Combining Hardwaremetry and Biometry for Human Authentication via Smartphones

Chiara Galdi[1], Michele Nappi[2], and Jean-Luc Dugelay[1]

[1]EURECOM, Sophia Antipolis, France
{galdi, dugelay}@eurecom.fr
[2]Università degli Studi di Salerno, Fisciano (SA), Italy
mnappi@unisa.it

Abstract. The role of smartphones in our life is ever-increasing. They are used to store and share sensitive data and to perform security critical operation online e.g. home banking transaction or shopping. This leads to the need for a more secure authentication process via mobile phones. Biometrics could be the solution but biometric authentication systems via mobile devices presented so far still do not provide a good trade-off between ease of use and high security level. In this paper we analyze the combination of sensor recognition (hardwaremetry) and iris recognition (biometry) in order to provide a double check of user's identity in one shot, i.e. a single photo of the eye captured by the Smartphone, without the need of additional or dedicated sensors. To the best of our knowledge, this is the first attempt to combine these two aspects.

Keywords: hardwaremetry · biometry · sensor recognition · iris recognition · mobile device

1 Introduction

Performing biometric recognition via mobile devices is an important issue due to the need of a secure use of critical services (e.g. home banking) and to protect sensitive data that nowadays are mostly stored on our personal smartphones or tablets.

Biometry is very suitable for human recognition on mobile devices in fact the users are used to employ the frontal camera of their personal mobile devices to capture pictures of themselves, the so called "selfie". One of the biometric traits that assures the highest recognition accuracy is the iris [25]. However, iris recognition performance on mobile phones suffers from several noise factors, e.g. specular reflections, out of focus images, occlusions, low resolution, etc. To improve the accuracy of an iris recognition system, it is possible to combine the iris with another user's distinctive feature.

Authentication can be performed based on one or a combination of the following items [1]:

- Something the user knows (e.g., password, personal identification number (PIN), secret answer, pattern);

adfa, p. 1, 2011.

- Something the user has (e.g., smart card, ID card, security token, software token);
- Something the user is or does (e.g. fingerprint, face, gait).

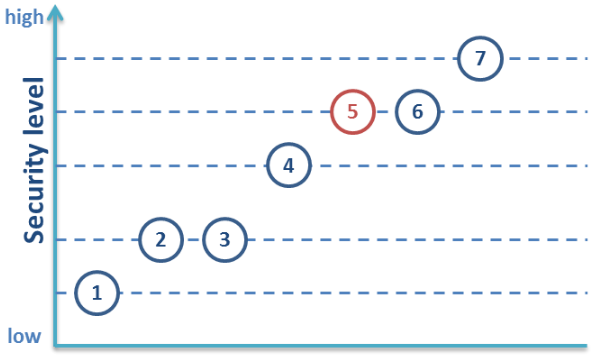

Fig. 1. Security levels**.** (1) Something the user knows; (2) Something the user has; (3) Something the user knows + something the user has; (4) Something the user is or does; (5) Something the user has + something the user is or does; (6) Something the user knows + something the user is or does; (7) Something the user knows + something the user has + something the user is or does.

One possible solution to improve a system's accuracy, is to combine different biometric traits, such systems are called multi-biometric systems. They could require to perform several acquisition phases, one for each biometric trait. In this paper we propose to combine iris recognition with sensor recognition, i.e. the recognition of the Smartphone employed by the user to get authenticated, this combination can assure an higher security level as shown in **Fig. 1**, (5) something the user has + something the user is [1], with respect to the use of biometric recognition only (4) something the user is or does. This kind of system is known as multimodal system.

The advantage in using the Smartphone is two-sided: first, the smartphone is a very personal object that nowadays is used to store and exchange sensitive data, this lead to a strict relation between the user and his/her smartphone, more than a simple smart card or a token generator. Secondly, Smartphones are equipped with high resolution cameras that can be used to perform biometric recognition (e.g. face, iris, etc.) without the need of additional or dedicated sensors.

