工學碩士 學位論文

생체정보와 위상 랩핑 방법을 이용한 암호화 및 복호화 시스템

Encryption and decryption system using bio-information and phase wrapping method

指導敎授 徐 東 煥

*2007*年 *2*月

韓國海洋大學校 大學院

電氣電子工學科

林 咏 進

本 論文을 林咏進의 工學碩士 學位論文으로 認准함

委員長 : 工學博士　　全 泰 寅 ㊞

委　員 : 工學博士　　張 樂 元 ㊞

委　員 : 工學博士　　徐 東 煥 ㊞

*2006*年　*12*月

韓 國 海 洋 大 學 校　大 學 院

電氣電子工學科

林　　咏　　進

목 차

그림 목차

<그림목차>

Encryption and decryption system using bio-information and phase wrapping method

by Young-Jin, Lim

Department of Electrical & Electronics Engineering
The Graduate School of Korea Maritime University
Busan, Republic of Korea

Abstract

In this paper, we propose an improved image encryption and fault-tolerance decryption method using bio-information and phase wrapping method in the frequency domain. An encrypted image in the encryption process is denoted the product of a phase-encoded arbitrary image and a random phase image. The encrypted image is zero-padded and Fourier transformed. Its real-valued data and bio-information image are phase-encoded. Both encrypted key and decrypting key are made of proposed phase wrapping method. The decryption is simply performed based on 2-f setup with spatial filter by Fourier transform for multiplication phase-encoded fingerprint image and the keys. The proposed method using arbitrary image, which does not contain any

information from the original image, prevents the possibility of counterfeiting from unauthorized people and also can be used as a current spatial light modulator technology by phase encoding of the real-valued data. Computer simulations show the validity of the encryption scheme and the robustness to noise of the encrypted key or the decryption key in the proposed technique.

제 *1* 장 서 론

정보화 사회에서는 정보산업의 기술발전과 인터넷의 발전으로 여권, 신용카드, 현금카드 등과 같은 개인의 신원을 인증할 수 있는 신분증의 사용이 늘어나고 있다. 그러나 프린터, 스캐너 및 복사기 등의 컴퓨터 관련 장비들과 소프트웨어 기술의 발달로 화폐뿐만 아니라 여러 이미지 패턴들의 복제가 쉽게 이루어지고 있다. 따라서 어떠한 경우에도 개인 정보보호 뿐만 아니라 위조나 복제를 근본적으로 차단할 수 있는 새로운 접근 방법에 관한 연구 개발이 절실히 요구되고 있다.[1-3] 최근에는 기존의 광세기 검출기(CCD 카메라, 복사기, 스캐너 등)로는 볼 수도 복제할 수도 없는 복소함수 형태의 랜덤 위상 패턴을 사용하는 새로운 광학적 정보보호 기술이 연구되고 있다. 광을 이용한 영상신호는 세기정보나 위상(phase)정보를 광학적인 매질 또는 공간광변조기(spatial light modulator)에 기록이 가능하다는 특성에 기인하며 광전자 소자들을 이용하여 실 시간적인 구현이 가능하고 랜덤 위상 암호 키를 사용함으로써 정보를 위조하거나 해독하지 못하도록 함으로써 우리의 생활을 심각하게 위협하는 개인정보보호의 문제를 해결할 수 있는 접근방법으로 제시되고 있다.

또한, 정보보호 수준의 향상을 위하여 생체의 일부 고유한 특징으로부터 개인을 식별하고 인증하는 생체측정학 (Biometrics)과 관련된 연구가 최근에 활발하게 진행되고 있다. 생체측정학에 이용되는 생체정보들은 지문, 음성, 서명, 망막, 얼굴, 유전자 등이 있다. 생체정보 중에서 지문은 개인의 감정, 질병, 노화, 등에 따라 잘 변하지 않으며, 또한 위조, 변조, 분실 등의 위험성이 적어서 식별과 인증이 필요한 분야에서 폭넓게 이용되고 있다. 더욱더 최근에 관련 산업 기술의 발달로 인하여 널리 활용되고 있다.

광 암호화 시스템은 주로 4-f 광 상관기(correlator)[4-7]나 간섭계구조[8]를 이용하여 원 영상을 재생하고, 진위 여부는 주로 암호화에 사용된 무작

위 위상 마스크에 의해서 판정하게 된다. 4-f 광 상관기를 이용한 이중 무작위 위상 부호화 방법(double random phase encoding)은 입력 평면과 푸리에 평면에 두개의 랜덤 위상 마스크를 두어 영상을 암호화하고, 랜덤 위상의 복소 공액 값을 가진 마스크를 푸리에 평면에 놓아 동일한 시스템을 이용하여 원 영상을 복원하게 된다. 이중 무작위 위상 부호화 방법(double random phase encoding)은 광축 정렬의 어려움과 정확한 복소 공액 값을 가지는 위상 카드제작의 어려움이 있으며, 정밀한 실험구성을 필요로 하며 외부 교란에 많은 영향을 받는다는 단점이 있다. 결합 변환 상관기(joint transform correlator, JTC)[9-11]는 광축 정렬이 필요 없고 외부교란에도 거의 영향을 받지 않는 장점이 있다. 그러나 결합 변환 상관기는 구조적인 특성 때문에 출력 평면에 자기상관 성분이 큰 세기로 나타나므로, 광 상관 시스템이나 광 보안 시스템에 이용하기에 어려움을 준다. 또한 앞서 제안한 방법에서 암호화된 영상이 여러 형태의 외부 영향에 얼마나 강한 방법인가를 확인하였다.[12-14]

세기정보 암호화 수준을 향상시키기 위하여 입력평면에 위상정보를 가지는 원 영상을 이용하여 암호화하는 방법[15-19]이 제안 되었으며 이는 위상정보를 암호화한 후 일반화된 위상세기 방법(generalized phase-contrast technique)을 이용하여 간단히 원 영상을 복원할 수 있는 방법으로 제안하였다. 이 방법의 단점은 광학적 시스템에서 암호화키의 블로킹 등 외부 영향에 민감하여 원 영상을 재생할 수 없고 복호화 과정에서 정확한 광축 정렬의 어려움을 가진다. 또한 앞서 제안된 방법들의 가장 큰 단점은 암호화키와 복호화키가 동일하므로 만약 허가되지 않은 사용자가 암호화된 영상을 푸리에 변환이나 위상 측정 방법 등으로 분석하여 암호화키를 파악함으로써 복원 영상을 예측할 수 있는 문제점이 있다. 이 문제점을 해결하기 위해 반복적인 알고리즘을 이용하여 임의의 세기 영상을 이용한 방법[20]이 제안되었으나 이 또한 광축 정렬의 어려움을 가지고 원 영상을 재생하기

위한 시간소모가 많은 단점이 있다.

본 논문에서는 생체정보와 위상 랩핑 방법을 이용하여 보다 향상된 수준의 광 암호화 방법을 제안하였다. 위상 변조된 생체정보를 이용하여 암호키의 분실 혹은 고의적인 양도에 의한 부정사용을 방지 할 수 있고 영상정보의 진위 여부를 개인의 인증을 통해서 가려낼 수 있다. 또한 위상 랩핑 방법을 이용하여 암호화 및 복호화에 사용될 위상 변조된 영상들을 각각 비선형적인 조합으로 표현한 후 이를 주파수 영역에서 암호화키와 복호화키를 실수 값으로 표현하여 위상 부호화하여 암호화 수준을 향상시키고 실질적인 광학적인 구현을 가능하게 하고 공간 필터를 2-f 광 상관기를 이용하여 원 영상을 복원하는 방법을 제안하였다.

제안한 암호화 영상은 원 영상이 아닌 위상 변조된 임의의 영상과 무작위 위상 영상을 곱하여 위상 랩핑과 제로 패딩(zero-padding)하여 푸리에 변환한 후 이 변환된 영상의 실수 값과 생체정보인 지문영상을 위상 부호화하여 만든다. 따라서 허가받지 않은 사용자가 위상 측정 방법 등을 통하여 암호화된 영상의 위상 값을 추출하더라도 복호화키의 정보 없이는 원 영상의 정보를 확인할 수 없게 됨으로써 높은 정보 보호가 가능하고 실수 값을 위상 부호화함으로써 현재에 사용되는 공간광변조기로 표현이 가능하다. 복호화 과정은 암호화된 영상과 위상 랩핑 방법에 의해 만들어진 푸리에 복호화키를 곱하여 푸리에 역 변환하여 출력평면에 공간필터를 두어서 원 영상을 복원함으로써 외란과 충격의 문제점과 4-f 시스템의 광축 정렬 문제를 해결할 수 있으며 픽셀 대 픽셀 대응을 용이하게 하여 복원영상의 해상도를 향상시키고자 제안하였다. 제안한 암호화 방법을 컴퓨터 모의실험을 수행하여 잡음이나 암호화된 영상의 블로킹에 강한 특성이 있음을 확인하였다.

