주파수 위상 부호화와 위상 랩핑 방법을 이용한 영상 암호화 및 복호화 시스템

서동환†

한국해양대학교 전기전자공학부
㉾ 606-791 부산광역시 영도구 동삼동 1

신창목 · 조규보

경북대학교 전자전기컴퓨터학부
㉾ 701-702 대구광역시 북구 산격동 1370

(2006년 6월 12일 받음, 2006년 12월 1일 수정본 받음)

본 논문에서는 출력평면에 나타나는 원 영상을 재생시키기 위하여 위상 랩핑 방법을 이용하여 암호화 수준을 향상시키고 주파수 영역에서 위상 부호화하여 암호화함으로써 잡음에 강한 복호화 방법을 제안하였다. 암호화된 영상은 원 영상이 아닌 위상 변조된 가상 영상과 무작위 위상 영상을 곱하고 제로 패딩(zero-padding)하여 푸리에 변환한 후 이 변환된 복소 영상을 데이터 전송 및 매핑을 용이하게 하기 위하여 실수 값으로 변환하여 위상 부호화하여 만든다. 복호화 과정은 제안한 선형적인 영상을 비선형적인 영상으로 변환시키는 위상 랩핑 방법에 의해 각각 만들어진 암호화된 영상과 복호화 키를 곱하여 푸리에 역변환하여 공간필터를 가진 출력평면에서 원 영상을 복원함으로써 광축 정렬 문제와 픽셀 대 픽셀 대응이 용이하여 복원영상의 해상도를 향상시킬 수 있다. 제안한 방법은 허가되지 않은 사용자가 암호화된 영상을 분석함으로써 있을 수 있는 복제 가능성을 원 영상의 어떤 정보도 포함하지 않은 가상 영상을 사용함으로써 배제할 수 있고 또한 실수값을 위상 부호화함으로써 현재에 사용되는 공간 광 변조기로 표현이 가능하다. 컴퓨터 모의 실험을 통하여 제안한 암호화 방법의 적합성과 암호화된 영상과 복호화 키 영상에 잡음이 발생하더라도 원 영상의 복원이 가능함을 확인하였다.

주제어 : Phase encoding, Optical correlator, Phase wrapping

Ⅰ. 서 론

현대 정보화 사회에서는 정보산업의 발전으로 개인의 정보와 신용이 더욱 더 중요시되고 여권, 신용카드, 은행카드 등과 같은 개인의 신원을 증명할 수 있는 신분증의 사용이 늘어나고 있다. 그러나 컴퓨터 관련 장비들과 소프트웨어 기술의 발달로 화폐뿐만 아니라 여러 이미지 패턴들의 복제가 쉽게 이루어지고 있으며, 위조 기술이 고도화되고 완벽해짐에 따라 어떠한 경우에도 개인 정보보호 뿐만 아니라 위조나 복제를 근본적으로 차단할 수 있는 새로운 접근 방법에 관한 연구 개발이 절실히 요구되고 있다. 최근에는 CCD 카메라, 복사기, 스캐너 등과 같은 기존의 광세기 검출기로는 볼 수도 복제할 수도 없는 복소함수 형태의 랜덤 위상 패턴을 사용하는 새로운 광학적 정보보호 기술이 연구되고 있으며 이는 광을 이용한 영상신호는 세기정보나 위상(phase) 정보를 광학적인 매질 또는 공간 광 변조기(spatial light modulator, SLM)에 기록이 가능하다는 특성에 기인하며 이러한 광학적 시스템은 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.

현재 사용되는 광 보안 시스템은 주로 4-f 광 상관시스템[1-4]이나 간섭계 구조[5]를 이용하여 원 영상을 재생하게 되는데, 이때 암호화에 사용된 무작위 위상마스크에 의해서 주로 진위 여부를 판정하게 된다. 이를 이용한 대표적인 방법은 이중 무작위 위상 부호화 방법(double random phase encoding)으로 이는 4-f 광 상관기를 이용하여 입력 평면과 푸리에 평면에 두개의 랜덤 위상 마스크를 두어 영상을 암호화하고, 영상의 복원은 랜덤 위상의 복소 공액값을 가진 마스크를 푸리에 평면에 놓아 동일한 시스템을 이용하여 원 영상을 복원하게 된다. 이 방법은 정확한 복소 공액값을 가지는 위상 카드제작의 어려움과 광축 정렬의 어려움이 있으며, 간섭계를 이용한 시스템은 정밀한 실험구성을 필요로 하며 외부 교란에 많은 영향을 받는다는 단점이 있다. 이에 반하여 결합 변환 상관기(joint transform correlator, JTC)[6-9]는 광축정렬이 필요 없고 외부교란에도 거의 영향을 받지 않는 장점이 있다. 그러나 결합 변환 상관기는 그 구조적인 특성 때문에 출력 평면에 큰 세기의 자기상관 성분이 나타나는데, 이는 결합 변환 상관기를 광 상관 시스템이나 광 보안 시스템에 이용하기 어렵게 만드는 주원인이 된다. 또한 앞서 제안한 방법에서 암호화된 영상이 여러 형태의 외부 영향에 얼마나 강한 방법인가를 확인하였다.[10-12]

