MobileTouchDB: Mobile Touch Character Database in the Wild and Biometric Benchmark

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

Abstract

In this paper, we introduce a new database of mobile touch on-line data named MobileTouchDB. The database contains more than 64K on-line character samples performed by 217 users, using 94 different smartphone models, with an average of 314 samples per user. In each acquisition session, users had to draw all numbers (from 0 to 9), upper- and lower-case letters (54), different symbols (8), and passwords composed of 4 numbers (6). Regarding the acquisition protocol, MobileTouchDB comprises a maximum of 6 captured sessions per subject with a time gap between them of at least 2 days. This database studies an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices. Users downloaded and used the acquisition app on their own devices freely. In addition, we also report a benchmark evaluation of biometric authentication on MobileTouchDB, providing an easily reproducible framework for two different scenarios of biometric user authentication: i) based on one character, and ii) based on character combinations.

The database was collected with three main goals in mind: i) analyse the discriminative power of novel human touch interaction dynamics, ii) enhance traditional password authentication systems through the incorporation of touch biometric information as a second level of user authentication, and iii) analyse the way we interact with mobile devices on a daily basis in order to enhance continuous authentication systems. MobileTouchDB is publicly available in GitHub[1].

1. Introduction

Passwords are still the most common way to authenticate users nowadays. They can range from Personal Identification Numbers (PIN) that require users to memorise them to One-Time Passwords (OTP) where the security system is in charge of selecting and providing to the user a different password each time it is required, e.g., sending messages to personal mobile devices or special tokens. We use passwords on a daily basis for all kinds of applications. However, are passwords secure enough? Apparently not, at least by themselves. Recent news put in evidence this fact, e.g., in January 2019 a total of 21 million passwords from all parts of the world were released together with their corresponding emails addresses [12]. This important problem is related not only to data breaches, but also to other many attack scenarios, as it has been pointed out in different studies [6, 10]. First, it is common to use passwords based on sequential digits (e.g., *"1 2 3 4 5 6"*), personal information such as birth dates, or simply words such as *"password"* or *"qwerty"* that are very easy to guess [20]. 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 by the impostors to guess lock patterns or passwords [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 [19, 29]. So, if we know that traditional passwords are not secure enough by themselves, but they continue to be present in our lives, how can we improve this type of authentication?

In this study we introduce the novel MobileTouchDB database and analyse the potential of incorporating touch biometrics to password authentication systems, asking the users to draw each digit of the password on the touchscreen instead of typing them as usual. One example of use that motivates our proposed approach is on internet payments with credit cards. Banks usually send a password (typically between 6 and 8 digits) to the user. This password must be inserted by the user in the security platform in order to com-

[1] https://github.com/BiDAlab/MobileTouchDB

Table 1: Most relevant features of touch biometric public databases.

Database	Method	# Users	# Sessions	Acquisition Time	# Devices
Serwadda [18]	Swipe	190	2	$\geq$ 1 Day	1
Frank [9]	Swipe	41	2	1 Week	4
Antal [3]	Swipe	71	-	4 Weeks	8
UMDAA-02 [14]	Swipe	48	248	1 Week	1
DooDB [15]	Graphical Passwords	100	2	2 Weeks	1
e-BioDigit [21, 24]	Handwritten Numbers	93	2	3 Weeks	1
MobileTouchDB	**Handwritten Characters**	**217**	**6**	**$\geq$ 3 Weeks**	**94**

plete the payment. Our proposed approach enhances such scenario by including a second authentication factor based on the user biometric information while drawing the digits.

The main contributions of this study can be summarised as follows:

- We present and describe the acquisition process of the new MobileTouchDB database. The database contains more than 64K on-line character samples performed by 217 users, using 94 different smartphone models, with an average of 314 samples per user. In each acquisition session, users had to draw all numbers (from 0 to 9), upper- and lower-case letters (54), different symbols (8), and passwords composed of 4 numbers (6). Regarding the acquisition protocol, MobileTouchDB comprises a maximum of 6 captured sessions per subject with a total time gap of at least 3 weeks. This database studies an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices. Users downloaded and used the acquisition app on their own devices freely. MobileTouchDB is publicly available in GitHub.

- We report a benchmark evaluation of biometric authentication on the novel MobileTouchDB database, providing an easily reproducible framework. Two different experiments have been carried out: *i)* one-character analysis in order to evaluate the discriminative power of each character, and *ii)* character combination analysis so as to measure the robustness of our proposed approach when increasing the length of the passwords from 1 to 9 characters.

