User Identification based on the Vein Pattern in Biometric Immobilizer

Michael A. Basarab[1], Tatyana I. Buldakova[2], Kristina A. Smolyaninova[3], Michael N. Sokolov[4]
Faculty of Informatics and Control Systems
Bauman Moscow State Technical University
Moscow, Russia
[1]bmic@mail.ru, [2]buldakova@bmstu.ru, [3]kriszzztina@yandex.ru, [4]mike.sv@mail.ru

***Abstract*— Article deals with the problem of vehicles protection against theft by using biometric immobilizers. The use of a vascular authentication method based on the vein pattern of the driver's finger is suggested. The flowcharts of algorithms for the image preprocessing and the formation of the biometric pattern are given.**

***Keywords*—biometry; pattern recognition; authentication algorithm; vein pattern; biometric immobilizer; vehicle**

I. Introduction

Nowadays we are facing the problem of vehicles protection from theft. More electronic devices are added to cars, and a growing number of vulnerabilities allow attackers to hack and steal the transport. At the same time, the ways of hacking become more sophisticated, therefore, the methods of protection should be more effective.

Traditional means of protecting vehicles are mainly related to scaring, tracing and attracting attention. Along with this, there are regular means of blocking the car, but intruders overcome them by prescribing counterfeit keys to the central control unit [1, 2].

The solution of this problem is the use of biometric immobilizers, which allow the vehicle's engine to be blocked by breaking critical electrical circuits [3]. Biometric signs of a person are unique, which allows them to be successfully applied in security systems for identification of users [4]. However, the disadvantage of existing biometric immobilizer systems is the use of the fingerprint authentication method [5–7]. This method is not safe, since various methods of imitating a fingerprint are known.

The article proposes to use the vascular authentication method, which provides high recognition accuracy and characteristics concealment. The pattern of the veins is only visible in the infrared spectrum, so it cannot be falsified [8, 9].

One of the key tasks of constructing biometric authentication systems based on finger veins is preliminary image processing, which cuts unnecessary areas and prepares image for extraction of the biometric features [10].

II. Functional Model of the Biometric Authentication Module

The technology of biometric authentication by vein pattern is based on optical visualization of human veins and their further recognition [11, 12]. Since hemoglobin in blood absorbs infrared radiation and other tissues reflect it, the veins appear darker in the image than other tissues. This allows us to use them for further user authentication.

The main element of the biometric immobilizer is the image capture and recognition module, as it provides the system with user identification functions. In Fig. 1 you can see the block diagram of the biometric module of user authentication.

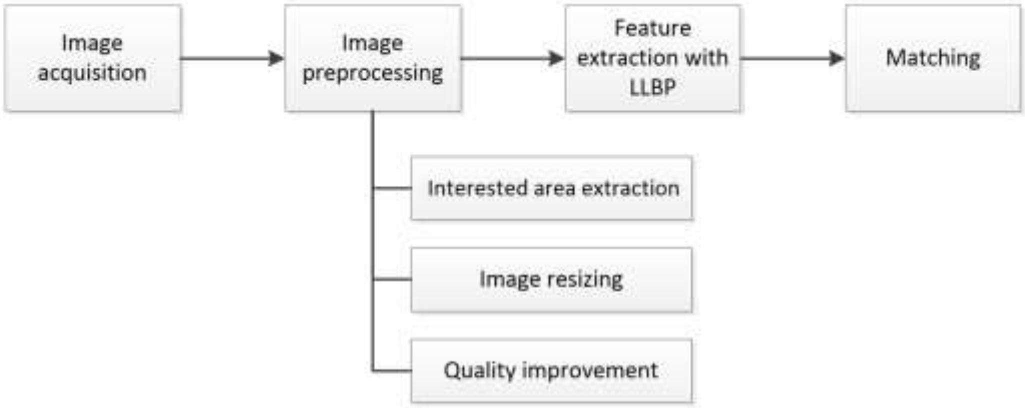

Fig. 1. Block diagram of the biometric module of user authentication

978-1-5386-5824-6/18/$31.00 ©2018 IEEE

The input of the module receives an image from the scanner, after that the image is pre-processed, which includes: 1) extraction of the area of interest; 2) resizing the image; 3) improving the quality of the image.

