情報保護學會論文誌
第13券 第2號, 2003. 4

다중 암호화 기법을 활용한 하이브리드 스마트카드 구현

이 성 은*, 장 홍 종**, 박 인 재***, 한 선 영****

Implementation of Hybrid Smartcard Using Multi Encryption Method

Seong-eun Lee*, Hong-jong Chang**, In-jae Park***, Sun-young Han****

요 약

정보통신의 급속한 발전으로 정보의 온라인 유통이 급증하고 있으며 이에 따른 유통 정보에 대한 보호가 중요해지고 있다. 현재 공개키 기반구조(Public Key Infrastructure, PKI)는 전자상거래를 위한 정보보호 기반구조로써 많이 활용되고 있으며 스마트카드는 공개키 기반구조를 가장 잘 적용할 수 있다. 그러나 공개키 기반의 인증서는 사용자의 인증 정보만을 제공하기 때문에 사용자의 본인확인 및 권한 정보가 필요한 응용에서는 그 사용이 제한적일 수밖에 없으며 스마트카드의 위·변조 가능성 또한 존재하고 있다.

이의 해결을 위해 본 논문에서는 인증서 유효성 검증만으로 해결할 수 없는 스마트카드의 위·변조에 대한 가능성을 광영상 암호화 기법인 각 다중화와 암호키다중화를 사용하여 위·변조를 방지하였고, 위·변조 시 이를 검증할 수 있도록 하였다. 또한, 보안성과 이동성이 뛰어난 스마트카드와 결합한 공개키 인증기반의 본인확인 기법을 제안하여 다중 인증 체계의 새로운 보안 인증시스템을 제안하였다.

ABSTRACT

With the rapid development of information and communication technology, online dissemination increases rapidly. So, It becomes more important to protect information. Recently the authentication system using public key infrastructure (PKI) is being utilized as an information protection infrastructure for electronic business transactions. And the smartcard system makes the most use of such an infrastructure. But because the certification based on the current PKI provides only basic user certification information, the use has to be limited in various application services that need the identification and authorization information as well as face-to-face information of the user.

In order to protect a system from various kinds hackings and related treats, we have proposed angular and private key multiplexing for prevention of smartcard forgery and alterlation based on a photopolymer cryptosystem. When smartcard becomes prone to forgery and alteration, we should be able to verify it. Also, our paper proposes a new authentication system using multi authentication based on PKI. The smartcard has an excellent advantage in security and moving.

Keyword : *Smartcard, hologram, optical encryption, PKI*

* 행정자치부
** 명지대학교 객원조교수
*** 숭실대학교 정보통신전자공학부 겸임교수
**** 건국대학교 정보통신원 원장

Ⅰ. 서 론

정보화 환경에서의 업무처리 방식은 종이문서위주, 대면위주의 처리방식에서 온라인 전자문서 기반으로 전환되어 표준화된 정보기술기반 위에서 각종 정보와 서비스를 신속하게 제공하고 있다.

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

네트워크를 통해 유통되는 정보에 대한 안정성 및 신뢰성을 확보하기 위해서 공개키 암호 기반을 적용하여 본인인증, 정보보호, 무결성 보장 및 부인봉쇄 등을 하고 있다. 공개키 암호 기반을 가장 유용하게 적용할 수 있는 기반은 스마트카드라고 할 수 있다.

스마트카드는 정보통신기반이 발전하면서 그 활용 분야가 전자화폐, 아이디카드, 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, 스마트카드의 전체 시장 규모가 1998년에는 8억 9,700만 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 보안성, 편리성, 다기능성, 비용효과성과 같은 사용 이점이 있기 때문이다. 그러나 스마트카드가 현재 기술수준으로 구현할 수 있는 보안성이 뛰어난 것으로는 인정되고 있으나 해킹될 경우 카드에 저장된 개인 정보와 비밀키까지도 추출이 가능해 IC칩에 저장된 정보 등에 대한 위·변조는 물론 개인정보의 악용까지도 초래할 수 있다. 이러한 스마트카드 해킹 기법은 암호기술 전문 업체인 크립토리서치사가 DPA(Differential Power Analysis)라는 해킹기술을 보유하고 있다[2,3]. 따라서 현재의 암호체계는 한가지의 암호 기술에 전적으로 의존하기보다는 생체 암호기술 등과 결합된 다중 암호기술을 도입하고 있으며, 이를 도입하여 상호 인증함으로서 위·변조의 위험을 줄이고 궁극적으로는 위·변조를 방지하고 위·변조 유무를 검증할 수 있는 시스템을 구현하는 것을 목표로 하고 있다.

