Journal of Korea Multimedia Society Vol. 17, No. 8, August 2014(pp. 968-976)
http://dx.doi.org/10.9717/kmms.2014.17.8.968

Using Keystroke Dynamics for Implicit Authentication on Smartphone

Son Do[†], Thang Hoang[††], Chuyen Luong[†††], Seungchan Choi[††††],
Dokyeong Lee[†††††], Kihyun Bang[††††††], Deokjai Choi[†††††††]

ABSTRACT

Authentication methods on smartphone are demanded to be implicit to users with minimum users' interaction. Existing authentication methods (e.g. PINs, passwords, visual patterns, etc.) are not effectively considering remembrance and privacy issues. Behavioral biometrics such as keystroke dynamics and gait biometrics can be acquired easily and implicitly by using integrated sensors on smartphone. We propose a biometric model involving keystroke dynamics for implicit authentication on smartphone. We first design a feature extraction method for keystroke dynamics. And then, we build a fusion model of keystroke dynamics and gait to improve the authentication performance of single behavioral biometric on smartphone. We operate the fusion at both feature extraction level and matching score level. Experiment using linear Support Vector Machines (SVM) classifier reveals that the best results are achieved with score fusion: a recognition rate approximately 97.86% under identification mode and an error rate approximately 1.11% under authentication mode.

Key words: Implicit User Authentication, Smartphone, Keystroke Dynamics, Gait, Multimodal Biometrics.

1. INTRODUCTION

Smartphone is becoming more and more popular to the human life. The number of smartphone sales even surpassed sales of feature phones for the first time in 2013 [1]. People can use their phone to send or receive emails, download apps, participate in a video call or video chat, manage and plan, keep entertained, get directions, recommendations, or other location-based information, etc. [2]. Secure authentication is required for access to data or applications. Moreover, the authentication system is demanded to be implicit with very minimum users' involvement. According to a survey which was conducted by Furnell et al. [3], users want increased security authentication that is transparent when authenticating individuals for the sake of their convenience. But remembrance issue and pri-

※ Corresponding Author : Deokjai Choi, Address: (500-757) Chonnam National University, Yongbong-dong, Buk-gu, Gwangju, TEL : +82-62-530-3429, FAX : +82-62-530-3439, E-mail : dchoi@jnu.ac.kr
Receipt date : May. 28, 2014, Revision date : Jul. 1, 2014
Approval date : Jul. 21, 2014
[†] Dept. of Electronics & Computer Eng., Graduate School, Chonnam National University
(E-mail : dvson167@gmail.com)
[††] Dept. of Electronics & Computer Eng., Graduate School, Chonnam National University
(E-mail : hmthang2812@gmail.com)
[†††] Dept. of Electronics & Computer Eng., Graduate School, Chonnam National University
(E-mail : luongchuyen0789@gmail.com)
[††††] Gwangju Science High School
(E-mail : chltmdcks97@naver.com)
[†††††] Dept. of Electronics & Computer Eng., Graduate School, Chonnam National University
(E-mail : ldk7175@nate.com)
[††††††] Dept. of Electronics & Computer Eng., Graduate School, Chonnam National University
(E-mail : badmanner@naver.com)
[†††††††] Dept. of Electronics & Computer Eng., Graduate School, Chonnam National University
※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2012R1A1A2007014).

vacy issues are the main drawbacks of current existing authentication methods on smartphone such as PINs, passwords, visual patterns, etc. [4]. It may be impractical for the users to remember all passwords or PINs from different sites. Moreover, the phone is easily lost, stolen or illegal access [4].

As each individual is identified by a set of unique characteristics and traits, also called as biometrics, these characteristics are good choices for authentication on smartphone with integrated sensors. Physiological biometrics (e.g. iris, fingerprint, etc.) can be implemented to completely overcome the issues of existing authentication methods [5, 6] on smartphone, but the data acquisition process requires users' interaction which does not satisfy the implicitness of user authentication. Behavioral biometrics (e.g. keystroke dynamics, gait, etc.), on the other hand, can be acquired easily and implicitly by using integrated sensors (e.g. touch sensor, motion sensors, etc.) on smartphone. Nevertheless, because of the inherent limitations [7, 8] such as noisy data, high intra-class variability, and high inter-class similarity, existing work on authentication using single behavioral biometric [9-14] did not achieve performance which is good enough to implement in real world. Thus, multimodal biometrics has been proposed to alleviate these limitations [7, 8].

