Authentication in mobile devices through hand gesture recognition

J. Guerra-Casanova · C. Sánchez-Ávila ·
G. Bailador · A. de Santos Sierra

Abstract This article proposes an innovative biometric technique based on the idea of authenticating a person on a mobile device by gesture recognition. To accomplish this aim, a user is prompted to be recognized by a gesture he/she performs moving his/her hand while holding a mobile device with an accelerometer embedded. As users are not able to repeat a gesture exactly in the air, an algorithm based on sequence alignment is developed to correct slight differences between repetitions of the same gesture. The robustness of this biometric technique has been studied within 2 different tests analyzing a database of 100 users with real falsifications. Equal Error Rates of 2.01 and 4.82% have been obtained in a zero-effort and an active impostor attack, respectively. A permanence evaluation is also presented from the analysis of the repetition of the gestures of 25 users in 10 sessions over a month. Furthermore, two different gesture databases have been developed: one made up of 100 genuine identifying 3-D hand gestures and 3 impostors trying to falsify each of them and another with 25 volunteers repeating their identifying 3-D hand gesture in 10 sessions over a month. These databases are the most extensive in published studies, to the best of our knowledge.

Keywords Biometrics · Hand gesture recognition · Mobile · Security · Sequence alignment · Accelerometer

1 Introduction

Identifying and authenticating people is one of the oldest problems of humanity. Knowing whether a person is who he/she claims to be is one of the most important issues involved in security. This question has been solved over time in different ways, from first-century seals to middle-age passwords or manuscript signatures. In the last century, a lot of research has been carried out, and a huge improvement in recognition techniques has been achieved. In this context, biometrics appeared, becoming today one of the most important methods of recognizing people.

Biometric techniques are usually divided into two groups depending on the characteristics used to identify a person, namely physical and behavioral [15]. Physical biometric techniques are based on a physical characteristic that a user possesses and is maintained over time (iris [4], fingerprint [2], hand geometry [17], face [29]), whereas behavioral techniques are related to something that the user is able to repeat in an identifying unique manner (handwriting signature [41], keystroke [33], gait [20]). Some methods may be considered as a combination of physical and behavioral techniques (e.g., voice is based on the shape and size of the lips, nasal cavities or mouth as well as the emotional state and the words used in the utterance [36]).

Most of these biometric techniques have been implemented and are already in use, improving the security of different situations. One of the next steps in the security industry is to adapt or create new biometric techniques valid to mobile devices. Users are currently able to perform numerous operations from a mobile device. Switching on the device, making use of special functions, phoning reserved numbers, reading mail and accessing some Internet applications such as e-commerce, electronic voting and e-learning are only a few examples of possible cases where the mobile device would take advantage of biometrics in spite of the use of passwords with all of their limitations. Some lines of research connected to the idea of authenticating the user in a mobile device using biometrics are [3,5,22,34,37].

In this article, we propose to authenticate people within a biometric technique consisting of recognizing a person performing a 3-D gesture with one of his/her hands while holding a mobile device that integrates an accelerometer. Within this embedded sensor, the acceleration of the movement of the gesture in the 3 axes in time is measured. According to this, each person has an associated 3-D identifying hand gesture (as an in-air signature), created by him/her, so when a gesture is identified, so does the person behind it.

User authentication involves two procedures: user enrollment and verification. The former requires the user to perform several times his/her identifying 3-D hand gesture. A biometric gestural template is created as a result of the previous acquisitions, according to his/her identity. The user must repeat his/her 3-D gesture prior to entering the system in subsequent accesses. This repetition will be compared with the template in order to decide whether the user is the one registered previously, assuming that no one else is able to repeat his/her identifying gesture with high accuracy. This assumption is discussed in subsequent sections.

This proposed 3-D hand gesture technique is similar to a traditional handwritten signature [7], as it is based on "something that the user knows" (the aspect of the signature) and "something the user knows how to do" (the way the signature is "written"). In spite of the similarities, the approach proposed in this article provides some advantages to the traditional one, as it will be much harder for an impostor to copy a 3-D hand gesture rather than a signature written on a 2-D surface, where references are easily obtained [10]. Besides, traditional signature techniques need a special device to write the signatures, store the information and analyze it, typically a touch screen or a digital-based pen. This approach proposes the authentication of the user directly on his/her mobile device (phone, PDA...) avoiding the use of an additional widget, so this recognition technique will be very convenient for users, as they will not need to worry about other gadgets but their own mobile device.

The only requirement for the mobile device to be valid for this technique is that it must include a 3-axis accelerometer embedded in it, so that the movement involved in the gesture can be registered. According to this, when the hand gesture is made, three signals are provided by the accelerometer, corresponding to the variation in the hand gesture speed along the three axis of the space. This demand is not a problem since leading mobile phone manufacturers are marketing phones capable of carrying out this task with an ever-increasing sales volume. It is expected that in several years time, most mobile phones will integrate an accelerometer making this proposed biometric technique accessible to most of the population. For example, Apple sold more than 4 million iPhone mobiles, incorporating an embedded an accelerometer, just in the first 3 months of 2009 [35].

Accelerometers have been already used in biometrics, as in gait applications, embedded in mobile phones to detect the movement of people when walking [13] or placed on their wrist to identify how they swing their arms when walking [8]. It is also very common to find accelerometer applications to recognize gestures [12,23], an area in which a lot of research has been carried out [11,24,25]. However, the vision of this article is absolutely different. Most of these works have tried to recognize some gestures made by different people in order to identify the gesture not the person [18,19].

In this article, we consider a different approach, as the goal is to recognize people through gestures instead of recognizing gestures made by different people. The first experiments on this approach were introduced in [26,30] where the authors present an initial study about the feasibility of this kind of authentication with databases of 22 and 12 users, respectively.

Moreover, a crucial point of this approach should contemplate that other people may try to forge someone else identifying gesture. Therefore, this technique should be able to distinguish those gestures belonging to the authentic person and those, similar but different, imitation attempts. Initial work has been carried out as well in terms of real falsification attempts in [9,21], where a database of 34 users was considered in the former and two databases of 10 users in the latter.

In this article, a complete evaluation of this biometric technique is presented by analyzing a much more extensive database (100 users) including real attempts at falsification carried out by the study of video records of authentic people making their identifying gesture in order to assure the feasibility of the gesture authentication technique in the real world.

This article is divided into the following sections: Sect. 2 presents the requirements any biometric technique should satisfy and to what extent our technique fulfills them. Next, Sect. 3 explains the mathematical method used to analyze the signals involved in the technique. Moreover, Sect. 4 provides an interpretation of how the algorithm works depending on the configuration of the parameters involved. The feasibility of this technique is evaluated with two different databases of 3-D hand gestures, as described in Sect. 5. Different experiments have been carried out, obtaining the results detailed in Sect. 6, including the evaluation of a "zero-effort attack" and an "active impostor attack" where the forged trials considered are original gestures of other users or real attempts at falsification, respectively. Finally, conclusions and future work are specified in Sect. 7.

2 Technique feasibility

A biometric technique should fulfill the following requirements to prove its robustness and be considered as a valid method of identifying people [14]:

- **Universality**: "*Everybody should possess the necessary characteristic to be identified.* The technique proposed in this paper is based on the movement of the hand, so the method is prepared to identify any person able to carry out a gesture involving moving an arm or a hand."
- **Collectively**: "*The biometric pattern should be obtained in a non-intrusive manner*". In this case, biometric data are effortlessly acquired, as the device used to make the 3-D hand gestures incorporates an accelerometer able to acquire all the information necessary to generate the template.
- **Acceptability**: "*Users should accept this method, feeling secure and comfortable when the biometric characteristics are extracted*". In this study, 3-D hand gestures have been made by the movement of a hand holding an iPhone with an embedded accelerometer. The users showed no resistance nor difficulty in handling the device. Furthermore, data acquisition and processings are absolutely transparent to the user.
- **Circumvention**: "*It should not be possible to forge the behavioral biometric characteristic*". A twofold analysis of the precautions against the forgery of the technique has been carried out: Firstly, a zero-effort attack has been simulated where users try to forge the signature of someone else by performing his/her own identifying 3-D hand gesture, resulting in a Equal Error Rate presented in Sect. 6.1. Secondly, extensive research into fraud detection has been analyzed with real falsification trials from the study of the records of people making their original 3-D hand gesture in front of a video camera. Results of this experiment are shown in Sect. 6.2.
- **Uniqueness**: "*The identifying characteristic should be distinctive among different individuals*". The uniqueness between different gestures is derived as well from the zero-effort test in Sect. 6.1 since the similarities between different gestures are compared.
- **Permanence**: "*The feature should remain invariable or with little variation over time*". This is a crucial requirement for this technique; in fact, users have been seen as being afraid of not being able to repeat a hand gesture over time with enough quality, even though they are. In Sect. 6.3, results of permanence evaluation are presented, proving that the variation in the 3-D hand gestures in time is low enough to make this technique work properly.
- **Performance**: "*A biometric technique fulfills the performance characteristic if it is robust, accurate and speedy enough*". In Sect. 6.4, a comparison between permanence and circumvention tests is made to study robustness and accuracy. Finally, in Sect. 6.5, an analysis of enrollment and verification duration in a personal computer and in a mobile device is carried out to attain the speed of the technique.

3 Authentication procedure

The overall authentication process takes place in two phases. Firstly, the user should enroll in the system by making a gesture in the air with the hand holding the accelerometer-embedded device. This 3-D hand gesture should be repeatable by the user, as it is used as his/her identifying template. Lately, in the access phase, the user should repeat the 3-D gesture made in the former step to gain right of entry to the system.

This section describes also the mathematical algorithm implemented in order to compare the different repetitions of gestures and quantify their differences as a means of deciding whether they have been made by the same person or not. The best results have been obtained applying the algorithm presented in this Section, which is based on sequence alignment [6] and similar to Dynamic Time Warping (DTW) [1]. This algorithm consists of aligning signals and the quantifying the differences between them using Euclidean distance. All the implementation concepts upon which this research is supported are explained in two sections, according to the two subsuming steps of the authentication process: enrollment and verification.

3.1 Enrollment phase

In this initial phase, an unknown user attempting to be registered in the system has to think about a 3-D gesture, repeatable by him/her but not so easy that another person glancing at him could reproduce it without any effort.

Actually, the device that integrates an accelerometer offers the following instruction to the users trying to be enrolled in the system:

"*To be enrolled in this device, take some minutes to think about a 3-D hand gesture you desire to be identified by, considering these three factors:*

- *You should be able to remember and repeat the gesture easily. An easy to remember or natural gesture is highly recommended.*
- *You should choose a complex enough gesture that does not permit anyone reproduce it immediately.*
- *It should last less than 6 s.*"

The chosen and distinctive hand gesture, which the user will use to be identified with, should be repeated three times, as precisely as possible, by holding a device including an accelerometer (i.e., an iPhone).