The input image contains an unwanted background, so the first step is to filter image and select the area of interest. Filtering allows you to distinguish significant areas of finger veins, reduce areas of noise and glare. Then the original image is converted to a binary code using the Otsu method [13]. Binarization allows you to determine the center of the finger and crop the image based on the selected center point.

To reduce the algorithm computation time and to further reduce noise, the size of the cropped image is scaled (its resolution is reduced). Since the resulting image, basically, has a low contrast level, it needs to be increased with a modified Gaussian high-pass filter.

This filter allows you to extract low-frequency components, such as the borders and veins of the finger. A flowchart of the algorithm for pre-processing of the user's venous finger image is shown in Fig. 2. Let us consider the main steps of the algorithm and their features.

III. Search of interested area

First, the input image is binarized using the Otsu method (Figure 3), and the barycenter of the white region (the conditional finger center) is determined in the binarized image. For this purpose, the sum of the multiplications of values of pixels by their position in the horizontal and vertical coordinates is calculated, i.e.

$$a_w = \sum_{j=1}^{Heigth} \sum_{i=1}^{Width} \left(p_{ij} \cdot x_i \right)$$

and

$$a_h = \sum_{i=1}^{Width} \sum_{j=1}^{Heigth} \left(p_{ij} \cdot y_j \right),$$

respectively. Here p_{ij} – value of pixel with coordinates x_i and y_j, *Width* – image width, *Heigth* – image heigth.

Barycenter coordinates is calculated as $B_x = a_w / W$ and $B_y = a_h / W$, where $W = \sum_{i=1}^{Width} \sum_{j=1}^{Heigth} p_{ij}$. Barycenter coordinates B_x and B_y is used as a reference point for determining the coordinates of the singular points of the vein pattern.

Based on the calculated point, the image is cropped to 480x160, and thus the area of interest is distinguished. In the future, to increase the speed of the algorithm, as well as to get rid of pixel noise, the cropped image is scaled to a resolution of 192x64 pixels.

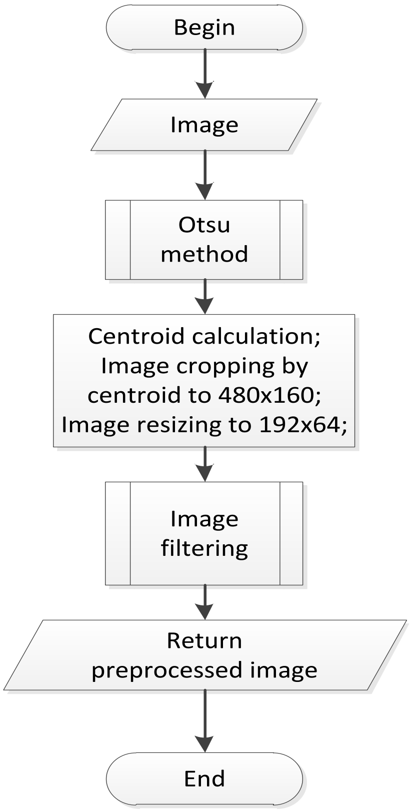
Begin
Image
Otsu method
Centroid calculation; Image cropping by centroid to 480x160; Image resizing to 192x64;
Image filtering
Return preprocessed image
End