In the mobile context, we found that most of the smartphone's users interact with the device (e.g. when typing a text message, when composing an email, etc.) through the touch sensor which is available on most of modern smartphones. Consequently, keystroke dynamics data can be collected without the awareness of the users. In addition, as devices are put into their owners' pocket for most of the day [4], walking gait signal can be acquired continuously and implicitly by using motion sensors on smartphone. And so, sensor-based gait authentication has a significant advantage in implementation on smartphone [9]. In this paper, we propose a biometric model involving keystroke dynamics for implicit authentication on smartphone. We first design a feature extraction method. And then, we build a fusion model of keystroke dynamics and gait to improve the authentication performance of single behavioral biometric on smartphone. We operate the fusion at both feature extraction level and matching score level. Support vector machines is selected to deal with high dimensional feature vectors. We achieved promising results under both identification and authentication mode when experimenting on real dataset.

The rest of this paper is organized as follow. Section 2 presents related work. Section 3 presents the proposed method. The experimental result is presented in section 4. Section 5 concludes the paper.

2. RELATED WORK

Single behavioral biometric authentication methods using keystroke dynamics or gait have been studied in the last decade. More details of these works are given in [9] and [10]. Recently in the mobile context, potential results have been achieved [10-14]. However, the inherent limitations of single behavior modalities make them difficult to achieve good result enough to implement in real world. To the best of our knowledge, the best result on gait authentication was achieved by T. Hoang [10] (in 2013) which was 94.93% recognition rate at zero false acceptance rate (FAR) and 3.89% false rejection rate (FRR). On keystroke dynamics, P.S. Teh [11] studied on multilayer fusion of keystroke dynamics (username, password, 13-character text) on 100 subjects using digraph features and achieved equal error rate (EER) at 1.401% when using template matching with Gaussian Probability Distribution Function and Direction Similarity Measure and score fusion. In 2013, M. Trojath [12] studied on 11-character password on 18 subjects with many features such as digraph, trigraph, pressure, etc. and used many classifiers such as

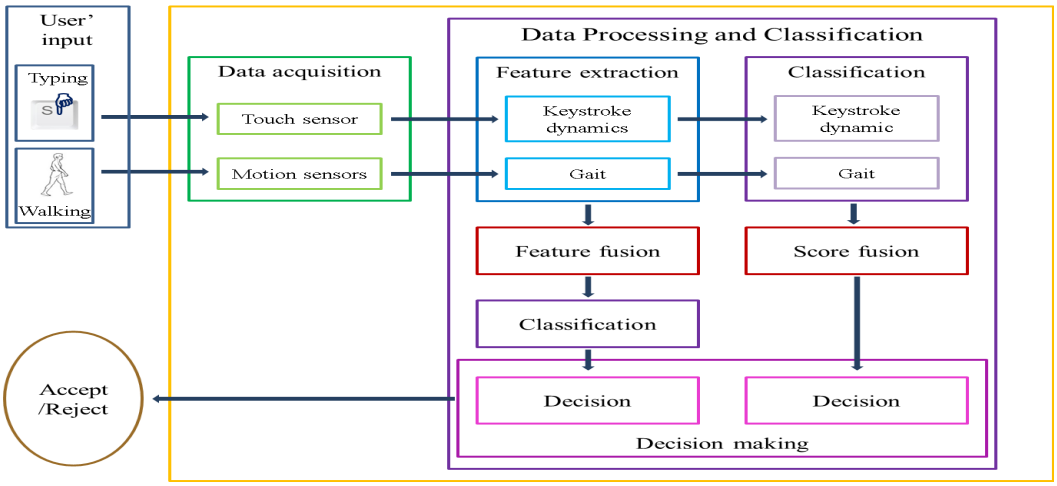

Fig. 1. The proposed system.

