결합 변환 상관 평면의 이동 변위와 무작위 위상 영상을 이용한 광 암호화 시스템

신창목 · 이우혁 · 조규보 · 김수중

경북대학교 전자전기컴퓨터학부

㉾ 701-702 대구광역시 북구 산격동 1370

서동환† · 이성근

한국해양대학교 전기전자공학부

㉾ 606-791 부산광역시 영도구 동삼동 1번지

(2006년 4월 3일 받음, 2006년 6월 5일 수정본 받음)

본 논문에서는 결합 변환 상관 평면에 이동 변위에 따른 위상 성분의 영향을 또 다른 암호화 매개변수로 이용하여 무작위 위상 영상과 매개 변수 값을 암호화 요소로 사용하는 광 암호화 방법을 제안하였다. 암호화 과정 시 사용자만이 알고 있는 이동 변위 수치를 원 영상에 더하여 위상 변조한 후, 위상 변조한 무작위 위상과 공간 영역에서 곱한다. 곱해진 영상을 푸리에 변환을 하여 최종 암호화 영상을 생성하며, 이 때 키 영상은 무작위 위상 영상을 푸리에 변환하여 얻는다. 생성된 암호화 영상은 원 영상을 재생 시 키 영상과 이동 변위 수치 정보가 동시에 필요로 하며, 키 영상은 복소함수로 세기 검출기로 쉽게 복제가 힘들뿐만 아니라 설사 키 영상이 복제하거나 도난 또는 분실된 경우에도 불법 사용자는 이동 변위 정보를 획득해야만 원 영상 정보를 재생할 수 있으므로, 좀 더 높은 암호화 수준으로 원 영상 정보를 보호할 수 있다. 복호화 과정은 결합 변환 상관 평면에 암호화 영상과 키 영상을 암호화 시 사용한 이동 변위 값에 따라 위치시켜 간단히 구현할 수 있으며, 간섭계 구조나 4-f 상관기 구조를 이용하지 않으므로 광축 정렬이나 외부 환경 변화에 영향을 받지 않고 원 영상을 재생할 수 있다.

주제어 : Joint transform plane, Random phase image, Phase shift variable.

I. 서 론

정보보호 기법들 중에서 최근에 광을 이용한 암호화 시스템[1-12]들이 활발히 연구되고 있다. 광 암호화 시스템은 기본적으로 광의 고속성과 병렬성을 이용할 수 있어서, 대용량의 정보를 고속으로 처리하는데 적합하며, 영상 신호를 위상 정보[2]로 기록이 가능할 뿐만 아니라 무작위 위상 마스크를 키 영상(key image)으로도 사용하기 때문에 시각이나 세기 검출기로는 위조가 어려운 장점을 가지고 있다. 광 암호화 시스템은 주로 4-*f* 광 상관기[3,4,11]나 마흐-젠더 간섭계[5,6], Weaver 등[7]이 제안한 결합 변환 상관기(joint transform correlator; JTC)를 이용하는데 이 중에 결합 변환 상관기는 다른 시스템과는 달리 광축 정렬이 필요 없고 복소 공액 마스크를 제작할 필요가 없으며 외부 교란에도 거의 영향을 받지 않는 장점이 있다. 또한 JTC는 현재 널리 사용되는 디지털 장비와 직접적인 결합을 통해서 실시간 처리에도 적합하다. 그러나 JTC는 구조적인 특성 때문에 출력 평면에 자기상관(auto correlation) 성분이 큰 세기로 나타나므로, 보안 시스템 이용에 어려움을 준다. 지금까지 자기상관 성분을 제거하거나 영향을 줄이는 연구가 여러 면에서 이루어지고 있으며 이를 바탕으로 Javidi[8,9], Park[10] 등의 많은 연구자들이 활발히 JTC 암호화 시스템[8-11]을 제안하였다. 그 중 Park 등은 JTC 입력 평면에 주파수 영역의 입력 영상과 기준 영상을 나란히 두고 한번의 푸리에 역변환 과정을 통하여 자기상관 성분 없이 입력 영상을 복원하는 방법을 제안하였다. 그러나 이 방법은 입력 영상과 기준 영상을 정확히 대칭적으로 위치시키지 않을 경우 발생하는 위상 성분 영향이 출력 평면에 여현 함수로 나타나므로 원 영상 복원이 어렵게 된다.

본 논문에서는 이러한 결합 변화 상관기의 출력 평면에 발생하는 위상 성분의 영향을 또 다른 암호화 매개변수로 이용하여 키 영상과 위상 변위 값을 동시에 활용하는 보다 향상된 수준의 광 암호화 방법을 제안하였다. 암호화 과정은 푸리에 변환의 위상 이동 특성을 기본적으로 사용하므로, 우선 사용자만이 알고 있는 이동 변위 수치를 원 영상에 더한다. 그 후 이동 변위 수치가 더해진 영상을 위상 변조하고, 무작위 위상 영상과 공간 영역에서 곱하며, 이 영상을 푸리에 변환하여 최종 암호화 영상을 생성한다. 이 때 암호화에 사용된 무작위 위상 영상을 푸리에 변환하여 진위 여부를 판별하는 복호화 키 영상으로 이용한다. 암호화된 영상은 키 영상이 없으면 원 영상 정보를 복원 할 수 없을 뿐만 아니라, 정확한 이동 변위 정보 없이도 원 영상 정보가 불가능하므로 키 영상의 복제나 도난, 분실이 발생할 경우 효과적으로 원 영상 정보를 보호할 수 있다. 제안한 복호화 시스템은 기본적으로 JTC 구조이므로, 광축 정렬문제나 화소 대 화소 정합

