

## 반복적인 위상 랩핑 방법을 이용한 실질적인 암호화 및 복호화 시스템

서동환† · 이성근\* · 김윤식\*

(원고접수일 : 2008년 7월 16일, 원고수정일 : 2008년 8월 27일, 심사완료일 : 2008년 8월 27일)

### Practical Encryption and Decryption System using Iterative Phase Wrapping Method

Dong-Hoan Seo† · Sung-Geun Lee\* · Yoon-Sik Kim\*

**Abstract :** In this paper, we propose an improved practical encryption and fault-tolerance decryption method using a non-negative value key and random function obtained with a white noise by using iterative phase wrapping method. A phase wrapping operating key, which is generated by the product of arbitrary random phase images and an original phase image, is zero-padded and Fourier transformed. Fourier operating key is then obtained by taking the real-valued data from this Fourier transformed image. Also the random phase wrapping operating key is made from these arbitrary random phase images and the same iterative phase wrapping method. We obtain a Fourier random operating key through the same method in the encryption process. For practical transmission of encryption and decryption keys via Internet, these keys should be intensity maps with non-negative values. The encryption key and the decryption key to meet this requirement are generated by the addition of the absolute of its minimum value to each of Fourier keys, respectively. The decryption based on 2-f setup with spatial filter is simply performed by the inverse Fourier transform of the multiplication between the encryption key and the decryption key and also can be used as a current spatial light modulator technology by phase encoding of the non-negative values. Computer simulations show the validity of the encryption method and the robust decryption system in the proposed technique.

**Key words :** Fourier optic(푸리에 광학), Phase wrapping(위상 랩핑), Optical information processing(광정보처리), Encryption and decryption(암호화 및 복호화)

#### 1. 서 론

현대 사회에 있어서 정보의 보호에 대한 필요성

온 공공기관, 연구소, 산업현장 뿐만 아니라 개인의 사생활에 이르기까지 다양한 분야에서 대두되고 있으며, 이에 따른 정보 보호 시스템에 대한 연구

† 교신저자(한국해양대학교 전기전자공학부. E-mail: dhseo@hhu.ac.kr, Tel: 051)410-4412)

\* 한국해양대학교 전기전자공학부

들이 다양하게 진행되고 있다. 하지만 각종 광학 장비 및 복사기의 발달로 인하여 각종 카드나 화폐들을 보다 정밀하게 복제 또는 위조하게 되었으며, 이로 인한 경제적 피해뿐만 아니라 개인의 인권에 대한 피해도 증가되고 있다. 특히 여권이나 신분증의 위조는 각종 범죄와 밀접국의 수단으로 사용되고 있어 사회불안에까지 영향을 미치고 있다. 이를 예방하기 위해서 최근에 CCD 카메라, 복사기, 스캐너 등과 같은 기존의 광세기 검출기로는 볼 수도 복제할 수도 없는 복소함수 형태의 랜덤 위상 패턴을 사용하는 광학적 정보보호 기술이 연구되고 있으며 이는 광을 이용한 신호는 세기정보와 위상(phase) 정보를 동시에 광학적인 매질 또는 공간 광 변조기(spatial light modulator, SLM)에 기록이 가능하다는 특성에 기인하며 이러한 광학적 암호화 시스템은 광전자 소자들을 이용하여 실 시간적인 구현이 가능하고 랜덤 위상 암호화 키를 사용함으로써 정보를 위조하거나 해독하지 못하도록 함으로써 우리의 생활을 심각하게 위협하는 개인정보보호의 문제를 해결할 수 있는 획기적인 접근방법으로 제시되고 있다. 광학적으로 암호화된 영상은 전통적인 상관 시스템이나 간섭계 시스템을 이용하여 원 영상을 재생하게 되는데, 이때 암호화에 사용된 무작위 위상마스크에 의해서 진위 여부를 판정하게 된다. 이를 이용한 광학적 암호화 시스템에는 이중 무작위 위상 부호화(double random phase encoding), XOR 연산, 위상 세기(phase-contrast) 방법, 위상 컴퓨터 형성 홀로그램(phase computer generated hologram), 결합 변환 상관기(joint transform correlator; JTC), 또는 반복 알고리즘을 이용한 방법 등이 있다<sup>[1]-[5]</sup>. 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. 이 방법은 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 상관기는 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<sup>[6]</sup>.

