

간섭을 기반으로한 컴퓨터형성홀로그램과 BaTiO₃를 이용한 안정한 광 정보보호 시스템의 구현

정회원 김철수*, 김종윤**, 박영호***, 김수중****, 준회원 조창섭****

Implementation of Stable Optical Information Security System using Interference-based Computer Generated Hologram and BaTiO₃

Cheol-Su Kim*, Jong-Yun Kim**, Young-Ho Park***,
Soo-Jung Kim****, Chang-Sop Cho**** *Regular Members*

요약

본 논문에서는 간섭원리에 기반한 컴퓨터형성홀로그램과 광굴절매질인 BaTiO₃를 이용하여 광 정보 보호 시스템을 구현하였다. 먼저 원영상을 재생할 수 있는 이진위상홀로그램을 생성한 후, 이를 암호화할 영상으로 간주한다. 그리고 이 홀로그램에 간섭 원리를 적용하여 암호화된 영상과 기준영상(키 정보)을 얻는다. 복호화과정은 Mach-Zehnder 간섭계에서 암호화된 영상과 기준영상과의 간섭을 통해 간섭세기 정보를 얻고, 이를 LCD를 이용하여 위상 정보로 변환한 후 푸리에 변환함으로써 원영상을 얻는다. 이 과정에서 두 영상의 간섭을 통해 얻어지는 세기 정보는 주위 진동에 상당히 민감하다. 그래서 광굴절매질인 BaTiO₃의 SPPCM 특성을 이용하여 안정한 간섭 무늬를 얻는다. 제안된 방법은 원래의 영상 대신 그 영상의 홀로그램을 암호화 하므로 이중 영상 암호 효과의 장점이 있다.

ABSTRACT

In this paper, we implemented an optical information security system using computer generated hologram based on the principle of interference and BaTiO₃ that is photorefractive material. First of all, we would generate binary phase hologram which can reconstruct the original image perfectly, and regard this hologram as the image to be encrypted. And then applying the interference rule to the hologram, encrypted and reference (key information) images are generated. In the decrypting process, we can get an interference intensity by interfering the reference image and the encrypted image in the Mach-Zehnder interferometer. and transforming interference intensity information into phase information using LCD(liquid crystal display) and finally recover original image by inverse Fourier transforming the phase information. In this process, the intensity information generated by interference of two images is very sensitive to external vibrations. So, we get a stable interference using the characteristic of SPPCM(self pumped phase conjugate mirror) of BaTiO₃ that is photorefractive material. The proposed method has an advantage of double image encryption by encrypting the hologram of the image instead of original image.

* 경주대학교 컴퓨터전자공학부 (kimcs@gyeongju.ac.kr),

** 경북대학교 정보통신공학부(kjyuni@k1.ac.kr)

*** 상주대학교 전자전기공학부(yhpark@sangju.ac.kr)

**** 경북대학교 전자전기공학부(sjkim@palgong.knu.ac.kr)

논문번호 : 030140-0331, 접수일자 : 2003년 3월 31일

I. 서론

현대 정보화 사회에서는 컴퓨터 시스템 및 통신 시스템의 결합으로 시공간을 초월하여 엄청난 양의 정보교환이 신속히 이루어지고 다양한 형태의 서비스 환경이 창출되어 사회 전반에 걸쳐 빠르게 확산됨에 따라 경제, 사회 등 전 분야에 큰 변화를 일으키고 있다. 이러한 사회는 우리생활을 보다 편리하게 만들어 주고 있지만 때로는 정보의 유출로 인한 막대한 피해를 주기도 하여서 정보보호가 매우 중요한 문제로 대두된다. 특히 정보의 공유와 개방을 목표로 개발된 인터넷으로 인해 통신선로를 통한 정보의 불법 침입이 새로운 사회적·법적 문제로 대두되고 있다. 또한 정보화 진전에 따라 개인의 정보의 신용이 중요시되고, 인터넷을 통한 상품구매, 의료비 결재를 위한 스마트 카드 보급계획, 여권, 신용카드, 은행카드 등과 같은 개인의 신원을 증명할 수 있는 신분증의 사용이 늘어나고 있다. 그러나 프린터, 스캐너, 복사기, 컴퓨터 관련 장치들과 각종 소프트웨어 기술의 발달로 인해 화폐, 각종 신용카드 뿐만 아니라 컴퓨터 칩과 같은 제조품의 위조 및 복제기술의 수준이 높아져 국내외적으로 이로 인한 피해액이 년간 수십 억 달러에 이르고 있는 실정이다. 이에 따라 최첨단 컴퓨터, 디지털 및 광학 기술들을 이용하여 위조 방지 시스템에 관한 연구가 전세계적으로 활발히 이루어지고 있지만 위조 및 복제 기술을 훨씬 능가하는 완벽한 보안시스템은 개발되지 않고 있다. 그러므로 위조나 복제에 대한 방지 기술은 반드시 연구, 개발되어야 한다.

