광상관기를 이용한 광 시각 암호의 암복호 평가

이 상 이, *류 충 상, **류 대 현, ***이 승 현, ***김 은 수
국가보안기술연구소, *전파연구소, **한세대학교, ***광운대학교
전화 : 042-860-6450 / 핸드폰 : 011-480-2402

Evauation for Optical Visual Cryptography Encryption by using Optical Correlator

Sang-Yi Yi, Chung-Sang Ryu, Dea-Hyun Ryu, Seung-Hyun Lee, and Eun-Soo Kim
National Security Research Institute
E-mail : syyi@etri.re.kr

Abstract

Optical visual cryptography was proposed by conjunction of the optical theory with the cryptography. However, it had some difficulties. The problems occurred in the process of transferring data processing system from visual to optics. Therefore, it is appropriate to approach these problems in terms of optics. The results show that the optical visual cryptography system has both the effectiveness and reliability as well as real-time implementation property.

I. 서론

시각 암호는 암호 분야에서 중요한 정보를 암호화하여 복수 회원에게 분산시킨 후 회원의 합의에 의하여 해독이 가능하게 하는 thresholding scheme[1]을 디지털 시스템에 의존하지 않고 인간의 시각 시스템으로 복호가 가능하도록 하였다[2]. 그러나 표현의 한계로 인하여 몇 가지 문제점을 안고 있었다. 이후 인간의 시각을 대신하여 레이저를 사용하는 광 시각 암호가 제안되어 광학 시스템에 암호 기능을 적용할 수 있게 되었다.[3] 그러나 이 시스템 역시 기존의 시각 암호의 문제점을 완전히 극복하지 못함으로 인하여 또 다른 문제를 발생하였다. 이것은 데이터 처리 시스템을 인간의 시각 시스템에서 광학 시스템으로 전환하는 과정에서 발생하였으므로 문제의 분석과 해결 역시 광학적으로 접근하는 것이 타당하다.

광학 시스템에서 잡음의 정도와 유사도를 판별하기에 적당한 방법은 2차원 광상관기를 사용하는 것이다. 광상관기는 단순한 영상의 화소 비교가 아니라 주파수 측면에서 진폭, 위상, 및 주파수 대역 별 비교가 가능하다[4].

이 논문에서는 광상관을 위하여 실시간 광상관 시스템 구현이 가능한 joint transform correlator(JTC)를 이용하여 광 시각 암호에서 발생하는 잡음의 정도와 암호 특성을 주파수 관점에서 분석하는 방법을 이용하여 광 시각 암호의 광학적인 성능 개선 방향을 제시하고자 한다.

II. 시각암호

Thresholding scheme에 기초하고 있는 시각 암호는 암호적인 투표 기법, 키 위탁 및 키 복구, 그룹 서명, 전자 화폐 등에 응용하려는 목적으로 연구가 진행되고 있다[3]. 시각 암호의 강점은 구현의 편리성이다. 암호화는 원 영상을 몇 장의 투명한 용지에 암호 알고리즘 기반으로 분산 구성하는 것으로 간단히 구현할 수 있으며, 암호 영상 위에 키 영상을 순서에 관계없이 겹치는 것만으로 복호화 할 수 있는 것이 특징이다. 시각 암호화는 별도의 복호 알고리즘을 수행하는 디지털

장치를 이용하지 않고 단순히 인간의 시각으로 복호가 이루어진다.

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

이와 같이 시각 암호화는 2차원 영상에 응용하는 것을 기반으로 하고 있으며 암호에 대한 지식이나 이를 수행하기 위한 장치 없이도 간단히 사용할 수 있는 강점이 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. 이것은 부화소로 구성하는 과정에서 발생하는 명도의 변화와 해상도 감소가 가장 큰 원인이다. 따라서 영상 분야에 적용되기 위해서는 이러한 두 가지 문제를 해결하는 것이 매우 중요하다.

Ⅲ. 광 시각 암호

암호 알고리즘은 디지털로 구현하기에 적당하도록 개발되고 있다. 따라서 광 암호 알고리즘이 동일한 비도를 유지하기 위해서는 입증된 암호 알고리즘을 디지털적으로 구성하고 광학적으로 수행될 수 있는 광디지털 하이브리드 암호 알고리즘에 대한 연구를 선행할 필요가 있다.

일반적으로 암호 시스템은 수학적으로 나머지 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 있으며, 병렬처리가 가능하다.

