JAM CM Journal of Applied Mathematics and Computational Mechanics 2017, 16(2), 173-185
www.amcm.pcz.pl p-ISSN 2299-9965
DOI: 10.17512/jamcm.2017.2.14 e-ISSN 2353-0588

THE OVERVIEW OF TRENDS AND CHALLENGES IN MOBILE BIOMETRICS

Agata Wojciechowska, Michał Choraś, Rafał Kozik

Faculty of Telecommunications, Computer Science and Electrical Engineering, UTP University of Science and Technology, Bydgoszcz, Poland
agata.wojciechowska@utp.edu.pl; michal.choras@utp.edu.pl; ralaf.kozik@utp.edu.pl

Received: 18 April 2017; accepted: 12 May 2017

Abstract. Currently, various biometric modalities are used to perform human identification or user verification. Although the research results are promising, the constant development of biometric systems is needed. Recently, biometric systems are also implemented for mobile devices, services and applications. In this article, the review of current trends in mobile biometrics is discussed. The paper also describes the most challenging aspects like aging, template protection or wide users' acceptance. Finally, palmprints are described as the trait that may give promising results and could be implemented widely in mobile biometrics.

MSC: *68U10*
Keywords: *mobile biometrics, palmprints, image processing, security*

1. Introduction

Using mobile phones is increasingly popular all over the world. The International Telecommunication Union presented statistics of mobile phone popularity [1], which show that the ratio between the number of an active mobile-cellular telephone subscription and the number of world inhabitants was 99.7% in 2016, while in developed countries the ratio was 126.7% (more multiple-numbers users). The ratio has been constantly increasing since 2005.

Hence, biometrics cannot miss such a big field of possible implementation. It is remarkable that almost each mobile device has its own built-in camera and other various elements (e.g. accelerometer, microphone) that may be used to acquire biometric data. On the other hand, the majority of mobile phones has a weak security mechanism like inappropriate passwords or even no protection. Most users are overwhelmed by passwords, which give access to various resources or services: e-mail box, mobile phone, bank account, credit card or even online shops, and it is hardly possible to remember each of them. However, the security level may be improved by biometrics [2].

The paper is the overview of the challenges in biometrics, and hereby the mobile approach is described in detail. It is organized as follows: section 2 contains the information about biometrics in general. In section 3, the mobile scenario of biometrics with current trends and problems is described. In section 4, the description of the possibility to use palmprint biometrics in the mobile scenario is given. The conclusions are provided afterwards.

2. Biometrics

2.1. Biometric features classification

However, in the artificial intelligence domain, biometrics is an automatic person recognition based on unique physical or behavioral attributes [3]. Fingerprints may be assumed as the oldest biometric trait. The fact of their existence has been known since ancient Babylon and China [4]. They impressed fingerprints into a clay tablet in order to prove the legacy of the contract. The first idea of fingerprint identification was proposed by Henry Faulds in his paper to Nature (1880). Then, the idea was widely implemented in forensic systems of Scotland Yard (1901) or FBI (1970s).

Nowadays, biometrics are used not only in criminal investigations but also for common user identification. Biometric attributes cannot be lost or forgotten and are mostly unchangeable during a human's life and are unique [5]. Their uniqueness is visible clearly in the case of twins, as presented in Figure 1. While it is difficult to distinguish between twins using face recognition (a), it is much easier to identify them by fingerprint (b) or iris (c).

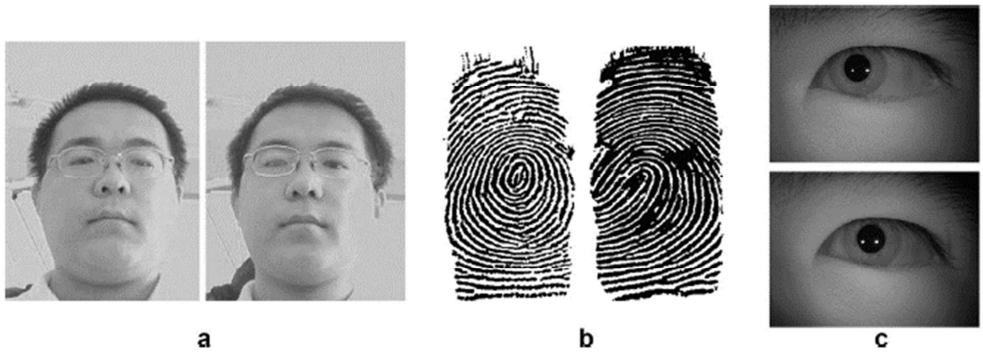

Fig. 1. Twins identification using different biometric traits [4]

