# 디지털 홀로그래피를 이용한 광 보안인증 및 암호키 복호화

# Optical Security Authentication and Decryption of Encryped key using Digital Holography

길상근, 박영민, 변현중, 이양재, 최진하, 하승호*
수원대학교 전자공학학과, *수원대학교 TIC
skgil@suwon.ac.kr

개방형 정보통신망이 사회 전반에 걸쳐 급속히 확산됨에 따라 정보통신 시스템의 보안 취약점이 심각하게 노출되기 시작하면서 보안의 필요성에 대한 인식이 높아지고 있다. 현재 네트워크에서 사용되는 보안은 그저 개인을 코드화하고 있는 시스템이며, 보안기능을 단지 소프트웨어에 의존하기 때문에 항시 정보 해킹의 위험에 노출되어져 있다. 이러한 문제점을 극복하기 위해 광학적 데이터 처리 기법을 이용한 다양한 정보보안 기법이 제안되고 있다[(1)-(3)]. 본 논문에서는 정보 데이터를 표시하기 위한 LCD와 홀로그램을 직접 기록하기 위한 CCD 카메라를 사용하여 구현되는 디지털 홀로그래피를 이용한 광 보안인증 및 암호키(비밀키) 복호화에 대한 새로운 기법을 제안한다. 제안된 시스템은 정보를 디지털 방식과 광학적 방법을 혼합하여 암호화, 전송, 복호화를 가능하게 하며, 인증후 부여받은 비밀키에 의해 보내고져 하는 데이터를 다시 암호화하여 전송할 수 있다.

(그림 1)은 본 논문에서 제안한 광 보안인증 및 암호키 복호화 시스템에 대한 그림이다. 개인 ID 데이터는 공통키에 의해 홀로그램으로 암호화되고 전송되어진 후 상대방에 의해서 공통키에 의해 복호화된다. 개인 ID가 인증이 되면 상대방이 랜덤하게 비밀키를 발생하여 전송되어 온 홀로그램 정보를 이용하여 다시 홀로그램으로 암호화한 후 반송한다. 반송되어 온 암호화된 비밀키는 자신이 ID 데이터를 암호화할 때 사용한 홀로그램 정보를 이용하여 복호화 한다. 이때 복원된 비밀키는 다시 정보를 보낼 때 암호화에 사용된다. (그림 2)는 디지털 홀로그래픽 암호화/복호화에 대한 광학적 장치도로 마흐-젠더 간섭계를 기본으로 한다. 예를 들어 S1, S2 스위치가 개방하고 S3 스위치를 닫으면, LCD1에 ID 데이터를 LCD2에 공통키가 참조광으로 하여 홀로그램으로 암호화된 정보는 CCD1에 기록되어 PC에 저장되고 전송된다. 한편 복호화 장치로 사용될 때는 홀로그램 정보를 LCD3에 공통키를 LCD2에 표시하여 ID 데이터를 복호화 한다. 이때 S1 스위치는 닫고 S2, S3 스위치는 개방하여 복원된 데이터가 CCD2에 기록된고 PC에 전송되어 ID를 확인한다. 마찬가지로 같은 장치구조에서 역전송된 홀로그램은 LCD3에 전송하였던 홀로그램 정보는 LCD2에 나타내어 정보를 CCD2에 복호시킨다.

$s(x,y), k(x,y)$를 각각 ID 데이터와 공통키 함수라 하고 푸리에 홀로그램을 구하여 복호화 하면

$$I_1(\alpha,\beta) = [S(\alpha,\beta) + K(\alpha,\beta)]^2 = [S]^2 + [K]^2 + SK^* + S^* K$$

$$H_1(\alpha,\beta) = S(\alpha,\beta)K^*(\alpha,\beta)$$

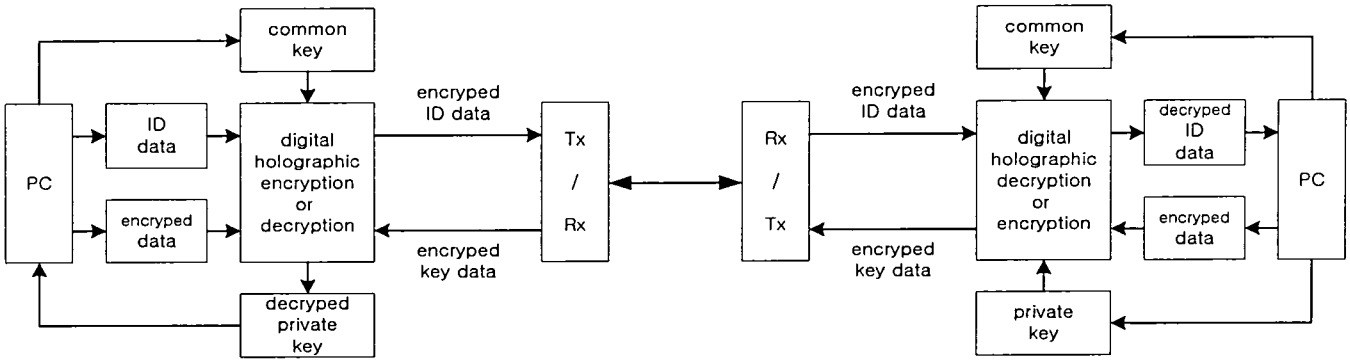
$$d_1(x,y) = F^{-1}[H_1(\alpha,\beta)K(\alpha,\beta)] = s(x,y)$$

