http://dx.doi.org/10.5392/IJoC.2013.9.2.014

A Study on Multibiometrics derived from Calling Activity Context using Smartphone for Implicit User Authentication System

Ali Fahmi Perwira Negara, Jaekeun Yeom
School of Electronics and Computer Engineering
Chonnam National University, Gwangju, 500-757, South Korea

Deokjai Choi
School of Electronics and Computer Engineering
Chonnam National University, Gwangju, 500-757, South Korea

ABSTRACT

Current smartphone authentication systems are deemed inconvenient and difficult for users on remembering their password as well as privacy issues on stolen or forged biometrics. New authentication system is demanded to be implicit to users with very minimum user involvement being. This idea aims towards a future model of authentication system for smartphones users without users realizing them being authenticated. We use the most frequent activity that users carry out with their smartphone, which is the calling activity. We derive two basics related interactions that are first factor being arm's flex (AF) action to pick a phone to be near ones' ears and then once getting near ear using second factor from ear shape image. Here, we combine behavior biometrics from AF in first factor and physical biometrics from ear image in second factor. Our study shows our dual-factor authentication system does not require explicit user interaction thereby improving convenience and alleviating burden from users from persistent necessity to remember password. These findings will augment development of novel implicit authentication system being transparent, easier, and unobtrusive for users.

Key words*: human, smartphone, implicit, authentication system, multibiometrics.*

1. INTRODUCTION

A Smartphone has been extensively adopted and integrated into the human life seamlessly. The omnipresent smartphone era marks a new computing paradigm where computing for human experience becomes ubiquitous and pervasive. The paradigm makes computing with smartphone more personalized yet powerful enough as it is strongly complemented by wide array of connectivity options and rich sensor input. Computing with the smartphone has enabled exciting massive user-generated contexts to be collectable with smartphone as a personal device. However, massive data generated from a vast number of smartphone users contain personal and sensitive data stored in smartphone. This situation raises security and privacy issues especially on unauthorized access to smartphone. Hence, the deployment of authentication system becomes very critical to ensure safe computing yet still being usable to user.

Addressing security and privacy issue, one of the methods to combat the potential damage from the unauthorized usage is to authenticate users for ensuring only authorized users to ably access their smartphone. Most smartphones deploy an authentication system which transfers the burden to authenticate to the user by depending on secret-knowledge (password, graphical patterns) that must be remembered all the time. The burden leads to several loopholes like using easy-guessed passwords, shared credentials, stolen passwords, and so on. Furnell et al. [1] reported in a survey that users want increased security authentication that is transparent when authenticating users for the sake of their convenience. The solution to this user demand is to develop an authentication system that implicitly authenticates users making use of user-generated data that can be collected in multiple modalities. The idea of this authentication system will raise a notion of future generation authentication system giving a cognitive security capability to a smart device like smartphone. This typical authentication system is suitable being geared towards ubiquitous computing security as the future of computing era.

In this paper, we present our study on authentication system using a smartphone in a users' calling activity scenario. The idea can be implemented with special smartphone apps that will enable the authentication mode upon request. The apps will trigger a notification to the authenticating parties only when needed. The users will wait when the authenticating parties

* *Corresponding author, Email : ali.fahmi.pn@gmail.com*
Manuscript received Oct. 29, 2012; revised Jun 07, 2013; accepted Jun 17, 2013

"callback" to users, which by that time the users will be authenticated implicitly. The system will implicitly and transparently authenticate customers when they initiate conversation using a smartphone thereafter. The authentication system will use combination from behavioral biometrics i.e. user's arm flexing (AF) and physical biometrics i.e. user's ear shape captured by the smartphone front camera when the smartphone gets near to user's ear. With this approach, our system might (1) alleviate burden of users from remembering secret knowledge, (2) are being inexpensive in deployment, and (3) are being unobtrusive and transparent to users.

The rest of this paper will be organized as follows. Section 2 discusses authentication systems that have been in market and researches environment. Section 3 presents aspects underpinning the conception of the new authentication idea and then the proposed novel authentication system design. Section 4 discusses and presents our experiments and their results. Section 5 summarizes and concludes our study.

