Application of LCS Algorithm to Authenticate Users within Their Mobile Phone Through In-Air Signatures

Javier Guerra-Casanova, Carmen Sánchez-Ávila, Gonzalo Bailador-del Pozo
and Alberto de Santos
Centro de Domótica Integral (CeDInt-UPM)
Universidad Politécnica de Madrid
Campus de Montegancedo, Madrid
Spain

1. Introduction

Authentication is one of the most important aspects regarding all the operations that may be performed from a mobile device. Starting up the device, making use of special functions, phoning reserved numbers, reading mail, accessing some Internet applications like e-commerce, electronic voting, e-learning, looking up the balance of a bank account or buying a product in an online shop are examples of operations that are nowadays performed from a mobile device and require authentication.

At present, most authentication procedures in mobile phones relies on handwritten passwords, with all their limitations. In this context, biometric techniques may offer a better solution to authenticate users according to their physical or behavioural characteristics.

Actually, there are already different approaches trying to join physical biometric techniques and mobile phones, as ho Cho et al. (2006), Jeong et al. (2005), Kurkovsky et al. (2010), Jeong et al. (2006) where users are authenticated through their iris or their faces Tao & Veldhuis (2006), yi Han et al. (2007), Ijiri et al. (2006). Besides, some work has been also developed with behavioral techniques in mobiles, authenticating users by means of their voice Shabeer & Suganthi (2007), Lapère & Johnson (1997), gait Mantyjarvi et al. (2005), Iso & Yamazaki (2006) or keystroke analysis Clarke & Furnell (2007), Saevanee & Bhatarakosol (2008).

In this chapter we propose to join handwritten signature, the most common biometric technique Nalwa (1997), in this mobile context. People are absolutely used to sign everyday when buying with their credit card, picking up a letter from the post office, authorizing operations on their name and lots of quotidian and legal scenarios else.

Consequently, we propose an adapted technique that allows people to authenticate themselves by a signature when they carry out, from their mobile phones, operations they used to perform in presence where they were used to authenticate themselves signing with their handwritten signature in a paper.

The biometric technique proposed consists of authenticating users when they execute an identifying gesture in the air (an in-air signature) while holding on their hand their mobile phone Guerra-Casanova et al. (2010). This identifying gesture should be easily remindful but complex enough to not being easily forgeable by other users. Creating a new personal gesture, easily to be repeated by the original user, but difficult to be reproduced by different people watching is not an easy task. Actually, most people who participated in this work chose their own handwritten signature as their identifying gesture, since it is a graph people is very used to repeat constantly.

To authenticate users within biometrics, it is necessary that users get enrolled in the system previously Jain et al. (2007). Actually, in the enrollment phase of the authentication technique based on gestures, users should repeat three times their identifying gesture to create their template of the gesture they will use as their signature to access the system.

When accessing the system, users only should repeat once their identifying gesture chose at enrollment phase. Then, the gesture performed is compared with the template stored, and if matches, the access is granted.

The main requirement of the technique is users should belong a mobile phone embedding an accelerometer since it is the sensor needed to extract the information of the performance of the gesture. This demand is not a problem since leader mobile phones manufacturers are marketing devices fulfilling this task with a very growing sales volume. It is expected that in several years, most mobile phones integrate an accelerometer resulting this proposed biometric technique accessible for most of the population. For example, Apple sold more than 4 million iPhone mobiles, embedding an accelerometer, just in the three first months of 2009 Steve Dowling (2009).

The in-air signature biometric technique provides several advantages:

- There are no additional widgets required to perform the signature, as any pen or any surface, so users only need their mobile phone to authenticate themselves by performing their signature in the air.
- The falsification of an in-air signature performed in this way is much harder to be forged as the gesture is performed in 3-D with no references as surfaces in handwritten signatures. Some experiments to verify this assumption are intended to be presented in this chapter.
- Users find this technique innovative but familiar so they are comfortable when performing their signature in this way whereas they are also grateful because they believe they are doing something novel.

According to these advantages, this authentication technique is expected to be widely accepted by people using their mobile phones to perform operations with a higher level of security. This assumption is based on the lack of invasiveness of the technique based on gestures, joined to the similarities to the high accepted and extended handwriting signature methods and the increase of security it provides Jain et al. (2002).

Although the in-air signature biometric technique seems quite similar to gesture recognition approaches, the point of view are radically different. In gesture recognition the crucial aim is to find a gesture from a database of known gestures that any person performs in a different manner, so it focus on finding similarities of samples of gestures. However, in our approach, we will find similar gestures performed by different people (for example one person trying to forge the authentic signature or another), but the main objective of this technique is to be able to differentiate from similar but different gestures, as they may come from impostor users Hsu et al. (2009), citeHe08.