세기정보 암호화 수준을 향상시키기 위하여 입력 평면에 위상정보를 가지는 원 영상을 이용하여 암호화하는 방법<sup>[7]</sup>이 제안 되었으며 이는 위상정보를 암호화한 후 일반화된 위상세기 방법(generalized phase-contrast technique)을 이용하여 간단히 원 영상을 복원할 수 있는 방법으로 제안 하였다. 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 예측 할 수 있는 문제점이 있다. 이 문제점을 해결하기 위해 반복적인 알고리즘을 이용하여 임의의 세기 영상을 이용한 방법<sup>[8]</sup>이 제안되었으나 이 또한 광축 정렬의 어려움을 가지고 원 영상을 재생하기 위한 시간소모가 많은 단점이 있다. 위에서 제안된 대부분의 방법은 암호화 및 복호화 키의 정보가 양의 실수 값이 아니므로 인터넷 등과 같은 매체를 통한 실질적인 영상 전송에는 어려움이 따라 그에 맞는 코딩 및 부호화 방법이 요구되고 이에 대한 해결책이 제안되었다<sup>[9]-[10]</sup>.

본 논문에서는 반복적인 위상 랩핑 방법과 양의 실수값을 가지는 키를 이용하여 실질적이고 보다 향상된 수준의 암호화 및 외부 영향에 강인한 복호화 시스템을 제안한다. 위상 변조된 원 영상과 N 개의 서로 다른 임의의 랜덤 위상 영상을 양의 실수값을 가지는 키를 생성하기 위하여 제로 패딩한 후 서로 곱하여 위상 연산기를 생성한다. 이렇게

생성된 위상 연산기를 외부 영향에 강인한 키로 만들기 위하여 주파수영역으로 변환하고 실수값을 취한 후 키의 최소값의 절대치를 푸리에 변환된 키에 더함으로써 양의 실수 값을 가지는 암호화 키가 만들어 진다. 복호화 키는 N개의 서로 다른 임의의 랜덤 위상 영상들의 위상 랩핑하여 생성 후 암호화키 생성과 비슷한 방법으로 양의 실수값을 가지도록 만든다. 이 암호화 및 복호화 키는 양의 실수값을 가지므로 인터넷과 같은 매체를 통한 실질적인 전송이 가능하게 된다. 복호화 과정에서는 디지털 및 광학적으로 영상 복원이 가능하며 디지털적으로는 단순히 암호화키와 복호화키를 더하여 푸리에 역변환 과정으로 재생이 가능하며 광학적인 시스템은 기존의 4-f 광상관기의 광축정렬 문제 및 간섭계가 가지는 외란 및 충격의 문제점을 해결한 공간필터를 가진 2-f 상관시스템이며 픽셀대 픽셀 대응을 용이하게 하여 복원영상의 해상도를 향상시킬 수 있다. 또한 허가받지 않은 사용자가 세기 측정 및 위상 측정 방법 등을 통하여 암호화된 영상의 위상 값을 추출하더라도 반복적인 위상 랩핑 방법을 통하여 원 영상의 정보의 분석을 어렵게 하였다.

## 2. 제안한 암호화 및 복호화 방법

원 영상  $f(x,y)$ , 임의의 무작위 영상  $r_i(x,y)$ , 연산기 영상  $a(x,y)$ 라고 하고 이 영상들을 위상 변조시켜서 표현하면 위상 변조된 원 영상  $f_p(x,y)$ 는 제안한 암호화 방법에서

$$\begin{aligned} f_p(x,y) &= \exp[j\pi f(x,y)] \\ &= \exp\left\{j\pi\left[\sum_{i=1}^N 2r_i(x,y) - a(x,y)\right]\right\}, \end{aligned} \quad (1)$$

로 표현되고 여기에서 원 영상  $f(x,y)$ 는 정규화과정을 통해서  $[0,1]$  사이 값을 가진다. 먼저 컴퓨터로 발생시킨 암호화에 필요한 임의의 무작위 영상  $r_i(x,y)$ 를 위상 변조한 영상  $r_{pi}(x,y)$ 는

$$r_{pi}(x,y) = \exp\{j\pi[2r_i(x,y)]\}, \quad (2)$$

와 같이 표현되며 변조된 임의의 무작위 영상  $r_{pi}(x,y)$ 의 위상 값은  $[0, 2\pi]$  사이이고 그 세기는

$|r_{pi}(x,y)|^2 = 1$ 로 주어진다. 식 (1)에서 위상 변조된 연산기 영상은

$$\begin{aligned} a_p(x,y) &= \exp[j\pi a(x,y)] \\ &= \exp\left\{j\pi\left[\sum_{i=1}^N 2r_i(x,y) - f(x,y)\right]\right\}, \end{aligned} \quad (3)$$

