BioTouchPass: Handwritten Passwords for Touchscreen Biometrics

Ruben Tolosana, Ruben Vera-Rodriguez, and Julian Fierrez, *Member, IEEE*

Abstract—This work enhances traditional authentication systems based on Personal Identification Numbers (PIN) and One-Time Passwords (OTP) through the incorporation of biometric information as a second level of user authentication. In our proposed approach, users draw each digit of the password on the touchscreen of the device instead of typing them as usual. A complete analysis of our proposed biometric system is carried out regarding the discriminative power of each handwritten digit and the robustness when increasing the length of the password and the number of enrolment samples. The new e-BioDigit database, which comprises on-line handwritten digits from 0 to 9, has been acquired using the finger as input on a mobile device. This database is used in the experiments reported in this work and it is available together with benchmark results in GitHub.[1] Finally, we discuss specific details for the deployment of our proposed approach on current PIN and OTP systems, achieving results with Equal Error Rates (EERs) ca. 4.0 percent when the attacker knows the password. These results encourage the deployment of our proposed approach in comparison to traditional PIN and OTP systems where the attack would have 100 percent success rate under the same impostor scenario.

Index Terms—Biometrics, passwords, handwriting, touch biometrics, mobile, deep learning, RNN, LSTM, DTW, e-BioDigit

1 Introduction

Mobile devices have become an indispensable tool for most people nowadays [1]. The rapid and continuous deployment of mobile devices around the world has been motivated not only by the high technological evolution and new features incorporated but also to the new internet infrastructures like 5G that allows the communication and use of social media in real time, among many other factors. In this way, both public and private sectors are aware of the importance of mobile devices for the society and are trying to deploy their services through user-friendly mobile applications ensuring data protection and high security.

Traditionally, the two most prevalent user authentication approaches have been Personal Identification Numbers (PIN) and One-Time Passwords (OTP). While PIN-based authentication systems require users to memorize their personal passwords, OTP-based systems avoid users to memorize them as the security system is in charge of selecting and providing to the user a different password each time is required, e.g., sending messages to personal mobile devices or special tokens. Despite the high popularity and deployment of PIN- and OTP-based authentication systems in real scenarios, many studies have highlighted the weaknesses of these approaches [2], [3]. First, it is common to use passwords based on sequential digits, personal information such as birth dates, or simply words such as "password" or "qwerty" that are very easy to guess. Second, passwords that are typed on mobile devices such as tablets or smartphones are susceptible to "smudge attacks", i.e., the deposition of finger grease traces on the touchscreen can be used for the impostors to guess the password [4]. Finally, password-based authentication is also vulnerable to "shoulder surfing". This type of attack is produced when the impostor can observe directly or use external recording devices to collect the user information. This attack has attracted the attention of many researchers in recent years due to the increased deployment of handheld recording devices and public surveillance infrastructures [5], [6]. Biometric recognition schemes are able to cope with these challenges by combining both a high level of security and convenience [7].

This study evaluates the advantages and potential of incorporating biometrics to password-based mobile authentication systems, asking the users to draw each digit of the password on the touchscreen instead of typing them as usual. This way, the traditional authentication systems are enhanced by incorporating dynamic handwritten biometric information. One example of use that motivates our proposed approach is on internet payments with credit cards. Banks usually send a numerical password (typically between 6 and 8 digits) to the user's mobile device. This numerical password must be inserted by the user in the security platform in order to complete the payment. Our proposed approach enhances such scenario by including a second authentication factor based on the user biometric information while drawing the digits. Fig. 1 shows a general architecture of our proposed password-based mobile authentication approach. The three following main modules are analyzed in this study: i) enrolment set, ii) password generation, and iii) touch biometric system. Depending on the final

1. https://github.com/BiDAlab/eBioDigitDB

• *The authors are with the Biometrics and Data Pattern Analytics - BiDA Lab, Escuela Politecnica Superior, Universidad Autonoma de Madrid, Madrid 28049, Spain. E-mail: {ruben.tolosana, ruben.vera, julian.fierrez}@uam.es.*

Manuscript received 17 Sept. 2018; revised 28 Mar. 2019; accepted 11 Apr. 2019. Date of publication 15 Apr. 2019; date of current version 3 June 2020. (Corresponding author: Ruben Tolosana.)
Digital Object Identifier no. 10.1109/TMC.2019.2911506

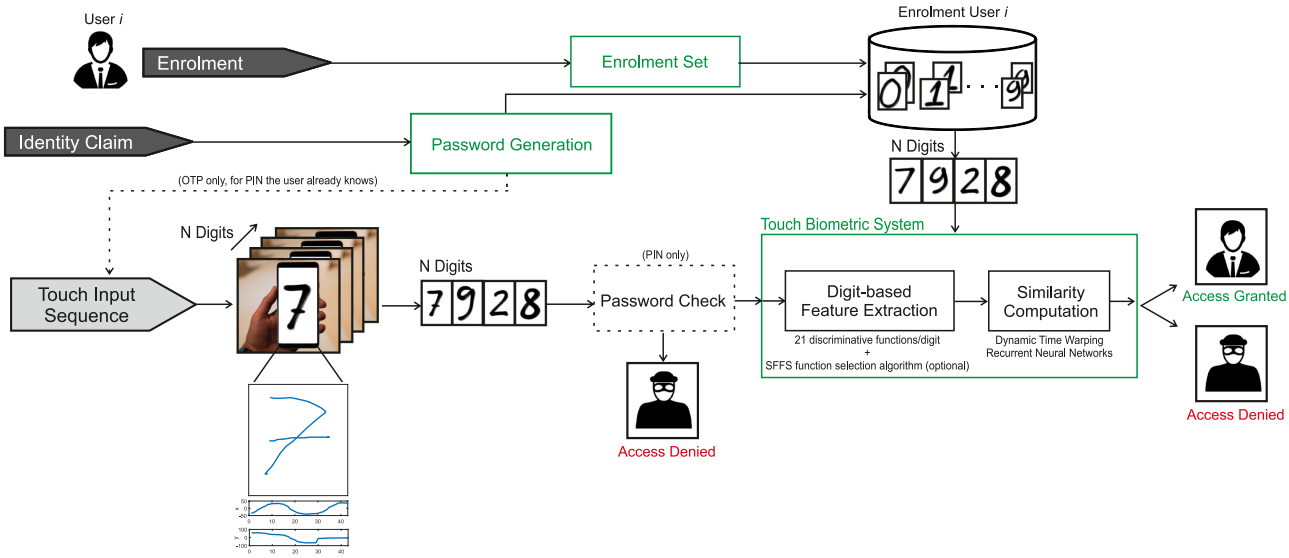


Fig. 1. Architecture of our proposed password-based mobile authentication approach including handwritten touch biometrics in a two-factor authentication scheme applicable both to user-generated PIN and OTP systems.

application (i.e., PIN or OTP), the handwritten digits can be first recognized using for example an Optical Character Recognition (OCR) system in order to verify the authenticity of the password. After this first authentication stage, the biometric information of the handwritten digits is compared in a second authentication stage to the enrolment data of the claimed user, comparing each digit one by one. In this study we focus on the second authentication stage based on the behavioral information of the user while performing the handwritten digits as the recognition of numerical digits has already shown to be an almost solved problem with errors close to 0 percent [8], [9]. Therefore, in this study we make the assumption that impostors pass the first stage of the security system (i.e., they know the password of the user to attack) and thus, the attack would have 100 percent success rate if our proposed approach was not present.

The main contributions of this study are related to our proposed architecture, the competitive results obtained with respect to related research, and our experimental findings:

- We survey and compare advantages and limitations of recent research on touch biometrics for mobile authentication.
- We incorporate biometrics to password-based mobile authentication. Two different state-of-the-art approaches are studied for the similarity computation: i) Dynamic Time Warping (DTW), which is widely used in many different fields such as handwriting and speech; and ii) Recurrent Neural Networks (RNNs), which are specific deep learning architectures considered for modelling sequential data with arbitrary length.
- We perform a complete analysis of the touch biometric system regarding the discriminative power of each handwritten digit. In addition, we analyze the robustness of our proposed approach when increasing the length of the handwritten password and the number of available enrolment samples per user.
- We discuss specific details for the deployment of our proposed approach on current PIN- and OTP-based authentication systems, including various strategies for password generation.
- We achieve better results than other verification schemes such as the handwritten signature and graphical passwords, as well as other recent works on touch biometrics.
- We introduce the new e-BioDigit database, which comprises on-line handwritten numerical digits from 0 to 9 for a total of 93 users, captured on a mobile device using finger touch interactions. Handwritten digits were acquired in two different sessions in order to capture the intra-user variability. This database is publicly available to the research community.

