편광 인코딩을 이용한 암호화 방법

°한 종 욱
*한국전자통신연구소

Encryption Method using the Polarization Encoding

°Jong-Wook Han
*Electronics and Telecommunications Research Institute

요 약

본 논문에서는 암호화 시스템상에서 일반적으로 사용이 되는 EX-OR(Exclusive-OR) 방법을 광학 소자인 상용 LCTV(Liquid Crystal Television)를 이용, 2차원적으로 구현하는 방법에 대하여 설명하였다. 본 논문에서 제안한 시스템은 상용 LCTV의 인가 전압에 따라 가변되는 편광 특성을 이용 편광 인코딩 방법으로 광학적 EX-OR를 수행하게 하였으며, 기존의 1차원적인 EX-OR를 2차원적으로 가능하게 하였다. 제안된 시스템은 2차원 데이타를 처리가 가능함으로 지문 인식이나 화상 인식을 통한 보안 시스템 구성 등에 그 응용이 가능하겠다.

1. 서 론

현대 사회가 점차 고도 정보화 사회로 발전함에 따라 음성, 화상, 데이타 등 다양한 종류의 정보를 교환하고 저장하는 통신 시스템이 일반화되고 있으며 이에따라 시스템의 안정성에 대한 중요성이 더욱 강조되고 있다. 그러므로 시스템 내부나 시스템 간의 통신에서 암호화 기술에 대한 관심이 고조되고 있고, 이를 위한 암호화 기술도 많은 연구가 계속되고 있다. 일반적으로 암호화 시스템에서 암호문을 만들어내는 방법으로는 평문과 알고리즘 출력을 EX-OR하는 방법이 많이 사용되고 있다.[1] 그런데 기존의 디지탈 암호화 방법은 1차원 데이타 처리에 국한, 적용되어 오고 있으므로 2차원 데이타 처리에는 적합하지 않다.

그러므로 본 논문에서는 EX-OR 과정의 처리를 전기 신호가 아닌 광을 사용하는 법을 제안하여 광이 지니고 있는 고속성과 병렬성의 특징을 사용하여 기존의 1차원적인 EX-OR 방법을 2차원적인 방법으로 바꾸어 실현함으로 해서 암호문 생성에 있어서 2차원 데이타 처리의 가능성을 보였다. 2차원적인 EX-OR처리를 위해서 광학 소자인 액정 소자를 도입하였으며 이 액정 소자의 편광 특성을 이용, 편광 인코딩 방법으로 2진수를 표현하여 줌으로써 논리 계산을 가능하게 하였다.

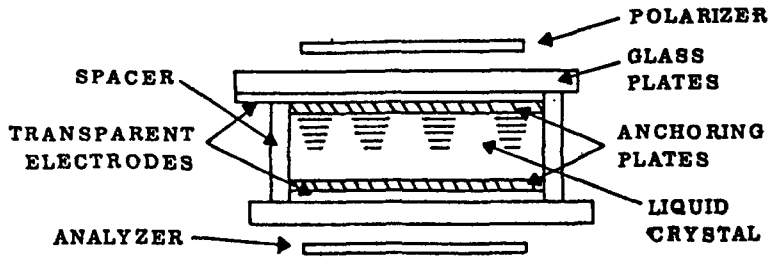
본 논문에서 제안한 시스템은 상용 LCTV 2개로 구성이 되는 광학적 방법을 사용, 2차원적으로 데이타를 암호화하였으며, 그로인하여 지문이나 얼굴 등의 화상을 통한 인식 시스템에 있어서 보안을 위한 암호화 방법으로의 응용 가능성을 보였다.

현재 광학 소자의 개발이 아직 발전 초기 단계로 보기 때문에 앞으로 더욱 고 해상도의 액정 소자가 개발이 되고 기타 광학 소자의 속도가 빨라진다면 완전한 광학 소자들로만의 시스템 구성이 가능하며, 또한 그 응용성이 커지리라 생각이 된다.

2. 액정 소자의 구조

본 논문에서 사용하는 액정 소자인 상용 LCTV는 입사되는 광 신호의 편광 성분을 인가되는 전압의 크기에 따라 회전시키는 Twisted Nematic Cell 구조를 가지고 있어 이를 이용하여 2진수의 표시와 EX-OR 처리를 가능하게 하였다.