- The MobileTouchDB database opens the doors to many different applications: *i)* analyse the discriminative power of novel human touch interaction dynamics, *ii)* enhance traditional password authentication systems through the incorporation of touch biometric information as a second level of user authentication, and *iii)* analyse the way we interact with mobile devices on a daily basis in order to enhance continuous authentication systems.

MobileTouchDB can be also useful for other research lines beyond touchscreen biometric authentication, e.g.: *i)* user-dependent effects [28], and development of user-dependent methods [7] for handwriting recognition, *ii)* the neuromotor processes involved in writing over touchscreens [13, 27], *iii)* sensing factors in obtaining representative [26] and clean [2] touch interaction signals, *iv)* human-device interaction factors [11] involving touchscreen signals [8], and development of improved interaction methods, and *v)* population statistics around touch interaction signals, and development of new methods aimed at recognising or serving particular population groups [1].

The remainder of the paper is organised as follows. Sec. II summarises public databases in touch biometrics for mobile scenarios. Sec. III describes the design and acquisition process of the MobileTouchDB database. Sec. IV describes the experimental protocol, and the benchmark evaluation carried out. Finally, Sec. V draws the final conclusions and points out some lines for future work.

2. Related Work

The design and acquisition of new databases is always a complex process that requires many efforts for both developers/supervisors and subjects. Not only because of the acquisition process but also due to all the legal aspects that must be carefully tackled to publicly release the data to the research community. Table 1 summarises the most relevant features of different touch biometric public databases.

In [18], the authors acquired a database composed of 190 subjects for the analysis of swipe gestures. Two applications were developed for data collection, running on Android and using one device model (Google Nexus S). In these applications, multiple choice questions were asked based on the images/texts one had to browse/read. Free interaction with the device was allowed, permitting both landscape and portrait orientation. Data were captured over two sessions, at least one day apart, recording the X and Y coordinates, the timestamp, the area covered by the finger, the pressure on the screen, and the device orientation. Only gestures obtained by swiping one finger on the screen were recorded. Multi-touch gestures, e.g. zooms, were ignored.

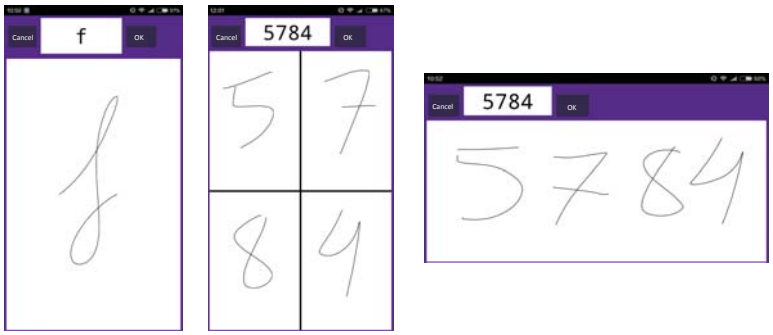


Figure 1: Different interfaces designed for the acquisition app. Both portrait and landscape orientations are considered in order to analyse different user experiences while drawing.

Fran *et al.* acquired in [9] a new database composed of swiping data generated by 41 users over two sessions, one week apart. Two Android applications were deployed for data acquisition, one for comparing images and another for reading texts, allowing the subject to move and interact freely with the screen. Both phone orientations were allowed. Multiple devices (operating on Android) with different sampling frequencies were employed, recording for each data point the X and Y coordinates, the timestamp, the area covered by the finger, the pressure, and the device orientation.

In [3], the authors acquired a new database composed of 71 users. For the acquisition process, eight different devices were used, including tablets with varying screen sizes. An application was developed for the acquisition, where subjects had to read texts, which required vertical swipes, and choose their favourite picture, which required horizontal swipes. The data were obtained during 4 weeks (not separated in sessions in the database), where each subject interacted with multiple devices, recording for each data point the same information as in the previous databases and allowing both phone orientations.

In [14], the authors introduced the UMDAA-02 database, which contains samples from 48 volunteers captured using Nexus 5 phones over two months. On the contrary to the other databases, free use of the devices was allowed during these two months, without requiring any concrete task to be performed. Thus, more data from each user are present. They divided the data in sessions from the unlocking of the device until it was locked again.

Touch biometrics has also been studied in other tasks, e.g., while drawing doodles or numbers [15, 21, 24]. In [15], the authors presented the DooDB, a doodle database containing data from 100 users captured with an HTC Touch HD mobile phone. Doodles were acquired in two different sessions, separated by an average period of two weeks. Finally, more related to the database presented here, we released in [21, 24] the e-BioDigit database composed of 93 users. During the acquisition process, users were asked to draw numerical digits from 0 to 9 on a Samsung Galaxy Note 10.1 tablet in two different sessions with a time gap of at least three weeks between them.

