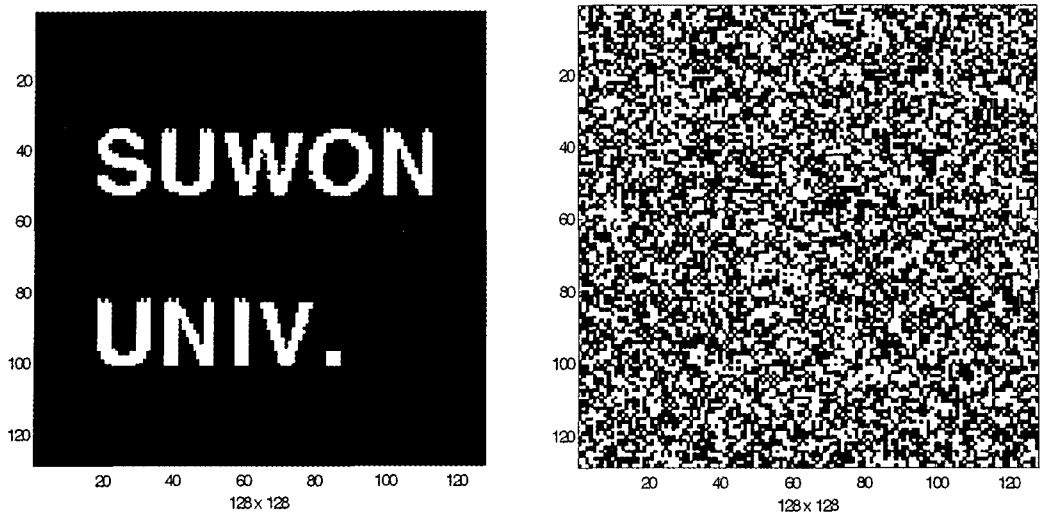



그림 7. (a)이진 영상, (b)랜덤 생성한 이진 암호키.

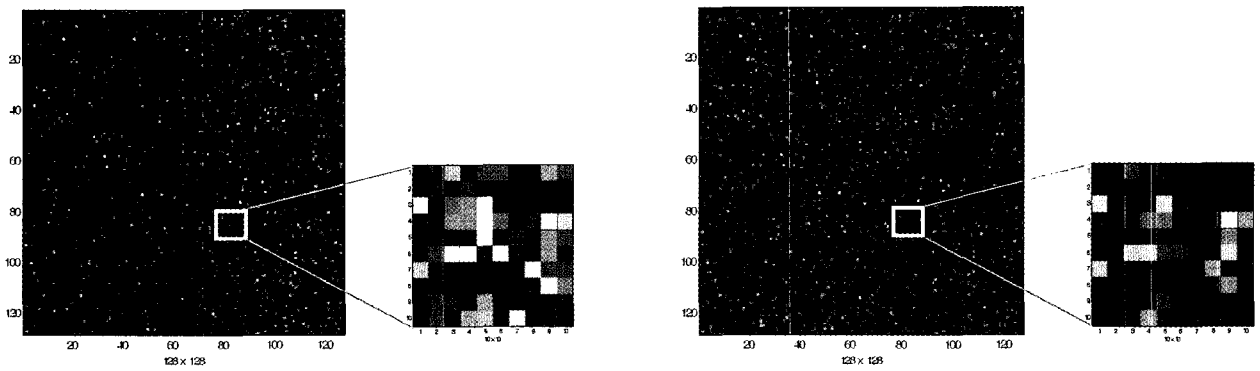



그림 8. 위상 천이 디지털 홀로그래피를 이용한 홀로그램.
(a)위상 천이 각이 0일 때, (b)위상 천이 각이 π/2일 때

다음은 입력 신호가 랜덤 이진 데이터가 아닌 이진 영상으로 실험한 결과이다.

그림 7은 각각 128×128 픽셀로 제작된 이진 영상(a)과 랜덤 생성한 이진 암호키(b)이다.