The system collects the variation in the speed of the device on each axis of the space when the hand gesture is being made. Thereafter, a data processing is carried out, obtaining some parameters required to create the biometric template used for authentication.

A mathematical detailed explanation of each step required to accomplish this phase is presented in the following sections.

3.1.1 Data acquisition

Each user U_i makes a gesture G_i that produces three different signals (G_i^x, G_i^y and G_i^z) corresponding to the accelerations of each gesture on each axis of the space. Each repetition j of the same gesture G_i performed by the user U_i is defined as $G_{i,j}$. Consequently, as three repetitions of the gesture are needed in the enrollment of a user U_i, nine signals are obtained: $G_{i,j}^x, G_{i,j}^y, G_{i,j}^z, j = 1, 2, 3$.

Figure 1 shows two repetitions of a gesture G_i by the user U_i on each axis. It is remarkable that the shape of the signals on each axis is very similar, but they are not completely aligned. Furthermore, there are some parts of one signal narrower in contrast to the other, due to slight changes in speed when the user reproduces the movement. The preprocessing of the signals attempts to correct these differences.

The biometric technique has been implemented with a sampling rate of 50 Hz, a frequency precise enough to obtain representative signals of a hand movement in the air [38]. As was explained before, gestures should last less than 6 s, so the accelerometer generates a signal on each axis X, Y, Z of 300 points. If the gesture lasts less than 6 s, the rest of the points of the signal will be filled with 0, whereas if it is longer, the signal will be truncated. Signals of each axis will be concatenated into a single vector, becoming a signal of 900 points, which is the one stored in the device for each gesture. Note that in Figs. 1, 2, 3 and 4, only the significant part of the signals appears, as the part filled with zeros has been truncated to improve its visualization.

Therefore, the biometric template of each user consists of three signals of 900 points corresponding to the accelerations of each repetition of the gesture and a parameter obtained from the analysis of these three signals, which is explained below.

3.1.2 Signal processing

When a user repeats his/her gesture, some speed variations in the signals may appear as some parts of the same gestures may be made slightly faster or slower. This error is compensated by an alignment processing which corrects those little variations, and therefore, when two instances of the same gesture by the same user are compared, the alignment of the signals will result in two quite similar signals whereas two different instances of a gesture will result in very different signals in spite of the alignment process.

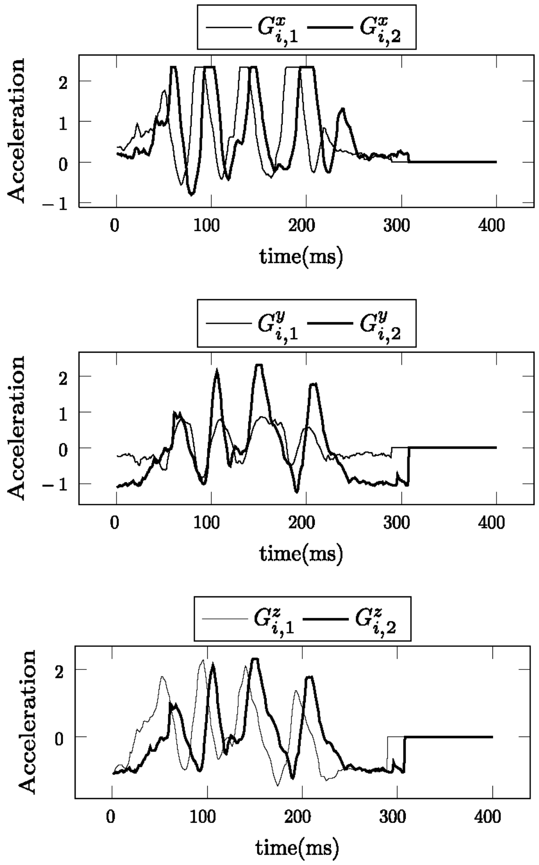

Fig. 1 Example of two repetitions of the same 3-D hand gesture made by the same user

In accordance with this, two acceleration signals from two gesture repetitions are analyzed through the following steps:

- Global sequence alignment algorithm.
- Optional interpolation of aligned signals.
- Quantification of differences of the aligned signals.

This whole process is carried out for each axis separately, so three signal processings are necessary for each pair of samples of gestures. As was explained in Sect. 3.1, the user should make three gestures in the enrollment phase. Consequently, as these three gestures will be processed in pairs, nine signal processings would be necessary at enrollment phase.

The following subsections describe in detail each step of the signal processing for two signals of two different

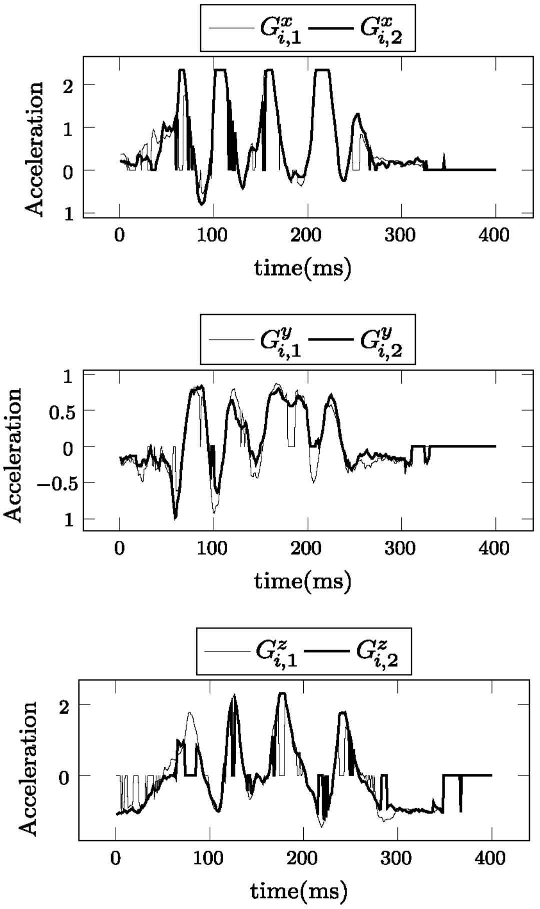

Fig. 2 Example of the alignment of two repetitions of the same 3-D hand gesture

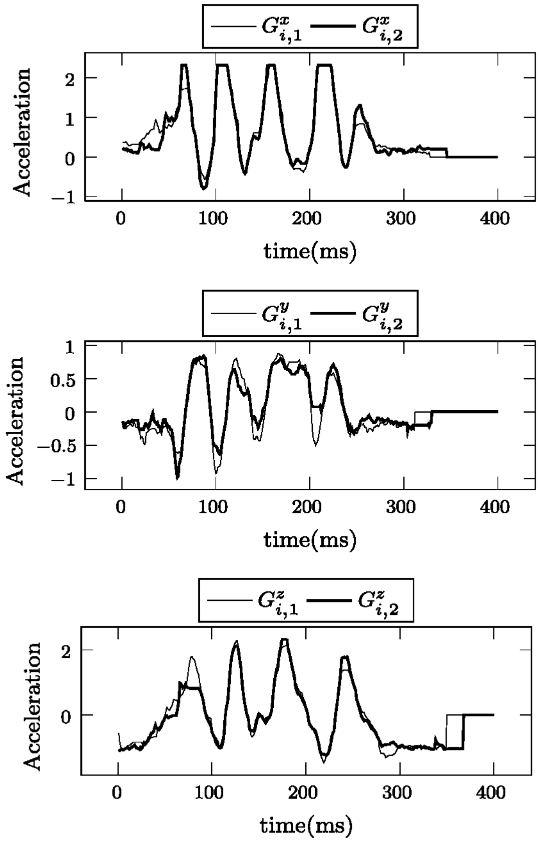

Fig. 3 Example of preprocessing two repetitions of the same 3-D hand gesture made by the same user

repetitions of the same gesture made on the same axis $\left(\text{i.e., } G^x_{i,1} \text{ and } G^x_{i,2}\right)$.

1. **Global sequence alignment algorithm**
   The soft adaptation algorithm implemented in this work is a global sequence alignment algorithm, similar to Dynamic Time Warping, used to obtain the best alignment result based on a defined metric.
   As has been previously introduced, the global sequence alignment developed tries to correct little deviations between very similar repetitions of gestures. This algorithm provides by itself a metric to compare two signals depending on the optimized value of the score presented in Eq. 1 and explained below. However, better results have been obtained when applying this algorithm only to align the signals and quantifying the differences between these aligned signals using other techniques presented later.
   The proposed algorithm to find the best global alignment between two sequences $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_m\}$ of equal length starts by the creation of a matrix of scores $M_{m\times m}$. The objective of the algorithm is to find the optimal path from $M_{1,1}$ to $M_{m,m}$ that maximizes the score in $M_{m,m}$. This matrix of scores is filled according to the expression defined in Eq. 1:

$$M_{i,j} = \max \begin{cases} M_{i,j-1} + h \\ M_{i-1,j-1} + \delta \\ M_{i-1,j} + h \end{cases} \qquad (1)$$

   where δ is a fuzzy decision function that represents the similarity between two points in each sequence:

$$\delta = e^{-\frac{(x-\mu)^2}{2\sigma^2}} \qquad (2)$$

   where $\mu = a_{i-1}$ and $x = b_{i-1}$ are the values of the previous points in base to whom the score of the new points $M(i, j)$ is calculated.
   According to the expression selected in Eq. 1 to calculate $M(i, j)$, three possible movements are defined. A horizontal, diagonal, or vertical movement is made whenever the first, second, or third expression is selected.
   Once matrix M is filled, a backtracking algorithm is carried out to obtain the optimal path from $M_{1,1}$ to

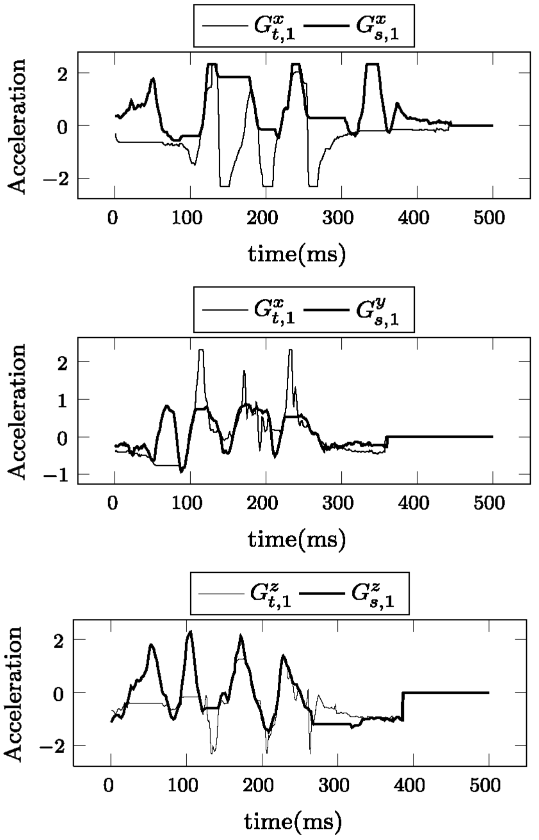

Fig. 4 Example of preprocessing a pair of samples of two different 3-D hand gestures corresponding to different users

$M_{m-1,m-1}$. This algorithm includes a zero value between a_i and a_{i+1} (or b_j and b_{j+1}) whenever a horizontal (or vertical) movement in Matrix $M(i, j)$ is required to obtain the optimal path.

