IE Interfaces
Vol. 25, No. 3, pp. 290-299, September 2012.

자유로운 문자열의 키스트로크 다이나믹스를 활용한 사용자 인증 연구

강필성[1] · 조성준[2†]

[1]서울과학기술대학교 글로벌융합산업공학과 / [2]서울대학교 산업공학과

A Study on User Authentication based on Keystroke Dynamics of Long and Free Texts

Pilsung Kang[1] · Sungzoon Cho[2]

[1]Assistant Professor, Department of Industrial and Information Systems Engineering,
Seoul National University of Science and Technology (Seoultech)
[2]Professor, Industrial Engineering, Seoul National University

Keystroke dynamics refers to a way of typing a string of characters. Since one has his/her own typing behavior, one's keystroke dynamics can be used as a distinctive biometric feature for user authentication. In this paper, two authentication algorithms based on keystroke dynamics of long and free texts are proposed. The first is the K-S score, which is based on the Kolmogorov-Smirnov test, and the second is the 'R-A' measure, which combines 'R' and 'A' measures proposed by Gunetti and Picardi (2005). In order to verify the authentication performance of the proposed algorithms, we collected more than 3,000 key latencies from 34 subjects in Korean and 35 subjects in English. Compared with three benchmark algorithms, we found that the K-S score was outstanding when the reference and test key latencies were not sufficient, while the 'R-A' measure was the best when enough reference and test key latencies were provided.

Keyword: keystroke dynamics, user authentication, free texts, kolmogorov-smirnov test, R-A measure

1. 서 론

정보통신 기술의 꾸준한 발전과 함께 언제 어디서나 접속이 가능한 유비쿼터스 네트워크(ubiquitous network) 환경이 구축됨으로 인하여 개인 정보 유출 및 계정 도용을 통한 피해 사례가 급증하고 있다. 이에 따라 네트워크 접속 및 이용 시 사용자 인증(user authentication) 강화 및 데이터 보호에 대한 요구가 급격히 증가하고 있으나, 현재까지 대부분의 웹기반 서비스들은 아이디와 패스워드의 문자열 조합에 기반을 두는 기본적인 인증 시스템만을 제공하고 있는 실정이다(Peacock *et al*., 2004). 패스워드 기반 사용자 인증 방법론은 개발, 운영, 및 유지 보수가 쉽고 비용이 적게 드는 장점이 있는 반면, 아이디와 짧은 길이의 패스워드 조합만으로 시스템에 접속하는 것이 가능하기 때문에 제 3자에 의해 아이디와 패스워드가 유출될 경우 보안에 매우 취약하다는 치명적인 단점을 가지고 있다(Yan *et al*., 2004).

이러한 패스워드 기반 사용자 인증 방법론의 약점을 극복하기 위하여 패스워드와 생체 기반 정보(biometrics)를 결합한 다양한 2차 인증 방법론들이 연구되었다(Furnell and Clarke, 2005; Jain *et al*., 1999; Prabhakar *et al*., 2003; Yager and Dunstone, 2010). 생체 기반 정보는 그 형태에 따라서 지문, 홍채, 동공 등 개인이 유전

본 연구는 서울과학기술대학교 교내연구과제의 지원을 받아 수행되었습니다.
†연락저자 : 조성준, 151-742 서울시 관악구 관악로 1 서울대학교 공과대학 산업공학과, Fax : 02-889-8560, E-mail : zoon@snu.ac.kr
투고일(2011년 07월 18일), 심사일(2011년 10월 04일), 게재확정일(2011년 12월 30일).

적으로 타고나는 생리학적 정보(physiological biometrics)와 음성 및 키스트로크 다이나믹스(keystroke dynamics)와 같이 행위를 통해 나타나는 행동 기반 정보(behavioral biometrics)로 나뉠 수 있다(Crawford, 2010). 키스트로크 다이나믹스(<Figure 1> 참조)는 개인이 특정한 문자열을 타이핑할 때 개별 문자열을 입력하는 방식으로써, 대부분의 사람들은 개인만의 독특한 타이핑 습관으로 인하여 각자 고유한 키스트로크 다이나믹스를 갖게 된다. 다른 생체 기반 정보의 경우, 2차 인증에 사용되기 위해서는 추가적인 하드웨어의 설치가 필수적인 반면에, 키스트로크 다이나믹스는 유일하게 소프트웨어만으로 개인의 생체 기반 정보를 처리할 수 있는 장점으로 인하여 웹 기반 서비스의 대표적인 2차 인증 방법론으로 널리 연구되어 왔다(Giot *et al*., 2010; Monrose *et al*., 2002; Monrose and Rubin, 2000; Peacock *et al*., 2004).

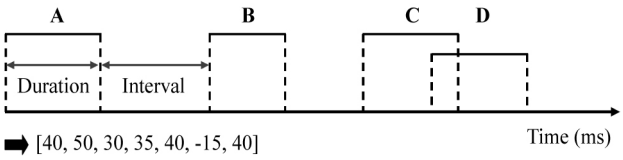


Figure 1. An Example of Keystroke Dynamics for the String 'abcd'

키스트로크 다이나믹스를 이용한 사용자 인증 시스템의 일반적인 구조는 <Figure 2>와 같다. 등록(enrollment) 단계에서는 정상적 사용자(valid user)로 등록함과 동시에 본인이 지정한 패스워드에 대한 일정 횟수의 타이핑 패턴 데이터를 제공한다. 인증 분류기 구축(classifier building) 단계에서는 등록 단계에서 제공된 정상적 사용자의 키스트로크 다이나믹스 데이터를 바탕으로 기계 학습(machine learning) 또는 패턴 인식(pattern recognition) 알고리즘을 사용하여 인증 분류기를 구축한다(Chen and Chang, 2004; Hosseinzadeh and Krishnan, 2008; Sinthupinyo *et al*., 2009; Sheng *et al*., 2005; Zhang *et al*., 2010). 일반적으로 인증 알고리즘의 복잡도가 증가할수록 등록 단계에서 요구하는 정상적 사용자의 키스트로크 다이나믹스 데이터 수집 횟수는 증가한다(Kang *et al*., 2008). 마지막으로 인증(login) 단계에서는 사용자의 접속 시도 시, 1차로 패스워드의 문자열을 비교하여 일치하지 않는 경우 해당 사용자의 접속을 허가하지 않는다. 패스워드의 문자열이 일치할 경우에는 2차적으로 해당 패스워드에 대한 키스트로크 다이나믹스를 미리 구축된 인증 분류기에 투입하여 정상적 사용자의 키스트로크 다이나믹스와의 일치 여부를 판별한 뒤, 키스트로크 다이나믹스 또한 정상적 사용자로 판별된 경우에만 접속을 허가하게 된다.