와 같고 연산기 영상은 위상 성분들의 단순한 선형적 가감법에 의해 생성된다. 이 영상의 키로 사용된다면 허가받지 않은 개인이나 그룹이 Zernike 위상 세기법 등을 통하여 위상값을 측정하여 원 영상의 정보에 대한 분석이 가능하다. 따라서 본 논문에서는 공간영역에서 반복적인 위상 랩핑 방법을 통하여 위상 값이 측정되더라도 원 영상의 정보의 분석이 어려운 방법을 제안한다. 즉 식 (3)에 표현된 선형적인 연산을 제안한 N개의 랜덤 함수를 반복적인 위상 랩핑 방법을 이용하여 비선형적인 값으로 변환한다. 임의의 위상영상  $\exp[j\pi p(x,y)]$ 에 기본적인 위상 랩핑 방법은

$$\exp[j\pi p(x,y)] = \exp\{j\pi[p(x,y) \pm 2n]\}, \quad (4)$$

와 같으며 여기에서 n은 정수이며 식 (4)의 위상 값은  $2\pi$ 의 정수배로 증가 및 감소하더라도 위상 영상 값의 변화가 없음을 알 수 있다. 따라서 먼저 공간영역에서 무작위 랜덤영상이 1개라고 가정하면 암호화에 필요한 위상 연산기  $\exp[j\pi a_A(x,y)]$ 는

$$\exp[j\pi a_A(x,y)] = \exp\{j\pi[2r_1(x,y) - f(x,y)]\}, \quad (5)$$

로 표현되며 이때 아래첨자 'A'는 단순한 산술연산을 표현한다.  $\exp[j\pi a_A(x,y)]$ 의 위상 값은  $[-\pi, 2\pi]$  사이이므로 이를  $[0, 2\pi]$  사이 값으로 위상 랩핑 시킨다. 따라서 암호화에 필요한 위상 랩핑 연산기  $\tilde{a}(x,y)$ 는

$$\tilde{a}(x,y) = \exp[j\pi a(x,y)] \quad (6)$$

$$= \begin{cases} \exp\{j\pi[a_A(x,y) + 2]\}, & -1 \leq a_A(x,y) < 0 \\ \exp\{j\pi[a_A(x,y)]\}, & 0 \leq a_A(x,y) < 2, \end{cases}$$

에 의해 표현되고 이를 다시 새로운 무작위 위상 영상을 곱하여 표현하면

$$\exp[j\pi \tilde{a}_A(x,y)] = \exp\{j\pi[2r_2(x,y) + \tilde{a}(x,y)]\}, \quad (7)$$

로 표현되며 이때  $\exp[j\pi\tilde{a}_A(x,y)]$ 의 위상값은  $[0, 4\pi]$  사이이므로 이를 다시  $[0, 2\pi]$  사이 값으로 위상 랩핑 시킨다. 따라서 동일한 위상 랩핑 연산기  $\tilde{a}(x,y)$ 는

$$\tilde{a}(x,y) = \begin{cases} \exp\{j\pi[\tilde{a}_A(x,y)]\}, & 0 \leq \tilde{a}_A(x,y) < 2 \\ \exp\{j\pi[\tilde{a}_A(x,y) - 2]\}, & 2 \leq \tilde{a}_A(x,y) < 4, \end{cases} \quad (8)$$

로 표현된다. 따라서 동일한 방법으로 무작위 영상을 컴퓨터로 N개 생성하여 식 (7)의 과정을 반복하여 위상 랩핑 연산기의 암호화 수준을 향상시키고 이에 따라 불법 사용자가 키 영상을 취득하더라도 원영상의 정보를 분석하기가 어렵게 한다. 반복적 위상 랩핑 방법으로 생성된 영상은 외부 영향에 강인 한 키로 만들기 위하여 주파수영역으로 변환한다. 이때 먼저 제로 패딩하고 푸리에 변환한 후 실수 값을 취하여 생성된 영상, 즉 푸리에 연산기  $A(u,v)$ 는

$$A(u,v) = FT_{\text{real}}\{\tilde{a}_z(x,y)\}, \quad (9)$$

로 표현되며 여기에서  $FT_{\text{real}}\{\cdot\}$ 은 푸리에 변환 후 실수 값을 취하는 연산이고 아래 첨자 z는 제로 패딩 연산자이다. 위의 수식 (5)에서 수식(9)에서 수행된 연산과 비슷한 방법으로 푸리에 랜덤 연산기  $R(u,v)$ 를 생성한다. 먼저 수식 (1)의 우변항 첫 번째 성분을 분리하여 표현하면 N개의 임의의 랜덤 위상 영상들을 곱하여 표현한 무작위 위상 영상  $r_p(x,y)$ 는

$$r_p(x,y) = \exp[j\pi r(x,y)] = \exp\left[j\pi\left(\sum_{i=1}^N 2r_i(x,y)\right)\right], \quad (10)$$

