Biometric identification and authentication based on a new method of a pulse wave contour forming

M S Gerashchenko¹ ², A G Fateev¹, M V Markuleva¹ ², A N Astafyev³, S L Zefirov¹ and S I Gerashchenko¹

¹Penza State University, 40 Krasnaya str., Penza, Russia, 440026
² "PROMED" L.L.C., 3-73 Ostrovsky str., Penza, Russia, 440011
³ Lipetsk State Technical University Lipetsk, 30 Moscow ave., Lipetsk, Russia

E-mail: mpo@list.ru

Abstract. The paper considers authentication methods, including biometric. The advantages, disadvantages and limitations of the known authentication methods are considered, and for the first time it is proposed to use hydrocuff pulse wave technology for biometric identification. A parameters set characterizing the pulse wave contour and its derivatives is defined. As the pulse wave mathematical processing result, a multiparametric feature space is formed. The paper considers the main problems that arise when collecting source data. To solve legal and ethical issues, as well as reduce the cost of forming a database, the possibility of applying algorithms for generating synthetic biometric images has been proved. Synthetic biometric images are designed to use neural network technologies for identification and authentication based on the large databases analysis.

1. Introduction

An information systems user authentication is a procedure for verifying its authenticity. Authentication is implemented by using authentication attributes. This procedure is usually classified according to which attribute is applied. A certain amount of information known to the user and the verifying system can be used as an attribute of the authentication procedure. Various devices can also be used – personal identifiers that store some information in the built-in memory that is used as an authentication attribute. The user's authenticity is confirmed by the presence of such a device. The use of personal identifiers requires the user to enter a value that confirms that the device can be used. As an example, there are various types of smart cards that require entering an attribute such as a PIN. At entering such an attribute corresponding to the device, the last is activated and the access possibility to its memory appears to read additional authentication attributes.

The reasons for the wide use of the described authentication methods are its implementation simplicity which does not requires from user special skills, the user authentication procedure minimal training time, low cost software and hardware that implement the procedure [1,2].

But in addition to the advantages, authentication using passwords or special devices has a number of limitations and disadvantages. The password can be materialized on any medium if it is difficult for the user to remember it. This makes possible for an intruder in getting the password. The device used in identification and authentication procedures may be lost or stolen.

Another type of authentication is biometric authentication, which consists of a person's identity unique features using. Biometric features are usually divided into static, which does not change or almost
does not change over a lifetime, and dynamic, which can change over a short period of time. Static features include fingerprints, 2D or 3D facial geometry, thermography, and others. Dynamic features include handwriting, keyboard typing, and voice. In this case, the voice can pronounce a keyword (password) or an entire phrase. Also, when using keyboard or handwriting, a keyword can be played. Using some features requires specific software and hardware, which is complex and has a high cost. For example, such software is necessary when using geometric features of the face or hand. Some features do not require such software, but there is a high probability of image forgery. For example, when using voice input of a keyword. Using keyboard input requires the user to be skilled with the keyboard, otherwise the system will not be able to recognize the user. Using handwritten input of a keyword or phrase requires the use of an input device (tablet and pen). However, there is also the possibility of handwriting forgery. In addition to these limitations, dynamic features have another specificity - dependency on the person emotional state. Emotional outbursts reduce the probability of the information system recognizing a person as a registered ("its") user.

Often the best option is considered to be using a fingerprint. The fingerprint does not change over a lifetime, and there are almost no factors that can affect the quality of recognition. However, recently there have been reports about the possibility of fingerprints forgery [3,4]. Moreover, manufactured moulages allow to pass identification and authentication procedures on behalf of the person whose fingerprint is forged. Noted that it was possible to make a moulage only from a photo of the hand on which the papillary pattern is visible.

Another difficulty in using biometric authentication is the need to train the system to successfully recognize the user. This requires the accumulation of a certain amount of data about the used trait(s) of personality. It also requires the user participation, so the user's time is required. Next, the checking whether the system is ready to recognize (authenticate) the user is needed (test the system). Besides, the system must be held through additional training periodically. It may be required periodically or when the number of errors in user recognition increases. The additional training consists in collecting additional data about the used biometric characteristic of the individual and adjusting the system parameters used in the user recognition and decision-making procedure.

The decision about the successful authentication possibility is made based on comparing the characteristics of the presented attribute with a certain standard of the attribute that was formed during the system training and testing. If the current value is inside the allowed deviation interval from the standard, the system considers that the user is registered. Thus, each characteristic of the attribute is checked. So, a certain measure of trust is established. If the characteristic value is outside this interval (confidence measure), the user does not pass the authentication procedure.

When performing an authentication procedure using biometric attributes, two types of measurement errors are possible: errors of the 1-st kind, when a user registered in the information system is not authenticated and is not recognized as an authorized user, and errors of the 2-nd kind, when the violator is successfully authenticated and recognized as a registered user.

To solve the problems that arise when using biometric features, it is proposed to use various methods. Both to protect against forgery, and to improve the user recognition accuracy, also to simplify the system training process and user authentication, etc. Therefore, a number of sources [5,6] consider the possibility of using other biometric features – electroencephalogram, features of the cardiovascular system functioning.

As an advantage of using biometric authentication of features related to the cardiovascular system functioning, it is noted that it is impossible to forge an image and, accordingly, it is impossible to impersonate another person. Attempts to influence the cardiovascular system operation will lead to the user authentication inability only. The user impersonation will be unsuccessful.