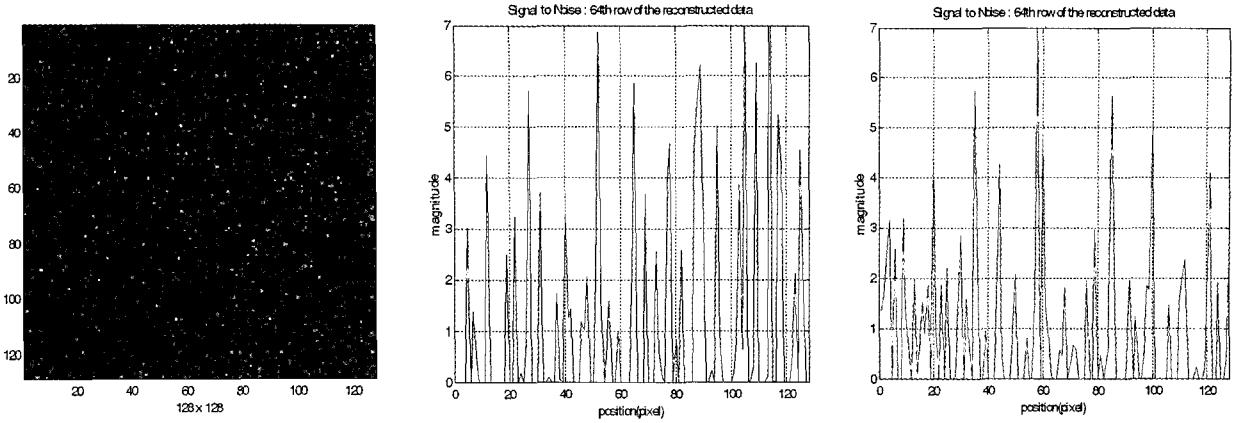
그림 8은 그림 7의 (a)와 (b)를 2 단계 위상 천이 디지털 홀로그래피에 적용하여 암호화된 디지털 홀로그램 간섭무늬이다. (a)는 위상 천이 각이 0일 때이고, (b)는 위상 천이 각이 $\pi/2$일 때이다. 각각 256 그레이 레벨로 양자화 되었다.

그림 9, 10, 11은 이진 영상의 복호를 보여준다.

그림 9의 (a)는 올바르지 않은 키를 사용하여 복원된 패턴이다. (b)와 (c)는 재생된 영상의 47번째 줄의 신호 비트와 잡음 비트의 크기 성분을 나타낸다. (b)와 (c)에서 볼 수 있듯이 일부 신호 비트가 잡음 비트보다 작아 복원이 되지 않은 경우이다.

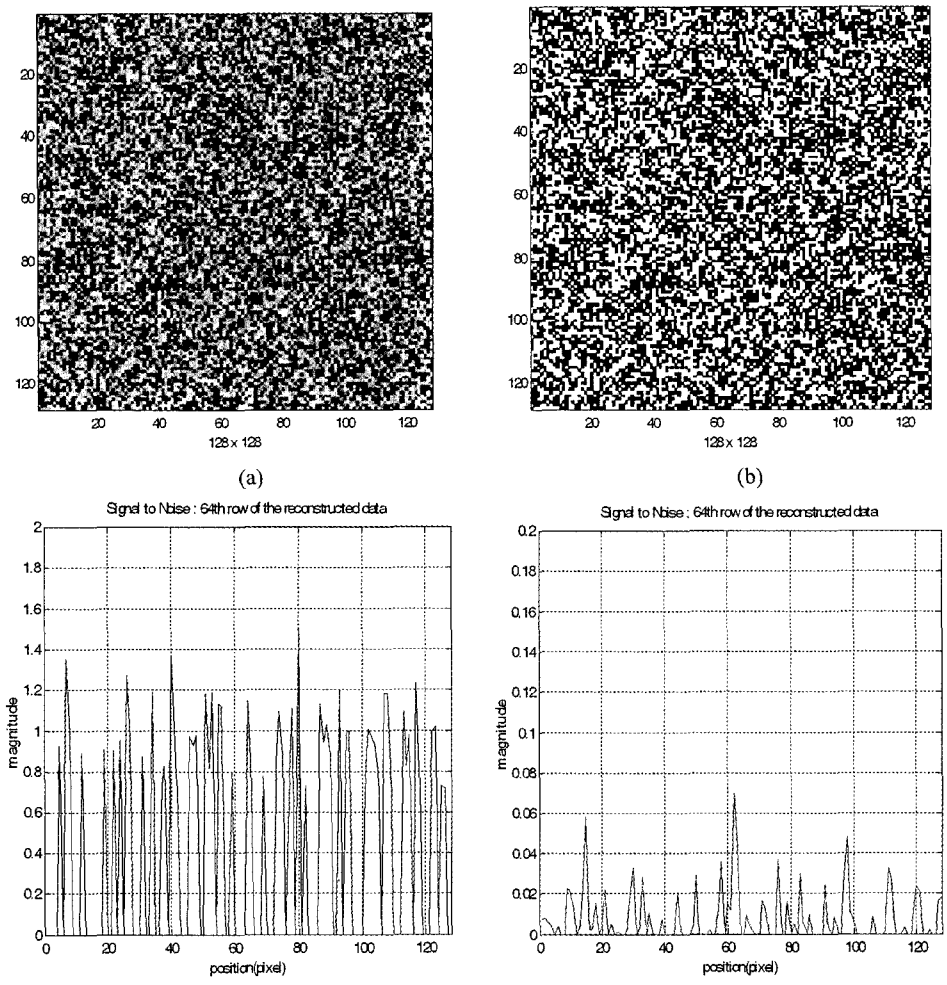
올바른 복원과정에서 올바른 키를 사용하였으나, 복호 과정 중 두 개의 간섭무늬에서 DC 성분 제거를 하지 않은 경우의 결과를 그림 10에서 보여준다. (c)와 (d)에서 살펴보면 (d)의 잡음 비트는 약 1 정도의 크기 성분이므로 잡음 비트를 제거 하기위해 1.0의 문턱 값으로 후처리하면 (c)에서 동그라미 부분처럼 신호 비트도 같이 제거 된다. 따라서 (b)처럼 일부 신호 비트가 제거 되어 에러가 나타난 영상 패턴을 얻게 된다. 이러한 영상 패턴은 신호 정보가 국한적인 부분에 몰려있어 복호화 과정에서 위상 정보 없이 크기 성분의 정보만 가지고도 비슷한 영상으로 재생되지만 결과적으로 그릇된 이미지이다. 만일, 랜덤 생성한 데이터와 같이 0과 1이 비교적 고루 분포된 이미지를 사용하면 원래의 데이터를 추측 혹은 유추할 수 없을 것이다.