로 표현되며 이를 위에서 사용한 동일한 위상 랩핑 방법을 적용하여 무작위 위상 랩핑 연산기를 생성한다. 즉 만약 두 개의 무작위 랜덤 위상 영상이 사용된다면 무작위 위상 연산기  $\exp[j\pi a_A(x,y)]$ 는

$$\exp[j\pi r_A(x,y)] = \exp[j\pi[2r_1(x,y) + 2r_2(x,y)]], \quad (11)$$

로 표현되며 이때  $\exp[j\pi r_A(x,y)]$ 의 위상 값은  $[0, 4\pi]$  사이이므로 이를  $[0, 2\pi]$  사이 값으로 위상 랩핑 시킨다. 따라서 무작위 위상 랩핑 연산기  $\tilde{r}(x,y)$ 는

$$\begin{aligned} \tilde{r}(x,y) &= \exp[j\pi r(x,y)] \\ &= \begin{cases} \exp\{j\pi[r_A(x,y)]\}, & 0 \leq r_A(x,y) < 2 \\ \exp\{j\pi[r_A(x,y) - 2]\}, & 2 \leq r_A(x,y) \leq 4, \end{cases} \end{aligned} \quad (12)$$

으로 위상 랩핑하고 동일한 방법으로 컴퓨터로 생성된 N개의 무작위 위상 영상들을 식 (12)의 과정을 반복하여 무작위 위상 랩핑 연산기를 생성하고 이를 제로 패딩하고 푸리에 변환한 후 실수 값을 취하여 생성된 영상, 즉 푸리에 무작위 연산기  $R(u,v)$ 는

$$R(u,v) = FT_{\text{real}}\{\tilde{r}_z(x,y)\}, \quad (13)$$

로 표현된다. 이렇게 주파수 영역에서 생성된 푸리에 연산기  $A(u,v)$ 와 푸리에 무작위 연산기  $R(u,v)$ 를 정규화 시키면 각각 테이터 값의 범위는  $[-1, 1]$  사이 값을 가지게 된다. 따라서 인터넷 같은 매체를 통하여 이 데이터들을 전송하기 위해서는 양의 실수 값을 가져야 하므로 푸리에 연산기와 푸리에 무작위 연산기를 각각

$$\begin{aligned} E(u,v) &= A(u,v) + |\min(A(u,v))| \\ D(u,v) &= R(u,v) + |\min(R(u,v))|, \end{aligned} \quad (14)$$

로 변환시켜 암호화 키  $E(u,v)$ 와 복호화 키  $D(u,v)$ 를 생성한다. 식 (14)에 생성된 키들을 이용한 복호화는 디지털 및 광학적으로 복원이 가능하다. 제안한 복호화 시스템의 광학적인 실험 구조도는 Fig. 1과 같으며 각각의 키 영상들은 위상 값으로

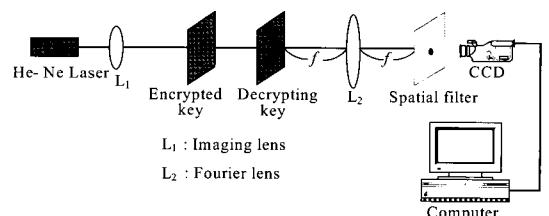


Fig. 1 Optical setup for decryption

표현이 가능한 위상변조 공간 광 변조기(LCSLM, liquid crystal spatial light modulator)를 이용하여 영상을 표현할 수 있으며 이 때 LCSLM에

표현되는 위상값을 감쇄시킴으로서 키들 간의 매핑을 원활히 할 수 있다. 따라서 광학적인 실험을 위한 식으로 식 (14)를 다시 표현하면

$$\begin{aligned}\tilde{E}(u,v) &= \exp\left(\frac{j\pi[E(u,v)]}{nC}\right) \\ \tilde{D}(u,v) &= \exp\left(\frac{j\pi[D(u,v)]}{nC}\right)\end{aligned}\quad (15)$$

와 같고 이들을 2-f 광 시스템 구성도의 푸리에 영역에 각각 위치시킨다. 이때 암호화 키와 복호화 키 사이의 공간이 존재하면 프레넬 회절이 발생함으로 이를 줄이기 위해서 동일한 푸리에 영역에 붙여서 놓아야 하며 여기에서 푸리에 렌즈  $L_2$ 를 통과하기 전의 영상은

$$\begin{aligned}\tilde{E}(u,v)\tilde{D}(u,v) &= \exp\left[\frac{j\pi E(u,v)}{nC}\right]\exp\left[\frac{j\pi D(u,v)}{nC}\right] \\ &= \exp\left\{\frac{j\pi}{nC}[E(u,v) + D(u,v)]\right\} \\ &\approx 1 + \frac{j\pi}{nC}[E(u,v) + D(u,v)]\end{aligned}\quad (16)$$

