Arm's Flex when Responding Call for Implicit User Authentication in Smartphone

Ali Fahmi Perwira Negara[1]*, Elyor Kodirov[2], Mohd Fikri Azli Abdullah[3], Deok-Jai Choi[4], Guee-Sang Lee[5] and Shohel Sayeed[6]

[1, 2, 4, 5] *School of Electronics and Computer Engineering (ECE)*
Chonnam National University (CNU), Gwangju, South Korea
[3, 6] *Faculty of Information Science and Technology (FIST)*
Multimedia University (MMU), Melaka, Malaysia
[1, 2, 3]*{ali.fahmi.pn, ekodirov, mfikriazli}@gmail.com,* [4, 5]*{dchoi, gslee}@jnu.ac.kr,*
[6]*shohel.sayeed@mmu.edu.my*

Abstract

From using secret knowledge like password up to physical traits as biometrics, current smartphone authentication systems are deemed inconvenience and difficult for users. Burdens on remembering password as well as privacy issue on stolen or forged biometrics have raised a new idea of authentication systems. New system is expected to be transparent to users without or with very minimum user involvement being as implicit authentication system. With user's convenience in mind yet without sacrificing security aspect, behavioral biometrics can be applied in implicit authentication system for security protection to users and their smartphones. Behavioral biometrics (behaviometrics) concept has emerged intending on both being inexpensive for deployment and being safe to user as compared on physical traits-based biometrics. One of the human behaviors considered being unique is arm's flex (AF). It is gestural pattern i.e. the way people bending their arm for picking a phone when responding to incoming calls. That arm's flexing is considered as a subset of gesture pattern in lower limb gesture. We study and evaluate arm's movements that take place when picking up smartphone to receive incoming phone call. Our study shows that arm's movements captured by smartphone built-in accelerometer are potentially useful for authentication system using smartphone. Our study shows that AF is indeed unique and has discriminant power to distinguish one user from others. These findings will promisingly augment development of novel implicit and transparent authentication system in smartphone so that authentication becomes easier and unobtrusive for user.

Keywords: *arm's flex (AF), behaviometrics, implicit user authentication, smartphone*

1. Introduction

The rapid growth and vast trend in smartphone as personal device carrying sensitive data are being the obvious reasons on why authentication for smartphone is critical. Apart from those intrinsic obstacles, at the user perspective, Furnell et al.[7] reported that users want increased security authentication that is transparent when authenticating users for their convenience. Another survey [8] also mentions about 60% of respondents that wish to have easier form of mobile authentications. The survey elaborates the inconvenience among users having 'fat' fingers with authentication system like password in tiny keyboard of smartphone.

The trends have given an idea on which Greenstadt and Beal [21] and Jakobsson et al. [23] present idea about giving cognitive ability to personal devices in an aspect of security especially in their authentication systems. The intelligent capability will not only improve the security authentication level but also will enrich user convenience. In this paper, we present our study on an approach to authenticate smartphone users implicitly and transparently using one of behavioral biometrics (behaviometrics) i.e. user's arm flexing when responding to incoming call. Through this behaviometrics, we aim on (1) alleviating burden of users from remembering secret knowledge, (2) being inexpensive in deployment, (3) being safer if compared to physical biometrics as exposed in [6], and lastly (4) on being unobtrusive and transparent to users.

The rest of this paper will be organized as follows. Section 2 surveys biometric-related works from other researchers. Section 3 will discuss AF and its characteristics as behavioral biometric (behaviometrics) for an authentication system. Section 4 discusses and presents our results and then discusses the overall findings together with evaluation over authentication performance. Section 5 summarizes and concludes our study as well as presents our future research direction.

2. Arm's flex for authentication system

In its biomechanics observation, even though visually the flexing movement pattern of picking a phone when responding to an incoming phone call is similar from one to another, Roman-Liu et al. [20] study on relationship between upper limb strength/force and upper limb posture in general which concluded that the posture affects the strength of upper limb strength during several motion simulations. Every person who bends their arm will have different strength measured by accelerometer using smartphone even if they own same AF pattern visually. The basis of this inference lies in a simple theory of kinematic physics in 2nd Newtonian Law, where acceleration is proportionally related to force exerted over a mass (a = F/m) in which bending action will result various unique traits due to various force strength exerted from various posture and biological muscular structure. In terms of usability, addressing incoming call or making phone call is reported by NQ Mobile in January 2012 survey [18] as the most frequent activity that one user does. Hence, making use AF that is common action related to call activity, AF will then augment authentication system as implicit.