The remainder of the paper is organised as follows. Section 2 summarizes related works in touch biometrics for mobile scenarios. Section 3 describes our proposed touch biometric system. Section 4 describes the new e-BioDigit database, which comprises on-line handwritten numerical digits from 0 to 9. Sections 5 and 6 describe the experimental protocol and results achieved using our proposed approach, respectively. Section 7 discusses specific details for the deployment of our proposed approach on current PIN- and OTP-based authentication systems, including password generation strategies. Finally, Section 8 draws the final conclusions and points out some future work lines.

2 Related Works

2.1 Handwriting Biometrics and Beyond

Touch biometrics are becoming a very attractive way to verify users on mobile devices [18], [20]. Table 1 summarizes relevant approaches in this area. For each study, we include information related to the verification method, features, classifiers and datasets considered. We also report in Table 1 the verification performance for the two impostor scenarios commonly considered in this area: i) *imitation attack*, the case in which impostors have some level of information about the user being

TABLE 1
Comparison of Different Touch Biometric Approaches for Mobile Scenarios

Study	Method	Features	Classifiers	Verification Performance		# Participants (Dataset)
				Random Attack	Imitation Attack	
Angulo et al. (2011) [10]	Lock Pattern Dynamics	Timing-related Features	Random Forest	-	EER = 10.39%	32
Lacharme et al. (2016) [11]	Lock Pattern Dynamics	Dynamic Features	Hamming Distance	-	EER = 15.0%	34
Zezschwitz et al. (2016) [12]	Lock Pattern Dynamics	Shape Features	Greedy Clustering	-	-	506
Buschek et al. (2015) [13]	Keystroke	Font Adaptation Features	Manual	Acc = 94.8%	-	91
Buschek et al. (2015) [14]	Keystroke	Touch-specific Features	GM, kNN, LSAD	EER = 13.74%	-	28
Li et al. (2013) [15]	Touchscreen Gestures	Static Features	SVM	EER = 3.0%	-	75
Sae-Bae et al. (2014) [16]	Touchscreen Gestures	Distance between Points	DTW	EER = 1.58%	-	34
Shen et al. (2016) [17]	Touchscreen Gestures	Static Features	SVM, Random Forest, kNN, Neural Networks	EER $\sim$ 3.0%	-	71
Fierrez et al. (2018) [18]	Touchscreen Gestures	Static Features	SVM, GMM	EER = 10.7%	-	190
Sae-Bae et al. (2014) [19]	Handwritten Signatures	Histogram Static Features	Manhattan Distance	EER = 5.04%	-	180
Tolosana et al. (2017) [20]	Handwritten Signatures	Dynamic Features	DTW	EER = 0.5%	EER = 17.9%	65
Khan et al. (2011) [21]	Graphical Passwords	Predefined Symbols	Exact Match	-	-	100
Martinez-Diaz et al. (2016) [22]	Graphical Passwords	Dynamic Features	DTW, GMM	EER = 3.4%	EER = 22.1%	100
Kutzner et al. (2015) [23]	Handwritten Password	Static and Dynamic Features	Bayes-Nets, KStar, kNN	-	FAR = 10.42% FRR = unknown	32
Nguyen et al. (2017) [24]	Handwritten Digits	Dynamic Features	DTW	-	EER = 4.84%	20
Tolosana et al. (2018) [25]	Handwritten Digits	Dynamic Features	DTW	-	EER = 5.5%	93
Proposed Approach	**Handwritten Digits**	**Dynamic Features**	**DTW, RNNs**	**-**	**EER = 3.8%**	**93**

Acc = Accuracy.

attacked [26]; and *2) random attack*, the case in which no information about the user being attacked is known. Note that most algorithms and experimental conditions vary between the listed works, e.g., the amount and type of training and testing data. Therefore, Table 1 should be mainly interpreted in general terms to compare different scenarios of use based on touch biometrics, but not individual algorithms.

In [10], Angulo et al. evaluated the use of lock pattern dynamic systems for user authentication. Users were asked to draw three different lock patterns a certain number of times (50 trials for each pattern), with each pattern consisting of six dots. Authors considered a total of 11 timing-related features extracted from the finger-in-dot time (i.e., the time in milliseconds from the moment the participant finger touches a dot to the moment the finger is dragged outside the dot area), and the finger-in-between-dots time (i.e., representing the speed at which the finger moves from one dot to the next) achieving results above 10.0 percent EER for imitation attacks. In [11], Lacharme et al. incorporated biometric dynamic features related to the position of the finger, pressure, finger size and accelerometer sensor to the traditional Android unlock patterns, achieving a final 15.0 percent EER for imitation attacks using a matching algorithm based on Hamming Distance. Zezschwitz et al. presented in [12] a similarity metric for Android unlock patterns to quantify the effective password space of user-defined gestures. The proposed metric was evaluated using 506 user-defined patterns revealing very similar shapes that only differ by simple geometric transformations such as rotation. Consequently, they presented an approach to increase the pattern diversity in order to strengthen user lock patterns.

Other studies have focused on the potential of keystroke biometrics for user authentication on mobile scenarios.

In [13], Buschek et al. introduced qualitative aspects like personal expressiveness in order to enhance traditional keystroke biometric systems based on quantitative factors such as error rates and speed. They introduced a dynamic font personalisation framework, TapScript, which adapted a finger-drawn font according to user behavior and context, such as finger placement, device orientation, and position of the user while typing (i.e., walking or sitting) - resulting in a handwritten-looking font. Following their new approach, users were able to distinguish pairs of typists with 84.5 percent accuracy and walking/sitting scenarios with 94.8 percent. The same authors compared in [14] touch-specific features between three different hand postures (i.e., one-thumb, two-thumb and index finger typing) and evaluation schemes: Gaussian Model without covariance (GM), k-Nearest-Neighbours (kNN) and Least Squares Anomaly Detection (LSAD). Authors concluded that spatial touch features reduces the Equal Error Rates (EER) by 26.4 - 36.8 percent compared to the traditional temporal features.

Biometric verification systems based on touchscreen gestures (i.e., scrolling, zooming and clicking) while using mobile devices in scenarios such as document reading, web surfing or free tasks are gaining a lot of impact nowadays [15], [16], [17], [18]. These approaches enable active or continuous authentication schemes, in which the user is transparently authenticated [27], [28]. Different features and algorithms have been proposed in this field achieving very good results against random attacks. In [16], the authors proposed a set of 22 multitouch gestures using characteristics of hand and finger movements with an algorithm robust to orientation and translation achieving a final result of 1.58 percent EER. In [18], a set of 100 static features extracted from swipe gestures and systems based on Support Vector Machines (SVM) and Gaussian Mixture Models (GMM) were considered obtaining performances up to 10.7 percent EER. Very good results have been also achieved in [15], [17] using verification algorithms such as SVM, kNN, Random Forest and Neural Networks.

Handwritten signature is one of the most socially accepted biometrics as it has been used in financial and legal agreements for many years [29], [30], [31], [32], and it also finds applications in mobile scenarios. In [33], the authors explored the use of new algorithms based on RNNs on traditional desktop scenarios for pen-based signature recognition achieving results below 5.0 percent EER for imitation attacks. However, a considerable degradation of the system performance with results around 20.0 percent EER is obtained for imitation attacks when testing on mobile scenarios using finger touch as input [19], [20]. The main reason for such degradation of the system performance when using finger touch compared to pen-based desktop scenarios is the fact that users tend to modify the way they sign between both approaches, e.g., users who perform their signatures using closed letters with a pen input tend to perform much larger writing executions when using the finger. Besides, users whose signatures are composed of a long name and surname (or two surnames) tend to simplify some parts of their signatures due to the small surface of the screen to sign on. Graphical passwords were studied in [21], [22]. In [22], the authors proposed an approach based on graphical passwords (doodles) achieving final results above 20.0 percent EER for imitation attacks. The main reason for such degradation of the system performance lays down on the specific task that the user needs to perform to be authenticated, e.g., doodles were difficult to memorize for most of the users as they didn't use them on a daily basis.

