A robustness verification system for mobile phone authentication based on gestures using Linear Discriminant Analysis

Javier Guerra-Casanova, Carmen Sánchez-Ávila,
Alberto de-Santos-Sierra, Gonzalo Bailador
CeDInt - UPM, Centro de Domótica Integral,
Universidad Politécnica de Madrid,
Campus de Montegancedo, 28223 Pozuelo de Alarcón, Madrid, Spain
{jguerra, csa, gbailador, alberto}@cedint.upm.es

Abstract—**This article evaluates an authentication technique for mobiles based on gestures. Users create a remindful identifying gesture to be considered as their in-air signature. This work analyzes a database of 120 gestures of different vulnerability, obtaining an Equal Error Rate (EER) of 9.19% when robustness of gestures is not verified. Most of the errors in this EER come from very simple and easily forgeable gestures that should be discarded at enrollment phase. Therefore, an in-air signature robustness verification system using Linear Discriminant Analysis is proposed to infer automatically whether the gesture is secure or not. Different configurations have been tested obtaining a lowest EER of 4.01% when 45.02% of gestures were discarded, and an optimal compromise of EER of 4.82% when 19.19% of gestures were automatically rejected.**

Keywords: Authentication, robustness verification, gestures, mobile phones, accelerometer

I. INTRODUCTION

Nowadays most people own a smartphone. From this new generation phone, many delicate operations may be performed requiring authentication. At present, most of this security is based on the use of passwords, with all their limitations and vulnerabilities.

Utilizing biometrics in mobile phones is one of the options to improve the security in this context. Actually, there are already different approaches joining biometric techniques and mobile phones to enhance their security. In [1] and [2] people are authenticated by the recognition of their face through the camera of a mobile phone. In [3] and [4] authentication is provided by means of iris and in [5] the characteristic biometric features are voice and fingerprint. Moreover, in [6] users are recognized by keystroke analysis.

In this article, we propose an adaptation of handwritten signature in Mobile phones. Therefore, users will authenticate themselves by performing a gesture in the air created by them (their in-air signature) with their hand holding a mobile phone. This mobile phone must embed an accelerometer to extract the information of the performance of the in-air signature. This biometric technique was introduced in [7] with promising Equal Error Rate results for a small database of 34 users.

This technique is interesting to improve the security in smartphones only if it includes a strength verification system to assure whether an in-air signature is robust or not. Otherwise people would enroll into the system within a very simple gesture that may be effortless forged by other people, reducing the security of the authentication technique.

This problematic is similar to textual password checkers, where the system automatically analyzes the strength of a password and infers whether the password chosen is valid to assure the robustness of the system [8-12].

In this work the need of a robustness verification system would be explained, as well as a first approximation to implement it using twelve simple features and a basic classifier (Linera Discriminant Analysis).

According to this, the article is divided into the following Sections. In Section II it is described the signal analysis method to compare different performances of gestures to elucidate if they come from the same user. Section III introduces the characteristics of the database of gestures developed to carry out this article. Then, Section IV explains the motivation of including a gesture strength verification system, whose procedure is described in Section V. The results of the evaluation of the different approaches developed are presented in Section VI. Finally, the article ends with some conclusions and future work.

II. SIGNAL ANALYSIS METHOD

This section explains how two different samples of gestures are compared to elucidate whether they have been made from the same person or not. When a gesture is performed in a mobile phone, three acceleration signals are extracted at a sampling rate of 50 Hz. [13], enough to distinguish between gestures. When two gestures are compared, the acceleration signals of each axis are analyzed separately, obtaining a punctuation value. The lower the value the most similar both signals. Section II.A describes the mathematical method followed to quantify the differences between two acceleration signals.

Besides, when users enroll the system they should repeat three times their identifying gesture. Then, some characteristics of the template will be extracted and utilized when they try to access again to the system at verification phase. Section II.B and II.C explain the enrollment and verification process respectively.