다음 (그림 1)은 Twisted Nematic Cell 구조를 나타낸 것이다.[2]

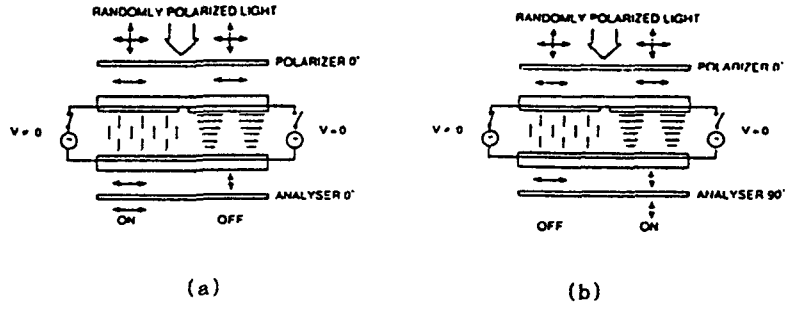


(그림 1) Twisted Nematic Cell 구조

위의 (그림 1)에서 편파기(Polarizer)와 해석기(Analyzer)가 양쪽 끝에 위치하여 인가 및 통과되는 광 신호를 제어하여 주게 되어 있다. 이 두개의 편광기는 0°에서 360° 까지 회전이 되어 수직 및 수평 편광 성분의 투과량을 조절한다. 앞면의 편파기는 액정 소자에 입력되는 편광 성분을 제어하고 뒷면의 해석기는 액정 소자를 통과한 편광 성분의 투과를 제어하게 된다.

액정 분자들은 두 투명 전극 층 사이에 위치하여 전계가 인가되게 되면 회전을 함으로써 입력 광의 수평, 수직 성분의 투과를 조절하여 준다. 최대 전압 V가 양단의 전극에 가해지게 되면 액정 분자들은 전극에 수직하게 배열이 되어 입력 편광 신호를 그대로 통과시키고, 전압이 인가되지 않으면 액정 분자들은 두 전극 사이에서 90°의 회전이 일어나게 되어 입력 편광 성분은 90° 회전을 하게 된다.

다음 (그림 2)는 외부의 편광판 배열에 따른 액정 Cell의 투과 특성을 나타내고 있다.[3]



(그림 2) 액정 Cell의 투과 특성

액정 Cell에 입력되는 광 신호는 임의의 편광 성분을 갖는 신호이며, 편파기를 통과하게 되면 0° 의 성분만 남은 상태가 되어 액정 Cell로 입력된다.

(그림 2)의 (a) 우측과 같이 아무런 전계가 가해지지 않았을 때는 때, 즉, V = 0일 때 두 전극 사이에서 90°의 회전이 일어나게 된다. 편파기를 통과하는 빛은 0° 성분만 남게 되고 액정 분자들을 통과하는 동안에 90° 회전하게 되며 다시 해석기를 통과하게 될 때는 이 90° 성분이 모두 차단 되므로 Cell은 Off가 된다.

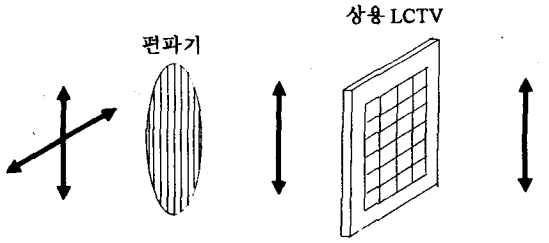
(그림 2)의 (a) 좌측의 경우에는 최대 전압 V가 양단의 전극에 가해지게 되면 액정 분자들은 전극에 수직하게 배열되어 0° 성분의 빛이 아무 변화없이 해석기를 통과하므로 Cell은 On 상태가 된다.

반면 (그림 2)의 (b) 경우처럼 액정 양단의 편광판들(편파기와 해석기)이 90° 의 각을 이루게 배치되면 (그림 2)의 (a) 경우와는 반대의 결과를 얻게 된다. 따라서 액정 소자의 투과 광의 입,출력 관계는 인가 전계의 강도와 두 편광판에 의해서 제어가 가능하게 되는 것이다.

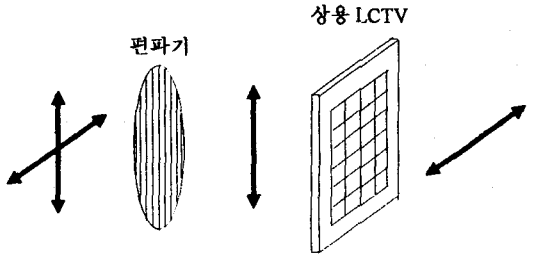
3. 광학적 EX-OR 방법

본 논문에서는 이와같은 Twisted Nematic Cell 구조를 갖고 있는 액정 소자의 하나인 상용 LCTV를 사용, LCTV가 갖고 있는 인가 전압에 따른 편광특성을 이용한 편광 인코딩 방법으로 평문과 알고리즘 출력의 EX-OR를 수행하게 하였다.