The MobileTouchDB database presented here allows to better analyse the discriminative power of novel human touch interaction dynamics as users had to perform 72 different characters and symbols. Additionally, it considers an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices as users downloaded and used the acquisition app on their own devices freely, simulating this way real scenarios.

3. MobileTouchDB Description

MobileTouchDB is a novel handwritten character mobile touch biometric database composed of more than 64K on-line character samples performed by 217 users. For the acquisition, we implemented an Android application. Fig. 1 represents the different interfaces designed for the acquisition. All interfaces are composed of: *i)* the character/password to draw (top, middle) and two buttons "OK" (top, right) and "Cancel" (top, left) to press after drawing if the sample was good or bad respectively. If the sample was not good, then it was repeated. And *ii)* a rectangular area to perform the character or password. In order to study an unsupervised mobile scenario, the acquisition app was uploaded to the Google Play Store. This way all participants could download and use the app on their own devices without any kind of supervision, simulating a practical scenario in which users can generate handwritten information in any possible scenario, e.g., standing, sitting, walking, indoors, outdoors, etc. As a result, 94 different models from the following 16 brands were used during the acquisition: *Alcatel, Blackberry, BQ, Coolpad, Doogee, Google, Huawei, LeTV, LG, Motorola, OnePlus, Samsung, Sony, UMIDIGI, Xiaomi, and ZTE*. The acquisition app was designed to cap-

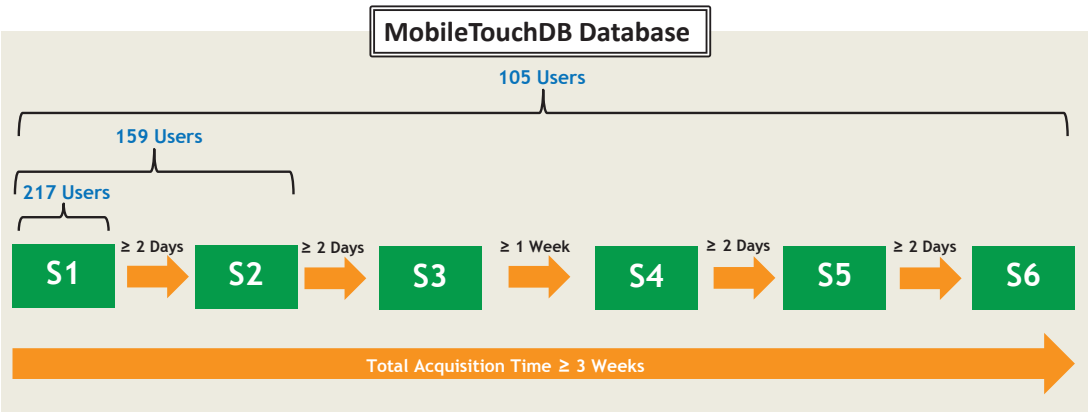


Figure 2: Description of the design and number of available users of the new MobileTouchDB database.

ture the following time signals: X and Y spatial coordinates, the area covered by the finger, timestamp, accelerometer, and gyroscope. However, information related to the area covered by the finger, accelerometer, and gyroscope was not available in some cases depending on how old the acquisition device was.

The acquisition protocol considered in the MobileTouchDB database is depicted in Fig. 2. It comprises a total of 6 sessions (i.e., S1-S6) with different time gaps among them. It is important to highlight that in all sessions, the time gap refers to the minimum time between one user finishes a session and the following session is available. However, participants usually performed their corresponding sessions later on thanks to notifications sent automatically by the acquisition app to the users. Regarding the data acquired, each session comprises 8 different capturing blocks (i.e., from Block1 to Block8). Fig. 3 shows some examples of each of the eight acquisition blocks for two different users (indicated in blue and red colours). The green dashed lines indicate pen up trajectories between strokes. In Block1, we asked users to draw all numbers (from 0 to 9). Block2 and Block3 comprise upper- and lower-case letters respectively, with a total of 27 letters each. Block4 is composed of 8 different symbols (i.e., *"?"*, *"#"*, *"*"*, *"@"*, *"%"*, *"="*, *"ϵ"*, *and "α"*). It is important to remark that inside each block, characters were randomised before asking users to draw them. This way, each user performs a different character sequence in each session. From Block1 to Block4, the acquisition interface was designed as portrait to provide a better user experience (see Fig. 1, left). After finishing the first 4 blocks focused on performing one single character at a time (one sample per character), we asked users to draw passwords composed of 4 numbers (always *"5 7 8 4"*) in different ways (6 samples in total). In Block5, users performed the password twice using a landscape orientation interface (see Fig. 1, right). We provided the users with a graphical visualization of the numbers while drawing them (i.e., visible mode). Then, in Block6, users had to repeat once the same task considered in Block5 but this time in an invisible mode, i.e., we did not provide to the users any visualization of the numbers while drawing them. The main motivation of this novel acquisition scenario is to protect us against shoulder surfing attacks, as commented in [17]. In Block 7, users had to draw each number of the password inside of each of the four available boxes (two times), considering first a visible mode (see Fig. 1, middle). Finally, in Block8 users had to repeat once the same task considered in Block7 but this time in an invisible mode. In both Block7 and Block8 the acquisition interface was kept portrait to analyse the user experience in different settings.