Fig. 2. Block diagram of the image preprocessing algorithm

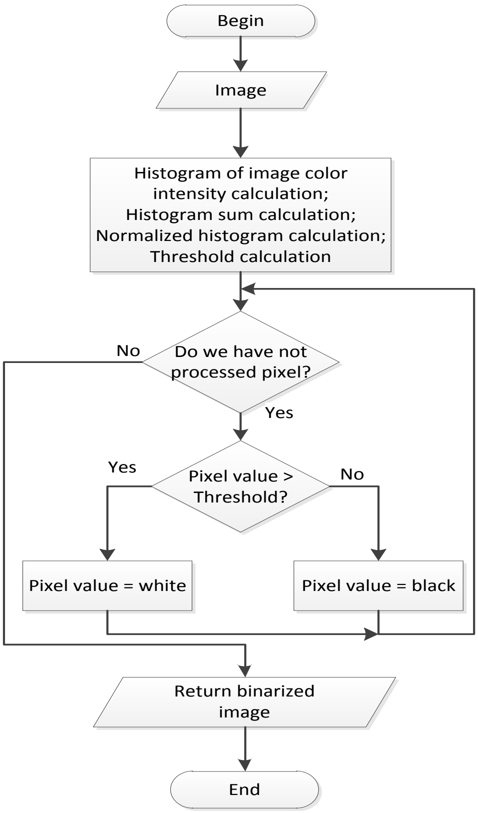
Begin
Image
Histogram of image color intensity calculation; Histogram sum calculation; Normalized histogram calculation; Threshold calculation
Do we have not processed pixel?
No
Yes
Pixel value > Threshold?
Yes
No
Pixel value = white
Pixel value = black
Return binarized image
End

Fig. 3. Block diagram of the Otsu method

Thus, binarization allows us to determine the center of the area of interest (the conditional center of the finger) and to obtain a scaled image that will be used to highlight the pattern of veins.

IV. Image Quality Improvement and Biometric Features Extraction

Next, it is necessary to create the biometric image that contains the features of user's finger veins as a digital code. But since the input image has a low contrast value, it needs to be increased. This procedure can be performed, for example, using a modified Gaussian high-pass filter [14]. The filter is calculated by the formula:

$$H(x,y)=a\left(1-e^{-D^2(x,y)/2D_0^2}\right)+b\,,$$

where $D(x,y)=\sqrt{(x-x_0)^2+(y-y_0)^2}$ – distance from a point (x, y) to a cutoff frequency locus with coordinates (x_0, y_0); D_0 – cutoff frequency locus distance from origin of coordinates; a and b – correcting variables for changing the amplitude and the initial level of the filter mask signal. An example of the filtering result is shown in Fig. 4.

After filtering, the image has a sufficient level of contrast to extract the biometric code, which describes the features of the venous pattern in the form of texture descriptors.

Different approaches to texture analysis are possible. In this case, the features of the venous finger pattern of vehicle user are detected using the algorithm LLBP (Local Line Binary Pattern). To extract the biometric image, this technique uses a new texture descriptor [15]. One of the advantages of the LLBP algorithm is that it can emphasize the change in image intensity (for example, in the area of bifurcation (separation) of vessels, in the areas of the end or bend of the vessel).

The operator used for texture analysis consists of two components: horizontal ($LLBP_h$) and vertical ($LLBP_v$) components. The LLBP value can be obtained by computing the binary string codes for both components. These components are calculated by the following formulas:

$$s(x)=\begin{cases}1, & x\geq 0,\\ 0, & x<0,\end{cases}$$

$$LLBP_h(x,y)=\sum_{n=1}^{c-1}s(h_n-h_c)\cdot 2^{c-n-1}+\sum_{n=c+1}^{N}s(h_n-h_c)\cdot 2^{n-c-1}\,,$$

$$LLBP_v(x,y)=\sum_{n=1}^{c-1}s(v_n-v_c)\cdot 2^{c-n-1}+\sum_{n=c+1}^{N}s(v_n-v_c)\cdot 2^{n-c-1}\,,$$

$$LLBP=\sqrt{LLBP_h^2+LLBP_v^2}\,,$$

where $s(x)$ – threshold function; N – length of pixel line; $c=N/2$ – central pixel position (h_c, v_c).

Fig. 5 shows the graphical result of the LLBP encoding for the vertical, horizontal, and final component.