광은 고유의 병렬성과 고속성을 가지므로 많은 양의 정보를 처리할 수 있고, 정보를 표현할 수 있는 방법이 다양하여 기존의 광 세기 검출기를 이용하더라도 복제할 수 없는 특징이 있으므로 차세대 정보보호 기술에 이용될 수 있다. 그러나 이러한 광 정보보호 기술을 완벽하게 지원해 줄 수 있는 소자들의 미개발로 인해 산업분야에 널리 활용되지 못하고 있으며, 이에 대한 연구가 세계적으로 활발하지 못한 실정이다. 하지만, 미래에는 현재 사용되고 있는 모든 정보보호 방법 및 기술들이 광 정보보호 기술로 대체될 것으로 확신한다.

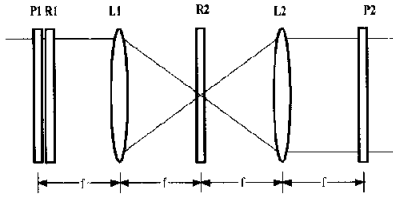
본 논문에서는 간접 위리에 기반한 컴퓨터형성홀로그램(computer generated hologram: CGH)과 광굴절매질을 이용하여 광 정보 보호 시스템을 구현하고자 한다. 암호화과정은 영상 정보를 손실없이 재생할 수 있는 이진 위상 홀로그램을 생성하고, 이를 암호화할 영상으로 간주한다. 이 홀로그램 영

상은 랜덤하게 발생된 이진 위상 영상으로 암호화된다. 키정보인 기준영상 또한 암호화된 영상으로부터 간접규칙을 적용하여 생성한다. 복원시에는 암호화된 영상과 기준 영상과의 간섭에 의해 간접세기를 인고, 간접세기정보를 위상정보로 변환한 후, 이를 역푸리에 변환함으로써 원래의 영상을 얻는다. 이때 두 영상의 간섭에 의해 생성되는 세기 정보는 주위의 진동에 상당히 민감하다. 이를 광굴절매질인 BaTiO₃의 SPPCM(self pumped phase conjugate mirror)특성을 이용하여 안정된 간접 푸리에 인고자 한다. 제안된 방법에서 누 랜덤 위상 영상(암호화된 영상, 기준 영상)은 원영상의 홀로그램에 대한 정보가 전혀없고, 기준 영상 정보가 없으면 복호화할 수 없다. 이와 같은 위상 정보는 육안이나 현미경으로 볼 수 없고, CCD 카메라로 복사할 수 없으므로 복제가 불가능하다. 제안된 정보보호 시스템은 원래의 영상을 암호화하는 것이 아니라 영상에 대한 홀로그램을 암호화하므로 두 번 암호화한 효과가 있으므로 정보보호를 필요로 하는 정부기관이나 산업체에 응용될 수 있을 것이다.

II. 기존의 광학적 영상 암호화 방법

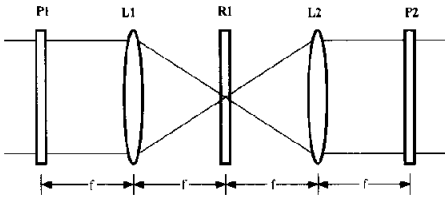
기존의 광학적 영상 암호화 방법 중 가장 널리 연구되고 있는 방법으로는 Refregier가 제안한 그림 1과 같은 4f 광상관기를 이용하여 입력 평면과 푸리에 평면에 랜덤위상 마스크를 사용하여 영상을 암호화하는 방법⁽¹⁾이다. 즉, 두 랜덤 마스크중 하나는 입력 평면에, 다른 하나는 공간 주파수 평면에 위치해서 궁극적으로 원영상이 stationary 백색잡음(white noise)형태로 변환되며, 복원 시스템에서는 암호카드 영상을 광학적으로 푸리에 변환한 후, 변환된 값에 암호키에 해당하는 랜덤 위상 마스크의 공액 복소값을 곱하게 된다. 그리고 그 결과를 광학적으로 다시 역푸리에 변환하여 검출기가 위치해 있는 평면에서 원영상을 복구하게 된다. 영상 복원 시스템은 그림 2와 같다. 그러나 이 방법은 암호화된 영상이 복소수 값을 가지므로 카드를 제작하기 어려운 뿐 아니라 복소수값을 나타낼 수 있는 실시간 공간광변조기(SLM; spatial light modulator)가 요구되는 문제점이 있다. 한편, Javidi는 더 단순한 방법으로 원영상 위에 랜덤 위상 마스크를 집착시킴으로써 영상을 암호화하고 그 위상 마스크의 푸리에 변환된 영상의 공액 복소 값을 푸리에 평면에서 곱하고 역푸리에 변환해서 영상을 복원하는 방법⁽²⁾을 제시하였다. 심각한 단점은 영상에 부착된 위상 마

스크를 영상에 손상을 주지 않으면서 교묘하게 떼어 내면, 카드의 위조가 가능해 진다는 것이다.



