Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.2, Apr. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.2.369

거리기반 키스트로크 다이나믹스 스마트폰 인증과 임계값 공식 모델*

이 신 철,[1†] 황 정 연,[2] 이 현 구,[1] 김 동 인,[1] 이 성 훈,[3] 신 지 선[1‡]
[1]세종대학교, [2]한국전자통신연구원, [3]과학기술연합대학원대학교

Distance-Based Keystroke Dynamics Smartphone Authentication and Threshold Formula Model*

Shincheol Lee,[1†] Jung Yeon Hwang,[2] Hyungu Lee,[1]
Dong In Kim,[1] Sung-Hoon Lee,[3] Ji Sun Shin[1‡]
[1]Sejong University,
[2]Electronics and Telecommunications Research Institute,
[3]University of Science & Technology

요 약

비밀번호 입력 또는 잠금 패턴을 이용한 사용자 인증은 스마트폰의 사용자 인증 방식으로 널리 사용되고 있다. 하지만 엿보기 공격 등에 취약하고 복잡도가 낮아 보안성이 낮다. 이러한 문제점을 보완하기 위해 키스트로크 다이나믹스를 인증에 적용하여 복합 인증을 하는 방식이 등장하였고 이에 대한 연구가 진행되어 왔다. 하지만, 많은 연구들이 분류기 학습에 있어서 비정상 사용자의 데이터를 함께 사용하고 있다. 키스트로크 다이나믹스를 실제 적용 시에는 정상 사용자의 데이터만을 학습에 사용할 수 있는 것이 현실적이고, 타인의 데이터를 비정상 사용자 학습 데이터로 사용하는 것은 인증 자료 유출 및 프라이버시 침해 등의 문제가 발생할 수 있다. 이에 대한 대응으로, 본 논문에서는 거리기반 분류기 사용에 있어서, 분류 시 필요한 임계값의 최적 비율을 실험을 통해 구하고, 이를 밝힘으로써 실제 적용에서 정상 사용자 자료만을 이용하여 학습하고, 이 결과에 최적 비율을 적용하여 사용할 수 있도록 공헌하고자 한다.

ABSTRACT

User authentication using PIN input or lock pattern is widely used as a user authentication method of smartphones. However, it is vulnerable to shoulder surfing attacks and because of low complexity of PIN and lock pattern, it has low security. To complement these problems, keystroke dynamics have been used as an authentication method for complex authentication and researches on this have been in progress. However, many studies have used imposter data in classifier training and validation. When keystroke dynamics authentications are actually applied in reality, it is realistic to use only legitimate user data for training, and using other people's data as imposter training data may result in problems such as leakage of authentication data and invasion of privacy. In response, in this paper, we experiment and obtain the optimal ratio of the thresholds for distance based classification. By suggesting the optimal ratio, we try to contribute to the real applications of keystroke authentications.

Keywords: Keystroke Dynamics, Distance-based classifications, Smartphone Authentication

Received(12. 28. 2017), Modified(01. 30. 2018), Accepted(01. 30. 2018)

* 본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2015-0-00168, 상황인지기반 멀티팩터 인증 및 전자서명을 제공하는 범용인증플랫폼기술 개발).

† 주저자, shincheol90@gmail.com
‡ 교신저자, jsshin@sejong.ac.kr(Corresponding author)

I. 서 론

스마트폰의 급속한 성장으로 인해 기존의 데스크톱에서의 작업들이 모바일 장치로 옮겨 가고 있다. 이에 따라, 일상생활 속에서 스마트폰을 통해 다양한 서비스를 제공받고 사용하는 반면에 사용자의 프라이버시(privacy)를 보호하기 위한 보안 조치는 정체되어 있는 상태이다[1, 2]. 현재 사용되고 있는 스마트폰 인증 방법으로 PIN(Personal Identification Number) 입력, 잠금 패턴이 가장 많이 사용되고 있으며 최근에는 지문 인식 또는 생체 데이터를 이용한 생체기반 인증도 많이 사용되고 있다[3, 4, 5]. 사용자 인증 수행 시 엿보기 공격으로 인해 PIN과 패턴이 유출될 수 있는 전자의 인증 방법보다 생체기반 인증은 더 안전하지만 지문 인식 등 생체 인증 과정에서 반복적인 인식 실패를 대비하여 PIN 입력 또는 잠금 패턴과 같은 백업 인증 방법을 대체(backup) 인증 방식으로 제공하고 있다. 결국, 이러한 경우에는 스마트폰 인증의 보안성이 PIN 입력이나 잠근 패턴 인증의 보안성으로 귀결되게 된다.

한편, 키스트로크 다이나믹스(keystroke dynamics)는 사용자의 입력 속도, 터치 사이즈 등 사용자의 입력 패턴을 비교하여 인증하는 방식으로 PIN 또는 잠금 패턴과 복합(multi-factor) 인증으로 결합함에 따라 사용자 인증을 더 강화할 수 있다[6]. 또한, 생체 인증과 비교하였을 때, 생체 데이터를 사용할 때 스마트폰이 생체 데이터를 안전하게 보호해야 한다는 중요한 문제점이 야기된다. 하지만 키스트로크 다이나믹스는 PIN 또는 잠금 패턴 변함에 따라 변경되기 때문에 키스트로크 다이나믹스를 인증 요소로 사용하게 되면 위험 요소가 줄어들게 된다. 이러한 키스트로크 다이나믹스를 인증으로 사용하기 위하여 다양한 연구가 진행되어왔다.

1.1 관련 연구

[Fig. 1]은 키스트로크 다이나믹스 연구의 흐름을 요약한 그림이다. 1975년부터 키스트로크 다이나믹스 연구가 시작되었고, 2008년까지는 PC 키보드 기반의 연구가 활발히 진행되었다. 2002년부터 2009년까지는 모바일폰의 키스트로크 다이나믹스 연구가 진행되었으며 이후 스마트폰의 발전으로 인해 2010년부터 현재까지 꾸준히 스마트폰의 키스트로크 다이나믹스 연구가 진행되어 오고 있다. 초기에는 스마트폰의 시간 특징과 터치 압력 특징만을 사용하였지만 이후 안드로이드(Android) 버전이 업그레이드 됨에 따라 터치 압력과 모션 데이터 특징, 터치스크린 정보와 목소리 특징을 이용한 연구가 계속해서 진행되고 있다. 또한, 2015년부터는 스마트폰뿐만 아니라 태블릿을 이용한 키스트로크 다이나믹스 연구가 진행되어오고 있다.

키스트로크 다이나믹스의 특징정보로는 R. Spillane가 처음으로 시간 특징과 터치 압력 특징을 제안하고 사용하였다[8]. 이후, D. Umphress와 G. Williams는 컴퓨터 키보드를 이용한 키스트로크 다이나믹스 실험에서 평균 latency 특징과 연속된 두 키를 누를 때 걸리는 평균 시간을 이용하여 정상 사용자의 reference profile을 만듦으로써 여러 사용자로부터 정상 사용자를 구분하도록 했다[9]. 평균 latency 특징은 문자를 입력할 때 문자들 사이의 평균 시간 간격을 의미하며, 이 연구에서는 11.7%의 FAR(False Acceptance Rate)와 5.8%의 FRR(False Rejection Rate) 실험 결과를 얻었다. 또한, J. Kim, H. Kim, 그리고 P. Kang은 영어뿐만 아니라 한글을 자유로운 문자열 형태로 입력받아 실험하였다. 5개의 시간 특징을 사용하여 실험한 이 연구는 한글의 경우 6.49%의 평균 EER(Equal Error Rate), 영어의 경우 6.69%의 평균 EER을 보였다[10].