Regarding the MobileTouchDB population statistics, 217 users completed the S1 acquisition session. S1 and S2 were completed by 159 users. Finally, a total of 105 users completed the six acquisition sessions. This participant reduction between S1 and S6 sessions is produced due to the challenging acquisition scenario considered in this study as it was completely unsupervised and comprised several acquisition sessions along time. Regarding the age distribution, 36.2% of the participants are younger than 22 years old, 31.9% are between 22 and 27 years old, and the remaining 31.9% are older than 27 years old. Regarding the gender, 63% of the participants were males, and 37% females. 96% of the population was righthanded.

4. MobileTouchDB Benchmark

This section reports the benchmark evaluation carried out for the MobileTouchDB database, providing an easily reproducible framework. Sec. 4.1 describes all the details of the experimental protocol considered. Then, Sec. 4.2 describes the touch biometric baseline system used in the

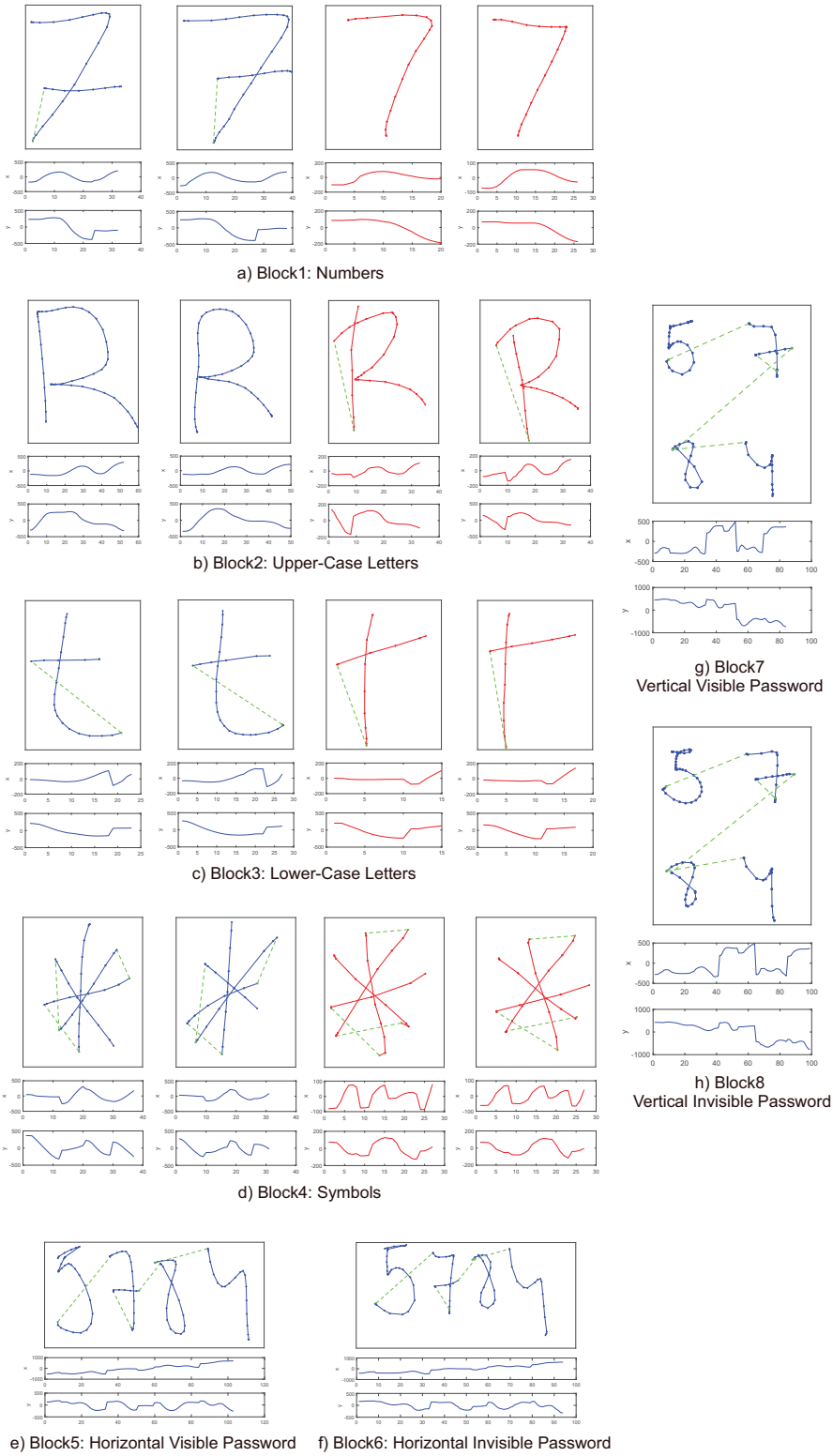


Figure 3: Example of the data collected in MobileTouchDB database. Blue and red colours represent samples drawn by different users. The green dashed lines indicate pen up trajectories between strokes. Curves under each character represent X and Y trajectories over time.

benchmark evaluation. Finally, we analyse in Sec. 4.3 and 4.4 the results obtained for the one-character and character combination scenarios.

4.1. Experimental Protocol

The experimental protocol is designed in order to assess the potential of our proposed password touch biometric approach in practical scenarios. Two different experiments are considered: *i)* one-character analysis in order to evaluate the discriminative power of each character, and *ii)* character combination analysis so as to measure the robustness of our proposed approach when increasing the length of the passwords from 1 to 9 characters. Due to the large amount of information acquired in MobileTouchDB, in this paper we focus on characters performed one at a time. Complete passwords acquired in Block5 to Block8 will be analysed in future studies.

Genuine scores are obtained using the set of 159 users with the S1 and S2 acquisition sessions completed. The S1 sample is always used as training sample whereas the S2 sample is considered for testing. This way we consider the inter-session variability problem as genuine samples from different acquisition sessions are used as enrolment and testing samples respectively. This effect has proven to be very important in many behavioural biometric traits such as the handwritten signature [25], as it can better simulate a real scenario.

For the impostor scenario, we consider all 217 users with the S1 acquisition session completed. Impostor scores are obtained by comparing the training samples from S1 with one sample of each of the remaining users (assuming that the impostor knows the password).

Finally, for the character combination analysis, the final score is produced by fusing the different one by one character score comparisons using the sum of the scores.

4.2. Baseline System

In order to provide an easily reproducible framework, we consider a baseline system based on Dynamic Time Warping (DTW) with the same fixed time functions for all characters. This system is commonly used as baseline in other biometric traits such as the handwritten signature [5, 22]. For each character, we extract the X and Y coordinates over time and their first- and second-order derivatives, ending up with a set of 6 time functions. For the matcher, DTW is used to compare the similarity between genuine and query input samples, finding the optimal elastic match among time sequences that minimises 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 [16].