그림 11은 올바른 키를 사용하고 DC 성분을 제거한 경우이다. (a)는 복원된 영상 패턴이다. (c)의 신호 비트 크기는 약 1이고, (d)의 잡음 비트 크기는 약 0.01이하 이므로 신호 대 잡음비는 약 100정도로 말할 수 있다. (d)의 잡음 비트를 제거하기 위해 0.5의 문턱 값으로 후처리하면 (b)과 같이 본




(a) (b) (c)

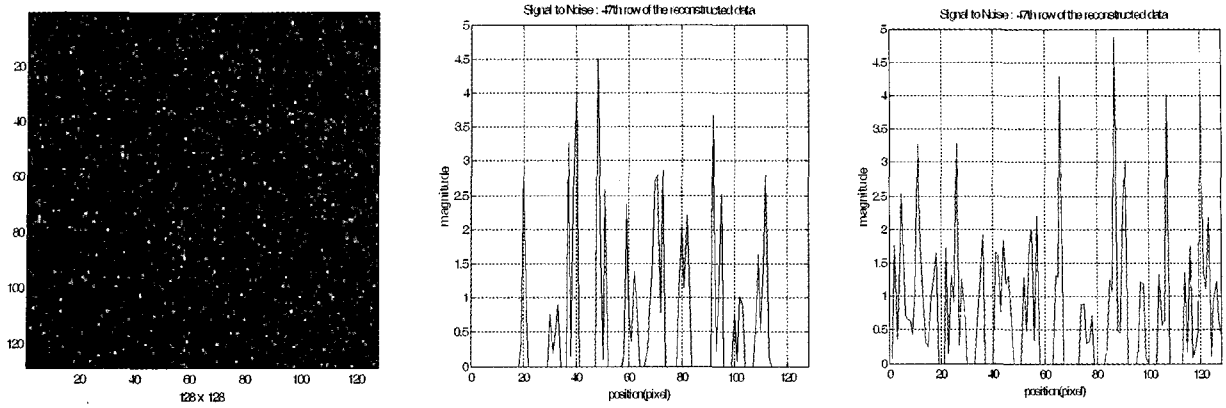
그림 5. 올바른 키를 사용하였으나 복원과정에서 DC 성분을 제거하지 않았을 때 (a)복원된 데이터 패턴, (b) (a)의 64번째 줄의 신호 비트, (c) (a)의 64번째 줄의 잡음 비트.




