《연구논문》 Hankook Kwanghak Hoeji, Volume 15, Number 2, April 2004

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

김용우 · 김태근†

세종대학교 광공학과

㉾ 143-747 서울시 광진구 군자동 98

(2003년 6월 9일 받음, 2004년 3월 18일 수정본 받음)

본 논문에서는 콘포칼 구조의 광학계를 이용하여 생체신호인 조상(nail bed)패턴을 추출하고 그를 암호키로 이용해 암호 키(key)의 고의적 양도나 부정사용을 방지해 높은 보안성을 갖는 광 암호화 및 복호화 방법을 제안한다. 또한 암호화된 영상은 생체정보를 포함하고 있기 때문에 영상정보의 진위여부를 개인의 인증(authentication)을 통해서 가려낼 수 있다.

주제어 : optical encryption and decryption, nail bed, key-code, biometric information, authentication.

I. 서 론

정보화 사회의 확대에 따라 필요한 정보의 양도 기하급수적으로 늘어나게 되고, 그 만큼 정보는 다양한 형태로 세분화되고 있다. 이에 따라 정보를 빠르게 처리할 수 있는 수단뿐 아니라 많은 양의 정보를 관리하는 방법도 필요하게 되었다. 컴퓨터와 정보통신 기술의 발전은 이러한 현대사회의 요구를 충족시키는데 결정적인 역할을 하게 되었다. 하지만 컴퓨터와 정보통신 기술의 발전에 따라 불법적인 해킹이나 정보사기 및 위조 기술 등도 보편화되고 있는 실정이다. 이로 인해 제한된 정보가 터무니없이 공개 되어버리는 보안성의 문제가 날로 심각하게 대두되고 있다. 따라서 정보사회 전 분야에 있어 정보보안 장치의 개발은 현재 가장 시급한 과제 중 하나가 되고 있다.

정보보안 장치는 여러 가지 정보보안 방법으로 개발되고 있다. 정보보안 방법은 크게 개인을 인증하여 저장된 정보에 대한 접근을 허가하는 개인인증(individual identification) 방법과 정보를 불규칙적으로 분포하여 암호화한 뒤 허가된 사람들에게만 배포하는 암호화(encryption) 방법으로 분류할 수 있다. 이중 개인인증 방법은 전자적 인증방식에서부터 보안 수준의 향상을 위해 바이오메트릭(biometric)을 이용한 생체인증 시스템[1-3]에 이르기까지 그 범위를 넓혀가고 있다. 최근에 암호화 방법에 있어서는 빠른 정보처리와 높은 보안성을 갖는 광 암호화 방법이 관심을 모으고 있다. 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 키의 분실 혹은 고의적 양도에 의한 부정사용을 방지하기가 어렵다는 것이다. 이에 본 논문에서는 손톱하부면에 위치하는 조상(爪床, nail bed)의 생체-광학적 특성을 이용하여 생체신호인 조상패턴을 추출하고, 추출된 조상패턴으로 만들어진 암호 키를 사용함으로서 기존의 정보보안장치의 주된 단점인 암호 키의 부정사용을 방지하여 보안성을 높이고, 동시에 실시간 처리가 가능한 광학적인 방법으로 암호화하는 광 암호화 시스템을 제안한다. 본 논문의 2장의 첫째 절에서는 손톱하부면의 조상의 구조와 조상의 생체-광학적 특성을 이용한 조상패턴의 추출에 대해 논한다. 둘째 절에서는 추출된 조상패턴을 이용하여 위상 마스크(phase mask)와 암호 키-코드(key-code)를 만들고, 셋째 절에서는 만들어진 암호 키를 이용하는 결합 변환 상관기(JTC, joint transform correlator)구조의 광 암호화 방법을 제안하고 논한다. 넷째 절에서는 각각의 조상패턴으로 만든 위상 마스크를 corrleation 하여 개인을 구별해내는 인증(authentication)기법을 제안한다. 마지막으로 3장에서는 컴퓨터 시뮬레이션을 통해 본 논문이 제안하는 광 암호화 방법과 인증방법이 실제로 가능함을 보인다.

II. 조상(nail bed)패턴을 이용한 광 암호화 및 복호화 시스템

광 기술을 이용한 암호화 및 보안 시스템은 그의 실시간 병렬처리 가능성으로 최근 연구가 활발하게 진행 중이다.[9-16] 광학적 암호화 시스템의 모태라 할 수 있는 두 개의 랜덤 위상 함수를 이용한 암호화 기술[9,10]은 데이터의 암호화가 정상 백색 랜덤 처리 과정을 통해서 이루어진다. 이 방법은 4f-system을 이용하므로 정확한 광 축 정렬을 요구하게 되고, 암호화되는 랜덤 위상 마스크의 정확한 복소공액(complex conjugate)의 제작을 요구하게 되는 단점이 있다.[9,10] 기존의 4f-system 의 단점을 극복하기 위한 연구는 정확한 광 축 정

†E-mail: takim@sejong.ac.kr

렬과 키-코드의 복소공액 제작을 요구하지 않는 결합 변환 상관기[17,18]를 찾아내었고, T. Nomura와 B. Javidi에 의해 결합 변환 상관기 구조를 기반으로 한 광 암호화 방법(optical encryption using a joint transform correlator architecture)이 제안되었다.[19]

본 논문에서는 생체신호인 조상신호를 추출하고 그를 합성해 결합변환 상관기 구조의 광 암호화기의 암호 키로 이용하는 광 암호화 방법을 제안한다. 그림 1은 본 논문이 제안하는 광 암호화 및 복호화 시스템의 구성을 보여준다. 제안하는 방법은 크게 암호화 부분과 복호화 부분으로 나뉜다. 암호화 부분에서는 조상추출기를 통해 A라는 사람의 조상신호를 추출하여 조상 위상 마스크를 합성하고 이것의 역 퓨리에 변환해 조상 키-코드를 만든다. 그림 1에서 $\mathfrak{I}\{\cdot\}$과 $\mathfrak{I}^{-1}\{\cdot\}$은 각각 퓨리에 변환(fourier transform) 연산자와 역 퓨리에 변환(inverse fourier transform) 연산자를 나타낸다. 이후 평행광(collimated light)에 의해서 독립된 랜덤 위상 마스크와 오리지널 영상(original image)이 곱해지고, 만들어진 조상 키-코드는 이들과 함께 나란히 결합 변환 상관기 구조의 광 암호화기를 통해 암호화 된 데이터(encrypted data)를 만든다. 이렇게 만들어진 암호화 데이터를 무선 또는 유선 통신망을 통해서 복호화 부분으로 전달하고, 조상 키-코드는 물리적으로 봉인된 안전한 통신 경로나 안전성이 확보된 방법을 통해 복호화 영역으로 전달한다. 이렇게 전달된 암호화 데이터는 암호 키인 조상 키-코드와 함께 광 복호화기를 통해 원래의 영상을 복원한다. 조상 키-코드가 A라는 사람으로부터 제작되었는지 그리고 정확히 복호영역에 전달되었는지 여부를 개인별로 만들어진 조상 위상 마스크를 correlation 하여 인증한다. 그림 1에서 A와 B는 각각 다른 사람이고, A′은 개인을 구별하기 위하여 A라는 사람의 조상신호를 다른 시간간격으로 추출해낸 것을 나타낸다. 이로서 제안하는 시스템은 결합변환 상관기 구조를 통한 광 암호화의 장점과 동시에, 생체신호를 키-코드로 사용하기 때문에 복호된 영상의 진위여부에 대한 인증이 가능하여 정보의 투명성을 확보할 수 있다.

