

가상 위상 영상을 이용한 광학적 암호화 시스템

서동환[†] · 신창목 · 김수중

경북대학교 전자전기컴퓨터학부

Ⓣ 701-702 대구광역시 북구 산격동 1370

배장근

구미1대학 전자정보과

Ⓣ 730-711 경북 구미시 부곡동 407

김철수

경주대학교 컴퓨터전자공학부

Ⓣ 780-712 경북 경주시 효현동 산 42-1

도양희

제주대학교 전자공학과

Ⓣ 690-756 제주도 제주시 아라1동 1

(2002년 11월 29일 받음, 2003년 4월 1일 수정본 받음)

본 논문에서는 위상 변조된 가상 영상과 간섭의 원리를 이용하여 영상의 암호화 및 복호화 수준을 향상시키는 방법을 제안하였다. 원 영상은 그레이 값을 가지는 가상 영상과 무작위 암호화 키, 그리고 복호화 키를 위상 변조하여 이들을 간섭계의 한 쪽 경로에 겹으로써 기준파와의 간섭에 의해서 간단히 복원될 수 있다. 제안한 암호화 과정은 원 영상의 어떤 정보도 포함하지 않은 위상 변조된 가상영상과 컴퓨터를 통해서 만들어진 무작위 영상(암호화 키)을 곱함으로써 암호화한다. 그러므로 허가되지 않은 사람들이 암호화키를 분석함으로써 있을 수 있는 복제 가능성을 배제하였다. 또한 그레이 영상을 암호화함으로써 이진 위상 암호화방법에 비해 암호화 수준이 높은 장점을 가진다. 컴퓨터 시뮬레이션과 광 실험을 통하여 제안한 방법이 광 암호화 시스템에 적합함을 확인하였다.

주제어 : optical encryption, Interferometer, Random phase.

I. 서 론

최근 광학적 암호화 기술에 관한 연구가 활발히 진행되고 있는데 이는 광을 이용한 영상처리기술은 위상정보와 세기정보를 동시에 광학매질에 기록할 수 있는 특성에 기인한다. 명암으로 기록되는 세기정보와는 달리 위상정보는 투명한 광학매질의 두께로 기록되므로 사람의 눈이나 기존의 세기검출기로는 위상정보를 추출하는 것이 불가능하다. 따라서 광 암호화 시스템은 무작위 위상마스크를 키 코드로 사용하여 원 영상을 암호화하며 이렇게 암호화된 영상은 세기검출기로는 추출이 불가능하고 무작위 특성에 의해서 원래의 패턴을 역추적하기가 어렵다는 특성을 가진다. 광학적으로 암호화된 영상은 전통적인 상관 시스템^[1,2]이나 간섭계 시스템을 이용하여 원 영상을 재생하게 되는데, 이때 암호화에 사용된 무작위 위상 마스크에 의해서 진위 여부를 판정하게 된다. 이러한 무작위 위상마스크를 부착하거나 위상패턴으로 제조된 카드나 신분증은 복제나 위조를 방지할 수 있는 효과적인 대안이 될 수 있

으므로 국내외적으로 광 암호화 시스템에 관한 많은 연구가 행해지고 있다.

광 암호화 시스템은 주로 4-f 광 상관기(correlator)를 이용하여 입력평면에 세기 정보를 가지는 원 영상을 백색잡음 형태를 가지는 복소함수로 암호화한 후 동일한 시스템을 이용하여 복호화 한다.^[3-5] 이 방법은 광학적 시스템 구성 시 광축 정렬이 어렵고 원 영상을 복원할 때 암호화에 사용된 위상마스크의 정확한 복소공액 마스크를 제작해야 한다는 어려움이 있다. 이를 해결하기 위해 광축 정렬이 필요 없는 결합 변환 상관기(joint transform correlator; JTC)를 이용한 방법^[6]과 광굴절매질을 이용하여 공액 복소빔을 이용한 방법^[7] 등이 제안되었다. 최근에는 세기정보 암호화 수준을 향상시키기 위하여 입력평면에 위상정보를 가지는 원 영상을 이용하여 암호화하는 방법^[8,9]들이 제안되었으며 이 중 Mosensen 등^[10,11]은 위상 정보를 암호화한 후 일반화된 위상 세기 방법(generalized phase-contrast technique)을 이용하여 간단히 원 영상을 복원할 수 있으나 복호화 과정에서 위상 세기 필터(phase-contrast filter)와 4-f 시스템을 이용하므로 광축 정렬의 어려움을 가진다. 앞서 제안된 방법들의 가장 큰 단점 중에 하나는 만약 허가되지

