광학적 간섭현상을 이용한 시각 암호화 기법

이 상 수, 김 종 윤, 박 세 준, 김 수 중, *김 정 우
경북대학교 전자전기공학부, *동양대학교 전자공학과
전화 : 053-940-8611 / 핸드폰 : 011-815-7511

Visual Cryptography based on Optical Interference

Sang Su Lee, Jong Yoon Kim , Se Joon Park, Soo Joong Kim, Jeong Woo Kim
Dept. of Electronic and Electric, KyungPook University
E-mail : amuro73@hotmail.com

Abstract

In this paper, we proposed a new visual cryptography scheme based on optical interference which improves the contrast and SNR of reconstructed images comparing with conventional visual cryptography method. We divided an binary image to be encrypted into *n* slides. To encrypt them, (*n*-1) random independent keys and one another random key by XOR process between four random keys were prepared. XOR between each divided image and each random key makes encrypted *n* encrypted images. From these images, encrypted binary phase masks can be made. For decryption all of phase masks should be placed together in the interferometer such as Mach-Zehnder interferometer.

I. 서론

현대 사회가 정보화 사회로 발전해 감에 따라, 이들 정보를 공유하기 위한 여러 가지 수단이 연구되어 왔으며, 여기에는 특정 정보를 허가되지 않은 개인이나 그룹에 의한 불법적인 접근과 사용으로부터 보호하기 위한 각종 보안 방안의 연구도 포함되어 있다. 일반적으로 회사나 주요 국가 기관 등에서는 제한된 정보의 접근을 제어하여 주는 보안 시스템을 사용하여 기밀 정보의 보호와 유출방지를 유지하고 있으며 심지어 일반 가정에서도 불법적인 침입 방지를 위하여 보안 시스템을 사용하는 경우가 늘어가고 있다. 이들 시스템에서는 접근을 허락 받은 개인의 각종 지문과 같은 자료를 암호화하고 이를 복원한 후 신원을 확인하는 방식이 주를 이루고 있다. 그러나 이러한 시스템은 불법적인 해킹 및 도청에 약하다는 단점이 있다. 즉, 사용자 중 한 사람이 시스템 접근을 위한 암호화 자료를 분실하거나, 아예 시스템 자체가 해킹 될 경우 심각한 정보유출 상황에 직면하게 된다. 현재 사용하고 있는 대부분의 보안 시스템은 자료를 중앙 집중화한 후, 사용자의 신원 확인에 따라 접근을 허용하는 이와 같은 방식이 주를 이루고 있다.

이와는 달리 처음부터 정보를 임으로 분할하여 이를 허가된 사용자들에게 배포한 후 이들의 합의에 의해서만 정보를 확인할 수 있는 방안도 연구되고 있다. 즉 군사분야 및 공동자산의 사용에서처럼 합의를 통한 정보 확인이 필요한 경우에 대해서는 앞서 언급한 것과는 다른 정보 보호 방법이 요구된다. 이러한 보안 방식에서는 어떤 사용자(혹은 정보 소유권자)가 자신의 소유 정보를 분실 혹은 해킹 당한다 하더라도 전체 정보는 확인 할 수 없으므로 일반적인 정보 보호 방식에 비해 안전한 장점을 지니게 되며, 이러한 보안 방식에 있어 가장 대표적인 것이 시각 암호화(Visual

Cryptography)이다.

본 논문에서는 빛의 간섭성을 이용한 시각 암호화 기법을 제안하였다. 즉, 어떤 이진 영상을 n개의 slides로 임으로 분할한 후 각각을 서로 다른 랜덤한 암호화 키와의 XOR 연산을 통해, 이들 slides를 암호화하고, 이를 다시 이진의 위상카드로 변환하여 정보 소유권자들에게 배포하게 된다. 원 영상을 복원하기 위해서는 정보 소유권자들의 공통된 합의하에 각 위상카드를 광학적인 간섭계에 위치시킨 후 이들의 간섭현상을 통해 영상을 복원해내게 된다. 이렇게 재생된 결과 영상은 기존의 시각 암호화방식을 통해 재생된 영상이 원 영상에 비해 해상도와 신호대잡음비가 저하되는데 반해, 원 영상과 동일한 해상도와 신호대잡음비를 가지게 된다.

Ⅱ. 시각 암호화

1979년 A. Shamir는 접근 권한이 동등한 회원으로 구성된 그룹에 적용하기 위한 평등한 비밀 분산법인 thresholding scheme을 제안하였으며, 이 후 thresholding scheme의 한가지 응용 형태인 시각 암호화 기법을 제안하였다. 기본적인 시각 암호화는 그림 1에서와 같이 두 장의 투명한 용지에 원 영상을 분산하여 구성하는 것으로 간단히 구현할 수 있으며 한 장을 암호 영상으로 선택하면 나머지 한 장은 키 영상이 된다. 복호는 더욱 간단하다. 암호 영상과 키 영상을 중첩시키면 원 영상이 나타난다.

