《연구논문》 Hankook Kwanghak Hoeji, Volume 18, Number 3, June 2007

공간광변조 특성을 이용한 광비쥬얼 크립토그래피

이상이

국가보안기술연구소
㉾ 305-700 대전시 유성구 가정동 161

위성민 · 이승현† · 유지상 · 김동욱

광운대학교 전자정보대학
㉾ 139-701 서울 노원구 월계동 447-1

(2007년 5월 29일 받음, 2007년 6월 13일 수정본 받음)

비쥬얼 크립토그래피(VC)의 복호 시스템으로써 인간의 시각을 대신하여 광학계를 사용하는 이진 컴퓨터형성홀로그램(BCGH) 기반의 광 비쥬얼 크립토그래피(OVC)가 제안되어 광학 시스템에 크립토그래피를 적용할 수 있게 되었으나 VC의 문제점을 극복하는 과정에서 또 다른 문제를 발생하였다. 본 논문에서는 공간광변조기의 위상변조 특성을 이용하여 광 크립토그래피를 구현하는 방법을 제시하고 시뮬레이션을 통하여 구현상의 문제점 및 타당성을 도출하였다. 제안한 광 크립토그래피는 액정디스플레이(LCD)를 활용하여 OVC로서 유용한 결과를 얻도록 하였으며, 기존 시각 암호에서 근본적으로 해결이 불가능하였던 해상도와 잡음 문제를 개선하였다.

주제어 : Binary computer generated hologram, Optical visual cryptography, Secret sharing, Spatial light modulator

I. 서 론

사회 구조가 복잡해짐에 따라 중요한 정보를 보호하기 위하여 복수 회원에게 정보를 분산시킨 후 비밀을 관리하는 구조가 발달하고 있다. Shamir에 의하여 제안된 평등한 비밀 분산법인 thresholding scheme[1]은 암호화된 데이터를 나누어 가지고 있다가 제한된 수 이상의 소유자가 모여 서로의 데이터를 합쳐 키 또는 plane text를 찾아내는 방식으로 크립토그래피에서 매우 중요한 부분을 차지하고 있다. 이 이후 thresholding scheme의 한 가지 응용 형태인 VC가 제안되었다.[2] VC는 복호를 위하여 수학적 연산이나 데이터 재배치를 요구하지 않는다. 출력된 암호문 몇 장을 겹치고 단지 인간의 시각으로 들여다보는 것만으로 복호가 가능하다. VC는 시각에 의한 복호와 병렬처리라는 장점에도 불구하고 이진 영상 사용, 원 영상 화소 크기의 확대, 복호 후 해상도 감소라는 단점이 있다.[3] 이러한 문제 극복을 위하여 그레이 영상 사용에 대한 연구가 계속되고 있으나 문제 극복과 동시에 새로운 단점도 동시에 증가하고 있다.

이를 광학적으로 해결하기 위하여 제안된 것이 BCGH에 기반한 OVC이다.[4] 이것은 원 영상을 보존하기 위하여 데이터 손상이 발생하는 VC 암복호 처리를 영상영역이 아닌 영상 주파수 영역에서 처리하는 방식이다. 암호화에 앞서 영상을 퓨리에 변환하여 BCGH로 만들고 VC를 적용한다. BCGH는 암호화된 share들을 만들고, share들을 겹치면 복호된다. 복호된 BCGH는 VC의 단점을 지니고 있지만 역퓨리에 변환을 통하여 영상을 복원하면 단점이 사라진다. 이것은 암호화를 위한 데이터로 그레이 레벨 영상을 사용할 수 있으며 입력 영상의 크기를 유지할 수 있다. 그러나 공간주파수 손상에 따른 white noise 발생과 시스템 구현에 어려움이 있다.[5,6]

