出國報告（出國類別：其他--學術交流）

2015 ICCSS 資料性和控制論的計算社會系統國際會議出席報告

服務機關：國立雲林科技大學資訊管理系
姓名職稱：施東河教授
派赴國家：中國大陸
報告日期：104 年 09 月 01 日
出國期間：104 年 08 月 12 日至 104 年 08 月 16 日

摘要

本次出國係參加由澳門大學所籌辦之資料性和控制論的計算社會系統（ICCSS）國際會議，職並於會中進行研究論文發表。參加研討會期間，聆聽與會學者研究論文發表並與中國大陸、香港、匈牙利、加拿大、美國等地與會學者交流，職發表的研究論文爲”移動設備上的一個輕擊生物驗証機制”，並與各地學者交換心得與研究方法實驗修正，另旁聽其他相關領域之優秀論文發表，交換研究心得與投稿方式，並加強與中國大陸、香港、匈牙利、加拿大、美國等地大學院校間的學術交流與未來的合作可能，相約投稿明年之研討會，以期能有更進一步之學術交流。

目次

一、目的

資料性和控制論的計算社會系統（ICCSS）國際會議自舉辦以來，已漸受計算機科學專家學者科學家之重視，許多從計算機，教育和控制領域之國際知名專家和 IEEE 院士皆曾經出席本會議。特邀嘉賓和參與者包括很多從研究和眾多知名國內外機構與高等院校來的專家，學者，科學家，技術人員和工程師。這些皆使得 ICCSS 國際會議成爲國際學術交流的良好平台。爲此， ICCSS 已成爲已經上市的“在線中國學術會議”優秀的研討會之一，所有會議報告都成爲“在線中國學術會議”收集的來源。資料性和控制論的計算社會系統（ICCSS 2015 年）國際會議，於 2015 年 8 月 13 日至 15 日在中國成都市四川大學望江校區舉行。ICCSS 2015 年的論文集將由 IEEE 出版，並進入 IEEE Xplore 的數據庫圖書館，並收錄於 EI 資料庫。職本次出國即是參加由澳門大學所籌辦之資料性和控制論的計算社會系統（2015 ICCSS）國際會議，除於會中進行研究論文發表外亦期盼與其他研究學者及新加入的學會會員相互認識，以冀日後能有進一步學術合作的機會並達到國際交流之目的。2015 資料性和控制論的計算社會系統國際會議，匯集了那些積極參與計算社會制度，控制論和信息處理的國際論壇，最先進的國家創新和發展報告，並在社會制度，計算，控制論和信息處理的各個方面交換意見和進步,其貢獻涵蓋理論發展和實際應用，它包括以下技術領域：計算社會制度，社會計算，社交網絡分析和網頁挖掘，數據挖掘和機器學習，數據分析和數據可視化，控制論和系統科學，智能系統，集體智慧，計算智能，位置和支撐位置智能，信號和圖像處理，小波多分辨率和信息處理，信息安全，模式識別和計算機視覺，機器人系統，服務體系和組織，智能傳感器網絡，系統建模與控制技術評估。

二、過程

會議第一天

104 年 08 月 13 日，由飯店搭計程車前往會議舉行地點成都市四川大學望江校區，辦理報到與註冊等手續，領取 2015 ICCSS 論文集，並參加由 ICCSS 主辦之相關活動。由於本次會議簽證較嚴格，又適逢歐美大學開學季，部分學者未能及時報到參與，因此今早活動略爲冷清。