패스워드의 키스트로크 다이나믹스를 사용한 사용자 인증은 패스워드의 문자열만을 사용한 사용자 인증에 비하여 보안 수준이 한층 강화되는 장점이 있는 반면, 상대적으로 짧은 길이의 문자열에 대한 키스트로크만을 사용함으로써 제 3자의 인증 성공 가능성은 여전히 존재한다. 또한, 최초 접속 시도 시에 정상 사용자로 판별이 되면 이후 접속을 종료할 때까지 해당 사용자의 정상적 사용 여부를 지속적으로 모니터링 하는 것이 불가능하다는 단점을 가지고 있다. 최근 화두가 되고 있는 클라우드 컴퓨팅(cloud computing) 환경이나 스마트 워크플레이스(smart workplace; SWP) 환경에서는 사용자가 장기간 네트워크에 접속하여 업무를 처리하는 상황이 매우 빈번하게 발생한다. 이 때, 최초에는 정상적인 사용자가 접속을 하였으나 비정상적으로 종료하거나 제 3자 혹은 침입자가 중간에 세션(session)을 탈취하여 해당 사용자의 권한을 사용하는 경우 이를 조기에 탐지하는 것이 매우 중요하다고 할 수 있다. 이를 위해서는 네트워크에 접속한 사용자의 행동을 지속적으로 모니터링하고 이를 데이터로 변환하여 수집하는 것이 필수적이다(Zissis and Lekkas, 2010; Subashini and Kavitha, 2011). 자유로운 문자열(long and free texts)의 키스트로크 다이나믹스는 이와 같은

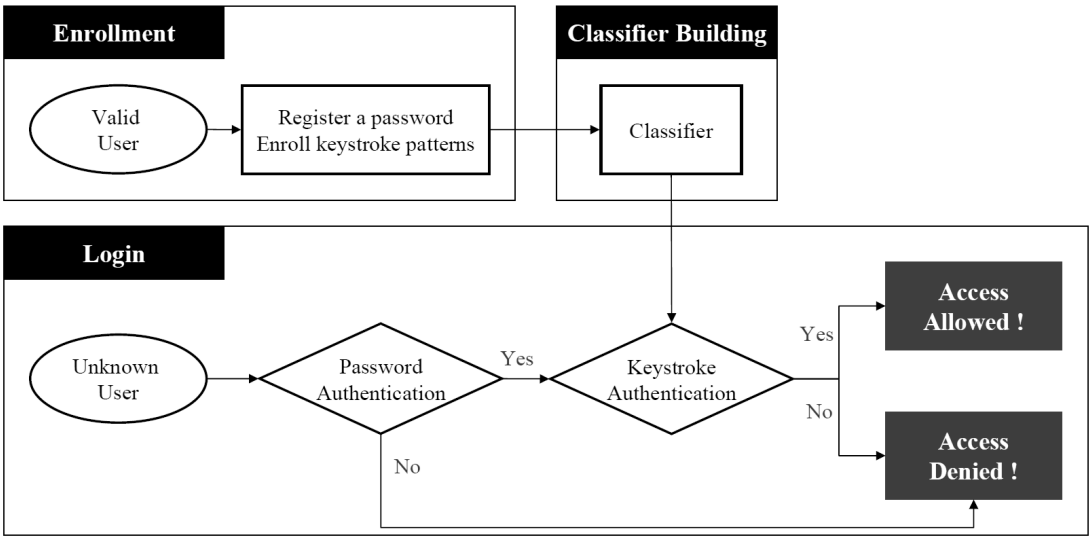


Figure 2. User authentication system based on keystroke dynamics (reprinted from Kang and Cho, 2009)

목적을 달성하기 위한 매우 좋은 도구라고 할 수 있다. 네트워크에 접속한 사용자는 메일 확인, 문서 작업 등을 통하여 지속적으로 타이핑 작업을 수행하기 때문에 간단한 키스트로크 다이나믹스 수집 프로그램을 설치하는 것만으로 네트워크에 접속 중인 사용자의 행동 패턴 모니터링이 가능하기 때문이다.

자유로운 문자열의 키스트로크 다이나믹스를 이용한 사용자 인증에 관련된 연구는 초기 단계라고 할 수 있으며, Filho and Freire(2006)와 Gunetti and Picardi(2005)의 연구가 대표적이다. Filho and Freire(2006)는 키 입력 시간(latency : <Figure 1>의 duration+interval)을 하나의 확률 변수(random variable)로 가정하고 자유로운 문자열 입력 시 발생하는 키 입력 시간의 로그 변환 및 정규 분포 근사를 통해 사용자 인증 성능이 향상될 수 있음을 보여주었다. Gunetti and Picardi(2005)는 키 입력 시간과 입력키의 전후 관계를 고려한 두 사용자 간의 순서 불일치 정도(degree of disorder)를 사용자 인증에 사용하였다. Gunetti and Picardi(2005)가 제안한 'R' 지표는 입력 시간 자체 보다는 상대적 순서의 불일치 정도를 측정하는 데 초점을 두고 있으며, 'A' 지표는 동일한 음절의 입력 시간 비율 차이를 측정하는 데 초점을 두고 있다. 또한 Gunetti and Picardi(2005)는 'R' 지표와 'A' 지표의 선형 결합을 통해 더욱 효과적인 사용자 인증 알고리즘을 구축할 수 있음을 보여주었다. 이를 바탕으로 Hu *et al.*(2007)은 k-인접 이웃 기법을 사용하여 'R' 지표와 'A' 지표의 인증 효율을 향상시키는 시도를 수행하였다.

앞서 언급된 연구들은 초기 단계의 연구로서의 몇 가지 한계점이 존재한다. 첫째, 자유로운 문자열에 대한 연구임에도 불구하고 수집된 키스트로크 다이나믹스 데이터가 충분하지 않은 편이다. Gunetti and Picardi(2005)는 사용자당 약 700~900개의 키 입력 시간을 수집하였으며, Filho and Freire(2006)는 사용자당 약 250개의 키 입력 시간을 수집하여 사용함으로써 다양한 사용자 인증 상황을 가정하기에는 제약이 존재한다. 둘째, 사용자 인증에 사용된 알고리즘의 가정이 매우 엄격하거나(Filho and Freire, 2006) 다수의 파라미터가 존재함으로써 최적화에 어려움이 존재한다(Gunetti and Picardi, 2005). 따라서 본 연구에서는 자유로운 문자열(long and free texts)의 키스트로크 다이나믹스를 활용한 두 가지의 효율적인 사용자 인증 알고리즘을 제안하고, 이를 다양한 사용자 인증 시나리오에 적용하여 그 효과를 비교 · 분석하고자 한다. 이를 위하여 총 35명의 피실험자들로부터 키스트로크 다이나믹스 데이터를 수집하였으며, 세 가지의 대표적인 사용자 인증 시나리오를 설계하였다. 수집된 데이터를 바탕으로 각 시나리오에 대해 제안된 두 가지 인증 알고리즘과 기존 알고리즘과의 비교 분석을 통하여 사용자 인증 성능을 평가하고 그 결과를 바탕으로 시사점을 도출하였다.

본 논문의 구조는 다음과 같다. 제 2장에서는 자유로운 문자열의 키스트로크 다이나믹스를 이용한 두 개의 사용자 인증 방법론이 제안된다. 제 3장에서는 제안된 사용자 인증 알고리즘의 효과를 분석하기 위해 설계된 사용자 인증 시나리오를 포함한 전반적인 실험 환경(데이터 수집, 비교 알고리즘 등)이 소개되며, 제 4장에서는 각 시나리오별 사용자 인증 방법론들의 인증 결과를 비교하고 분석하여 시사점을 도출할 것이다. 마지막으로 제 5장에서는 결론과 함께 본 연구의 한계점을 언급하고 이를 개선하기 위한 향후 연구 방향에 대한 논의를 할 것이다.

2. 자유로운 문자열의 키스트로크 다이나믹스 기반 사용자 인증 방법론

본 연구에서는 기본적으로 키 입력 시간(latency)을 기본적인 측정 단위로 사용한다. 이를 바탕으로 입력키의 전후 관계를 고려하지 않은 Kolmogorov-Smirnov Test 기법과 입력키의 전후 관계를 고려한 'R-A' 지표의 두 가지 사용자 인증 방법론을 제안한다.