로 표현되며 여기에서 C값은 LCSLM에 표현되는 위상값을 감쇄시키는 상수로서 이 값이 충분히 크다면 테일러 급수(Taylor series)에 의해 근사화된다. 따라서 푸리에 렌즈  $L_2$ 에 통과한 식 (16)의 영상은

$$\begin{aligned}\text{FT}\left\{1 + \frac{j\pi}{nC}[A(u,v) + |\min(A(u,v))|] + R(u,v) + |\min(R(u,v))|\right\} \\ = \delta(x,y) + \frac{j\pi}{nC}\text{FT}[A(u,v) + R(u,v)]\end{aligned}\quad (17)$$

로 표현된다. 여기에서 1과  $|\min(A(u,v))|$  및  $|\min(R(u,v))|$  값은 모두 상수값을 가지므로 푸리에 변환을 하면 멜타함수  $\delta(x,y)$ 가 된다. 따라서 식 (17)에서 우변항의 첫 번째 성분인 영차 성분(zero-order component)은 공간 필터에 의해 제거되고 그에 따른 CCD에 나타나는 출력세기함수는

$$\begin{aligned}O_{CCD}(x,y) &= \left|\frac{j\pi}{nC}\text{FT}[A(u,v) + R(u,v)]\right|^2 \\ &= \left(\frac{\pi}{nC}\right)^2 |\tilde{a}_z'(x,y) + \tilde{r}_z'(x,y)|^2 \\ &= \left(\frac{\pi}{nC}\right)^2 \{|\tilde{a}_z'(x,y)|^2 + |\tilde{r}_z'(x,y)|^2 \\ &\quad + \tilde{a}_z''(x,y)\tilde{r}_z'(x,y) + \tilde{a}_z'(x,y)\tilde{r}_z''(x,y)\} \\ &= \left(\frac{\pi}{nC}\right)^2 \{1 + 1 + \exp\{j\pi[r_z'(x,y) - a_z'(x,y)]\} \\ &\quad + \exp\{-j\pi[r_z'(x,y) - a_z'(x,y)]\}\} \\ &= \left(\frac{\pi}{nC}\right)^2 \{1 + 1 + \exp[j\pi f_z'(x,y)] + \exp[-j\pi f_z'(x,y)]\} \\ &= \left(\frac{\pi}{nC}\right)^2 \{2 + 2\cos[j\pi f_z'(x,y)]\}\end{aligned}\quad (18)$$

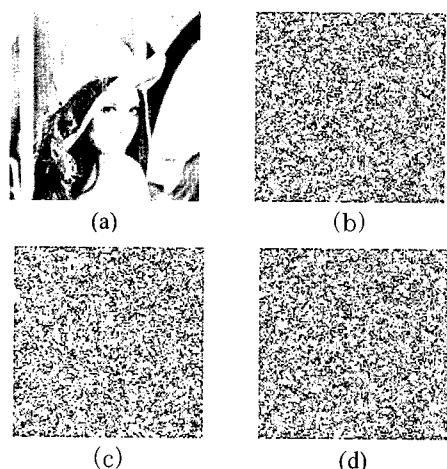
와 같다. 여기서  $\{ \cdot \}^*$ 는 복소 공액을 나타낸다. 식 (18)에서 제로 패딩한 영상  $\tilde{a}_z(x,y)$  와  $\tilde{r}_z(x,y)$ 를 푸리에 변환하여 실수 값만 취해 역 푸리에 변환한 영상인  $\tilde{a}_z'(x,y)$ 와  $\tilde{r}_z'(x,y)$ 는 제로 패딩하기 전 영상 성분인  $\tilde{a}(x,y)$ 와  $\tilde{r}(x,y)$ 가 각각 영차성분을 중심으로 쌍으로 존재하는 특성을 가지게 되고 또한 위상 성분  $a_z'(x,y)$ 는 식 (6)에서 표현한  $a(x,y)$ 의 성분을, 위상 성분  $r_z'(x,y)$ 는 식 (10)에서 표현한  $r(x,y)$ 의 성분을 각각 영차성분을 중심으로 쌍으로 존재하게 된다. 따라서 식 (18)에서와 같이 복호화 과정을 거치게 되면, 한 영상 내에 두 개의  $f(x,y)$  성분이 대칭적으로 존재하는  $f_z'(x,y)$  영상이 CCD 평면상에서 나타난다. 식 (18)에서 원 영상의 반전된 영상이 복원되고 여현 함수의 비선형성에 의해 영상의 왜곡이 발생함을 알 수 있으나 이는 컴퓨터의 후처리를 통하여 간단히 복원 가능하다. 또한 디지털적인 방법을 통한 영상 복원은 간단하게 암호화 키  $E(u,v)$ 와 복호화 키  $D(u,v)$ 를 더한 후 푸리에 변환하면

$$\begin{aligned}\text{FT}[A(u,v) + |\min(A(u,v))| + R(u,v) + |\min(R(u,v))|] \\ = \delta(x,y) + \text{FT}[A(u,v) + R(u,v)].\end{aligned}\quad (19)$$

와 같이 얻을 수 있으며 이는 식 (17)과 식 (18)에 의해 동일한 결과 값을 얻게 된다.

