*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.233

# 지문 영상 복원 기반의 스마트 기기 지문 스머지 공격 연구*

이 호 연,† 권 태 경‡
연세대학교 정보보호연구실

# Fingerprint Smudge Attacks Based on Fingerprint Image Reconstruction on Smart Devices*

Hoyeon Lee,† Taekyoung Kwon‡
Information Security Lab, Graduate School of Information, Yonsei University

요 약

지문 인증은 개인의 고유한 지문 특징 정보를 바탕으로 사용자를 식별하기 때문에 유출이나 분실, 망각의 위험이 없으며 편리하고 안전하여 여러 스마트 기기에 적용되고 있다. 하지만 스마트 기기를 사용한 후 남아있는 지문의 흔적은 스머지 공격에 취약하다. 본 논문에서는 사용자의 스마트 기기 사용 패턴을 분석하고 스마트 기기에 남아있는 지문 스머지를 이용하여 손상된 지문 영상을 복원하는 기법을 제안한다. 스마트 기기 사용 시 빈번하게 보이는 행동 패턴으로 구성된 시나리오에서 지문 스머지를 수집 및 복원하였으며 복원 지문 영상을 이용한 스머지 공격의 유효성에 대하여 실험하였다. 실험 결과, 지문 인증 시스템에서 높은 공격 성공률을 보였으며 스머지 공격에 취약함을 실증적으로 검증하였다.

ABSTRACT

Fingerprint authentication identifies individuals based on user specific information. It is widely used as it is convenient, secure and has no risk of leakage, loss, or forgotten. However, the latent fingerprints remaining on the smart device's surface are vulnerable to smudge attacks. We analyze the usage patterns of individuals using smart device and propose methods to reconstruct damaged fingerprint images using fingerprint smudges. We examine the feasibility of smudge attacks with frequent usage situations by reconstructing fingerprint smudges collected from touch screens. Finally, we empirically verify the vulnerability of fingerprint authentication systems by showing high attack rates.

**Keywords:** Smart Device, Fingerprint Authentication, Fingerprint Reconstruction, Smudge Attacks

## I. 서 론

최근 스마트폰, 태블릿 PC와 같은 터치스크린 패널이 탑재된 스마트 기기를 위한 주요 인증 매커니즘으로 생체 인증 기술이 활용되고 있다. 생체 인증 기술은 개인의 고유한 생체 정보를 이용하여 사용자를 인증하는 것으로, PIN(Personal Identification Number) 또는 패스워드와 같은 기존 인증 방식에

Received(03. 13. 2017), Modified(04. 06. 2017), Accepted(04. 07. 2017)
* 본 논문은 2017년도 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2012-0-00646). 또한 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2015R1A2A2A01004792)
† 주저자, yeoni_2@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

비해서 타인에 의한 유출 및 도용 가능성이 현저히 적다. 생체 인증 기술 중 하나인 지문 인증은 지문 인식 센서를 통해 입력받은 지문 영상 내에 존재하는 특징점(minutiae) 정보를 추출하고 이를 지문 템플릿(template)의 특징점과 정합(matching)을 수행함으로써 사용자를 인증한다[1]. 이는 다른 인증 기술에 비해서 높은 안전성과 사용성을 제공하기 때문에 특히 많이 활용되고 있다[2].

사용자가 스마트 기기를 사용하는 동안 여러 유형의 터치 활동이 일어나고 기기 표면에 터치의 흔적, 즉 지문 자국이 남게 되는데 이를 스머지(smudges 또는 oily residues)라 한다(Fig.1.). 기기 표면에 남아있는 스머지는 터치가 일어난 위치 뿐만 아니라 어떤 손가락으로 터치했는지 추측할 수 있도록 하며, 이를 통해 사용자의 민감 정보를 추출하는 것을 스머지 공격(Smudge Attacks)이라 한다. 2010년 Aviv는 안드로이드 패턴 락 시스템에 대한 스머지 공격을 처음으로 제안하였으며, 스머지는 단순 터치로 인해 끊임없이 발생하고 잘 지워지지 않아 카메라와 같은 장비를 통해 수집 및 분석이 용이하기 때문에 스머지 공격의 위험성은 모든 스마트 기기에서 존재한다고 언급하였다[3].

