主題

광기술을 이용한 차세대 정보보안 기술

충북대학교 전기전자공학부 윤진선, 김 남

차 례

1. 서 론

현대 지식정보 사회의 정보 통신망에서 개인정보 침해가 극심해지고 있는 것으로 나타났다. 한국 통신부 자료에 따르면 정통부 산하 개인정보 침해신고센터에 접수된 개인정보 침해 건수는 2000년 4월부터 2000년 12월까지 2297건이나 됐으며, 2001년 1월부터 4월까지 3074건으로 급격히 증가한 것으로 나타났다. 이는 2000년 월 평균 255건이던 신고 건수가 2001년 들어서는 768건으로 무려 3배나 늘어난 수치다. 주요 개인정보 침해 유형은 개인 정보를 제공자의 동의 없이 도용, 개인정보 열람·정정·삭제 요구에 불응, 본인의 동의 없이 개인 정보를 제3자에게 제공하거나 목적 외에 사용, 본인 동의 없는 개인정보 수집, 개인정보 수집 목적 달성후 미파기, 개인정보 수집시 의무고지사항 미이행, 목적 이외의 과도한 개인정보 수집 등이었다.

인터넷을 이용한 전자상거래 및 주식, 각종 금융거래가 이루어짐에 따라 해킹에 대한 관심이 고조되고 있는 가운데, 여권, 신용카드, 각종 카드 등의 위조 여부를 확인하기 위한 수단으로 일반적으로 사진, 얼굴, 지문 등이 사용되고 있으나 최근, 영상처리용 소프트웨어 기술과 컴퓨터, 프린터, 스캐너, 복사기, CCD 카메라와 같은 하드웨어 기술의 빠른 발전으로 인해 위조 및 복제가 고도로 정교하게 이루어지고 있어, 은행이나 소비자 대상의 사업 뿐 만 아니라 현대 신용 사회에 직면한 심각한 사회적 문제로 대두되고 있어 이를 해결하기 위한 암호화 방법들이 연구되고 있다.

이와 같은 시대적·사회적 요구로 인해 최근 광기술을 이용한 광 메모리 암호화 시스템과 보안 인증 시스템이 광 정보처리 분야에서 활발하게 연구되고 있다. 광 정보 처리 시스템은 고속 처리 및 병렬 처리가 가능하므로 광 메모리 암호화와 보안 인증 응용에 특히 유용하다. 따라서, 사기와 위조를 방지하기 위해 보안 시스템에서 이러한 광 정보 처리 시스템을 이용하는 여러 기술들이 제안되고 있다. 그들 중 많은 방법들이 암호화 및 해독 키로서 주로 복소 위상

인코딩 기술을 이용한다. 이러한 복소 위상/진폭 인코딩 키는 사진, 컴퓨터, 스캐너, CCD 카메라 등을 이용해서 복제될 수 없으므로 데이터를 효과적으로 암호화할 수 있게 해주고, 허가받지 않은 사용자들로부터 메모리 접근을 차단할 수 있게 해주며, 허가받은 사용자만이 메모리 접근을 허용하도록 인증 여부를 판별할 수 있게 해준다.[1-3]

일반적으로 암호 기술의 기본 기능은 비밀성 기능과 인증 기능으로 나눌 수 있다. 비밀성 기능이란 정보 통신망에서 전송되는 중요 데이터의 불법적인 노출을 방지하는 기능으로, 메시지를 제3자가 해독 불가능한 형태로 변형하거나 또는 암호화된 통신문을 해독 가능한 형태로 변환하기 위한 원리, 수단, 방법 등을 취급하는 기술을 말한다. 암호의 인증 기능이란 현대 사회의 업무가 고도 지식정보사회로 변형되는 과정에서 새롭게 야기되는 정보보호 문제 즉, 통신하는 사람간의 신분확인 문제, 전송되는 전자문서의 위·변조 방지 문제, 사이버 공간상에서 발생하는 전자적 행위에 대한 사후 부인을 방지하는 문제, 계약 시간을 확인해 주는 시점확인 문제 등을 해결하는 기능으로, 정보화 사회가 활성화될수록 매우 중요한 역할을 담당하게 된다.[4] 암호 기술의 기본 기능 중 비밀성 기능을 갖는 광 암호화를 이용한 광 메모리 암호화 기술과 인증 기능을 갖는 광 암호화를 이용한 보안 인증 기술에 대한 국내외 동향을 분석한다.