P1 : Input image
R1, R2 : Phase mask
P2 : Encrypted image
L1, L2 : Fourier lens

그림 1. Refregier가 제안한 영상 암호화 시스템



P1 : Encrypted image
R1 : Key card
P2 : Decrypted image

그림 2. Refregier가 제안한 영상 복원 시스템

최근에는 암호화된 정보를 단순화하여 정확하게 표현할 수 있고, 또한 쉽게 구현할 수 있는 광 정보 보호 시스템 구현하려는 연구들이 많이 진행되고 있다.^[3-4] 국내에서도 광학적으로 영상 암호화 및 복원 기법에 대한 연구가 일부에서 진행되고 있는데, 그 중 하나가 홀로그래픽 기법을 이용하여 영상 정보를 암호화하고 복원할 수 있는 방법이다.^[5] 이 방법에서는 기존의 방법과 큰 차이가 없으며, 방법 과정에 디지털 처리가 들어가고, 복원시 영상 주변에 많은 잡음이 생성되는 단점이 있다. 이외에도 XOR 연산을 이용하는 방법과 phase-contrast 기술을 이용한 방법 등이 광학적 영상 암호화에 사용되었다.

Han은 원영상을 bit-plane으로 각각 나누어 암호화 키와 XOR 연산을 수행함으로써 영상을 암호화하는 방법^[6]을 제시하였다. 그러나 이 방법은 시스템이 복잡하고 영상을 bit-plane으로 변환하기 위해 디지털적인 처리가 필요하므로 광학적 장치만으로는 구현이 불가능한 단점이 있다.

그리고, Neto는 영상 암호화를 위한 위상 마스크 제작에 phase-contrast 기술과 랜덤 위상을 이용

하였다. 암호화할 입력 영상을 위상 정보로 변환하고, 다시 랜덤 발생시킨 위상 정보와 더한 후 이를 감광매질에 기록하였고, 복원할 때에는 랜덤 위상 정보의 복소 공액을 곱한 후, phase-contrast 기술을 이용하여 원래의 영상을 복원하였다.^[7] 이 방법은 암호화 시 반복적인 알고리즘을 사용하지 않으므로 시간은 단축되지만 phase-contrast 기술 적용할 때 세기에 비례하는 위상값의 근사식에 대한 에러가 복원영상의 왜곡으로 나타나게 된다.

III. 제안한 광 정보보호 시스템

1. 홀로그램과 간섭을 이용한 영상 암호화

1-1. SA 알고리즘을 이용한 컴퓨터형성홀로그램 설계

1948년 Gabor에 의해 제시된 홀로그램은^[8] 물체에 의해 산란된 파면의 크기와 위상정보를 기준과 간섭을 통하여 세기의 형태로 기록한 것이며, 이를 통하여 물체의 영상 정보를 충실히 재현할 수 있다. 특히 CGH는 회절이론에 의한 수학적 연산을 통해 이상적인 간섭 파면을 계산하여 기록한 것이다. 연속정보의 CGH 제작은 기록소자의 해상도 제한, 정보의 저장 및 전송에서 많은 문제점이 있으므로 정보의 이진화가 요구된다. 그러나 연속정보를 이진화하면 정보의 손실이 발생하고, 영상재생시 양자화 잡음으로 나타난다. 이를 해결하는 여러 방법들 중 최적의 해를 구할 수 있는 방법인 SA(simulated annealing)알고리즘이다.^[9]

통계열역학에서 비롯된 SA 알고리즘은 복잡한 최적해를 풀기 위한 반복적인 알고리즘으로써 국소 최적해에서 벗어날 수 있는 반면 많은 반복과정을 수행해야 하므로 시간이 많이 소요된다. 본 논문에서는 SA 알고리즘을 이용하여 암호화할 원영상에 대한 최적의 이진 위상 홀로그램을 설계하였다. 원영상 함수 $h(x,y)$ 는 SA 알고리즘을 통해 설계된 이진 위상 홀로그램 $H(u,v)$ 을 푸리에 변환 하므로써 얻을 수 있다. 각 함수는 $N \times N$ 화소들로 구성 되어 있으며, 이들의 이산적인 표현은

$$h_{mn} = \frac{1}{N^2} \sum_{k=-N/2}^{N/2-1} \sum_{l=-N/2}^{N/2-1} \times H_{kl} \exp\left(j2\pi\left(\frac{km}{N} + \frac{ln}{N}\right)\right) \quad (1)$$

와 같다. 여기서 H_{kl} 는 $H(u,v)$ 의 (k,l) 번째 표본화 값이며, h_{mn} 는 $h(x,y)$ 의 (m,n) 번째 표본화 값이다. 원영상 생성을 위해 SA 알고리즘에서 사용된 비용함수를 제한된 영역내에서 목표영상과 재

생된 영상 사이의 평균자승오차 E 로 정의하였다.

$$E = \frac{1}{AB} \sum_{m=m_0}^{m_0+A-1} \sum_{n=n_0}^{n_0+B-1} \eta_t \times | |f_{mn}|^2 - |h_{mn}|^2 |^2 \quad (2)$$

여기서 η_t 는 목표 효율을 나타내고, A 와 B 는 각각 목표영상의 가로 및 세로의 크기를 나타내며, f_{mn} 는 목표영상의 전체 에너지를 나타낸다. 이 비용함수는 제한된 영역내에서 목표영상을 찾아가도록 함으로써 관심영역 밖의 배경잡음을 줄여 더욱 높은 효율을 가질 수 있게 한다. 이전 위상 홀로그래프의 최적설계를 위한 SA 알고리즘의 순서도는 그림 3과 같으며, 수행과정은 H_{kl} 의 초기값을 '1', 또는 '-1'로 무작위 선택하고, 비용함수 E^{old} 를 계산한 후, 이로부터 SA 알고리즘에 사용되는 초기온도 T_{init} , 냉각속도 D_t , 그리고 반복횟수 N 를 결정한다. H_{kl} 의 한 화소를 1에서 -1로 또는 -1에서 1로 바꾼후 비용함수를 새로이 계산한다. 만약 바꾼 화소값에 의해 새로이 계산된 비용함수가 감소하면 그 변화를 무조건 받아들이고, 그렇지 않으면 무조건 배척하는 것이 아니라 다음과 같은 확률을 도입하여 조건적으로 받아들인다.