[†]E-mail: dhseo@palgong.knu.ac.kr

많은 사용자가 암호화된 영상을 분석하여 암호화키를 파악함으로써 복원 영상을 알 수 있는 문제점이 있다. 따라서 암호화된 영상이 분석되더라도 복원 영상의 파악이 불가능한 방법이 필요하다.^[12]

본 논문에서는 위상 변조된 원 영상의 정보를 세 개의 위상 변조된 영상 즉 가상 영상, 무작위 영상, 복호화키 영상에 각각 배분시키고 가상 영상과 무작위 영상을 이용하여 암호화함으로써 암호화키인 무작위 영상을 분석 및 파악함으로써 있을 수 있는 복제 가능성을 배제시켜 암호화 수준을 향상시켰고 간섭의 원리를 이용하여 간단히 원 영상을 복원하는 방법을 제안하였다. 제안한 방법은 먼저 원 영상의 정보가 없는 가상 영상을 위상변조하고, 무작위 패턴을 컴퓨터로 발생시켜 위상 변조한 후 두 위상 변조된 영상을 공간영역에서 곱해서 순수한 위상 값만 가지는 패턴으로 만들어 암호화된 영상으로 사용하여 허가되지 않은 개인이나 그룹이 암호화된 영상을 분석하더라도 가상영상을 원 영상으로 오인하게 된다. 따라서 복호화 키의 정보 없이는 결코 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다는 장점을 가진다. 또한 공간영역에서 암호화함으로써 그레이위상 CGH로 양자화하는 과정에 따른 영상의 정보손실이 없다. 원 영상의 복호화 과정은 암호화된 영상과 제안한 위상 대응 규칙으로 만든 복호화 키를 간섭계의 한 쪽 경로에 위치시킨 후 기준빔과 간섭시킴으로써 간단히 복원되므로 간섭계가 가지는 화소 대 화소 대응을 용이하게 하여 복원영상의 해상도를 향상시킬 수 있다. 컴퓨터 시뮬레이션과 광 실험을 통하여 제안한 방법이 광 암호화 시스템에 적용 가능함을 확인하였다.

II. 암호화 및 복호화 과정

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

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

로 표현되고 $\hat{f}(x, y)$ 은 원 영상의 반전된 영상을 나타낸다. 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

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

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

$$e(x, y) = v_p(x, y)r_p(x, y) = \exp[j\pi\{v(x, y) + r(x, y)\}] \quad (3)$$

와 같고 암호화된 영상도 순수한 위상함수이므로 그 세기는 '1'이 된다. 또한 암호화된 영상 $e(x, y)$ 의 위상 값은 가상 영상과 무작위 영상의 선형적인 합임을 알 수 있고 만약 허가되

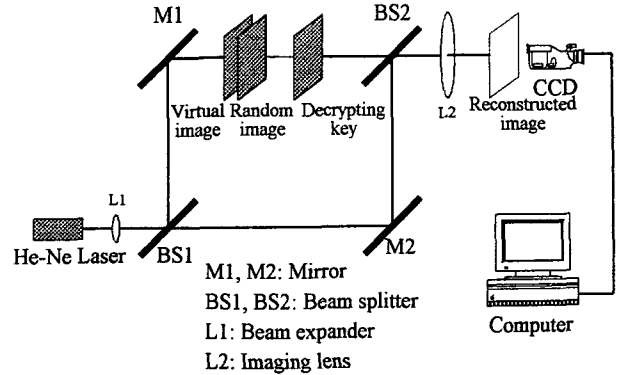


그림 1. 제안한 영상 복원을 위한 마흐 쟈더 간섭계.