A. Two signal comparison analysis.

Acceleration signals of in-air signatures are analyzed in the following steps:

- A global alignment algorithm [14,15] is executed to correct slightly differences between similar gestures.
- An interpolation method is carried out to correct the gaps introduces when aligning.
- Euclidean distance between the aligned and interpolated signals is calculated.

Therefore, when two signals of acceleration *v*, *w* are compared, a matrix *S* of punctuations is created and filled dynamically following Equation 1:

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

In this global alignment Equation, it is observed that:

The overall punctuation is increased by penalty h when the punctuation on a point *S(i,j)* of the matrix comes from its vertical or horizontal neighbor. Furthermore, h should accomplish $h<0.5$ so that the algorithm works properly.

The punctuation of a diagonal movement depends on the value of a fuzzy function *Δ*, representing to what extent two points *v(i)* and *w(j)* are similar. *Δ* follows Equation 2, where σ is a parameter used to normalize the difference of two points into a Gaussian.

$$\Delta = e^{-\frac{(v(i)-w(j))^2}{2\sigma^2}} \tag{2}$$

Consequently, matrix *S* is completed depending on the punctuation filled in the previous point of the signals and also depending on whether the two points of the sequences compared are more similar than the penalty of including a gap to find the best global alignment.

At this point, the general analysis method executes a backtracking algorithm in order to find the aligned optimally signals *v'* and *w'*. This algorithm consists on discover the path to travel on matrix *S* from *S(m,n)* to *S(1,1)* depending on the expression selected in Equation 1 to calculate each point of the path. Any vertical or horizontal movement means to include a zero in that point of *v* or *w*. Consequently, *v'* and *w'* are obtained by including some zeros in particular points in order to be aligned optimally. Those zero values are interpolated and thereafter Euclidean distance is calculated in order to measure the differences between the signals already aligned, as in Equation 3:

$$\delta = \sqrt{\sum_{t=0}^{L'}(v'(t)-w'(t))^2} \tag{3}$$

According to this, *δ* offers a value quantifying how similar are two acceleration signals, after a preprocessing consisting of aligning and interpolating them. Besides, there are three other values derived from this analysis which are considered in Section V.B:

- *L'*, which is the length of the aligned sequences.
- *S(m,n),* which is the value of the matrix *S* at the last point and corresponds to the maximized value obtained for the score in Equation 1 when aligning two signals.
- *#gaps*, which is the number of zeros included in signals *v* and *w* when the backtracking algorithm is executed.

B. Enrollment

As gesture samples consists of three signals of acceleration (one for each axis), when two gestures are compared, three executions of the algorithm in Section II.A are required and three punctuations of *δ* are obtained, one for each axis. *Ψ* denotes the average of the three punctuations obtained when analyzing all the signals of each axis and represents the quantification of the differences between the two gestures inspected.

A user who enrolls in the system should repeat three times his/her identifying gesture. Afterwards, each pair of gestures is analyzed, obtaining three resulting values of *Ψ*. The average of the comparison of each pair of the three performances of gestures at enrollment is symbolized as μ according to Equation 4. This value is stored with those signals as the identifying gesture template of the user.

$$\mu = \frac{1}{3}(\Psi_{1,2}+\Psi_{1,3}+\Psi_{2,3}) \tag{4}$$

C. Verification

When a user already enrolled desires to access the system, he/she should carry out once his/her identifying gesture. Then, this sample is compared with the three gestures performed at enrolling phase, obtaining three values *Ψj* (*j* means the sample of the template which has been compared with). The final value *Ψ* is calculated as the average of each *Ψj* and represents to what extent the gesture executed is similar to all the samples in the template. The lower it is, the most similar the performance of the gesture is in relation to the template.