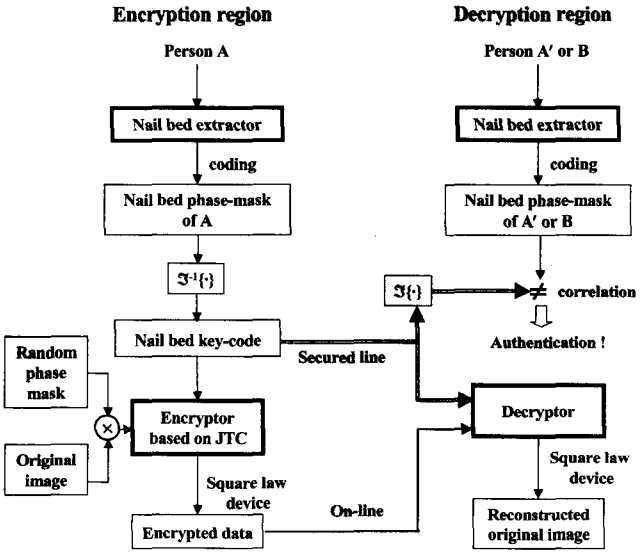


그림 1. Block diagram of the proposed optical encryption and decryption system.

2.1. 손톱하부면의 조상(nail bed)의 구조와 조상(nail bed)패턴의 추출

조상은 손톱하부면의 진피층과 조판사이에 위치하며 조상패턴은 불규칙한 간격의 융선과 골로 구성된 선으로 이루어져 있으며 개인별로 각각 상이하다.[4] 융선에는 혈액이 흐르는 모세혈관 고리(capillary loops)가 모여 있고 골에는 피부조직인 진피(dermis)로 이루어져 있다. 이때 670 nm 파장의 레이저 빛은 융선에 밀집되어있는 혈액에서 강하게 흡수되고, 골에 해당하는 진피에서는 산란되어 진다.[5,6] 이렇게 손톱하부면 조상의 해부학적 구조에 따른 생체-광학적 특성에 따라 그림 2의 콘포칼 구조의 광 스캐닝 시스템[7]을 이용하여 실제로 인간의 손톱을 스캐닝해 조상패턴을 추출해 낸다.[8] 그림 2의 광학계는 670 nm 파장의 레이저(laser), 빔 스플리터(beam splitter), 스캐닝 거울(scanning mirror), 대물 렌즈(objective lens), 집광 렌즈(collecting lens), 광 검출기 (photo-detector) 그리고 밴드 패스 필터(band pass filter)로 구성되어 있다. 레이저에서 나오는 빛은 빔 스플리터를 거쳐 스캐닝 거울에 입사되고 스캐닝 거울은 입사된 빛을 시간에 따라 다른 각도로 반사한다. 스캐너가 빛을 시간에 따라 다른 각도로 반사함으로 초점이 맞추어진 레이저 빔은 조상을 스캐닝하게 된다. 조상의 융선에 모세혈관이 밀집되어있고 모세혈관에 흐르는 혈액에 $670nm$ 파장의 레이저 빛이 강하게 흡수됨에 따라 융선과 골은 상이한 반사율을 갖게 된다. 그러므로 스캐닝 위치에 따라 반사되는 빛의 양이 상이하게 된다. 스캐닝 위치에 따라 상이한 양의 반사된 빛은 스캐닝 빛이 입사된 반대 방향으로 진행해 렌즈를 지나 스캐닝 거울에 의해 반사되고 빔 스플리터에 인가된다. 빔 스플리터에 인가된 빛의 반은 빔 스플리터에 의해 반사되어 집광 렌즈에 인가된다. 집광 렌즈에 인가된 빛은 집광 렌즈에 의해 광 검출

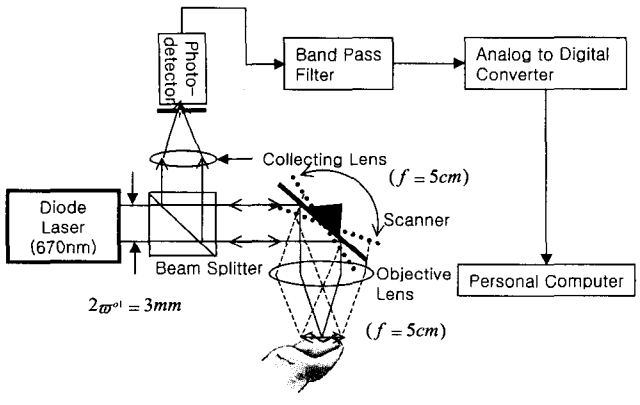


그림 2. Confocal scanning optical system.

기에 모아진다. 광 검출기는 광 검출기에 인가된 빛의 양에 비례해서 전기신호를 만들어 낸다. 만들어진 조상패턴의 전기신호를 밴드패스 필터에 인가하여 여과(filtering) 시킴으로써 손톱표면에서 반사된 고주파성분의 빛과 벗어난 초점(defocused)영역에 의한 저주파 성분의 잡음(noise)을 제거한다. 여과된 전기신호는 아날로그-디지털 변환기(A/D converter)에 의해 451개의 디지털 신호로 표본화(sampling) 되어 컴퓨터에 입력된다.[8] 본 논문에서는 콘포칼 구조의 광 스캐닝 시스템에 의해 조상신호를 추출하고 그를 암호 키로 이용하는 광 암호화 및 복호화 시스템을 제안한다.