본 논문에서는 VC에서 나타나는 잡음 및 영상 크기변화 문제점을 해결하기 위하여 공간광변조기(SLM)의 위상 특성을 이용하는 새로운 광 크립토그래피를 제안한다. SLM은 공간영역에서 위상특성을 조절할 수 있고 위상은 "XOR" 연산을 가능하게 한다. "XOR"은 암호학에서 가장 중요한 연산 방법의 하나로 thresholding scheme에서도 매우 중요하다. 기본 개념은 두 장 이상의 SLM을 겹쳐놓고 한 장씩 제어하는 것이다. 즉 앞에 있는 SLM에 어떤 데이터가 있던지 두 번째 SLM이 모든 데이터를 바꿀 수 있게 된다. 세 번째 SLM이 있으면 다시 모든 데이터를 바꿀 수 있으며, SLM의 수가 증가하면 데이터 변화도 계속된다. 이 방식은 암호화를 위하여 화소 확대가 없고, 잡음 문제를 해결할 수 있어 해상도 감소도 없다. 그러면서도 여전히 디지털 연산장치 없이 병렬로 복호할 수 있다. 이것은 공간주파수영역에서 프로세싱하는 BCGH 기반 OVC와 달리 공간영역에서 데이터를 처리하므로 시스템 구성이 간단하여 LCD를 이용하여 쉽게 시스템을 구현할 수 있다. 제안된 방식의 성능을 평가하기 위하여 위상 표현이 가능한 2개의 SLM에 기반한 시스템을 제안하였다. 시스템은 컴퓨터 시뮬레이션으로 시험하였으며, 두 개의 share를 사용하는 VC와 비교분석 하였다.

II. 비쥬얼 크립토그래피

접근 권한이 대등한 회원을 갖는 평등한 비밀 분산법인 (k,

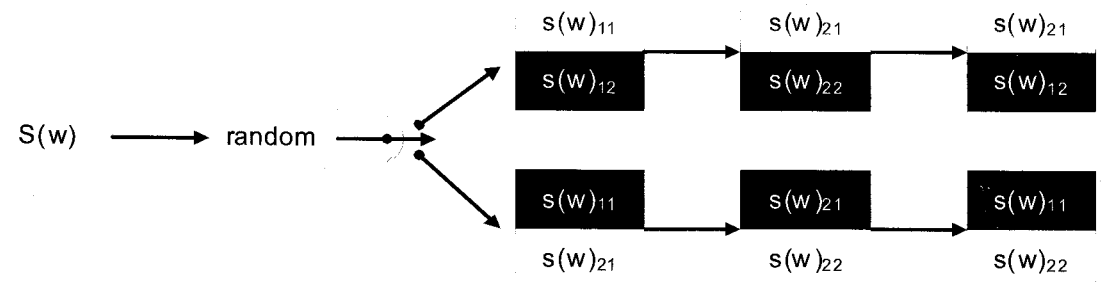
† E-mail: shlee@kw.ac.kr

n) 임계치 방식이 A. Shamir에 의해 제안된 후, 분산된 비밀 영상을 복잡한 암호적인 연산 없이 복호할 수 있는 VC가 제안되었다.[2] 이 방식은 기존의 (k, n) 임계치 비밀 분산 방식을 영상 정보에 적용하여 시각적으로 복호할 수 있도록 변형한 것이다. 즉, n명의 회원에게 미리 배포된 서로 다른 슬라이드 중에 임의의 k명 이상의 슬라이드를 중첩시키면 숨겨진 비밀 영상을 볼 수가 있으나, k명 미만으로는 숨겨진 비밀 영상에 관한 아무런 정보도 얻을 수 없도록 하는 것이다.

