Journal of Machine Construction and Maintenance
PROBLEMY EKSPLOATACJI
QUARTERLY ISSN 1232-9312 3/2017 (106)
p. 97–101

Agata WOJCIECHOWSKA, Michał CHORAŚ, Rafał KOZIK
University of Science and Technology, Faculty of Telecommunications,
Computer Science and Electrical Engineering, UTP Bydgoszcz, Poland
agata.wojciechowska@utp.edu.pl, michal.choras@utp.edu.pl, rafal.kozik@utp.edu.pl

THE METHOD AND AN EXAMPLARY BIOMETRIC SYSTEM TO VERIFY USERS

Key words: biometrics, user verification, palmprint, image processing, pattern recognition.

Abstract: Currently, multiple areas are restricted, and it is necessary to know PIN codes or a proper passwords. However, it is reasonable to use biometrics in order to verify users. This kind of systems are widely known and implemented in our daily life. In this article, the method and an exemplary system to verify users on the basis of palmprint biometrics is proposed. The paper includes the concept and of the device with a full description of all physical elements and algorithms implemented in the system. Finally, it also contains the accuracy results obtained from multiple experiments. The results show that this kind of user verification may be successful and should be developed. In the article, there are also some possible extensions and real-life implementations enumerated.

Metoda i modelowy system biometryczny do weryfikacji użytkowników

Słowa kluczowe: biometria, weryfikacja użytkownika, odciski wewnętrznych części dłoni.

Streszczenie: W dzisiejszych czasach wiele miejsc pozostaje zabezpieczonych przed niepowołanym dostępem. Aby się tam dostać, należy podać numer PIN lub odpowiednie hasło. Rozsądnym wydaje się jednak wykorzystanie biometrii do weryfikowania użytkowników. Ten sposób sprawdzania tożsamości osób jest już dość szeroko stosowany w codziennym życiu. W artykule została zaprezentowana metoda oraz modelowy system, które wykorzystują dane biometryczne w postaci odcisków wewnętrznych części dłoni do weryfikacji użytkowników. Artykuł zawiera opis koncepcji działania urządzenia, wszystkich elementów systemu oraz zaimplementowanych algorytmów. Zawiera także wyniki skuteczności działania urządzenia otrzymane w wyniku przeprowadzonych eksperymentów. Otrzymane wyniki pokazują, że taki sposób weryfikacji użytkowników może być skuteczny i powinien być rozwijany. Omówiono również możliwe rozszerzenia przedstawionego systemu oraz jego możliwe zastosowania w życiu codziennym.

Introduction

Nowadays, each person has multiple passwords to remember and keys to carry. They are essential to log in to email accounts, to open the office's doors, or to unlock mobile phones. Those techniques of user verification are called '*what we posses*' (keys, tokens) and '*what we remember*' (passwords, PIN numbers). However, there is another technique, biometrics. It may be called '*what we are*' [1]. Biometrics analyses different parts of human body or user behaviour in order to recognize the person. This approach is fast, safe, and simply makes life easier. Parts of body that may be a biometric trait are numerous: faces, fingerprints, iris, palmprints, and many others, while among the behavioural traits are gait, signature, and typing, etc. [2, 3]. The biometrics based system of user verification has some typical steps [4]. First, a biometric trait is acquired from the person as a sample. The sample may be an image, voice, or a record. Then, the pre-processing step is performed. It is necessary to enhance the sample and resize it properly. The next part is features extraction, which changes the sample into a vector of features. Then, in the matching step, the vector is compared to the other vectors stored in a database. The last step is getting the final result/decision, which is true if recognized person should get access to the protected resources or false otherwise.

In this article, we present a possible transfer of the biometric pattern recognition to a real user verification system. The system may be implemented next to doors of the restricted areas or offices. The paper is organized as follows: in Section 1, the palmprint as a biometric trait is described. In Section 2, the physical deployment of the device is presented, while Section 3 includes the experiments. Conclusions are provided afterwards.

