

# 위상천이 디지털 홀로그래피를 이용한 영상정보의 광암호화 기법

전석희\* · 길상근\*\*

## 1. 서 론

인간은 삶의 질을 향상시키기 위하여 다양한 지식을 만들고 매우 다양한 분야를 연구 발전시켜 왔으며, 이런 연구는 매우 많은 정보를 양산하였고 정보가 곧 자원이 되는 정보화 사회로 접어들게 되었다. 또한 컴퓨터와 통신기술은 정부기관, 전력시스템, 의료시스템, 은행, 군사시설 등 다양한 분야에서의 핵심 요소로 역할을 하고 있고, 세계 경제 기반은 한층 더 정보기술에 의존하고 있다. 또한 현대 정보화 사회에서는 활발한 정보교환이 신속히 이루어지고 다양한 형태의 서비스 환경이 창출되어 사회 전반에 걸쳐 빠르게 확산됨에 따라 정보를 보다 효율적으로 유통, 관리하고 이를 적극 활용하려는 노력이 가속화 되고 있다. 하지만 이러한 정보는 유출로 인한 막대한 피해를 주기도 하고 심지어는 범죄에도 이용되기도 한다. 이러한 정보의 해킹을 막기 위해 현재까지 많은 전문가들이 정보 보안 방법에 대해 연구 개발되어 왔으나 대부분 소프트웨어 기반의 디지털 암호화 알고리즘에 관한 것이다. 하지만 이러한 디지털

방식은 아직 보안성에 한계가 있고 많은 문제점을 내포하고 있다. 이러한 문제를 해결하기 위해 정보를 암호화하는 방법으로 광정보처리 기법을 활용한 광암호화 기술이 1990년대 초부터 암호화하고자 하는 정보를 디지털 처리가 아닌 아날로그 처리를 하는 광암호화 기법들이 연구되어 왔으며 이 중에서 디지털 홀로그래피(digital holography)를 응용한 연구가 주를 이루고 있다. 광을 이용한 광정보처리 시스템은 광의 고속성과 병렬성을 이용하여 실시간 처리가 가능하고 공간광변조기(SLM : Spatial Light Modulator), 광검출기(CCD : Charge Coupled Device)와 홀로그래피 기법을 이용하여 광학적 암호화 방법들이 많이 연구되고 있다. 정보 보안을 위하여 이용하는 홀로그래피 기법은 물체광(object beam)과 참조광(reference beam)을 간섭시켜 필름과 같은 매질에 정보를 기록하는 기법인데 이렇게 만들어진 홀로그램 데이터는 전체적으로 복소수이다. 이렇게 매질을 이용하여 암호화된 홀로그램을 만드는 것도 가능하지만 데이터를 통신망을 통하여 전송할 경우 양자화하여야 하기 때문에 실시간 처리가 불가능하다. 이러한 이유로 디지털 홀로그래피를 이용하게 되는데 이러한 디지털 홀로그래피의 특징은 필름과 같은 매질을 사용하는 것이 아니라 CCD와 같이 빛을 양자화 할 수 있는 장치를 이용하여 컴퓨터

※ 교신저자(Corresponding Author) : 길상근, 주소 : 경기도 화성시 봉담읍 와우안길 17, 전화: 031)220-2664, FAX: 031)220-2664, E-mail : skgil@suwon.ac.kr

\* 인천대학교 전자공학과

(E-mail : icujeon@incheon.ac.kr)

\*\* 수원대학교 전자공학과

를 통하여 실시간으로 정보를 처리하는 것이며, 단점으로는 디지털 홀로그램의 해상도가 저하된다는 단점이 있다. 현재까지 연구되어 오고 있는 광암호화 기법에는 XOR 연산을 이용한 방법[1], 이중 랜덤 위상 부호화를 이용한 방법[2], 결합변환상관기(JTC : Joint Transform Correlator)를 이용한 방법[3], phase-contrast를 이용한 방법[4], 위상 컴퓨터 형성 홀로그램을 이용한 방법[5], 반복 알고리즘을 이용한 방법[6], fractional Fourier 변환을 이용한 방법[7], Mach-Zehnder 간섭계를 이용한 방법[8], 위상천이 디지털 홀로그래피를 이용한 방법[9] 등이 있다. 본고에서는 최근 우리가 연구하여 왔던 위상천이 디지털 홀로그래피를 이용한 광암호화 기법[10-12]에 대하여 설명한다.

## 2. 위상천이 디지털 홀로그래피 기법을 이용한 광암호화

### 2.1 위상천이 디지털 홀로그래피 광암호화 장치

광암호화 시스템을 구현하기 위한 디지털 홀로그래피 기술을 응용하는데 있어서 좀 더 효율적인 방법은 위상천이 디지털 홀로그래피(phase-shifting digital holography)를 사용하여 복소수 정보를 기록하는 것이다. 이 위상 측정 기술은 빛의 크기와 위상을 재생하는데 홀로그램의 기법만이 아닌 전혀 새로운 기법으로 Skarman이 제안하였고, 비축 홀로그램을 디지털적으로 기록하는 기법보다 더 정확하다. 그는 초기의 위상을 계산하기 위해서 위상천이 알고리즘을 사용하였다. 후에 Yamaguchi는 위상천이 디지털 홀로그래피를 개선하였다. 본 논고에서는 256 gray-level로 표현되는 영상 정보를 QPSK(Quadrature Phase Shift Keying) 디지털 변조 방식과 위상천이 디지

