특 집

광기술을 이용한 정보보안

윤 진 선*, 김 남*, 전 용 성**, 정 교 일**
*충북대학교 전기전자공학부, **한국전자통신연구원

I. 서 론

일반적인 보안 시스템에서 데이터가 외부로 유출될 경우 손쉽게 데이터의 복사가 이루어지게 될 수 있으므로 안전성에 문제가 발생할 수가 있게 된다. 또한 영상 회의 시스템이나 2차원 데이터 저장을 위한 메모리 등에도 제3자에 의한 불법적인 도청이나 접근 시도로부터 원래의 정보를 안전하게 보호할 수 있어야 하므로 이에 대한 해결책으로 저장된 정보나 전송로 상에서 전달되는 정보에 대한 암호화 방법들이 연구, 제안되고 있다.

특히 여권, 신용카드, 각종 카드 등의 위조 여부를 확인하기 위한 수단으로 사진, 얼굴, 지문 등이 사용되고 있으나 최근, 영상처리용 소프트웨어와 컴퓨터, 프린터, 스캐너, 복사기와 같은 하드웨어 기술의 발달과 더불어 각종 카드, 로고, 화폐, 그림 등의 위조가 고도로 정교하게 이루어지고 있어 현대 신용 사회에서 심각한 사회적 문제로 대두되고 있다.

근래에는 보다 발전된 형태로 신용카드와 여권 등에 홀로그램이 널리 이용되고 있으나 이것은 사람의 눈에 의해 식별되는 것으로 이론적으로는 복제될 수 없지만 실제의 경우 홀로그램 패턴이 광세기 패턴으로 사진 또는 CCD와 같은 기존의 광 검출기로 쉽게 검출되어 새로운 홀로그램의 합성과 복제가 가능하게 된다. 따라서 카드 위조나 복제를 근본적으로 차단할 수 있는 시스템의 설계가 시급히 요구되고 있다. 또한 인터넷을 이용한 전자상거래 및 주식, 각종 금융거래가 이루어짐에 따라 해킹 사고가 급속히 증가하였다.

이와 같은 시대적·사회적 요구로 인해 최근 광기술을 이용한 광 암호화 시스템과 광 인증 시스템이 광 메모리와 광 정보처리 분야에서 활발하게 연구되고 있다. 그들 중 많은 방법들이 데이터를 암호화하는데 복소 위상 인코딩 기술(홀로그래픽 위상 패턴 기술)을 이용한다. 이러한 복소 위상 인코딩 패턴은 현미경, 사진, 컴퓨터 스캐너 등을 이용해서 복제될 수 없으므로 데이터를 암호화하고, 인증되지 않은 사용자로부터 메모리로의 접근을 보호할 수 있게 해준다.

광 암호화를 적용한 응용기술 분야는 초고속 정보 통신 분야, 초고속 대용량 광정보 저장 분야 및 광정보 처리 분야 등과 맞물려 있는 핵심 기술로서 정보 통신 산업, 멀티미디어 산업, 광산업 등에만 국한되는 것이 아니고 다양한 응용분야로 전개될 가능성이 높은 기술로 파악되고 있으며, 가까운 장래에 우리나라에서도 상용화를 기대할 수 있는 분야로 예측된다.

II. 광 암호화 및 보안 인증 시스템의 기술 동향 및 분석

광기술을 이용한 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 패턴인식 시스템과 암호화 기술 등의 활발한 연구가 진행되고 있으나, 아직까지는 주로 대학과 연구소를 중심으로 하는 초보적인 단계이다.