제 2 장 결합 변환 상관기와 이중 랜덤 위상 암호화

2.1 전통적인 결합 변환 상관기

결합 변환 상관기(joint transform correlator, JTC)[21]는 입력영상과 기준영상을 JTC의 결합 입력 평면에 동시에 두기 때문에 광축 정렬 문제를 해결할 수 있는 광 상관 시스템이다. 전통적인 JTC의 시스템은 그림 1과 같다. 그림 1에서 공간광변조기(spatial light modulator; SLM)는 입력 영상들이 올라가는 결합 입력 평면을, 렌즈 L은 푸리에 변환렌즈를, P는 출력평면을 나타내며, f는 렌즈의 초점거리이다. 그림 1에서 $r(x,y)$는 중심이 $(-x_0,0)$에 배치되는 기준영상이고 $h(x,y)$는 중심이 $(x_0,0)$에 배치되는 입력영상이다. 따라서 결합 입력 평면은

$$e(x,y)=h(x-x_0,y)+r(x+x_0,y), \tag{1}$$

로 주어지며, 결합 입력 평면은 렌즈 L에 의해서 푸리에 변환 되는데 이는

$$E(u,v)=H(u,v)\exp(-j2\pi x_0 u)+R(u,v)\exp(j2\pi x_0 u), \tag{2}$$

와 같이 표현되고, 출력평면 P에 놓인 세기 검출기(intensity detector)에 나타나는 출력 단위 광세기 함수 JPS는

$$|E(u,v)|^2 = |H(u,v)|^2 + |R(u,v)|^2 \quad (3)$$
$$+ H(u,v)R^*(u,v)\exp(-j4\pi x_0 u)$$
$$+ H^*(u,v)R(u,v)\exp(j4\pi x_0 u),$$

와 같이 표현된다. 식 (2)와 (3)에서 나타나는 위상 성분은 입력 영상과 기준 영상의 원래 중심이 결합 입력 평면에서는 $\pm x_0$만큼 이동하기 때문에 발생한다. CCD로 검출된 광세기 함수는 컴퓨터를 통하여 다시 SLM에 올려지게 되고, L에 의해서 푸리에 역 변환된다. 이때 출력 평면에서의 광분포 함수는

$$g(x,y) = h \star h + r \star r \quad (4)$$
$$+ h \star r^* \delta(x+2x_0, y) + r \star h^* \delta(x-2x_0, y),$$

와 같다. 여기서 ★는 상관자(correlation operator)를, *는 상승자(convolution operator)를 뜻한다. 식 (3)에서 상관은 세기 검출기 특성에 의해서 발생하게 되고 식 (4)의 앞의 두 항은 각각의 입력영상의 자기상관(autocorrelation) 성분이며, 뒤의 두 항은 각 입력영상간의 상호상관(crosscorrelation) 성분이다. 자기상관의 세기는 상호상관의 세기에 비해 아주 크므로 광 상관 시스템에서는 오인식을 유발시키며, 광 암호화 시스템에서는 영상의 복원을 어렵게 만든다.

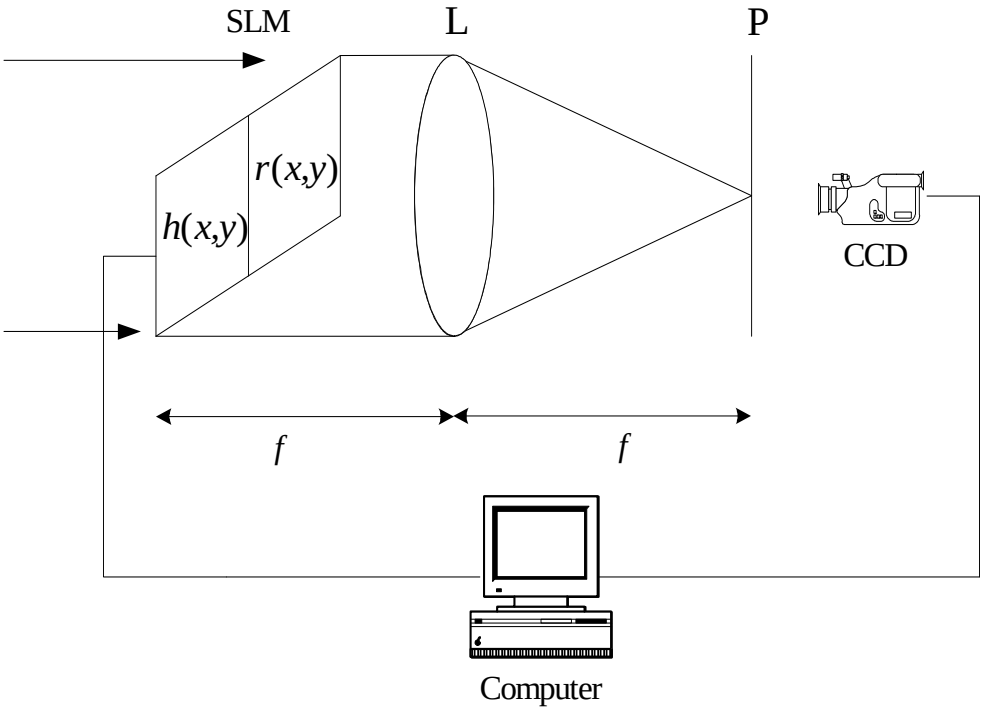


그림 1. 전통적인 결합 변환 상관기

Fig. 1. The Conventional joint transform correlator.

2.2 결합 변환 상관기를 이용한 암호화 시스템

Park 등은 결합 변환 상관기의 자기상관 성분을 이용하여 원 영상을 재생할 수 있는 주파수 영역에서의 암호화 시스템을 제안하였다.[22] 암호화 시스템은 이진영상을 위상 변조하고, 무작위 이진패턴을 컴퓨터로 발생시켜 위상 변조한다. 두 위상 변조된 영상을 공간영역에서 곱해서 순수한 위상 값만 가지는 무작위 패턴으로 만든 후 이를 푸리에 변환한다. 복호화 방법은 암호화된 영상을 JTC의 자기상관 연산 과정으로 원 영상을 복원한다.

암호화 할 이진 영상 $f(x,y)$와 컴퓨터로 만든 이진 무작위 영상$r(x,y)$을 위상 변조하면, 위상 변조된 각각의 영상 $f_p(x,y)$, $r_p(x,y)$는

$$f_p(x,y) = \exp[j\pi f(x,y)] \tag{5}$$
$$r_p(x,y) = \exp[j\pi r(x,y)],$$

와 같이 표현된다. 두 위상 변조된 영상을 곱한 암호화 영상 $h(x,y)$는

$$h(x,y) = f_p(x,y) r_p(x,y) \tag{6}$$
$$= \exp\{j\pi[f(x,y)+r(x,y)]\},$$

와 같다. 식 (6)의 $h(x,y)$를 푸리에 변환하면 암호영상 $H(u,v)$, $r_p(x,y)$를 푸리에 변환하면 진위를 판별하는 키 영상 $R_p(u,v)$을 얻는다.

암호화된 영상 $H(u,v)$는 그림 1의 결합 입력 평면의 우반 평면에, 진위

를 판별하는 키 영상 $R_p(u,v)$는 좌반 평면에 각각 놓여진다. 암호화된 영상은 주파수 영역이고 각각의 입력 영상들이 JTC의 결합 입력 평면에 나란히 놓여 지므로 원래의 중심에 대해서 $(\pm u_0,0)$만큼 이동하게 된다. 따라서 결합 입력 평면 $O(u,v)$는

$$O(u,v)=H(u-u_0,v)+R_p(u+u_0,v), \tag{7}$$

과 같다. 결합 입력 평면은 렌즈 L에 의해서 푸리에 역 변환되며 이는

$$o(x,y)=h(x,y)\exp(-j2\pi u_0 x)+r_p(x,y)\exp(j2\pi u_0 x), \tag{8}$$

로 주어진다. 여기서 $\exp(\pm j2\pi u_0 x)$는 주파수 영역에서 중심의 이동에 의해 생기는 출력 평면에서의 위상 성분이다. 출력 평면에 놓인 CCD 카메라에 의해 검출되는 복원 영상은

$$\begin{aligned}|o(x,y)|^2 &= |h(x,y)|^2+|r_p(x,y)|^2 \\ &\quad +h(x,y)r_p^*(x,y)\exp(-j4\pi u_0 x) \\ &\quad +h^*(x,y)r_p(x,y)\exp(j4\pi u_0 x),\end{aligned} \tag{9}$$

와 같고 식 (6)에 의해,

$$
\begin{aligned}
|o(x,y)|^2 &= 1+1 \\
&\quad +\exp[j\pi f(x,y)]\exp(-j4\pi u_0 x) \\
&\quad +\exp[-j\pi f(x,y)]\exp(j4\pi u_0 x) \\
&= 2+2\cos\left[\pi f(x,y)-4\pi u_0 x\right],
\end{aligned} \tag{10}
$$

으로 되며, 이는 이진 값으로 구성되는 원 영상의 각 화소 값에 따라

$$
o(x,y)=\begin{cases} 2+2\cos(4\pi u_0 x), \text{ if } f(x,y)=0 \\ 2-2\cos(4\pi u_0 x), \text{ if } f(x,y)=1, \end{cases} \tag{11}
$$

과 같이 정리된다. 식 (11)에서 재생된 영상의 세기에 미치는 u_0는 입력 영상과 기준 영상의 각각의 중심 위치이며, 영향이 없는, 즉 $\cos(4\pi u_0 x)=1$인 경우이면,

$$
o(x,y)=\begin{cases} 4, \text{ if } f(x,y)=0 \\ 0, \text{ if } f(x,y)=1, \end{cases} \tag{12}
$$

와 같이 나타나서 원래 영상의 명암이 반전된 영상이 나타나게 된다.

