홀로그래픽 암호화 기법을 적용한 스마트카드 위·변조 차단

장 홍 종† · 이 성 은†† · 이 정 현†††

요 약

기존의 스마트카드는 사용자의 인증, 접근제어, 정보 저장·관리기능 등을 수행하기에 보안성이 매우 뛰어난 기반으로 부각되고 있으며 시장 또한 급성장하고 있다. 그러나 이런 급성장에 따라 해킹에 의한 위·변조 가능성 역시 점점 더 높아지고 있다. 이에 본 논문에서는 홀로그래픽 암호화 기반에서 각 다중화 및 암호키 다중화 기법을 사용하여 위·변조를 차단하였다. 또한 스마트카드 칩과 홀로그래픽 메모리 칩을 채택하여 기존의 스마트카드에서는 불가능했던 위·변조의 검증이 가능한 시스템을 제안하였다.

Cut off of Smartcard Forgery and Alteration Based on Holographic Security Encryption

Hong-Jong Chang† · Seong-Eun Lee†† · Jung-Hyun Lee†††

ABSTRACT

Smartcard is highlighted as infrastructure that has an excellent security for executing functions such as user authentication, access control, information storage and control, and its market is expanding rapidly. But possibilities of forgery and alteration by hacking are increasing as well. This paper makes cut off of Smartcard forgery and alteration that use angular multiplexing and private key multiplexing hologram on holographic security Encryption, and proposes system capable verfication of forgery and alteration impossible on existing smartcard by adopting smartcard chip and holographic memory chip.

키워드 : 스마트카드(Smartcard), 홀로그램(hologram), 위조(Forgery), 변조(Alteration), PKI, 광영상 암호화(optical encryption)

1. 서 론

지식 정보화 환경에서의 업무처리는 종이문서위주, 대면 위주의 사무처리방식에서 온라인 전자문서 기반으로 전환되어 표준화된 정보기술기반 위에서 각종 정보와 서비스를 신속하게 제공하게 될 것이다.

그러나 네트워을 통한 주요 자료 및 개인정보의 유통이 급격하게 증가될수록 온라인 상에서 유통되는 정보들에 대한 불법적인 도청, 위·변조 및 신분위장 등 각종 역기능에 의한 침해를 고려해야만 한다.

이에 유통정보에 대한 안정성 및 신뢰성을 확보하기 위해서 공개키 암호 기술을 적용하여 본인인증, 정보보호, 무결성 보장 및 부인봉쇄 등을 하고 있다. 이와 같은 기반구조를 가장 유용하게 운영할 수 있는 기반은 스마트카드 시스템이라고 할 수 있다.

스마트카드는 정보통신기반이 발전되면서 그 활용 분야가 전자화폐, ID카드, 전화, 로열티카드, 교통, 의료 등에 이르기까지 다양한 분야에 사용되고 있다. 또한 스마트카드는 사용자 인증, 접근제어, 정보의 저장·관리 기능 등을 수행하기에 필요한 안전성과 신뢰성 및 보안성을 확보할 수 있는 기반으로 인정되고 있다.

시장조사 전문 기관인 데이터퀘스트사에 따르면,

〈표 1〉 스마트 카드 사용 이점

1. 보 안 성	: 사용자 인증, 접근제어를 통한 보안성 강화
2. 편 리 성	: 전자상거래, 화폐거래 감축, 다양한 서비스 제공을 통한 편리성 증진
3. 다 기 능 성	: ID 카드, 전자화폐 등과 같은 다양한 용도를 하나의 카드로 수행
4. 비용효과성	: 일정 수준의 보안성을 제공하는 비용 및 유지·관리에 드는 비용 효과성 증대

스마트카드의 전체 시장 규모가 1998년에는 8억 9,700만

† 정 회 원 : 행정자치부 전문위원, 성결대학교 겸임교수
†† 정 회 원 : 행정자치부
††† 종신회원 : 인하대학교 컴퓨터공학부 교수
논문접수 : 2001년 11월 17일, 심사완료 : 2002년 1월 7일

달러이던 것이 연 평균 31.8% 성장하여, 2003년에는 그 네 배에 달하는 35억 6,100만 달러 규모에 이를 전망이다[1].

이와 같이 스마트카드가 급성장하고 있는 것은 사용자와 공급자 모두에게 <표 1>과 같은 운영상의 이점이 있기 때문이다. 그러나 스마트카드가 현재 기술수준으로 구현할 수 있는 보안성이 가장 뛰어난 것으로는 인정은 되고 있으나 해킹될 경우 카드에 저장된 개인신용정보나 전자서명 생성키까지도 추출이 가능해 IC칩 기반의 본인인증서, 전자화폐 등에 대한 위·변조는 물론 개인정보의 악용까지도 초래할 수 있다. 이러한 해킹 기술은 이미 미국의 암호기술 전문업체인 크립토리서치사가 DPA (Differential Power Analysis)라는 해킹기술을 보유하고 있는 것으로 밝혀졌다[2]. 따라서 스마트카드 해킹에 의한 위·변조를 차단하고 위·변조 유무를 검증할 수 있는 기반이 요구되고 있다.