### 3. 컴퓨터 모의실험 및 고찰

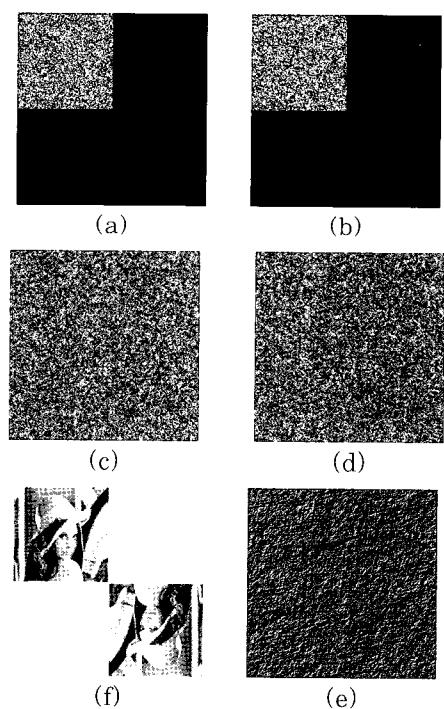
Fig. 2는 컴퓨터 모의실험을 수행하기 위해 사용한 영상들로 그 화소수는  $128 \times 128$ 이다. Fig. 2(a)는 복원할 원 영상  $f(x,y)$ 로 ‘Lena’를 사용하였고 그레이 값은 가지고 Fig. 2(b)는 컴퓨터로 발생시킨 N개의 무작위 영상들 중 하나인  $r_i(x,y)$ 이며 이를 각각  $[0, 1]$ 사이의 값으로 정규화 시키고 램프 방법에 의해 범위가  $[0, 2]$ 사이 값으로 변환한 암호화에 사용될  $a(x,y)$ 를 Fig. 2(c)에 나타내었으며 이는 복원할 원 영상의 정보가 비선형성에 의해 무작위 패턴으로 나타남을 알 수 있다. Fig. 2(d)는 램프 방법에 의해 복호화에 사용될  $r(x,y)$ 를 나타내었다.



**Fig. 2** Images used for computer simulation ( $128 \times 128$ ): (a) original image  $f(x,y)$ , (b) random image  $r_i(x,y)$ , (c) wrapping image for encryption  $a(x,y)$ , and (d) wrapping image for encryption  $r(x,y)$

Fig. 3(a)와 3(b)는 암호화에 사용될  $a(x,y)$ 와 복호화에 사용될  $r(x,y)$ 를 각각 위상 변조하고  $256 \times 256$ 로 제로 패딩한 영상이며 위상 변조된 영상들은 눈으로 볼 수 없는 복소함수이므로 위상을 세기 패턴으로 나타내었다. Fig. 3(c)와 3(d)는

Fig. 3(a)와 3(b)를 각각 푸리에 변환한 후 실수 값을 취하고 인터넷 등을 통한 영상 전송을 위하여 양의 실수 값을 가지는 영상으로 변환된 암호화키 영상  $E(u,v)$ 과 복호화 키 영상  $D(u,v)$ 이다. Fig. 3(e)와 3(f)는 각각 광학적 실험을 위하여 사용된 식(15)의 위상 변조된 암호화키와 위상 변조된 복호화키를 사용하여 Fig. 1의 광 구성도에 의해 복원한 영상과 허가되지 않은 임의의 사용자가 컴퓨터를 통해 만든 거짓 복호화키를 이용하여 복원한 영상을 컴퓨터 모의실험으로 나타낸 것이다. 또한 Fig. 3(e)와 3(f)는 식 (19)와 같이 디지털적인 실험을 통하여 동일한 결과를 얻을 수 있으며 그레이 영상을 재생함으로써 식 (18)의 결과에서 알 수 있듯이 여현 함수에 의해 원 영상의 약간의 왜곡이 발생하는데 Fig. 3(f)에서 이를 보상하지 않았지만



**Fig. 3** Simulation results ( $256 \times 256$ ): (a) zero-padded key phase image  $\tilde{a}_z(x,y)$ , (b) zero-padded random phase image  $\tilde{r}_z(x,y)$ , (c) encryption key  $E(u,v)$ , (d) decryption key  $D(u,v)$ , (e) inverted reconstructed images using correct key, and (f) reconstructed image using false key.

후처리를 통하여 간단히 보상하거나 혹은 암호화 및 복호화 키 영상 자체를 여현함수의 영향을 고려하여 생성하여 보상할 수 있다.