다음 (그림 3)은 상용 LCTV를 이용한 편광 인코딩 방법을 나타낸 것이다.



(a) 논리 "1" 상태 (V > 0)



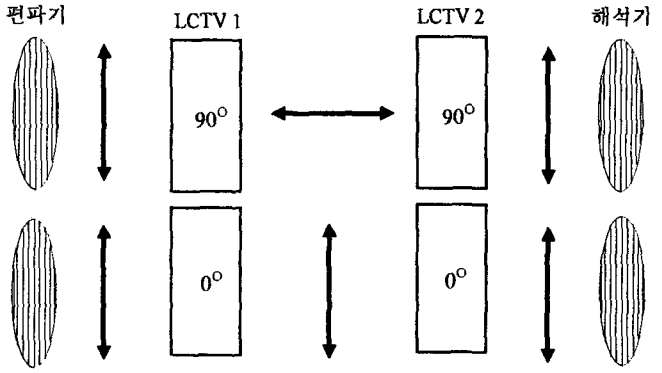
(b) 논리 "0" 상태 (V = 0)

(그림 3) 상용 LCTV를 이용한 편광 인코딩 방법

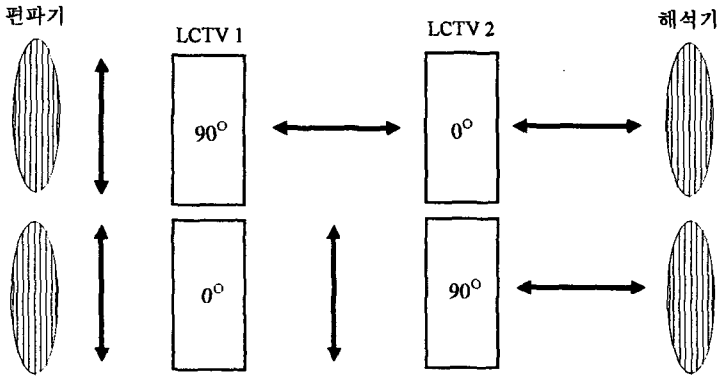
논리 "1" 상태는 입력 편광 성분을 회전없이 그대로 통과시키고, 논리 "0" 상태는 입력 편광 성분을 90° 회전시키게 하며 수직 성분은 수평 성분으로 수평 성분은 수직 성분이 되게 한다. 이와같이 상용 LCTV에 논리 상태에 따라 전압을 인가하여 편광 인코딩을 수행하며, 상용 LCTV의 편광기중 해석기는 제거하여야만 한다. 즉, 인가되는 광 신호는 편파기에 의하여 수직 성분만이 남게 되는데 이 입력 편광 성분이 상용 LCTV를 통과하면서 LCTV상의 패턴이 논리 "0"이면 90°만큼 회전하여 수평 성분이 되고, 상용 LCTV상의 패턴이 논리 "1" 상태이면 수직 성분 그대로 통과를 하게 되는 것이다.

(그림 3)의 (b)와 같이 논리 "0" 상태를 의미하는 패턴은 입력 수직 편광 성분이 LCTV내의 액정 분자들을 따라서 90°만큼 회전하게 만들고, 논리 "1" 상태를 의미하는 패턴은 (그림 3)의 (a)와 같이 액정 분자들을 회전없이 그대로 통과시키게 되어 수직 성분이 출력된다.[4][5]

(그림 4)는 (그림 3)의 상용 LCTV뒤에 한개의 상용 LCTV를 추가하여 두 상용 LCTV상에 표현되는 2진수간의 EX-OR 과정을 설명한 것이다.