4.3. One-Character Analysis

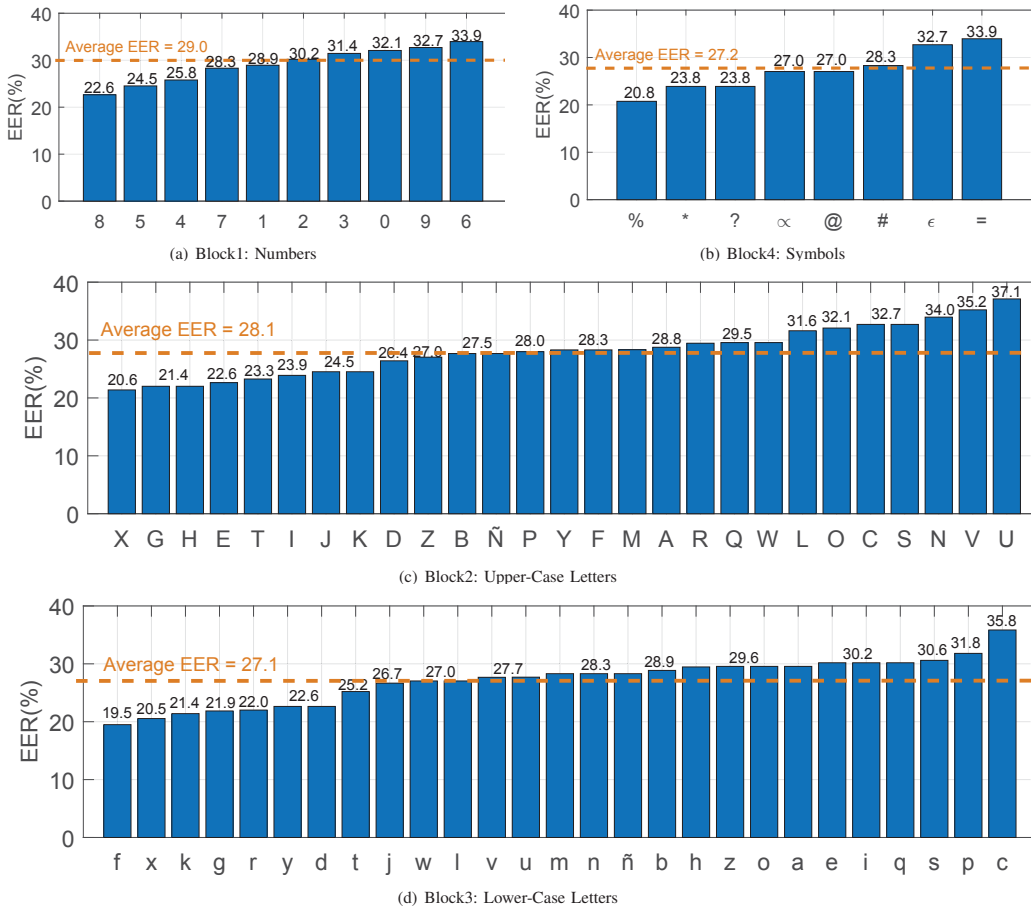
This section analyses the potential of each individual character for the task of user authentication. Fig. 4 shows the system performance of each character, grouped according to their corresponding acquisition block, and from lower to higher EERs.

We first analyse in Fig. 4(a) the system performance when drawing numbers. Number *"8"* achieves the best system performance with a 22.6% EER, an absolute improvement of 11.3% EER compared to number *"6"*, which has resulted to be the least discriminative number. This first experiment puts in evidence the different user verification capacity achieved by each number. Fig. 3 shows examples of the number *"7"* performed by 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 characters in a different way, i.e., starting from a different stroke or even removing some of them such as the crossed horizontal stroke of the number *"7"*.

Symbols are shown to be very discriminative as well. Fig. 4(b) depicts the EER achieved for each of them. In general, symbols provide an average 27.2% EER, an absolute improvement of 1.8% EER compared to numbers, achieving therefore a higher discriminative capacity against impostors. We believe this improvement is produced due to symbols such as "%" and "*" are composed of more strokes, providing a higher inter-user variability. Fig. 3 shows examples of the symbol "*" performed by two different users. As it can be seen, users tend to perform symbols in a different way, e.g., starting and finishing in different strokes.

We now compare the results of both upper- and lower-case letters in Fig. 4(c) and (d). Analysing the average EER, lower-case letters provide an absolute improvement of 1.0% EER compared to the upper-case letters, proving the higher discriminative power of lower-case letters. We believe this is produced because most upper-case letters are based on simple straight strokes, and not in curved strokes, providing therefore less variability among users. In addition, we usually write using lower-case letters, adapting our original writing model to more user-specific features compared to upper-case letters. One example that justifies our hypothesis is letter *"f/F"*. In Fig. 4(d), letter *"f"* provides the best result with a 19.5% EER. However, in Fig. 4(c), the EER increases up to 28.3% when using letter *"F"*. Similar conclusions are applied to other letters such as *"r/R"* and *"y/Y"*. However, there are some cases where both upper- and lower-case letters obtain very similar results, such as letters *"x/X"* and *"g/G"* with results below 22.0% EER.

In general, good authentication results are obtained taking into account that we consider a baseline system based on a simple and fixed set of time functions for all characters. Regarding the discriminative power of each character, a high variability is produced among them, e.g., there is an



(a) Block1: Numbers

(b) Block4: Symbols

(c) Block2: Upper-Case Letters

(d) Block3: Lower-Case Letters

Figure 4: System performance as EER(%) of each individual character. (a) Block1: Numbers. (b) Block4: Symbols. (c) Block2: Upper-Case Letters. (d) Block3: Lower-Case Letters.

absolute improvement of 17.6% EER between the *"f"* letter in Fig. 4(d) and the *"U"* letter in Fig. 4(c).

