ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 23-02-05
j.inst.Korean.electr.electron.eng.Vol.27,No.2,159~164,June 2023
https://doi.org/10.7471/ikeee.2023.27.2.159
33

위상천이 디지털 간섭계를 이용한 암호화된 지문 정합 필터 기반의 인증 기법

Authentication method based on an encrypted finger print matched filter using phase-shifting digital interferometry

전 석 희*, 길 상 근**★

Seok-Hee Jeon*, Sang-Keun Gil**★

Abstract

A novel authentication method based on a matched filter using digital interferometry is proposed in which a matched filter set of complex holograms is constructed by encrypting a user's personal information QR code with a finger print as a private key. Authentication is accomplished by decrypting the user's QR code with the finger print. The proposed method has feasibility to confirm that mean square error of auto-correlation is 5.55% which is 13.7 times less than that of cross-correlation output, 76.17%, and it can provide high secure authentication system for finger print hacking due to the storage of the encrypted personal finger prints in the database.

요 약

본 논문은 디지털 간섭계를 이용한 정합 필터 기반의 새로운 인증 기법을 제안한다. 제안한 인증 시스템에서 광학적 위상 천이 간섭계 기법을 적용하여 QR code로 변환된 사용자들의 개인 정보를 사용자 지문 개인키로 암호화함으로써 복소 홀로그램 형태의 정합 필터를 구성한다. 사용자의 인증은 사용자의 지문 개인키를 통한 사용자의 QR code를 복호화하고 확인함으로써 이루어진다. 제안한 방법은 자기 상관 출력 평균제곱오차(MSE)가 약 5.55%로 상호 상관 MSE 76.17%보다 약 13.7배 적게 나와 인증에 타당함을 확인하였고, 데이터 베이스에서 개인 지문의 정보가 암호화 형태로 저장되므로 기존의 인증 방법에서의 지문 정보 해킹에 대하여 강한 인증시스템을 제공할 수 있다.

Key words : Authentication, Optical encryption, Digital interferometry, Fourier optics, Security.

Ⅰ. 서론

정보통신 시스템에서 네트워크 서버에 접근하기 위해서는 개인의 ID와 비밀번호(password)를 사용하여 인증을 얻은 후 네트워크에 접속하도록 하고 있다. 이러한 방법은 디지털 암호화를 통하여 수행되는데 여전히 해킹을 통하여 개인 정보가 누출될 수 있다. 최근에는 이러한 문제점을 해결하기 위하여 1990년대 초부터 다양한 광학적 방법을 이용한 정보의 암호화[1] 및 지문 등 생체 정보를 이용한 인증 기법[2]이 소개되고 있다. 또한 홀로그

* Dept. of Electronics Engineering, Incheon National University
** Dept. of Electronics Engineering, The University of Suwon
★ Corresponding author
E-mail : skgil@suwon.ac.kr, Tel : +82-31-220-2664
※ Acknowledgment
This work was supported by Incheon National University Research Grant in 2022.
Manuscript received May. 21, 2023; revised Jun. 11, 2023; accepted Jun. 18, 2023
This is an Open-Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http : //creativecommons.org/licenses/by-nc/3.0) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

래픽 광 간섭계를 기반으로 하는 정보 영상 암호화 방법 등도 제안되었다[3][4]. 인증 시스템에서 보다 안전하게 개인을 인증하기 위해서는 ID와 비밀번호 등과 같은 개인 정보를 개인키(private key)를 사용하여 암호화하면 해킹의 위험을 감소시킬 수 있다. 하지만 이러한 개인키의 암호화도 디지털 암호화 시스템에서는 결코 안전할 수 없다. 한편 광학적 정합 필터를 이용한 코히어런트(coherent) 광 상관기의 연구는 Vander Lugt의 정합 필터 설계[5] 이후 위상 정합 필터를 이용한 광 상관기[6] 등 많은 연구자들에 의해 발전해 왔다. 따라서 본 논문에서는 위상 천이 디지털 홀로그래픽 간섭계(phase-shifting digital interferometry)를 이용하여 개인 정보를 내포하는 QR code를 개인 지문의 비밀키로 암호화한 디지털 홀로그램으로서의 정합 필터를 구성하고, 이것의 상관 함수(correlation function)를 이용한 새로운 인증 방법을 제안하면서 간단한 사례를 통하여 그 성능을 보여준다.