(a) (b)

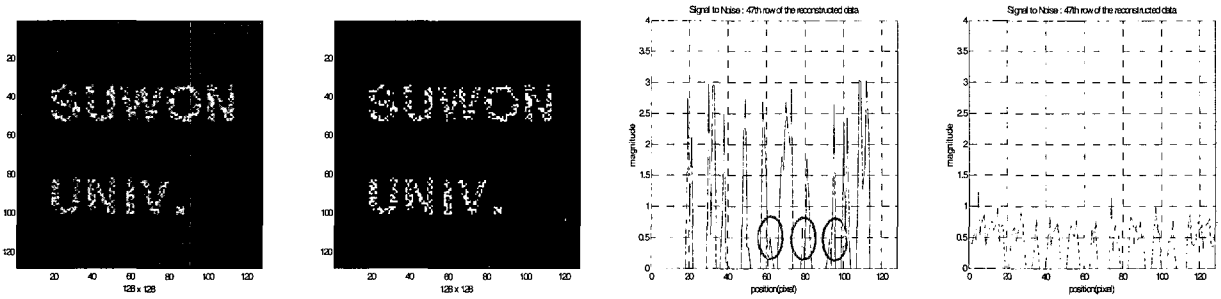
(c) (d)

그림 6. 올바른 키를 사용하고 복원과정에서 DC 성분을 제거하였을 때 (a)복원된 데이터 패턴, (b) 문턱 값 0.5로 후처리한 패턴, (c) (a)의 64번째 줄의 신호 비트, (d) (a)의 64번째 줄의 잡음 비트.



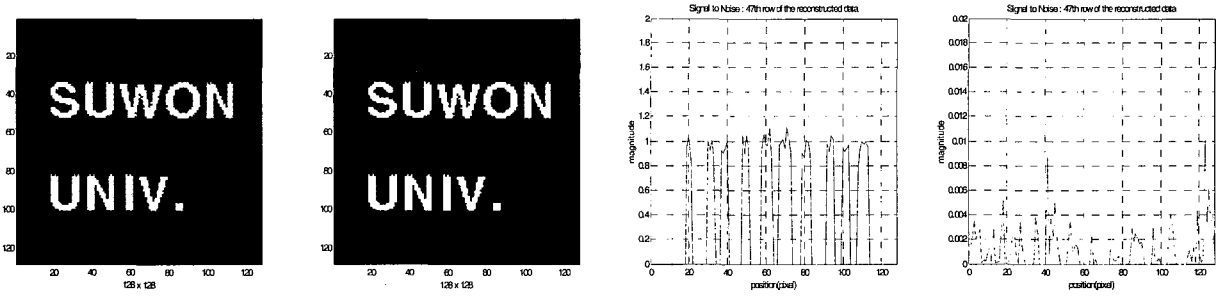

(a) (b) (c)

그림 9. 올바르지 않은 키로 복원하였을 때 (a)복원된 영상 패턴, (b) (a)의 47번째 줄의 신호 비트, (c) (a)의 47번째 줄의 잡음 비트.




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

그림 10. 올바른 키를 사용하였으나 DC 성분을 제거하지 않았을 때 (a)복원된 영상 패턴, (b) 문턱 값 1.5로 후처리한 패턴, (c) (a)의 47번째 줄의 신호 비트, (d) (a)의 47번째 줄의 잡음 비트.




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

그림 11. 올바른 키를 사용하고 복원과정에서 DC 성분을 제거하였을 때 (a)복원된 데이터 패턴, (b) 문턱값 0.5로 후처리한 패턴, (c) (a)의 47번째 줄의 신호 비트, (d) (a)의 47번째 줄의 잡음 비트.

래의 영상과 똑같은 정보를 얻을 수 있다.

다음은 두 가지 오차 발생 경우에 대한 픽셀의 오차 증가에 따른 데이터 복원 시 오차 픽셀 개수와 MSE를 나타낸 그래프이다. 그림 2에 나타난 랜덤 생성한 이진 데이터와 이진 암호키를 사용하였고, 오차 발생 픽셀 역시 랜덤으로 선택하였다. 모든 결과 그래프는 100번 반복 실험한 결과의 평균을 나타낸다.