2.2. 조상(nail bed)패턴을 이용한 키(key)-코드(code)의 제작

암호 키는 추출된 조상패턴을 이용 아래의 과정을 통해 합성된다. L개의 디지털 정보로 저장되어진 조상패턴은 이산신호(discrete signal)인 1차원 행렬 $s[l]$로 표현된다.

$$s[l]=[\,a_1\ a_2\ a_3 \ldots\ a_l \ldots\ a_L]=(\,a_l)_{L\times 1} \tag{1}$$

위에서 a_l은 $s[l]$의 행렬요소(matrix element)이고 l 이라는 index number를 갖는다. $s[l]$는 $L\times 1$의 크기를 갖는 이산신호 행렬이며 $(\,a_l)_{L\times 1}$로 축약해서 기술한다. 우선 행렬 $s[l]$를 아래의 방법을 통해 변환해 $M\times N$의 크기를 갖는 2차원 행렬, $\Pi[i,k]$를 합성한다.

$$\Pi[i,k]=\begin{bmatrix} b_{11} & b_{12}\ldots & b_{1i}\ldots & b_{1N} \\ b_{21} & b_{22}\ldots & b_{2i}\ldots & b_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ b_{k1} & b_{k2}\ldots & b_{ik}\ldots & b_{kN} \\ \vdots & \vdots & \vdots & \vdots \\ b_{M1} & b_{M2}\ldots & b_{Mi}\ldots & b_{MN} \end{bmatrix}=(\,b_{ik})_{M\times N} \tag{2}$$

위에서 b_{ik}는 $\Pi[i,k]$의 행렬요소이며 $s[l]$의 행렬요소 a_l에 대하여 다음의 관계를 갖는다.

$$b_{ik}=a_{\mathrm{mod}[\frac{i+k-1}{L}]} \tag{3}$$

여기서 $\mathrm{mod}[\frac{i+k-1}{L}]$는 modulus 연산자로 $(i+k-1)$을 L로 나눈 나머지 값이다. 본 연구에서는 M과 N을 86으로 하고, L을 451로 한다. $\Pi[i,k]$는 L개의 디지털 정보로 구성된 조상패턴을 $M\times N$ 화소의 크기를 갖는 행렬 데이터로 재구성한 것이다. 해독에 유리한 규칙성을 제거하기위해 키의 위상성분 $G_\Pi[i,k]$는 $\Pi[i,k]$를 아래와 같이 합성해 제작한다.

$$G_\Pi[i,k]=\Pi+\Pi'+flip[\Pi]+flip[\Pi'] \tag{4}$$

위에서 Π'는 Π의 전치행렬(transpose matrix)이고 $flip[\cdot]$는 임의의 행렬 U에 대해서;

$$U=\begin{bmatrix} u_{11} & u_{12}\ldots & u_{1n} \\ u_{21} & u_{22}\ldots & u_{2n} \\ \vdots & \vdots & \vdots \\ u_{m1} & u_{m2}\ldots & u_{mn} \end{bmatrix},\quad flip[U]=\begin{bmatrix} u_{1n} & \ldots u_{12} & u_{11} \\ u_{2n} & \ldots u_{22} & u_{21} \\ \vdots & \vdots & \vdots \\ u_{mn} & \ldots u_{m2} & u_{m1} \end{bmatrix} \tag{6}$$

로 정의되는 연산자이다. $G_\Pi[i,k]$를 위상정보로 갖는 위상마스크, $G[i,k]$는 다음과 같이 합성되어진다.

$$G[i,k]=\exp[j\{\,G_\Pi[i,k]\}] \tag{7}$$

이산 공간(discrete space)에서 키-코드, $g[m,n]$는 $G[i,k]$의 이산 역 퓨리에 변환(IDFT, inverse discrete fourier transform)으로 아래와 같이 주어진다.[21]

$$g[m,n]=\frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{k=0}^{N-1}G[i,k]\,e^{+j\frac{2\pi}{M\times N}(im+kn)} \tag{8}$$

여기서 m과 n은 역 퓨리에 변환된 영역의 좌표계이다. 2.3절의 광 암호화기에서 이 이산신호는 공간 광 변조기(SLM, spatial light modulator)[22]에 의해서 연속적인 광 신호(continuous optical signal)로 변환되어 처리된다. 공간 광 변조기에 의한 이산신호의 연속 광 신호로의 변환은 수학적으로 2-D ZOH(2-dimensional zero-order holder)[21]로 모델 되어 다음과 같이 주어진다.

$$g(x,y)=g[m,n] \tag{9}$$

위 식에서 $g(x,y)$는 연속신호이며 x와 y가 $m\Delta x < x < (m+1)\Delta x$, $n\Delta y < y < (n+1)\Delta y$의 범위를 만족할때 이산신호, $g[m,n]$의 값을 갖는다.[21] 이때 공간 광 변조기의 영역이 X와 Y일 때 $\Delta x=\frac{X}{M}$이고 $\Delta y=\frac{Y}{N}$이다. 이렇게 만들어진 $g(x,y)$는 아날로그 광 정보처리를 위한 조상 키-코드가 된다.

2.3. 조상(nail bed)패턴을 이용한 광 암호화 및 복호화

그림 3은 결합변환 상관기 구조를 이용한 광 암호화 및 복호화 시스템을 보여준다. $i(x,y)$는 암호화시킬 영상이며 0에서부터 1의 양의 실수 값을 갖는다. $r(x,y)$은 임의의 독립된 순수 랜덤 위상 마스크이고, $g(x,y)$는 앞 2.2절에서 정의된 조상패턴을 이용한 키-코드이다. 그림 3(a)의 조상 키-코드를 이용한 암호화 과정은 다음과 같다. 초점거리 f를 갖는 렌즈의 앞 초점 면(front focal plane)을 입력 면(input plane)이라 하고, 복소 값의 구성을 갖는 공간 광 변조기(complex-valued SLM)[22]를 입력 면에 배치시킨다. 배치된 공간 광 변조기의 왼쪽 면에는 임의의 순수 랜덤 위상 마스크인 $r(x,y)$과 암호화시킬 영상정보인 $i(x,y)$를 겹쳐서 x축을 중심으로 $+x_0$지점에 배치시키고, 오른쪽 면에는 조상 키-코드인 $g(x,y)$를 x축을 중심으로 $-x_0$지점에 배치시킨다. 초점거리 f를 갖는 렌즈의 뒤 초점 면(back focal point)인 출력 면(output plane)에 제곱법칙 검출기(square-low detector)를 배치시킨다. 입력 면에 평행 광(collimated light)이 입사되고 입사된 평행광에 의해서 $r(x,y)$과 $i(x,y)$가 곱해지고, 곱해진 $r(x,y)$과 $i(x,y)$는 x축을 중심으로 $2x_0$만큼 차이를 두어 $g(x,y)$와 더해진다. 이것은 퓨리에 렌즈를 통해 퓨리에 변환이 되고, 출력 면에 $r(x,y)$, $i(x,y)$, $g(x,y)$의 정보가 응집되어 기록

