Optical Information Processing Lab. for Optical Encryption Technology

광기술 연구 개발현황

광암호화 기술을 활용한 정보보호

강봉균 · 김 남
충북대학교 전기전자공학부

서 론

다가오는 21세기의 정보화 사회에서, 정보사기는 은행, 사업, 그리고 소비자에 있어서 매우 중대한 문제이며, 최근 우리는 면허증, 신분증, 신용카드, 현금카드, 보험카드 등의 사용이 기하급수적으로 증가함에 따라, 사람과 그들이 가지고 있는 카드의 신속하고 정확한 인식이 요구되고 있다. 이에 따라 위조 기술도 보편화되고 가능해지고 있다. 컴퓨터, CCD 카메라 기술, 영상처리에 관한 하드웨어 및 소프트웨어 기술, 프린터, 스캐너, 복사기 기술의 급격한 발달은 그림이나 로고, 화폐와 같은 패턴도 점점 더 쉽게 복제가 가능해지고 있다.

또한, 생체인식 뿐만 아니라 암호, 보안, 위조방지를 위한 광정보처리 시스템이 보다 넓게 연구되고 있다. 광정보처리 시스템은 다음과 같은 여러 이유들 때문에 암호와 보안부문의 응용에 커다란 잠재를 가지고 있다. 첫째, 광시스템은 복소수 진폭과 위상정보를 병렬로 읽고 쓰는 것이 가능하며, 공간위상 코딩 정보는 명암의 구분이 없기 때문에 명암 복사가 불가능하다는 점이다. 둘째, 고밀도 광매질의 작은 영역에 대용량의 입체정보를 코딩할 수 있으며, 코딩의 차원이 증가할수록 그것을 깰 수 있는 수학적 방법의 수는 증가된다는 점이다. 셋째, 최근에 개발된 기술들을 이용하여 그레이 스케일 또는 복소수 데이터의 고속 병렬 코딩, 디코딩이 가능하다는 점이다.

그러므로, 본 글은 최근 부각되고 있는 실시간 광정보처리 기술을 이용한 데이터의 암호화와 보안 인증 시스템에 관하여 설명한다.

광기술을 이용한 암호화의 개념

인가 받지 않은 사람에게 데이터의 접근을 방지하기 위해 암호를 통해 보안이 이루어진다. 최근에 B. Javidi 등에 의해 제안된 광기술을 이용한 암호화 방법은 부호화된 영상 (이차원 데이터 배열)이 백색 잡음 형태로 기록되고, 재생 방법은 매우 간단하고 견고하여 광학적으로 최적의 효율을 가지게 구현할 수 있다.

이 광정보처리 기술을 이용한 암호화 방법을 간단히 설명해 보면, $f(x, y)$를 암호화시킬 영상이라 하자. 또한 $n(x, y)$와 $b(\alpha, \beta)$를 각각 0에서 2π사이에 균일하게 분포된 두개의 독립된 백색 잡음이라 하자. 여기서 x, y를 공간 좌표계를 나타내고, α, β는 주파수

영역의 좌표계를 나타낸다. 암호화 과정시 사용되는 임의의 공간영역에서의 위상함수를 exp[$jn(x, y)$]라 하고, Fourier(퓨리에) 영역에서의 위상 함수를 exp[$jb(\alpha, \beta)$]라 하면, 암호화된 영상은 다음과 같이 표현된다.

$$\phi(x, y) = f(x, y)\exp[jn(x, y)] * \upsilon(x, y) \qquad (1)$$

여기서 $\upsilon(x, y)$은 exp[$jb(\alpha, \beta)$]의 역 퓨리에 변환을 나타내고 *는 컨볼루션 연산을 나타낸다. $\phi(x, y)$는 정상 백색 랜덤 처리과정(stationary white random process)를 나타내며, 이 영상은 암호키가 되는 exp[$jb(\alpha, \beta)$]를 사용해야만 해독이 된다.

이 영상을 해독하기 위해서 $\phi(x, y)$의 퓨리에 변환에 암호를 푸는 마스크 exp[$jb(\alpha, \beta)$]가 곱해진다. 그러면 암호 위상함수 exp[$jb(\alpha, \beta)$]에 암호 해독키인 exp[$jb(\alpha, \beta)$]가 곱해져 상쇄되게 된다. 따라서 원래의 영상이 공간 영역에서 출력이 exp[$jn(x, y)$]과 곱해져 복원이 된다. 만약 저장된 영상이 양의 값이라면 위상함수 exp[$jn(x, y)$]는 두번째의 exp[$jn(x, y)$]없이도 위상 마스크 비디오 카메라와 같은 빛의 세기에 의존하는 장치에 의해 제거될 수 있다. 만약 암호키 exp[$jb(\alpha, \beta)$]를 모르거나 다른 함수가 사용된다면 영상은 복원되지 않고 랜덤 잡음 형태로 남게 된다.