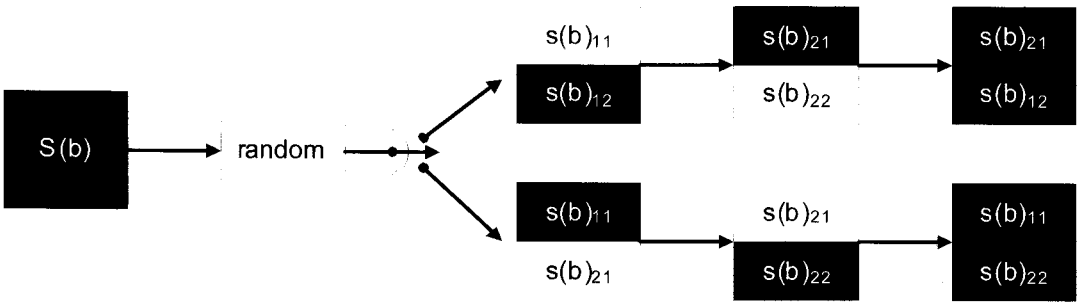
Thresholding scheme에 기초하고 있는 VC는 암호적인 투표 기법, 키 위탁 및 키 복구, 그룹 서명, 전자 화폐 등에 응용하려는 목적으로 연구가 진행되고 있다. VC의 장점은 구현의 편리성이다. 암호화는 몇 장의 투명한 용지에 원 영상을 분산하여 구성하는 것으로 간단히 구현할 수 있다. 여러 장으로 분산된 투명한 용지중 임의의 한 장 또는 몇 장을 암호 영상으로 선택하면 나머지 용지는 키 영상이 된다. 그러나 나머지 용지 모두가 키 영상이 되는 것은 아니다. 여기까지는 출력 데이터를 투명한 용지에 그렸다는 것을 제외하면 thresholding scheme과 별다른 차이점이 없다. 그러나 복호는 상당한 차이가 있다. 복호가 너무 간단하다. 암호 영상 위에 키 영상을 순서에 관계없이 겹쳐서 중첩시키면 원 영상이 나타난다. 이와 같이 시각 암호화는 별도의 복호 알고리즘을 수행하지 않고 단순히 인간의 시각으로 복호할 수 있다.

구체적으로 구현을 위해서는 영상을 암호적으로 분할하기 위하여 secret sharing problem를 풀어야 한다.[7-9] 시각 암호화에 의한 secret sharing problem의 가장 간단한 방식은 화상이 흑색과 백색의 2진 화소들의 집합으로 구성되고 독립적으로 조작되는 것을 전제로 한다. 원 화상은 n개의 share들로 구성되는 슬라이드에 균등하게 분배된다. 각 share는 m개의 흑/백 부화소의 집합이다. 이를 만족하기 위하여 원영상의 하나의 화소를 $n \times m$ boolean matix $s = [s_{ij}]$로 확장할 수 있으며 이것은 basis matrix로 불린다. 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 m벡터 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 $H(V) < d - \alpha \cdot m$이면 백으로 시각적으로 보인다.

2개의 슬라이드를 사용하여 구성하는 경우는 그림 1과 같이 구성이 가능하다. 첫 번째 슬라이드는 share1, 두 번째 슬라이드는 share2를 나타낸다. 원 영상의 하나의 화소가 백화소 S(w)인 경우를 나타내는 그림 1(a)에서 원 화소는 랜덤변수에 의하여 첫 번째 슬라이드에서 2개의 부화소(subpixel) $s(w)_{11}$, $s(w)_{12}$로 구분되고 각각의 흑화소의 위치가 결정된다. 이어서 두 번째 슬라이드의 부화소 $s(w)_{21}$, $s(w)_{22}$도 자동으로 결정된다. 랜덤값에 의하여 위쪽이 선택된 경우, 복호를 위하여 두개의 화소를 중첩하고 빛을 비추면 백화소는 마지막 슬라이드의 $s(w)_{21}$가 나타날 것이고 흑화소는 첫 번째 슬라이드의 $s(w)_{12}$가 나타난다. 원 영상의 화소가 흑화소인 경우 S(b)는 그림 1(b)와 같이 동작한다. 이것은 빛이 차단되는 효과가 "OR" 동작을 하는데 기인하고 있다. 그림 1(a)의 복호된 화소는 그림 1(b)에 비하여 상대적으로 백화소로 시각은 인지하게 된다.



(a) 백화소



(b) 흑화소

그림 1. 비쥬얼 크립토그래피에서 화소의 랜덤분할과 합성.

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

III. BCGH에 근거한 광비쥬얼 크립토그래피

VC는 이진화된 입력 영상의 사용, 낮은 해상도 등으로 인한 표현의 한계를 극복하기 위하여 BCGH에 VC를 적용하는 OVC가 제안되었다. OVC에서는 "OR" 연산 특성을 지닌 시각 암호 기법을 BCGH에 적용하여 홀로그램 정보를 보호하는 방법을 사용한다. 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. 이 방법은 시각 암호에서 사용하는 영상은 이진화된 영상의 특성을 제거하는데 중요한 목적을 두고 있다. 일반적으로 이진화된 영상은 백화소 주변의 화소는 백화소일 가능성이 매우 높고 흑화소 주변의 화소는 흑화소일 가능성이 매우 높은데 BCGH를 대상으로 시각암호를 적용하여 이러한 문제를 해결하고자 하였다. 또한 암복호 과정에 OR 연산만이 존재하므로 백화소 부분에는 각 화소 당 하나 이상의 흑 부화소가 존재하여 신호 대 잡음비가 떨어지는 문제를 극복하고자 원화상이 있는 영상 평면이 아닌 공간주파수 평면에서 처리하고자 하였다. 이는 불가피하게 발생하는 흑화소를 백색 잡음화 하도록 한다.