II. 본론

1. 정합 필터 이론

광학적 정합 필터는 2-차원 공간적으로 정의된 선형 공간-불변(linear space-invariant) 필터로, 만약 시스템의 충격 응답 함수(impulse response function)가 $h(x, y)=s^*(-x, -y)$으로 주어지면 어떤 특별한 입력 신호 함수 $s(x, y)$에 정합되었다고 정의되고 자기 상관 함수(auto-correlation function)로 인식된다[5]. 여기서 * 는 공액(conjugate)을 의미한다. 만약 입력 함수 $g(x, y)$가 $s(x,y)$에 정합된 필터에 가해지면 출력 함수 $v(x, y)$는 다음과 같이 계산되며

$$v(x,y)=\iint_{-\infty}^{\infty} g(u,v)s^*(u-x,v-y)dudv \tag{1}$$

이 함수는 두 함수 $g(x, y)$와 $s(x, y)$의 상호 상관 함수(cross-correlation function)로 인식된다. 만약 n명 사용자의 각기 다른 정합 필터가 n개 있는 시스템에서 어떤 특별한 사용자 k의 입력 함수가 $g(u, v)=s_k(u, v)$이면, 정확한 정합 필터의 출력 함수는

$$|v_k|^2=\frac{\left|\iint_{-\infty}^{\infty}|s_k|^2dudv\right|^2}{\iint_{-\infty}^{\infty}|s_k|^2dudv}=\iint_{-\infty}^{\infty}|s_k|^2dudv \tag{2}$$

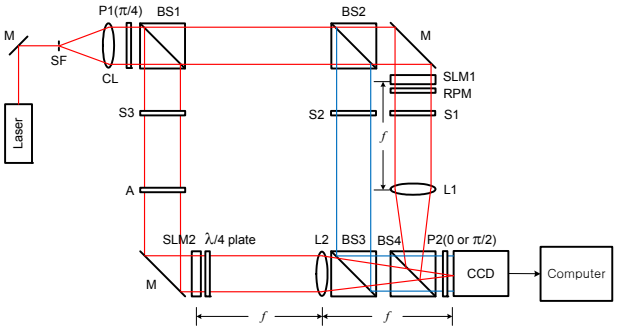
으로 주어지고, 반면에 다른 사용자 n의 입력 함수가 틀리게 정합된 필터의 출력 함수는

$$|v_n|^2=\frac{\left|\iint_{-\infty}^{\infty}s_ks_n^*dudv\right|^2}{\iint_{-\infty}^{\infty}|s_n|^2dudv} \tag{3}$$

으로 주어진다. 이때 자기 상관 함수의 출력이 최대치를 나타내며 상호 상관 함수 출력보다 항상 $|v_n|^2 \le |v_k|^2$의 관계를 가진다.

2. 디지털 간섭계를 이용한 정합 필터 및 인증

본 논문에서 제안하는 정합 필터 기반의 인증 기법은 그림 1이 보여주는 위상 천이 디지털 간섭계 원리를 적용하여 디지털 홀로그램의 정합 필터를 만들고 이를 생체 지문 개인키를 통하여 상관 함수의 패턴 결과로 인증을 하는 방식이다. 이때 디지털 홀로그램은 푸리에 변환 홀로그램으로 구현되는데 통상적으로 푸리에 홀로그램을 구현하는데 있어서 빛은 푸리에 변환 함수의 특성에 의해 선형 공간-불변 시스템을 통하여 전파된다. 먼저 각 사용자의 개인 정보(ID와 비밀번호 등)를 사용자 지문의 비밀키로 암호화함으로써 정합 필터를 구성하는 과정을 설명한다. 참고로 2-단계 위상 천이 간섭계를 이용하여 디지털 홀로그램을 생성하는 과정은 참고문헌 [7]에 기술되어 있다.