Finally, strongly related to the present work, in [23], [24] the authors proposed the use of handwritten passwords to be authenticated. In [23], Kutzner et al. asked the users to perform an 8-digit password on the screen of a tablet device. For each handwritten password, a total of 25 static and dynamic features were extracted and tested using many different authentication algorithms. However, the authentication scenario considered in that approach restricts the deployment of the technology in real mobile applications as: i) the authors considered a large number of training samples (12), and ii) it seems to be only applicable to devices with large screens (such as tablets) as it would be very difficult for the users to perform such a long password (8 digits) on a screen of much smaller size. In [24], Nguyen et al. evaluated the use of handwritten touch biometrics for PIN-based authentication systems. Their proposed authentication approach overcame some of the drawbacks previously cited as they asked users to draw each digit of the PIN one by one. A final 4.84 percent EER was achieved using a biometric system composed of 5 dynamic features and a matcher algotithm based on DTW. Finally, a preliminary study of the work presented here was published in [25]. In that work we performed an initial analysis of the touch biometric system only for OTP authentication schemes. In addition, DTW was the only approach considered for the similarity computation.

The study presented here extends the preliminary analysis carried out in [25]. The main improvements over [25] are:

- Our preliminary touch biometric system in [25] based on DTW has been extended by incorporating RNN deep learning architectures. To the best of our knowledge, this is the first work to date that studies recurrent Siamese networks to model handwritten password authentication systems.
- Our analysis in [25] studied only OTP schemes. Here we also study PIN authentication, as depicted in Fig. 1.
- The system architecture includes 2 new blocks with respect to [25]: i) enrolment set, and ii) password generation; which are discussed in the text and evaluated experimentally.
- Section 2 has been included to survey and compare advantages and limitations of recent research on touch biometrics for mobile authentication.
- The results achieved in the present study outperform our initial results presented in [25] with a final 3.8 percent EER, a relative improvement of 30.9 percent EER compared to [25]. This result outperforms other touch biometric approaches and considers fewer enrolment samples.
- Section 7 has been included to discuss specific details for the deployment of our proposed approach on practical PIN and OTP authentication systems, including various strategies for password generation.

TABLE 2
Set of Time Functions Considered in this Work

#	Feature
1	X-coordinate: x_n
2	Y-coordinate: y_n
3	Path-tangent angle: θ_n
4	Path velocity magnitude: v_n
5	Log curvature radius: ρ_n
6	Total acceleration magnitude: a_n
7-12	First-order derivative of features 1-6: $\dot{x_n}, \dot{y_n}, \dot{\theta_n}, \dot{v_n}, \dot{\rho_n}, \dot{a_n}$
13-14	Second-order derivative of features 1-2: $\ddot{x_n}, \ddot{y_n}$
15	Ratio of the minimum over the maximum speed over a 5-samples window: v_n^r
16-17	Angle of consecutive samples and first-order derivative: α_n, $\dot{\alpha_n}$
18	Sine: s_n
19	Cosine: c_n
20	Stroke length to width ratio over a 5-samples window: r_n^5
21	Stroke length to width ratio over a 7-samples window: r_n^7

2.2 Two-Factor Password Authentication

The incorporation of biometric information on traditional password-based systems can improve the security through a second level of user authentication. Two-factor authentication approaches have been very successful in the last years. These approaches are based on the combination of two authentication stages. For example: i) the security system checks that the claimed user introduces its unique password correctly, and ii) its behavioral biometric information is used for an enhanced final verification [24], [34]. This way the robustness of the security system increases as impostors need more than the traditional password to get access to the system. This approach has been studied in previous works. In [10], the authors proposed a two-factor verification system based on timing-related features for dynamic lock patterns, achieving a final average EER of 10.39 percent for imitation attacks. A similar two-factor authentication approach was proposed in [11] for traditional Android unlock patterns but considering biometric dynamic features related to the position of the finger, pressure, finger size and accelerometer sensor achieving a final 15.0 percent EER for imitation attacks. Two-factor authentication approaches have also been expanded to physiological biometric traits. In [35], Jenkins et al. proposed a system based on features extracted for periocular images acquired using an iPhone 5, achieving very good results for the task of identification.

3 Touch Biometric System

3.1 Digit-Based Feature Extraction

In this work we evaluate the potential of touch biometric verification systems based on time functions [36]. Signals captured by the digitizer (i.e., X and Y spatial coordinates) are used to extract a set of 21 time functions for each numerical digit sample (see Table 2). Information related to pressure, pen angular orientations or pen ups broadly used in other biometric traits such as handwriting and handwritten signature is not considered here as this information is not available in all mobile devices when using the finger touch as input.

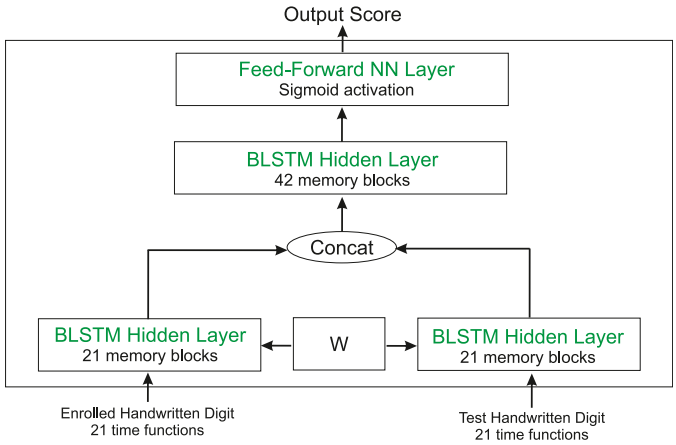


Fig. 2. Proposed end-to-end writer-independent BLSTM touch biometric system based on a Siamese architecture.

Sequential Forward Floating Search (SFFS) algorithm is used for the DTW algorithm in some of the experiments in order to select the best subsets of time functions for each handwritten digit and improve the system performance in terms of EER (%).

3.2 Similarity Computation

3.2.1 Dynamic Time Warping

DTW is used to compare the similarity between genuine and query input samples, finding the optimal elastic match among time sequences that minimizes a given distance measure. Scores are obtained as $score = e^{-D/K}$, where D and K represent respectively the minimal accumulated distance and the length of the warping path [37].

3.2.2 Recurrent Neural Networks

Some of the fields in which RNNs have caused more impact in the last years is in handwriting recognition and writer identification [38], [39]. This study explores the potential of RNNs for the task of handwritten passwords. In particular, we consider an adaptation of our original RNN systems proposed in [33] for the task of on-line handwritten signature verification. In that work we proposed RNN systems based on a Siamese architecture. The main goal was to learn a dissimilarity metric from data minimizing a discriminative cost function that drives the dissimilarity metric to be small for pairs of genuine samples from the same subject, and higher for pairs of samples coming from different subjects. Both Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) systems were studied in [33], outperforming a state-of-the-art DTW system in challenging scenarios where skilled forgeries were considered. In addition, in [33] we also studied bidirectional schemes (i.e., BLSTM and BGRU), which allow access to future context, achieving much better results compared to the original schemes that only had access to past and present contexts.