In this paper we present a technique that combines the recognition of the iris (Biometry), with the recognition of the Smartphone (Hardwaremetry) that captured the photo containing the biometric trait. In one single shot, it is possible to authenticate both the user and his/her Smartphone in order to provide a double check of user's identity. The objective is to provide a system more robust to security flaws and spoofing attacks, e.g. if somebody capture a photo of a person's iris and try to access the system, the device recognition module will detect that the smartphone used for the authentication is not the one belonging to the authentic user. In a hypothetical usage scenario of the system, first an enrollment phase is exploited in which the user register his/her iris and his/her smartphone providing few eye photos. Then, at authentication time, only the couple user-smartphone previously enrolled is accepted as genuine user. In case the user changes his/her Smartphone, a new enrollment is required.

We tested our approach on the available online MICHE database [2, 3], and it is worth to notice that this is the first database that provides pictures of irises of a large number of people, captured with different mobile devices and that allows to perform a realistic performance assessment of iris and device recognition on mobile phones. We assessed performance in terms of Receiver Operating Characteristic (ROC) curve, Cumulative Match Score (CMS) curve, Area Under ROC Curve (AUC), Equal Error Rate (EER), False Rejection Rate (FRR), False Acceptance Rate (FAR), and Recognition Rate (RR).

2 Related works

Biometric recognition on mobile devices is an issue already addressed in few works that we will briefly list in this section.

The biometric trait firstly chosen for biometric recognition on mobile phones, leveraging the presence of embedded cameras, is of course the face. In fact face recognition algorithms do not require high resolution images, and for this reason face was more suitable than iris at the beginning, when the resolution provided by mobile phone embedded cameras was limited. Some example of works on face recognition on mobile phones are presented in [4] and [5], the latter also address the problem of performing complex face-recognition tasks on a mobile terminal. This could shorten the battery lifetime, while it is better to use the mobile phone only as an interface and perform all computationally heavy operations on the server side. In [6] the face recognition system presented also addresses the issue of using biometric recognition for security-critical operations, e.g. home banking, providing also an anti-spoofing module and the opportunity of performing continuous recognition.

Nowadays Smartphones provide built-in high resolution imaging sensors. This gave the researchers the green light to study proper solutions to perform all the phases of iris recognition on mobile phones. For what concerns iris detection, in [7] and [8] methods for pupil and iris boundaries detection are presented, in these two works however, the databases employed were collected respectively with a Samsung SPH-S2300 and Samsung SPH-2300 [9] (in [7] only 132 images were captured with the mobile phone and the others were from CASIA database [10]) which embed a 3.2 megapixel digital camera with a 3X optical zoom, which is a very specific imaging sensor that cannot commonly be found in the most popular Smartphones. Toward the aim of providing a solution suitable for any kind of mobile devices, in [11] and [12] a database acquired with different mobile devices, namely MICHE database [3], is employed to test the iris segmentation algorithm.

One of the first works investigating the possibility to optimize iris segmentation and recognition for mobile phones is [13], the authors propose a method for computing the iris code based on Adaptive Gabor Filter. In [14], Park et al. present a recognition method based on corneal specular reflections, while Kang in [15] presents a method to pre-process iris in order to remove the noise related to occlusions of eyelids and improve system performance. In [16] and [17] authors presents an iris recognition system based on Spatial Histograms. Finally, in [18], authors present a face and iris recognition system for mobile devices that also provides an anti-spoofing module.

3 Method

The system is made up by two main modules: sensor recognition module and iris recognition module. When a picture of the eye is captured, it is employed to check both device's and user's identity. In our experiments, we observed that selecting a sub-region (512x512 pixel) of the picture is sufficient to perform sensor recognition with high accuracy and it also speeds up the recognition process. In **Fig. 2** the architecture of the system is shown. In this section we will describe the algorithms employed to perform sensor recognition, iris recognition and the fusion technique used to improve system's reliability.