neural networks, Bayesian classifier, etc. The best result which was achieved was EER at 2%. Keystroke dynamics on thumbnails was studied as well. T.Y. Chang [13] (2012) studied on 3-6 thumbnails on 100 subjects using pressure and four types of latencies and achieved EER at 6.9% by using statistical classifier. In 2013, N. Jeanjaitrong [14] studied on 4-16 thumbnails on 10 subjects using four features: dwell time, interval time, interval timing ratio and distance, and achieved recognition rate at 82.18%. In the same year, J. Draffin [15] studied characteristics of single keypress such as touch position, touch force, finger drift and the area of touch for passive authentication by using both discriminant model and generative model. The achieved experimental result on 13 subjects is the recognition rate (RR) at 67.7% within 5 keypresses and after 15 keypresses, this value is 86%.

Some fusion model using keystroke dynamics have been proposed [16-18] to improve the equal error rate of the authentication. In 2010, R. Giot [16] studied on 100 subjects and operated fusion of key-

Table 1. Recent research on biometric identification and/or authentication systems on smartphone (KD - Keystroke dynamics, RR - recognition rate, EER - equal error rate)

Literature	Number of subjects	Modality	Fusion method	Results
[10] (2013)	38	Gait	-	94.93% RR
[11] (2011)	100	KD	Multilayer fusion	1.401% EER
[12] (2013)	18	KD	-	2% EER
[13] (2012)	100	KD	-	6.9% EER
[14] (2013)	10	KD	-	82.18% RR
[15] (2013)	13	KD	-	67.7% RR (5 keys), 86% RR (15 keys)
[16] (2010)	100	KD, 2D face	Score fusion	2.22% EER
[17] (2012)	30	KD, behavioral profiling, linguistic profiling	Score fusion	8% EER
[18] (2013)	150	Face, voice	Feature fusion, Score fusion	Approximately 2% EER

stroke dynamics (16-character password with 1 space) and 2D face at matching score level and achieved EER at 2.22%. In 2012, H. Saevanee [17] studied on 30 subjects on fusion of keystroke dynamics (4-digit number, 11 digit number, text message with average length of 14-word), behavioral profiling, linguistic profiling and achieved EER at 8% using score fusion. In 2013, P. Tresadern [18] studied feature fusion and score fusion of face and voice on 150 subjects and achieved EER at approximately 2%. These approaches and their performances on mobile platform with various evaluation metrics such as EER, RR are summarized in Table 1.

3. PROPOSED METHOD

Fig. 1 shows the proposed method where the processing steps for gait biometrics comes from [9]. Fusion can be operated in feature extraction level or matching score level.

3.1 Data acquisition

There is no public dataset on multimodal biometrics which consists of keystroke dynamics and gait. Moreover, it is difficult to collect a multimodal dataset. Therefore, we create a virtual database from two separate dataset to use in this study. The specifications of devices used in this experiment are summarized in table 2.

We used the *MotionEvent* in the Android SDK and the LG Optimus G E975 phone to collect keystroke dynamics data. The phone do not run any other application during data collection. There were 38 volunteers including 28 males and 10 females participated in this experiment. Participants who had original state of health were asked to sit as comfortable as possible at a chair under standard laboratory condition. The phone was hold freely at hand. Participants were asked to type a user-selected long sentence or paragraph (length greater than 50) and each of which is entered for ten times. In total, we collected 133905 seconds of keystroke dynamics of 38 volunteers. An example of collected data of two characters "S" and "O" is showed in Fig. 2. The data in each line consist of time-stamp in millisecond, X and Y coordinate of the touch point, touch size, touch pressure, touch action, and the typed character.

In addition, we collect the same data and in same condition of ten participants (among 38 participants) on the HTC Desire 500 phone. Totally 3552 seconds of keystroke dynamics was collected.