지 않은 개인이나 그룹이 암호화된 영상을 분석하더라도 가상 영상을 원 영상으로 오인하게 된다. 따라서 복호화키의 정보 없이는 결코 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다는 장점을 가지고 이 위상 영상들은 공간 광 변조기나 광학적 리소그라피를 통하여 만들 수 있다. 또한 기존의 푸리에 영역에서 암호화하는 방법에서 영상을 CGH로 변환시킬 때의 샘플링 오차로 인한 영상의 왜곡이 생기는 문제를 해결하고 영상의 복원 시 암호화에 사용된 무작위 영상을 복호화키로 사용함으로써 기존의 반복 알고리즘을 이용한 암호화 시스템이 가지는 정확한 복호키를 재생하기 위한 시간소모를 줄일 수 있고 또한 암호화된 영상은 복소함수 값을 가지므로 세기검출기로 복사되지 않는 광 보안 시스템의 장점을 그대로 가지게 된다.

간섭의 원리를 이용하여 위상 정보를 세기 정보로 변환시키는 영상의 복원 시스템 구성도는 그림 1과 같다. 암호화된 영상 $e(x, y)$ 와 위상 대응 규칙으로 만든 위상 변조된 복호화키 $d_p(x, y)$ 를 간섭계의 한 쪽 경로에 위치시킨 후 광 경로가 동일한 기준빔과 간섭시킴으로써 간단히 복원된다. 두 위상카드가 위치한 경로의 정합된 영상 $m(x, y)$ 는

$$\begin{aligned} m(x, y) &= e(x, y)d_p(x, y) \\ &= v_p(x, y)r_p(x, y)d_p(x, y) \\ &= \exp[j\pi\{v(x, y) + r(x, y) + d(x, y)\}] \\ &= \exp[j\pi\hat{f}(x, y)] \end{aligned} \quad (4)$$

이고 여기서 위상 대응 규칙을 이용하여 복호화키 영상 $d(x, y) = \hat{f}(x, y) - v(x, y) - r(x, y)$ 가 되도록 제작하고 정합된 영상 $m(x, y)$ 의 위상값은 가상 영상, 무작위 영상 그리고 복호화키 영상의 선형적인 합임을 알 수 있다.

따라서 그림 1의 간섭계를 이용한 출력 평면에 나타나는 간섭영상의 세기는

$$\begin{aligned} I(x, y) &= |R(x, y) + R(x, y)m(x, y)|^2 \\ &= |R(x, y)|^2 |1 + \exp[j\pi\hat{f}(x, y)]|^2 \end{aligned} \quad (5)$$

이다. 여기서 기준빔 $R(x, y) = E\exp(j\phi)$ 이고 E 는 파의 크기이고 ϕ 는 초기 위상이다. 따라서 $|R(x, y)|^2 = |E\exp(j\phi)|^2 = |E|^2$ 이다. 이때 복호화키를 만드는 제안한 위상 대응 규칙은

$$I(x,y)=|E|^2 \begin{cases} \hat{f}(x,y)=2n & 0 \leq x,y < 2n \\ \hat{f}(x,y)=2n+1 & 2n \leq x,y < 4n \end{cases} \quad (6)$$

이며 여기서 n 은 정수이다. 즉 복원하고자 하는 원 영상 $f(x,y)$ 가 밝으면 이 되도록 $d(x,y)$ 를 만들고 반면에 어둡게 나타나면 $\hat{f}(x,y)=2n+1$ 이 되도록 하면 간섭 세기 값이 각각 $4|E|^2$ 과 0 이 되어 이진 원 영상 $f(x,y)$ 를 $d(x,y)$ 의 값으로 정확히 복원할 수 있다. 제안한 방법에서 가상 영상, 무작위 영상과 복호화키는 그레이 영상을 사용하였고 복원하고자 하는 영상은 이진 영상이 되도록 하였다. 물론 복원 영상을 그레이 영상으로 확장하여 나타낼 수 있으나 식 (5)에서 여현 함수의 비선형성에 의해 영상의 왜곡이 발생함을 알 수 있으며 이를 해결하기 위해서는 컴퓨터의 후처리가 동반되어야 하는 단점을 가지고 있다. 제안한 방법은 간섭계의 한 경로에만 위상 영상들을 중첩시켜 둠으로써 영상들 간의 화소 대 화소의 정합 문제로 인한 회절효과를 줄일 수 있으며 두 빔 사이의 경로차나 마스크 제작상의 문제로 인한 영상의 왜곡이 발생하더라도 컴퓨터로 복원 영상과 복원 영상의 반전 영상을 함께 얻는다면 원 영상을 복원할 수 있음을 컴퓨터 모의 실험을 통하여 확인하였다.