2. 광 메모리 암호화 시스템과 보안 인증 시스템의 기술동향 및 분석

광기술을 이용한 차세대 정보보안 분야에 대한 국내외의 연구 개발 동향을 보면, 1995년 미국 Hesselink 교수 팀에 의해 write-once 광 폴리머, 1GB의 광학적 데이터 베이스를 이용해 빠른 전송률과 8×8×3.6 인치의 크기를 갖는 최초의 광학적 지문 인식 시스템을 발표하였고, 1995년 같은 해에 미국의 B. Javidi 교수 팀이 광학적 기술을 이용한 정보 보호 시스템을 발표한 이래로 현재 대용량의 데이터를 저장할 수 있는 DREXLER사의 홀로그래픽 카드 시스템으로까지 발전을 하였다. 국내에서도 현재 광 메모리 암호화 시스템과 보안 인증 시스템에 대한 연구가 활발히 진행되고 있으나, 아직까지는 주로 충북대, 광운대, 부경대 등의 대학 및 몇몇 연구소와 이미 시제품을 개발 완료하고 상업화에 주력하고 있는 프리즘 테크, 맥스 소프트 등의 기업이 있다.

최근 활발히 연구 보고 되고 있는 광 암호화를 이용한 광 메모리 암호화 기술과 보안 인증 기술에 관한 가장 대표적인 방식에는 홀로그래픽 위상 마스크 키를 이용하는 이중 랜덤 위상 인코딩 방식[5-7]과 XOR 연산을 이용하는 비트 평면 인코딩 방식[8], 고속으로 키 재생성이 가능한 CGH 방식[9-10] 등이 있다. 그들 중에서, 1995년 Ph. Refregier와 B. Javidi[5]에 의해 제안된 이중 랜덤 위상 인코딩이 가장 일반적인 기술이다. 광기술을 이용한 각 방식에 관한 대표적인 기술은 표 1과 같다.

표 1. 광 암호화 방식의 대표적인 기술

광 암호화를 이용한 광 메모리 암호화 기술	- 이중 랜덤 위상 인코딩을 이용한 광 메모리 암호화 기술 - 프레넬(Fresnel) 영역에서 3차원 키를 이용한 광 메모리 암호화 기술 - 비트 평면 인코딩을 이용한 광 메모리 암호화 기술 - CGH를 이용한 광 메모리 암호화 기술
광 암호화를 이용한 보안 인증 기술	- 위상 인코딩 키를 이용한 보안 인증 기술 - CGH를 이용한 보안 인증 기술

이중 랜덤 위상 인코딩을 이용한 광 메모리 암호화 기술은 백색잡음으로 영상이 암호화되므로 암호화 효과가 크지만 키로써 복소 공액의 위상 함수를 사용하므로 시스템의 정교한 정렬과 정밀한 마스크 키의 제작이 요구된다는 특징을 지닌다. 비트 평면 인코딩을 이용한 광 메모리 암호화 기술은 암호화 방법은 간단

하지만 광학적인 구현이 복잡하다는 특징을 지닌다. CGH를 이용한 광 메모리 암호화 기술은 CGH 키를 최적으로 설계함에 따라 이미지의 질이 향상[10]되고, CGH 키가 프로그래머블 SLM에 의해 생성되면 고속 랜덤 위상 키를 업데이트하는 것이 가능[9-10]하지만, SLM의 셀 크기가 고정되어 있으므로 생성될 수 있는 키 코드에 한계가 있다는 특징이 있다. 광 암호화를 이용한 광 메모리 암호화 기술과 보안 인증 기술은 광 메모리 시스템 또는 결합 변환 상관기(joint transform correlator: JTC), Vander Lugt 상관기(VanderLugt correlator: VLC), 주파수 평면 상관기(frequency plane correlator: FPC) 등을 토대로 실현된다. 본 장에서는 각 방식에 관한 대표적인 기술들의 동작 원리 및 특징에 대해 기술한다.

2.1 광 암호화를 이용한 광 메모리 암호화 기술

(1) 이중 랜덤 위상 인코딩을 이용한 광 메모리 암호화 기술

입력 평면과 퓨리에 평면에서 이중 랜덤 위상 인코딩을 이용한 광 메모리 암호화 기술[5-7]을 실현하기 위한 광학적 구성은 그림 1과 같다. 파장이 514.5nm인 레이저를 광원으로 이용하고, 랜덤 위상 함수는 32×32 셀들로 구성되며, 7.2mm×7.2mm의 크기로 제작되었다.

