Incorporating Touch Biometrics to Mobile One-Time Passwords: Exploration of Digits

Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez and Javier Ortega-Garcia
Biometrics and Data Pattern Analytics (BiDA) Lab
Universidad Autonoma de Madrid, 28049 Madrid, Spain
{ruben.tolosana, ruben.vera, julian.fierrez, javier.ortega}@uam.es

Abstract

This work evaluates the advantages and potential of incorporating touch biometrics to mobile one-time passwords (OTP). The new e-BioDigit database, which comprises on-line handwritten numerical digits from 0 to 9, has been acquired using the finger touch as input to a mobile device. This database is used in the experiments reported in this work and it is publicly available to the research community. An analysis of the OTP scenario using handwritten digits is carried out regarding which are the most discriminative handwritten digits and how robust the system is when increasing the number of them in the user password. Additionally, the best features for each handwritten numerical digit are studied in order to enhance our proposed biometric system. Our proposed approach achieves remarkable results with EERs ca. 5.0% when using skilled forgeries, outperforming other traditional biometric verification traits such as the handwritten signature or graphical passwords on similar mobile scenarios.

1. Introduction

Mobile devices have become an indispensable tool for most people nowadays [16]. This rapid and continuous deployment of mobile phones around the world has been motivated not only for the high technological evolution and new features incorporated by the mobile phone sector but also to the new internet infrastructures that allow the communications 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 phones for the society and are trying to deploy their services through user-friendly mobile applications ensuring data protection and a high security access level. However, this idea is difficult to accomplish using only the traditional One-Time Password (OTP) security approaches based on PINs (Personal Identification Numbers). Biometric recognition schemes seem to cope with these problems as they combine both high performance and convenience as they are part of ourselves [12].

Biometric behavioural verification systems are becoming a very attractive way to verify users on mobile devices. One of the most socially accepted traits is the handwritten signature as it has been used in financial and legal agreements scenarios for many years [5, 13, 14]. Biometric verification systems based on on-line handwritten signature are very effective against both skilled (i.e., the case in which impostors have some level of information about the user being attacked and try to forge their signature claiming to be that user in the system) and random impostors (i.e., the case in which no information about the users being attacked is known and impostors present their own signature claiming to be another user of the system). In [18], the authors explored the use of new algorithms based on Recurrent Neural Networks (RNNs) on office-like scenarios for pen-based signature recognition achieving results below 5.0% Equal Error Rate (EER) for skilled impostors. However, a considerable degradation of the system performance with results around 20.0% EER is produced for skilled forgeries when testing on universal mobile scenarios using finger touch for signature generation [2, 15, 17]. The reason for such degradation of the system performance compared to pen-based office-like scenarios is due to the fact that users tend to modify the way they sign, e.g., users who perform their signatures using closed letters with a pen input tend to perform much larger writing executions in comparison with other letters due to the lower precision they are able to achieve 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. In [11], the authors proposed a different approach based on graphical passwords with free doodles for mobiles achieving final results above 20.0% EER for skilled forgery scenarios. 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