본 논문에서는 스마트카드의 위·변조를 차단하고 검증하기 위한 방법으로 영상 암호화기반의 각 다중화 및 암호키 다중화 기법을 이용하여 스마트카드 위·변조 방지 및 검증 시스템을 제안한다.

2. 주요 기반기술

2.1 비밀키 암호화

암호화 방식에는 크게 공개키 암호화 방식과 비밀키 암호화 방식 두 가지로 나눌 수 있다. 공개키 암호화 방식은 공개키를 이용해서 데이터를 암호화하고 비밀키를 이용해서 복호화 시킨다.(비대칭키 방식) 이 방식은 키 분배 문제는 쉽지 해결 될 수 있지만 처리 속도가 느린 단점이 있다. 또한 비밀키 암호화 방식은 암호화와 복호화 시 동일한 키를 사용하며(대칭키 방식), 공개키 암호화 방식에 비해 처리 속도가 빠른 장점이 있다.

〈표 2〉 원타임 패스워드 생성방법

1. 동기화된 시간을 유지하여 Time-Stamp사용
2. 양쪽의 임의의 패스워드 리스트 내의 위치를 동기화
3. Sequence generator의 상태를 동기화하여 임시적인 sequence number사용
4. Challenge-Response Schemes이용

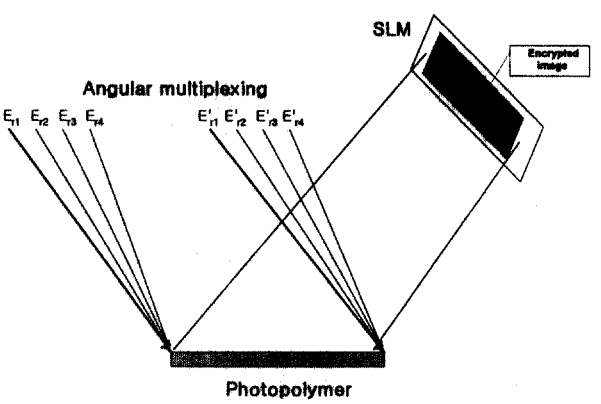
본 논문에서는 비밀키 암호화 방식을 사용하며 여러 가지 비밀키 암호화 방식 중 Differential Crypto Analysis에서 매우 안전한 것으로 알려져 있고 알고리즘 구조가 Block Cipher알고리즘이며, 소프트웨어나 하드웨어 구현에 있어서도 모두 용이한 IDEA 비밀키 암호화 방식[3]으로 제안한다.

이를 소프트웨어로 구현하면 프로세싱 속도가 DES와 거의 비슷한 강점을 가지고 있다. 비밀키의 길이도 IDEA가 DES 에 비해 두 배나 길어 매우 안전하다. 연산 반복수행 역시 DES가 16번 반복 수행하는 것에 비해 IDEA는 그에 반밖에(8번) 수행하지 않으므로 이에 따른 처리 속도도 매우 빨라진다. 스마트카드에 기록된 정보는 해킹 될 가능성을 가지고 있고, 해킹 된 정보는 불법적으로 위·변조가 가능하므로 스마트카드의 위·변조 유무를 검증할 수 있는 방법이 요구된다. 이에 본 논문에서는 RFC1938[4]에 기술된 Challenge Response Schemes 원타임패스워드를 암호화키로 이용하여 이를 광폴리머에 저장함으로써 스마트카드 위·변조 유무 검증이 가능하도록 하였다.

이러한 원타임패스워드 시스템을 구현하기 위한 방법으로는 <표 2>와 같다

2.2 영상 암호화 및 복호화 기법

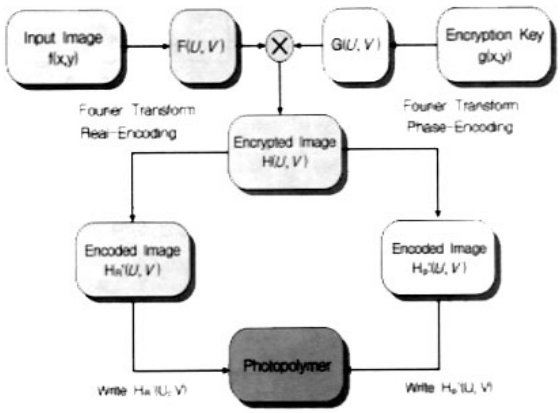
근래에는 보다 발전된 형태로 신용카드와 여권 등에 홀로그램을 널리 이용하고 있으나 이것은 사람의 눈에 의해 검색되는 것으로 이론적으로는 복제될 수 없지만 실제의 경우 홀로그램 패턴이 광세기 패턴으로 CCD(Charge Coupled Device)와 같은 기존의 광검출기로 쉽게 검출되어 새로운 홀로그램의 합성과 복제가 가능하게 된다. 따라서, 어떠한 경우에도 ID카드 위조나 복조를 근본적으로 차단할 수 있는 새로운 접근 방법에 대한 많은 연구가 이루어지고 있으며, 최근에는 CCD와 같은 기존의 광세기 검출기로는 볼 수도, 복제될 수 없는 복소함수 형태의 랜덤 위상 패턴을 사용하는 새로운 광학적 보안 기법이 제시되고 있다. 이러한 영상 암호화 방법으로는 Refregier[5]와 Javidi[6] 등에 의해 연구된 위상정보를 이용한 암호화 방법과 편광 특성을 이용한 암호화 방법으로 나눌 수 있다. 본 논문에서는 Refregier 시스템의 단점인 암호화된 영상이 복소수 값을 갖는 문제를 해결한 JTC(Joint Transform Correlator)[7]를 이용하여 영상을 암호화하고 암호화된 임의의 영상을 각다중화 방법에 의해 하나의 광폴리머에 여러 방향으로 기록을 한다. 만약 기록된 정보를 복사하더라도 광폴리머에 기록된 정보의 복호화 과정에서 기록된 위치마다 암호화 영