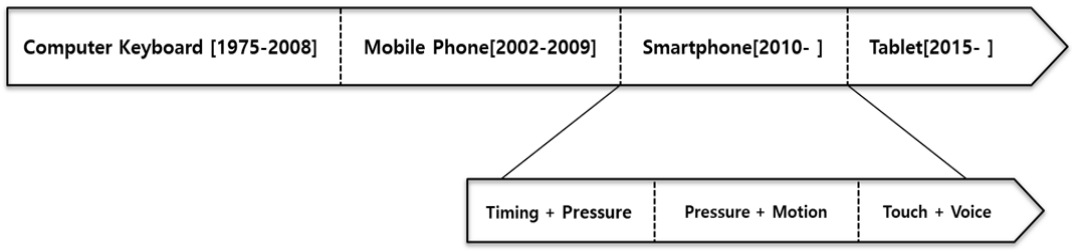


Fig. 1. The evolution of touch dynamics biometrics research[7]

모바일 통신 기술의 급속한 발전으로 인해 모바일 플랫폼의 사용자 인증에 키스트로크 다이나믹스 개념을 적용하기 위한 노력이 증가하기 시작했다[11]. [Table 1]은 모바일 플랫폼 환경에서의 키스트로크 다이나믹스 연구들을 요약한 내용으로 해당 연구의 실험 방법 및 실험 결과를 보여준다. 2002년, 모바일 장치에서의 키스트로크 다이나믹스 연구가 처음 제안되었다[12, 13, 14]. N.L. Clarke와 S. M. Furnell은 30명의 참가자에게 전화번호와 문자 메시지를 입력받은 후, latency 특징과 hold-time 특징을 이용하여 모바일 사용자를 확인하는 실험을 한 결과 4자리 PIN은 8.5%의 EER, 11자리 PIN은 4.9%의 EER 결과를 얻었다[14]. 이 연구에 사용된 latency 특징은 연속적인 문자열에 대해 첫 번째 키를 눌렀을 때와 마지막 키를 해제할 때 사이의 시간 간격을 의미하며, hold-time 특징은 한 문자에 대해 눌렀을 때와 해제할 때의 시간 간격을 의미한다.

H. Saevanee는 터치스크린을 눌렀을 때의 손가락 압력을 이용하는 키스트로크 다이나믹스를 제안하였다[24]. PNN(Probabilistic Neural Network)를 사용한 이 연구는 99%의 정확도(accuracy)를 보여주었다. 또한, 안드로이드 1.6의 'Donut'이 출시됨에 따라 많은 연구에서 손가락 끝의 크기, 모바일 장치의 방향(orientation) 및 각도(angle) 등 다양한 특징들을 추출하기 시작했다[25]. J. B. Kim, M. K. Lee은 그 중에서도 터치스크린의 좌표 특징을 이용하여 4자리 PIN, 6자리 PIN, 11자리 전화번호에 대해 실험한 결과 각각 EER 8.1%, 6.2%, 8.1%를 결과를 보였다[26].

2010년 12월, 안드로이드 2.3이 출시됨에 따라 자이로스코프(gyroscope), 회전 벡터(rotation vector), 선형 가속도계(linear accelerometer), 그리고 중력(gravity)과 같은 더 많은 특징을 추출할 수 있었다. L. Cai와 H. Chen은 키스트로크 다이나믹스의 특징으로 모바일 장치의 방향 특징을 사용했다. 이 연구에서는 키 숫자를 추측하기 위해 x축(azimuth), y축(pitch) 그리고 z축(roll)의 각도를 주요 수치로 사용하여 71.5% 정확도의 실험 결과를 얻었다[27]. 이후, Z. Xu는 입력된 키를 추측하기 위해 모바일 장치의 가속도계 특징과 방향 특징을 사용하여 이전 연구보다 높은 88.7%의 정확도를 보였다[28]. 또한 C. Jung, R. Jang, D. Nyang, 그리고 K. Lee는 가속도계와 진동 센서를 이용하여 사용자가 터치스크린을 터치하지 않고 PIN을 입력할 수 있는 방법을 제안하였다[29].

사용자를 분류하는 방법으로 statistical 분류기, neural network 분류기 외에도 거리기반 분류기를 사용한 연구가 진행되었다. 4자리 PIN에 대해 거리기반 분류기를 사용한 결과 Nearest Neighbor 거리기반 분류기는 EER 3.65%[15], Euclidean 거리기반 분류기는 EER 20%[16]의 실험 결과를 보였다. 거리기반 분류기끼리의 성능을 비교한 연구 결과에서는 kNN(k-Nearest Neighbor) Manhattan weighted 거리기반 분류기와 kNN Manhattan scaled weighted 거리기반 분류기가 각각 0.08%의 EER로 가장 좋은 성능으로 평가되었으며[17], Manhattan, Mahalanobis, Euclidean 세 가지 거리기반 분류기를 비교한 다른 연구 결과는 Manhattan 거리기반 분류기가 EER 12.9%로 다른 분류기보다 약 3% 우수하다고 평가되었다[18].

거리기반 분류기 비교뿐만 아니라 키스트로크 특징들의 성능 비교, 특징들의 조합 실험, 사용자별 맞춤형 특징 집합을 위한 연구들이 진행되었다. 키스트로크 데이터 중 시간 특징과 터치 사이즈 특징들의 성능을 비교한 결과 터치 사이즈 특징이 특징들 가운데 가장 좋은 성능을 보였으며[6], 가속도계, 방향 특징과 같은 모션 특징과 시간 특징, 터치 압력 특징, 터치 사이즈 특징들의 성능을 비교한 연구 결과도 있었다[19, 20]. 특징들을 조합하여 실험한 연구에서는 시간 특징과 터치 압력 특징을 조합한 결과[21]는 EER 8.4%, 시간 특징과 터치 압력 특징, 좌표 특징을 조합한 결과[22]는 EER 2.8%로 조합들 가운데 가장 좋은 성능을 보였다. 또한, 사용자별 맞춤형 특징을 제공하는 연구에서는 시간 특징과 자이로스코프, 보정되지 않은 자이로스코프(uncalibrated gyroscope), 가속도계, 선형 가속도계, 4개의 모션 특징을 사용하여 실험하였고, 실험 결과 6명의 사용자에 대한 사용자별 맞춤형 특징이 전체 특징을 사용한 경우보다 평균적으로 EER 6% 이상 성능이 향상됨을 보였다[23].