This authentication technique provides an immediate application to the industry of mobile phones. It might be adopted to increase the security of different operations:

- Operations in the mobile phone: In this case, the template of the user should be stored in the mobile phone, and all the process to authenticate the user is executed in the device.
- Operations in a server: When users desire to execute an operation in a server through Internet, they should authenticate previously by performing their in-air signature holding their mobile. In this case, the in-air signature should be stored in the databases of the server, carrying out the authenticating process out of the mobile.
- E-commerce operations: Operations requiring authorization of the bank would be authenticated by performing an in-air signature. In this context, users should have been enrolled previously in the bank, in whose databases the in-air signatures are stored.

This chapter is divided into the following Sections:

- Section 2 describes how the in-air signature technique has been implemented on a mobile device. It starts with a motivation subsection where it is explained why a sequence alignment algorithm has been selected to analyze the in-air signatures. After that, Longest Common Subsequence algorithm is remembered to explain how has been adapted to this context in the different approaches evaluated in this chapter. Finally, it is described how the enrollment and authentication process is performed.
- Section 3 provides the description of the database of in-air signatures developed and considered in this chapter, as well as the results obtained for the different approaches assessed.
- Section 4 concludes the chapter with the conclusions obtained and the future work that may follow this study.

2. Implementation

This Section describes all the analysis method aspects included in the in-air signature biometric technique proposed in this work. It starts with the motivation of applying an algorithm based on obtaining the Longest Common Subsequence Bergroth et al. (2000). After that, a short review of LCS algorithm is included to be able to explain, afterwards, the generalization of LCS algorithm used in this work. Besides, another approach based on LCS is presented, consisting of using LCS to find the optimal global alignment and reconstruct two repetitions of an in-air signature to calculate the similarity value with a direct distance. Finally, the implementation of the algorithm in enrolling and verification phase is presented.

2.1 Motivation of applying Longest Common Subsequence algorithms to analyze acceleration signals of in-air signatures

Users authentication by means of gestures in the air involves a high intra-class deviation between the different performance of the in-air signatures, due to the fact that users are not able to repeat their identifying gestures with full precision. Consequently, applying a direct comparison method as Euclidean distance does not work properly.

Anytime users repeat their identifying gesture, they perform some parts of it faster or slower, more or less pronounced, or holding the mobile slightly different. In spite of all these variations, there exists an intrinsic part of the gestures remaining invariant that may be used to recognize the person. Indeed, although users do not repeat exactly their identifying gesture, when they get used to repeat them, they are able to perform them naturally and in a quite similar manner but with some little differences.

Particularly, the following differences are found in acceleration signals when repeating gestures are found:

- Although the segmentation of the in-air signature is performed manually (there is a button to push at the start and stop of the performance of the in-air signature), the beginning of the gesture does not coincide. This happens because the time between users push the button and starts drawing their in-air signature is variable.
- In spite of performing the same in-air signature, there may exist peaks of acceleration more pronounced than others, relatives to more abrupt movements.
- Gestures do not long exactly the same, since any repetition is different from each other.
- Furthermore, it may happen that differences between repetitions occur only in certain parts of the performances of the gestures, where only some transitions are faster or slower than their respective.

Correcting most of those little deviations is the main aim of preprocessing acceleration signals of gestures through an alignment, keeping the intrinsic characteristics of the signals and rectifying slightly variations. As a consequence, in spite of the different, but quite similar, performance of the gesture, the system is able to assure the authenticity of the user.

According to this, the analysis algorithm required to compare the signals involved should correct slightly differences but this characteristic is as important as not compensating excessively. Otherwise, impostors would be able to imitate easily the gesture of another and forge the system, compromising the security of the authentication technique.

Indeed, the problem introduced to analyze acceleration signals of gestures has some analogies to global alignment algorithms, as Longest Common Subsequences, where the objective is to find the invariant information stored in two sequences independently of slightly differences. Consequently, both problems provide two signals to be compared which may have little differences but an important part of them remaining invariant.

2.2 LCS algorithm review

This algorithm provides directly a similarity value between two different sequences of values. LCS algorithm is based on finding the longest common subsequence of two sequences Wagner & Fischer (1974). This common subsequence is the one with lower edition distance, so both initial sequences can derived into the longest common subsequence within the lowest number of insertion and deletion operations Durbin et al. (2006).

Formally, a common subsequence of two sequences $\mathbf{v} = v_1 \ldots v_n$, $\mathbf{w} = w_1 \ldots w_m$ is defined as a sequence of positions in $\mathbf{v}$, so that $1 \leq i_1 \leq \ldots \leq i_k \leq n$ and a sequence of positions in $\mathbf{w}$, so that $1 \leq j_1 \leq \ldots \leq j_k \leq m$ fulfilling that the respective values of positions in $\mathbf{v}$ and $\mathbf{w}$ coincide, which means that, $v_{it} = w_{jt} for 1 \leq t \leq k$.