1. Palmprint as a biometric trait

Palmprint recognition is still not as popular as fingerprint or iris recognition. However, there are numerous researches performed with promising results obtained (over 99% of successful recognition in [5] and over 98% in [6]). Palmprints may be an efficient biometric feature because of their uniqueness. They are formed in the womb and are different even in the case of twins. They have a very rich structure with multiple lines, wrinkles, and ridges. Furthermore, the structure remains unchanged during the human's life, but the most important is that palmprints may be analysed by using even low resolution images [7, 8]. A possibility of using low resolution images leads to the implementation of the palmprint recognition systems on mobile devices and single-board computers [9]. Samples of palmprints may be acquired from a person in a contactless manner [10]. This fact makes the acquisition process easier and more userfriendly. Some examples of palmprints from the available online PolyU database are presented in Fig. 1.

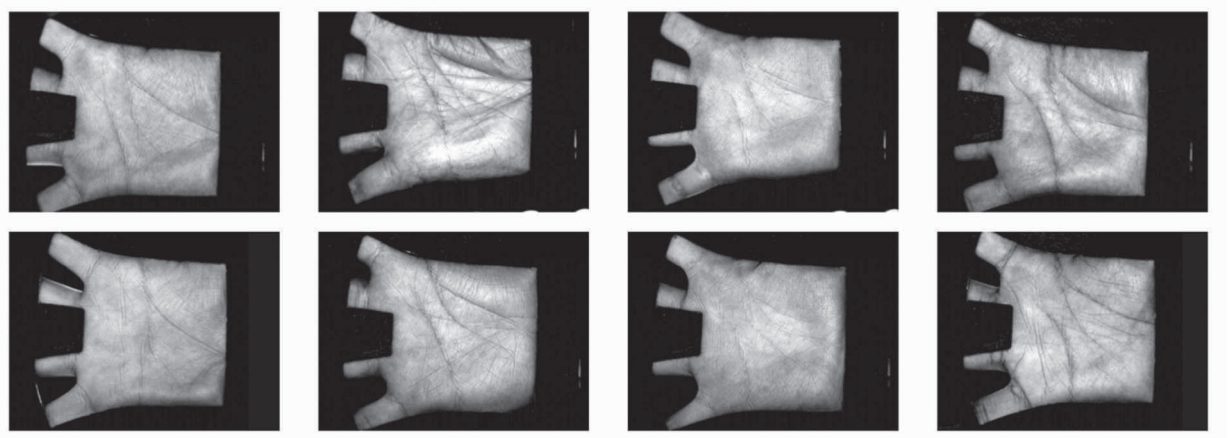

Fig. 1. Examples of palmprints from the PolyU database [11]

Nevertheless, there are multiple challenges in using palmprints as a biometric trait. They are numerated in [12]. First of all, the illumination may change. In [13] the authors proposed the pre-processing method, which eliminates correcting non-uniform illumination or shading effects. The distance between an acquiring device and a palmprint also needs to be fixed, but it depends on the implemented approach. Kim et al. in [14] presented a dedicated interface for mobile phones. This graphic interface helps to put a hand in the proper position, where only the centre of the hand is visible. In [15, 16], it was necessary to take o photo of the whole hand. Acquiring only a part of the palmprint would not provide any successful verification. Using dirty hands for verification may also disturb the process or even make it impossible to run. The last but not least are fake samples. The most often used technique is lifeless detection, which checks if the object in front of the acquiring device is real (human hand) or fake (e.g., printed photo of the human hand) and is described in [17].

2. The biometrics device's concept

The verifying device is based on Raspberry Pi 2 (model B). This single-board computer, despite its compact size, may run very powerful operations. It has a Linux operating system on board and may cooperate with popular image processing libraries like OpenCV. As input elements, it uses a traditional webcam camera (Logitech C130) and a button. Of course, there are many others cameras, including Raspberry Pi dedicated cameras. Nevertheless, we decided to use this camera due to its advantages, like sufficient resolution and low price. The device uses LED diodes as an output. First one (red) gives information about the device – if it is ready to perform the verification. The second one (green) gives information about the verification performed. All elements are packed together in the dedicated case printed on the 3D printer.