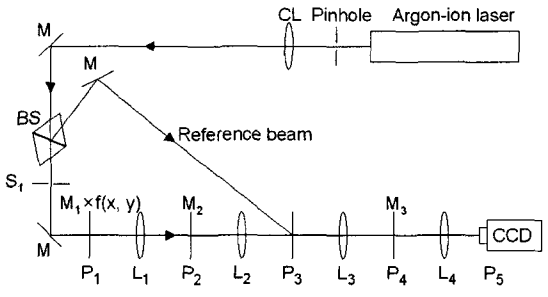


그림 1. 이중 랜덤 위상 인코딩 함수를 이용한 광 메모리 암호화 시스템

메모리 기록 과정은 다음 ①~④ 과정에 의해 생성된다.

① 암호화되려는 데이터 이미지는 P_1 평면에 놓이게 되고, 랜덤 위상 함수 M_1이 입력 평면에서 데이터 이미지에 곱해진다.

② 이미지와 랜덤 위상 함수의 곱에 대한 퓨리에 변환이 L_1에 의해 퓨리에 평면 P_2에서 얻어진 후, P_2 평면에 있는 또다른 랜덤 위상 함수 M_2와 곱해진다.

③ 또다른 퓨리에 변환이 렌즈 L_2에 의해 수행되고, 암호화된 이미지 데이터는 출력 평면 P_3 평면에서 얻어진다. P_3 평면에 광학 기록매질을 위치시킴으로써, 홀로그래픽 광 메모리에 저장된다.

④ 위의 ①~③ 과정을 반복함으로써, 다중 이미지가 서로 독립적인 다른 랜덤 위상 함수를 가지고 같은 메모리에 기록될 수 있다.

메모리 해독 과정은 다음 ①~② 과정에 의해 이뤄진다.

① P_3 평면에 놓인 암호화된 이미지에 대한 퓨리에 변환값은 렌즈 L_3에 의해 P_4 평면에서 얻어진다. 이때, P_4 평면에 놓인 랜덤 위상 함수 M_2의 공액 복소쌍인 랜덤 위상 함수 M_3와 곱해지게 된다.

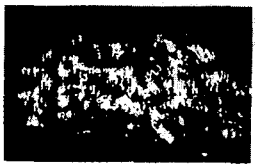
② 렌즈 L4에 의한 또다른 퓨리에 변환이 얻어지고, CCD 카메라에 의해 출력 평면 P_5에서 랜덤 위상 함수 M_1이 제거된 해독된 원래의 이미지 데이터가 얻어진다.

여기서, 랜덤 위상 함수는 복소 위상 인코딩 키를 말한다. 메모리 해독 과정에서, $M_3=M_2^*$는 해독을 위한 키로서 작용된 것이다. 이러한 키가 없으면 암호화된 이미지는 복구될 수 없다. 다중 이미지 메모리가 P_3 평면에 위치할 때, 특별한 데이터 이미지는 메모리로부터 대응하는 키 즉, 랜덤 위상 함수 M_3가 있어야만 해독될 수 있다. 반면, 다른 데이터는 암호화된 상태로 남아있게 된다.

입력 패턴으로는 지문, 얼굴 영상, 서명, ID 카드, 주민등록 번호, 화폐 등의 다양한 패턴을 이용할 수 있다. 그림 2(a)는 광학 실험에서 입력 패턴으로 이용된 문자 E와 Q 이미지로서, 서로 다른 랜덤 위상 함수를 사용함으로써 같은 메모리에 순차적으로 암호화된다. 그림 2(b)는 암호화된 메모리이고, 그림 2(c)는 평면 P_5에서 얻어진 해독된 데이터 이미지이다. 만일 틀린 위상 함수가 이미지를 해독하는데 이용된다면 그림 2(d)와 같이 단지 잡음만이 얻어지게 된다.