The further authentication process is based on comparing the extracted features with template features stored in the database. When identifying, the similarity between them can be measured using, for example, the Hamming distance.

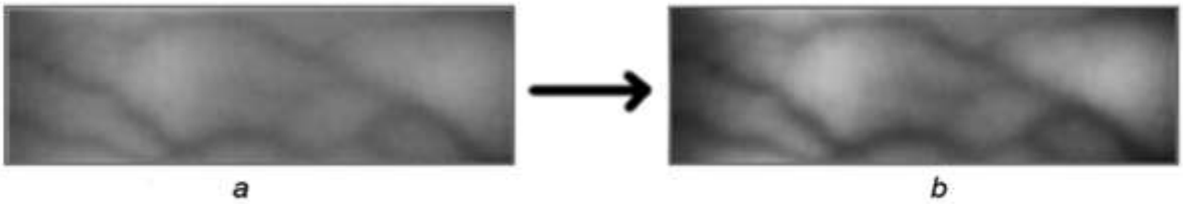

Fig. 4. Image filtering result: *a* – original image, *b* – filtered image

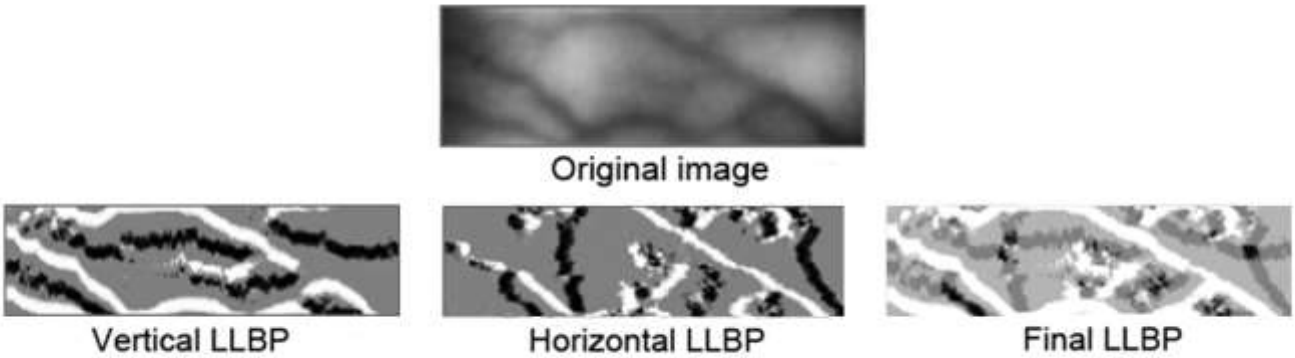

Fig. 5. Result of encoding by the LLBP method

Since the images of one user, calculated at different time intervals with different positions of the finger, can differ from each other, the recognition algorithm shall consider these differences. Therefore, the comparison is performed using a threshold value, the change of which will influence the recognition accuracy and the magnitude of the errors of the first and second kind. In the presence of these errors there is a successful authentication of the user who is absent in the database, or access to a legal user is denied, respectively [16].

The threshold value should be selected based on statistical error rates for different threshold values [17]. At the choice of value it is required to minimize indicators of errors of the first and second kind.

V. Conclusion

The biometric image, extracted from the image of the blood vessels and defining the specific points of the veins, makes it possible to accurately identify a specific user. Patterns of blood vessels are unique for each person and, unlike fingerprints, they can not be faked, so it is not necessary to re-register users through certain periods.

In this research, a functional model of the work of the biometric authentication module based on finger veins was developed; algorithms for image pre-processing and biometric features extracting were considered.

Depending on the mode of operation of the biometric immobilizer module, the extracted image is either recorded in the database or compared with the existing etalon images in the database. In the second case, a decision about the degree of images coincidence is made.