4.4. Character Combinations

This section evaluates the robustness of our touch biometric approach when increasing the length of the password. Fig. 5 shows the evolution of the system performance in terms of EER (%) when increasing the length of the password. Passwords are created following the results extracted in the one-character analysis of Sec. 4.3, including the top ranked most discriminative characters at a time, e.g., the *"f"* and *"x"* letters are used for a two-character password.

Analysing the results obtained in Fig. 5, a considerable system performance improvement is achieved when increasing the length of the password. A password composed of just two characters achieves a 16.4% EER, an absolute improvement of 3.1% EER compared to the case of using a password with just a single character. This result is further improved when increasing the length of the password from 1 to 9 characters, achieving a final 5.9% EER, an absolute improvement of 13.6% EER compared to the case of using a single character.

Table 2: Comparison of different handwritten character mobile touch approaches on public databases.

Work	Training Samples	Password Legth	Performance (EER)
e-BioDigit database [24]	1	9	9.0%
Proposed Approach	**1**	**9**	**5.9%**

Our proposed approach is now compared to the e-BioDigit public database presented in [21, 24]. Information related to the number of training samples considered per user, length of the password, and verification performance in terms of EER is included in Table 2 for completeness. The work presented here has further improved previous studies. In [21, 24], we analysed the discrimina-

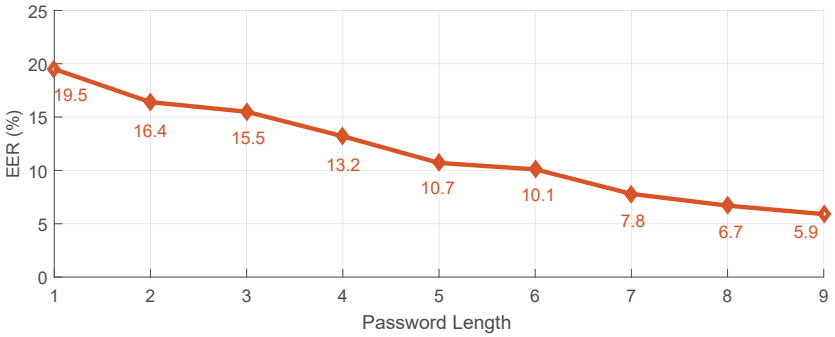


Figure 5: Evolution of the system performance in terms of EER (%) when increasing the length of the password.

Table 3: System performance as EER(%) of five top 10 common passwords of 2018 using our proposed touch biometric approach.

Password	EER (%)
123456	17.0
password	13.2
sunshine	12.1
qwerty	12.1
iloveyou	11.3

tive power of numbers acquired through a Samsung Galaxy Note 10.1 tablet in a supervised scenario. The best system performance achieved in [24] was 9.0% EER. In the present study, this result has been further improved, achieving a final 5.9% EER under more practical experimental conditions (unsupervised scenario with 94 different smartphone models). This result proves the higher discriminative power of characters and symbols for the task of user authentication as in [21, 24] only numbers were considered whereas in the present study, no numbers are included in the best password combinations (i.e., *"f x X % k G H g r"*).

Finally, Table 3 shows the system performance in terms of EER(%) for some of the most common passwords of 2018 [20]. It is important to remark the impostor scenario considered as the attackers know the password. Results between 11-17% EER are obtained in this study when including a second authentication stage based on the touch biometric information of the users. These results encourage the deployment of our proposed approach in comparison to traditional systems where the attack would have 100% success rate under the same impostor scenario.

5. Conclusion

In this paper, we have introduced a new database of mobile touch on-line data named MobileTouchDB. The database contains more than 64K on-line character samples performed by 217 users, using 94 different smartphone models, with an average of 314 samples per user. In each acquisition session, users had to draw all numbers (from 0 to 9), upper- and lower-case letters (54), different symbols (8), and passwords composed of 4 numbers (6). Regarding the acquisition protocol, MobileTouchDB comprises a maximum of 6 captured sessions per subject. This database studies an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices. Users had to download and use the acquisition app on their own devices freely. MobileTouchDB is publicly available in GitHub[2].

In this study we have reported a benchmark evaluation of the novel MobileTouchDB database. Two different experiments have been carried out: *i)* one-character analysis, and *ii)* character combination analysis. Our proposed approach has been compared to the e-BioDigit public database presented in [21, 24], achieving a final 3.1% EER absolute improvement under more practical experimental conditions (unsupervised scenario with 94 different smartphone models), proving the higher discriminative power of characters and symbols for the task of user authentication.

For future work, we expect to further reduce the EER through more advanced techniques based on deep learning [23]. Additionally, we will study the discriminative power of new features acquired in the database such as the area covered by the finger, accelerometer, and gyroscope. Finally, we will also analyse the user experience in different acquisition settings through the analysis of the information acquired from Block5 to Block8 of the MobileTouchDB.

