《연구논문》 Hankook Kwanghak Hoeji, Volume 13, Number 1, February 2002

이중 임의 위상판을 이용한 광학상의 암호화 및 암호화 수준 분석

김병철 · 차성도 · 신승호†

강원대학교 물리학과

㉾ 200-701 강원도 춘천시 효자2동 192-1

(2001년 8월 29일 받음, 2001년 12월 26일 수정본 받음)

회전창을 첨가한 임의 위상판(random phase mask; RPM)을 이용하여 광학상 암호화 장치의 암호화수준을 향상시키는 방법을 제시하였다. 이중 임의 위상판으로 암호화된 광학상은 광굴절 $LiNbO_3$:Fe 결정에 기록되고 위상공액파를 이용하여 재생하였으며, 세기변조 함수를 이용하여 아날로그 입력상에 대한 암호화 수준을 분석하였다.

주제어 : optical information processing.

I. 서 론

정보통신 분야의 급격한 발달로 인해 방대한 양의 정보를 저장하기 위한 수단이 절실히 요구되고 있으며 광 정보처리 기술 중 홀로그램을 이용한 고밀도 광메모리분야의 연구가 활발하다. 또한 고밀도 정보저장 시스템을 고도의 보안 모듈로 암호화하는 연구도 활발하다.[1-5] 광학계를 이용하여 정보를 암호화하는 경우 정보들이 위상, 파장, 공간 주파수와 같은 요소들의 변화에 따라 저장되므로, CCD와 같이 빛의 세기에 반응하는 검출기로는 해독이 불가능하다.[6-9] 광정보처리 시스템은 본래의 특성에 의하여 복소수 진폭과 위상정보를 병렬로 읽고 쓰는 것이 가능하다.[10,11] 특히 위상변조를 이용한 코딩은 명암의 구분이 없기 때문에 명암 복사가 불가능하고 고밀도 광 매질의 작은 영역에 대용량의 입체 정보를 기록 할 수 있다. 암호화의 수준이 증가할수록 그것을 해독하기 위한 수학적 방법의 수는 엄청나게 증가되어 해독이 불가능해진다. 최근 광정보처리 시스템으로 Two-lens classical processors와 VanderLugt correlators[12]의 두 장치를 혼합한 암호화 방법 중 double-phase encoding 방식이라는 새로운 암호화 방법이 제시되었는데, 이 방식은 안정적인 방법으로 평가되고있다. double-phase encoding 방식에서 암호화된 영상은 백색 노이즈의 형태로 기록되며, 재생방법이 매우 간단하고 견고하여 광학적으로 최적의 효율을 가지게 구현할 수 있다.

본 논문에서는 Fresnel영역에 위상판을 위치시키는 방법을 기초로 하여 기존 위상판의 병진 운동에 회전창을 추가하여 암호화 수준을 높일 수 있다. 본 시스템의 정확한 암호화 수준을 측정하기 위하여 선명도 변조[13,14]의 방법을 사용하여 아날로그 입력에 대한 암호화 수준을 분석하였다.[15,16]

II. RPM을 이용한 암호화

그림 1은 Javidi[17,18] 등이 제안한 Fresnel 영역 암호화 방법을 보여준다. 이 방법에서는 임의 위상판의 위치가 입사면과 Fresnel 영역 사이에 놓이므로 위상판 그 자체가 키 역할을 할 뿐 아니라 위상판의 위치정보가 키 역할을 하게 되어 보안 문제까지 해결하게 할 수 있다. 원본이미지 $f(x,y)$는 입력면과 첫 번째 렌즈 사이에 놓인 RPM1($\exp\{i2\pi p(x,y)\}$)에 의해 일차 암호화 된 후 푸리에 렌즈에 의해 푸리에 변환된다. 이때 다시 렌즈와 푸리에 평면 사이에 놓인 RPM2($\exp\{i2\pi b(\alpha,\beta)\}$)에 의해 2차 암호화되어 광굴절 매질에 저장된다. 이때 암호화된 출력 $\phi(x,y)$은 다음과 같다.