If Equation 5 is accomplished, the user would access the system. Otherwise, he/she would be rejected. Obviously, the higher the threshold *θ* is, the more falsification attempts would forge the system but the less original users would be rejected, and vice versa.

$$\frac{\Psi}{\mu} < \theta \tag{5}$$

III. DATABASE OF GESTURES

In order to carry out this work, a database of gestures of different difficulty has been developed. 120 users have participated by inventing and performing an identifying gesture while holding their mobile phone (embedding an accelerometer). Users repeated their own in-air signature 7 times in front of a video camera. From these original records, other users tried to forge each truthful gesture. Each gesture was attempted to be falsified by at least three people and 8 trials each.

Some instructions were provided to encourage users to perform remindful gestures in order to be repeatable by them through the time. Actually, the identifying gestures created by users include:

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

It seems quite obvious that not all the gestures are equally effortful falsifiable by other users. Indeed, simple gestures corresponding to draw elementary figures in the air are much more easy to be falsified than others much more complex were impostors studying a video recording can hardly understand what the gesture the user is performing.

Summarizing, this work has been carried out within a database of 120 different gestures, of different vulnerability (840 truthful gesture samples) and their respective real falsification attempts (2880 falsification attempt samples).

IV. STRENGTH VERIFICATION MOTIVATION

When users enroll in secure systems a robust password is required in order to reduce the possibility of being forged by anyone else. In this biometric technique, users should, as well, create an identifying gesture complex enough so that other people can not repeat it accurately.

According to this, False Acceptance Rate (*FAR*) and False Rejection Rate (*FRR*) of all the gestures (of different robustness) on the database have been calculated. The intersection between both rates coincides with the Equal Error Rate (*EER*), which is the most common ratio to measure the performance in biometrics [16-17]. An *EER* of 9.19% has been obtained, as represented in Figure 1.

However, most of the errors of the gesture database come from vulnerable gestures that have been easily forged by impostors. In Figure 2, a histogram of the percentage of falsification attempts whose punctuation is under the threshold corresponding to *EER* (θ_{EER} = 1.3) is shown. From this figure, it is concluded that most of the gestures on the database have never been accurately enough falsified. On the other hand, there are some gestures whose falsifications attempts include a high number of errors in *FAR* (and obviously in *EER*).

Therefore, according to this biometric technique, a strength verification system of the gestures created to be used as signatures in mobile phones is required. Thus, the global *EER* of the system would decrease, since if users are not allowed to enroll with a vulnerable gesture, then, most of the succeeding falsification attempts will not compute.

Figure 1. EER result analyzing all the gestures in the database of different robustness.

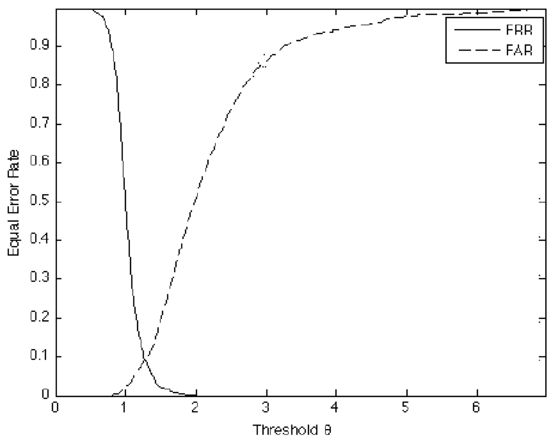
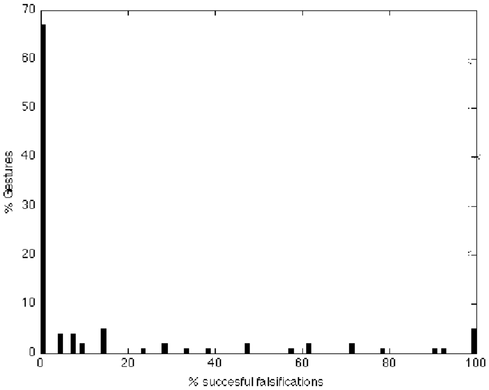


Figure 2. Histogram of percentage of falsifications whose punctuations Ψ/μ are lower than θ_{EER} (1.3)



However, the classification of robust and vulnerable gestures should be automatically derived at any enrollment, without waiting for falsification results. This task is the main objective of this article and it has been accomplished as a supervised learning.