그림 1은 랜덤 위상을 이용한 간단하고 실제적인 광학적 구현 장치를 나타내고 있으며, 그림 1(a)에서는 광영상 암호화에 사용될 수 있는 광정보처리 시스템을 보여준다. x, y 면은 입력 면이고, α, β면은 퓨리에 면이다. 암호화될 영상은 입력 면에 위치하며, 암호화된 영상이 출력 면에 나타난다. 그리고 그림 1(b)에서는 광영상 암호화에 사용되었던 광처리시스템이 복원시에도 이용될 수 있음을 보여준다. 암호화된 영상은 입력 면에 넣고, 해독에 필요한 키를 퓨리에 면에 넣게 되면, 해독된 영상이 출력 면에 나타난다.

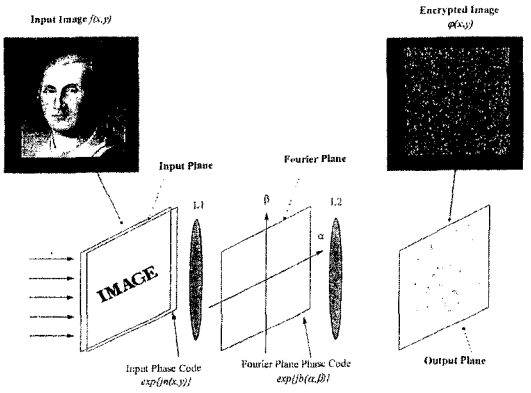

그림 1. (a) 광영상 암호화에 사용될 광정보처리 시스템

광정보처리 기술을 활용한 암호화

과거 보안 인증 시스템에서는 미리 허가된 사람의 판독을 위하여 음성이나 영상, 패스워드와 같은 데이터 등을 이용되었는데, 최근에는 이 중 음성이나 영상과 같은 각각 개인의 신체의 독특한 특징을 이용한 시스템에 관한 연구가 활발히 진행되고 있다. 그리고, 보안 인증 시스템은 데이터가 외부로 유출될 경우 손쉽게 데이터의 복사가 이루어지게 될 수 있으므로 안전성에 문제가 발생할 수가 있게 된다. 또 영상 회의 시스템이나 2차원 데이터 저장을 위한 메모리 등에도 제 3자에 의한 불법적인 도청이나 접근 시도로부터 원래의 정보를 안전하게 보호할 수 있어야 하므로 이에 대한 해결책으로 저장된 정보나 전송로상에서 전달되는 정보에 대한 암호화 방법들이 연구되어 제안되고 있다.

광암호화에 활용되는 광정보처리 기술은 신용카드나 여권 등 각종 신분증을 보안검색을 하는데 사용되며, 이러한 기술들은 카드들을 복제하기 어렵게 하여, 복소수 위상과 명암패턴들이 CCD 카메라와 같은 빛의 세기를 측정하는 기기로부터 복제가 불가능하게 하여 ID

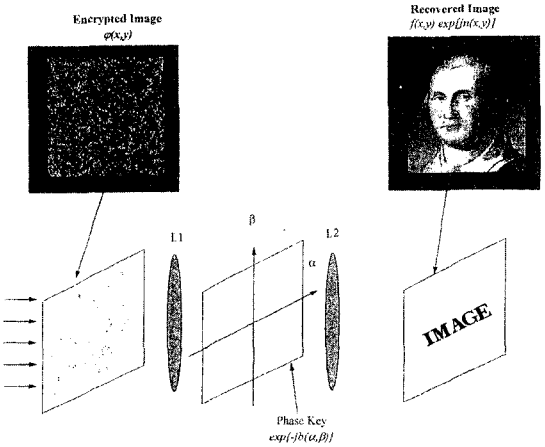

그림 1. (b) 광영상 복원에 사용되는 광정보처리 시스템

데이터를 보호하게 된다. 보안 인증 시스템에 있어서도 인식 속도가 중요하기 때문에 데이터를 암호화하는데 이어서 키를 아는 사람에게는 복호화가 용이하고, 그렇지 않는 사람에게는 어렵게 만드는 알고리즘이 필요하게 만드는 것이다.