Obviously, modalities which can be analyzed in biometric systems are numerous, for instance: face by Zhao et al. in [6], palmprint by Zhang et al. in [5], ear by Choraś in [7], ear 3D by Nappi et al. in [8] or iris by Daugman in [9]. The full

variety of biometrics features is presented in Figure 2. It is visible that there many possible attributes to analyze. The whole biometric recognition system has to fulfil such requirements as [3, 10]:

– acceptability: a society widely accepts the identification method;
– circumvention: the identification process is invariant to fraudulent samples;
– collectability: an acquiring process is easy to perform;
– invariance: the attribute is invariant against time;
– performance: a high accuracy achieved in an accepted time of computing;
– uniqueness: each person has a single identification;
– universality: each person possesses a recognized feature.

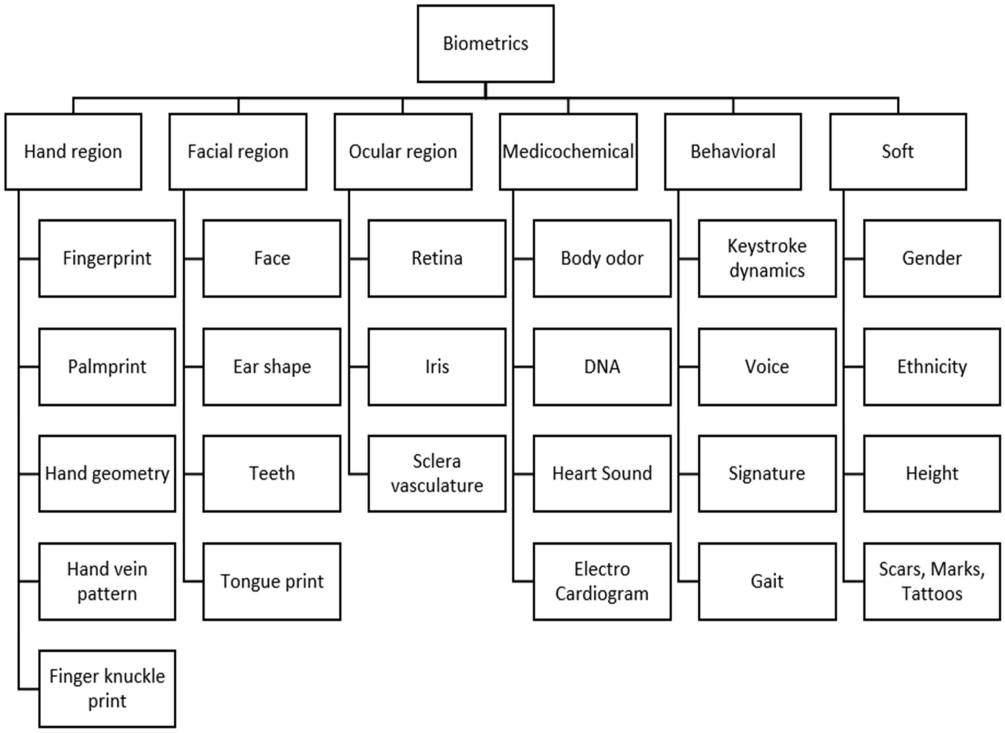

Fig. 2. The variety of biometrics features [3]

2.2. Biometric systems

The system uses information about a person and identifies him or her. In general, it is a pattern recognition system. The main idea, explaining how it works, is presented in Figure 3. Before the identification, an enrollment process has to be performed. In this step, the samples are analyzed and stored in a database. There are many sets of samples available online and, due to their diversity, they are described in detail afterwards. The proper identification consists basically of four

steps. In the sample acquisition part, the system gets the sample using different acquiring devices like a camera, microphone or a special iris scanner. Then, the pre-processing has to be performed to enhance the sample (image, voice record or other) and provide higher accuracy. The next part is features extraction, where the sample is converted into a vector of features. The last step is comparing the vector of features with vectors stored in the database.