LCS algorithm is implemented defining a Matrix S that will be filled recursively with dynamic programming technique. The size of Matrix S is $n \times m$ and it is completed according to Equation 1:

$$s_{i,j} = \max \begin{cases} s_{i-i,j} + 0 \\ s_{i,j-1} + 0 \\ s_{i-1,j-1} + 1, \text{ if } v_i = w_j \\ s_{i-1,j-1} + 0, \text{ if } v_i \neq w_j \end{cases} \tag{1}$$

This equation includes the following aspects:

- The fist term of Equation 1 corresponds to the case when v_i is not present in the longest common subsequence of v and w (deletion in v_i or insertion in w_j).
- The second term represents the case when w_j is not present (deletion in w_j or insertion in v_i)
- The third term symbolizes the possible case when v_i and w_j are part of the longest common subsequence. Actually, when it happens that $v_i = w_j$ a 1 values is added in order to find the longest common subsequence.
- The forth term stands for the case when neither v_i nor w_j are part of the longest common subsequence (two deletions or insertions in v_i and w_j)

When matrix S is completed, the value of $\delta = s_{n,m}$ provides the length of the longest common subsequence. This value is itself a metric that compares the similarity of two sequences, the higher the more similar and vice versa.

2.3 Generalization of LCS algorithm

Classical LCS algorithm only assume that two points of the sequences in comparison belong to the longest common subsequence when their value is exactly equal. This premise is widely used when the alphabet of the values of the sequences is closed, which means that the possible values of the sequences are known and limited. For example, in genetic sequence alignment problems, the possible values of the genes are previously recognized and easily differentiabled. However, in the context of acceleration signals, quite similar values that belongs to the same point are classified as different, when it might not be.

According to this, a generalization of LCS algorithm is proposed by extending Equation 1 with Equation 2:

$$s_{i,j} = \max \begin{cases} s_{i-i,j} + 0 \\ s_{i,j-1} + 0 \\ s_{i-1,j-1} + 1, \text{ if } |v_i - w_j| \leq \psi \\ s_{i-1,j-1} + 0, \text{ if } |v_i - w_j| \nleq \psi \end{cases} \tag{2}$$

Consequently, in this approach it is not necessary that v_i and w_j are exactly the same values, but only with a lower difference than ψ.

This generalization may be represented by Equation 3:

$$s_{i,j} = \max \begin{cases} s_{i-i,j} + 0 \\ s_{i,j-1} + 0 \\ s_{i-1,j-1} + \zeta(v_i, w_j, \psi) \end{cases} \tag{3}$$

In Equation 3 ζ is a function of v_i and w_j according to Equation 4

$$\zeta(v_i, w_j, \psi) = \max \begin{cases} 1, if |v_i - w_j| \leq \psi \\ 0, if |v_i - w_j| \nleq \psi \end{cases} \quad (4)$$

According to this Equation, classical LCS algorithm is a particular method of this expression with $\psi = 0$. In this work, it has been proposed a step function to model ζ, however, some other functions may be useful in order to compare whether two points of two sequences belong to the longest common subsequence. Furthermore, an extension of this algorithm may be proposed including fuzzy logic so that two points have a percentage of probability to belong to the longest common subsequence, which may be modeled by a Gaussian, sigmoid or linear function.

2.4 An alignment and reconstructing approach

Previously, a metric based on the value of $s_{n,m}$ has been proposed to compare the similarity of two sequences. A different approach introduced in this work relies on utilizing the longest common subsequence as a method to find the optimal alignment between two sequences, and after that, trying to rebuild them in an optimal manner.

The longest common subsequence is obtained directly from matrix S. The procedure consists of finding the path joining element $s_{n,m}$ with $s_{1,1}$, considering that in the Equation of filling S:

- If the maximum value has been obtained through the first element, it correspond a $\leftarrow$ movement in S.
- If the maximum value has been obtained from the second element, the correspondent movement is vertical $\uparrow$.
- If the maximum value comes from the third element, it represents a diagonal movement in $S \nwarrow$.

The optimal alignment of two sequences when their longest common subsequence has been obtained consists of including a gap ("zero value") in v_i when a horizontal movement is required or a gap in w_j when the movement is vertical. Diagonal movements do not include gaps.

Then, every zero value is interpolated in order to reduce the differences between aligned signals. The interpolation method consists of substituting each zero value by the previous non-zero value of the sequence.

In this point, the initial sequences v and w have been aligned optimally and interpolated, deriving in v' and w'. The metric used to quantify the similarities between them implies calculating the absolute distance of v' and w' following Equation 5.

$$\delta = \sum_{i=0}^{L'} (v'_i - w'_i)^2 \quad (5)$$

Because of including gaps in the sequences in the optimal alignment procedure, the length of the signals may have increased to L', whose maximum values is $L' \leq m + n$.

In conclusion, after the analysis of two sequences, a score value δ has been obtained quantifying the similarity of both sequences. In the previous approach, the higher δ is the more similar sequences are, but in this one, it happens the opposite; the more similar sequences are those with a lower δ.