만일, 기록 이미지가 실수 이미지라면 위상 코드의 정확한 정렬이 퓨리에 평면에서만 요구되고, 기록 이미지가 복수 이미지라면 정확한 정렬이 공간 평면과 퓨리에 평면에서 모두 요구된다. 그 이유는 실수 이미지라면, 공간 평면에서의 위상 변조는 CCD에 의해 제거되기 때문이다. 그렇다 하더라도, 해독 과정에서 정밀한 정렬이 요구되므로 이러한 특성은 공간 평면과 퓨리에 평면에서 랜덤 위상 함수를 이용하는 시스템의 단점으로 작용한다.

(a) 입력 패턴



(b) 암호화된 메모리

(c) 해독된 데이터 이미지

(d) 틀린 위상 함수를 이용하여 해독된 이미지

그림 2. 광학 실험 데이터 및 실험 결과

(2) 프레넬 영역에서 3차원 키를 이용한 광 메모리 암호화 기술

1999년 O. Matoba와 B. Javidi[11]에 의해 제안된 이 방식은 프레넬 영역에서 두 개의 랜덤 위상 함수와 그들의 위치는 이미지를 암호화시키는 3차원 키로 이용되었고, 원래의 데이터를 복구하는 키로서 이용되었다. 즉, 위상 정보와 더불어, 두 개의 랜덤 위상 함수의 위치가 데이터를 해독하는 작업을 매우 어렵게 만드는 역할을 한다. 그림 3은 실험 구성을 보여준다.

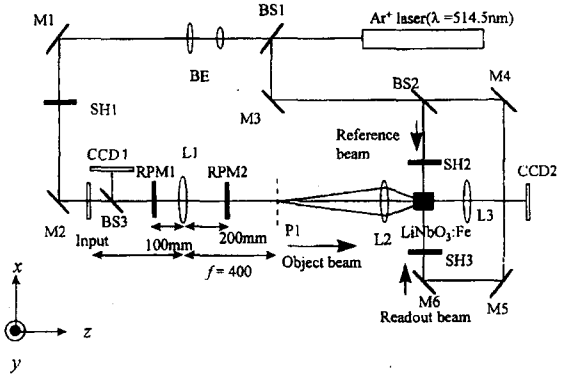


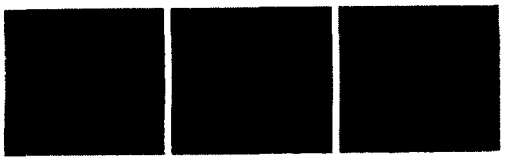
그림 3. 프레넬 영역에서 3차원 키를 이용한 광 메모리 암호화 시스템

파장이 514.5nm인 Ar 레이저가 광원으로서 이용되었다. 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 공액

쌍을 판독하기 위한 참조파로 분리되는 것이다. 입력 이미지는 평행광으로 조사된 후, 렌즈 L1에 의해 퓨리에 변환된다. 퓨리에 평면 P1을 지나, 축소된 퓨리에 변환된 이미지는 렌즈 L2에 의해 $LiNbO_3$ 결정에 기록된다.

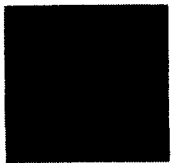
두 개의 랜덤 위상 함수 RPM1과 RPM2는 입력 평면과 L1 사이, 그리고, L1과 P1 사이에 위치한다. 따라서, 두 개의 랜덤 위상 함수가 입력 이미지를 해독하기 위한 3차원 키로서 제공되며 프레넬 영역에 위치하기 때문에, 위상 변조는 광축에 따른 위상 마스크의 위치에 의존한다. 이러한 의존이 3차원 키에 대한 정보가 없으면 해독을 어렵게 만드는 것이다. 참조파의 위상공액쌍을 이용하여 판독되는 이상적인 재생빔은 두 개의 랜덤 위상 함수에서 발생되는 위상 변조를 제거할 수 있기 때문에, 같은 위상 함수가 홀로그램이 기록된 곳과 같은 위치에 놓이게 된다면, CCD2에서 원 이미지의 재생을 얻을 수 있고, 위상 함수가 다른 경우는 원 이미지를 복원할 수 없다. 그 결과로서, 그림 4(a)는 3개의 입력 이미지를 보여주고, 그림 4(b)는 암호화된 이미지이며, 그림 4(c)은 기록에 이용된 같은 위치에 같은 위상 함수를 위치시킨 경우 재생된 이미지를 보여준다. 그림 4(d)는 광축을 따라 3.7mm만큼 위상 함수 RPM1이 천이된 경우 재생된 이미지이고, 그림 4(e)는 광축에 수직으로 40μm 만큼 위상 함수 RPM1이 천이된 경우 재생된 이미지로서, 그림 4(d)와 그림 4(e)는 이미지가 복원되지 않았음을 알 수 있다.