OVC의 입력 영상이 이진화 되어 있을 필요는 없다. 이 영상은 직접 이용되는 것이 아니라 광학적 처리를 위하여 BCGH로 제작하여 VC를 적용하기 때문이다. BCGH는 알고리즘에 따라 여러 장의 슬라이드로 나뉘어 진다. 요구되는 share들이 중첩되면 복호화되어 BCGH 가 복원된다. 그러나 암호화 이전의 BCGH와 동일하지는 않을 것이다. 본래의 BCGH 셀이 share 구성을 위하여 서브 셀로 만들어지는 과정에서 발생한 잡음이 추가되었기 때문이다. 복호된 BCGH에는 상대적으로 흑화소가 증가해 있다. 그러나 수는 원 BCGH의 백색 셀의 수와 일치한다. 백화소의 부화소를 구성하는 범위로 제한되어 있다. 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. 이 방법은 그레이 영상을 사용할 수는 있으나 BCGH를 구성해야 하는 과정에서 원영상에 변화가 가해지고, 복원 후 백색잡음이 발생하는 문제를 동반하고 있다. 또한 구현을 위하여 홀로그램 단위에서 슬라이드를 중첩시키고 영상의 복원을 위하여 레이저를 사용해야 하는 등 또 다른 중대한 문제를 야기하고 있다.