2.1 Kolmogorov-Smirnov Score(K-S 스코어)

Kolmogorov-Smirnov Test(이하 K-S Test, Frank and Massey, 1951)는 분석에 사용되는 데이터가 특정 분포로부터 추출되지 않은 경우, 두 집단의 분포 유사성을 측정하는데 널리 사용되는 방법이다. N_1을 정상적 사용자(valid user)의 키 입력 시간의 총 수, N_2를 검증 사용자(test user)의 키 입력 시간의 총 수라고 정의하면 각 사용자의 키 입력 시간 데이터에 대한 경험적 분포 함수(empirical distribution function) F는 다음과 같이 정의될 수 있다.

$$F_{N_1}(x)=\frac{1}{N_1}\sum_{i=1}^{N_1} I(X_i \le x),\ F_{N_2}(x)=\frac{1}{N_2}\sum_{i=1}^{N_2} I(X_i \le x) \tag{1}$$

여기서 X_i는 독립적이고 동일한 분포(i.i.d.; independent and identically distributed)로부터 추출된 확률 변수이고 $I(X_i \le x)$는 지시 함수(indication function)로써 $X_i \le x$이면 1을 반환하고, 그렇지 않은 경우에는 0을 반환한다. 이렇게 정의된 경험적 분포 함수로부터 다음과 같이 K-S 통계량(K-S statistics) 및 K-S 스코어(score)를 계산할 수 있다.

$$\text{K-S 통계량} : D_{N_1,N_2}=sup_x|F_{N_1}(x)-F_{N_2}(x)| \tag{2}$$

$$\text{K-S 스코어} : \Pr\left(K \ge \sqrt{\frac{N_1\times N_2}{N_1+N_2}}\right), \quad =1-\Pr\left(K \le \sqrt{\frac{N_1\times N_2}{N_1+N_2}}\right) \tag{3}$$

$$\Pr(K \le x) = 1-2\sum_{i=1}^{\infty}(-1)^{i-1}e^{2i^2x^2} = \frac{\sqrt{2\pi}}{x}\sum_{i=1}^{\infty}e^{2(i-1)^2\pi^2/(8x^2)} \tag{4}$$

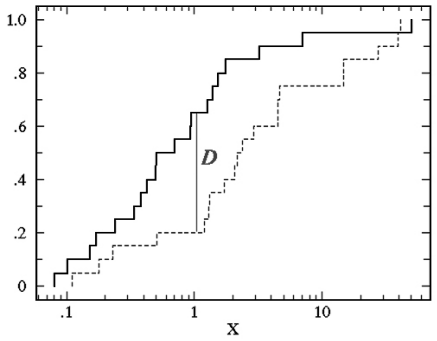


Figure 3. Cumulative Empirical Distribution Functions of Two Data Sets and Their K-S Statistics(x-axis : Data Value, y-axis : Cumulative Probability)

K-S 통계량은 <Figure 3>에서 나타난 바와 같이 두 데이터 집합의 누적 확률 분포 차이의 최대치로써, 두 데이터 집합이 서로 속성이 상이한 분포로부터 추출될수록 값이 크게 나타나게 되며 이 때 K-S 스코어의 값은 감소하게 된다. 키스트로크 다이나믹스를 활용한 사용자 인증에서는 개인별로 독특한 키 입력 시간의 분포를 갖게 되므로 특정한 사용자가 합법적 사용자인지를 판단하기 위해서 해당 사용자의 키 입력 시간 데이터와 검증 사용자의 키 입력 시간 데이터의 K-S 스코어를 산출하여 이 값이 충분히 크면 합법적 사용자로 판단하고 그렇지 않을 경우 잠재적 침입자로 판단하는 인증 시스템을 구축할 수 있다.

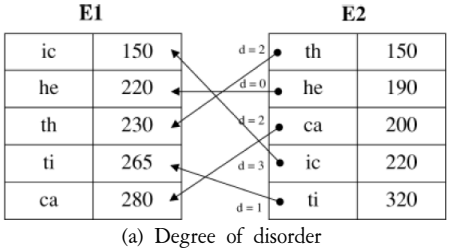
2.2 'R-A' 지표

앞 절에서 설명된 K-S Test는 사용자가 어떠한 키를 입력하는가를 고려하지 않고 모든 키 입력 시간을 1차원적인 분포로 해석하는 방법론이다. 그러나 키스트로크 다이나믹스 데이터를 수집할 경우, 입력키에 대한 정보가 함께 수집되는 것이 일반적이다. 따라서 본 연구에서는 Gunetti and Picardi(2005)가 제안한 'R' 지표와 'A' 지표를 효과적으로 결합하여 입력키에 대한 정보를 함께 고려한 사용자 인증 방법론을 제안한다.

먼저, 'R' 지표와 'A'지표를 계산하는 방법은 다음과 같다. 두 명의 사용자(E1, E2)로부터 <Figure 4>와 같은 키 입력 시간 데이터를 수집했다고 가정하자. 이 데이터를 사용하여 두 사용자가 공통적으로 입력한 음절들을 추출한 뒤, 해당 음절들에 대한 키 입력 시간의 평균을 기준으로 <Figure 5>(a)와 같이 오름차순으로 정리하고 이를 통하여 '순서 불일치 정도(degree of disorder)'를 계산한다.

- E1 : 0 a 180 u 440 t 670 h 890 e 1140 n 1260 t 1480 i 1630 c 1910 a 2010 t 2320 i 2600 o 2850 n
- E2 : 0 t 150 h 340 e 550 o 670 r 990 e 1230 t 1550 i 1770 c 1970 a 2100 l

Figure 4. The Typed Characters and Latencies of Two users E1 and E2 (Gunetti and Picardi, 2005)



(a) Degree of disorder

E1		E2		
280	**ca**	200	(280/200 = 1.400)	
220	**he**	190	(220/190 = 1.157)	(similar pair)
150	**ic**	220	(220/150 = 1.466)	
230	**th**	150	(230/150 = 1.533)	
265	**ti**	320	(320/265 = 1.207)	(similar pair)

(b) Latency similarity

Figure 5. Computing the Degree of Disorder and Latency Similarity between Two Users (Gunetti and Picardi, 2005)

순서 불일치 정도는 공통된 음절의 입력 시간이 개별 사용자의 입력 시간 순서에서 어느 위치를 차지하고 있는가를 비교하는 것으로 <Figure 5>(a)의 예시에서는 다음과 같이 계산된다. 음절 'ic'는 사용자 E1은 가장 빠르게 입력하였고 사용자 E2는 네 번째로 빠르게 입력하였다. 따라서 음절 'ic'에 대한 순서 불일치 정도는 3(= |1-4|)이 된다. 또한 음절 'he'는 사용자 E1과 E2가 모두 두 번째로 빠르게 입력한 음절이므로 순서 불일치 정도는 0이 된다. 이와 같이 모든 음절에 대한 순서 불일치 정도를 산출할 수 있으며, <Figure 5>(a) 예시의 전체 순서 불일치 정도는 8이 된다. 'R' 지표는 식 (5)와 같이 두 사용자 사이에 나타날 수 있는 키 입력 시간의 순서 불일치 정도를 최대 가능 순서 불일치 정도로 나눈 값으로써, <Figure 5>(a)의 예시의 최대 순서 불일치 정도는 12(= $(5^{2-1})/2$)이므로 사용자 E1과 E2의 'R' 지표는 1/3(= 1-8/12)이 된다.

$$\text{'R' 지표} : 1-\frac{\text{degree of disorder}}{\text{max. degree of disorder}} \tag{5}$$

'R' 지표는 각 사용자의 키 입력 시간의 상대적인 순서를 비교하기 때문에, 전반적인 입력 속도는 다르지만 유사한 입력 순서를 나타내는 두 사용자를 구분하기 어렵다는 단점이 있다. 'A' 지표는 이를 보완하기 위해 개발된 것으로써 다음과 같은 절차를 통하여 산출할 수 있다. 우선 'R' 지표 산출에서와 동일하게 두 사용자가 공통적으로 입력한 음절들을 추출한 뒤 식 (6)과 같이 음절 입력 시간의 비율이 특정 수준(θ) 이하인 입력 시간 유사(latency similarity) 음절의 수를 계산한다.