† E-mail: dhseo@bada.hhu.ac.kr

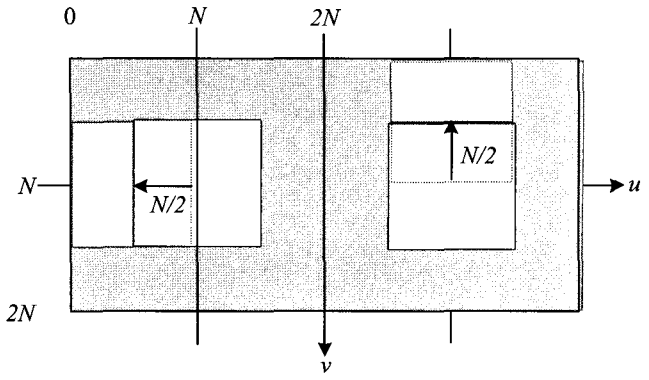


그림 1. 이동 변위 수치의 범위.

문제에 영향을 거의 받지 않으며, 복호화 시 JTC 입력 평면에 암호화 영상과 키 영상을 암호화에 사용한 이동 변위에 해당하는 값만큼 위치시키고 이를 역푸리에 변환하므로 간단히 원 영상 정보를 복호화 할 수 있다.

제안한 암호화 방법의 타당성을 컴퓨터 모의실험 영상으로 확인하였고, 실제 구현 시 발생할 수 있는 여러 문제들을 고려해 정보손실 및 잡음에 대한 영향을 상관계수 및 PSNR (peak signal to noise ratio) 수치값들로 분석하였다.

II. 제안한 암호화 과정

먼저 암호화 할 원 영상 $f(x,y)$에 이동 변위 수치를 더한 영상이 $f_s(x,y)$이면,

$$f_s(x,y)=f(x,y)/f_{\max}+\frac{4a}{2N}x+\frac{4b}{2N}y=f(x,y)/f_{\max}+\frac{2a}{N}x+\frac{2b}{N}y \tag{1}$$

과 같이 표현되며, $f_{\max}$ 는 원 영상 $f(x, y)$의 최대 화소값을 의미한다. 여기서 a와 b는 그림 1을 통해 복호화시 공간 광 변조기의 결합 입력 평면 화소 범위 내에 두기 위해[0, $N/2$] 의 자연수 값을 가지도록 하였으며, N은 입력 영상의 전체 화소 크기이다.

이동 변위 함수가 더해진 영상 $f_s(x,y)$와 무작위 영상 $r(x,y)$를 각각 위상 변조한 영상 $f_p(x,y)$와 $r_p(x,y)$는

$$f_p(x,y)=\exp\{j\pi f_s(x,y)\} \tag{2}$$
$$r_p(x,y)=\exp\{j2\pi r(x,y)\}$$

와 같고, 이 때 $r(x,y)$는 [0, 1] 사이의 값을 가지며, 위상 변조된 영상들의 세기는

$$|f_p(x,y)|^2=|r_p(x,y)|^2=1 \tag{3}$$

과 같이 '1' 이므로 세기 검출기나 인간의 시각으로는 복사나 구별이 불가능하다.

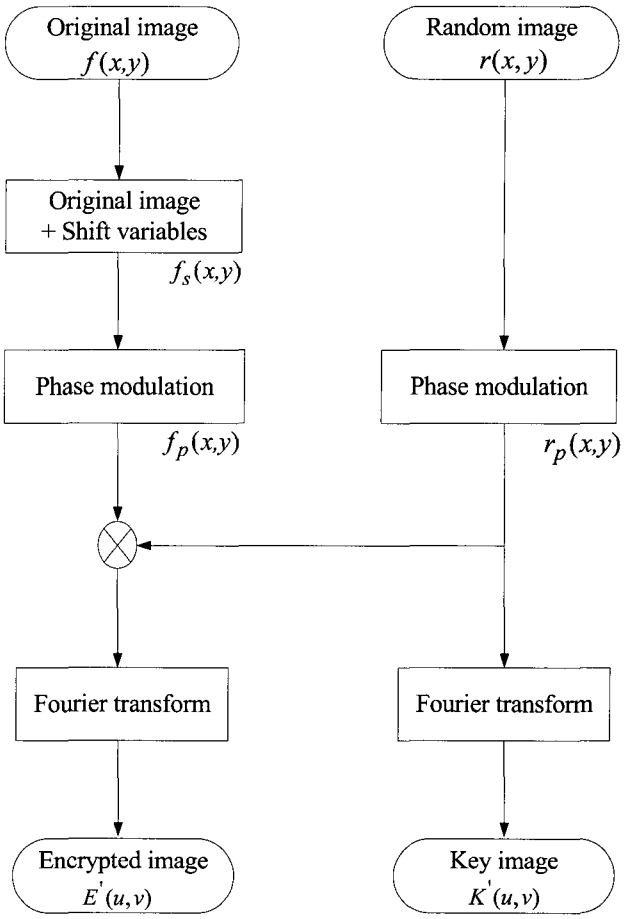


그림 2. 제안한 암호화 방법의 블록 다이어그램.

