Face recognition for authentication on mobile devices

Esteban Vazquez-Fernandez, Daniel Gonzalez-Jimenez

GRADIANT (Galician Research and Development Center in Advanced Telecommunications)

Abstract

Accessing information from mobile devices has become mainstream nowadays; besides the clear benefits that mobility provides as a mean to improve efficiency, productivity and user convenience, it in turn does require proper methods for secure access control. In this paper, we discuss the use of face biometric technology and share our thoughts on key related issues and concerns: usability, security, robustness against spoofing attacks, and user privacy among others.

Keywords: face recognition, mobile devices, biometrics

1. Mobile face recognition

Information access from smartphones and tablets has become mainstream both in business and personal environments over the last years. The use of these devices for accessing services like social networks, email or electronic commerce and banking has surpassed the access from traditional computers [1], turning mobile devices into essential tools in our everyday life. Mobility and ubiquity work are powerful tools for increasing efficiency and productivity in business (and also in personal life). However, without the proper usage, companies and users may be exposed to security risks and threats.

Security in the access to information is one of the most important issues to consider in mobility scenarios. Passwords have been the usual mechanism for user authentication for many years. However, there are many usability and security concerns that compromise their effectiveness. People use simple passwords, they reuse them on different accounts and services, passwords can be shared and cracked, etc. The amount of different accounts and passwords we deal with these days contributes in making harder the proper usage and maintenance. As a result, we often see news and reports that alert of stolen accounts and passwords [2]. This problem becomes critical in mobile devices, since they can be easily lost or stolen. Nevertheless, mobile devices can also become part of the solution, providing increased levels of security due to their new authentication options and capabilities.

The use of biometrics brings a more secure and convenient authentication method than traditional passwords. In the 2015 Biometrics Institute Industry Survey [1] [3] the use of biometrics for mobile access control has been established as the most significant development in the biometrics world over the last year. In addition, the survey points to other new applications for biometrics in mobile devices, such as mobile payments or law enforcement.

There are different biometric modalities that can be integrated in mobile devices: face, speaker, iris, fingerprint, etc. All of them have advantages and disadvantages, but one of the main benefits of face recognition (together with speaker recognition) is that, since smartphones already have integrated cameras, no additional hardware is required. Regardless of which biometric modality is used, for achieving a really effective system the following requirements must be accomplished:

- Usability: Ease of use is a key factor for achieving low false rejection rates.
- Security: It is important to avoid impostors to get access to the system (i.e. low false acceptance rate).

Email address: evazquez@gradiant.org (Esteban Vazquez-Fernandez)

[1] http://www.biometricsinstitute.org

- Availability: The verification method should be usable anywhere and at any time.

Face recognition meets these requirements and brings a powerful biometric authentication solution for mobile devices since:

- It is easy to use and user friendly, since the user is already familiar with using the camera on the phone.
- Current face recognition systems achieve high recognition rates, suitable for secure authentication [4] [5] [6].
- As stated before, face recognition does not need any additional hardware on the mobile devices. It takes advantage of the integrated camera so it is available in most smartphones.

However, there are some relevant issues for face recognition on mobile devices that remain unsolved or not enough studied. These concerns need to be addressed shortly for face recognition to be a leading contender in mobile device authentication. In the following sections, a brief review of some of these issues will be presented, including liveness detection anti-spoofing methods, template protection, power consumption, availability under changing scenarios and adverse conditions or inter-device performance.

2. Anti Spoofing

Some biometric traits might be easily captured by an attacker. This is the case of faces, since almost everyone has photos publicly available in social networks like LinkedIN or Facebook. This problem motivates the recent efforts in liveness detection for a secure use of face biometrics [7]. Anti-spoofing methods go from simple ones, for example those based on blink detection, to more complex algorithms for analysing the texture or the light in the scene.

As shown in different publications [8], these machine learning-based anti-spoofing methods tend to be strongly dependent on the dataset used for training the model. This means that the robustness of the liveness analysis depends on the training dataset (genuine accesses and attacks) and the technology used for face presentation and acquisition, so several concerns appear. Can their behaviour be predicted in the presence of a new attack which has not been taken into account in the training set? Can a single anti-spoofing method be enough to guarantee the security of the system?

Given the cross-dataset analysis in recent publications and real scenario tests [9] [8] it does not seem a good idea entrusting the security of the system to a single anti-spoofing method. This is why we believe the use of a single non-collaborative liveness detection method is not enough for guaranteeing the security of the system in real scenarios, now and in the future, since their robustness is dependent on the presentation technology used by the attacker (video quality measures, light reflectance analysis, etc.).