$$A_{count} = \sum_{k=1}^{d} I\left(\frac{\max(X_i^k, X_j^k)}{\min(X_i^k, X_j^k)} \le \theta\right). \tag{6}$$

식 (5)에서 d는 사용자 i와 사용자 j가 공통적으로 입력한 음절의 총 수이고, X_i^k는 사용자 i가 k번째 공통 음절을 입력하는

데 소요되는 평균 시간이며, X_j^k는 사용자 j가 k번째 공통 음절을 입력하는 데 소요되는 평균 시간이고, I는 지시 함수로써 괄호 안의 조건을 만족하면 1을 반환하고 그렇지 않을 경우 0을 반환한다. 'A' 지표는 전체 공통 입력 음절 중, 음절 입력 시간의 비율이 θ 이하인 음절의 비율로써 식 (7)과 같이 계산된다.

$$\text{'A' 지표} : \frac{A_{count}}{d} \tag{7}$$

<Figure 5>(b)의 예시에서 θ를 1.3으로 정의할 경우, 입력시간 유사 음절의 수는 2개가 되고, 'A' 지표는 2/5가 된다. 또한, Gunetti and Picardi(2005)는 'R' 지표와 'A' 지표를 식 8과 같이 선형 결합을 함으로써 음절 간 입력 시간의 상대적인 차이와 절대적인 차이를 동시에 고려하는 것도 가능함을 보였다.

$$(\text{'R' 지표}) + \alpha \times (\text{'A' 지표}) \tag{8}$$

그러나 식 (8)의 형식으로 결합하게 될 경우 결합 가중치 α로 인해 사전적으로 정의가 필요한 파라미터의 수가 증가한다는 단점과 함께 0과 1사이에 존재하는 'R' 지표와 'A' 지표와는 다르게 제안된 지표의 범위는 결합 가중치 α에 영향을 받게 되는 단점이 존재한다. 실제로 Gunetti and Picardi(2005)의 실험 결과, 결합 가중치 α의 값에 따라 사용자 인증 정확도의 변동이 매우 크게 나타나는 것을 확인할 수 있다. 이를 통해 두 지표의 단순 선형 결합은 인증 모델의 일반화 성능을 저하시키는 과적합(over-fitting)의 위험이 큰 방법이라는 것을 확인할 수 있다. 따라서 본 연구에서는 'R' 지표와 'A' 지표의 장점을 동시에 수용함과 동시에 사전적 파라미터를 증가시키지 않고 범위 또한 'R' 지표 및 'A' 지표와의 일관성을 유지할 수 있도록 하기 위하여 선형 결합이 아닌 식 (9)와 같은 형태의 'R-A' 지표를 제안한다.

$$\text{'R-A' 지표} = (\text{'R' 지표}) \times (\text{'A' 지표}) \tag{9}$$

제안된 'R-A' 지표는 'R' 지표와 'A' 지표를 곱함으로써, 선형 결합 시 발생하는 사전 파라미터가 필요하지 않는 장점이 있다. 또한 각각 0과 1 사이의 범위를 갖는 'R' 지표와 'A' 지표에 의해 'R-A' 지표도 역시 0과 1사이에 존재하게 됨으로써 사용자 인증 시 정상적 사용자와 잠재적 침입자를 구분하는 기준을 정립하는 데 있어 사용자 독립적인 기준 수립을 가능하게 한다.

3. 사용자 인증 실험 설계

3.1 데이터 수집

제 2장에서 제안된 자유로운 문자열의 키스트로크 다이나믹스 기반 사용자 인증 알고리즘의 성능을 분석하기 위하여 <Figure 6>과 같은 프로그램을 통하여 키 입력 시간을 수집하였다. 입력 장치로는 개인의 PC 키보드를 사용하였으며, 입력 언어에 따른 인증 성능을 알아보기 위하여 국문 및 영문 두 가지 언어에 대해 피실험자 개별적으로 제공되는 3,500~4,000자의 텍스트를 입력하도록 실험을 설계하였다. 본 연구에서는 사용자의 행동 요인에 의한 인증 성능 분석에 중점을 두기 위하여 입력 기기의 영향력을 최소화 하고자 일반적으로 가장 많이 사용되는 106key 키보드를 이용하여 실험을 수행하도록 권고하였다. 피실험자는 대부분 20대 중반에서 30대 초반 사이의 남녀 대학원생들로서, 34명이 국문 키스트로크 다이나믹스 데이터를 제공하였고, 35명이 영문 키스트로크 다이나믹스 데이터를 제공하였다. 모든 실험에서 키스트로크 다이나믹스 데이터는 한 키를 누른 시점부터 다음 키를 누를 때까지의 시간인 키 입력 시간(latency)을 측정하여 수집하였으며, 특수 문자 및 문장 부호(마침표, 물음표, 쉼표 등)는 키 입력 시간 수집에서 제외하였다. 또한 영문의 경우 26개의 알파벳 키에 스페이스 바 및 백스페이스를 포함한 28개 키의 조합에 대한 입력 시간을 수집하였으며, 국문의 경우 영문 데이터 수집에서 사용된 28개 키에 된소리를 입력하는데 필요한 좌 · 우 시프트 키를 포함하여 30개 키의 조합에 대한 입력 시간을 수집하였다.

Figure 6. Data Collection Program for the Keystroke Dynamics of Long and Free Text

A

	a	b	c
a		50	120
b			100
c	150		

B

	a	b	c
a	80		100
b		70	
c	100		

Figure 7. An Example of Digraph Matrix of Two Users A and B (milliseconds)

3.2 비교 인증 알고리즘 및 성능 평가 지표

제안된 K-S Test와 'R-A' 지표의 사용자 인증 성능을 평가하기 위하여 본 연구에서는 'R-A' 지표의 개별 구성 요소인 'R' 지표와 'A' 지표, 그리고 Bleha *et al.*(1990)이 제안한 알고리즘을 자유로운 문자열 기반으로 확장한 음절 행렬 거리(distance between digraph matrix)의 세 가지 인증 알고리즘을 비교 대상으로 선정하였다. 'R' 지표와 'A' 지표를 산출하는 제 2.2절에 자세히 설명되어 있기 때문에 본 절에서는 음절 행렬 거리를 이용한 사용자 인증 방식을 간단히 설명한다.

사용자로부터 키스트로크 다이나믹스 데이터가 수집되면 시작 키를 행(row)으로 하고 종료 키를 열(column)로 하며, 해당 셀(cell)의 값은 시작 키와 종료 키 사이의 평균 키 입력 시간(latency)으로 구성된 음절 행렬(digraph matrix)을 구축할 수 있다. 예를 들어, 'a', 'b', 'c'의 세 개의 문자로만 구성된 텍스트를 두 사용자 A와 B가 입력할 경우 각 사용자에 해당하는 음절 행렬은 <Figure 7>과 같이 생성될 수 있다. 두 사용자의 음절 행렬 거리는 공통된 음절의 평균 입력 시간의 차이를 측정하는 지표로써, 식 (10)과 같은 형태로 계산될 수 있다.

$$d(A, B) = \sqrt{\frac{1}{|I|}\sum_{(i,j)\in I}(A_{ij}-B_{ij})^2}, \quad I=\{(i, j)|A_{ij}\neq 0, B_{ij}\neq 0\} \tag{10}$$

여기서 I는 두 사용자가 공통적으로 입력한 음절들에 대한 색인 집합이다. <Figure 7>의 예시에서 사용자 A와 B의 음절 행렬 거리는 약 38.08($=\sqrt{\frac{(120-100)^2+(150-100)^2}{2}}$)이 된다. 두 사용자의 키스트로크 다이나믹스가 유사할수록 음절 행렬 거리는 작게 되므로 이를 이용하여 사용자 인증을 수행할 수 있다.