The gait dataset was manually collected by the authors in [10] using a Google Nexus One mobile phone with built-in accelerometer sensor and magnetometer sensor. In the data collection for

```
1400690765915 157.5 975.951 0.26666668 0.2 TOUCH_DOWN S
1400690765932 157.5 975.951 0.26666668 0.20400001 TOUCH_MOVE S
1400690765970 157.5 976.5436 0.26666668 0.21200001 TOUCH_MOVE S
1400690765985 157.5 976.451 0.26666668 0.18800001 TOUCH_MOVE S
1400690765999 157.5 976.451 0.26666668 0.18800001 TOUCH_UP S
1400690766195 614.0 824.951 0.33333334 0.23600002 TOUCH_DOWN O
1400690766252 614.0 824.951 0.26666668 0.172 TOUCH_MOVE O
1400690766258 614.0 824.951 0.26666668 0.172 TOUCH_UP O
```

Fig. 2. Collected information for the input "SO".

Table 2. Short specification of the phones used for data acquisition.

Device name	Android's version	Screen size	Sensor used	Sampling rate	Modality
LG Optimus G E975	4.1.2	768×1280 (4.7in)	Touch sensor	-	Keystroke Dynamics
HTC Desire 500	4.1.2	480×800 (4.3in)	Touch sensor	-	Keystroke Dynamics
Google Nexus One	2.1	480×800 (3.7in)	Accelerometer, magnetometer	27Hz	Gait

gait, the phone is freely put into its owner's trouser pocket.

3.2 Keystroke dynamics feature extraction

For keystroke dynamics data, we ignore the preprocessing steps because we aim in extracting dynamic features from the original data. Segmentation is performed on each data instance corresponds to a text sample to extract patterns. This is done by cutting the long sentence at punctuations such as dots, commas, etc.

After obtaining raw keystroke related information, vital features are extracted and analyzed for training. During a keystroke, the user's finger/touch pen is usually drifted over the key's surface, therefore multiple touches can be recorded (see Fig. 3) where "press" and "release" respectively correspond to "TOUCH_DOWN" and "TOUCH_UP" which are defined on the Android SDK. According to the information that can be acquired, we can extract and analyze the following features which are related to keystroke dynamics and touch screen behavior which have been developed in the literature: (1) *digraph* including *dwell time* (holding time of a key) and *flight time* or *latency* (time difference between "press" action and "release" action of two consecutive keys, of four types: "press-press", "press-release", "release-press", "release-release"); (2) *N-graph* (time difference of "press-press" between a key and the N-th key in the sequence from its position); (3) *pressure:* the pressure a user applies to the touch surface; (4) *size:* the size of the touch area; (5) *position*: position a user touches to the touch surface; (6) *drift:* the displacement of the finger/touch pen during a keystroke in X and Y direction; (7) *typing speed:* the average time to type a key; and (8) *error rate:* the ratio of the number of times the backspace key is pressed to the total number of keys pressed.

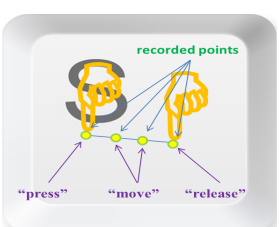

Fig. 3. Data collection during a keystroke.

We use statistical features in this paper: mean and standard deviation of dwell time, flight time, trigraph (N-graph with N=3), displacement; minimum, mean and maximum of pressure; standard deviation of size and position; typing speed, error rate.

3.3 Fusion method

Because keystroke dynamics has limitations such as noisy data, high intra-class variation, high inter-class similarity, we build a multimodal authentication system involving keystroke dynamics and gait. Gait biometric is used because it is easy to acquire using integrated accelerometer of smartphone. Moreover, the phones are put to their owner' pocket most of the day [4]. Therefore, walking gait is appropriate to authenticate on smartphone. In practice, we can collect gait data in separate manner with the keystroke dynamics. And anytime we perform keystroke dynamics authentication, we retrieve the prestored gait data for fusion. We apply the feature extraction method which was proposed in [10] to extract gait features.