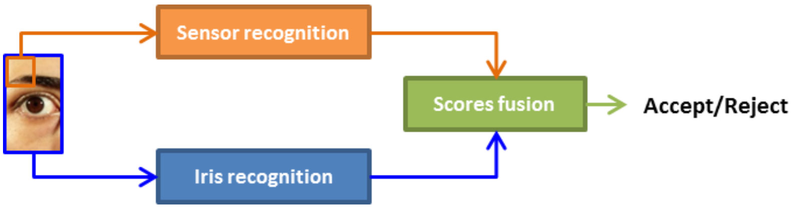

Fig. 2. System architecture.

3.1 Sensor recognition module

In order to recognize the sensor that captured a given photo, we implemented the Enhanced Sensor Pattern Noise (ESPN) based algorithm presented by Li in [19]. This method extracts from a picture the noise pattern of the sensor that acquired the photo, it can also be used to distinguish cameras of the same model [20, 21] [24]. The approach presented by Li, is based on a previous work by Lukás et al. [20] in which the authors present the algorithm for extracting the Sensor Pattern Noise (SPN).

In order to compute the ESPN, first the Sensor Pattern Noise (SPN) is extracted accordingly with the formula presented in [20]:

$$n = \mathrm{DWT}(\mathrm{I}) - \mathrm{F}(\mathrm{DWT}(\mathrm{I})) \tag{1}$$

where *DWT()* is the discrete wavelet transform to be applied on image *I* and *F()* is a denoising function that filters out the SPN in the DWT domain. For *F()* we used the filter proposed in appendix A in [20]. Then the SPN is enhanced as suggested in [19] with the following formula:

$$n_e(i,j) = \begin{cases} e^{-0.5n^2(i,j)/\alpha^2}, & \text{if } 0 \le n(i,j) \\ -e^{-0.5n^2(i,j)/\alpha^2}, & \text{otherwise} \end{cases} \tag{2}$$

where n_e is the ESPN, n is the SPN, i and j are the indices of the components of n and n_e, and α is a parameter that we set to 7, as indicated in [19].

To determine which sensor captured a given photo, we have to compare the ESPN extracted from the picture with the Reference Sensor Pattern Noise (RSPN) of the sensor. The RSPN is obtained by averaging the SPN over N photos acquired with the given camera (see section 4.2 for details):

$$\mathrm{n_r} = \frac{1}{\mathrm{N}} * \sum_{\mathrm{k}=1}^{\mathrm{N}} \mathrm{n_k} \tag{3}$$

Finally, the correlation between the ESPN and the RSPN is computed as follows:

$$\mathrm{corr}(\mathrm{n_e}, \mathrm{n_r}) = \frac{(\mathrm{n_e} - \overline{\mathrm{n_e}}) * (\mathrm{n_r} - \overline{\mathrm{n_r}})}{\|\mathrm{n_e} - \overline{\mathrm{n_e}}\| \|\mathrm{n_r} - \overline{\mathrm{n_r}}\|} \tag{4}$$

where the bar above a symbol denotes the mean value.

3.2 Iris recognition module

The iris recognition module employs the Cumulative SUMs (CSUM) algorithm [22]. This method analyzes the local variation in the gray levels of an image. The image is first normalized transforming the Cartesian coordinates in polar ones, obtaining a rectangular shape. Then the image is subdivided in cells and, for each cell, the representative value X is computed as the average gray level. Then the cells are grouped (horizontally and vertically in turn) and the average value $\overline{\mathrm{X}}$ of the representatives of the cells of each group is computed. The cumulative sums are computed over each group as follows:

$$\mathrm{S_0} = 0$$

$$\mathrm{S_i} = \mathrm{S_{i-1}} + (\mathrm{X_i} - \overline{\mathrm{X}}) \qquad \text{for } \mathrm{i} = 1, 2, \ldots, \mathrm{N}$$

where N is the size of the group.

Finally, the iris code is generated comparing each pair of consecutive sums and assigning values 1 or 2 to a cell if the value of the corresponding sum contributes respectively to an upward slope or to a downward slope. Otherwise, value 0 is assigned to the cell.

The matching of the iris codes computed as explained before, is performed by Hamming distance.