광 시각 암호에서는 "OR" 연산 특성을 지닌 시각 암호 기법을 BCGH(binary computer generated hologram)에 적용하여 홀로그램 정보를 보호하고 있다. 이 방법은 BCGH의 각각의 셀을 시각 암호의 화소로 대체하고 시각 암호화를 수행하는 것으로 간단히 이루어지며, 기존 시각 암호로 복호된 영상에 비하여 높은 해상도를 지닌다. 그럼에도 불구하고 시각 암호와 동일한 비도를 유지한다[5].

컴퓨터로 계산된 복소 파두면을 이진 패턴으로 인코딩하는 BCGH는 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 공간 광 변조기 기술과 접목하여 보다 쉽게 응용이 가능하게 되었다.

BCGH는 이진값으로 구성되어 있어도 회색 준위의 영상을 표현할 수 있다. 특히 광 패턴 인식에 이용되는 binary phase-only filter는 백화소 주변의 화소가 백화소일 가능성은 약 50%를 유지하며, 이것은 흑화소의 경우에도 동일하다.

BCGH를 이용하는 광 시각 암호 구성 방법은 그림 1과 같다. 사용되는 입력 영상은 이진화되어 있을 필요는 없다. 이 영상은 직접 이용되는 것이 아니라 광학적 처리를 위하여 BCGH로 제작되기 때문이다. BCGH가 완성되면 다음 단계로 시각 암호가 적용된다. BCGH는 디지털 암호 알고리즘에 기반하여 여러 개의 share로 나뉘어질 것이며 각각의 share는 서로 다른 사람들이 보관하게 될 것이다. 이때 발생하는 share의 개수는 사용하고자 하는 용도와 알고리즘에 따라 결정된다. 복호는 요구되는 임계치 숫자 만큼의 share가 겹쳐지면 이루어진다. 복호된 결과는 BCGH이다. 마지막으로 복호된 BCGH를 역퓨리에 변환하면 입력영상이 복원된다.

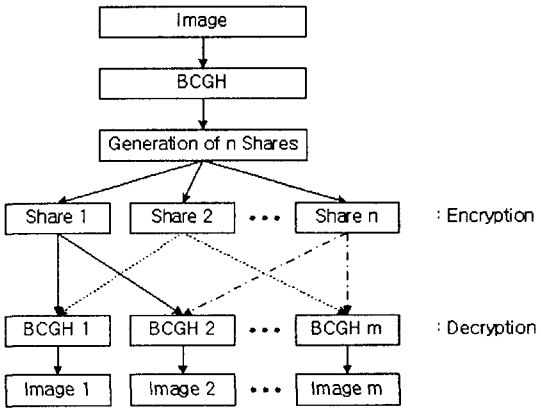


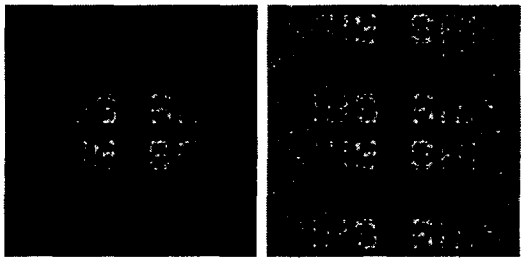
그림 1. 광 시각 암호 구성 절차

이 과정에서 복호된 BCGH와 이전의 BCGH는 동일하지는 않을 것이다. 암호화 이전 BCGH의 셀이 share 구성을 위하여 부화소로 만들어지는 과정에서 발생한 잡음이 추가되어 있다.

복호된 BCGH에는 상대적으로 흑화소가 증가해 있을 것이다. 백화소의 수는 암호화 이전의 BCGH의 백색 셀의 수와 일치할 것이나 위치가 변하여 있을 것이다. 그러나 무작위로 변하는 백화소 위치는 하나의 화소가 부화소를 만들기 위해 확장한 해상도 범위내로 한정된다. 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.

이상의 방법에 따라 얻은 결과를 그림 2에 나타내었다. 그림 2(a)는 BCGH를 변화 없이 사용하여 복원한 것이고 (b)는 3 out of 4 visual secret sharing으로 BCGH를 암화화하고 복호화한 이후 복원한 영상이다. 사용한 secret share는 4장을 모두 겹쳐서 복호하였다. 그림 2(a)에 비하여 그림 2(b)가 낮은 신호대잡음비를 나타내고 있으나 이는 단순히 시각 암호화를 적용한 것보다는 우수한 결과를 나타내고 있음을 직관적으로 살펴볼 수 있다. 자세한 평가 및 분석은 다음 장에서 기술한다.