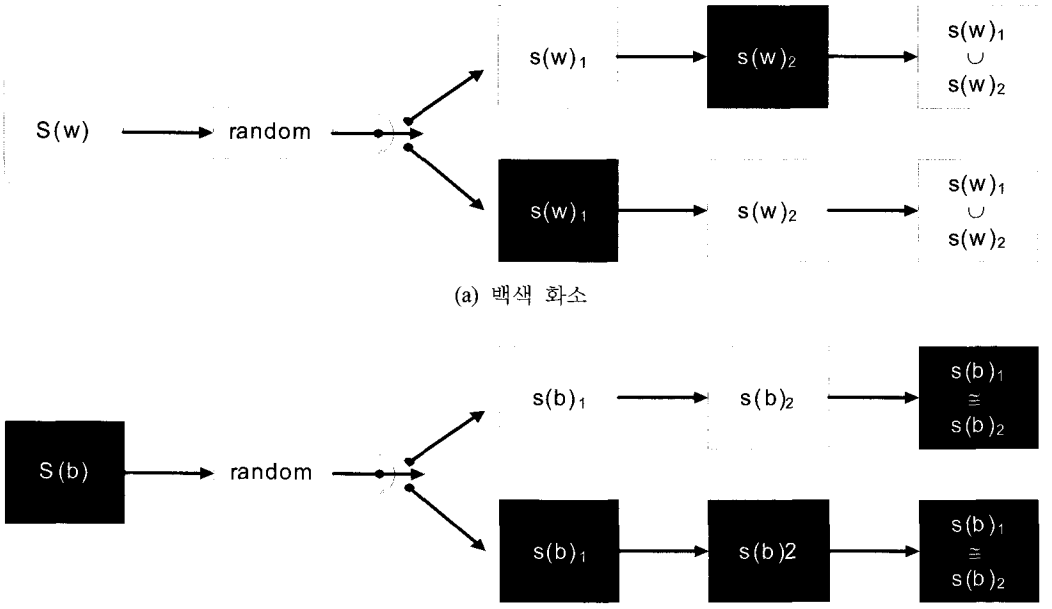
IV. 공간광변조기를 이용한 광비쥬얼 크립토그래피

일반적으로 디지털 암호 시스템은 modula 연산이나 "XOR" 연산을 이용하고 있으며 필수적으로 컴퓨터와 같은 연산장치를 필요로 하고 있다. 시각 암호는 복호를 위하여 "OR" 연산을 기반으로 하고 있으나 별도의 전기적 연산 장치 없이 시각을 이용하여 병렬로 복호가 가능하다. 공간영역에서 정보처리를 하는 시각암호와 달리 공간주파수 영역에서 정보처리가 가능한 광학시스템 은 영상의 주파수를 이용하여 정보처리가 가능하다. 특히 주파수 성분중 위상은 매우 중요한 특성을 갖는다. 위상 값을 양자화 하여 간단한 모듈러 연산이 가능하며, 양자화 값을 2로 결정하면 "XOR" 구현에 가능해진다. 그리고 이러한 특성을 시각암호에 적용하면 광학적 특성을 지닌 암호시스템 구성이 가능해진다.

양자화 된 2진 위상 값을 이용하여 암호시스템을 구성하기 위해서는 시각암호화와 유사하게 영상을 암호적 으로 분할할 수 있도록 secret sharing problem를 풀어야 한다. 기본적으로 화상은 흑색과 백색의 2진 화소들의 집합으로 구성되고 독립적으로 조작되는 것을 전제로 한다. 원 화상은 n개의 share들로 구성되는 슬라이드에 균등하게 분배된다. 각 share는 1개의 흑 또는 백 부화소로 구성된다. 구조는 boolean vector $s=[s_i]$로 조작될 수 있으며 이것은 basis vector로 한다. s_i는 i번째 슬라이드의 부화소가 흑임을 의미한다. r개의 슬라이드 $i_1, i_2, \cdots, i_r$이 함께 포개졌을 때 결합된 share의 준위는 "XOR"된 값으로 나타난다. 이것은 시각 암호와 달리 슬라이드 당 부화소수의 증가가 없고, 복호된 영상이 원 영상과 정확히 일치하는 특성을 갖는다.

위상 표현이 가능한 2개의 슬라이드를 사용하면 그림 2와 같은 연산의 표현이 가능하다. 원영상의 하나의 화소 가 백화소 S(w)인 경우를 가정한 그림 1(a)에서 원화소는 랜덤 변수에 의하여 첫 번째 슬라이드에서 2개의 부화소 $s(w)_1$의 화소 색상이 결정된다. 이어서 두 번째 슬라이드의 부화소 $s(w)_2$의 색상도 자동으로 결정된다. 복호를 위하여 두개의 화소를 중첩하고 코히어런트한 빛을 비추면 마지막 슬라이드에 $s(w)_1 \oplus s(w)_1$가 나타날 것이다. 화소가 흑화소인 경우 S(b)는 그림 2(b)와 같이 첫 번째 슬라이드와 두 번째 슬라이드의 화소가 서로 다른 색상의 부화소를 갖게 된다. 서로 다른 색을 갖는 두 화소는 이것은 코히어런트한 빛이 위상차에 의하여 "XOR" 동작을 하는데 중요한 요소이다.

그림 2의 연산을 위상변조 SLM을 이용하면 구현이 가능하다.[10] SLM은 하나의 셀이 하나의 화소를 나타낼 수 있다. 즉 화소의 상태는 셀의 상태를 나타내고 화소 색상의 변화를 통해서 셀 단위로 위상제어가 가능해지는 것이다. 화소의 크



(a) 백색 화소

(b) 흑색 화소

그림 2. 광비쥬얼 크립토그래피에서 화소의 랜덤분할과 합성.

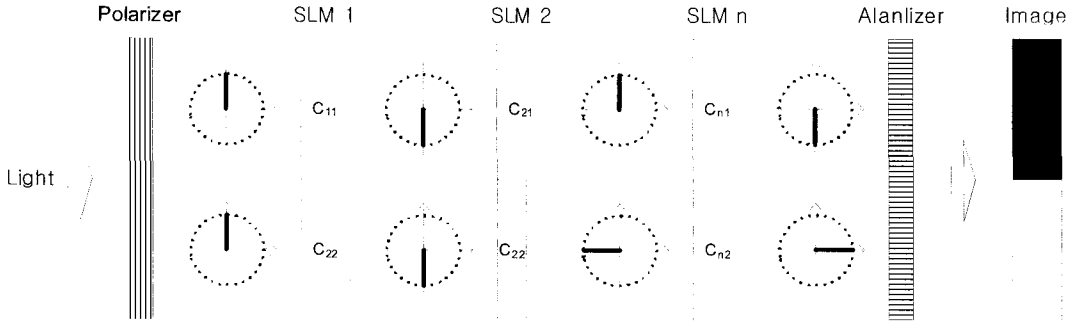


그림 3. 공간광변조기의 위상특성을 이용한 광비쥬얼 크립토그래피.