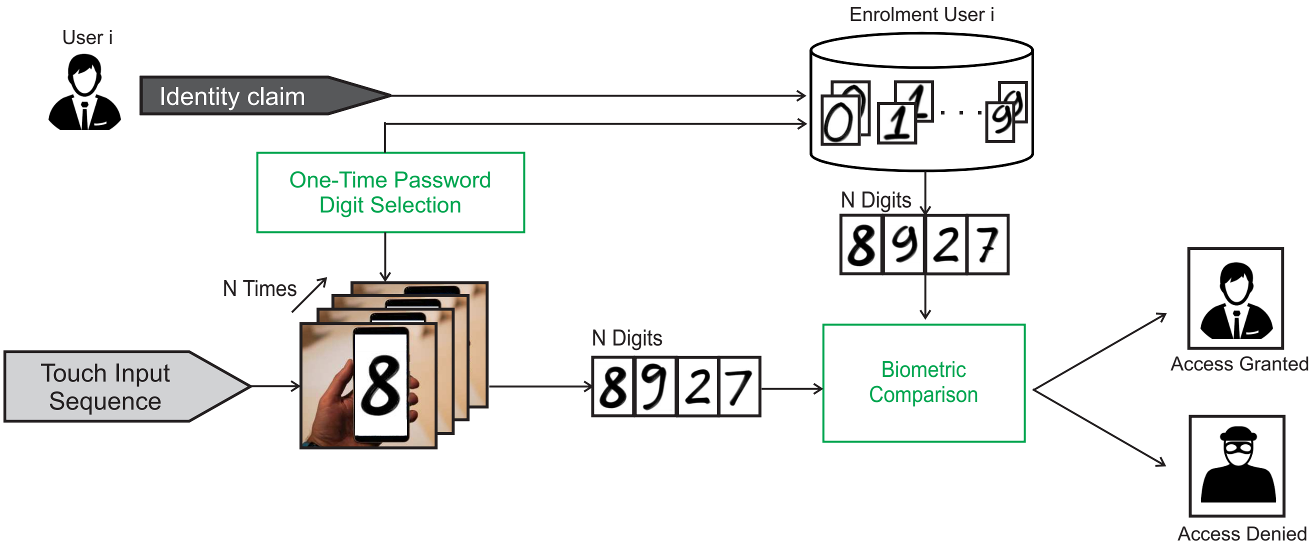


Figure 1. Architecture of our proposed one-time password system including touch biometrics for mobile scenarios.

for most of the users as they didn't use them on daily basis. Consequently, many researchers are putting their efforts to develop more robust and user-friendly security schemes on mobile devices.

Two-factor authentication approaches have gained a lot of success in the last years in order to improve the level of security. These approaches are based on the combination of two authentication stages. For example, one possible case could be the following: 1) the security system checks that the claimed user introduces its unique password correctly, and 2) its behavioural biometric information is used for an enhanced final verification [9]. 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 [1], the authors proposed a two-factor verification system based on dynamic lock patterns, achieving a final average value of 10.39% EER for skilled forgeries. A similar approach based on OTP with dynamical lock patterns was considered in [8] extracting features such as the X and Y position, pressure or finger size with very good results. This approach has also been expanded to periocular biometrics [6].

This work proposes a novel OTP system, where the users perform handwritten numerical digits on the screen of a mobile device. This way, the traditional OTP is enhanced by incorporating biometric dynamic handwritten information. Two different aspects of the security system are analysed. First, the analysis of the OTP regarding which are the most discriminative handwritten digits and how robust the system is when increasing the number of them in the user password. Second, the analysis of the biometric system in terms of which are the best features extracted for each handwritten numerical digit. One example of use that motivates our proposed approach is focused on internet payments by means of credit cards. Banks usually send a numerical code (typically between 6 and 8 digits) to the user mobile phone. This numerical code 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 performing the handwritten digits.

The main contributions of this work are the following:

- We incorporate touch biometrics to mobile OTP. An exhaustive analysis of the OTP regarding which are the most discriminative handwritten digits and how robust the system is when increasing the number of them in the user password is carried out.
- An analysis of our proposed system regarding the best features extracted for each handwritten digit.
- The new e-BioDigit database, comprising 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[1].

The remainder of the paper is organized as follows. Sec. 2 describes our proposed OTP system including touch biometrics for mobile scenarios. In Sec. 3, we describe the new e-BioDigit database which comprises on-line handwritten numerical digits from 0 to 9. Sec. 4 and 5 describes the

[1] https://atvs.ii.uam.es/atvs/e-BioDigit.html

experimental protocol and results achieved using our proposed approach, respectively. Finally, Sec. 6 draws the final conclusions and points out some lines for future work.

2. Proposed System

In this work we propose an OTP system which includes touch biometrics for mobile scenarios, as shown in Fig. 1. In our proposed approach, users have to perform the handwritten numerical digits (one at a time) of the traditional OTP on the screen to be authenticated. This group of handwritten digits is then compared to the enrolment data of the claimed user comparing one by one each digit. This way the final score is produced after averaging the different one by one digit score comparisons. First, we analyse the case of just using one digit for user verification and then we analyse the discriminative power of the combination of several digits. Only the behavioural information of the user while performing the handwritten digits is analysed in this work making the assumption that impostors pass the first stage of the security system (i.e., they know the password of the attacked users).