최근에는 세기정보 암호화 수준을 향상시키기 위하여 입력

† E-mail: dhseo@bada.hhu.ac.kr

평면에 위상정보를 가지는 원 영상을 이용하여 암호화하는 방법[13-17]들이 제안되었으며 이 중 Mogensen 등[15,16]은 위상 정보를 암호화한 후 일반화된 위상 세기 방법(generalized phase-contrast technique)을 이용하여 간단히 원 영상을 복원할 수 있는 방법이 제안하였다. 이 방법은 공간 영역에서 암호화 및 복호화가 이루어지므로 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 단점 중에 하나는 암호화키와 복호화키가 동일하므로 만약 허가되지 않은 사용자가 암호화된 영상을 분석하여 암호화키를 파악함으로써 복원 영상을 예측할 수 있는 문제점이 있다. 이 문제점을 해결하기 위해 반복적인 알고리즘을 이용하여 가상 세기 영상을 이용한 방법[18]이 제안되었으나 이 또한 4-*f* 광 상관기를 이용하므로 여전히 광축 정렬의 어려움을 가지고 원 영상을 재생하기 위한 시간소모가 많은 단점이 있다.

본 논문에서는 암호화 및 복호화에 사용될 위상 변조된 영상들을 각각 위상 랩핑 방법을 이용하여 비선형적인 조합으로 표현한 후 이를 주파수 영역에서 암호화키와 복호화키를 실수값으로 표현하여 위상 부호화하여 암호화함으로써 암호화 수준을 향상시키고 실질적인 광학적인 구현을 가능하게 하고 공간 필터를 가진 2-*f* 광 상관기를 이용하여 원 영상을 복원하는 방법을 제안하였다. 제안한 암호화 영상은 원 영상이 아닌 위상 변조된 가상 영상과 무작위 위상 영상을 곱하여 위상 랩핑과 제로 패딩(zero-padding)하여 푸리에 변환한 후 이 변환된 영상의 실수값을 위상 부호화하여 만든다. 따라서 허가되지 않은 사용자가 푸리에 변환이나 위상 측정 방법을 통하여 암호화된 영상의 위상값을 추출하더라도 복호화 키의 정보 없이는 결코 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하고 실수값을 위상 부호화함으로써 현재에 사용되는 공간 광 변조기로 표현이 가능하다. 복호화 과정은 암호화된 영상과 제안한 위상 랩핑 방법에 의해 만들어진 푸리에 복호화 키를 곱하여 푸리에 역변환하여 공간필터를 가진 출력 평면에서 원 영상을 복원함으로써 간섭계가 가지는 외란과 충격의 문제점과 4-*f* 시스템의 광축 정렬 문제를 해결할 수 있으며 픽셀 대 픽셀 대응을 용이하게 하여 복원영상의 해상도를 향상시킬 수 있다. 컴퓨터 모의 실험을 통하여 제안한 암호화 방법이 잡음이나 암호화된 영상의 블로킹에 강한 특성이 있음을 확인하였다.

II. 제안한 암호화 및 복호화 과정

원 영상 $f(x, y)$, 암호화할 가상 영상 $v(x, y)$, 무작위 영상 $r(x, y)$, 연산키 영상 $d(x, y)$라고 하면 위상 변조된 원 영상 $f_p(x, y)$는 제안한 암호화 방법에서

$$f_p(x,y)=\exp[j\pi f(x,y)]=\exp\{j\pi[v(x,y)+2r(x,y)-d(x,y)]\} \quad (1)$$

로 표현되며 여기에서 원 영상 $f(x, y)$는 정규화과정을 통하여 [0, 1]사이 값을 가진다. 먼저 암호화할 가상 영상 $v(x, y)$와 컴퓨터로 발생시킨 무작위영상 $r(x, y)$을 각각 위상 변조하고 위상 변조된 각각의 영상 $v_p(x,y)$, $r_p(x,y)$는

$$v_p(x,y)=\exp[j\pi v(x,y)]\ ,r_p(x,y)=\exp[j2\pi r(x,y)] \quad (2)$$

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

$$\begin{aligned}\exp[j\pi e_A(x,y)]&=v_p(x,y)r_p(x,y) \\ &=\exp\{j\pi[v(x,y)+2r(x,y)]\}\end{aligned} \quad (3)$$