최근 활발히 연구 보고 되고 있는 광 암호화를 이용한 암호화된 광 메모리 기술과 보안 인증 기술에 관한 가장 대표적인 방식에는 퓨리에 영역에서 랜덤 위상 마스크를 곱한 후 다시 역퓨리에 변환하여 암호화된 영상을 얻는 방식과 XOR 연산을 이용하는 방식, 그리고 광학적 간섭 특성을 이용한 방식 등이 있다. 랜덤 위상 마스크를 이용한 암호화된 광 메모리 기술은 백색잡음으로 영상이 암호화되므로 암호화 효과가 크지만 키로써 복소 공액의 위상 마스크를 사용하므로 시스템의 정교한 정렬과 정밀한 마스크 제작이 요구된다는 특징을 지닌다. XOR 연산을 이용한 암호화된 광 메모리 기술은 암호화 방법은 간단하지만 광학적인 구현이 복잡하다는 특징을 지닌다. 광학적 간섭을 이용한 암호화된 광 메모리 기술은 키와 암호화된 영상이 세기 검출기로는 확인이 되지 않아 복제가 어렵고 단순한 시스템이 구현된다는 특징이 있다. 본 장에서는 각 방식에 관한 대표적인 기술들의 동작 원리 및 특징에 대해 기술한다.

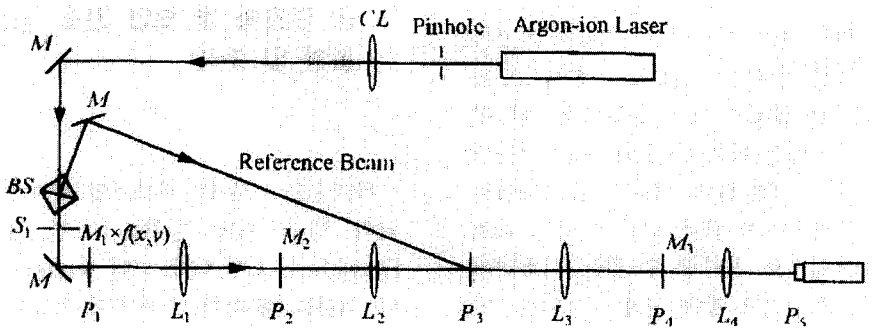
1. 광 암호화를 이용한 암호화된 광 메모리 기술

1) 두개의 랜덤 위상 마스크를 이용한 암호화된 광 메모리 기술

광 메모리의 암호화 기술을 실현하기 위한 광학적 구성은 〈그림 1〉과 같다. 파장이 514.5nm인 레이저를 광원으로 이용하고, 랜덤 위상 마스크는 32×32 셀(7.2mm×7.2mm)로 구성되며, 두개의 랜덤 위상 마스크를 입력 평면과 퓨리에 평면에 각각 위치시킨다. 대부분의 광 암호화 시스템에서 암호화 키로서 주로 이용되는 복소 위상/진폭 인코딩 패턴(랜덤 위상 마스크)은 볼 수도 없고, CCD 카메라와 같은 세기측정 검출기에 의해 복사될 수도 없다.

암호화되려는 데이터 이미지는 P_1 평면에 놓이고, 랜덤 위상 마스크 M_1과 곱해진다. 데이터 이미지와 랜덤 위상 마스크의 곱에 대한 퓨리에 변환이 L_1에 의해 퓨리에 평면 P_2에서 얻어진 후, P_2 평면에 있는 랜덤 위상 마스크 M_2와 곱해진다. 그 결과는 렌즈 L_2에 의해 퓨리에 변환이 수행되고, 암호화된 데이터 이미지가 출력 평면 P_3 평면에서 얻어지므로 광학 기록매질을 위치시킴으로써, 홀로그래픽 광 메모리에 저장된다. 이러한 과정을 반복함으로써, 다중 이미지가 서로 독립적인 다른 랜덤 위상 마스크를 가지고 같은 메모리에 암호화되어 기록된다.

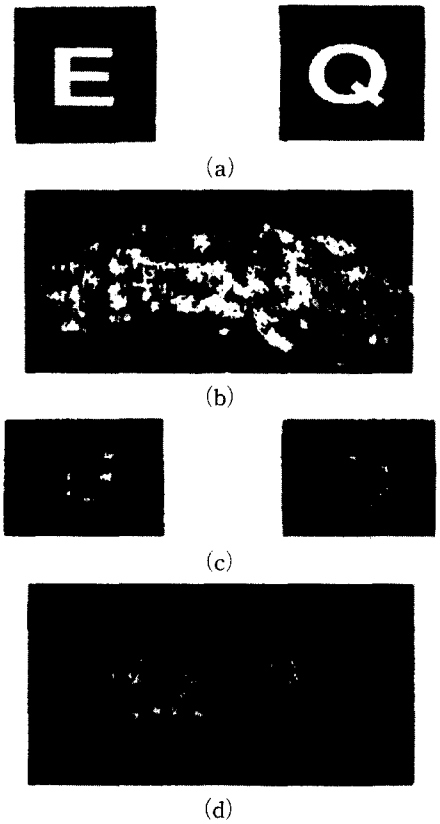
P_3 평면에 놓인 암호화된 이미지에 대한 퓨리에 변환값은 렌즈 L_3에 의해 P_4 평면에서 얻어진다. 이때, P_4 평면에 놓인 랜덤 위상 마스크 M_2