원 영상을 복원하는 과정에 광 신호 처리 중 발생하는 영향을 고려하면, JTC의 입력과 출력 평면은 각각 표본화된 영역이므로 표본화된 영상의 주파수 영역과 공간 영역의 관계는

$$\Delta d = \frac{1}{2f_{x0}} \tag{13}$$

$$x = k\Delta d = k\frac{L}{N_x}$$

$$u = k\frac{1}{\Delta d} = k\frac{N_x}{L}, \qquad k = 0,1,...,N_x - 1$$

으로 주어지며 편의상 x축과 u축만 표시 하였다. 여기서 Δd는 표본화 간격, f_{x0}는 영상의 x축의 최고 주파수, L은 x축의 영상 길이, k는 화소번호이며 N_x는 표본화 개수이다. 그림 1에서 암호화 된 영상과 복호화키 영상의 중심이 $(\pm u_0, 0)$에 있으므로 각각의 중심이 복호화 시스템의 주파수 영역의 결합 입력 평면의 1/4, 3/4 지점에 위치하는 것과 같은 의미를 가진다. 따라서 식 (13)을 식 (11)에 대입하여 정리하면

$$\begin{aligned} |o(x,y)|^2 &= 2 + 2\cos\left[4\pi\left(\frac{1}{4\Delta d}\right)(k_x \Delta d)\right] \\ &= 2 + 2\cos(\pi k_x), \end{aligned} \tag{14}$$

와 같으며 여기서 n은 정수이고, k_x는 x축의 화소 번호이다. 식 (14)에서 얻은 결과는 x축의 화소 위치에 따라서

$$o(x,y) = \begin{cases} 4, & k_x = 2n \\ 0, & k_x = 2n+1, \end{cases} \tag{15}$$

와 같은 복원 영상을 얻게 된다. 따라서 이 방법은 입력 영상과 기준 영상의 중심 이동에 따른 위상 성분의 영향이 출력 평면에 발생하게 되어 재생 영상에 영향을 미치는 문제를 발생시킨다.

2.3 이중 랜덤 위상 암호화

2.3.1 진폭형(Amplitude based method)

그림 2와 같이 암호화 할 원영상의 입력영상은 $f(x,y)$로 나타내며, 입력면의 랜덤 위상 함수와 푸리에 면의 랜덤 위상 함수를 각각 $\exp[j2\pi p(x,y)]$와 $\exp[j2\pi b(u,v)]$로 표기 한다. 이때 (x,y)는 공간 영역의 좌표를 나타내고, (u,v)는 푸리에 영역에서의 좌표를 나타낸다. 입력 영상 $f(x,y)$는 0과 1사이의 값으로 규격화된 양의 실수 함수로 가정하며, $p(x,y)$와 $b(u,v)$는 서로 독립적이며, 이 또한 0과 1사이에서 균일하게 분포된 랜덤 함수라 가정한다. 진폭형 이중 랜덤 위상 암호화 방법은 간단하게 2단계로 처리된다. 먼저 첫 번째 입력 함수 $f(x,y)$와 입력 랜덤 위상 마스크 $\exp[j2\pi p(x,y)]$와 곱한다. 즉, 입력함수와 랜덤위상의 곱은 $H(u,v)$의 푸리에 변환인 임펄스응답(impulse response) $h(x,y)$와 컨볼루션(convolution)이 된다. 이 처리과정은

$$\psi_A(x,y)= \{f(x,y)\exp[j2\pi p(x,y)]\}*h(x,y), \tag{16}$$

와 같다. 이때 *는 컨볼루션(convolution) 연산을 의미한다. 이 암호화의 처리과정은 광학적 또는 전자적으로 구현 할 수 있다. 그러나 어떠한 경우든 암호화된 영상 $\psi_A(x,y)$는 진폭과 위상이 모두 표현될 수 있어야 한다.

암호화 영상 $\psi_A(x,y)$복원과정은 그림 2(b)와 같이 암호화된 영상을 푸리에 변환한 뒤, 암호화 과정에서 사용한 랜덤 위상 함수의 복소공액을 곱해준다. 그 다음으로 푸리에 역변환을 취하므로 원 영상을 복원 할 수 있

다. 즉

$$\mathcal{A}(x,y)\exp[j2\pi\mathcal{P}(x,y)] = \mathcal{F}^{-1}\{\mathcal{F}\{\mathcal{A}(x,y)\exp[j2\pi\mathcal{P}(x,y)]\} \times H(u,v)\times H^{*}(u,v)\}. \quad (17)$$

이때 $\mathcal{F}\{\cdot\}$ 와 $\mathcal{F}^{-1}\{\cdot\}$ 는 각각 푸리에 변환과 역변환을 나타내며, 위첨자 *는 복소공액을 나타낸다. 원 영상의 복원은 CCD와 같은 세기 검출기로 사용하면 $|\exp[j2\pi p(x,y)]|^2 = 1$에 의하여 원 영상 $f(x,y)$를 복원 할 수 있다.

2.3.2 위상형(Phase based method)

위상형 암호화 방법은 진폭형과 유사하며, 그림 2(a)의 입력영상 $f(x,y)$ 대신 위상 변조 된 $\exp[j\pi f(x,y)]$를 입력한다. 이때 진폭형 암호화 방법에서 가정한 것과 동일하게 입력영상 $f(x,y)$는 0과 1사이의 균일한 분포를 가지므로 위상 변조된 입력영상 $\exp[j\pi f(x,y)]$는 $[0,\pi]$의 분포를 가진다. 위상형 암호화 영상 $\psi_P(x,y)$은

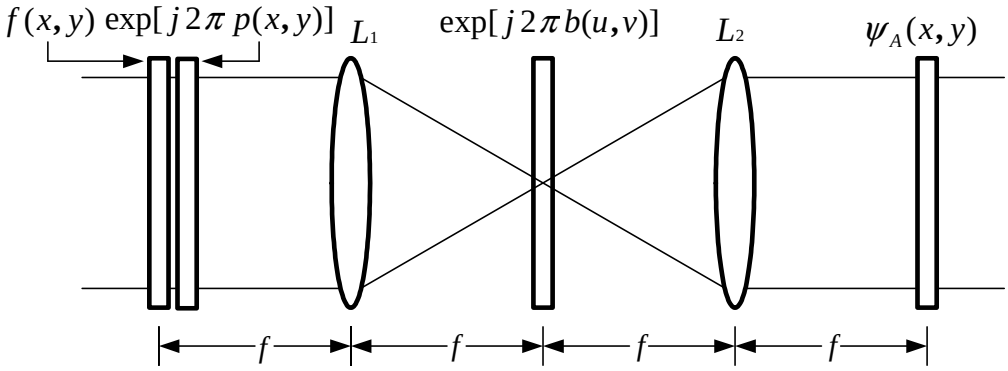
$$\psi_P(x,y) = \{\exp[j\pi f(x,y)]\times\exp[j2\pi p(x,y)]\}*h(x,y), \quad (18)$$

으로 표현된다. 또한 광학적인 방법이나 전자적인 방법으로 구현 될 수 있으나 광학적인 시스템으로 구성하기 위해서는 복소함수를 표현할 수 있는 영상 장치가 필요하고, 올바른 복호화를 위해서는 암호화 과정에서 사용된 랜덤 키의 복소공액이 있어야 한다는 단점을 가기고 있기에 전자적으로 구

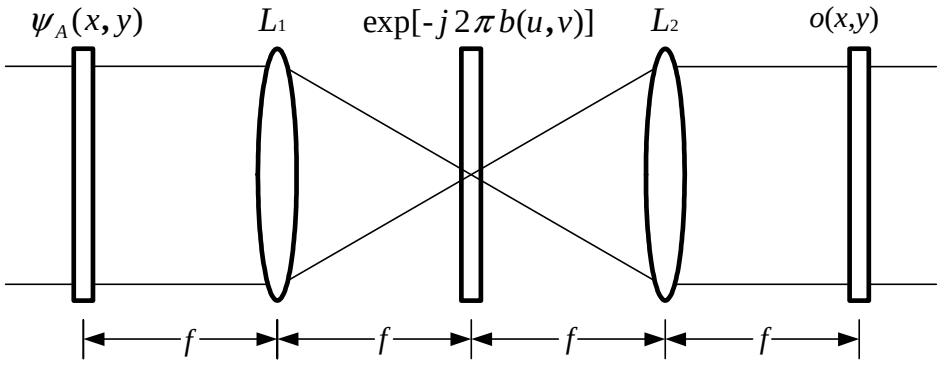
현하는 경우가 광학적인 구현 방법보다 훨씬 더 간단하며, 우수한 성능을 발휘 한다. 복원 방법은 진폭형의 암호화 의 복원 방법과 동일하게 처리한다. 즉

$$\exp[j\pi f(x,y)]\times\exp[j2\pi p(x,y)] \tag{19}$$
$$=\mathcal{F}^{-1}\{\mathcal{F}\{\exp[j\pi f(x,y)]\times\exp[j2\pi p(x,y)]\}\times H(u,v)\times H^{*}(u,v)\}.$$

식 (19)에서 $\exp[-j2\pi p(x,y)]$를 곱한 뒤 위상만을 추출하여 π를 나누어서 원 영상 $f(x,y)$를 구할 수 있다.