Ⅱ. 주요 기반기술

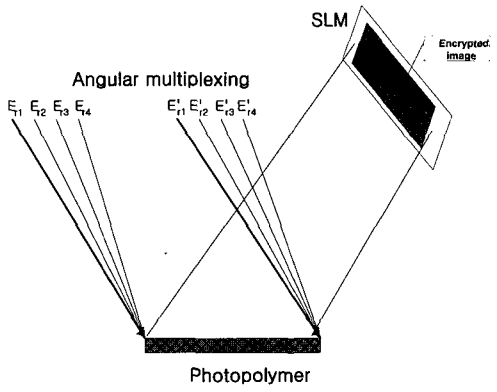
2.1 영상 암·복호화 기법

근래에는 보다 발전된 형태로 신용카드와 여권 등에 홀로그램을 널리 이용되고 있으나 이것은 사람의 눈에 의해 검색되는 것으로 이론적으로는 복제될 수 없지만 실제의 경우 홀로그램 패턴이 광세기 패턴으로 CCD(Charge Coupled Device)와 같은 광검출기로 쉽게 검출되어 새로운 홀로그램의 합성과 복제가 가능하게 된다. 따라서, 어떠한 경우에도 ID카드 위조나 복조를 근본적으로 차단할 수 있는 새로운 접방법에 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[4]와 Javidi[5] 등에 의해 연구된 위상정보를 이용한 암호화 방법, 편광 특성을 이용한 암호화 방법으로 나눌 수 있다. 본 논문에서는 Refregier 시스템의 단점인 암호화된 영상이 복소수 값을 갖는 문제를 해결한 JTC(Joint Transform Correlator)[6]를 이용하여 영상을 암호화하고 암호화된 임의의 영상을 각 다중화 방법에 의해 하나의 광 폴리머에 여러 방향으로 기록을 한다. 이는 만약 기록된 정보를 복사하더라도 광 폴리머에 기록된 정보의 복호화 과정에서 기록된 위치마다 암호화 영상의 복원여부를 검출하여야 하고 기록된 부분 중에서 하나라도 복원되지 않는다면 이는 위조된 것으로 간주하기 때문에 사실상 위·변조가 불가능하다.

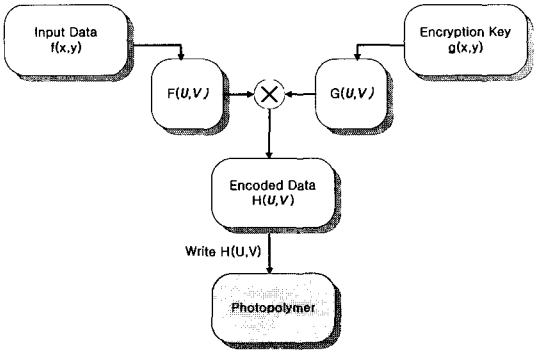
본 논문에서는 [그림 1]과 같은 각 다중화 방법을 이용, 영상 암호화 시 암호화키도 다중화하는 기법을 제안한다. 각 다중화 방법에 의해 [그림 2]와 같이 암호화된 영상을 다중화된 각각의 암호키로 [그림 3]과 같이 복원, 검출함으로써 한 단계 높은 보안성 및 신뢰성을 보장하였다.

2.2 공개키 인증기반

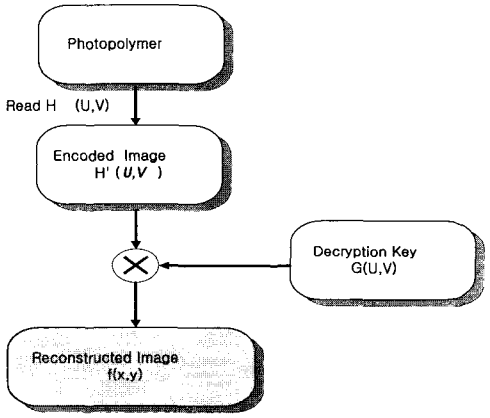
공개키 암호기술은 보안이 필요한 응용 분야에 널리 사용된다[7,8,9]. 이 기반 기술에서는 비밀키와 공개키를 이용한다. 비밀키는 그 소유자만이 알고 있고 공개키는 공개된다. 또한, 공개키 암호 기술은 위조