〈그림 1〉 암호화된 광 메모리 시스템

의 공액 복소쌍인 랜덤 위상 마스크 M_3와 곱해지게 된다. 렌즈 L_4에 의해 퓨리에 변환된 결과가 얻어지고, CCD 카메라에 의해 출력 평면 P_5에서 랜덤 위상 마스크 M_1이 제거된 해독된 이미지 데이터가 얻어진다. 해독 과정에 서, $M_3 = M_2^*$가 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(랜덤 위상 마스크 M_3)가 있어야만 해독될 수 있다. 반면, 다른 데이터는 암호화된 상태로 남아 있게 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 마스크를 사용함으로써 같은 메모리에 순차적으로 암호화된다. 〈그림 2(b)〉는 암호화된 메모리이고, 〈그림 2(c)〉는 평면 P_5에서 얻어진 해독된 데이터 이미지이다. 비록 영상이 제대로 복원은 되었지만, 약간의 clutter 잡음이 존재함을 볼 수 있다. 그 이유는 시스템의 대역폭이 제한되고, 제작된 홀로그래픽 위상 마스크의 공간 대역폭 곱이 제한되기 때문이다. 만일 틀린 위상 마스크가 이미지를 해독하는데 이용된다면 〈그림 2(d)〉와 같이 단지 잡음만이 얻어지게 된다.



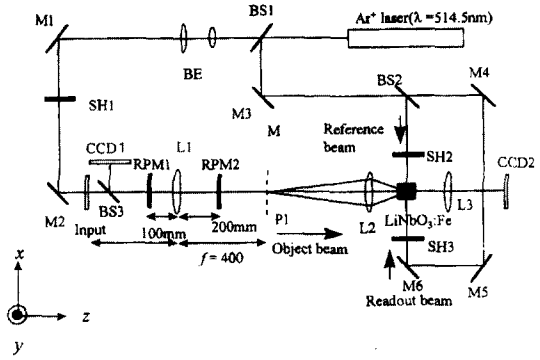
〈그림 2〉 광학 실험 데이터 및 실험 결과
(a) 입력 패턴, (b)는 암호화된 메모리,
(c) 해독된 데이터 이미지,
(d) 틀린 위상 마스크를 이용하여 해독된 이미지

공간 또는 퓨리에 평면에서의 홀로그래픽 위상 마스크로서 전자적으로 주소가 부여되는 위상형 SLM을 이용할 수도 있다. 이러한 시스템이 구성된다면, 시스템을 구성할 때 단지 한번만 정교한 정렬을 해주면 되므로 홀로그래픽 위상 마스크의 제작 과정이 필요없게 되어 더욱 단순하고, 실시간 제어가 용이한 정보보안 시스템이 구현될 수 있다.

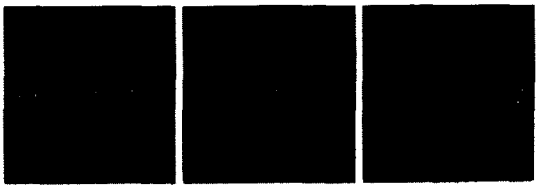
2) 프레넬(Fresnel) 영역에서 3차원 키를 이용하여 암호화된 광 메모리 기술

프레넬 영역에서 두 개의 랜덤 위상 마스크와 그들의 위치는 이미지를 암호화시키는 3차원 키로 이용되었고, 원래의 데이터를 복구하는 키로서 이용되었다. 〈그림 3〉은 실험 구성으로서, 두 개의 랜덤 위상 마스크가 입력 이미지를 해독하기 위한 3차원 키로서 제공되며 프레넬 영역에 위치하기 때문에, 위상 변조는 광축에 따른 위상 마스크의 위치에 의존한다. 따라서, 위상 정보와 더불어 3차원 키에 대한 정보가 없으면 해독을 어렵게 만드는 것이다.