암호화 과정은 앞서 위상 변조된 $f_p(x,y)$와 $r_p(x,y)$를 곱한 암호화 데이터 $E(x,y)$, 복호화에 사용될 키 데이터 $K(x,y)$는

$$E(x,y)=\exp\{j\pi f_s(x,y)\}\exp\{j2\pi r(x,y)\} \tag{4}$$
$$K(x,y)=\exp\{j2\pi r(x,y)\}$$

과 같다. 이 두 영상들을 푸리에 변환 시키면 암호화 된 영상 $E'(u,v)$ 와 사용되는 키 영상 $K'(u,v)$ 를 얻을 수 있다.

$$E'(u,v)=\mathrm{FT}[\exp\{j\pi f_s(x,y)\}\exp\{j2\pi r(x,y)\}] \tag{5}$$
$$K'(u,v)=\mathrm{FT}[\exp\{j2\pi r(x,y)\}]$$

여기서 연산자 FT{·}는 푸리에 변환을 나타내며 제안한 암호화 방법의 과정을 그림 2와 같이 블록 다이어그램으로 나타내었다.

E'과 K'는 모두 암호화된 정보이므로 둘 중 하나를 사용자의 키 영상 정보로 사용할 수 있다. 만약 E'을 시스템의 내부 키로 사용한다면 K'을 복소 마스크 형태로 제작한 후 사용자

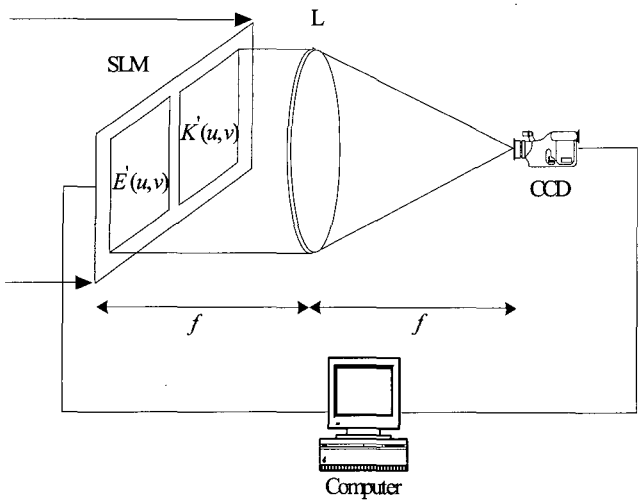


그림 3. JTC를 이용한 복호화 시스템.

에게 키 카드로 제공하여 직접 시스템에 입력하는 방법을 통해 복호화에 이용하게 할 수 있고, 네트워크 망을 통할 경우엔 키 영상 정보를 사용자에게 전송한 후 필요에 따라 사용자의 키 정보를 전송받아 복호화에 사용할 수도 있다.

III. 결합 변환 상관기에 의한 복호화 과정

결합 입력 평면 $O(u,v)$가 암호 영상과 키 영상이 각 축의 중심에서부터 $(\pm\frac{u_0}{2N},\pm\frac{v_0}{2N})$ 만큼 떨어져 표현된다고 하면,

$$O(u,v)=E'(u-u_0,v-v_0)+K'(u+u_0,v+v_0) \tag{6}$$

이며, 출력평면에선 그림 3의 렌즈 L에 의해서 푸리에 변환되어

$$o(x,y)=E(x,y)\exp(-j2\pi\frac{u_0}{2N}x)\exp(-j2\pi\frac{v_0}{2N}y) \tag{7}$$
$$+K(x,y)\exp(j2\pi\frac{u_0}{2N}x)\exp(j2\pi\frac{v_0}{2N}y)$$

로 주어진다. 그러므로 출력 평면에 놓인 CCD 카메라에 의해 검출되는 복원 영상은

$$|o(x,y)|^2=|E(x,y)|^2+|K(x,y)|^2 \tag{8}$$
$$+E(x,y)K^*(x,y)\exp(-j4\pi\frac{u_0}{2N}x)\exp(-j4\pi\frac{v_0}{2N}y)$$
$$+E^*(x,y)K(x,y)\exp(j4\pi\frac{u_0}{2N}x)\exp(j4\pi\frac{v_0}{2N}y)$$

와 같고, 식 (4)에 의해서,

$$\begin{aligned}|o(x,y)|^2 &= 1+1 \\ &+\exp\{j\pi f_s(x,y)\}\exp\{-j4\pi u_0x\}\exp\{-j4\pi v_0y\} \\ &+\exp\{-j\pi f_s(x,y)\}\exp\{j4\pi u_0x\}\exp\{j4\pi v_0y\} \\ &= 2+2\cos[\pi f_s(x,y)-4\pi u_0x-4\pi v_0y]\end{aligned} \tag{9}$$