The development of a strength verification system of in-air signatures includes the following steps, explained in the next Section:

- A definition of the features of the gesture selected to evaluate its strength.
- A prior classification of the gestures to train the strength verification system, based on the percentage of falsifications lower than a threshold.
- An automatic classification of the gestures based on Linear Discriminant Analysis. The classifier is trained by a subset of the gestures previously classified and evaluated by the rest of gestures in the database.

V. STRENGTH VERIFICATION PROPOSAL

The experimental work developed in this article is based on a supervised classification of the robustness of the gestures of the database. The procedure begins with the extraction of the features of the templates of all the gestures in the database, as explained in Section V.A, and the expected classification of the robustness of all of them as described in Section V.B. Next, the classification procedure and its evaluation is detailed in Section V.C.

A. Definition of the features of the template considered

When users enroll the system, they are required to repeat three times the identifying gesture they select as their in-air signature. As explained in Section II.A, four parameters of the template created have been obtained for each signal comparison. The average of these parameters corresponds to 4 of the features the strength verification system will use to determine the vulnerability of the gestures, as represented in Equations 6-9:

$$f_1 = \mu \qquad (6) \qquad f_2 = S(n,m)_{avg} \qquad (7)$$

$$f_3 = \# gaps_{avg} \qquad (8) \qquad f_4 = L'_{avg} \qquad (9)$$

Features 5-8 are obtained from the same parameters than the previous but calculating the difference between them instead of the averages, as defined in Equations 10-13.

$$f_5 = \frac{1}{3}(|\Psi_{1,2} - \Psi_{1,3}| + |\Psi_{1,2} - \Psi_{2,3}| + |\Psi_{1,3} - \Psi_{2,3}|) \qquad (10)$$

$$f_6 = \frac{1}{3}(|S(n,m)_{1,2} - S(n,m)_{1,3}| + |S(n,m)_{1,2} - S(n,m)_{2,3}| + |S(n,m)_{1,3} - S(n,m)_{2,3}|) \qquad (11)$$

$$f_7 = \frac{1}{3}(|\# gaps_{1,2} - \# gaps_{1,3}| + |\# gaps_{1,2} - \# gaps_{2,3}| + |\# gaps_{1,3} - \# gaps_{2,3}|) \qquad (12)$$

$$f_8 = \frac{1}{3}(|L'_{1,2} - L'_{1,3}| + |L'_{1,2} - L'_{2,3}| + |L'_{1,3} - L'_{2,3}|) \qquad (13)$$

Features 1-8 stand for characteristics of the repetition of the gestures at enrollment.

Furthermore, four more characteristics of the template have been extracted by analyzing the values of the accelerations from each of the gestures g_i, providing Features 9-12 (Equation 14-17):

$$f_9 = \frac{1}{3}\sum_{i=1}^{3}\sum_{j=1}^{L} g_i(j) \qquad (14) \qquad f_{10} = \frac{1}{3}\sum_{i=1}^{3}\sum_{j=1}^{L} |g_i(j)| \qquad (15)$$

$$f_{11} = \frac{1}{3}\sum_{i=1}^{3} std(g_i) \qquad (16) \qquad f_{12} = \frac{1}{3}\sum_{i=1}^{3} std(|g_i|) \qquad (17)$$

Features 9-12 are very simple characteristics of the performance of the gestures, representing the richness of the gesture (length, different movements, spins, etc.). Many other features would be studied in future works.

When users enroll the system, features (1-12) are calculated. From them, the strength verification system would derive automatically whether the gesture is robust enough or not without requiring to study the behavior of the gesture to falsification attempts.