본 절에서는 광기술을 이용한 광암호화 시스템 기술에 대해 살펴본다. 즉, 광기술을 이용한 광암호화 시스템 기술로 첫째, 두개의 랜덤 위상 함수를 이용한 암호화 기술, 둘째, 프레넬(Fresnel) 영역에서 3차원 키를 이용한 암호화 기술, 셋째, XOR 연산을 이용한 암호화 기술 등을 살펴본다.

3.1. 두개의 랜덤 위상 함수를 이용한 암호화

입력 면과 퓨리에 면에서 두개의 랜덤 위상 인코딩 기술을 이용한 광암호화 기술에 대해 설명한다. 이 광기술을 이용하여 암호화를 실현하기 위한 광학적 구성은 그림 2와 같은데, 파장이 514.5nm인 레이저를 광원으로 이용하고, 랜덤 위상 함수는 32×32 셀(7.2mm×7.2mm)로 구성한다. 이 광암호화 기술은 영상을 독립적으로 저장하고, 각각의 저장된 영상은 암호화되어 유일한 한 코드나 공유 코드에 의해서만 해독되도록 한다. 암호화 과정은 우선 저장된 영상을 랜덤 위상 함수에 의해 곱해지고, 퓨리에 면에 영상과 랜덤 위상 함수를 곱한 것의 퓨리에 변환 값을 또 다른 랜덤 위상 함수와 곱한다. 다음 역 퓨리에 변환을 수행한 후, 출력 면에서 암호화된 영상을 얻어 그 암호화된 영상을 홀로그래피 광메모리에 저장하는 개념이다. 다른 광암호화 기술과 비교해 보면, 이 광암호화 기술은 최대 엔트로피를 제공하는 백색 가우시안 정상 랜덤 처리과정으로 저장되도록 영상을 변환하는 것이 특징이다.

그러나, 이 광암호화 기술은 기록 영상이 실수 영상이라면, 위상 코드의 정확한 정렬이 퓨리에 면에서만 요구되고, 기록 영상이 복수 영상라면, 정확한 정렬이 공간 면과 퓨리에 면에서 모두 요구된다. 그 이유는 실수 영상라면, 공간 평면에서의 위상 변조는 CCD에 의해 제거되기 때문인데, 그렇다 하더라도, 해독 과정에서 정밀한 정렬이 요구되므로 이러한 특성은 공간 면과 퓨리에 면에서 랜덤 위상 함수로 하는 시스템의 단점으로 작용한다.

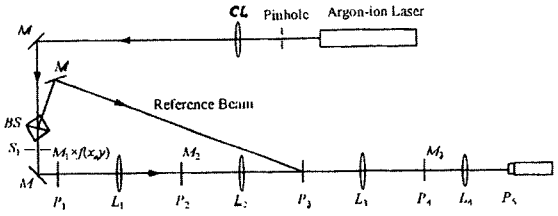

그림 2. 광메모리 기술을 이용한 암호화 시스템

3.2. 프레넬(Fresnel) 영역에서 3차원 키를 이용한 암호화

또 다른 광암호화 기술은 프레넬 영역에서 두 개의 랜덤 위상 코드와 그 코드들의 위치가 영상을 암호화시키는 제 3차원 키를 제공하게 되고, 원래의 데이터를 복구시키는 중요한 키로써 이용되며, 여기서, 프레넬 영역에 위치시켜 두 개의 랜덤 위상 코드를 이용해 암호화된 원래의 영상을 광굴절 매질에 홀로그래픽 기법으로 저장한다.

이 광암호화 시스템은 그림 3과 같이 구성한다. 이 시스템에선 파장이 514.5nm인 Ar 레이저가 광원으로서 이용한다. 이 빔은 홀로그래픽 기록을 위해 빔 분리기 BS1에 의해 물체파와 참조파로 분리된다. 참조파는 빔 분리기 BS2에 의해 두 개의 참조파로 분리되는데, 홀로그램을 기록하기 위한 참조파와 위상 공액쌍을 판독하기 위한 참조파로 분리되는 것이다. 입력 영상은 평행광으로 조사된 후, 렌즈 L1에