〔그림 1〕 광폴리머를 이용한 암호화 영상의 기록



〔그림 2〕 암호화 과정



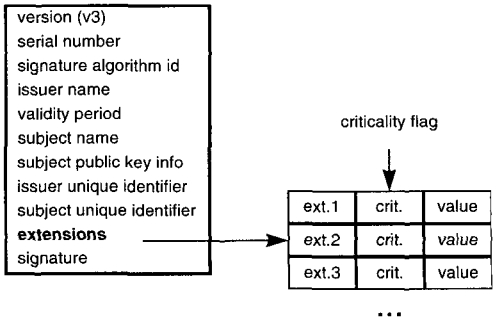
〔그림 3〕 복호화 과정

불가(Unforgeable),서명자인증(User Authentication), 부인방지(Non-Repudiation), 변경불가(Unalterable), 재사용불가 (Not Reusable)와 같은 5가지 기본 보안 서비스를 제공한다. 공개키를 공개하는 문제는 매우 단순한 것 같지만 공개키를 공개하는 데에 사용되는 메커니즘(공개키 디렉토리, 게시판 등)이 자체적으로 안전하지 않아 누구든 쉽게 접근하여 정보 변경이 가능하므로 공개키의 위·변조 문제를 야기시킨다.

예를 들어, A가 B에게 문서를 비밀리에 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 A가 문서를 보내려고 했던 B가 아닌 C가 그 문서를 읽게 될 것이다. 인증서는 신뢰할 수 있는 제3자의 서명문이므로 신뢰의 객체가 아닌 사람은 그 문서의 내용을 변경할 수 없도록 하고 있다. 이렇게 제3자인 인증기관을 통해 공개된 공개키가 위·변조되지 않았음을 보장한다.

2.3 인증서 구조

인증서의 일반적인 구조는 [그림 4]와 같다. 인증서가 가지고 있는 정보 중개인에 관한 정보는 이름(subject name)뿐이다. 따라서 인증서만 가지고는 서비스를 신청하는 사람이 본인인지를 확인할 수 있는 방법은 없다. 이는 단지 서비스를 신청하는 신청인이 사용한 인증서의 유효성밖에 알 수가 없다. 따라서 이름이 같을 경우 인증서의 유효성만 검증한다면 본인확인이 필요한 중요 정보라도 얼마든지 서비스를 받을 수 있다. 예로써 정부기관에 민원신청을 할 때 본인확인이 필요한 민원을 서비스하기 위해서는 신청자가 서비스를 받을 본인이라는 것을 반드시 확인해야 한다. 그러나 이름만 가지고 본인확인을 하는 경우에 동명이인인 경우에는 동일인으로 처리된다. 따라서 편리성을 위하여 제공되는 온라인 민원 서비스 등이 사회적, 경제적 혼란을 야기 시킬 수 있다.



〔그림 4〕 X.509 V3 인증서 구조

Ⅲ. 제안 시스템

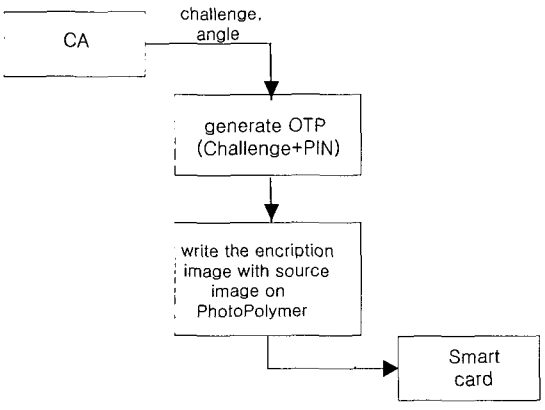
3.1 광 영상 암·복호화

영상 암호화를 위해서 FIPS 186[10] 난수 생성기를 이용하여 몇 개의 임의의 각도값과 챌린지값을 인증서버(CA : Certification Authority)에서 생성한다. 이렇게 생성된 챌린지 값과 핀(PIN : Personal Identification Number)값으로 IDEA알고리듬을 이용원타임패스워드[11]를 만든다. 본 논문에서의 핀 값은 공개키 기반의 인증서 발급번호를 사용한다.