Fig. 4는 제안한 위상랩핑 방법의 타당성을 검증하기 위해 자기상관성분의 단면도를 나타내었다. Fig. 4(a)는 래핑이 없는 경우 식 (5)의 위상성분  $a_A(x,y)$ 를 자기상관한 결과이고 Fig. 4(b)는 래핑한 경우 식 (6)의 위상성분  $a(x,y)$ 를 자기상관한 결과이며 Fig. 4(c)는 식 (8)에 의해 래핑한 후 위상변조된 영상  $\tilde{a}(x,y)$ 를 자기상관한 결과이다. 따라서 위상랩핑한 영상이 화이트 노이즈 분포를 가짐으로서 복호화 키 없이는 원 영상의 재생이 어렵다는 것을 알 수 있다.

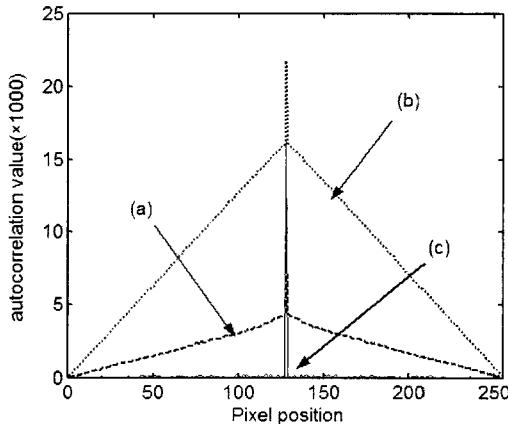


Fig. 4 Cross section of autocorrelation graphs: (a)  $a_A(x,y)$ , (b)  $a(x,y)$ , and (c)  $\tilde{a}(x,y)$

Fig. 5는 제안한 방법에서 광학적인 영상 복원을 위해서는 복원영상의 해상도가 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

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

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

을 표현하는 bit 수이다. Fig. 5에서 PSNR은 C 값이 [0, 20] 정도에서 급격히 증가하다가 20 이상에서 서서히 증가함을 알 수 있으며 C 값이 클수록 복원 영상의 해상도는 증가하지만 실질적인 공간 광변조기가 표현할 수 있는 범위가 제한되어 있고 보통 40dB가 넘으면 두 영상의 차이를 눈으로 구분할 수 없음으로 C 값을 20로 선택하여 컴퓨터 모의 실험을 수행하였다. 또한 실제 위상 암호화 시스템은 세기 암호화 시스템보다 암호화 수준은 향상되지만 잡음이나 위상 마스크의 흠집 등에 민감하여 영상의 왜곡이 발생할 수 있다. 따라서 암호화 키 영상이나 복호화 키 영상의 계속적인 사용으로 인한 흠집 등의 문제로 인한 복원 영상의 왜곡이 발생할 수 있으므로 암호화된 영상을 임의로 블로킹하여 그에 대응하는 복원 영상을 표현하였다.

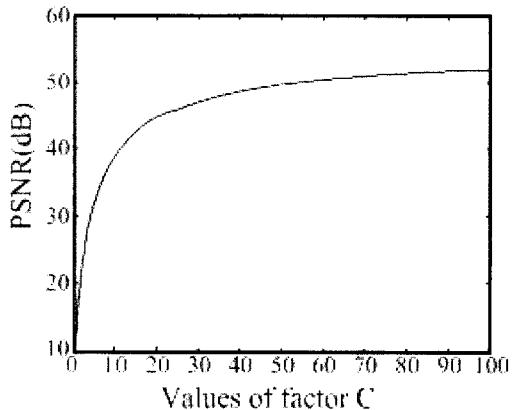
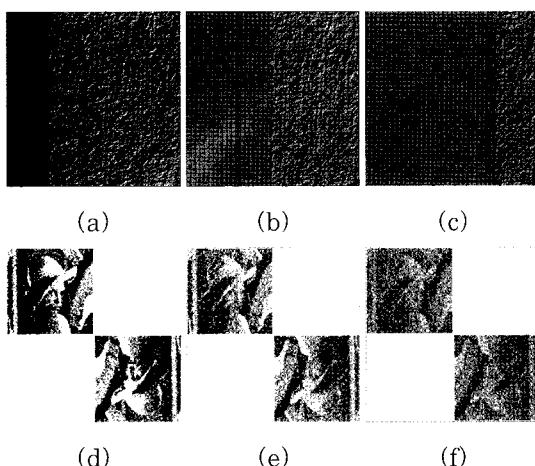