B. Prior classification of gestures to train the system through the falsification results

In this supervised problem, it is also necessary to provide the strength verification system the expected classification of the gestures the system is trained. In this article two different classification schemas are proposed, based on dividing all the gestures in two classes (Robust or Vulnerable), or in three (Robust, Medium and Vulnerable). This classification procedure is performed as follows:

Firstly, a threshold ζ is fixed and for each gesture, the percentage of falsification attempts whose punctuations when comparing with its original template are lower than ζ is calculated. Then P_R (and P_M if three classes approach) is defined as the percentage limit to consider the gesture as Robust (and Medium). Consequently, in two classes approach all the gestures with a lower percentage of falsification access lower than P_R are considered as Robust whereas the rest are defined as Vulnerable. On the other hand, in the three classes approach, the gestures whose percentage of falsification access is lower than P_R are considered as Robust, those between P_R and P_M are classified as Medium and the rest as Vulnerable.

In Section VI results are presented for different types of classification (two or three classes) and for different values of ζ, P_R, and P_M (if three classes approach).

C. Classfication procedure

The classification procedure has considered six different values of ζ {*1, 1.1, 1.2, 1.3, 1.4, 1.5*}. Besides, both classification approaches (two and three classes division) have been studied, with different configurations of the values of P_R and P_M (two configurations in two classes approach and three in three classes).

Moreover, the database of gestures is divided into two groups: training and verification. Two different divisions have been considered: 30%Training-70%Testing and 50%Training-50%Testing. All these gestures have been introduced to train a classifier based on linear discriminant analysis [18]. After training, the gestures in the verification group have been injected in the classifier, which has classified them as Robust or Vulnerable (and Medium if three classes approach).

Once the strength verification system has classified the gestures, the *ERR* of each group of gestures has been obtained. For this purpose and since the accessing samples are not involved in this analysis, the *FRR* obtained in Figure 1 has been considered the same for all the scenarios. According to this, the evaluation of how the strength verification system works do not depend on how original users repeated their own in-air signature, but it only does in how impostors were able to falsify gestures. Therefore, each group of gestures would derive into a *FAR* rate, whose intersection with the *FRR* rate would obtain the *EER* needed to evaluate the performance of the system.

Another parameter to measure the performance of the verification system is the percentage of Robust gestures found. The optimal scenario would include an EER_R (the *EER* of Robust gestures) as low as possible obtained with a percentage of gestures classified as Robust (PC_R) as high as possible. This would mean that only the gestures including the highest amount of errors (and consequently, the most vulnerable) are discarded.

In this work Linear Discriminant Analysis is used to classify the robustness of the gestures. Many other classifiers would be studied in future works.

VI. RESULTS

In this approach, cross validation has been carried out. Each experiment has been repeated 50 times. The results presented are the average of all of them. According to this, the *EER* results and percentage of Robust gestures are presented for each different scenario:

Tables 1 and 2 represent the values of percentage of gestures classified as Robust (PC_R) and the *EER* obtained when analyze *FAR* of all of them (EER_R). In both tables, the a priori classification of gestures to train the classifier has been obtained with a value of P_R of 0 or 10 (0% or 10% of falsification attempts punctuations lower than ζ). Table 1 and Table 2 represent the results when the training group was composed by the 30% and 50% of the gestures of the database respectively.

TABLE I. RESULTS WHEN CLASSIFICATION GESTURES IN TWO CLASSES AND 30% OF TRAINING GESTURES

ζ	$P_R = 0$		$P_R = 10$	
	EER_R	PC_R	EER_R	PC_R
1	6.34	87.69	7.11	89.54
1.1	5.92	82.79	6.11	88.29
1.2	5.30	81.15	5.57	82.17
1.3	5.18	72.56	5.22	80.10
1.4	5.47	64.28	5.29	74.03
1.5	4.98	56.06	4.98	64.68