3.3 Fusion technique

The choice of the fusion strategy mostly depends on the application scenario of the system. For example it could be preferable to have a high security access to restricted areas, or just to provide a privileged access to a sub-set of users (e.g. fast track in airports).

We performed fusion at score level and employed the weighted sum technique with the aim of improving system performance (high security scenario).

In next section we will explain in detail these approaches and we will show the results obtained.

4 Experimental results

Performing iris recognition on mobile devices may introduce many noise factors during the acquisition phase due to the fact that:

- the user may need to get authenticated at any time and in any place, with different illumination conditions, while walking, standing or sitting;
- the user holds the mobile device by his hand and may involuntarily move the device;
- the acquisition device characteristics may influence the acquisition: resolution of the sensor, presence of the frontal camera, possibility of using voice control to take the picture, etc.

In order to develop a robust solution for iris recognition on mobile devices, the database used for testing should simulate the uncontrolled acquisition conditions described above.

For this reason, for the experiments we used the MICHE database [2, 3], a database composed by 75 subjects, with at least 40 images per subject, captured in different illumination conditions and with, when possible, different cameras (front and rear) of the three mobile devices employed for the acquisition.

This database perfectly fits our problem because it contains pictures of the same subjects captured with different mobile devices. Performances were assessed in terms of ROC curve, CMS curve, AUC, EER, FRR, FAR, RR.

4.1 Data set

MICHE database contains photos captured indoor and outdoor with three different mobile devices: Samsung Galaxy S4 (hereinafter GS4), iPhone 5 (hereinafter iP5) and Samsung Galaxy tab 2. As we performed iris recognition, among the three devices, we selected the two with highest resolution cameras: GS4 and iP5. Both the front and the rear cameras of these two devices were used. For our experiments we selected 2 photos acquired with the front camera and 2 photos acquired with the rear camera for each device, for a total of 8 pictures per subject, for a total of about 600 images.

Some examples of MICHE database are shown in **Fig. 3**.

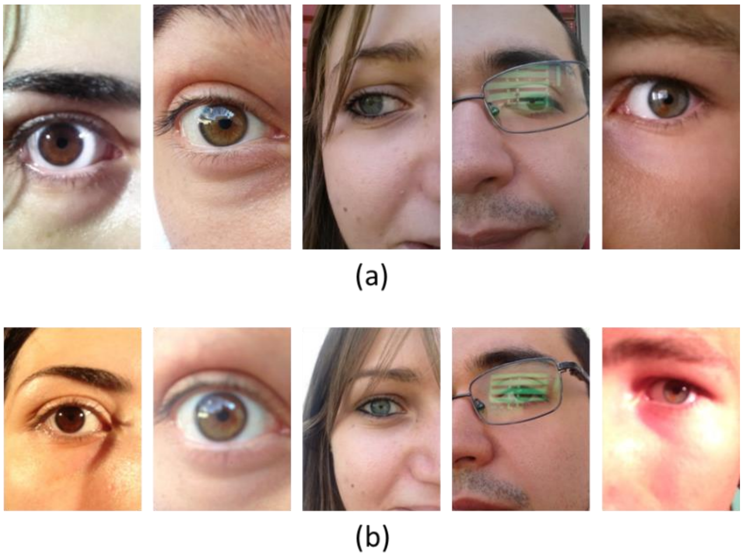

Fig. 3. Examples of images in MICHE database: (a) captured from Galaxy S4; (b) captured from iPhone 5. In both rows are shown, in corresponding positions, the same subjects acquired in the same conditions (i.e. indoor/outdoor, front/rear camera).

4.2 Sensor recognition

To extract the ESPN, in appendix A of [20], it is suggested to process large images by blocks of 512x512 pixel, but during our experiments we observed that using just one block is sufficient to obtain a RR of 98%, for this reason, in our experiments we extracted from all the images a block of size 512x512 starting from the top-left corner of the photo.