III. 컴퓨터 모의 실험과 광 실험

3.1. 컴퓨터 모의 실험

그림 2는 컴퓨터 모의실험을 위하여 제작된 영상들로 그 화소수는 128×128 이다. 그림 2(a)는 복원할 원 영상으로 이진 값을 가지는 영문자 'OPTIC'를 사용하였고 그림 2(b)는 암호화된 가상 영상으로 Lena 영상을 사용하였고 그림 2(c)는 컴

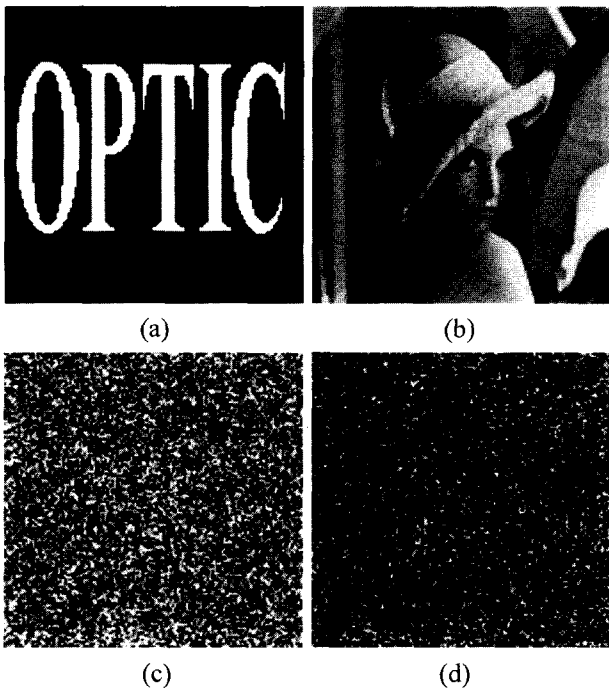


그림 2. 컴퓨터 모의실험에 사용된 영상. (a) 원 영상, (b) 가상 영상, (c) 무작위 영상, (d) 암호화된 영상.

퓨터로 발생시킨 무작위 영상이며 이들을 각각 $[0, 1]$ 사이의 값으로 정규화 시켜 위상 변조하여 서로 곱한 영상을 그림 2(d)에 나타내었으며 이 암호화된 영상은 0 과 π 사이의 위상 값을 가지므로 CCD나 사람의 눈으로는 명암을 판별할 수 없으므로 편의를 위해 그레이 값으로 각각 대응시켜 표현했으며 이는 가상 영상과는 전혀 관계없는 무작위 패턴으로 나타남을 확인할 수 있다. 또한 만약 허가되지 않은 사람들이 암호화키를 분석하더라도 가상 영상을 원 영상으로 오인하게 되므로 복제 가능성을 배제할 수 있다. 그림 3(a)와 (b)는 각각 복원 영상을 얻기 위해 위상 대응 규칙으로 만든 올바른 복호화키와 컴퓨터를 통해 만든 거짓 키이며 그림 3(c)와 (d)는 이에 각각 대응되는 복원 영상으로 거짓 키로는 영상이 재생되지 않음을 확인할 수 있다.

그러나 실제로는 마흐-젠더 간섭계를 이용한 암호화 시스템은 진동이나 외부 교란으로 인해 위상 지연이 발생할 수 있으므로 실험구성이 정밀해야 하고 특히 위상 암호화 시스템은 세기 암호화 시스템보다 암호화 수준은 향상되지만 잡음이나 위상 마스크의 흠집 등에 민감하여 영상의 왜곡이 발생할 수 있다. 따라서 간섭계의 두 경로 차나 부정확한 마스크 제작으로 인한 위상 차가 발생할 수 있으므로 이로 인한 영상왜곡의 특성을 고려하면 식 (5)는

$$I(x,y)=|R(x,y)+R(x,y)n_a \exp(j\phi_w)m(x,y)\exp(j\pi\phi_p)|^2 = |R(x,y)|^2 |1 + \exp(j\phi_w)\exp[j\pi\{\hat{f}(x,y)+\phi_p\}]|^2 \quad (7)$$