In this study we adapt the original BLSTM system proposed in [33] to handwritten passwords for touchscreen biometrics. To the best of our knowledge, this is the first work to date that studies recurrent Siamese networks to model handwritten password authentication systems. Fig. 2 shows our proposed end-to-end writer-

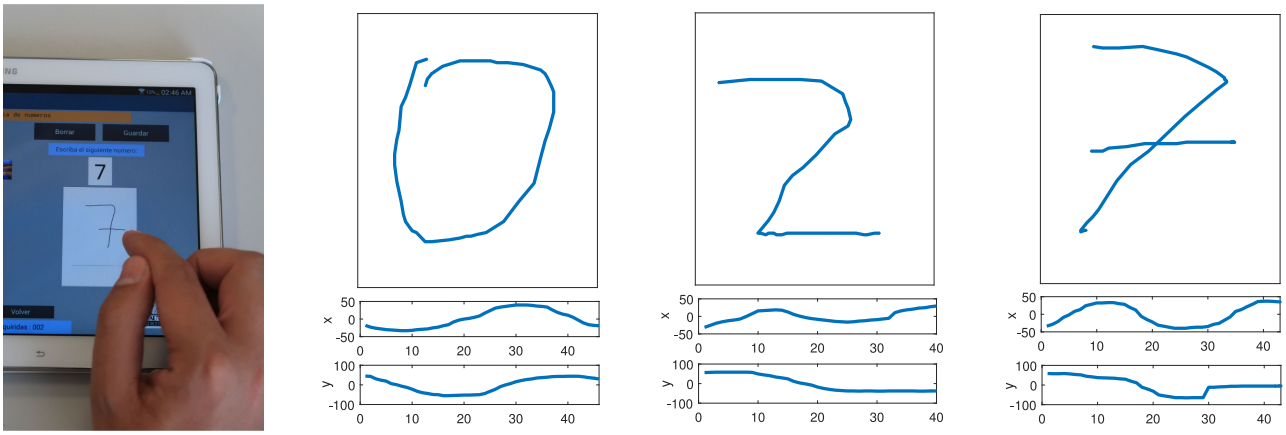


Fig. 3. (a) Acquisition setup. (b)-(d) Examples of different handwritten numerical digits of the e-BioDigit database. *X* and *Y* denote horizontal and vertical position versus the time samples.

independent BLSTM touch biometric system based on a Siamese architecture. For the input of the system, we feed the network with as much information as possible, i.e., all 21 time functions per digit. The first layer is composed of two BLSTM hidden layers with 21 memory blocks each, sharing the weights between them. The outputs of the first two parallel BLSTM hidden layers are concatenated and serve as input to the second layer, which corresponds to a BLSTM hidden layer with 42 memory blocks. Finally, a feed-forward neural network layer with a sigmoid activation is considered, providing an output score for each pair of digits. It is important to highlight that our approach is trained to distinguish between genuine and impostor patterns from all numerical digits and users. Thus, we just train one writer-independent system for all digits and users through a development dataset.

4 Database e-BioDigit

The new e-BioDigit database was captured in order to perform the experimental work included in this article. This database comprises on-line handwritten numerical digits from 0 to 9 acquired using a Samsung Galaxy Note 10.1 general purpose tablet. This device has a 10.1-inch LCD display with a resolution of 1280 $\times$ 800 pixels.

Regarding the acquisition protocol, subjects had to perform handwritten numerical digits from 0 to 9, one at a time. The acquisition setup and some examples of the handwritten numerical digits of the e-BioDigit database are depicted in Fig. 3. Additionally, samples were collected in two sessions with a time gap of at least three weeks between them in order to consider inter-session variability, very important for behavioral biometric traits [40]. For each session, users had to perform a total of 4 numerical sequences from 0 to 9 using the finger as input. Therefore, there are a total of 8 samples per numerical digit and user.

The software for capturing handwritten numerical digits was developed in order to minimize the variability of the user during the acquisition process. A rectangular area with a writing surface size similar to a 5-inch screen smartphone was considered, see Fig. 3a. A horizontal line was represented on top of the drawing rectangular area, including two buttons "OK" and "Cancel" to press after writing if the sample was good or bad respectively.

The database comprises a total of 93 users. Regarding the age distribution, the majority of the subjects (85.0 percent) are between 17 and 27 years old, as the database was collected in a university environment (36.6 percent between 17 and 21). Regarding the gender, 66.7 percent of the subjects were males and 33.3 percent females whereas for the handedness distribution, 89.2 percent of the population was righthanded.

5 Experimental Protocol

The experimental protocol designed in this study intends to cover all details of the two following main modules of our proposed password-based touch biometric system (see Fig. 1):

- *Enrolment Set.* When designing biometric authentication systems for real applications, there are usually two conflicting factors: i) the amount of data requested to the user during the enrolment, and ii) the security level provided by the biometric system. From the point of view of the security system, it seems clear that the ideal case would be to have as much information of the user as possible. However, in most real scenarios, the feasibility and success depend on the development of user-friendly applications.

  This aspect has shown to be crucial for different tasks such as the handwritten signature. In [41], we evaluated this effect using statistical systems based on HMM and GMM, achieving an absolute improvement of 11.7 percent EER when training the user models with 41 genuine signatures instead of just 4. In this work, we analyze the intra-user variability on this new authentication scenario and perform a complete analysis of how the biometric system performance changes with the number of enrolment samples acquired per digit.
- *Password Generation.* The selection of a password that is robust enough for a specific application is a key factor. The number of digits that comprise the password depends on the scenario and level of security

TABLE 3
System Performance as EER(%) of Each Numerical Digit for the **1vs1** Case on the Evaluation Dataset

	Numerical Digit									
	0	1	2	3	4	5	6	7	8	9
DTW Baseline	34.9	32.3	32.8	35.0	23.5	24.4	36.9	**22.5**	26.0	29.6
DTW Adapted	33.0	34.0	30.9	32.3	22.0	**21.7**	33.6	21.8	21.8	27.0
BLSTM	32.8	30.8	32.8	32.3	26.2	**19.6**	35.2	28.5	21.7	23.8

TABLE 4
System Performance as EER(%) of Each Numerical Digit for the **4vs1** Case on the Evaluation Dataset

	Numerical Digit									
	0	1	2	3	4	5	6	7	8	9
DTW Baseline	33.1	28.5	30.2	32.6	**18.0**	20.3	36.6	19.2	22.7	25.0
DTW Adapted	31.4	33.1	27.9	29.7	19.2	**16.9**	29.7	20.3	18.6	23.3
BLSTM	31.4	27.9	31.4	26.2	24.4	**17.4**	35.4	24.4	18.0	20.9

considered in the final application. For example, for everyday applications such as Facebook or Gmail, it is not reasonable from the point of view of the users to memorize passwords composed of 12 digits. Additionally, OTP-based systems could request longer passwords compared to PIN-based systems as users do not have to memorize them, i.e., the security system is in charge of selecting and providing the password to the user.

In this experimental work we evaluate the robustness of handwritten passwords regarding the three following features: i) which digits better discriminate users, ii) whether repetitions of the same numerical digits in a password can help to discriminate users or not, and iii) the length of the password. For short passwords (i.e., fewer than 6 digits), this analysis is carried out performing all possible digit combinations, whereas for longer passwords, the SFFS algorithm is used to select the best digit combinations due to the high cost of performing all possible comparisons.

In order to perform a complete analysis of these two modules, the e-BioDigit database is divided into development (the first 50 users) and evaluation (the remaining 43 users) datasets.

For the development of our proposed handwritten touch biometric systems, N genuine signatures (up to 4) from the first session can be used as enrolment samples, whereas the 4 remaining genuine samples from the second session are used for testing. Impostor scores are obtained by comparing the N enrolment samples with one genuine sample of each of the remaining users (simulating this way the imitation attack in which the impostor knows the password).

For the evaluation of our proposed touch biometric system, different scenarios are generally considered regarding the number of available enrolment samples per user (i.e., Nvs1), in which the final score is performed as the average score of N one-to-one comparisons. In addition, in case of using passwords composed of several digits, the final score is produced after averaging the different one by one digit score comparisons.

It is important to highlight that the inter-session variability problem is also considered in the experimental protocol carried out in this work as genuine digit samples from different sessions are used as enrolment and testing samples respectively. This effect has proven to be very important for many behavioral biometric traits such as the case of the handwritten signature [40].