$$P(\Delta E) = \exp(-\Delta E / T_n), \quad (3)$$

$$T_n = (D_t)^n T_{init}$$

여기서 P 는 수용 확률을 나타내고, ΔE 는 비용함수의 변화량을 나타낸다. 그리고 T_n 는 n 번째 반복 과정에서의 온도를 나타내는 매개 변수이다. 위의 과정이 모든 화소에 대하여 반복 수행된다. 홀로그래프를 구성하는 모든 화소들이 선택되면 한 번의 반복 과정이 끝나게 되고, 위에서 설명한 일련의 과정을 반복 횟수 만큼 수행하게 된다.

1-2 간섭 이론

초기 위상이 ϕ , 주파수가 ω , 전파 상수가 k 이고 z 방향으로 진행하는 평면파는

$$E = E_0 \cos(kz - \omega t + \phi) \quad (4)$$

와 같이 표현되고, 같은 방향(z)으로 진행하는 두 파동을 각각 E_1, E_2 라고 하면 어느 주어진 시각에서 두 파동의 합성은

$$E = E_1 + E_2 = E_{01} \cos(kz_1 - \omega t + \phi_1) + E_{02} \cos(kz_2 - \omega t + \phi_2) \quad (5)$$

이 된다. 이러한 파동이 가지는 조도 I 는

$$I = \epsilon \nu \langle E^2 \rangle \quad (6)$$

이다. 여기서, $\langle \rangle$ 는 시간적 평균값을 의미한다.

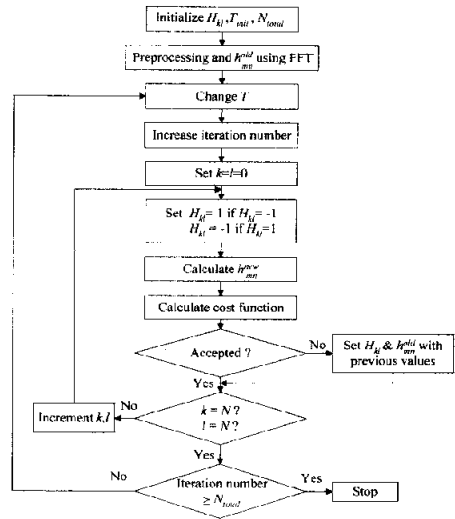


그림 3. 이전 위상 홀로그래프의 최적설계를 위한 SA 알고리즘의 순서도

그런데 $\epsilon \nu$ 는 상수이므로 균일한 매질내에서 밝기만을 비교하면 I 는 파동을 각각 E_1, E_2 라고 하면 어느 주어진 시각에서 두 파동의 합성은

$$E = E_1 + E_2 = E_{01} \cos(kz_1 - \omega t + \phi_1) + E_{02} \cos(kz_2 - \omega t + \phi_2) \quad (5)$$

이 된다. 이러한 파동이 가지는 조도 I 는

$$I = \epsilon \nu \langle E^2 \rangle \quad (6)$$

이다. 여기서, $\langle \rangle$ 는 시간적 평균값을 의미한다. 그런데 $\epsilon \nu$ 는 상수이므로 균일한 매질내에서 밝기만을 비교하면 I 는

$$I = \langle E^2 \rangle = \langle (E_1 + E_2)(E_1 + E_2) \rangle = \langle E_1^2 \rangle + \langle E_2^2 \rangle + 2 \langle E_1 E_2 \rangle = I_1 + I_2 + I_{12} \quad (7)$$

와 같이 된다. 여기서 간섭항 I_{12} 를 구해보면

$$I_{12} = E_{01} E_{02} \times \cos[k(z_1 - z_2) + (\phi_1 - \phi_2)] \quad (8)$$

이 되고, $I_i (i=1, 2)$ 는

$$I_i = \langle E_i^2 \rangle = \frac{1}{2} E_{0i}^2 \quad (i=1, 2)$$

이 된다. 따라서

$$I = I_1 + I_2 + 2\sqrt{I_1 I_2} \times \cos[k(z_1 - z_2) + (\phi_1 - \phi_2)] = I_1 + I_2 + 2\sqrt{I_1 I_2} \cos \Delta \quad (9)$$

$$\Delta = k(z_1 - z_2) + (\phi_1 - \phi_2)$$

그러므로 두 빛을 간섭시킨 결과는 각 빛의 밝기를 더한 밝기 ($I_1 + I_2$)와 다름을 알 수 있다. 간섭 무늬의 밝기는 위상차 Δ 값에 의하여 결정되며, 이를 그림 4에 나타내었다.