된다. 기록된 데이터는 제곱법칙 검출기에 의해 검출되어진다. 검출되어진 데이터는 암호화 데이터가 되고 암호화 데이터는 제곱법칙 검출기에 의해서 순수 실수 값(real-only valued)만을 갖는다. 암호화 데이터가 기록된 결합 파워 스펙트럼(joint power spectrum)을 $E(p,q)$라 정의하면, $E(p,q)$는 다음과 같다.

$$\begin{aligned} E(p,q) &= |\Im[r(x-x_0,y)i(x-x_0,y)+g(x+x_0,y)]|^2 \\ &= |R(p,q)\otimes I(p,q)\exp(-jx_0p)+G(p,q)\exp(jx_0p)|^2 \\ &= |R(p,q)\otimes I(p,q)|^2+|G(p,q)|^2 \\ &+ [R(p,q)\otimes I(p,q)]^*G(p,q)\exp(j2x_0p) \\ &+ [R(p,q)\otimes I(p,q)]\ G^*(p,q)\exp(-j2x_0p) \end{aligned} \quad (10)$$

여기서 $\Im[\cdot]$는 퓨리에 변환 연산자를 나타내고, 퓨리에 변환은 함수 $f(x,y)$에 대해서

$$\Im\{f(x,y)\}=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}f(x,y)\ e^{-ipx-iqy}dxdy=F(p,q) \quad (11)$$

과 같이 정의된다.[23] 그리고 ⊗는 convolution 연산자를 나타내며 convolution 은 함수 $f(x,y)$와 $h(x,y)$에 대하여

$$f(x,y)\otimes h(x,y)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}f(x',y')h(x-x',y-y')dx'dy' \quad (12)$$

과 같이 정의된다.[23] 위 첨자 *는 복소공액(complex conjugate)을 의미한다.

그림 3(b)의 복호화 과정은 다음과 같다. 각각 초점거리 f를 갖는 두 개의 렌즈를 이용하여 그림 3(b)에서와 같이 4개의 초점거리를 갖는 4f-system을 구성한다. 첫 번째 렌즈(lens-1)의 앞 초점면인 입력면에 조상 키-코드인 $g(x,y)$를 x축을 중심으로 $-x_0$지점에 배치시킨다. 이때 $g(x,y)$가 배치되는 위치는 암호화 과정에서 $g(x,y)$를 배치한 위치와 동일하다. 첫 번째 렌즈의 뒤 초점면이자 두 번째 렌즈(lens-2)의 앞 초점면인 퓨리에면에 암호화된 파워 스펙트럼인 $E(p,q)$를 중앙에 배치시킨다. 두 번째 렌즈의 뒤 초점면인 출력 면에는 암호화 과정과 동일하게 제곱법칙 검출기를 배치시킨다. 위의 복호화 시스템의 입력 면에 평면 광이 입사되면 첫 번째 퓨리에 렌즈(lens-1)를 통해 퓨리에 변환이 되어지고, 퓨리에 변환된 조상 키-코드는 $E(p,q)$와 곱해지게 된다. 배치된 조상 키-코드가 첫 번째 렌즈(lens-1)를 통해 퓨리에 변환이 되어 $E(p,q)$와 곱해진 면에서의 빛의 분포, $D(p,q)$는 아래와 같다.

$$\begin{aligned} D(p,q) &= E(p,q)\Im[g(x+x_0,y)] \\ &= E(p,q)G(p,q)\exp(jx_0p) \\ &= |R(p,q)\otimes I(p,q)|^2G(p,q)\exp(jx_0p) \end{aligned}$$

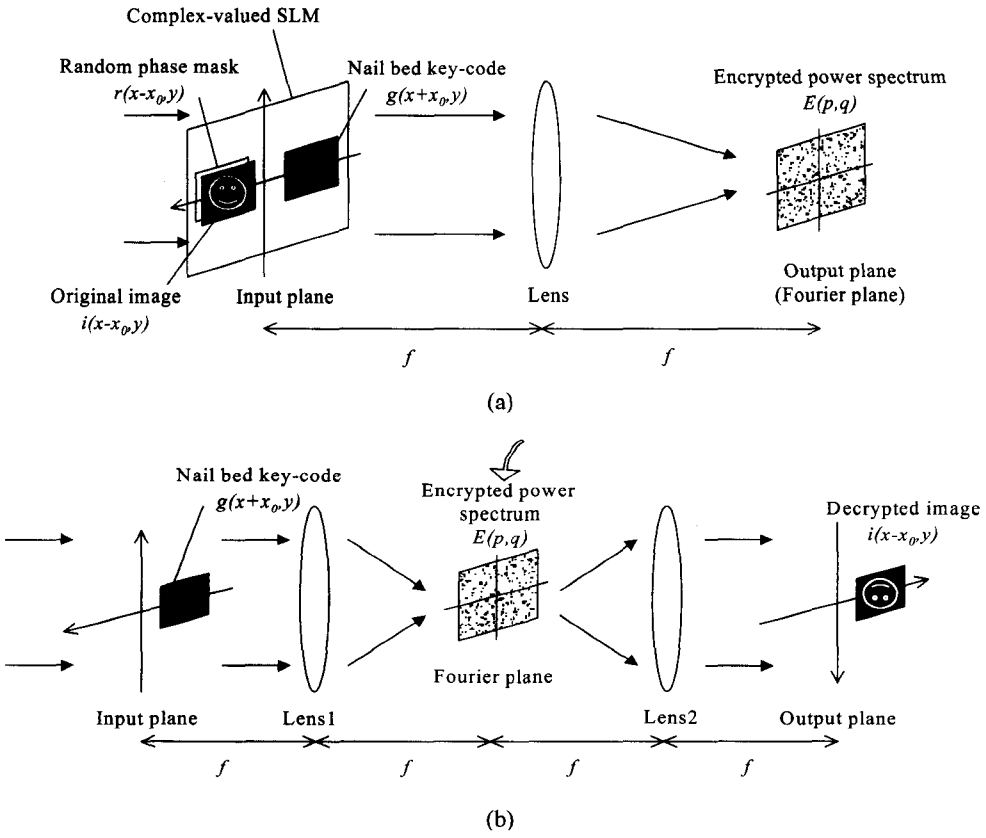


그림 3. (a) Optical encryption system and (b) decryption system.

