Image and Vision Computing xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Image and Vision Computing

journal homepage: www.elsevier.com/locate/imavis

Position paper

Signature analysis in the context of mobile devices☆

Raul Sanchez-Reillo

University Group for Identification Technologies, Carlos III University of Madrid, Avda. Universidad, 30, Leganes, Madrid E-28911, Spain

ARTICLE INFO

Article history:
Received 31 January 2016
Accepted 29 March 2016
Available online xxxx

Keywords:
Handwritten signature
Biometrics
Static signature recognition
Dynamic signature recognition
Forgeries
User confidence

ABSTRACT

Handwritten signature is one of the oldest means of the human being to both authenticate him/herself and state that a certain document has been understood and accepted. In the modern world, this biometric modality was translated to the use of peripheral pads that allow the signature to be performed by the user. However, in the recent years, the proliferation of mobile devices with touch screens has paved the path to deploy this biometric modality beyond the limits of a desktop. Bringing this biometric modality to mobile devices open several challenges, being some of them already covered, but some others needing further study. This paper provides an overview of these challenges and point to future research works that can help to the continuous deployment of this biometric modality.

1. Introduction

From the so-called behavioural modalities in biometrics, handwritten signature is gaining much attention recently. One of the reasons for such interest is the deployment of devices that, intrinsically, can capture handwritten data, such as touch screens. However, such proliferation of the technology may not necessarily mean an improvement in the performance, although it is, for sure, a magnificent opportunity to popularize this biometric modality. Laptop computers, tablets, and smartphones are currently in the hands of any kind of user. Furthermore, companies have seen in this new technologies the opportunity to avoid paper handling in actions such as credit card payments or parcel delivery, saving huge amount of money in expenses. However, some clarity shall be provided as well as focus on further research to be done in order to improve the current state of the art.

The first thing to clarify is that under the term of handwritten signature biometrics, there are two different modalities involved [1]: (a) static signature (also called off-line signature), which is simply based on the graph generated after signing, such as the information obtained when scanning a page with a signature already written, and (b) dynamic signature (also called on-line signature), which is based on the set of temporal signals generated while the signature is being written, such as horizontal and vertical movements, pressure, etc. Each of these modalities has its own characteristics and challenges. Static signature is currently the most deployed one (used in card payments and couriers), not really used as a biometric modality but only as a means to save on paper handling (i.e., no comparison is made when the signature is performed as the only interest is to store the graph with the acceptance document). Several studies have demonstrated that, when used as a biometric modality, static signature presents low performance and little robustness against fraud, unless taken under the analysis of a human expert. Dynamic signature has shown to be a much better solution for automatic verification, including larger robustness against forgeries when being used by a machine [2].

Most of the studies that have given such conclusions were working with desktop devices specialized in digitalizing the act of signing. However, bringing the technology to the use of current mobile devices takes further considerations to be studied, in particular related with user interaction and technology dependence. Therefore, this paper will place these two biometric modalities in the context of mobile devices, analyzing the recent advances and studying the challenges to be faced. Thus, the following section gives an overview of the main challenges that biometric systems (in general) have to face when being migrated to this new world. Then Section 3 will focus on the challenges that handwritten signature biometrics is facing, to end with a set of conclusions in Section 4.

2. Main challenges when merging biometrics and mobile devices

Migrating biometrics to mobile devices is not a straightforward process. There are several constraints that can drive the biometric solution to fail or, at least, to underperform. This is a common problem to all biometric modalities, although the impact may differ from one to another. This section covers briefly the most important challenges.

☆ This paper has been recommended for acceptance by Sinisa Todorovic, PhD.

E-mail address: rsreillo@ing.uc3m.es.

http://dx.doi.org/10.1016/j.imavis.2016.03.011
0262-8856/

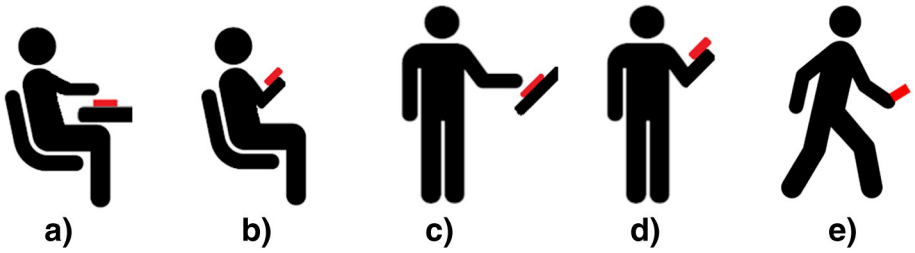

Fig. 1. Several ways the user can interact with the mobile device when performing a biometric authentication.