下午第一場(1:30PM-3:00PM)，聆聽 2 場學者發表他们的研究論文，分別爲: 郭齊 (中國傳播大學)，講題爲立體的錄像的自動水準的調整的研究，由於全世界立體電影受歡迎" 化身 "，立體的錄像已經成爲工業的焦點，以及大大促進立體的錄像的發展。現下在市場上，立體的錄像投搖籃頭透過觀察水準尺的變化使主要的水準面透過獨立的球形門柄的手工底座和三腳架的腿。如果三腳架不夠穩定，錄像位置和角度將改變。文章是關於投搖籃頭的立體的錄像的自動調整。收集的信號將透過 A/D 轉換模板傳送，三軸加速表作爲收集位置和姿態數據的模件在搖籃勞動上安裝。王董(濟南大學)，講題爲用多個場所預言蛋白質亞細胞的地方化的一種新的特徵熔化方法，這篇文章爲蛋白質亞細胞的多個場所的地方化預言提議一種新的特徵熔化方法。幾類特徵被用於這種新的蛋白質編碼法。第一個是氨基酸的組成。第二個是假的氨基酸組成，這主要按照蛋白質順序選出每氨基酸殘渣的單元訊息。最後，氨基酸本地順序的訊息被在這研究過程中考慮。通常，k 最近鄰近演算法，支援向量機和其他方法，使用在蛋白質亞細胞的地方化預測領域。在作者的研究過程中，多標籤的 k 最近鄰近演算法受雇於分類模型。總體的準確比率可以在數據集裡達到 66.73%。二位學者分別對研究與未來發展作陳述，惟發表的論文與本人之研究有落差, 欲延伸深入研究之機會並不大。第二場(3:30PM-5:00PM)，由本人進行論文發表，論文的題目爲”移動設備上的一個輕擊生物驗証機制”，智慧型手機現下不僅爲通訊而且有很多新興的應用，例如行動商務被使用。而，生物驗証方法能提供安全的驗証。在這篇論文裡，我們使用從智慧型手機的加速表傳感器和觸摸屏收集的訊息提議一個新的生物驗証機制。我們設計了從採用從那些改變的特徵的一個驗証機製。實驗結果顯示被提議的生物驗証能爲智慧型手機用戶建造一種堅固的驗証環境。主持

人與會學者皆給予建議與討論，在討論中，獲得相當多的寶貴建議，並相約是否有合作研究的空間。

會議第二天

104 年 08 月 14 日，早上 08:45-12:00 聆聽 3 場論文演講，第一場爲泰國曼谷先皇技術學院 Chanawee Chanavaltada，講題爲推薦系統的改進-透過協同過濾法找到適當的徵人候選人，徵人給機構化性能影響相當多。徵人者期望爲合適的工作見到最合適的雇員，但是許多簡歷對他們的決定更難做。因此，這篇論文提議推薦系統在決定過程中支援徵人者並且管理徵人。兩種技術包括相配和合作的過濾。在符合過程裡，爲了排列那些候選人，它比較外形數據並且採取一個得分。不過，贏得保持候選人得分是低的散佈的一些問題。因此，合作的過濾技術用來解決贏的問題。結果顯示得分調整區別，合作過濾能改進和容易鑑定最適當候選人。第二場爲朝鮮電子技術研究所 Hyoseok Yoon，講題爲立即的弗裡克察覺和漂亮的遙遠合作系統的自動決定，在遙遠嚴厲的合作應用裡，分享在一個本地場所和交往的遙遠參加者之間的無縫和一致的訊息必要。當不一致的直觀訊息由於不同的設計者照相機系統(ProCams)被分享時，經常視覺縫被創建，一個知名的問題正搖曳噪音從重新奪取的計畫的現場用 ProCams 的照相機出現。在這篇文章裡，他們設計和實現自動和立即無閃爍的校準。提議的方法，ProCams 能除去或者減輕搖曳問題以控制兩個照相機兩個 ProCams 的放映機識別並且決心搖曳。他們提出樣品 ProCams 構造，搖曳察覺選擇和自動閃爍決議策略。第三場爲澳門大學陳俊龍教授，講題爲完全連結模糊的推論體制的新快 F-CONFIS 演算法，在這篇論文裡，模糊的神經網路(FNN)被改變成完全連結的等價物，神經模糊的推論體制(F-CONFIS)是不同於傳統的神經網路，依靠並且重複的重物的一新型神經網路。對這些特別的特性來說，它的學習算法應該不同於傳統的神經網路。因此，F-CONFIS 的一種新有效率的培養訓練算法被提議。 類比例子被給證實其有效性，並且有令人滿意的結果。在使用 FNN 的全部工程應用方面，發展快的 F-CONFIS 訓練有它的新興的價值。