TABLE 5
Time Functions Selected for the Baseline System

#	Time-function description
1	X-coordinate: x_n
2	Y-coordinate: y_n
7-8	First-order derivate of features 1-2: $\dot{x_n}, \dot{y_n}$
13-14	Second-order derivate of features 1-2: $\ddot{x_n}, \ddot{y_n}$

6 Experimental Results

6.1 One-Digit Analysis

This section analyzes the potential of each numerical digit (i.e., from 0 to 9) for the task of user authentication. We consider three different systems: i) a baseline DTW system, ii) an adapted DTW considering feature selection, and iii) a system based on RNNs.

Experimental results on the evaluation dataset for these three systems are shown in Tables 3 and 4 in terms of EER (%) for the cases of 1vs1 and 4vs1 comparisons, respectively.

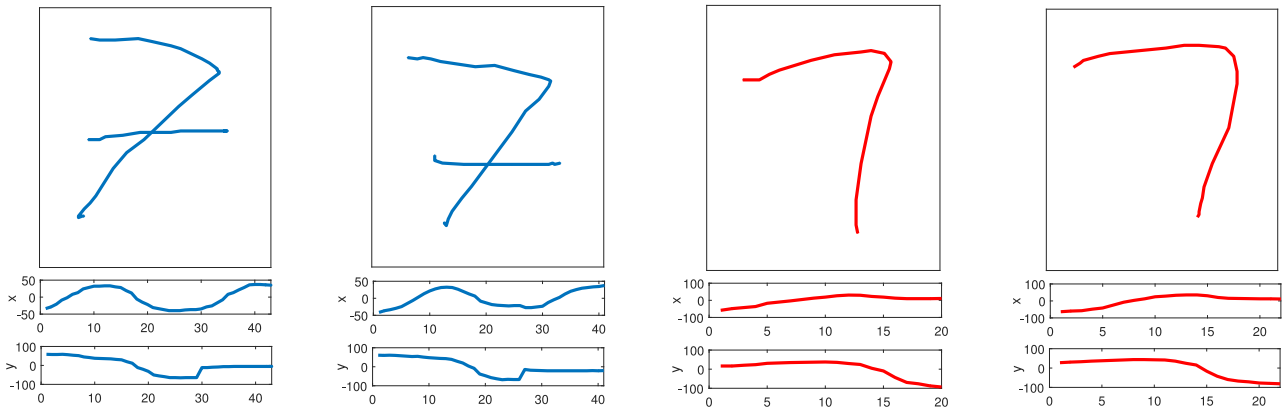
6.1.1 DTW Baseline System

In order to provide an easily reproducible framework, we first consider a baseline system based on DTW with the same fixed time functions for all numerical digits. Table 5 shows the time functions selected, which are commonly used as baseline in other biometric traits such as the handwritten signature [20], [42].

Analyzing the first rows of Tables 3 and 4 we can see how very good authentication results are obtained by the DTW Baseline System taking into account that we only consider one digit and the same time functions for all numerical digits.

Analyzing in Table 3 the extreme scenario of having just one available digit sample during the enrolment (1vs1), the numerical digit 7 achieves the best result with 22.5 percent EER. In addition, other numerical digits such as 4 or 5 achieve similar results with EERs below 25.0 percent. This first experiment puts in evidence the discriminative power of each handwritten digit. Fig. 4 shows examples of the digit 7 performed by two different users in order to observe the low intra- and high inter-user variability of this number. This effect is produced as different users tend to perform a specific digit in a different way, i.e., starting from a different stroke of the digit or even removing some of them such as the crossed horizontal stroke of the number 7.

Analyzing in Table 4 the scenario of using four enrolment samples (4vs1), an average absolute improvement of 3.2 percent EER is achieved compared to the 1vs1 scenario showing the importance of acquiring more than one sample during the enrolment stage, if possible. For this scenario, the digit 4 achieves the best result with 18.0 percent EER.



(a) User A, sample 1 (b) User A, sample 2 (c) User B, sample 1 (d) User B, sample 2

Fig. 4. Examples of the digit 7 performed by two different users.

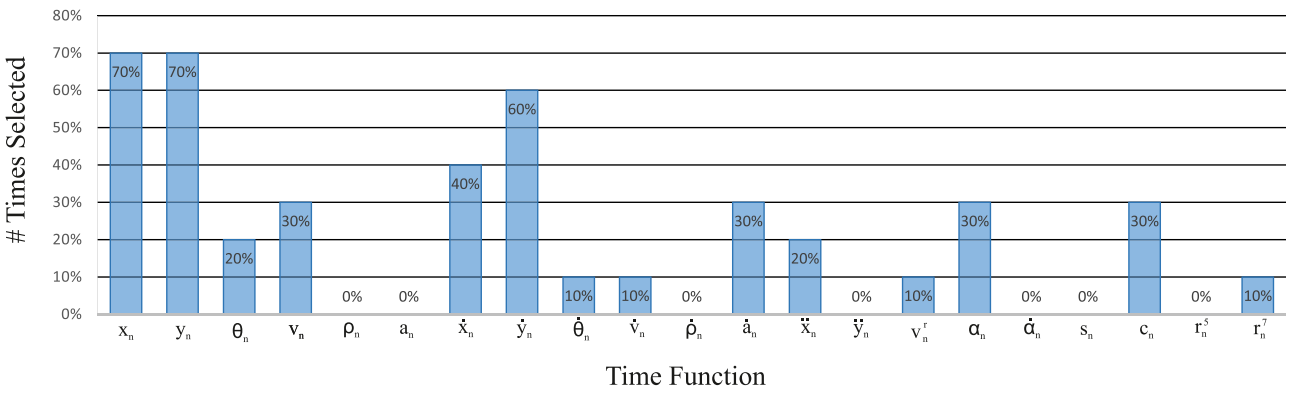


Fig. 5. Histogram of functions selected by SFFS for our DTW adapted system. Functions described in Table 2.

6.1.2 DTW Adapted System

We now apply SFFS over the development dataset in order to enhance the DTW touch biometric system through the selection of specific time functions for each handwritten digit. Fig. 5 shows the number of times each time function is selected in our DTW Adapted System from the 21 total time functions described in Table 2. In general, we can highlight the importance of x_n, y_n time functions as they are selected for 70 percent of the numerical digits. In addition, time functions $\dot{x_n}, \dot{y_n}$ related to X and Y time derivatives seem to be very important as they are selected for near half of the digits. Other time functions such as ρ_n, $\dot{\rho_n}$, $\dot{\alpha_n}$ and s_n related to geometrical aspects of the numerical digits are proven not to be very useful to discriminate between genuine and impostor users.

The second rows of Tables 3 and 4 show the results achieved for each digit using our DTW Adapted System over the evaluation dataset for both 1vs1 and 4vs1 cases, respectively. In general, better results are achieved compared to the DTW Baseline System. Analyzing the 1vs1 scenario, our DTW Adapted System achieves an average absolute improvement of 2.0 percent EER, being the numerical digit 5 the one that provides the best result with a 21.7 percent EER. Analyzing the 4vs1 scenario, our DTW Adapted System achieves an average absolute improvement of 1.6 percent EER, being again the numerical digit 5 the one that achieves the best result with a 16.9 percent EER. These results put in evidence the importance of considering different time functions for each digit in order to develop more robust biometric authentication systems against attacks.

6.1.3 BLSTM System

We now explore the potential of state-of-the-art deep learning technology applied to our touch biometric data. Our proposed end-to-end writer-independent BLSTM system is trained using only the 50 users of the development dataset. Samples from all numerical digits (i.e., from 0 to 9) and development users are considered together during training as we intend to distinguish between genuine and impostor handwritten digit samples regardless of the user and the numerical digit. This approach resulted in better generalisation results compared to the case of training one system per numerical digit. Therefore, our BLSTM system is trained considering two different cases: i) pairs of genuine digit samples drawn by the same user, and ii) pairs of genuine and impostor digit samples, one performed by the claimed user and the other one by an impostor. For each case there are a total of 4 train samples $\times$4 test samples $\times$10 numerical digits $\times$50 users $\simeq$ 8,000 comparisons, having the same number of genuine and impostor comparisons. Our BLSTM System has been implemented under Keras using Tensorflow as backend, with a NVIDIA GeForce RTX 2080 Ti GPU. Adam optimizer is considered with a learning rate of 0.001 and a loss function based on binary cross-entropy.