Consequently, from this algorithm, two sequences A' and B' are obtained, made up of the initial signals A and B, and filled by a number of zero values at certain points in order to find an optimal alignment between them. The length of A' and B' fulfills $m < L' < 2m$ depending on the number of zeros introduced into them.

Furthermore, in Eqs. 1 and 2, there are two parameters that should be configured:

- h is a constant (gap) representing when the algorithm considers two very similar values of the signals [27].
- σ is a constant used to normalize the differences between the values of the points of these signals.

The optimal configuration of the algorithm in terms of h and σ will be selected according to the results obtained in Sects. 6.1 and 6.2. Furthermore, the number of corrections of the algorithm depends on the values of h and σ. When a large number of zero values are included in two signals (very little differences are corrected), the rhythm of correction is high and vice versa. The interpretation of the different configurations of the algorithm is discussed in Sect. 4.

Besides, by definition of this algorithm, $M_{1,1} = 0$ and $M_{1,j} = M_{j,1} = h \times j$.

Figure 2 illustrates an example of the result of applying this algorithm to the signals on each axis of the two gestures in Fig. 1, where the inclusion of zero values to align both signals can be seen.

2. **Interpolation of aligned signals**

This is an optional phase consisting of correcting the zero values from the aligned signals introduced by the previously described algorithm. It works by substituting any zero value found by the average value of its neighbors (not being zero). This may be a good strategy when the alignment algorithm has included too many zero values even though the points of the signals were quite similar (high correction rhythm).

Let $I(i, j)$ be an interval of zero values in the sequence A', so $a'_i = a'_{i+1} = \cdots = a'_j = 0$, obviously, $a'_{i-1} \neq 0$ and $a'_{j+1} \neq 0$. Then, interpolation is implemented as follows:

$$a'_k = \frac{a'_{k-1} + a'_{j+1}}{2}, \quad \forall k = i, \ldots, j \tag{3}$$

The result of the interpolation of signals of Fig. 2 is shown in Fig. 3. It can be seen that the signals have been aligned accurately by implementing the alignment algorithm and the interpolation of the zero values included to maximize the alignment process. This high degree of accuracy is a consequence of the huge similarity between the signals analyzed. Moreover, as we assume that only one person is able to repeat his/her gesture so accurately, it can be concluded that the same person made both gestures.

If the same process of alignment and interpolation is applied to signals from different gestures, the result is not so good (Fig. 4), since these algorithms correct only little variations between signals. Consequently, if the original signals are not very similar, there is an appreciable difference between the sequences despite the processing algorithm.

The inclusion of this interpolation phase obtains good performance results when the rhythm of correcting is very high, and a high amount of zero values have been included when comparing two signals.

This behavior may be expected since, when the correcting rhythm of the algorithm is very high, lots of zero values were introduced even though two points of the signal were quite similar. Consequently, interpolating these zero values may provide a reliable representation of the differences between the two signals compared. However,

when the rhythm of correcting is low and a small amount of zero values are introduced, the algorithm works better without interpolation since when only the greater differences between points of the signals are corrected, it is better to maintain or enlarge those differences by including zero values, without compensating them with interpolation.
According to this, including an interpolation phase in the analysis of two acceleration gesture signals may improve the results obtained depending on the configuration of the alignment algorithm in terms of h and σ. This assumption is demonstrated through the results of the experiments in Sects. 6.1 and 6.2.

3. **Quantification of the differences of the aligned signals**
A metric to quantify the similarities between two gestures has been defined in order to make possible an accurate decision on the authorship of both gestures. In this context, Euclidean distance is proposed to quantify the difference between the aligned and optionally interpolated signals A' and B', where L' is the length of the aligned signals.

$$\delta_{A,B} = \sqrt{\sum_{i=0}^{L'} (a'_i - b'_i)^2} \tag{4}$$

3.1.3 Biometric hand gesture template obtention

At the beginning of enrollment phase, a specific user U_T repeated the same enrolling gesture G_T three times ($G_{T,1}$, $G_{T,2}$, $G_{T,3}$), and their respective signals of acceleration in each axis were obtained.

Analyzing all the signals of the enrollment phase implies 9 repetitions of the processing algorithm to obtain the differences in every gesture with the other two. The reader must note that this operation involves the execution of an algorithm for each axis. Consequently, the following distance values are obtained: $\delta^x_{j,k}$, $\delta^y_{j,k}$, $\delta^z_{j,k}$ for $j, k = 1, 2, 3$ and $j \neq k$ where, for instance, $\delta^x_{j,k}$ represents the distance between aligned signals $G_{T,j}$ and $G_{T,k}$, only in the x-direction.

The difference between two samples $G_{T,j}$ and $G_{T,k}$ of a gesture G_T is finally calculated by the following equation:

$$\delta_{j,k} = \frac{\delta^x_{j,k} + \delta^y_{j,k} + \delta^z_{j,k}}{3} \tag{5}$$

According to Eq. 5, the differences between each sample of the enrollment gesture ($\delta_{1,2}$, $\delta_{1,3}$ and $\delta_{2,3}$) are computed. The average difference in the template, namely μ_T, is defined as the average of the differences between the three gestures made to enroll in the system (Eq. 6).

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

Finally, the biometric template of the user, which is stored in the mobile device to authenticate the user, is made up of:

- Signals $G_{T,1}$, $G_{T,2}$ and $G_{T,3}$, which include the accelerations on each axis of each gesture repetition.
- Parameter μ_T, obtained in Eq. 6, representing the similarity between the three repetitions of a gesture made by the user.

The lower the μ_T, the safer the biometric template. μ_T represents the facility of a user to repeat his/her gesture closely. In other words, when μ_T is low, an imposter trying to forge the gesture should do it as precise as the authentic user does. On the other hand, a high value of μ_T means that the authentic user is not able to repeat his/her own gesture accurately, so the access threshold should be higher, facilitating an attacker to fake the original gesture. In fact, from this value, a 3-D gesture strength measurement may be implemented easily in order to avoid people enrolling in the system with easily forgeable gestures. An important and complementary study of other characteristics of the gestures that make them difficult imitate should be studied in future works.

3.2 Verification phase

Once a user has been enrolled in the system by repeating a certain gesture three times, he/she is able to access the system by performing his/her identifying gesture again. The mobile device will record the accelerations of the access gesture G_V on each axis, obtaining G^x_V, G^y_V and G^z_V signals.

Next, a preprocessing between access and template signals ($G_{T,1}$,$G_{T,2}$,$G_{T,3}$) is carried out, providing the differences between the access gesture and template ones $\delta_{V,1}$, $\delta_{V,2}$, $\delta_{V,3}$ (Eq. 5). From these three values, δ_V is calculated as the average of all of them.

This distance lacks interest if it is not compared to other equivalent distances. Therefore, an indicator is proposed to compare the two averages of differences defined in this exposition: μ_T obtained from the enrollment and δ_V from the access phase. This function must provide a high score if both parameters are similar enough, and otherwise a low one. Since both averages of differences are real numbers, a simple fraction δ_V / μ_T meets the goal of comparing these two values: the closer to 1, the more similar the numbers.

Consequently, a threshold θ has been defined, so any access gesture can gain access to the system if the following equation is fulfilled:

$$\delta_V / \mu_T < \theta \tag{7}$$

Parameter θ indicates to what extent the access gesture is similar to stored template gestures. Obviously, the closer to 1, the more similar the access gesture and the template are. In this article, we will try to find the optimal threshold that minimizes the overall error of impostor access and genuine rejecting. An evaluation of this threshold value is discussed in Sect. 6.4.

4 Interpretation of the global sequence alignment algorithm in terms of h and σ

The previously described global sequence alignment algorithm includes two parameters (h and σ) defining the behavior of the algorithm when two signals are compared.

It is remarkable that the algorithm does not work properly unless the condition in Eq. 8 is accomplished:

$$h < 0.5 \tag{8}$$

This requirement is demonstrated as follows:

According to Eq. 1, $M_{i,j-1}$ and $M_{i-1,j}$ are calculated as in Eqs. 9 and 10, respectively:

$$M_{i,j-1} = \max \begin{cases} M_{i,j-2} + h \\ M_{i-1,j-2} + \delta \\ M_{i-1,j-1} + h \end{cases} \tag{9}$$

$$M_{i-1,j} = \max \begin{cases} M_{i-1,j-1} + h \\ M_{i-2,j-1} + \delta \\ M_{i-2,j} + h \end{cases} \tag{10}$$

Therefore, expressions in Eq. 11 are deducted:

$$\begin{aligned} M_{i,j-1} &\geq M_{i-1,j-1} + h \\ M_{i-1,j} &\geq M_{i-1,j-1} + h \end{aligned} \tag{11}$$

Consequently, by applying those results to the first and the third expressions in Eq. 1, expressions in Eq. 12 are inferred by adding h to each term:

$$\begin{aligned} M_{i,j-1} + h &>= M_{i-1,j-1} + 2h \\ M_{i-1,j} + h &>= M_{i-1,j-1} + 2h \end{aligned} \tag{12}$$

Within both expressions in Eq. 12, a minimal value of the first and the third expressions in Eq. 1 has been found. According to this, the second expression in Eq. 1 would be never selected when $2h > \delta$. Besides, considering the fact that $0 \leq \delta \leq 1$ is equivalent to $h > 0.5$, demonstrating the requirement in Eq. 8.

Moreover, according to the preceding demonstration, when two points of the signals are compared, the algorithm in Eq. 1 would admit that both points are the same when Eq. 13 is fulfilled:

$$\delta > 2h \tag{13}$$

Whenever the algorithm in Eq. 1 finds two points that do not comply with Eq. 13, it introduces a zero value in order to correct it.

Consequently, the parameters h and σ would define the rhythm, and the algorithm corrects differences between signals, according to the following behaviors:

- The lower the value of h, the lower δ should be, to consider the two points as the same, meaning that corrections would appear only when great differences between points of the signals are found. Therefore, the algorithm with a low h introduces a low quantity of zero values to find the optimal alignment between two signals. On the other hand, when h is high and close to $h = 0.5$, little deviations between the signals would be corrected, introducing a high amount of zero values.
- The lower the σ, the higher the denominator in the exponent in Eq. 2 is, and obviously, the lower δ is as well. In this case, as specified by Eq. 13, the more difficult two points are considered the same, and consequently, the more corrections would be introduced. Evidently, with higher σ values, the behavior of the algorithm would be the reverse, including a low amount of zero values.