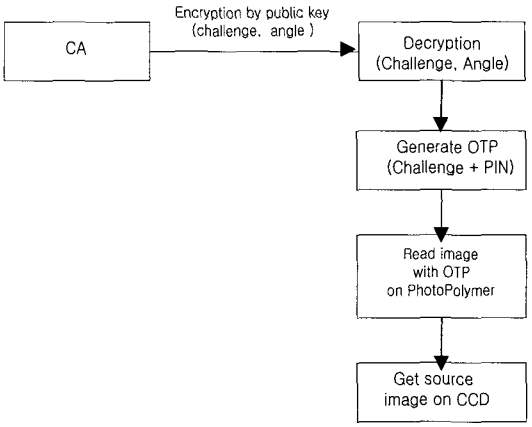
사용된 임의의 각도값과 챌린지는 영상 복호화를 위해 CA에 보관된다. 생성된 원타임패스워드를 위상 마스크 코드(Phase mask code)로 사용하여 [그림 2]와 같이 암호화를 한 후, 포토폴리머에 암호화된 영상을 임의의 각도값(Random Angle)에 따라 각 다중화 방법으로 기록한다.[그림 5]

영상 복호화 시 스마트카드 인증 및 위·변조 유무의 검증을 위하여 인증서버로부터 홀로그램을 읽기 위해 저장된 각도값과 원타임패스워드의 생성을 위한 챌린지 값을 인증서의 공개키로 암호화하여 가져온다. 원타임패스워드의 생성은 챌린지 값과 핀(인증서 발급번호)을 이용하여 생성한다. 인증서버로부터 전달받은 각도값과 생성된 원타임패스워드를 이용하여 영상을 읽은 후 [그림 6]과 같이 복호화 한다.

본 논문에서는 각 다중화 시 랜덤값을 사용하여 각을 정하고, 위상 마스크 코드(Phase mask code)를 원타임 패스워드로 다중화 함으로써 위·변조에 대한 가능성을 방지 하였다.



〔그림 5〕 영상 암호화



〔그림 6〕 영상 복호화

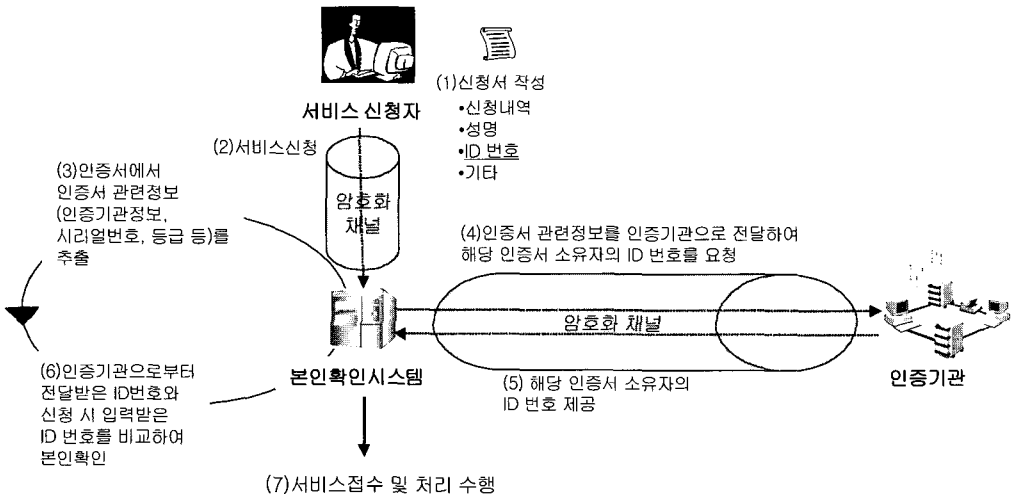
3.2 본인확인

인증서 유효성 검증만으로 해결할 수 없는 본인확인의 문제를 해결하고자 [그림 7]과 같은 방법을 제안하며, 처리 절차는 다음과 같다.