In order to extract the RSPN for each camera, we computed the average SPN, as explained in section 3.1, over around 100 photos of the blue sky. We employed this kind of images because they do not contain details that, as the noise, are located in the high frequencies of the image and can be confused with the sensor's noise [20].

We used the RSPNs extracted from the four cameras as Gallery set and the ESPNs extracted from each photo as Probe set.

It must be noted that the iPhone 5 was changed with another device of the same model during the acquisition process of the MICHE database. This means that starting from the subject with ID=49, the photos were acquired with an iP5 but with a different sensor and thus they integrate a different SPN. Since we extracted the RSPN from the new iP5 device, pictures relative to IDs less than 49, should be detected as unenrolled subjects. The presence of unenrolled subjects in the probe, i.e. pictures captured with a device of which we do not have the corresponding RSPN ("old" iP5) in the Gallery, makes the system performance assessment more reliable.

The system obtained a RR equal to 98% and a very low average FAR of about 5%. Results for sensor recognition are shown in **Fig. 5** and the performance values are reported in **Table 1**.

Table 1. Sensor recognition performance

Exp.	**EER**	**avg. FAR**	**avg. FRR**	**AUC**	**RR**
Sensor	0.04	0.05	0.56	0.99	0.98

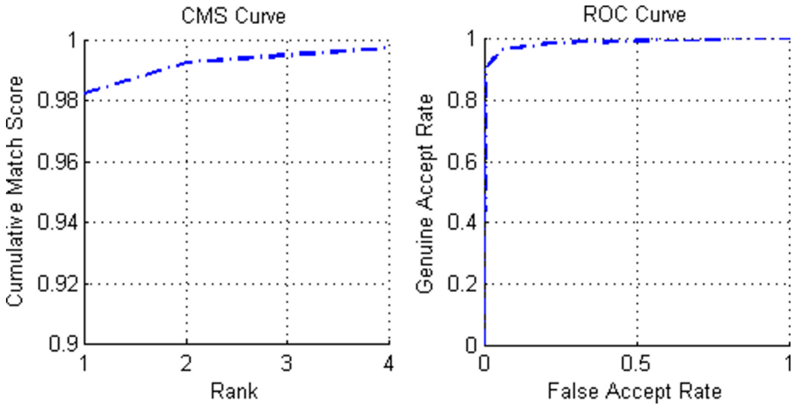

Fig. 4. Sensor recognition performance

4.3 Iris recognition

To assess the performance of the iris recognition algorithm, we employed the same dataset used for the sensor recognition experiment but in this case we split the images so that for each subject half of the pictures (4 images) are in the Probe and the remaining are in the Gallery. Then, to better test the reliability of the system, we removed half of the subjects from the Gallery in order to simulate the attempt of unenrolled users to access the system.

It must be noted that MICHE is a very challenging database, containing pictures affected by many noise factors. Iris recognition system performances could be improved by preprocessing iris images to remove the noise. However, since this goes beyond the aim of the paper, we have not addressed the noise problem.

The system has an 85% RR and an AUC of 77%. Results for iris recognition are shown in **Fig. 5** and the performance values are reported in **Table 2**.

Table 2. Iris recognition performance

Exp.	**EER**	**avg. FAR**	**avg. FRR**	**AUC**	**RR**
Iris	0.29	0.27	0.60	0.77	0.85