2.5 Application to in-air signatures

According to the previous subsections, when two sequences are compared a value δ is obtained in order to quantify the similarity of both sequences. This is also extensive to in-air signature acceleration signals, with only one consideration: Each in-air signature repetition consists of three signals, representing the accelerations on axes X, Y and Z.

In this work we propose to compare two repetitions of in-air signatures by evaluating the acceleration signal of each axis separately. Consequently, for each in-air signature comparison, three signal comparisons are required, deriving in three values δ_x, δ_y and δ_z representing the similarity of the signal of each axis separately.

Finally, the value of similarity of the complete signatures, Δ, is obtained as the average of the values obtained on each axis separately.

2.6 Implementation of enrolling process

Users enrolling with their mobile phones should repeat three times their identifying gesture, as precisely as they are able.

These three repetitions are analyzed by pairs, obtaining three values of the similarities between the different performances of their in-air signatures ($\Delta_{1,2}$, $\Delta_{1,3}$ and $\Delta_{2,3}$).

From these values, the parameter μ_T is calculated following Equation 6:

$$\mu_T = \frac{\Delta_{1,2} + \Delta_{1,3} + \Delta_{2,3}}{3} \tag{6}$$

Parameter μ_T provides information about the ability of the user to repeat his/her in-air signature, which would be essential in the access process to infer whether the accessing attempt belongs to the real user or not.

The in-air signature template of each user is composed by:

- The signals of accelerations on each axis of each repetition of the in-air signature the user performed at enrollment phase.
- Parameter μ_T representing the similarity between both three repetitions.

2.7 Implementation of accessing process

Users should authenticate themselves in their mobile phone by repeating once the in-air signatures they chose at enrolment phase.

This accessing in-air signature includes three acceleration signals, corresponding to the three axes X, Y and Z. This access attempt is compared with each of the three samples composing the template, deriving in three similarity values ($\Delta_{A,1}$, $\Delta_{A,2}$ and $\Delta_{A,3}$) obtained as described previously.

Finally, a global score is calculated including the similarities with each sample of the template as well as parameter μ_T obtained at enrollment phase. This global score follows Equation 7

$$\Psi = \frac{\Delta_{A,1} + \Delta_{A,2} + \Delta_{A,3}}{3\mu_T} \tag{7}$$

Finally, depending on the behavior of the similarity values, the accessing attempt is rejected or accepted according to a threshold value Θ following these considerations:

- If a high δ stands for high similarity, the accessing attempt is accepted when $\Psi > \Theta$, otherwise is rejected.

- If a high δ represents low similarity, the accessing attempt is accepted when $\Psi < \Theta$, otherwise is rejected.

It is remarkable that the selection of an optimal Θ is crucial in order to reduce false positives and negatives errors. In this approach, Θ value will be set up to the value of Equal Error Rate, when the False Rejection Rate is equal to the False Acceptance Rate. In spite of this, Θ value might be modified in order to reduce one of the rates at the expense of increase the other. This might be interesting if users do not care about repeating sometimes twice their in-air signature.

3. Experiments

3.1 Database

According to the knowledge of the authors, there are no public databases of in-air signatures performed a mobile embedding an accelerometer. Therefore, a private database has been created in order to obtain a significant number of samples in order to evaluate the algorithms previously proposed.

This database contains in-air signatures of 50 different users, who have created their identifying gesture trying to select in-air signatures easily remindful and complex enough to not be forged automatically. Most of the users chose to perform in the air their own handwritten signature as their identifying gesture in this biometric technique.

Users repeated 8 times their in-air signature in front of a video camera. Afterwards, 6 people tried to falsify each original in-air signature from studying those records. Each falsifier tried 7 times to forge each in-air signature.

All of the original and falsifying samples of the database have been obtained sampling the in-air signatures at a rate of 50 Hz.

3.2 Results

From the analysis of the samples in the database created, an “active impostor attack” scenario has been represented, to evaluate the performance of the in-air signature biometric technique with real attempts of falsification.

Three random samples of each user would be considered as the repetitions performed at enrollment phase. With these samples, the enrollment procedure is execute, obtaining parameter μ_T for each user. The rest of samples of each user would be considered as original access attempts whereas the falsifying samples of each user will symbolize fraudulent access attempts to the system.

Each experiment presented in this work has been repeated five times; each repetition implies a different selection of the samples composing the template of each user. Results present the average and deviation of all of them.

The metric used to evaluate the performance of the algorithm will be Equal Error Rate Wayman et al. (2004). This rate is obtained as follows:

- Analysis of original samples: The original access attempt samples of each gesture are used to calculate False Rejection Rate, since they are authentic attempts of accessing the system. For each original trial Ψ is obtained when comparing the accessing gesture with the three gestures of the original user template, considering the correspondent μ_T of the user.