Acknowledgments

This work has been supported by projects: BIBECA (MINECO), 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/MobileTouchDB

References

[1] A. Acien, A. Morales, J. Fierrez, R. Vera-Rodriguez, and J. Hernandez-Ortega. Active Detection of Age Groups Based on Touch Interaction. *IET Biometrics*, 8:101–108, 2019. 2

[2] F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia. Quality Measures in Biometric Systems. *IEEE Security and Privacy*, 10(9):52–62, 2012. 2

[3] M. Antal, Z. Bokor, and L. Szabó. Information Revealed From Scrolling Interactions on Mobile Devices. *Pattern Recognition Letters*, 56:7–13, 2015. 2, 3

[4] A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith. Smudge Attacks on Smartphone Touch Screens. In *Proc. of the 4th USENIX Conference on Offensive Technologies*, pages 1–7, 2010. 1

[5] 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. 6

[6] 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. Symp. on Security and Privacy*, pages 553–567, 2012. 1

[7] 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. 2

[8] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales. Benchmarking Touchscreen Biometrics for Mobile Authentication. *IEEE Trans. on Information Forensics and Security*, 13(11):2720–2733, 2018. 2

[9] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication. *IEEE Transactions on Information Forensics and Security*, 8(1):136–148, 2013. 2, 3

[10] J. Galbally, I. Coisel, and I. Sanchez. A New Multimodal Approach for Password Strength Estimation Part I: Theory and Algorithms. *IEEE Transactions on Information Forensics and Security*, 12:2829–2844, 2017. 1

[11] M. Harbach, A. Luca, and S. Egelman. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proc. Conference on Human Factors in Computing Systems*, pages 4806–4817, 2016. 2

[12] T. Hunt. *The 773 Million Record "Collection #1" Data Breach*, 2019. 1

[13] M.A. Ferrer, M. Diaz, C.A. Carmona, and R. Plamondon. iDeLog: Iterative Dual Spatial and Kinematic Extraction of Sigma-Lognormal Parameters. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2018. 2

[14] U. Mahbub, S. Sarkar, V. Patel, and R. Chellappa. Active User Authentication for Smartphones: A Challenge Data Set and Benchmark Results. In *Proc. Int. Conf. on Biometrics Theory, Applications and Systems*, 2016. 2, 3

[15] M. Martinez-Diaz, J. Fierrez, and J. Galbally. The DooDB Graphical Password Database: Data Analysis and Benchmark Results. *IEEE Access*, 1:596–605, 2013. 2, 3

[16] 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. 6

[17] T. Nguyen, N. Sae-Bae, and N. Memon. DRAW-A-PIN: Authentication Using Finger-Drawn PIN on Touch Devices. *Computers & Security*, 66:115–128, 2017. 4

[18] A. Serwadda, V. Phoha, and Z. Wang. Which Verifiers Work?: A Benchmark Evaluation of Touch-Based Authentication Algorithms. In *Proc. International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 1–8, 2013. 2

[19] D. Shukla, R. Kumar, A. Serwadda, and V. Phoha. Beware, Your Hands Reveal Your Secrets! In *Proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014. 1

[20] SplashData. *The Top 50 Worst Passwords of 2018*. 1, 8

[21] R. Tolosana, R. Vera-Rodriguez, and J. Fierrez. BioTouchPass: Handwritten Passwords for Touchscreen Biometrics. *IEEE Transactions on Mobile Computing*, 2019. 2, 3, 7, 8

[22] 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. 6

[23] 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. 8

[24] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia. Incorporating Touch Biometrics to Mobile One-Time Passwords: Exploration of Digits. In *Proc. Conference on Computer Vision and Pattern Recognition Workshops*, pages 471–478, 2018. 2, 3, 7, 8

[25] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia. Reducing the Template Aging Effect in On-Line Signature Biometrics. *IET Biometrics*, 2019. 6

[26] 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. 2

[27] R. Vera-Rodriguez, R. Tolosana, and *et al.* Modeling the Complexity of Signature and Touch-Screen Biometrics using the Lognormality Principle. *R. Plamondon, A. Marcelli, and M.A. Ferrer (Eds.), The Lognormality Principle and its Applications, World Scientific*, 2019. 2

[28] N. Yager and T. Dunstone. The Biometric Menagerie. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(2):220–230, 2010. 2

[29] Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu, and W. Zhao. My Google Glass Sees Your Passwords! In *Black Hat USA*, 2014. 1