본 연구에서는 자유로운 문자열의 키스트로크 다이나믹스 기반 사용자 인증 알고리즘의 성능 평가 지표로 동등 에러 비율(equal error rate; 이하 EER)을 사용하였다. 사용자 인증에는 두 종류의 오분류(misclassification error)가 존재한다. 누락(false acceptance rate; FAR)은 현재 타이핑을 하고 있는 사용자가 불법적인 사용자임에도 불구하고 이를 탐지하지 못하고 정상 사용자로 인식하는 오류이며, 오경보(false rejection rate; FRR)는 현재 타이핑을 하는 사용자가 정상적인 사용자임에도 불구하고 잠재적 침입자로 잘못 탐지하는 오류이다. 누락과 오경보는 한쪽을 감소시키기 위해서는 필연적으로 다른 쪽이 증가하는 대립 균형(trade-off) 관계에 있다. 이는 알고리즘의 인증 기준(threshold)을 어떻게 정하느냐에 따라 누락과 오경보의 수치가 변화하게 됨을 의미하므로, 본 연구에서는 인증 기준에 독립적인 성능 평가 지표인 EER을 사용하였다. EER은 <Figure 8>에서 나타난 바와 같이 누락과 오경보의 비율이 동일해지는 지점으로써, EER이 낮을수록 우수한 인증 알고리즘이라고 평가할 수 있다.

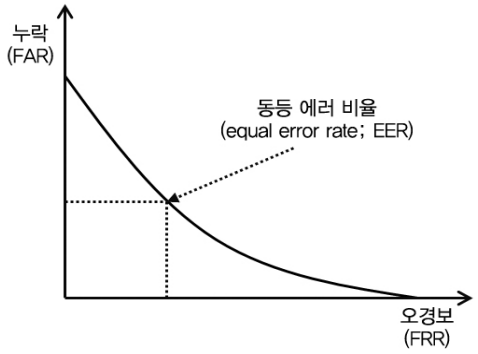


Figure 8. Equal error rate

최종적으로 본 연구에서는 두 개의 제안된 인증 알고리즘과 세 개의 비교 알고리즘을 포함하여 총 다섯 개의 인증 알고리즘을 사용하여 키스트로크 다이나믹스 기반 사용자 인증을 수행하였다. K-S Test는 시작 키와 종료 키의 문자 정보를 고려하지 않는 1차원의 키 입력 시간을 사용한 인증 알고리즘이며, 'R' 지표, 'A' 지표, 'R-A' 지표 및 음절 행렬 거리는 시작 키와 종료 키의 문자 정보를 고려한 2차원 음절 행렬에 기반한 인증 알고리즘이다. 이 중, 'A' 지표와 'R-A' 지표의 경우 음절 입력 시간 비율의 유사도를 판별하기 위한 사전 파라미터 θ의 설정이 필요하며, 본 연구에서는 1.0부터 1.5까지 0.1단위로 'A' 지표의 성능을 평가한 후 최종적으로 1.3을 θ의 최종 값으로 사용하였다. Gunetti and Picardi(2005)에 의해 제안된 'R' 지표와 'A' 지표의 선형 결합은 선형 조합 파라미터에 따라 인증 결과의 변동성이 매우 높게 나타나기 때문에 실제 인증 모델 구현에 사용하기에는 적절하지 못한 것으로 판단되어 본 연구의 비교 대상에서는 제외하였다.

Table 1. User Authentication Scenarios Based on Keystroke Dynamics

시나리오	테스트 문자열의 길이	예상 환경
1	Short, 2~3문장	메신저 대화 시도, 짧은 이메일 작성
2	Medium, 1~2문단	일상적인 메신저 대화 및 일반적인 이메일 작성
3	Long, 1페이지 이상	일반적인 문서 작업

Table 2. The Number of Keystrokes in Reference and Test Sets and the Number of Authentication Data Sets

시나리오	테스트 집합 키스트로크 횟수	참조 집합 키스트로크 횟수	인증 데이터 세트 수 (세트 당 N-1개의 정상 및 침입자 데이터)
1	100	100	25
		500	21
		1,000	16
2	500	500	17
		1,000	12
3	1,000	1,000	7

3.3 사용자 인증 시나리오

본 연구에서는 다양한 키스트로크 다이나믹스 기반 사용자 인증 환경을 테스트하기 위하여 사용자 인증에 사용되는 테스트 문자열의 길이에 따라 <Table 1>과 같이 세 가지의 시나리오를 설계하고 각 시나리오에 대해 참조 문자열의 길이에 따른 사용자 인증 성능을 평가하였다. 먼저 키스트로크 다이나믹스를 활용한 사용자 인증 상황은 테스트 문자열의 길이, 즉 현재 타이핑을 하고 있는 사용자가 정상적 사용자인지 비정상 사용자인지를 판별하기 위해 제공되는 키스트로크 다이나믹스 데이터의 양에 따라 크게 세 가지로 구분할 수 있다.

첫 번째 상황은 매우 짧은 2~3문장만을 입력하는 경우로써, 메신저의 대화 시도 및 짧은 이메일 답장 등이 이에 포함된다. 실제로도 메신저의 계정 정보를 탈취한 뒤 금전적인 도움을 요청하는 메신저 피싱의 피해 사례가 급증하고 있는 상황이며, 초기에 짧은 키스트로크 다이나믹스 데이터를 가지고 해당 사용자의 정상 여부를 판별할 수 있게 될 경우, 이러한 피해가 크게 감소할 것으로 기대할 수 있다. 두 번째 상황은 약 1~2문단에 해당하는 문자열을 입력하는 상황으로써, 일정 수준 이상의 메신저 대화나 일반적인 이메일 작성 등이 이에 해당한다. 이는 사용자가 최초에 정상적으로 시스템에 접속했을지라도 중간에 메신저 로그아웃을 하지 않거나 잠시 자리를 비운 사이 제 3자에 의해 계정이 사용되는 상황으로 가정할 수 있다. 마지막 상황은 매우 긴 문자열을 지속적으로 입력하는 상황으로써, 일반적인 문서 작업이 이에 해당한다고 할 수 있다. 최근 클라우드 컴퓨팅(cloud computing) 개념이 도입되면서 서버에 모든 프로그램과 데이터를 저장한 상태로 언제 어디서나 네트워크에 접속하여 작업을 수행할 수 있는 스마트 워크플레이스(smart workplace; SWP) 환경이 점차 구축되고 있다. 이러한 클라우드 컴퓨팅 환경에서는 사용자가 일반적으로 장기간 시스템에 접속하여 여러 가지 업무를 수행하게 되는데, 세 번째 시나리오는 이러한 상황에서의 사용자 인증 및 모니터링 환경을 모사한 것이라고 할 수 있다.