본 논문에서는 지문 인식 센서를 탑재한 스마트폰 표면에 남아있는 지문 스머지를 카메라로 수집하고 이를 이용하여 손상된 지문 영상을 복원하는 기법을 제안한다. 또한 복원이 완료된 지문 영상을 지문 템플릿과 정합을 수행함으로써 스머지 공격의 유효성을 실험하고, 지문 인증 시스템의 안전성을 실증적으로 검증한다.

본 연구의 주요 사항은 다음과 같다.

- 스마트 기기 사용 시 나타나는 여러 행동 패턴으로 구성된 시나리오에서 실제 지문 스머지 수집 및 손상 영역 복원

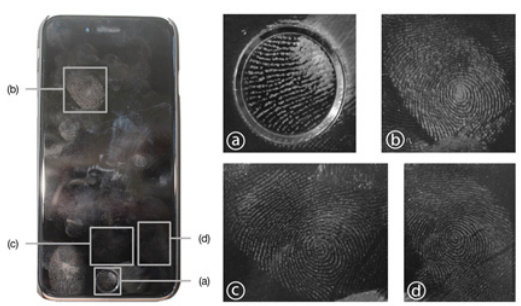



Fig. 1. Fingerprints smudges on iPhone 6

- AFIS(Automated Fingerprint Identification System)를 이용한 지문 유사도 측정 및 결과 비교 분석

## II. 관련 연구

지문 영상의 정확한 특징점 정보 추출 및 인증을 위한 연구에는 지문 영상의 개선(enhancement), 복원(reconstruction) 등이 있다[4,5,6,7].

Hong 등은 가보 필터(gabor filter)를 이용하여 잡음(noise)을 제거하고 융선 구조를 선명히 보존하여 지문 영상으로부터 정확한 특징점 정보를 추출하였다. 또한, 지문 영상 간 특징점 정합의 정확도를 향상시켰다[4].

Chikkerur 등은 비정상적 신호 분석에 사용되는 STFT(Short Time Fourier Transform) 분석을 이용하여 품질이 낮은 지문 영상을 강화하는 기법을 제안하였으며 기존 강화 기법보다 개선된 성능을 보였다[5].

Feng 등은 지문 구조에 내재된 사전 정보를 이용하는 orientation field estimation 알고리즘을 제안하였다. STFT 분석을 사용한 [5]를 포함하여 기존 연구보다 지문 인식률이 더 높게 측정됨을 보였다[6].

Cappelli 등은 지문 표준 템플릿(ISO/IEC 19794-2)으로부터 orientation field 및 융선 구조를 추출하고 지문 이미지를 복원하는 기법을 제안하였다. 여러 지문 인식 알고리즘이 복원 지문을 이용한 위장 공격(masquerade attack)에 취약함을 보였다[7].

스머지 공격에 대한 연구는 2010년 Aviv에 의해 처음 등장하였다. Aviv 등은 안드로이드 패턴 락 시스템에서 구체적인 실험을 통해 처음으로 스머지 공격의 가능성을 보였다. 터치스크린 패널에 남은 스머지가 선명하게 노출될 수 있는 촬영 환경(카메라와 조명의 각도, 방향)을 조사하였으며, 터치스크린과 카메라 렌즈 사이의 각도가 60°일 때 스머지가 가장 선명히 노출됨을 보였다. 또한 단순 터치, 어플리케이션 사용, 와이핑(wiping), 스마트폰을 주머니에 넣는 등 실제 스마트폰 사용 후 패턴이 입력되더라도 스머지를 통한 비밀 패턴 추측이 가능함을 보였다[3].

한편 Andriotis 등은 이미지 전처리 알고리즘과 기계 학습(machine learning) 기반의 스머지 공격을 제안하였지만, 구체적인 실험 방법과 공격을 통

한 패턴 추측 결과에 대해서는 언급하지 않았다[8].