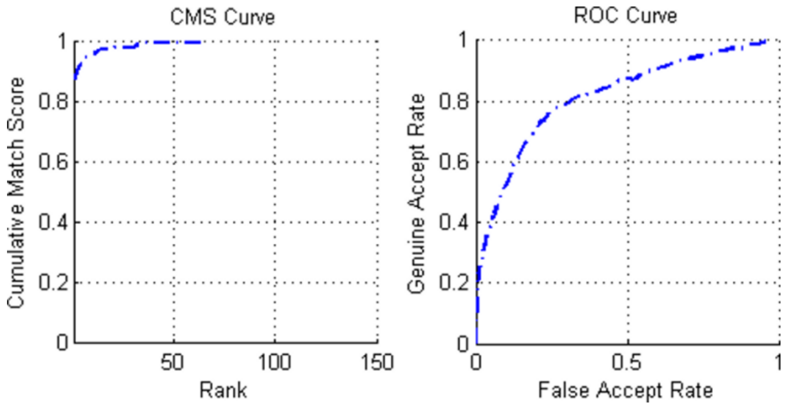

Fig. 5. Iris recognition performance

4.4 Fusion

To test the fusion of iris and sensor recognition, we split the dataset into Gallery and Probe so that in each set we had for each subject four pictures, one for each sensor: GS4 front camera, Gs4 rear camera, iP5 front camera and iP5 rear camera. In **Fig. 6** we present the results of the fusion obtained combining the device and the iris recognition scores via the weighted sum technique. To set the weights associated with the scores, we choose values proportional to the RR obtained by each system. The combination device-iris recognition obtained a RR of 86% and AUC = 98%. The performance values are reported in **Table 3**.

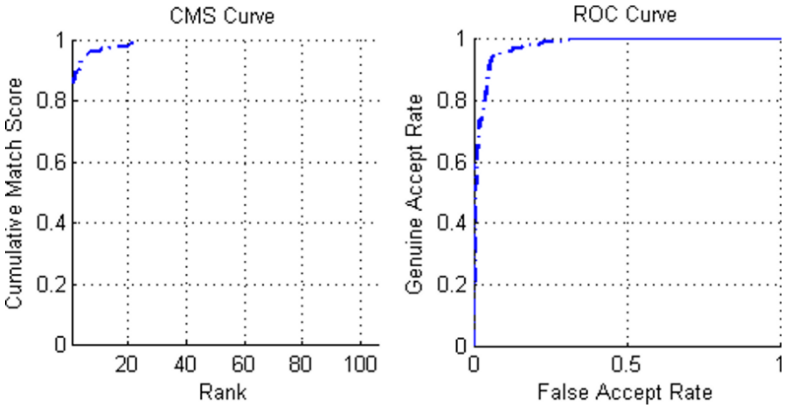

Fig. 6. Fusion performance: iris recognition + device recognition

Table 3. Experimental results**.** Fusion of the sensor recognition scores with the iris recognition ones.

Exp.	**EER**	**FAR avg.**	**FRR avg.**	**AUC**	**RR**
Fusion	0.09	0.26	0.37	0.98	0.86

5 Conclusions

Combining the output of a device recognition module with the output of an iris recognition module, we provided an approach that, based on a single image captured with a mobile device, can assure a higher security level with respect to an authentication system based only on biometrics. In addition, our approach does not require any additional or dedicated sensors as it leverages the presence of high resolution imaging sensors embedded in common Smartphones. In further works we will study the development of a complete system combining hardwaremetry and biometry, further improving the security level adding a liveness detection module. Another aspect that can be improved is the extraction of the RSPN, currently obtained from images of the blue sky, which could be replaced by the technique presented in [23], where the images employed are of any kind, e.g. landscapes, indoor or outdoor photos, etc. Finally, to properly test the system, a biometric database acquired with different sensors is needed, the MICHE database is rich enough to analyze the advantages of combining sensor and iris recognition, but would be interesting to analyze the possibility of developing a multi-biometric system, e.g. iris + face, face + voice, iris + voice, etc., towards the aim of providing higher security through a simple authentication process.