(1) 서비스 신청서를 작성하고 성명과, 아이디, 기타 정보를 입력한다.
(2) 전자 서명한 후 서비스 기관에 서비스 요청을 한다.
(3) 서비스 기관의 본인확인 시스템에서는 인증서에 포함된 관련정보(인증기관정보, 시리얼번호, 등급) 등을 추출한다.
(4) 추출한 정보를 [표 1]과 같은 요청전문을 인증기관으로 전달하여 인증서 소유자의 아이디 정보를 요청한다.
(5) 인증기관은 인증서 소유자의 아이디를 제공한다.
(6) 인증기관으로부터 전달받은 아이디 번호와 서비스 요청시 입력된 아이디 번호를 비교하여 본인

〔표 1〕 요청 메세지

Field name		Type	Remarks
Message code		Char(2)	RQ:Request AN:Answer
Data transmitted		Char(14)	YYYYMMDDhhmmss
No. of record		Number	
DATA	Length of record	Number	
	Service classification code	Char(2)	01: Identify 02: Check certification 03: 01 + 02
	Classification serial number of inquiry request server	Vchar(20)	
	DN name of certification issuing agency	Vchar(256)	
	Serial number of certification	Char(20)	
	ID No	Vchar(20)	



〔그림 7〕 본인확인 처리 절차

여부를 확인한 후 [표 2]와 같은 응답전문을 서비스 기관으로 보낸다.

(7) (6)의 결과에 따라 다음 서비스를 수행한다.

3.3 위·변조 유무 검증

본 논문에서는 본인확인 및 위·변조 방지를 위하여 다중 인증 방식을 사용하였다. 1차적인 방법은 스마트카드에 보관된 인증서를 통해 본인확인이 가능하도록 하였다. 그러나 1차적 방법의 본인 확인만으로는 스마트카드의 위·변조 유무를 검증할 수 없다. 이에 본 논문에서는 2차적으로 위·변조가 불가능한 광 폴리머에 기록된 정보와 스마트카드 메모리의 정보를 비교하여 위·변조 유무를 판별 검증 할 수 있도록 하였다. 이의 처리 흐름은 [그림 10]과 같으며 처리절차는 다음과 같다.

〔표 2〕 응답 메세지

Field name		Type	Remarks
Message code		Char(2)	AN:Answer
Data transmitted		Char(14)	YYYYMMDDhhmmss
No. of record		Number	
DATA	Length of record	Number	
	Service classification code	Char(2)	
	Classification serial number of inquiry request server	Vchar(20)	
	DN name of certification issuing agency	Vchar(256)	
	Serial number of certification	Char(20)	
	ID No	Vchar(20)	
	Answer code	Char(3)	
	Answer message	Vchar(200)	
Electronic signature value		Vchar(172)	Electronic signature value

(1,2) 인증서버로부터 각도값과 챌린지 값을 인증서 내의 공개키로 암호화 후 가져온다.

(3) 가져온 데이터를 비밀키로 복호화 한다.

(4) 복호화 된 챌린지 값과 핀을 이용하여 원타임 패스워드를 생성한다.

(5) 광폴리머에 저장된 정보를 읽는다.

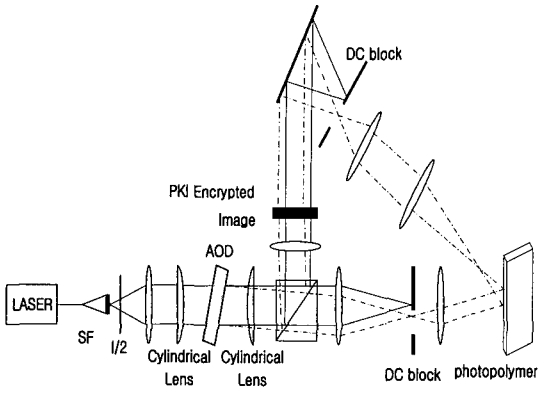
(6) 얻어진 정보를 해쉬 처리한다.

(7) 스마트카드 메모리내의 저장 정보 중 비교 검증할 정보를 비밀키로 복호화 한 후 이를 해쉬 처리한다.