After preprocessing and segmentation, the following features [10] are extracted from each component (e.g. Z-dimensional signal, magnitude of the XY-dimensional signal, and magnitude of the signal) of a particular segment: root mean square, mean, standard deviation, average absolute different, waveform length, 10-bin histogram distribution, first 40 fast Fourier transform (FFT) coefficients, and first 40 discrete Cosine transform (DCT) coefficients.

3.3.1 Feature fusion

In feature fusion, two feature vectors from an instance of keystroke dynamics and an instance of

Table 3. Overall identification result

	Keystroke dynamics	Gait	Feature fusion	Score fusion (Sum)	Score fusion (Product)	Score fusion (Average)
RR (%)	92.17	94.93	95.52	97.14	97.37	97.86

Table 4. Overall authentication result

	Keystroke dynamics	Gait	Score fusion (Average)
EER (%)	3.23	2.70	1.11

gait are fused by concatenation. Given two feature vector fv_1 and fv_2 of length D which comes from two modalities, the concatenation looks like this:

$$fv = [fv_1 \ fv_2] \quad (1)$$

And before being fed into the SVM classifier, fv is normalized into the interval [-1, 1] based on the min-max rule [7]. In order to balance the number of features of fv_1 and fv_2, we reduce the number of gait's features by extracting only one component and reducing the number of coefficients of the FFT and DCT. The final classification result is the average result of the three gait's components.

In enrollment phase, we calculate and store the parameters of the SVM classifier. In test phase, a test feature vector is first normalized into the same space. And then, it is fed into the SVM classifier. We use the linear SVM for classification instead of the kernel method because the performance of kernel SVM is sensitive to model's parameters changes [19].

3.3.2 Score fusion

In fusion at matching score level, features from two modalities are classified separately to obtain the score z_i. For a particular test instance, the SVM classifier returns a vector of values indicating the probability that the test instance is in each class. Fusion is operated on these values which come from two test instance of two modalities. Because the scores are generally come from different domain, they are normalized to the same domain using the min-max rule [7]. For fusion, sum, product and averaging rule is used in this paper.

$$z = z_1 + z_2 \quad \text{(sum rule)} \quad (2)$$

$$z = z_1 * z_2 \quad \text{(product rule)} \quad (3)$$

$$z = \frac{w_1 z_1 + w_2 z_2}{w_1 + w_2} \quad \text{(average rule, } w_1 = w_2 = 1\text{)} \quad (4)$$

4. RESULTS

Totally 6100×2 patterns are extracted from the virtual dataset by using segmentation algorithms. There are around 160 patterns corresponding to each participant. These patterns are split into two equal parts: the first part is used for training and the remaining one is used for prediction. We use libsvm [19] as the tool to perform linear SVM classification. In authentication mode, we calculate the EER based on the probability values which are estimated by using the libsvm[19].

We first validate the goodness of the features of keystroke dynamics. The identification result in Fig. 4 reveals that dwell time, flight time and pres-

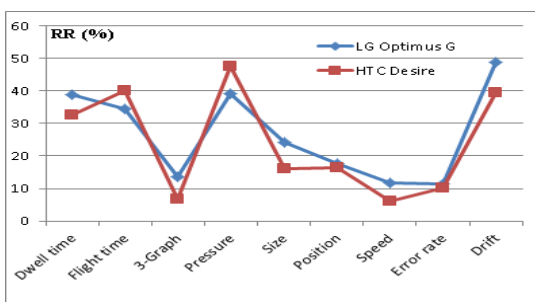

Fig. 4. Keystroke dynamics identification with single type of feature.