참조파의 위상공액쌍을 이용하여 판독되는 이상적인 재생빔은 두개의 랜덤 위상 마스크에서 발생되는 위상변조를 제거할 수 있기 때문에, 같은 위상 마스크가 홀로그램이 기록된 곳과 같은 위치에 위치된다면, CCD2에서 원 이미지를 해독할 수 있고, 위상 마스크가 다른 경우는 원 이미



〈그림 3〉 랜덤 위상 마스크와 그들의 위치에 따른 광 암호화 시스템

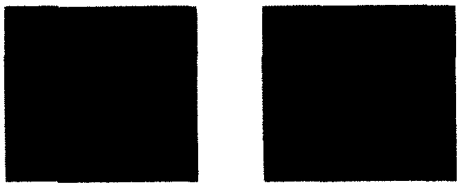


〈그림 4〉 입력 패턴

〈그림 5〉 암호화된 메모리

〈그림 6〉 기록에 이용된 같은 위치에 같은 위상 마스크를 위치시킨 경우 해독된 이미지

지를 복원할 수 없다. 그 결과로서, 〈그림 4〉는 3개의 입력 패턴을 보여주고, 〈그림 5〉는 암호화된 메모리이고, 〈그림 6〉은 기록에 이용된 같은 위치에 같은 위상 마스크를 위치시킨 경우 해독된 이미지를 보여준다. 〈그림 7〉은 광축을 따라 3.7 mm 또는 수직으로 40 m 만큼 위상 마스크가 천이된 경우 해독된 이미지를 나타낸다.



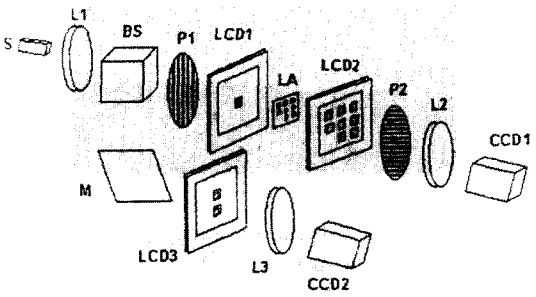
(a) (b)

〈그림 7〉 랜덤 위상 마스크가 틀린 위치에 놓일 때 해독된 이미지

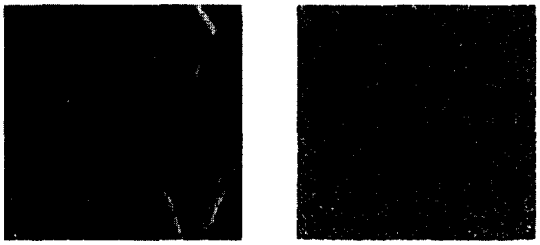
3) XOR 연산을 이용한 암호화된 광 메모리 기술

〈그림 8〉은 제안된 광학적 보안 시스템으로서, 디지털 암호화 알고리즘으로 만들어진 키 비트 열(key bit stream)과 비트 평면들을 나타내는데 두 LCD(liquid crystal display)를 사용하고, 결합 변환 상관기(JTC : joint transform correlator)를 구성하기 위하여 또 다른 LCD를 사용한다. LCD1, LCD2, 두 개의 편광기(P1과 P2), 렌즈 L2, CCD1을 이용하여 XOR 연산이 수행된다.

입력 그레이 레벨의 영상은 열 암호 시스템에서 암호화 방법으로 사용되는 XOR 연산을 수행하기 위하여 이진 영상으로 전환되어야 하므로, 8개의 비트 평면으로 바뀌어 LCD2에 디스플레이 된다. LCD1에 나타낸 키 비트 열은 렌즈 배열(LA)로 8개 비트 평면으로 재생성 되어 키 비트 열과 비트 평면 사이의 광학적 XOR 연산이 LCD의 편광 특성을 이용하여 수행되어 암호화가 된다. 그 결과는 CCD로 검출되며 암호화된 그레이 레벨 영상으로 변환된다.