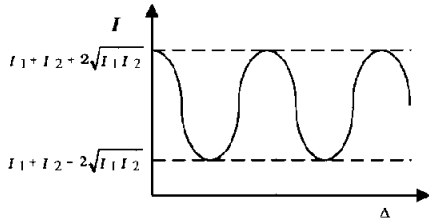


그림 4. 위상차에 따른 간섭 무늬의 최대 및 최소값.

최대값은 보강간섭에 의해 각각의 밝기를 더한 값보다 큰 값인 ($I_1 + I_2 + 2\sqrt{I_1 I_2}$)으로, 최소값은 상쇄간섭에 의해 ($I_1 + I_2 - 2\sqrt{I_1 I_2}$)로 구해진다. 최대값이 가장 크고, 최소값이 가장 작아지는 즉 대비도(contrast)가 가장 좋은 조건은 두 빛의 밝기가 같은 때이고, 이 때 각 빛의 밝기를 I_0 라 하면 식 (9)는 다음과 같이 표현할 수 있다.

$$I = 2I_0(1 + \cos \Delta) = 4I_0 \cos^2\left(\frac{\Delta}{2}\right) \quad (10)$$

따라서 이 경우, 최대값은 각 빛 밝기의 4배가 되며, 최소값은 0이 된다. 이러한 두 빛의 간섭이 일어나기 위해서는 두 빛의 편광 방향이 동일해야 하고, 위상차가 일정하게 유지되는 가간섭 광원이어야 한다.⁽¹⁰⁾ 본 논문에서는 수평 편광된 가간섭 광원인 He-Ne 레이저를 사용하고 Mach-Zehnder 간섭계를 구성함으로써 이러한 두 빛의 간섭 현상을 이진 위상 홀로그래프의 암호화 및 복원에 이용하였다.

1-3 영상 암호화

본 논문에서 제안한 암호화 방법은 원래의 영상정보를 암호화 시키는 것이 아니라 원영상의 홀로그래프 정보를 암호화 시키는 것으로 그 과정은 그림 5와 같다. 홀로그래프는 그 정보의 일부를 잃어도 원영상을 복원할 수 있는 성질이 있으므로 정보의 전송과 정에서 생길수 있는 각종 잡음 등에 상당히 둔감하다. 먼저 원영상 정보를 손실없이 재생할 수 있는 이진 위상 홀로그래프를 SA 알고리즘을 이용하여 생성한다. 이를 암호화하기 위하여 암호키로 사용될 기준영상을 랜덤하게 발생시킨 이진 위상으로 정하고, 이를 간섭이론에 근거한 표 1의 규칙을 적용하면 홀

로그래프에 대한 암호화 영상을 구할수 있다.

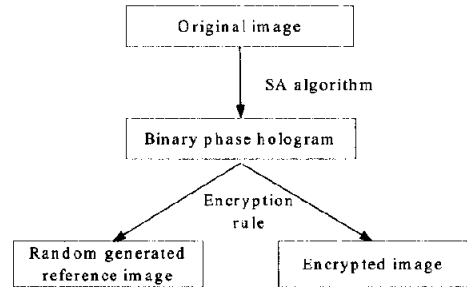


그림 5. 영상 암호화를 위한 블록도.

간섭이론에서처럼 기준 영상과 암호화된 영상을 구성하고 있는 각 화소에서의 위상차를 반과장의 짝수 배 또는 홀수 배로 차이나게 하여 두 성분만을 가지는 홀로그래프 간섭 정보를 만들어 낼 수 있다. 만약 두 영상내 각 화소의 위상차를 다중 레벨로 한다면 연속적인 간섭무늬를 얻을 수 있고, 이로부터 연속적인 홀로그래프 정보를 얻을 수 있어 보다 원영상에 가까운 정보를 복원할 수 있을 것이다.

표 1. 홀로그래프 간섭 정보에 대한 기준 영상과 암호 영상의 위상값

Interference intensity	Reference image	Encrypted image
0	0	π
	π	0
1	0	0
	π	π

2. 영상 복호화

Mach-Zehnder 간섭계의 두 경로에 암호화된 영상과 기준영상을 두면 두 영상을 구성하고 있는 각 화소들의 위상값에 따라 홀로그래프 정보를 가지는 간섭 세기 패턴이 나타난다. 이 세기 정보를 LCD와 같은 위상변조기를 이용하여 위상 성분으로 바꾼 후, 이들 역푸리에변환하면 원영상을 복원할 수 있다. 이 과정을 그림 6에 나타내었다. 이때 생기는 간섭 무늬는 주위의 진동에 상당히 민감하므로 이를 안정화 시킬수 있는 방법이 필요하다. 두 랜덤 위상 영상(암호화된 영상, 기준 영상)은 홀로그래프 영상에 대한 정보가 전혀없고, 기준 영상 정보가 없으면 복호화할 수 없다. 이와 같은 위상 정보는 육안이나 현미경으로 볼 수 없고, CCD 카메라와 같은 세기 검출기를 이용하여 복제할 수도 없다.