(a) 입력 이미지

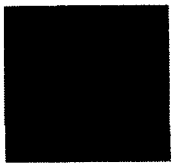


(b) 암호화된 이미지

(c) 기록에 이용된 같은 위치에 같은 위상 함수를 위치시킨 경우 재생된 이미지



(d) RPM1이 광축을 따라 3.7mm 천이된 경우 재생된 이미지



(e) RPM1이 광축에 수직으로 40μm 천이된 경우 재생된 이미지

그림 4. 광학 실험 데이터 및 실험 결과

(3) CGH를 이용한 광 메모리 암호화 기술

CGH를 이용한 홀로그래픽 광 메모리 암호화 장치의 대표적인 예로서, 1999년 T. Nomura와 B. Javidi[9]에 의해 제안된 이진 인코딩 알고리즘을 이용한 고속 광 메모리 암호화 기술과 2001년 T. Nomura와 B. Javidi[10]에 의해 제안된 최적으로 설계된 이진 CGH 키를 이용한 고속 광 메모리 암호화 기술을 들 수 있다. 특히, 최적으로 설계된 이진 CGH 키를 이용한 고속 광 메모리 암호화 방식은 CGH 키를 최적으로 설계함에 따라 이미지의 질이 향상된다는 특징을 지닌다. 이진 컴퓨터 생성 홀로그램에 의해 설계된 이진 키 코드를 이용한 광 암호화 시스템으로서, 이러한 이진 키를 CGH 키라 한다.

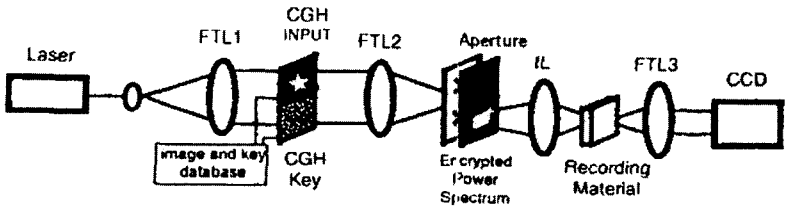


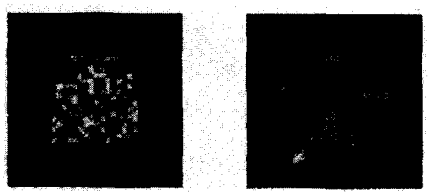
그림 5. JTC 구조를 토대로 이진 CGH 키 코드를 이용한 이중 랜덤 위상 암호화 시스템. FTL: 퓨리에 변환 렌즈, IL: 이미징 렌즈

그림 5는 JTC 구조를 토대로 이진 CGH 키 코드를 이용한 이중 랜덤 위상 암호화 시스템이다. 입력 랜덤 위상 마스크와 접촉되어 암호화될 입력 이미지와, 퓨리에 위상 마스크의 퓨리에 변환 CGH로서 합성된 CGH 키가 입력 평면에 차례대로 놓여진다. 암호화되려는 이미지와 CGH 키 모두 데이터베이스에 저장되고, 이진 SLM인 ferroelectric 액정 디스플레이 장치에 고속으로 업데이트될 수 있다.

기존의 이진 우회 위상 CGH에서, 설계된 파면은 1차 회절 빔으로 재생되었다. 그러므로, 필요한 신호를 추출하기 위해 개구면을 이용한다. 입력 이미지들의 결합 퓨리에 전력 스펙트럼과 CGH 키는 이미징 렌즈를 통해 암호화된 결합 전력 스펙트럼으로서 기록 매질에 기록되는 암호화 과정이 이뤄졌다. 해독과정에서, 암호화된 결합 전력 스펙트럼이 같은 CGH 키의 1차 회절 빔에 의해 조사된다면, 이미지는 정확하게 해독될 수 있었다.