2. CONVENTIONAL AUTHENTICATION SYSTEM

An authentication system for smartphones is critical and thus gaining many research interests. The rapid growth of smartphone users and vast trend for smartphones becoming a personal device carrying sensitive data are being the obvious reasons. Authentication methods for smartphone have encompassed many approaches as being implemented either using single or multi authentication factors. When relying on secret knowledge, smartphones use secret knowledge like passwords either from alphanumeric PINs to graphical click-based or pattern passwords [2][3]. This type of authentication system imposes some burdens to users to remember the secret knowledge. On the other hand, some authentication systems use idea of authenticating someone based on one's own characters either physical or behavioral human traits. There are few smartphones incorporating physical biometric features like those reported in [4] and [5]. In spite of physical biometrics' good performance, physical traits biometrics-based authentication system in general poses several limitations. They are considered as being expensive in smartphone setting, having privacy disaster issue towards stolen and possible forged biometrics' feature of individuals, and even hazardous and harmful to individuals as in case of stolen car at 2005 in Malaysia [6].

Multi-factor authentication (MFA) especially using a mobile phone has been proposed around as in [7] researchers propose on combination One-Time Password (OTP) and SMS-based factors for accessing services using mobile phone. More generally, ideas on MFA have been varying from a combination of tokenized pseudo-random number and the user specific fingerprint as shown in [8] up to a combination of graphical password and image challenge in [9]. However, none of them addresses obtrusiveness and user inconvenience issue during their authentication processes thus deemed unusable effectively according to user perspective as reported in [10]. According to that report, users tend to choose their devices unlocked (reluctant to be password-protected) and perpetually are logged on leaving to least or no protection at all.

Conventional knowledge-based and token-based authentication systems have several known weaknesses. Commonly, they provide only one-time verification within a lengthy period such as authenticated only upon switch-on then perpetually open for the remaining session. In addition, many users are reluctant to keep their devices secured as they tend to let their devices open because they feel the usage of common authentication like phone PIN is of inconvenience [2].

In those weaknesses, biometrics authentication in smartphone offers promising answers as no passwords to remember, nothing written/given can be lost as in token, no need to bring things (token) everywhere, and it is harder to bypass. However, most biometrics face less suitability issue to be deployed on smartphones. In fingerprint-based authentication system, it is hindered by expensive deployment and potentially dangerous as reported in [6]. Gait recognition by camera or motion requires lengthy observation. Hand geometry is not applicable due to size requirement. Thus, to accommodate the usability while preserving high degree of recognition accuracy, we must combine authentication factors that are convenient to users with strong, contextual algorithm.

3. GRADED & IMPLICIT AUTHENTICATION SYSTEM

In order to put users in convenience, we select authentication factors that are natural or preferred by users. Being natural means that an authentication process is frequently performed thus common by users and/or simple to perform. As we see in Figure 1, a common activity among smartphone users is where authentication usually is not associated with authentication process (implicit authentication). Moreover, process authentication must be done during an activity that originally intended to other aims apart from authentication. According to survey presented in Figure 1, the most activity users do is making phone calls.

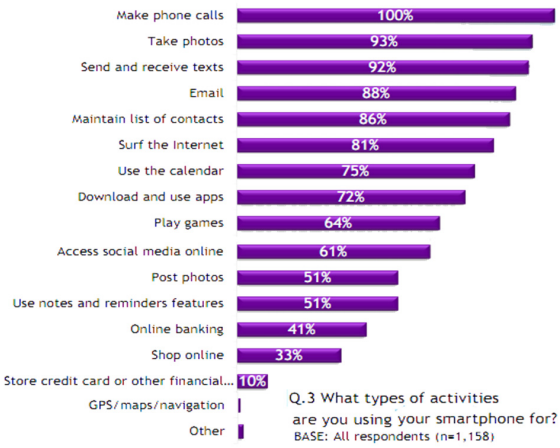

Fig. 1. Types of activities among smartphones and users

The rationale of multibiometrics combining two biometrics factors comes down to a fact that one level of authentication is not always desired by users in terms of usability. Hence, we propose to rely on multi level of authentication score and its tolerance in our proposed system called as graded security system. Through this approach, we will evaluate the degree of

criticality in a condition when authentication system takes place, considering the degree level of access rom requesting users. This approach will assign different levels of security to different applications by applying different strength of authentication requirement over various applications. For an instance, a non-sensitive application like games or educational applications typically doesn't need protection thus protection is not necessary by graded security system. Unlocking a device or opening a camera phone is relatively less critical thus an authentication algorithm with moderate error recognition tolerance is acceptable. For sensitive access to financial banking applications, phone call privileges, messaging, and so on, we must deploy a mechanism that achieves recognition error tolerance as slightest as possible (like system with 98% accuracy). Here, the idea of graded security implement basic principle of security that is to protect what is worth more beyond the cost of a security protection.