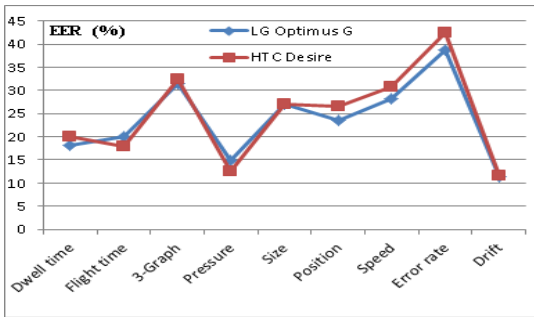

Fig. 5. Keystroke dynamics authentication with single type of feature.

sure which have been developed in the literature are reliable in this context as well. The experimental result shows that the drift features take advantage over features in the literature. Type of devices does not affect much to the performance of those feature. Similar result is obtained in authentication mode (see Fig. 5).

The performance of keystroke dynamics identification method using all features is 92.17%. We operate fusion of keystroke dynamics and gait at both feature extraction level and matching score level. Table 3 shows the overall identification result. Because it's difficult to operate fusion at feature extraction level, the fusion at matching score level yields better result. The highest recognition rate is achieved when using averaging for score fusion. We use this result in authentication mode.

The number of participants is thirty-eight. For each genuine user, we consider all the remaining as imposters. For measuring the error, the EER value is estimated based on the probability values which are estimated by using the libsvm [19]. The result is showed in Table 4.

5. CONCLUSION

In this paper, we propose a method for implicit authentication on smartphone involving keystroke dynamics and gait. The purpose is to take advantage of integrated sensors for implicit authentication on smartphone. We design a feature extraction method for keystroke dynamics. And then, we operate fusion to eliminate the impact of changing conditions such as bad quality data samples or sensor errors in both feature extraction level and matching score level. We use the linear SVM classifier for classification. The experimental result reveals that a significant improvement in authentication performance of method using multimodal modalities is achieved when compared with method using only one modality.

REFERENCE

[1] J. Rivera and R. van der Meulen, *Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013*, The Gartner, Egham, 2014.

[2] M. Duggan, *Cell Phone Activities 2013*, Pew Research Center's Internet & American Life Project, 1615 L St., N.W., Suite 700, Washington, D.C. 20036, 2013.

[3] S. Furnell, N. Clarke, and S. Karatzouni, "Beyond the PIN: Enhancing User Authentication for Mobile Devices," *Computer Fraud & Security*, Vol. 2008, Issue 8, pp. 12-17, 2008.

[4] F. Breitinger and C. Nikel, "User Survey on Phone Security and Usage," *Proceeding of the Special Interest Group on Biometrics and Electronic Signatures*, Vol. 164GI, pp. 139-144, 2010.

[5] A.K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transaction on Circuits and System for Video Technology*, Vol. 14, Issue 1, pp. 4-20, 2004.

[6] Y. Ou and K.H. Rhee "Secure Biometric Hashing by Random Fusion of Global and Local Features," *Journal of Korea Multimedia Society*, Vol. 13, No. 6, pp. 875-883, 2010.

[7] A. Ross and A. Jain, "Multimodal Biometrics: An Overview," *Proceeding of 12th European Processing Conference*, pp. 1221-1224, 2004.

[8] Y. Wang and Z. Liu, "A Survey on Multimodal Biometrics," *Lecture Notes in Electrical Engineering*, Vol. 123, Issue 2, pp. 387-396, 2011.

[9] P.S. Teh, A.B.J. Teoh, and S. Yue, "A Survey of Keystroke Dynamics Biometrics," *The Scientific World Journal*, Volume 2013, Article ID 408280, 24 pages, 2013, doi:10.1155/2013/408280.

[10] T. Hoang, D. Choi, V. Vo, A. Nguyen, and T. Nguyen, "A Lightweight Gait Authentication on Smartphone Regardless of Installation Error," *IFIP AICT*, Vol. 405, pp. 83-101, 2013.

[11] P.S. Teh, A.B.J. Teoh, C. Tee, and T.S. Ong, "A Multiple Layer Fusion Approach on Keystroke Dynamics," *Pattern Analysis and Applications*, Vol. 14, Issue 1, pp. 22-36, 2011.

[12] M. Trojahn and F. Ortmerier, "Toward Mobile Authentication with Keystroke Dynamics on Smartphones and Tablets," *Proceeding of 27th WAINA*, pp. 697-702, 2013.