〈그림 8〉 제안된 인증 시스템



(a) (b)

〈그림 9〉 (a) 암호화될 입력 패턴, (b) 랜덤 키 비트 열

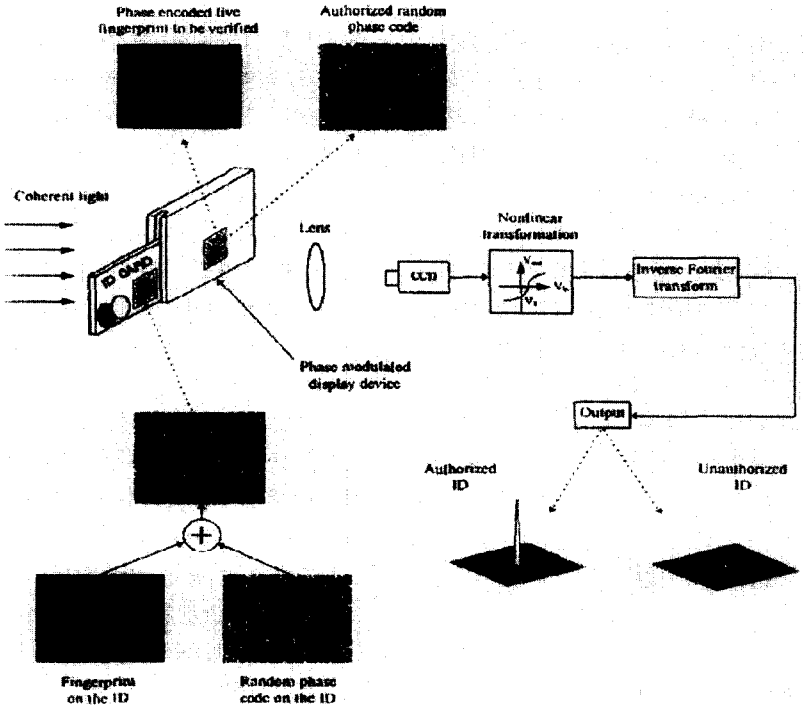
이와 같이 암호화된 영상은 데이터베이스화된 참조 영상과 비교되기 위하여 결합 변환 상관기의 입력(LCD3)으로 이용된다. 참조 영상과 입력 영상은 암호화된 영상으로 사용되기 때문에 제안된 시스템은 안전하다. 암호화된 영상을 광학적으로 해독하려면, 암호화 영상의 비트 평면들이 〈그림 8〉처럼 LCD2에 나타나야만 한다. 암호화 과정에서 사용한 키 비트 열과 암호화 영상의 비트 평면 사이의 광학적 XOR 연산이 수행되어지고 광학적 XOR 연산의 결과는 CCD1으로 검출된다.

〈그림 9〉는 컴퓨터 시뮬레이션을 하기 위한 입력 패턴으로서, (a)는 입력 패턴, (b)는 키 비트 열이다. 해독 과정에서 암호화 과정에서 이용된 같은 키 비트 열을 사용하면, (a)와 동일하게 해독된 이미지를 얻을 수 있다.