기에 비하여 SLM 간의 거리가 매우 가깝게 위치한다면 회절현상은 무시할 수 있게 된다. SLM을 이용한 시스템 구성은 그림 3과 같이 n개의 SLM을 이용하여 구성할 수 있다. 위상변조 프로세싱을 위하여 편광판을 통과한 빛은 단 방향성을 갖는다. 동일한 특성을 갖고 입력된 광은 SLM1, SLM2, …, SLMn을 통과하면서 화소색상에 의하여 제어된 셀의 상태에 따라 위상변조가 발생한다. SLM1의 C_{11}이 180° 위상차를 발생시키는 두께를 갖는다고 가정하면, 같은 두께를 지니고 있는 C_{21} 역시 동일하게 180° 위상차를 발생시켜 최종 360° 위상차가 발생한다. 이후 C_{n1}까지 180° 변화만 존재한다면 최종 광 신호는 검광판에 의해 제거되고, 시각적으로 검게 나타나게 된다. SLM1의 아래쪽을 통과하는 광은 C_{22}에서 180° 위상차가 발생하지만 90° 위상을 갖는 C_{21}을 통과한 빛은 최종 270° 위상차가 발생한다. 이후 C_{n1}까지 180° 변화만 존재한다면 검광판을 통과한 빛은 백색으로 나타날 것이다.

이러한 구조는 BCGH를 기반으로 한 OVC가 홀로그램 수준의 화소 조정을 해야 하는 것과 달리 화소가 확대되어도 문제가 발생하지 않으면서도 시각암호의 고유특성을 유지한다. 복호를 위하여 별도의 디지털 연산이 필요 없으며, 병렬처리가 가능하다.

V. 시뮬레이션

SLM을 이용한 위상변조는 상용의 광학소자를 이용하여 구현이 가능하다. 특히 제안한 방법과 같이 화소 단위로 제어를 할 수 있고 셀 크기가 큰 투과형의 위상변조 SLM으로는 LCD 소자가 적절하다. 일반적으로 활용되고 있는 LCD에서 양단의 편광판과 색상 필터를 제거하면 위상변조 SLM으로 활용이 가능하다. 그림 4는 LCD를 이용하여 구성하는 OVC 시스템이다. 시스템은 1개의 광축에서 2개의 편광기와 n개의 LCD 패널을 이용하여 간단히 구성된다. 코히어런트한 광원으로 레이져를 사용하고 편광판1을 편광판으로 편광판2를 검광판으로 사용한다. LCD1, LCD2, …, LCDn은 share들을 나타내는데 사용한다. 시스템 동작은 먼저 첫 번째 share