털 홀로그래피를 이용하여 광학적 암호화 방법에 대해 기술한다. 우선 한 화소(pixel)당 gray-level 영상 정보는 ASCII 인코딩 방법에 의해 8-bits 이진 데이터로 양자화 되고, 해당 8-bits 이진 데이터 코드는 QPSK 변조 방식에 의하여 2x2 화소로 구성되는 블록 안에 네 쌍의 직교(quadrature) 위상 값으로 표현된다. 이렇게 변환된 QPSK 위상 값은 암호화 시키고자 하는 암호키와 더불어 SLM에 표시되는데, 암호화 하고자 하는 QPSK 이진 위상 값들은 물체광으로 암호키는 참조광으로 작용하여 CCD 상에서 간섭된 광세기 형태로 디지털 홀로그램으로 암호화 된다. 이때 얻어지는 암호화된 디지털 홀로그램은 256 gray-level로 양자화 되어 CCD에 기록된다. 이렇게 암호화된 디지털 홀로그램은 컴퓨터에 저장되고 디지털 네트워크 통신망을 통해 전송되어 지고, 전송되어진 디지털 홀로그램은 수신단에서 똑같은 암호키에 의하여 암호화되기 전의 QPSK 위상 값이 복원된다. 복원된 이러한 직교 위상 값들은 다시 QPSK 복조에 의해 8-bits 이진 데이터로 변환되며, 이진 데이터는 다시 ASCII 디코딩 방법에 의해 원래의 gray-level 값으로 복호화 된다. 그림 1은 정보의 암호화, 전송, 복호화를 수행하는 보안 시스템 블록도이다. 정보 데이터는 보안키(공동키 또는 개인키)에 의해 광학적으로 암호화되어 전송되어진 후 상대방에 의해서 같은 보안키에 의해 복호화된다. 암호화된 정보는 보안키를 이용한 광학적 복호화가 될 수도 있고, 컴퓨터를 이용한 복호화도 될 수가 있다. 한편 이진 데이터 정보로 변환된 물체광과 이진 데이터로 표현된 암호키의 참조광을 간섭시키기 위하여 Mach-Zehnder 간섭계 형태를 디지털 홀로그램을 얻기 위한 광학적 장치로 사용한다. 이때 암호화 방법으로써 위상천이 간섭기법을 이용하며, 사용된 위상천이 간섭기법은

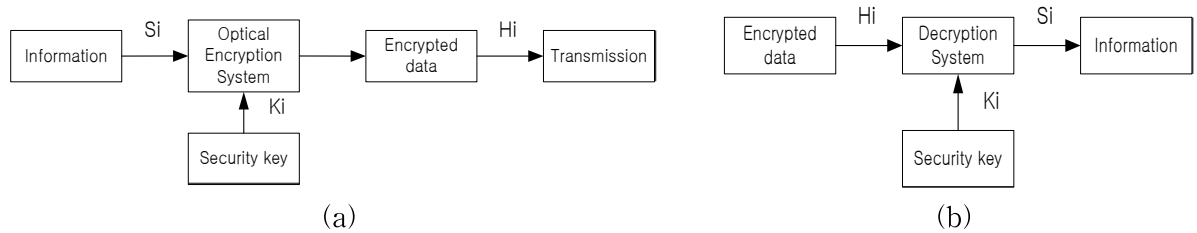


그림 1. 정보의 암호화, 전송, 복호화 과정: (a) 송신단-암호화, (b) 수신단-복호화

4-step 위상천이 간섭 또는 2-step 위상천이 간섭을 사용할 수 있으나 본고에서는 2-step 위상천이 디지털 홀로그래피 기법을 이용한 암호화 및 복호화 하는 방법에 대해서만 기술한다.

그림 2는 마흐-젠더 간섭계를 기반으로 제안한 위상천이 디지털 홀로그래피 광암호화 장치를 보여준다. 그림에서 공간필터(SF)와 시준렌즈(CL)는 레이저 빔을 평행광으로 확장시키고, 빔 분리기(beam splitter) BS1은 시준 광을 물체광과 참조광으로 나눈다. 셔터 S를 열면 물체광은 거울 M에서 반사되어 암호화시킬 QPSK 위상 이진 데이터가 표현될 SLM(spatial light modulator)과 랜덤 위상 마스크(random phase mask)로 조사된다. 이것은 위상형 SLM1과 랜덤 위상 마스크가 곁해진 형태로 푸리에 렌즈 L1을 거쳐 푸리에 변환되어 CCD 카메라에 기록된다. 여기서 랜덤 위

상 마스크는 공간주파수 영역에서의 푸리에 변환의 동적 영역을 확대시키는 역할을 한다. 한편 빔 분리기(BS1)로부터 나온 참조광은 PZT 거울에 반사되어 위상형 SLM2로 조사되고, 푸리에 렌즈 L2에 의해서 푸리에 변환되어 CCD 카메라에 기록된다. 여기서 암호키는 이진 위상으로 랜덤하게 발생시켰으며 이 암호화 코드는 SLM2에 표시된다. 본 연구에 사용된 랜덤 위상 마스크 개념은 Javidi 그룹에서 발표한 이중 랜덤 위상 인코딩 기법[2]과 유사하다. 하지만 제안한 본 광암호화 시스템은 위상 마스크를 공간주파수 영역에 위치시키지 않고 입력 공간 영역에 하나의 위상 마스크를 사용하기 때문에 이중 랜덤 위상 인코딩 기법보다 랜덤 위상 마스크의 개수가 적으며 훨씬 간단하고 광학소자들을 정밀하게 정렬하기 쉽다는 장점이 있다. 또한 물체광에 사용된 랜덤 위상

