MULTI-BIOMETRIC RECOGNITION ON MOBILE DEVICES

On-going Research Activities at Biometric and Image Processing Lab (BIPLab)

Andrea F. Abate[1], Silvio Barra[2], Maria De Marsico[3], Chiara Galdi[1], Michele Nappi[1], Fabio Narducci[1], Stefano Ricciardi[1], Daniel Riccio[4], and Genoveffa Tortora[1]

[1]University of Salerno, Via Giovanni Paolo II, 132, 84084 Fisciano (SA), [2]University of Cagliari, Via Università 40, 09124 Cagliari, [3]Sapienza University of Rome, Piazzale Aldo Moro 5, 00185 Roma, [4]University of Naples, Via Cintia 21, 80126, Napoli

Abstract: The group working in BIPLab at University of Salerno has addressed problems related to biometrics and image processing on mobile devices. This paper describes FIRME (Face and Iris Recognition for Mobile Engagement) as a biometric application based on a multimodal recognition of face and iris, which is designed to be embedded in mobile devices.

Key words: Mobile devices; face authentication; iris authentication; anti-spoofing

1. INTRODUCTION

Phones, which are the most common representatives of the class of the mobile devices, are now no longer used just for making calls. On the contrary, the main use of smart-phones, has moved from a role of simple tools for remote communication to a more complex set of features. The downside of this improvement in the ability to handle and share information is the increased vulnerability of users to fraud, due to the use of mobile devices for storing and exchanging sensitive information. One possible solution is to use biometrics, with benefits for both the safety and the comfort and ease of use. FIRME1 is a modular system, implemented on Android, that can perform face and iris recognition. It is also suitable for

security-critical operations as it provides tools for spoofing detection, continuous recognition, and best sample selection.

2. FIRME ARCHITECTURE

As stated before, FIRME1 is composed by separate modules. Iris and face are acquired at the same time by the acquisition module, then the two biometrics traits are processed separately by specialized modules: f1) face detection, f2) face segmentation, f3) spoofing test, f4) face feature extraction, f5) face template selection, and f6) face matching; i1) iris detection, i2) iris segmentation, i3) iris feature extraction, i4) iris template selection; i5) iris matching. Scores obtained by face matching and iris matching modules, are then combined in a single final score by the fusion module.

The recognition process may be repeated in a cyclic way to support continuous reidentification. As the reader can see, FIRME also implements a module for face spoofing detection. In the following we will give a brief overview of the techniques used in each system module. For further information the reader may refer to De Marsico *et al.* 1.

2.1 Acquisition and detection

Face and iris acquisition is performed in one shot through the device embedded camera. Viola-Jones algorithm3 is first used to detect face and then it is reused, on the cropped image and with different parameter, to locate eyes and mouth (eyes and mouth positions will be used to estimate face pose).

2.2 Face Recognition

BIPLab research group has been working for long on face recognition. FIRME implements a face recognition algorithm based on correlation and system robustness is improved by integrating anti-spoofing and best template selection techniques.

Preprocessing

For sake of computational resources, we decided to avoid computationally heavy pose normalization techniques considering that users will assume a frontal pose necessarily having to look at the screen of the

device during authentication operations. Eyes and mouth positions are used to estimate face pose and discard those samples which would require pose correction. Finally, an image correction routine is used to normalize illumination. FIRME implements a Self Quotient Image (SQI) algorithm4.

Spoofing detection

FIRME implements an anti-spoofing techniques based on 3D geometric invariants, a simple and robust way to estimate the structure of the face[55]. Observing a set of reference points on a 2D image of a 3D object, we note that even if distances between them change as the capture viewpoint changes, some relationships between them, under specific conditions, remain invariant to the viewpoint, and are therefore called geometric invariants.

In FIRME a set of five points is selected (the outer corner of the right and left eyes, the extreme left and right of the face, and the nose tip), for which the coplanarity constrains is normally strongly violated. The user is required to move the face in order to change the capture viewpoint, while the spoofing detection routine estimates the geometric invariant relative to the identified set of points; if the invariant holds, the points comply with the constraint of coplanarity: this means that the captured face image must be a photo (spoofing); otherwise the points are not coplanar and the three-dimensionality of the face is guaranteed and thus the captured image corresponds to a real (live) user.

Best template selection

During the acquisition phase, the camera captures a high number of frames, aiming at maximizing the accuracy of the recognition. Among the captured frames, only the best one is then used for recognition. The sample selection mechanism is based on entropy1. The selection requires to calculate the correlation between all pairs of faces in the currently acquired sequence of frames. The obtained value of the correlation index (usually in the interval [-1, 1]) is normalized to the range [0,1]. Given a pair of samples, this index can be interpreted as the probability that they conform to each other, and can be used in a way similar to De Marsico *et al.*6.