Alternatively, to counteract presentation attacks, a more robust solution would be the combination of several methods working together and combining automatic analysis tools with user interaction. If the system is able to provoke a reaction in the user and then analyse this reaction, fake attempts using photos or videos from the genuine users could be detected and avoided. Unfortunately, interaction can be a time consuming operation and it could reduce the usability, so the challenge here is to achieve a proper balance between security and convenience. The less perceptible the interaction is, the more usable and difficult to spoof the system will be. Current methods rely on asking the user to perform some action, but we think the future points to unconsciously action-reaction interaction analysis in order to increase both security and usability.

3. Template protection

Continuing with another security threat in biometric systems, one of the main concerns both from user and service provider sides is what happens if someone steals the biometric templates. A hacker might directly access system databases, obtaining the biometric templates from the users. A recent example can be found in the US government data breach in December 2014, when 5.6 million fingerprints were stolen. With them, the hacker could get improper access to the system, to other systems, and even track users in different systems. This is a big threat for the privacy of the users and the security of the system. Besides, another question arises: will the stolen biometric traits be persistently invalidated?

This threat motivates the need of protected biometric templates. The industry and the scientific community are now making big efforts for researching, standardising and extending the use of protection mechanisms, since we are aware of the problems related to the use of unprotected biometric templates. As defined in the standard ISO/IEC 24745 for biometric information protection, protected templates are required to comply with some requirements, namely:

- Irreversibility: property of a transform that creates a biometric reference from biometric samples or features such that knowledge of the transformed biometric reference cannot be used to determine any information about the original biometric samples or features.

- Renewability: property of a transform or process to create multiple, independent transformed biometric references derived from one or more biometric samples obtained from the same data subject and which can be used to recognize the individual while not revealing information about the original reference.

- Revocability: ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference.

The use of template protection schemes is not as extended in mobile face recognition systems as it is in other biometrics (e.g. fingerprint) [10], so we believe it is one of the keystones to be developed shortly, in order to achieve the desired levels of privacy and security. Some of the problems to solve are to properly characterise the output signals from the different face recognition algorithms and to get the amount of entropy required for the template protection schemes to achieve a good performance in terms of recognition rates, response time and, at the same time, comply with privacy requirements.

4. Embedded processing

Being able to embed the biometric processing in the mobile devices has gained a lot of interest for face recognition systems [3]. Some of the advantages of the algorithms being embedded in the device are:

- Reduced volume of data exchanged over the network, since sending the video stream to a server is not needed. This allows an off-line use of the system and also response time is reduced.

- The privacy of the users is better preserved, since their biometric data stay in their own devices.

- Scalability: the computational power of the server (for biometric template extraction) does not need to grow with the number of users as much as if the processing were performed in the server.

- Some recent interoperability standards for online identification, like the one proposed by the FIDO Alliance[2], require a secure unlock operation (biometric or not) to release the cryptographic keys. This is accomplished through a safe action, such as the use of biometrics, but the biometric information is required to never leave the user device, so embedded biometric processing is mandatory.

However, an essential challenge remains on mobile face recognition scenario. The duration of the battery remains to be one the biggest weakness in mobile devices. Since energy efficiency is not a problem for traditional server-based face recognition systems, it is usually overlooked (at least, more than it would be desired for mobile scenarios). Nevertheless, it is a key issue in mobile embedded face recognition systems, so a broad study on more efficient algorithms, parallel computing optimization and exploitation of the hardware resources need to be done, as recent works point out [11].

An interesting topic related to the above point is the implementation of the recent Deep Neural Network paradigms for face recognition [12] [13] into mobile devices, taking advantage of the embedded GPU and exploiting its capabilities for energy-optimized real-time processing. Some questions to solve are how to design a proper net architecture for mobile computing or the effects of feature representation and net dimensionality on mobile face recognition accuracy.

5. Availability under different conditions

Can mobile face recognition be used in the dark? Unfortunately, the answer is no, at least with the typical RGB sensor available in common smartphones. But we do not even have to think about

[2] `https://fidoalliance.org`

such a complex scenario as face recognition in darkness. Problems arise also for outdoors face recognition where the systems have to deal with sunlight and strong shadows.

Robust face recognition systems and algorithms are continuously improving their performance under such realistic conditions, thanks to advanced illumination correction algorithms, precise detection and alignment mechanisms or advanced machine learning techniques (e.g. Deep Learning). In any case, we have to deal with some of the problems linked to the hardware characteristics (e.g. sensor dynamic response) and to the scenario (poor lighting). Consequently, face recognition in difficult lighting conditions remains a challenge [6].

This is why we believe in multibiometrics for increasing the availability of biometric systems, and thus the security and convenience. As stated before, we cannot use face recognition in the dark, but we could use other modalities like speaker or fingerprint recognition. Some recent commercial systems have started to move towards multibiometrics, e.g. by combining face and voice. However, the modalities are usually combined at application level, for example asking the user for a second biometric confirmation. Therefore, we can figure out a wide range for improvement in studying better fusion mechanisms, from feature level fusion to continuous and adaptive authentication.