The other thing is user verification, where the system has to decide if the evaluated person may get the access to the protected resource or not. However, this kind of system works similar to the biometric identification system.

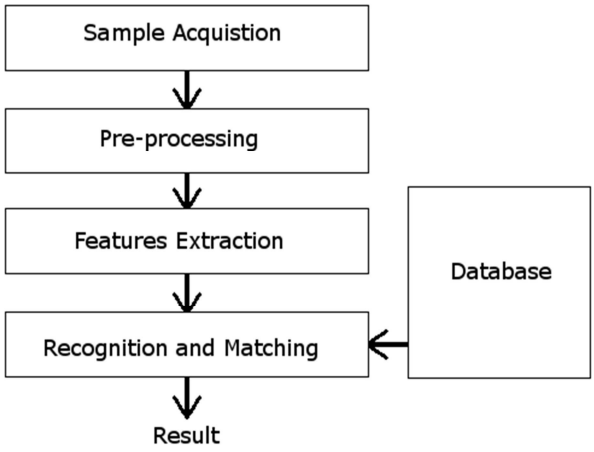

Fig. 3. Biometric recognition system [11]

3. Mobile biometrics

3.1. Classic vs. mobile approach

Jillela and Ross in [12] presented some key points of biometrics in a mobile scenario, which are:

- Data privacy: the identification template is usually stored in the mobile phone memory. Thus, it has to be protected carefully and encrypted to protect the data from leaking.
- Ease of multi-biometric data acquisition: a smartphone is equipped with various sensors, while a multimodal system is claimed to be more reliable.
- Low operational cost: due to a reducing size and an increasing computational power of processing units, the cost of performing the identification seems to be minimal.
- Market penetration: the popularity of mobile phones is enormous and is still increasing. In highly developed countries, even children own their mobile phones.

– Multi-factor authentication: thanks to the specific construction of mobile phones, the biometric identification may be combined with some traditional kinds of protection like a password or with the geospatial data (GPS).
– Portability: the mobile phone is carried by its owner to different places and locations.
– Remote identification: according to the lower computational power, the mobile system may be implemented rather for verification purpose (1:1 matching) than for identification (1:N matching). However, the identification is possible, when the biometric data is securely transferred to the server or to the cloud.

3.2. Template protection

While the mobile technology is developing and mobile phones include a constantly growing number of biometric sensors, more and more sensitive biological data is stored in the smartphone memory. This kind of data, often called the template, has to be protected. Recently, some reports have been published that the biometric data may be intercepted or leaked without owner permission. It is remarkable that any password once stolen may be changed, although the fingerprint cannot be changed. In [13] authors claimed that fingerprint samples may be stolen by hackers from Samsung Galaxy S5 devices running the Android 4.4 or older operating system. The same research team found a security hole in a HTC Max One device. In this case, the scanned fingerprint image was stored in a BMP file without any encryption. Moreover, access to this file was opened for all running applications. Earlier, a group of German scientists proved that fingerprint scanners in Samsung Galaxy S5 and iPhone 5 are possible to defraud with a false fingerprint sample [14]. All vendors received notifications from researchers and claimed to patch all detected vulnerabilities.

3.3. The effect of aging

Biometric features are useful in human identification, however they may be affected and become different while the time is passing. Lanitis in [15] and Backer et al. in [16] proved that each biometric feature is more or less sensitive to aging, which is presented in Table 1. The age progression may affect biometric features in numerous ways. First of all, some minutiae may become less visible or even disappear (fingerprints). Features are not robust to many diseases that may change human movement (gait) or appearance (face).

In the mobile scenario as well as others, the aging may be a difficulty. Nowadays, people at every age possess and commonly use mobile phones. A sample acquired from one person as a child may not be accurate for this person as an adult.