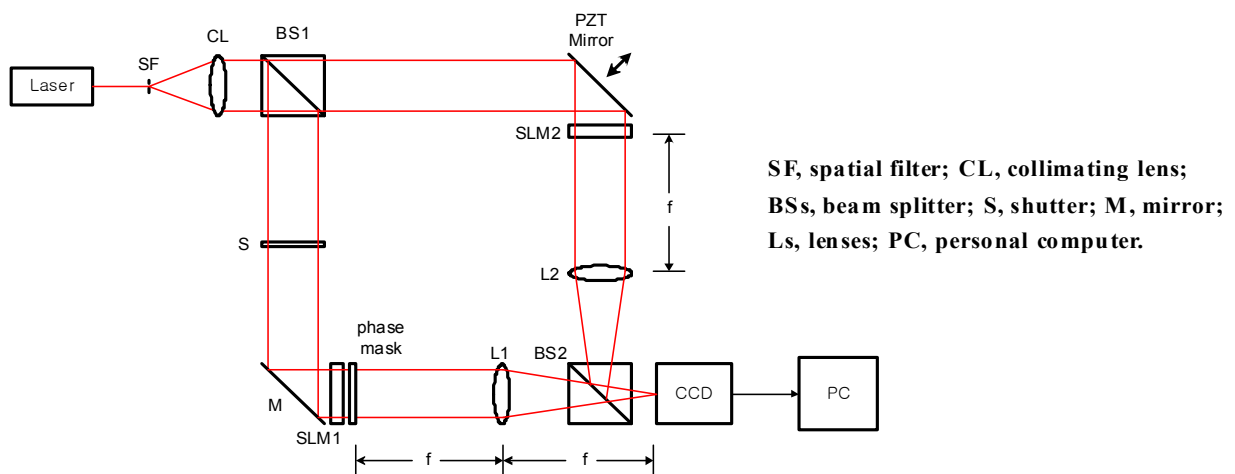


그림 2. PZT 거울을 이용한 위상천이 디지털 홀로그래피 광암호화 장치

마스크 패턴의 코드 정보는 디지털 간섭 홀로그램을 만들 때 참조광에서의 암호화 키 코드와 같은 랜덤 위상 패턴으로도 동시에 사용될 수도 있다. 이는 랜덤 위상 패턴의 사용을 간단히 하는 장점이 있지만 새로운 다른 랜덤 위상 패턴을 암호화 키로 사용하면 광암호화 시스템을 좀 더 복잡하고 높은 수준의 암호화 시스템으로 만들 수 있다.

보통 위상천이 간섭계에서 위상천이의 방법은 그림 2와 같이 거울에 PZT 소자를 붙여 가해진 전압에 비례하는 정확한 광경로 차이를 발생시켜 원하는 위상천이량을 얻는 것이다. 하지만 이 방법은 정확한 위상천이량을 얻기 위해서 PZT 소자의 수축, 팽창을 정확히 제어해야만 하고, 이러한 전기적, 기계적 동작으로 인한 위상천이 간섭계에서 정확한 위상천이량을 구현하기를 힘들게 하기 때문에 위상천이 오차를 발생시킨다. 이러한 단점을 극복하기 위해 우리는 위상지연 소자(phase retarder)와 직교 편광(orthogonal polarization)을 이용한 새로운 2-step 위상천이 디지털 홀로그래피를 구성하고 이를 광암호화 장치에 응용하였다. 그림 3은 제안한 직교 편광을 이용한 위상천이 디지털 홀로그래피 광암호화 장치를 보여준다. 여기서 위상지연 소자로는  $\lambda/4$ -wave plate를 사용

하였고 이를 통해 수직 편광방향으로 위상천이량이 없는 참조광과의 간섭과 수평 편광방향으로  $\pi/2$  위상천이량이 있는 참조광과의 간섭을 얻어 2-step 위상천이 푸리에 변환 디지털 홀로그래피를 구현하였다. 그림 3에서 공간필터(SF)와 시준렌즈(CL)를 통해 만들어진 평행광은 수평방향에 대해  $45^\circ$  기울어진 선형 편광기(P1)를 통과하고, 빔 분리기 BS1은 시준광을 물체광과 참조광으로 나눈다. 셔터 S1을 열면 물체광은 거울 M에서 반사되어 이진 데이터가 표현될 SLM1과 랜덤 위상 마스크로 조사된다. 이것은 푸리에 렌즈 L1을 거쳐 푸리에 변환되어 SLM1과 랜덤 위상 마스크가 컨볼루션 형태로 CCD 카메라에 기록된다. 한편 빔 분리기(BS1)로부터 나온 참조광은 거울에 반사되어 위상형 SLM2로 조사되고, 푸리에 렌즈 L2에 의해서 푸리에 변환되어 CCD 카메라에 기록된다. 여기서 수직방향을 따라 fast-axis가 정렬된  $\lambda/4$ -wave plate는 오직 수평방향으로만  $\pi/2$  위상천이량을 발생시킨다. 이때 물체광과 참조광의 수직성분끼리의 간섭 홀로그램 세기는 수직방향으로 정렬된 선형 편광기(P2)를 통과한 후 CCD에 기록된다. 한편 수평성분끼리의 간섭 홀로그램 세기는 수평방향으로 정렬된 선형 편광기(P2)를

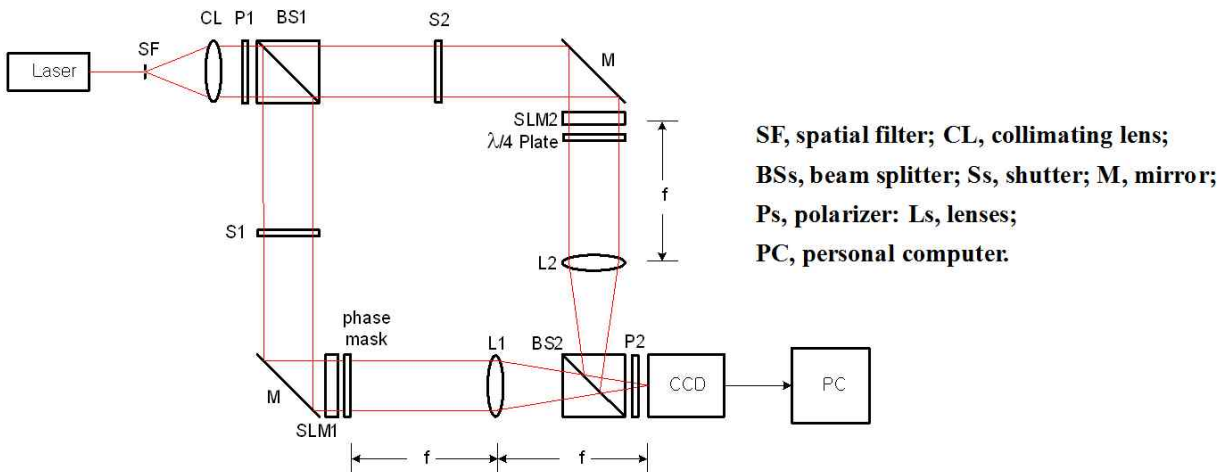


그림 3. 직교 편광을 이용한 위상천이 디지털 홀로그래피 광암호화 장치

통과한 후 CCD에 기록된다. 이들은 서로  $\pi/2$  위상천이를 가지는 두 개의 디지털 홀로그램이고 암호화된 데이터이다.