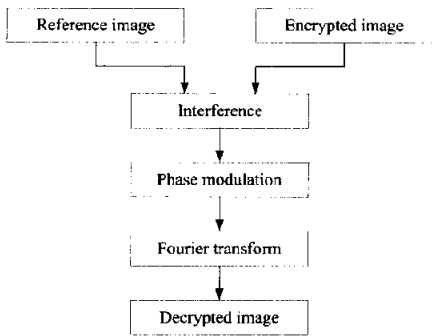


그림 6. 영상 복호화를 위한 블록도

3. SPPCM을 이용한 안정한 간섭패턴

간섭계를 이용하는 작업에서 가장 중요한 요구사항은 간섭 필드의 안정성을 높게 유지하는 것이며, 이는 안정된 간섭패턴을 이용한 측정에 있어서 정밀성을 확보해 주기 때문이다. 그러나 온도 변화 또는 진동 등과 같은 환경적 영향에 따라 위상 변동이 생긴 때 간섭패턴의 대비도가 감소되거나 간섭 모양이 시리지게 되고 결과적으로 측정 오차가 발생한다. 이러한 위상 변동 영향으로 발생하는 오차를 줄이기 위해 본 논문에서는 광굴절 매질인 BaTiO₃의 SPPCM특성을 이용하는 방법을 제안하였다. 진동에 의해 생길수 있는 간섭무늬의 변화를 BaTiO₃ 매질에 적절한 각도로 입사시켜주면 매질내에서 빔의 패닝현상과 전반사에 의해 입사빔과 반대 방향으로 되돌아 나오는 빔은 입사빔의 위상공액 및 시간 평균된 결과가 되므로 진동과 같은 위상 잡음이 존재할 때에도 원하는 깨끗한 간섭무늬를 얻을 수 있다.

IV. 시뮬레이션 및 실험 결과

본 논문에서 제안한 이중 암호화/복호화 방법에 의한 결과를 검증하기 위해 컴퓨터 시뮬레이션 및 광실험을 하였다. 먼저 암호화할 영상을 결정한 후, 이 영상에 대한 이진 위상 홀로그래프를 SA 알고리즘을 이용하여 설계하였다. 이 홀로그래프 정보를 랜덤 이진 위상 발생기 및 간섭 원리에 근거하여 암호화 하였다. 그림 7은 간단한 이진 문자 정보에 대한 암호화 결과이며, 그림 8은 Lena 영상의 눈 부분만을 취한 명암도 영상(gray image)에 대한 암호화 결과를 나타낸다. 그림 7, 8의 (b), (c) 그리고 (d)에서 검은 화소 부분은 위상이 ' π '이고, 흰 화소 부분은 '0'을 나타낸다. (c), (d) 영상의 각 화소에서 위상값이 같으면 보강간섭에 의해 간섭세기가 밝

고, ' π '만큼 차이가 나면 상쇄간섭에 의해 어둡게 되어 (b)와 같게 된다.

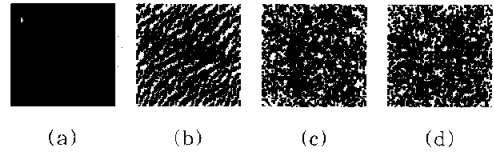


그림 7. 이진 영상에 대한 홀로그래프 및 암호화 결과 (a) 원영상, (b) 이진 위상 홀로그래프, (c) 암호화된 영상, (d) 기준영상

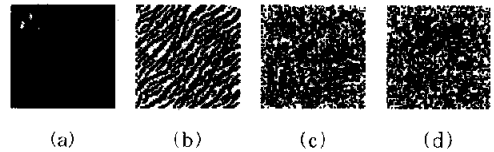
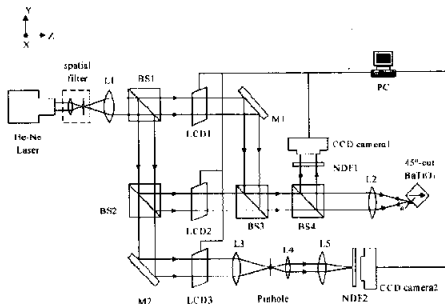


그림 8. 명암도 영상에 대한 홀로그래프 및 암호화 결과 (a) 원영상, (b) 이진 위상 홀로그래프, (c) 암호화된 영상, (d) 기준영상

이와 같이 얻어진 세기 정보는 LCD와 같은 위상 변조기에 의해 두 위상 성분으로 변조될 수 있다. 제안한 암호화 방법에서는 많은 정보량을 가지는 명암도 영상도 두 위상 성분으로 쉽게 암호화 될 수 있어 정보전송 분야에도 효과적으로 응용될 수 있을 것으로 기대된다. 컴퓨터 시뮬레이션을 통해 얻은 홀로그래프 정보에 대한 암호화 영상과 키(key) 정보 역할을 하는 기준영상을 이용하여 실시간 적으로 복호화할 수 있는 광 복호화 시스템의 구성도는 그림 9와 같다. 복호화 실험하기 전에 LCD의 위상 변조 능력을 알아보기 위해 Mach Zehnder 간섭 실험을 하였으며, 그 결과를 그림 10에 나타내었다. Mach-Zehnder 간섭계의 한쪽 경로에 인가되는 입력 영상의 미디오 레벨에 따라 간섭 무늬의 어긋나는 정도가 변화는 것으로 보아 LCD가 위상 변조 능력이 있음을 확인하였으며, '0'레벨일 때 ' π '만큼의 위상변화가 있음을 알 수 있다. 즉 LCD에 밝기 정보를 인가하면 위상 정보로 변조된다. 그림 7, 8의 암호화된 영상을 광학적으로 복호화 하기 위해 암호화된 영상과 이를 복호화할 수 있는 키 정보인 기준영상을 간섭계 내의 LCD1과 LCD2에 각각 입력하였다. 이들 두 영상에 의한 간섭패턴이 BS3과 BS4 사이에서 나타나는데, 주위의 진동에 상당히 민감하다. 그래서 생성된 간섭계를 다시 광굴절매질인 BaTiO₃에 입사시켜 매질의 SPPCM 특성에 의해 반사되는 빔을 광세기 검출기인 CCD 카메라에서 획득하여 안정된 간섭무늬를 얻을 수 있도록 시스템을 구성하였다.