- Analysis of falsified samples: All the impostor attempts trying to access the system are used to evaluate False Acceptance Rate. For each falsification trial, Ψ is also obtained as the value of comparing the sample with the template considering, as well, parameter μ_T of the user.
- Obtention of False Acceptance Rate (FAR) and False Rejection Rate (FRR): FAR and FRR are obtained in terms of Θ as follows:
  - If a high δ value stands for high similarity, the % of original samples that are under Θ in case of False Rejection Rate and the % of falsified samples that are over Θ in case of False Acceptance Rate. In this case, it is accomplished that when Θ is very high, most falsifications are rejected but so do some original access. However, the lower Θ, the more original access are authentic allowed but also the more falsifications are granted.
  - If a low δ value stands for high similarity, the % of original samples that are over Θ in case of False Rejection Rate and the % of falsified samples that are under Θ in case of False Acceptance Rate. In this case, the behaviour of FAR and FRR in respect with Θ is the opposite.
- Obtention of Equal Error Rate (EER): EER is defined as the value of the error when False Acceptance Rate is equal to False Rejection Rate, and it is the metric commonly used to measure the performance of the biometric technique.

Usually, the performance of the biometric systems is represented by a Receiver Operating Characteristic figure (ROC) Fawcett (2006), where axis X represents False Matching Rate (FMR) and axis Y True Matching Rate (TMR). When Failure-to-acquire (FTA) rate is 0 (as in the experiments presented in this article, since the samples evaluated come from a closed database), it is verified that FMR=FAR and FNMR=FRR. Besides, FNMR is defined as FNMR=1-TMR. Consequently, when FTA=0, it is equivalent to represent a ROC figure within FMR vs. TMR and FAR vs. (1-FRR). Moreover, Equal Error Rate is defined as the intersection of the line where FAR=FRR so it is also equivalent to calculate EER as 1-EER′ considering EER′ the intersection between ROC curve and FAR=1-FRR line.

Assuming all these considerations, the following approaches to calculate the similarity score between two acceleration signals are evaluated:

- Calculating similarity score applying LCS algorithm.
- Calculating similarity score through absolute distance, aligning previously the sequences with LCS.
- Calculating similarity score applying Generalized LCS algorithm.
- Calculating similarity score through absolute distance, aligning previously the sequences with Generalized LCS.

3.2.1 Calculating similarity score applying LCS algorithm

When applying Longest Common Subsequence algorithm to analyze the in-air signatures of the database created as explained in Section 2.2, the following results are obtained.

In Table 1 the Equal Error Results obtained on each of the repetition of the experiment is presented, as well as the average value:

These values are represented in Figure 1:

An average value of EER of 5.28±0.63% is finally obtained with this approach.

EER_1	EER_2	EER_3	EER_4	EER_5	$EER_{average}$	EER_{std}
5.37%	6.09%	5.22%	5.40%	4.33%	5.28%	0.63%

Table 1. EER results when obtaining the similarity score of in-air signatures applying LCS algorithm

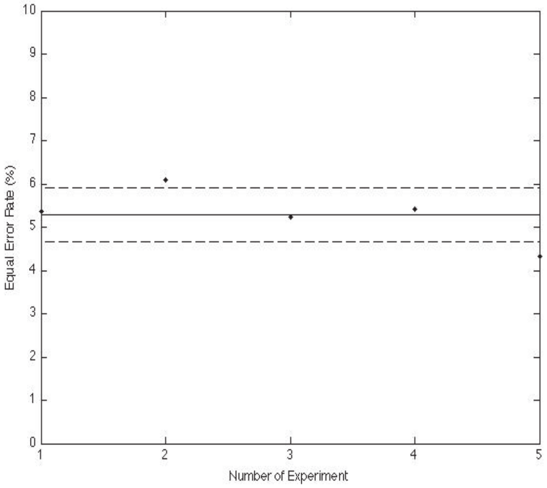

Fig. 1. Representation of EER results when obtaining the similarity score of in-air signatures applying LCS algorithm

EER_1	EER_2	EER_3	EER_4	EER_5	$EER_{average}$	EER_{std}
14.51%	10.63%	12.48%	14.09%	12.96%	12.93%	1.52%

Table 2. EER results when finding the optimal alignment within LCS algorithm, interpolating and calculating absolute distance as the similarity score of in-air signatures

3.2.2 Calculating similarity score through absolute distance, aligning previously the sequences with LCS

When utilizing LCS algorithm to find the optimal alignment of two in-air signatures, and then interpolating as explained in 2.4, the results of each repetition of the experiment are presented in Table 2:

These values are represented in Figure 4:

This approach obtains an EER value of 12.93±1.52 %, much worse than obtaining directly the score of LCS.