(a) (b)

그림 2. 복원 영상
(a) 암호 기능을 적용하지 않은 경우
(b) 암호 기능을 적용한 경우

Ⅳ. 성능 평가 및 분석

별도의 정합필터를 이용하지 않는 JTC는 퓨리에 입력 평면을 2단으로 분리하여 한쪽 반평면에 기준 평면 그리고 다른 쪽에 비교 평면을 동시에 위치시키고 상관을 시키게 된다. 이 논문에서는 그림 3과 같이 상하로 2단 분리하여 구성하였다. 상단은 기준 평면으로 BCGH로부터 직접 얻은 값이 위치하고 있으며, 하단은 비교 영상으로 광 시각 암호의 출력 영상이 위치하고 있다.

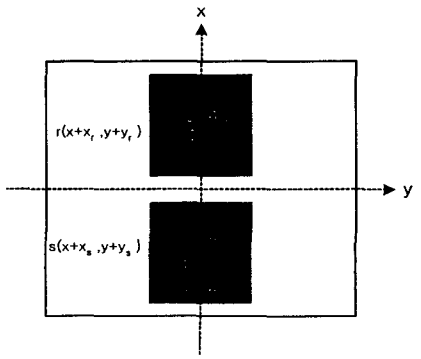


그림 3. JTC 입력 평면

두 평면으로 구성된 이력 평면을 동시에 퓨리에 변환하여 디지털 카메라와 같은 광 세기 검출기로 검출하면 식(1)과 같은 광간섭세기분포인를 얻을 수 있다.

$$\begin{aligned} E_{JTC}(u,v) &= |E_r(u,v)+E_s(u,v)|^2 \\ &= |E_r(u,v)|^2+|E_s(u,v)|^2 \\ &+ E_r^*(u,v)E_s(u,v)+E_r(u,v)E_s^*(u,v) \end{aligned} \quad (1)$$

여기서 $E_r(u,v)$는 상단 평면의 공간 주파수 성분이며, $E_s(u,v)$는 하단 평면의 주파수 성분이다. *는 복소공액을 나타낸다. 식(1)은 크게 자기 상관과 상호 상관 2가지 성분으로 나누어 해석할 수 있다. 자기 상관 성분은 자기자신간에 발생한 성분이므로 서로 다른 영상간의 상관관계를 측정하려는 목적에 맞지 않는 성분으로 잡음으로 작용한다. 상호상관 성분만이 필요하다. 따라서 필요한 자기 상관 값만을 추출할 필요가 있는데, 이것은 식(2)로써 구현이 가능하다.

$$\begin{aligned} E_{NEW}(u,v) &= E_{JTC}(u,v)-|E_r(u,v)|^2-|E_r(u,v)|^2 \\ &= E_r^*(u,v)E_s(u,v)+E_r(u,v)E_s^*(u,s) \end{aligned} \quad (2)$$

식(2)는 두 평면의 영상이 서로 교대하며 복소수로 이루어진 공간정합필터와 입력으로 작용하고 있다. 그러나 그 값은 실수이며 서로간에 원점 대칭을 이루고 나타난다. 식(2)의 구현은 이미 실험적으로 증명이 되었다.

식(2)를 역퓨리에 변환하면 식(3)의 결과를 얻을 수 있다.

$$\begin{aligned} c(x,y) &= r(x,y)\otimes s(x,y)*\delta\{x+(x_r-x_s),y+(y_r-y_s)\} \\ &+ r(x,y)\otimes s(x,y)*\delta\{x-(x_r-x_s),y-(y_r-y_s)\} \end{aligned} \quad (3)$$

식(3)의 결과는 자기상관에 따른 DC 성분 없이 두 평면간에 상관 결과만이 발생하고 있다.

그림 4는 광 시각 암호가 적용된 영상의 상관 결과이다. 출력 평면에는 모두 4개의 상관 첨두치가 발생하였으나, 대칭을 이루는 두 개는 제외하였다. 우측의 상관첨두치는 암복호되지 않은 영상의 상관결과이며 좌측의 상관첨두치는 광 시각 암호를 적용한 결과이다. 자기상관과 동일한 좌측의 상관첨두치와 비교하여 암호가 적용된 영상이 90% 이상의 유사도를 나타내고 있음을 확인할 수 있다. 그러나 만일 secret share가 위조되었다면 BCGH가 복원되지 않을 것이고 상관첨두치도 발생하지 않을 것이다.