Graded security can be seen as either a role-based hierarchical system to provide access to certain areas of the secured device. In our system, we enforce security clearances representing levels of security to be fulfilled. The fulfillment of clearances can be done by having an authentication score equal or more than a score threshold in each level. The user has to provide either one or two factor authentication to get authentication values by which she can be evaluated whether accessible to data or not. Here, we can see that each access request has to be authenticated individually differently. This is contrast to conventional authentication systems that apply one chunk of access to users, who can access everything on the system once authentication has been passed. On our smartphone, the user may need to provide the first factor of authentication like arm's flex (AF), and then further authentication with user's ear shape whenever to log into his or her financial account.

We believe that if users are asked to do something they frequently do, then it will come natural and convenient. In a phone call, there are two interrelated actions picking smartphone (AF) and putting it near the ear (ear image) visualized in Figure 2. In this common activity, users are already accustomed to perform in time-to-time basis. Besides, different to a specific 3D gesture to authenticate, AF edges it out due to the simplicity and frequent action over one that is uncommon to perform (thus awkward and not natural). The same thing goes to ear shape biometrics. The authentication process doesn't need a special, explicit posing face, for example, in face recognition but just an action naturally listening to phone speaker.

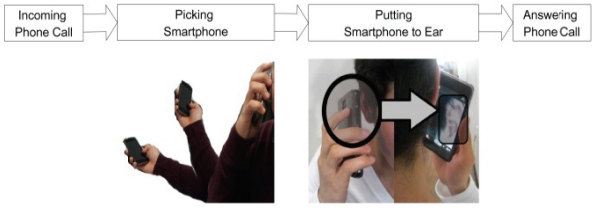

Fig. 2. Calling sequence involves multibiometrics

3.1 Arm's Flex-based Authentication System Module

Roman-Liu et al. [11] study on relationship between upper limb strength/force concluded that the posture affects the strength of upper limb strength during several motion simulations. While the arm is the biggest portion of upper limb and postural can be interpreted as different upper limb in size and length to result in unique strengths/forces, we can infer that 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 theory of kinematic 2nd Newtonian Law, where acceleration is proportionally related to force exerted over a mass (a = F/m) in which bending action will result in different unique traits due to unique force strengths exerted from various postures and biological muscular structures.

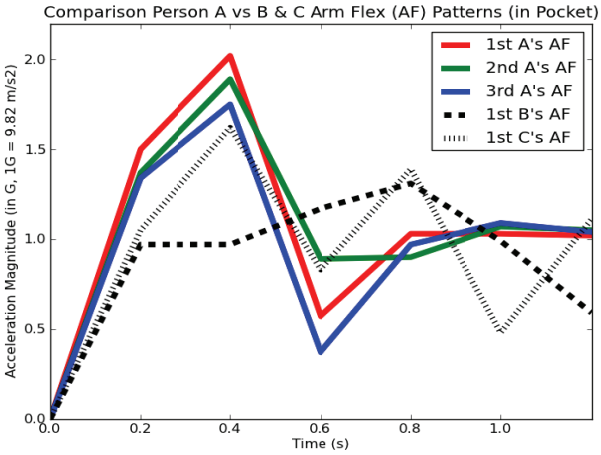

Fig. 3. Comparison of A's AF versus B's and C's AF

We then study the acceleration in AF generated by respondents from our department members using our smartphone. In our study, we use accelerometer outputs as a vector in respect to a theory of physics related to the gravity, in which is represented as = (A_X, A_Y, and A_Z) in 3D spaces. A_X, A_Y, and A_Z are projections of such output vectors onto X, Y, and Z axes respectively where |A| is the amplitude [12] computed from the square root of summation over each projections' to the power of two in each axis. Our initial study [13] uses the acceleration magnitude to discover patterns' trend among AF patterns generated by our respondents. It shows that an AF from each different person A, B, and C has different pattern trend visually as depicted in Figure 3. On the other hand, an AF from one person A has similar pattern trend portrayed in Figure 3 as well. Hence, the AF will be able to serve as an authentication factor from behavior biometrics perspective.

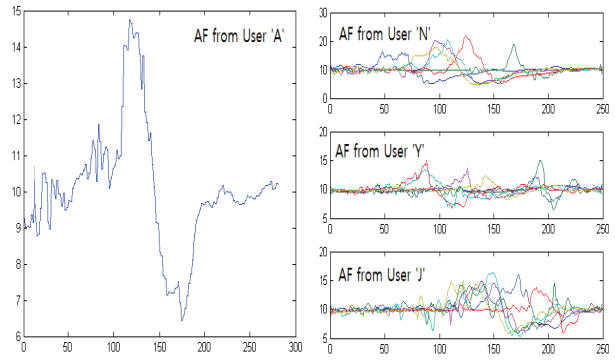

Fig. 4. Arm flexes generated from different users

Our first authentication system component is based on arm flex force exerted to a smartphone when smartphone is being lifted for calling/receiving a phone call. In this component, user flexing activity while picking up a phone will be recorded and measured. In our research, we use pattern similarity matching and alignment algorithm to figure out whether one user can be distinguished from others.