(a) 동일한 입력에 대한 EX-OR 과정



(b) 다른 입력에 대한 EX-OR 과정

(그림 4) 각 입력에 대한 EX-OR 과정

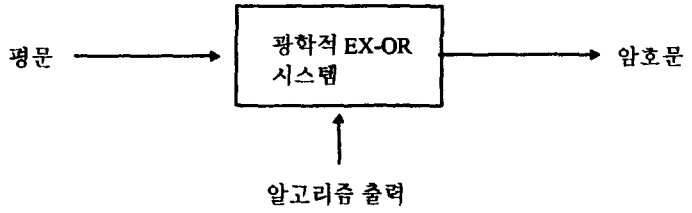
(그림 4)에서 상용 LCTV안에 90°라고 표시한 것은 LCTV에 전원이 인가되지 않은 상태로 입력되는 편광 성분을 90°만큼 회전시킨다는 의미이고, 반면에 0°는 LCTV에 전원이 인가된 상태로 입력되는 편광 성분을 회전없이 그대로 통과시킨다는 것을 의미하는 것이다. 평문이 표현되는 상용 LCTV1에서는 해석기를 제거하고, 알고리즘 출력이 표현되는 상용 LCTV2에서는 편파기를 제거하여 EX-OR를 수행하게 하여야 한다.

(그림 4)의 (a)는 평문과 암호 알고리즘 출력이 동일한 논리 상태로 LCTV에 동일한 전압을 인가함으로써 표현되며, 결과로 수직 성분이 출력되므로 수직으로 배열된 해석기를 통과할 수 있어 논리 "0" 상태가 된다. 즉, 각각 논리 "0" 상태일 경우에는 입력 수직 편광 성분이 180°회전하여 입력 그대로의 출력을 볼 수 있고, 각각 논리 "1" 상태일 경우에는 입력 수직 편광 성분이 회전없이 통과되어 역시 입력 그대로의 출력을 볼 수가 있다.

반면 (그림 4)의 (b)는 평문과 암호 알고리즘 출력이 서로 다른 논리 상태일 때로 수평 성분의 출력이 나오게 되어 해석기에 의해 출력 광이 통과가 되지 않으므로 논리 "1" 상태가 된다. 즉, 두 논리 상태가 다르게 되면 한 LCTV에서는 90°회전이 발생이 되고 다른 LCTV에서는 회전없이 통과가 되므로 입력 편광 성분과 최종 출력의 편광 성분간에는 90°편차가 발생하여 수평 편광 성분만이 나오게 된다. 그러므로 최종 출력단에서는 편광기인 수직 해석기에 의해서 출력 편광 성분이 제어되어 수직 성분만이 출력으로 나오게 되는 것이다.

4. 암호화 시스템의 실현

다음의 (그림 5)는 본 논문에서 제안한 광학적 암호화 방법을 도입한 암호화 시스템의 블럭도로 기존 1차원의 평문 및 알고리즘 출력을 입력 받아 광학적 방법에 의해 2차원으로 EX-OR한 후 다시 1차원의 암호문으로 출력하게 구성이 된다.



(그림 5) 광학적 암호화 방법을 도입한 암호화 시스템의 블럭도

본 논문에서 제안한 암호화 시스템은 알고리즘 출력 발생 회로로 부터 알고리즘 출력을 받아서 이를 상용 LCTV에 2차원적으로 표현하여 주고, 또한 입력되는 평문을 다른 상용 LCTV에 표현하여준 후 이 2개의 상용 LCTV를 서로 곱하여 그 출력을 Photo-Detector로 측정, 제어 회로에서 그 출력에 따른 암호문을 발생시켜 주게 되어 있다.

다음의 (그림 6)은 본 논문에서 제안한 광학적 EX-OR를 수행하는 시스템의 구성도이다.

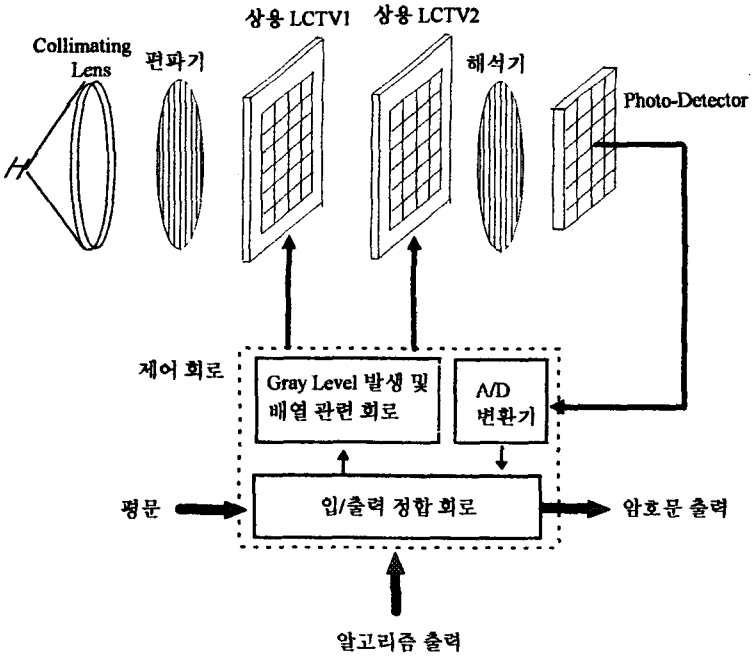
본 논문에서 사용한 상용 LCTV는 평문을 표현하여 주는 LCTV의 경우에는 해석기를 제거하고 , 알고리즘 출력을 표현하여 주는 LCTV의 경우에는 편파기를 제거하여 사용하여야만 한다.