SF: Spatial filter, CL: collimating lens, P: polarizer, BS: beam splitter, S: shutter, A: attenuator, M: mirror, L: lens, SLM: spatial light modulator, RPM: random phase mask

Fig. 1. Phase-shifting digital interferometry.
그림 1. 위상천이 디지털 간섭계

그림 1에서 보듯이 레이저 광원의 평면파는 서로 다른 방향으로 물체파와 참조파로 나뉜다. 여기서 SLM1은 암호화하는 사용자 개인 정보의 QR code를 표시하고 SLM2는 사용자의 개인키 지문을 표시한다. 만약 사용자 k의 QR code 함수를 $Q_k(x, y)$, 개인키 지문 함수를

$F_k(x, y)$라 하면, 참조파 입력 함수는 $r_k(x, y)=Q_k(x, y)\exp[jq(x, y)]$으로 물체파 입력 함수는 $s_k(x, y)=\exp[j\pi F_k(x, y)]$으로 표현한다. 여기서 $q(x, y)$는 [0, 2π] 사이에서 무작위로 발생한 값을 가지는 2차원 배열 함수로 $\exp[jq(x, y)]$는 무작위 위상 마스크(RPM) 함수를 나타낸다. 따라서 참조파와 물체파의 CCD 면에서입력 함수의 푸리에 변환된 함수 분포는 다음과 같다.

$$R_k(u,v)=\iint_{-\infty}^{\infty} r_k(x,y)\exp\left[-j\frac{2\pi}{\lambda f}(ux+vy)\right]dxdy \quad (4)$$
$$=|R_k(u,v)|\exp\left[j\phi_{R_k}(u,v)\right]$$

$$S_k(u,v)=\iint_{-\infty}^{\infty} s_k(x,y)\exp\left[-j\frac{2\pi}{\lambda f}(ux+vy)\right]dxdy \quad (5)$$
$$=|S_k(u,v)|\exp\left[j\phi_{S_k}(u,v)\right]$$

광학 시스템에서 $\lambda/4$ plate에 의한 위상 천이는 p/2이므로 두 파동의 2-단계 위상 천이 간섭에 의한 CCD 면에서의 간섭 세기 분포 함수는

$$I(u,v;0)=|R_k(u,v)+S_k(u,v;0)|^2 \quad (6)$$
$$=|R_k|^2+|S_k|^2+2|R_k||S_k|\cos\Delta\phi_k$$

$$I(u,v;\pi/2)=|R_k(u,v)+S_k(u,v;\pi/2)|^2 \quad (7)$$
$$=|R_k|^2+|S_k|^2+2|R_k||S_k|\sin\Delta\phi_k$$

이고, 여기서 $\Delta\phi_k(u,v)=\phi_{S_k}(u,v)-\phi_{R_k}(u,v)$으로 물체파와 참조파의 위상차를 나타낸다. CCD에 기록된 간섭 세기 (6)식과 (7)식에서 상수항 $|R_k|^2$과 $|S_k|^2$을 제거한 나머지 세기 분포 함수 $I_1(u, v; 0)$과 $I_2(u, v; p/2)$로부터 복소 디지털 홀로그램 함수를 다음 식과 같이 계산하여 얻을 수 있고 이는 사용자 k의 정합 필터 함수이다.

$$H_k(u,v)=A_k\exp[j\Delta\phi_k] \quad (8)$$

여기서 진폭 $A_k(u, v)$와 위상차 $\Delta\varphi_k(u, v)$는 다음과 같이 계산된다.

$$A_k(u,v)=|R_k||S_k| \quad (9)$$
$$=\sqrt{\{I_1(u,v;0)\}^2+\{I_2(u,v;\pi/2)\}^2}$$

$$\Delta\phi_k(u,v)=\phi_{S_k}(u,v)-\phi_{R_k}(u,v) \quad (10)$$
$$=\tan^{-1}\left[\frac{I_2(u,v;\pi/2)}{I_1(u,v;0)}\right]$$

이제 사용자 k의 개인키 지문 함수 $F_k(x, y)$를 통해서 복호화 키에 해당하는 복소 디지털 홀로그램을 생성하고 이를 정합 필터에 적용하여 사용자 인증을 하는 과정을 설명한다. 그림 1에서 BS2에 의해서 아래로 진행하는 광파가 크기가 일정한 평행광이면 참조파 입력 함수는 $r_k(x, y)=R_k(u, v)=1$로 표현된다. 만약 사용자 k의 개인키 지문 함수 $F_k(x, y)$가 물체파 입력 함수로 사용되면 $s_k(x, y)=\exp[j\pi F_k(x, y)]$로 표현되고 CCD 면에서의 함수 분포는 (5)식과 동일하다. 이때 CCD 면에서의 2-단계 위상 천이 간섭에 의한 간섭 세기 분포 함수는

$$I(u,v;0)=|1+S_k(u,v;0)|^2 \quad (11)$$
$$=1+|S_k|^2+2|S_k|\cos\Delta\psi_k$$

$$I(u,v;\pi/2)=|1+S_k(u,v;\pi/2)|^2 \quad (12)$$
$$=1+|S_k|^2+2|S_k|\sin\Delta\psi_k$$