와 같고 암호화할 가상 영상과 무작위 영상의 선형적인 합임을 알 수 있다. 여기에서 $\exp\{j\pi e_A(x, y)\}$를 암호화키를 만들기 위한 산술 연산키라고 가정하고 아래첨자 'A'는 산술연산을 표현한다. 만약 이 산술 연산키를 암호화키로 사용한다면 위상성분들의 산술적인 연산에 의해 가상 영상의 정보가 암호화키에 포함되어 있어서 암호화된 영상이 불법적인 사용자에 의해 분석이 용이하게 된다. 따라서 이 선형적인 합을 제안한 위상 랩핑 방법(phase wrapping method)을 이용하여 비선형적인 값으로 변환하여 암호화 연산키 및 복호화 연산키를 만든다. 이 방법은

$$\begin{aligned}\exp[j\pi e_A(x,y)]&=\exp\{j\pi[e_A(x,y)\pm 2n]\} \\ \exp[j\pi d_A(x,y)]&=\exp\{j\pi[d_A(x,y)\pm 2n]\}\end{aligned} \quad (4)$$

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

$$\begin{aligned}\tilde{e}(x,y)&=\exp[j\pi e(x,y)] \\ &=\begin{cases}\exp\{j\pi[e_A(x,y)]\}, & 0\le e_A(x,y)<2\\ \exp\{j\pi[e_A(x,y)-2]\}, & 2\le e_A(x,y)<3\end{cases}\end{aligned} \quad (5)$$

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

$$E(u,v)=\mathrm{FT}_{\mathrm{real}}\{\tilde{e}_z(x,y)\} \quad (6)$$

로 표현되며 여기에서$\mathrm{FT}_{\mathrm{real}}\{\bullet\}$은 푸리에 변환 후 실수 값을 취하는 연산이고 아래 첨자 z는 제로 패딩 연산자이다. 이를 위상 변조시킨 최종 암호화키 $\tilde{E}(u,v)$ 는

$$\tilde{E}(u,v)=\exp\left[\frac{j\pi E(u,v)}{nC}\right] \quad (7)$$

로 표현된다. 여기에서 n은 실수 값의 정규화를 위한 값이고

C는 복호화 과정에서 Zernike 위상 세기법에 의해 필요한 요소이다. 이때 만약 허가되지 않은 개인이나 그룹이 암호화키를 푸리에 변환이나 위상 측정 방법 등으로 분석하더라도 가상영상 조차 얻기가 어려우며 만약 가상영상이 분석되더라도 암호화키에서는 원 영상의 정보를 포함하고 있지 않기 때문에 정확한 복호화키 없이는 결코 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다는 장점을 가진다. 또한 본 논문에서 시스템 내부에 존재하는 복호화키 영상을 분석함으로써 있을 수 있는 복제 가능성을 배제하기 위하여 동일한 위상 랩핑 방법을 복호화 연산키 $\exp\{j\pi d(x, y)\}$에 적용한다. 먼저 복호화키 영상을 재생하기 위하여 식 (1)에서 표현된 위상성분들의 단순한 가감법에 의해

$$\exp[j\pi d_A(x,y)] = \exp\{j\pi[v(x,y)+2r(x,y)-f(x,y)]\} \quad (8)$$

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 랩핑을 적용한다. 즉 복호화 산술 연산키 $\exp\{j\pi d_A(x, y)\}$의 위상 값은 $[-\pi, 3\pi]$사이 이므로 이를 $[0, 2\pi]$사이 값으로 위상 랩핑(phase wrapping) 시킨다. 따라서 복호화 연산키 $\exp\{j\pi d(x, y)\}$는

$$\tilde{d}(x,y) = \exp[j\pi d(x,y)] \quad (9)$$
$$= \begin{cases} \exp\{j\pi[d_A(x,y)+2]\}, & -1 \le d_A(x,y) < 0 \\ \exp\{j\pi[d_A(x,y)]\}, & 0 \le d_A(x,y) < 2 \\ \exp\{j\pi[d_A(x,y)-2]\}, & 2 \le d_A(x,y) < 3 \end{cases}$$