이 되고 여기서 ϕ_w 는 두 파 사이의 위상차이고 n_a 는 위상 마스크에 묻은 먼지나 흠집에 의한 크기이고 ϕ_p 는 마스크 제

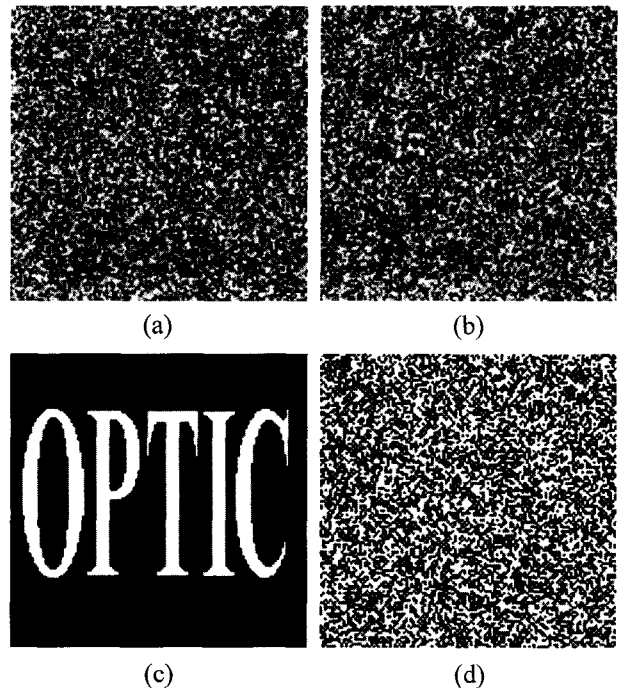


그림 3. 컴퓨터 모의실험 결과. (a) 올바른 복호화키, (b) 거짓 복호화키, (c) 올바른 복호화키로 재생된 영상, (d) 거짓 복호화키로 재생된 영상.

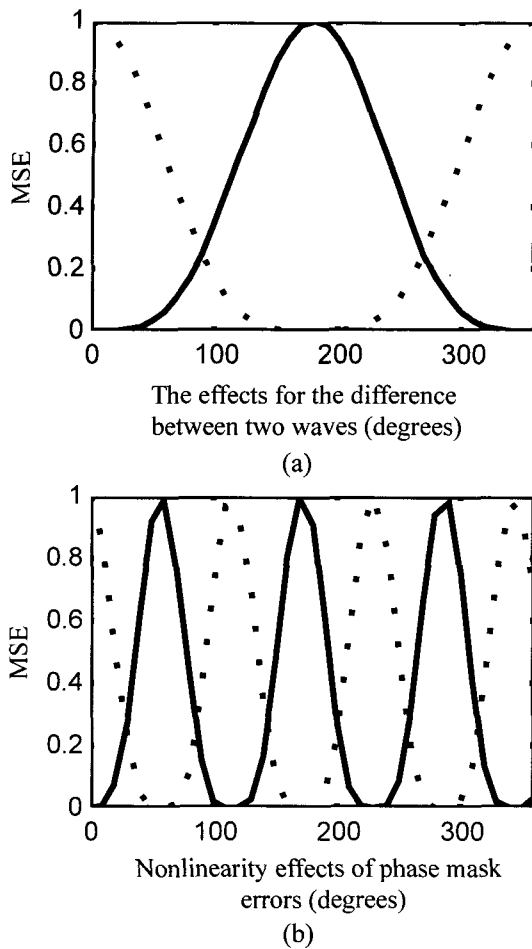


그림 4. 위상차로 인한 평균 제곱 오차. (a) 두 파의 위상차가 있을 경우, (b) 마스크 제작상의 문제로 인한 위상차.