$$\phi(x,y)=[f(x,y)\exp\{i2\pi p(x,y)\}]*F\cdot T^{-1}[\exp\{i2\pi b(\alpha,\beta)\}] \quad (1)$$

$F\cdot T^{-1}$: inverse Fourier tranform, $*$: convolution operation

암호화 해독과정의 개념도인 그림 2에서 보듯이 위상 보정능력을 가진 위상공액파가 광굴절 결정에 입사하여 암화화과정(그림 1)의 역순으로 진행하면서 원본이미지를 재생한다. 이때 RPM의 위치 정보가 변하지 않는다고 가정하면 해독시의 출력 $g(x,y)$은 다음과 같다.

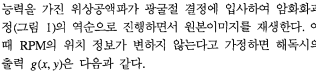


그림 1. 두 개의 임의 위상판을 이용한 광학상의 암호화과정.

그림 2. 암호화한 상을 위상공액파를 이용하여 해독하는 과정.

†E-mail: shinsh@kangwon.ac.kr

$$g(x,y)=[\phi(x,y)*F\cdot T^{-1}[\exp\{-i2\pi b(\alpha,\beta)\}]]\exp\{-i2\pi p(x,y)\}$$
$$=[f(x,y)\exp\{-i2\pi b(x,y)\}]*F\cdot T^{-1}[\exp\{i2\pi b(\alpha,\beta)\}]$$
$$*F\cdot T^{-1}[\exp\{-i2\pi b(\alpha,\beta)\}]\exp\{-i2\pi p(x,y)\} \quad (2)$$
$$=[[f(x,y)\exp\{i2\pi p(x,y)\}]*\delta(x,y)]\exp\{-i2\pi p(x,y)\}$$
$$=f(x,y)\exp\{i2\pi p(x,y)\}\exp\{-i2\pi p(x,y)\}$$
$$=f(x,y)$$

위상공액파로 재생시에 RPM의 위치가 달라지면 RPM1(exp{$-i2\pi p(x,y)$})과 RPM2(exp{$-i2\pi b(\alpha,\beta)$})의 정보가 변하므로 왜곡된 상으로 재생된다. 따라서 이 시스템의 경우 RPM의 위치정보가 해독시의 키가 되므로 동일한 위상판과 위치정보를 알지 못하면 원본이미지를 해독할 수 없다.

그림 3은 실험장치도이다. Ar ion laser(λ = 514.5 nm)에서 나오는 광속을 PBS(polarizing beam splitter)를 이용하여 신호광속과 기준광속으로 분리한다. 기준광속은 BS(beam splitter)에 의해 기록을 위한 기준광속과 암호 해독을 위한 광속으로 나누어져서 Fe가 0.02-mol% 첨가된 $LiNbO_3$(10 mm× 10 mm×10 mm)에 입사된다. 이때 매질은 x-z평면상에 놓여있고, C-축은 크리스탈 표면에 대하여 45° 방향에 있다. 입력상은 렌즈 L1에 의해 점선으로 표시된 푸리에 평면상에 푸리에 변환되고 푸리에 변환된 입력상은 렌즈 L2에 의해 $LiNbO_3$:Fe 결정에 결상되어 기준광속과 간섭하게 된다. 이때 RPM1은 입력영상을 위상 변조시킴과 동시에 암호 해독시의 입사 위상코드가 된다.

RPM2는 푸리에 평면사이에 놓여 입력상을 2차 위상 변조시키고 해독시에 역시 푸리에 위상코드가 되도록 위치시켰다. 실험에 있어 회전형 코드를 더하기 위하여 지름 26 mm의 원형 엠보싱 필름을 RPM으로 사용하였다. 실험에서 RPM1은 렌즈 L1으로부터 100 mm, 그리고 RPM2는 L1으로부터 200 mm에 위치하고 렌즈 L1, L2, L3의 초점거리는 각각 300 mm, 50 mm, 125 mm이다. RPM2의 위치 이동은 PZT로 제어하였다.