3. Arm's flex experiment

3.1. Arm's flex data collection

Our study is conducted with smartphone Pantech Sky Vega Racer which has built-in MEMS Invensense tri-axial accelerometer sensor on its MPU-6000 module. Application's development is under Android OS (Gingerbread 2.3.3) environment. We collect several acceleration data obtained from 6 volunteers that perform a simulation of picking phone from a table and from users' pants pocket. Each of users will perform two types of AF pattern where each arm's bending pattern will be repeated five times resulting data in total as many as 6 respondents with 2 typical categories with each repetitive 10 pattern data resulting 120 data collected.

We use two types of bending situation simulated for (a) picking phone from table denoted as situation *sD* and (b) picking phone from user's pocket as situation *sP*, as they are depicted in Figure 1 and Figure 2 exhibiting two smartphone's positions during experiment from incoming call up to getting near/touching user's ear.

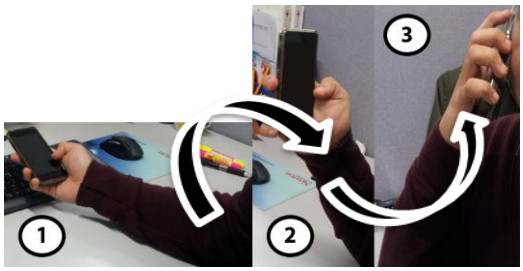

Figure 1. Picking from table (sD)

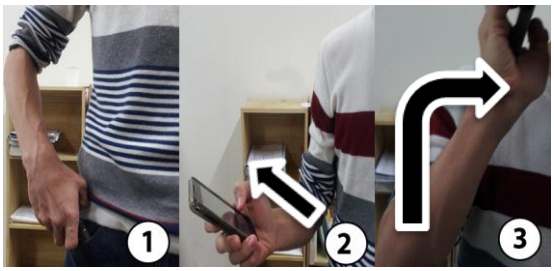

Figure 2. Picking from pocket (sP)

4. Result and evaluation

4.1. Arm's flex trend similarity analysis

Throughout this paper, we evaluate and analyze our experiment results by contrasting one user labeled as person *A* with other person *B* and *C* as the unauthorized users. Therefore, for example in a situation *sP*, we denote three vectors representing each acceleration magnitude resulted from person *A* arm's flexes in each cycle within similar time period from t_1 to t_n in vector space X = $\{x_1, x_2, \ldots, x_n\}$, Y = $\{y_1, y_2, \ldots, y_n\}$, and Z = $\{z_1, z_2, \ldots, z_n\}$. We also let two vectors representing each acceleration magnitude resulted from two different persons as *B* and *C* within similar time period from t_1 to t_n as B = $\{b_1, b_2, \ldots, b_n\}$ and C = $\{c_1, c_2, \ldots, c_n\}$. Using these vector representations in vector spaces of acceleration magnitude, we will further evaluate the similarity among X, Y, Z, B, and C where X, Y, and Z are generated from one person *A* while B and C are from person *B* and *C* respectively. Similarity of those vectors can be evaluated using Cosine Similarity method as in formula (1) and Euclidean Distance computation as in formula (2) denoted as follows:

$$\mathrm{Sim}(\mathrm{V},\mathrm{W}) = \cos(\theta) = = \frac{\mathrm{V}\cdot W}{|\mathrm{V}||W|} = \frac{\sum_{i=1}^{n} V_i \times W_i}{\sqrt{\sum_{i=1}^{n} V_i^2} \times \sqrt{\sum_{i=1}^{n} W_i^2}} \quad (1)$$

$$\mathrm{D}(\mathrm{V},\mathrm{W}) = \sqrt{(V_1 - W_1)^2 + (V_2 - W_2)^2 + \cdots + (V_n - W_n)^2} \quad (2)$$

We want to measure similarity in 'closeness-similarity' as well as magnitude of similarity via Cosine Vector similarity and Euclidean Distance respectively. Thus, both methods are used in unison analysis manner. Our statistical computation is presented in following Table 1 below:

Table 1. Similarity Comparison on Pattern *A* vs *B* vs *C*

$D(V,W)/\cos\theta$	X	Y	Z	B	C
X		$0.39/0.99$	$0.38/0.99$	$1.42/0.88$	$0.93/0.91$
Y	$0.39/0.99$		$0.52/0.98$	$1.22/0.92$	$0.93/0.89$
Z	$0.38/0.99$	$0.52/0.98$		$1.31/0.89$	$0.94/1.31/0.93$
B	$1.42/0.88$	$1.22/0.92$	$1.31/0.89$		$1.04/0.92$
C	$0.93/0.91$	$0.93/0.89$	$0.94/0.93$	$1.04/0.92$	

In Table 1, we could deduce that among X, Y, and Z they are strongly inferable being closely similar both in vector direction and their angles. In distance, they are also close among them. For example, a different angle more than 20 ° difference is pretty big (based on our experimental experience) to say one vector is similar to each other, then θ value for one vector related to its counterpart cannot be less than 0.9395 (≈ 0.94). Thus, all θ value less than 0.9395 between two vectors are equally considered as having big difference in which two vectors are said to be 'one vector is different from other vector'. Only vector X, Y, and Z have θ value more than 0.9395 thus rendering them said to be 'one vector similar to another'.

Besides using Cosine Similarity, we also evaluate them in pair using their Euclidean Distance. Similarly, the distance among three AF patterns from one person *A* is said to be close to each other. The farthest distance among those three AF pattern alike is only 0.52. In contrast, when we compare patterns from person *A* with other patterns from person *B* and *C* the distances are doubled the distance of the farthest (0.52) in average. We can conclude that X, Y, and Z are highly likely to be from same source (person *A*). On the other hand, having X, Y, Z as templates to be matched and compared, our computation shows that B and C are more possibly generated from different sources. Furthermore, B and C are also evaluated to be different persons' arm's flexes respectively. B and C as seen in Table 1 have shown that they relatively have big angle difference as well as they are far from each other in distance. Let us set φ as ratio of distance D (V, W) over cosine θ similarity denoted as:

$$\varphi = \frac{D(V,W)}{\cos(\theta)} \qquad (3)$$

We can notice from Table 1 that for each pair of vector X, Y, and Z they have φ value less than one (1) while each vector pair from B either with any of X, Y, Z or C the value of φ is greater than one (1). Same φ value from B also occurs to each pair of vector C with any of X, Y, Z, or B. This is really exciting finding as we have one discrete value that can be used as a threshold to determine similarity or difference of one pattern to templates.

Figure 3 reflects on different persons' AF pattern can be distinguished from three pattern generated from one source AF patterns of person *A*. Visually, the conclusion can be intuitively evaluated from Figure 3.

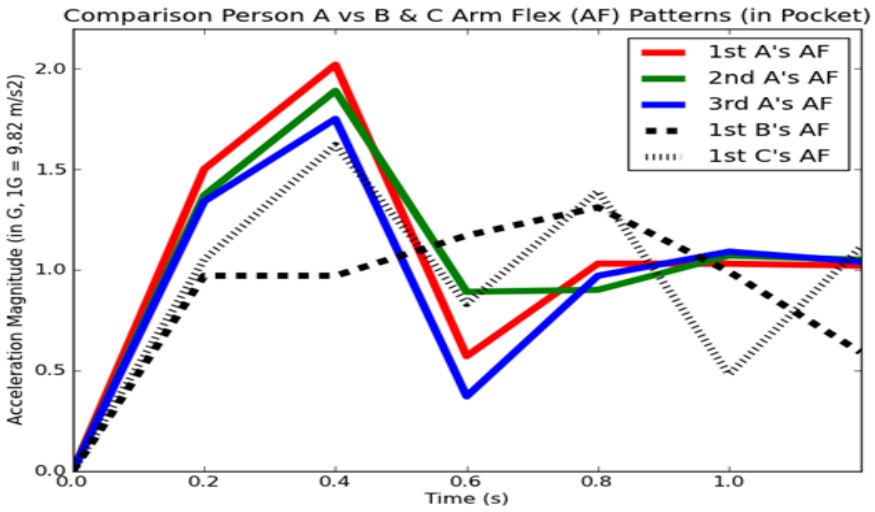

Figure 3. Comparison on Acceleration Pattern A vs B vs C

In Figure 4, we have five patterns consists of three AF patterns from person *A* that are plotted in solid thick lines, one AF pattern from person *B* plotted in solid dashed line, and one AF pattern from person *C* plotted in solid dotted line. In Figure 4, our similarity computation and analysis can intuitively be justified where the difference among patterns from person *A* to person *B* and person *C* are clear. Figure 4 depicts on how patterns' trend from person *A* is similar among them while pattern from person *B* and person *C* are obviously and perceivably different from the rest of the patterns.