이고, 여기서 $\Delta\psi_k(u,v)=\phi_{S_k}(u,v)$이다. 정합 필터 함수를 만들 때와 마찬가지로 (11)식과 (12)식에서 상수항을 제거한 두 세기 분포 함수 I_1과 I_2로부터 정합에 필요한 복소 디지털 홀로그램 함수를 다음 식과 같이 얻을 수 있고 이는 사용자 k의 인증을 위한 입력 함수이다.

$$G_k(u,v)=B_k\exp[j\Delta\psi_k]=|S_k|\exp[\phi_{S_k}] \quad (13)$$

만약 이 함수가 사용자들의 정합 필터들에 입력되어 사용자 k의 필터 함수와 정합되면 자기 상관은 다른 사용자의 상호 상관보다 큰 값을 나타내게 되어 사용자 k의 인증을 보장한다. 정합 과정은 다음과 같은 관계식으로 표현된다.

$$D_k(u,v)=\frac{H_k^*(u,v)G_k(u,v)}{|S_k(u,v)|^2} \quad (14)$$
$$=\frac{|R_k||S_k|\exp[\phi_{R_k}-\phi_{S_k}]|S_k|\exp[\phi_{S_k}]}{|S_k(u,v)|^2}$$
$$=|R_k|\exp[\phi_{R_k}]=R_k(u,v)$$

정합 과정을 통해 얻어진 (14)식의 출력 결과는 (4)식과 같고 이를 역푸리에 변환하면 사용자 k의 $r_k(x, y)=Q_k(x, y)\exp[jq(x, y)]$ 함수로 사용자 k의 QR code $Q_k(x, y)$가 근사화되어 복호화된다.

$$d_k(x,y)=F^{-1}\{D_k(u,v)\}=|r_k(x,y)|=\widetilde{Q}_k(x,y) \quad (15)$$

3. 제안한 방법에 대한 성능 분석

본 논문에서 제안한 디지털 간섭계를 이용한 정합 필터 기반의 인증 시스템에 대해서 성능과 타당성을 검증한다. 예시적으로 정합 필터를 구성하는 사용자 수를 6명으로 가정하였고, 정합 및 인증을 위한 입력 함수로 사용된 QR code와 사용자 지문 영상의 데이터 크기, 무작위 위상 마스크 크기는 256×256 화소의 2차원 배열을 사용하였다.

그림 2는 정합 필터를 생성할 때 6명 사용자들의 개인 정보(이름, ID, 비밀번호 등)를 나타내고, 그림 3은 그 내용을 포함하는 QR code로 변환된 데이터 영상 함수 $Q_k(x, y)$를 보여준다. 한편 그림 4는 정합 필터인 디지털 홀로그램을 생성할 때 개인 정보 QR code를 암호화하고 정합을 통한 인증을 수행하기 위해서 필요한 개인키에 해당하는 사용자 지문의 영상 함수 $F_k(x, y)$를 보여준다. 획득한 지문은 회전, 이동 및 크기 조정에 대하여 영상처리를 통하여 보정된 지문으로 가정한다.

(4)식과 (5)식으로 표현되는 참조파 함수와 물체파 함수는 CCD 면에서 간섭을 발생시키는데 이때 2-단계 위상 천이 간섭 기법을 적용하면 그 간섭 패턴의 세기 분포 함수가 (6)식과 (7)식의 함수로 표현되며 이를 이용한 사용자의 정합 필터 함수는 (8)~(10)식과 같이 복소 디지털 홀로그램 함수로 표현된다. 그림 5는 각 사용자가 각자의 비밀키함수에 의해 생성된 정합 필터의 위상 지도 함수 $\Delta\varphi_k(u, v)$ 함수를 보여준다.