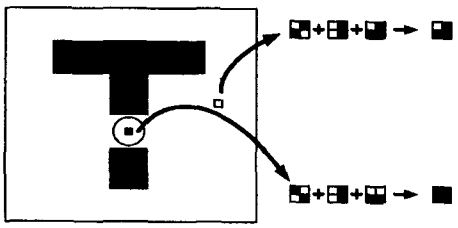


그림 1. 시각암호화 방법의 예시

이와 같이 시각 암호화는 별도의 복호 알고리듬을 수행하지 않고 단순히 인간의 시각으로 복호할 수 있으므로 암호에 대한 지식이나 이를 수행하기 위한 별도의 장치 없이도 간단히 사용할 수 있다는 장점이 있다. 이러한 장점에 비하여, 시각 암호의 특성상 원 영상의 분산 과정에서 생성되어지는 다수의 부화소에 의해 복원 영상의 해상도와 신호대잡음비가 감소하는 단점을 지니고 있다.

Ⅲ. 빛의 간섭현상

간섭성을 지니는 두 빛을 간섭계와 같은 구조를 통해 간섭을 일으킬 경우, 두 빛의 위상차에 따라 명암의 밝기가 달라지는 것을 확인할 수 있으며, 특히 두 빛의 위상차가 0 와 π일 경우 이들의 간섭 결과는 각각 백과 흑의 세기패턴으로 나타나게 된다. 즉, 두 빛 중 하나를 기준 광으로 볼 때, 다른 빛이 이와 동일한 위상을 지니면 그 간섭세기는 최대의 밝기를 나타내게 되고, 이와 반대로 π의 위상 차이를 갖게 될 경우, 가장 어두운 밝기를 나타내게 된다. 이러한 현상은 논리적인 XOR 연산과 아주 흡사한 것을 알 수 있다.

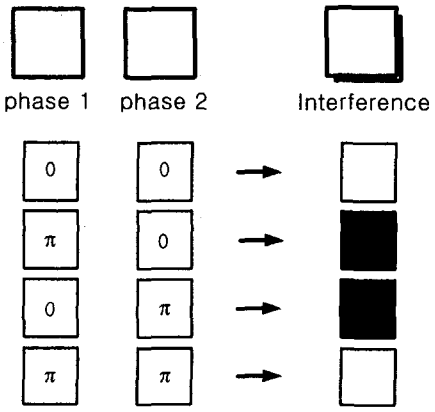


그림 2. 빛의 간섭현상

Ⅳ. 제안한 암호화 방법

본 논문에서는 앞서 언급한 시각 암호화에서의 부화소 생성과 이에 따른 해상도 및 신호대잡음비의 저하를 막기 위해 그림 3과 같은 광학적인 빛의 간섭현상을 이용한 새로운 암호화 방법을 제안하였다. 즉, 어떤 정보를 임의의 키와 논리적인 XOR 연산을 한 후, 동일한 키와 다시 한번 XOR시킬 경우, 원래의 정보를 복원할 수 있다는 사실을 이용하여, 어떤 비밀 영상을 임의의 개수의 slides로 분할 한 후, 이를 각각 서로 다른 랜덤한 암호화 키와의 XOR 연산을 통해 암호화한다. 이때 만약 전체 slides의 수가 n장일 경우, $(n-1)$장의 랜덤키를 생성시킨 후 이들 모두의 XOR에 의한 새로운 키를 하나 더 생성시킨다. 이렇게 생성된 n장의 암호화 키를 각각의 slide와 XOR시킴으로써 분할된 영상들을 암호화한다. 다음으로 암호화된 slides들이 가지는 흑/백 화소에 각각 $0/\pi$의 위상을 대응시킨

위상카드를 제작하게 되는데 여기에는 광학적인 리소그라피와 같은 방법을 이용한다.

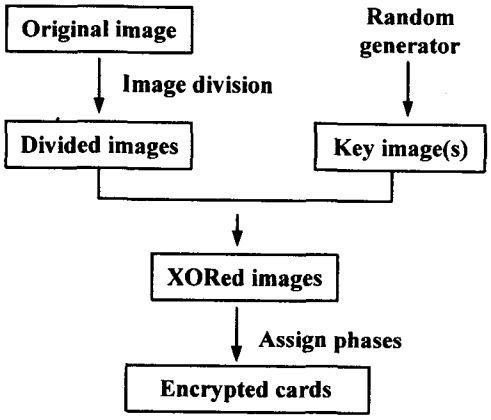


그림 3. 제안한 암호화 절차

원 영상의 복호를 위해서는 그림 4에서와 같은 마흐젠더 간섭계의 경로 상에 각각의 암호화된 위상카드들을 위치시킴으로써 원 영상을 복원해낼 수 있다. 즉 위상카드의 한 픽셀을 지난 빛은 위상카드에 입사되기 전과 비교할 때, 그 픽셀이 나타내는 위상값에 해당하는 위상 지연을 갖게 되며 이렇게 위상 지연이 된 빛들의 간섭현상은 그 결과의 세기 패턴을 놓고 볼 때, 일종의 XOR연산으로 볼 수 있다. 따라서 디지털 적인 XOR연산에 의해 암호화된 영상들을 광학적인 간섭현상에 의한 유사 XOR 과정에 의해 다시 복원해내게 된다.