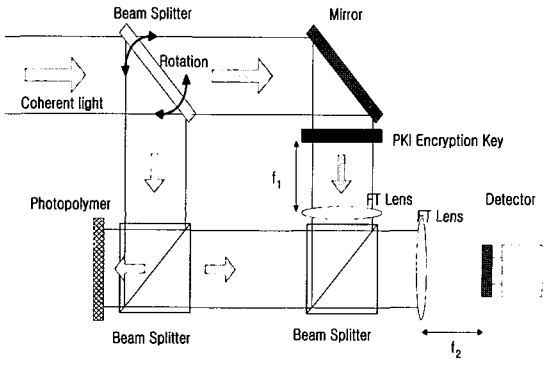
(8) (6)와 (7)의 해쉬값을 비교하여 위·변조 여부를 검사한다.

3.4 실험 및 결과

본 논문에서 제안한 광 영상 암호화 기반에서의 스마트카드 위·변조 방지에 관한 실험을 위해 [그림 8, 9]와 같이 인코더 및 디코더를 구축하였다. 구축된 인코더 및 디코더을 이용, [그림 10, 11]의 실험을 통해 본 논문에서 제안된 시스템을 검증하였다.구현된 시스템 [그림 16]을 적용한 결과는 [그림 12, 13]과 같다. [그림 12]는 광정보보호 기법으로 광정보보호 기법으



〔그림 8〕 영상 인코더

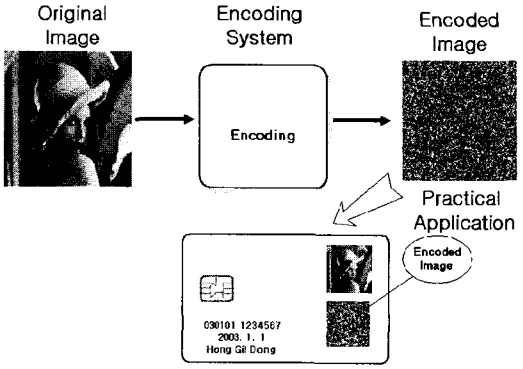


〔그림 9〕 영상 디코더

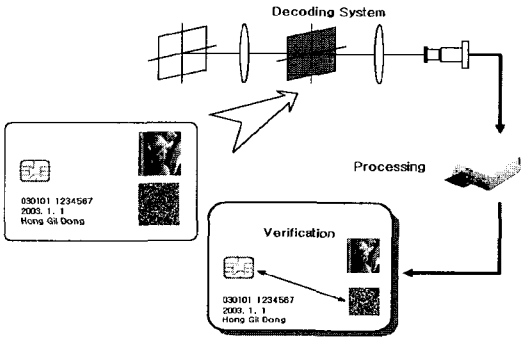
로 광 폴리머에 저장된 상태를 나타내며 [그림 13]은 저장된 정보를 조회 했을 때의 상태를 보여주고 있다. 두 개의 그림이 보여주는 것과 같이 기록된 자료와 조회된 자료가 일치됨을 알수 있다. 본인확인을 위해 구축된 시스템(H/W : IBM P660 6H1, O/S : AIX 4.3.3, 사용언어 : C)을 이용, [그림 14]의 실험을 통해 본 논문에서 제안된 시스템을 검증하였으며 이를 적용한 결과는 [그림 15]와 같이 얻었다. 이를 통해 본 논문의 보안성을 입증하였다.

Ⅳ. 결 론

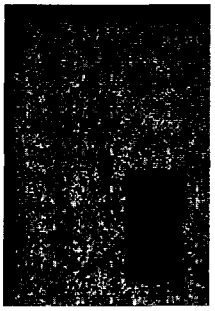
정보화 환경에서는 표준화된 정보기술기반 위에서 각종 정보와 서비스를 신속하게 제공하고 있다. 가상 환경에서의 주요 자료 및 개인정보의 유통이 급격하게 증가됨에 따라 유통 정보들에 대한 불법적인 도청, 위·변조 및 신분위장 등 각종 역기능에 의한 위협의 노출은 점점 더 커지고 있다.