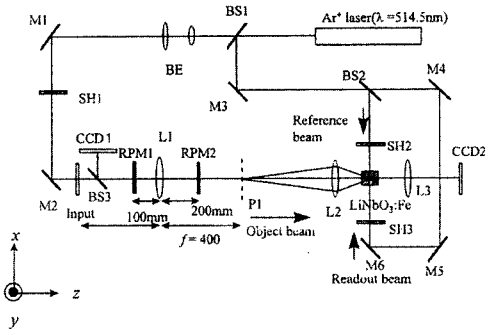

그림 3. 프레넬(Fresnel) 영역에서 3차원 키를 이용한 광암호화 시스템

의해 퓨리에 변환된다. 퓨리에 평면 P1을 지나, 축소된 퓨리에 변환된 영상은 렌즈 L2에 의해 $LiNbO_3$ 결정에 기록된다. 두 개의 랜덤 위상 함수인 RPM1과 RPM2는 입력평면과 L1 사이, 그리고, L1과 P1 사이에 위치한다. 따라서, 두 개의 랜덤 위상 함수가 입력 영상을 해독하기 위한 3차원 키로서 제공되며 프레넬 영역에 위치하기 때문에, 위상 변조는 광축에 따른 위상 마스크의 위치에 의존한다. 이러한 의존이 3차원 키에 대한 정보가 없으면 해독을 어렵게 만드는 것이다. 참조파의 위상공액쌍을 이용하여 판독되는 이상적인 재생빔은 두 개의 랜덤 위상 함수에서 발생되는 위상 변조를 제거할 수 있기 때문에, 같은 위상 함수가 홀로그램이 기록된 곳과 같은 위치에 위치된다면, CCD2에서 원래의 영상을 재생을 얻을 수 있고, 위상 함수가 다른 경우는 원래 영상을 복원할 수 없다.

3.3 XOR 연산을 이용한 암호화

또 다른 하나의 광암호화 기술은 XOR 연산을 이용한 광기술인데, 이것의 기본적인 개념은 다음과 같다. 첫째, 영상의 암호화를 위하여 한 그레이 레벨의 영상이 8개의 비트 평면들로 바뀌어 액정 디스플레이(liquid crystal display : LCD)에 표현되고, 둘째, XOR 연산은 흔히 사용하는 잘 알려진 암호화 기법으로 비트 평면은 디지털 암호화 알고리즘으로 만들어진 키 비트 열(key bit stream)과 함께 광 XOR 연산이 편광 인코딩 기법으로 수행되어 암호화가 된다. 셋째, CCD 카메라로 검출되는 XOR 연산 결과는 암호화된 그레이 레벨 영상으로 바뀌게 되고, 이 영상은 참조 영상과 비교하기 위하여 이진 위상 추출 결합 변환 상관기(BPEJTC)의 입력으로 사용된다.

선형 궤환 전이 레지스터(linear feedback shift register : LFSR)라 부르는 키 열 발생기를 이용한 비트 면으로의 변환 과정을 통해, 입력 그레이 레벨의 영상은 열 암호 시스템에서 암호화 방법으로 사용되는 XOR 연산을 수행하기 위하여 이진 영상으로 전환되어야만 한다. 각 픽셀 값을 8비트로 나타낸다면, 원 영상은 8개의 NN 비트 평면(0비트 평면에서 7비트 평면까지)의 집합으로 분해될 수 있다.

또한, LCD의 편광 특성을 이용한 편광 부호화 과정은 두 LCD의 조합을 통해 키 비트 열과 평면들 사이의 광학적 XOR 연산은 편광 부호화 방법으로 수행되는데, 입력 영상은 디지털로 8개의 비트 면으로 바뀌며, 8개의 비트 면들은 그림 4의 LCD2에 나타나며, 디지털 암호화 알고리즘으로 생성된 키 비트 열은 LCD1에 나타난다. 키 비트 열은 작은 렌즈 배열과 XOR 연산으로 광학적으로 8개의 비트 면들로 재생성 되고, XOR 연산이 편광 부호화로 수행된다.

이러한 두 가지 개념, 비트 면으로의 변환 과정과 LCD의 편광 특성을 이용한 편광 부호화 과정 등을 기초로 하여 구성된 광암호화 시스템은 그림 4과 같다. 입력 그레이 레벨 영상의 키 비트 열과 비트 면들을 나타내는데 두 LCD를 사용하고, JTC를 구성하기 위하여 또 다른 LCD를 사용한다. LCD1, LCD2, 두 개의 편광기(P1과 P2), 렌즈 L2, CCD1을 이용하여 XOR 연산이 수행된다. 그레이 레벨 입력 영상은 8개의 비트 면으로 바뀌어 LCD2에 나타난다. LCD1에 나타낸 키 비트 열은 렌즈 배열(LA)로 8개 비트 면으로 재생성 되어 키 비트 열과 비트 면 사이의 광학적 XOR 연산이 수행된다. 그 결과는 CCD 카메라로 검출되며 암호화된 그레이 레벨 영상으로 변환된다.