작 상의 문제로 인한 위상차이다. 여기서 n_a 는 실제 시스템에서 중요한 문제지만 위상 암호화 시스템에서는 크기 성분을 보통 '1'로 둔다.⁹⁾ 그림 4(a)와 (b)는 각각 두 파의 위상차 (ϕ_w)가 있을 경우와 마스크 제작상의 문제로 인한 위상차 (ϕ_p)가 있을 경우를 분리하여 복원 영상의 평균제곱오차(mean square error; MSE)를 나타내었다. 여기에서 사용된 평균제곱 오차의 표준¹⁰⁾은

$$MSE = E \left\{ \frac{1}{N \times M} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} [|f_o(x, y)| - |f_d(x, y)|]^2 \right\} \quad (8)$$

이며 여기서 $f_o(x, y)$ 와 $f_d(x, y)$ 는 각각 원 영상과 복원 영상이고 $N \times M$ 은 원 영상의 픽셀 수이며 $E\{\cdot\}$ 는 평균값이다. 그림 4에서 실선은 복원 영상이 위상차가 발생할 경우 원 영상과의 정규화 평균제곱오차를 표현하고 점선은 위상차가 발생한 복원 영상의 반전 영상과 원 영상과의 정규화된 평균제곱 오차를 표현한 것이며 이는 컴퓨터로 복원 영상과 그것의 반전 영상을 모두 얻는다면 원 영상의 복원이 가능함을 나타낸다. 그러나 그림 4(a)에서 90°와 270°, 그림 4(b)에서 90/π°부터 180/π° 간격으로 점선과 실선이 만나는 교점에서 정확한

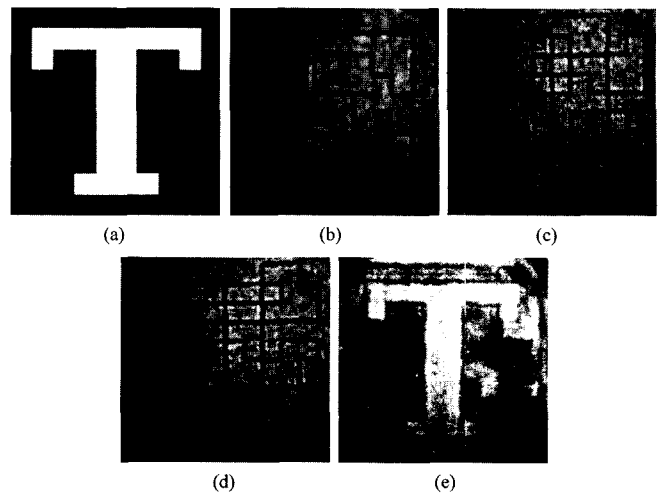


그림 5. 광 실험. (a) 원 영상, (b) 가상 영상, (c) 암호화된 영상, (d) 복호화키, (e) 복원 영상.

복호화키를 사용하더라도 복원 영상과 반전영상으로 원 영상의 정보를 알 수 없음을 나타낸다.

3.2. 광 실험

그림 5는 간단한 광학적 실험을 하기 위한 이진 위상 마스크를 그려서 광학적 리소그래피를 이용하여 유리판을 식각하여 제작하였다. 마스크로 사용된 유리판의 시간당 식각율을 계산하여 원하는 두께가 될 때까지 식각 용액 속에 넣어 두는데 이때 필요한 두께를 계산하는 식은

$$D = \frac{\lambda \phi}{2\pi(n-1)} \quad (9)$$

와 같고 여기서 D 는 식각하고자 하는 유리판의 두께, λ 는 영상 복원시 사용할 레이저의 파장, n 은 유리판의 굴절률, ϕ 는 제어하고자 하는 위상을 나타낸다. 유리판의 식각을 위하여 사용한 용액은 BHF(buffered hydrofluoric acid)로써 이에 의한 유리판의 식각률은 분당 약 0.15로 측정되었으며, 여러 번의 실험을 통해 박막두께 측정기(α -step)로 식각 두께를 점검하면서 오차를 줄여나가도록 하였다. 그림 5(a)는 복원할 원 영상으로 영문자 'T'를, 그림 5(b)는 위상 변조된 가상 영상으로 영문자 'E'를 나타내었으며 그림 5(c)와 (d)는 각각 위상 변조된 암호화 영상과 위상 대응 규칙으로 만들어진 복호화키이며 그 화소수는 10×10이며 위상마스크의 전체 크기는 1.5×1.5 cm²이고 한 화소의 크기는 1.5×1.5 mm²이다. 본 실험에서는 λ 는 632.8 nm, n 은 1.52, ϕ 의 값은 식각 과정에서 PR(photoresistor)이 용액에 견디는 시간을 고려하여 π 로 선택하여 식 (9)에 대입하였을 때 식각두께 D 의 값은

$$D = \frac{632.8 \times 10^{-9} \times \pi}{2\pi(1.52 - 1)} \approx 0.608 \mu\text{m} \quad (10)$$