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

$$D(u,v) = \mathrm{FT}_{\mathrm{real}}\{\tilde{d}_z(x,y)\} \quad (10)$$
$$\tilde{D}(u,v) = \exp\left[\frac{j\pi D(u,v)}{nC}\right]$$

제안한 복호화를 위한 실험 구성도는 그림 1과 같으며 복호화 과정에서 암호화키 $\tilde{E}(u,v)$와 복호화키 $\tilde{D}(u,v)$ 는 2-f 광시스템 구성도의 푸리에 영역에 각각 위치하며 이때 암호화키와 복호화 키 사이의 공간이 존재하면 프레넬 회절이 발생함으로 이를 줄이기 위해서 동일한 푸리에 영역에 붙여서 놓아야 하며 여기에서 푸리에 렌즈 L_2를 통과하기 전의 영상은

$$\tilde{E}(u,v)\tilde{D}(u,v) = \exp\left[\frac{j\pi E(u,v)}{nC}\right]\exp\left[\frac{j\pi D(u,v)}{nC}\right] \quad (11)$$
$$= \exp\left\{\frac{j\pi}{nC}[E(u,v)+D(u,v)]\right\}$$
$$\approx 1+\frac{j\pi}{nC}[E(u,v)+D(u,v)]$$

로 표현되며 여기에서 C 값이 충분히 크다면 Zernike 위상 세기법에 의해 근사화 된다. 따라서 푸리에 렌즈 L_2에 통과한 식 (11)의 영상은

$$\mathrm{FT}\left\{1+\frac{j\pi}{nC}[E(u,v)+D(u,v)]\right\} \quad (12)$$
$$= \delta(x,y)+\frac{j\pi}{nC}\mathrm{FT}[E(u,v)+D(u,v)]$$

로 표현된다. 식 (12)에서 우변항의 첫 번째 성분인 영차 성분(zero-order component)은 공간 필터에 의해 제거되고 그에 따른 CCD에 나타나는 출력세기함수는

$$O_{CCD}(x,y) = \left|\frac{j\pi}{nC}\mathrm{FT}[E(u,v)+D(u,v)]\right|^2 \quad (13)$$
$$= \left(\frac{\pi}{nC}\right)^2\left|\tilde{e}_z'(x,y)+\tilde{d}_z'(x,y)\right|^2$$
$$= \left(\frac{\pi}{nC}\right)^2\{|\tilde{e}_z'(x,y)|^2+|\tilde{d}_z'(x,y)|^2$$
$$+\tilde{e}_z'(x,y)\,\tilde{d}_z'^*(x,y)+\tilde{e}_z'^*(x,y)\tilde{d}_z'(x,y)\}$$
$$= \left(\frac{\pi}{nC}\right)^2\{1+1+\exp\{j\pi[e_z'(x,y)-d_z'(x,y)]\}$$
$$+\exp\{-j\pi[e_z'(x,y)-d_z'(x,y)]\}\}$$
$$= \left(\frac{\pi}{nC}\right)^2\{1+1+\exp[j\pi f_z'(x,y)]+\exp[-j\pi f_z'(x,y)]\}$$
$$= \left(\frac{\pi}{nC}\right)^2\{2+2\cos[\pi f_z'(x,y)]\}$$

와 같다. 여기서 { * }는 복소 공액을 나타낸다. 식 (13)에서

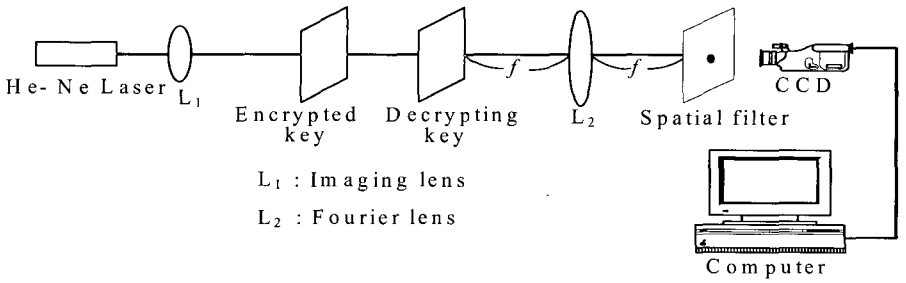

그림 1. 영상 복원을 위한 광 구성도.