1.2 논문의 목표와 기여

본 논문에서는 터치스크린과 온보드(on-board) 모션 센서(가속도계, 자이로스코프 등)가 장착된 스마트폰에 초점을 맞춘 키스트로크 다이나믹스에 대해

Table 1. Comparison of previous keystroke dynamics experiment methods and results

Study	Year	Subject size	Input type	Input length	Motion data	Classifier	EER(%)
Clarke et al. [14]	2007	32	D	4 / 11	X	neural network	8.5 / 4.9
Zheng et al. [15]	2014	80	D	4 / 8	O	Nearest Neighbor distance	3.65 / 4.45
Mendizabal-Vazquez et al. [16]	2014	80	D	4	O	Euclidean distance	20
Giuffrida et al. [17]	2014	20	C	8-9	O	kNN(k=1) Manhattan weighted kNN(k=1) Manhattan scaled weighted	0.08
Antal and Szabo [18]	2014	42	C	10	X	Manhattan distance	12.9
Ho [19]	2014	55	D	4	O	SVM	FAR 4.4%, FRR 5.3%
Wu and Chen [20]	2015	100	D	8	O	statistical	0.556
Tasia et al. [21]	2014	100	D	4-10	X	statistical	8.4
Jain et al. [22]	2014	30	D	10	X	SVM	2.8
Teh et al. [6]	2016	50	C	4 / 16	X	Gaussian estimation, z-score matching function, standard deviation drift	6.27
		150					5.49
Lee et al. [23]	2017	6	D	6	O	OC(One-Class)SVM	5.27
C : Character, D: Digit							

알아본다.

본 논문이 기여하고자 하는 바는 다음과 같다. 기존의 키스트로크 다이나믹스 연구에서는 실험을 위해 비정상 사용자(imposter)의 데이터를 정상 사용자의 학습 데이터로 구성하여 실험하였다. 하지만 실제 인증 시스템에서는 시스템 구성, 개인정보 보호의 문제로 비정상 사용자의 데이터를 정상 사용자의 학습 데이터로 사용하는 것은 불가능하다. 본 논문에서는 비정상 사용자의 데이터를 학습 데이터로 사용하지 않고 정상 사용자 학습만으로 임계값(threshold)을 구할 수 있도록, 임계값을 구하는 방법을 공식화하여 제공하고자 한다.

우선적인 대상으로 본 논문에서는 거리기반 분류기에 초점을 맞추어 실험을 진행하였다. 거리기반 분류에서는 정상 사용자 학습 데이터의 평균점을 구하여 평균점과의 거리를 임계값으로 정하는데, 이때 정상 사용자의 데이터와 비정상 사용자의 데이터를 이용하여 오류율을 최소화하는 거리로 분류의 임계값을 정하게 된다. 따라서 사용자별로 학습을 통해 최적의 임계값을 정하는데 이때 비정상 사용자 데이터가 사

용되게 된다. 본 논문에서는 임계값을 구하는 학습에서 비정상 사용자 데이터 없이 임계값을 정할 수 있도록 공식을 제시하기 위하여, 평균점으로부터 가장 먼 정상 사용자와의 최대 거리 $d_{\max}$를 구하고, 임계값을 최대 거리로부터의 비율 α로 정한다. (즉, $threshold = d_{\max} * \alpha$). 실험을 통해 최적의 비율 α 값을 찾고, 이 값이 모든 사용자에 대해서 근사한 값으로 수렴됨을 실험으로 보이고, 제시한다. 이를 통해 추후에 적용에 있어서 정상 사용자 데이터만으로 평균점과 최대거리를 구하고, 이에 최적 비율을 곱하여 거리 분류의 임계값으로 사용하도록 한다. 따라서 본 논문의 실험을 통해 키스트로크 다이나믹스에 최적화된 α 값을 찾을 수 있는지 검토해보고 권장하는 α 값을 제안하는 것을 목표로 한다.

1.3 논문의 구성

본 논문의 구성은 다음과 같다. 2장에서 정상 사용자를 분류하기 위해 사용하는 거리기반 알고리즘에 대해 알아본다. 3장에서는 실험에 사용된 특징과 데이터 수집에 대해 설명하고 4장에서는 성능 평가를 위한 3가지 오류율에 대해 알아본다. 5장에서는 실험 방법과 실험 결과에 대해 자세하고 분석하고 마지막으로 6장에서는 본 논문의 결론과 향후 연구 계획을 기술한다.

II. 거리기반 분류기

키스트로크 다이나믹스는 키보드 또는 모바일 장치에서 사용자 고유의 입력 패턴과 행동을 인증 기준으로 사용한다. 인증을 위한 첫 단계로 정상 사용자의 특징 데이터를 이용하여 정상 사용자의 템플릿을 생성하며, 생성된 템플릿은 비정상 사용자로부터 정상 사용자를 분류하기 위해 사용된다. 정상 사용자를 분류하기 위해 SVM(Support Vector Machine), statistical, kNN 그리고 거리기반 분류기 등 다양한 분류기가 사용된다.

본 논문에서는 거리기반 분류기를 사용하여 사용자 샘플의 평균점과 샘플 사이의 거리를 계산함으로써 정상 사용자인지 아닌지를 분류한다. 거리기반 분류기를 사용하기 위한 첫 번째로 다른 특징 크기로부터 영향을 덜 받기 위해서 샘플 데이터를 스케일링(scaling)한다. 거리기반 분류의 경우, 사용하기 위한 거리 메트릭(distance metric)을 설정해야 하는데 본 실험에서는 Euclidean 거리와 Manhattan 거리를 선택하였다. 각각의 거리에 대한 정의는 2.2 거리 메트릭에 설명되어 있다.

2.1 스케일링

모바일 장치에는 다양한 온보드 센서로 인해 수집되는 데이터의 단위는 센서 유형별로 다르다. 따라서 올바른 값을 사용하기 위해서 데이터는 동일하거나 고정된 범위 내로 스케일링한다. 서로 다른 단위를 사용할 경우 예상하지 못한 가중치가 되어 원치 않은 실험 결과를 얻을 수 있다.

다양한 단위를 스케일링하기 위해 본 논문에서는 Min-Max 스케일링과 Standard 스케일링 방법을 사용하였다.

2.1.1 Min-Max 스케일링

Min-Max 스케일링은 데이터를 0과 1 사이의 고정된 범위로 스케일링하는 방법으로써 Min-Max 스케일링 공식은 다음과 같다.

$$X_{sc} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}$$

여기서 X는 데이터 집합, $X_{\min}$은 데이터의 최소값, $X_{\max}$은 데이터의 최대값, X_{sc}는 스케일링 결과를 의미한다.

2.1.2 Standard 스케일링

Standard 스케일링은 전체 데이터의 분포를 평균이 0, 표준편차가 1이 되도록 스케일링하는 방법으로써 Standard 스케일링 공식은 다음과 같다.

$$z = \frac{x - \mu}{\sigma}$$

여기서 μ는 의 평균, σ는 x의 표준편차, z는 스케일링 결과를 의미한다.