(a) 암호화 과정



(b) 복호화 과정

그림 2. 진폭형 이중 랜덤 위상 암호화 방법: (a) 암호화 과정, (b) 복호화 과정

Fig. 2. Amplitude-based double random phase encoding method : (a) Encryption process, (b) Decryption process

제 3 장 제안한 암호화 및 복호화 방법

기존의 광 암호화 시스템에서 이중 무작위 위상 부호화 방법은 광축 정렬의 어려움과 정확한 복소 공액 값을 가지는 위상 카드제작의 어려움이 있고 결합 변환 상관기를 기반으로 한 암호화 시스템은 출력 평면에 큰 세기의 자기상관이 나타나므로 광 보안 시스템에 이용하기에 어려움이 있다. 그래서 본 논문에서 제안한 방법은 위상 랩핑 방법을 이용하여 암호화 및 복호화에 사용될 위상 변조된 영상들을 각각 비선형적인 조합으로 표현한 후 이를 주파수에 영역에서 암호화키와 복호화키를 실수 값으로 표현하여 위상 부호화하여 암호화하고 생체 정보인 지문영상을 이용함으로써 암호화 수준을 향상시키고 실질적인 광학적인 구현을 가능하게 하고 공간 필터를 2-f 광 상관기를 이용하여 원 영상을 복원하는 방법을 제안하였다.

제안한 암호화 영상은 원 영상이 아닌 위상 변조된 임의의 영상과 무작위 위상 영상을 곱하여 위상 랩핑과 제로 패딩하여 푸리에 변환한 후 이 변환된 영상의 실수 값과 생체정보인 지문영상을 위상 부호화하여 만든다. 따라서 허가받지 않은 사용자가 위상 측정 방법 등을 통하여 암호화된 영상의 위상 값을 추출하더라도 복호화키의 정보 없이는 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하고 실수 값을 위상 부호화함으로써 현재에 사용되는 공간광변조기로 표현이 가능하다. 복호화 과정은 암호화된 영상과 위상 랩핑 방법에 의해 만들어진 푸리에 복호화키를 곱하여 푸리에 역 변환하여 출력평면에 공간필터를 두어서 원 영상을 복원함으로써 외란과 충격의 문제점과 4-f 시스템의 광축 정렬 문제를 해결할 수 있으며 복원영상의 해상도를 향상시킬 수 있다.

3.1 암호화 방법

그림 3은 본 논문에서 제안한 암호화 방법의 블록 다이어그램이다.

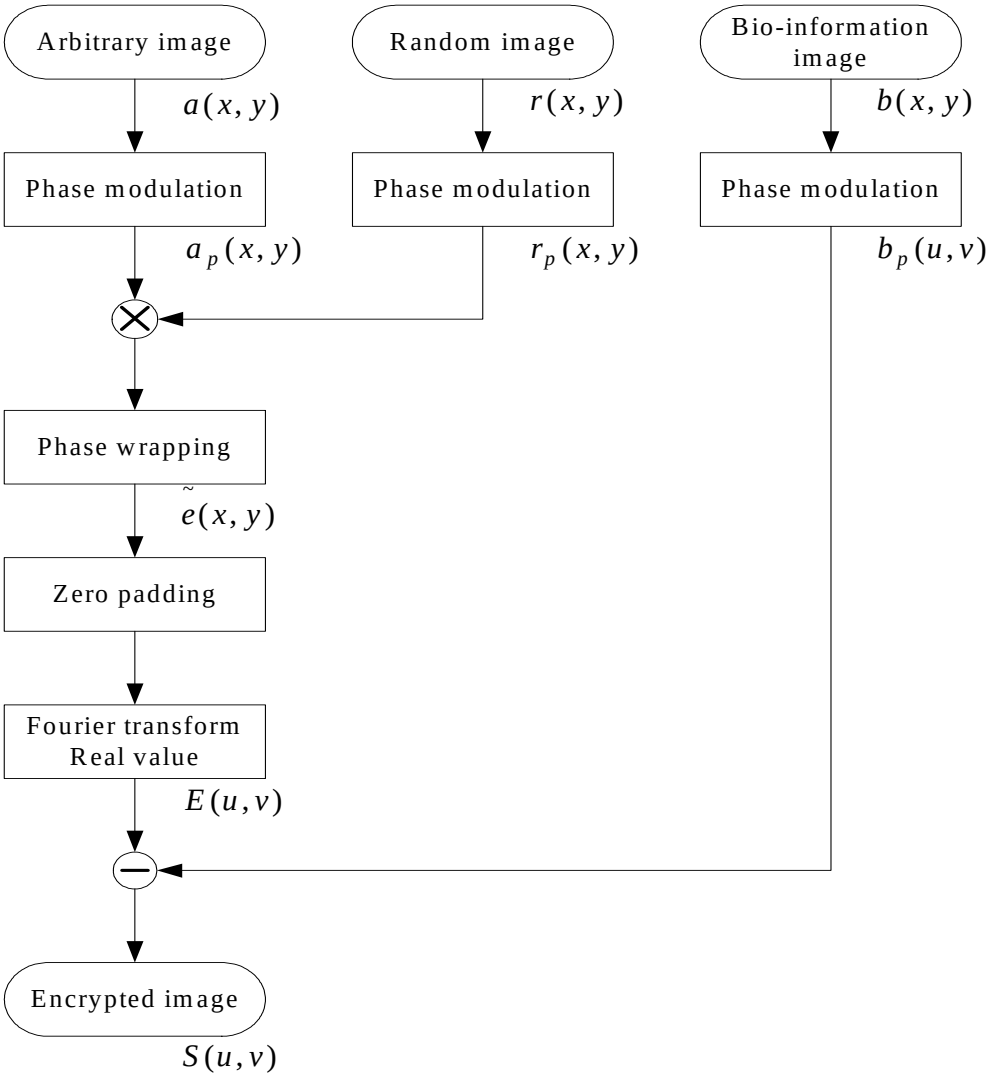


그림 3. 제안한 암호화 방법의 블록 다이어그램

Fig. 3. The block diagram of proposed encryption method.

암호화 할 원 영상 $f(x,y)$, 암호화에 필요한 임의의 영상 $a(x,y)$, 무작위 영상$r(x,y)$, 연산키 영상 $d(x,y)$라고 하면 위상 변조된 원 영상 $f_p(x,y)$는 제안한 암호화 방법에서

$$f_p(x,y) = \exp[j\pi f(x,y)] = \exp\{j\pi[a(x,y) + 2r(x,y) - d(x,y)]\}, \tag{20}$$

로 표현되고 여기에서 암호화 할 원 영상 $f(x,y)$는 정규화과정을 통해서 $[0,1]$사이 값을 가진다. 먼저 암호화에 필요한 임의의 영상 $a(x,y)$와 컴퓨터로 발생시킨 무작위 영상 $r(x,y)$을 각각 위상 변조하고 위상 변조된 각각의 영상 $a_p(x,y), r_p(x,y)$는

$$a_p(x,y) = \exp[j\pi a(x,y)],\ r_p(x,y) = \exp[j2\pi r(x,y)], \tag{21}$$

와 같이 표현되며 변조된 영상의 위상 값은 각각 $[0,\pi]$ 와 $[0,2\pi]$사이이고 그 세기는 '1'이므로 $|a_p(x,y)|^2 = |r_p(x,y)|^2 = 1$로 주어진다. 두 위상 변조된 영상을 곱한 영상은

$$\begin{aligned} \exp[j\pi e_A(x,y)] &= a_p(x,y) r_p(x,y) \\ &= \exp\{j\pi[a(x,y) + 2r(x,y)]\}, \end{aligned} \tag{22}$$

와 같고 암호화에 필요한 임의의 영상과 무작위 영상의 선형적인 합임을 알 수 있다. 여기에서 $\exp\{j\pi e_A(x,y)\}$를 암호화에 필요한 산술 연산키라고 가정하고 아래첨자 'A'는 산술연산을 표현한다. 만약 이 암호화에 필요한 산술 연산키를 사용한다면 위상성분들의 산술적인 연산에 의해 암호화에

필요한 임의의 영상의 정보가 암호화키에 포함되어 있어서 암호화된 영상이 불법적인 사용자에 의해 분석이 용이하게 된다. 따라서 이 선형적인 합을 제안한 위상 랩핑 방법을 이용하여 비선형적인 값으로 변환하여 암호화에 필요한 위상 랩핑 연산키 및 복호화 연산키를 만든다. 이 방법은

$$\exp[j\pi e_A(x,y)] = \exp\{j\pi[e_A(x,y) \pm 2n]\} \tag{23}$$
$$\exp[j\pi d_A(x,y)] = \exp\{j\pi[d_A(x,y) \pm 2n]\},$$

의 원리를 이용하며 여기에서 n은 정수이다. 즉 암호화에 필요한 산술 연산키 $\exp\{j\pi e_A(x,y)\}$의 위상 값은 $[0,3\pi]$ 사이이므로 이를 $[0,2\pi]$ 사이 값으로 위상 랩핑시킨다. 따라서 암호화에 필요한 위상 랩핑 연산키 $\tilde{e}(x,y)$는

$$\tilde{e}(x,y) = \exp[j\pi e(x,y)] \tag{24}$$
$$= \begin{cases} \exp\{j\pi[e_A(x,y)]\}, & 0 \le e_A(x,y) < 2 \\ \exp\{j\pi[e_A(x,y)-2]\}, & 2 \le e_A(x,y) < 3, \end{cases}$$