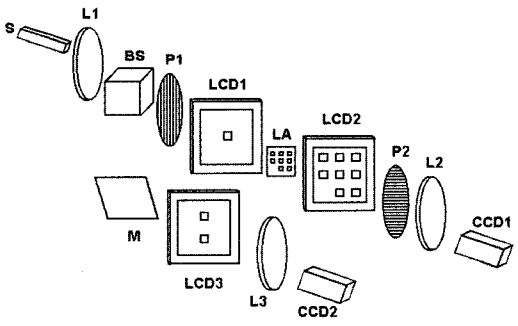

그림 4. 제안된 보안 인증 시스템

이 암호화된 영상은 데이터베이스와 비교되기 위하여 JTC의 입력(LCD3)으로 이용된다. 암호화된 영상은 참조 영상으로 기억장치에 저장되며 사용시에 암호화된 영상의 진위을 확인하기 위하여 비교된다. 참조 영상과 입력 영상은 암호화된 영상으로 사용되기 때문에 제안된 시스템은 안전하다. 암호화된 영상을 광학적으로 해독하려면, 암호화 영상의 비트 면들이 그림 4처럼 LCD2에 나타나야만 한다. 암호화 과정에서 사용한 키 비트 열과 암호화 영상의 비트 면

사이의 광학적 XOR 연산이 수행되어지고 광학적 XOR 연산의 결과는 CCD1으로 검출된다. 이와 같은 XOR 연산을 이용한 광암호화 기술은 방법은 간단하지만 광학적인 구현이 복잡하다는 단점을 지닌다.

앞에서 설명된 세 가지의 암호화 기술들을 간단히 비교 정리하면 다음과 같다. 랜덤 위상 함수를 이용한 광암호화 기술은 백색 잡음으로 영상이 암호화되므로 암호화 효과가 크지만, 키로써 복소 공액의 위상 함수를 사용하므로 시스템의 정교한 정렬과 정밀한 마스크 제작이 요구되는 특징을 가진다. XOR 연산을 이용한 광암호화 기술은 암호화 방법은 간단하지만 광학적인 구현이 복잡하다는 특징을 가지며, 광학적 간섭을 이용한 광암호화 기술은 키와 암호화된 영상이 세기 검출기로는 확인이 되지않아 복제가 어렵고 단순한 시스템이 구현된다는 특징이 있다.

광영상인식 기술을 이용한 보안 인증

보안 검증을 위해 복소 위상/명암 패턴을 사용한 보안 인증 기술은 위상으로 데이터를 암호화시키기 때문에 보이거나 빛의 세기에 의존하는 검출기에 의해 복제되지 않는다. 위상코드와 지문, 얼굴, 서명과 같은 생체 특징체와 위상코드의 복합체는 진위 판별시 사용된다. 위상마스크와 주 패턴은 마스크 코드를 알고있는 광프로세서나 상관기를 통해 판별된다.

패턴의 위상부분은 일반 빛으로는 보이지 않는 이차원 위상 마스크로 구성되어 있다. 이 이상 마스크의 차원이 매우 크기 때문에 그 구성 성분을 알아내기는 매우 어렵다. 그 마스크는 현미경이나 사진이나 컴퓨터 스캐너 등으로도 분석이 안된다. 위상 마스크는 다른 기술과 같이 사용되거나 또는 단독으로도 사용된다. 예를 들면 위상마스크는 주 패턴에 단단히 부착된 얇고 투명한 플라스틱 막으로 제작할 수 있다. 이 위상 마스크는 컴퓨터 칩과 같은 제품에 부착되어 광상관기에 의해 읽어지고 검색이 된다. 이 마스크를 다른 패턴으로 변경하려는 어떠한 시도에 의해 마스크를 분리할 때 마스크는 망가지게 된다. 위상함수는 수학적으로 $\exp[jM(x, y)]$로 표시된다. 여기서 $M(x, y)$는 $[-\pi, \pi]$사이의 값을 갖는 실수함수이다. 상업용으로 구입이 가능한 광학필름이나 매질은 분해능이 높기 때문에 $M(x, y)$는 수백만의 화소로 구성되지만 마스크의 크기는 매우 작아진다.