$$+ G(p,q)\exp(j x_0 p)$$
$$+ [R(p,q)\otimes I(p,q)]^* G(p,q)G(p,q)\exp(j3 x_0 p)$$
$$+ [R(p,q)\otimes I(p,q)]\ G^*(p,q)G(p,q)\exp(-j x_0 p) \quad (13)$$

$D(p,q)$는 다시 두 번째 퓨리에 렌즈(lens-2)를 통해 역퓨리에 변환되어 출력 면에서 아래와 같은 빛의 분포를 갖는다.

$$d(x,y) = \mathfrak{I}^{-1}\{D(p,q)\}$$
$$= g(x,y)\otimes[r(x,y)i(x,y)]\odot[r(x,y)i(x,y)]\otimes\delta(x+x_0,y)$$
$$+ g(x,y)\otimes\delta(x+x_0,y)$$
$$+ g(x,y)\otimes g(x,y)\odot[r(x,y)i(x,y)]\otimes\delta(x+3x_0,y)$$
$$+ r(x,y)i(x,y)\otimes\delta(x-x_0,y) \quad (14)$$

위에서 $\mathfrak{I}^{-1}\{\cdot\}$는 역 퓨리에 변환 연산자를 나타내고, 역 퓨리에 변환은 주파수 영역 함수 $F(p,q)$에 대해서

$$\mathfrak{I}^{-1}\{F(p,q)\} = \frac{1}{4\pi^2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}F(p,q)\ e^{jpx+jqy}dxdy = f(x,y) \quad (15)$$

과 같이 정의되고 $\odot$는 함수 $f(x,y)$와 $h(x,y)$에 대해서

$$f(x,y)\odot h(x,y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}f(x',y')h(x+x',y+y')dx'dy' \quad (16)$$

과 같이 정의되는 correlation 연산자이다.[23] 위의 식 (14)는 출력 면에 모든 영상들이 결합 변환 상관기 구조의 이동불변(shift-invariance)특성[17,18]에 따라서 x축을 중심으로 각각, $+x_0 - x_0$, $-3x_0$의 지점에서 개별적으로 분리되어 나타남을 보여준다. $d(x,y)$는 출력 면에 배치된 제곱법칙 검출기에 의해서 intensity term으로 검출된다.

식 (14)의 $r(x,y)i(x,y)\otimes\delta(x-x_0,y)$에서는 오리지널영상인 $i(x,y)$가 랜덤 위상 마스크인 $r(x,y)$과 곱해져서 x축을 중심으로 $+x_0$지점에 나타남을 보여준다. 이때 제곱법칙 검출기에의해서 $r(x,y)$은 순수위상(phase-only)함수이기 때문에 $|r(x,y)|^2=1$이 되어 삭제되고, $i(x,y)$는 양의 실수(positive-real)값이기 때문에 복원된다. 이외에 원하지 않는 다른 intensity term들은 오리지널 영상과 분리되어 나타나며, 각각 x축을 중심으로 $-x_0$와 $-3x_0$ 지점에 백색 잡음(noise like)형태로 나타난다. 따라서 제곱법칙 검출기를 이용하여 $d(x,y)$를 검출함으로서 다른 영상잡음으로부터 방해받지 않고 오리지널 영상, $i(x,y)$를 복호할 수 있다.

암호화 과정에서는 조상 키-코드와 랜덤 위상 마스크를 이용하여 결합 변환 상관기 구조의 암호화 시스템을 통해 암호화된 파워 스펙트럼을 얻는다. 그리고 복호화 과정에서는 암호화된 파워 스펙트럼과 함께 암호화 과정에서 사용된 조상 키-코드를 그대로 사용하여 4f-system 구조의 복호화 시스템을 통해 복호화된 영상을 얻어낸다. 기존의 두 개의 랜덤 위상함수를 이용한 광 암호화 방법은 복호화 과정에서 키-코드의 정확한 복소공액을 요구한다. 그러나 결합 변환 상관기 구조를 이용한 광 암호화 방법은 암호화 및 복호화 과정에서 같은 키-코드를 이용하므로 키-코드의 복소공액을 요구하지 않는다.[19] 또한 암호화된 데이터가 복소 값을 기반으로 하는 4f-system 과는 다르게 결합 변환 상관기 구조를 이용한 광 암호화 방법은 암호화된 데이터가 결합 파워 스펙트럼으로 기록되어 제곱법칙 검출기인 CCD(charge-coupled device) 카메라와 같은 디지털 디바이스나 통신선로에 직접적으로 전송될 수 있다.[19,20]

2.4. 조상(nail bed) 위상-마스크(phase-mask)를 이용한 인증(authentication)

기존의 광 암호화 방법에서 사용된 임의의 랜덤 위상 함수를 이용한 키-코드는 제작과정에서부터 키-코드의 소유여부가 불투명하다. 만일 키-코드가 분실 혹은 고의적 양도에 의해서 다른 사람의 손에 들어가게 된다면 정보보안에 있어서 상당히 치명적이다. 이것은 암호화된 정보를 복호하려는 사람이 암호화된 정보의 제작자로부터 영상정보가 정확하게 전달되고 인수되었는지, 혹은 암호화된 정보의 제작자가 영상정보를 제작자 자신이나 전달받아야 하는 타인이 올바르게 소유하고 있는지를 알 방도가 없다. 이에 본 논문에서는 생체신호인 조상 위상 마스크를 correlation하여 개인을 구별함으로서 영상정보의 진위여부를 판별해내는 인증기법을 제안한다.