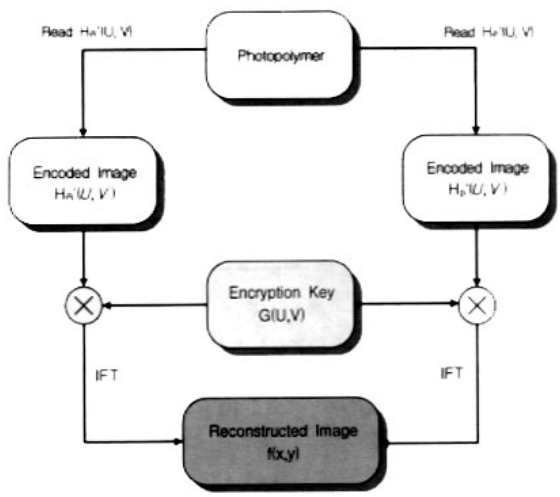
(그림 1) 광폴리머를 이용한 암호화 영상의 기록

상의 복원여부를 검출하여야 하고 기록된 부분 중에서 하나라도 복원되지 않는다면 이는 위조된 것으로 간주하기 때문에 사실상 위·변조가 불가능하도록 하였다.

본 논문에서는 (그림 1)과 같은 각다중화 방법을 이용, 영상 암호화시 암호화키도 다중화하는 기법을 제안한다. 각 다중화 방법에 의해 (그림 2)와 같이 암호화된 영상을 다중화된 각각의 암호키로 (그림 3)과 같이 복원, 검출함으로써 한 단계 높은 보안성 및 신뢰성을 보장하였다.



(그림 2) 암호화 과정



(그림 3) 암호화 영상의 복호화 과정

2.3 PKI 인증기반

공개키 암호기술은 보안이 필요한 응용 분야에 널리 사용된다[8].

이 기반 기술에서는 비밀키와 공개키를 이용한다. 비밀키는 그 소유자만이 알고 있고 공개키는 공개된다. 공개키를 공개하는 문제는 매우 단순한 것 같지만 공개키를 공개하는 데에 사용되는 메커니즘(공개키디렉토리, 게시판 등)이 자체적으로 안전하지 않아 누구든 쉽게 접근하여 정보 변경이 가능하므로 공개키의 위·변조 문제를 야기 시킨다.

A가 B에게 문서를 비밀리 보내고자 하는 경우 A는 B의 공개키로 그 문서를 암호화할 것이다. 그런데 제 3자인 C가 공개키 디렉토리에 접근하여 B의 공개키를 자신의 공개키로 바꾸어 버리고 전송되는 암호문을 중간에 가로채 버린다면 B가 아닌 C가 그 문서를 읽게 될 것이다. 이렇게 공개된 공개키는 위·변조 될 수 있으므로 이를 방지하기 위한 것이 필요하며, 이를 위해 현재 PKI 기반의 인증서를 이용하고 있다. 인증서는 신뢰할 수 있는 제3자 (인증기관)의 서명문이므로 신뢰의 객체가 아닌 사람은 그 문서의 내용을 변경할 수 없도록 하고 있다.

PKI는 <표 3>과 같은 5가지 기본 보안 서비스를 제공한다.

〈표 3〉 PKI 보안 기본 서비스

1. 위조불가(Unforgeable) : 합법적인 서명자만이 전자서명을 생성할 수 있음.
2. 서명자 인증 (User Authentication) : 전자서명의 서명자를 불특정 다수가 검증 할 수 있어야 함.
3. 부인방지 (Non-Repudiation) : 서명자는 서명행위 이후에 서명한 사실에 대해 부인할 수 없음.
4. 변경불가 (Unalterable) : 서명한 문서의 내용을 변경 할 수 없음
5. 재사용불가 (Not Reusable) : 전자문서의 서명을 다른 전자문서의 서명으로 사용할 수 없음.