그림 5는 동일한 데이터에 대하여 랜덤 변수 발생기의 씨앗 값을 바꾸면서 이 과정을 반복하며 측정한 상관첨두치 변화를 기록한 것이다. 일반적으로 랜덤 변수 발생기는 특성상 씨앗 값의 변화에 따라 완전히 다른 값을 나타내게 되어 있다. 여기서 적용한 알고리즘 역시 LFSR에 기반하고 있는 강력한 암호 알고리즘이다. 그림 5는 씨앗 값을 50회 바꾸며 유사도를 판정한 것이다. 씨앗 값에 관계없이 상관첨두치의 변동폭은 광 시각 암호를 적용하지 않은 상관첨두치의 85% 이상을 유지하였다. 이것은 씨앗 값에 관계없이 상관첨두치의 변화량이 매우 적다는 것을 나타내는 것이다.

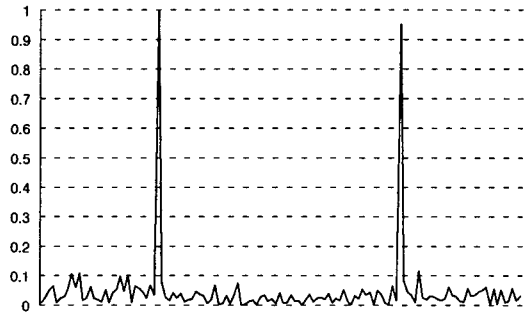


그림 4. 유사도 판정 결과

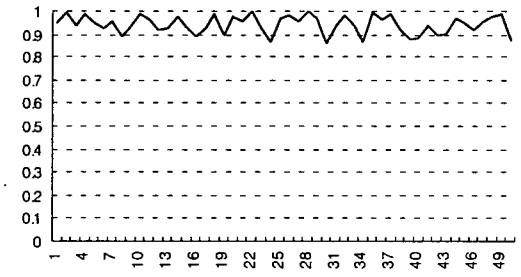


그림 5. 랜덤 변수 발생기의 씨앗 값을 바꾸며 연속하여 시험한 결과

그림 5의 결과는 BCGH가 암호화되는 과정에서 첨가된 잡음이 심각한 영향을 미치지 않고 있음을 나타내는 것으로 광 시각 암호가 타당하다는 것을 나타내는 것이다.

이상에서 광 시각 암호는 이진 그레이 준위를 가진 영상을 암호화할 수 있을 뿐만 아니라 암호화가 BCGH에 적용되므로 원 영상의 화소를 부화소로 구성함으로 인하여 시각 암호에서 발생하는 문제들을 극복하였다는 것을 상관 결과를 통하여 입증하였다. 즉 광 시각 암호는 암호학을 광학에 적용하기에 타당한 알고리즘으로 해석이 가능하다.

V. 결론

본 논문에서는 시각 암호가 광학에 접목시키기 타당한 알고리즘이라는 것을 실험적으로 증명하였다. 최종 출력 결과가 화소대 화소 방식으로 1:1 비교를 하면 모든 화소가 원 영상과 차이가 있을 지라도 주파수 관점에서 영상대 영상의 유사도로 측정하며 유사도가 매우 높아 실제 응용이 가능한 수준이라는 것을 알 수 있었다. 광 암호는 단지 BCGH를 암호화하는 방법을 제시한 것만은 아니다. 시각 암호화의 응용분야를 확장함으로써 기존에 수학적으로 응용되는 암호 기술을 광학에는 적용할 수 있도록 하는 것이다. 그러나 아직까지는 LCD들 간의 화소를 일치시키는 문제와 같은 어려운 문제들이 남아 있어 추가의 연구를 계속해서 진행할 필요가 있다.

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] S. Y. Yi, C. S. Ryu, D. G. Kim, and S. H. Lee "Encryption of Optical Image using BCGH and Visual Cryptography," *ICO XVIII, Proc. of SPIE*, Vol.3749, pp.276-277, 1999.

[4] S. Y. Yi, C. S. Ryu, D. H. Ryu, and S. H. Lee, "Evaluation of Correlation in Optical Encryption by using Visual Cryptography," *Proc. of SPIE*, Vol. 4387, pp.238-246, 2001.

[5] G. Tricoles, "Computer Generated Holograms: an Historical Review," *Appl. Opt.*, Vol.26, No.20, pp.4351-4360, 1987.