Zhang 등은 터치스크린 패널이 탑재된 디바이스에 입력된 패스워드를 추측하는 스머지 공격을 제안하였다. 지문 분말(fingerprint powder)을 이용하여 터치스크린에 남은 지문 스머지를 추출하고 이미지 전처리(image preprocessing) 과정을 거친 뒤 이를 가상 키패드와 매핑(mapping)하여 실제 입력된 패스워드를 추측하는데 성공하였다[9].

본 연구에서는 선행 연구에서 제안한 지문 영상의 이미지 전처리 및 스머지 수집 기법을 이용하여 수집한 지문 스머지의 손상된 영역을 복원하고 이를 이용한 스머지 공격을 새롭게 제안한다.

## III. 지문 영상 복원 기반의 스머지 공격

본 연구에서는 터치스크린에 남아있는 지문 스머지를 활용하여 지문 인식 센서에 남아있는 지문 스머지의 손상된 부분을 복원한다. 또한 이를 지문 템플릿과 정합하여 지문 스머지 공격의 유효성을 실험한다. 센서 위에 남은 지문 스머지는 실제 지문 인증에 활용되었을 가능성이 높기 때문에 이를 기준으로 지문 영상을 복원한다.

본 논문에서 제안하는 지문 영상 복원을 이용한 스머지 공격 절차는 Fig.2.와 같으며 크게 지문 스머지 수집(fingerprint smudge collection), 이미지 전처리(image preprocessing), 손상 식별(damage identification), 손상 복원(damage correction)의 4단계로 구성된다.

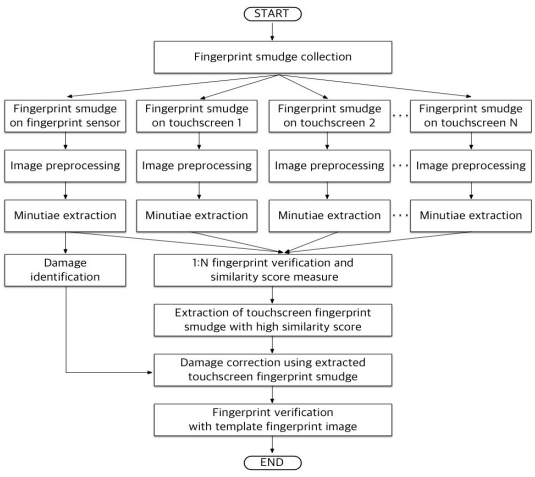



Fig. 2. Fingerprint image reconstruction based smudge attack procedure

### 3.1 지문 스머지 수집

스마트 기기에 남은 지문 스머지가 선명히 노출될 수 있도록 터치스크린과 카메라 렌즈 사이의 각도는 60°로 설정하였으며, 거리는 Aviv의 연구보다 10cm 가까운 15cm로 설정하였다[3]. 실험에는 Canon EOS 700D 카메라(EFS 18-55mm F3.5-5.6 IS STM lens) 및 ARRI 650W Thungsten Light를 사용하여 스머지 영상을 수집하였다.

### 3.2 이미지 전처리

이미지 전처리는 지문 영상의 잡음을 제거하고 융선 구조를 명확히 하여 품질을 향상시키고 지문 영상으로부터 적합한 특징점 정보를 추출할 수 있도록 한다. 실험에는 대표적인 지문 영상 전처리 알고리즘인 히스토그램 평활화(histogram equalization), 가보 필터(gabor filter), 세선화(thinning)를 사용하였다.

히스토그램 평활화는 지문 영상의 어두운 부분은 밝게, 밝은 부분은 어둡게 하여 명암 값의 분포를 균일하게 한다[10]. 실험에는 대비 제한 적응 히스토그램 평활화(CLAHE, Contrast Limited Adaptive Histogram Equalization)를 사용한다. 이는 일정 크기의 블록 단위로 발생 빈도에 대해 상한을 설정하여 기존의 히스토그램 평활화보다 개선된 성능을 보인다[11].

가보 필터는 지문 영상의 잡음을 줄인 후에 융선의 방향과 주파수를 정확히 추출하여 융선 구조를 효과적으로 보존한다[12].

전처리의 마지막 단계인 세선화는 지문 융선을 한 픽셀 두께의 융선으로 만들어 지문 영상의 골격(skeleton)을 추출한다[13].