TABLE II. RESULTS WHEN CLASSIFICATION GESTURES IN TWO CLASSES AND 50% OF TRAINING GESTURES

ζ	$P_R = 0$		$P_R = 10$	
	EER_R	PC_R	EER_R	PC_R
1	5.76	86.18	6.08	88.34
1.1	5.38	83.04	5.76	88.65
1.2	5.07	82.37	5.03	83.35
1.3	5.20	76.68	5.14	82.02
1.4	4.94	63.61	4.66	74.21
1.5	4.01	54.98	4.38	64.59

As it can be derived from the previous tables, when ζ grows, the percentage of gestures classified as Robust increases as well. As there are more Robust gestures, the probability of these gestures to include high falsification punctuations is also bigger, deriving in a higher value of EER_R. Therefore, it should be a compromise between the percentage of gestures discarded at enrollment and the *EER* obtained. The lowest *EER* obtained is 4.01%, which is 5.18% lower than when no verification strength system was included. The optimal scenario is the one whose value (EER_R /PC_R) is minimal, and it is emphasized in the Tables.

Similarly, Tables 3 and 4 represent the results when three possible classifications of gestures were taken into consideration for a training group of 30% and 50% of the gestures of the database respectively. Both tables include the results when the a priori classification was defined within three different configurations of P_R and P_M.

TABLE III. RESULTS WHEN CLASSIFICATION GESTURES IN THREE CLASSES AND 30% OF TRAINING GESTURES

ζ	$P_R = 0; P_M = 10$		$P_R = 0; P_M = 20$		$P_R = 10; P_M = 20$	
	EER_R	PC_R	EER_R	PC_R	EER_R	PC_R
1	5.80	83.04	5.56	81.80	-	-
1.1	5.26	76.72	5.22	79.22	5.63	87.30
1.2	4.80	75.99	5.03	70.97	5.39	72.33
1.3	5.63	67.40	5.19	67.37	5.21	79.62
1.4	5.22	57.65	4.86	59.24	4.98	68.99
1.5	4.36	45.77	4.59	45.77	4.83	57.05

TABLE IV. RESULTS WHEN CLASSIFICATION GESTURES IN THREE CLASSES AND 50% OF TRAINING GESTURES

ζ	$P_R = 0; P_M = 10$		$P_R = 0; P_M = 20$		$P_R = 10; P_M = 20$	
	EER_R	PC_R	EER_R	PC_R	EER_R	PC_R
1	5.09	82.06	5.25	84.18		
1.1	5.13	77.78	5.15	81.47	5.42	87.16
1.2	4.85	80.49	5.04	73.50	5.12	72.44
1.3	4.94	67.70	4.74	67.50	4.82	80.65
1.4	4.64	56.75	4.57	57.84	4.67	69.97
1.5	4.20	43.13	4.30	46.74	4.16	58.24

The same behavior derived from Tables 1 and 2 can be inferred from Tables 3 and 4 as well. In this case, the lowest EER_R obtained is 4.16%, reducing in 5.03% the *EER* with no verification strength system. The optimal scenarios are also emphasized following the policy of minimal (EER_R / PC_R). The optimal result of all the scenarios is the one in Table 4, where a 4.82% of *EER* has been obtained by discarding only the 19.35% of the gestures.

VII. CONCLUSIONS

This article is focused on developing an authentication technique for mobile phones avoiding the use of passwords. For this purpose, this article proposes a biometric technique based on performing an identifying gesture while holding the mobile phone on the hand. This biometric technique obtains an *EER* around 9% when analyzing a database of 120 users who have created their own in-air signature with different robustness.

In a similar manner that password checkers do not let users to access the system with a password too easy to guess, a verification strength system should be implemented for gestures in order to assure users that their in-air signature is robust enough to be imitated by anyone studying a record of it. According to this, *EER* should decrease when the vulnerable in-air signatures are discarded.

Therefore, this article develops a verification strength system for gestures that infers the robustness of the gesture created when performing it at enrollment. Consequently, users would be previously warned if they had selected a vulnerable gesture.

For this purpose, 12 different features have been extracted from the gestures performed at enrollment, and different a priori classification configurations have been tested to train the verification system.