평문과 알고리즘 출력은 모두 같은 크기의 2차원 구조를 갖으며 2차원구조를 형성하는 각 블럭도 또한 같은 갯수의 Pixel로 구성이 된다. 각 블럭은 논리 "0"이나 논리 "1" 상태를 나타내므로 평문을 나타내는 상용 LCTV 1의 경우에는 입력 수직 편광 성분의 회전 여부를 결정하게 되며, 알고리즘 출력을 표현하여 주는 상용LCTV 2의 경우에는 입력되는 편광 성분의 회전 여부의 결정 및 해석기를 이용한 출력 편광 성분의 통과 여부를 결정하게 된다.

제안된 시스템은 입력 광을 만들어 내기 위한 광원과 Collimating Lens, 입력 평문 값을 위한 상용 LCTV와 알고리즘 출력 값을 위한 상용 LCTV, Photo-Detector, 그리고 기타 제어 회로 등으로 이루어져 있다.

제어회로는 Photo-Detector의 신호를 수신하여 암호문으로 출력하고 Gray Level 발생 및 배열 관련 회로는 입력받은 평문과 알고리즘 출력들을 같은 비트 수 만큼 2차원 Gray Level로 상용 LCTV1,2에 표현하여 주게 된다. 즉, LCTV의 화면을 구성하는 Pixel을 조합하여 하나의 블럭을 구성하여 N x N 형태의 이미지 패턴을 형성하며 그 이미지 패턴은 논리 상태"0"과 "1"을 표현하여 주는 두 값중 하나로 나타나게 된다.

Collimating된 광 신호는 편파기를 거친 후 상용LCTV1에 표현된 N x N의 평문과 곱해지게 되며, 다시 그 값은 상용 LCTV2의 N x N 알고리즘 출력 값과 EX-OR가 된다. 그 출력값은 Photo-Detector에 수광되어 A/D변환기를 통하여 입/출력 정합 회로에 의해 이진수의 암호문 출력으로 변환, 출력이 된다.



(그림 6) 제안된 광학적 EX-OR 구현 시스템

만약 평문의 값이 논리 "1"이면 상용 LCTV2에 입력이 되는 편광 성분은 수직 성분이고 이때 알고리즘 출력이 논리 "1"이면 Photo-Detector에 수광되는 출력 광이 존재하게 되므로 제어 회로에 의하여 암호문 출력은 논리

상태 "0"으로 나오게 된다. 반면 마찬가지로 평문의 값이 논리 "1" 상태로 편광 성분이 수직 성분이고 알고리즘 출력이 논리 "0"이면 상용 LCTV2에 입력되는 수직 성분의 광 신호는 LCTV2를 통과하면서 다시 90° 회전하여 뒷면의 해석기에 의해 통과가 되지 못하므로 Photo-Detector에 수광되는 출력 광이 존재하지 않게 된다. 그러므로 출력되는 암호문의 값은 논리 "1"상태로 나오게 된다. 즉, 수광되는 광 신호가 있으면 논리 "0"으로, 광 신호가 없으면 논리 "1"상태로 출력되게 제어 회로를 구성하였다.

현재 개발되어 사용이 되는 상용 LCTV의 경우 이론적으로는 LCTV에 전압이 인가되지 않았을 때 입력되는 수직 편광 성분의 회전 각도는 90°이나 일반적으로는 TV에서 필요로 되는 30Hz의 Frame Rate를 얻기 위해 90° 이하의 회전 각도를 갖게 된다. 그러므로 본 논문에서 제안된 시스템을 구성할 때는 이를 고려하여 편광기의 각도를 맞추어 주어야만 한다. 즉, Gray Level과 각 편광 성분의 투과도 간의 변화 관계를 구함으로써 입력 수직 편광 성분의 회전량을 알아내어 그에 따른 편광기 각도를 찾아낸다. 이때 실제 상용 LCTV의 Contrast값을 측정하기가 어려우므로 LCTV에 부착된 Contrast 단자의 가변 저항을 이용하여 그 가변 저항에 걸리는 바이어스 전압과 각 편광 성분의 투과도 간의 변화 관계를 구하여야 한다.