Prior to similarity and matching evaluation, in our experiment, we realize that there are at least two main sources of noise when dealing with accelerometer built-in smartphone. They are irregular sampling rates and the noise inherent in discrete physical sampling of a continuous function. Moreover, the signal from one to another may also vary due to various picking style as well as possible shifted time period when doing AF as in one individual signal in Figure 4 (left). Thus, we need to perform preprocessing to obtain accurate analysis and to extract relevant information.

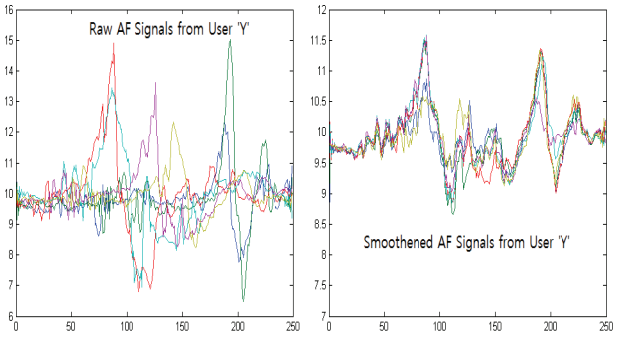

Fig. 5. Arm flexes generated by single individual

From several users' individual signals, we group them into the sets on which we preprocess the signal sets with signal linearization and time interpolation. Thereby, we will have signals with standardized length of 250. The preprocessing will either stretch short raw signals (l < 250) or shrink the long raw signal (l >250) into normalized signals without changing the shape of waveform or changing the trend and features. The linearization is necessary because in smartphone acceleration magnitude being captured is sampled and recorded irregularly due to the nature of smartphone accelerometer. By doing this way, the problem of inconsistent signals caused by irregular sampling is addressed.

Furthermore, after linearization and interpolation, we also want to solve the noise problem inherent in discrete physical sampling. For this, smoothing function is useful to reduce the noise that appears in signal. We apply 2n+1-moving average filter to reduce noise with n = 2 after several experiments show that it is the best smoothen factor in 2n+1-moving average that does not make signals lose information. The result over the final preprocessing is ready to be used for similarity and matching evaluation algorithm as seen in Figure 5. In Figure 5 (right), the signals are grouped into one set as template signals (reference) and then contrasted to test signals from user either Y or other users.

In pattern similarity and matching evaluation, we use Dynamic Time Warping (DTW) [14] to compute the minimized distances among aligned signals denoting the more minimized distance between one to others, the greater similarity they are. In this approach, suppose that we have two AF accelerations measured from users represented in time series V and W with length m and n respectively as represented as V = $\{v_1, v_2,\ldots,v_m\}$ and W = $\{w_1, w_2,\ldots,w_n\}$ then we need to construct m-by-n matrix where (i^{th},j^{th}) element of the matrix will contain the distance (v_i, w_j) between two points v_i and w_j. A warping path P exists as a contiguous set of matrix elements that defines a mapping between V and W. The k^{th} element of P is defined as $p_k = (i,j)_k$ so we have P = p_1, p_2, …, p_k that satisfy max(m,n) ≤ K ≤ (m+n-1). There are many warping paths but we will concern on path minimizing the warping cost as:

$$\mathrm{DTW}(V,W) = \min\left\{\sqrt{\sum_{k=1}^{K} w_k}/K\right\} \quad (1)$$

The K in the denominator is used to compensate for the fact that warping paths may have different lengths. This path can be found very efficiently using dynamic programming to evaluate the following recurrence which defines the cumulative distance D(i,j) as the distance $d_{i,j}$ found in the current cell and the minimum of cumulative distances of adjacent elements as follows:

$$D(i,j) = d_{i,j} + \min\{d_{i-1,j-1}, d_{i-1,j}, d_{i,j-1}\} \quad (2)$$

We use cumulative distance in eq. (2) when we try to find and match similar signals that belong to one user in contrast to other signals from other users' AF acceleration magnitude. Among 25 respondents' data with each performs ten repetitive telebanking activity simulation, we collect 250 data in total. We divide signals from one user to be template signal as references and as testing signals. From each user generating ten signals, we group into two sets making six into template signal and remaining four as the ones we test the similarity against the template. We obtain AF acceleration magnitude resulting in typical signals in waveform as denoted in Figure 8 where we present one individual signal from a user as well as two sets of signals in which each set has six signals because each set serves as template signals.