### 3.3 손상 식별

센서 위에 남아있는 지문 스머지의 영상에서 손상된 범위를 식별하는 단계이며, 본 연구에서는 SIFT (Scale-Invariant Feature Transform) 알고리즘을 사용하였다. SIFT 알고리즘은 크기와 방향에 무관하게 이미지에서 특징점(keypoint)을 추출하는 알고리즘으로 물체 인식에 많이 사용된다[14,15].

이점에 착안하여 SIFT 알고리즘을 지문 스머지

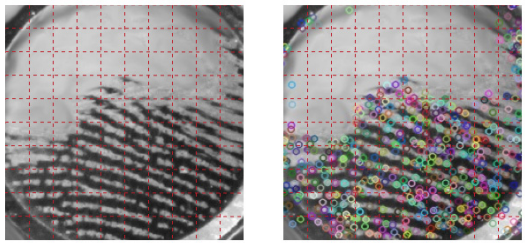



Fig. 3. Damage identification (a) divided by 25×25 pixel image blocks (b) keypoints (represnted as color dots) extracted by SIFT algorithm

영상에 적용할 경우 영상 내에 존재하는 윤선의 코너(corner)를 인식하여 이를 특징점으로 추출한다. 실험에서는 영상 내의 손상된 범위를 탐색하기 위하여 SIFT 알고리즘을 사용한 후 Fig.3.와 같이 250×250 pixel 이미지를 10×10의 25×25 pixel 이미지 블록으로 나누었다. 그리고 블록 별로 추출된 특징점의 개수를 저장한 뒤 평균 개수 보다 적은 수의 특징점을 포함하는 이미지 블록을 손상 부분으로 식별하였다.

### 3.4 손상 복원

지문 영상 복원의 마지막 단계인 손상 복원 단계에서는 특징점 정보 기반의 지문 인식 시스템인 SourceAFIS[16]를 활용하여 센서에 남은 지문 스머지와 터치스크린에 남은 지문 스머지 영상간 1:N 특징점 정보 비교 후 유사도 점수(similarity score)를 측정한다. 그 중 센서에 남은 지문 스머지와 가장 높은 유사도 점수를 가지는 터치스크린 스머지 영상을 추출하고 이를 이용하여 센서에 남은 지문 스머지의 손상 부분을 대치함으로써 손상 영역을 복원한다.

손상 영역 복원을 위하여 세선화 이미지를 대상으로 SIFT descriptor 기반 Brute-Force matching을 수행하고 복원 기준점을 설정한다(Fig.4.). 이 때 센서 및 터치스크린에 남은 지문 스머지 영상에서 추출되는 각각의 descriptor간 거리(distance)가 낮은 matches를 복원 기준점으로 활용한다[17]. 실험에는 최대 5회까지 지문 인증을 시도할 수 있는 iPhone의 Touch ID를 대상으로 공격하기 때문에 거리가 가장 낮은 5개의 matches를 고려한다[18].

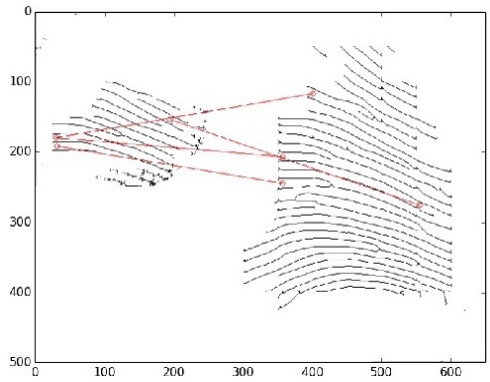



Fig. 4. Brute-Force matching with SIFT descriptors for establishment of reconstruction basis

## IV. 실험 및 결과

주요 인증 매커니즘으로 지문 인증을 활용하는 스마트 기기에 대한 스머지 공격 가능성을 분석하기 위하여 본 연구에서는 Touch ID를 탑재한 iPhone 6를 대상으로 실험한다.