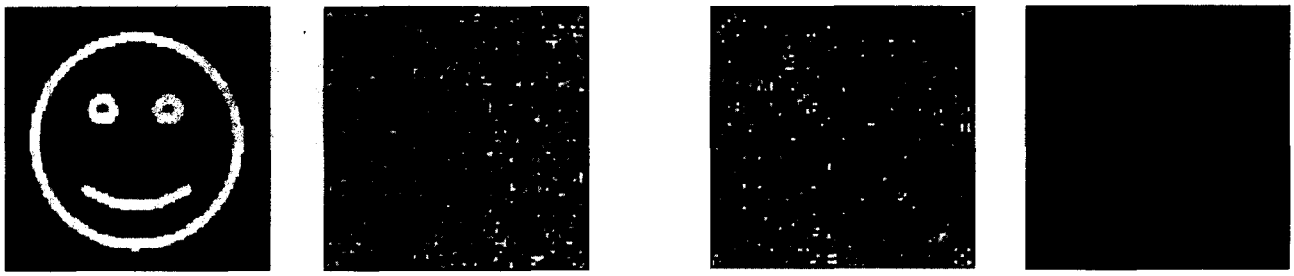
조상 키-코드, $g(x,y)$와 퓨리에 변환 관계를 갖는 조상 위상 마스크는 $G(p,q)$이다. 조상 위상 마스크, $G(p,q)$의 아래와 같이 정의된 correlation을 구하여 개인을 식별한다.

$$G_{n1}(p,q)\odot G_{n2}(p,q)$$
$$= \int\int G_{n1}(p',q')G_{n2}(p+p',q+q')dp'dq' \quad (17)$$

위에서 $G_{n1}(p,q)$과 $G_{n2}(p,q)$는 각각의 조상패턴을 이용한 조상 위상 마스크이다. 이때 $G_{n1}(p,q)$과 $G_{n2}(p,q)$가 각각 동일인의 조상 위상 마스크인 경우 correlation peak를 얻을 수 있으며 동일인이 아닌 조상 위상 마스크인 경우에는 correlation peak를 얻을 수 없다. 이렇게 개개인의 조상 위상 마스크를 correlation 하여 비교함으로서 암호화된 영상이 누구에 의해서 암호화되었는지에 대한 인증이 가능하다. 다시 말해 어떤 조상-키로 암호화된 문서가 복호되었을 때 복호에 쓰인 그 조상-키의 조상 위상 마스크와 A라는 사람의 조상을 추출해 합성한 조상-키의 조상 위상 마스크의 correlation 결과가 correlation peak를 출력한다면 이는 복호화된 영상이 A라는 사람에의 해서 암호화됐다는 사실을 증거하며 이를 통해 영상 제작자의 진위여부를 생체신호를 통해 인증한다. 이를 통해 정보화 사회에 있어 가장 중요한 문제의 하나인 정보제작자의 인증을 생체신호를 이용해 가능케 한다.

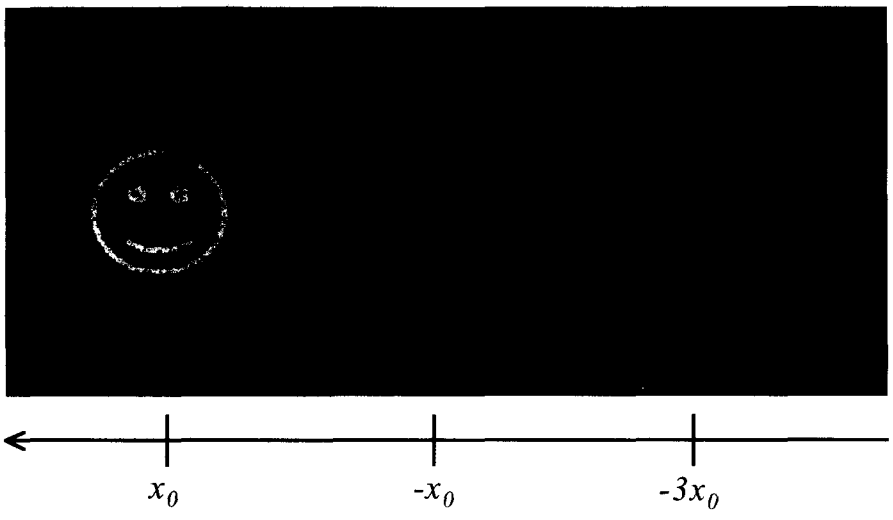
III. 컴퓨터 시뮬레이션

본 절에서는 실험을 통해 추출된 조상패턴을 암호 키로 이용하는 결합 변환 상관기 구조의 광 암호화 및 복호화 방법이 실제적으로 가능함을 보이기 위해 컴퓨터 시뮬레이션 한다. 그림 4(a)는 암호화될 오리지널 영상인 $i(x,y)$을 나타내며, 그림 4(b)는 독립된 순수 랜덤 위상 마스크인 $r(x,y)$, 그림 4(c)는 조상 키-코드인 $g(x,y)$를 나타낸다.

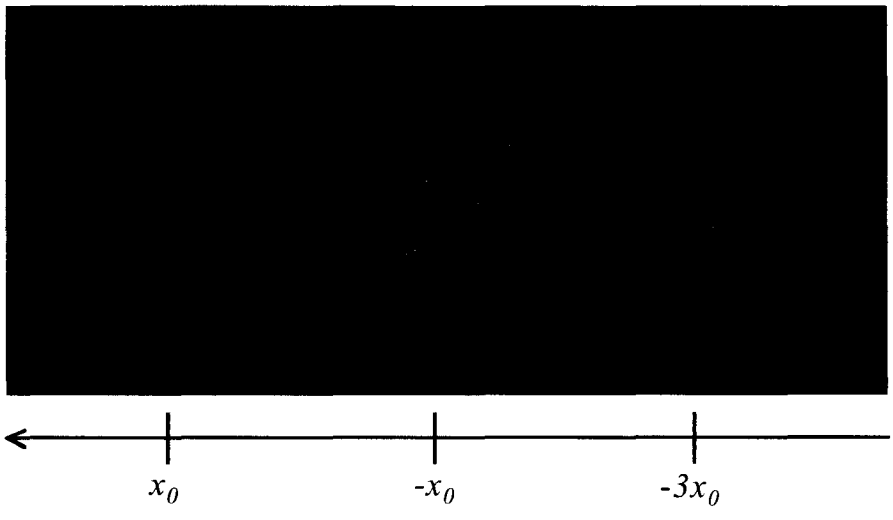


(a) (b) (c) (d)

그림 4. Images used proposed encryption technique: (a) original image, (b) random phase mask, (c) nail bed key-code, and (d) computer simulation result: encrypted power spectrum.



(a)



(b)

그림 5. Computer simulation result: reconstructed image (a) with correct nail bed key-code and (b) with incorrect nail bed key-code.