When a user wants to be authorized, he has to put his palm in front of the camera and press the switch. After a positive authorization, the green diode lights up. In the case of negative authorization, nothing changes. In Fig. 2, the proposed device is presented. The software working on the device is a common pattern recognition system. First, the learning process is conducted. During this process, three positive samples (called patterns) are collected from a 'positive' user. Those will become the pieces of the comparing set. Apart from the patterns, there are 7 samples taken from the PolyU database in the set. When the learning step is performed and the switch is pressed, the sample is acquired and it needs to be pre-processed. Thus, the region of interests (ROI)

Fig. 2. The device for verification. A – positive verification, B – standby mode

Source: Authors.

is chosen from the whole image and is slightly blurred with the Gaussian filter. Blurring ensures that there will not be any unwanted details, while choosing the ROI reduces the size of the sample. Then, the HOG (Histogram of Oriented Gradients) feature extractor is used. In the HOG method, the image is divided into small connected parts, called cells. For each cell, a gradient of intensity is calculated. Then values have to be normalized. Normalization is performed in each block, which is a larger region of image then a cell. This method is not invariant to samples rotations, but the ROI extraction algorithm reduces them effectively. Each image processing step is presented in Fig. 3.

Unfortunately, the picture of the palmprint has to be taken up front, in the single colour and dark background (as presented in Fig 3A.) and in sufficient illumination conditions. This requirement is caused by the image segmentation process performed during the preprocessing part of the system. In real-life application, it may be reasonable to ensure the additional source of light to provide sufficiently light foreground.

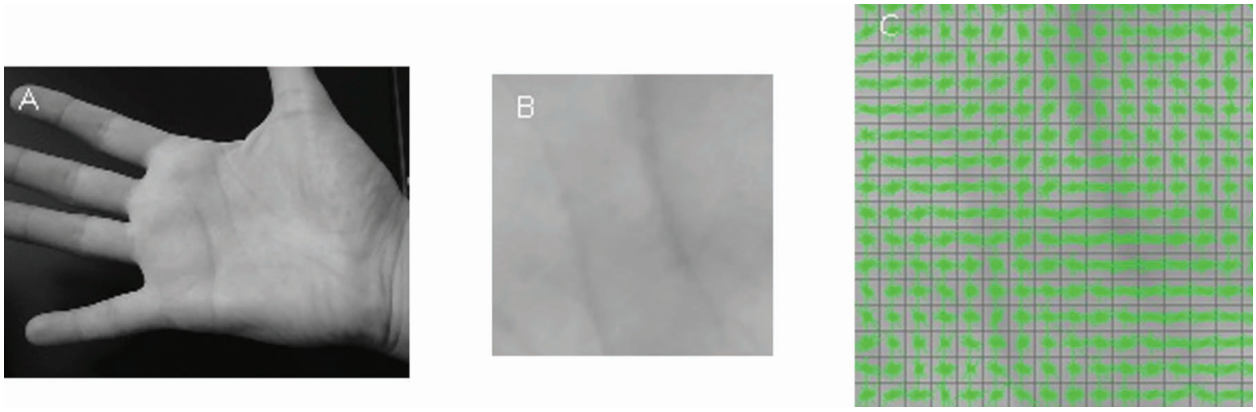

Fig. 3. A – an original image taken from user, B – a Region of Interests extracted, C – a Histogram of Oriented Gradients visualisation

Source: Authors.