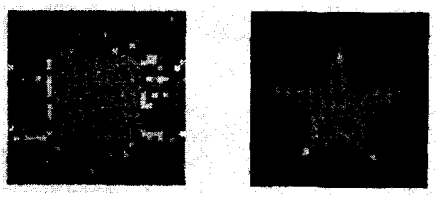
암호화 시스템에서, CGH 키는 다음의 두 가지 제약조건들을 만족해야만 한다. 첫째, 키의 퓨리에 변환의 1차 진폭 분포는 균일하다. 둘째, 키의 퓨리에 변환의 1차 위상 분포는 균일하게 랜덤하다. 그러나, 기존의 CGH 키는 제약조건들을 만족하지 않는다. 그림 6(a)는 기존의 우회 위상 기법에 의해 생성된 CGH 키의 1차 진폭 분포로서, 분포가 균일하지 않음을 알 수 있다. 그림 6(b)는 기존의 CGH 키를 이용해 해독된 이미지이다. 키가 이상적이라면, 해독된 이미지는 이진 별모양 이미지이다. 이미지의 질이 키의 진폭 변조 때문에 좋지 않다.

최적으로 설계된 이진 CGH 키를 적용하면 이러한 문제를 해결할 수 있다. 균일한 CGH 키의 1차 진폭 분포를 만들기 위해, SA 알고리즘을 이용해 키를 설계하였다. 이러한 시뮬레이션에서, 1차 위상 분포는 고려하지 않았다. 그림 7(a)는 최적으로 설계된 키의 1차 진폭 분포를 컴퓨터 시뮬레이션으로 나타낸 것으로서, 분포가 균일함을 알 수 있다. 1차 진폭 분포와 위상 분포의 히스토그램은 그림 8에 나타내었다. 진폭 분포가 거의 균일하며, 위상 분포를 고려하지 않더라고 키가 균일하게 랜덤함을 주시하자. 해독된 이미지를 그림 7(b)에 나타내었다. 이미지의 질이 기존의 CGH 키에 비해 개선되었음을 알 수 있다.



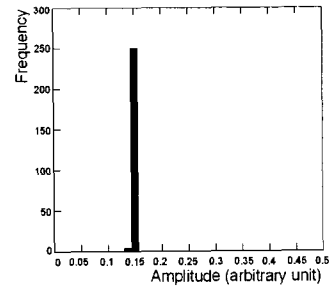
(a) CGH 키의 1차 진폭 분포 (b) 해독된 이미지

그림 6. 기존의 우회 위상 기법에 의해 생성된 CGH 키의 1차 진폭 분포와 해독된 이미지

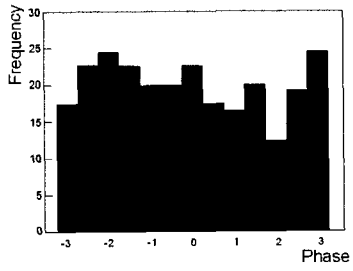


(a) CGH 키의 1차 진폭 분포 (b) 해독된 이미지

〈그림 7〉 최적으로 설계된 CGH 키의 1차 진폭 분포와 해독된 이미지



(a) 진폭 분포의 히스토그램



(b) 위상 분포의 히스토그램

〈그림 8〉 최적으로 설계된 CGH 키의 1차 진폭 분포와 위상 분포의 히스토그램

2.2 광 암호화를 이용한 보안 인증 기술

(1) 위상 인코딩 키를 이용한 보안 인증 기술

1994년 B. Javidi와 J. L. Horner[12]에 의해 제안된 이 방식에서는 쉽게 복제할 수 없는 신용카드, 여권 등을 만들기 위한 보안 인증 기술로서 입력 평면에서 위상 인코딩 키를 이용한다. 입력 이미지를 위상 인코딩시킨 후, $0 \sim 2\pi$에서 균일하게 분포된 랜덤 위상 함수와 곱한다. 즉, 영구히 검색할 수 없게 랜덤 위상 함수와 결합시킨다. 그 결과와 참조 이미지와의 상관 피크치를 CCD 카메라를 통해 출력 평면에서 검출하게 된다.[12-13] 이러한 과정을 수행하기 위한 광 상관 처리 시스템으로는 결합 변환 상관기, 주파수 평면 상관기, VanderLugt 상관기 등의 광 상관기가 주로 이용된다.