### 4.1 실험 설계

지문 복원을 이용한 스머지 공격의 유효성을 실증적으로 검증하기 위하여 실제 사용자가 스마트 기기를 사용할 때 빈번하게 보이는 행동 패턴을 바탕으로 다음과 같은 시나리오를 구성하였다.

- Tapping: 스크롤 사용이 없는 단순 터치
- Passcode-typing: 터치스크린의 가상 키패드를 사용하여 패스워드 입력
- Text-typing: 터치스크린의 가상 키보드를 사용하여 텍스트 입력
- Application: Facebook 어플리케이션 사용
- Wiping: 터치스크린을 닦아냄
- In-pocket: 스마트폰을 주머니에 넣음

모든 참가자들은 iPhone 6를 사용하여 6가지 시나리오를 수행하였으며, 각 시나리오 별로 Touch ID 및 터치스크린에 남은 지문 스머지들을 수집하였다. 촬영 환경은 3.1과 같다.

또한 실제 지문 인증과 같이 직접 수집한 지문 및 복원 지문을 지문 템플릿과 비교하기 위하여 참가자로부터 고품질의 지문을 추가로 수집하였으며 이를 템플릿으로 활용하였다.

#### 4.1.1 실험 환경

실험에는 C# 기반의 SourceAFIS를 바탕으로 지문 영상 간 특징점 정보 비교 및 유사도 점수를 측정하였다. 이는 ISO 테스트 기준 1.17% EER(Equal Error Rate), 0.01% FAR(False Acceptance Rate), 2.5% FRR(False Rejection Rate)의 높은 정확도를 가진다. 또한 지문 템플릿의 국제 표준(ISO/IEC 19794-2) 형식을 지원한다[15].

### 4.2 실험 결과

약 4개월에 걸쳐 Touch ID 사용 경험이 있는 iPhone 사용자 총 6명(남자 3명, 여자 3명, 오른손잡이)이 실험에 참여하였고 36개의 사용자 케이스를 촬영하였다.

#### 4.2.1 지문 스머지 수집 결과

총 36개의 사용자 케이스로부터 358개(Touch ID 위에 남은 지문 스머지 36개, 터치스크린에 남은 지문 스머지 322)의 지문 스머지 영상을 수집하였다. 스머지 수집 결과 Wiping, In-pocket을 제외한 시나리오에서 평균 10개 이상의 스머지 영상을 수집할 수 있었다(Table 1.).

Tapping은 공격자가 스머지를 수집하기 가장 이상적인 시나리오로서 지문 스머지의 손상이나 변형을 일으키는 와이핑(wiping) 및 접촉이 없었다. 모든 참가자로부터 복원에 활용 가능한 고품질의 스머지를 수집할 수 있었다.

Passcode-typing에서는 터치스크린에 나타나는 원형 모양의 가상 키패드를 이용하여 숫자코드를 입력했다. 참가자들은 숫자코드를 입력할 때 비교적 강하게 터치하여 원형의 가상 키패드와 유사한 크기의 지문 스머지를 남겼다.

Text-typing에서 참가자들이 가상 키보드를 이용하여 텍스트를 입력할 때 가벼운 터치가 특정 위치(키보드 위)에 한하여 빈번하게 일어나는 것을 확인하였다. 때문에 많은 지문 스머지를 수집할 수 있었지만 대부분 크기가 작고 서로 겹쳐져 있어 복원에 활용하기 어려웠다.

Application에서는 터치스크린 패널을 손가락으로 밀어내는 확대/축소(zooming), 스크롤(scroll)이 타 시나리오에 비해 상대적으로 많이 발생하여 대부분의 지문 스머지에 손상이나 변형이 존재하였다.

Table 1. Number of fingerprint smudges collected from touchscreen per scenario

| Scenario | Mean | Max | Min |
|---|---|---|---|
| Tapping | 11.2 | 14 | 10 |
| Passcode-typing | 11.8 | 19 | 8 |
| Text-typing | 10.3 | 16 | 7 |
| Application | 10 | 12 | 7 |
| Wiping | 4.2 | 9 | 0 |
| In-pocket | 6.2 | 9 | 1 |

Wiping에서는 참가자들의 평소 Wiping 습관(엄지 손가락으로 닦는 경우, 옷 소매를 이용하여 닦는 경우 등)에 따라 터치스크린에 남은 지문 스머지의 개수가 상이했다.