2.2 Two-step 위상천이 디지털 홀로그래피 광암호화 및 복호화

제안한 그림 2와 그림 3의 위상천이 디지털 홀로그래피를 이용한 gray-level 영상 정보의 광암호화 및 복호화 원리는 다음과 같다. 먼저 암호화할 256 gray-level의 영상 함수를  $f(x,y)$ 라 하고, 이 gray-level 영상 함수는 ASCII 인코딩 방법에 의해 8-bits 데이터로 이진화 된다. 여기서 하나의 gray-level 값을 가지는 한 화소에 해당하는 8-bits 이진 데이터 코드는 QPSK 변조 방법에 의해서  $2 \times 2$  화소로 구성되는 블록 안에 네 쌍의 직교 위상 값으로 변환된다. 이때 8-bits 이진 데이터의 MSB(most significant bit)으로부터 각각 두 비트씩 묶어서 QPSK 위상 값을 구한다. 그림 4는 이러한 변환 과정을 보여준다. 만약 gray-level 영상이  $128 \times 128$  화소수를 갖는 크기라면 QPSK 변조에 의해 변환된 이진 위상 데이터는 원 영상의 크기보다 2배 큰  $256 \times 256$  화소 수를

갖게 된다.

다음은 함수  $f(x,y)$ 가 ASCII 인코딩과 QPSK 변조과정을 통해 변환된 직교 위상 함수를  $s(x,y)$ 라 하자. 이러한 QPSK 위상 값은 위상형 SLM1에 표시되기 위해서 아래의 수식과 같이 표현된다. 여기서  $x$ 와  $y$ 는 공간 영역에서의 직교 좌표축이다.

$$a(x,y) = e^{js(x,y)} = e^{j0} \text{ or } e^{j\frac{\pi}{2}} \text{ or } e^{j\pi} \text{ or } e^{j\frac{3\pi}{2}} \quad (1)$$

그리고 공간주파수 영역에서 간섭의 영역을 넓히기 위해 랜덤 위상 마스크에 사용된 랜덤 위상 함수를 랜덤 발생기를 통해서 얻어진다고 하고, 이렇게 발생된 이진 코드를  $k(x,y)$ 라 한다.  $k(x,y)$ 가 1 또는 0의 이진 값이면 이진 위상 패턴  $\theta(x,y) = \pi \{1 - k(x,y)\}$  또는  $\theta(x,y) = \pi k(x,y)$ 로 표현할 수 있다. 따라서 랜덤 위상 마스크에 표현되는 위상 패턴 함수  $b(x,y)$ 는

$$b(x,y) = e^{j\theta(x,y)} = e^{j\pi} \text{ or } e^{j0} \quad (2)$$

이다. 만약 이진 코드  $k(x,y)$ 가 랜덤하면 위상 패턴 함수  $b(x,y)$ 도 랜덤한 성질을 갖는다. 이러한

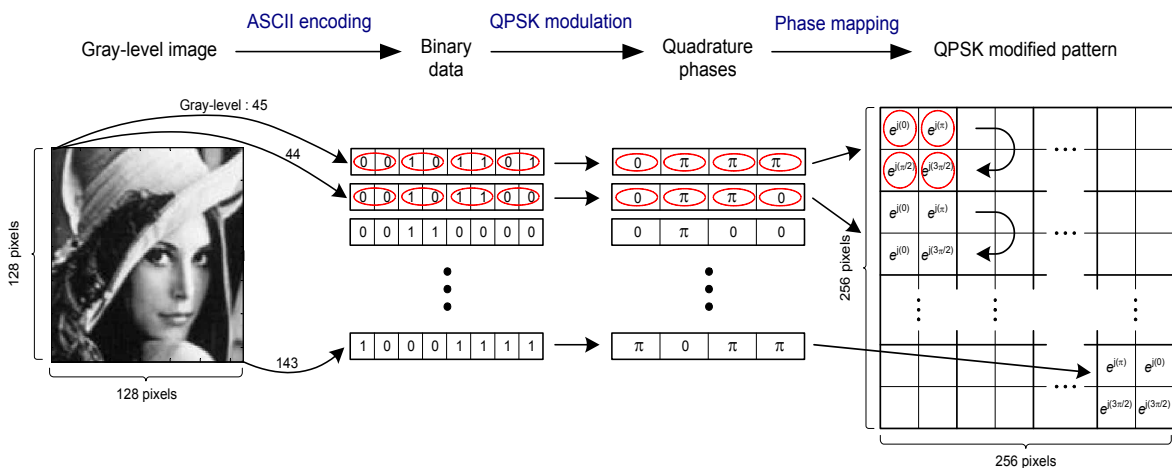


그림 4. 256 gray-level 영상을 이진 위상 값으로 변환시키기 위한 ASCII 인코딩과 QPSK 변조 과정

랜덤 위상 패턴 함수와 암호화를 위해 변환된 영상 정보의 QPSK 위상 함수의 곱은 다음과 같이 표현된다.

$$o(x, y) = a(x, y)b(x, y) = e^{js(x, y)}e^{j\theta(x, y)} = e^{j\{s(x, y)+\theta(x, y)\}} \quad (3)$$

식 (3)을 렌즈 L1을 거쳐 푸리에 변환하면

$$O(\alpha, \beta) = F\{o(x, y)\} = |O(\alpha, \beta)|e^{j\phi_o(\alpha, \beta)} \quad (4)$$

이 되고, 이는 마흐-젠더 간섭계를 이용하여 제안된 광암호화 장치에서 물체광의 역할을 한다. 여기서  $a$ 와  $\beta$ 는 공간주파수 영역에서의 좌표축이다.