Finally, the lowest *EER* obtained when analyzing only the gestures automatically classified as robust was 4.01% and the optimal result discarded the 19.35% of the gestures obtaining an *EER* of 4.82%.

These promising results should be improved in future works including the evaluation of more gesture features, other classifiers such as SVM or MPL and other a priori classification procedures of the gestures.

REFERENCES

[1] Tao, Q., Veldhuis, J.; Biometric Authentication for a Mobile Personal Device. In: Mobile and Ubiquitous Systems: Networking & Services, 2006 Third Annual International Conference on , (2006)

[2] Ijiri, Y., Sakuragi, M., Shihong L.; Security Management for Mobile Devices by Face Recognition. In 7th International Conference on Mobile Data Management. (2006)

[3] Dal-ho Cho and Kang Ryoung Park and Dae Woong Rhee and Yanggon Kim and Jonghoon Yang. Pupil and Iris Localization for Iris Recognition in Mobile Phones. In: International Conference on Software Engineering. (2006)

[4] Jeong, D., Park, H., Park, K., Kim, J..; Iris Recognition in Mobile Phone Based on Adaptive Gabor Filter. In In: Zhang, D., Jain, A. (eds.). LNCS, vol. 3832, pp. 457-463. Springer, Heidelberg (2005)

[5] Shabeer, H.A., Suganthi, P.. Mobile Phones Security Using Biometrics. In: Computational Intelligence and Multimedia Applications, International Conference on. pp 270-274. (2007)

[6] Clarke, N., Furnell, S.; Authenticating mobile phone users using keystroke analysis. International Journal of Information Security. Vol 6 Issue 1, pp 1—14. (2007)

[7] Guerra-Casanova J, Sánchez-Ávila C., de-Santos-Sierra A., Bailador, G, Jara-Vera, V.; A Real-Time In-Air Signature Biometric Technique Using a Mobile Device Embedding an Accelerometer. NDT (1). editor(s) Filip Zavoral and Jakub Yaghob and Pit Pichappan and Eyas El-Qawasmeh. Communications in Computer and Information Science, (87) 497-503, Springer, Year 2010.

[8] Bishop, M. Improving system security via proactive password checking. Computers and Security 14(3). 1995

[9] Gehringer, E. F. Choosing passwords: security and human factors. In: Technology and Society, 2002 International Symosioum on. 2002

[10] Dell'Amico, M., Michiardi, P. and Roudier, Y. Password Strength: An Empirical Analysis 2010. In INFOCOM, 2010 Proceedings IEEE. (2010)

[11] Zviran, M., Haga, W.; Password security: an empirical study. J. Manage. Inf. Syst., 15(4):161-185, March 1999.

[12] Vu, Kim-Phuong L., Proctor, Robert W., Bhargav-Spantzel, Abhilasha, Tai, Bik-Lam ., Cook, Joshua and Eugene Schultz, E. Improving password security and memorability to protect personal and organizational information. International Journal of Human-Computer Studies Volume 65 Issue 8, August, 2007.

[13] Kela, J.,, Korpipää, P., Mäntyjärvi, J., Kallio, S., Savino, G., Jozzo, L., Marca, S.; Accelerometer-based gesture control for a design environment. Personal and Ubiquitous Computing. (2006)

[14] Durbin, R., Eddy, S., Krogh, A., Mitchison, G.; Biological sequence analysis. Ed. Press, Cambridge U. (2006)

[15] Bellman, R.; Dynamic Programming. Princeton Univ Pr (June 1957)

[16] Jain, A. K., Flynn, P., Ross, A. A.; Handbook of Biometrics. Springer-Verlag New York, Inc. (2007)

[17] Phillips, P.J., Martin, A., Wilson C.L., Przybocki M.; An Introduction to Evaluating Biometric Systems. Computer 21(2). (2000)

[18] Duda, R.O., Hart P.E., Stork, D.G.; Pattern Classification. Wiley-Interscience, 2 edition, November 2001.