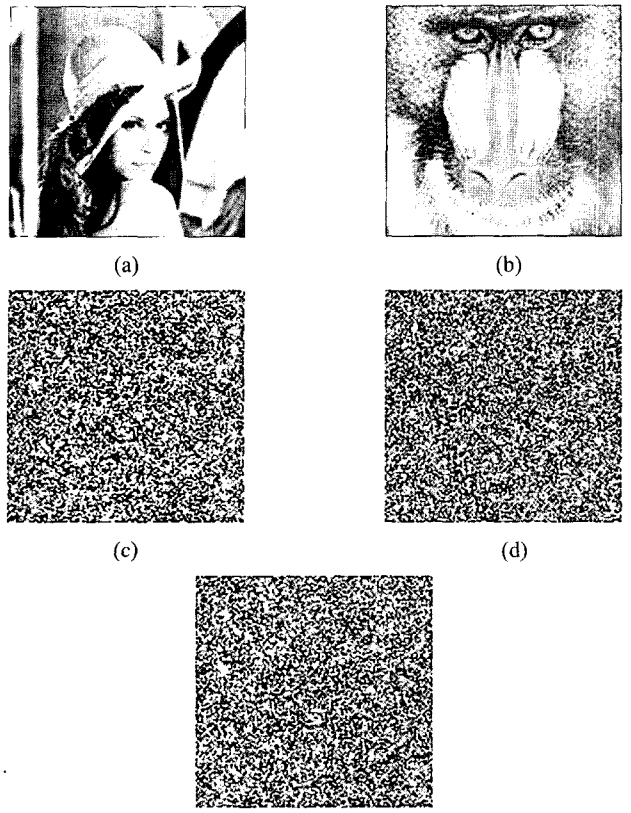

그림 2. 컴퓨터 모의실험에 사용된 영상. (a) 원 영상 f(x, y), (b) 가상 영상 v(x, y), (c) 무작위 영상 r(x, y), (d) 암호화에 사용하는 영상 e(x, y), (e) 복호화에 사용하는 영상 d(x, y).

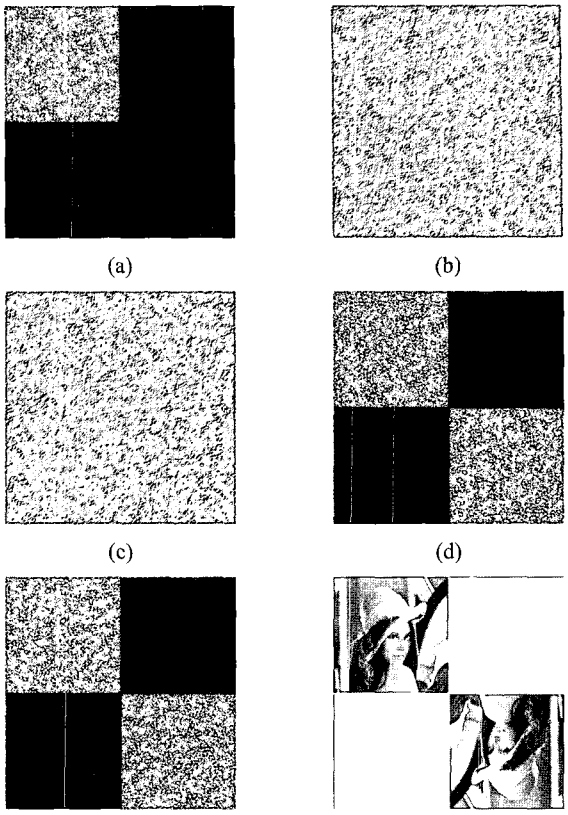

그림 3. 컴퓨터 모의실험 결과. (a) 제로 패딩 영상 $\widetilde{e_z}(x,y)$, (b) 암호화키 영상 $\widetilde{E}(u,v)$, (c) 복호화키 영상 $\widetilde{D}(u,v)$, (d) $E(u,v)$의 푸리에 변환 영상 $\widetilde{e_z}'(x,y)$ (e) $D(u,v)$의 푸리에 변환 영상 $\widetilde{d_z}'(x,y)$ (f) 반전된 복원 영상.