Then, after the pre-processing step and the features extraction process, HOG features are compared to features taken in the dataset. Due to the limited computational resources available in the single-board computer, the matching algorithm has to be very simple. Other commonly used algorithms seemed to be too complicated and complex. Most of them (like SVM or Neural Network) are artificial intelligence methods and need much computation power. That is why the Euclidean distance is implemented in the device. Equation 1 presents the calculation performed for each point from the features vectors, where p is the point from the analysed image and q is the point from the database image. Then the average value is calculated from the distances. Finally, according to the fixed threshold, the decision whether the verification is positive or negative is performed.

$$d(q,p) = \sqrt{(q_x - p_x)^2 + (q_y - p_y)^2} \tag{1}$$

Each biometric verification system has to fulfil some requirements. Table 1 contains these essential points with the explanation, and how it works in the designed system.

Table 1. Requirements for biometric verification systems

Requirement	Explanation
UNIVERSALITY	All requirements are provided by the biometric feature – palmprint.
PERMANENCE	
UNIQUENESS	
USER - FRIENDLINESS	User does not have to touch any sensor and uncover any intimate parts of his body.
REAL-TIME CALCULATIONS	Despite of the small size, Raspberry Pi 2 is a relatively powerful computer (900MHz quad-core ARM Cortex-A7 CPU and 1 GB RAM). Due to using this kind of single-board computer, it was possible to ensure real-time calculations.
LOW RESOLUTION IMAGES	Choosing palmprints as a biometric feature enables using low resolution images. In the designed device the input image size was 640x480 px.
ACCURACY	The designed system has a promising accuracy level. This parameter is discussed in the next section.

3. Evaluation

The proposed system was evaluated in terms of accuracy. The way to calculate the accuracy is presented using Eq. 2, where TP – true positives (positive samples well verified), TN – true negatives (negative samples well verified), N – a total number of samples (sum of positive and negative).

$$ACC = \frac{TP + TN}{N} \cdot 100\% \tag{2}$$

In order to check whether the system works sufficiently correct, multiple experiments were performed. For executing them, 3 learning sets were used (3 positive and 7 negative samples) and 10 testing sets (10 positive and negative samples). For 30 experiments, the accuracy was promising. Its value was in range from 85% to 94%. The results are presented in Table 2. In biometric verification systems, there are two additional important measures: FAR (false acceptance rate) and FRR (false rejection rate). FAR is the percentage of samples that were accepted but they should not be, while FRR is the percentage of samples that were not accepted but they ought to be. In the proposed system, the FAR was in range from 1% to 3% with the average value of 1.3%; whereas, the FRR was in range from 11.1% to 28.6% with the average value of 21.6%.

Table 2. Results of experiments

Experiment number	Accuracy	Experiment number	Accuracy	Experiment number	Accuracy
1	88%	11	85%	21	94%
2	87%	12	86%	22	94%
3	88%	13	86%	23	94%
4	87%	14	86%	24	94%
5	86%	15	86%	25	94%
6	87%	16	85%	26	94%
7	88%	17	86%	27	94%
8	87%	18	86%	28	94%
9	86%	19	86%	29	94%
10	87%	20	86%	30	94%

Conclusions and possible extensions

In this article, the possible real-life implementation of the biometric verification system is presented. The provided results show that using palmprints in such a system may be reasonable and efficient. The big advantage of this approach is the total cost. Web cameras are relatively cheap, while for instance fingerprints scanners can be far more expensive. For real-life application, device development is essential. It is possible to replace one of the diodes to a mechanism that would be able to unlock secured doors. We plan to deploy and implement the device in a real life access control system at our university in order to evaluate it on a large set of users. The other idea for implementation of this kind of system is placing the device next to the machine: a lathe or a milling machine. This kind of system would verify the operator. In the case of negative verification, the machine will be switched off. In both systems, the additional light source may be added. It would ensure the good quality of taken samples.

There is also one more possible extension. It is called multimodal biometrics and has been increasingly popular recently. There are multiple systems that prove the higher accuracy level of the multimodal approach then accuracy level of unimodal approach [18]. Taouche in [19] presents some advantages of implementing multimodal biometric systems as follows:

- Lower sensitiveness to imposter attacks,
- Lower sensitiveness to noise, and
- Successful when a single trait is not enough.