Ageing in biometrics has two different meanings. The first is the absolute age of the identified person, but it is also the time gap between the sample acquiring and the identification process.

Table 1

Aging effects for different biometric features [15]

Feature	Aging effects
Face	growth, lower skin elasticity, obesity, lifestyle, diabetes
Iris	cataract, glaucoma
Fingerprints	lower skin elasticity, injuries
Hand geometry	growth, arthritis
Palmprint	lower skin elasticity, injuries
Voice	lower ability to pump air by lungs, atrophy of vocal muscle, laryngitis, neck cancer
Gait, body movement	reduced muscle strength, Parkinson disease, strokes
Signature	decreased velocity and acceleration of writing

3.4. Vulnerability

While the biometric traits are used for user identification, the whole process is performed without any supervision. Thus, the system may be at risk of attack. Basically, there are two kinds of attacks: direct, where the fake biometric trait e.g. gummy finger is used to identification or indirect, where the application mechanism is corrupted. In [17] it was assumed that a fake biometric sample has a different quality than the real acquired sample. The possible differences are among others color, luminance and sharpness. Then, by calculating some measures, it was possible to verify whether the sample was fake or not. In [18] it was assumed that spoofing attacks are performed mostly by acquiring the sample from the screen of a mobile device or from a printed picture. However, both the screen and the piece of paper are surfaces where reflectance is different from the human skin.

3.5. Computing

Obviously, a computing performance available in a mobile phone is lower than in a personal computer or any server. Thus, processing may be performed: by a mobile phone, by a server or in a cloud.

Computing performed by a mobile phone was proposed among others in [19] to real time voice and face recognition, where the whole biometric process has to be extremely well optimized, and the recognition pattern stored in the memory has to be secured. As a part of optimization, it was assumed that a face is placed in the middle of the acquired image. The other aspect is implementing the Boosted Binary Features for voice analysis instead of a commonly used artificial neural network.

The other solution is to move computing tasks to a server, where the most important aspect is to provide a secure connection between the mobile device and the server. In [20] Wu et al. proposed a three-factor remote authentication system based on: the biometrics, the password and the storage device. Positive authentication is possible only in the following situation: The imprint, the password and some hash functions are used to calculate the message, which is sent to the server and

encrypted there. Then the server sends a second message, which is decrypted by the mobile and verified. Three wrong verifications are possible, then the user is rejected.

Computing performed in a cloud was described for instance by Bommagani et al. in [21] to face recognition, where providing the cloud and the connection security is essential. Moreover, the additional method of template protection was proposed. The acquired image is processed by a face detector, pre-processing and eventually the template h based on the LBP histogram is generated. The template is modified by an orthonormal matrix A, random permutation matrix P and a blinding vector b. The template H stored in database is calculated as a result of the Eq. (1).

$$H = \big((A \cdot P) \cdot h\big) + b \tag{1}$$

3.6. User acceptance

Although biometrics is increasingly popular, the users' acceptance seems to be discussed less often than it should be. A consumer perspective of a biometric system are presented, for instance, by Lancelot Miltgen et al. in [22] or by El-Abed et al. in [23]. In state-of-art articles, the following factors may be important in studying the users' perception:

- Sociodemography: depends on age, gender, religion, abilities and personal experiences of users;
- Confidence: depends on users' feedback and if they trust the system;
- Ease of use: depends on processing time and a sensor quality;
- Privacy issues: depends on potential risk, if the system is easy to defraud, if the template is secured;
- Physical invasiveness: depends on a biometric sensor, if the contact is needed or the sample acquisition is contactless;
- Cultural issues: depends on the user culture.

3.7. Databases

As mentioned before, there are numerous biometric features that may be used for the identification or the authorization process. Afterwards, the most popular databases with a short description and a set of samples are presented.

CASIA Databases [24] are widely used in biometric research. The exemplary images are presented in Figure 4. Iris, fingerprint, face, palmprint, handwriting and signature databases are provided.

PolyU Databases [25] were created at the University in Hong Kong and also may be used to analyze different features. This set of samples regards to the hand region (knuckles, palmprints), the facial region (irises, faces, tongues, ears), and to health features (pulse, ECG). Images coming from the PolyU databases are presented in Figure 5.