여러 가지 다른 기술들도 마스크를 구성하는데 사용될 수 있다. 마스크는 여러 신용카드에 찍힌 홀로그램처럼 엠보싱 기술에 의하여 얇은 플라스틱에 매질에다 만들 수 있다. 또한 굴절 또는 회절 광학계를 만드는 기술로 제작될 수 있고, 사진 필름을 표백해서 만들기도 한다. 마스크를 인식하는 프로세서가 많은 수의 위상 마스크를 저장하는 광메모리를 사용하기 때문에 마스크들은 많은 수의 코드를 포함하는 중첩형태로 될 수 있다.

카드를 읽는 검색시스템은 여러 가지 광상관기 기술 중에 하나가 될 수 있다. 영상(또는 주 패턴) $g(x, y)$는 검색이 요구되는 생체패턴이고

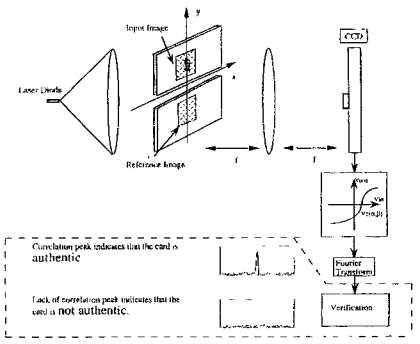

그림 5. (a) 비선형 JTC를 이용한 광암호화용 인증 시스템

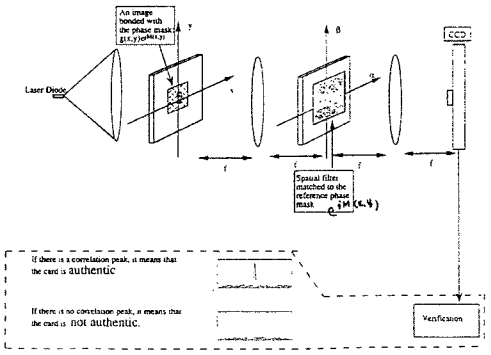

그림 5. (b) 주파수 평면 광상관기를 이용한 광암호화용 인증 시스템

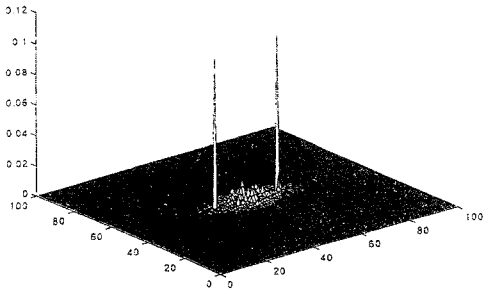

그림 5. (c) 정확한 얼굴 영상과 랜덤 위상코드가 비선형 JTC의 입력면에 보여질 때 비선형 JTC를 이용한 인식(verification)의 실험적 결과

여기에 위상마스크가 더해져 상관기의 입력면에 놓여진다. 이 복합 입력 신호는 다음과 같다.

$$i(x, y) = g(x, y)\exp[jM(x, y)] \qquad (2)$$

간섭성이 있는 빛을 이 복합 마스크에 비추어 반사시키거나 카드의 투명한 부분으로 투과시키거나 해서 신호를 끌어낸다. 프로세서는 이 마스크에 대한 주요정보 $\exp[jM(x, y)]$를 기지고 있다. 한개의 공간 필터가 상관기의 주파수 평면인 퓨리에 평면에 놓여있어서 코드(생체 패턴)을 검색한다.

입력 마스크와 필터 함수사이의 출력인 상관(correlation)이 CCD 영상 센서에 의하여 검출된다. 상관의 세기가 입력 마스크와 저장된 원 마스크간의 유사도를 결정짓게 된다. 만약 공간 필터와 일치하거나 입력 마스크와의 상관의 강도가 세면 높은 세기의 스폿이 CCD에 의하여 검출된다. 만약 이 세기가 일정 값 이상이 되면 진짜로 판명이 되고 만약 세기가 일정값 이하가 되면 입력 위상마스크는 위조된 것으로 판명이 된다. 만약 주 패턴이 없고 단지 위상마스크 $\exp[jM(x, y)]$로만 검색에 사용된다면 $g(x, y)$는 상수 함수가 된다. 하지만 주 패턴이 검색에 이용된다면 검색기는 $g(x, y)$에 대한 사전 정보를 가지고 있어야 한다.

보안 인증 시스템 기술에 이용되는 광상관기에는 대표적으로 결합 변환 상관기(joint transform correlator : JTC)와 주파수 평면 광상관기가 주로 사용된다. 그림 5(a)는 비선형 JTC를 이용하는 경우이며 그림 5(b)는 주파수 평면 광상관기를 이용한 경우이다.