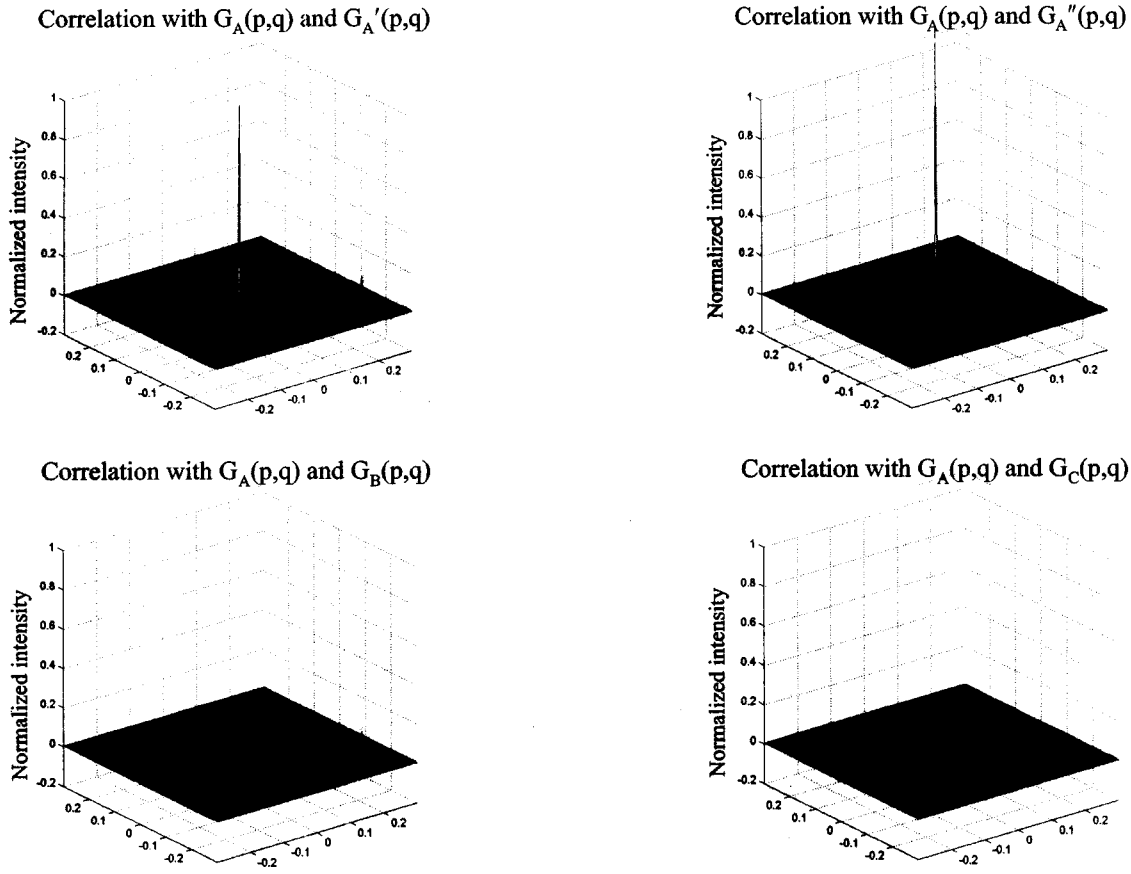


그림 6. Computer simulation result: correlation peak.

이들은 모두 앞 2.2절에서 정의된 바와 같으며 크기는 86 ×86 화소(pixels)로 한다. 이렇게 $i(x,y)$, $r(x,y)$, $g(x,y)$ 세 개의 마스크를 이용하여 제안된 방법으로 암호화하면 암호화된 파워 스펙트럼(encrypted power spectrum); $E(p,q)$가 그림 4(d)에서 보는 것과 같이 나타난다.

그림 5는 제안된 복호화 시스템에 의해 복호화된 영상이, 암호화 과정에서 배치된 위치와 대칭적으로 x축을 중심으로 각각 $+x_0$, $-x_0$, $-3x_0$의 지점에서 세 개의 term으로 나타남을 보여준다. 그림 5(a)는 정확한 조상 키-코드에 의해서 복호화된 영상이다. 즉, A라는 사람의 조상신호로 만든 조상 키-코드를 이용하여 암호화했을 때 정확히 A라는 사람의 조상 키-코드를 이용하여 복호화한 영상이다. 여기서는 같은 조상 키-코드를 이용함으로서 오리지널 영상 $i(x,y)$가 $+x_0$지점에 복원되고, 나머지 원하지 않는 영상들은 $-x_0$와 $-3x_0$지점에 백색 잡음 형태로 나타남을 보여준다. 반면 그림 5(b)는 정확하지 않는 키-코드, 다시 말해 A라는 사람의 조상 키-코드를 이용하여 암호화했을 때 A라는 사람이 아닌 다른 임의의(B 또는 C라는 사람의) 조상 키-코드를 이용하여 복호화한 결과이다. 여기서는 오리지널 영상이 복원되어야하는 $+x_0$지점까지도 백색 잡음 형태로 나타남을 볼 수 있다. 이 결과는 잘못된 조상 키-코드로는 영상정보의 복호가 불가능함을 보여준다. 위의 결과는 암호화된 정보를 제작한 조상 키-코드만이 정보의 복호를 가능하게 하여 타인으로부터 정보의 접근을 불가능하게 함을 알 수 있다.

그림 6은 각각의 조상 위상-마스크를 앞 2.4절의 식 (17)과 같이 정의된 correlation을 한 결과들이다. 그림 6에서 $G_A(p,q)$, $G_B(p,q)$, $G_C(p,q)$는 각각 다른 A, B, C의 세 사람의 조상패턴을 추출하여 만든 조상 위상 마스크이다. 그리고 $G_A'(p,q)$과 $G_A''(p,q)$은 개인을 비교하기 위해 A라는 사람의 조상을 각각 다른 시간간격으로 두 번째(A′)와 세 번째(A″) 추출한 조상 위상 마스크이다. 그림 6은 $G_A(p,q)$를 기준으로 하여 각각 $G_A'(p,q)$, $G_A''(p,q)$, $G_B(p,q)$, $G_C(p,q)$를 차례대로 correlation하여 나타낸 결과이다. 이 결과 $G_A(p,q)$와 $G_A'(p,q)$, $G_A(p,q)$와 $G_A''(p,q)$의 correlation은 correlation peak 값을 얻으며 그 최대값이 1에 가까운 반면에 $G_A(p,q)$와 $G_B(p,q)$, $G_A(p,q)$와 $G_C(p,q)$의 correlation은 correlation peak 값을 거의 얻을 수 없어 그 값이 0에 가깝다. 그러므로 그림 6에서와 같은 correlation peak 를 통해 A와 A′, A와 A″은 동일인의 조상 위상 마스크이고 A와 B, A와 C는 동일인의 조상 위상 마스크가 아님을 판별해 낼 수 있다. 이 결과는 조상 위상 마스크의 correlation을 통해 개인을 구별함으로서 영상정보의 진위여부를 가려내는 인증이

가능함을 보여준다.