The use of proper fusion schemes will also contribute to increase the security (lower false acceptance rate) and the usability (lower false rejection rates). Other stages of the system, like template protection or anti-spoofing liveness check, can also benefit from advanced multibiometrics schemes: e.g. increased entropy for template protection or multimodal liveness detection.

6. Device dependent performance

In this section we will set out some questions regarding the characteristics of mobile devices that should also be carefully considered for face recognition performance.

One interesting question related to face recognition performance evaluation is if the evaluation of mobile embedded face recognition systems needs to be performed within the devices. The problem here is the uncertainty in the processes and vague specifications. Sometimes the evaluation is done in a server or PC version of the algorithms or worse, it is not specified where the evaluations is performed. The inner calculations can be very dependent on the used libraries and CPU or GPU architectures, so one concern arises: Can the provided performance estimation be guaranteed if not tested within the deployment device?

Speaking about the quality and performance of the cameras in mobile devices, it is about time for vendors to provide reliable and usable information. Information about number of megapixels and lens aperture is usually available, but we hardly ever find other basic information like noise performance, lens distortion, dynamic range of the sensor, etc. These characteristics are essential for the performance of face recognition and other image processing based analysis so, since these functionalities are increasingly present in mobile devices, vendors should take note and incorporate them to their product datasheets. In the same manner, face recognition providers should also take these parameters into account when specifying the performance of their algorithms.

Finally, people use multiple mobile devices such as smartphones, tablets or wearables. To replicate biometric authentication systems over the different devices is a weak spot in user experience. One single enrolment should be enough for accessing different devices and services, in order to achieve a better user experience. Unfortunately, the operation of a face recognition system usually varies due to the use of different camera and optics (capture device). This points out a question very related to the above point: the analysis of cross-device performance and how the performance can be affected if different devices are used for enrolment and for authentication. More research on multimodal cross-device authentication needs to be done for a better mobile biometric authentication experience.

References

[1] The u.s. mobile app report, Tech. rep., comScore (August 2014).

[2] A. Pascual, 2014 identity fraud report: Card data breaches and inadequate consumer password habits fuel disturbing fraud trends, Tech. rep., Javelin (February 2014).

[3] B. Institute, Biometrics institute industry survey 2015, Tech. rep., Biometrics Institute (July 2015).

[4] P. Grother, M. Ngan, Face recognition vendor test (frvt) - performance of face identification algorithms. nist interagency report 8009, Tech. rep., NIST (May 2014).

[5] E. Learned-Miller, G. Huang, A. RoyChowdhury, H. Li, G. Hua, Labeled faces in the wild: A survey.
URL `http://vis-www.cs.umass.edu/lfw/`

[6] A. K. Jain, K. Nandakumar, A. Ross, 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognition Letters (2016) –.

[7] I. Chingovska, J. Yang, Z. Lei, D. Yi, S. Li, O. Kahm, C. Glaser, N. Damer, A. Kuijper, A. Nouak, J. Komulainen, T. Pereira, S. Gupta, S. Khandelwal, S. Bansal, A. Rai, T. Krishna, D. Goyal, M.-A. Waris, H. Zhang, I. Ahmad, S. Kiranyaz, M. Gabbouj, R. Tronci, M. Pili, N. Sirena, F. Roli, J. Galbally, J. Ficrrcz, A. Pinto, H. Pedrini, W. Schwartz, A. Rocha, A. Anjos, S. Marcel, The 2nd competition on counter measures to 2d face spoofing attacks, in: 2013 International Conference on Biometrics (ICB), 2013, pp. 1–6.

[8] T. de Freitas Pereira, A. Anjos, J. De Martino, S. Marcel, Can face anti-spoofing countermeasures work in a real world scenario?, in: Biometrics (ICB), 2013 International Conference on, 2013, pp. 1–8.

[9] Z. Boulkenafet, J. Komulainen, A. Hadid, Face antispoofing based on color texture analysis, in: I2015 IEEE International Conference on mage Processing (ICIP), 2015, pp. 2636–2640.

[10] S. Rane, Standardization of biometric template protection, MultiMedia, IEEE 21 (4) (2014) 94–99.

[11] M. Bordallo López, A. Nieto, J. Boutellier, J. Hannuksela, O. Silvén, Evaluation of real-time lbp computing in multiple architectures, Journal of Real-Time Image Processing (2014) 1–22.

[12] C. Ding, D. Tao, Robust face recognition via multimodal deep face representation, IEEE Transactions on Multimedia 17 (11) (2015) 2049–2058.

[13] F. Schroff, D. Kalenichenko, J. Philbin, Facenet: A unified embedding for face recognition and clustering, in: Computer Vision and Pattern Recognition (CVPR), 2015 IEEE Conference on, 2015, pp. 815–823.