3.2.3 Calculating similarity score applying Generalized LCS algorithm

One more approach previously explained is based on generalize LCS algorithm with a step function $\zeta(v_i, w_j, \psi)$. In Table 3 the average EER results for different values of ψ are presented,

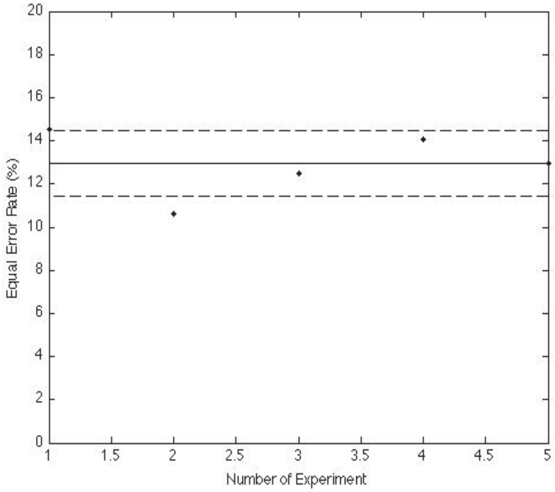

Fig. 2. Representation of EER results when obtaining the similarity score of in-air signatures applying LCS algorithm to align the signals, interpolating and calculating the absolute distance of the signals

ψ	$EER(\%)$
0.05	5.65±0.47
0.1	3.94±0.21
0.15	3.58±0.78
0.2	4.27±0.52
0.25	5.05±1.12
0.3	4.92±0.45
0.35	5.50 ±0.84
0.4	6.41±0.45
0.45	6.40±0.31

Table 3. EER results when obtaining the similarity score of in-air signatures applying a generalized LCS algorithm

utilizing LCS algorithm as a direct manner to obtain a similarity score between two in-air signature repetitions.

These values including average and deviation results are represented in Figure 3:

Some configurations of generalized LCS improve the performance results of classic LCS. In particular, an optimal EER value of 3.58±0.78 has been obtained when utilizing $\psi = 0.15$ as the maximum value that two points are considered that belongs to the longest common subsequence.

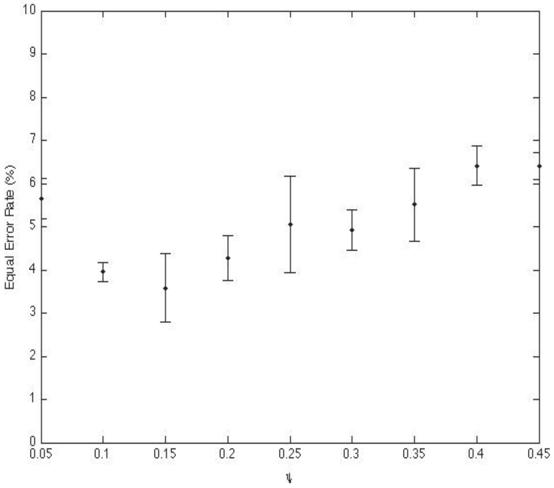

Fig. 3. Representation of EER results when obtaining the similarity score of in-air signatures applying a generalized LCS algorithm

ψ	$EER(\%)$
0.05	9.12±1.05
0.1	6.63±1.07
0.15	6.11±0.82
0.2	6.24±0.89
0.25	5.67±0.63
0.3	6.25±0.81
0.35	7.08±0.87
0.4	6.84±1.25
0.45	7.06±0.98

Table 4. EER results when finding the optimal alignment within a generalized LCS algorithm, interpolating and calculating absolute distance as the similarity score of in-air signatures

3.2.4 Calculating similarity score through absolute distance, aligning previously the sequences with generalized LCS

The generalization of LCS depending on ψ has been also applied to the optimal alignment and interpolation approach, obtaining the average EER results presented in Table 4:
These values with their respective deviations are represented in Figure 4:

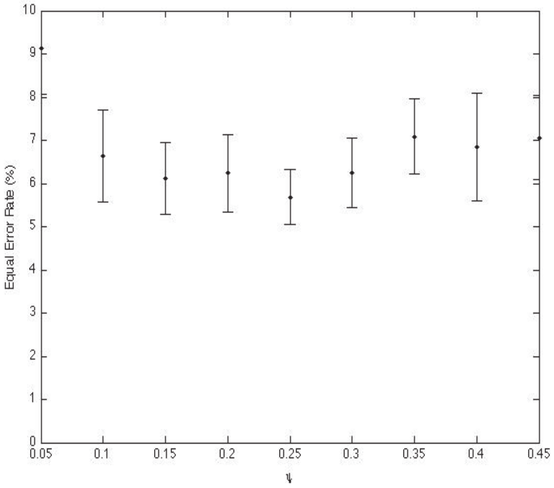

Fig. 4. Representation of EER results when obtaining the similarity score of in-air signatures applying a generalized LCS algorithm to align the signals, interpolating and calculating the absolute distance of the signals

In this case, utilizing a $\psi > 0$ value in the generalization of LCS implies a much better performance in respect to utilizing LCS to align and calculating afterwards a direct distance. In spite of this, the results when obtaining the score directly from the LCS algorithm are much better than this interpolating and calculating distance approach.

4. Conclusion and future work

Security in mobile devices may take advantage of the use of biometrics in order to authenticate the identity of the real person behind a mobile device. Nowadays, most of the applications requiring authentication rely on the use of passwords, with all their limitations.