TABLE 6
Evolution of the System Performance in Terms of EER (%) on the Evaluation Dataset

		# Digits that comprise the password							
		1	2	3	4	5	6	7	8
# Enrolment samples	1	21.7	14.0	11.6	11.6	9.3	8.5	8.5	8.5
		[5]	[5, 8]	[5, 7, 9]	[1, 5, 7, 9]	[2, 5, 6, 7, 8]	[2, 3, 5, 6, 7, 8]	[1, 2, 3, 5, 6, 7, 8]	[2, 3, 4, 5, 6, 7, 8, 9]
	2	18.6	11.6	9.3	7.4	7.3	4.6	4.6	4.6
		[5]	[5, 8]	[2, 5, 8]	[2, 5, 8, 9]	[1, 2, 5, 7, 9]	[2, 5, 6, 7, 8, 9]	[1, 2, 3, 5, 7, 8, 9]	[1, 2, 3, 4, 5, 6, 7, 8]
	3	16.3	9.5	7.4	5.9	4.7	4.6	**3.8**	4.6
		[5]	[2, 8]	[1, 2, 8]	[2, 5, 8, 9]	[1, 2, 5, 8, 9]	[1, 2, 3, 5, 8, 9]	**[1, 2, 3, 4, 5, 8, 9]**	[0, 1, 2, 3, 4, 5, 7, 8]
	4	16.9	11.6	7.0	6.1	4.7	4.6	4.3	4.8
		[5]	[5, 8]	[7, 8, 9]	[5, 7, 8, 9]	[1, 5, 7, 8, 9]	[1, 2, 5, 7, 8, 9]	[1, 2, 3, 5, 7, 8, 9]	[0, 1, 2, 3, 4, 5, 7, 8]

The best system performance achieved and the corresponding handwritten digits selected are shown on the top and bottom of each cell, respectively.

The third rows of Tables 3 and 4 show the results achieved for each digit using our BLSTM System over the evaluation dataset for both 1vs1 and 4vs1 cases, respectively. In general, better results are achieved compared to the DTW Baseline System. Analyzing the 1vs1 scenario, our BLSTM System achieves an average absolute improvement of 1.4 percent EER, being the numerical digit 5 the one that provides the best result with a 19.6 percent EER. Analyzing the 4vs1 scenario, our BLSTM System achieves an average absolute improvement of 0.9 percent EER, being again the numerical digit 5 the one that achieves the best result with a 17.4 percent EER.

Finally, we compare our BLSTM System to the DTW Adapted System. In general, very similar results have been achieved for both authentication systems. For example, analyzing the 1vs1 case in Table 3, the BLSTM System has outperformed the DTW Adapted System for the 50 percent of the numerical digits (i.e., 0, 1, 5, 8, and 9), proving the potential of deep learning technologies even when just a single enrolment sample is considered. Despite these improvements, the DTW Adapted System outperforms slightly the BLSTM System in general, achieving an average absolute improvement of 0.5 and 0.7 percent EER for the 1vs1 and 4vs1 cases, respectively.

6.2 Digit Combinations

This section explores the robustness of our proposed approach when increasing the length of the password and also the number of available enrolment samples. The DTW Adapted System is considered in this analysis as it has outperformed the other systems studied. Regarding the type of digits that comprises the password, repetitions of the same numerical digits are allowed. However, the number of repetitions is restricted to 4, e.g., "2 5 8 8 8 8". The reason for this limitation is motivated due to only 4 samples were acquired per digit during the second session of the e-BioDigit database. Table 6 shows the evolution of the system performance in terms of EER (%) on the evaluation dataset when increasing the length of the handwritten password (from 1 to 8 digits) and also the number of available enrolment samples (from 1 to 4).

First, we analyze how the length of the handwritten password affects the system performance. In general, a considerable system performance improvement is achieved when adding more handwritten digits to the password. For example, for the case of having just one enrolment sample per user (1vs1), a password that is composed of just two handwritten digits achieves a 14.0 percent EER, an absolute improvement of 7.7 percent EER compared to the case of using a password with just one digit. This result is further improved when increasing the number of handwritten digits of the password with a final 8.5 percent EER for the case of considering a 6-digit password. However, there seems to exist a limit in the system performance improvement with the number of digits that comprise the password. In our experiments, the best results are obtained for passwords with a length of 6 and 7 digits.

Now, we analyze the effect of the number of available enrolment samples on the system performance. In general, the system performance improves with the number of enrolment samples. For example, for the case of having just one enrolment sample and a password composed of just one digit, the biometric system achieves a 21.7 percent EER. This result is further improved when increasing the number of enrolment samples to 4, achieving a final value of 16.9 percent EER, an absolute improvement of 4.8 percent EER. However, there seems to exist a limit in the system performance improvement with the number of enrolment samples. In our experiment, very similar results are obtained when considering 3 or 4 enrolment samples, achieving a final value of 3.8 percent EER when considering 3 enrolment samples and a handwritten password of 7 digits. This interesting finding is different compared to other behavioral biometric traits such as the handwritten signature as the system performance keeps improving even with large number of enrolment samples [41]. This effect may be due to the lower intra-user variability of our proposed touch biometric approach compared to other behavioral biometrics as well as the DTW similarity computation algorithm considered.

Finally, we pay attention to the content and the number of possible combinations of the best handwritten passwords using our proposed touch biometric system so as to achieve the best system performance. Table 6 indicates in the bottom of each cell the best handwritten digits selected but not their order, as the final score of our proposed touch biometric system is produced after averaging the different one by one digit score comparisons. Therefore, for the case of having a password comprised of n digits, there are a total of $n!$

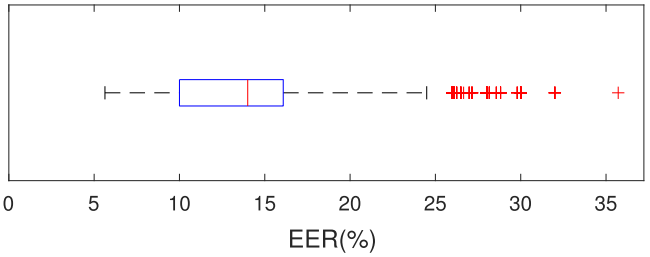


Fig. 6. **PIN System**: Boxplot for the case of considering all 4-digit password combinations. On the box, the central mark indicates the median, and the left and right edges of the box indicate the 25th and 75th percentiles, respectively.

possible password combinations (note that in our experiments we did not have any case of repetitions of digits achieving the best results).

6.3 Comparison to the State of the Art

Our proposed approach is now compared to other state-of-the-art biometric authentication approaches described in Table 1. In order to perform a fair analysis, we compare our proposed approach to all studies that consider the same type of impostors, i.e., imitation attacks.

In general, our proposed approach achieves better results than other touch biometric approaches. For the case of lock pattern dynamic systems [10], [11], the best system performance reported was an average 10.39 percent EER. Our proposed approach also outperforms other biometric methods such as the handwritten signature or graphical passwords [20], [22]. In [20], the authors proposed handwritten signature verification systems adapted to mobile scenarios, i.e., using mobile devices such as smartphones and tablets with the finger as input, achieving EERs around 20.0 percent. In [22], the authors proposed the use of graphical doodles and pseudosignatures (i.e., simplified versions of the signatures drawn with the finger). EERs above 20.0 percent were obtained in both cases for imitation attacks.

Finally, our proposed approach has been compared to other state-of-the-art authentication systems based on handwritten passwords. In [23], the authors proposed the use of handwritten passwords with a fixed length of 8 characters, achieving a final False Acceptance Rate (FAR) of 10.42 percent when using a total of 12 training samples per user (the False Rejection Rate FRR was not provided by the authors). In [24], Nguyen et al. evaluated the potential of drawing each digit of a 4-digit PIN one by one, achieving a final result of 4.84 percent EER when considering a total of 5 enrolment samples. Our proposed approach achieves a final value of 3.8 percent EER and it is able to mitigate the limitations of [23] about the size of the touchscreen, as users perform numerical digits one at a time. Additionally, we only consider 3 enrolment samples and not 5 as in [24] in order to improve the usability of our approach.