한편 마찬가지로 랜덤 발생기를 통해 랜덤하게 발생시킨 이진 암호키 코드를  $c(x, y)$ 라 하고,  $c(x, y)$ 가 1 또는 0의 이진 값이면 암호키의 이진 위상 패턴  $\theta_c(x, y)$ 는 이진 키 부호에  $\pi$ 를 곱해서  $\theta_c(x, y) = \pi\{1 - c(x, y)\}$  또는  $\theta_c(x, y) = \pi c(x, y)$ 로 표현할 수 있다. 따라서 SLM2에 표현되는 함수  $r(x, y)$ 는

$$r(x, y) = 1 \cdot e^{j\theta_c(x, y)} \quad (5)$$

이다. 여기서 크기가 1로 표현된 것은 참조광에서 암호화 키가 표시된 SLM2에 입사되는 평면파를 의미한다. 식 (5)를 렌즈 L2를 거쳐  $r(x, y)$ 를 푸리에 변환하면 다음과 같다.

$$R(\alpha, \beta) = F\{r(x, y)\} = |R(\alpha, \beta)|e^{j\phi_R(\alpha, \beta)} \quad (6)$$

식 (4)와 식 (6)으로 표현되는 물체광  $O(\alpha, \beta)$ 와 참조광  $R(\alpha, \beta)$ 는 CCD상에서 다음과 같은 간섭무늬의 세기로 기록된다.

$$I(\alpha, \beta) = |O(\alpha, \beta) + R(\alpha, \beta)|^2$$

$$= |O(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2 + 2\sqrt{|O(\alpha, \beta)||R(\alpha, \beta)|} \cos \Delta\phi \quad (7)$$

여기서 물체광과 참조광 사이의 위상차는  $\Delta\phi = \phi_O - \phi_R$ 이다. 그러나 식 (7)로부터 얻은 정보를 가지고는 간섭 신호의 세기만 알 수 있고 위상 정보를 알 수 없기에 정확한 간섭 신호의 위상과 크기를 복원할 수 없다. 따라서 위상과 크기의 정보를 모두 구하기 위하여 위상천이 간섭계 기법을 사용한다. 위상 천이 간섭계에서 간섭무늬 광세기는

$$I_i(\alpha, \beta) = |O(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2 + 2\sqrt{|O(\alpha, \beta)||R(\alpha, \beta)|} \cos(\Delta\phi - \phi_i) \quad (8)$$

$i=2, 3, 4, \dots$ 로 표현되며, 4-step 위상천이 간섭계는  $i=4$ 인 경우이고, 2-step 위상천이 간섭계는  $i=2$ 인 경우이다. 위상천이는 그림 2와 같은 장치도에서는 PZT 거울을 제어하여 광 경로차를 발생 시킴으로써 구현하고, 그림 3과 같은 장치도에서는 위상지연 소자  $\lambda/4$ -wave plate와 편광기 (polarizer)를 사용하여 이를 통해 수직 편광방향과 수평 편광방향 사이의  $\pi/2$  위상천이량이 있는 간섭을 얻어 2-step 위상천이 디지털 홀로그래피를 구현한다. 보통 2-step 위상천이 간섭계가 multi-step 방법보다 디지털 홀로그램의 개수를 줄이는 장점을 가진다.

2-step 위상천이 간섭계의 위상천이 각을 각각  $0, \pi/2$ 라고 하면 식 (8)은 다음과 같이 표현된다.

$$I_1(\alpha, \beta) = |O(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2 + 2\sqrt{|O(\alpha, \beta)||R(\alpha, \beta)|} \cos \Delta\phi \quad (9)$$

$$I_2(\alpha, \beta) = |O(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2 + 2\sqrt{|O(\alpha, \beta)||R(\alpha, \beta)|} \cos(\Delta\phi - \pi/2)$$

식 (9)의 두 개의 디지털 홀로그램은 이진 데이

터 정보  $s(x,y)$ 가 암호화된 정보를 나타내며, 이들은 컴퓨터에 저장되어 디지털 통신망을 통하여 전송된다.

전송되어진 디지털 홀로그램 정보는 상대방에서 수신된 후에 암호할 때 사용한 똑같은 암호키에 의해 복호화 과정을 통해 원래의 영상 정보로 복원된다. 식 (9)에서 DC 성분을 나타내는  $|O(\alpha,\beta)|^2 + |R(\alpha,\beta)|^2$ 을  $A(\alpha,\beta)$ 로, AC 성분을 나타내는  $2\sqrt{|O(\alpha,\beta)||R(\alpha,\beta)|}$ 를  $B(\alpha,\beta)$ 라 놓으면 다음과 같이 다시 표현할 수 있다.

$$\begin{aligned} I_1(\alpha,\beta) &= A(\alpha,\beta) + B(\alpha,\beta)\cos\Delta\phi \\ I_2(\alpha,\beta) &= A(\alpha,\beta) + B(\alpha,\beta)\cos(\Delta\phi - \pi/2) \\ &= A(\alpha,\beta) + B(\alpha,\beta)\sin\Delta\phi \end{aligned} \quad (10)$$

식 (9)에서 DC 성분인  $A(\alpha,\beta)$ 를 제거하면 수정된 간섭무늬의 세기는 다음과 같다.

$$\begin{aligned} I_1'(\alpha,\beta) &= I_1(\alpha,\beta) - A(\alpha,\beta) = B(\alpha,\beta)\cos\Delta\phi \\ I_2'(\alpha,\beta) &= I_2(\alpha,\beta) - A(\alpha,\beta) = B(\alpha,\beta)\sin\Delta\phi \end{aligned} \quad (11)$$

따라서 식 (11)로부터 물체광과 참조광 사이의 위상차와 크기는 아래와 같이 구할 수 있다.

$$\Delta\phi = \Delta\phi_O - \Delta\phi_R = \tan^{-1}\left(\frac{I_1'}{I_2'}\right) \quad (12)$$

$$A_{OR} = |O(\alpha,\beta)||R(\alpha,\beta)| = \frac{1}{4}\{(I_1')^2 + (I_2')^2\} \quad (13)$$

위 식으로부터 간섭무늬의 위상 정보를 알기 위해서는 DC 성분을 꼭 제거해야만 한다는 것을 알 수 있다. 지금까지 2-step 위상천이 디지털 홀로그래피 방법으로 구한 위상과 크기로부터 암호화된 복소 홀로그램은 다음과 같이

$$H(\alpha,\beta) = A_{OR} e^{j\Delta\phi} \quad (14)$$

로 나타낼 수 있으며, 이 복소 홀로그램과 우리가 알고 있는 암호키 정보를 이용하면 원 정보를 재생할 수 있다.