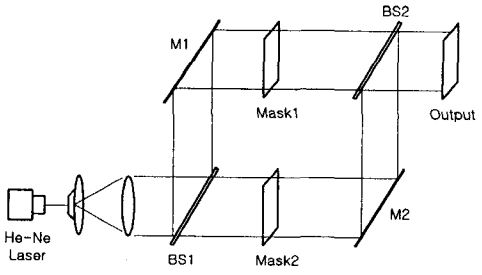


그림 4. 영상 복원을 위한 마흐젠더 간섭계

V. 컴퓨터 시뮬레이션

slide의 수(n)이 5인 경우를 예로 들면, 그림 5와 같이 원 영상을 다섯 개의 slides로 분할한다

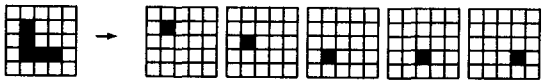


그림 5. 영상의 분할

그리고 이들 분할된 slides를 암호화하기 위한 키를 생성시키기 위해 그림 6에서 처럼 일단 4가지의 독립된 랜덤키를 생성한 후 이들의 XOR에 의해 나머지 하나의 랜덤키를 생성한다.

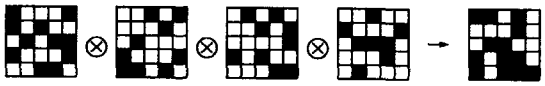


그림 6. 암호화를 위한 랜덤키의 생성
⊗: XOR 연산

이렇게 생성된 다섯 개의 랜덤키와 분할된 영상들을 각각 1:1로 XOR 연산을 함으로써 아래와 같이 암호화된 slides를 얻는다.

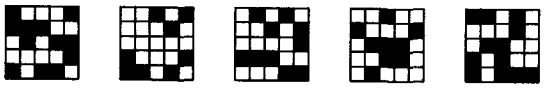
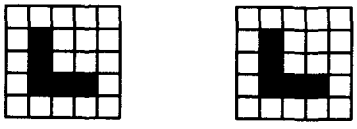


그림 7. 암호화된 영상

다음으로 이들 암호화된 slides의 백과 흑 화소에 각각 0 와 π의 이진 위상을 대응시킨 위상카드를 제작한다. 위상카드의 제작에는 광학적인 리소그라피를 이용할 수 있다. 원 영상을 복원하기 위해서는 제작된 위상카드들을 모두 마흐젠더 간섭계의 간섭 경로상에 위치시켜야 한다. 이때 위상카드들은 마흐젠더 간섭계의 두 가지 경로 중 어느 쪽에 놓여도 상관없으며, 같은 경로상의 위상카드들에 위한 위상지연은 각 카드의 위상지연에 대한 선형적인 합으로 나타나게 된다. 이렇게 위상 지연된 빛들의 간섭결과는 CCD와 같은 광세기 검출기에 의해 검출되며 그 결과는 아래 그림과 같이 원 영상과 동일한 영상을 얻게 된다.



(a) (b)

그림 8. (a)원영상과 (b)복원된 영상

Ⅵ. 결론

일반적인 암호화 시스템과는 달리 원래의 영상을 다수의 slides로 분할하여 이를 암호화하는 시각 암호화 기법은 간단하면서도 효율적인 암호화 기법임에도 불구하고 증가된 화소수에 의해 복원된 영상의 해상도 및 신호대잡음비가 감소되는 특징을 가진다. 본 논문에서는 어떤 이진 영상을 n장의 slides로 분할 한 후, 각 slide를 서로 다른 랜덤키와의 XOR에 의해 암호화한다. 이때 미리 $(n-1)$장의 랜덤키를 생성한 후 이들의 XOR에 의해 또 다른 랜덤키를 생성하게 된다. 이렇게 암호화된 영상들은 흑과 백의 화소값에 따라 0 와 π의 위상값을 가지는 이진 위상 카드로 변환되며, 이들 모두를 간섭계의 경로상에 위치시킴으로써 원 영상을 복원할 수 있다. 이렇게 복원된 영상은 기존의 시각 암호화와는 달리 원 영상에 비해 동일한 해상도와 신호대잡음비를 가지는 장점을 가진다.

참고문헌(또는 Reference)

[1] B. Javidi, J. L. Honor, "Optical pattern recogniton for validation and security verification," Opt. Eng., 1994.

[2] R. Refregier, B. Javidi ,"Optical image encryption based on input plane and Fourier plane random encoding," Optics Letters, 1997.

[3] M. Naor, A. Shamir, "Visual Cryptography," Advances in Cryptology_EUROCRYPT'94, 1994.

[4] Jong Yun Kim *et al.*, "Optical image encryption using interferometry-based on phase masks," Electronics Letters. 2000.