2.2 거리 메트릭

2.2.1 Euclidean 거리

Euclidean 거리는 두 개의 n차원 점 $p(p_1,p_2,\cdots,p_n)$와 $q(q_1,q_2,\cdots,q_n)$ 사이의 직선거리를 계산하는 방법으로써, Euclidean 거리 계산 공식은 다음과 같다.

$$d(p,q)=\sqrt{(q_1-p_1)^2+(q_2-p_2)^2+\cdots+(q_n-p_n)^2}$$

$$=\sqrt{\sum_{i=1}^{n}(q_i-p_i)^2}$$

2.2.2 Manhattan 거리

Manhattan 거리는 두 개의 n차원 점 $p(p_1,p_2,\cdots,p_n)$와 $q(q_1,q_2,\cdots,q_n)$ 사이의 차를 계산할 후 절댓값을 취하는 방법으로써, Manhattan 거리 계산 공식은 다음과 같다.

$$d(p,q)=|q_1-p_1|+|q_2-p_2|+\cdots+|q_n-p_n|$$

$$=\sum_{i=1}^{n}|q_i-p_i|$$

III. 특징 및 데이터 수집

스마트폰에서 추출 가능한 데이터는 크게 키스트로크 데이터와 모션 데이터 두 그룹으로 나뉜다. 스마트폰의 터치 입력을 인식하는 gesture API(Application Programming Interface)가 '시간', '사이즈', '좌표' 등 키스트로크 데이터를 수집한다. '시간'은 이벤트가 발생한 시간, '사이즈'는 터치스크린을 누른 손가락의 크기, '좌표'는 사용자가 터치하는 지점의 좌표를 각각 반환한다. 모션 센서 데이터에서는 가속도계, 자이로스코프와 관련된 움직임을 추출할 수 있다. 다음 장에서 각 특징에 대해 설명한다.

3.1 키스트로크 데이터

3.1.1 시간 (time)

'time' 특징에는 DT(Down-Time)와 4가지 유형의 FT(Flight-Time)이 있다. 〔Fig. 2〕에서와 같이 DT는 하나의 키에 대해서 사용자가 키를 누른 순간(dn)부터 키를 해제할 때(up)까지의 시간 간격을 의미한다. FT는 DT와 달리 두 개의 키 간의 눌렀을 때와 해제할 때의 시간차를 의미하는데 FT1은 키를 해제할 때의 순간부터 다음 키를 누를 때까지의 시간 간격, FT2는 키를 해제할 때의 순간부터 다음 키를 해제할 때까지의 시간 간격, FT3은 키를 누른 순간부터 다음 키를 누를 때까지의 시간 간격, FT4는 키를 누른 순간부터 다음 키를 누를 때까지의 시간 간격을 의미한다. 따라서 'time' 데이터는 1개의 키 당 1개의 DT와 4개의 FT로 구성되며, 수집된 6자리 PIN의 1개의 샘플에는 6개의 DT와 20개의 FT, 총 36개의 원시 데이터(raw data)로 구성된다.

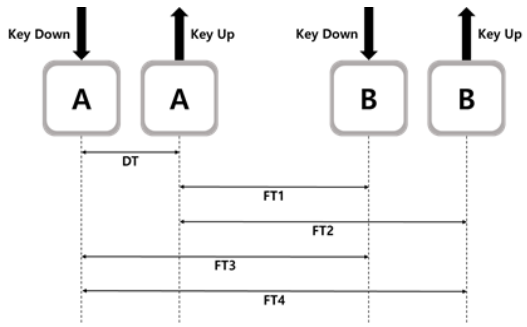


Fig. 2. Time feature configuration

3.1.2 사이즈 (size)

'size'는 사용자가 키를 눌렀을 때와 해제할 때 사용자의 손가락 크기를 추출한다. 'size' 데이터는 1개의 키당 눌렀을 때(sizeDn)와 해제할 때(sizeUp)의 사이즈로 구성된다. 따라서 수집된 6자리 PIN의 1개의 샘플에는 6개의 sizeDn과 6개의 sizeUp, 총 12개의 원시 데이터로 구성된다.

3.1.3 좌표 (coordinate)

'coordinate'는 사용자가 키를 눌렀을 때와 해제할 때의 스마트폰 터치스크린의 가로 x축 정보와 세로 y축 정보를 추출한다. 'coordinate' 데이터는 1개의 키당 키를 눌렀을 때의 x축, y축 정보(xyDn)와 해제할 때의 x축, y축 정보 (xyUp)로 구성된다. 따라서 수집된 6자리 PIN의 1개의 샘플에는 각각 6

개의 xyDn, xyUp 총 24개의 원시 데이터로 구성된다.

3.2 모션 데이터

3.2.1 가속도계 (accelerometer)

'acc'는 사용자의 중력값을 이용하여 〔Fig. 3〕(a)와 같이 스마트폰의 3축 가속도계(m/s^2), 가로 x축, 세로 y축, 수직 z축을 측정한다. 측정되는 모션 데이터의 원시 데이터의 수는 샘플마다 다르기 때문에 추가적인 데이터 재구성 과정을 걸쳐 정규 형식으로 만들어진다. 데이터를 재구성하기 위한 공식과 과정은 3.2.3 모션 데이터 공식에 설명되어 있다.

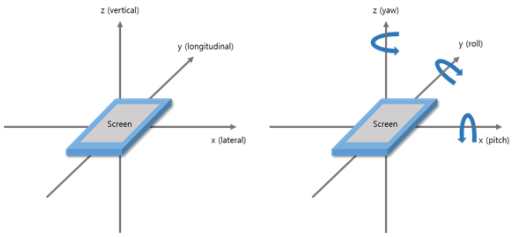


Fig. 3. Axis configuration of motion sensor (a) accelerometer and (b) gyroscope

3.2.2 자이로스코프 (gyroscope)

'gyr'는 〔Fig. 3〕(b)와 같이 x축, y축, z축을 이용하여 스마트폰이 각 축에 대해 회전하는 각속도를 측정한다. 'gyr'는 'acc'에서 측정할 수 없는 방위각을 측정하기 때문에 'gyr'와 'acc'의 측정 데이터를 합치면 정확한 움직임을 파악할 수 있다〔30〕.

3.2.3 모션 데이터 공식

앞서 언급했듯이, 'acc', 'gyr'의 2가지 유형의 모션 데이터는 샘플마다 측정되는 원시 데이터가 일정하지 않고 지나치게 많은 데이터를 포함하기 때문에 이들은 여러 공식에 의해 재구성될 필요가 있다. 먼저 DT 간격으로 데이터를 그룹화하고 DT 간격 이외의 모션 데이터는 사용하지 않는다. 그룹화된 데이터는 평균 값(mean), 평균 제곱근(rms), 양수 값의 합(pos), 음수 값의 합(neg), 표준편차(std) 등 5개의 공식에 의해 계산된다〔17〕.

n개의 원소를 가진 $X= x_1+x_2+\cdots+x_n$ 의 경우 평균 값(X_{mean}), 평균 제곱근(X_{rms}), 양수 값의 합(X_{pos}), 음수 값의 합(X_{neg}), 표준편차(X_{std})를 구하기 위한 공식은 다음과 같다.

$$X_{mean} = \frac{x_1+x_2+\cdots+x_n}{n}$$

$$X_{rms} = \sqrt{\frac{1}{n}(x_1^2+x_2^2+\cdots+x_n^2)}$$

$$X_{pos} = \sum_{i=1}^{n} x_i (where\, x_i > 0)$$

$$X_{neg} = \sum_{i=1}^{n} x_i (where\, x_i < 0)$$

$$X_{std} = \sqrt{\frac{\sum_{i=1}^{n}(x_i-\overline{x})^2}{n}} (where\, \overline{x}\, is\, mean)$$

3.3 원시 데이터 수집 및 특징 추출

〔Fig. 4〕와 같이 본 논문에서는 6자리 PIN인 '766420'을 입력하여 원시 데이터를 수집하는 안드로이드 app을 개발했다. PIN은 터치스크린에서 숫자들의 다양한 위치를 고려하여 생성하였다〔6, 31〕. 실험을 위해 Nexus 5X에 ETRI keystroke

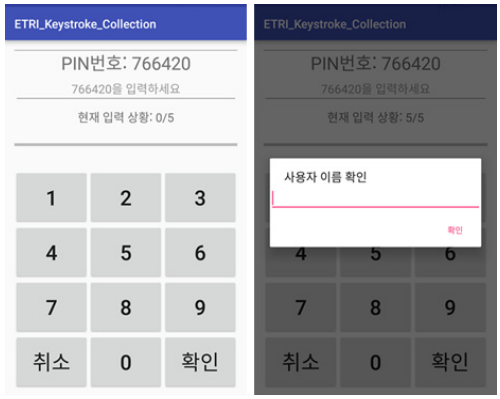


Fig. 4. The user interface of the ETRI key collection app. After entering PIN '766420', users enter their name to save the data.