물체에 대한 광상관기 한 예가 JTC인데, 기준함수 $r(x, y)$와 임의의 입력 물체 $s(x, y)$가 같은 입력면에 놓인다 그림 5(a)은 그들의 연결된 또는 결합 퓨리에 변환이 렌즈를 지나 초평면에서 이루어진다. 만약 JTC가 CCD와 같은 에너지 검출기나 감광 필름에 기록된 다음 두 번째의 퓨리에 변화을 하면 두 물체는 상관이 이루어진다. JTC의 가장 큰 잇점은 입력신호와 기준신호가 동시에 퓨리에 변환이 되고 변환간의 간섭이 한단계로 이루어진다. 따라서 필터를 만들 필요가 없어진다.

비선형 JTC는 광소자의 제한된 영역 때문에 더욱더 실용적이다. 더군다나 비선형 JTC는 상관의 성능면에서 많은 잇점을 준다. 즉, 비선형 JTC의 특성을 토대로 제안된 시스템은 광학적으로 구성하기 쉽고 시스템의 배치가 용이하며, 전자적 또는 광학적인 메모리에 저장된 입력 면에서 참조 영상을 갱신함으로써 학습됨과 동시에 필터나 홀로그램으로 생산할 필요가 없다. 또한, 퓨리에 평면에서 비선형 변환을 이용하기 때문에, 광시스템은 입력 영상의 조명의 변화에 영향이 적고, 판별 감도가 좋으며, 천이 불변 특성과 상업적으로 구할 수 있는 전자광학 장치를 이용하여, 낮은 가격의 소형 시스템으로 구성될 수 있다는 장점을 가지고 있다. 여기서 입력영상은 입출력 광학소자나 실시간 구동의 공간 광변조기로 나타낸다. 그림 5에 비선형 JTC 구도가 카드의 진위를 판명하기 위해 사용되었다. 그림 5(b)는 입력 면에 위상 코드와 하나의 랜덤 위상 코드에 부착된 얼굴 영상을 놓고 비선형 JTC를 이용해 인식하는 실험 결과를 나타낸다.

또한, JTC와 주파수 평면 광상관기를 이용한 광암호화 보안 인증시스템은 그림 6의 위상 인코딩ID 기술로도 적용이 모두 가능하다.

앞 절에서 살펴본 광기술을 활용한 암호화 및 보안 인증 시스템 기술을 간단히 정리해 보면, 암호화에 있어 부호화 방법은 입력 영상을 두 개 또는 세 개의 키를 이용한 정상 백색 잡음으로 변화시키고, 원래의 영상은 비밀키를 이용하여 복원된다. 암호화 시스템에 있어 위상 암호화는 하나의 키와 생체인식을 부호화 하는 등에 사용될 수 있으며 비선형 JTC 기술은 식별 확인을 위해서 이용된다. 특히, 앞

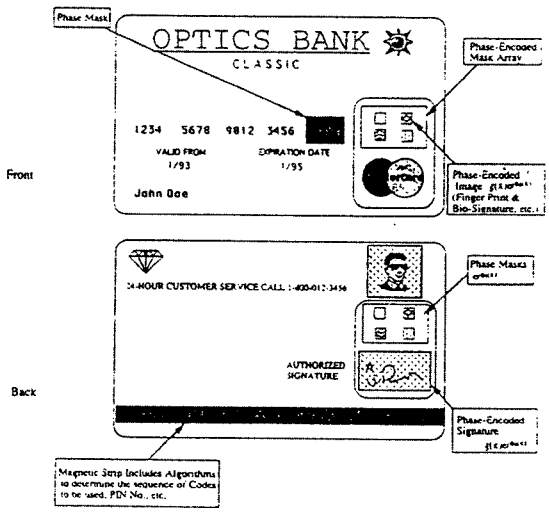

그림 6. 위상 인코딩ID 카드

으로 광재료, 장치, 알고리즘, 그리고 시스템에 대한 지속적인 연구와 개발이 이루어진다면, 이러한 기술들은 소형이며 대량으로 저가의 광정보처리 기술을 활용한 광암호화 시스템의 설계 및 제작이 가능하게 될 것이다.