In our experiments, we contrast each of test signals with sets of template signals (references). Figure 6 depicts how one signal from user 'A' is being compared to two sets of user 'A' template signals itself and another user (user 'E'). We can intuitively perceive that a single signal being contrasted is strongly similar to the right ('A') templates than the left ('E') templates. In the left template similarity and matching, we can see that the slope and waveform shape perceivably different compared to the right template one when the slope between test signals is almost as steep as the template A. The right one also has almost identical waveform shape between test and template.

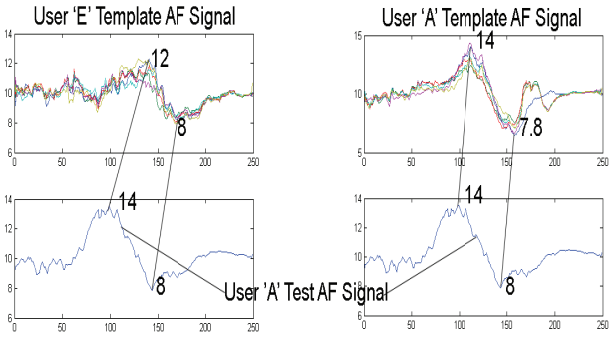

Fig. 6. Comparison of real owner 'A' AF versus impostor 'E'

3.2 Ear Image-based Authentication System Module

The second component of our authentication system is based on physical biometrics from ear image taken by smartphone front camera when smartphone is detected as getting near to ear when a user picking phone for calling/receiving a phone call. In this telebanking authentication, the front camera of smartphone will capture the ear image once user's ear detected and then perform preprocessing. Before it can capture successfully, users must make sure their ears are not covered nor hindered by physical objects like cap or long hair, just like face blocked by spectacles or face covers. Once finished, ear image will be represented with Local Binary Pattern (LBP) representation with mathematically computed as in Eq. (3) and rotational invariant geometric analysis as depicted below in Figure 7 and Figure 8.

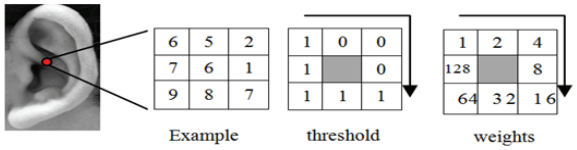

Fig. 7. Visual LBP operations on one sample image

$$\mathrm{LBP}_{P,R}(x_c, y_c) = \sum_{p=0}^{p-1} s(g_p - g_{pc}) 2^p, \; s(x) \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases} \quad (3)$$

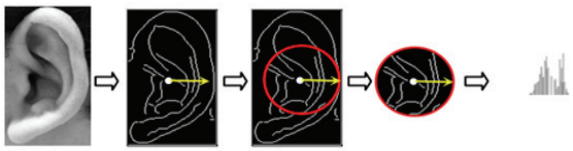

Fig. 8. Geometric analysis on one sample image

Ear biometrics has been long dubbed by French criminologist Alphonse Bertillon since 1890 as the reliable passive biometrics to discriminate criminals. There are a number of advantageous factors using ear shape compared to face as a biometrics. First, ear is immutable during human life as ascertained by Imhofer [15], where a face changes more significantly with age. Moreover, color distribution in ear is more uniform than in a human face, iris, and retina i.e. while working with grayscale we do not lose much information. Besides, the ear is smaller than face so a system can work faster and more efficient with the images in lower resolution. Ultimately, in our system, ear recognition will best fit as another (the second one) factor because the ear is passive biometrics that using ear shape will enable implicit and transparent authentication to users.

To represent an ear, we use Local Binary Pattern (LBP) [16] to extract its feature in biometric and rotation invariant geometric analysis as in Figure 7 and Figure 8 respectively. This operator works with the eight neighbors of a pixel, using the value of this center pixel as a threshold. If a neighbor pixel has a higher gray value than the center pixel (or the same gray value) than a one is assigned to that pixel, else it gets zero. The LBP code for the center pixel is then produced by concatenating the eight ones or zeros to a binary code as shown in Figure 7 using LBP operator as denoted in Eq. (3).