2.1. Feature Extraction and Selection

In this work we propose a biometric verification system based on time functions (a.k.a. local system) [19]. 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 1). Information related to pressure, pen angular orientations or pen ups broadly used in other biometric traits such as the handwritten signature is not considered here as this information is not available in universal mobile scenarios using finger touch as input.

Sequential Forward Feature Selection (SFFS) is considered in some of the experiments so as to select subsets of time functions that improve the system performance in terms of EER (%). In addition, SFFS is also used in the experimental work to analyse the discriminative power of digit combinations.

2.2. User Verification

Dynamic Time Warping (DTW) is used to compare the similarity between time functions from handwritten digit samples. Scores are obtained as:

$$\mathit{score} = e^{-D/K} \quad (1)$$

where *D* and *K* represent respectively the minimal accumulated distance and the number of points aligned between two digit samples using the DTW algorithm [10].

Table 1. *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 1-7: $\dot{x_n}, \dot{y_n}, \dot{\theta_n}, \dot{v_n}, \dot{\rho_n}, \dot{a_n}$
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

3. Database e-BioDigit

The new e-BioDigit database was captured in order to perform the experimental work included in this article. This database is comprised of 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 × 800 pixels. Information related to pressure (1024 levels) and pen-ups trajectories are also available when using the pen stylus. However, as this work is focused on universal mobile scenarios, samples were acquired using only the finger as input so only *X* and *Y* spatial coordinates are used.

Regarding the acquisition protocol, data subjects had to perform handwritten numerical digits from 0 to 9 one at a time. Some examples of the handwritten numerical digits acquired for the e-BioDigit database are depicted in Fig. 2. 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 behavioural biometric traits. For each session, users had to perform a total of 4 numerical sequences from 0 to 9. 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. A horizontal line was represented in the bottom part of the rectangular area, including two buttons OK and Cancel to press after writing if the sample was good or bad respectively. If the sample was not good, then it was repeated.

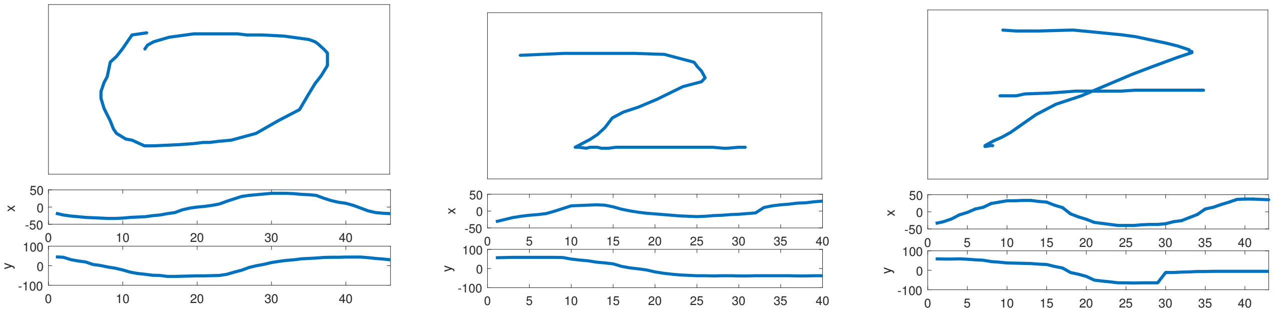


Figure 2. Examples of different handwritten numerical digits of the e-BioDigit database. *X* and *Y* denote horizontal and vertical position versus the time samples.