<Table 1>에서 설정된 세 가지 시나리오를 구현하기 위하여 개인별로 수집된 키스트로크 다이나믹스 데이터를 다음과 같은 방식으로 인증 모델 구축 데이터와 인증 테스트 데이터로 구분하였다. 첫째, 각 시나리오에 대응하는 인증 모델 구축 키스트로크(키 입력 시간) 횟수는 각각 100, 500, 1,000회로 가정하였다. 둘째, 인증 테스트 키스트로크의 횟수는 인증 모델 구축 키스트로크 횟수보다 적거나 같다고 가정하고 Table 2에 나타난 조합에 대한 사용자 인증 성능 평가를 수행하였다. 마지막으로 N명의 사용자에 대해 각각 (N-1)개의 본인 키스트로크 데이터와 나머지 (N-1)명의 잠재적 침입자 키스트로크 데이터를 하나의 인증 세트로 구성하였으며, 인증 모델 구축과 인증 테스트 키스트로크 횟수에 따른 전체 인증 세트의 수는 <Table 2>에 나타난 바와 같다. 예를 들어 국문 타이핑을 하는 시나리오 1에서 500회의 키스트로크를 사용하여 인증 모델을 구축하고 100회의 키스트로크를 사용하여 사용자 인증을 수행하는 경우, 실험자 1의 첫 번째 인증 세트에서는 본인의 최초 500회의 키스트로크가 인증 모델 구축 데이터로 사용한다. 또한 사용자 인증을 위해 501개 이후의 키스트로크의 길이를 100회로 고정시킨 상태로 10회 단위로 이동하여(501~600, 511~610, 521~620 등) 생성된 총 33개의 정상 사용자 데이터 세트와 본인을 제외한 나머지 33명의 501번째부터 600번째 키스트로크를 잠재적 침입자 데이터로 정의하여 총 33개의 잠재적 침입자 데이터 세트로 구성된 인증 데이터 1세트가 구성된다. 두 번째 인증 세트에서는 본인의 101회~600회의 키스트로크가 인증 모델 구축 데이터로 사용되며, 601개 이후의 키스트로크에 대해 생성된 총 33개의 정상 사용자 데이터 세트와 본인을 제외한 나머지 33명의 601번째부터 700번째 키스트로크를 추출한 잠재적 침입자 데이터 세트를 사용한다.

4. 사용자 인증 실험 결과

국문 및 영문의 자유로운 문자열을 입력할 때 수집된 키스트로크 다이나믹스를 이용한 다섯 가지의 사용자 인증 알고리즘의 평균 EER은 각각 <Table 3>과 <Table 4>에 나타나 있으며 각 시나리오의 테스트 키스트로크와 참조 키스트로크 횟수 조합에 대해 가장 낮은 EER은 밑줄과 함께 굵게 표시하였다. <Table 3>과 <Table 4>를 바탕으로 자유로운 문자열 기반 사용자 인증 알고리즘 성능 평가를 통해 다음과 같은 결과를 추론할 수 있다.

첫째, 키스트로크 다이나믹스는 입력 언어에 크게 영향을 받지 않는 개인의 고유한 행동 속성임을 다시 한 번 확인할 수 있다. <Table 3>과 <Table 4>의 수치에서 알 수 있듯이 테스트 및 참조 키스트로크의 횟수가 동일할 경우, 각 인증 알고리즘은 국문과 영문 두 가지 언어에 대해 유사한 인증 성능을 나타내고 있다. 이를 통하여 키스트로크 다이나믹스는 입력 언어와는 독립적인 개인의 고유한 행동 기반 생체 정보이며, 이를 통하여 2차 인증 시스템을 구축하는 것이 효과적이라는 결론을 내릴 수 있다. 둘째, 음절 행렬 거리를 이용한 사용자 인증은 나머지 인증 알고리즘에 비하여 상대적으로 낮은 인증 성능을 나타내고 있음을 알 수 있다. 상대적으로 인증이 가장 어려운 상황인 100회의 참조 키스트로크와 100회의 테스트 키스트로크 조합에서 음절 행렬 거리 알고리즘은 40.48%(국문)과 36.84%(영문)의 EER을 나타냄으로써, 두 번째로 낮은 성능을 보이는 'R' 지표(28.64%(국문), 28.65%(영문)) 대비 각각 11.76%p, 8.19%p나 인증 오분류율이 증가하는 것으로 나타나고 있다. 셋째, 음절 행렬 거리를 제외한 나머지 네 가지의 인증 알고리즘들은 EER의 측면에서 유사한 양상을 보이고 있음을 알 수 있다. 이는 테스트 키스트로크의 횟수와 참조 키스트로크의 횟수가 증가할수록 EER은 크게 감소하는 경향으로써, 특히 참조 키스트로크 횟수가 고정인 상태에서 테스트 키스트로크의 횟수를 증가시킬 때 더욱 뚜렷하게 나타난다. 예를 들어 K-S Test의 경우 참조 키스트로크의 수를 1,000회로 고정시키고 테스트 키스트로크가 100, 500, 1,000인 경우를 살펴보면 EER이 각각 13.64%, 4.25%, 2.36%로써 급격하게 감소하는 것을 확인할 수 있다.

Table 3. Authentication Performance in Terms of EER When Users Typed in Korean

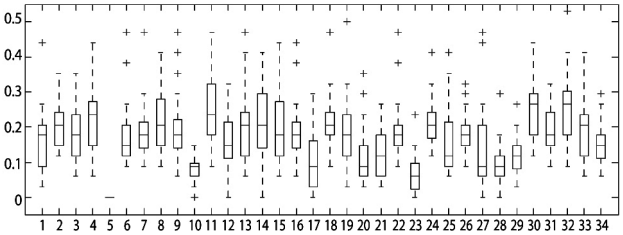
시나리오	테스트 키스트로크	참조 키스트로크	'R' 지표	'A' 지표	음절행렬 거리	K-S Test	'R-A' 지표
1	100	100	28.64	24.45	40.48	**17.18**	22.80
		500	22.61	17.65	39.18	**13.88**	15.80
		1,000	20.73	16.08	39.19	**13.64**	13.89
2	500	500	9.47	7.44	34.70	**5.28**	5.33
		1,000	7.38	4.86	35.75	4.25	**3.27**
3	1,000	1,000	3.57	2.72	32.69	2.36	**1.54**

Table 4. Authentication Performance in Terms of EER When Users Typed in English

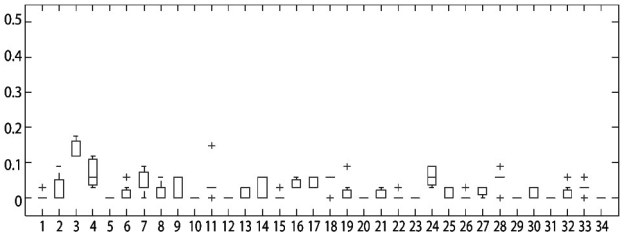
시나리오	테스트 키스트로크	참조 키스트로크	'R' 지표	'A' 지표	음절행렬 거리	K-S Test	'R-A' 지표
1	100	100	28.65	22.69	36.84	**17.23**	21.02
		500	20.66	16.96	36.07	15.37	**14.38**
		1,000	19.47	17.47	35.27	14.99	**13.93**
2	500	500	7.36	6.38	27.71	6.72	**4.22**
		1,000	6.08	4.78	27.37	6.19	**3.12**
3	1,000	1,000	3.30	2.93	24.85	4.23	**1.72**