에 의해 표현되고 이를 제로 패딩하고 푸리에 변환한 후 실수 값을 취하여 푸리에 암호화키 $E(u,v)$는

$$E(u,v) = FT_{real}\{\tilde{e_z}(x,y)\}, \tag{25}$$

로 표현되며 여기에서 $FT_{real}\{\bullet\}$은 푸리에 변환 후 실수 값을 취하는 연

산이고 아래 첨자 z는 제로 패딩 연산자이다. 제안한 논문에서 생체정보로 사용되는 특정인 지문을 사용하기 위하여 지문영상 $b(u,v)$을 위상 변조하고 위상 변조된 영상 $b_p(u,v)$는

$$b_p(u,v) = \exp[j\pi b(u,v)] \tag{26}$$

와 같이 표현되며, 보안 암호화키 $S(u,v)$는

$$S(u,v) = E(u,v) - b_p(u,v) \tag{27}$$

와 같이 나타낸다. 최종 암호화키 $\widetilde{E}(u,v)$는 식 (26)과 (27)에 의해서,

$$\widetilde{E}(u,v) = \exp\left\{\frac{j\pi[S(u,v)+b_p(u,v)]}{nC}\right\} \tag{28}$$

로 표현된다. 여기에서 n은 실수 값의 정규화를 위한 값이고 C는 PSNR에서 필요한 요소이다. 이때 만약 허가되지 않은 개인이나 그룹이 암호화키를 위상 측정 방법 등으로 분석하더라도 임의의 영상조차 얻기가 어려우며 만약 임의의 영상이 분석되더라도 암호화키에서는 원 영상의 정보를 포함하고 있지 않기 때문에 정확한 복호화키 없이는 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다.

3.2 복호화 방법

그림 4는 본 논문에서 제안한 복호화 방법의 블록 다이어그램이다.

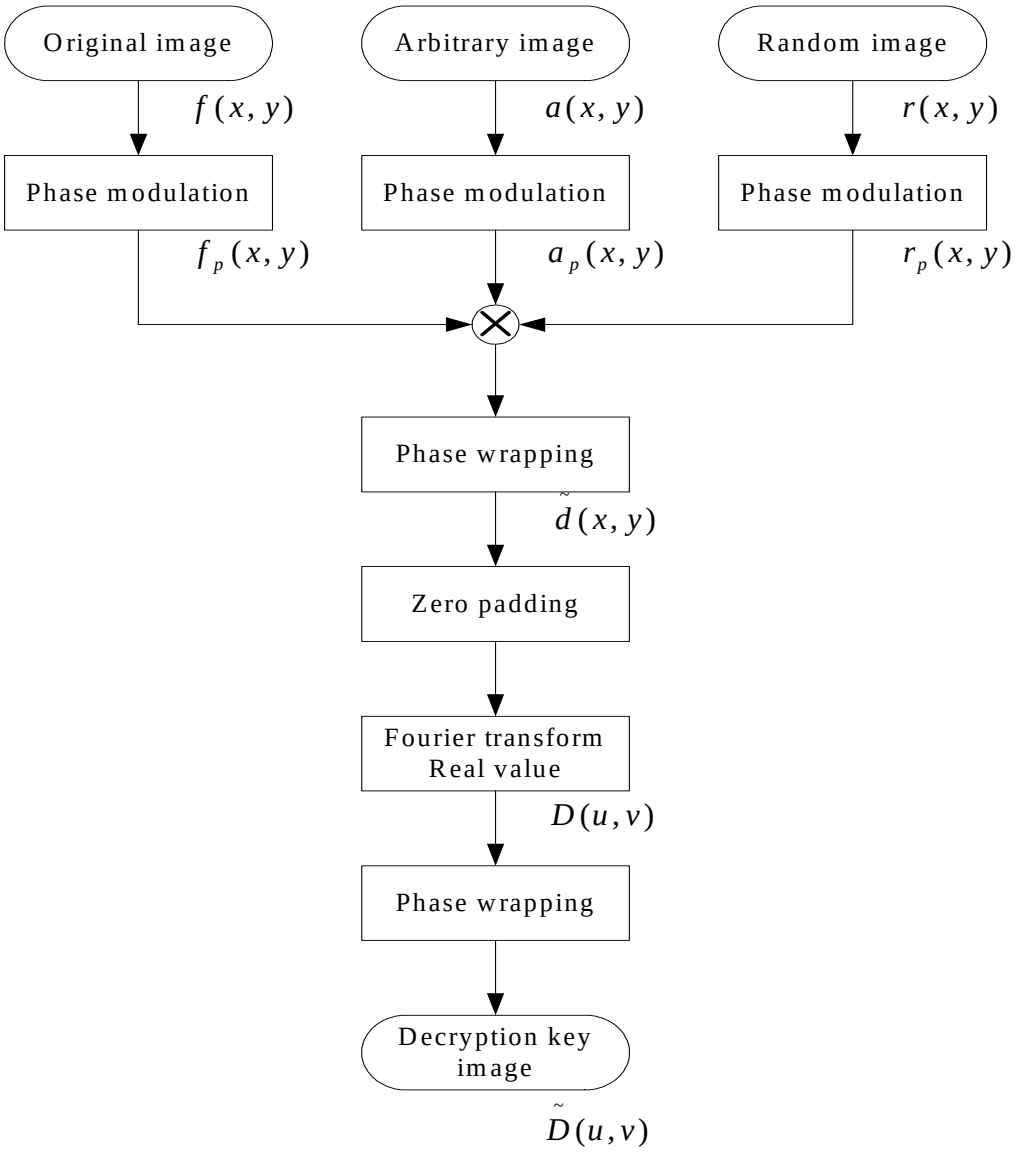


그림 4. 제안한 복호화 방법의 블록 다이어그램

Fig. 4. The block diagram of proposed decryption method.

복호화 방법은 시스템 내부에 존재하는 복호화키 영상을 분석함으로써 있을 수 있는 복제 가능성을 배제하기 위하여 암호화에 이용한 동일한 위상 랩핑 방법을 복호화 연산키 $\exp\{j\pi d(x,y)\}$에 적용한다. 먼저 복호화키 영상을 재생하기 위하여 식 (20) 에서 표현된 위상성분들의 단순한 가감법에 의해

$$\exp[j\pi d_A(x,y)] = \exp\{j\pi[a(x,y)+2r(x,y)-f(x,y)]\}, \tag{29}$$

와 같이 표현할 수 있으며 여기에서 $\exp\{j\pi d_A(x,y)\}$를 복호화키를 만들기 위한 복호화 산술 연산키라고 가정하고 암호화키를 만드는 과정과 동일하게 위상 랩핑 방법을 적용한다. 즉 복호화 산술 연산키 $\exp\{j\pi d_A(x,y)\}$의 위상 값은 $[-\pi,3\pi]$사이이므로 이를 $[0,2\pi]$사이 값으로 위상 랩핑(phase wrapping)시킨다. 따라서 복호화 연산키 $\exp\{j\pi d(x,y)\}$는

$$\exp[j\pi d(x,y)] = \begin{cases} \exp\{j\pi[d_A(x,y)+2]\}, & -1 \le d_A(x,y) < 0 \\ \exp\{j\pi[d_A(x,y)]\}, & 0 \le d_A(x,y) < 2 \\ \exp\{j\pi[d_A(x,y)-2]\}, & 2 \le d_A(x,y) < 3, \end{cases} \tag{30}$$

에 의해 만들어지고 이를 암호화에서와 같이 동일한 방법으로 제로 패딩하고 푸리에 변환한 후 실수 값을 취하여 푸리에 복호화키 $D(u,v)$를 얻을 수 있고 이를 위상 변조시켜 최종 복호화키 $\widetilde{D}(u,v)$를 아래식과 같이 얻을 수 있다.

$$D(u,v) = FT_{real}\left\{\widetilde{d}_z(x,y)\right\} \tag{31}$$

$$\widetilde{D}(u,v) = \exp\left[\frac{j\pi D(u,v)}{nC}\right].$$

제안한 복호화를 위한 실험 구성도는 그림 5와 같으며 복호화 과정에서 위상 변조된 영상 $b_p(u,v)$와 보안 암호화키 $S(u,v)$에 의해 표현되는 최종 암호화키 $\widetilde{E}(u,v)$와 최종 복호화키 $\widetilde{D}(u,v)$는 2-f 광 시스템 구성도의 푸리에 영역에 각각 위치한다.