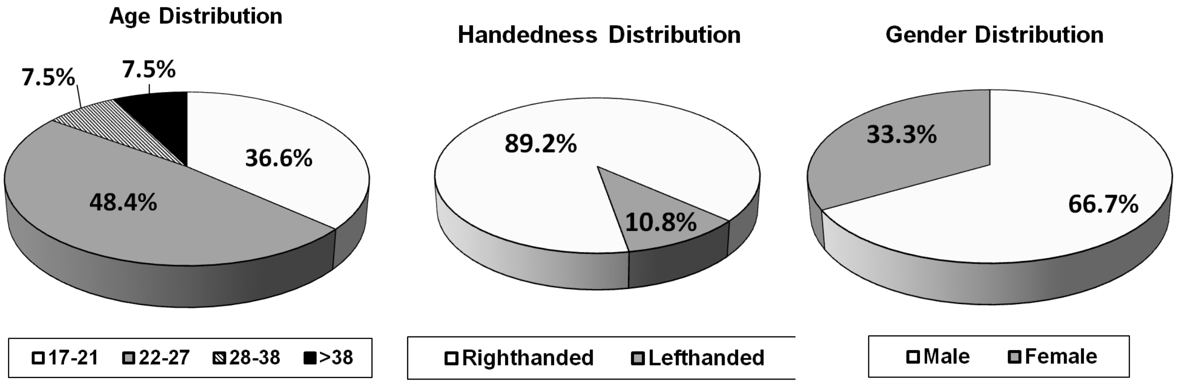


Figure 3. Statistics for the distribution of user population in e-BioDigit database.

The database is comprised of a total of 93 users. Fig. 3 shows the statistics for the distribution of user population in e-BioDigit database. Regarding the age distribution, the majority of the subjects (85.0%) are between 17 and 27 years old, as the database was collected in a university environment. Fig. 3 also shows the handedness and the gender distributions. The gender was designed to be as balanced as possible, having 66.7% of males and 33.3% of females whereas for the handedness distribution, 89.2% of the population was righthanded.

4. Experimental Protocol

The experimental protocol is designed in order to assess the potential of our proposed digit-based biometric verification system in real mobile scenarios. Thus, 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 approach, the SFFS algorithm is applied to each handwritten numerical digit in order to select the most discriminative time functions for each digit. For that, the 4 available genuine samples from the first session are used as enrolment samples, whereas the remaining 4 genuine samples from the second session are used for testing. Impostor scores are obtained by comparing the enrolment samples with one genuine sample of each of the remaining users.

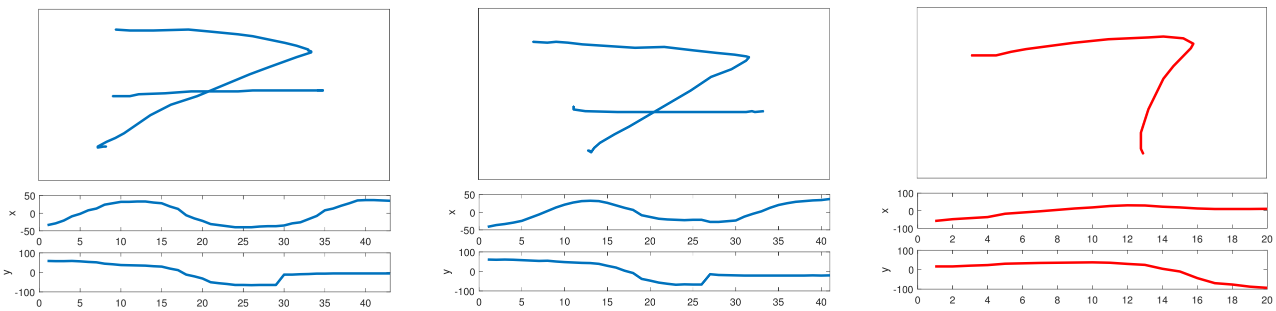
For the evaluation of our proposed approach, the following two scenarios are considered: 1) having just one genuine sample per digit as enrolment (i.e., 1vs1), and 2) performing the average score of four one-to-one comparisons (i.e., 4vs1) when the number of enrolment samples is four genuine digit samples per user. In addition, for both scenarios, in case of using passwords comprised 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 behavioural biometric traits such as the case of the handwritten signature.

5. Experimental Results

5.1. Experiment 1. Baseline System: One-Digit Results

This section analyses the potential of each numerical digit (i.e., from 0 to 9) in terms of EER(%) for the task of user verification. In order to provide an easily reproducible



(a) User A, sample 1

(b) User A, sample 2

(c) User B

Figure 4. Examples of the numerical digit 7 performed for two different users.