At present, there are already other works trying to utilize biometric characteristics in mobile devices to authenticate users. In this article, a handwritten signature technique adapted to mobiles is proposed. This biometric technique is based on recognizing an identifying gesture carried out in the air. To accomplish this aim, users are authenticated by a gesture they perform moving their hand holding an accelerometer-embedded mobile device.

Authentication procedure requires uses to be enrolled in the system by repeating three times their in-air signature, invented by them. Afterwards, they are able to entry the system by performing it again.

As users are not able to repeat their in-air signatures accurately, different algorithm based on sequence alignment have been proposed to correct slightly differences between different repetitions of a gesture and provide a metric to quantify the similarities between them.

In particular, we have utilized four approaches based on the Longest Common Subsequence:

- The LCS algorithm to obtain a score of similarity of two sequences.

- The LCS algorithm to perform an optimal global alignment between two sequences, an interpolation the gaps previously introduced and a calculation of the absolute distance.
- A generalized LCS algorithm to obtain the score.
- A generalized LCS to align, interpolate and calculate absolute distance.

All these approaches have been evaluated within a database of 50 users who repeated 8 times their in-air signature holding a mobile device, and 6 people trying to forge each original gesture from video records.

From the results presented it can be concluded that:

- The performance of the LCS algorithm to obtain the score is better than to align the signals, interpolate and calculate absolute distance.
- Including the generalization proposed improves the results of classical LCS algorithm.
- An optimal EER value of 3.58±0.78 (%) has been obtained with utilizing the generalized ($\psi = 0.15$) LCS algorithm to obtain the similarity score to compare two performances of in-air signatures.

As future work, some other time series distances, as Dynamic Time Warping Berndt & Clifford (1994), may be used or other different approaches based on statistical method should be evaluated Suk et al. (2010), Lee & Kim (1999).

5. References

Bergroth, L., Hakonen, H. & Raita, T. (2000). A survey of longest common subsequence algorithms, *String Processing and Information Retrieval, 2000. SPIRE 2000. Proceedings. Seventh International Symposium on*, pp. 39–48.

Berndt, D. J. & Clifford, J. (1994). Using dynamic time warping to find patterns in time series, *KDD Workshop*, pp. 359–370.

Clarke, N. & Furnell, S. (2007). Authenticating mobile phone users using keystroke analysis, *International Journal of Information Security* 6: 1–14.

Durbin, R., Eddy, S., Krogh, A. & Mitchison, G. (2006). *Biological sequence analysis: Probabilistic Models of Proteins and Nucleic Acids*, eleventh edn, Cambridge University Press.

Fawcett, T. (2006). An introduction to roc analysis, *Pattern Recogn. Lett.* 27: 861–874.

Guerra-Casanova, J., Sánchez-Ávila, C., de Santos-Sierra, A., del Pozo, G. B. & Jara-Vera, V. (2010). A real-time in-air signature biometric technique using a mobile device embedding an accelerometer., *in* F. Zavoral, J. Yaghob, P. Pichappan & E. El-Qawasmeh (eds), *NDT (1)*, Vol. 87 of *Communications in Computer and Information Science*, Springer, pp. 497–503.

ho Cho, D., Park, K. R., Rhee, D. W., Kim, Y. & Yang, J. (2006). 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: 197–201.

Hsu, W.-H., Chiang, Y.-Y., Lin, W.-Y., Tai, W.-C. & Wu, J.-S. (2009). Integrating lcs and svm for 3d handwriting recognition on handheld devices using accelerometers, *Proceedings of the 3rd International Conference on Communications and information technology*, CIT'09, World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, Wisconsin, USA, pp. 195–197.

Ijiri, Y., Sakuragi, M. & Lao, S. (2006). Security management for mobile devices by face recognition, *Mobile Data Management, 2006. MDM 2006. 7th International Conference on*, pp. 49 – 49.

Iso, T. & Yamazaki, K. (2006). Gait analyzer based on a cell phone with a single three-axis accelerometer, *MobileHCI '06: Proceedings of the 8th conference on Human-computer interaction with mobile devices and services*, ACM, New York, NY, USA, pp. 141–144.

Jain, A. K., Flynn, P. & Ross, A. A. (2007). *Handbook of Biometrics*, Springer-Verlag New York, Inc., Secaucus, NJ, USA.

Jain, A. K., Griess, F. D. & Connell, S. D. (2002). On-line signature verification, *Pattern Recognition* 35(12): 2963 – 2972.

Jeong, D., Park, H.-A., Park, K. & Kim, J. (2005). Iris recognition in mobile phone based on adaptive gabor filter, *in* D. Zhang & A. Jain (eds), *Advances in Biometrics*, Vol. 3832 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, pp. 457–463.