4.2. Authentication system with arm's flex

Every new signal will be evaluated against templates to produce decision whether one person represented by currently evaluated signal is an authorized person (thus the signal must be highly similar or matching with templates). Simultaneously, if we let templates size as *N*, then we will have *N* score records. Every score records represent ratio of distance over magnitude for each vector pair [Test, Templates [N_i]] where $i = 1, 2, \ldots, N$. Correspondingly, we will have *N* decision records where we compare score in each pair with threshold 1 (one). We set one (1) as threshold as we already learn from our empirical experiment previously that threshold of 1 (one) is the minimum ratio (φ) to determine similarity. One signal is similar with each record on template if its ratio is less than 1.

4.3. Implementing arm's flex into authentication system prototype

We split our data from 120 records into 60 (50%) as templates and remaining half of 60 (50%) as test data. As we have 2 situations as *sD* and *sP*, we will have 30 records templates and 30 records too as test data in each of situation *sD* and *sP* making data in each situation times 60 records to be 120 records in total. In our experiment, we have 6 respondents as person *A, B, C, D, E,* and *F*. In Figure 6, in each situation we take 5 records as templates then let the remaining 5 records as test data labeled as authentic combined with other 25 records labeled as impostor. We split iteration as having individual situation meaning that, say in *sD*, we firstly iterate A as authorized user having authentic pattern then we will compare templates from A against other 30 records where from the 30 records test data, they consist of 5 test data from A and other 25 records from B, C, D, E, F (as impostors with 5 records per person respectively) making it in total as 30 records. We iterate the test from A to F by making use system flow as in Figure 5. These iteration tests try to simulate on use case as in Section 2 that one of the use case is during smartphone theft or lost.

After finishing system testing, we then get result as seen in modified confusion matrix as in Table 2 below:

Table 2. Result from Authentication System

		TP	TN	FP	FN
sD	A	5	23	2	0
	B	5	22	3	0
	C	5	20	5	0
	D	4	21	4	1
	E	5	21	4	0
	F	5	22	3	0
sP	A	5	23	2	0
	B	5	22	3	0
	C	5	21	4	0
	D	4	22	3	1
	E	5	21	4	0
	F	5	24	1	0

Upon testing, we further evaluate our authentication engine being judged by accuracy based on value of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). The accuracy is given by accurately distinguishing true positive as well as true negative. Practically, it means that the authentication system is able to determine legitimate user over illegitimate ones. The formula is to measure accuracy of our authentication system where N = 6 iterations given as:

$$\text{Accuracy} = \frac{\sum_1^N (Accurate)}{\sum_1^N (Error)} = \frac{\sum_1^N (TP+TN)}{\sum_1^N (TP+TN+FP+FN)} \qquad (4)$$

In a situation where phone is picked from desktop table, the accuracy is obtained from 158 correct pattern classifications out of 180 possible classifications resulting 87.8 % accuracy. In another situation where phone is picked up from pocket, the accuracy is obtained from 162 correct pattern classifications out of 180 possible classifications resulting 90% accuracy. These accuracy results are proving that simple authentication system can benefit from AF pattern with achieving pretty good authentication accuracy.

Moreover, as a behaviometrics, upon proposing AF pattern we must evaluate AF pattern in terms of two aspects that are (1) its false acceptance rate or false match rate (FAR/FMR) and (2) false rejection rate or false non-match rate (FRR/FNMR). FAR/FMR measures in percentage how much a system identifies a non-matching test pattern to templates as correctly match (accept error) where FRR/FNMR measures on how much a system identifies a matching pattern to its template as incorrect match (reject error). FAR/FMR is computed using formula (5) while FRR/FNMR is computed using formula (6) as follows:

$$FAR\ (FMR) = \frac{\#False\ Acceptance}{\#Total\ Impostors\ Attempts} \qquad (5)$$

$$FRR\ (FNMR) = \frac{\#False\ Rejections}{\#Total\ Authentics\ Attempts} \qquad (6)$$

In a situation where phone is picked from desktop table, we obtain FAR/FMR as from 21 patterns incorrectly accepted as matching patterns out of 150 impostors' attempts resulting 14 % FAR/FMR. In another situation where phone is picked up from pocket, we obtain

FAR/FMR as from 17 patterns incorrectly accepted as matching pattern out of 150 impostors' attempts resulting 11.3 % FAR/FMR.