References

[1] S. Tillich, M. Wójcik "Security Analysis of an Open Car Immobilizer Protocol Stack" in Proceedings of 4th International Conference on Trusted Systems. Lecture Notes in Computer Science. C.J. Mitchell and A. Tomlinson, Eds. 2012. Vol. 7711. Pp. 83-94. https://doi.org/10.1007/978-3-642-35371-0_8.

[2] J. Wei, Y Matsubara and H. Takada, "HAZOP-Based Security Analysis for Embedded Systems: Case Study of Open Source Immobilizer Protocol Stack". In Recent Advances in Systems Safety and Security. Studies in Systems, Decision and Control. E. Pricop and G. Stamatescu, Eds. 2016. Vol. 62. Pp. 79-96.

[3] J.C. van Ours, B. Vollaard, "The Engine Immobiliser: A Non- starter for Car Thieves". The Economic Journal. 2016. Vol. 126, No. 593. Pp. 1264–1291.

[4] S. Prabhakar, S. Pankanti and A.K. Jain, "Biometric recognition: security and privacy concerns", IEEE Security & Privacy,vol. 99, Issue 2, pp. 33-42, Mar-Apr 2003.

[5] C.-N. Liang, H.-B. Huang and B.-C. Chen, "Fingerprint Identification Keyless Entry System," International Journal of Electronics and Communication Engineering, vol. 2, No. 8, pp. 1554-1559, 2008.

[6] A. Kumar, Y. Zhou, "Human identification using finger images," IEEE Transactions on Image Processing, 21 (4), pp. 2228-2244, 2012.

[7] S.C. Draper, A. Khisti, E. Martinian, A. Vetro and J.S. Yedidia, "Using distributed source coding to secure fingerprint biometrics". IEEE International Conference on Acoustics, Speech and Signal Processing, Hawaii, pp. 129–132, 2007.

[8] Y. Zhou and A. Kumar, "Human identification using palm-vein images". IEEE Transactions on Information Forensics and Security. 6 (4), pp. 1259-1274, 2011.

[9] S. Liu and Sh. Song, "An embedded real-time finger-vein recognition system for mobile devices". IEEE Transactions on Consumer Electronics, vol. 58, Issue 2, pp. 522-527, May 2012. DOI: 10.1109/TCE.2012.6227456

[10] S.I. Suyatinov, S.V. Kolentev and T.I. Bouldakova, "Criteria of identification of the medical images". Proceedings of SPIE - The International Society for Optical Engineering, vol. 5067, pp. 148-153, 2002.

[11] N. Kaur and P. Chopra, "Vein Pattern Recognition: A secured way of authentication". International Journal of Engineering And Computer Science, vol. 5, Issue 10, pp. 18377-18383, Oct. 2016. DOI: 10.18535/ijecs/v5i10.26

[12] C. Wilson, Vein Pattern Recognition: A Privacy-Enhancing Biometric, CRC Press, 2017, 307 p.

[13] N. Otsu, "A threshold selection method from gray-level histograms," IEEE Transaction Systems, Man, and Cybernetics, vol. 9, No. 1, pp. 62-66, 1979.

[14] E.C. Lee, H. Jung and D. Kim, "New finger biometric method using near infrared imaging," Sensors, 11(3), pp. 2319–2333, 2011.

[15] A.R. Bakhtiar, W.S. Chai and A.S. Shahrel, "Finger Vein Recognition Using Local Line Binary Pattern," Sensors, 11(12), pp. 11357-11371, 2011. doi:10.3390/s111211357

[16] K.W. Ko, J. Lee, M. Ahmadi and S. Lee, "Development of Human Identification System Based on Simple Finger-Vein Pattern-Matching Method for Embedded Environments," International Journal of Security and Its Applications, vol. 9, No. 5, pp. 297-306, 2015. URL: http://dx.doi.org/10.14257/ijsia.2015.9.5.29

[17] R. Chopra and S.Kaur, "Finger print and finger vein recognition using repeated line tracking and minutiae," International Journal of Advanced Science and Research, vol. 2, Issue 2, pp. 13-22, 2017.