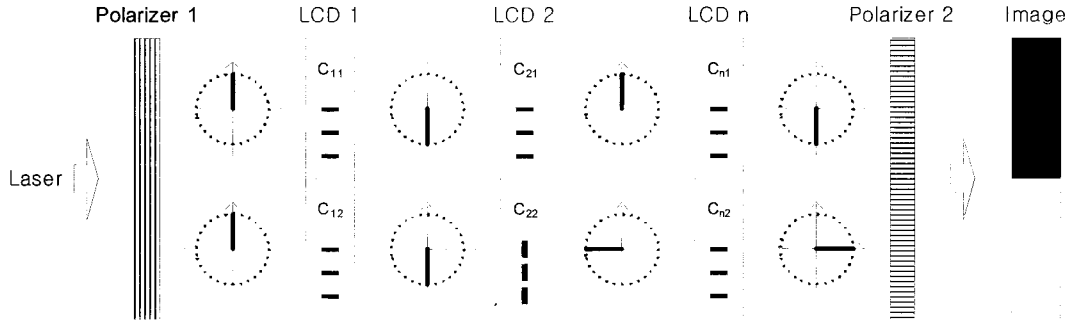


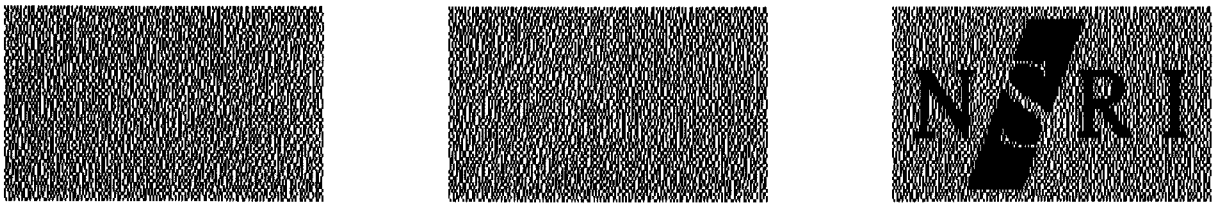
그림 4. LCD에 의한 광비쥬얼 크립토그래피 구현.

영상을 SLM1, 두 번째 share 영상을 입력 받아 SLM2에 나타내고, n번째 영상을 입력받아 SLMn에 나타낸 후 레이져를 비추면 편광판2를 통과해 복호된 plane text image가 나타난다.

시뮬레이션은 VC와 제안한 OVC를 대상으로 실시하였다. 사용된 share는 2개를 사용하였다. 암복호 시뮬레이션을 위하여 입력은 100×61 화소의 이진 값을 갖는 영상을 사용하였다. 입력 영상은 알고리즘 적용을 위하여 2×2를 하나의 화소로 확대 재구성하여 그림 5에 나타내었다.

그림 5. 입력영상.

그림 6은 VC를 이용하여 암복호한 결과이다. Share는 2×2 boolean matix로 구성하였다. 부 화소 크기는 정방형을 이루기 위하여 하나의 화소를 1×2로 하였다. 구성된 share는 그림 6(a), (b)와 같다. 각 화소들은 양자와 같이 물리적으로 랜덤하게 존재하는 소스에서 데이터를 추출하거나 암호학적으로 충분히 랜덤하게 구성할 수 있는 알고리즘을 사용하여 One Time Password를 만들어 적용하면 각각의 화소를 통하여 원 영상을 유추할 수 없다. 이 시뮬레이션에서는 128 bit AES를 output feedback 모드로 사용하여 One Time Password를 만들어 사용하였다. 그림 6(c)는 그림 6(a)와 (b)를 중첩시켜 복호한 결과이다. 그림 7은 VC를 이용하여 암복호한 결과이다. Share는 2 boolean vector로 구성하였다. 제안한 방법은 연산을 위하여 부화소를 확대할 필요가 없으나 VC와 비교를 위하여 하나의 화소를 2×2로 단순히 확대하여 처리하였다. 구성된 share는 그림 7(a), (b)와 같다. 각 화소들은 그림 6에서와 같은 알고리즘을 사용하여 충분히 랜덤하게 구성하였으며, 각각의 화소를 통하여 원 영상을 유추할 수 없도록 하였다. 그림 7(c)는 그림 7(a)와 7(b)의 각 화소들을 XOR 시켜 복호한 결과이다. 그림 6(c)는 흑색화소의 해상도는 변화 없이 유지되어 시각적으로는 원 화상을 유추할 수 있으나, 백색화소는 해상도가 50% 감쇄되어 전체적으로 해상도가 낮게 나타나 있다. 이것은 VC가 OR 연산을 사용하는 특성상 피할 수 없는 부분이다. 이것은 share의 수가 늘어



(a) Share 1 (b) Share 2 (c) 복호된 결과

그림 6. 비쥬얼 크립토그래피에 의한 암복호 결과.

(a) Share 1 (b) Share 2 (c) 복호된 결과

그림 7. 광비쥬얼 크립토그래피에 의한 암복호 결과.

나 여러 영상을 중첩해야 복호가 되는 조건이 성립하면 더욱 심각한 문제로 발생하게 된다. 반면에 그림 7(c)는 부화소를 구성하는 과정에서 화소수가 증가하지 않았고 원화상과 해상도에서도 동일함을 인지할 수 있다. 따라서 위상 표현이 가능한 SLM을 사용하여 이 결과를 적용하면 VC와 동일한 비도를 유지하면서 VC의 복호 영상 해상도 및 암호문의 크기 증가 문제를 극복한 시스템 구성이 가능하게 된다.