본 논문에서 제안된 시스템은 지문이나 얼굴과 같은 화상 인식을 통한 보안 시스템 등에 그 응용이 가능하다. 보안 시스템의 경우 저장된 데이타의 암호화는 필수적이므로 이러한 시스템에 본 논문에서 제안된 시스템을 응용하여 2차원 영상을 그대로 처리할 수가 있으며, 또한 제안된 시스템을 확장하여 패턴 인식 시스템으로도 응용이 가능함으로 보안 시스템으로의 응용성은 더욱 커지리라 사료된다.

현재 시판이 되고 있는 상용 LCTV중 480 x 640 Pixel이나 512 x 512 Pixel 등의 크기를 갖는 상용 LCTV를 사용하여 제안된 시스템을 구성할 수 있으므로 방대한 양의 2차원 영상 처리가 가능하겠으며, 또한 광 정보 처리용으로 개발된 LCD(Liquid Crystal Display)의 경우에는 이보다 더욱 큰 가로, 세로가 1000 Pixel 이상이 되므로 이를 이용할 경우 그 응용 용량은 더욱 커지리라 생각된다.

현재 광학 소자의 개발이 아직 발전 초기 단계로 보기 때문에 앞으로 더욱 고 해상도의 액정 소자 및 광학 소자가 개발이 된다면 완전한 광학 소자들로만의 시스템 구성이 가능할 것이다.

5. 결 론

본 논문은 일반적으로 암호화 시스템에서 암호문을 만들어 내는 방법으로 많이 사용하는 평문과 알고리즘 출력을 EX-OR하는 방법에 대하여 광학적으로 처리하는 시스템을 제안하였다.

기존에 사용이 되던 1차원적인 EX-OR 방법을 2차원적인 방법으로 바꾸어 실현함으로 해서 암호문 생성에 있어서영상과 같은 2차원 데이타 처리의 가능성을 보였다. 2차원적인 EX-OR처리를 위해서 광학 소자인 상용 LCTV를 도입하였으며 이 상용 LCTV가 갖고 있는 편광 특성을 이용, 이진수를 표현하여 줌으로써 논리 계산을 가능하게 하였다.

본 논문에서 제안된 시스템은 지문이나 얼굴과 같은 영상등을 인식하여 출입을 제한하는 보안 시스템 등에 그 응용이 가능하겠다. 보안 시스템의 경우 데이타의 저장시 암호화는 필수적이므로 이러한 시스템에 본 논문에서 제안된 시스템을 응용하여 입력되는 2차원 영상을 그대로 처리할 수가 있겠다. 또한 제안된 시스템을 확장, 응용하여 패턴 인식 시스템으로도 사용이 가능함으로 보안 시스템에서 2차원 데이타의 암호화 처리 및 저장되었던 데이타와의 비교등을 수행할 수 있으므로 그 응용 가능성은 더욱 기대가 되겠다.

제안된 시스템은 상용 LCTV 2개로 구성이 되며 현재 광학 소자의 개발이 아직 발전 초기 단계로 보기 때문에 앞으로 더욱 고 해상도의 액정 소자 및 광학 소자가 개발이 된다면 그 응용성은 더욱 커질 것이며, 현재 기존의 반도체 소자를 대신할 수 있는 광학 소자가 연구 또 개발되는 상황에서 본 논문에서 제안한 시스템을 하이브리드 시스템이 아닌 완전하게 광학으로만 수행되는 시스템으로의 확장도 기대가 되겠다.

참고문헌

1. Man-Young Rhee, Cryptography and Secure Communications, McGraw-Hill, pp.1-23, 1994.
2. J.L.Horner, Optical Signal Processing, Academic Press, pp.148-156, 1987.
3. M.Kranzdorf, "Optical connectionist machine with polarization-based bipolar weight values," Opt. Eng., Vol.28, No.8, pp.844-848, 1989.
4. D.A.Gregory, "Full complex modulation using liquid-crystal televisions," Appl. Opt. Vol.31, pp.163-165, 1992.
5. F.T.S. Yu, "Application of position encoding to a complex joint transform correlator," Appl. Opt., Vol.34, No.8, pp.1386-1388, 1995.