However, it is important to remember that multimodal biometrics is more complicated. It has one more step in the verification system that is making decisions.

References

1. Jain A.K.: Biometric recognition: how do I know who you are? In: Signal Processing and Communications Applications Conference, 2004. Proceedings of the IEEE 12th., pp. 3–5. IEEE (2004).
2. Unar J.A., Seng W.C., Abbasi A.: A review of biometric technology along with trends and prospects. Pattern Recognit. 47, 2673–2688 (2014).
3. Jain A.K., Nandakumar K., Ross A.: 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognit. Lett. 79, 80–105 (2016).
4. Pravallika P., Prasad K.S.: SVM classification for fake biometric detection using image quality assessment: Application to iris, face and palm print. In: Inventive Computation Technologies (ICICT), International Conference on. pp. 1–6. IEEE (2016).
5. Xu X., Lu L., Zhang X., Lu H., Deng W.: Multispectral palmprint recognition using multiclass projection extreme learning machine and digital shearlet transform. Neural Comput. Appl. 27, 143–153 (2016).
6. Sherawat H., Dalal S.: PALMPRINT RECOGNITION SYSTEM USING 2-D GABOR AND SVM AS CLASSIFIER. IJITR. 4, 3007–3010 (2016).
7. Harb A., Abbas M., Cherry A., Jaber H., Ayache M.: Palm print recognition. In: 2015 International Conference on Advances in Biomedical Engineering (ICABME). pp. 13–16. IEEE (2015).
8. Wojciechowska A., Choraś M., Kozik R.: The overview of trends and challenges in mobile biometrics. J. Appl. Math. Comput. Mech. 16, 173–185 (2017).
9. Choraś M., Kozik R.: Contactless palmprint and knuckle biometrics for mobile devices. Pattern Anal. Appl. 15, 73–85 (2012).
10. Jadhav S.B., Raut M.S.D., Humbe V.T., Kartheeswaran T.: A Low-Cost Contactless Palm Print Device to Recognize Person based on Texture Measurement. (2016).
11. http://www4.comp.polyu.edu.hk/~biometrics/.
12. Leng L., Liu G., Li M., Khan M.K., Al-Khouri A.M.: Logical conjunction of triple-perpendicular-directional translation residual for contactless palmprint preprocessing. In: Information Technology: New Generations (ITNG), 2014 11th International Conference on. pp. 523–528. IEEE (2014).
13. Javidnia H., Ungureanu A., Costache C., Corcoran P.: Palmprint as a smartphone biometric. 2016 IEEE Int. Conf. Consum. Electron. ICCE. 463–466 (2016).
14. Kim J.S., Li G., Son B., Kim J.: An empirical study of palmprint recognition for mobile phones. IEEE Trans. Consum. Electron. 61, 311–319 (2015).
15. Moco N.F., Lobato Correia P.: Smartphone-based palmprint recognition system. Presented at the 21st International Conference on Telecommunications (ICT) , Lisbon, Portugal (2014).
16. Yoruk E., Konukoglu E., Sankur B., Darbon J.: Shape-based hand recognition. IEEE Trans. Image Process. 15, 1803–1815 (2006).
17. Aishwarya D., Gowri M., Saranya R.K.: Palm print recognition using liveness detection technique. In: Science Technology Engineering and Management (ICONSTEM), Second International Conference on. pp. 109–114. IEEE (2016).
18. Khellat-Kihel S., Abrishambaf R., Monteiro J.L., Benyettou M.: Multimodal fusion of the finger vein, fingerprint and the finger-knuckle-print using Kernel Fisher analysis. Appl. Soft Comput. 42, 439–447 (2016).
19. Taouche C., Batouche M.C., Berkane M., Taleb-Ahmed A.: Multimodal biometric systems. In: Multimedia Computing and Systems (ICMCS), 2014 International Conference on. pp. 301–308. IEEE (2014).