Binary Computer Generated Hologram의 암호화

이 상 이[A], 이 승 현[B], 정 교 일[A], 김 은 수[B]
[A]한국전자통신연구원, 정보보호기술연구본부
Tel: 042-860-6450, Fax: 042-860-5611, E-mail: syyi@etri.re.kr
[B]광운대학교 전자공학과

Encryption of Binary Computer Generated Hologram

Sang-Yi Yi[A], Seung-Hyun Lee[B], Kyo-Il Chung[A], Eun-Soo Kim[B]
[A]Electronics and Telecommunications Research Institute
Tel: 042-860-6450, Fax: 042-860-5611, E-mail: syyi@etri.re.kr
[B]Dept. of Electronic Engineering, Kwangwoon Univ.

Abstract

중요한 정보 암호화하여 복수 회원에게 분산시킨 후 회원의 합의에 의하여 해독이 가능하게 하는 thresholding scheme은 visual cryptography에 의하여 시각적인 표현이 가능하게 되었다. 그러나 visual cryptography는 표현의 한계로 응용범위가 극히 제한되었다. 이 논문에서는 visual cryptography의 응용범위를 수학에서 광학으로 확장하기 위하여 binary computer generated hologram을 encryption하는 방법을 제시하고 security 특성을 분석한다.

1. 서론

사회 구조가 복잡해짐에 따라 중요한 정보를 보호하기 위하여 복수 회원에게 정보를 분산시킨 후 회원의 합의에 의하여 접근이 허가되는 비밀 관리의 구조가 발달하고 있다. 1979년 A. Shamir는 접근 권한이 동등한 회원으로 구성된 그룹에 적용하기 위한 평등한 비밀 분산법인 thresholding scheme 제안하였으며[1], 이후 thresholding scheme의 한가지 응용 형태인 시각 암호화 기법을 제안하였다.[2]

기본적인 시각 암호화는 두 장의 투명한 용지에 원 영상을 분산하여 구성하는 것으로 간단히 구현할 수 있다. 한 장을 암호 영상으로 선택하면 나머지 한 장은 키 영상이 된다. 복호는 더욱 간단하다. 암호 영상 위에 키 영상을 중첩시키면 원 영상이 나타난다. 이와 같이 시각 암호화는 별도의 복호 알고리즘을 수행하지 않고 단순히 인간의 시각으로 복호할 수 있으므로 암호에 대한 지식이나 이를 수행하기 위한 장치 없이도 간단히 사용할 수 있는 장점이 있다. 이러한 장점에 비하여 화소를 부화소로 구성하는 과정에서 발생하는 명도의 변화와 해상도 감소라는 두 가지 큰 단점이 있다. 기존의 방법을 이용하여 해상도 향상시키는데 대한 한계가 수학적으로 증명되어 있다.

광학에서 홀로그램은 광정보처리에서 매우 중요한 역할을 하고 있다. 특히 컴퓨터를 이용하여 구성하는 CGH(computer generated hologram)는 3차원 영상 합성을 비롯하여 공간정합필터 구성에 효과적으로 이용되고 있다.[3] 이러한 CGH에는 매우 중요한 정보가 수록될 수 있음에도 불구하고 기록된 정보를 보호하려는 시도는 미미한 상태로 최근 연구가 진행되고 있다.[4]

일반적인 암호 시스템은 수학적으로 modula 연산이나 "XOR"를 이용하고 있다. 이것은 컴퓨터를 이용하여 구현하기에는 효율적이나 광학시스템으로 구현하기에는 매우 비효율적이다. 이와 달리 시각 암호화는 복호를 위하여 "OR" 연산을 수행하는데, 이것은 광학에서도 간단히 이루어질 수 있다.

본 논문에서는 "OR" 연산 특성을 지닌 시각 암호 기법을 BCGH(binary computer generated hologram)에 적용하여 홀로그램 정보를 보호할 수 있는 방법을 제안한다. 이 방법은 BCGH의 각각의 셀을 시각 암호의 화소로 대체하고 시각 암호화를 수행하는 것으로 간단히 이루어진다. 제안된 방법으로 복호 및 복원된 영상은 기존 시각 암호화 방법으로 복호된 영상에 비하여 높은 해상도를 지닌다. 그럼에도 불구하고 시각 암호와 동일한 비도를 유지한다.