2.4 Hash 알고리즘

해쉬알고리즘은 임의의 길이의 비트 열을 고정된 길이의 출력값인 해쉬코드로 압축시키는 알고리즘으로써 <표 4>와 같은 성질을 만족한다. <표 4>의 2에서 암호학적 응용에 사용되는 대부분의 해쉬알고리즘은 위의 두 성질뿐만 아니라 이보다 강한 충돌 저항성을 지닐 것이 요구된다. 즉, 같은 출력을 내는 임의의 서로 다른 두 입력 메시지를 찾는 것이 계산상 불가능하다(collision-resistance).

암호학적 해쉬알고리즘의 충돌 저항성은 전자서명 에서 송신자외의 제 3자에 의한 문서위조를 방지하는 부인봉쇄 서비스를 제공하기 위한 필수적인 요구조건이 된다.

해쉬알고리즘은 크게 DES와 같은 블록 암호알고리즘에 기초한 해쉬알고리즘과 전용 해쉬알고리즘으로 나눌 수 있다. 블록암호를 이용한 해쉬알고리즘은 이미 구현되어 사용되고 있는 블록암호를 사용할 수 있다는 이점이 있으나, 대부분의 블록 암호알고리즘의 속도가 그리 빠르지 않을뿐더러 이를 기본함수로 이용한 해쉬알고리즘의 경우 블록암호보다도 훨씬 더 속도가 떨어지므로 현재는 대부분의 응용에서 전용 해쉬알고리즘이 주로 이용된다.

대부분의 전용 해쉬알고리즘은 덧붙이기, 분할, 반복연산의 과정을 거쳐 계산된다. 임의의 길이의 메시지 X를 입력단위의 배수가 되도록 덧붙이기 하여 t개의 입력 블록 $(X_1, \cdots, X_t)$으로 분할한다. 해쉬코드는 각 블록 X_i 에 대

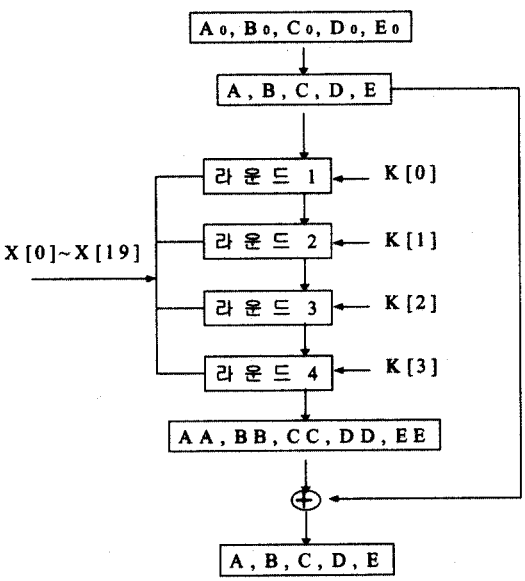
해 연쇄변수를 주어진 초기값(IV)으로 초기화한 후 압축함수를 반복적으로 적용하여 계산되며, 그 처리과정은 다음과 같이 기술할 수 있다.

$$H_0 = IV,$$
$$H_i = f(H_{i-1}, X_i),\ 1 \le i \le t,$$
$$h(X) = H_t$$

〈표 4〉 Hash 알고리즘의 기본 성질

1. 주어진 출력에 대하여 입력값을 구하는 것이 계산상 불가능.
2. 주어진 입력에 대하여 같은 출력을 내는 또다른 입력을 찾아내는 것이 계산상 불가능.
3. 같은 출력을 내는 임의의 서로 다른 두 입력 메시지를 찾는 것이 계산상 불가능.(collision - resistance).

여기서 f는 h의 압축함수이며, H_i는 단계 $i-1$과 단계 i의 중간계산 값이다. 본 논문에서는 (그림 4)와 같은 구조의 HAS-160[9]을 사용하였다.