가 된다. 본 실험에서 위상 카드 사이의 회절 효과를 최소화하기 위해서 세 개의 위상 카드를 중첩시켜서 실험하였으며 그림 5(e)는 그림 1에서와 같은 제안한 광학적 시스템을 이용

하여 CCD 카메라로 받은 복원된 영상이다. 컴퓨터 시뮬레이션과 광 실험 결과의 해상도 오차는 위상 마스크 제작 시 두께와 간섭계의 떨림으로 인한 오차라고 사료되므로 정확한 마스크의 제작과 실험 환경이 개선된다면 보다 나은 영상을 얻을 수 있을 것이다.

VI. 결 론

본 논문에서는 공간영역에서 간섭계의 원리와 위상 변조된 영상들을 이용하여 새로운 영상 암호화 및 복호화 방법을 제안하였다. 제안한 방법은 가상 영상을 이용함으로써 허가되지 않은 개인이나 그룹이 암호화된 영상을 다양한 위상 측정 방법으로 분석하더라도 그들은 가상 영상을 원 영상으로 오인하게 됨으로 어떠한 경우에도 원 영상을 복호화할 수 없는 장점을 가지고 위상 카드들의 굵과 기준빔과의 간섭에 의해 영상이 복원되므로 위상 카드 사이에서 발생할 수 있는 회절효과를 줄일 수 있다. 또한 위상 카드의 제작 과정과 두 파 사이의 경로차에 의한 위상 지연이 발생하더라도 컴퓨터로 복원 영상과 그것의 반전 영상을 모두 얻는다면 원 영상의 정보를 얻을 수 있음을 확인하였으며 컴퓨터 모의 실험과 광 실험을 통하여 제안한 암호화 방법의 타당성을 검증하였다.

감사의 글

본 연구는 정보통신부 기초기술연구지원사업(과제번호 : C1-2002-012-0-3) 지원으로 수행되었음.

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. Ahozi, "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] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phaseconjugation in a photorefractive crystal," *Appl. Opt.*, vol. 37, no. 35, pp. 8181-8186, 1998.
- [8] 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.
- [9] 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.
- [10] P. C. Mogensen and J. Gluckstad, "Phase-only optical encryption," *Opt. Lett.*, vol. 25, no. 8, pp. 566-568, 2000.
- [11] P. C. Mogensen and J. Gluckstad, "Phase-only optical decryption of a fixed mask," *Appl. opt.*, vol. 40, no. 8, pp. 1226-1235, 2001.
- [12] Hsuan 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.

Optical encryption system using phase-encoded virtual image

Dong-Hoan Seo[†], Chang-Mok Shin, and Soo-Joong Kim

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

[†]*E-mail: dhseo@palgong.knu.ac.kr*

Jang-Keun Bae

Department of Electronic Information, Kumi college, Kyungpook, 730-711, KOREA

Cheol-Su Kim

School of Computer and Electronic Engineering, Kyongju University, Kyungpook 780-712, KOREA

Yang-Hoi Doh

Department of Electronic Engineering, Cheju National University, Cheju, 690-756, KOREA

(Received November 29, 2002, Revised manuscript April 1, 2003)

In this paper, we propose an improved image encryption and decryption method using a phase-encoded virtual image and interference. An original image is simply decrypted by interfering a reference wave with the wave passing through a decrypting key and the encrypted image, where every image has grey level. The proposed encryption is performed by the multiplication of an encrypting key and a phase-encoded virtual image which does not contain any information for the original image. Therefore even if unauthorized people analyze the encrypted image, they cannot reconstruct the original image. Also grey image encryption can improve the encryption level compared to binary image encryption. Computer simulation and optical experiments confirmed that the proposed technique is a simple for optical encryption.

OCIS Codes : 100.1160, 120.3180, 120.5060.