생체신호인 조상(nail bed)패턴을 이용한 영상정보의 광 암호화 및 복호화

Optical encryption and decryption of image information by use of nail bed patterns

김용우, 김태근
세종대학교 광 공학과
e-mail: takim@sejong.ac.kr

대량의 정보가 생산되고 유통되는 21 세기 정보화 사회에 있어 정보사기 및 위조는 가깝게는 은행, 사업자, 소비자를 위시한 경제 활동 관계자로부터 크게는 정보 사회 전 분야에 있어 가장 시급하고 중요한 과제이다. 그러나 높은 단계의 보안성을 갖으며 실-시간 처리가 가능한 전자적 보안 시스템의 부재는 정보보호 기술개발의 다급함에도 불구하고 정보보호를 위한 해를 제시하지 못하고 있는 실정이다. 기존의 정보보안 장치에서 정보의 암호화는 암호 키(key)를 이용하여 전자적인 방법으로 암호화해 전송하고, 전송된 신호를 전자적인 방법으로 복호화하는 과정을 통해 이루어졌다. 전자적인 방법을 이용한 정보의 암호화와 복호화는 다음과 같은 단점이 있다. 첫째는 대량의 정보의 경우 정보저장이 어려우며 막대한 연산량 때문에 초고속 통신에 있어 필수요소인 실시간 정보처리가 불가능하다는 것이고, 둘째는 암호 키(key)의 분실 혹은 고의적 양도에 의한 부정사용을 방지하기가 어렵다는 것이다. 이에 본 논문에서는 생체신호인 조상(爪床, nail bed)패턴으로 만들어진 암호 키(key)를 사용함으로서 보안성을 높이고, 동시에 막대한 연산시간을 극복하고 실시간 처리가 가능한 광학적인 방법으로 암호화하는 광 암호화 시스템을 제안한다.

혼탁매질인 손톱의 하부면에는 개인별로 상이한 융선 과 골 구조의 패턴인 조상(nail bed)이 있다. 이 중 융선에는 혈액이 흐르는 모세혈관 고리(capillary loop)가 밀집 되 있고 융선과 융선은 모세혈관 고리가 밀집 되 있지 않은 골로 구분되어있다. $670nm$ 파장의 레이저 빛은 피부의 진피(dermis)에서 산란특성을 가지며 혈액에는 강하게 흡수된다. 이와 같은 생체-광학적 특성에 착안하여 콘포칼 광 스케닝(confocal optical scanning)방법으로 조상(nail bed)패턴을 실제 실험을 통해 추출해 낸다.[(1)] 추출된 조상(nail bed)패턴을 이용하여 그림 1과 같은 방법으로 조상(nail bed) 키(key)-코드(code)를 만들고, 만들어진 키(key)-코드(code)를 암호 키(key)로 사용하는 그림 2의 결합 변환 상관기(JTC)구조의 광 암호화기와 복호화기를 통해 영상정보를 암호화하고 복호화한다.[(2)] 그리고 조상(nail bed) 키(key)-코드(code)와 퓨리에 변환(fourier transform)관계를 갖는 조상(nail bed) 위상-마스크(phase-mask) G(p,q)를 개인별로 correlation 하여 correlation peak의 유무를 통해 인증(authentication)함으로서 영상정보의 진위여부를 판별한다. 그림 3과 그림 4는 제안된 방법이 실제로 가능함을 보이기 위한 컴퓨터 시뮬레이션 결과이다. 본 논문이 제안하는 방법은 기존의 광 암호화 시스템에 대해서 다음과 같은 장점을 갖는다. 첫째, 조상(nail bed)의 생체-광학적 특성에 착안하여 생체신호인 조상(nail bed)패턴을 추출하여 암호 키(key)-코드(code)로 사용함으로서 기존의 정보보안 장치의 주된 단점인 암호 키(key)의 분실 혹은 고의적 양도에

의한 부정사용을 방지하여 보안성을 높이게 된다. 둘째, 이와 동시에 제안하는 방법은 조상(nail bed) 위상 마스크(phase mask)를 correlation 하여 개인을 구별해냄으로서 제작자와 소유자의 판독을 가능하게 하는 암호 키(key)의 투명성을 확보하게 된다.

참고문헌

1. 김태근, 김용우, 김해일, "손톱하부면 조상(nail bed)패턴의 콘포칼 광 스케닝 방법을 이용한 추출과 개인인증," 한국광학회지 제13권 제2호, 2002년 4월.
2. T. Nomura, B. Javidi, "Optical encryption using a joint transform correlator architecture," *Opt. Eng.*, Vol. 38, No. 8, pp. 2031-2035, 2000.

