A real-time in-air signature biometric technique using a mobile device embedding an accelerometer

J. Guerra Casanova, C. Sánchez Ávila, A. de Santos Sierra, G. Bailador del Pozo, and V. Jara Vera

Centro de Domótica Integral (CeDInt-UPM) Universidad Politécnica de Madrid
Campus de Montegancedo, 28223 Pozuelo de Alarcón, Madrid
{jguerra,csa,alberto,gbailador,vjara}@cedint.upm.es

Abstract. In this article an in-air signature biometric technique is proposed. Users would authenticate themselves by performing a 3-D gesture invented by them holding a mobile device embedding an accelerometer. All the operations involved in the process are carried out inside the mobile device, so no additional devices or connections are needed to accomplish this task. In the article, 34 different users have invented and repeated a 3-D gesture according to the biometric technique proposed. Moreover, three forgers have attempted to falsify each of the original gestures. From all these in-air signatures, an Equal Error Rate of 2.5% has been obtained by fusing the information of gesture accelerations of each axis X-Y-Z at decision level. The authentication process consumes less than two seconds, measured directly in a mobile device, so it can be considered as "real-time".

Key words: Biometrics, gesture recognition, accelerometer, mobile devices, dynamic time warping, fuzzy logic.

1 Introduction

Nowadays most mobile devices provide access to Internet where some operations may require authentication. Looking up the balance of a bank account, buying a product in an online shop or gaining access to a secure site are some actions that may be performed within a mobile phone and may require authentication. In this mobile context, biometrics promises to raise again as a method to ensure identities. Some works trying to join classical biometric techniques in a mobile scenario have been already developed, based on iris recognition [1], face [2], voice recognition [3] or multimodal approaches [4].

In this article, a new mobile biometric technique is proposed. This technique is based on performing a 3-D gesture holding a mobile device embedding an accelerometer [5]. This gesture is considered as an in-air biometric signature, with information in axes X-Y-Z. This biometric technique may be considered as a combination between behavioral and physical techniques, since the repetition of a

gesture in the space depends not only on the shape and the manner of performing the in-air signature but also on physical characteristics of the person (length of the arm, capability of turning the wrist or size of the hand holding the device). This 3-D signature technique proposed is similar to traditional handwritten-signature [6], but adapted to a mobile environment.

In this proposal, feature extraction is directly performed within a mobile device without any additional device requirement. Besides, through this biometric technique based on 3-D gestures, it is intended to perform all the authentication process inside the device, executing all the algorithms involved without any additional device or server. Therefore, and due to the increasing process power of mobile devices, this biometric technique would achieve an important requirement: "real-time".

This article is divided in the following Sections. Firstly, Section 2 describes the method of analysis of gesture signals involved in this study. Next, Section 3 details the in-air gesture biometric database created to support the experiments of the article. Section 4 includes an explanation of the experimental work carried out, as well as Time and Equal Error Rate Results obtained. Finally, in Section 5, conclusions of this work and future lines are introduced.

2 Analysis method proposed

In this article, an algorithm based on Dynamic Time Warping [7] has been developed to analyze different signals, in order to elucidate whether a sample is truthful or not. For that purpose, the algorithm tries to find the best possible alignment between two signals in order to correct little variations at the performing of the gesture.

A score matrix is calculated for each point of both sequences [8], and later, the path in this matrix that maximizes this score is obtained. Any vertical or horizontal movement in this path implies adding a zero value in a sequence to correct little deviations. The algorithm includes a fuzzy function in the score equation [9] representing to what extend a user is able to repeat a gesture. The score equation is shown in Equation 1.

$$s_{i,j} = \max \begin{cases} s_{i,j-1} + h \\ s_{i-1,j-1} + \Delta \\ s_{i-i,j} + h \end{cases} \tag{1}$$

where h is a constant, known as gap penalty in the literature [10], whose value is obtained to maximize the overall performance and Δ is a fuzzy decision function that represents a Gaussian distribution:

$$\Delta = e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{2}$$

where μ and x are the values of the previous points in base to whom the score of the new points (i, j) are calculated. Finally, σ is a constant stating to what extend two values are similar.