Table 2. **Experiment 1: Time functions 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: $\ddot{x_n}, \ddot{y_n}$

framework, we first consider in this section a Baseline System with the same fixed time functions for all numerical digits. Therefore, no development through the use of the SFFS algorithm is considered in this first experiment. Table 2 shows the time functions selected for the Baseline System. We select this set of time functions as baseline as they are commonly used as baseline in other biometric traits such as the handwritten signature [3, 17].

The system performance results in terms of EER(%) obtained for each numerical digit on the evaluation dataset using the Baseline System are depicted in Table 3. Overall, very good verification results are obtained in this first experiment taking into account that only one numerical digit and a Baseline System are considered for verification.

Analysing 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% EER. In addition, other numerical digits such as 4 or 5 achieve similar results below 25.0% EER. This first experiment puts in evidence the different user verification capacity achieved by each numerical digit. Fig. 4 shows examples of the numerical digit 7 performed for two different users in order to see the low intra- and high inter-user variability of this number. This effect is produced because each person tends to perform numerical digits in a different way, i.e., starting from a different stroke of the numerical digit or even removing some of them such as the crossed horizontal stroke of the number 7.

Analysing the scenario of having four digit samples during the enrolment (4vs1), an average absolute improvement of 3.2% EER is achieved compared to the 1vs1 scenario showing the importance of acquiring as much information as possible during the enrolment stage. For this scenario, the digit 4 achieves the best result with 18.0% EER.

5.2. Experiment 2. Proposed System: One-Digit Results

We apply SFFS over the development dataset in order to enhance the biometric verification system through the selection of specific time functions for each numerical digit. Fig. 5 shows the number of times each time function is selected in our Proposed System from the 21 total time functions described in Table 1. In general, we can highlight the importance of x_n, y_n time functions as they are selected for 70% 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 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 samples.

Table 4 shows the results achieved for each digit using our Proposed System over the evaluation dataset. In general, better results are achieved compared to the Baseline System (Table 3). Analysing the 1vs1 scenario, our Proposed System achieves an average absolute improvement of 2.0% EER, being the numerical digit 5 the one that provides the best result with a 21.7% EER. Analysing the 4vs1 scenario, our Proposed System achieves an average absolute improvement of 1.6% EER, being again the numerical digit 5 the one that achieves the best result with a 16.9% EER. These results put in evidence the importance of considering different time functions for each numerical digit in order to develop more robust biometric verification systems based on handwritten digits.

5.3. Experiment 3: Digit Combinations

This section evaluates the robustness of our proposed digit-based biometric verification approach when increasing the number of digits that comprise the user password. Fig.

Table 3. **Experiment 1**: System performance as EER(%) of each numerical digit using the **Baseline System** on the evaluation dataset.

	Numerical Digit									
	0	1	2	3	4	5	6	7	8	9
1vs1 scenario	34.9	32.3	32.8	35.0	23.5	24.4	36.9	**22.5**	26.0	29.6
4vs1 scenario	33.1	28.5	30.2	32.6	**18.0**	20.3	36.6	19.2	22.7	25.0

Table 4. **Experiment 2**: System performance as EER(%) of each numerical digit using the **Proposed System** on the evaluation dataset.

	Numerical Digit									
	0	1	2	3	4	5	6	7	8	9
1vs1 scenario	33.0	34.0	30.9	32.3	22.0	**21.7**	33.6	21.8	21.8	27.0
4vs1 scenario	31.4	33.1	27.9	29.7	19.2	**16.9**	29.7	20.3	18.6	23.3