By joining the behaviors of the two parameters, it can be concluded that the algorithm would correct at a high speed, including a large amount of zero values, when h is high and σ is low, whereas when h is low and σ is high, the algorithm would correct at a low speed by introducing a low number of zero values. In the other two cases (h high and σ high, h low and σ low), both behaviors tend to compensate each other, correcting signals at an intermediate speed.

Sections 6.1 and 6.2 provide a study of the optimal configuration of the parameters h and σ of the algorithm within a database of real gestures.

5 Databases

To the knowledge of the authors, there are no public databases of identifying 3-D hand gestures made in the air with a mobile with an embedded accelerometer. Therefore, two different databases have been created in order to evaluate the requirements of the biometric technique, introduced in Sect. 2.

The first database (GB2SGestureDB1) has been created to verify the robustness of the technique against different attacks. In particular, two complementary tests have been carried out: A zero-effort attack (an impostor attempts to authenticate into the system with a false identity but using his/her own identifying 3-D hand gesture) and an Impostor attack (an impostor studying and trying to repeat the original hand gesture of a authentic user).

GB2SGestureDB1 contains identifying 3-D hand gestures of 100 different users made using a mobile device with an embedded accelerometer. Each user repeated his own gesture 8 times, while being recorded on video. From the study of these records, 3 different people have attempted attempts to forge each gesture (7 trials each). Accelerations of 3-D hand gestures on axis *x*-*y*-*z* have been obtained at a sampling rate of 100 Hz (10 ms.).

The second database (GB2SGestureDB2) has been generated in order to study the permanence of the performance of the hand gestures over time. According to this, GB2SGestureDB2 is a database of 25 people repeating their 3-D hand gestures at 10 sessions within a month. At each session, each user made his/her 3-D hand gesture 5 times. Accelerations of 3-D gestures have been extracted, as well, at a sampling rate of 100 Hz (10 ms.).

In summary, GB2SGestureDB1 consists of 800 (100 users, 8 times) samples of original 3-D hand gestures and 2100 (100 gestures, 3 impostors, 7 trials) attempts of falsification, whereas GB2SGestureDB2 is made up of 1250 (25 users, 10 sessions, 5 times) repetitions of 3-D hand gestures over time.

6 Experimental results

The following tests have been carried out to evaluate the feasibility of the novel biometric technique proposed and verify the characteristics described in Sect. 2:

- **Zero-effort impostor detection test**: This test studies to what extent the biometric technique proposed is vulnerable to an attack where an impostor attempts to access the system with his/her identifying 3-D hand gesture as if he/she where someone else. To accomplish this task, GB2SGestureDB1 has been analyzed, following the operations to access the system explained in Sect. 3.2. The metric to evaluate the robustness of the system in this kind of attack will be the standard in the field of biometrics, the Equal Error Rate (EER), obtained from False Rejection Rates (FRR), and False Acceptance Rates (FAR) [31]. The lower the EER, the better the circumvention the technique provides. This test will be carried out for different values of the parameters of the algorithm explained in Sect. 3.1.2, in order to find a configuration of the algorithm with optimal error rates. In addition to this, all the configurations have been evaluated with and without the interpolation phase, as a means of assessing the benefit of interpolating and confirming the behavior of the algorithm described in Sect. 3.1.2. Obviously, a low EER value implies also a high level of unicity between different hand gestures.
- **Active impostor detection test**: This study aims to assess whether anybody is able to forge the system, accessing without being the legitimate user but trying to falsify his/her identifying 3-D hand gesture. Also, in the previous test, the EER has been obtained in order to evaluate the results of the test, by using the original 3-D hand gesture and their attempts of falsifying of GB2SGestureDB1. This test evaluates the fraud resistance of the technique and completes the study of circumvention, as covered by the study of attempting to forge the system by imitating the own hand gesture of the real person. Different configurations of the parameters of the algorithms have been tested as well as applying interpolation phase or not in order to find the lowest possible EER.
- **Permanence evaluation**: This experiment attempts to assess to what extent a user is able to reproduce a hand gesture over time, verifying the persistence of the biometric technique when users repeat their identifying gesture often. To achieve this aim, GB2SGestureDB2 has been examined obtaining the trend of the repeatability of the 3-D hand gestures by the users in different sessions spread over a month. Furthermore, an updating strategy has been tested, so user templates are constantly adapted to the variation on the way of making their 3-D hand gestures. This test is carried out with the optimal configuration of the algorithm for the two previous tests.
- **Feasibility evaluation**: This essay intends to join together the impostor detection and permanence test to study whether a legitimate user is able to repeat a 3-D hand gesture in spite of the passage of time with much more quality than an impostor does. To accomplish this task, a global evaluation of the results of the previous tests is described.
- **Time Analysis**: Finally, the results of the duration of enrollment and verification phases in a mobile device and a personal computer are presented.

6.1 Zero-effort impostor detection test

This test examines the robustness of the system when other users attempt to forge the identity of another user by performing their own 3-D hand gesture. In this test, the analysis is carried out exactly in the same manner as the verification phase explained in Sect. 3.2. Consequently, for each user, at first, three of his/her original samples are considered as the enrollment repetitions of his/her identifying 3-D hand gesture by calculating μ_T following the mathematical operations previously described. The rest of the original samples of the user the template is calculated are regarded as authentic accesses, whereas the samples of 3-D hand gestures not made by the user represent impostor attempts of forging the identity. This test has been carried out by analyzing GB2SGestureDB1. In these conditions, the Equal Error Rate has been calculated from FRR (False Rejection Rate) and FAR (False Acceptance Rate) as follows [39]:

- Template Creation: Three samples of each hand gesture are considered as the template of the user. Then, the μ_T for each user is calculated as explained in Sect. 3.1.3.

Table 1 EER (%) zero-effort impostor detection test results with different configurations of h, σ and applying the interpolating phase

σ	h									
	0.05	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45	0.50
0.05	**8.68**	**9.65**	**10.96**	**10.60**	**11.21**	**11.51**	**19.71**	**22.60**	**24.29**	**44.26**
0.10	**3.19**	**4.35**	**4.97**	**5.47**	**6.37**	**9.52**	**11.28**	**14.26**	**19.35**	**44.26**
0.15	**2.26**	**3.04**	**3.30**	**3.21**	**3.54**	**5.31**	**7.26**	**9.16**	**15.26**	**44.26**
0.20	**2.09**	**2.57**	**2.50**	**2.74**	**2.91**	**3.43**	**4.19**	**6.16**	**10.29**	**44.26**
0.25	**2.05**	**2.45**	**2.41**	**2.48**	**2.54**	**2.93**	**3.36**	**4.18**	**7.40**	**44.26**
0.30	**2.22**	**2.31**	**2.38**	**2.19**	**2.17**	**2.61**	**3.09**	**3.48**	**5.86**	**44.26**
0.35	**2.23**	**2.21**	**2.38**	**2.17**	**2.17**	**2.20**	**2.71**	**3.38**	**4.95**	**44.26**
0.40	**2.31**	**2.39**	**2.23**	**2.19**	**2.14**	**2.38**	**2.27**	**2.75**	**4.48**	**44.26**
0.45	**2.17**	2. 45	**2.56**	**2.22**	**2.11**	**2.35**	**2.37**	**2.56**	**3.73**	**44.26**
0.50	2.17	**2.31**	**2.26**	**2.34**	**2.31**	**2.20**	**2.32**	**2.41**	**3.11**	**44.26**
0.55	2.30	2.31	2.38	**2.09**	**2.31**	**2.41**	**2.38**	**2.38**	**3.11**	**44.26**
0.60	2.43	2.25	2.39	**2.19**	**2.21**	**2.41**	**2.45**	**2.42**	**2.67**	**44.26**
0.65	2.59	2.42	2.41	**2.04**	**2.17**	**2.73**	**2.58**	**2.45**	**2.39**	**44.26**
0.70	2.85	2.57	2.52	**2.04**	**2.22**	**2.56**	**2.64**	**2.38**	**2.38**	**44.26**
0.75	2.98	2.73	2.73	**2.11**	2.28	2.61	**2.50**	**2.38**	**2.22**	**44.26**
0.80	3.02	2.99	3.06	**2.17**	**2.13**	2.28	**2.56**	**2.56**	**2.12**	**44.26**
0.85	3.26	2.99	3.30	**2.38**	2.17	2.42	**2.38**	**2.56**	***2.01***	**44.26**
0.90	3.14	3.15	3.42	**2.58**	2. 46	2.38	2.52	2.75	**2.06**	**44.26**
0.95	3.22	3.12	3.49	**2.66**	2.53	2.38	2.38	**2.75**	**2.20**	**44.26**

- Analysis of original samples: The remaining five original samples of each gesture are used to calculate the False Rejection Rate, since they are truthful attempts at accessing the system. For each original trial, the δ_V/μ_T is obtained when comparing the accessing gesture with the three gestures of the original user template.
- Analysis of falsified samples: All the impostor attempts at trying to access the system are used to evaluate the False Acceptance Rate. For each falsification trial, δ_V/μ_T is also obtained.
- Obtaining of False Acceptance Rate (FAR) and False Rejection Rate (FRR): The FAR and FRR are obtained in terms of θ as the % of original samples that are over θ in the case of False Rejection Rate and the % of falsified samples that are under θ in the case of False Rejection Rate. It has been showed that when θ is very low, most falsifications are rejected but so are some authentic attempts. However, the higher the θ, the more original access are justifiably allowed but so to are the more falsifications granted.
- Obtaining the Equal Error Rate (EER): The EER is defined as the value of the error when the False Acceptance Rate is equal to the False Rejection Rate, and it is the most commonly used metric to measure the performance of biometric techniques.

Therefore, the FRR has been obtained from 500 samples (100 users, 5 accessing attempts) and FAR from 79200 samples (100 original 3-D hand gestures, 99 impostor gestures, 8 samples).

In this approach, the EER has been evaluated for different values of h and σ, according to the condition of Eq. 8. Besides, the EER has been obtained when applying interpolation phase or not, originating the results presented in Tables 1 and 2, when interpolation was applied in the former and not applied in the latter.

The lowest EER result for each configuration of h and σ of both tables is symbolized in bold, in order to represent in which configurations interpolating reduces or increases the EER result. In addition to this, the optimal value of each table is highlighted in bold italics.

The lowest Equal Error Rates obtained reach a value of 2.01% with a configuration of $h = 0.45$, $\sigma = 0.85$ with interpolation (highlighted in Table 1) and $h = 0.05, \sigma = 0.55$ without interpolation (highlighted in Table 2). There are several configurations with higher but close rates in respect to the optimal, since the variations in h and σ are very small between configurations.