Jeong, D. S., Park, H.-A., Park, K. R. & Kim, J. (2006). Iris recognition in mobile phone based on adaptive gabor filter, *Advances in Biometrics, International Conference, ICB 2006, Hong Kong, China, January 5-7, 2006, Proceedings*, pp. 457–463.

Kurkovsky, S., Carpenter, T. & MacDonald, C. (2010). Experiments with simple iris recognition for mobile phones, *Information Technology: New Generations, Third International Conference on* 0: 1293–1294.

Lapère, M. & Johnson, E. (1997). User authentication in mobile telecommunication environments using voice biometrics and smartcards, *IS&N '97: Proceedings of the Fourth International Conference on Intelligence and Services in Networks*, Springer-Verlag, London, UK, pp. 437–443.

Lee, H.-K. & Kim, J. H. (1999). An hmm-based threshold model approach for gesture recognition, *IEEE Transactions on Pattern Analysis and Machine Intelligence* 21: 961–973.

Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S. M. & Ailisto, H. A. (2005). Identifying users of portable devices from gait pattern with accelerometers, *Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP '05). IEEE International Conference on*, Vol. 2, pp. ii/973–ii/976 Vol. 2.

Nalwa, V. S. (1997). Automatic on-line signature verification, *Proceedings of the IEEE*, pp. 215–239.

Saevanee, H. & Bhatarakosol, P. (2008). User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device, *Computer and Electrical Engineering, International Conference on* 0: 82–86.

Shabeer, H. A. & Suganthi, P. (2007). Mobile phones security using biometrics, *Computational Intelligence and Multimedia Applications, International Conference on* 4: 270–274.

Steve Dowling, Nancy Paxton, J. H. (2009). Apple reports first quarter results.
URL: *http://www.apple.com/pr/library/2009/01/21results.html*

Suk, H. I., Sin, B. K. & Lee, S. W. (2010). Hand gesture recognition based on dynamic bayesian network framework, *Pattern Recogn.* 43: 3059–3072.

Tao, Q. & Veldhuis, R. (2006). Biometric authentication for a mobile personal device, *Mobile and Ubiquitous Systems, Annual International Conference on* 0: 1–3.

Wagner, R. A. & Fischer, M. J. (1974). The string-to-string correction problem, *J. ACM* 21: 168–173.

Wayman, J. L., Jain, A. K., Maltoni, D. & Maio, D. (2004). *Biometric Systems: Technology, Design and Performance Evaluation*, Springer-Verlag New York, Inc., Secaucus, NJ, USA.

yi Han, S., Park, H.-A., Cho, D. H., Park, K. R. & Lee, S. (2007). Face recognition based on near-infrared light using mobile phone, *Adaptive and Natural Computing Algorithms, 8th International Conference, ICANNGA 2007, Warsaw, Poland, April 11-14, 2007, Proceedings, Part II*, pp. 440–448.

Advanced Biometric Technologies
Edited by Dr. Girija Chetty

ISBN 978-953-307-487-0
Hard cover, 382 pages
Publisher InTech
Published online 09, August, 2011
Published in print edition August, 2011

The methods for human identity authentication based on biometrics â€“ the physiological and behavioural characteristics of a person have been evolving continuously and seen significant improvement in performance and robustness over the last few years. However, most of the systems reported perform well in controlled operating scenarios, and their performance deteriorates significantly under real world operating conditions, and far from satisfactory in terms of robustness and accuracy, vulnerability to fraud and forgery, and use of acceptable and appropriate authentication protocols. To address some challenges, and the requirements of new and emerging applications, and for seamless diffusion of biometrics in society, there is a need for development of novel paradigms and protocols, and improved algorithms and authentication techniques. This book volume on â€œAdvanced Biometric Technologiesâ€ is dedicated to the work being pursued by researchers around the world in this area, and includes some of the recent findings and their applications to address the challenges and emerging requirements for biometric based identity authentication systems. The book consists of 18 Chapters and is divided into four sections namely novel approaches, advanced algorithms, emerging applications and the multimodal fusion. The book was reviewed by editors Dr. Girija Chetty and Dr. Jucheng Yang We deeply appreciate the efforts of our guest editors: Dr. Norman Poh, Dr. Loris Nanni, Dr. Jianjiang Feng, Dr. Dongsun Park and Dr. Sook Yoon, as well as a number of anonymous reviewers.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Javier Guerra-Casanova, Carmen Sánchez-Ávila, Gonzalo Bailador-del Pozo and Alberto de Santos (2011). Application of LCS Algorithm to Authenticate Users within Their Mobile Phone Through In-Air Signatures, Advanced Biometric Technologies, Dr. Girija Chetty (Ed.), ISBN: 978-953-307-487-0, InTech, Available from: http://www.intechopen.com/books/advanced-biometric-technologies/application-of-lcs-algorithm-to-authenticate-users-within-their-mobile-phone-through-in-air-signatur

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820

www.intechopen.com

Fax: +385 (51) 686 166
www.intechopen.com

Fax: +86-21-62489821