그림 12와 그림 13은 양자화 레벨 변화량 $\Delta_g$가 ±1일 때, 랜덤 선택된 디지털 홀로그램 간섭무늬의 픽셀 수를 변화시키며 나타나는 복원 데이터의 MSE와 오차 픽셀 개수를 보여주고 있다. 그림 13에서 보면 디지털 홀로그램의 오차 픽셀이 약 3,500개 정도에서부터 복원 시 에러가 한 개씩 나타남을 알 수 있다. 디지털 홀로그램의 오차 픽셀이 증가할수록 복원이 되지 않는 것을 보여준다.

그림 14와 그림 15에서는 양자화 레벨 변화량 $\Delta_g$가 ±1, ±2, ±3 일 때, 데이터 복원 시 나타나는 MSE와 오차 픽셀 개수를 함께 도시하였다. 그림 15에서 보면 $\Delta_g$가 ±2일 때는 약 900 픽셀부터, $\Delta_g$가 ±3일 때는 약 400 픽셀부터 에러가

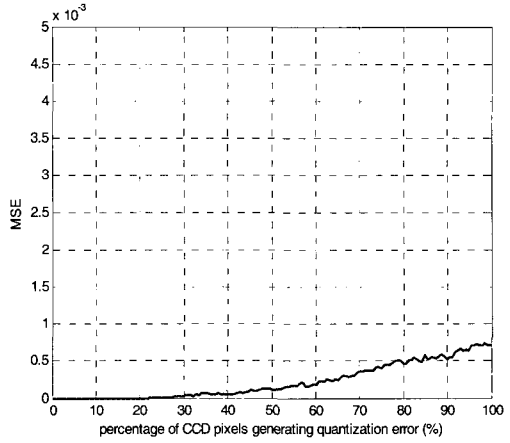



그림 12. 256 gray level CCD에서 양자화 레벨 변화량 $\Delta_g$이 ±1 일 때, CCD 오차 픽셀 변화에 따른 복원 데이터의 MSE.

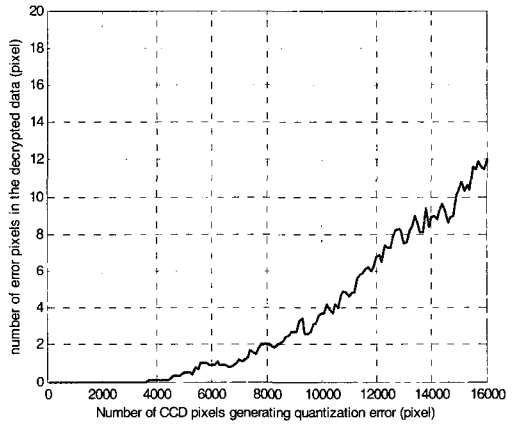



그림 13. 256 gray level CCD에서 양자화 레벨 변화량 $\Delta_g$이 ±1 일 때, CCD 오차 픽셀 변화에 따른 복원 데이터의 오차 픽셀 개수.

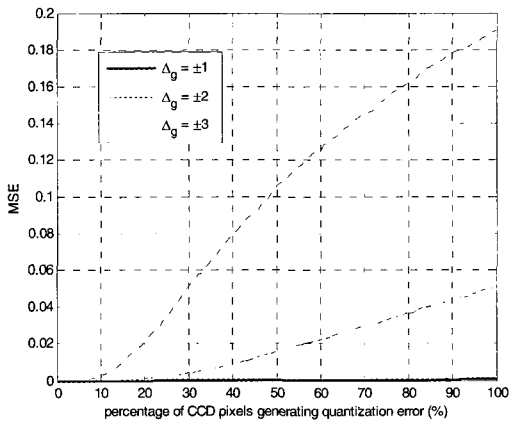



그림 14. 양자화 레벨 변화량 $\Delta_g$이 ±1, ±2, ±3 일 때, CCD 오차 픽셀 변화에 따른 복원 데이터의 MSE.

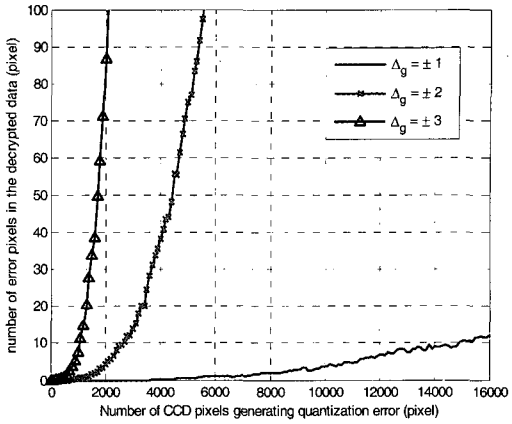



그림 15. 양자화 레벨 변화량 $\Delta_g$이 ±1, ±2, ±3 일 때, CCD 오차 픽셀 변화에 따른 복원 데이터의 오차픽셀 개수.

