# Face Recognition on Android Smartphones

Antonia Rana, Andrea Ciardulli
*European Commission*
*Joint Research Centre*

## Abstract

*Smartphones are becoming day by day more powerful. As the same time their use is becoming more and more common in applications such as transport, healthcare, security, and surveillance functioning as a multi-purpose, ubiquitous device. In this paper we describe the preliminary results of our experience in using an Android smartphone as a tool which can be used to verify the identity of individuals through the use of two functionalities provided by the most recent generations of smartphones: NFC and face recognition. The scenario that we used for our tests was that of an emergency situation in which identities can be verified by comparing a picture stored in an id card with a picture taken on the spot.*

## 1. Introduction

With the rapid increase in the processing power, sensors and supported communication protocols, more and more advanced and unforeseen uses of smartphones emerge and become integral part of our everyday life. Areas in which smartphones are being piloted already since years are authentication and identification in the context of law enforcement or border control, transport and mobile payments. The availability of high quality cameras and fast CPUs open up the possibility to use these devices efficiently for fast face recognition and to handle this information securely, while the availability of NFC communication enables using them with identity tokens, such as electronic travel documents (passports) or badges. The possibility to use mobile devices to verify the identity of an individual as claimed on an electronic document has been discussed at length in NIST as well as in EU initiatives [1][2][3]. In this short paper we present an application that we have developed for the automated verification of persons in the context of a participatory surveillance application in which smartphones were used to verify the identity and presence of the expected persons at a gathering point [4]. Participatory surveillance can be defined as the use of ubiquitous mobile devices to sense the environment and collect surveillance information. In our particular case, our participatory surveillance application was defined as an emergency evacuation in which mobile devices were used to send location information to a control room and one particular device was used to check the identity of all people gathered at the gathering point. The case of emergency evacuation is one example of a situation in which a quick, secure, reliable mechanism to identify the people involved and check that the persons gathered at the meeting point are all those who are expected is a crucial step. This paper will present the identity verification component of our participatory surveillance scenario. This component consists mainly of an Android app which uses a smartcard (e.g. an employee badge) and the NFC capability of an Android smartphone to verify the identity of a person and talks to a remote control room to report about missing individuals.

In our application we have used a simple badge as an identity token, however, smartphones with NFC capability are being studied for identity verification (1:1 matching) or even for identification (1:n matching) in the context of law enforcement applications with more complex identity documents such as the electronic (biometric) passport [2][3]. Free and commercial applications are available on app stores which enable citizens to read an electronic passport using an NFC enabled Android device, however to our knowledge they are limited to reading the content of the chip and do not attempt to perform any facial image matching.

## 2. Mobile identity verification

By mobile identity verification we mean the verification of the identity of an individual using a mobile device, a picture of the facial image of the person taken on the fly and a picture of the individual stored either in a remote database server or on a token carried by the individual such as an employee badge, an identity card or an electronic passport.

### 2.1 Use scenarios

In our participatory surveillance scheme [4], we identified two possible scenarios in which the identity of a person can be verified using a smartphone. Both scenarios assume that a person has been enrolled into a system in which a picture of the facial image is taken and stored either in a smartcard (used as identity token), or in a remote database (employee database).

- In the first scenario the picture taken for identity verification is matched against the picture stored in the smartcard in the enrollment phase.
- In the second scenario the picture taken for identity verification is matched against the one stored in the remote employees database in the enrollment phase.

The two scenarios have of course different implications both in terms of architecture and network connectivity required and in terms of privacy and data protection. In the first case, no sensitive information is transmitted over the network connecting the smartphone to the control room since the mobile device has all the information it needs to perform the matching between the two facial images and can process them locally. The app will just send an OK/NOT OK message to the control room depending on weather the matching score between the two images was above the selected threshold. In the second case, the reference picture is stored on the remote server, therefore either it or the picture taken on the spot need to be transferred over a network to perform the matching together with an identifier that links the picture to the person identity. Privacy and data protection concerns have been taken into account in both scenarios using encryption: in the first scenario the data stored on the smartcard is encrypted using the built-in smartcard facilities, in the second scenario, data in transit to the control room is encrypted using SSL. Signal processing [1][3] and matching are executed respectively on the smartphone and on the remote server.

### 2.2 Architecture

Our mobile identity verification app runs on an Android smartphone. Results of the biometric data processing or biometric data for remote signal processing are communicated to a remote control room via WiFi or via UMTS/GPRS. The components which constitute the architecture of app are illustrated in figure 1(b).

## 3. Storing and processing biometric data

### 3.1 Smartcards and NFC

One of the main ideas in this application was to store identity information about a person on a cheap smartcard in a secure way in order to protect the privacy of sensitive information, such as the facial image and to check identity using a standard off-the shelf device. It was important to select a smartcard which had some security features and which did not require additional modules to be connected to an off-the-shelf smartphone. The availability of the NFC communication stack [5] on medium-high end Android devices made the choice of contactless smartcards an obvious one. NFC is an efficient technology to pass small amounts of information between two devices with no complex set-up requirements. The standard, developed by the NFC-forum is based on RFID, the main difference being that while RFID supports only communication between a passive tag and a powered device which uses inductive coupling to transmit data, in NFC both devices can be active. When using a contactless smartcard, an NFC enabled smartphone works exactly as a desktop RFID reader, establishing a radio communication between a smartphone (the reading devices) and unpowered chips (contactless smartcards or tags) in close proximity (few centimetres).

The NFC Forum specifications define four types of tags which provide different communication speeds and capabilities in terms of configurability, memory and security.