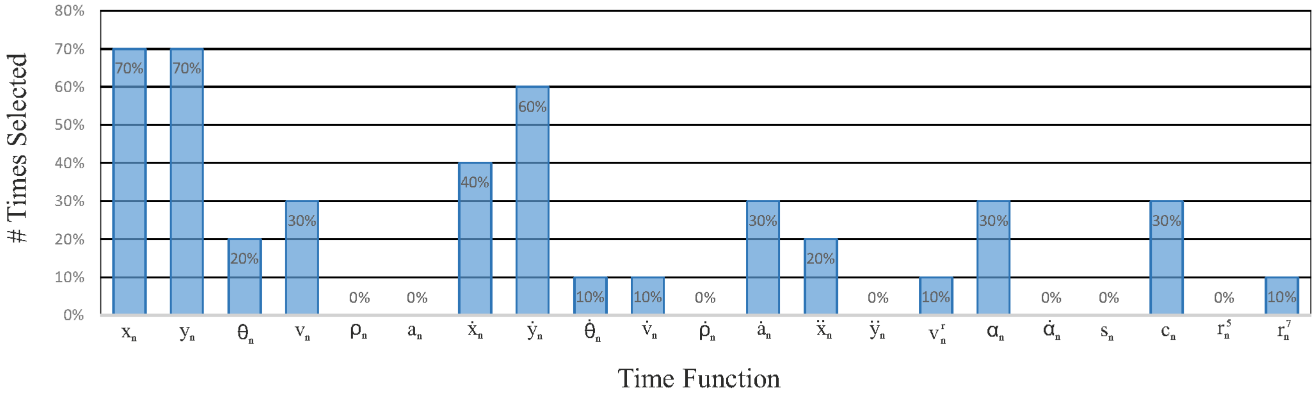


Figure 5. **Experiment 2**: Histogram of functions selected by SFFS for our Proposed System. Functions described in Table 1.

6 shows the evolution of the system performance in terms of EER (%) on the evaluation dataset when increasing the number of handwritten numerical digits of the password.

Analysing the 1vs1 scenario, a considerable improvement of the system performance is achieved when adding more handwritten digits to the password. A password that is comprised of just two handwritten numerical digits achieves a 16.0% EER, an absolute improvement of 5.8% EER compared to the case of using a password with just one handwritten digit. This result is further improved when increasing the number of handwritten digits of the password with a final 9.0% EER for the case of considering a handwritten numerical password of 8 digits.

For the scenario of acquiring 4 genuine samples per digit during the enrolment (i.e., 4vs1), much better results are achieved because the intra-user variability is better modelled. In this case, a password comprised of just two handwritten numerical digits achieves a value of 11.0% EER, an absolute improvement of 7.6% EER compared to the case of using a password with just one handwritten digit.

Our proposed approach is now compared to other existing state-of-the-art biometric verification approaches for mobile scenarios. Information related to the verification method, and verification performance in terms of EER is included in Table 5 for each study.

In general, our proposed approach achieves good results in comparison to other approaches. For the case of lock pattern dynamic systems [1], the best system performance reported was a 10.39% EER whereas for other methods such as the handwritten signature or graphical password [11, 15, 17], results in the range of 20.0% EER were achieved for skilled forgeries. Additionally, our proposed approach has been compared to other state-of-the-art approaches based on handwritten passwords. In [7], the authors proposed the use of handwritten passwords with a fixed length of 8 characters. Regarding the acquisition process, users had to perform all 8 characters at the same time on the screen of a tablet device. For each handwritten password, a total of 25 static and dynamic features were extracted achieving a final False Acceptance Rate (FAR) of 10.42% with a KStar classifier and using a total of 12 training samples per user. However, that approach seems to be only applicable to devices with big screens such as tablet devices but not to smartphones as it would be very difficult for the users to perform such a long password on a much smaller size screen. Our proposed approach achieves a final value of 5.5% EER for skilled forgeries and is able to mitigate the effect commented before about the size of the screen devices as users have to perform numerical digits one at a time. Additionally, only 4 training samples and not 12 are considered in our proposed approach so it would be easier to deploy on real applications.