6 References

1. http://www.ffiec.gov/pdf/authentication_guidance.pdf
2. http://biplab.unisa.it/MICHE/database/
3. M. De Marsico, M. Nappi, D. Riccio, H. Wechsler, "Mobile Iris Challenge Evaluation - MICHE - I, Biometric iris dataset and protocols". Pattern Recognition Letters (2015), doi:10.1016/j.patrec.2015.02.009
4. B. Chen, J. Shen, H. Sun, "A fast face recognition system on mobile phone," Systems and Informatics (ICSAI), 2012 International Conference on. IEEE, 2012, pp. 1783-1786.
5. K. Imaizumi, V. G. Moshnyaga, "Network-based face recognition on mobile devices," Consumer Electronics ?? Berlin (ICCE-Berlin), 2013. ICCEBerlin 2013. IEEE Third International Conference on, pp. 406-409.
6. S. Barra, M. De Marsico, C. Galdi, D. Riccio, H. Wechsler, "FAME: Face Authentication for Mobile Encounter," Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2013 IEEE Workshop on, pp. 1-7.
7. D.H. Cho, K.R. Park, D.W. Rhee, Y.G. Kim, J.H. Yang, "Pupil and iris localization for iris recognition in mobile phones," Proceedings of the SNPD (2006), pp. 197–201
8. D.H. Cho, K.R. Park, D.W. Rhee, "Real-time iris localization for iris recognition in cellular phone," International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (2005), pp. 254–259.
9. http://www.samsung.com/

10. http://www.sinobiometrics.com
11. M. Frucci, C. Galdi, M. Nappi, D. Riccio, G. Sanniti di Baja, “IDEM: Iris DEtection on Mobile devices,” 22nd International Conference on Pattern Recognition, ICPR2014, August 24-28, 2014
12. A. F. Abate, M. Frucci, C. Galdi, D. Riccio, “BIRD: watershed Based IRis Detection for mobile devices,” Pattern Recognition Letters, available online 14 November 2014, doi:10.1016/j.patrec.2014.10.017
13. D.S. Jeong, H.A. Park, K.R. Park, J. Kim, “Iris recognition in mobile phone based on adaptive Gabor filter,” International Conference on Advances on Biometrics (ICB ’06) 3832LNCS (2006), pp. 457–463.
14. K.R. Park, H. Park, B.Y. Kang, E.C. Lee, D.S. Jeong, “A study on iris localization and recognition on mobile phone,” Eur. J. Adv. Signal Process. (2007), pp. 1–12.
15. J.S. Kang, “Mobile iris recognition systems: an emerging biometric technology,” International Conference on Computational Science (ICCS) (2010).
16. S. Barra, A. Casanova, F. Narducci, S. Ricciardi, “Ubiquitous iris recognition by means of mobile devices,” Pattern Recognition Letters, available online 28 October 2014, doi:10.1016/j.patrec.2014.10.011
17. A. F. Abate, M. Nappi, F. Narducci, S. Ricciardi, “Fast Iris Recognition on Smartphone by means of Spatial Histograms,” Biometric Authentication, Lecture Notes in Computer Science, Springer International Publishing, 2014, pp 66-74.
18. M. De Marsico, C. Galdi, M. Nappi, D. Riccio, “FIRME: face and iris recognition for mobile engagement,” Image Vis. Comput. (2014) Volume 32, Issue 12, December 2014, pp. 1161–1172.
19. C.-T. Li, “Source camera identification using enhanced sensor pattern noise,” IEEE Transactions on Information Forensics and Security 5(2): pp. 280-287, 2010.
20. J. Lukás, J. Fridrich, and M. Goljan, “Digital camera identification from sensor pattern noise,” IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 205–214, Jun. 2006.
21. M. Chen, J. Fridrich, M. Goljan, and J. Lukás, “Determining image origin and integrity using sensor noise,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 74–90, Mar. 2008.
22. J.-G. Ko, Y.-H. Gil, J.-H. Yoo, K.-I. Chung, “A novel and efficient feature extraction method for iris recognition,” ETRI J. 29 (3), 2007, pp. 399–401.
23. W. Taktak, J.-L. Dugelay, “Digital Image Forensics: A Two-Step Approach for Identifying Source and Detecting Forgeries,” The Era of Interactive Media, Springer New York, 2013, pp 37-51.
24. J. A. Redi, W. Taktak, and J.-L. Dugelay, “Digital image forensics: a booklet for beginners,” Multimedia Tools and Applications, vol. 51, no. 1, pp. 133–162, 2011.
25. J. Daugman, “How iris recognition works,” Image Processing. 2002. Proceedings. 2002 International Conference on (Volume: 1), pp. I-33 - I-36 vol.1.