Table 2. Experiment environment

Collect method	ETRI key collection app
Collect device	Nexus 5x
# of collect	22

collection app〔Table 2〕을 설치하였으며 22명의 사용자를 대상으로 키스트로크 데이터를 수집하였다. 6자리 PIN을 한번 입력 시 한 개의 샘플이 저장되며 사용자당 100개 이상의 샘플을 수집하였다.

수집된 샘플의 구성은 〔Table 3, Table 4〕와 같다. 하나의 샘플당 26개의 'time' 특징(DT, FT1, FT2, FT3 그리고 FT4), 12개의 'size' 특징(sizeDn, sizeUp), 24개의 'coordinate' 특징(xyDn, xyUp), 5개 방법(mean, pos, neg, rms, neg)으로 추출한 모션 데이터 각각 18개의 'acc' 특징(x, y, z), 18개의 'gyr' 특징(x, y, z)으로 구성되므로 한 개의 샘플에는 총 242개의 특징으로 구성된다.

IV. 성능 평가

사용자 인증에서는 성능을 평가하기 위해 3가지 유형의 오류율〔Fig. 5〕을 사용한다. 오류율에 대한 설명은 다음과 같다.

FAR(False Acceptance Rate) : 비정상 사용자를 정상 사용자로 인식하여 승인하는 확률
FRR(False Rejection Rate) : 정상 사용자를 비정상 사용자로 인식하여 거부하는 확률
EER(Equal Error Rate) : FAR과 FRR이 같아지는 비율

FAR은 시스템의 견고성을 의미함에 따라, 만약 FAR이 높으면 공격자를 포함한 비정상 사용자는 쉽게 인증 시스템을 통과할 수 있다. 반면에 FRR은 사용성과는 별개로 시스템의 완전성을 의미함에 따라, 만약 FRR이 높으면 정상 사용자는 인증에 실패할 수 있으며 인증 절차를 반복해서 다시 시도해야 한다. 퍼지(fuzzy) 기반 인증 시스템에서 사용하는 인증 요소에는 항상 잡음이 존재하기 때문에 견고성과 완전성은 완벽할 수 없다. 실제 응용프로그램에서는 시스템의 완전성보다 견고성이 더 중요함에 따라 사용자들에게 2~3번의 재시도를 요구한다. 따라서 시스템은 사용자들에게 신뢰할 수 있는 수준의 보안을 제공할 수 있다.

Table 3. Features and number of keystroke type of PIN '766420' sample

Sample											
Type	Keystroke										
Feature	Time					Size		Coordinate			
	DT	FT1	FT2	FT3	FT4	sizeDn	sizeUp	xDn	yDn	xUp	yUp
Each #	6	5	5	5	5	6	6	6	6	6	6
	26					12		24			
	62 features										

Table 4. Features and number of motion type of PIN '766420' sample, The total number of features of the PIN '766420' sample.

Sample										
Type	Motion									
Feature	mean		pos		neg		rms		neg	
	acc	gyr	acc	gyr	acc	gyr	acc	gyr	acc	gyr
Each #	18	18	18	18	18	18	18	18	18	18
	36		36		36		36		36	
	180 features									
Total #	1 sample = 62 features+ 180 features = 242 features									

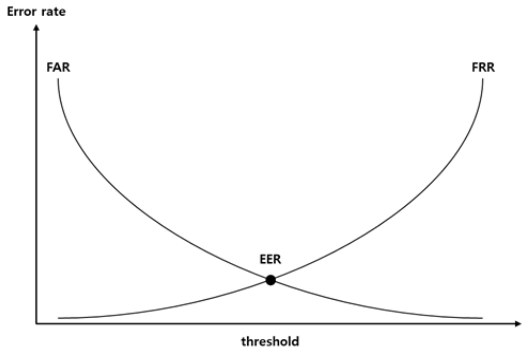


Fig. 5. The relationship between the FRR, FAR, and EER[7]

비정상 사용자들로부터 정상 사용자를 구별하기 위해 FAR과 FRR 값을 조절할 수 있는 임계값을 사용한다. 일반적으로 FAR을 줄이면 FRR이 증가하고, FAR을 증가시키면 FRR이 증가하게 된다.

만약 FAR과 FRR이 같아졌을 때, 이때를 EER이라고 부른다. EER은 종종 퍼지기반의 인증 결과를 평가하기 위한 성능으로 사용된다. FAR과 FRR이 EER에 가까워질 때, 대략 $\frac{(FAR+FRR)}{2}=EER$의 관계를 만족시킨다. 따라서 EER이 계산된 후, 원하는 오류율(예: FAR)을 조절하고자 할 때는 $\frac{(FAR+FRR)}{2}=EER$ 의 관계를 이용하여 다른 오류율(예: $FRR=(2*EER)-FAR$)을 조절할 수 있다.

V. 실험 방법 및 결과

5.1 실험 방법

본 논문에서는 수집된 데이터를 활용하여 각각의 특징들의 성능을 비교하고 특징들을 조합하여 조합된 특징들의 성능을 비교한다. 또한, 거리기반 분류기에서 계산된 기본 임계값에 α 값을 곱한 결과를 임계값으로 설정하여 비교함으로써 키스트로크 다이나믹스에 최적화된 α 값을 찾는다.

실험을 위해 스케일링, 거리기반 분류기, 학습, 검증 & 최적화(validation & optimization)의 과정이 필요하다. 다음은 4가지 실험 과정에 대한 설명이다.

5.1.1 스케일링

수집된 데이터의 단위는 센서 유형별로 다르기 때문에 데이터들을 동일하거나 고정된 범위 내로 스케일링해야 한다. 모든 데이터에 대해 스케일링함으로써 원하지 않는 가중치가 생기는 것을 방지할 수 있다.

5.1.2 거리기반 분류기

정상 사용자와 비정상 사용자를 분류하기 위한 다양한 분류기가 사용되지만 본 논문에서는 거리기반 분류기를 사용하여 정상 사용자를 분류한다.

실험에서 사용할 스케일링과 거리 메트릭을 설정하기 위해 Ⅱ. 거리기반 분류기에서 언급한 스케일링, 거리 메트릭 각각 2가지 방법에 대해 조합하여 성능을 비교하였다. 비교 결과 Standard 스케일링과 Manhattan 거리의 조합이 가장 좋은 성능을 보여 본 논문에서는 스케일링은 Standard 스케일링, 거리 메트릭은 Manhattan 거리를 사용하였다[Table 5].