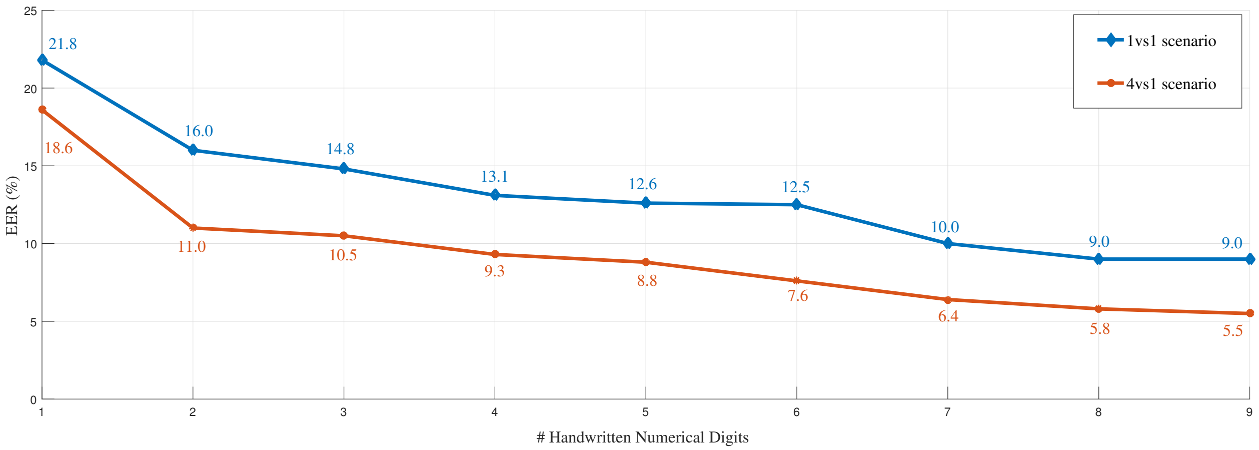


Figure 6. **Experiment 3**: Evolution of the system performance in terms of EER (%) on the evaluation dataset when increasing the number of handwritten numerical digits of the password.

Table 5. Comparison of different finger touch biometrics approaches for mobile scenarios.

Work	Method	Verification Peformance (EER)		Participants
		Random Forgeries	Skilled Forgeries	
Angulo and Wastlund (2011) [1]	Lock Pattern Dynamics	-	10.39% avg.	32
Martinez-Diaz *et al.* (2016) [11]	Graphical Passwords	3.4%	22.1%	100
Sae and Memon (2014) [15]	Handwritten Signatures	5.04%	-	180
Tolosana *et al.* (2017) [17]	Handwritten Signatures	0.5%	17.9%	65

Kutzner *et al.* (2015) [7]	Handwritten Characters	-	FAR = 10.42%
			FRR = unknown
				32

Proposed Approach	**Handwritten Digits**	**-**	**5.5%**	**93**

These results show the benefits of our proposed handwritten digit-based scheme not only in terms of accuracy but also usability for real applications on mobile scenarios.

6. Conclusions

This work evaluates the advantages and potential of incorporating touch biometrics to mobile one-time passwords (OTP). The new e-BioDigit database which has been acquired comprising handwritten numerical digits from 0 to 9 is used in the experiments reported in this work and it will be made publicly available to the research community. Data was collected in two sessions with a time gap of at least three weeks between them for a total of 93 subjects. Handwritten numerical digits were acquired using the finger touch as the writing input on a Samsung Galaxy Note 10.1 general purpose tablet device.

For the new e-BioDigit database, we report a benchmark evaluation using our proposed digit-based system. The following three different experiments are considered: 1) a Baseline System comprised of a set of simple and fixed time functions for all numerical digits in order to make our work easily reproducible; 2) an study of the best features for each handwritten numerical digit through the SFFS algorithm on the development dataset; and 3) an analysis of the OTP system regarding which are the most discriminative handwritten digits and how robust the system is when increasing the number of digits included in the OTP.

Our proposed approach achieves remarkable results with EERs ca. 5.0% when using skilled forgeries, outperforming other traditional biometric verification traits such as the handwritten signature or graphical password on similar mobile scenarios.

Future work will be oriented to investigating how the different discriminative performance shown by individual digits can be exploited to design robust passwords, i.e., the OTP Digit Selection module in Fig. 1. Additionally, the integration of individual digits into a combined biometric decision [4] is subject of further investigation, i.e., the Biometric Comparison module in Fig. 1. The core matcher in that module can be also improved following recent advances from the machine learning community exploiting deep learning for on-line handwriting biometrics [18, 20].