또한 In-pocket에서는 iPhone이 주머니에 완전히 들어가지 않아 밖으로 노출된 부분이 존재할 경우 지문 스머지가 지워지지 않음을 확인하였다.

이는 실제 스마트 기기 사용 시 지문 스머지가 자연스럽게 손상되거나 지워질 수 있지만 스머지 공격으로부터 안전하지 않음을 보여준다.

#### 4.2.2 지문 영상 복원을 이용한 지문 스머지 공격 결과

본 논문에서는 지문 스머지 공격의 유효성을 실증적으로 보이기 위하여 앞서 구성한 시나리오에서 스머지를 수집하고 이를 이용하여 손상 영역을 복원하였다(Fig.2.). 또한, 복원 이전 지문 영상(손상 지문 영상) 및 이를 복원한 지문 영상을 미리 저장한 지문 템플릿 영상과 비교하고 유사도 점수를 측정하였다.

측정 결과, 모든 시나리오에서 복원 지문과 템플릿 영상 간의 유사도 점수가 손상 지문과 템플릿 영상 간의 유사도 점수보다 높은 사용자 케이스를 발견하였다. 다음 Fig.5.는 SourceAFIS에서 손상-템플릿 지문 영상 간 유사도 점수보다 복원-템플릿 지문 영상 간 유사도 점수가 높은 사용자 케이스의 비율을 보여준다. 모든 시나리오에서 평균 35%의 비율을 보였으며, Tapping에서는 88%로 가장 높았다.

이는 지문 영상 복원을 이용한 스머지 공격으로 손상된 지문 영상의 품질을 개선하고 정상적인 사용자의 지문 템플릿과 유사한 지문 영상을 만드는 것이 가능함을 의미한다.

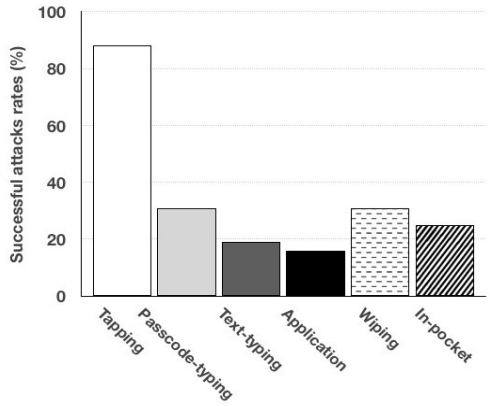



Fig. 5. Successful attacks rates per scenario

## V. 결 론

본 논문에서는 스마트 기기의 터치스크린에 남은 지문 스머지를 이용하여 센서에 남은 지문 스머지 영상의 손상된 부분을 복원하고 지문 인식 시스템에서 스머지 공격의 가능성을 분석하였다.

사용자가 스마트 기기를 사용할 때 빈번하게 보이는 행동 패턴을 바탕으로 지문 스머지를 수집한 결과, 지문 스머지의 손상 영역 복원에 이용 가능한 고품질의 지문 스머지를 수집할 수 있었다. 또한 대부분의 사용자는 지문 인증을 시도할 때 사용하는 손가락과 스마트 기기 사용을 위하여 터치스크린 입력 시 사용하는 손가락이 같기 때문에 동일한 손가락의 지문 스머지를 수집할 가능성이 높다[19].

수집한 지문 스머지를 이용하여 손상 영역을 복원하였으며 모든 시나리오에서 복원 지문 영상이 복원 이전의 지문 영상보다 유사도 점수가 높은 사용자 케이스가 존재함을 보였다. 이를 통해 지문 영상 복원을 이용한 스머지 공격에 매우 취약하다는 것을 검증할 수 있었다.

실험에서는 연구 편의성을 위해 온라인 지문 인식 시스템을 이용하여 정합을 수행하였지만 이는 지양해야 한다. 보다 신뢰성 있는 연구 결과를 위해 실리콘이나 젤라틴으로 만들어진 복원 지문 영상을 스마트 기기에 탑재된 지문 인식 센서에 인증을 시도하고 안전성을 면밀히 분석해야 한다.