Despite a user performs the same gesture holding the mobile device in the same way, there will be always some little variations on the speed and manner the user performs his/her 3-D signature. This algorithm aligns a pair of signals, correcting those little deviations without compensating high differences by including some zero values and interpolating them in order to maximize the overall score function. As a result of this algorithm, signals length is duplicated.

When the optimal alignment of the signals is accomplished, Euclidean distance is calculated in order to measure the differences between aligned signals. Consequently, a numerical value is obtained at the end of the analysis process; the lower the value is, the more similar the analyzed signals are, and viceversa.

3 Database description

This article is developed with a database of 34 gestures of different users. This database has been obtained in two sessions:

A first session where each user had to invent an identifying gesture and perform it in the air holding an embedding accelerometer device. This gesture is considered as the in-air biometric signature of this biometric technique based on gesture recognition. In this first session, 34 volunteers (from ages 19 to 60, 15 women and 19 men) have participated performing the gesture they would choose as their in-air signature in this technique by holding a device embedding an accelerometer. For this purpose, an application for iPhone 3G (an embedding accelerometer mobile device) has been developed to obtain the accelerations of the movement of the hand on each axis X-Y-Z while carrying out a gesture at a sampling rate of 10 ms; frequency precise enough to get representative signals of a hand movement in the air [11].

Each user has repeated 7 times his/her gesture, with intervals of 10 seconds in between, to reduce dependence between samples. Some instructions have been provided to help the volunteers in this aim, in order to perform remindful and complex enough gestures so that anyone except the truthful user may reproduce it immediately. Furthermore, all of these sessions of performing new gestures have been recorded on video.

Users have reacted differently to the task of inventing a gesture repeatable by them and not easy to be forged by anyone who might see them. In fact, users have solved this proposal by:

- Writing a word or a number in the air.
- Performing an usual gesture: Playing the guitar, an own salute, using a tennis racket...
- Drawing a symbol in the air: A star, a treble, a clef...
- Drawing something real in the air: Clouds, trees...
- Performing a complex gesture by concatenating simple gestures as squares, triangles, circles, turns...
- Making their own signature in the air.

In this study, 18 of 34 gestures (53%) are the truthful signatures of each person performed in the air whereas the rest are gestures of unlike levels of difficulty.

At the end of this first session, all volunteers have answered a survey to assess (1 very good - 5 very bad) different issues of the in-air gesture biometric technique proposed. Results are presented in Table 1:

Question	Average	Mode	Standard deviation
Ease to invent an in-air signature	2.1	2	0.65
Ease to repeat an in-air signature	1.9	2	0.45
Collectively of the technique	1.9	1	0.71
Acceptability of the technique	2.7	2	0.85

Table 1. Volunteers answers to different issues in order to validate the feasibility of the technique from user-experience point of view.

From those answers, it can be inferred that users had low difficulty in inventing and repeating a 3-D gesture with a mobile device. As biometric data are acquired in a non-intrusive manner, users have evaluated the collectively of the technique as very low [12]. Besides, users have felt secure and comfortable when biometric characteristics have been extracted, so acceptability also receives a low score.

Moreover, volunteers have been asked to compare the confidence of this in-air gesture biometric technique proposed respect to iris, face, handwritten signature, hand and fingerprint recognition techniques. In average, participants evaluated the confidence of in-air gesture signature over handwritten signature, next to face and hand recognition and far from iris and fingerprint.

On the other hand, a second session has been performed by studying the videos recorded in the previous session. In this session, three different people have tried to forge each of the 34 original in-air biometric signatures. Each falsifier attempted to repeat each gesture seven times.

As a result of both sessions, 238 samples of truthful gestures (34 users x 7 repetition) and 714 falsifications (34 users x 3 forgers x 7 attempts) have been obtained. An evaluation of the error rates of the technique has been developed from all the samples of the database created. The experiments and results obtained are described in Section 4.