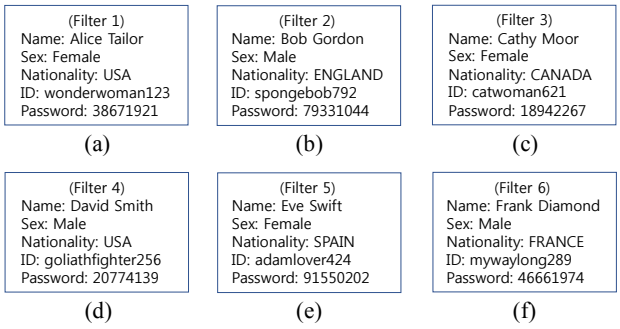


Fig. 2. (a)~(f) users' personal information.
그림 2. (a)~(f) 사용자 개인 정보.

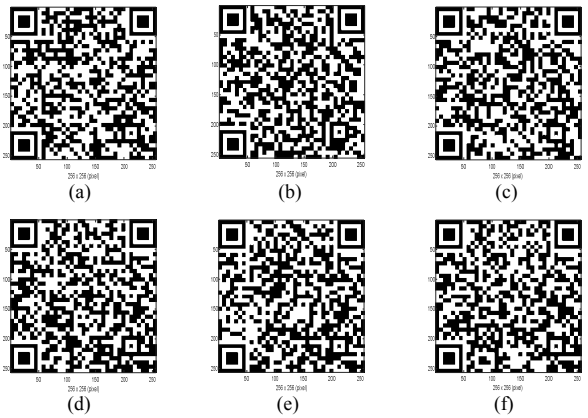


Fig. 3. (a)~(f) QR code of users' personal information.
그림 3. (a)~(f) 사용자 개인 정보의 QR code.

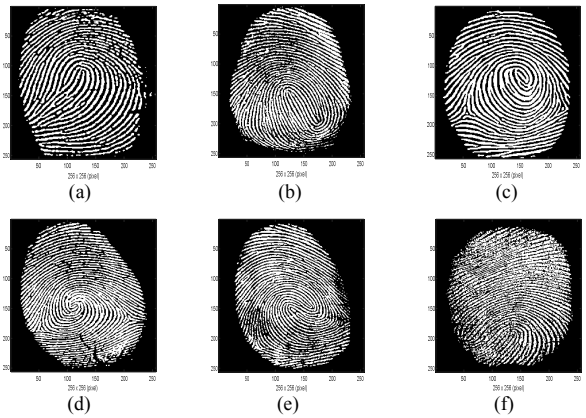


Fig. 4. (a)~(f) users' finger print as a private key.
그림 4. (a)~(f) 비밀키로 사용되는 사용자 개인 지문.

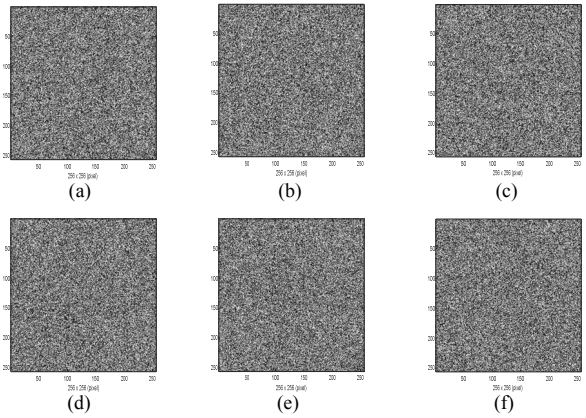


Fig. 5. (a)~(f) Phase map of users' matched filter.
그림 5. (a)~(f) 사용자들의 정합 필터에 대한 위상 지도.

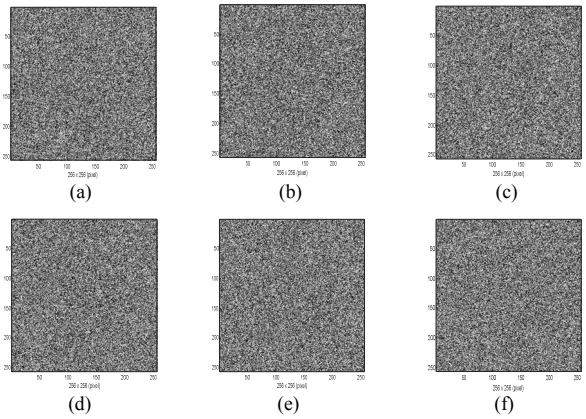


Fig. 6 (a)~(f) Phase map of users' finger print private key.
그림 6. (a)~(f) 사용자들의 지문 개인키 입력 함수에 대한 위상 지도