로 정리할 수 있다. 여기서 $f_s(x,y)$는 식 (1)과 같으므로,

$$\begin{aligned}|o(x,y)|^2 &= 2+2\cos[\pi f_s(x,y)-2\pi\frac{u_0}{N}x-2\pi\frac{v_0}{N}y] \\ &= 2+2\cos[\pi f(x,y)/f_{\max}+\frac{2\pi ax+2\pi by-2\pi u_0x-2\pi v_0y}{N}]\end{aligned} \tag{10}$$

이 된다. 사용자가 미리 정해 둔 위상 변위 수치 (a, b) 만큼 복호화시 결합 입력 평면에 두 영상을 위치시키면 즉, $a=u_0, b=v_0$가 되면 식 (10)은

$$|o(x,y)|^2=2+2\cos[\pi f(x,y)/f_{\max}] \tag{11}$$

과 같으며, 이는 실제 CCD를 통해 검출되어 양자화된 영상이므로 식 (11)에서 얻은 결과를 간단한 디지털 후처리 과정을 거쳐

$$f(x,y)=\frac{f_{\max}}{\pi}\cos^{-1}\left(\frac{|o(x,y)|_Q^2-2}{2}\right) \tag{12}$$

와 같이 원 영상을 복원해 낼 수 있다. 이 때 $|o(x,y)|^2_Q$는 CCD 동작특성에 따라 양자화된 영상을 의미한다. 만약, $a\neq u_0,\ b\neq v_0$이면 식 (11)과 같이 원 영상만 남지 않고 원하지 않는 이동 성분이 존재하게 되어 코사인 함수의 특성상 함수 내의 원 영상과 원하지 않는 이동 성분들이 랩핑(wrapping)되어 원 영상을 복원 할 수 없게 된다.

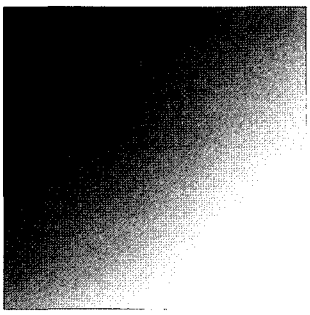
실제 SLM으로 그림 3과 같은 복호화 시스템 구현시 단일 SLM만으로는 복소값을 표현하는 것이 거의 힘들므로, 두 개의 SLM을 나란히 밀착시켜 화소 대 화소 정합 문제를 최소화한 후 하나는 크기값만, 또 하나는 위상값만을 표현하도록 시스템을 구성하여 식 (6)의 복소함수 E'과 K'을 구현할 수 있다.

IV. 모의 실험 및 분석

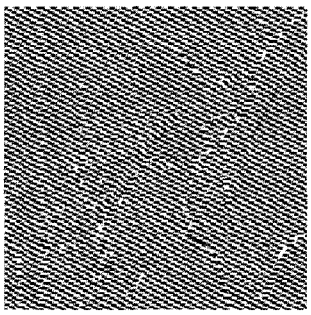
4.1 암호화 및 복호화 모의 실험

128×128 화소 크기의 Lena 영상을 그림 4(a)와 같이 원 영상으로 한 후, 여기에 식 (1)과 같이 x와 y의 성분을 모두 가지는 대각선의 이동 변위 함수를 더하면 그림 4(b)가 된다. 이동 변위가 더해진 영상을 위상 변조하면 그림 4(c)가 된다. 그림 5(a)는 그림 4(c)에 무작위 위상 영상인 그림 5(b), 즉

(a)

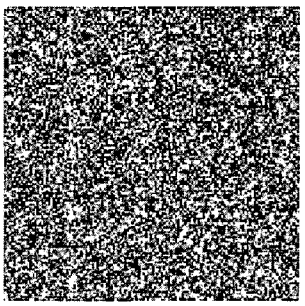


(b)

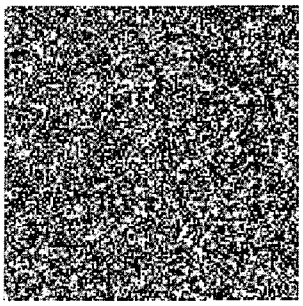


(c)

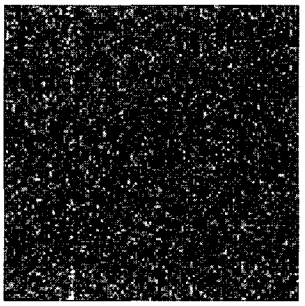
그림 4. 컴퓨터 실험 결과: (a) 원 영상 $f(x,y)$, (b) 이동 변위 수치가 더해진 원 영상 $f_s(x,y)$, (c) 그림 (b) 의 위상 변조 영상 $f_p(x,y)$.



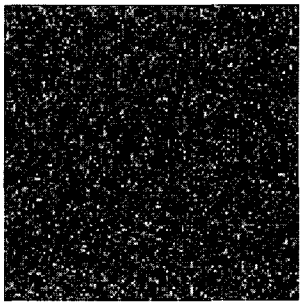
(a)



(b)



(b)



(c)

그림 5. 컴퓨터 실험 결과: (a) 암호화 데이터 영상 $E(x,y)$, (b) 키 데이터 영상 $K(x,y)$, (c) 푸리에 변환된 암호 영상 $E'(u,v)$, (d) 푸리에 변환된 키 영상 $K'(u,v)$.