2.1. Computational power

Obviously, the computational power of a mobile device is much lower than that one of a mainframe, a server, or even a desktop computer, but this constraint may not be relevant depending the situation. For most algorithms, the computational power of current 32-bit processors and available memory is enough for a real-time execution. In particular, most applications of biometrics in mobile biometrics are implemented to perform 1:1 comparisons or in the worst case 1:few. Therefore, the comparison process should not be compromised. The only step in the process where the computation power may be a problem is in those cases where the enrolment is based on intensive training, although the biometric system may consider executing the enrolment outside of the mobile device.

2.2. Data protection and privacy

Biometrics is based on personal data, which should be protected against copy or robbery. In contrast to the use of biometrics in servers or personal computers, handling personal data in mobile devices increase the risk of losing such data. Mobile devices may be lost, forgotten, or most probably used by others. Therefore, any implementation of biometrics in mobile devices should include those mechanisms that may guarantee the privacy of the citizen [3].

2.3. Acquisition of biometric data

The most important technological constraint deals with the act of acquiring the biometric sample. There are two possibilities depending on the biometric modality. The first one is to use an external sensor connected to the mobile device through either a wire or a wireless. This case is quite inconvenient to the user as he/she will have to carry an additional device, and in order to minimize this, the sensor should be small and operated with a single hand, which minimizes the capture capabilities.

The other possibility is to use a component intrinsic to the mobile device (e.g., the touch screen), which provides better ergonomics and convenience for the user as well as higher marketing options, as user investment is not needed for using the biometric solution, at least in hardware devices. The drawback is that such component was not designed for being a biometric sensor, and therefore its features may differ a lot from the ones required by traditional biometric systems. In other words, the biometric solution shall be adapted to the sensor, instead of having a sensor adapted to the biometric solution.

2.4. User interaction

The biggest challenge is dealing with the way the biometric solution is used. In contrast to traditional biometric systems, a mobile device can be used in any position, situation, and scenario (See Fig. 1.). The user can be standing, walking, sitting on a chair, or even lying on the bed. The solution can be used indoors or outdoors and with variable illumination and humidity. This leads to a huge variety of interactions between the user and the biometric sensor. Therefore, the samples captured will differ much more than in traditional systems, compromising the false-negative rates (i.e., FNMR) and the failure to acquire (i.e., FTA).

3. Handwritten signature biometrics in mobile devices

When the above-mentioned constraints are applied to handwritten biometrics, a set of challenges can be specified in order to outline future research lines that will help in the correct massive deployment of the technology.

3.1. Impact due to user interaction

As handwritten signature is a behavioural modality, user interaction may distort the information acquired. There have been studies that have shown difference in performance depending on the capture device, although not as large as initially expected [4,5]. However, further studies shall be carried out to better determine the dependence between the interaction and the biometric sample. This is needed to try to discover a way to isolate the deviation on the biometric sample due to a specific interaction model from the original biometric reference.

In addition, although previous studies have analyzed different interaction, all those were only depending on the user, but not on the platform the user is located. For example, it is of interest to analyze the impact originated by those cases where the user is on a moving platform, such as a train.

Another open issue, in particular due to the fact that handwritten signature is a behavioural biometric modality, is to analyze the impact of the user mood when performing the signature. In this respect, there have been initial studies considering the stress of the user [6] or the user personality [7], but many more studies should follow.

3.2. The impact of technology

For simplicity, we use the term "mobile devices," but such term bring a wide variety of technological features that may bring important impact to the migration of biometrics. Even simplifying the term by only considering smartphones and tablets still brings many parameters to consider, such as size, operating system, sensor technology, etc. In the case of using mobile phones for handwritten signature biometrics, the focus is placed on the touch screen, both in its size and in its technology (i.e., capacitive, resistive, dual, etc.).