이제 사용자 지문 함수 $F_k(x, y)$의 물체파 함수와 평면광의 참조파 함수를 가지고 2-단계 위상 천이 간섭 기법을 적용하여 CCD 면에 생성된 간섭 세기 분포 함수는 (11)식과 (12)식의 함수로 표현된다. 이 두 식으로부터 사용자 인증을 위한 입력 함수는 (13)식과 같이 복소 디지털 홀로그램 함수로 주어진다. 그림 6은 각 사용자의 지문 정보에 의한 비밀키 함수에 의해 생성된 입력 함수들의 위상 지도 함수 $y_k(u, v)$ 함수를 보여준다.

만약 그림 6(c)로 주어지는 사용자 3의 입력 함수가 그림 5(c)의 사용자 3의 정합 필터에 입력되면 (14)식에 의해 자기 상관 함수의 출력을 나타내고, (15)식에 의해 역푸리 변환하면 그림 7(a)의 출력 결과를 보여준다. 그림 7(b)는 2차원적 영상이다. 그림에서 보듯이 복호화된 출력 패턴은 원래의 사용자 3의 QR code 영상과는 약간의 오차를 보여주는데 이는 디지털 간섭계를 이용하여 CCD에 256 gray-level로 기록되어서 복호화시 화소에서의 오차가 발생하기 때문이다. 그림 7(c)는 자기 상관 함수의 출력에 적절한 문턱값(threshold)을 설정하여 이진화(0 또는 1)한 데이터로 그림 3(c)와 같은 원래의 사용자 3의 QR code 영상을 보여주고 이를 decoding하면 그림 2(c) 사용자 3의 개인 정보를 얻어 인증을 확인할 수 있다. 한편, 그림 6(a)로 주어지는 사용자 1의 입력 함수가 그림 5(c)의 사용자 3의 정합 필터에 입력되면 (14)식에 의해 상호 상관 함수의 출력을 나타내고, (15)식에 의해 역푸리 변환하면 그림 7(d)와 7(e)의 출력 결과를 보여준다. 그림 7(f)는 마찬가지로 자기 상관 함수의 출력에 사용한 같은 문턱값에 의해 이진화한 데이터로 그림에서 보듯이 출력 패턴은 사용자 정보를 알 수 있는 QR code 영상을 보여주지 못한다.

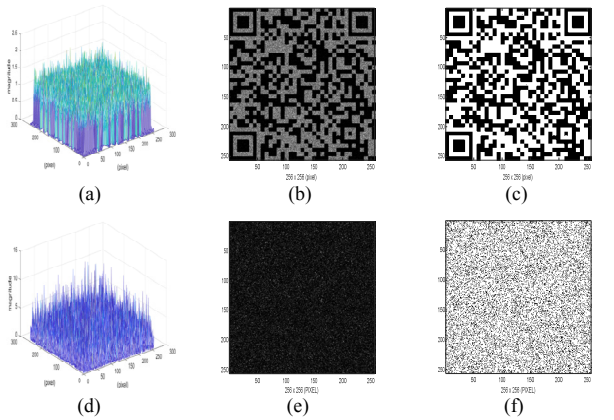


Fig. 7. (a)~(c) Auto-correlation function output of user 3, (d)~(f) Cross-correlation function output between user 3 and user 1.

그림 7. (a)~(c) 사용자 3의 자기 상관 함수 출력, (d)~(f) 사용자 3과 사용자 1의 상호 상관 함수 출력

제안한 정합 필터 기반의 자기 상관과 상호 상관의 출력 결과에 대한 신뢰성을 분석하기 위해 (15)식의 복호화된 결과 함수의 평균 제곱 오차(MSE : Mean Square Error)를 분석하였다. 원래의 영상 함수와 복원된 영상 함수와의 MSE는

$$MSE = \frac{\sum_{x,y=1}^{256} |d_k(x,y) - Q_k(x,y)|^2}{\sum_{x,y=1}^{256} |s_k(x,y)|^2} \times 100\% \qquad (16)$$

으로 계산되고, 여기서 $d_k(x,y)$는 (15)식으로 얻어지는 복호화된 상관 함수이고 $Q_k(x,y)$는 사용자의 원래 QR code 함수이다. 표 1에서 알 수 있듯이 자기 상관 출력에 대한 MSE는 약 5.55% 이고 상호 상관 출력에 대한 MSE는 약 76.17% 이므로 정합시 상관 출력 오차가 비정합시 상호 상관 오차보다 약 13.7배 큼을 알 수 있으므로 정합 필터를 통한 개인 인증이 가능함을 확인할 수 있다. 또한 제안한 방법은 데이터 베이스에서 인증에 필요한 지문 및 개인 정보가 암호화되어 있어 서버의 지문 정보 해킹에 강한 보안 시스템을 제공할 수 있다.