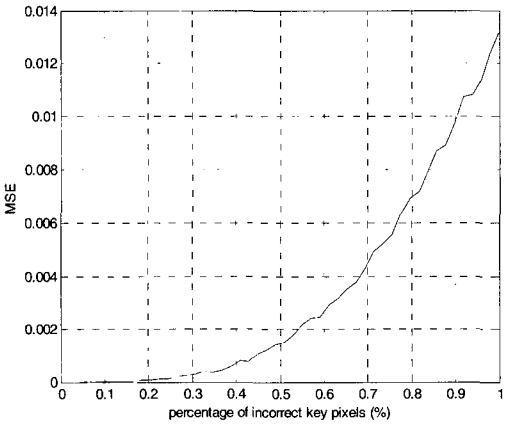



그림 16. 이진 암호키의 오차 비율에 따른 복원 데이터의 MSE.

발생하여 정확한 입력 정보가 복원이 되지 않음을 알 수 있다. 양자화 레벨 변화량 $\Delta_g$가 증가할수록 복원 시 에러가 커져 복원이 되지 않음을 보여준다.

그림 16과 그림 17은 복원 시 이진 암호키의 오차에 따른 MSE와 데이터 복원 오차 픽셀 수를 나타내는 그래프이다. 그림 17에서 볼 수 있듯이 이진 암호키의 오차 픽셀이 8개가 발생하였음에도 불구하고 원래 데이터가 에러 없이 복원되었으며, 이는 홀로그래피의 특징인 연상 저장(associative memory) 능력에 기인된 것으로 보인다. 하지만 전체 128×128=16,384 픽셀의 암호키 데이터 중 8개 픽셀의 오차는 약 0.05%이하로 미미하다고 할 수 있다.

## VI. 결 론

본 논문에서는 2-단계 위상 천이 디지털 홀로그래피를 이용하여 이진 정보의 광학적 암호화 기법을 제안하였다. 256 그레이 레벨을 가지는 CCD로 0과 $\pi/2$의 위상 천이 각을 갖는 두 개의 홀로그램 간섭무늬와 신호광과 기준광의 크기 성

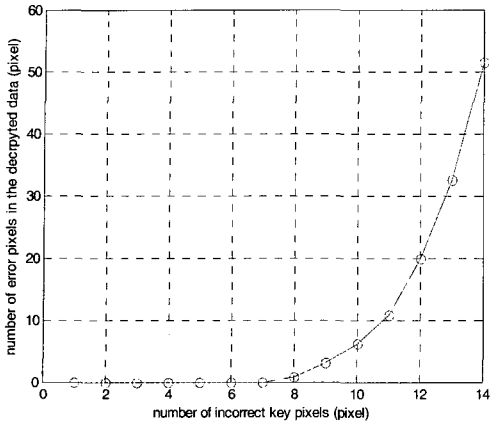



그림 17. 이진 암호키의 픽셀 오차에 따른 복원 데이터의 오차 픽셀 개수.

분을 획득하여 입력 정보를 복원하였다. 마흐-젠더 간섭계를 기본으로 하였고, 위상 타입의 SLM을 사용하여 랜덤 위상 마스크를 하나만 사용하도록 하였다. 이진 데이터와 영상 복원 시 DC 성분의 제거가 필수임을 확인할 수 있었다. 신호대 잡음비는 랜덤 생성한 이진 데이터의 경우는 약 10, 실험에 사용한 이진 영상의 경우는 약 100 정도를 나타내었다. CCD 상에서의 256 양자화 과정 중 생기는 양자화 레벨 변화량과 오차 픽셀 개수가 증가할수록 복원 시 에러가 발생하는 픽셀 수도 증가하였다. 양자화 레벨 변화량 $\Delta_g$가 ±1, ±2, ±3 일 때 디지털 홀로그램 간섭무늬의 오차 픽셀이 약 3,500, 900, 400 픽셀 이상부터 복원 시 에러가 나타나기 시작하였다. 이진 암호키의 정보는 8개 픽셀이하 일치하지 않더라도 본래의 입력 정보가 복원되었다. 위상 천이 간섭계 중에 대표적인 4-단계 위상 천이 간섭계는 $0, \pi/2, \pi, 3\pi/2$의 4개의 위상 천이 각을 갖는다. 이 기법은 정보 복원 과정에서 4개의 간섭무늬를 획득해야 하기에 2개의 간섭무늬를 획득해야하는 2-단계 위상 천이 간섭계보다 많은 데이터가 요구된다. 때문에 컴퓨터 프로세스 및 데이터의 전송 관점에서 보면 데이터의 양이 적은 2-단계 위상 천이 간섭계가 4-단계 위상 천이 간섭계보다 더 효율적이라 할 수 있다. 정보 암호화 시스템에서 2-단계 위상 천이 디지털 홀로그래피 기법을 이용한 광 암호화 장치를 구현할 수 있으며, 암호화된 홀로그램 정보로부터 원래의 정보를 완벽하게 복원할 수 있음을 확인하였다.