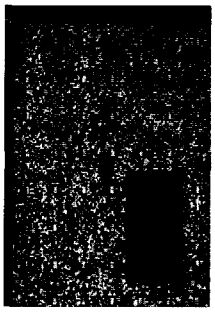
〔그림 10〕 영상 인코딩 실험



〔그림 11〕 영상 디코딩 실험

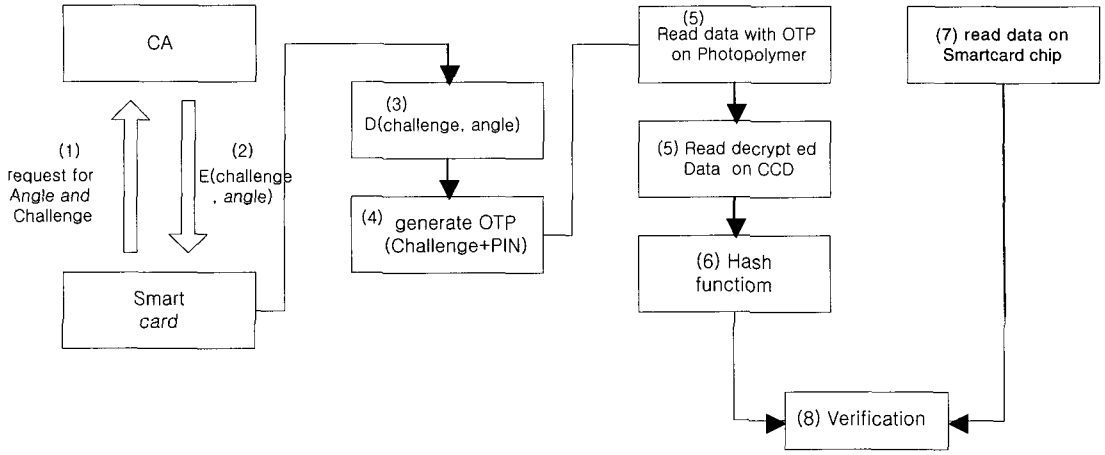


〔그림 12〕 Direct SLM picture



〔그림 13〕 recovered hologram

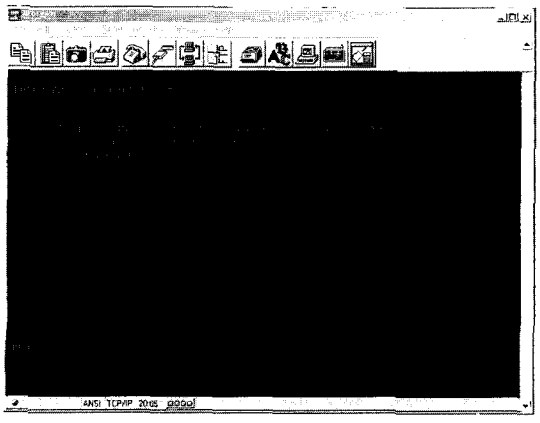
이를 방지하기 위해서는 대면 수준의 본인확인 등 신뢰성 기반 확보가 가장 중요하다고 할 수 있겠다. 그러나 현재의 공개키 기반 인증서는 사용자의 기본적인 인증 정보만을 제공하기 때문에 사용자의 대면 수준의 본인확인 및 권한 정보가 필요한 각종 응용 서비스에서는 그 사용이 제한적일 수밖에 없다. 이에 본 논문에서는 기존 시스템에서의 인증서 유효성 검



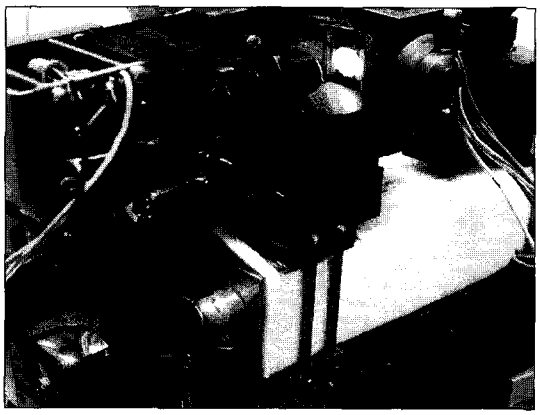
〔그림 14〕 위·변조 검증 절차

증만으로 해결할 수 없는 본인확인의 문제를 해결하고자 기존의 인증서 유효성에 대한 정보 외에 본인확인 방법을 제안함으로써 인증에 대한 신뢰성을 확보하였다.

디스크, CD-ROM, 디스켓 등 기존의 매체는 공개키 기반 인증서의 이동과 보안에 취약하여 이동성과 보안성이 뛰어난 스마트카드를 도입하여 사용하고 있다. 하지만 스마트카드에 대한 해킹기법이 실존하고 있고 위·변조 가능성 역시 있어 본 논문에서는 광영상 암호화 기법인 각 다중화 및 암호키 다중화 방법을 적용, 위·변조를 방지하였고 위·변조시 이를 검증할 수 있도록 하였다. 제안된 스마트카드 위·변조 방지시스템은 각 다중화 및 암호키 다중화를 이용한 영상 암호화기반 구조로 구성하였다.