그림 9는 비선형 결합 변환 상관기를 이용한 광 상관 처리 시스템으로서, 보안 인증 시스템이다. 입력 랜덤 위상 함수와 참조 랜덤 위상 함수 사이의 상관을 구하거나, 입력 이미지와 참조 이미지 사이의 상관을 구하는데 이용되었다. 즉, 비선형 결합 변환 상관기는 랜덤 위상 함수를 검증함으로써 ID 카드가 인지된 카드인지 또는 지문과 같은 입력 이미지를 검증함으로써 카드가 인지된 사람의 것인지를 판별하는 것이다. 이 시스템은 그림 10과 같이 홀로그래픽 위상 인코딩 ID 카드로서, 고성능 · 초고속 · 대용량의

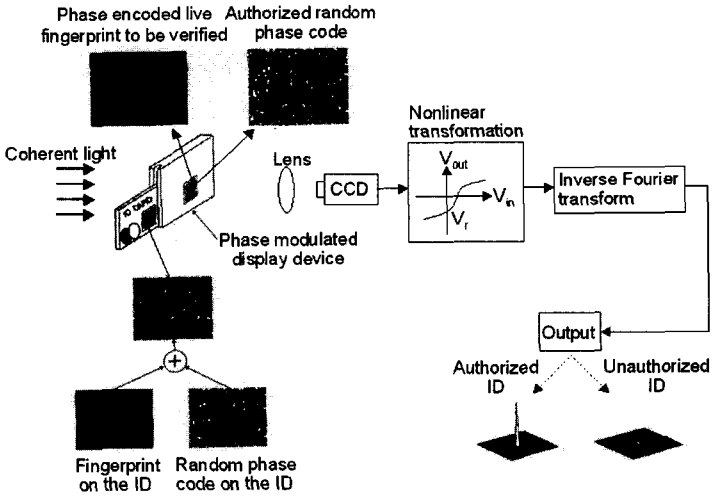


그림 9. 광 암호화를 이용한 보안 인증 시스템

차세대 스마트 카드로도 응용될 수 있으며, 기존의 카드를 대체할 새로운 기술로 주목받고 있다. 또한, 제한구역의 접근 허가를 위하여 개개인의 진위를 확인하는 안전한 출입시스템에도 적용할 수 있다.

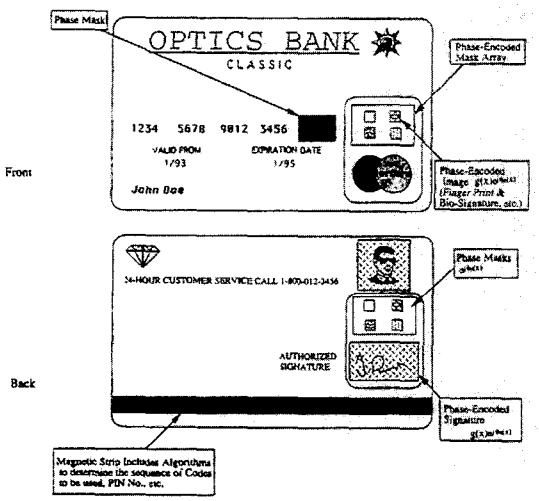


그림 10. 위상 인코딩 ID 카드

3. 결 론

임의의 정보 보호 기술에 대한 필요성은 수많은 통계 자료로부터 알 수 있으며, 위조품의 사용에 따른 사고율도 현저히 증가하고 있다. 또한, 제한 구역의 접근 허가를 위해 관계자를 확인하는 보안 시스템의 기억장치를 도난 당하거나 허가받지 않은 사람이 보안 시스템 통신망의 전송선을 모니터링하여 중요한 정보를 취득할 수 있으므로, 정보 보호는 필수적인 일이 되었다. 따라서, 사람이나 제품에 대한 진위 여부를 신빙성 있게 증명할 수 있는 암호화 시스템의 수요가 점차 증가되고 있는데, 현재 연구되고 있는 광기술을 이용한 광 메모리 암호화 시스템과 보안 인증 시스템은 암호화 키와 동일한 해독 키가 존재하지 않으면 암호화된 정보를 복원할 수 없는 신뢰도가 매우 우수한 성능의 시스템이다.