The ear representation will be having numerical sub regions that eventually translated into a histogram. For example, one ear image in LBP operation divided into four regions can have 59 contiguous sub regions per region so resulting in 236 numerical sub regions in total. In geometric analysis, we will calculate another two additional values of mean and variance values derived from Euclidean distance computed from a point in the most outer edge of ear image with its center. This analysis is independent from rotation movement from users and is important to be robust from various rotation possibly made by users related to phone-on-ear handling style.

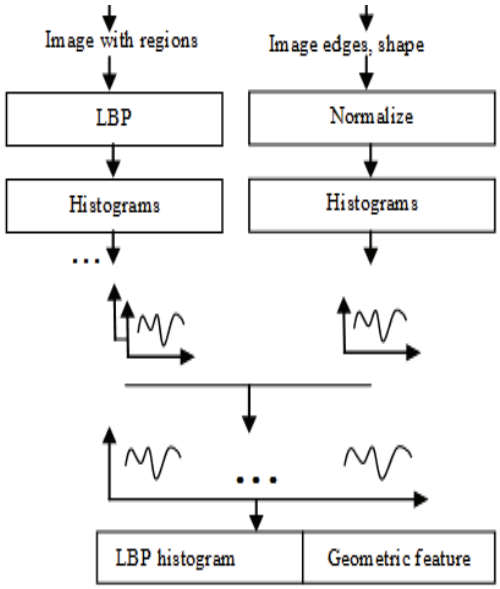

Fig. 9. Histogram LBP & GA as feature for authentication

In a pictorial description, Figure 9 visualizes the process to get ear representation that is used to compare the similarity of one signal to others in which similar signals belong to the same user. Two techniques will obtain values being all concatenated and translated into histogram. We use this histogram to compare similar ear images which belong to a particular user.

4. AUTHENTICATION EXPERIMENT

In the first component of authentication system, we denote two vectors representing each acceleration magnitude resulted from AF templates in each cycle within similar time period from t_1 to t_n in vector space $X = \{x_1, x_2, \ldots, x_n\}$ while evaluated AF test data as $Y = \{y_1, y_2, \ldots, y_n\}$. Our authentication system uses dual components on which each individual component will be able to score maximum score of 1.00 so that in total the maximum score will be 2.00.

We use a nearest neighbor classifier with basis of computation for each score of factor based on (1) minimized cumulative distance obtained from the DTW algorithm for authentication using AF (1st score) and (2) Euclidean distance from a histogram as an ear representation for authentication using ear image (2nd score). We statistically prove and determine the rank of nearest template patterns according to

each test signals.

Table 1. Matching score by k-NN classifier for one AF sample

DTW	Sets of Templates									
	A	***J***	***K***	***H***	***E***	***NH***	***NM***	***T***	***Y***	***S***
AFT1A	**7**	86	55	258	122	89	156	83	245	144
	56	155	**54**	233	176	103	193	97	233	132
	27	126	71	187	211	122	223	121	203	99
	19	157	153	152	187	117	198	122	187	102
	13	170	96	96	113	154	221	153	198	112
	22	74	151	153	197	137	110	132	183	117

Table 2. Matching score by k-NN classifier for one image sample

D	Sets of Templates									
	A	***J***	***K***	***H***	***E***	***NH***	***NM***	***T***	***Y***	***S***
HISTT1A	**342**	1,098	1,337	1,898	1,267	2,003	2,445	1,651	1,376	1.907
	851	1,256	1,258	1,137	1,256	1,446	1,256	1,532	1,437	1,256
	515	1,034	1,631	1,002	1,037	1,075	1,043	1,631	1,990	1,309
	703	1,941	1,311	1.445	1,097	1,044	1,337	1,746	2,488	1,900
	464	1,578	1,545	1,179	1,348	1,573	1,328	1,786	1,443	1,872
	388	1,254	1,150	1,234	1,573	1,200	1,054	1,497	1,254	1,003

Our nearest neighbor classifier (k-NN Classifier) yields one table per each test signal from AF and histogram comparison from ear image with their sets of templates as exemplified in Table 1 and Table 2 respectively. In Table 1, out of 6 test data from user A is found matching with five A templates thus generating result 5 out of 6 to score 0.833. In Table 2, for each ear image test data from A to template of A's ear image, it is found matching with all six A templates thus generating result 6 out of 6 to score 1.00.