결 론

지금까지 다양한 문제들과 응용분야에서 훌륭한 수행을 보여준 암호화, 보안, 그리고 위조방지 등에 대한 새로운 광정보처리 기술 및 광시스템 기술을 살펴보았다. 이러한 광정보처리 기술은 병렬로 처리가 되어 전송 및 처리 속도가 매우 빠르다는 장점과 위상이 CCD와 같은 빛의 세기에 반응하는 검출기로는 복제가 불가능한 잇점을 가지는 등 정보들이 위상, 파장, 공간 주파수, 편광 등과 같이 다양한 형태로 쉽게 숨겨질 수 있는 데이터의 보안에 장점을 가지고 있음을 알았다. 데이터에 대한 보안 및 인증이 일상생활에서 매우 중요한 영역으로 될 21세기 정보통신 시대에서 암호화, 정보보호 및 인증을 위한 광암호화 및 보안 인증 시스템은 이를 필요로 하는 정부 및 산업체 등에서 매우 유용하게 사용될 것이다.

끝으로 본 연구는 2000년도 한국정보보호센터의 위탁과제(암호기술연구00-4) 재정지원으로 수행되었음을 밝힙니다.

참고문헌

[1] B. Javidi, "Optical spatial filtering for image encryption and security systems," SPIE, Vol. 3386, pp. 14-23, 1998.
[2] O. Matoba, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett., Vol. 24, NO. 11, pp. 762-764, 1999.
[3] B. Javidi, "Fully phase encoded key and biometrics for security verification," Opt. Eng., Vol. 36, No. 3, pp. 935-942, 1997.
[4] B. Javidi, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," Opt. Eng., Vol. 35, No. 9, pp. 2506-2512, 1996.
[5] N. Towghi, B. Javidi and Z. Luo, "Fully phase encrypted image processor," Opt. Soc. Am., Vol. 16, No. 8, 1999.
[6] B. Javidi, L. Bernard and N. Towghi, "Noise performance of double-phase encryption compared to XOR encryption," Opt. Eng., Vol. 38, No. 1, pp. 9-19, 1999.
[7] B. Javidi, A. Sergent, G. Zhang and L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," Opt. Eng., Vol. 36, No. 4, pp. 992-998, 1997.
[8] E. G. Johnson and J. D. Brasher, "Phase encryption of biometrics in diffractive optical elements," Opt. Lett., Vol. 21, No. 16, 1996.
[10] B. Javidi, A. Sergent and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," Opt. Eng., Vol. 37, No. 2, pp. 565-569, 1998.
[11] B. Javidi and J. L. Horner, Real-time Optical Information Processing, Academic Press, New York, N.Y., 1994.
[12] VanderLugt, Optical Signal Processing, John Wiely and Sons, New York, N.Y., 1992.
[13] B. Javidi and J. L. Honer, "Optical pattern recognition for validation and security verification", Opt. Eng., Vol. 33, pp. 1752-1756, 1994.
[14] J-W Han et al., "Optical image encryption based on XOR operations," Opt. Eng. Vol. 38, No. 1, pp. 47-54, 1999.
[15] B. E . A. Saleh and M. C. Teich, *Fundamentals of Photonics*, John Wiely and Sons, New York, N.Y., 1991.
[16] J. W. Goodman, Interoduction to Fourier optics, 2nd edition, McGraw-Hill, New York, N.Y.,1996.
[17] B. Javidi, "Optical information processing for encryption and security systems," Optics & Photonics News, pp. 29-33, March 1997.
[18] S. Zhang and M. A. Karim, "High-security optical integrated stream ciphers," Opt. Eng., Vol. 38, No. 1, pp. 20-24, 1999.

[19] Naor M and Sharmir A., "Visual Cryptography," Eurocrypt '94 Springer-Verlag LNCS, Vol. 950, No. 1996, pp. 15-27, 1996.
[20] D. J. Lee, N. Kim et al., "Dynamic optical interconnection in free-space switching system," Opt. Rev., Vol. 3, No. 6B, pp. 475-477, 1996.

약 력

강봉균

현재근무처 : 충북대학교 대학원 정보통신공학과 박사과정
최종학력 : 1998, 충북대학교 대학원 정보통신공학과 공학석사
1993, 충북대학교 정보통신공학과 공학사
주요경력 : 1992-1995, LG전자 연구원
1997-1999, 한국전자통신연구원(ETRI) 위촉연구원
E-mail : bgkang@osp.chungbuk.ac.kr

김 남

현재근무처 : 충북대학교 전기전자공학부 교수
최종학력 : 1988, 연세대학교 전자공학과 공학박사
1983, 연세대학교 전자공학과 공학석사
1981, 연세대학교 전자공학과 공학사
주요경력 : 2000-2001, 미 Caltech 연구교수
1992-1993, 미 Stanford 대학 방문교수
E-mail : namkim@cbucc.chungbuk.ac.kr