Table 1. MSE of correlation function outputs.

표 1. 상관 함수 출력에 대한 MSE (단위 : %)

Input \ Matched filter	H_1^*	H_2^*	H_3^*	H_4^*	H_5^*	H_6^*
G_1	5.31	70.63	73.86	75.62	76.73	79.87
G_2	71.54	5.73	76.32	77.65	75.09	78.35
G_3	73.45	77.29	5.43	76.28	74.55	76.37
G_4	75.48	77.29	76.54	5.38	77.12	77.53
G_5	76.52	74.89	74.73	75.05	5.49	78.03
G_6	78.64	78.29	76.03	77.21	78.15	5.98

Ⅲ. 결론

본 논문에서는 디지털 간섭계를 이용한 정합 필터 기반의 새로운 인증 기법을 제안한다. 정합 필터는 위상 천이 간섭계 기법을 적용하여 사용자들의 개인 정보를 사용자들의 지문 개인키로 암호화함으로써 복소 홀로그램 형태로 구성한다. 인증은 사용자의 지문 개인키를 입력으로 하여 정합 여부에 따라 출력 상관 함수의 오차 크기 비교에 의해 결정한다. 제안한 방법에 의하면 자기 상관 출력 오차가 상호 상관 오차보다 약 13.7배 적은 큰

차이를 보이므로 인증 판단에 적합하며, 또한 개인 인증에 필요한 지문 및 ID와 비밀정보 등이 암호화되어 저장되어서 기존의 디지털 인증 방법에 비해 데이터 베이스에서의 개인 정보의 해킹에 강한 인증시스템을 제공할 수 있다.

References

[1] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Phot.*, vol.6, pp.120-155, 2014.
DOI: 10.1364/AOP.6.000120
[2] B. Javidi and A. Sergent, "Fully phase encoded key and biometrics for security verification," *Opt. Eng.* vol.36, no.3, pp.935-942, 1997.
DOI: 10.1117/1.601259
[3] Y. Zhang and B. Wang, "Optical image encryption based on interference," *Opt. Lett.*, vol.33, no.21, pp.2443-2445, 2008. DOI: 10.1364/OL.33.002443
[4] S. H. Jeon and S. K. Gil, "QPSK modulation based optical image cryptosystem using phase-shifting digital holography," *J. Opt. Soc. Korea*, Vol.14, pp.97-103, 2010.
DOI: 10.3807/JOSK.2010.14.2.097
[5] A. Vander Lugt, "Signal Detection by complex spatial filtering," *IEEE Trans. Info. Theory* IT-10, no.2, pp.139-145, 1964.
DOI: 10.1109/TIT.1964.1053650
[6] J. Horner and P. Gianino, "Phase-only matched filtering," *Appl. Opt.* vol.23, no.6, pp.812-816, 1984. DOI: 10.1364/AO.23.000812
[7] S. K. Gil, "2-step quadrature phase-shifting digital holographic optical encryption using orthogonal polarization and error analysis," *J. Opt. Soc. Korea,* vol.16, pp.354-364, 2012.

BIOGRAPHY

Seok-Hee Jeon (Member)

1981 : BS degree in Electronic Engineering, Yonsei University.
1983 : MS degree in Electronic Engineering, Yonsei University.
1990 : PhD degree in Electronic Engineering, Yonsei University.
2001~2002 : Visiting Scholar in UC Santa Barbara.
1991~present : Professor in Electronic Eng. Incheon National University.

Sang-Keun Gil (Member)

1984 : BS degree in Electronic Engineering, Yonsei University.
1986 : MS degree in Electronic Engineering, Yonsei University.
1992 : PhD degree in Electronic Engineering, Yonsei University.
1993~1998 : Senior researcher in Advanced Technology Institute.
1998~present : Professor in Electronic Eng. The University of Suwon.