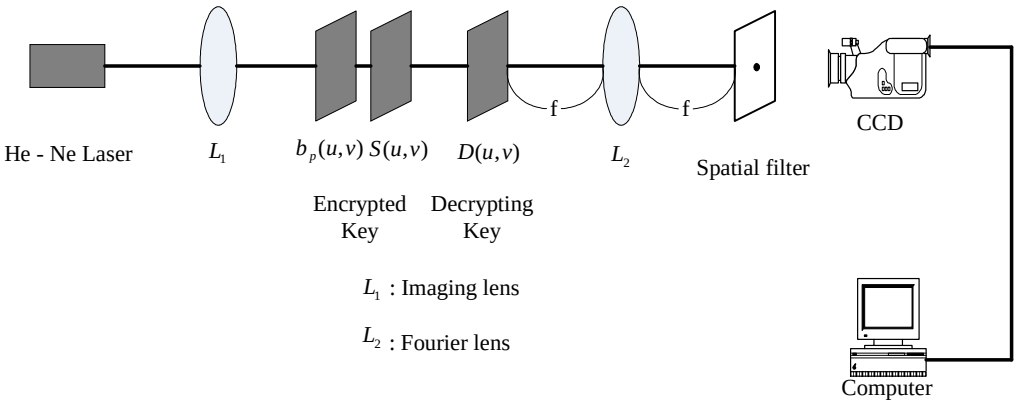


그림 5. 영상 복원을 위한 광 구성도

Fig. 5. Optical setup used for image decryption

이때 키들 사이의 공간이 존재하면 프레넬 회절이 발생함으로 이를 줄이기 위해서 동일한 푸리에 영역에 붙여서 놓아야 하며 여기에서 푸리에 렌즈 L_2를 통과하기 전의 영상은

$$\widetilde{E}(u,v)\widetilde{D}(u,v) = \exp\left[\frac{j\pi S(u,v)}{nC}\right]\exp\left[\frac{j\pi b_p(u,v)}{nC}\right]\exp\left[\frac{j\pi D(u,v)}{nC}\right] \tag{32}$$

$$= \exp\left\{\frac{j\pi}{nC}[E(u,v)+D(u,v)]\right\}$$

$$\approx 1+\frac{j\pi}{nC}[E(u,v)+D(u,v)],$$

로 표현되고 여기에서 C값이 충분히 크다면 테일러급수(Taylor series)에 의해 근사화 되므로 푸리에 렌즈 L_2에 통과한 식 (32)의 영상은

$$FT\left\{1+\frac{j\pi}{nC}FT[E(u,v)+D(u,v)]\right\} \tag{33}$$

$$= \delta(x,y)+\frac{j\pi}{nC}FT[E(u,v)+D(u,v)],$$

로 표현된다. 식 (33)에서 우변항의 $\delta(x,y)$는 영차 성분(zero-order component)으로 공간 필터에 의해 제거되고 그에 따른 CCD에 나타나는 출력세기함수는

$$O_{CCD}(x,y)=\left|\frac{j\pi}{nC}\mathrm{FT}[E(u,v)+D(u,v)]\right|^2 \tag{34}$$

$$=\left(\frac{\pi}{nC}\right)^2\left|\widetilde{e_z}'(x,y)+\widetilde{d_z}'(x,y)\right|^2$$

$$=\left(\frac{\pi}{nC}\right)^2\Big\{\left|\widetilde{e_z}'(x,y)\right|^2+\left|\widetilde{d_z}'(x,y)\right|^2$$

$$+\widetilde{e_z}'(x,y)\,\widetilde{d_z}'^{*}(x,y)+\widetilde{e_z}'^{*}(x,y)\widetilde{d_z}'(x,y)\Big\}$$

$$=\left(\frac{\pi}{nC}\right)^2\{1+1+\exp\{j\pi[e_z'(x,y)-d_z'(x,y)]\}$$

$$+\exp\{-j\pi[e_z'(x,y)-d_z'(x,y)]\}\}$$

$$=\left(\frac{\pi}{nC}\right)^2\{1+1+\exp[j\pi f_z'(x,y)]+\exp[-j\pi f_z'(x,y)]\}$$

$$=\left(\frac{\pi}{nC}\right)^2\{2+2\cos[\pi f_z'(x,y)\},$$

와 같으며 여기서 {*}는 복소 공액을 나타낸다. 식 (34)에서 제로 패딩한 영상 $\widetilde{e_z}(x,y)$ 와 $\widetilde{d_z}(x,y)$를 푸리에 변환하여 실수 값만 취해 역 푸리에 변환한 영상인 $\widetilde{e_z}(x,y)$와 $\widetilde{d_z}(x,y)$는 제로 패딩하기 전 영상성분인 $\tilde{e}(x,y)$와 $\tilde{d}(x,y)$가 각각 영차성분을 중심으로 쌍으로 존재하는 특성을 가지게 되고 또한 위상 성분 $e_z'(x,y)$는 식 (22)에서 표현한 $a(x,y)$와 $2r(x,y)$의 성분을 영차 성분을 중심으로 쌍으로 존재하게 되고, 위상 성분 $d_z'(x,y)$는 식 (30)에서 표현한 $d(x,y)$의 성분을 영차성분을 중심으로 쌍으로 존재하게 된다. 따라서 식 (34)에서와 같이 복호화 과정을 거치게 되면, 한 영상 내에 두 개의 $f(x,y)$성분이 대칭적으로 존재하는 $f_z'(x,y)$영상이 CCD평면상에서 나

타난다. 식 (34)에서 원 영상의 미러 영상이 포함된 반전 영상이 복원되고 비선형성을 가지는 여현 함수에 의해 영상의 왜곡이 발생함을 알 수 있으나 이는 컴퓨터의 후처리를 통하여 복원 가능하다.

제 4 장 실험 및 고찰

4.1 실험

본 논문에서는 컴퓨터 모의실험을 수행하기 위해 사용한 영상들을 그림 6에 나타내었고 화소수는 128×128이다. 그림 6(a)는 복원할 원 영상 $f(x,y)$로 'Lena'를 사용하였고 그레이 값을 가지고 그림 6(b)는 암호화될 임의의 영상 $a(x,y)$로 'baboons'영상이고 그림 6(c)는 컴퓨터로 발생시킨 무작위 영상 $r(x,y)$이며 이들을 각각 $[0,1]$사이의 값으로 정규화 시키고 랩핑 방법에 의해 범위가 $[0,2]$사이 값으로 변환한 암호화에 사용될 $\tilde{e}(x,y)$를 그림 6(d)에 나타내었으며 이는 임의의 영상과는 전혀 관계없는 무작위 패턴으로 나타남을 확인할 수 있다. 또한 만약 허가되지 않은 사용자가 암호화키를 분석하더라도 임의의 영상을 복원할 원 영상으로 오인하게 되므로 복제 가능성을 배제할 수 있다. 그림 6(e)는 위상 랩핑 방법에 의해 복호화에 사용될 $\tilde{d}(x,y)$를 나타내었으며 이는 복원할 원 영상의 정보가 비선형성에 의해 무작위 패턴으로 나타남을 알 수 있다.

그림 7(a)는 암호화에 사용될 $\tilde{e}(x,y)$를 위상 변조하고 257×257로 제로 패딩한 영상이며 위상 변조된 영상은 눈으로 볼 수 없는 복소함수이므로 위상을 세기 패턴으로 나타내었다. 그림 7(b)는 그림 7(a)를 푸리에 변환한 후 실수 값을 취하여 위상 변조하여 제안한 방법에서 사용될 최종 암호화키 $S(u,v)$이고 그림 7(c)는 생체정보로 사용되는 특정인 지문영상 $b(u,v)$이며 그림 7(d)는 제안한 위상 랩핑 방법에 의해 만들어진 올바른 최종 복호화키 $\tilde{D}(u,v)$를 나타내었으며 그림 7(e)는 최종 암호화키와 위상 변조된 지문영상과 최종 복호화키를 그림 5의 광 구성도에 의해 복원한 영상의 반

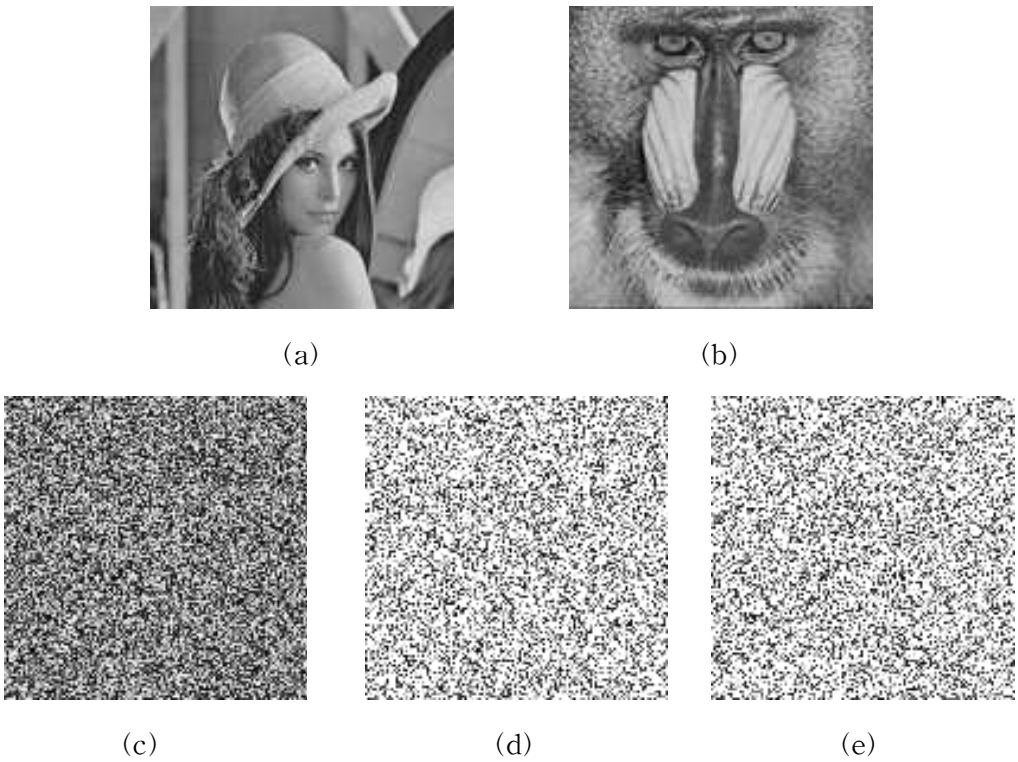


그림 6. 컴퓨터 실험 결과 (128×128): (a) 원 영상 $f(x,y)$, (b) 임의의 영상 $a(x,y)$, (c) 무작위 영상 $r(x,y)$, (d) 암호화에 필요한 위상 랩핑 영상 $\tilde{e}(x,y)$, (e) 복호화에 필요한 위상 랩핑 영상 $\tilde{d}(x,y)$.