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 위상성분 $e_z'(x,y)$는 식 (3)에서 표현한 $v(x,y)$와 $2r(x,y)$의 성분을, 위상 성분 $d_z'(x,y)$는 식 (9)에서 표현한 $d(x,y)$의 성분을 각각 영차성분을 중심으로 쌍으로 존재하게 된다. 따라서 식 (13)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 (13)에서 원 영상의 반전된 영상이 복원되고 여현 함수의 비선형성에 의해 영상의 왜곡이 발생함을 알 수 있으나 이는 컴퓨터의 후처리를 통하여 간단히 복원 가능하다.

III. 컴퓨터 모의실험 및 고찰

그림 2는 컴퓨터 모의실험을 위하여 사용된 영상들로 그 화소수는 128×128이다. 그림 2(a)는 복원할 원 영상 $f(x, y)$로 그레이 값을 가지는 'Lena'를 사용하였고 그림 2(b)와 (c)는 각각 암호화될 가상 영상 $v(x, y)$로 'baboon' 영상과 컴퓨터로 발생시킨 무작위 영상 $r(x, y)$이다. 이들을 각각[0, 1]사이의 값으로 정규화 시키고 랩핑 방법에 의해 범위가[0, 2]사이 값으로 변환한 암호화에 사용될 $e(x, y)$를 그림 2(d)에 나타내었으며 이는 가상 영상과는 전혀 관계없는 무작위 패턴으로 나타남을 확인할 수 있다. 또한 만약 허가되지 않은 사용자가 암호화키를 분석하더라도 가상 영상을 원 영상으로 오인하게 되므로 복제 가능성을 배제할 수 있다. 그림 2(e)는 위상 랩핑 방법에 의해 복호화에 사용될 $d(x, y)$를 나타내었으며 이는 원 영상의 정보가 비선형성에 의해 무작위 패턴으로 나타남을 알 수 있다.

그림 3(a)는 암호화에 사용될 $e(x, y)$를 위상 변조하여 257×257로 제로 패딩한 영상이며 여기서 위상 변조된 영상은 눈으로 볼 수 없는 복소함수이므로 편의를 위해서 위상을 세기 패턴으로 나타내었다. 그림 3(b)와 3(c)는 각각 그림 3(a)를 푸리에 변환한 후 실수 값을 취하여 위상 변조하여 제안한 방법에서 사용될 암호화키$\widetilde{E}(u,v)$ 와 제안한 위상 랩핑 방법에 의해 만들어진 올바른 복호화키 $\widetilde{D}(u,v)$ 를 나타내었다. 그림 3(d)와 3(e)는 식 (13)에서 표현한 $E(u,v)$와 $D(u,v)$를 각각 푸리에 변환한 영상 $\widetilde{e_z}'(x,y)$와 $\widetilde{d_z}'(x,y)$를 세기 패턴으로

나타내었으며 여기에서 $\tilde{e}(x,y)$ 와$\tilde{d}(x,y)$가 각각 영차성분을 중심으로 쌍으로 존재함을 알 수 있다. 그림 3(f)는 암호화키와 올바른 복호화 키를 그림 1의 광 구성도에 의해 복원한 영상의 반전 영상을 표현한 것이다. 여기에서 그레이 영상을 재생함으로써 식 (13)의 여현 함수의 비선형성에 의해 원 영상의 왜곡이 발생하는데 그림 3(f)에서 이를 보상하지 않았지만 후처리를 통하여 보상할 수 있다.

그림 4(a)와 4(b)는 각각 허가되지 않은 임의의 사용자가 컴퓨터를 통해 만든 거짓 복호화키와 이에 대응되는 복원 영상으로써 거짓 키로는 영상이 재생되지 않음을 확인할 수 있다.

그림 5는 제안한 방법에서 복원영상의 해상도는 Zernike 근사화를 위한 C 값에 영향을 미치게 되므로 C값에 따른 원 영상과 복원 영상의 해상도를 표현하는 첨두치 신호 대 잡음비(Peak signal-to noise ratio, PSNR)를 나타내었다. 여기서 사용된 PSNR의 표준은

$$\mathrm{PSNR}=20\log\frac{2^{n_{bit}}}{\left\{\frac{1}{N\times M}\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left[\|f(x,y)|-|f'(x,y)\|^2\right]\right\}^{1/2}} \tag{14}$$