키 데이터 $K(x,y)$를 곱한 암호화 데이터 $E(x,y)$이며, 암호화 데이터와 키 데이터를 각각 푸리에 변환할 경우 최종 암호화 영상 $E'(u,v)$와 키 영상 $K'(u,v)$가 그림 5(c), 5(d)로 각각 나타난다. 여기서 암호화 데이터와 키 데이터의 위상값들은 실제 눈에 보이지 않으므로 편의상 그레이 값 범위의 [0; 255]로 대응시켜 표현하였다.

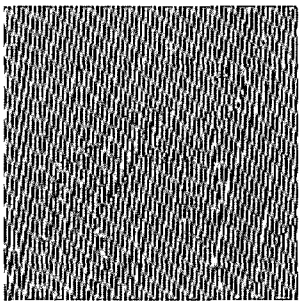
그림 5. 컴퓨터 실험 결과: (a) 암호화 데이터 영상 $E(x,y)$, (b) 키 데이터 영상 $K(x,y)$, (c) 푸리에 변환된 암호 영상 $E'(u,v)$, (d) 푸리에 변환된 키 영상 $K'(u,v)$.

CCD로 인한 양자화 레벨이 8 비트라고 가정하여 키 정보와 이동 변위 수치를 다르게 했을 경우 나타나는 복호화 결과들을 그림 6과 같이 나타내었다. 그림 6에서 나타나듯 올바른 이동 변위 수치와 키를 동시에 사용했을 경우에만 그림 6(a)와 같이 원 영상정보가 재생됨을 확인할 수 있다. 따라서 이동 변위 수치를 사용자만 아는 암호화 시스템의 인증값으로, 키 영상을 시스템의 키로 사용할 경우, 키 영상 분실이나 복제에 대해 강한 특성을 가진 암호화 시스템 구현이 가능하다.

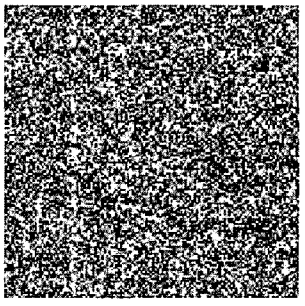
4.2 제안한 암호화 시스템의 이동 변위 수치에 대한 고찰

복호화 된 영상은 여현함수에서 디지털 후 처리를 통해 재생되므로, 여현함수의 주기 값에 영향을 받을 수 있다. 그러므로 암호화의 중요한 매개변수인 이동 변위 수치가 여현함수의 주기성에 의해 결합 상관 입력 평면 중 정수배가 되는 위치에서 원하지 않는 영상으로 재생되면 시스템의 신뢰도

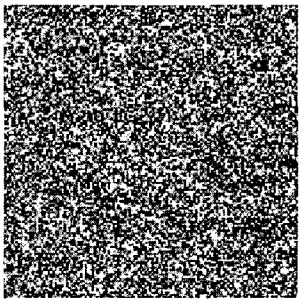
(a)



(b)



(a)



(b)

그림 6. 컴퓨터 실험 결과: (a) 올바른 이동 변위 수치에 의해 복원된 영상, (b) 거짓 이동 변위 수치와 키 영상에 의해 복원 된 영상, (c) 올바른 이동 변위 수치와 거짓 키 영상에 의해 복원 된 영상, (d) 거짓 이동 변위 수치와 거짓 키 영상에 의해 복원 된 영상.

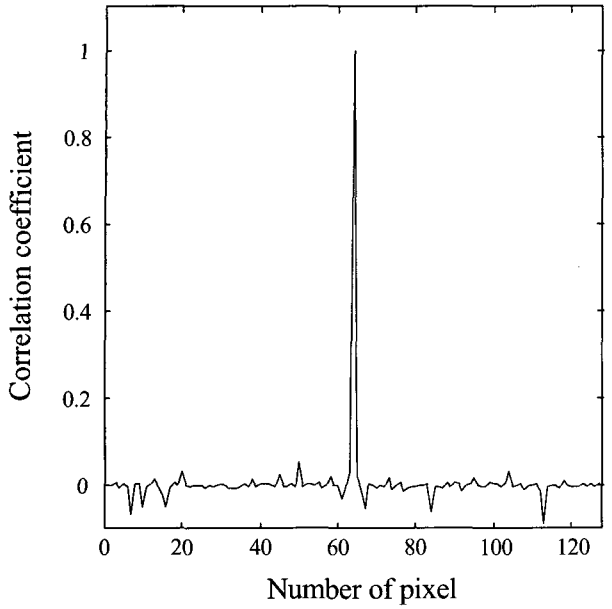


그림 7. 원 영상과 거짓 이동 변위 화소에 따른 재생 영상의 상관 계수.