Table 5. The scaling and distance metric used in the experiment.

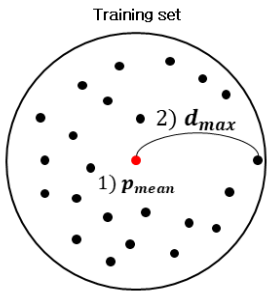
Scaling	Standard scaling
Distance metric	Manhattan distance

5.1.3 학습

스케일링 된 정상 사용자의 데이터에 대해 moving window 기법을 이용하여 정상 사용자를 학습한다. 정상 사용자로부터 수집된 전체 데이터에서 50개의 데이터를 하나의 윈도우로 정의한 후, 이를 학습 데이터와 검증을 7:3 비율로 나누어 실험한다.

본 논문의 실험 결과는 정상 사용자의 전체 데이터에 대해 50개 크기만큼 moving window을 반복해서 실험한 결과의 평균을 EER로 사용한다.

학습을 위해 정상 사용자의 학습 데이터에 대해서 먼저 평균점을 구하고, 평균점으로부터 가장 멀리 있는 학습 데이터와의 거리를 계산하여 기본 임계값으로 설정한다[Fig. 6].



1) p_{mean} : mean point of train data

2) d_{max} : distance between mean point & farthest point

Fig. 6. Distance definition to calculate the $d_{\max}$ (initial threshold)

5.1.4 검증 & 최적화

스케일링 된 정상 사용자의 검증 데이터와 스케일링 된 비정상 사용자의 데이터에 대해 EER을 최소로 하는 α 값을 구한다. 학습 과정에서 계산된 기본 임계값($d_{\max}$)의 배수를 의미하는 α 값을 구하기 위해 $0.5 \leq \alpha \leq 2.5$의 범위 내에서 0.1 단위로 반복해서 실험하여 가장 좋은 성능을 보이는 α 값을 실험적으로 구한다. 최적화를 위해 사용되는 임계값 계산 공식은 다음과 같다.

$$threshold = d_{\max} * \alpha$$

5.2 실험 결과

본 논문에서는 $d_{\max}$ 대비 최적의 임계값의 비율인 α 값을 실험적으로 구하기 위하여 먼저 최선의 EER이 되는 특징 조합(feature combination)을 찾는 실험을 선행하였다. 첫 번째로 특징 별 순위를 계산하는 실험을 하였고, 이를 바탕으로 특징 조합을 통해 최선의 EER을 갖는 특징 조합을 실험적으로 구하였다. 마지막으로, 이러한 특징 조합에 대한 실험 결과로 α 값이 1.1일 때 최적임을 실험적으로 보였다.

5.2.1 특징 별 순위 계산 실험

특징 별 순위 계산 실험은 각 특징들의 성능을 비교하여 순위를 매기기 위한 실험으로써, 'time' 특징, 'size' 특징, 'coordinate' 특징의 키스트로크 데이터와 모션 데이터의 'acc' 특징, 'gyr' 특징을 사용하여 실험하였다. 특징 별 순위 계산 실험에 사용된 특징의 수는 키스트로크 데이터의 'time' 특징 5개, 'size' 특징 2개, 'coordinate' 특징 2개, 모션 데이터의 'acc' 특징 15개, 'gyr' 특징 15개로 총 39개

Table 6. The result of experiment for calculating feature ranks and optimal α

Rank	Feature	EER (%)	Optimal α
1	FT4	21.947	0.6
2	FT2	22.705	0.6
3	xyDn	23.684	0.8
4	DT	23.716	0.9
5	FT3	23.911	0.6
6	FT1	24.569	0.5
7	sizeDn	25.861	0.8
8	pos-acc-y	28.568	1.1
9	pos-gyro-y	29.342	0.8
10	xyUp	29.983	0.6
11	neg-gyro-y	30.599	0.8
12	rms-gyro-x	30.602	0.8
13	mean-acc-y	30.732	1.1
14	rms-acc-y	30.732	1.2
15	pos-acc-z	30.813	0.9
16	mean-acc-x	31.072	1.1
17	neg-acc-x	31.201	0.7
18	pos-acc-x	31.321	0.8
19	pos-gyro-x	31.935	0.8
20	mean-gyro-y	32.071	0.8
21	rms-acc-z	32.645	1
22	mean-acc-z	32.740	1
23	rms-gyro-y	32.842	0.8
24	rms-gyro-z	33.014	0.9
25	mean-gyro-x	33.218	0.8
26	sizeUp	33.392	0.8
27	rms-acc-x	34.739	0.8
28	neg-gyro-x	34.769	0.9
29	std-gyro-x	35.239	0.7
30	std-gyro-z	35.555	0.6
31	std-acc-y	35.702	0.6
32	pos-gyro-z	36.011	0.7
33	std-acc-x	36.189	0.6
34	neg-gyro-z	36.633	0.8
35	std-gyro-y	36.635	0.6
36	std-acc-z	37.121	0.7
37	mean-gyro-z	37.676	1
38	neg-acc-z	46.942	0.7
39	neg-acc-y	48.458	1.1

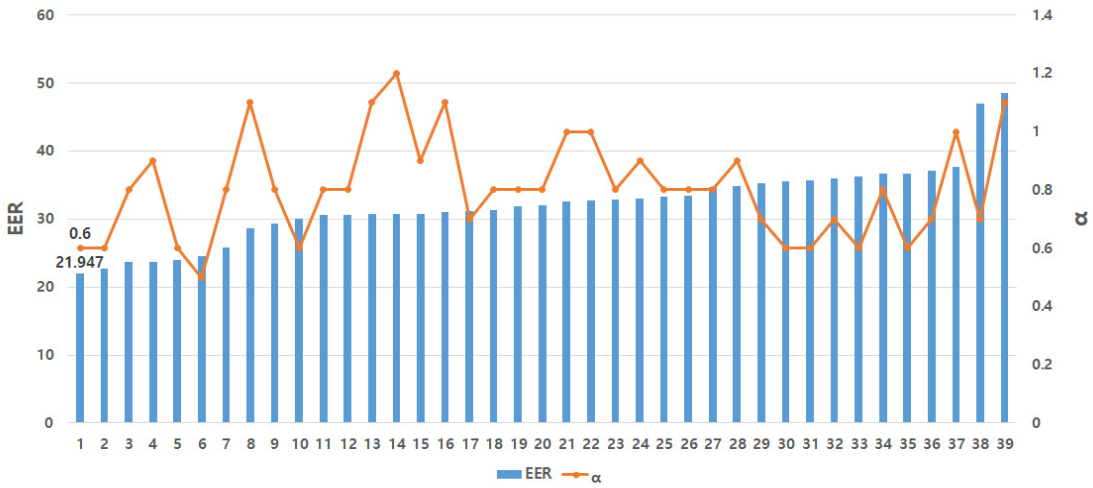


Fig. 7. The result of experiment for calculating feature ranks and optimal α

특징을 사용하였다.