Fig. 5 PSNR for decrypted images with different values of factor C

Fig. 6(a), 6(b)와 6(c)는 각각 암호화 키 영상인 Fig. 3(c)를 각각 25%, 50%와 75%를  $u$ 축으로 블로킹하였을 경우와 이를 Fig. 1의 실험 구성도에 의해 복원되었을 경우 그에 대응되는 복원 영상을 각각 Fig. 6(d), (e)와 (f)에 나타내었다. 여기에서 암호화 키 영상의 블로킹되는 픽셀의 위치 정보가 무작위로 변하더라도 동일한 해상도를 가짐을 모의 실험을 통해서 확인하였다. Fig. 6(f)에서 암호화된 영상의 75%가 블로킹되더라도 원 영상의 정보를 얻을 수 있음을 알 수 있다. 이 주파수 영역에서 암호화가 이루어짐으로써 공간영역의 정

보를 가지고 있음을 나타낸다. 기존의 암호화 방법이 실수 값이나 복소수 값으로 암호화 및 복호화되므로 공간광변조기에 영상을 표현하기 어려운 문제점이 있었는데 제안한 방법에서는 양의 실수값을 가지는 암호화 및 복호화 방법을 제안하여 이러한 문제점을 해결할 수 있다. 또한 제안한 방법은 현재의 공간광변조기의 기술이 크기 변조 혹은 위상변조에 대한 성분만을 기록할 수 있으므로 실질적인 광 실험을 위해서 암호화키와 복호화키를 위상부호화하여 표현하였고 또한 최근의 위상 변조 공간광변조기가 표현할 수 있는 위상값의 범위가  $2\pi$  이상이다. 하지만 실질적인 실험상에서는 공간대역 폭제한과 공간광변조기의 양자화 손실로 인한 영상의 해상도가 떨어지는 단점을 가진다.



**Fig. 6** The occluded encrypted images of (a) 25%, (b) 50%, and (c) 75%, and the corresponding reconstructed images of (d), (e), and (f), respectively

#### 4. 결 론

본 논문에서는 선형적인 영상을 비선형적인 영상으로 변환하는 반복적인 위상 랩핑 방법을 이용하여 암호화 수준을 향상시키고 주파수영역에서 양의 실수값을 가지는 암호화 및 복호화 키를 생성하여 외부 잡음에 강하고 실질적인 영상 전송이 가능한 디지털 및 광학적 암호화 시스템을 제안하였다. 제

안한 암호화 방법은 반복적인 위상 랩핑을 통하여 허가되지 않은 개인이나 그룹이 암호화키나 복호화 키를 푸리에 변환이나 세기 및 위상측정 등으로 분석하더라도 키의 정보 확인을 어렵게 하였다. 또한 복호화 과정에서 푸리에 역 변환하는 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.

#### 참고문헌

- [1] 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.
- [2] 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.
- [3] B. Javidi and E. Ahouzi, "Optical security system with Fourier plane encoding," Appl. Opt., Vol. 37, No. 26, pp. 6247-6255, 1998.
- [4] 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.
- [5] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng., Vol. 39, No. 8, pp. 2031-2035, 2000.
- [6] 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.
- [7] P. C. Mogensen and J. Gluckstad, "Phase-only optical encryption," Opt. Lett., Vol. 25, No. 8, pp. 566-568, 2000.
- [8] C. H. Yeh, H. T. Cahng, H. C. Chien, and C. J. Kuo, "Design of caseaded phase Keys for a hierarchical security system," Appl. Opt., Vol. 41, No. 29, pp. 6128-6314, Oct. 2002
- [9] M. Z. He, L. Z. Cai, Q. Liu, X. C. Wang, X. F. Meng, "Multiple image encryption and watermarking by random phase matching," Opt. Commun. 247 pp. 29-37, 2005.
- [10] D-H Seo, C-M Shin, and K-B Cho, "Image encryption and decryption system using frequency phase encoding and phase wrapping method," Hankook Kwanghak Hoeji, Vol. 17, No. 6, pp.507-513, 2006.

**김윤식(金潤植)**

1955년 4월생, 1977년 한국해양대학교 기관공학과 졸업, 1979년 동 대학원 졸업(석사), 1986년 동경공업대학 대학원 졸업(석사), 1989년 동 대학원 졸업(박사), 1999년 12월-2001년 2월 미국 University of Colorado 방문교수, 현재 한국해양대학교 전기전자공학부 교수

## 저 자 소 개

**서동환(徐東煥)**

1970년 10월생, 1996년 경북대학교 전자공학과 졸업, 1999년 동 대학원 졸업(석사), 2003년 동 대학원 졸업(박사), 2004년 3월-현재 한국해양대학교 전기전자공학부 조교수

**이성근(李成根)**

1959년 1월생, 1983년 한국해양대학교 기관공학과 졸업, 1990년 동 대학원 졸업(석사), 1998년 동 대학원 졸업(박사), 1992년 3월-1998년 8월 대덕대학 제어계측과 조교수, 1998년 9월-현재 한국해양대학교 전기전자공학부 교수