Fig. 6. Computer simulation results (128×128): (a) the original image $f(x,y)$, (b) the arbitrary image $a(x,y)$, (c) the random image $r(x,y)$, and (d) the image $\tilde{e}(x,y)$, and (e) the image $\tilde{d}(x,y)$

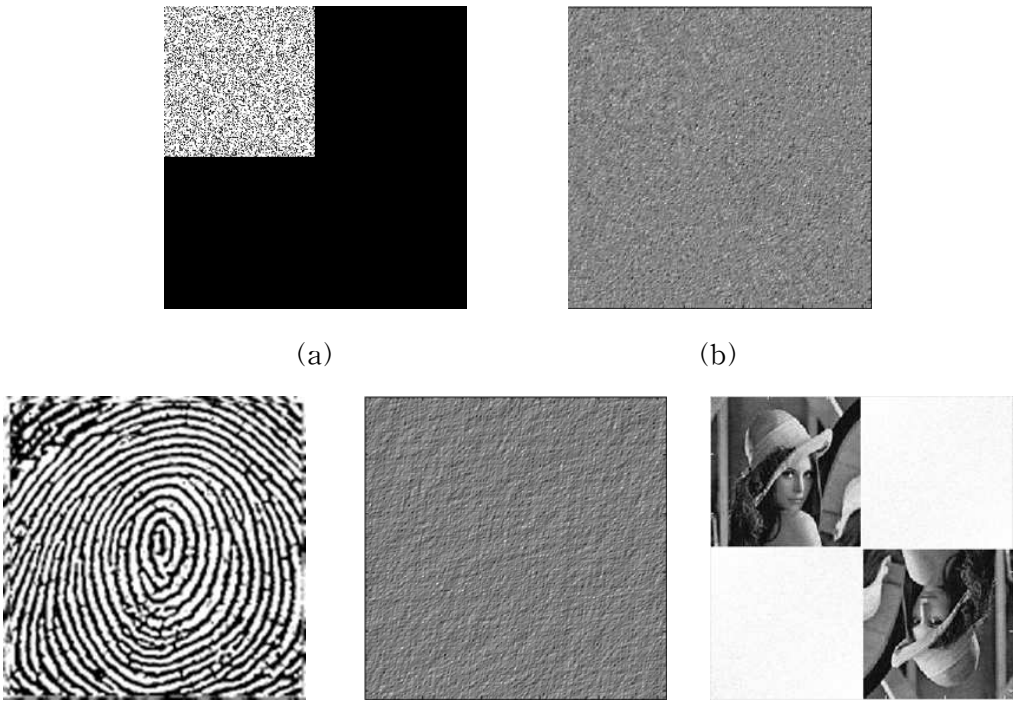
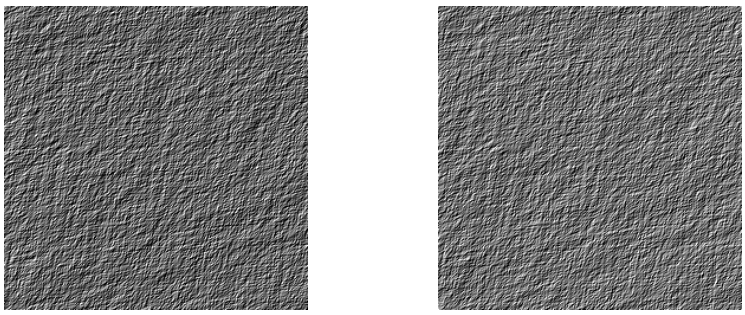


그림 7. 컴퓨터 실험 결과 (257×257): (a) 제로 패딩 영상 $\widetilde{e_z}(x,y)$, (b) 최종 암호화키 영상 $S(u,v)$, (c) 지문 영상 $b(u,v)$, (d) 최종 복호화키 영상 $\widetilde{D}(u,v)$, (e) 반전 복원된 영상

Fig. 7. Computer simulation results (257×257): (a) zero-padding image $\widetilde{e_z}(x,y)$, (b) encryption key image $S(u,v)$, (c) fingerprint image $b(u,v)$, (d) decryption key image $\widetilde{D}(u,v)$, and (e) reversal reconstructed image

전 영상을 나타낸 것이다. 여기에서 그레이 영상을 재생함으로써 식 (34)에서 비선형성을 가지는 여현 함수에 의해 원 영상의 왜곡이 발생하는데 그림 7(e)에서 이를 보상하지 않았지만 후처리를 통하여 보상할 수 있다.



(a) (b)

그림 8. 컴퓨터 실험 결과 : (a) 거짓 복호화키, (b) 거짓 복호화키로 재생된 영상.

Fig. 8. Computer simulation results : (a) incorrect order of keys, (b) Decryption key image with inaccuracy.

그림 8(a)는 허가되지 않은 임의의 사용자가 컴퓨터를 통해 만든 거짓 복호화키이고 그림 8(b)는 이에 대응되는 복원 영상으로써 제안한 위상 랩핑 방법을 이용한 올바른 복호화키의 정보 없이 거짓 키로는 영상이 올바르게 재생되지 않음을 확인할 수 있다.

4.2 암호화된 영상의 손실에 대한 고찰

그림 9는 제안한 방법에서 복원영상의 해상도는 C 값에 영향을 미치게 되므로 C 값에 따른 원 영상과 복원 영상의 해상도를 표현하는 첨두치 신호 대 잡음비(Peak signal-to noise ratio, PSNR)를 나타내었다 여기서 사용된 PSNR의 표준은

$$\mathrm{PSNR} = 20\log \frac{2^{n_{bit}}}{\left\{ \frac{1}{N \times M} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \left[\| f(x,y) | - | f'(x,y) \|^2 \right] \right\}^{1/2}} \tag{35}$$

이며 여기서 $N \times M$은 각 영상의 픽셀 수이며 $f(x,y)$와 $f^{'}(x,y)$는 원 영상과 복원 영상이며 n_{bit}는 픽셀을 표현하는 bit 수이다.

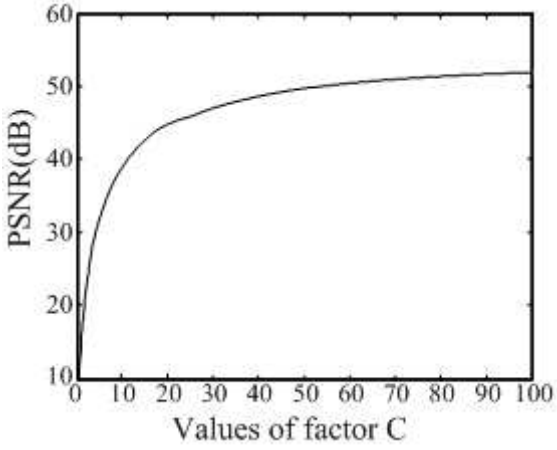


그림 9. C 값의 변화에 따른 복원영상의 PSNR

Fig. 9. PSNR of reconstructed image according to C

그림 9에서 PSNR은 C 값이 [0,20]정도에서 급격히 증가하다가 20이상에서 서서히 증가함을 알 수 있으며 C 값이 클수록 복원 영상의 해상도는 증가하지만 실질적인 공간광변조기가 표현할 수 있는 범위가 제한되어 있고 보통 30dB가 넘으면 두 영상의 차이를 눈으로 구분할 수 없음으로 C 값을 15로 선택하여 컴퓨터 모의실험을 수행하였다.

또한 실제 위상 암호화 시스템은 세기 암호화 시스템보다 암호화 수준은 향상되지만 잡음이나 위상 마스크의 흠집 등에 민감하여 영상의 왜곡이 발생할 수 있다. 따라서 암호화키 영상이나 복호화키 영상의 계속적인 사용으로 인한 흠집 등의 문제로 인한 복원 영상의 왜곡이 발생할 수 있으므로 암호화된 영상을 임의로 블로킹하여 그에 대응하는 복원 영상을 표현하였다. 그림 10(a), 10(b)와 10(c)는 각각 암호화키 영상인 그림 7(b)를 각각 25%, 50%와 75%를 u축으로 블로킹하였을 경우와 이를 그림 5의 실험 구성도에 의해 복원되었을 경우 그에 대응되는 복원 영상을 각각 그림 10(d), (e)와 (f)에 나타내었다. 여기에서 암호화키 영상의 블로킹되는 픽셀의 위치 정보가 무작위로 변하더라도 동일한 해상도를 가짐을 모의실험을 통해서 확인하였다. 그림 10(f)에서 암호화된 영상의 75%가 블로킹되더라도 원 영상의 정보를 얻을 수 있음을 알 수 있다. 제안한 방법은 현재의 공간광변조기의 기술이 크기 변조 혹은 위상 변조에 대한 성분만을 기록할 수 있으므로 실질적인 광 실험을 위해서 암호화키와 복호화키를 위상 부호화하여 표현하였고 또한 최근의 위상 변조 공간광변조기가 표현할 수 있는 위상값의 범위가 2π이상이다. 하지만 실질적인 실험상에서는 공간대역폭제한과 공간광변조기의 양자화 손실로 인한 영상의 해상도가 떨어지는 단점을 가진다.