下午聆聽二場學者發表他们的研究論文，分別爲: 北京交通大學林教授，發表論文爲基於人造蜜蜂殖民地算法在考場欺騙行爲的察覺方法，在考場基於人造蜜蜂殖民地算法欺騙行爲的一種察覺方法被提出。移動目標發現的問題被轉換成在前景和背景之間的色值的差別功能。人造蜜蜂殖民地算法被用來優化目標函數。背景組成部分被用與適當的門檻相比較的價值與順序圖像隔開，移動的目標軌道可被成功選出。真正的監視試驗中，圖像顯示方法能適合發現在考場內活動物體的軌道取得好結果並且取得檢測的目的欺騙的行爲。另外，長沙理工大學 Hong Mo 教授，發表論文爲變化時間的基於宇宙的調節平行的交通燈的設計的語言的動態特性分析，交通燈的合理時間設計能整整齊齊引起並且保持運輸系統。怎樣分發時間是關鍵。在論文裡，變化時間的宇宙的理論用來描述圈時間，並且相應模糊那些宇宙也被討論朝塑造那些情勢的運輸流量，然後平行交通管理和控制方法因爲時間變化而變成動態。當運輸流量爲一個十字路口隨著變化時間是變化時，一個類比例子被提供分析語言的動態的調節交通燈的設計的演化。二位學者分別對研究與發展作陳述，論文發表完成後進行詢答，有學者提出了幾個大但與論文議題較無關的問題。多位學者分別對問題作陳述，收穫良多，惟欲延伸深入研究之機會並不大。

會議第三天

104 年 08 月 15 日，上午主辦單位並未安排相關論文發表，相反的主辦單位安排四川大學校園參觀與隨後的組織委員會會議，由於被告知會議內容不能透露，因此擬不附在本次報告內。組織委員會會議後任意參觀了主辦單位之相關參展活動便結束本次研討會的參與。

三、心得

1.此次參與澳門大學與四川大學舉辦之 2015 ICCSS 資料性和控制論的計算社會系統國際性學術研討會，國內學者與學生參與此次研討會屬少數誠屬可惜，參加 2015 ICCSS 國際性學術研討會除了可與各國學者國際交流、交換名片及分享研究心得，能拓展國際觀與國際合作

的機會外，也能多與國內相同領域學者進行交流與合作，加強國際學者之間的交流與合作。在研討會期間，聆聽各國學者在研討會所發表之論文，除了解現今各國學術研究的熱門議題與研究方法之外，亦從中獲得許多寶貴的發現與研究題目，對爾後之學術研究，助益良多。

2.在 2015 ICCSS 資料性和控制論的計算社會系統國際研討會期間與各國學者及學生之間的交流、互動與經驗分享，更是增長見識與國際觀，對於英文語文能力、論文發表與學術研究知名度的提升，都是閉門研究或國內研討會所不能及的，因此，多多參加國際研討會，更能學習國內外學長之所長，對學術研究與貢獻，有更大增益的空間。職參與此次學術交流活動，著實有不少的收穫。

四、建議事項

感謝學校的支持與補助，參與國際性研討會，每次的國際性交流都是非常寶貴的經驗，除了能夠拓展視野之外，也提升台灣學術研究的能見度。也希望與建議政府部門能夠持續且多多支持與鼓勵台灣學者出國參與國際性研討會，以促進學術交流與合作，培養國內學術人才的國際觀。另外對經費補助亦冀望能卓予提升，大陸學者經費補助充足，與國際學者交流多，反觀國內學者礙於經費補助之不足，與國際學者互動缺乏，大大影響我大專院校學者的研究能量與研究產出，將來勢必失去國際優勢，值得深思。

五、附錄: 研討會發表之論文

A Flick Biometric Authentication Mechanism on Mobile Devices

Dong-Her Shih
Department of Information Management,
National Yunlin University of Science and Technology
Douliu, Yunlin, TAIWAN
shihdh@yuntech.edu.tw

Chia-Ming Lu
Department of Information Management,
National Yunlin University of Science and Technology
Douliu, Yunlin, TAIWAN
joe@jiahsing.com.tw