Acknowledgments

This work has been supported by project TEC2015-70627-R MINECO/FEDER and by UAM-CecaBank Project. Ruben Tolosana is supported by a FPU Fellowship from Spanish MECD.

References

[1] J. Angulo and E. Wastlund. Exploring Touch-Screen Biometrics for User Identification on Smart Phones. *J. Camenisch, B. Crispo, S. Fischer-Hbner, R. Leenes, G. Russello (Eds.), Privacy and Identity Management for Life, Springer*, pages 130–143, 2011. 2, 6, 7

[2] M. Antal and A. Bandi. Finger or Stylus: Their Impact on the Performance of On-line Signature Verification Systems. In *Proc. of the 5th International Conference on Recent Achievements in Mechatronics, Automation, Computer Sciences and Robotics*, 2017. 1

[3] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, and J. Liu-Jimenez. Performance Evaluation of Handwritten Signature Recognition in Mobile Environments. *IET Biometrics*, 3:139–146, 2014. 5

[4] J. Fierrez, A. Morales, R. Vera-Rodriguez, and D. Camacho. Multiple Classifiers in Biometrics. Part 2: Trends and Challenges. *Information Fusion*, 44:103–112, 2018. 7

[5] J. Fierrez and J. Ortega-Garcia. On-line signature verification. *A.K. Jain, A. Ross and P.Flynn (Eds.), Handbook of Biometrics, Springer*, pages 189–209, 2008. 1

[6] J. Jenkins, J. Shelton, and K. Roy. One-Time Password for Biometric Systems: Disposable Feature Templates. In *Proc. SoutheastCon*, 2017. 2

[7] T. Kutzner, F. Ye, I. Bonninger, C. Travieso, M. Dutta, and A. Singh. User Verification Using Safe Handwritten Passwords on Smartphones. In *Proc. 8th International Conference on Contemporary Computing, IC3*, 2015. 6, 7

[8] P. Lacharme and C. Rosenberger. Synchronous One Time Biometrics With Pattern Based Authentication. In *Proc. 11th Int. Conf. on Availability, Reliability and Security, ARES*, 2016. 2

[9] A. Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. Touch Me Once and I Know Its You! Implicit Authentication based on Touch Screen Patterns. In *Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, pages 987–996, 2012. 2

[10] M. Martinez-Diaz, J. Fierrez and S. Hangai. Signature Matching. *S.Z. Li and A. Jain (Eds.), Encyclopedia of Biometrics, Springer*, pages 1382–1387, 2015. 3

[11] M. Martinez-Diaz, J. Fierrez, and J. Galbally. Graphical Password-based User Authentication with Free-Form Doodles. *IEEE Trans. on Human-Machine Systems*, 46(4):607–614, 2016. 1, 6, 7

[12] W. Meng, D. Wong, S. Furnell, and J. Zhou. Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys Tutorials*, 17(3):1268–1293, 2015. 1

[13] R. Plamondon and S. Srihari. Online and Off-Line Handwriting Recognition: a Comprehensive Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22:63–84, 2000. 1

[14] R. Plamondon, G. Pirlo and D. Impedovo. Online Signature Verification. *D. Doermann and K. Tombre (Eds.), Handbook of Document Image Processing and Recognition, Springer*, pages 917–947, 2014. 1

[15] N. Sae-Bae and N. Memon. Online Signature Verification on Mobile Devices. *IEEE Transactions on Information Forensics and Security*, 9(6):933–947, 2014. 1, 6, 7

[16] M. Salehan and A. Negahban. Social Networking on Smartphones: When Mobile Phones Become Addictive. *Computers in Human Behavior*, 29(6):2632–2639, 2013. 1

[17] 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*, 2017. 1, 5, 6, 7

[18] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia. Exploring Recurrent Neural Networks for On-Line Handwritten Signature Biometrics. *IEEE Access*, 6:5128–5138, 2018. 1, 7

[19] 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*, 3:478 – 489, 2015. 3

[20] X. Zhang, G. Xie, C. Liu, and Y. Bengio. End-to-End Online Writer Identification With Recurrent Neural Network. *IEEE Transactions on Human-Machine Systems*, 47:103–112, 2017. 7