실험에서 모든 광속은 정상편광이고, 기록시간은 120초이다. 기록이 끝난 후 암호화된 상은 렌즈 L3에 의해 역 푸리에 변환 된 후 CCD2으로 결상하였다. 기록하는 동안 셔터 S1과 셔터 S3를 열고 셔터 S2는 닫는다. 암호화된 상을 해독할 때에는 S1과 S3를 닫고 S2를 열어 CCD1로 관측하였다.

실험은 입력상을 RPM으로 암호화를 시키고 RPM의 위치이동 없이 위상공액파로 해독할 수 있는지 확인 후, RPM의 위치정보가 해독 상의 키역할을 확인하기 위해 RPM을 광속의 진행방향과 수직인 x-축 방향과 진행방향인 z-축, 또는 회전시키면서 해독영상을 알아볼 수 없을 때까지 위치를 이동시키면서 해독영상을 관찰하였다.

아날로그 입력상을 암호화 한 후 RPM2를 x-축, z-축, 그리고 회전으로 위치이동 시켜 CCD1로 영상을 입력받아 저장하였다. 입력 신호가 USAF 검사표와 같은 아날로그 입력일 때 시스템의 성능을 평가하는 유용한 지수는 선명도 변조 $\gamma = I_{max} - I_{min}/I_{max} + I_{min}$이다.[13,14] 수준 분석을 위해 저장된 영상의 선택된 영역에 대한 세기 분포의 그래프로 변환하여 위치이동 없이 원본의 재생 이미지의 세기분포를 1로 놓고 위치 이동후 저장한 재생이미지의 세기분포에 대해 선명도 변조 γ 값을 얻었다. 이 값으로부터 암호 해독 경우의 수를 구하여 시스템의 암호화 수준을 분석하였다.

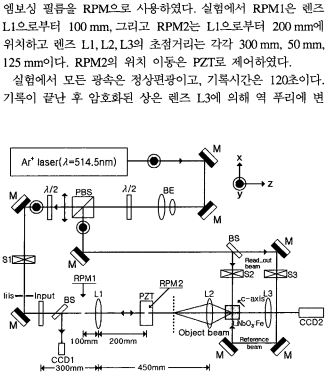


그림 3. 암호화 및 해독을 위한 실험장치도.

III. 실험결과

그림 4(a)와 (b)는 위상공액파로 RPM을 기록할 때와 같은 위치에 고정하고 재생한 영상이다. 그림 4(a)는 일반 영상의 재생 영상으로 원형의 지름은 9 mm이다. 이때 RPM의 위치 변화가 없으면 원본이미지가 완벽히 재생함을 볼 수 있다. 그림 4(b)는 아날로그 입력상의 암호화 수준을 분석하기 위하여 사용한 USAF resolution target을 재생한 것으로 사용된 부분은 Group 3, Number 5로 12.7 line pair/mm의 공간주파수를 가진 영역이다. 그림 4(c)는 'OPT'원본영상이 RPM1과 RPM2를 사용하여 암호화된 상태를 보여준다. 이 경우에는 원본 이미지를 알아볼 수가 없는 노이즈의 형태로 암호화되어 있음을 알 수 있다.

RPM 자체가 암호화 키 역할을 하는지 여부를 확인하기 위해 RPM1과 PRM2를 각각 제거하거나 같은 위치에서 서로 바꾸어 실험하였다. 그림 5는 RPM을 제거하거나(a, b) 다른 RPM으로 교체하였을 때(c) 재생되는 상을 기록한 것으로 RPM의 위치와 종류가 바뀌면 원본을 재생하지 못하는 것을

(a) (b) (c)

그림 4. (a) 위상공액파로 RPM의 위치 변화 없이 원본 'OPT'를 재생한 영상. (b) 원본영상 'USAF resolution targetd'을 RPM의 위치 변화 없이 재생한 영상. (c) 원본 'OPT'를 RPM을 사용하여 암호화한 영상.