이제 식 (14)로부터 복소 분포 함수  $O(\alpha,\beta)$ 를 구하고 원래의 256 gray-level 영상을 복호화하기 위해서 암호키 코드 위상 패턴의 복소 함수  $R(\alpha,\beta)$ 이 필요하다. 하지만 이 복소 함수  $R(\alpha,\beta)$ 은 암호키 이진 코드로부터 만들어졌기 때문에 암호키로부터 구할 수가 있다. 또한 원 정보의 복원을 위해선 암호키 코드의 위상 패턴의 세기 분포 함수  $|R(\alpha,\beta)|^2$ 가 필요하다. 이 세기 패턴은 마흐-젠더 광암호화 장치에서 참조광을 차단함으로써 물체광만 CCD에 기록된 광세기 분포와 같다. 이것은 그림 2에서 셔터 S와 그림 3에서 셔터 S1을 닫음으로써 광학적으로 얻어진다. 이러한 복소 홀로그램과 암호키 정보를 이용하여 복원시킨 복소 분포 함수는 다음과 같이 구해진다.

$$\begin{aligned} G(\alpha,\beta) &= \frac{H(\alpha,\beta)R(\alpha,\beta)}{|R(\alpha,\beta)|^2} \\ &= \frac{|O(\alpha,\beta)||R(\alpha,\beta)|e^{j(\phi_O - \phi_R)}|R(\alpha,\beta)|e^{j\phi_R}}{|R(\alpha,\beta)|^2} \\ &= O(\alpha,\beta)e^{j\phi_O} \end{aligned} \quad (15)$$

식 (15)를 역 푸리에 변환하면 물체광의 정보 데이터가 재생되고 이 재생된 데이터는 QPSK 위상 함수와 랜덤 위상 패턴 함수의 곱  $o(x,y)$ 을 나타낸다.

$$\begin{aligned} g(x,y) &= F^{-1}\{G(\alpha,\beta)\} = F^{-1}\{O(\alpha,\beta)\} \\ &= o(x,y) = a(x,y)b(x,y) \end{aligned} \quad (16)$$

식 (16)으로부터 다시 원래의 QPSK 변조된 위상 함수를 구하기 위해 암호화할 때와 같은 랜덤 위상 패턴 함수의 공액 함수를 이용한다.

$$p(x,y) = g(x,y)b^*(x,y) = a(x,y) \quad (17)$$

따라서 식 (17)로부터 ASCII 디코딩함으로써 원래의 256 gray-level의 영상 함수  $f(x,y)$ 를 구할 수 있다.

### 3. 컴퓨터 시뮬레이션

제안한 광암호화 시스템은 컴퓨터 시뮬레이션을 이용하여 그 성능을 보여준다. 그림 5-(a)는 제안한 광암호화 시스템에서 암호화 하고자 하는 128×128 크기의 화소 수를 갖는 gray-level의 Lena 영상을 보여주고, 그림 5-(b)는 256 gray-level의 Lena 영상이 ASCII 인코딩 기법에 의해 이진 데이터로 바뀐 다음 QPSK 변조를 통해 변환된 위상 값들을 나타낸다. 여기서 하나의 gray-level 값을 가지는 한 화소는 8-bits 이진 데이터로 인코딩되고 다시 네 쌍의 직교 위상 값으로 대응되어 2×2 화소로 구성된 블록에 시계 방향으로 배열되어 위치한다. 결국 SLM1에 표시될 입력 이진 데이터는 256×256 크기를 갖게 된다. 그림 5-(c)는 암호화와 복호화에 사용될 1과 0의 조합으로 구성되고 랜덤하게 발생된 암호키 코드

를 나타내는데 256×256 크기를 갖는다. 여기서 흰색 화소는 1 값을 검은색 화소는 0 값을 나타내고, 암호키 코드 패턴은 MATLAB 프로그램의 랜덤 발생기를 통해 생성하였다.

그림 6은 위상천이 디지털 홀로그래피 기법을 통해 만들어진 두 개의 암호화된 디지털 홀로그램을 보여준다. 여기서 각 홀로그램은 256 gray-level로 양자화 된다. 이렇게 QPSK 이진 위상 패턴이 암호화되어 만들어진 디지털 홀로그램에 의해 구해진 복소 홀로그램으로부터 같은 암호키를 사용하여 암호화된 위상 정보는 성공적으로 복호화 된다.

그림 7은 QPSK 디지털 변조에 의해 gray-level 영상으로부터 만들어진 암호화된 위상과 제안된 광암호화 시스템에서 복원된 위상 사이의 위상 오차를 보여준다. 그림 7-(a)는 올바른 암호키가 사용됐을 때 복원된 위상을 보여주며, 정확한 원래의 직교 위상 값은 적절한 estimation과 decision 기법에 의해 복원된 위상으로부터 구할 수 있다. 그림 7-(b)는 틀린 암호키가 사용됐을 때 복원된 위상을 보여주며, 몇몇 복원된 위상은 원래의 직교 위상 값과 상당히 틀린 위상 값을 나타