7 Password Generation and System Setup

In this section we discuss specific details for the deployment of our proposed approach in real scenarios considering the same experimental protocol described in Section 5. The DTW Adapted System has been considered for this analysis.

First, we focus on PIN-based systems. For this scenario, we propose to use passwords based on 4 digits as users have to memorize them and it is not feasible from the point of view of the user to consider longer passwords. Regarding the enrolment stage, we propose to request 3 enrolment samples per digit to each user. We consider this as something feasible for real applications as users would have to perform a total of 4 digits $\times 3$ samples/digit $= 12$ samples, i.e., 12 samples $\times 2$ seconds/sample $\simeq 25$ seconds.

Once we have fixed the number of enrolment samples and digits parameters, we design what type of passwords we let users to use (i.e., we design the Password Generation module in Fig. 1). The following cases are considered regarding both the system performance and number of possible combinations: i) ALL password combinations are allowed, and ii) only combinations using the BEST 4 digits selected in Table 6 and with no repetitions (recall in Section 6.2 we obtained that the most discriminative password combinations in terms of touch biometric information didn't include repeated digits). Fig. 6 shows the EER distribution values obtained for all possible password combinations. On the box, the central mark indicates the median, and the left and right edges of the box indicate the 25th and 75th percentiles, respectively. The whiskers extend to the most extreme data points not considered outliers, and the outliers are plotted individually. In general, we can see that the 75 percent of password combinations provide results below 16.2 percent EER. Analyzing the case ALL, the system performance results achieved are between 5.9 and 35.7 percent EER with a total of 10^4 combinations. The performance is improved in the case BEST with a 5.9 percent EER for all considered combinations. However, users would be able to choose only among $4!$ combinations (i.e., 24). Besides, the security level of the first authentication stage would decrease as fewer password combinations would be possible. Therefore, a good choice could be to select all possible passwords that provide results in a range of EERs. For example, permitting between 5.9 and 10.0 percent EER. This approach would allow users to choose among 2,956 different 4-digit passwords.

Now, we analyze the OTP-based system. For this scenario, we propose to use passwords composed of 7 digits, similar to current OTP-based applications, as users do not have to memorize the password, i.e., the system is in charge of selecting and providing different passwords to the user each time is required. Regarding the enrolment stage, we also propose to request 3 enrolment samples per digit so users would have to perform a total of 10 digits $\times 3$ samples/digit $= 30$ samples, i.e., 30 samples $\times 2$ seconds/sample $\simeq 1$ minute.

Once we have fixed both the number of enrolment samples and the length of the password, we analyze the content of the passwords. For this scenario, the following cases are considered: i) ALL digit combinations are allowed, and ii) only combinations using the BEST 7 digits selected in Table 6 with no repetitions. Table 7 depicts the number of possible combinations as well as the EER (%) for both cases. Analyzing the case in which users can choose any possible combination, the system performance results achieved are between 3.8 and 14.0 percent EER. However, it is important to remark that for this case (longer passwords) results were

TABLE 7
OTP System: Number of 7-Digit Possible Combinations and System Performance Results

	# Password Combinations	EER(%)
Case ALL	10^7	3.8 to 14.0
Case BEST	5,040	3.8

obtained due to experimental restrictions using the SFFS algorithm and limiting the maximum number of digit repetitions to 4, so the final 14.0 percent EER might get a bit worse in practice when considering all possible digit combinations. This approach is further improved in the case BEST with a final 3.8 percent EER. For this scenario we propose to use this second case as there would be a total of 7! (i.e., 5,040) combinations that provide the best system performance for our proposed touch biometric approach.

8 Conclusions

This work evaluates the advantages and potential of incorporating handwritten touch biometrics to password-based mobile authentication systems. The new e-BioDigit database that comprises handwritten numerical digits from 0 to 9 is used in the experiments reported in this work and it is available together with benchmark results in GitHub.[2] Data were collected in two sessions for a total of 93 subjects. Handwritten numerical digits were acquired using the finger touch as the input on a Samsung Galaxy Note 10.1 general purpose tablet device.

For the new e-BioDigit database, we report a benchmark evaluation using two different state-of-the-art approaches: i) DTW in combination with the SFFS function selection algorithm, and ii) RNN deep learning technology. Both approaches have been compared, achieving very good results even for the case of using just a single enrolment sample. In addition, we perform a complete analysis of the touch biometric system regarding the discriminative power of each handwritten digit, and the robustness of our proposed approach when increasing the length of the password and the number of enrolment samples per user.

Our proposed approach achieves good results with EERs ca. 4.0 percent when considering imitation attacks, outperforming other traditional biometric verification traits such as the handwritten signature or graphical passwords on similar mobile scenarios. Additionally, we discuss specific details for the deployment or our proposed approach on current PIN- and OTP-based authentication systems.

Future work will be oriented to enlarge the current e-BioDigit database in order to consider lower- and upper-case letters and also to train more complex deep learning architectures.

Acknowledgments

This work has been supported by projects: BIBECA (RTI2018-101248-B-I00 MINECO/FEDER), Bio-Guard (Ayudas Fundación BBVA a Equipos de Investigación Científica 2017) and by UAM-CecaBank. Ruben Tolosana is supported by a FPU Fellowship from Spanish MECD.

2. https://github.com/BiDAlab/eBioDigitDB

References

[1] M. Salehan and A. Negahban, "Social networking on smartphones: When mobile phones become addictive," *Comput. Human Behavior*, vol. 29, no. 6, pp. 2632–2639, 2013.
[2] J. Bonneau, C. Herley, P. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proc. IEEE Symp. Secur. Privacy*, 2012, pp. 553–567.
[3] J. Galbally, I. Coisel, and I. Sanchez, "A new multimodal approach for password strength estimation—Part I: Theory and algorithms," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 12, pp. 2829–2844, Dec. 2017.
[4] A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, "Smudge attacks on smartphone touch screens," in *Proc. 4th USENIX Conf. Offensive Technol.*, 2010, pp. 1–7.
[5] D. Shukla, R. Kumar, A. Serwadda, and V. Phoha, "Beware, your hands reveal your secrets!" in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 904–917.
[6] Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu, and W. Zhao, "My Google glass sees your passwords!" in *Proc. Black Hat USA*, Las Vegas, USA, 2014.
[7] W. Meng, D. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1268–1293, Jul.–Sep. 2015.
[8] L. Wan, M. Zeiler, S. Zhang, Y. LeCun, and R. Fergus, "Regularization of neural networks using DropConnect," in *Proc. 30th Int. Conf. Mach. Learn.*, 2013, pp. 1058–1066.
[9] M. Liang and X. Hu, "Recurrent convolutional neural network for object recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2015, pp. 3367–3375.
[10] J. Angulo and E. Wastlund, "Exploring touch-screen biometrics for user identification on smart phones," in *Privacy and Identity Management for Life*, J. Camenisch, B. Crispo, S. Fischer-Hbner, R. Leenes, and G. Russello, Eds. Berlin, Germany: Springer, 2011, pp. 130–143.
[11] P. Lacharme and C. Rosenberger, "Synchronous one time biometrics with pattern based authentication," in *Proc. 11th Int. Conf. Availability Rel. Secur.*, 2016, pp. 260–265.
[12] E. von Zezschwitz, M. Eiband, D. Buschek, S. Oberhuber, A. D. Luca, F. Alt, and H. Hussmann, "On quantifying the effective password space of grid-based unlock gestures," in *Proc. Int. Conf. Mobile Ubiquitous Multimedia*, 2016, pp. 201–212.
[13] D. Buschek, A. D. Luca, and F. Alt, "There is more to typing than speed: Expressive mobile touch keyboards via dynamic font personalisation," in *Proc. Int. Conf. Human-Comput. Interaction Mobile Devices Serv.*, 2015, pp. 125–130.
[14] D. Buschek, A. D. Luca, and F. Alt, "Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices," in *Proc. CHI Conf. Human Factors Comput. Syst.*, 2015, pp. 1393–1402.
[15] L. Li, X. Zhao, and G. Xue, "Unobservable reauthentication for smartphones," in *Proc. 20th Netw. Distrib. Syst. Secur. Symp.*, pp. 1–16, 2013.
[16] N. Sae-Bae, N. Memon, K. Isbister, and K. Ahmed, "Multitouch gesture-based authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 4, pp. 568–582, Apr. 2014.
[17] C. Shen, Y. Zhang, X. Guan, and R. Maxion, "Performance analysis of touch-interaction behavior for active smartphone authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 3, pp. 498–513, Mar. 2016.
[18] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales, "Benchmarking touchscreen biometrics for mobile authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 11, pp. 2720–2733, Nov. 2018.
[19] N. Sae-Bae and N. Memon, "Online signature verification on mobile devices," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 6, pp. 933–947, Jun. 2014.
[20] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Benchmarking desktop and mobile handwriting across COTS devices: The e-BioSign biometric database," *PLoS ONE*, vol. 12, 2017, Art. no. e0176792.
[21] W. Khan, M. Aalsalem, and Y. Xiang, "A graphical password based system for small mobile devices," *Int. J. Comput. Sci.*, vol. 5, no. 2, pp. 145–154, 2011.
[22] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "Graphical password-based user authentication with free-form doodles," *IEEE Trans. Human-Mach. Syst.*, vol. 46, no. 4, pp. 607–614, Aug. 2016.