광기술을 이용한 광 메모리 암호화 시스템과 보안 인증 시스템은 카드 및 여권의 위조나 복제를 근본적으로 차단할 수 있고, 보안 시스템 상에서 발생할 수 있는 불법적인 데이터 유출을 방지할 수 있는 차세대 정보보안 시스템으로서, 정부 기관의 신분 보안 및 복제방지 시스템 · 출입 관리 시스템, 금융 기관의 신분보안 인증 시스템 · 신용카드 결제 시스템, 초고속 정보 통신 분야의 도청 방지 시스템, 네트워크 산업 분야의 정보보호 광학 데이터베이스 시스템, 인터넷 전자상거래 분야의 정보보호 및 검색 시스템, 차세대 IC 카드 및 카드리더 시스템 등 우리의 실생활에 직접 사용할 수 있는 신뢰성이 뛰어난 정보 보호 및 보안 인증 시스템으로 이용될 수 있으며, 향후 보다 안전한 시스템 개발에 선두 역할을 할 수 있을 것으로 기대된다.

참 고 문 헌

[1] J. S. Yoon and N. Kim, "Triple encryption packaging scheme for preserving from the reproduction and protecting the information," Jpn. J. Appl. Phys., PT. 2, vol. 41, no. 3B, pp. L305-L306, Mar. 2002.

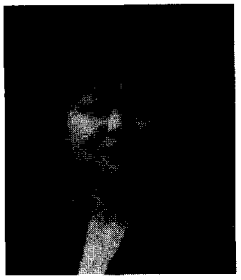
[2] 윤진선, 김남, 전용성, 정교일, "광기술을 이용한 정보보안", 전자공학회지, 제28권 제6호, pp. 65-72, 2001년 6월.

[3] 한국전자통신연구원, "차세대 IC 카드를 위한 홀로그래픽 위상 패턴을 이용한 신분 복제방지 기술에 관한 연구", 2000년 11월.

[4] 김승주, 이홍섭, "암호기술 동향," 전자공학회지, 제28권 제6호, pp. 22-29, 2001년 6월.

[5] Ph. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20, no. 7, pp. 767-769,

Apr. 1995.
[6] B. Javidi, G. Zhang, and J. Li, "Encrypted optical memory using double-random phase encoding," Appl. Opt., vol. 36, no. 5, pp. 1054-1058, Feb. 1997.
[7] B. Javidi, G. Zhang, and J. Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," Opt. Eng., vol. 35, no. 9, pp. 2506-2512, Sept. 1996.
[8] J. W. Han, C. S. Park, D. H. Ryu, and E. S. Kim, "Optical image encryption based on XOR operation," Opt. Eng., vol. 38, no. 1, pp. 47-54, Jan. 1999.
[9] T. Nomura and B. Javidi, "High-speed optical encryption using binary encoding algorithms," LEOS '99, vol. 1, pp. 192-193, Nov. 1999.
[10] T. Nomura, B. Javidi, S. Mikan, and Y. Morimoto, "Optical image encryption using an optically designed encryption key," CLEO/Pacific Rim 2001, vol. 2, pp. 492-493, 2001.
[11] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett., vol. 24, no. 11, pp. 762-764, June 1999.
[12] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng., vol. 33, no. 6, pp. 1752-1756, June 1994.
[13] B. Javidi and A. Sergent, "Fully phase encoded key and biometrics for security verification," Opt. Eng., vol. 36, no. 3, pp. 935-942, Mar. 1997.
[14] M. Yamazaki, "Optimization of encrypted holograms in optical secirity systems", Opt. Eng., vol. 40, no. 1, pp. 132-137, Jan. 2001.
[15] K. H. Fielding, J. L. Horner, and C. K. Makekau, "Optical fingerprint identification by binary joint transform correlation", Opt. Eng., vol. 30, no. 12, pp. 1958-1961, Dec. 1991.



윤 진 선

1992年 2月 : 충북대학교 정보통신공학과(공학사),
1997年 2月 : 충북대학교 정보통신공학과(공학석사)
2002年 8月 : 충북대학교 정보통신공학과(공학박사)
▶주관심 분야 : Optical Encryption, Optical Security, Optical Pattern Recognition, Optical Information Processing, Optical Interconnection

김 남

1981年 2月 : 연세대학교 전자공학과(공학사)
1983年 2月 : 연세대학교 전자공학과(공학석사)
1988年 8月 : 연세대학교 전자공학과(공학박사)

1992年 8月-1993 年 8 月 : 미 Stanford대학 방문교수, 2000年 3月-2001年 2月 : 미국 caltech 방문교수, 1992年 8月-현재 : 충북대학교 전기전자공학부 교수. ▶주관심 분야 : Optical Encryption, Optical Security, Diffractive Optics, Optical Memory, Holography Application