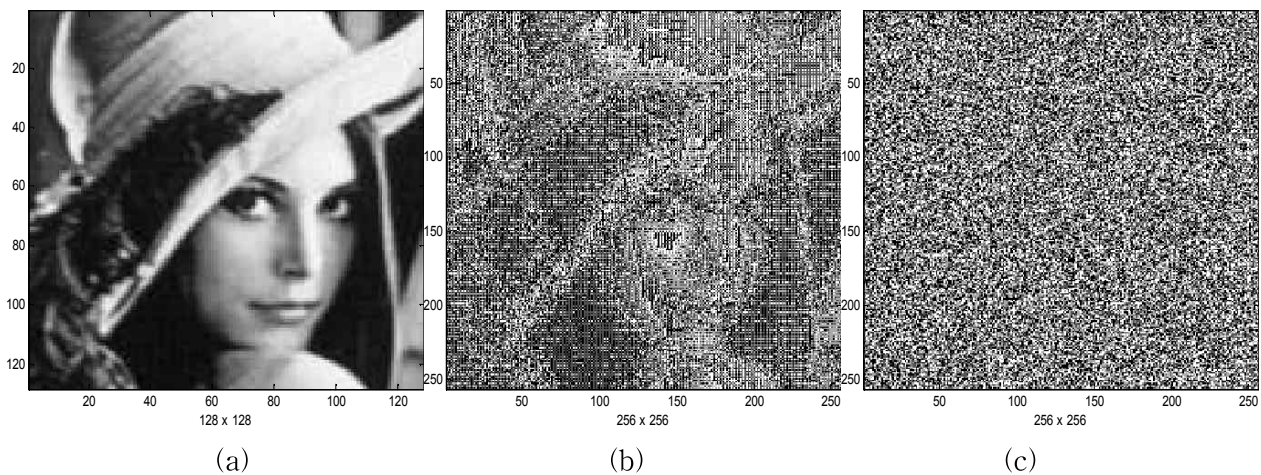


그림 5. 컴퓨터 시뮬레이션을 위한 입력 데이터: (a) 암호화할 256 gray-level 영상, (b) ASCII 인코딩과 QPSK 변조를 통해 변환된 이진 위상 데이터, (c) 랜덤 발생된 암호키 이진 코드 패턴



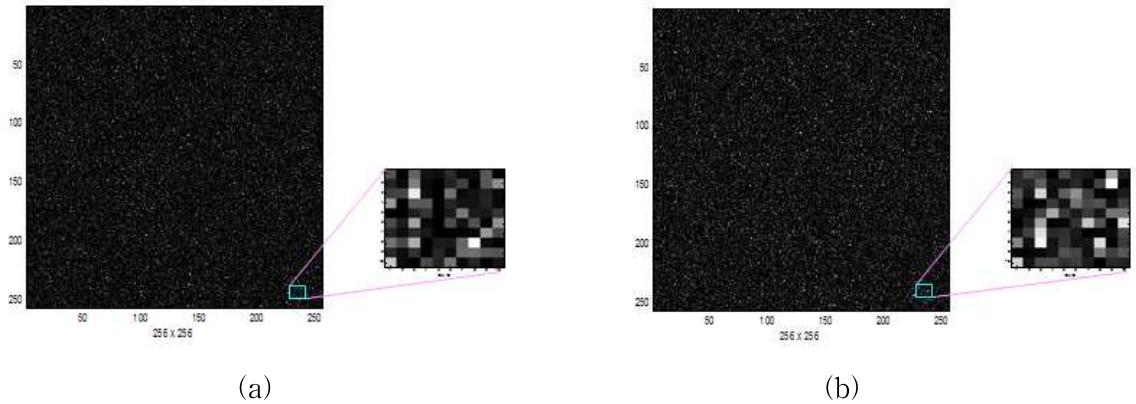


그림 6. 2-step 위상천이 디지털 홀로그래피로부터 얻어진 암호화된 디지털 홀로그램: (a) 위상천이  $\phi=0$ 일 때 광세기 패턴, (b) 위상천이  $\phi=\pi/2$ 일 때 광세기 패턴

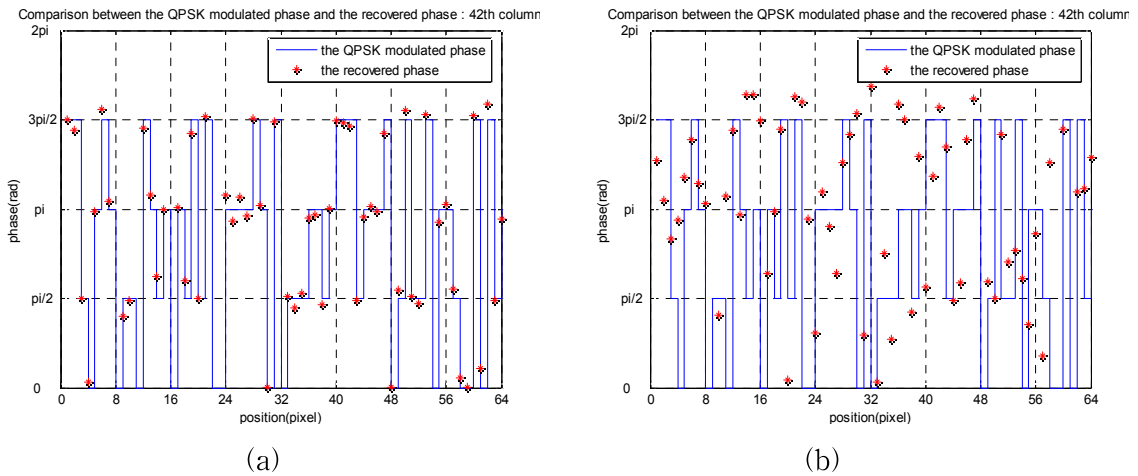


그림 7. QPSK 변조 위상과 제안한 광암호화 시스템으로 복원된 위상의 비교: (a) 올바른 암호키로 복원하였을 때, (b) 틀린 암호키로 복원하였을 때

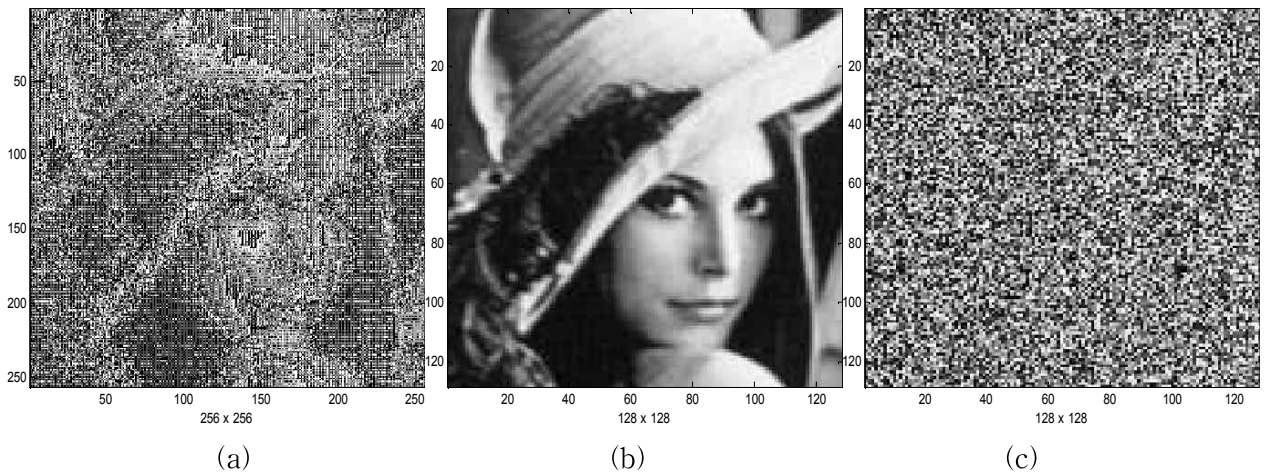


그림 8. 복호화 결과: (a) 올바른 암호키가 사용됐을 때 복원된 위상 패턴, (b) QPSK 복조와 ASCII 디코딩에 의해 복호화된 256 gray-level 영상, (c) 틀린 암호키로 복호화 하였을 때 복원된 영상

내고 있다.