The other database is IITD [26]. It contains the following biometric features: a palmprint, an ear and an iris. The images from this database are presented in Figure 6.

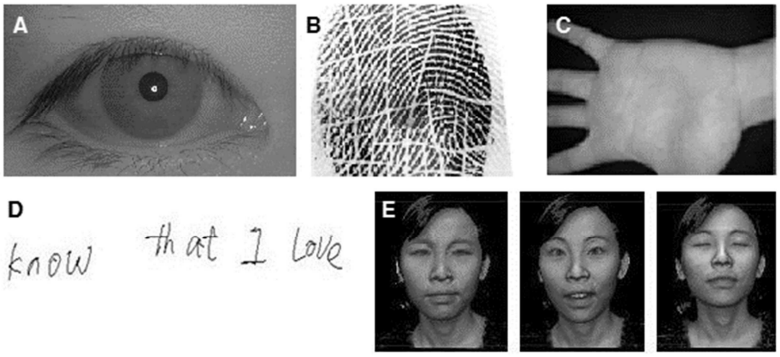

Fig. 4. Images form CASIA databases: A) an iris, B) a fingerprint, C) a palmprint, D) a handwriting and E) a face [24]

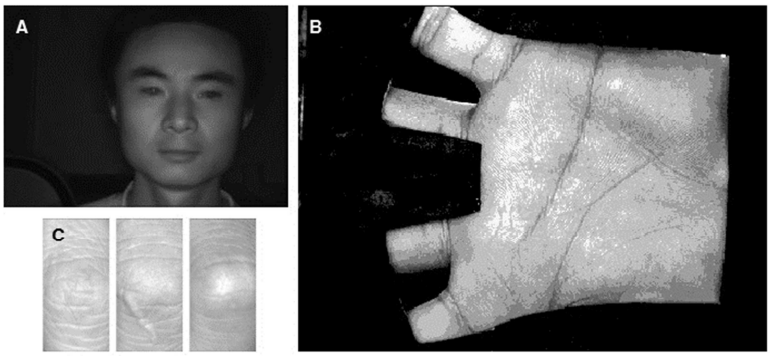

Fig. 5. Images from PolyU databases: A) face, B) palmprint and C) knuckle [25]

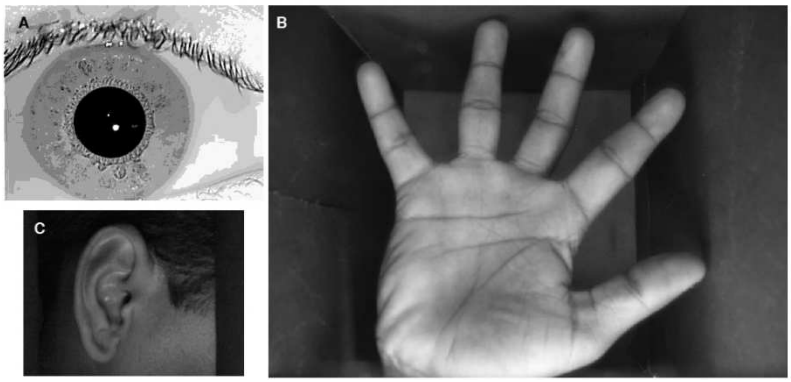

Fig. 6. Images from IITD databases: A) an iris, B) a palmprint and C) an ear [26]

However, all above-mentioned databases are not truly multimodal. They consist of a few databases, each concerning one specific biometric feature. Nevertheless, they do not ensure that the same set of people was involved in the process of acquiring samples. On the other hand, real multimodal databases are also available. As an example, the BiosecurID database proposed by Fierrez et al. in [27] may be enumerated. It includes eight biometric traits acquired from 400 people. The sample of a database contents is presented in Figure 7. Apart from fingerprints, palmprints, irises and faces, which are visible in the Figure, samples of speech, handwritten signature, handwritten text and keystroking are available.