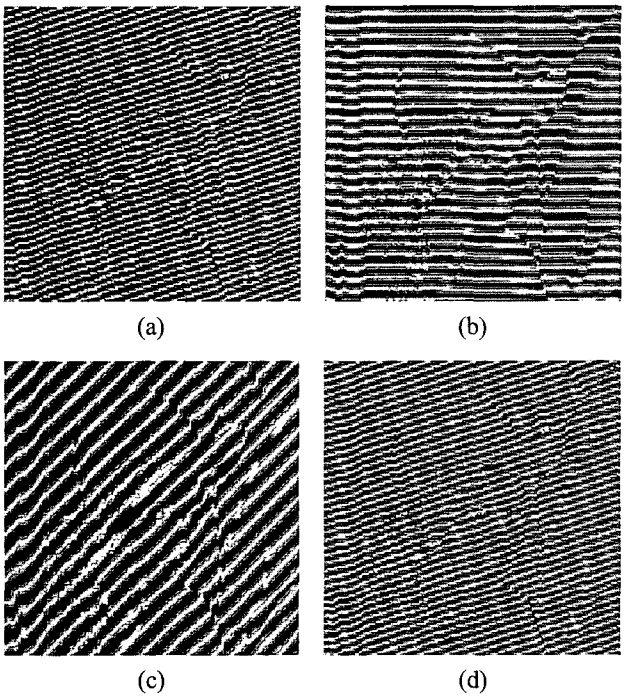


그림 8. 거짓 이동 변위 값에 따른 재생 영상들: (a) $(u_0=63, v_0=63)$일 경우, (b) $(u_0=63, v_0=64)$일 경우, (c) $(u_0=64, v_0=65)$일 경우, (d) $(u_0=65, v_0=65)$일 경우.

를 크게 떨어뜨리는 결과를 초래한다. 따라서 JTC 결합 입력 평면에 놓여지는 영상들의 위치를 달리하여 재생되는 영상과 원 영상의 상관 계수(correlation coefficient; CC) 분포를 식 (13)을 통해 구한 후 제안한 암호화 시스템의 타당성을 확인하였다.

$$CC=\frac{\mathrm{Cov}(E,E_s)}{S_E S_{E_s}} \tag{13}$$

여기서 $\mathrm{Cov}(E,E_s)$는 올바른 위치에서 재생된 영상 E와 다른 픽셀에서 재생된 영상 E_s간의 공분산(covariance)을 의미하며, S_E와 S_{E_s}는 두 영상들의 표준편차를 나타낸다.

이동 변위 수치를 각각 a=64, b=64 로 사용해 암호화 했을 경우, 거짓 변위에 의한 화소이동으로 나타나는 상관 계수 분포 곡선은 그림 7과 같다. 그림 7에서 나타나듯 이동 변위 수치가 달라졌을 경우 키 영상을 사용했을 경우라도 원 영상이 재생되지 않음을 보여주며, 이를 통해 이동 변위 수치가 수준이 높은 암호화 매개 변수로 사용 가능함을 알 수 있다.

사용된 이동 변위 수치와 인접한 값으로 암호 영상과 복원 키 영상을 대각선 방향으로 이동, u축으로 한 픽셀 이동, v축으로 한 픽셀 이동하여 위치시키는 방법으로 위치시켜 복원 되는 영상들은 그림 8에 나타내었다. 그림 8을 통해 암호 영상과 복원 키 영상을 정확한 이동 변위 수치 값으로 결합 상관 평면에 위치 시켜야만 원 영상이 복원 되는 것을 시각적으로 확인 할 수 있다.

4.3 암호화된 영상의 손실에 대한 고찰

제안한 암호화 방법이 실제 구현 시 발생하는 오류들에 대해 사용 가능함을 확인하기 위해 키 영상의 정보에 손실을 가한 후 원 영상을 재생하였다. 그림 9 (a), (b), (c)는 키 영상의 정보를 각각 25%, 50%, 75% 만큼 무작위 형태로 손실 시켰을 경우의 영상들을 나타내며, 그림 9 (d), (e), (f)는 이에 대한 재생 결과 영상들이다. 그림 10 (a), (b), (c)는 키 영상을 u 축에 따라 각각 25%, 50%, 75% 차단했을 때의 영상들이며, 이에 대해 재생된 결과 영상들은 그림 10 (d), (e), (f)와 같다. 사용자의 키 영상 정보가 정보 손실이나 잡음과 같은 요인에 의해 일부 손실이 생기더라도 그림 9와 10의 결과와 같이 정보 손실전의 영상에 비해 여전히 식별 가능하므로, 제안한 방법에 의한 암호화 시스템은 원치 않는 외부 환경에 강인한 특성을 가지며 영상의 복호화나 사용자의 인증을 할 수 있다는 장점이 있다.

4.4 위상 잡음에 대한 고찰

제안된 복호화 방법으로 영상을 복원할 때 재생된 영상은 위상마스크나 SLM 위의 먼지, 진동, 위상 마스크의 두께 변화, SLM에 인가되는 전압 변화등의 요소에 영향을 받는다. 따라서 이러한 잡음의 영향을 고려하여 제안한 암호화 시스템의 충실도를 시험해 볼 필요가 있다. 본 논문에서 키 영상은 위상 변조 되어 푸리에 변환된 영상이므로 위상 잡음만을 고려하여 시험하였다. 위상 잡음이 첨가될 경우 재생된 원 영상에 미치는 영향을 알아보기 위해 암호 영상에 평균값은