암호화수준 분석

$$\gamma = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}$$

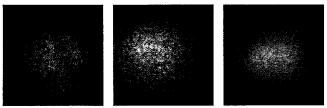


그림 5. (a) RPM1을 제거시 재생영상. (b) RPM2를 제거시 재생영상. (c) RPM을 서로 교체시 재생 영상

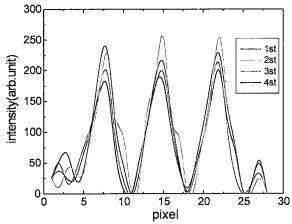


그림 6. 동일한 실험조건에서 기록 후 RPM2를 5 μm 이동한다음 반복하여 얻은 재생상의 세기분포.

알 수 있다. 이를 통해 RPM자체로도 암호화 키가 됨을 확인할 수 있다. 따라서 만일 재생시 원본영상을 매칭에 기록할 때와 다른 RPM을 사용하거나 RPM의 위치의 정보가 틀리다면 원본 영상을 재생할 수 없게 된다.

그림 6은 실험의 신뢰도를 점검하기 위해 모든 실험조건을 동일하게 하고 기록매질에 같은 입력영상의 암호화 영상을 반복하여 기록한 재생상의 세기분포로 그림 4(b) 영상을 입력영상으로 하여 얻은 결과이다. 각 재생상은 암호화시킨 후 RPM2를 x-축으로 5 μm 위치 이동하여 얻은 것으로 반복적인 기록과 소거에도 재생상의 위치와 선명도는 거의 동일함을 알 수 있다.

그림 7(a)는 암호화된 영상을 기록한 후 RPM2를 x-축 으로 이동시키면서 CCD2의 입력영상으로부터 얻은 세기분포에 의해 구한 γ 값의 변화 그래프이다. 10 μm이상 이동시키면 γ의 변화가 급격히 일어나고 18 μm이상이면 판독이 불가능하다. 또한 그림 7(b)와 같이 z-축의 γ 값의 변화를 살펴보면 임계값이 2.4 mm임을 알 수 있다. x-축으로 이동 할 때와 z-축 이동시의 임계값의 차이가 많이 나는 것은 RPM을 광속이 진행방향으로 움직였을 경우 보다 수직으로 움직였을 경우가 더 민감하다 하다는 것을 보여 준다.

그림 7(c)는 RPM2를 회전시켰을 때의 재생상의 선명도변조의 변화를 보여준다. RPM2를 0.23° 이상 회전시키면 γ가 급격하게 작아지며 0.3° 이상이면 판별이 불가능하다. RPM의 회전시에는 x-y축의 위상변화가 같이 일어나므로 회전 RPM

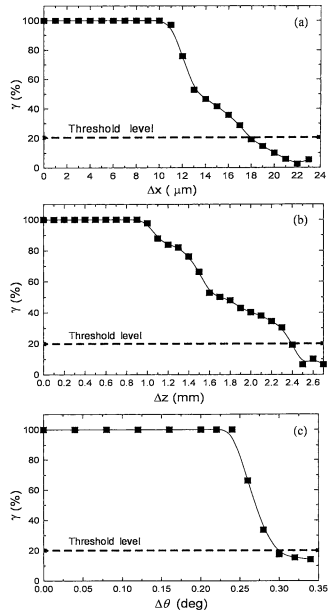


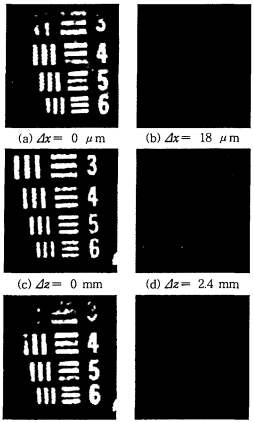
그림 7. x-축(a), z-축(b), 회전방향(c)으로 RPM2를 이동해 얻은 재생상의 선명도 변조 그래프.