In our AF disposal, we have four test signals per user thus we have pattern similarity and matching 40 times experiments from ten respondents. In each experiment time, the test signal will compute minimized cumulative distance using DTW of one test signal with ten sets of templates. Hence, we will have 40 matching score tables like in Table 1. In each table, a majority voting is considered when the NN classifier has ranked the similarity and matching among one test signal to signal templates like in Table 1. In the case of Table 1, because ranks 1 to 6 are all actually from template A, we decide that T1 (test data no. 1) from A belong to user 'A' because when being tested 5 out of 6 templates are successfully categorized as 'A'. In other exemplary case, say if a signal is contrasted to sets of templates with the NN classifier that rank 1-3 belong to user 'A', 4-5 belong to user 'H', and rank 6 belongs to user 'Y', the authentication system decides a signal belongs to user 'A' based on majority voting. Should the voting result is evenly to one template and non-template, e.g. 3 for 'A' and 3 for 'K' we consider this situation as unmatched decision. However, during experiment we never encounter such this situation.

In addition to AF, we also experiment with 40 test ear image data that will be compared with 60 templates from ear images because in our disposal, just like AF acceleration magnitude signals, we have four ear images per user. Hence, we have pattern similarity and matching in ear images 40 times experiments from ten respondents. In each experiment, each testing process will compute Euclidean distance of one ear image represented as histogram as in Figure 12 with ten sets of templates where each set contains six templates. Hence, we will have 40 tables like Table 2. In each table, a majority voting is also considered during NN classifier ranking process just like in AF experiment cases.

Table 3. Overall experiment result (Confusion Matrix)

	A	***J***	***K***	***H***	***E***	***NH***	***NM***	***T***	***Y***	***S***
A	**3**	0	0	0	0	**1**	0	0	0	0
J	0	**4**	0	0	0	0	0	0	0	0
K	0	0	**4**	0	0	0	0	0	0	0
H	0	0	0	**4**	0	0	0	0	0	0
E	0	0	0	0	**4**	0	0	0	0	0
NH	0	0	0	0	0	**3**	**1**	0	0	0
NM	0	0	0	0	0	**1**	**3**	0	0	0
T	0	0	0	0	0	0	0	**4**	0	0
Y	0	0	0	0	0	0	0	0	**4**	0
S	**1**	0	0	0	0	0	0	**1**	0	**2**

In all our experiment either in AF or ear image, we have T1-T4 belong to A or to have T5-T8 belongs to J and so on. After experiment, we obtain experiment results as in Table 3. Overall experiment will depend on a value δ denoted as a threshold overall score value to determine whether a score is accepted as successful authentication or not. We test 3 thresholds as δ_1, δ_2, and δ_3. The higher threshold value is, the stricter authentication score is demanded. The δ with value of 1.2 is easier to achieve for impostor. Our δ values from δ = {1.4, 1.6, 1.8} produce various results. The worst accuracy performance is achieved when δ value is set to 1.8. Overall experiment result for δ = 1.8 from combining AF and the ear image in authenticating users can be observed and learned being presented as confusion matrix as in Table 3. From Table 3 our experiment shows our approach for user authentication achieves correct user authentication 35 times out of 40 times experiment yielding 87.5 % system accuracy with δ = 1.8. As for remaining δ values, our system produces 92.5 % and 95% for δ values of 1.4 and 1.6 respectively.

5. CONCLUSION

We present our study on a novel idea for authentication system based on two unobtrusive biometric factors generated from a common calling activity using a smartphone. The deployment of our idea manages to address implicit and

transparent authentication to users so that the increased usability in security system is expected. In addition, this idea lessens the hassles of remembering password or any secret knowledge like passphrase, secret number or even security token.

We put considerations as our future work to study many aspects of each user individual style to pick a smartphone and swing it with her arm from many different positions. A further analysis with Receiver Operating Characteristics (ROC) is also currently performed so that the performance of the authentication system can be clearly seen. Moreover, a comparison study to other multibiometrics systems is also being carried out.

We present our study about a novel approach of security system in smartphone empowered intelligently by cognitive security capability for smartphone. We use dynamic, behavioral AF as first authentication factor and static, physiological ear shape image as second authentication factor. Our study shows that a context of call activity is effective and feasible to implement special authentication system being implicit and transparent. Our system characterizes an authentication security system for smartphone users being natural, convenient thus improving usability and user acceptance.

6. ACKNOWLEDGEMENTS

This research was supported by Basic Science Research program through the National Research Fund of Korea (NRF) funded by the Ministry of Education, Science, and Technology (MEST), Korea (2012-035454) and by the Ministry of Knowledge Economy (MKE), Korea, under Information Technology Research Center (ITRC) support program supervised by National IT Industry Promotion Agency (NIPA) (NIPA-2012-H0301-12-3005).