Up to a limit, size is important, but mainly depending both in the user and in the size of the signature to write. Recent studies [8,9] have shown that when the screen is larger than 4.5, "users do not seem to worry much, neither performance is highly modified. If screen is large enough, e.g. larger than 10", then the user typically demands placing the device on a surface (e.g., a table) to perform the signature. However, apart from these considerations, size may not be a deterministic factor.

What it is much more important is the technology involved, as depending on it, the information captured may differ greatly. In general,

Please cite this article as: R. Sanchez-Reillo, Signature analysis in the context of mobile devices, Image Vis. Comput. (2016), http://dx.doi.org/10.1016/j.imavis.2016.03.011

we have two cases: those touch screens that can capture also the pressure when writing and those when the pressure is not directly obtained (e.g., capacitive screens, which are the most deployed nowadays). Also, capacitive screens are expected to be used simply with the user's finger, not using any kind of stylus. That led to the idea of signing using the finger, in contrast with the traditional way of signing, i.e., with a stylus or pen. The potential lack of confidence on the user signing with the finger has driven the creation of portable stylus that can be connected to the mobile device (e.g., via Bluetooth). In summary, this bring different kind of scenarios when signing, which have to be analyzed, even considering the interoperability among those. Although some preliminary studies have been published [8], further work has to be done, not only in analyzing the impact but also in compensating such impact in a real world application.

However, there is still the problem of acquiring or not the pressure. Although the channels to be used is still an open issue [10], for forensic experts, it is a must to know such pressure. This brings several problems that will have to be solved. The first one is how a forensic analysis can be done from a static signature acquired in a device that do not capture pressure (i.e., does not have different stroke shapes during the signature), as it is so common in several payment and courier systems.

The second problem is if it is possible to emulate the pressure by counting the number of touched pixels when signing. Some trials are being done, but it is not yet demonstrated if such emulation may be equivalent to the pressure expected to be acquired.

Finally, an important issue is to further study the impact of removing the pressure channel from the comparison algorithm in a dynamic signature, and whether this impact is much more important on forgeries than on bona fide signatures.

3.3. Which algorithm and how many channels

As from the very beginning of the study of dynamic signature biometrics, more work shall be applied in determining better algorithms, and in particular for the application to be executed in the mobile device. There have been multiple attempts with multiple algorithms, providing a whole variety of results [2]: DTW, RBF, HMM, SVM, GA, etc. The question to answer is which is expected to be better for an authentication application in a personal device, when certain limitations on the computational power may exist (in particular during enrolment).

This is also highly bound with which channels to use and which of its derivatives to analyze, which again get us to the constraints highlighted in the previous sub-clause, and may present an important role when fighting against forgeries, as it will be discussed in the following subclause. The higher the number of channels, the larger the information available to exploit but, at the same time, the larger the amount of information to store and process. In addition, depending on the technology, the more channels available to be acquired, the more computationally demanding is the acquisition process, which may compromise the sampling rate. This is certainly one of the hot topics to be analyzed in future research works.

In addition, other imaginative approaches have appeared, such as taking the signature information, not from the touch screen but from the gyroscope and accelerometers of the device, in what it has been called as “signature on the air” [11]. Results have shown promising future research lines.

3.4. Robustness against forgeries

As mentioned several times in this paper, the detection of forgeries is something to be fully studied, not only on mobile devices but also on desktop applications. Anyway, the analysis and detection in mobile devices may become more complex, as the lack of resolution (e.g., in the case of static signature) and the added noise to the acquired signals (e.g., additional device movement related to the proper movement of the user) will confuse those algorithms initially thought for desktop computers. A possible solution may be to perform a holistic approach by analyzing not only the movements detected by the touch screen but also those of the device obtained though the gyroscope.

Also, it is important to analyze the attack potential in the specific application using biometrics in the mobile device, as the complexity of the detection mechanisms should be in accordance of the probability of an attack to be performed, as well as the benefit that the attacker will gain from a potential successful attack. Some forensic experts have started to question if those long-time discarded channels, such as azimuth, should be taken into account again, not so much to improve the algorithm performance but to better detect forgeries.