2. 시각 암호화

시각 암호화에 의한 secret sharing problem의 가장 간단한 방식은 화상이 흑색과 백색의 2진 화소들의 집합으로 구성되고 독립적으로 조작되는 것을 가정한다. 원 화상은 n개의 share들로 구성되는 슬라이드에 균등하게 분배된다. 각 share는 m개의 흑/백 부화소의 집합이며, 서로 매우 근접하게 인쇄된다. 구조는 $n\times m$ boolean matix $S=[s_{ij}]$로 조작될 수 있으며, s_{ij}는 i번째 슬라이드의 j번째 부화소가 흑임을 의미한다. r개의 슬라이드 $i_1, i_2, \cdots, i_r$이 함께 포개졌을 때 결합된 share의 회색 준위는 "OR"된 m 벡터 V의 해밍 가중치 $H(V)$에 비례한다. 이 회색 준위는 어떤 고정된 임계치 $1\le d\le m$과 상대적인 차 $\alpha>0$에 대해 만일 $H(V)\ge d$ 이면 흑으로 $H(V)<d-\alpha m$이면 백으로 시각적으로 보인다.

n 개의 visual secret sharing에서 k 개를 뽑아내는 문제를 위한 해는 $n\times m$ 부울 행렬들의 두 집합 C_0, C_1으로 구성한다. 백화소를 분배하기 위하여 제공자는 C_0에 있는 하나의 행을 임의로 선택하고, 흑화소를 분배하기 위하여 C_1에 있는 하나를 임의로 선택한다. 선택된 행렬은 n 슬라이드 각각에 대해 m 개의 부화소의 색을 정의한다. 만일 다음의 3 가지 조건에 부합한다면 해는 유효하다.

1. C_0에 있는 임의의 S에 대하여 n 행들 중 임의의 k에 대한 "OR" V는 $H(V)\ge d$ 를 만족한다.
2. C_1에 있는 임의의 S 에 대하여 n 행들중의 임의의 k 에 대한 "OR" V는 $H(V)\le d-\alpha\cdot m$을 만족한다.
3. $q<k$ 인 $\{1,2,\cdots,n\}$의 임의의 부분집합 $\{i_1, i_2, \cdots, i_q\}$에 대해 C_0에 있는 각 $n\times m$ 행렬의 행들 $i_1, i_2, \cdots, i_q$로 제한함으로써 얻어진 $q\times m$ 행렬들의 $t\in\{0,1\}$ 대한 두 집합 D_t는 동일한 빈도를 가진 동일한 행렬들을 포함하는 의미에서 분간할 수 없다.

조건 1, 2는 share를 겹쳤을 때 복원되는 화상의 휘도를 나타내며, 조건 3은 강력한 암호 분석기 조차도 k 개의 share보다 더 적은 중첩에 의해서는 분배된 화소가 백인지 흑인지 결정할 때 어떤 정보도 알 수 없다.

이러한 조건을 만족하도록 암호화되고 복호화된 영상은 단지 시각적으로만 의미를 지닐 뿐 원 영상과 차이를 갖는다. 이것은 원영상을 구성하는 화소의 색상에 관계없이 암호화하는 과정에서 하나 이상의 흑 부화소가 할당되고 복호 과정에서 사라지지 않고 나타나기 때문이다. 따라서 복호된 영상의 신호대잡음비가 급격히 나빠져 신호처리와 같은 응용 기술에 적용하기는 제한적이다.

따라서 시각 암호화는 복호된 영상을 직접 응용하기보다는 다음과 같은 분야에 적용하는 것이 효과적인 것으로 알려져 있다.

- 암호적인 투표 기법
- 키 위탁 및 키 복구
- 그룹 서명
- 전자 화폐

이와 같이 시각 암호화는 2차원 영상에 응용하는 것을 기반으로 하고 있음에도 불구하고 영상처리 분야보다는 기존의 암호학적 응용 분야에 제한되고 있다. 이것은 지금까지 시각 암호가 적용되는 영상이 2진 영상이며 복호 후 해상도가 급격히 나빠지는데 원인이 있다.

따라서 영상 분야에 적용되기 위해서는 이러한 두 가지 문제를 해결하는 것이 매우 중요하다.