## 감사의 글

본 논문은 한국과학재단 목적기초연구(R01-2005-000-10528-0(2005)) 지원으로 수행되었습니다.

## 참고문헌

[1] B.Javidi , J.L.Horner, "Optical pattern recognition for validation and security verification", *Opt. Eng.*, vol. 33, pp. 1752-1756, 1994.

[2] P.Refregier, B.Javidi, "Optical image encryption using input plane and Fourier plane random encoding", *Opt. Lett.*, ol. 34, pp. 6012-6015, 1995.

[3] G. Unnikrishnan and K. Singh, "Double random fractional Fourier domain encoding for optical security", *Opt. Eng.*, vol. 39, pp.2853-2859, 2000.

[4] B. Javidi , T. Nomura, "Securing information by means of digital holography", *Opt. Lett.*, vol. 25, pp.28-30, 2000.

[5] T. Nomura, A. Okazaki and B. Javidi, "Image reconstruction from compressed encrypted digital hologram", *Opt. Eng.*, vol. 44, 2005.

[6] I. Yamaguchi , T. Zhang, "Phase-shifting digital holography," *Opt. Lett.*, vol. 22, pp. 610-612, 1998.

[7] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry", *Appl. Opt.*, vol. 39, pp.2313-2320, 2000.

[8] Thomas M. Kreis, Werner P. O. Juptner "Suppression of the dc term in digital holograph", *Opt. Eng.*, vol. 36, 1997.

[9] 이현진, 변현중, 길상근, "위상 천이 디지털 간섭계를 이용한 정보 암호화" COOC 2005.

[10] 변현중, 길상근, "2-step 위상천이 디지털간섭계를 이용한 이진 데이터 암호화 및 복호화", *한국광학회 2006년도 하계학술발표대회*, 2006.

[11] U. Schnars, W. Jueptner, "Digital Holography", Springer, Berlin, Germany, 2005.

[12] Joseph W. Goodman, "Introduction to Fourier Optics", *Roberts & Company Publishers*, Colorado, USA, 2005.

# Optical Encryption of Binary Information using 2-step Phase-shifting Digital Holography

Hyun Joong Byun, and Sang Keun Gil†

*Department of Electronics, the University of Suwon, Hwasung Gyonggi 445-743, Korea*

† *E-mail: skgil@suwon.ac.kr*

(Received September 1, 2006, Revised manuscript October 12, 2006)

We propose an optical encryption/decryption technique for a security system based on 2-step phase-shifting digital holography. Phase-shifting digital holography is used for recording phase and amplitude information on a CCD device. 2-step phase-shifting is implemented by moving the PZT mirror with phase step of 0 or $\pi/2$. The binary data and the key are expressed with random code and random phase patterns. The digital hologram is a Fourier transform hologram and is recorded on CCD with 256 gray level quantization. We remove the DC term of the digital hologram for data reconstruction, which is essential to reconstruct the original binary input data/image. The error evaluation for the decrypted binary data is analyzed. One of errors is a quantization error in detecting the hologram intensity on CCD, and the other is generated from decrypting the data with the incorrect key. The technique using 2-step phase-shifting holography is more efficient than a 4-step method because 2-step phase-shifting holography system uses less data than the 4-step method for data storage or transmission. The simulation shows that the proposed technique gives good results for the optical encryption of binary information.

OCIS code : 070.2580. 070.4560. 090.2880.