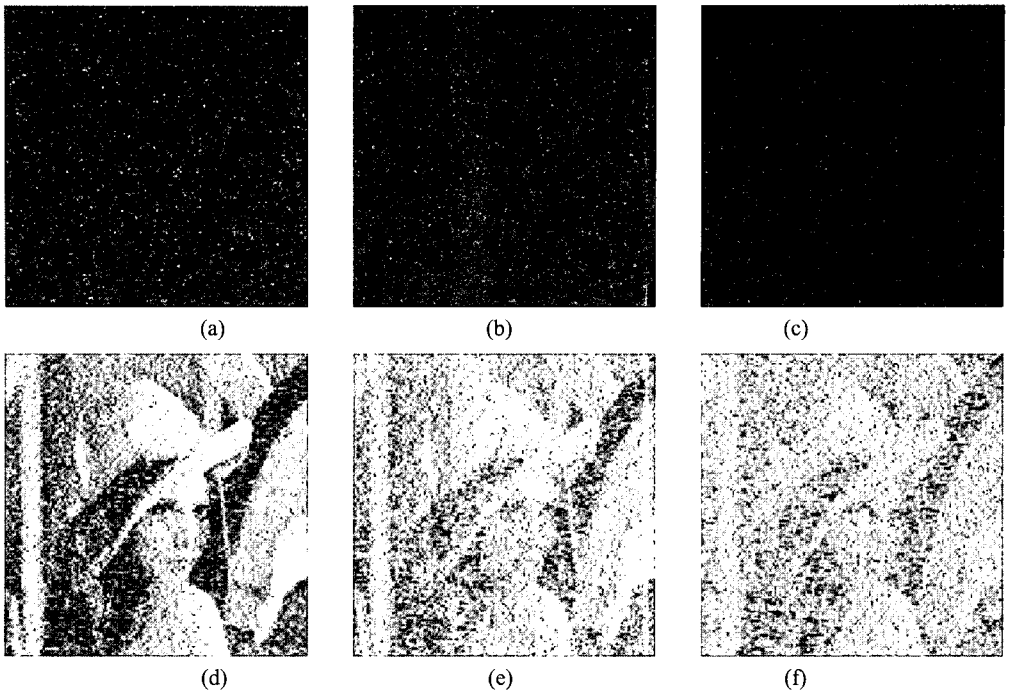


그림 9. 키 영상의 임의 차단에 따라 재생된 영상: (a) 25% 차단, (b) 50% 차단, (c) 75% 차단, (d) (a)에 의해 재생된 영상, (e) (b)에 의해 재생된 영상, (f) (c)에 의해 재생된 영상.

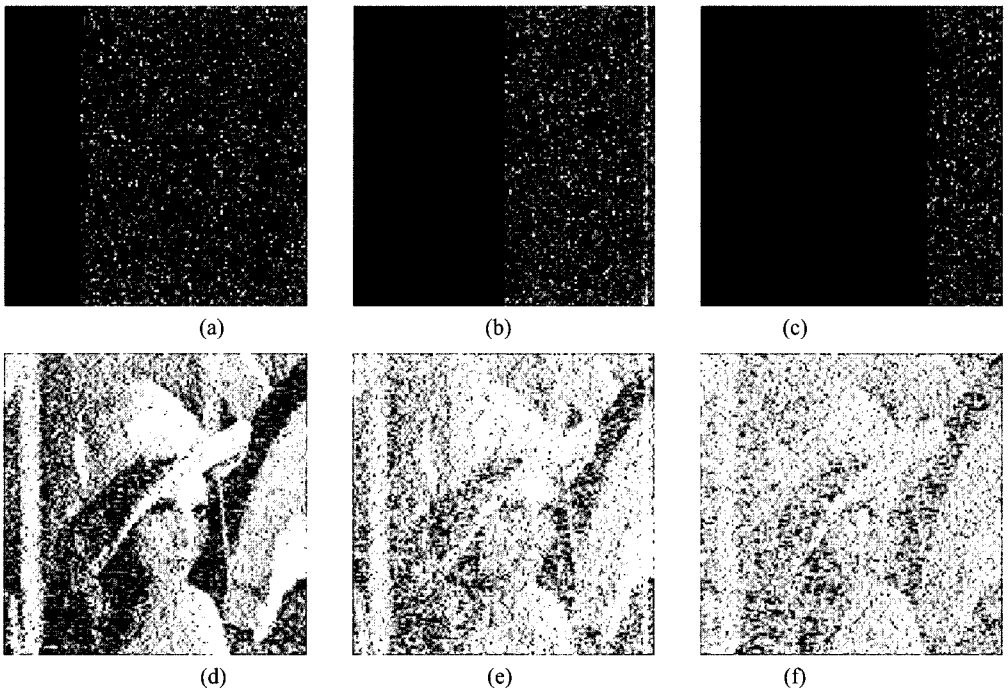


그림 10. 키 영상의 u 축 차단에 따라 재생된 영상; (a) 25% 차단, (b) 50% 차단, (c) 75% 차단, (d) (a)에 의해 재생된 영상, (e) (b)에 의해 재생된 영상 (f) (c)에 의해 재생된 영상.

0이며, 표준 편차 값은 변화를 준 백색 가우시안 잡음을 첨가하였다. 그림 11 (a), (b), (c), (d)는 위상 잡음의 표준 편차가 각각 0.02, 0.4, 1.0, 2.0일 때의 재생 영상을 나타내었다.