Moreover, there are some expected behaviors of the different configurations of the algorithm explained in Sect. 4, which are concluded by examining the results of Tables 1 and 2:

Table 2 EER (%) zero-effort impostor detection test results with different configurations of h, σ and without applying the interpolating phase

σ	h									
	0.05	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45	0.50
0.05	15.30	16.80	17.04	18.94	19.43	21.51	21.65	24.48	24.83	45.60
0.10	8.23	9.41	10.96	12.19	13.42	14.81	16.67	18.77	21.48	45.60
0.15	4.87	6.10	6.92	7.71	9.27	10.57	12.97	14.70	18.67	45.60
0.20	3.90	4.31	5.09	5.94	6.71	7.69	9.20	11.97	15.10	45.60
0.25	3.28	3.69	3.99	4.35	5.31	6.16	7.62	9.38	13.30	45.60
0.30	2.97	3.19	3.58	3.89	4.07	5.33	6.20	7.55	11.80	45.60
0.35	2.69	2.93	3.25	3.53	3.92	4.05	5.21	6.62	10.19	45.60
0.40	2.45	2.67	2.93	3.19	3.43	3.99	4.25	5.86	8.60	45.60
0.45	2.33	**2.45**	2.61	2.90	3.13	3.63	4.01	5.09	7.48	45.60
0.50	**2.10**	2.33	2.50	2.63	2.81	3.33	3.83	4.23	6.73	45.60
0.55	***2.01***	**2.14**	**2.33**	2.46	2.70	3.03	3.61	4.12	6.22	45.60
0.60	**2.31**	**2.08**	**2.09**	2.40	2.60	2.67	3.29	3.85	5.39	45.60
0.65	**2.34**	**2.25**	**2.07**	2.14	2.49	2.75	3.02	3.72	5.17	45.60
0.70	**2.59**	**2.41**	**2.14**	2.16	2.23	2.62	2.66	3.67	4.71	45.60
0.75	**2.70**	**2.57**	**2.31**	2.16	**2.14**	**2.44**	2.78	3.32	4.36	45.60
0.80	**2.88**	**2.71**	**2.58**	2.23	2.17	**2.18**	2.67	3.07	4.08	45.60
0.85	**2.92**	**2.79**	**2.76**	2.41	**2.13**	**2.16**	2.67	2.81	3.98	45.60
0.90	**2.92**	**2.99**	**2.75**	2.58	**2.21**	**2.20**	**2.45**	**2.62**	3.85	45.60
0.95	**2.95**	**2.85**	**2.89**	2.77	**2.45**	**2.17**	**2.18**	2.88	3.61	45.60

- As was expected, when h does not satisfy Eq. 8 ($h < 0.5$), the algorithm does not work. Actually, the EER results when $h = 0.5$ are very high and do not depend on the σ value, since the algorithm does not align at all.
- When a configuration of the parameters implies a high speed correction (h high and σ low) and a large number of zero values are included, it is shown that by including the interpolating phase, the EER results improve (Top-right values in bold in Table 1).
- On the other hand, when the configuration of the parameters involves a low speed correction (h low and σ high) and only a low number of zero values are introduced, the algorithm works better without interpolation (Bottom-left values in bold in Table 2).

Furthermore, the results of the zero-effort detection test have been also obtained by using the maximized score directly, according to Eq. 1. This is a dynamic-programming-like quantification in order to compare the metric to quantify the similarity between two sequences. In this approach, a high value of the score means a great similarity of the sequences (as opposed to the method proposed based on aligning, interpolating (or not) and calculating Euclidean distance). This difference is solved by modifying the sign in Eq. 7 in order to consider an authentic access to any attempt whose δ_V/μ_T value is over the threshold θ. The EER results for each configuration of h and σ are presented in Table 3.

It is remarkable that the lowest EER obtained according to the score approach is 3.14% significantly higher (1.13% higher) than aligning, interpolating (or not) and quantifying by the Euclidean distance.

In summary, an optimal Equal Error Rate of 2.01% has been obtained by evaluating the different values of h, σ and interpolating or not, for 100 users in a zero-effort attack scenario. This result is very competitive, improving the EER results in [30], where an EER of 5% was obtained from 22 testers grasping and shaking their phone, and also better than in [26], where the EER of 8% (4% if updating) was achieved from 12 users making a star shape.

6.2 Active impostor detection test

Following the scope of the biometric technique proposed and its applications, it might be possible for users to make their identifying 3-D hand gesture in places where there are other people who may see them. According to this, the biometric technique should be robust enough to assure that even though someone else may look at the making of the gesture, he/she is not able to reproduce it accurately.

In trying to illustrate this scenario, this test studies the strength of the biometric technique proposed when other people study the making of the 3-D hand gestures recorded on video. To accomplish this task, forgeries in GB2SgestureDB1 have been analyzed.

From this database of gestures, the Equal Error Rate has been obtained as in previous test, with the only difference being that the False Acceptance Rate is calculated with real

Table 3 EER (%) zero-effort detection test results using the score obtained when aligning according to Eq. 1 with different configurations of h, σ

σ	h									
	0.05	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45	0.50
0.05	5.16	5.23	5.30	5.45	5.86	6.06	6.34	6.93	7.92	50.00
0.10	3.90	4.08	4.23	4.21	4.26	4.54	4.78	5.28	6.18	50.00
0.15	3.41	3.53	3.53	3.67	3.96	4.13	4.27	4.56	5.31	50.00
0.20	3.22	3.16	3.26	3.52	3.56	3.59	4.05	4.16	4.78	50.00
0.25	3.23	3.22	3.18	3.20	3.33	3.53	3.59	4.12	4.40	50.00
0.30	3.21	3.20	***3.14***	3.26	3.22	3.26	3.53	3.70	4.21	50.00
0.35	3.26	3.23	3.20	3.20	3.24	3.25	3.35	3.54	4.17	50.00
0.40	3.38	3.31	3.27	3.21	3.22	3.30	3.24	3.46	3.87	50.00
0.45	3.54	3.42	3.36	3.29	3.24	3.25	3.27	3.35	3.71	50.00
0.50	3.41	3.53	3.53	3.67	3.96	4.13	4.27	4.56	5.31	50.00
0.55	3.76	3.67	3.60	3.46	3.40	3.29	3.24	3.23	3.51	50.00
0.60	4.03	3.80	3.67	3.58	3.43	3.36	3.27	3.24	3.40	50.00
0.65	4.08	3.98	3.79	3.64	3.52	3.42	3.30	3.26	3.32	50.00
0.70	4.26	4.08	3.90	3.67	3.53	3.41	3.41	3.25	3.25	50.00
0.75	4.35	4.21	4.04	3.81	3.68	3.49	3.35	3.28	3.22	50.00
0.80	4.48	4.35	4.06	3.94	3.69	3.56	3.41	3.29	3.26	50.00
0.85	4.73	4.48	4.35	4.03	3.82	3.67	3.45	3.30	3.20	50.00
0.90	4.89	4.53	4.35	4.12	3.94	3.65	3.53	3.32	3.27	50.00
0.95	5.05	4.87	4.49	4.31	4.00	3.76	3.58	3.36	3.28	50.00

attempts of forging instead of with the original signature of someone else. Therefore, the FRR is obtained from 500 samples (100 users, 5 accessing trials), whereas the FAR is calculated from 2100 samples (100 original signatures, 3 impostors, 7 samples).

This test has been carried out with different configurations of the parameters h and σ of the algorithm, originating the EER results presented in Tables 4 and 5, when the interpolating phase was included or not, respectively. As well as in the previous Section, the lowest EER value of each configuration between both tables is presented in bold, representing the best performance between interpolating or not. In addition to this, the lowest value of each table is also highlighted in bold italics.

Therefore, an optimal Equal Error Rate of 4.82% has been obtained (zoom in Fig. 5) within the analysis of gestures in GB2SGestureDB1 database and the configuration of the algorithm of $h = 0.45, \sigma = 0.8$ and including the interpolating phase (highlighted in Table 4). On the other hand, when no interpolation is carried out, the optimal EER result is 4.87%, which corresponds to $h = 0.10, \sigma = 0.6$ (highlighted in Table 5).

By analyzing the results in Tables 4 and 5, the same expected behaviors as in the previous test are found: When $h = 0.5$, the algorithm does not work, and depending on the rhythm of introducing zero values, interpolation improves or worsens the performance, as explained in Sect. 4.

These EER results are higher than in the previous test because in this Section, False Acceptance Rate has been calculated through real falsification attempts.

Besides, the active impostor detection test has also been made by using the score when aligning two sequences according to Eq. 1 as the metric to quantify the similarity between the sequences in comparison. The resulting EER for each configuration of h and σ is presented in Table 6.

It is noticeable that following the score approach, as well as in the previous test, the lowest EER found is 7.63%, significantly higher than when applying alignment, interpolation (or not) and quantification of the differences with Euclidean distance.

In summary, an optimal Equal Error Rate of 4.82% has been achieved by analyzing a database of 100 users including real falsification trials.

This error rate is competitive with the results obtained in [21], where a lowest EER of 10% was obtained with a database of 10 gestures obtained with falsifications when the attacker knows the gesture but does not see the authentic user performing their gesture, and an estimated EER of 3% when the movement is able to be studied. Furthermore, these results are also competitive with [9], where an initial work was carried out with 34 users obtaining a 2.5% of EER. It is remarkable that the results presented in this article are obtained from a database of gestures of 100 users, ten times higher than in [21] and three times than in [9], evaluating the

Table 4 EER (%) of active impostor detection test results with different configurations of h, σ and applying the interpolating phase