[13] T.Y. Chang, C.J. Tsai, and J.H. Lin, "A Graphical-based Password Keystroke Dynamic Authentication System for Touch Screen Handheld Mobile Devices," *The Journal of Systems and Software*, Vol. 85, Issue 5, pp. 1157-1165, 2012.

[14] N. Jeanjaitrong and P. Bhattarakosol, "Feasibility Study on Authentication Based Keystroke Dynamic over Touch-screen Devices," *Proceeding of 13th ISCIT*, pp. 238-242, 2013.

[15] B. Draffin, J. Zhu, and J.Z. Zhang, "KeySens: Passive User Authentication through Micro-behavior Modeling of Soft Keyboard Interaction," *Proceeding of MobiCASE*, pp. 184-201, 2013.

[16] R. Giot, B. Hemery, and C. Rosenberger, "Low Cost and Usable Multimodal Biometric System based on Keystroke Dynamics and 2D Face Recognition," *Proceeding of 20th ICPR*, pp. 1128-1131, 2010.

[17] H. Saevanee, N.L. Clarke, and S.M. Furnell, "Multi-modal Behavioral Biometric Authentication for Mobile Devices," *Proceeding of SEC 2012*, IFIP Advances in Information and Communication Technology, Vol. 376, Issue 2012, pp. 465-474, 2012.

[18] P. Tresadern, T.F. Cootes, N. Poh, P. Matejka, A. Hadid, and C. Lévy et al., "Mobile Biometrics: Combined Face and Voice Verification for a Mobile Platform," *IEEE Pervasive Computing*, Vol. 12, Issue 1, pp. 79-87, 2013.

[19] C. Chang and C.J. Lin, "LIBSVM: a Library for Support Vector Machines," A*CM TIST*, Vol. 2, Issue 3, Article No. 27, 27 pages, 2011.

Son Do

He received BS degree in Department of Math and Computer Science, University of Science, VNU-HCMC in 2011. He is currently studying for his MS Degree in School of Electronics and Computer Engineering, Chonnam National University, South Korea. His research interests are context awareness, and pattern recognition.

Thang Hoang

He received BS degree in Department of Computer Science, University of Science, VNU-HCMC in 2010. He is currently studying for his MS Degree in School of Electronics and Computer Engineering, Chonnam National University, South Korea. His research interests are context awareness, ubiquitous computing, mobile computing, biometrics, cryptography and pattern recognition

Chuyen Luong

She received Engineering degree in School of Electronics and Telecommunications from Hanoi University of Sciences and Technology, Vietnam in 2012. She is currently studying for her MS Degree in School of Electronics and Computer Engineering, Chonnam National University, South Korea. Her research interests are mainly in the field of context awareness, pattern recognition

Seungchan Choi

He graduated his middle school in 2013, and now is at Gwangju Science Highschool. He has interest in using smart phone, and likes to use computer for the science problem solving.

Dokyeong Lee

He received the B.Eng in Information & Communication Engineering from Honam University in early 2013. Since 2013, he has been with the Network Systems Lab, Chonnam National University, Gwangju, Korea, pursuing a Master degree in Electronics & Computer Engineering. His main research interests include sensor network development and internet of things

Kihyun Bang

He received Engineering degree in Faculty of Life Science and Technology, Chonnam National University in 2013. He is currently studying for his MS Degree in School of Electronics and Computer Engineering, Chonnam National University, South Korea. His research interests are computer network, software defined networking and ubiquitous healthcare.

Deokjai Choi

He is full professor of Computer Engineering Department at Chonnam National University, South of Korea. He received BS degree in Department of Computer Science, Seoul National University, in 1982. He got MS degree in Department of Computer Science, KAIST, South Korea in 1984. He got PhD degree in Department of Computer Science and Telecommunications, University of Missouri-Kansas City, USA in 1995. His interest on research spans from context awareness, pervasive computing, sensor network, future Internet and IPv6.