재생된 영상의 식별 가능 정도를 보다 수치적으로 표현하기 위해 PSNR(peak signal-to-noise ratio; PSNR)을 이용하여 잡음에 대한 PSNR 값들을 그림 12와 같이 나타내었다.

$$\mathrm{PSNR}=20\log_{10}\left\{\frac{255}{\sqrt{\mathrm{MSE}[o_r(x,y)]}}\right\} \tag{14}$$

여기서 MSE(mean squared error; MSE)는 잡음이 들어간 키 영상으로부터 재생된 영상$o_r(x,y)$와 잡음 없이 재생된 영상$o(x,y)$의 평균 자승 오차를 나타낸다.

그림 12의 PSNR 값들은 각각 표준 편차가 0.02일 경우 30dB, 0.4는 20dB, 1.0은 16dB, 마지막으로 2.0는 11dB이다. 그러므로 표준 편차가 0.02인 경우(PSNR=30), 높은 시각적 퀄러티(high visual quality) 뿐만 아니라, 표준 편차가 0.4인 경우(PSNR=20), 적절한 시각적 퀄러티(acceptable visual quality)도 보여주므로 제안한 암호화 시스템은 위상 잡음에 의한 왜곡에도 견실함을 알 수 있다.

V. 결 론

본 논문에서는 키 영상뿐만 아니라, 결합 변환 상관 평면에 이동 변위에 따른 위상 성분의 영향을 또 다른 암호화 매개변수로 이용하여 보다 향상된 수준의 광 암호화 방법을 제안하였다. 키 영상은 그레이 값을 가지는 복소 위상 영상으로 단순한 세기 검출기로 복사나 유포가 힘들 뿐 아니라, 키 영상의 도난이나 분실 시에도 암호화 매개변수를 사용자만이 아는 인증정보로 사용할 경우 원 영상의 정보를 효과적으로 보호할 수 있다. 복호화 시스템은 결합 변환 상관기에 기반을 두고 있으므로 원 영상 복호화 시 4-*f* 구조 등에서 발생하는 광축 정렬이나 화소 대 화소 대응 문제를 최소화 할 수 있다. 컴퓨터 실험을 통하여 제안한 암호화 방법의 타당성뿐만 아니라 차단 및 외부 잡음 등의 의한 키 정보 손실에 대해 제안한 시스템이 강한 특성을 가짐을 확인하였다. 또한 이동 변위 수치에 따라 복호화되는 영상과 원 영상간의 상관계수를 통해 이동 변위 수치의 암호화키로써의 타당성을 분석하였다. 앞으로 복소값의 영상을 표현할 수 있는 컴퓨터 형성 홀로그램 기법(CGH)과 공간 광변조기(SLM) 등과 같은 광학소자의 성능개선이 위상 마스크의 식각 기술과 더불어 향상된다면 제안한 방법의 실질적인 광 실험 구현이 가능할 것이라 생각된다.

감사의 글

이 논문은 2005년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (KRF-2005-003-D00253)

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

[3] 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.

[4] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," *Appl. Opt.*, vol. 39, no. 14, pp. 2313-2320, 2000.

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

[6] D. H. Seo and S. J. Kim, "Interferometric phase-only optical encryption system that uses a reference wave," *Opt. Lett.*, vol. 28, no. 5, pp. 304-306, 2003.

[7] C. S. Weaver and J. W. Goodman, "A technique for optically convolvoing two functions," *Appl. Opt*, vol. 5, no. 8, pp. 1248-1249, 1966.

[8] T. Nomura and B. Javidi, "Optical encryption system with a binary key code," *Appl. Opt.*, vol. 39, pp. 4783-4787, 2000.

[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] 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," *Opt. Rev.*, vol. 8, no. 6, pp. 413-412, 2001.

[11] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Opt. Lett.*, vol. 29, no. 14, pp. 1584-1586. 2005.

Optical Encryption using a Random Phase Image and Shift Position in Joint Transform Correlation Plane

Chang-Mok Shin, Woo-Hyuk Lee, Kyu-Bo Cho, and Soo-Joong Kim

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

Dong-Hoan Seo†, and Sung-Geun Lee

Division of Electrical and Electronics Engineering, Korea Maritime University, Pusan 606-791, Korea

† *E-mail: dhseo@bada.hhu.ac.kr*

(Received April 3, 2006, Revised manuscript May 5, 2006)

Most optical security systems use a 4-f correlator, Mach-Zehnder interferometer, or a joint transform correlator(JTC). Of them, the JTC does not require an accurate optical alignment and has a good potential for real-time processing. In this paper, we propose an image encryption system using a position shift property of the JTC in the Fourier domain and a random phase image. Our encryption system uses two keys: one key is a random phase mask and the other key is a position shift factor. By using two keys, the proposed method can increase the security level of the encryption system. An encrypted image is produced by the Fourier transform for the multiplication image, which resulted from adding position shift functions to an original image, with a random phase mask. The random phase mask and position shift value are used as keys in decryption, simultaneously. For the decryption, both the encrypted image and the key image should be correctly located on the JTC. If the incorrect position shift value or the incorrect key image is used in decryption, the original information can not be obtained. To demonstrate the efficiency of the proposed system, computer simulation is performed. By analyzing the simulation results in the case of blocking of the encrypted image and affecting of the phase noise, we confirmed that the proposed method has a good tolerance to data loss. These results show that our system is very useful for the optical certification system.

OCIS Codes : 100.1160, 120.3180, 120.5060.