σ	h									
	0.05	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45	0.50
0.05	**14.38**	**15.08**	**14.32**	**15.60**	**15.62**	**17.98**	**18.95**	**20.47**	**22.30**	**46.21**
0.10	**7.54**	**8.87**	**7.67**	**9.09**	**9.98**	**11.95**	**13.53**	**14.63**	**19.07**	**46.21**
0.15	**6.06**	**7.76**	**7.27**	**7.66**	**7.10**	**7.83**	**10.60**	**11.75**	**17.07**	**46.21**
0.20	**6.00**	7.13	**5.73**	**6.65**	**7.10**	**7.09**	**6.95**	**8.29**	**13.08**	**46.21**
0.25	6.21	7.45	**5.99**	**6.56**	**5.76**	**6.77**	**7.07**	**7.10**	**10.64**	**46.21**
0.30	6.21	6.43	**6.07**	**5.99**	**5.99**	**6.02**	**6.29**	**6.98**	**8.73**	**46.21**
0.35	5.76	6.23	**5.99**	**6.21**	**5.90**	**5.78**	**5.58**	**7.10**	**7.76**	**46.21**
0.40	6.29	6.23	**5.78**	**5.70**	**6.28**	**5.66**	**5.54**	**5.76**	**7.30**	**46.21**
0.45	6.35	6.06	6.28	6.21	6.21	**6.02**	**6.14**	**5.85**	**7.10**	**46.21**
0.50	5.99	6.24	6.21	5.99	**5.99**	**5.84**	**5.82**	**6.04**	**6.65**	**46.21**
0.55	5.99	6.46	6.43	5.54	6.00	6.18	**6.21**	**5.88**	**5.76**	**46.21**
0.60	6.84	6.18	6.32	**5.40**	6.12	5.76	**5.58**	**5.76**	**5.76**	**46.21**
0.65	6.89	6.43	6.21	5.70	6.00	5.76	**6.04**	**6.09**	**5.99**	**46.21**
0.70	7.21	6.65	6.37	5.70	6.41	5.99	6.06	**5.99**	**5.76**	**46.21**
0.75	7.72	6.87	6.73	5.34	6.19	5.82	5.99	**6.18**	**5.46**	**46.21**
0.80	7.84	7.54	6.87	5.52	6.18	5.94	5.88	6.32	***4.82***	**46.21**
0.85	7.60	7.66	7.76	5.82	6.21	6.35	5.99	6.00	**4.92**	**46.21**
0.90	8.19	7.54	7.76	6.18	6.53	6.12	6.06	6.12	**5.10**	**46.21**
0.95	7.76	7.78	7.76	**6.87**	6.59	6.24	5.95	6.21	**5.10**	**46.21**

Table 5 EER (%) of active impostor detection test results with different configurations of h, σ and without applying the interpolating phase

σ	h									
	0.05	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45	0.50
0.05	16.60	18.17	18.86	20.45	21.30	23.26	23.86	26.95	27.82	47.60
0.10	9.98	11.75	12.16	13.77	14.88	16.50	17.81	20.07	23.41	47.60
0.15	7.32	8.51	9.88	10.05	11.44	12.41	14.85	16.04	19.84	47.60
0.20	6.81	**7.05**	7.83	8.43	9.20	10.05	11.97	13.60	16.32	47.60
0.25	**6.18**	**6.87**	6.65	7.37	8.34	8.01	10.28	11.64	14.84	47.60
0.30	**6.18**	**5.99**	6.65	6.65	6.65	8.23	8.46	10.20	13.21	47.60
0.35	**5.60**	**5.92**	6.11	6.77	6.87	6.92	8.24	9.24	12.29	47.60
0.40	**5.32**	**5.84**	5.95	6.02	6.94	7.08	6.68	8.43	11.12	47.60
0.45	**5.32**	**5.39**	**5.76**	**5.84**	**5.93**	6.86	6.76	7.69	10.20	47.60
0.50	**5.25**	**5.49**	**5.48**	**5.95**	6.11	6.41	6.92	6.72	9.09	47.60
0.55	**5.00**	**5.23**	**5.50**	**5.41**	**5.66**	**6.06**	6.79	7.00	8.65	47.60
0.60	**5.32**	***4.87***	**5.33**	5.54	**5.53**	**5.76**	6.45	6.65	8.27	47.60
0.65	**5.40**	**5.15**	**4.98**	**5.20**	**5.41**	**5.57**	6.09	6.84	7.76	47.60
0.70	**6.07**	**5.34**	**5.10**	**5.29**	**5.33**	**5.54**	**5.76**	6.91	7.64	47.60
0.75	**6.52**	**5.87**	**5.34**	**5.03**	**5.14**	**5.32**	**5.68**	6.43	7.18	47.60
0.80	**6.79**	**6.43**	**5.96**	**5.11**	**5.20**	**5.21**	**5.71**	**6.11**	6.91	47.60
0.85	**6.87**	**6.69**	**6.83**	**5.62**	**5.10**	**5.11**	**5.43**	**5.99**	6.79	47.60
0.90	**6.89**	**6.77**	**6.43**	**6.11**	**5.32**	**5.25**	**5.34**	**5.65**	6.54	47.60
0.95	**7.38**	**6.77**	**6.70**	6.90	**5.72**	**5.26**	**5.34**	**5.52**	6.84	47.60

possible feasibility of developing this biometric technique in the real world where a huge amount of different identifying gestures could be made.

Moreover, these results are also close to online handwritten signature technique error rates. The best results of online signature analysis in some of the most important works on

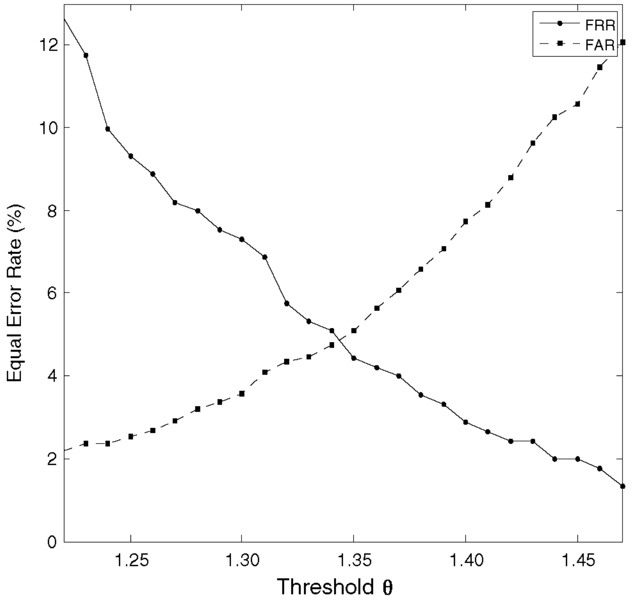

Fig. 5 Resulting EER (%) of active impostor test

this subject are EER of 3.6% [28], FAR of 1.6% and FRR of 2.8% [16] and EER of 2.84% [40].

As this test is carried out with real falsification trials, the threshold where the EER is achieved provides a significant information as to which value should be chosen at the point to accept or reject in a real application. In this test, the threshold value where the EER was reached is 1.35, so when accessing the system, any value of δ_V / μ_T lower than 1.35 will be accepted whereas any higher will be rejected.

Joining the results of zero-effort and active impostor tests, it is concluded that the optimal configurations for the parameters of the algorithm when including the interpolation phase are $h = 0.45$ and $\sigma = 0.85$ or $\sigma = 0.88$. Table 7 provides the average results of the EER of the two forgeries tests when applying interpolation. The average EER obtained in the optimal configuration is 3.47%.

Moreover, Table 8 presents the average of the zero-effort and active impostor tests when not applying interpolation. The lowest EER in this table is 3.48%, reached with the configuration of $\sigma = 0.55$ and $h = 0.05$.

Therefore, when including interpolation, a slight improvement in the EER is obtained. However, the approach presented in this article based on aligning, interpolating (or not) and Euclidean distance provides a significantly better performance than obtaining the score directly from Eq. 1.

6.3 Permanence evaluation

This test aims to study whether a user is able to repeat his/her gesture over time accurately. The results of this test have been obtained from GB2SGestureDB2, where 25 volunteers have had 10 sessions of 5 repetitions of their identifying gesture. These sessions have been spread over a month, without any

Table 6 EER (%) of active impostor detection test results using the score obtained when aligning according to Eq. 1 with different configurations of h, σ

σ	h									
	0.05	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45	0.50
0.05	12.47	12.86	12.98	13.27	13.61	14.19	14.80	15.80	17.43	49.8
0.10	10.26	10.07	10.10	10.54	10.89	11.42	12.16	12.90	14.36	49.8
0.15	9.20	9.29	9.31	9.46	9.73	10.04	10.75	11.18	13.08	49.8
0.20	8.03	8.15	8.43	8.76	9.09	9.32	9.71	10.41	11.63	49.8
0.25	7.76	7.98	7.94	8.08	8.51	8.88	9.07	9.72	10.76	49.8
0.30	7.98	7.76	7.90	7.89	8.00	8.41	8.84	9.27	10.29	49.8
0.35	8.20	8.10	7.78	7.81	7.78	7.97	8.50	8.89	9.92	49.8
0.40	8.58	8.24	8.11	7.82	7.70	7.90	7.95	8.71	9.59	49.8
0.45	9.34	8.66	8.20	8.22	7.86	***7.63***	7.81	8.35	9.28	49.8
0.50	9.60	9.31	8.56	8.20	8.21	7.90	7.81	8.07	8.90	49.8
0.55	9.75	9.68	9.13	8.52	8.25	8.00	7.77	7.66	8.78	49.8
0.60	10.27	9.76	9.79	9.09	8.46	8.22	7.84	7.74	8.82	49.8
0.65	10.63	10.13	10.00	9.72	8.99	8.33	8.13	7.70	8.41	49.8
0.70	11.10	10.62	10.14	9.91	9.50	8.62	8.31	7.77	7.99	49.8
0.75	11.29	11.01	10.76	10.12	9.84	9.02	8.23	7.97	7.87	49.8
0.80	11.46	11.19	10.97	10.55	10.07	9.53	8.55	8.06	8.00	49.8
0.85	12.17	11.37	11.07	10.86	10.26	9.91	8.89	8.07	7.90	49.8
0.90	12.95	11.86	11.25	10.92	10.87	10.10	9.15	8.11	7.84	49.8
0.95	13.27	12.66	11.57	10.99	10.92	10.29	9.57	8.26	7.80	49.8

Table 7 Average of EER (%) results in the zero-effort impostor detection test and the active impostor detection test results with different configurations of h, σ and applying the interpolating phase

σ	h									
	0.05	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45	0.50
0.05	**11.53**	**12.36**	**12.64**	**13.10**	**13.41**	**14.75**	**19.33**	**21.53**	**23.29**	**45.23**
0.10	**5.36**	**6.61**	**6.32**	**7.28**	**8.17**	**10.73**	**12.40**	**14.45**	**19.21**	**45.23**
0.15	**4.16**	**5.40**	**5.29**	**5.44**	**5.32**	**6.57**	**8.93**	**10.46**	**16.17**	**45.23**
0.20	**4.04**	**4.85**	**4.11**	**4.70**	**5.00**	**5.26**	**5.57**	**7.23**	**11.69**	**45.23**
0.25	**4.13**	**4.95**	**4.20**	**4.52**	**4.15**	**4.85**	**5.22**	**5.64**	**9.02**	**45.23**
0.30	**4.21**	**4.37**	**4.22**	**4.09**	**4.08**	**4.31**	**4.69**	**5.23**	**7.29**	**45.23**
0.35	**4.00**	**4.22**	**4.18**	**4.19**	**4.04**	**3.99**	**4.15**	**5.24**	**6.36**	**45.23**
0.40	4.30	4.31	**4.00**	**3.95**	**4.21**	**4.02**	**3.91**	**4.26**	**5.89**	**45.23**
0.45	4.26	4.25	4.42	**4.21**	**4.16**	**4.18**	**4.25**	**4.21**	**5.41**	**45.23**
0.50	4.08	4.27	4.23	**4.16**	**4.15**	**4.02**	**4.07**	**4.23**	**4.88**	**45.23**
0.55	4.14	4.39	4.41	**3.82**	**4.15**	**4.29**	**4.29**	**4.13**	**4.44**	**45.23**
0.60	4.63	4.21	4.36	**3.80**	4. 16	**4.09**	**4.02**	**4.09**	**4.22**	**45.23**
0.65	4.74	4.43	4.31	3.87	4.08	4.25	**4.31**	**4.27**	**4.19**	**45.23**
0.70	5.03	4.61	4.45	3.87	4.32	4.27	4.35	**4.18**	**4.07**	**45.23**
0.75	5.35	4.80	4.73	3.73	4.23	4.21	4.24	**4.28**	**3.84**	**45.23**
0.80	5.43	5.27	4.97	3.85	4.15	4.11	4.22	**4.44**	*3.47*	**45.23**
0.85	5.43	5.33	5.53	4.10	4.19	4.39	4.18	**4.28**	*3.47*	**45.23**
0.90	5.67	5.35	5.59	4.38	4.50	4.25	4.29	4.43	**3.58**	**45.23**
0.95	5.49	5.45	5.63	**4.77**	4.56	4.31	4.16	4.48	**3.65**	**45.23**