3. BCGH

3차원 영상을 기록하기에 가장 효과적인 홀로그램은 물체파와 기준파에 의하여 야기된 간섭패턴을 기록하는 방법으로 구성한다. 컴퓨터를 이용하여 가상의 물체에 대한 간섭패턴을 수학적으로 합성하고, 매체에 기록하는 방법으로 구성하는 홀로그램을 CGH라 한다. CGH는 물체가 수학적으로 존재하기만 한다면 구성이 가능하다. 최근의 고속 컴퓨터와 DSP 기술은 CGH를 이용하여 기존 광학 홀로그램의 대부분을 표현할 수 있게 하였으며, 효용성을 더욱 높여 3차원 동영상까지도 표현이 가능하게 하였다.[5]

CGH를 제조하기 위해서는 컴퓨터로 합성한 홀로그래픽 데이터를 필름과 같은 물리적 매개체에 기록하면 된다. 따라서 데이터를 물질적 매개체에 효과적으로 전달하기 위해서 많은 기술들이 연구되었다. 결과적으로 홀로그래픽 데이터는 많은 경우에서 디지털 코드화되어 실제 홀로그램을 만들어낼 수 있음이 밝혀졌다.

특히 컴퓨터로 계산된 복소 파두면을 이진 패턴으로 인코딩하는 홀로그램이 BCGH이다. BCGH의 패턴 기록 방법은 다양하게 알려져 있으나 기본적인 원리는 같다. 불투명한 배경에 많은 투명한 점을 구성하는 것이다. 광투과가 '0'혹은 '1'에 지나지 않을지라도 기록되고 복원되는 영상은 그레이 준위를 지닌 홀로그램과 유사한 성능을 지닌다. 몇 가지의 이진 코딩기술은 최근 급격히 발전하고 있는 공간광변조기 기술과 접목하

여 보다 쉽게 응용이 가능하게 되었다.

현재 CGH는 광정보처리, 광패턴인식, 3 차원 영상 복원, optical interconnection 등 다양한 분야에 응용되고 있다. 이러한 중요성에도 불구하고 이들 정보를 보호하고자 하는 노력은 미비한 상태이다.

기존의 암호 방법은 디지털 처리에는 적당하나 광학에 적용하기는 매우 비효율적이다. 기존의 알고리즘을 적용하기 위해서는 광 데이터를 디지털로 전환하여 보관하고 복호하여 다시 광 데이터로 전환해야 한다. 이것은 적당하지 못한 방법으로 암호 알고리즘을 광시스템에 적용하기 위해서는 광학적으로 복호하는 것이 필수적이다. 즉 CGH에 기록되는 정보는 블록 암호, 스트림 암호, 공개키 암호 등과 같이 기존에 암호학에서 알려진 방법을 직접 적용하기에는 적당하지 않다.

따라서 암호화는 디지털적으로 이루어져도 복호는 광학적으로 수행될 수 있는 알고리즘이 요구된다.

4. BCGH 암호화

시각 암호화는 강력한 영상 암호 기능을 지니고 있음에도 불구하고 많은 제한점을 갖고 있다. 대상이 되는 영상은 이진화되어 있어야 한다. 일반적으로 이진화된 영상은 백화소 주변의 화소는 백화소일 가능성이 매우 높고 흑화소 주변의 화소는 흑화소일 가능성이 매우 높다. 이것은 안전성를 낮추는 강한 요인이 된다. 또한 암복호 과정에 부화소의 더하기 과정만이 존재하므로 복호된 영상의 백화소 부분에는 각 화소당 하나 이상의 흑 부화소가 존재하여 신호대잡음비가 낮다.

BCGH는 이진값으로 구성되어 있어도 회색 준위의 영상을 표현할 수 있다. 특히 패턴인식에 이용되는 binary phase-only filter는 백화소 주변의 화소가 백화소일 가능성은 50%이며 흑화소의 경우에도 동일하다.

BCGH는 시각 암호화에서 요구하는 입력 조건을 만족하고 있다. 따라서 BCGH에는 시각 암호화 기법을 적용할 수 있으며 보호된 BCGH는 시각 암호의 안전성을 갖는다.

시각 암호화는 화소를 부화소로 나누어 암호화하므로 원 영상의 해상도를 낮춘다. 즉 복호된 BCGH의 해상도가 낮아진다. BCGH의 해상도가 낮아지면 BCGH 내에 기록된 영상은 크게 손상을 입을 것임을 예측할 수 있다.