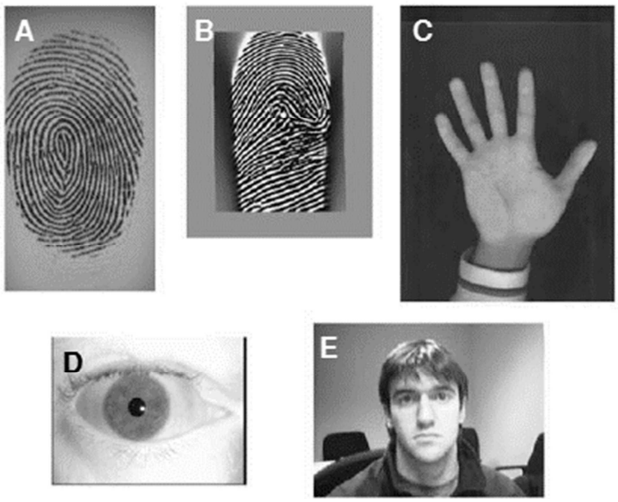

Fig. 7. Images from BiosecurID database: A) a fingerprint acquired by an optical sensor, B) a fingerprint acquired by a thermal sensor, C) a palmprint, D) an iris and E) a face [27]

3.8. Multi-modality

According to the Ross and Jain overview in [28], the biometric system that analyses a single feature can be affected by a variety of problems such as noisy data, intra-class variations, spoof attacks or unacceptable error rates. To overcome these limitations, the multimodal systems are provided. However, a tradeoff between computing cost and matching accuracy has to be estimated [29]. Depending on the kind of a multiplication, various scenarios are possible.

– Multiple sensors: several sensors acquire a multiple sample of the same biometric feature, which are analyzed with the same algorithms;
– Multiple units: two or more samples are acquired, it is possible especially in case of fingerprints or iris, where two fingers or two eyes may be analyzed;
– Multiple classifiers: one sample is acquired and it is analyzed more than once, multiple classifiers operate on the same set of extracted features,

– Multiple snapshots: two samples of the same feature are acquired by the same sensor and analyzed with the same algorithms;
– Multiple features: multiple features are analyzed; two different sensors are essential.

3.9. Feature extraction

One of the key points of biometric identification system is features extraction. There are dozens of methods available, but of image based biometrics they may be divided into three groups:
– Color: the most intuitive approach, for instance a histogram can be calculated, a color may be analyzed both in the RGB and HSV domain like in [30];
– Shape: this approach uses the geometry of biometric traits, for instance the shape of a human ear in [31], where an area, a perimeter, an eccentricity, an elongation, a compactness, a horizontal height, a vertical height, a major axis, a minor axis, a circularity and a rectangularity are estimated;
– Texture: the most popular approach, for instance it is a 2D Gabor filter, which is represented in Eq. (2) and used in [32]

$$G(x, y, \theta, u, \sigma) = \frac{1}{2\pi\sigma^2} exp\left\{-\frac{x^2+y^2}{2\sigma^2}\right\} \times exp\{2\pi i(uxcos\theta + uysin\theta)\} \quad (2)$$

– Hybrid: in this approach, two types of features are extracted, like color and texture features used in [33].

3.10. Limitations

Apart from the effect of aging, biometric systems have other common limitations. First of all, there is a problem of acquiring device. While for acquiring the image of the user's face only the camera is needed, for getting the gait sample is much more complicated. There are also numerous applications of veins pattern recognition systems [34], but is hardly possible to implement them widely, due to the cost of the very specific devices.

The other limitation may be a liveliness detection [35]. It may be described as checking, if the acquired sample is real or fake. This weakness of biometric face recognition system was used to false verification to personal computer and Android phones as well, where the photo of real user was placed in front of the camera and the system verified it positively. To solve this problem, different approaches were presented, for instance eye tracking in [36] or optical flow calculation in [37].

The last but not least are the methods limitations. Some features extraction methods are not invariant to sample rotations (HOG) or illumination variations (eigenfaces technique).