마지막으로, 각 시나리오별로 인증 알고리즘의 성능을 비교해보면 테스트 및 참조 키스트로크의 횟수가 짧을수록 K-S Test가 효과적이며, 테스트 및 참조 키스트로크의 횟수가 증가할수록 'R-A' 지표가 효과적임을 알 수 있다. 국문의 경우 시나리오 1에서는 참조 키스트로크의 횟수에 관계없이 K-S Test가 가장 우수한(낮은) EER을 나타내고 있음을 <Table 3>으로부터 확인할 수 있다. 또한 시나리오 2에서는 참조 키스트로크가 500회일 경우에는 K-S Test가 가장 우수한 성능을 나타내고 있으며 참조 키스트로크의 횟수가 1,000회로 증가하면서 'R-A' 지표가 가장 우수한 성능을 나타낸다. 마지막으로 시나리오 3에서는 'R-A' 지표가 1.54%라는 매우 낮은 EER을 나타내면서 다섯 가지 사용자 인증 알고리즘 중에서 가장 우수한 성능을 나타내는 것을 확인할 수 있다. 이는 다음과 같은 원인으로 인해 발생하는 결과라고 할 수 있다. 참조 및 테스트 키스트로크 횟수가 적을 경우에는 'R-A' 지표에서 사용하는 공통 음절의 수가 많지 않을뿐더러, 공통 음절간 입력 시간의 평균 또한 대표성을 지니기 힘들다. 반면에 입력하는 키의 선후관계를 고려하지 않고 키 입력 시간만을 1차원 데이터로 사용하는 K-S Test의 경우에는 상대적으로 개인의 속성을 파악할 수 있는 정보가 충분히 축적되어 있기 때문에 K-S Test의 인증성능이 'R-A' 지표의 인증 성능보다 높게 나타나게 된다. 반면에 테스트 및 참조 키스트로크의 횟수가 증가하면 'R-A' 지표에서 요구하는 정보량을 어느 정도 충족하게 되며, 이를 통해 입력하는 키의 선후관계를 고려하는 기법의 장점이 발현되어 K-S Test보다 우수한 성능을 나타내는 것으로 추론할 수 있다.

<Figure 9>는 국문 입력 시 테스트 키스트로크 100회, 참조 키스트로크 100회일 때의 실험자별 EER과 테스트 키스트로크 1,000회, 참조 키스트로크 1,000회일 때의 실험자별 EER을 상자그림으로 도시한 것이다. 테스트 및 참조 키스트로크 횟수가 상대적으로 적을 경우에는 실험자에 따라서 EER의 산포도가 크게 분포하는 것을 볼 수 있다(<Figure 9>(a) 참조). EER이 0%로 나타나는 5번 실험자를 제외한 나머지 실험자들의 EER의 평균은 약 10%에서 20% 사이에 위치하며 인증 세트에 따라 EER의 변화가 상대적으로 큰것을 확인할 수 있다. 반면, 테스트 및 참조 키스트로크 횟수가 충분할 경우에는 3번 실험자를 제외한 모든 실험자들의 EER이 10% 이하를 나타내며, 8명의 사용자는 0%의 EER을 보임으로써 키스트로크 다이나믹스를 이용하여 타인으로부터 본인을 완벽하게 구분할 수 있다는 것을 보여주고 있다(<Figure 9>(b) 참조). 또한 테스트 및 참조 키스트로크의 수가 커질수록 실험자들의 EER 분포가 좁혀지는 것 또한 확인할 수 있다.

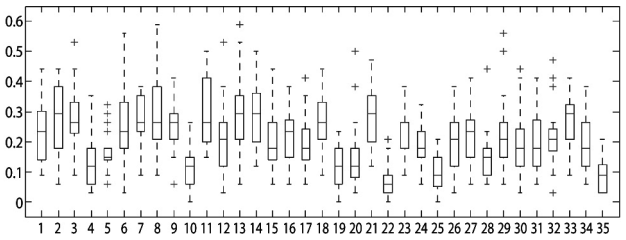


(a) Test keystrokes : 100, reference keystrokes : 100(x-axis : subject ID, y-axis : EER(%))

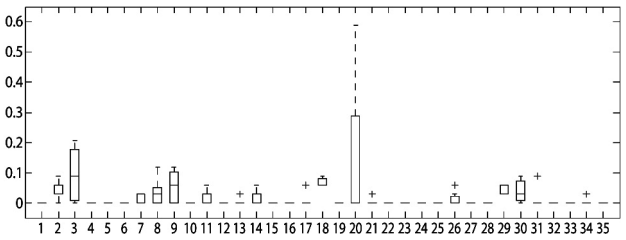


(b) Test keystrokes : 1,000, reference keystrokes : 1,000(x-axis : subject ID, y-axis : EER(%))

Figure 9. Authentication Performance of Each User with K-S Test (Korean)



(a) Test keystrokes : 100, reference keystrokes : 100(x-axis : subject ID, y-axis : EER(%))



(b) Test keystrokes : 1,000, reference keystrokes : 1,000(x-axis : subject ID, y-axis : EER(%))

Figure 10. Authentication Performance of Each User with R-A Score(English)

<Figure 10>은 영문 입력 시 테스트 키스트로크 100회, 참조 키스트로크 100회일 때의 실험자별 EER과 테스트 키스트로크 1,000회, 참조 키스트로크 1,000회일 때의 실험자별 EER을 상자 그림으로 도시한 것이다. <Figure 10>으로부터 우리는 다음과 같이 <Figure 9>에서와 유사한 사항들을 확인할 수 있다. 첫째, 언어 및 인증 알고리즘이 다를 경우라도 테스트 및 참조 키스트로크 횟수가 적으면 실험자에 따른 EER의 분포가 넓게 퍼져 있는 것을 확인할 수 있다(<Figure 10>(a) 참조). 특히, 'R-A' 지표는 입력키의 전후 관계를 고려하는 알고리즘으로써, 충분하지 않은 수의 키스트로크 데이터를 바탕으로 인증을 하는 경우에는, 실험자에 따라 EER의 변동 폭이 K-S 스코어에 비해 크게 나타나게 된다. 둘째, 테스트 및 참조 키스트로크의 수가 충분할 경우 실험자들의 평균 EER은 급격히 감소하는 것을 확인할 수 있다. 특히, 입력키의 전후 관계에 대한 정보가 충분히 반영되는 시나리오 3(<Figure 10>(b) 참조)의 경우, 절반이 넘는 18명의 실험자가 0%의 EER을 나타내고 있으며, 실험자들의 평균 EER의 감소폭 또한 K-S 스코어에 비해 크게 나타나는 것을 알 수 있다.

본 연구의 실험 결과가 시사하는 바는 다음과 같이 요약될 수 있다. 첫째, 키스트로크 다이나믹스는 입력 언어에 관계없는 개인의 고유한 행동 패턴으로써, 사용자 인증에 효과적으로 사용될 수 있는 속성임이 입증되었다. 둘째, 제안된 K-S 스코어와 'R-A' 지표는 자유로운 문자열의 키스트로크 다이나믹스 기반 사용자 인증을 효과적으로 수행할 수 있음이 입증되었다. 특히 키스트로크 데이터의 수가 부족한 환경에서는 K-S 스코어가 보다 적합한 방법론이며, 충분한 키스트로크 데이터가 수집될 경우에는 'R-A' 지표가 매우 우수한 인증 성능을 나타내는 것으로 확인되었다. 마지막으로, 사용자는 본인의 고유한 키스트로크의 속성을 소유하고 있기 때문에, 적용 알고리즘에 대한 개인별 사용자 인증 성능에는 차이가 존재한다는 것을 확인하였으며, 이는 추가 연구를 통하여 사용자별 최적화가 필요한 부분이라고 할 수 있다.

5. 결론 및 향후 연구 방향

본 연구에서는 자유로운 문자열을 입력할 때 발생하는 키스트로크 다이나믹스 데이터를 사용하여 사용자 인증을 수행하는 두 가지 알고리즘을 제안하였다. K-S 스코어는 두 데이터 분포의 경험적 누적 분포 함수 차이의 최대치를 사용하여 두 분포의 동일성을 측정하는 지표이며 'R-A' 지표는 입력키의 전후 관계를 고려한 입력 속도의 상대적 순서 및 비율을 함께 고려한 지표이다. 제안된 두 알고리즘의 인증 성능을 평가하기 위하여 총 34명의 실험자로부터 3,000자 이상의 국문 키스트로크 데이터를 수집하였으며, 35명의 실험자로부터 3,000자 이상의 영문 키스트로크 데이터를 수집하였다. 또한 세 가지의 시나리오를 설계하고 세 개의 기존 인증 알고리즘과의 비교를 통하여 제안된 K-S 스코어는 참조 및 테스트 키스트로크 횟수가 상대적으로 적을 경우 매우 효과적인 인증 방법론이며, 'R-A' 지표는 참조 및 테스트 키스트로크 횟수가 상대적으로 충분할 경우 우수한 인증 성능을 나타내는 것을 실험적으로 입증하였다.