복호된 BCGH에는 상대적으로 흑화소가 증가해 있으나 백화소의 수는 원 BCGH의 백색 셀의 수와 일치하며 위치 변화도 제한적이다. 백화소의 이동은 하나의 셀을 화소로 해석하고 부화소를 만들기 위해 확장한 해상도 범위내이다. 단지 그 위치가 무작위로 변화하고 있을 뿐이다. 즉 백화소와 백화소간의 평균 간격 비율은 BCGH의 흰색 셀 간격 비율과 일치한다. 따라서 복호된 BCGH를 퓨리에 변환하면 원영상이 복원된다. 무작위 변화는 퓨리에 변환하면 백색잡음으로 변하여 전대역에 걸쳐 나타난다.

아래 그림은 BCGH를 이용하여 복원된 영상을 나타낸 것이다. 그림 1은 제안한 방법을 이용하여 보호하고자 하는 영상으로 회색 준위를 갖고 있어 시각 암호화 기법을 직접 적용할 수는 없다.

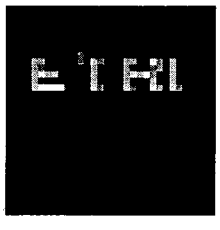
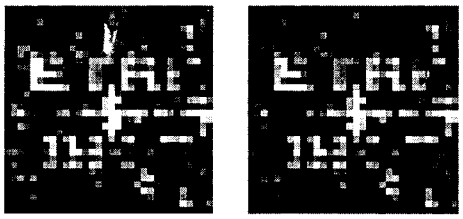


그림 1. BCGH와 시각 암호화를 이용하여 보호하고자 하는 영상

그림 2에서 (a)는 BCGH를 변화 없이 사용하여 복원한 것이고 (b)는 3 out of 3 visual secret sharing으로 BCGH를 암화화하고 복호화한 이후 복원한 영상이다. 그림 1에 비하여 그림 2의 해상도나 낮아진 것은 홀로그램을 제작하는 과정에서 나타난 것으로 암호화와는 무관하다. (b)에 비하여 (a)가 낮은 신호대잡음비를 나타내고 있으나 이는 단순히 시각 암호화를 적용한 것에 비하여 우수한 결과를 나타내고 있다. 이것으로 시각 암호화를 BCGH를 통해 광학에 적용할 수 있음이 입증되었다.



(b) (c)

그림 2. BCGH와 시각 암호화에 의한 영상 보호
(a) BCGH에 의하여 복원된 영상
(b) BCGH와 시각 암호를 적용하여 복호화한 영상

제안된 방법을 적용하는 BCGH는 회색준위를 이용하는 CGH에 비하여 상대적으로 셀당 면적이 넓어지고 다시 시각암호화를 위하여 부화소를 만드는 과정에서 화소당 면적이 넓어지는 단점을 지니고 있다.

5. 결론

본 논문에서는 BCGH로 기록되는 영상은 시각 암호화를 적용하여 보호하는 것이 효과적임을 살펴보았다. 이것은 단지 BCGH를 암호화하는 방법을 제시한 것만은 아니다. 시각 암호화의 응용분야를 확장함으로써 기존에 수학적으로 응용되는 암호 기술을 광학에는 적용할 수 있도록 하는 것이다.

참고문헌

[1] A. Shamir, "How to share a secret," *Communications of ACM*, Vol. 22, pp.612-613, 1979.

[2] M. Naor and A. Shamir, "Visual Cryptography," *Advances in Cryptography Eurocrypt94*, Vol.950, pp.1-12, 1995.

[3] C. Blundo, A. De Santis and D. R. Stinson, "On the contrast in visual cryptography schemes," ftp://theory.lcs.mit.edu/pub/tcrytol/96-13.ps, 1996.

[4] Sang-Yi Yi, Chung-Sang Ryu, Seung-Hyun Lee, and Eun-Soo Kim "Encryption of Cell-Oriented Computer Generated Hologram by using Visual Cryptography," *CLEO/Pacific Rim'99*, 1999.

[5] G. Tricoles, "Computer generated holograms: an historical review," *Appl. Opt.*, Vol.26, No.20, pp.4351-4360, 1987.