을 사용하여 3차원 암호화 키 값만 사용하는 경우보다 입력상의 암호화 수준을 높일 수 있다. 그림 8은 RPM2를 각각 x-축, z-축, 회전방향으로 RPM2가 위치이동 하기 전의 재생상(a, c, e)과 γ 값이 20%가 되는 위치이동시의 재생상(b, d, f)을 보여 준다.

여기서 x, y, z 방향의 이동과 회전을 고려하면 하나의 RPM에 의하여 만들어 질 수 있는 경우의 수 V는 다음과 같다.

$$V=\frac{R^2}{\Delta x\Delta y}N_z N_\theta,$$
$$N_z=L/\Delta z,\quad N_\theta=360/\Delta\theta \tag{3}$$

이때 x, y, z-축은 그림 3과 같고, R은 RPM의 반지름, Δx, Δy, Δz는 각각 입력상의 해독 가능한 RPM의 최대 이동 거



(a) $\Delta x = 0\ \mu m$ (b) $\Delta x = 18\ \mu m$

(c) $\Delta z = 0$ mm (d) $\Delta z = 2.4$ mm

(e) $\Delta\theta = 0^{\circ}$ (f) $\Delta\theta = 0.32^{\circ}$

그림 8. x-축(a, b), z-축(c, d), 회전방향(e, f)으로 RPM2의 위치 이동시의 재생상.

리이며 L은 z축으로 RPM이 이동할 수 있는 최대 거리이다. N_θ는 RPM의 회전에 따른 경우의 수이고 $\Delta\theta$은 입력상의 해독이 가능한 RPM의 최대회전각이다. 두개의 RPM에 의한 암호해독의 경우의 수 $N = V^2$이므로 임계 γ 값과 실험결과($\Delta x \approx \Delta y \approx 18\ \mu m$, $\Delta z \approx 2.4$ mm, $\Delta\theta \approx 0.3^{\circ}$)를 사용하여 계산한 암호해독 경우의 수는 $N \simeq 6\times 10^{21}$이다.

기존의 3차원의 키에서 회전항을 추가하여 4차원의 키를 구현하여 선명도 변조변화의 방법으로 시스템의 암호화 수준을 분석한 결과 본 시스템의 경우 3차원 병진운동의 암호화 수준 보다 암호화 수준이 ~10^6 정도 향상되었다.

IV. 결 론

Ar ion 레이저($\lambda = 514.5$ nm)를 광원으로, 광굴절 결정($LiNbO_3$:Fe)을 기록매질로 사용하여 기존의 Fresnel 영역 암호화 방식에 임의 위상판의 회전항을 더하여 암호화 수준을 향상시켰다. 광굴절 결정에 90° 광학계를 사용하여 암호화된 2차원 평면 영상을 기록하고 위상공액파를 이용하여 해독할 수 있었다. 이 암호화 시스템의 경우, 위상 암호화의 방식으로 위상판의 자체뿐만 아니라 그 위치의 정보가 암호화 키 역할을 한다는 것을 확인하였다. 2차원의 평면 영상의 아날로그 영상의 암호화 시스템을 분석하기 위하여 RPM의 위치 변화에 따른 선명도 변조 변화를 측정하여 암호화 시스템의 수준을 분석하였다. 기존의 3차원의 키에서 회전의 한 차원을 더하여 4차원의 키를 구현한 결과 기존의 RPM의 회전항을 고려하지 않은 값 N~4×10^{15}과 비교해 볼 때 암호화 수준을 ~10^6 정도 향상시킬 수 있었다. 임의 위상판의 위상변조 셀의 크기가 작은 것을 사용한다면 암호화 수준은 더욱 향상시킬 수 있을 것이다. RPM의 위치 정보를 이용한 광학상의 암호화 방법은 기록시의 RPM의 정확한 위치 정보를 알지 못하면 암호의 해독이 불가능하므로 홀로그램 광 기억장치의 보안에 매우 유용한 암호화 방법임을 확인하였다.