VI. 결 론

제안한 방식은 시뮬레이션을 통해 VC에 비하여 원 영상 복원과 해상도 면에서 우수한 결과를 나타내었다. 기존의 시스템에서는 VC가 단지 투명한 슬라이드에 출력하여 겹치는 것만으로도 복호가 가능하데 비하여, 제안한 방식은 카메라를 통하여 읽어 들인 share를 전기적으로 구성되는 SLM에 디스플레이 하고, 광원으로 코히어런트한 광을 사용해야 복호가 가능하다. 이를 위해 위상표현이 가능한 LCD와 디지털 카메라의 최신 기술을 사용하면 시스템구성이 가능하다. 그리고 여러 장의 LCD를 중첩시킬 수 있다면 VC에서 이루어진 연구를 보다 확장하여 적용이 가능할 것이다. 특히 LCD는 +1, 0, -1을 모두 표현할 수 있으므로 적절한 암호 알고리즘과 결합하면 암호학적으로 중요한 의미를 지닐 수 있다.

감사의 글

본 연구는 교육인적자원부에서 지원받은 2006년 광운대학교 대학특성화사업(차세대 신성장 동력산업을 위한 실감 IT 전문인력 양성사업)의 일환으로 진행되었으며 이에 감사를 드립니다.

참고문헌

[1] A. Shamir, "How to share secret," *CACM*, vol. 22, pp. 612-613, 1979.

[2] M. Naor and A. Shamir, "Visual cryptography," *Proc. Eurocrypt'94*, pp. 1-12, 1994.

[3] C. Blundo, A. De Santis, and D. Stinson, "On the contrast in visual cryptography schemes," ftp://theory.lcs.mit.edu/pub/tcryptol/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] Sang-Yi Yi, Chung-Sang Ryu, Dea-Hyun Ryu, and Seung-Hyun Lee, "Evaluation of correlation in optical encryption by using visual cryptography," *Proc. SPIE*, vol. 4387, pp. 283-246, 2001.

[6] 이상이, 이승현, "BPEJTC를 이용한 광비쥬얼 크립토그래피," *전자공학회지*, 제 40SD권 8호, pp. 47-55, 2003.

[7] T. Katoh and H. Imai, "On reducing the share size of visual secret sharing schemes," *Proc. ISITA*, vol. 4, no. 1, pp. 67-70, 1996.

[8] W. Ogata and K. Kurosawa, "Optimum secret sharing scheme secure against cheating," *Proc. Eurocrypt'96*, pp. 200-211, 1996.

[9] T. Katoh and H. Imai, "On human identification schemes using visual secret sharing," *IEICE Technical Report IT95-44*, 1995.

[10] A. V. Oppenheim and J. S. Lim, "The importance of phase in signal," *Appl. Opt.*, vol. 28, no. 6, pp. 1044-1046, 1989.

Optical Visual Cryptography using the Characteristics of Spatial Light Modulation

Sang-Yi Yi

National Security Research Institute, 161 Gajeong-Dong, Yuseong-Gu, Daejeon 305-700, Korea

Sung-Min Wi, Seung-Hyun Lee†, Ji-Sang Yoo, and Dong-Wook Kim

College of Electronics and Information Engineering, Kwangwoon University, 447-1, Wolgye-Dong, Nowon-Gu, Seoul 139-701, Korea

† *E-mail: shlee@kw.ac.kr*

(Received May 29, 2007, Revised manuscript June 13, 2007)

Optical visual cryptography (OVC) based on binary computer generated holograms (BCGH) is proposed. OVC used optics instead of human eyesight for decryption of visual cryptography (VC). As a result, it was possible to adapt cryptography to an optical system. However, it also had some difficulties because it did not overcome the existing problems of VC completely. This paper suggests a method of optical cryptography implementation based on the phase modulation characteristics of a liquid crystal display (LCD). The problems are evaluated by simulation. This system shows that the noise is reduced and resolution is improved compared with the conventional OVC.

OCIS code : 090.1760,100.2000,200.4740.