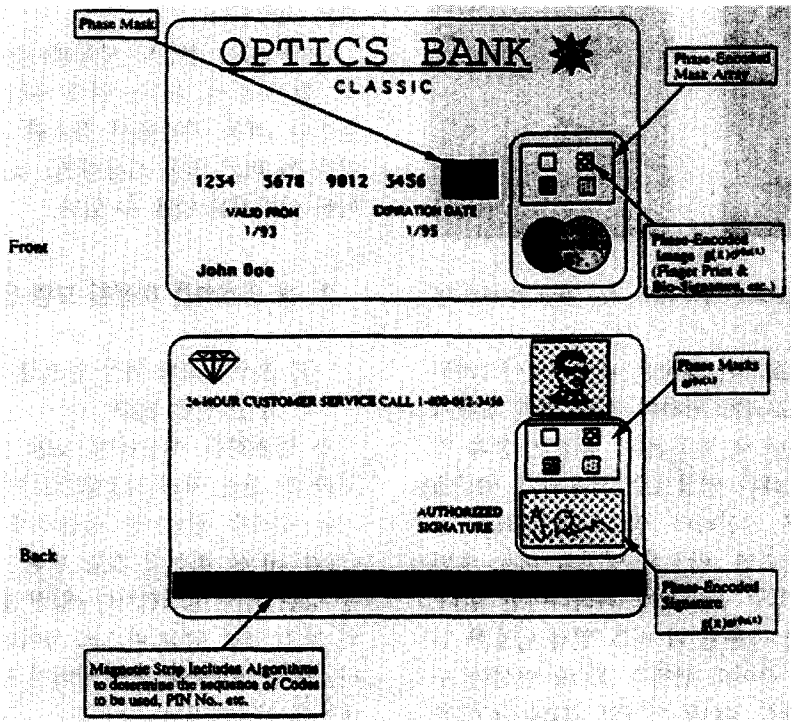
2. 광 암호화를 이용한 보안 인증 기술

1) 홀로그래픽 위상 인코딩 키를 이용한 보안 인증 기술

광 암호화를 이용하여 보안 인증을 수행하기 위한 광 상관 처리 시스템으로는 결합 변환 상관기와 주파수 평면 광 상관기가 주로 이용된다. 〈그림 10〉은 비선형 결합 변환 상관기를 이용한 광 상관 처리 시스템이다. 입력 랜덤 위상 마스크와 참조 랜덤 위상 마스크 사이의 상관을 구하거나, 입력 이미지와 참조 이미지 사이의 상관을 구하는데 이용되었다.



〈그림 10〉 광 암호화를 이용한 보안 인증 시스템



〈그림 11〉 홀로그래픽 위상 인코딩 ID 카드

입력 이미지를 위상 인코딩시킨 후, $0\sim2\pi$에서 균일하게 분포된 랜덤 위상 마스크와 곱한다. 즉, 영구히 검색할 수 없게 랜덤 위상 마스크와 결합된 후, 참조 이미지와의 상관 피크치를 CCD를 통해 출력 평면에서 검출한다. 랜덤 위상 마스크를 검증함으로써 ID 카드가 인증된 카드인지 또는 입력 이미지(지문)를 검증함으로써 카드가 인증된 사람의 것인지를 판별하는 것이다. 이 시스템은 〈그림 11〉과 같이 위상 인코딩 ID 카드 기술로도 적용이 가능하다. 즉, 제한구역의 접근 허가를 위하여 개개인의 진위를 확인하는 안전한 출입시스템에도 적용할 수 있다.

Ⅲ. 결 론

임의의 정보 보호 기술에 대한 필요성은 수 많은 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 중요한 데이터가 보안 시스템 통신망의 전송선을 모니터링하여 가로채이게 된다면 허가받지 않은 사람이 용이하게 중요한 정보를 취득하게 되므로 정보보호는 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 암호화된 메모리 시스템 및 보안 인증 시스템은 동일한 암호화 키가 존재하지 않으면 암호화된 이미지를 복원할 수 없는 신뢰도가 매우 우수한 성능의 시스템이다.

광기술을 이용한 암호화된 메모리 시스템 및 보안 인증 시스템은 카드 및 여권의 위조나 복제를 근본적으로 차단할 수 있고, 보안 시스템 상에서 발생할 수 있는 불법적인 데이터 유출을 방지할 수 있는 시스템으로서, 정부의 신분 보안 시스

템, 금융의 신용카드 결제 시스템, 통신 분야의 도청 방지 시스템, 네트워크 산업 분야의 정보보호 광학 데이터베이스(secure optical database) 시스템, 자동차 기술 분야의 부품 도용 방지 시스템, 의료 분야의 의약품 도용 방지 시스템, 의류 분야의 브랜드 도용 방지 시스템, 인터넷 전자상거래 분야의 정보보호 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.