감사의 글

본 논문은 한국과학재단 목적기초연구(2000-2-1100-00 3-3) 지원으로 수행되었음.

참고문헌

[1] F. H. Mok, "Angle-multiplexed storage of 5000 holograms in lithium niobate" *Opt. Lett.*, vol 18, no 11, pp. 915-917, 1993.
[2] X. An, D. Psaltis, and G. W. Burr, "Thermal fixing of 10,000 holograms in $LiNbO_3$:Fe," *Appl. Opt.*, vol. 38, no. 2, pp. 386-393, 1999.
[3] B. Javidi, "Securing information with optical technologies," *Physics Today*, March, 27, 1997.
[4] J. F. Heanue, M. C. Bashaw, and L. Hesselink, "Encrypted holographic data storage based on orthogonal-phase-code multiplexing," *Appl. Opt.*, vol. 34, no. 26, pp. 6012-6015, 1995.
[5] R. K. Wang, I. A. Watson and C. R. Chatwin, "Random phase encoding for optical security," *Opt. Eng.*, vol. 35, pp. 2464-2469, 1996.
[6] H. S. Li. Y. Qiao, and D. Osaltis, "Optical network for real-time face recognition," *Appl. Opt.*, vol. 32, no. 26, pp. 5026-5035, 1993.
[7] R. L. van Reneese, ed., *Optical Document Security* (Artech House, Boston. 1994).
[8] K. H. Fielding, J. L. Horner, and C. K. Makekau, "Optical fingerprint identification by joint transform correlation," *Opt. Eng.*, vol. 30. pp. 1958-1961, 1991.
[9] H. Rajenbach, "Dynamic holography in optical pattern recognition," *Proc. SPIE*, vol. 2237, pp. 329-346, 1994.
[10] B. E. A. Saleh and M. Teich, Fundamentals of Photonics, (Wiley, New York, 1991).
[11] B. Javidi and J. L. Horner, Eds., *Real-time Optical information Processing* (Academic Press, New York, 1994).
[12] J. W. Goodman, *Introduction to Fourier Optics* (McGraw-Hill, New York, 1968).
[13] 장 수, 조재홍 외, 응용광학(대웅, 서울, 1997).
[14] E. Hecht, *Optics* (Addison Wesley, 1987).
[15] 김병철, 차성도, 신승호, "회전형 임의 위상판을 이용한 광학상의 암호화," 제5회 광정보처리 학술발표회, 한국광학회, 서울, 2000, pp. 203-206.

[16] 김병철, 차성도, 신승호, "임의 위상판에 의한 광학상 암호화의 분석," 한국광학회 2001년도 동계학술발표회, 한국광학회, 서울, 2001, pp. 72-73.
[17] P. Refregier and B. Javidi, "Optical image encryption based on input plans and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767-769 1995.
[18] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.*, vol. 24, no. 11, pp. 762-764, 1999.

Optical image encryption by use of double random phase mask and analysis of its encryption level

Byeongchul Kim, Sungdo Cha, and Seung-Ho Shin†
Department of Physics, Kangwon National University, Chunchon 200-701, KOREA
†E-mail: shinsh@kangwon.ac.kr

(Received August 29, 2001 ; revised manuscript received December 26, 2001)

We present a method to improve encryption level by use of a rotational term in the double random-phase-mask(RPM) encryption system. Encrypted optical images are recorded in a photorefractive $LiNbO_3$:Fe crystal and reconstructed by using a phase conjugated reading beam. The encryption level for the analog image is analyzed by use of visibility function.

Classification code : IP.010.