Ming-Hung Shih
Department of Electrical and Electronics Engineering,
Iowa State University,
Ames, IA 50011, USA
dannysmh@gmail.com

***Abstract*—Smartphones nowadays are used not only for communication but also for many emerging applications, such as m-commerce. And, biometric methods can provide promising applications to secure mobile devices. In this paper, we propose a novel authentication mechanism using the information collected from the accelerometer sensor and touchscreen of the smartphone. We design an authentication mechanism that adopts features transformed from those readings. Experimental result show that the proposed mechanism can build a robust authentication environment for smartphone users.**

Keywords-Mobile Security, Biometrics Authentication, accelerometer sensor, touchscreen

I. INTRODUCTION

Common authentication methods like passcodes or visual patterns on mobile devices may be evaded by an attacker or may even be lost or unattended. In the meanwhile, biometric authentication methods can provided as an alternative or addition to passcodes. Physical biometric traits based on physiological characteristics of people also include iris or face recognition. Behavioral modalities in contrast to fingerprint recognition require subjects to perform a behavior over time, like gait or keystroke recognition. Modern smartphones and tablets are equipped with a growing number of sensors [1] such as accelerometer, ambient light sensor, digital compass, gyroscope, GPS, proximity sensor, touchscreen or WiFi. Such sources can be adopted for behavioral verification [2]. Extracted data from different sources can be used for user authentication, adding further protection against unauthorized access. The goal of this paper is to investigate the feasibility of using behavioral biometrics collected from the accelerometer sensor and touchscreen on smartphone to authenticate smartphone users.

II. PRELIMINARIES

A. Touchscreen-based Authentication

De Luca et al. [3] introduce an implicit biometric authentication approach that aims to enhance the Android login procedure. A password or unlock screen is used as an additional security feature. They developed an Android application with four different unlock screens as well as password patterns to collect user data and evaluate their approach. Every 9 to 12 milliseconds, the application logged the following data available from the touchscreen: pressure, size, x/y coordinates and time. Feature analysis is done by DTW to distinguish between different users. Better results were achieved by using password patterns. Sae-Bae et al. [4] present a different authentication technique. A comprehensive set of five-finger and palm touch gestures are extracted. An iPad application was developed which has the capability to track up to 5 points at a time. To verify the input of the user, all the touch points need to be ordered in a consistent way. A DTW algorithm is also used to compute the distance between the stored template and the captured multi-touch gesture. Finally, a dissimilarity score is calculated to accept or decline a user. Angulo et al. [5] developed an Android application to collect data about users draw lock patterns on a touchscreen. 32 volunteers were asked to draw lock patterns consisting of six dots. By using a Random Forest machine learning classifier for pattern matching, an average EER of approximately 10.39% was reached. Frank et al. [6] propose a set of 30 behavioral touch features. They designed an experiment to collect the touch behavior of 41 subjects to evaluate their proof-of-concept framework using a k-nearest neighbor and a Gaussian kernel support vector machine. FAST [7] is a novel touchscreen based authentication approach on Android mobile devices introduced by Feng et al. FAST complements and validates collected data using a digital sensor glove with IMU digital combo boards. Classification algorithms used are: Decision Trees, Random Forest and Bayes Net Classifier. Seo et al. [8] analyzed the users input patterns on touchscreen. They implemented a BPN as learning algorithm which is a pattern recognition method that uses the LSM. The results show that this method effectively identifies users with high accuracy.

B. Accelerometer-based Approaches

Nickel et al. [9] introduced a biometric gait recognition approach to authenticate users via their mobile phones accelerometer. To extract the features, x-, y- and z-direction, as well as magnitude vectors were collected and transformed using statistical analysis. They showed that their algorithm performs well in a controlled environment while leaving open

eventual external influences. Tanviruzzaman et al. [10] propose an adaptive authentication process using gait recognition and location tracks. FastDTW was used to compute similarity scores between samples. Another accelerometer-based approach is described by Boyle et al. [11]. By using wavelet transform to extract features from raw acceleration data. The data was classified using k-nearest neighbor and carried out 5 experiments by walking at a constant pace in a controlled environment.