감사의 글

본 원고는 2000년도 한국전자통신연구원의 연구지원으로 수행되었으며, 지원에 감사드립니다.

참 고 문 헌

〔1〕 B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification", Opt. Eng., 33 (6), pp. 1752-1756, June 1994.

〔2〕 B. Javidi, G. Zhang, and J. Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification", Opt. Eng., 35(9), pp. 2506-2512, Sept. 1996.

〔3〕 B. Javidi and A. Sergent, "Fully phase encrypted key and biometrics for security verification", Opt. Eng., 36(3), pp. 935-942, March 1997.

〔4〕 B. Javidi, G. Zhang, and J. Li, "Encrypted optical memory using double-random phase encoding", Appl. Opt., 36(5), pp. 1054-1058, Feb. 1997.

〔5〕 P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding", Opt. Letters, 20(7), pp. 767-769, April 1995.

〔6〕 O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain", Opt. Letters, 24(11), pp. 762-764, June 1999.

〔7〕 B. Javidi, L. Bernard, and N. Towghi, "Noise performance of double-phase encryption compared to XOR encryption", Opt. Eng., 38(1), pp. 9-19, Jan. 1999.

〔8〕 J. W. Han, C. S. Park, D. H. Ryu, and E. S. Kim, "Optical image encryption based on XOR operations", Opt. Eng., 38(1), pp. 47-54, Jan. 1999.

〔9〕 K. H. Fielding, J. L. Horner, and C. K. Makekau, "Optical fingerprint identification by binary joint transform correlation", Opt. Eng., 30(12), pp. 1958-1961, Dec. 1991.

〔10〕 M.Yamazaki, "Optimization of encrypted holograms in optical secirity systems", Opt. Eng., 40(1), pp. 132-137, Jan. 2001.

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

저 자 소 개

尹鎭善

1969년 2월 4일생, 1992년 2월 충북대학교 정보통신공학과(공학사), 1997년 2월 : 충북대학교 정보통신공학과(공학석사), 2000년 2월 충북대학교 정보통신공학과 박사과정 수료, 1993년 9월~1995년 9월 : 옥천공동직업훈련원 정보통신공과 교사, 〈주관심 분야 : Optical Encryption, Optical Security, Optical Pattern Recognition, Optical Information Processing, Optical Interconnection〉

金 男

1959년 3월 30일생, 1981년 2월 연세대학교 전자공학과(공학사), 1983년 2월 연세대학교 전자공학과(공학석사), 1988년 8월 연세대학교 전자공학과(공학박사), 1992년 8월~1993년 8월 : 미 Stanford대학 방문교수, 2000년 3월~2001년 2월 : 미국 caltech 방문교수, 1992년 8월~현재 : 충북대학교 전기전자공학부 교수, 1995년 4월~현재 : 한국전자파학회 표준규격심의위원, 1998년 4월~현재 : 3D 선행기술교류회 위원, 1997년 11월~현재 : 옥천전문대학교 운영위원, 〈주관심 분야 : Diffractive Optics, WDM Optical Filter & DEMUX, Optical Memory, Holography Application, 디지털 이동통신, EMI/EMC 및 전자파 인체보호 규격〉

全容成

1968년 5월 18일생, 1990년 2월 경북대학교 전자공학과(공학사), 1992년 2월 경북대학교 전자공학과(공학석사), 1992년 3월~1999년 10월 : 국방과학연구소 선임연구원, 1999년 11월~현재 : 한국전자통신연구원 정보보호연구본부 IC 카드 OS 연구팀 선임연구원, 〈주관심 분야 : 디지털 회로 설계, 생체인식, 영상처리 등임〉

鄭敎逸

1957년 11월 3일생, 1981년 2월 한양대학교 전자공학과(공학사), 1983년 8월 한양대학교 산업대학원 전자계산학과(공학석사), 1997년 8월 한양대학교 대학원 전자공학과(공학박사), 1992년 3월~1999년 10월 : 국방과학연구소 선임연구원, 1981년 12월~현재 : 한국전자통신연구원 정보보호연구본부 기반연구부 부장/책임연구원, 〈주관심 분야 : IC Card, Security, Biometry, 정보전, 신호처리〉