As for FRR/FNMR, in a situation where phone is picked from desktop table, we obtain FRR/FNMR as the rejection of correctly matching pattern from 1 correct pattern out of 30 authentic patterns resulting 3.3 % rate. In a situation where phone is picked from users' pocket, we obtain FRR/FNMR as the rejection of correctly matching pattern also from 1 correct pattern out of 30 authentic patterns thus resulting 3.3 % rate too.

We already measure our simple authentication system through accuracy performance and FAR combined with FRR. The accuracy result is pretty promising while rates of FAR-FRR are considerably good. Eventually, we can deduce that those accuracy result and FAR/FMR combined with FRR/FNMR are proving that simple authentication system can benefit from AF pattern with achieving pretty good authentication accuracy and acceptable FAR/FRR measurements.

5. Conclusion

Throughout this paper, we present our preliminary study about AF as a subset of upper limb gesture when responding to call. The eventual aim in this research is to propose an implicit authentication system that both give smartphones a cognitive capability to augment its authentication system as well as capability on better understanding their users during protection. Although we have measured our system achieving pretty good authentication accuracy and acceptable FAR/FRR measurements, we still feel the necessary to increase accuracy and performance on FAR-FRR. Therefore, we foresee that to increase the accuracy of authentication system, the solid judgment on authenticating users can be achieved by a fusion of multiple sub authentication systems coming from multimodal human contexts. This AF-based authentication system can be one of several sub authentication system. Thus, we aim in future to complete our ongoing project on multimodal human contexts authentication system with smartphone with this arm's bending-based authentication system making it as the initial phase.

Acknowledgements

This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency)" (NIPA-2012-H0301-12-3005).

References

[1] Malaysia car thieves steal finger, http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm, **(2012)**.
[2] S. Furnell, N. Clarke and S. Karatzouni, Computer Fraud and Security, vol. 8, **(2008)**.
[3] Survey Shows Smartphone Users Choose Convenience over Security, http://www.confidenttechnologies.com/news_events/survey-shows-smartphone-users-choose-convenience-over-security, **(2011)**.
[4] Report on Consumer Behaviors and Perceptions of Mobile Security, NQ Mobile, January 2012, http://docs.nq.com/NQ_Mobile_Security_Survey_Jan2012.pdf, **(2012)**.
[5] D. Roman-Liu and T. Tokarski. Int. J. of Industrial Ergonomics, vol. 35, no. 1, **(2005)**.
[6] R. Greenstadt and J. Beal, Proceedings of the 1st ACM Workshop on AISec (AISec '08), **(2008)** 27 Oct; Virginia, VA, USA.
[7] M. Jakobsson, E. Shi, P. Golle and R. Chow, Proceeding of 4th USENIX Conference on Hot Topics in Security (HotSec'09), **(2009)** August 10-14; Montreal, Canada.

Authors

Ali Fahmi Perwira Negara received his Bachelor in IT from Multimedia University, Malaysia in 2010. He is currently a Master Degree student in School of Electronics and Computer Engineering, Chonnam National University, South Korea. His main research interests are computer & system security and ubiquitous & mobile computing.

Elyor Kodirov received his Bachelor in IT from Tashkent University of Information Technologies, Uzbekistan in 2011. He is currently Master Degree student in School of Electronics and Computer Engineering, Chonnam National University, South Korea. His main research interests are pattern recognition and image & video processing.

Mohd Fikri Azli bin Abdullah received his MSSE from University of Melbourne, Australia in 2005. Since August 2005, he was a lecturer at the Faculty of Information Science and Technology, Multimedia University, Malaysia. His main research interests are in the area of context aware system and mobile computing.

Deok-Jai Choi

Deok-Jai Choi received his PhD in Computer Science from University of Missouri-Kansas City, USA in 1995. Since 1996, he is a Professor in Department of Computer Science at Chonnam National University, South Korea. His main research interests are in the area of next-generation network, network management, and ubiquitous computing.

Guee-Sang Lee received his PhD in Computer Science from Pennsylvania State University, USA in 1991. Since 1995, he is a Professor in Department of Computer Science at Chonnam National University, South Korea. His main research interests are in the area of image processing, computer vision and video technology.

Md. Shohel Sayeed received his PhD in Engineering from Multimedia University, Malaysia in 2010. Currently he is a Senior Lecturer at Multimedia University, Malaysia. His main research interests are in the area of biometrics, pattern recognition, image and signal processing.