III. THE PROPOSED APPROACH

A major challenge in using biometric data collected by mobile devices is that most of the data acquired by sensors does not feature the same level of uniqueness as iris patterns or fingerprints. A set of multiple features, such as gait, keystroke dynamics and micro movements, may affect accuracy in environments. There is an emerging trend to combine multiple biometric features for biometric authentication. Therefore, we have proposed a combined biometric authentication mechanism in this section.

A. Data Collection

Participants were asked to sit down in calm situation and perform a task using virtual touch keyboards over a predefined period of time. Gathering data is implemented with invisible data collection processes on mobile phones. The touch gesture of smartphone apps is classified into several types: left-right flick, up-down flick, spread, pinch, etc. However, we design an app on HTC™ Desire 600 with Android™ 4.3 platform to collect user's behavioral biometrics using circle flicks from touchscreen and accelerometer sensor. As shown in Fig. 1 and 2, the circle flick is used to collect the holding behavior while a user conducts a flick motion of her/his finger. Once a user's finger touches the screen of the smartphone, the app continuously collects the accelerometer-sensor-based features at a sampling rate of 50 Hz until her/his finger is out.

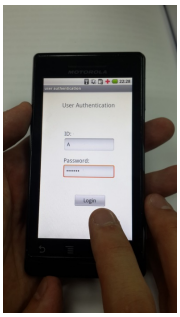

Figure 1. Login

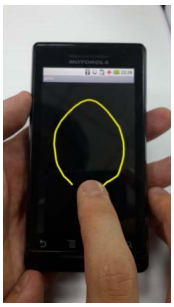

Figure 2. Circle flicks

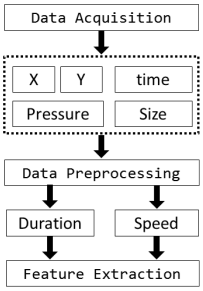

Figure 3. Extracted feature

B. Biometric Features and Classification

Bo et al. [12] have introduced a SilentSense framework which combines touch behavior of a user and micro-movement of the device. Therefore, a joint analysis of features from both touching behavior and the acceleration of the device are used in our approach for user verification. The first authentication step after data collection is to interpolate raw data to a fixed sampling rate. In our experiment, circle flick time, pressure and press size are collected, where pressure and press size data are using getPressure() and getSize() in Android API. X-axis and Y-axis are obtained by event.getX()and event.getY() functions. And, a normalization step is necessary. To separate normalized data into parts for classifiers a sliding window approach with overlapping rectangular windows is used [13].

For pattern recognition purpose different classifier could be identified in literature such as Naïve Bayes, SMO and J48.

C. System Modeling and Authentication

Flowchart of flick biometric authentication is shown in Fig. 4. In the enrollment phase, stepwise linear regression is adopted to select a good feature subset from features for each participant, and Naïve Bayes, SMO, J48 classifiers are used for classification in the authentication phase. Each participant should have an individual authentication model.

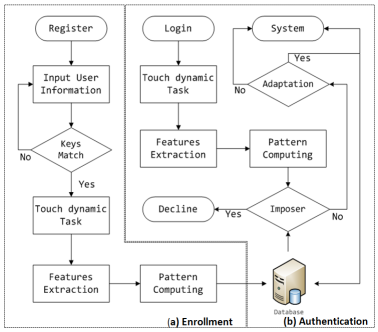

Figure 4. Flowchart of touchscreen authentication

IV. EXPERIMENTAL RESULTS

Ten participants including 6 males and 4 females were recruited in our experiment. They are 22 to 30 years old, and have different smartphone experiences. Two data sets were collected: one is for the flick of touchscreen and the other is from the accelerometer. These participants used the same smartphone to produce a total of 5,175 samples for each of the two data sets. The proposed approach was evaluated by two performance measures: the false acceptance rate (FAR) and the false rejection rate (FRR). These two performance measures were estimated by the leave-one-person-out strategy based on the test step as shown in Fig. 5. Table 1 show the Naïve Bayes, SMO and J48 results of the proposed approach with respect to these two data sets. We found that the performance is great in a convincible way.