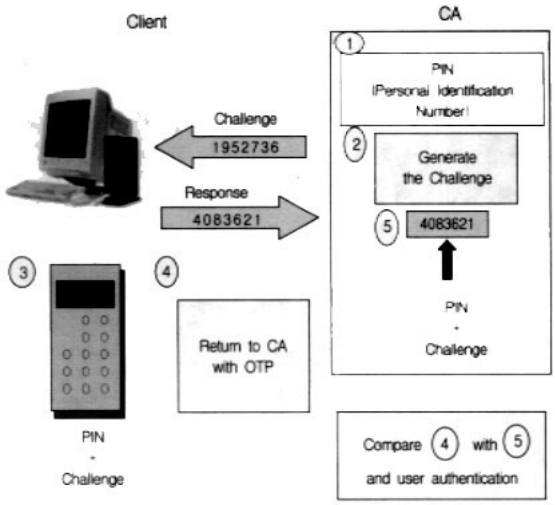


(그림 4) HAS-160 구조도

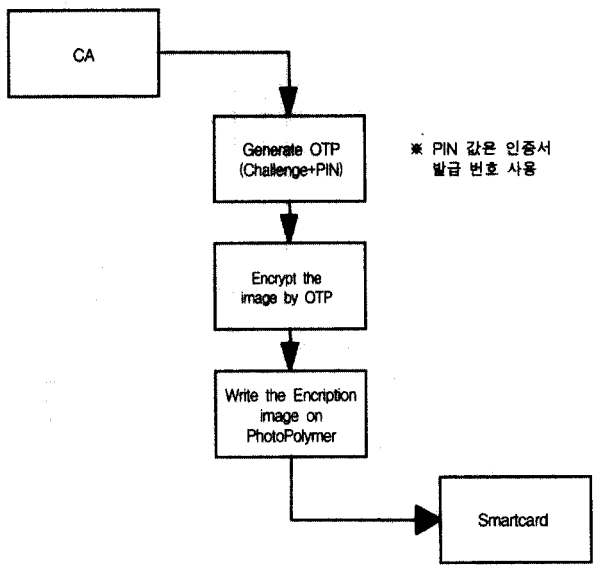
3. 제안 시스템

3.1 영상 암호화

영상 암호화를 위해서 FIPS 186[10]생성기를 이용하여 몇 개의 랜덤한 Angle값과 Challenge를 CA(Certification Authority)에서 생성한다. 이렇게 생성된 Challenge값과 PIN (Personal Identification Number)을 이용하여 원타임패스워드를 만든다. 일반적인 Challenge 운영 방식은 (그림 5)와 같으나 본 제안에서는 PIN을 PKI기반의 인증서 발급번호로 사용하였다.



(그림 5) 일반적인 Challenge 운영 방식



(그림 6) 영상 암호화

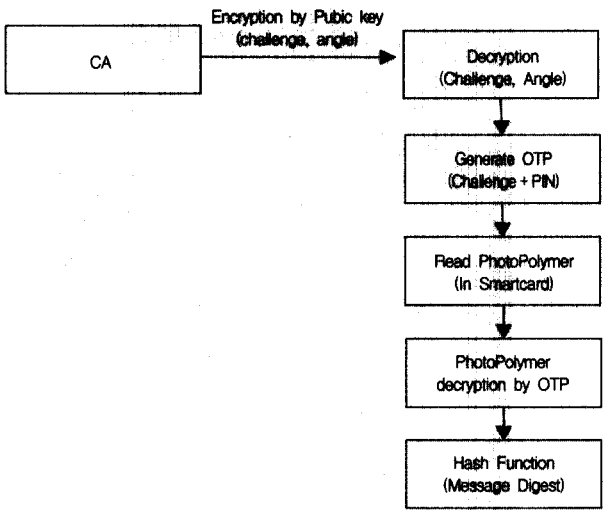
생성된 랜덤값(Angle)과 챌린지값(Challenge)은 영상 복호화를 위해 CA에 보관된다. 생성된 원타임패스워드를 암호키로 사용하여 (그림 2)와 같이 암호화를 한 후, 광폴리머에 암호화된 영상을 랜덤값에 따라 각다중화 방법으로 (그림 6)과 같이 기록한다.

3.2 영상 복호화

스마트카드 인증 및 위·변조 유무의 검증을 위해 인증서버로부터 홀로그램을 읽기 위한 저장된 Angle 값과 원타임패스워드를 생성하기 위한 Challenge값을 인증서의 공개키로 암호화하여 가져온다. 복호화를 위한 원타임패스워드의 생성은 Challenge값과 PIN(인증서 발급번호)을 이용하여 생성한다.

〈표 5〉 FIPS 186을 이용한 난수 생성 방법

○ FIPS 186 생성기는 FIPS에서 승인 받은 의사 난수 발생기임.
1. 입력 : 정수 m과 비트 소수 q를 입력한다.
2. 생성과정
(1) 필요에 따라 적당한 b를 고르고 b비트의 씨앗값 s를 생성한다. t는 FIPS에서 주어진 160비트 스트링이다.
(2) m개의 b스트링 yi를 입력하거나 0으로 놓는다.
(3) I는 1부터 m까지 zi ← (s+ yi) mod 2b , ai ← G(t, zi) , s← (1+s+ai) mod 2b을 수행한다. G는 SHA-1이나 DES와 같은 일방향 함수를 사용한다.
3. 출력 : m개의 64비트 의사난수 (x1, x2, … , xm)을 출력한다.



(그림 7) 영상 복호화

CA로부터 전달받은 Angle값과 생성된 원타임패스워드를 이용 영상을 읽은 후 (그림 7)과 같이 복호화 한다.

결론적으로 본 논문에서는 각다중화 시 랜덤값을 사용하여 각을 정하고 그에 따른 암호키를 원타임패스워드로 다중화함으로써 위·변조에 대한 가능성을 완전히 차단할 수 있도록 하였다.

3.3 본인확인 및 위·변조 유무 검증

1차적인 본인확인은 스마트카드에 보관된 인증서를 통한 PKI기반으로 본인확인이 가능하도록 하였다. 그러나 1차 본인확인만으로는 스마트카드 해킹에 의한 위·변조 유무를 검증할 수 없다. 이에 본 논문에서는 위·변조가 불가능한 포토폴리머에 기록된 정보와 스마트카드 메모리의 정보를 비교하여 위·변조 유무를 판별 검증 할 수 있도록 하였다. 또한 검증을 위해 인증서버로부터 Angle값과 Challenge값을 인증서내의 공개키로 암호화하여 가져온 후 그 값으로 전자서명키를 복호화 하였고 Challenge 값과 PIN을 이용, 원타임패스워드를 생성한다. 광폴리머에 저장된 영상(정보)을 이 Angle값과 원타임패스워드로 복호화 시키고 이렇게 복호화된 영상(정보)을 해쉬함수로 처리한다[11].