〔Table 6〕과 〔Fig. 7〕은 특징 별 순위 계산 실험에 대한 결과를 보여준다. 〔Fig. 7〕은 〔Table 6〕를 바탕으로 작성되었으며 〔Fig. 7〕의 x축은 〔Table 6〕의 rank를 의미한다. 실험 결과 'time' 특징, 'coordinate' 특징, 'size' 특징의 키스트로크 데이터가 대체적으로 좋은 성능을 보이는 가운데 'time' 특징의 'FT4' 특징이 EER 21.947%로 가장 좋은 성능을 보였으며 음수 값의 합(neg)으로 추출한 모션 데이터의 'acc-y축' 특징이 EER 48.458%, 'acc-z축' 특징이 EER 46.942%로 가장 안 좋은 성능을 보였다.

5.2.2 특징 조합 실험 및 권장 α 값

특징 조합 실험은 각 특징들을 조합하여 성능을 비교한 후 좋은 성능의 조합을 찾기 위한 실험으로 〔Table 6〕의 특징 별 순위 계산 실험 결과를 바탕

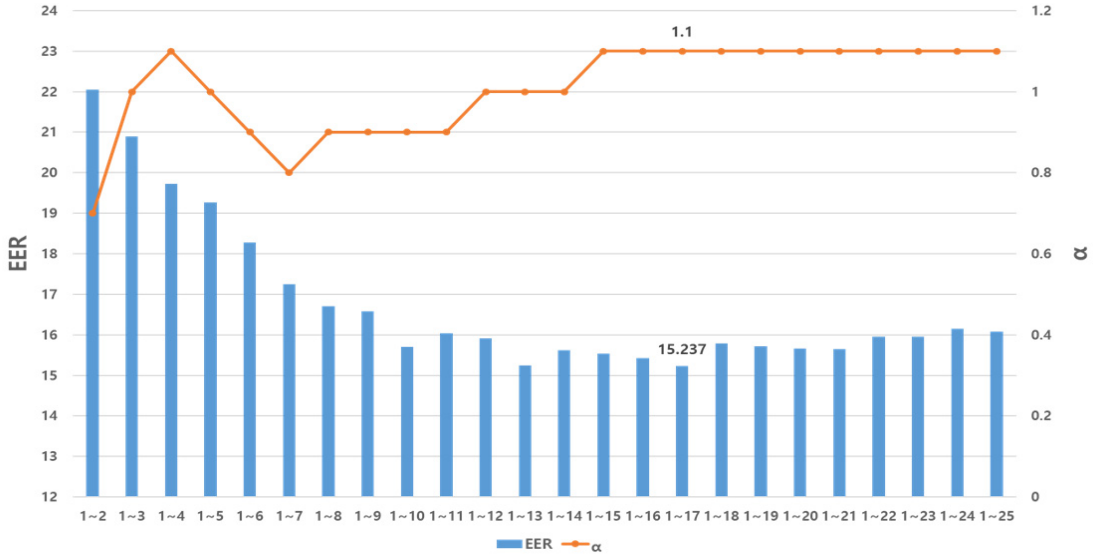


Fig. 8. The result of experiment for performance comparison of combined features and for calculating optimal α

으로 실험하였다.

〔Fig. 8〕은 특징 조합 실험에 대한 결과를 보여준다. 〔Fig. 8〕의 x축은 1번 특징부터 조합된 특징의 수를 의미하며, 예를 들어 〔Fig. 8〕의 x축이 10일 경우 〔Table 6〕의 rank 1부터 rank 10까지의 특징 조합을 의미한다. 특징 조합 실험에서 사용된 조합은 총 24개 조합으로 높은 순위의 특징들을 최소 2개부터 최대 25개까지 조합하여 실험하였다.

〔Fig. 8〕에서 나타난 것과 같이 실험 결과 17개 특징 조합이 EER 15.237%, 13개 특징 조합이 EER 15.247%로 가장 좋은 성능을 보였으며 10개 미만의 특징 조합, 24개 이상의 특징 조합들이 대체적으로 안 좋은 성능을 보였다. 〔Fig. 8〕에서 선(solid line)은 각각의 조합에 대해 최적의 EER을 주는 α 값이다. 그래프에서 볼 수 있듯이 15개 이상의 특징 조합들의 경우 최적화 된 α 값이 1.1로 고정됨을 확인할 수 있었다.

따라서 실험을 통하여 $d_{\max}$대비 임계값의 비율인 α 값이 1.1일 때 최적의 임계값을 가질 수 있음을 실험적으로 보여주었고, 또한 이를 통해서 사용자별로 비정상 사용자 데이터를 통한 학습 없이 정상 사용자 데이터만으로 구한 평균값과 최대 거리 값을 $d_{\max}$ 이용하여 다음의 임계값을 이용하는 방안을 제시한다.

$$threshold = d_{\max} * 1.1$$

VI. 결 론

본 논문에서는 키스트로크 다이나믹스에 최적화된 조합과 α 를 찾기 위해 22명의 사용자로부터 데이터를 수집하여 실험하였다. 특징 별 순위 계산 실험, 특징 조합 실험, 2가지 실험을 진행하였으며 실험을 위해 수집한 데이터의 특징 추출, 스케일링, 거리기반 분류기, 학습, 검증 & 최적화의 과정을 걸쳐 실험 결과를 얻었다.

특징 별 순위 계산 실험에서는 39개 특징들 가운데 'FT4' 특징이 EER 21.947%로 가장 좋은 성능을 보였으며 특징 별 순위 계산 실험 결과를 바탕으로 진행한 특징 조합 실험에서는 좋은 성능의 17개 특징 조합이 EER 15.237%, α 값이 1.1의 결과를 보였다. 따라서 실험을 통해 키스트로크 다이나믹스에 최적화된 조합은 좋은 성능의 17개 특징 조합, 최적화된 α 값은 1.1임을 확인하였다.

향후 본 연구를 바탕으로 차원축소와 같은 추가적인 전처리 과정과 다른 분류 방법을 사용하여 실험을 계속 진행하여 더 낮은 EER을 얻기 위한 연구를 지속할 예정이다.

References

〔1〕 Statista, "Number of smartphone users in the U.S. 2010- 2022," https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/

〔2〕 Statista, "Number of smartphone users in South Korea from 2015 to 2022," https://www.statista.com/statistics/467171/forecast-of-smartphone-users-in-south-korea/

〔3〕 N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller, "On the need for different security methods on mobile phones," Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, ACM, pp. 465-473, Aug. 2011.

〔4〕 T. Y. Chang, C. J. Tsai, W. J. Tsai, C. C. Peng, and H. S. Wu, "A changeable personal identification number-based keystroke dynamics authentication system on smart phones," Security and Communication Networks, vol. 9, no. 15, pp. 2674-2685, Oct. 2016.

〔5〕 P.K. Sari, G. S. Ratnasari, and A. Prasetio, "An evaluation of authentication methods for smartphone based on users' preferences," IOP Conference Series: Materials Science and Engineering, IOP Publishing, vol. 128, no. 1, pp. 012036, Apr. 2016.