이며 여기서 $f(x, y)$와 $f'(x, y)$는 각각 원 영상과 복원 영상이며 $N\times M$은 각 영상의 픽셀 수이며 n_{bit}는 픽셀을 표현하는 bit 수이다. 그림 5에서 PSNR은 C값이 [0, 20]정도에서 급격히 증가하다가 20이상에서 서서히 증가함을 알 수 있으며 C값이 클수록 복원 영상의 해상도는 증가하지만 실질적인 공간 광 변조기가 표현할 수 있는 범위가 제한되어 있음으로 C값을 10으로 선택하여 40.3dB에서 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 6(a), 6(c)와 6(e)는 각각 암호화키 영상인 그림 3(b)를 각각 25%, 50%와 75%를 u축으로 블로킹하였을 경우와 이를 그림 1의 실험 구성도에 의해 복원되었을 경우 그에 대응되는 복원 영상을 각각 그림 6(b), 6(d)와 6(f)에 나타내었다. 여기에서 암호화키 영상의 블로킹되는 픽셀의 위치 정보가 무작위로 변하더라도 복원 영상의 해상도

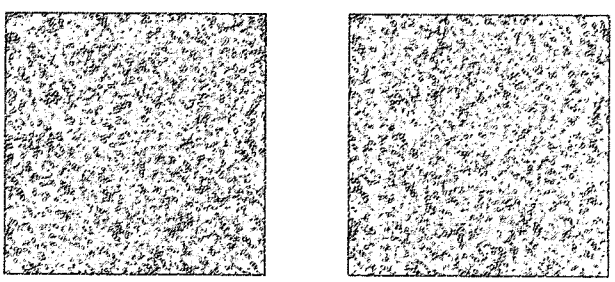

그림 4. 컴퓨터 모의실험 결과. (a) 거짓 복호화키, (b) 거짓 복호화키로 재생된 영상.

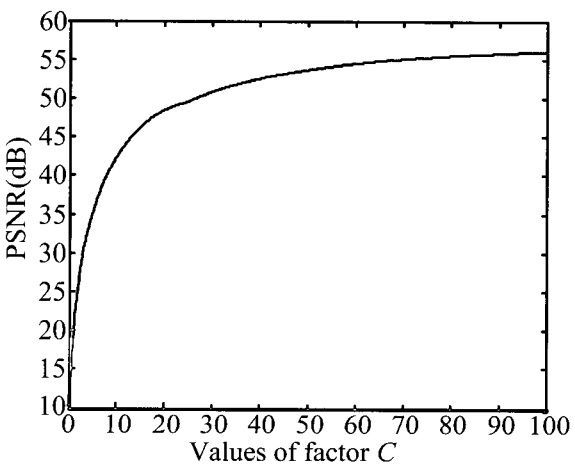

그림 5. C값의 변화에 따른 복원영상의 PSNR.

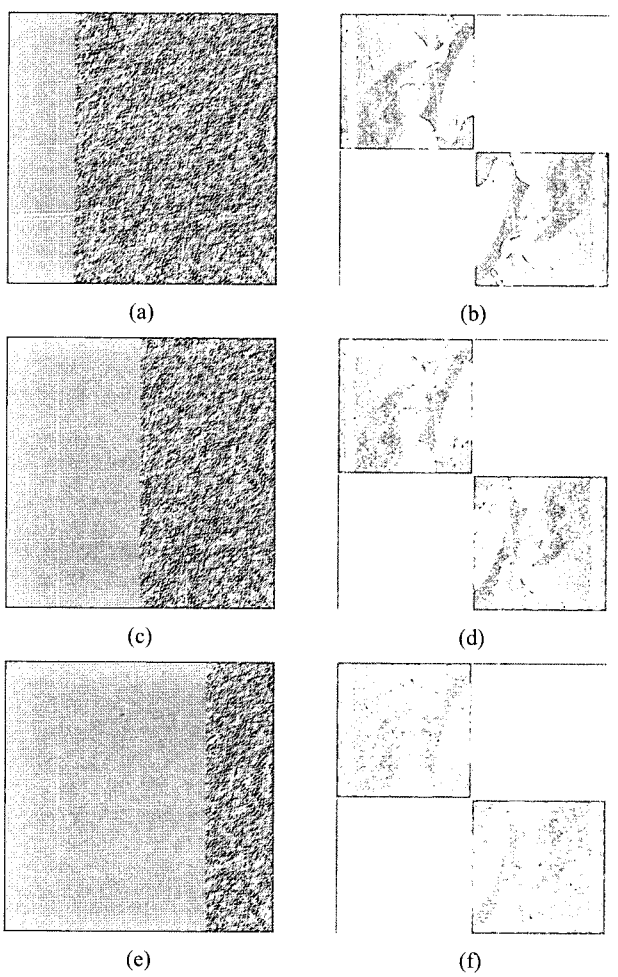

그림 6. 암호화 영상의 블로킹에 따른 컴퓨터 모의실험 결과: u축을 따라 암호화 된 영상이 각각 (a) 25%, (c) 50%, (e) 75% 블로킹되었을 때 그에 대응하는 복원된 영상 (b), (d), (f).