본 연구는 자유로운 문자열의 키스트로크를 활용한 사용자 인증 방법론을 개발하고 그 효과를 분석하는데 의의가 있으며, 본 연구 결과를 통해 추후 진행되어야 할 향후 연구 방향은 다음과 같다. 첫째, 본 연구에서는 입력 기기로 PC의 키보드만을 고려하였다. 그러나 최근 스마트폰 및 스마트 패드의 보급이 급속하게 진행되고 있으며 시간과 공간의 제약이 없이 언제 어디서나 네트워크에 접속이 가능한 유비쿼터스 환경에서는 다양한 입력 기기로부터 입력된 자유로운 문자열 기반 키스트로크 다이나믹스를 활용한 사용자 인증 방법론에 대한 연구가 필요하다고 할 수 있다. 둘째, 본 연구에서 제안된 K-S 스코어와 'R-A' 지표는 자유로운 문자열의 키스트로크 다이나믹스에서 추출 가능한 속성의 일부분만을 고려한 인증 알고리즘이다. 따라서 자유로운 문자열의 키스트로크 다이나믹스에 대한 보다 다양한 특성을 고려한 속성 추출 및 인증 알고리즘 개발이 진행되어야 할 것이다. 셋째, 키스트로크 다이나믹스는 개인의 고유한 속성으로써, 인증 알고리즘 및 활용 데이터의 규모에 따라 인증 성능이 크게 좌우된다. 따라서 키스트로크 다이나믹스의 속성 분석을 통해 해당 사용자에게 최적의 인증 알고리즘 및 데이터의 규모를 예측할 수 있는 방법론에 대한 연구가 필요할 것이다. 마지막으로, 본 연구에서는 사용자의 키스트로크 다이나믹스가 변하지 않는 것으로 가정하였으나, 실제로 개인의 키스트로크는 점진적으로 변화할 가능성이 존재한다. 따라서 이러한 속성의 변화를 고려한 증가 학습(incremental learning)에 대한 연구도 수행되어야 할 것이다.

참고문헌

Bleha, S., Slivinsky, C., and Hussien, B. (1990), Computer-access Security Systems using Keystroke Dynamics, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **12**(12), 1217-1222.

Chen, W. and Chang W. (2004), Applying Hidden Markov Models to Keystroke Pattern Analysis for Password Verification, *Proc. 2004 IEEE Int. Conf. on Information Reuse and Integration*, 467-474.

Crawford, H. (2010), Keystroke Dynamics : Characteristics and Opportunities, *Proc. Int, Conf. on Privacy, Security, and Trust*, 205-212.

Filho, J. R. M. and Freire, E. O. (2006), On the Equalization of Keystroke Timing Histograms, *Pattern Recognition*, **27**(13), 1440-1446.

Frank, J. and Massey, Jr. (1951), The Kolmogorov-Smirnov Test for Goodness of Fit, *Journal of the American Statistical Association*, **46**(253), 68-78.

Furnell, S. and Clarke, N. (2005), Biometrics : No Silver Bullets, *Computer Fraud and Security*, **2005**(8), 9-14.

Giot, R., Hemery, B., and Rosenberger, C. (2010), Low Cost and Usable Multimodal Biometric System based on Keystroke Dynamics and 2D Face Recognition, *Proc. Int. Conf. on Pattern Recognition*, 1128-1131.

Gunetti, D. and Picardi, C. (2005), Keystroke Analysis of Free Text, *ACM Transaction on Information System Security*, **8**(3), 312-347.

Hosseinzadeh, D. and Krishnan, S. (2008), Gaussian Mixture Modeling of Keystroke Patterns for Biometric Applications, *IEEE Transactions on Systems, Man, and Cybernetics-Part C : Applications and Reviews*, **38**(6), 816-826.

Hu, J., Gingrich, D., and Sentosa, A. (2007), A k-Nearest Neighbor Approach for User Authentication through Biometric Keystroke Dynamics, *Proc. 2007 IEEE Int. Conf. on Communications*, 1156-1560.

Jain, A. K., Bolle, R., and Pankanti, S. (1999), *Biometrics : Personal Identification in Networked Society*, Kluwer, Massachusetts, USA.

Kang, P. and Cho, S. (2009), A Hybrid Novelty Score and Its Use in Keystroke Dynamics-based User Authentication, *Pattern Recognition*, **42**(11), 3115-3127.

Kang, P., Park, S., Hwang, S., Lee, H., and Cho, S. (2008), Improvement of Keystroke Data Quality through Artificial Rhythms and Cues, *Computers and Security*, **27**(1-2), 3-11.

Monrose, F., Reither, M. K., and Wetzel, S. (2002), Password Hardening based on Keystroke Dynamics, *International Journal of Information Security*, **1**(2), 69-83.

Monrose, F. and Rubin, A. D. (2000), Keystroke Dynamics as a Biometric for Authentication, *Future Generation Computer Systems*, **16**(4), 351-359.

Peacock, A., Ke, X., and Wilkerson, M. (2004), Typing Patterns : A Key to User Identification, *IEEE Security and Privacy*, **2**(5), 40-47.

Prabhakar, S., Pankanti, S., and Jain, A. K. (2003), Biometric Recognition : Security and Privacy Concerns, *IEEE Security and Privacy*, **1**(2), 33-42.

Sheng, Y., Phoha, V. V., and Rovnyak, S. M. (2005), A Parallel Decision Tree-based Method for User Authentication based on Keystroke Patterns, *IEEE Transactions on Systems, Man, and Cybernetics-Part B : Cybernetics*, **35**(4) 826-833.

Sinthupinyo, S., Roadrungwasinkul, W., and Chantan, C. (2009), User Recognition via Keystroke Latencies using SOM and Backpropagation Neural Network, *Proc. Int. Joint Conf. on Institute of Control, Robotics, and Systems (ICROS) and Society of Instrument and Control Engineers (SICE)*, 3160-3165.

Subashini, S. and Kavitha, V. (2011), A Survey on Security Issues in Service Delivery Models of Cloud Computing, *Journal of Network and Computer Applications*, **34**(1), 1-11.

Yager, N. and Dunstone, Y. (2010), The Biometric Menagerie, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **32**(2), 220-230.

Yan, J., Blackwell, A., Anderson, R., and Grant, A. (2004), Password Memorability and Security : Empirical Results, IEEE Security and Privacy, **2**(5), 25-31.

Zhang, Y., Chang, G., Liu, L., and Jia, J. (2010), Authenticating User's Keystroke based on Statistical Models, *Proc. 4th Int. Conf. on Genetic and Evolutionary Computing*, 578-581.

Zissis, D. and Lekkas, D. (2010), Addressing Cloud Computing Security Issues, *Future Generation Computer Systems* doi:10.1016/j.future.2010.12.006.

강 필 성

서울대학교 산업공학과 학사
서울대학교 산업공학과 박사
현재 : 서울과학기술대학교 글로벌융합 산업공학과 조교수
관심분야 : 데이터마이닝/기계학습 알고리즘 및 산업 응용

조 성 준

서울대학교 산업공학과 학사
University of Washington 컴퓨터공학 석사
University of Maryland 컴퓨터공학 박사
관심분야 : 데이터마이닝, 텍스트마이닝, 기계학습