4. Palmprints in a mobile biometric system

Palmprints are not as popular as fingerprints or an iris, while the palmprint research are promising, for instance having 98.41% accuracy in [38] or 98.15% in [39]. Despite a smaller popularity, they are very good features to distinguish individuals, even in the case of twins. They are formed between the 3rd and 5th month of pregnancy. First of all, palmprints have a rich texture. Thus, availability of many key points enables more efficient recognition, and lower resolution images are needed to proceed the identification. It may indicate that the size of an analyzed image is reduced and eventually, the whole process uses less computational power. Unfortunately, most databases are not designed for a mobile application. Some of them use special devices for acquiring the sample, for instance the iris scanner, which is not included in the smartphone in general. That may be a reason for creating the new database dedicated to the mobile scenario exclusively. Acquiring a palmprint sample is relatively simple. The only device needed is a camera, which is available on each smartphone. The quality of samples is sufficient, because smartphones are equipped with cameras with good parameters (one of commonly used Sony smartphone, Sony Xperia Z5 has 23 Mpix camera). This kind of sample acquisition is also user-friendly, because touching any device is not essential.

5. Conclusions

In this paper, the crucial aspects of mobile biometrics are discussed. We have elaborated on the motivation to use mobile biometric systems, on their security, protection and computing performance. Moreover, we have discussed the challenges such as ageing, feature extraction, database creation and multimodality. Finally, palmprints are described as having great potential for application in mobile scenarios.

The plans and the future work is to propose innovative methods for mobile biometrics using a palmprint as modality. The methods will be based on image processing and machine learning.

References

[1] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[2] Siddique K., Akhtar Z., Kim Y., Biometrics vs passwords: a modern version of the tortoise and the hare, Comput. Fraud Secur. 2017, 2017, 1, 13-17.

[3] Unar J.A., Seng W.C., Abbasi A., A review of biometric technology along with trends and prospects, Pattern Recognit. 2014, 47, 8, Aug., 2673-2688.

[4] Jain A.K., Nandakumar K., Ross A., 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognit. Lett. 2016, 79, Aug., 80-105.

[5] Zhang D., Kong W.-K., You J., Wong M., Online palmprint identification, IEEE Trans. Pattern Anal. Mach. Intell. 2003, 25, 9, 1041-105.

[6] Zhao W., Chellappa R., Phillips P.J., Rosenfeld A., Face recognition: A literature survey, ACM Comput. Surv. CSUR 2003, 35, 4, 399-458.

[7] Choras M., Ear biometrics based on geometrical feature extraction, ELCVIA Electron. Lett. Comput. Vis. Image Anal. 2005, 5, 3, 84-95,.

[8] Nappi M., Ricciardi S., Tistarelli M., Real Time 3D Face-Ear Recognition on Mobile Devices: New Scenarios for 3D Biometrics 'in-the-Wild', [In:] Human Recognition in Unconstrained Environments, Academic Press, 2017, 55-75.

[9] Daugman J., How iris recognition works, IEEE Trans. Circuits Syst. Video Technol. 2004, 14, 1, Jan., 21-30.

[10] Hong L., Jain A., Integrating faces and fingerprints for personal identification, IEEE Trans. Pattern Anal. Mach. Intell. 1998, 20, 12, 1295-1307.

[11] Nigam A., Tiwari K., Gupta P., Multiple texture information fusion for finger-knuckle-print authentication system, Neurocomputing 2016, 188, May, 190-205.

[12] Jillela R.R., Ross A., Segmenting iris images in the visible spectrum with applications in mobile biometrics, Pattern Recognit. Lett., 2015, 57, May, 4-16.

[13] Zhang Y., Chen Z., Hui X., Wei T., Fingerprints on Mobile Devices Abusing and Leaking, https://www.blackhat.com/docs/us-15/materials/us-15-Zang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf

[14] https://srlabs.de/bites/spoofing-fingerprints, Security Research Labs.

[15] Lanitis A., A survey of the effects of aging on biometric identity verification, Int. J. Biom. 2009, 2, 1, 34-52.

[16] Baker S.E., Bowyer K.W., Flynn P.J., Phillips P.J., Template aging in iris biometrics, [In:] Handbook of Iris Recognition, Springer, 2013, 205-218.