L : lens M : mirror
 BS1 : beam splitter (50 : 50)
 BS2 : beam splitter (65 : 35)
 NDF : neutral density filter
 PC : personal computer
 LCD1 : reference image
 LCD2 : encrypted image
 LCD3 : binary phase hologram

그림 9. 제안된 안전한 복호화 시스템



그림 10. LCD의 위상 변조 실험 결과 (a) 입력 영상 (192, 128, 0 레벨), (b) 그림 7(a)에 의한 간섭 패턴

그리고 이 간섭계를 LCD3에 다시 입력하여 위상 변조시키면 렌즈 L3, L4 그리고 L5의 조합에 의해 푸리에 변환이 되어 원래의 영상이 복원된다. 이때 암호화된 영상과 기준 영상은 위상 정보만을 가지므로 복사하기 어렵고, 만약 기준 영상 정보를 모른다면 암호화된 영상 정보를 복원할 수 없다. 복호화 실험하기 전에 BaTiO₃의 SPPCM 특성을 이용함으로써 간섭계가 진동에 안정한지 여부를 먼저 실험하였고, 그 결과를 그림 11에 나타내었다. 실험결과를 보면 진동이 존재하는 환경에서 광굴절 매질인 BaTiO₃를 이용함으로써 안정한 간섭무늬를 얻을 수 있음을 알 수 있다.

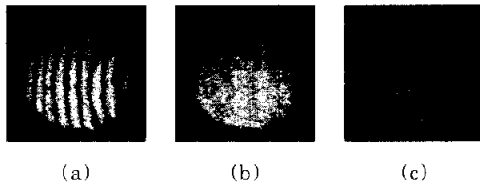


그림 11. SPPCM을 이용한 위상잡음 제거 실험에서의 결과 영상 (a) 진동이 없을 때 (b) 진동이 존재할 때 (c) SPPCM을 이용해서 얻은 결과 영상

이와 같이 얻어진 간섭계기는 다시 LCD3과 같은 위상변조기를 통해 위상 성분으로 변조되고, 렌즈들의 조합을 통해 역푸리에 변환함으로써 원영상을 복원할 수 있다. 컴퓨터 시뮬레이션 및 광실험을 통해 복호화된 결과들을 그림 12, 13, 그리고 14에 나타내었다.

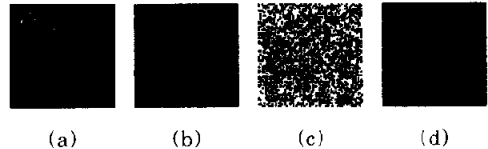


그림 12. 컴퓨터 시뮬레이션을 통한 복호화된 이진 영상 (a) 정확한 기준 영상을 사용했을 때, (b) 기준 영상이 없을 때, (c) 틀린 기준 영상, (d) 틀린 기준 영상을 사용했을 때

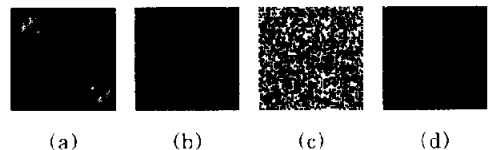


그림 13. 컴퓨터 시뮬레이션을 통한 복호화된 이진 영상 (a) 정확한 기준 영상을 사용했을 때, (b) 기준 영상이 없을 때, (c) 틀린 기준 영상, (d) 틀린 기준 영상을 사용했을 때

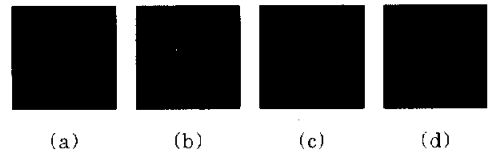


그림 14. 광실험을 통한 복호화된 영상 (a) 정확한 기준 영상을 사용했을 때, (b) 기준 영상이 없을 때, (c) 틀린 기준 영상(그림 8(c))을 사용했을 때, (d) 틀린 기준 영상(그림 9(c))을 사용했을 때

컴퓨터 시뮬레이션 및 광실험 결과에서 정확한 기준영상을 사용했을 경우에만 원영상에 가까운 영상들이 복호화되고, 기준영상이 입력되지 않거나 틀린 기준영상이 입력되면 원영상이 복호화되지 않음을 확인할 수 있다. 복호화된 영상에서 원래의 영상 외에 역상이 나타나는 것은 위상 홀로그램의 정보가 이진으로 구성되어 있기 때문이며, 다중 위상 정보로 홀로그램을 설계하고, 암호화한다면 그 역상을 없앨 수가 있어 출력 대역폭을 넓게 활용할 수 있으며, 효율 또한 개선시킬 수 있다. 그러나 다중 위상으로 표현하게 되면 홀로그램을 설계하는데 많은 시간이 소요된다. 그림 14의 광실험 결과에서 재생되는 영상의 위치가 컴퓨터 시뮬레이션 결과와 차이가 나는 것을 볼 수 있는데, 이는 광실험시 LCD에 입력되는 데이터가 위치 변편되었기 때문이라고 판단되며, 실험전에 이를 고려하여 입력하면 컴퓨터 시뮬레이션 결과와 같은 결과를 얻을 수 있다.