IV. 결 론

조상의 생체-광학적 특성에 착안하여 콘포칼 광 스케닝 구조의 광학계를 제안하고, 제안된 콘포칼 구조의 광 스케닝 시스템을 이용 인간의 손톱을 스케닝해 조상패턴을 추출해 냈다. 추출된 조상패턴을 이용해 키-코드를 만들고, 만들어진 키-코드를 암호 키로 사용하는 결합 변환 상관기구조의 광 암호화 및 복호화 방법을 제안하였으며 컴퓨터 시뮬레이션을 통해 제안된 방법이 실제로 가능함을 보였다.

본 논문에서 제안하는 방법은 광학적인 방법으로 영상정보를 암호화하고 복호화하기 때문에 실시간 병렬처리가 가능하며 기존의 광 암호화 시스템에 대해서 다음과 같은 장점을 갖는다. 첫째, 조상의 생체-광학적 특성에 착안하여 생체신호인 조상패턴을 추출하여 암호 키-코드로 사용함으로서 기존의 정보보안 장치의 주된 단점인 암호 키의 분실 혹은 고의적 양도에 의한 부정사용을 방지함으로 높은 보안성을 갖는다. 둘째, 조상 위상 마스크를 correlation하여 개인을 구별해 냄으로서 제작자와 소유자의 판독을 가능하게 하는 암호 키의 투명성을 확보하게 된다.

감사의 글

본 논문은 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초연구지원사업의 연구결과입니다.

참고문헌

[1] R. W. Frischholz and U. Dieckmann, "BioID: a multimodal biometric identification system," *IEEE Computer*, vol. 33, no. 2, pp. 64-68, 2001.

[2] R. Adhami and P. Meenen, "Fingerprinting for security," *IEEE Potential*, vol. 20, no. 3, pp. 33-38, 2001.

[3] S. Liu and M. Silverman, "A practical guide to biometric security technology," *IT Professional*, vol. 3, no. 1, pp. 27-32, 2001.

[4] Sttephen S. Sternberg, eds, *Histology for Pathologists*, 2nd Edition, Chapter 3, pp. 47-68, Lippincott-Raven, Philadelphia, New York, 1997.

[5] M. J. C. Van Gemert et. al., "Skin Optics," *IEEE Transaction on Biomedical Engineering*, vol. 36, no. 12, pp. 1146-1154, 1989.

[6] W.-F. Cheong, S. A. Prahl, and A.J. Welch, "A review of the optical properties of biological tissues," *IEEE Journal of Quantum Electronics*, vol. 26, no. 12, pp. 2166-2185, 1990.

[7] T. R. Corle and G. S. Kino, *Confocal Scanning Optical Microscopy and Related Imaging Systems*, Academic Press, San Diego, 1996.

[8] 김태근, 김용우, 김해일, "손톱하부면 조상(nail bed)패턴의 콘포칼 광 스케닝 방법을 이용한 추출과 개인인증," 한국광학회지 제 13권 2호, 2002년 4월.

[9] B. Javidi and J. L. Horner, "Optical recognition for validation and security verification," *Opt. Eng.*, vol. 33, no. 6, pp. 1752-1756. 1994.

[10] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random phase encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767-769, 1995.

[11] B. Javidi et al., "Experimental demonstration of the random phase encoding technique for image encryption and security verification," *Opt. Eng.*, vol. 35, no. 7, pp. 2506, 1996.

[12] B. Javidi, "Processing for encryption and security systems," *Optics & Photonics News*, pp. 29-33, March 1997.

[13] B. Javidi, "Optical spatial filtering for image encryption and security systems," *SPIE*, vol. 3386, pp. 14-23, 1998.

[14] O. Matoba, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.*, vol. 24, no. 11, pp. 762-764, 1999.

[15] B. Javidi, L. Bernard, and N. Towghi, "Noise performance of double-phase encryption compared to XOR encryption," *Opt. Eng.*, vol. 38, no. 1, pp. 9-19, 1999.

[16] J-W Han et al., "Optical image encryption based on XOR operations," *Opt. Eng.*, vol. 38, no. 1, pp. 47-54, 1999.

[17] J. W. Goodman, *Introduction to Fourier optics*, 2nd edition, Chap 8, pp. 217-294, McGraw-Hill, New York, 1996.

[18] C. S. Weaver and J. W. Goodman, "Technique for optically convolving two functions," *Appl. Opt.*, vol. 5, pp. 1248-1249, 1966.

[19] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Opt. Eng.*, vol. 38, no. 8, pp. 2031-2035, 2000.

[20] S. J. Park, D.-H. Seo, J.-Y. Kim, J.-K. Bae, C.-S. Kim, and S.-J. kim, "Binary image encryption technique and decryption system using Joint Transform Correlator," *Proc. SPIE.*, vol. 4386, pp. 164-171, 2001.

[21] D. K. Linder, *Introduction to signals and systems*, International Editions, chap 19-20, pp. 723-808, McGraw-Hill, New York, 1999.

[22] B. Geoffrey and C.E. Sadik, eds, "SPATIAL LIGHT MODULATORS," *Opt. Soc. Am.*, TOPS vol. 14, Washington DC., 1997.

[23] P. P. Banerjee and T.-C. Poon, *Principles of Applied* Optics, Aksen, 1991.

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

Yong Woo Kim and Taegeun Kim†

Department of Optical Engineering, Sejong University
98 Kunja-Dong, Kwangjin-Ku, Seoul, Korea 143-747
† E-mail: takim@sejong.ac.kr

(Received June 9, 2003, Revised manuscript March 18, 2004)

In this paper, we proposed an optical encryption and decryption technique that uses a nail bed pattern as a key-code. Since the technique uses a nail bed pattern that is a biometric signal of an encryptor, the technique is robust about a fake key or illegal use of a key. In addition to this, the encrypted image contains the biometric information of the encryptor. This makes the proposed technique also be applied to authentication.

OCIS Codes: 070.4550, 070.5010, 170.1790, 070.6020.