REFERENCES

[1] S. Furnell, N. Clarke, and S. Karatzouni, “Beyond the PIN: Enhancing User Authentication for Mobile Devices,” *Computer Fraud & Security*, vol. 8, August 2008, pp.12-17.

[2] S. Chiasson, R. Biddle, and P. C. v. Oorschot, “A second look at the usability of click-based graphical passwords,” *Proc. SOUPS '07*, 2007, pp.1-12.

[3] Google, Inc., “Enhancing Security with Device Management Policies”, Retrieved September 15, 2012, from Android OS Developer Guide: http://developer.android.com/training/enterprise/device-management-policy.html [Online]

[4] M.A. Carrera-Perpinan, “Compression neural networks for feature extraction: Application to human recognition from ear images”, *Master (M.Sc) Thesis*, Technical University of Madrid, 1995

[5] H. Chen and B. Bhanu, “Human Ear Recognition in 3D,” *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol.29, no.4, April 2007, pp.718-737.

[6] J Kent, “Malaysia car thieves steal finger”, Retrieved March 31, 2005, from BBC News UK: http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm [Online]

[7] F. Aloul, S. Zahidi, and W. El-Hajj, “Multi Factor Authentication Using Mobile Phones,” *Int. J. of Math and Comp. Sci.*, vol. 4, no. 2, July 2009, pp. 65–80.

[8] A.T.B. Jin, D. N. C. Ling, and A. Goh, “Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number,” *J. of Pattern Recognition* vol. 37, no. 11, November 2004, pp.2245-2255.

[9] A.P. Sabzevar and A. Stavrou, “Universal Multi-Factor Authentication Using Graphical Passwords,” *Proc. SITIS’08*, pp.625-632.

[10] Confident Technologies, Inc., *Survey Shows Smartphone Users Choose Convenience over Security*, Retrieved September 29, 2011, from Confident Technologies’ News Event: http://www.confidenttechnologies.com/news_events/survey-shows-smartphone-users-choose-convenience-over-security [Online]

[11] D. Roman-Liu and T. Tokarski, “Upper limb Strength in Relation to Upper Limb Posture,” *Int. J. of Industrial Ergonomics* vol.35, no.1, January 2005, pp.19-31.

[12] A.K. Bourke, J.V. O’Brien, G.M. Lyons, “Evaluation of A Threshold-based Tri-axial Accelerometer Fall Detection Algorithm,” *J Gait and Posture* vol. 26, no. 2, July 2007, pp.194-199..

[13] Ali Fahmi PN, E. Kodirov, M. F. A. Abdullah, D. Choi, and S. Sayeed, “Arm’s flex when responding Call for Implicit User Authentication in Smartphone,” *Int. J. of Security and Its Applications* vol. 6, no. 3, July 2012, pp. 58-64.

[14] D. J. Berndt and J. Clifford, “Using Dynamic Time Warping to Find Patterns in Time Series,” In *AAAI Technical Report ’94 Workshop on Knowledge Discovery in Databases (KDD-94)*, pp.359-370

[15] M. Burge and W. Burger, “Ear Biometrics”, In A. Jain R. Bolle and S. Pankanti, editors, *Biometics: Personal Identfication in a Networked Society*, Kluwer Academic, Dordrecht-The Netherlands, 1998, pp. 273-286.

[16] T. Ojala, M. Pietikäinen, and D. Harwood, “A comparative study of texture measures with classification based on feature distributions,” *Pattern Recognition*, vol. 29, no.1, January 1996, pp. 51-59.

Ali Fahmi Perwira Negara

He received the B.IT in information technology from Multimedia University, Malaysia in early 2011. Since 2011, he has been with the Advanced Network Lab, Chonnam National University, Gwangju, Korea, pursuing a Master degree in Computer Engineering. His main research interests include security in computer & system, ubiquitous computing, and pattern recognition for cognitive security in mobile devices.

Jaekeun Yeom

He received the B.S in information communication from School of Electronics and Computer Engineering, Chonnam National University, Korea in late 2011. Upon graduation, he has been pursuing a Master degree with the Advanced Network Lab, Chonnam National University, Gwangju, Korea, for a Master degree in Computer Engineering. His main research interests include network management and sensor network.

Deokjai Choi

He received the B.S., M.S in computer science from Seoul National University, Korea in 1982 and from KAIST 1984 respectively and also received Ph.D. in computer science and telecommunication from University of Missouri-Kansas City, USA in 1995. Since 1996 until now, he has been serving as Professor in School of Electronics and Computer Engineering, Chonnam National University, Korea. His main research interests include topics on context-awareness, pervasive computing, sensor network, future internet, and IPv6.