V. DISCUSSION AND CONCLUSION

Biometric applications can include authentication and access control. It has been reported that the physiological approaches typically show better performance than behavioral models [14][15]. The accuracy of the accelerometer sensor-based biometrics may not be comparable with the strong biometric modalities such as fingerprints. However, we do not propose accelerometer sensor as a replacement or sole mechanism of authentication but rather than a complementary mechanism that can be used to improve security in mobile devices. Users can still use other biometrics or password explicitly when authenticating for the first time. And after that,

our proposed flick biometric authentication can be applied implicitly for re-verification in a better secure scenario.

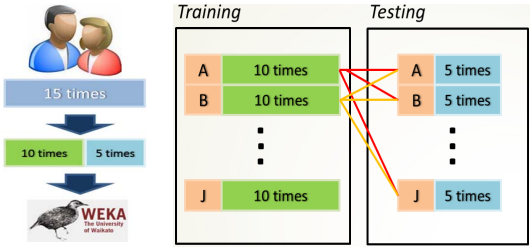

Figure 5. Testing scenario

TABLE I. AUTHENTICATION RESULT BY THREE CLASSIFIERS

Naive Bayes	TP	FN	FP	TN	Accuracy	Precision	Recall	F-Measure	FRR	FAR
A	5	0	0	45	1.000	1.000	1.000	1.000	0.000	0.000
B	3	2	0	45	0.960	1.000	0.600	0.750	0.400	0.000
C	5	0	0	45	1.000	1.000	1.000	1.000	0.000	0.000
D	4	1	3	42	0.920	0.571	0.800	0.667	0.200	0.067
E	5	0	0	45	1.000	1.000	1.000	1.000	0.000	0.000
F	5	0	1	44	0.980	0.833	1.000	0.909	0.000	0.022
G	4	1	0	45	0.980	1.000	0.800	0.889	0.200	0.000
H	5	0	2	43	0.960	0.714	1.000	0.833	0.000	0.044
I	5	0	0	45	1.000	1.000	1.000	1.000	0.000	0.000
J	5	0	0	45	1.000	1.000	1.000	1.000	0.000	0.000
SUM	46	4	6	444	0.980	0.912	0.920	0.905	0.080	0.013

SMO	TP	FN	FP	TN	Accuracy	Precision	Recall	F-Measure	FRR	FAR
A	0	5	0	45	0.900	0.000	0.000	0.000	1.000	0.000
B	0	5	0	45	0.900	0.000	0.000	0.000	1.000	0.000
C	4	1	0	45	0.980	1.000	0.800	0.889	0.200	0.000
D	0	5	0	45	0.900	0.000	0.000	0.000	1.000	0.000
E	0	5	0	45	0.900	0.000	0.000	0.000	1.000	0.000
F	0	5	0	45	0.900	0.000	0.000	0.000	1.000	0.000
G	2	3	0	45	0.940	1.000	0.400	0.571	0.600	0.000
H	0	5	0	45	0.900	0.000	0.000	0.000	1.000	0.000
I	4	1	0	45	0.980	1.000	0.800	0.889	0.200	0.000
J	0	5	0	45	0.900	0.000	0.000	0.000	1.000	0.000
SUM	10	40	0	450	0.920	0.300	0.200	0.235	0.800	0.000

J48	TP	FN	FP	TN	Accuracy	Precision	Recall	F-Measure	FRR	FAR
A	5	0	3	42	0.940	0.625	0.940	0.946	0.000	0.067
B	0	5	1	44	0.880	0.000	0.000	0.000	1.000	0.022
C	5	0	0	45	1.000	1.000	1.000	1.000	0.000	0.000
D	5	0	1	44	0.980	0.833	1.000	0.909	0.000	0.022
E	4	1	0	45	0.980	1.000	0.800	0.889	0.200	0.000
F	5	0	0	45	1.000	1.000	1.000	1.000	0.000	0.000
G	4	1	0	45	0.980	1.000	0.800	0.889	0.200	0.000
H	5	0	0	45	1.000	1.000	1.000	1.000	0.000	0.000
I	5	0	0	45	1.000	1.000	1.000	1.000	0.000	0.000
J	5	0	1	44	0.980	0.833	1.000	0.909	0.000	0.022
SUM	43	7	6	444	0.974	0.829	0.854	0.854	0.140	0.013