〔그림 15〕 본인확인 실험 결과



〔그림 16〕 구현된 스마트카드 시스템

본 논문은 공개키 기반에서의 본인확인 체계와 영상 암호화 기반에서의 위·변조 방지 시스템을 구축함으로서 다중 인증 방식인 교차 인증을 통해 인증에 대한 신뢰성을 더욱 강화하였다.

참 고 문 헌

[1] Dataquest , July 1999

[2] Poul Kocher, Joshur Jaffe and Benja-min 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, Springer, 1991. Lecture Notes in Computer Science No. 547.

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

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

[6] B. Javidi, "Nonlinear joint power spectrum based optical correlation", Appl. Opt., vol.28, pp.2358~2367, 1989.

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

[8] Shimshon Berkovits, Santosh Chokhani, Judith A. Furlong, Jisoo A. Geiter, Jonathan C. Guild, Public Key Infrastructure Study: Final Report, Produced by the MITRE Corporation for NIST, April 1994.

[9] R.L.Rivest, A.Shamir and L.Adleman, "A method of obtaining digital signatures and public key cryptosystem," Comm. ACM, 21, 2, 1978, pp.120~126.

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

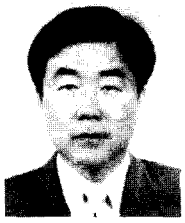
[11] Haller, N., "A One-Time Password System", RFC 1938, Bellcore, May 1996.

〈著者紹介〉

이 성 은 (Seong-Eun Lee)
1987년 2월~한양대학교 산업공학과 졸업
1992년 8월~한양대학교 산업대학원 전자계산학(공학석사)
2002년 8월~건국대학교 대학원 컴퓨터정보통신공학과(박사과정수료)
1990년 11월~1996년 10월 : 아주대학교, 중앙일보
1996년 10월~현재 : 행정자치부
<관심분야> 정보보안, 암호학, 스마트카드

장 홍 종 (Hong-Jong Chang)
1992년 2월~한양대학교 전자계산공학과 (공학석사)
2002년 8월~인하대학교 전자계산공학과 (공학박사)
1983년~1998년 : (재)건설기술교육원 전산실장
1999년 3월~2000년 2월 : 경인여자대학 겸임교수
2000년 5월~2001년 12월 : 행정자치부 전문위원
2000년 3월~현재 : 성결대학교 겸임교수
2002년 3월~현재 : 명지대학교 객원조교수
<관심분야> 정보보안, 암호학, 음성인식, 스마트카드, HCI

박 인 재 (In-Jae Park)
1989년~숭실대학교 전자공학과 졸업
1991년~숭실대학교 대학원 전자공학과(공학석사)
1997년~숭실대학교 대학원 전자공학과(공학박사)
1993년 11월~1996년12월 : 대우통신 종합연구소 연구원
1997년 2월~현재~행정자치부 정부전산정보관리소 전문위원
2000년 9월~현재~숭실대학교 정보통신전자공학부 겸임교수
<관심분야> PKI, KMI 등 정보보호기반 분야



한 선 영 (Sun-young Han)
1977년 서울대학교 계산통계학과(학사)
1979년 한국과학기술원 전산학 석사
1988년 한국과학기술원 전산학 박사
1981년~현재 건국대학교 컴퓨터공학과 교수
1989년 1월~1990년 1월 미국 Maryland대 컴퓨터 과학과 객원부교수
1990년 1월~현재 개방형 컴퓨터 통신 연구회 이사
1990년 9월~1997년 12월 한국과학기술원 인공지능 연구센터 참여교수
1991년 7월~1993년 12월 한국 정보과학회 정보통신연구회 부위원장
1996년 1월~1998년 1월 개방형 컴퓨터 통신 연구회 총무이사
1998년 1월~1999년 1월 미국 Maryland 대학교 컴퓨터 과학과 객원교수
2000년 3월~현재 건국대학교 정보통신원 원장
<관심분야> 인터넷 프로토콜, 네트워크 멀티미디어