3.5. Legal binding

Last but not least (although a bit far from the biometric recognition field), there is the need to offer the user the same kind of service as with the traditional paper signature, i.e., binding the signature with the document signed. There are currently some commercial platforms that offer this kind of service by the joint use of the biometric handwritten signature and cryptography, but further analysis should be performed to guarantee such binding as well as to protect the document from disclosing the signature data or discarding the signature from the document.

In addition, local, national, and international legislation should guarantee that the legal implication of a biometric handwritten signature is equivalent to that of the traditional signature or the electronic signature. In addition, the signing process shall be presented to the user in a way that the user is confident in what he/she is signing is the document on the screen.

4. Conclusions

Handwritten signature, both in its static and in its dynamic modality, is being widely deployed nowadays. The technology is working nicely, even when being used in mobile devices, either personal ones (e.g., a smartphone) or an application-specific one (e.g., a credit card payment terminal). However, there are still many things to improve in the technology, as to keeping the path of gaining the confidence of the citizen. Improvement in algorithms as well as in acquisition devices is a must. In addition, the biometric solution shall be focussed not only on the biometric algorithm but also in acquiring other co-lateral information (e.g., movement of the device) as to be able to better asses on the correctness of the signature, as well as being able to better discard forgeries. There are several groups working in the research lines outlined in the previous section, expecting a huge improvement of these biometric modalities in the following years.

References

[1] R. Plamondon, S. Shriari, On-line and off-line handwriting recognition, IEEE Trans. Pattern Anal. Mach. Intell. 22 (1) (2000) 63–84.
[2] D. Impedovo, G. Pirlo, Automatic signature verification—state of the art, IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. 38 (5) (September 2008) 609–635.
[3] P. Campisi, Security and Privacy in Biometrics, Springer-Verlag, 2013, ISBN 978-1-4471-5229-3, http://dx.doi.org/10.1007/978-1-4471-5230-9.
[4] R. Blanco-Gonzalo, O. Miguel-Hurtado, R. Sanchez-Reillo, A. Gonzalez-Ramirez, Usability analysis of a handwritten signature recognition system applied to mobile scenarios, 47th International Carnahan Conference on Security Technology (ICCST) 8-11 Oct. 2013, pp. 1–6.
[5] M. Brockly, S. Elliott, J. Burdine, M. Frost, M. Riedle, R. Guest, An investigation into biometric signature capture device performance and user acceptance, Security Technology (ICCST), 2014 International Carnahan Conference on 13-16 Oct. 2014, pp. 1–5.
[6] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, E. Bella-Pulgarin, Automatic usability and stress analysis in mobile biometrics, Image Vis. Comput. 32 (12) (December 2014) 1173–1180.
[7] O. Miguel-Hurtado, R. Guest, S.V. Stevenage, G.J. Neil, The relationship between handwritten signature production and personality traits, Biometrics (IJCB), 2014 IEEE International Joint Conference on Sept. 29 2014–Oct. 2 2014, pp. 1–8.

Please cite this article as: R. Sanchez-Reillo, Signature analysis in the context of mobile devices, Image Vis. Comput. (2016), http://dx.doi.org/10.1016/j.imavis.2016.03.011

[8] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, J. Liu-Jimenez, Performance evaluation of handwritten signature recognition in mobile environments, IET Biom. 3 (3) (2014) 139–146.
[9] R. Vera-Rodriguez, R. Tolosana, J. Ortega-Garcia, J. Fierrez, E-biosign: stylus- and finger-input multi-device database for dynamic signature recognition, Biometrics and Forensics (IWBF), 2015 International Workshop on March 2015, pp. 1-6–3-4.
[10] J.M. Pascual-Gaspar, V. Cardenoso-Payo, C.E. Vivaracho-Pascual, Practical On-Line Signature Verification, Advances in Biometrics: Proceedings of the Third International Conference, ICB 2009, Alghero, Italy, June 2–5, 2009, volume 5558 of the series Lecture Notes in Computer ScienceSpringer 2009, pp. 1180–1189.
[11] J. Guerra-Casanova, C. Sanchez-Avila, G. Bailador, A. Santos Sierra, Authentication in mobile devices through hand gesture recognition, Int. J. Inf. Secur. 11 (2) (2012) 65–83.

Please cite this article as: R. Sanchez-Reillo, Signature analysis in the context of mobile devices, Image Vis. Comput. (2016), http://dx.doi.org/10.1016/j.imavis.2016.03.011