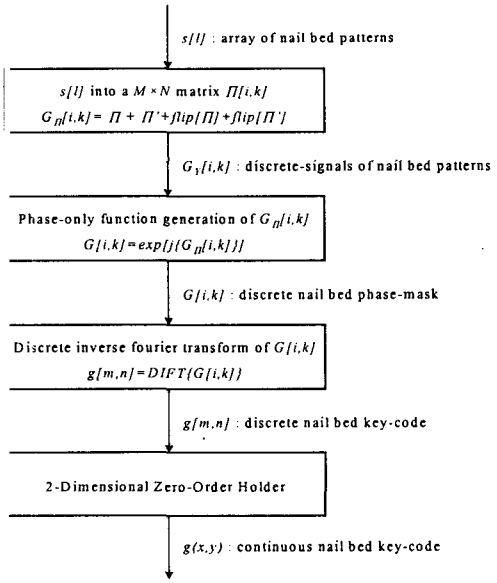

그림 1. Nail bed key-code generation.

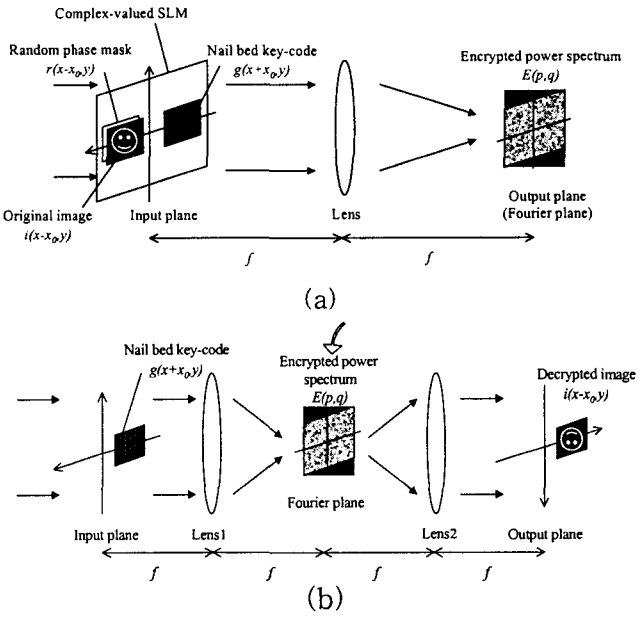

그림 2. (a) Optical encryption system and (b) decryption system.

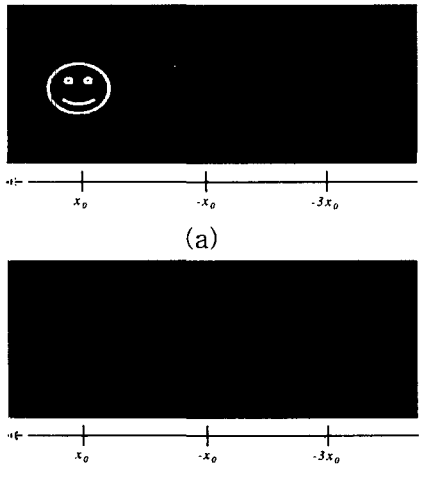

그림 3. Decrypted image
(a) with correct nail bed key-code and
(b) with incorrect nail bed key-code.

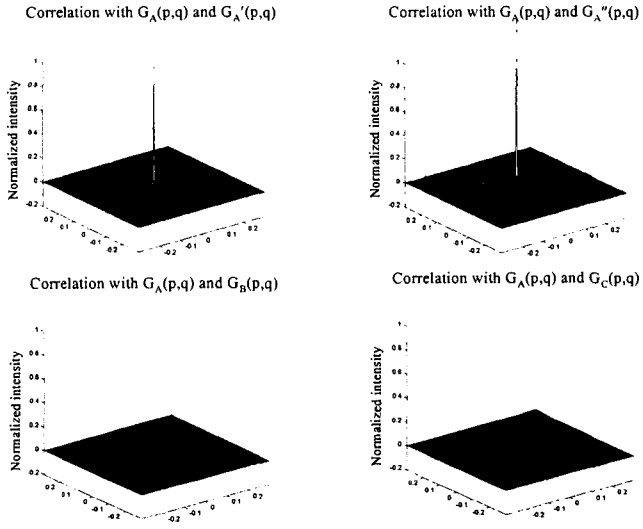

그림 4. Correlation peak