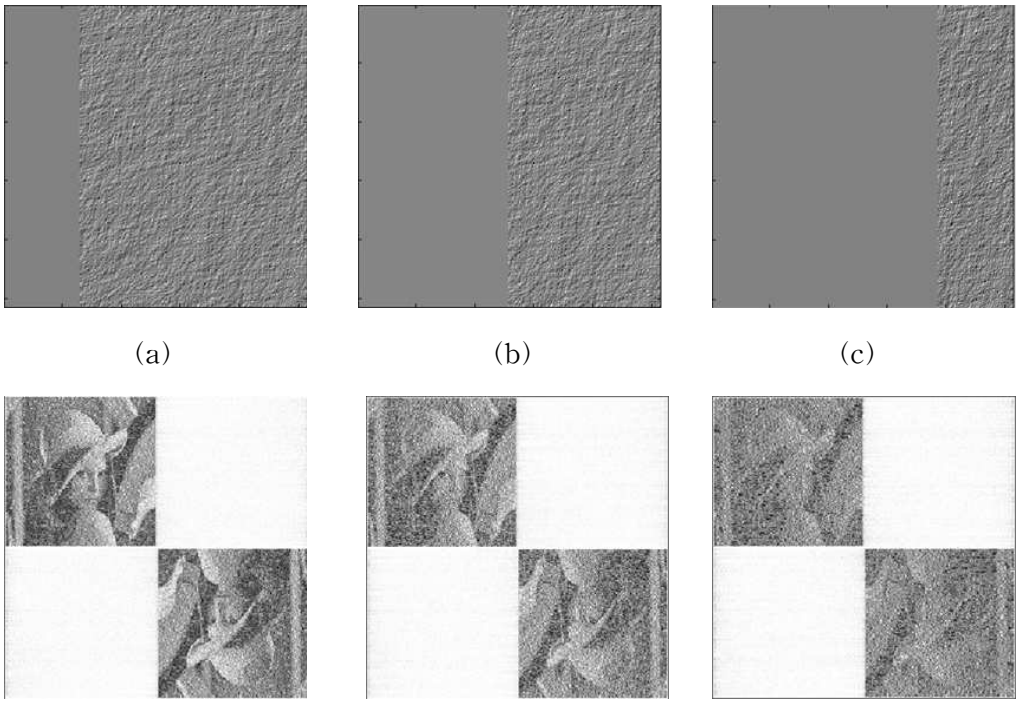


그림 10. 암호화된 영상의 u 축 차단에 따라 재생된 영상; (a) 25% 차단, (b) 50% 차단, (c) 75% 차단, (d) (a)에 의해 재생된 영상, (e) (b)에 의해 재생된 영상 (f) (c)에 의해 재생된 영상

Fig. 10. Reconstructed images from the encrypted image according to the u-axis blocking; (a) 25% blocked encrypt image, (b) 50% blocked encrypt image, (c) 75% blocked encrypt image, (d) reconstructed image of (a), (e) reconstructed image of (b), and (f) reconstructed image of (c).

Ⅴ. 결 론

본 논문에서는 생체정보와 위상 랩핑 방법을 이용하여 주파수 영역에서 위상 부호화하여 외부 잡음에 강한 보다 향상된 수준의 암호화 방법을 제안하였다. 제안한 암호화 방법은 푸리에 변환된 영상의 실수값을 취하고 위상 부호화하여 표현함으로써 실질적인 광 암호화 시스템에서 복소값을 표현하기 어려운 단점을 해결할 수 있다. 생체정보인 지문영상을 이용함으로써 암호 키의 부정사용을 방지 할 수 있고 영상정보의 진위 여부를 개인의 인증을 통해서 가려낼 수 있다. 복호화 과정에서 푸리에 역변환하는 한 과정만 이용하므로 기존의 4-f 광 상관기의 광축 정렬 문제와 간섭계 등에서 나타나는 외란 등의 영향에 강한 특성을 가짐으로써 복원영상의 해상도를 향상시켰다.

컴퓨터 모의실험을 통하여 제안한 암호화 방법을 검증하였으며 암호화키 영상이 블로킹되더라도 원 영상의 정보를 가지고 있음을 확인하였다. 기존의 암호화 시스템에서 광축 정렬 문제와 복소 공액 값을 가지는 위상 카드 제작의 어려운 단점을 보완하였으며 생체정보와 위상 랩핑 방법을 이용함으로써 허가받지 않은 사용자가 위상 측정 방법 등을 통하여 암호화된 영상의 위상 값을 추출하더라도 복호화키의 정보 없이는 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다. 광학 소자의 성능 개선이 위상 정보를 표현하는 식각 기술과 더불어 향상된다면 제안한 방법의 실질적인 광 실험 구현이 가능할 것이라 생각된다.

참 고 문 헌

[1] B. Schneier, Applied cryptography-protocol, algorithms, and source code in C, 2nd ed., John Wiley & Sons, New York, 1995.

[2] A. Shamir, "How to share secret," *Communications of ACM*, vol. 22, pp. 612-613, 1979.

[3] H. Naor and A. Shamir, "Visual cryptography," Advanced in Cryptography Eurocrypto'94, vol. 950, no. 7, pp. 1-12, 1995.

[4] B. Javidi, and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng., vol. 33, no. 6, pp. 1752-1756, 1994.

[5] R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," Opt. Eng., vol. 35, no. 9, pp. 2464-2469, 1996.

[6] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20, no. 7, pp. 767-769, 1995.

[7] B. Javidi, G. Zhang, and Jian Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," Opt. Eng., vol. 35, no. 9, pp. 2506-2512, 1996.

[8] B. Javidi and E. Ahouzi, “Optical security system with Fourier plane encoding,” Appl. Opt., vol. 37, no. 26, pp. 6247-6255, 1998.

[9] T. Nomura and B. Javidi, “Optical encryption using a joint transform correlator architecture,” Opt. Eng., vol. 39, no. 8, pp. 2031-2035, 2000.

[10] T. Nomura and B. Javidi, “Optical encryption system with a binary key code,” Appl. Opt., vol. 39, no. 26, pp. 4783-4787, 2000.

[11] M. Yamazaki and J. Ohtsubo, “Optimization of encrypted holograms in optical security systems,″ Opt. Eng., vol. 40, no. 1, pp. 132-137, 2001.

[12] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, “Fault tolerance properties of a double phase encoding encryption technique,” Opt. Eng., vol. 36, no. 4, pp. 992-998, 1997.

[13] B. Javidi, A. Sergent, and E. Ahouzi, “Performance of double phase encoding encryption technique using binarized encrypted images,” Opt. Eng., vol. 37, no. 2, pp. 565-570, 1998.

[14] B. Wang, C. C. Sun, W. C. Su, and A. E. T. Chiou, “Shift-tolerance property of an optical double-random phase-encoding encryption system,” Appl. Opt., vol. 39, no. 26, pp. 4788-4793, 2000.

[15] N. Towghi, B. Javidi, and Z. Luo, “Fully phase encrypted image processor,” J. Opt. Soc. Am. A, vol. 16, no. 8, pp. 1915-1927, 1999.

[16] X. Tan, O. Matoba, T. Shinura, K. Kuroda, and B. Javidi, “Secure optical storage that uses fully phase encryption,” Appl. Opt., vol. 39, no. 35, pp. 6689-6694, 2000.

[17] P. C. Mogensen and J. Gluckstad, “Phase-only optical encryption,” Opt. Lett., vol. 25, no. 8, pp. 566-568, 2000.

[18] P. C. Mogensen and J. Glückstad, “Phase-only optical decryption of a fixed mask,” Appl. Opt., vol. 40, no. 8, pp. 1226-1235, 2001.

[19] J. Ohtsubo and A. Fujimoto, “Practical image encryption and decryption by phase-coding technique for optical security systems,” Appl. Opt., vol. 41, no. 23, pp. 4848-4855, 2002.

[20] H. T. Chang, “Image encryption using separable amplitude-based virtual image and iteratively retrieved phase information,” Opt. Eng., vol. 40, no. 10, pp. 2165-2171, 2001.

[21] C. S. Weaver and J. W. Goodman, “A technique for optically convolvoing two functions,” *Applied Optics*, vol. 5, no. 8, pp. 1248-1249, 1966.

[22] S. J. Park, C. S. Kim, J. G. Bae, and S. J. Kim, “Fourier-plane encryption technique based on removing the effect of phase terms in JTC,” Optical Review, vol. 8, no. 6, pp. 413-412, 2001.