4 Experimental results

Three original samples of each gesture chosen randomly have been considered as the 3D biometric signature template; the other four original samples represent truthful attempts of verification that should be accepted. All impostor samples symbolize false trials that should be rejected. Summarizing, Equal Error Rate (EER) [13] have been calculated in this article from 136 (34 users, 4 accessing samples each) truthful and 714 (34 users, 3 forgers, 7 samples each) impostor access samples.

This technique is assessed as powerful whether not only good results of EER are obtained, but also signal analysis carries a reasonable time to be considered "real-time". According to this, a reader should notice that the longer the signals, the longer time to execute the algorithm. Furthermore, this growth in time is not linear but exponential. On the other hand, if the number of performances of the algorithm grows up with a constant length of signals, the total time to complete the whole process increases linearly.

Each 3-D signature carries informations about the accelerations on each axis when the gesture is performed. Three different biometric fusion strategies have been tested: fusion at decision level, fusion at matching score and fusion at feature extraction [14]. In this article, only the first strategy is explained since best results have been obtained from it. Fusing information at decision level implies to execute in parallel but separately the alignment algorithm of each axis signal and calculate a unique comparison metric value from all of them. The resulting comparison metric value for two gestures A and B is calculated by Equation 3:

$$d_{A,B} = \frac{d^x_{A,B} + d^y_{A,B} + d^z_{A,B}}{3} \tag{3}$$

where $d^x_{A,B}$, $d^y_{A,B}$ and $d^z_{A,B}$ are the values obtained by aligning the signals of each axis x, y and z separately and calculating their Euclidean distance by Equation 4

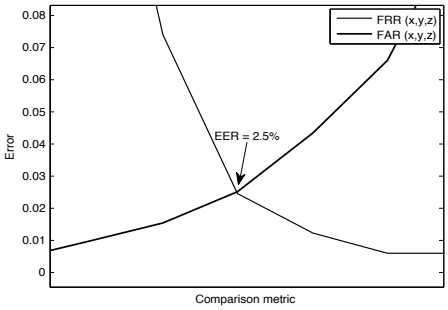
$$d^e_{A,B} = \sum_{i=1}^{2L} (A'_{x,i} - B'_{x,i})^2 \tag{4}$$

where A and B are the two gestures of length L trying to be analyzed. A'_e and B_e are the result of aligned the signals A and B corresponding to axis e. Since the length of these aligned signals is $2L$, the resulting value $d^e_{A,B}$ for each axis e is obtained by calculating the differences between each point and from all the length of the signals.

According to the proposed fusion information scenario, the algorithm is executed three times, one for each axis signal separately. The information is fused at decision level by calculating the average of the result of each process of each axis signal. With all these conditions, an Equal Error Rate of 2.5% has been obtained (Figure 1). This value has been obtained as the intersection of False Acceptance Rate (FAR) curve when falsifiers tried to forge the system, and False Rejection Rate (FAR) curve obtained from the rejection error when truthful users tried to access the system performing their own signature.

Let T_E be the execution time of the alignment algorithm; which is the most consuming time process in an authentication activity. Then, the time consumed in this experiment for each comparison of two gesture samples is equivalent to three times the execution of the algorithm with two signals of length L ($3T_E(L)$). This time has been measured in a mobile device (iPhone 3G) resulting to be 1.51 seconds in average. The calculation of this time has been obtained by the average

Fig. 1. Resulting EER (%) of fusing X, Y and Z signals at decision level.



of executing 10 times in a row an alignment algorithm of signals of 600 points (a six seconds gesture with a sampling rate of 100Hz).

5 Conclusion and future work

In this article, a proposal of a biometric technique in mobile devices has been explained. By analyzing an in-air signature performed by a gesture holding a mobile device embedding an accelerometer, a user is authenticated with low Equal Error Rates in "real time". All the operations involved are carried out inside the mobile device taking advantage of the improving capacity of processing of mobile device.