## References

[1] A. Jain, L. Hong and R. Bolle, "On-Line Fingerprint Verification," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 4, pp. 302-313, Apr. 1997.

[2] A. Goode, "Bring your own finger-how mobile is bringing biometrics to consumers," Biometric Technology Today, vol. 2014, no. 5, pp. 5-9, May. 2014.

[3] A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J.M. Smith, "Smudge Attacks on Smartphone Touch Screens," In Proc. of the 4th USENIX Conference on Offensive Technologies (WOOT'10), pp. 1-7, Aug. 2010.

[4] L. Hong, Y. Wan and A.K. Jain, "Fingerprint Image Enhancement: Alogrithm and Performance Evaluation," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, pp. 777-789, Sept. 1998.

[5] S. Chikkerur, A.N. Cartwright and V. Govindaraju "Fingerprint enhancement using STFT analysis," Pattern Recognition, vol. 40, no. 1, pp. 198-211, Jan. 2007.

[6] J. Feng, J. Zhou and A. K. Jain, "Orientation Field Estimation for Latent Fingerprint Enhancement,", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 4, pp. 925-940, Apr. 2013.

[7] R. Cappelli, D. Maio and A. Lumini, "Fingerprint Image Reconstruction from Standard Templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 9, Sept. 2007.

[8] P. Andriotis, T. Tryfonas and Z. Yu, "POSTER: Breaking the Android Pattern Lock Screen with Neural Networks and Smudge Attacks," In Proc. of the sixth ACM conference on Security and privacy in wireless and mobile networks (WiSec'14), Jul. 2014,

[9] Y. Zhang, P. Xia, J. Luo, Z. Ling, B. Liu and X. Fu, "Fingerprint Attack against Touch-enabled Devices," In Proc. of the second ACM workshop on Security and privacy in smartphones and mobile devices, pp. 57-68, Oct. 2012.

[10] S. Greenberg, M. Aladjem, D. Kogan and I. Dimitrov, "Fingerprint Image Enhancement Using Filtering Techniques," In Proc. of the 15th International Conference on Pattern Recognition, pp. 3-7, Sept. 2000.

[11] K. Zuiderveld, "Contrast Limited Adaptive Histogram Equalization," Graphics Gems IV, Academic Press Professional, Inc., pp.474-485, 1994.

[12] L. Hong, A. Jain, "Fingerprint Image Enhancement," Automatic Fingerprint Recognition Systems, pp. 127-143, 2004.

[13] R. Thai, "Fingerprint Image Enhancement and Minutiae Extraction," Ph. D. Thesis, School of Computer Science and Software Engineering, The University of Western Australia, 2003.

[14] D.G. Lowe, "Object Recognition from Local Scale-Invariant Features," In Proc. of the Seventh IEEE International Conference on Computer Vision, vol. 2, pp. 1150-1157, Sept. 1999.

[15] D.G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," International Journal of Computer Vision, vol. 60, no. 2, pp. 91-110, Nov. 2004.

[16] R. Važan, "SourceAFIS," http://www.sourceafis.org/blog/.

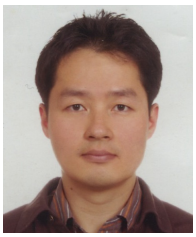
[17] "OpenCV" https://opencv-python-tutroals.readthedocs.io/en/latest/py_tutorials/py_feature2d/py_matcher/py_matcher.html#matcher.

[18] Apple Inc, "About Touch ID security on iPhone and iPad," https://support.apple.com/en-us/HT204587.

[19] Anonymous Authors, Full paper in preparation.

## 〈저자소개〉

이 호 연 (Hoyeon Lee) 학생회원
2016년 2월: 전북대학교 컴퓨터공학 학사
2016년 3월~현재: 연세대학교 정보대학원 석사과정
〈관심분야〉 스마트폰 보안, Authentication, Usable Security, HCI 등



권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년 Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호 프로토콜, 네트워크 프로토콜, 사물인터넷 보안, Usable Security, HCI 등