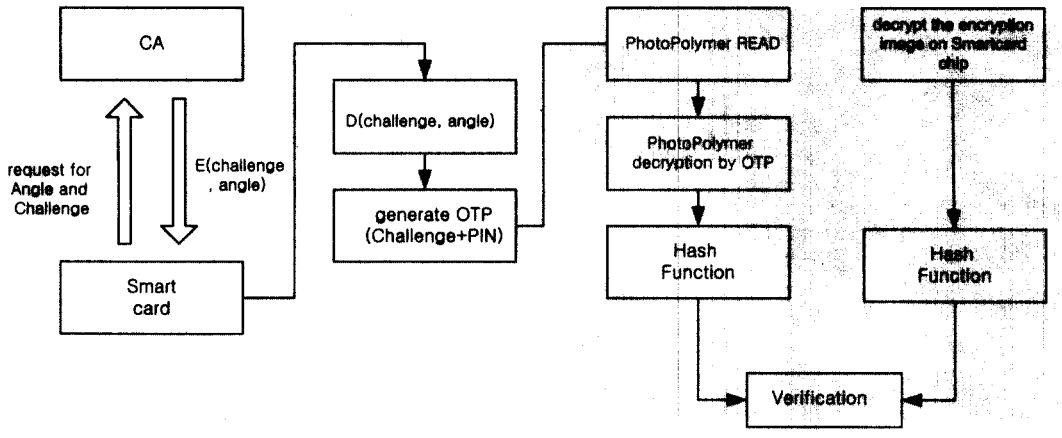
또한, 스마트카드 메모리내에 저장된 비교 검증할 정보를 암호생성키로 복호화 시킨 후 해쉬함수 처리를 한다. 각기 해쉬함수로 처리된 정보들을 서로 비교하여 (그림 8)과 같이 위·변조를 판단하고 PKI인증서 기반을 이용하여 본인확인을 한다.

3.4 실험 및 결과

본 논문에서 제안한 홀로그래픽 암호화 기법을 적용한 스마트카드 위·변조 차단에 관한 실험은 (그림 9), (그림 10)과 같은 방식으로 데몬스트레이터를 (그림 11), (그림 12)와 같이 구축하였다.

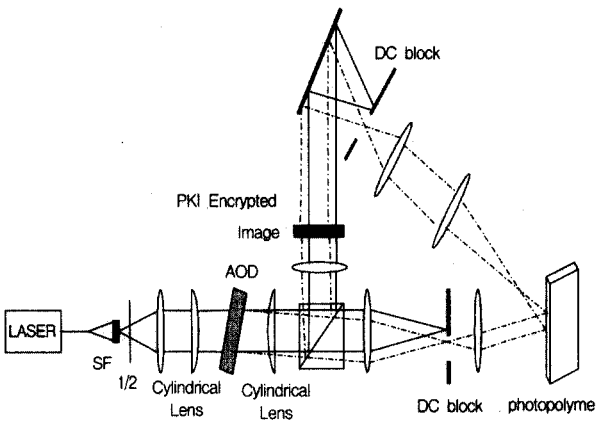
구축된 데몬스트레이터는 에러율(Error rate)이 CD나 DVD와 같이 10^{-10}~10^{-12}이고 사용자 데이터 밀도는 5MB/cm^2이며 총 용량은 5MB, 쓰기 속도는 1Kb/s, 읽기 속도는 2Kb/s이다.

홀로그램 기록 매질은 아조벤젠 폴리에스터(Azobenzene polyester)를 사용하였으며 이 매질의 특성은 유용한 파장 범위가 400~550nm 이고 쓰고 지우는 것이 가능하며 감도는 대략 1 J/Cm^2, 열의 안전성은 150도 이하이다.



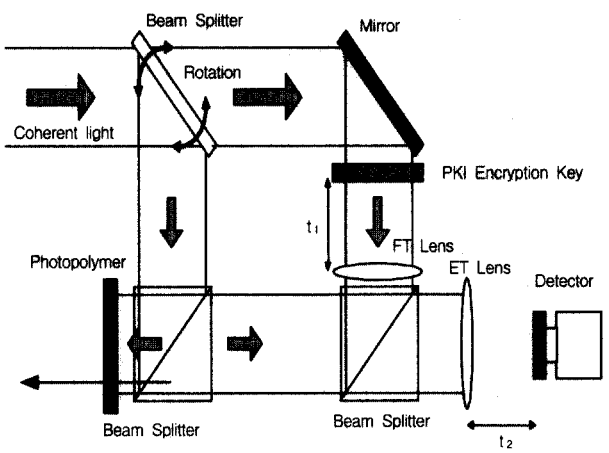
(그림 8) 제안시스템의 처리절차

이와 같은 데몬스트레이터와 매질을 사용, (그림 13)과 같이 인코딩하여 (그림 14)와 같이 디코딩 및 검증 실험을 실시하였다. 이 실험에서 (그림 15)와 같은 SLM의 그림이 (그림 16)과 같이 재생되었다.