Table 8 Average of EER (%) results in the zero-effort impostor detection test and the active impostor detection test results with different configurations of h, σ and without applying the interpolating phase

σ	h									
	0.05	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45	0.50
0.05	15.95	17.49	17.95	19.70	20.37	22.39	22.75	25.71	26.33	46.60
0.10	9.10	10.58	11.56	12.98	14.15	15.66	17.24	19.42	22.45	46.60
0.15	6.10	7.30	8.40	8.88	10.35	11.49	13.91	15.37	19.26	46.60
0.20	5.36	5.68	6.46	7.19	7.96	8.87	10.59	12.79	15.71	46.60
0.25	4.73	5.28	5.32	5.86	6.83	7.09	8.95	10.51	14.07	46.60
0.30	4.58	4.59	5.12	5.27	5.36	6.78	7.33	8.88	12.50	46.60
0.35	4.15	4.42	4.68	5.15	5.40	5.49	6.72	7.93	11.24	46.60
0.40	**3.88**	**4.26**	4.44	4.60	5.18	5.54	5.47	7.14	9.86	46.60
0.45	**3.83**	**3.92**	**4.19**	4.37	4.53	5.24	5.38	6.39	8.84	46.60
0.50	**3.67**	**3.91**	**3.99**	4.29	4.46	4.87	5.38	5.48	7.91	46.60
0.55	**3.51**	**3.69**	**3.91**	3.94	4.18	4.54	5.20	5.56	7.43	46.60
0.60	**3.81**	*3.48*	**3.71**	3.97	**4.06**	4.22	4.87	5.25	6.83	46.60
0.65	**3.87**	**3.70**	**3.52**	**3.67**	**3.95**	**4.16**	4.55	5.28	6.46	46.60
0.70	**4.33**	**3.87**	**3.62**	**3.73**	**3.78**	**4.08**	**4.21**	5.29	6.18	46.60
0.75	**4.61**	**4.22**	**3.82**	**3.59**	**3.64**	**3.88**	**4.23**	4.87	5.77	46.60
0.80	**4.84**	**4.57**	**4.27**	**3.67**	**3.69**	**3.70**	**4.19**	4.59	5.50	46.60
0.85	**4.90**	**4.74**	**4.79**	**4.01**	**3.62**	**3.63**	**4.05**	4.40	5.39	46.60
0.90	**4.90**	**4.88**	**4.59**	**4.34**	**3.77**	**3.73**	**3.90**	**4.13**	5.19	46.60
0.95	**5.17**	**4.81**	**4.80**	4.83	**4.08**	**3.71**	**3.76**	**4.20**	5.22	46.60

additional help except what they remembered. Each session of each user has been separated by a minimum of 1 day and a maximum of 5.

For this test, the first session of each user has been considered as the enrollment phase, so the template of the gesture corresponding to each person is made up of three of the samples of this first session. The value μ_T for each identifying 3-D gesture has been obtained from these samples of the template, as it was described in Sect. 3.1. The rest of samples of the first session were discarded.

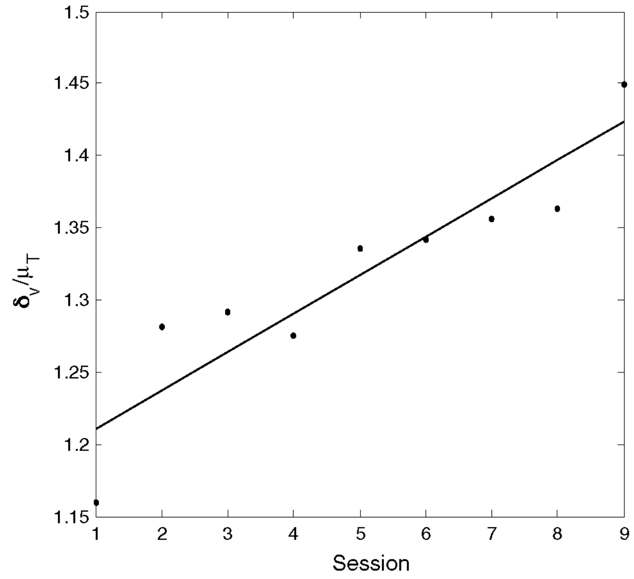

Fig. 6 Evolution of identifying 3-D hand gestures repetition along the time

Each sample of the following 9 sessions has been considered as the accessing trials of the original user. For each sample, δ_V is calculated as in Sect. 3.2, measuring the difference between each sample and the template. In this analysis, the parameters of the algorithm are set to the optimal values obtained in Sects. 6.1 and 6.2, so $h = 0.45$ and $\sigma = 0.85$.

Finally, the average of δ_V/μ_T is calculated for all the samples of each session and each user, obtaining a value that the higher it is the more different the sample of the 3-D hand gesture of the session was respect to the template, and vice versa.

Figure 6 represents the average of δ_V/μ_T on each session of the experiment for all of the users in the database. In this figure, the trend of the ability of users of repeating over time their identifying 3-D hand gesture is symbolized by the linear regression of the values on each session [32].

From this behavior, it is inferred that users are not able to repeat their 3-D hand gesture accurately over time. Moreover, a particular behavior of the evolution of the ability to repeat their 3-D hand gesture can be deducted: Users need a period of time to get used to their performance of their hand gestures and modify continuously but slightly the way they make their gesture from one session to the next.

Actually, on the first sessions, when the users have just made their 3-D hand gesture for the first times, the variability is high. After some sessions, when the users get used to the way they make their identifying hand gesture, it is much easier for them to repeat it.

This behavior is represented in Fig. 7, where the relative average of access punctuations between sessions is presented. Each point in this figure symbolizes the difference between the average of δ_V/μ_T of one session and the previous one. It is remarkable that this trend is stable and slightly negative.

In conclusion, although the repetition of the hand gesture in different sessions over time is not fully precise, the variance of the performance of the identifying 3-D hand gestures varies slightly between sessions. This characteristic opens up a new research line in this field in order to study different template updating strategies that minimize the variation of the user performance over time.

An evaluation of the permanence evaluation results in comparison with the previous two tests is introduced in the next subsection.

6.4 Analysis of results

The goal of this subsection is to compare the results of the two previous tests to verify that the hand gesture is easily repeatable by the user (Permanence evaluation) and, at the same time, forgeable with difficulty by the other users (active impostor detection test). The compromise of these two parameters is a crucial point regarding this technique.

In active impostor detection test, the final threshold θ was set to 1.35 (zoomed in Fig. 5) since it was where the EER was achieved representing the point of minimal global error of impostor accessing and authentic rejecting samples in the system. The resulting figure of the permanence test (Fig. 6) shows the evolution on average of the repetition of the identifying a 3-D hand gesture over time. From this figure, it is shown that in spite of the passage of time, users, on average, still repeat their identifying hand gesture below 1.35, although very close to it. Consequently, users over short time are able to repeat their original 3-D hand gestures with greater accuracy than impostors do.

The resulting trend of the permanence test implies that in long terms, the variation of the performance of the 3-D hand gestures will get higher and above 1.35, so it is essential a continuous updating of the template that lets the system work only in short-term conditions. A valid updating strategy would be at each granted access to the system, change the oldest sample of the template by the accessing sample.

Furthermore, by examining Fig. 7, it is deducted that after some sessions, users make their identifying 3-D hand gesture in a much more similar way over time and with insignificant higher punctuation in comparison with the value of the threshold. As a consequence, introducing an enrollment process where users make their three repetitions of the 3-D hand gestures over several days would improve permanence results and the feasibility of the technique, as well as implementing an updating method to adapt the template of users to the manner in which they modify the performance of their gestures.

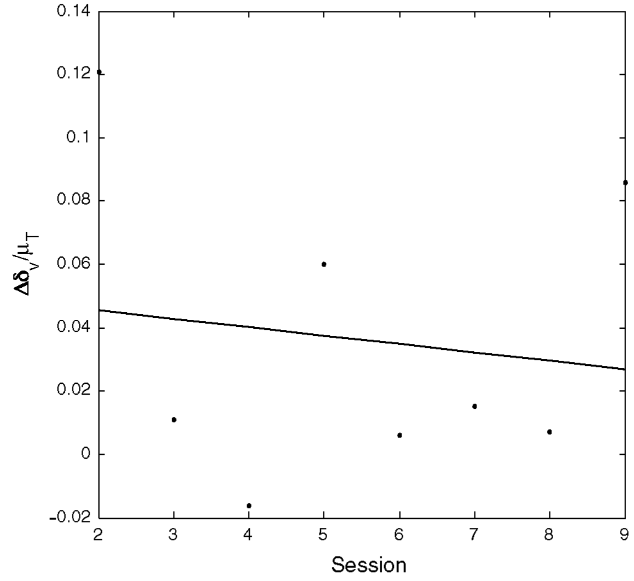

Fig. 7 Evolution of identifying 3-D hand gesture repetition in respect to the previous session

Table 9 Time analysis results

Time (ms)	1 preprocessing algorithm	Enrollment	Verification
Mac	0.26	2.45	2.46
iPhone	107	992	987

6.5 Time analysis

The algorithm of this technique has been carried out on two devices: Firstly, the algorithm has been developed and evaluated on a Mac Computer at 2.4 GHz Intel Core 2 Duo with 1 GB RAM. Finally, the algorithm has been integrated on an Iphone 3G and tested with real people enrolling and accessing the system. Time results for one implementation of the preprocessing algorithm, one enrollment phase and one verification phase for each device are shown in Table 9. All these values have been obtained as the average of 1000 operations.