Feature extraction and matching

In De Marsico *et al.* 6 a more complex version of the algorithm for best sample selection described above is used, i.e. a localized version of the correlation index that is used as similarity measure. This provides more accurate results, but is much more computationally expensive. For this reason in FIRME this version is used only for face matching.

In FIRME recognition step, such correlation is adapted to work on individual sub-regions r_1 and r_2 of the images I_1 and I_2 2 6. For each sub-

region r_1 in I_1, the region r_2 that maximizes the correlation coefficient $s(r_1,r_2)$ is searched, extending this search in a narrow window around the corresponding position in I_2. The global correlation $S(I_1, I_2)$ between the two images I_1 and I_2 is the sum of these local maxima.

2.3 Iris Recognition

Iris recognition, especially in uncontrolled settings, is another important research area for the BIPLab.

Acquisition and segmentation

The segmentation algorithm used in FIRME is ISIS (Iris Segmentation for Identification Systems)7. It was designed and implemented to address under-controlled acquisition conditions, therefore it is well suited to be used on mobile devices. It is robust to the presence of reflections and requires a limited computational time.

Feature extraction and matching

Feature extraction is performed by the CSUM (Cumulative SUMs) algorithm proposed in Ko *et al.* 8. The method is based on the analysis of local variations of grey levels in the image. It is simple to implement, and does not require high computational costs. Last but absolutely not least, it is robust to under-controlled iris acquisition conditions. These features make it appropriate for mobile processing, therefore it was chosen for FIRME1.

2.4 Fusion schema

In FIRME, confidence values (for details see 1 [955]) produced by face and iris systems are computed to fuse their returned distances in order to produce a weighted sum, which corresponds to the global distance produced by the system.

3. CONCLUSIONS AND FURTHER WORKS

This paper describes on-going Research Activities at Biometric and Image Processing Lab (BIPLab). We present FIRME (Face and Iris recognition for Mobile Engagement) which summarizes our efforts in integrating biometric recognition on mobile devices. FIRME was extensively

tested, to evaluate both its performance in terms of accuracy, and its acceptability and usability (see De Marsico *et al.* 1 for details). Further works will focus on integrating other biometric recognition techniques on mobile devices, including for example soft biometrics such as gaze analysis[10 11].

REFERENCES

1. M. De Marsico, C. Galdi, M. Nappi, and D. Riccio, FIRME: Face and Iris Recognition for Mobile Engagement, Image and Vision Computing, 2014. Available online: http://www.sciencedirect.com/science/article/pii/S0262885614000055

2. M. De Marsico, M. Nappi, D. Riccio. "Face: face analysis for Commercial Entities," in 17th IEEE International Conference on Image Processing (ICIP '10), Honk Kong, China, 2010, pp.1597-1600.

3. P. Viola and M. Jones, Rapid Object Detection Using a Boosted Cascade of Simple Features, in IEEE CVPR, pp. 511–518, 2001.

4. H. Wang; S. Z. Li, Y. Wang, and J. Zhang, "Self quotient image for face recognition", in International Conference on Image Processing (ICIP '04), Singapore, 2004, pp. 1397-1400.

5. M. De Marsico, M. Nappi, D. Riccio, J-L Dugelay. "Moving face spoofing detection via 3D projective invariants", in 5th IAPR International Conference on Biometrics (ICB '12), New Delhi, India, 2012, pp.73-78.

6. M. De Marsico, M. Nappi, D. Riccio." ES-RU: an entropy based rule to select representative templates in face surveillance", Multimedia Tools and Applications, Special Issue on Human Vision and Information Theory, Springer Journal, published online November 08, 2012. Available: http://link.springer.com/article/10.1007%2Fs11042-012-1279-6?LI=true

7. M. De Marsico, M. Nappi, D. Riccio, "ISIS: Iris Segmentation for Identification Systems", in 20th International Conference on Pattern Recognition (ICPR '10), Istanbul, 2010, pp.2857-2860.

8. J.-G. Ko, Y.-H. Gil, J.-H. Yoo, K.-I. Chung. "A novel and efficient feature extraction method for iris recognition." ETRI Journal Vol. 29, n. 3, pp. 399–401, 2007

9. M. De Marsico, M. Nappi, D. Riccio, G. Tortora. "NABS: Novel Approaches for Biometric Systems." IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol.41, no.4, pp.481-493, July 2011.

10. C.Galdi, M. Nappi, D. Riccio, V. Cantoni, M. Porta, "A New Gaze Analysis Based Soft-Biometric" Pattern Recognition, Lecture Notes in Computer Science Volume 7914, 2013, pp 136-144.

11. V. Cantoni, C. Galdi, M. Nappi, M. Porta, D. Riccio, "GANT: Gaze analysis technique for human identification" Pattern Recognition, Available online 13 March 2014: http://www.sciencedirect.com/science/article/pii/S0031320314000697