이다. 한편, $r(x,y)$를 비밀키 함수라 하고 $F^{-1}[H_1]$을 참조광으로 홀로그램을 구하여 복호화 하면

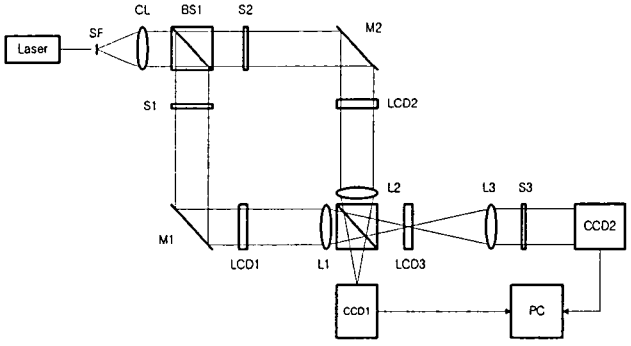
$$I_2(\alpha,\beta) = [R(\alpha,\beta) + h_1(\alpha,\beta)]^2 = [R]^2 + [h_1]^2 + Rh_1{}^* + R^* h_1$$

$$H_2(\alpha,\beta) = R(\alpha,\beta)h_1{}^*(\alpha,\beta)$$

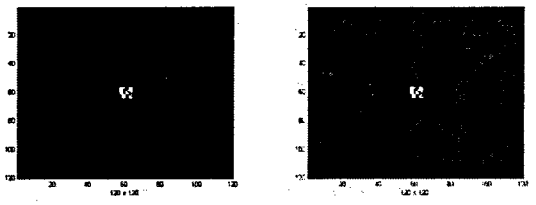
$$d_2(x,y) = F^{-1}[H_2(\alpha,\beta)h(\alpha,\beta)] = r(x,y)$$




(그림 1) 광 보안인증 시스템

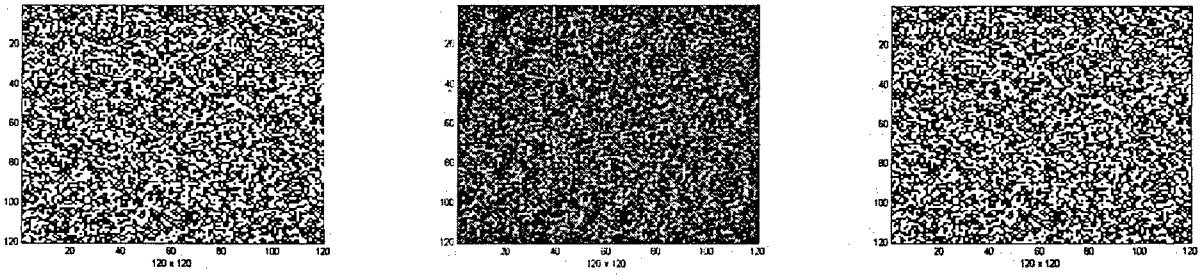



(그림 2) 디지털 홀로그래피 광 암호화/복호화 장치



(a) (b)

(그림 3) (a) ID 데이터 (b) 복호화된 ID 데이터 : 'skgil123'의 ASCII code



(a) (b) (c)

(그림 4) (a) 비밀키 데이터 (b) 복호화된 비밀키(threshold 전) (c)복호화된 비밀키(threshold 후)

*본 연구는 한국과학재단 목적기초연구(R01-2003-000-10528-0(2003)) 지원으로 수행되었습니다.

**참고문헌**

1. B. Javidi, T. Nomura, "Securing information by use of digital holography", Opt. Lett. 25, No.1, Jan.(2000).
2. S. Zhang, M. A. Karim, "High-security optical integrated stream ciphers", Opt. Eng. 38(1), Jan.(1999).
3. T. Kawase, A. Watanabe and I. Sasase, "Proposal of secure remote access using encryption", IEEE, (1998).