For our mobile identity verification scenario we chose the Mifare DESFire 8k V1 [6], which operates in accordance with the international standard ISO/IEC 14443A as regards air interface (the same standard is used for electronic passports) and in accordance with ISO/IEC 7816-4 as regards data command sent by the reading device to the smartcard. This contactless smartcard has 8Kbyte non-volatile memory and a number or features which fulfilled our security and privacy requirements (e.g. high speed triple-DES and AES data encryption, mutual three pass authentication, data encryption on the RF-channel and data authentication at the application level).

Mifare DESFIre supports multiple applications. In our app we implemented a single application using the native card file system and we used the access control and authentication features provided by the card at the application level. These features allowed us to encrypt the files (i.e. the facial image and the personnel ID information used for communication with the control room) on the card. An enrollment application was used to capture facial images in controlled lighting conditions and store them securely on the smartcard. Different settings were used to define the optimal conditions to obtain images small enough to fit into the limited storage space of the smartcard, yet still providing good matching results. The limitations on the size of the image were a consequence of the decision to store the images rather than features on the smartcard. This choice enabled us to be independent of any proprietary feature extraction algorithm. The possibility to work with facial images instead of features templates is also in line with the electronic passports specifications so that results obtained in this work could be applied also when using an electronic passport as the identity token.

 

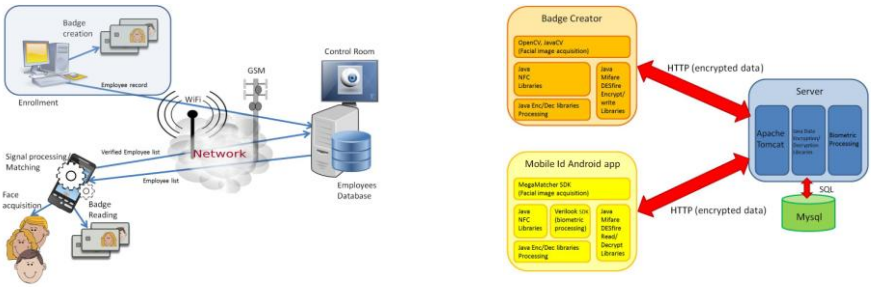


**Figure 1. (a) Local matching scenario, (b) mobile identity verification application architecture**

### 3.2 Matching faces

Biometric match between the facial image stored on the smartcard and a picture of the person taken for identity verification is done on the smartcard. The images are extracted from the smartcard and kept in the internal memory of the phone only for the time necessary for the matching operations.

Tests were performed with 15 individuals enrolled in the system in controlled conditions which included lighting, distance of the face from the camera and elements which could cover partially the face (e.g. beard, glasses, hair, scarves). In the test exercise only three participants were not correctly matched against the picture stored on the badge. However failures were not due to failures in the matching process per se, rather they were related to improper processing at the enrollment level were pictures which had face partially covered by hair or non-frontal face images were improperly stored in the badge. On the other hand, our application successfully identified attendees with reading glasses although during the enrolment process they did not wear them and it also correctly identified attendees with beard, even if during the enrolment phase they did not have it and vice-versa.

In the first implementation of our smartcard based face recognition application we used embedded VeryLook SDK to implement signal processing on the facial images.

## 4. Conclusions

Our initial tests were aimed at identifying the best conditions (at enrollment and in pre-processing the picture) to obtain a facial image file small enough yet still performing well in identity verification on the smartphone. Tests executed with a limited set of participants were successful. Our next step will be to replace the face recognition SDK used in the first phase with a new set of face recognition algorithms which have been shown to have better results on platforms with limited processing power, in particular we have started experimenting with Local Binary Pattern (LBP) algorithms available through the OpenCV open source platform [7]. Face recognition approach on mobile devices based on LBP has already been experimented in [8] which examines the computational burden on two different Android devices and demonstrates the feasibility of a face-recognition approach based on Local Binary Patterns (LBP). LBP promises to have powerful and computationally efficient feature extractor on mobile platforms with low computational cost. The drawback seems to be low efficiency with non-frontal faces. Our future work is directed towards using LBP in our application and experimenting with its limitations in dealing with non-frontal images, benchmarking it against the results obtained using more traditional approaches to face recognition.

## 5. Acknowledgements

The views expressed in this article are those of the authors, and in no way represent the European Commission's official position.

## 6. References

[1] NIST (2009), Mobile ID Device Best Practice Recommendation, Version 1.0, NIST Special Publication 500-280

[2] E-MOBIDIG (2013); http://www.e-mobidig.eu/ (13 September 2013)

[3] Rana, A. Alessandroni A. (2011), Mobile identification, EUR 25037, European Commission

[4] Rana, A. Ciardulli (2012), Identity verification using smartphones In a participatory surveillance scenario, EUR 25746 EN, European Commission

[5] NFC forum specifications (2013): http://www.nfc-forum.org/specs/ (13 September 2013)

[6] MIFARE DESFire EV1 (2013), http://www.mifare.net/en/products/mifare-smartcard-ic-s/mifare-desfire-ev1/ (13 September 2013)

[7] OpenCV (Open Source Computer Vision): http:// http://opencv.org/ (31 January 2014)

[8] Vazquez-Fernandez, E., Garcia-Pardo, H., Gonzalez-Jimenez, D. and Perez-Freire, L. (2011), "Built-in face recognition for smart photo sharing in mobile devices", IEEE International Conference on Multimedia and Expo (ICME), pp.1-4

 