[17] Pravallika P., Prasad K.S., SVM classification for fake biometric detection using image quality assessment: Application to iris, face and palm print, Inventive Computation Technologies (ICICT), International Conference on, 2016, 1, 1-6.

[18] Bhilare S., Kanhangad V., Chaudhari N., A study on vulnerability and presentation attack detection in palmprint verification system, Pattern Anal. Appl. 2017, Feb.

[19] Tresadern P. et al., Mobile biometrics: Combined face and voice verification for a mobile platform, IEEE Pervasive Comput. 2013, 121, 79-87.

[20] Wu F., Xu L., Kumari S., Li X., A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client-server networks, Comput. Electr. Eng. 2015, 45, 274-285, Jul.

[21] Bommagani A.S., Valenti M.C., Ross A., A Framework for Secure Cloud-Empowered Mobile Biometrics, Proc. of IEEE Military Communications Conference (MILCOM), Baltimore, MD, 2014, October, 255-261.

[22] Lancelot Miltgen C., Popovič A., Oliveira T., Determinants of end-user acceptance of biometrics: Integrating the 'Big 3' of technology acceptance with privacy context, Decis. Support Syst., Elsevier, 2013, 56, 103-114, Dec.<10.1016/j.dss.2013.05.010>

[23] El-Abed M., Giot R., Hemery B., Rosenberger C., A study of users' acceptance and satisfaction of biometric systems, in Security Technology (ICCST), 2010 IEEE International Carnahan Conference on, 2010, 170-178.

[24] http://biometrics.idealtest.org/index.jsp.

[25] http://www4.comp.polyu.edu.hk/~biometrics/.

[26] http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm.

[27] Fierrez J. et al., BiosecurID: a multimodal biometric database, Pattern Anal. Appl. 2010, 13, May, 2, 235-246,.

[28] Ross A., Jain A.K., Multimodal biometrics: An overview, Signal Processing Conference, 2004 12th European, 2004, 1221-1224.

[29] Taouche C., Batouche M.C., Berkane M., Taleb-Ahmed A., Multimodal biometric systems, Multimedia Computing and Systems (ICMCS), 2014 International Conference on, 2014, pp. 301--308.

[30] Gupta G., Dixit M., CBIR on Biometric Application using Hough Transform with DCD, DWT Features and SVM Classification, Image (IN), 2016, 5, 12.

[31] Lobiyal D.K., Mohapatra D.P., Nagar A., Sahoo M.N. (eds.), Proceedings of the International Conference on Signal, Networks, Computing, and Systems, vol. 395. Springer India, New Delhi 2017.

[32] Jaswal G., Nath R., Kaul A., Texture based palm Print recognition using 2-D Gabor filter and sub space approaches, Signal Processing, Computing and Control (ISPCC), 2015 International Conference on, 2015, 344-349.

[33] Jayanthi K., Karthikeyan M., An experimental comparison of features in content based image retrieval system, Computational Intelligence and Computing Research (ICCIC), 2015 IEEE International Conference on, 2015, 1-4.

[34] Czajka A., Bulwan P., Biometric verification based on hand thermal images, 2013 International Conference on Biometrics (ICB), 2013, 1-6.

[35] Jasiński P., Forczmański F., Combined imaging system for taking facial portraits in visible and thermal spectra, Image Process. Commun. Chall. 2015, 7, 389, 63-71.

[36] Killioğlu M., Taşkiran M., Kahraman N., Anti-spoofing in face recognition with liveness detection using pupil tracking, Applied Machine Intelligence and Informatics (SAMI), 2017 IEEE 15th International Symposium on, 2017, 87-92.

[37] Smiatacz M., Liveness measurements using optical flow for biometric person authentication, Metrol. Meas. Syst. 2012, 19, 2, Jan.

[38] Bounneche M.D., Boubchir L., Bouridane A., Nekhoul B., Ali-Chérif A., Multi-spectral palmprint recognition based on oriented multiscale log-Gabor filters, Neurocomputing 2016, 205, September, 274-286.

[39] Sherawat H., Dalal S., Palmprint recognition system using 2-D Gabor and SVM as classifier, IJITR 2016, 4, 3, 3007-3010.