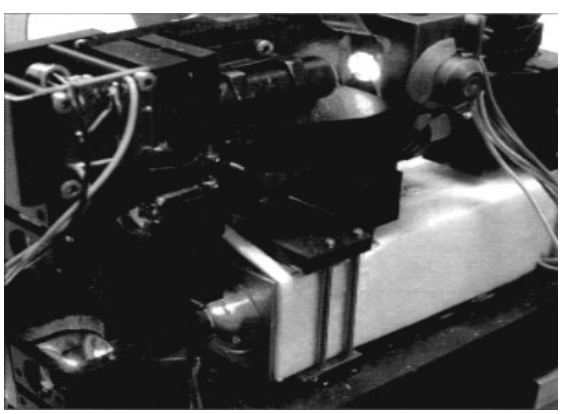


(그림 9) 영상 인코더

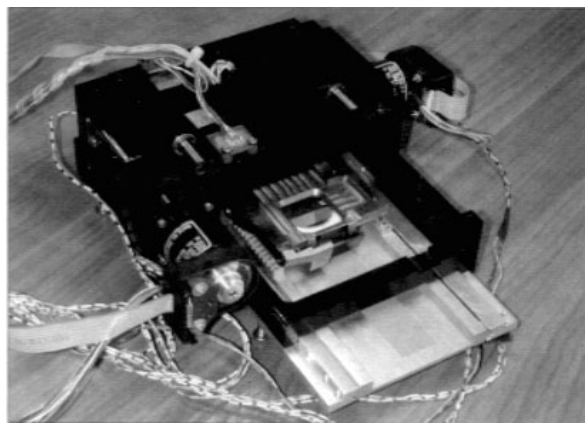
결론적으로 본 논문에서 제안된 시스템의 위·변조 차단에 대한 타당성이 검증되었다.