V. 결 론

본 논문에서는 간섭원리에 기반한 컴퓨터형성홀로그램과 광결절매질인 BaTiO₃의 SPPCM특성을 이용한 안정한 광 정보보호 시스템을 구현하였다. 제안된 방법의 암호화과정은 원영상 정보를 암호화하는 것이 아니라 먼저 원영상을 손실없이 재생할 수 있는 이진 위상 홀로그램을 설계하고, 이를 암호화할 영상으로 간주하였으며, 설계된 홀로그램의 암호화를 위해 랜덤하게 발생시킨 이진 위상 정보를 기준영상으로 하고, 간섭규칙에 근거하여 홀로그램 정보를 암호화 하였다. 복호화과정은 암호화된 영상과 기준영상과의 간섭을 통해 간섭세기 무늬를 얻고, 이를 다시 LCD를 이용하여 위상만을 가지는 이진 위상 홀로그램 정보로 변환한 후, 역푸리에 변환함으로써 원영상을 얻을 수 있었으며, 간섭무늬 획득 시 주위 진동에 상당히 민감하다는 단점을 광결절매질인 BaTiO₃의 SPPCM의 특성을 이용함으로써 안정된 간섭무늬를 얻을 수 있었다. 제안된 방법은 암호화 및 복호화 과정이 간단하고, 암호화된 정보가 위상만을 가지므로 육안으로 볼 수 없으며, CCD카메라 등에 의해 복제할 수도 없을 뿐만 아니라 두 번의 암호화 효과가 있어 정보보호를 필요로 하는 여러 분야에 응용될 수 있을 것이다.

참 고 문 헌

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 32, no. 7, pp. 767-769, 1995

[2] B. Javidi and J. L. Honer, "Optical pattern recognition for validation and security verification", *Optical Engineering*, vol.33, no. 6, pp. 1752- 1756, 1994

[3] P. C. Mogensen and J. Gluckstad, "Phase-only optical decryption of a fixed mask", *Applied Optics*, vol. 40, no. 8, pp. 1226-1235, 2001

[4] J. Ohtsubo and A. Fujimoto "Practical image encryption and decryption by phase-coding technique for optical security systems" *Applied Optics*, vol. 41, no. 23, pp. 4848-4855, 2002

[5] 양훈기, 정대섭, 김은수, "홀로그래픽 영상 암호

화 및 디코딩 기법", *대한전자공학회 논문지*, 제 33권 12호, pp. 97-103, 1996

[6] J. W. Han, C. S. Park, D. H. Ryu, and E. S. Kim, "Optical image encryption based on XOR operations," *Optical Engineering*, vol 38, no 1, pp. 47-54, 1999

[7] L. G. Neto, "Implementation of image encryption using the phase-contrast technique," *Proceedings of SPIE*, vol. 3386, pp. 284-290, 1998

[8] J. W. Goodman, *Introduction to Fourier Optics*, Chapter 8, McGraw-Hill, New York, 2nd Ed., 1996

[9] C. S. Kim, D. H. Kim, J. W. Kim, J. K. Bae, and S. J. Kim, "Real time optical image generation using phase grating with simulated annealing algorithm," *Journal of IEEK*, vol. 32-A, pp. 149-155, June, 1995

[10] E. Hect, *Optics*, Chapter 9, Addison-wesely, Reading, Mass., 3rd ED., 1997

김 철 수(Cheol-Su Kim) 정회원
한국통신학회 논문지 제 28권 5C호 참조
현재 경주대학교 컴퓨터전자공학부 조교수

김 종 윤(Jong-Yun Kim) 정회원
1995년 2월 : 경북대학교 전자공학과(공학사)
1997년 2월 : 경북대학교 전자공학과(공학석사)
2001년 2월 : 경북대학교 전자공학과(공학박사)
현재 경동대학교 정보통신공학부 교수
<주관심분야> 광암호화, 광신호처리 등

박 영 호(Young-Ho Park) 정회원
1989년 경북대학교 전자공학과(공학사)
1991년 경북대학교 대학원 전자공학과(공학석사)
1995년 경북대학교 대학원 전자공학과(공학박사)
현재 : 상주대학교 전자전기공학부 부교수
<주관심분야> 정보보호, 이동통신 등

조 창 섭(Chang-Sop Cho) 준회원
한국통신학회 논문지 제 28권 5C호 참조
현재 경북대학교 전자공학과 박사과정

김 수 중(Soo-Jung Kim) 정회원
한국통신학회 논문지 제 28권 5C호 참조
현재 경북대학교 전자전기공학부 교수