It is notable that an operation of enrollment or verification needs less than a second on a mobile, which is a very reasonable amount of time for a user who needs authentication on his/her mobile.

All the experiments included in this article have been developed with a sampling rate of 50 Hz, although initially 3-D hand gestures in databases were extracted at 100 Hz. The results when analyzing signals at 100 Hz were not significantly better than those presented in this article; however, the consumption time was multiplied by 3.

7 Conclusion and future work

In this article, a novel biometric technique based on hand gesture recognition has been proposed. To accomplish this aim, a user is identified by a 3-D gesture he/she makes moving one of his/her hands holding an accelerometer-embedded mobile device. A user is enrolled in the system by repeating his/her identifying 3-D hand gesture three time, and he/she is able to enter the system by doing it again.

By correcting slightly the differences in accelerations when a user repeats his/her hand gesture over time is the main point in this article. This task has been solved by developing a signal preprocessing algorithm, based on sequence alignment, able to find the best alignment between two samples.

Universality, collectively, acceptability, uniqueness, circumvention and permanence of the biometric technique proposed have been evaluated in this paper with three different tests.

For this task, two different databases of 3-D hand gestures have been analyzed: GB2SDatabaseDB1, made up of 100 genuine identifying 3-D hand gestures and 3 impostors trying to falsify each of them by studying video records, and GB2SDatabaseDB2 where 25 volunteers have participated repeating their identifying 3-D hand gesture in 10 sessions over a month.

From the analysis of GB2SDatabaseDB1, two attacks have been simulated obtaining different optimal values of EER: 2.01 and 4.82% in a zero-effort and active impostor test. From the results of these experiments, an optimal configuration of the algorithm proposed to analyze the signals has been determined, as well as the threshold to access the system. These results are obtained in a fixed-parameter approach, where h and σ are parameters of the algorithm, the same values for all the users. The generality of the optimal configuration of the algorithm should be evaluated in future works to determine to what extent h and σ are optimal for each signature or for different sets of signature enrollment samples. In spite of this, the optimal value of EER in this article represents how efficient signatures in the air can be separable through this fixed-parameter approach (between them and in respect to falsification attempts).

In addition to this, a different approach will be also studied in the future, where h and σ will depend on the user signature. In this case, for each user signature, the h and σ values will be obtained at enrollment and will belong to the template of the user template. This future approach will include different training techniques in order to find the most appropriate h and σ values for each user signature. The future work objective based on user-dependent parameters should try to improve the optimal EER value obtained in this article, where the optimal h and σ values are fixed for all the signatures.

Besides, two more conclusions have been derived as a consequence of these tests:

- An approach based on aligning the acceleration signals, interpolating them (or not) and calculating the Euclidean distance provides a significantly better performance in terms of EER than quantifying the difference of the signals by the value of the score of the global alignment process.

- The interpolating phase introduces slight improvement than no interpolating, since a lower optimal EER has been obtained. However, it has been demonstrated that the interpolation phase is significantly useful when the alignment speed is high so a lot of zero values are included to align the signals (configurations of high h and low σ). On the other hand, it has also been proved that it is significantly better not to include the interpolation phase when the alignment speed is low (configurations of low h and high σ).

Finally, from the study of the hand gestures in the database GB2SDatabaseDB2, it can be concluded that users vary their performance of the 3-D hand gesture over time slightly after a period of getting accustomed to it, so in the short term, an original user is able to repeat his/her hand gesture more accurately than an impostor. However, an optimal updating phase of the templates should be investigated to correct the deviation in the long term, in addition to a process to habituate users to their gestures at the enrollment phase.

Bellman, R.: Dynamic Programming. Dover Publications, New York

Chin, Y.J., Ong, T.S., Goh, M.K., Hiew, B.Y.: Integrating palmprint and fingerprint for identity verification. In: International Conference on Network and System Security, pp. 437–442 (2009)

Cho, D., Park, K.R., Rhee, D.W., Kim, Y., Yang, J.: Pupil and iris localization for iris recognition in mobile phones. In: International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, and International Workshop on Self-Assembling Wireless Networks, pp. 197–201 (2006)

Chowhan, S., Shinde, G.N.: Iris biometrics recognition application in security management. Congr. Image Signal Process. **1**, 661–665 (2008)

Clarke, N.L., Furnell, S.M.: Authenticating mobile phone users using keystroke analysis. Int. J. Inf. Secur. **6**(1), 1–14 (2006)

Durbin, R., Eddy, S., Krogh, A., Mitchison, G.: Biological Sequence Analysis, 11th edn. Cambridge University Press, Cambridge (2006)

Friederike, A.J., Jain, A.K., Griess, F.D., Connell, S.D., Lansing, E.J.M.: On-line signature verification. Pattern Recognit. **35**, 2963–2972 (2002)

Gafurov, D., Snekkkenes, E.: Arm swing as a weak biometric for unobtrusive user authentication. In: International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1080–1087 (2008)

Guerra-Casanova, J., Sánchez-Ávila, C., Santos-Sierra, A., Bailador, G., Jara-Vera, V.: A real-time in-air signature biometric technique using a mobile device embedding an accelerometer. In: Zavoral, F.,Yaghob, J., Pichappan, P., El-Qawasmeh, E. (eds) Networked Digital Technologies, Communications in Computer and Information Science, vol. 87, pp. 497–503. Springer, Berlin (2010)

Guo, J., Doermann, D., Rosenfeld, A.: Local correspondence for detecting random forgeries. In: International Conference on Document Analysis and Recognition, p. 319 (1997)

He, Z., Jin, L., Zhen, L., Huang, J.: Gesture recognition based on 3d accelerometer for cell phones interaction. In: IEEE Asia Pacific Conference on Circuits and Systems, 2008. APCCAS 2008, pp. 217–220 (2008)

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

Iso, T., Yamazaki, K.: Gait analyzer based on a cell phone with a single three-axis accelerometer. In: MobileHCI '06: Proceedings of the 8th Conference on Human-Computer Interaction with Mobile Devices and Services, pp. 141–144. ACM, New York, NY (2006)

Jain, A., Hong, L., Pankanti, S.: Biometric identification. Commun. ACM **43**(2), 90–98 (2000)

Jain, A.K., Flynn, P., Ross, A.A.: Handbook of Biometrics. Springer, Secaucus, NJ (2007)

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

Kanhangad, V., Kumar, A., Zhang, D.: Combining 2d and 3d hand geometry features for biometric verification. In: Computer Vision and Pattern Recognition Workshop, pp. 39–44 (2009)

Keir, P., Payne, J., Elgoyhen, J., Horner, M., Naef, M., Anderson, P.: Gesture-recognition with non-referenced tracking. In: IEEE Symposium on 3D User Interfaces, 2006. 3DUI 2006, pp. 151–158 (2006)

Kela, J., KorpipŠŠ, P., MŠntyjŠrvi, J., Kallio, S., Savino, G., Jozzo, L., Marca, S.: Accelerometer-based gesture control for a design environment. Pers. Ubiquitous Comput. **10**, 285–299 (2006)

Little, J., Boyd, J.E.: Recognizing people by their gait: the shape of motion. Videre. **1**, 1–32 (1996)

Liu, J., Wang, Z., Zhong, L., Wickramasuriya, J., Vasudevan, V.: uWave: accelerometer-based personalized gesture recognition and its applications. In: IEEE International Conference on Pervasive Computing and Communications, pp. 1–9 (2009)

Manabe, H., Yamakawa, Y., Sasamoto, T., Sasaki, R.: Security evaluation of biometrics authentications for cellular phones. In: International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 34–39 (2009)

Mäntyjärvi, J., Kela, J., Korpipää, P., Kallio, S.: Enabling fast and effortless customisation in accelerometer based gesture interaction. In: MUM '04: Proceedings of the 3rd International Conference on Mobile and Ubiquitous Multimedia, pp. 25–31. ACM, New York, NY (2004)

Mäntyjärvi, J., Kela, J., Korpipää, P., Kallio, S.: Enabling fast and effortless customisation in accelerometer based gesture interaction. In: Proceedings of the 3rd International Conference on Mobile and Ubiquitous Multimedia, MUM '04, pp. 25–31. ACM, New York, NY (2004)

Mantyla, V.M., Mantyjarvi, J., Seppanen, T., Tuulari, E.: Hand gesture recognition of a mobile device user. In: 2000 IEEE International Conference on Multimedia and Expo, 2000. ICME 2000, vol. 1, pp. 281 –284 (2000)

Matsuo, K., Okumura, F., Hashimoto, M., Sakazawa, S., Hatori, Y.: Arm swing identification method with template update for long term stability (2007). Lecture Notes in Computer Science; SP: 211

Miller, W.: An introduction to bioinformatics algorithms Neil C. Jones and Pavel A. Pevzner. J. Am. Stat. Assoc. **101**, 855–855 (2006)

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

Nandini, C., RaviKumar, C.N.: Multi-biometrics approach for facial recognition. In: International Conference on Computational Intelligence and Multimedia Applications, vol. 2, pp. 417–422 (2007)

Okumura, F., Kubota, A., Hatori, Y., Matsuo, K., Hashimoto, M., Koike, A.: A study on biometric authentication based on arm sweep action with acceleration sensor. In: International Symposium on Intelligent Signal Processing and Communications, 2006. ISPACS '06, pp. 219–222 (2006)

Phillips, P.J., Martin, A., Wilson, C.L., Przybocky, M.: An introduction to evaluating biometric systems. Computer **21**(2), 56–63 (2000)

Poh, N., Kittler, J., Smith, R., Tena, J.R.: A method for estimating authentication performance over time, with applications to face biometrics. In: CIARP'07: Proceedings of the Congress on Pattern Recognition 12th Iberoamerican Conference on Progress in Pattern Recognition, Image Analysis and Applications, pp. 360–369. Springer, Berlin (2007)

Rybnik, M., Tabedzki, M., Saeed, K.: A keystroke dynamics based system for user identification. International Conference on Computer Information Systems and Industrial Management Applications **0**, pp. 225–230 (2008)

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

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

Tadeusiewicz, R., Demenko, G.: Voice as a key. In: International Conference on Biometrics and Kansei Engineering, pp. 28–33 (2009)

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

Verplaetse, C.: Inertial proprioceptive devices: self-motion-sensing toys and tools. IBM Syst. J. **35**(3–4), 639–650 (1996)

Wayman, J.L., Jain, A.K., Maltoni, D., Maio, D.: Biometric Systems: Technology, Design and Performance Evaluation. Springer, New York (2004)

Yeung, D.Y., Chang, H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., Rigoll, G.: Biometric Authentication, chap. SVC2004: First International Signature Verification Competition, pp. 1–30. Springer, Berlin (2004.

Zhu, Y., Tan, T., Wang, Y.: Biometric personal identification based on handwriting. In: International Conference on Pattern Recognition, vol. 2, p. 2797 (2000)