〔6〕 P. S. Teh, N. Zhang, A. B. J. Teoh, and K. Chen, "TDAS: a touch dynamics based multi-factor authentication solution for mobile devices," International Journal of Pervasive Computing and

Communications, vol. 12, no. 1, pp.127-153, Apr. 2016.
〔7〕 P. S. Teh, N. Zhang, A. B. J. Teoh, and K. Chen, "A survey on touch dynamics authentication in mobile devices," Computers & Security, vol 59, pp. 210-235, Jun. 2016.
〔8〕 R. Spillane, "Keyboard apparatus for personal identification," IBM Technical Disclosure Bulletin, vol. 17, no. 3346, Apr. 1975.
〔9〕 D. Umphress and G. Williams, "Identity verification through keyboard characteristics," International Journal of Man-Machine Studies, vol. 23, no. 3, pp. 263-273, Apr. 1985.
〔10〕 J. Kim, H. Kim, and P. Kang, "Enhanced keystroke dynamics user authentication Based on free text strings," Proceedings of the Korean Operations and Management Science Society Conference, pp. 1846-1876, Apr. 2016.
〔11〕 ITU, "The world in 2014: ICT facts and f igures," International Telecommunication Union, http://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf (accessed: 15 January 2015).
〔12〕 N.L. Clarke, S.M. Furnell, B.M. Lines, and P.L. Reynolds, "Subscriber authentication for mobile phones using keystroke dynamics," Proceedings of the Third International Network Conference (INC 2002), Plymouth, UK, pp. 347-355, Jul. 2002.
〔13〕 N.L. Clarke, S.M. Furnell, B.M. Lines, and P.L. Reynolds, "Keystroke dynamics on a mobile handset: a feasibility study," Information Management & Computer Security, vol. 11, no. 4, pp. 161-166, Oct. 2003.
〔14〕 N.L. Clarke and S.M. Furnell, "Authenticating mobile phone users using keystroke analysis," International Journal of Information Security, vol. 6, no. 1, pp. 1-14, Jan. 2007.
〔15〕 N. Zheng, K. Bai, H. Huang, and H. Wang, "You Are How You Touch: User Verification on Smartphones via Tapping Behaviors," Network Protocols (ICNP), 2014 IEEE 22nd International Conference on. IEEE, pp. 221-232, Oct. 2014.
〔16〕 I. De Mendizabal-Vazquez, D. de Santos-Sierra, J. Guerra- Casanova, and C. Sanchez-Avila, "Supervised classification methods applied to keystroke dynamics through mobile devices," 2014 International Carnahan Conference on Security Technology (ICCST), pp. 1-6, Oct. 2014.
〔17〕 C. Giuffrida, K. Majdanik, M. Conti, and H. Bos, "I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics," International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 92-111, Jul. 2014.
〔18〕 M. Antal, L. Z. Szabó and I. László, "Keystroke dynamics on android platform," Procedia Technology, vol. 19, pp. 820-826, Jan. 2015.
〔19〕 G. Ho, "Tapdynamics: Strengthening User Authentication on Mobile Phones with Keystroke Dynamics," Technicalreport, StanfordUniversity, 2014.
〔20〕 J. Wu and Z. Chen, "An Implicit Identity Authentication System Considering Changes of Gesture Based on Keystroke Behaviors," International Journal of Distributed Sensor Networks, vol. 11, no. 6, pp. 470274, Jan. 2015.
〔21〕 C. J. Tasia, T. Y. Chang, P. C. Cheng, and J. H. Lin, "Two novel biometric features in keystroke dynamics authentication systems for touch screen devices," Security and Communication Networks,

vol. 7, no. 4, pp. 750-758, Apr. 2014.

[22] L. Jain, J. V. Monaco, M. J. Coakley, and C. C. Tappert, "Passcode Keystroke Biometric Performance on Smartphone Touchscreens in Superior to That on Hardware Keyboards," International Journal of Research in Computer Applications and Information Technology, vol. 2, no. 4, pp. 29-33, Jul. 2014.

[23] S. H. Lee, J. H. Roh, S. Kim, and S. H. Jin, "A Study of Adaptive Feature Subset for Improving Accuracy of Keystroke Dynamics Authentication on Mobile Environment," The 2017 Spring Conference of the KIPS, 24(1), pp. 287-290, Apr. 2017.

[24] H. Saevanee and P. Bhattarakosol, "Authenticating user using keystroke dynamics and finger pressure," Consumer Communications and Networking Conference, CCNC 2009, 6th IEEE, pp. 1-2, Jan. 2009.

[25] M. Trojahn and F. Ortmeier, "Biometric authentication through a virtual keyboard for smartphones," International Journal of Computer Science & Information Technology, vol. 4, no. 5, pp. 1, Oct. 2012.

[26] J. B. Kim and M. K. Lee, "User authentication using touch positions in a touch-screen interface," Journal of the Korea Institute of Information Security and Cryptology, 21(1), pp. 135-141, Feb. 2011.

[27] L. Cai and H. Chen, "TouchLogger: Inferring Keystrokes on Touch Screen from Smartphone Motion," HotSec, vol. 11, pp. 9, Aug. 2011.

[28] Z. Xu, K. Bai, and S. Zhu, "Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors," Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, pp. 113-124, Apr. 2012.

[29] C. Jung, R. Jang, D. Nyang, and K. Lee, "Technique for PIN Entry Using an Accelerometer Sensor and a Vibration Sensor on Smartphone," KIPS Transactions on Computer and Communication Systems, 6(12), pp. 497-506, Dec. 2017.

[30] Wikipedia, "Gyroscope", https://en.wikipedia.org/wiki/Gyroscope

[31] S. Zahid, M. Shahzad, S.A. Khayam, and M. Farooq, "Keystroke-Based User Identification on Smart Phones," International Workshop on Recent Advances in Intrusion Detection, pp. 224-243, Sep. 2009.

〈저자소개〉

이 신 철 (Shincheol Lee) 학생회원
2015년 2월: 목원대학교 정보통신공학과 졸업
2017년 3월~현재: 세종대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 사용자 인증

황 정 연 (Jung Yeon Hwang) 정회원
1999년 2월: 고려대학교 수학과 졸업
2003년 2월: 고려대학교 정보보호대학원 석사
2006년 8월: 고려대학교 정보보호대학원 박사
2009년 5월~현재: 한국전자통신연구원 책임연구원
〈관심분야〉 암호이론, 프라이버시 강화 암호 기법, 바이오인증

이 현 구 (Hyungu Lee) 학생회원
2016년 2월: 세종대학교 정보보호학과 졸업
2016년 3월~현재: 세종대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 사용자 인증

김 동 인 (Dong In Kim) 학생회원
2016년 2월: 충북대학교 소프트웨어학과 졸업
2016년 9월~현재: 세종대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 사용자 인증

이 성 훈 (Sung-Hoon Lee) 학생회원
2011년 8월: 충주대학교 컴퓨터공학과 졸업
2011년 9월~현재: 과학기술연합대학원대학교 정보보호공학과 통합과정
2011년 9월~현재: 한국전자통신연구원 UST 연구생
〈관심분야〉 사용자 인증, 모바일 보안, 피싱

신 지 선 (Ji Sun Shin) 종신회원
2001년 2월: 서울대학교 컴퓨터공학과 졸업
2009년 5월: 메릴랜드 주립대학(University of Maryland at College Park) 컴퓨터 과학과 박사
2009년 9월~2012년 2월: 삼성 SDS 책임연구원
2012년 3월~현재: 세종대학교 조교수
〈관심분야〉 정보보호, 암호학, 컴퓨터 보안