In order to study the feasibility of this technique, an in-air gesture biometric database has been created. For that purpose, 34 different users have invented and repeated an in-air signature performed with a mobile device. Besides, three falsifiers have attempted to forge all truthful gestures from video records. The volunteers involved in the construction of the database have assessed positively the ease, acceptability, collectively and confidence of the biometric technique proposed.

From all the information stored in it, different scenarios of fusing information have been studied, obtaining best results when the fusion was carried out at decision level.

Equal Error Rate has been calculated with truthful gestures to obtain False Reject Rate and falsifications of original gestures have been utilized to determine False Acceptance Rate. As a result, an Equal Error Rate of 2.5% has been obtained, validating the feasibility of the in-air signature biometric technique proposed in this article.

Furthermore, an application has been developed in an embedding accelerometer mobile device to measure the consumption time involved in the authentication process. In 1.51 seconds all the required operations are completed without any additional devices.

In future works other studies to reduce consumption time may be proposed following different strategies: Reducing sampling rates of the feature extraction of the gesture, applying slide windows in the algorithms or operating only with part of all the information. Besides, the most important parts of the signals

and the axis of accelerations which carries more distinctive information may be evaluated in order to reduce the length or the parts of the signals required to obtain low Equal Error Rates so that consuming time would decrease.

References

1. ho Cho, D., Park, K.R., Rhee, D.W., Kim, Y., Yang, J.: Pupil and iris localization for iris recognition in mobile phones. Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, International Conference on & Self-Assembling Wireless Networks, International Workshop on **0** (2006) 197–201
2. Tao, Q., Veldhuis, R.: Biometric authentication for a mobile personal device. Mobile and Ubiquitous Systems, Annual International Conference on **0** (2006) 1–3
3. Shabeer, H.A., Suganthi, P.: Mobile phones security using biometrics. Computational Intelligence and Multimedia Applications, International Conference on **4** (2007) 270–274
4. Manabe, H., Yamakawa, Y., Sasamoto, T., Sasaki, R.: Security evaluation of biometrics authentications for cellular phones. Intelligent Information Hiding and Multimedia Signal Processing, International Conference on **0** (2009) 34–39
5. Matsuo, K., Okumura, F., Hashimoto, M., Sakazawa, S., Hatori, Y.: Arm swing identification method with template update for long term stability. In: ICB. (2007) 211–221
6. Friederike, A.J., Jain, A.K., Griess, F.D., Connell, S.D., Lansing, E., J, M.: On-line signature verification. Pattern Recognition **35** (2002)
7. Sakoe, H., Chiba, S.: Dynamic programming algorithm optimization for spoken word recognition. IEEE Transactions on Acoustics, Speech and Signal Processing **26**(1) (1978) 43–49
8. Durbin, R., Eddy, S., Krogh, A., Mitchison, G.: Biological sequence analysis. 11th edn. Cambridge University Press (2006)
9. de Santos Sierra, A., Avila, C., Vera, V.: A fuzzy dna-based algorithm for identification and authentication in an iris detection system. In: Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on. (Oct. 2008) 226–232
10. Miller, W.: An introduction to bioinformatics algorithms. neil c. jones and pavel a. pevzner. Journal of the American Statistical Association **101** (June 2006) 855–855
11. Verplaetse, C.: Inertial proprioceptive devices: self-motion-sensing toys and tools. IBM Syst. J. **35**(3-4) (1996) 639–650
12. Jain, A., Hong, L., Pankanti, S.: Biometric identification. Commun. ACM **43**(2) (2000) 90–98
13. Jain, A.K., Flynn, P., Ross, A.A.: Handbook of Biometrics. Springer-Verlag New York, Inc., Secaucus, NJ, USA (2007)
14. Ross, A., Jain, A.: Information fusion in biometrics. Pattern Recognition Letters **24**(13) (September 2003) 2115–2125