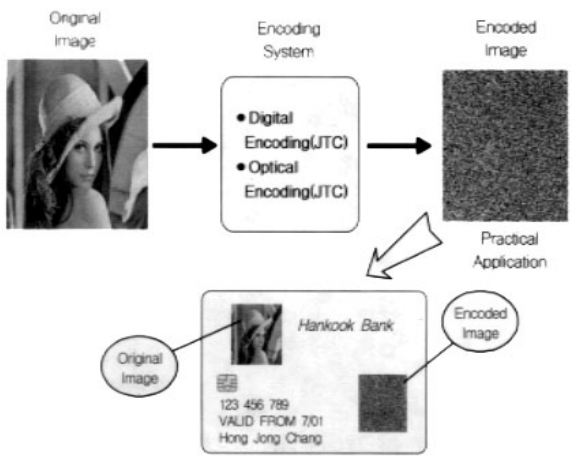
(그림 10) 영상 디코더



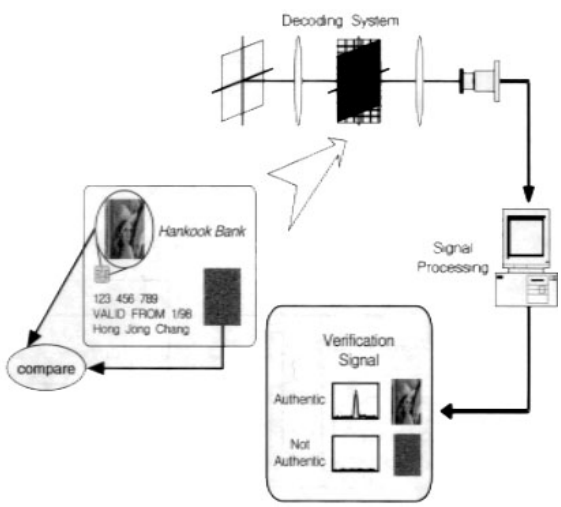
(그림 11) 영상 시스템 데몬스트레이터



(그림 12) 스마트 카드 칩의 홀로그래픽 보안카드 로딩 장치



(그림 13) 영상 인코딩 실험

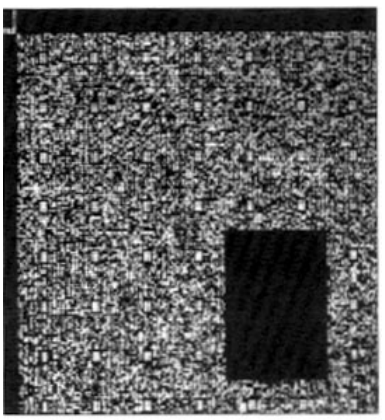


(그림 14) 영상 디코딩 및 검증 실험

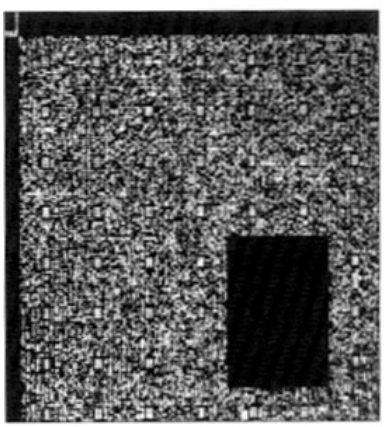
4. 결 론

지식 정보화 사회에서는 표준화된 정보기술기반 위에서

각종 정보 서비스를 신속하게 제공하게 될 것이다. 가상환경에서의 주요 자료 및 개인정보의 유통이 급격하게 증가됨에 따라 유통 정보들에 대한 불법적인 도청, 위·변조 및 신분위장 등 각종 역기능에 의한 위협의 노출은 점점 더 커지고 있다.



(그림 15) Direct SLM picture



(그림 16) Recovered hologram

이를 방지하기 위해서는 대면 수준의 본인확인 등 신뢰성 기반 확보가 가장 중요하다고 할 수 있겠다. 스마트카드에 대한 다양한 해킹기법이 실제로 존재하고 있어 본 논문에서는 각 다중화와 암호키 다중화 기법을 사용하여 홀로그래픽 암호화 기반에서 위·변조를 차단하였고 스마트카드칩을 위·변조하더라도 이를 검증할 수 있도록 하였다. 제안된 스마트카드 위·변조 방지시스템은 각다중화 및 암호키다중화를 이용한 영상 암호화기반구조로 구성하였다. 또한 PC의 하드디스크나 플로피디스켓에 보관된 인증서는 이동이 제한적이었으나 스마트카드를 사용함으로써 이동성을 보장하였다.

결론적으로 본 논문에서는 PKI기반의 인증과 영상 암호화 기반에서의 위·변조 차단 및 스마트카드와의 비교 검증을 통해 교차 인증할 수 있게 함으로써 인증에 대한 신뢰성을 확보하였다.

참 고 문 헌

[1] Dataquest, July, 1999.

[2] Poul Kocher, Joshur Jaffe and Benjamin Jun, "Differential Power Analysis," Cryptography Reacrch, Inc.

[3] X. Lai and J. L. Massey, Markov ciphers and differential cryptanalysis. In D. W Davies, editor, Proc. EUROCRYPT 91, Lecture Notes in Computer Science No.547, Springer, 1991.

[4] Haller, N., "A One-Time Password System," RFC 1938, Bellcore, May, 1996.

[5] P. Refregier and Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., Vol.20, pp.767-769, 1995.

[6] B. Javidi and J. L. Honer, "Optical Pattern recognition for validation and security verification," Opt. Eng., Vol.33, pp. 1752-1756, 1994.

[7] B. Javidi, "Nonlinear joint power spectrum based optical correlation," Appl. Opt., Vol.28, pp.2358-2367, 1989.

[8] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, IT-22. (6) : 644-654, November, 1976.

[9] HAS-160 : 해쉬 알고리즘 표준 (TTA.IS-10118)-Hash Algorithm Standard (HAS-160), 한국정보통신기술협회, 1998.

[10] NIST, FIPS PUB 186, U.S Department of Commerce, 1994.

[11] Rivest, R., "The MD5 Message-Digest Algorithm," Internet report, RFC 1321, Apr. 1992.

장 홍 종

e-mail : realking@gcc.go.kr

1992년 한양대학교 전자계산공학과 (공학석사)

2000년 인하대학교 전자계산공학과 (박사 수료)

1983년~1998년 (재)건설기술교육원 전산실장

1993년~2000년 인천전문대학교 강사

1995년~1998년 수원과학대학 겸임교수

1998년~1999년 썬버드 전산부장

1999년~2000년 인하대학교 강사

1999년~2000년 경인여자대학 겸임교수

2000년~현재 성결대학교 겸임교수

2000년~현재 행정자치부 전문위원

관심분야 : 정보보안, 정보보호시스템 평가, 음성인식, 암호학, 스마트카드, HCI

이 성 은

e-mail : pinetree@gcc.go.kr

1987년 한양대학교 졸업(공학사)

1992년 한양대학교 산업대학원 전자계산학 (공학석사)

2001년 건국대학교 대학원 컴퓨터정보통신공학과(박사과정)

1990년~1996년 (주)대상, 아주대학교의료원, 중앙일보

1996년~현재 행정자치부

관심분야 : 정보보안, 암호학, 스마트카드, 지불시스템, 뉴럴네트웍

이 정 현

e-mail : jhlee@inha.ac.kr

1977년 인하대학교 전자공학과 졸업

1980년 인하대학교 대학원 전자공학과 (공학석사)

1988년 인하대학교 대학원 전자공학과 (공학박사)

1979년~1981년 한국전자기술연구소 시스템 연구원

1984년~1989년 경기대학교 전자계산학과 교수

1989년~현재 인하대학교 컴퓨터공학부 교수

관심분야 : 자연어처리, HCI, 정보검색, 음성인식, 음성합성, 컴퓨터구조, 정보보안