시각 암호와 간섭계를 이용한 광 암호화

Optical Encryption based on Visual Cryptography and Interferometry

이상수, 서동환, 김종윤, 박세준, 신창목, 김수중, 박상국*
경북대학교 전자공학과, *포항산업과학연구원
amuro73@hotmail.com

Abstract

In this paper, we proposed an optical encryption method based in the concept of visual cryptography and interferometry. In our method a secret binary image was divided into two sub-images and they were encrypted by 'XOR' operation with a random key mask. Finally each encrypted image was changed into phase mask. By interference of these two phase masks the original image was obtained. Compared with general visual encryption method, this optical method had good signal-to-noise ratio due to no need to generate sub-pixels like visual encryption.

글로벌화 되어가는 현대 사회에서 자원과 정보의 공유는 산업과 학문 전반에 걸쳐 커다란 화두이며 이에 대한 여러 가지 방안들이 연구되어 왔다. 그러나 이러한 정보공유의 필요성이 커질수록, 한편으로 공유의 권한을 특정 인물들에 국한하여 불법적인 접근으로부터 정보를 보호하기 위한 연구도 활발히 진행되고 있다. 여기에는 개인 인증을 통해 저장된 정보에 대한 접근권을 확인하는 방법들[1]과 이와는 달리 처음부터 어떤 정보를 고르게 분산시켜 허가된 인물들에게만 배포한 후, 이들의 합의를 통해서만 정보를 확인할 수 있는 방안등이 있다. 후자의 방법중 가장 대표적인 것이 시각 암호화(Visual Encryption)이다.[2]

본 논문에서는 시각 암호화와 빛의 간섭성을 이용한 암호화 방식[3]을 적용하여 어떤 영상을 분할하여 암호화하고 이를 다시 복원하는 새로운 방식을 제안하였다. 즉 한 영상을 두 개의 분할된 이진 위상의 암호화 영상으로 변환한 후 이들의 간섭현상을 이용해 원 영상을 재생할 수 있다. 우선 암호화 과정에서 암호화 하고자 하는 이진 영상을 시각 암호화의 개념에 따라 두 개의 이진 영상으로 분할한다. 이때 일반적인 시각 암호화 방식과는 달리 원 화소에 대한 부화소를 따로이 생성시킬 필요가 없다. 이렇게 분리된 영상들은 임의로 생성된 랜덤키와 XOR 연산을 취하여 암호화된다. 마지막으로 이들 암호화된 영상들은 그 화소값(Black/White)에 대응되는 이진의 위상형태(π/0)를 가지는 이진 위상 카드로 제작되는데 여기에는 광학적 lithography를 이용할 수 있다. 이렇게 제작된 두 개의 이진 위상 카드는 원 영상을 균등하게 분할하여 나누어 가지고 가시적으로는 암호화된 위상의 패턴을 확인할 수 없다. 그리고 암호화에 사용되었던 랜덤키의 정보는 영상복원시 XOR 연산에 의해 소거되므로 랜덤키는 더 이상 필요치 않게 된다. 즉 두 장의 위상카드를 소지한 인물만이 원 영상과 복호화에 대한 키를 지니게 된다. 이들 두 위상 카드는 각각 상대 카드에 대해 복호화의 키가 되므로, 두 장이 한자리에 모이지 않는 한

원 영상을 복구하는 것은 불가능하다. 암호화된 영상의 복호화를 위해서는 두 장의 위상 카드를 각각 마흐첸더 간섭계의 간섭 경로상에 위치시킴으로써 이들의 위상간섭현상에 의해 원 영상을 복구할 수 있다. 두 위상카드의 대응화소가 동일 위상값일 때와 반대 위상 값일때의 서로 다른 간섭현상에 의해 원 영상을 재생할 수 있으며 이러한 위상 간섭현상을 광학적인 XOR 작용으로 볼 수 있다. 이렇게 재생된 영상은 원 영상과 동일한 화소수를 가지므로 일반적인 시각 암호화 방식과는 달리 원 영상에 비해 동일한 신호대잡음비를 가진다.

1. B. Javid and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33**, 1752-1756(1994)
2. M. Naor and A. Shamir, "Visual Cryptography," Advances in Cryptography-Eurocrypt' 94, **950**, 1-12(1995)
3. J. Kim, "Optical image encryption using interferometry-based phase masks," Electronics Letters **36**, 874-875(2000)

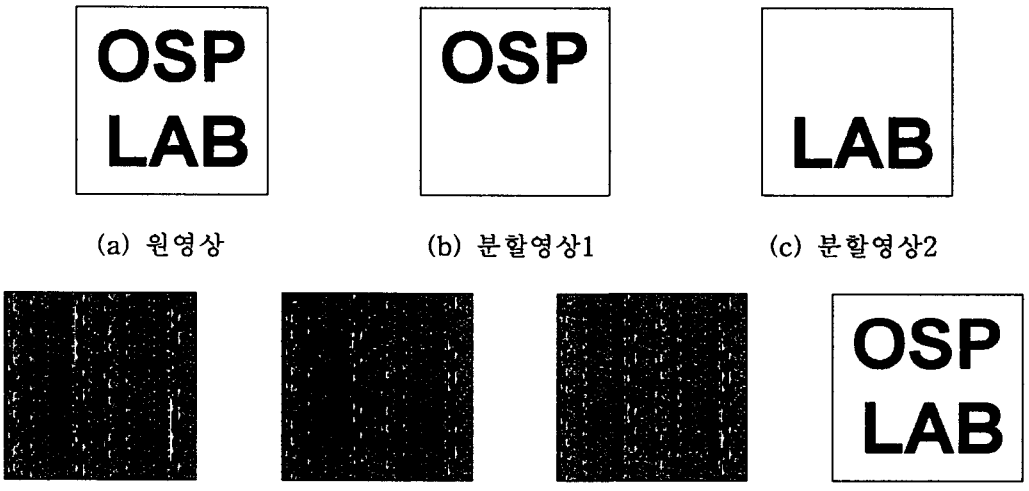

그림 1. 영상의 암호화 및 복호화 과정

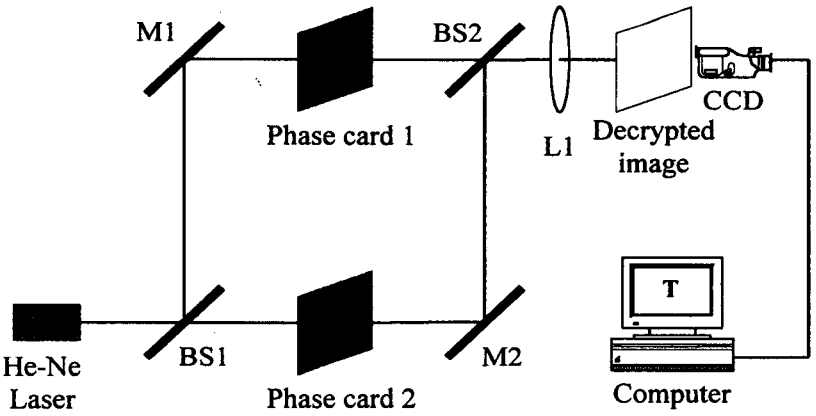

그림 2. 광학적 간섭계를 이용한 영상 복호화 시스템