[23] T. Kutzner, F. Ye, I. Bonninger, C. Travieso, M. Dutta, and A. Singh, "User verification using safe handwritten passwords on smartphones," in *Proc. 8th Int. Conf. Contemporary Comput.*, 2015, pp. 48–53.
[24] T. Nguyen, N. Sae-Bae, and N. Memon, "DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices," *Comput. Secur.*, vol. 66, pp. 115–128, 2017.
[25] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Incorporating touch biometrics to mobile one-time passwords: Exploration of digits," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops*, 2018, pp. 584–5847.
[26] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Presentation attacks in signature biometrics: Types and introduction to attack detection," in *Handbook of Biometric Anti-Spoofing*, S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, Eds., 2nd ed. Berlin, Germany: Springer, 2019.
[27] A. Serwadda, V. Phoha, and Z. Wang, "Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms," in *Proc. Int. Conf. Biometrics: Theory Appl. Syst.*, 2013, pp. 1–8.
[28] V. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," *IEEE Signal Process. Mag.*, vol. 33, no. 4, pp. 49–61, Jul. 2016.
[29] J. Fierrez and J. Ortega-Garcia, "On-line signature verification," in *Handbook of Biometrics*, A. K. Jain, A. Ross, and P. Flynn, Eds. Berlin, Germany: Springer, 2008, pp. 189–209.
[30] R. Plamondon and S. Srihari,"On-line and off-line handwriting recognition: A comprehensive survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 1, pp. 63–84, Jan. 2000.
[31] R. Plamondon, G. Pirlo, and D. Impedovo, "Online signature verification," in *Handbook of Document Image Processing and Recognition*, D. Doermann and K. Tombre, Eds. Berlin, Germany: Springer, 2014, pp. 917–947.
[32] M. Diaz, M. Ferrer, D. Impedovo, M. Malik, G. Pirlo, and R. Plamondon, "A perspective analysis of handwritten signature technology," *ACM Comput. Surveys*, vol. 51, 2019, Art. no. 117.
[33] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Exploring recurrent neural networks for on-line handwritten signature biometrics," *IEEE Access*, vol. 6, pp. 5128–5138, 2018.
[34] A. Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and I know itgs you! Implicit authentication based on touch screen patterns," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2012, pp. 987–996.
[35] J. Jenkins, J. Shelton, and K. Roy, "One-time password for biometric systems: Disposable feature templates," in *Proc. SoutheastCon* , Charlotte, USA, 2017.
[36] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia, and J. Fierrez, "Preprocessing and feature selection for improved sensor interoperability in online biometric signature verification," *IEEE Access*, vol. 3, pp. 478–489, 2015.
[37] M. Martinez-Diaz, J. Fierrez, and S. Hangai, "Signature matching," in *Encyclopedia of Biometrics*, S. Z. Li and A. Jain, Eds. Berlin, Germany: Springer, 2015, pp. 1382–1387.
[38] A. Graves, M. Liwicki, S. Fernandez, R. Bertolami, H. Bunke, and J. Schmidhuber, "A novel connectionist system for unconstrained handwriting recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 5, pp. 855–868, May 2009.
[39] X. Zhang, G. Xie, C. Liu, and Y. Bengio, "End-to-end online writer identification with recurrent neural network," *IEEE Trans. Human-Mach. Syst.*, vol. 47, no. 2, pp. 285–292, Apr. 2017.
[40] J. Galbally, M. Martinez-Diaz, and J. Fierrez, "Aging in biometrics: An experimental analysis on on-line signature," *PLoS ONE*, vol. 8, no. 7, 2013, Art. no. e69897.
[41] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia, and J. Fierrez, "Update strategies for HMM-based dynamic signature biometric systems," in *Proc. 7th IEEE Int. Workshop Inf. Forensics Secur.*, 2015, pp. 1–6.
[42] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, and J. Liu-Jimenez, "Performance evaluation of handwritten signature recognition in mobile environments," *IET Biometrics*, vol. 3, pp. 139–146, 2014.

Ruben Tolosana received the MSc degree in telecommunication engineering from the Universidad Autonoma de Madrid, in 2014. In April 2014, he joined the Biometrics and Data Pattern Analytics - BiDA Lab, Universidad Autonoma de Madrid, where he is currently collaborating as an assistant researcher working toward the PhD degree. Since then, he has been granted with several awards such as the FPU research fellowship from Spanish MECD in 2015, and the European Biometrics Industry Award from EAB in 2018. His research interests are mainly focused on signal and image processing, pattern recognition, deep learning, and biometrics, particularly in the areas of handwriting and handwritten signature. He is the author of several publications and also collaborates as a reviewer in many different international conferences (e.g., ICDAR, ICB, EUSIPCO, etc.) and high-impact journals (e.g., the *IEEE Transactions of Information Forensics and Security*, the *IEEE Transactions on Cybernetics*, the *ACM Computing Surveys*, etc.). Finally, he has participated in several National and European projects focused on the deployment of biometric security through out the world.

Ruben Vera-Rodriguez received the MSc degree in telecommunications engineering from the Universidad de Sevilla, Spain, in 2006, and the PhD degree in electrical and electronic engineering from Swansea University, United Kingdom, in 2010. Since 2010, he has been affiliated with the Biometric Recognition Group, Universidad Autonoma de Madrid, Spain, where he has been currently an associate professor since 2018. His research interests include signal and image processing, pattern recognition, and biometrics, with emphasis on signature, face, gait verification, and forensic applications of biometrics. He is actively involved in several National and European projects focused on biometrics. He has been the program chair for the IEEE 51st International Carnahan Conference on Security and Technology (ICCST) in 2017 and the 23rd Iberoamerican Congress on Pattern Recognition (CIARP 2018) in 2018.

Julian Fierrez received the MSc and PhD degrees in telecommunications engineering from the Universidad Politecnica de Madrid, Spain, in 2001 and 2006, respectively. Since 2002, he has been with the Biometric Recognition Group, Universidad Politecnica de Madrid. Since 2004, he has been with the Universidad Autonoma de Madrid, where he is currently an associate professor. From 2007 to 2009, he was a visiting researcher with Michigan State University, under a Marie Curie Fellowship. His research interests include signal and image processing, pattern recognition, and biometrics, with an emphasis on multibiometrics, biometric evaluation, system security, forensics, and mobile applications of biometrics. He has been actively involved in multiple EU projects focused on biometrics (e.g., TABULA RASA and BEAT), and has attracted notable impact for his research. He was a recipient of a number of distinctions, including the EAB European Biometric Industry Award 2006, the EURASIP Best PhD Award 2012, the Miguel Catalan Award to the Best Researcher under 40 in the Community of Madrid in the general area of science and technology, and the 2017 IAPR Young Biometrics Investigator Award. He is an associate editor of the *IEEE Transactions on Information Forensics and Security* and the *IEEE Transactions on Image Processing*. He is a member of the IEEE.