에는 영향을 미치지 않고 복호화 키가 블로킹되더라도 동일한 해상도를 가짐을 모의실험을 통해서 확인하였다. 그림 6(f)에서 암호화된 영상의 75%가 블로킹되더라도 원 영상의 정보를 얻을 수 있음을 알 수 있다. 제안한 방법은 현재의 공간 광 변조기의 기술이 크기 변조 혹은 위상 변조에 대한 성분만을 기록할 수 있으므로 실질적인 광 실험을 위해서 암호화키와 복호화키를 위상 부호화하여 표현하였고 또한 최근의 위상 변조 공간 광 변조기가 표현할 수 있는 위상값의 범위가 2π 이상이다. 하지만 실질적인 실험상에서는 공간대역폭제한과 공간 광 변조기의 양자화 손실로 인한 영상의 해상도가 떨어지는 단점을 가진다.

IV. 결 론

본 논문에서는 선형적 영상의 합을 비선형적 영상으로 변환시키는 위상 랩핑 방법을 이용하여 암호화키와 복호화키의 암호화 수준을 향상시키고 이를 주파수 영역에서 위상 부호화하여 외부 잡음에 강한 암호화 방법을 제안하였다. 제안한 암호화 방법은 푸리에 변환된 영상을 실수값을 취하여 위상 부호화하여 표현함으로써 실질적인 광 암호화 시스템에서 복소값을 표현하기 어려운 단점을 해결할 수 있다. 또한 복호화 과정에서 암호화키와 복호화키를 일대일 정합시키고 푸리에 역 변환하는 한 과정만 이용하므로 픽셀 대 픽셀 대응을 용이하게 하여 기존의 4-f 광상관기의 광축정렬 문제와 간섭계 등에서 나타나는 외란 등의 영향에 강한 특성을 가짐으로써 복원영상의 해상도를 향상시킬 수 있다. 컴퓨터 모의실험을 통하여 제안한 암호화 방법의 타당성을 검증하였으며 암호화키 영상 혹은 복호화키 영상이 블로킹되더라도 원 영상의 정보를 가지고 있음을 확인하였다. 앞으로 그레이 레벨의 복소값 영상을 표현할 수 있는 공간 광 변조기나 영상의 왜곡을 최소화 할 수 있는 컴퓨터 형성 홀로그램 등과 같은 광학 소자의 성능 개선이 위상 정보를 표현하는 식각 기술과 더불어 향상된다면 제안한 방법의 실질적인 광 실험 구현이 가능할 것이라 생각된다.

참고문헌

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

[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] 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.

[4] 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.

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

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

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

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

[9] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," *Appl. Opt.*, vol. 37, no. 35, pp. 8181-8186, 1998.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

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

[17] 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.

[18] 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.

Image Encryption and Decryption System using Frequency Phase Encoding and Phase Wrapping Method

Dong-Hoan Seo†

Division of Electrical & Electronics Engineering, Korea Maritime Univerity, Busan, 606-791, Korea

† *E-mail: dhseo@bada.hhu.ac.kr*

Chang-Mok Shin and Kyu-Bo Cho

School of Electrical Engineering & Computer Science, Kyungpook National University, Daegu 702-701, Korea

(Received June 12, 2006, Revised manuscript December 1, 2006)

In this paper, we propose an improved image encryption and fault-tolerance decryption method using phase wrappingand phase encoding in the frequency domain. To generate an encrypted image, an encrypting key which denotes the product of a phase-encoded virtual image, not an original image, and a random phase image is zero-padded and Fourier transformed and its real-valued data is phase-encoded. The decryption process is simply performed by performing the inverse Fourier transform for multiplication of the encrypted key with the decrypting key, made of the proposed phase wrapping method, in the output plane with a spatial filter. This process has the advantages of solving optical alignment and pixel-to-pixel mapping problems. The proposed method using the virtual 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.

OCIS code : 070.0070, 070.2590, 100.1160, 120.5060.