그림 8은 제안한 광암호화 시스템을 이용하여 복원된 이진 위상 데이터와 복호화된 영상에 대한 결과를 보여준다. 그림 8-(a)는 올바른 암호키가 사용됐을 때 복원된 위상 패턴이며, 그림 8-(b)는 복조된 QPSK 위상으로부터 ASCII 디코딩을 통해 복호화된 256 gray-level 영상이다. 한편 암호화 키와 다른 틀린 암호키로 복호화 하였을 때 복원된 영상은 그림 8-(c)와 같이 원래의 Lena 영상이 복원되지 않음을 보여준다.

#### 4. 결 론

정보화 사회에서 정보 보호 및 보안은 매우 중요한 사항이다. 최근 보다 확고한 정보 보안을 유지하기 위해 광정보처리 기술을 이용한 광암호화 기법에 대한 연구가 활발히 이루어지고 있다. 광암호화 시스템은 디지털 방식에 비해 정보 보안성이 우수하며 대용량의 정보를 고속으로 암호화할 수 있을 뿐만 아니라 암호화된 정보가 백색 잡음과 같은 아날로그 신호 형태로 해킹에도 매우 강한 장점이 있다. 최근에는 SLM과 CCD 등 디지털 소자의 발전과 더불어 광과 디지털이 하이브리드 시스템으로 결합된 디지털 홀로그래피를 이용한 광암호화 기법이 차세대 광보안 시스템의 구현 기술로 유용하게 대두되고 있다.

본 논문은 ASCII 인코딩 기법 및 QPSK 디지털 변조 기법과 2-step 위상천이 디지털 홀로그래피를 이용하여 새로운 광암호화 시스템을 제안하였다. 제안된 시스템의 위상천이를 얻는 방법은 PZT로 동작되는 거울을 사용하는 방법과 편광기와 위상지연 소자  $\lambda/4$ -wave plate를 사용한 방법에 대해 기술하였다. 또한 본 논문에서 제시하고 있는 시스템은 디지털 통신망에서 영상 정

보의 매우 높은 수준의 암호화 및 복호화에 응용될 수 있으며 인증 및 보안 시스템에도 응용이 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," *Opt. Eng.*, Vol. 38, No. 1, pp. 47~54, 1999.
- [2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, Vol. 20, pp. 767-769, 1995.
- [3] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Opt. Eng.*, Vol. 39, No. 8, pp. 2031~2035, 2000.
- [4] L. G. Neto, "Implementation of image encryption using the phase-contrast technique," *Proceedings of SPIE*, Vol. 3386, pp. 284~290, 1998.
- [5] P. Stepien, R. Gajda, and T. Szoplik, "Distributed kinoforms in optical security applications," *Opt. Eng.*, Vol. 35, No. 9, pp. 2453~2458, 1996.
- [6] T. Sasaki, H. Togo, J. Tnida, and Y. Ichioka, "Stream cipher based on pseudorandom number generation with optical transformation," *Applied Optics*, Vol. 39, No. 14, pp. 2340~2346, 2000.
- [7] G. Unnikrishnan, K. Singh, "Double random fractional Fourier-domain encoding for optical security", *Opt. Eng.* Vol. 39, pp. 2853~2859, 2000.
- [8] J. Y. Kim, S. J. Park, C. S. Kim, J. K. Bae, and S. J. Kim, "Optical image encryption using interferometry-based phase masks," *Electron. Lett.*, Vol. 36, No. 10, pp. 874~875, 2000.
- [9] I. Yamaguchi and T. Zhang, "Phase-shifting

digital holography," *Opt. Lett.*, Vol. 22, pp. 610-612, 1998.

[10] S. K. Gil, S. H. Jeon, N. Kim and J. R. Jeong, "Successive encryption and transmission with phase-shifting digital holography", *Proceedings of SPIE*, Vol. 6136, 2006.

[11] S. H. Jeon, Y. G. Hwang, and S. K. Gil, "Optical encryption of gray-level image using on-axis and 2-f digital holography with two-step phase-shifting method", *Opt. Rev.* Vol. 15, pp. 181~186, 2008.

[12] S. K. Gil and S. H. Jeon, "QPSK modulation based optical image cryptosystem using phase-shifting digital holography", *J. Opt. Soc. Korea*, Vol. 14, No. 2, pp. 97-103, 2010.

[13] B. Javidi and J. L. Honor, "Optical pattern recognition for validation and security varification," *Opt. Eng.*, Vol. 33, pp. 1752-1756, 1994.



전 석 희

- 1977년~1981년 연세대학교 전자공학과 학사
- 1981년~1983년 연세대학교 전자공학과 석사
- 1983년~1990년 연세대학교 전자공학과 박사
- 1991년~현재 인천대학교 전자공학과 교수
- 2001년~2002 UC Santa Barbara 방문교수
- 2012년~현재 인천대학교 공학교육혁신센터 센터장
- 관심분야 : 광정보처리, 광암호화, 홀로그래피 응용



길 상 근

- 1980년~1984년 연세대학교 전자공학과 학사
- 1984년~1986년 연세대학교 전자공학과 석사
- 1987년~1992년 연세대학교 전자공학과 박사
- 1993년~1998년 고등기술연구원 책임연구원
- 1998년~현재 수원대학교 전자공학과 교수
- 관심분야 : 광정보처리, 광암호화, 광센서, 광계측