In this paper, we have presented a flick biometric approach available for authentication on mobile devices in a convincible way. However, it is important to develop a biometric approach in background service. Developers have to be aware that not every feature is obtained as expected. For example touchscreen data outside an application is not available since user may not activate its app. Furthermore, a combination of biometric traits like gait, gesture and hand movement appears very suitable for future continuous verification. However, the changing of user's behavior has to be considered. Feature selection and biometric combination appears as the most challenging task. User's behavior models may contain multiple features of user's activity and mobile device's response as well as the verification strategy should also be planned as well.

ACKNOWLEDGMENT

This work was partially supported by the Ministry of Science and Technology, Taiwan, under Grant MOST 103-2410-H-224-011.

REFERENCES

[1] N. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. Campbell, "A survey of mobile phone sensing," IEEE Communications Magazine, vol. 48, no. 9, pp. 140–150, 2010.

[2] W. Khan, Y. Xiang, M. Aalsalem, and Q. Arshad, "Mobile phone sensing systems: A survey," IEEE Communications Surveys Tutorials, vol. 15, no. 1, pp. 402–427, 2013.

[3] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!: implicit authentication based on touch screen patterns," in Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems. ACM, 2012, pp. 987–996.

[4] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: a novel approach to authentication on multi-touch devices," in Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems. ACM, 2012, pp. 977–986.

[5] J. Angulo and E. Wstlund, "Exploring touch-screen biometrics for user identification on smart phones," in Privacy and Identity Management for Life, ser. IFIP Advances in Information and Communication Technology, J. Camenisch, B. Crispo, S. Fischer-Hbner, R. Leenes, and G. Russello, Eds. Springer Berlin Heidelberg, 2012, vol. 375, pp. 130–143.

[6] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 136–148, 2013.

[7] T. Feng, Z. Liu, K. A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in 2012 IEEE Conference on Technologies for Homeland Security (HST), 2012, pp. 451–456.

[8] H. Seo, E. Kim, and H. K. Kim, "A novel biometric identification based on a users input pattern analysis for intelligent mobile devices," International Journal of Advanced Robotic Systems, 9, 2012. DOI: 10.5772/51319

[9] C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-nn algorithm," in Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2012, pp. 16–20.

[10] M. Tamviruzzaman, S. I. Ahamed, C. S. Hasan, and C. O'brien, "epet: When cellular phone learns to recognize its owner," in Proceedings of the 2Nd ACM Workshop on Assurable and Usable Security Configuration, ser. SafeConfig '09. ACM, 2009, pp. 13–18.

[11] M. Boyle, A. Klausner, D. Starobinski, A. Trachtenberg, and H. Wu, "Poster: Gait-based smartphone user identification," in Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services, ser. MobiSys '11. ACM, 2011, pp. 395–396.

[12] C. Bo, L. Zhang, X. Y. Li, Q. Huang, and Y. Wang, "Silentsense: Silent user identification via touch and movement behavioral biometrics," in Proceedings of the 19th Annual International Conference on Mobile Computing & Networking, ser. MobiCom '13. ACM, 2013, pp. 187–190.

[13] C. Nickel, H. Brandt, and C. Busch, "Classification of acceleration data for biometric gait recognition on mobile devices," in Proceedings of the Special Interest Group on Biometrics and Electronic Signatures. GI, 2011, pp. 57–66.

[14] R. Bolle, J. H. Connell, and N.K. Ratha, " Biometric perils and patches", Pattern Recognition, vol. 35, pp. 2727-2738, 2002.

[15] S. Furnell, N. Clarke, and S. Karatzouni, "Beyound the PIN: Enhancing user authentication for mobile devices," Computer Fraud & Security, pp. 12-17, August 2008.