In [7,8,9], the using photoplethysmogram (PPG) possibilities in biometric authentication systems were evaluated. However, it should be noted that this approach is characterized by disadvantages: the signal-to-noise low ratio value, a complex mathematical relationship that connects the pulse wave shape with the cardiovascular system state, the sensor positioning errors, and the biometric images owners features. The method's noted disadvantages allows to conclude that it is difficult to use this method and
lead to the need to use other biometric data. Its obtaining based on the analysis of the pulse wave contour (PWC). Some various characteristics in the time domain as biometric descriptors have been described in a number of papers. For example, the rising and descending front and the peak time (duration) were used [10]. The zero intersection of the first and second derivatives of the photoplethysmographic signals was also used to identify points of interest [11].

The main focus is on the use of peak positions, relative amplitudes, slopes (fronts) based on derivatives, and time intervals between experiments. In some studies, it was proposed to use up to 40 characteristics using the algorithm for ranking characteristics with K-dimensional clustering [12].

2. Materials and methods
This paper proposed person identification method based on hydroplethysmogram processing. A hydroplethysmogram (HPG) is a pulse wave signal forming based on pressure changes in the occlusive cuff fixed on various parts of the body (finger phalanges, forearm, wrist). [13]. This method's peculiarity is the presence of functional relationship of pressure in the artery under hydrocuff, with a hydrocuff pressure change during the pulse wave passage under hydrocuff (PWHC). This makes possible to use hydrocuff technology to identify individuals on the cardiovascular system state individual characteristics basis.

When a pulse wave passes under the cuff, the pressure in the artery causes a proportional pressure change in the cuff. Figure 1 shows the pressure change in the hydrocuff for a single heartbeat and the first derivative of pulse wave (PW).

![Figure 1](image)

The pulse wave has characteristic individual patterns that reflect the heart and arteries activity. The left ventricle contraction is associated with increased pressure in the arteries. As a result, there is an increase in the hydrocuff pressure in proportion to the systolic pressure to the value of $P_{\text{max}}$. This is followed by a pressure drop to $P_{\text{min}}$. On the pressure drop curve, there is a slight increase in pressure $\Delta P$, formed by the arteries contraction. The values of the basic characteristic points $P_{\text{max}}$, $P_{\text{min}}$, $\Delta P$, the cuff pressure rate of increase and decrease $V_{\text{max}1}$, $V_{\text{max}2}$ allows to form a multiparametric feature space that underlies the person identification procedure.

In real conditions, the curve amplitude-time characteristics differ. This results in the formation of a parameters scatter dynamic range that underlie the object image creation. In this regard, the characteristic points of the pulse waves formed are accompanied by a natural process of changing the heart and blood vessels activity over time and their variability depending on the state of individual at the image formation moment and the person identification.

Additionally, it is necessary to take into account errors in the characteristic points estimation values, the rise and fall rate of the pulse wave values.
As a result of the conducted studies of the regularities that characterize the process of PW formation, taking into account the parameters variability and errors in their estimation, the following data values are obtained, given in table 1.

Table 1. Statistical characteristics of the characteristic points position parameters variability on the pulse wave and its derivative.

| Parameter | Mathematical expectation | Average square deviation | Error |
|-----------|--------------------------|--------------------------|-------|
| $P_{\text{max}}$ | 110                      | 8                        | 5     |
| $P_{\text{min}}$ | 80                       | 5                        | 3     |
| \(\Delta P\) | 12                       | 1                        | 1     |
| $V_{\text{max1}}$ | 153                      | 3                        | 1     |
| $V_{\text{max2}}$ | 267                      | 2                        | 3     |

An analysis of the values shown in the table indicates that PWRC signals may represent potential for use in authentication, but the results are characterized by errors comparable with the standard deviations values. In this regard, there is a need for additional research related to the formation of expanded different individuals database.

One of the important tasks that need to be solved in biometric authentication is to determine the characteristics that will be recorded at system training and forming the registered user image. This characteristics set is used to create the user reference image. The same characteristics are recorded each time a user tries to authenticate for comparison with the reference image. For example, when using handwriting, the characteristics display the pen movement on the tablet when writing a password word or phrase. When using any biometric attribute, a similar approach is used to create the user reference image and compare the current recorded values with the reference. Additional parameters are proposed to be formed on the calculation of the first, second and third PW signal derivatives basis. Figure 2 shows the graphical dependencies of the PW contour and its derivatives. By axle 0Y, the PW amplitude in millimeters of Hg is deposited. For results clarity presentation, coefficients are selected for derivative curves, the coefficients for the first derivative are 6, for the second 60, and for the third 600. Similarly, the derivatives curves are raised relative to the reference point by 80 mmHg for the 1st derivative, 77 mmHg for the 2nd derivative, and 75 mmHg for the 3rd derivative.

![Figure 2. The PW Curve and its derivatives of 1,2,3 order.](image)

The recorded signal individual pulse waves are analyzed. This raises the problem that the duration of one full heart cycle depends on the instantaneous pulse rate, which is controlled by the autonomic nervous system. Therefore, matching is a complex procedure for any two pulses, even those received from the same person, with different instantaneous pulse rates (for example, before and after the experiment). This problem can be solved by selecting the most informative cycle. The assumption is
that any biometric system that uses HPG signals must show the ability to adapt a wide range of instantaneous heart rate values.

The signal is approximated by Gauss functions. The main key points (characteristics) are the systolic peak, diastolic peak, dicrotic surge, and the pulse base. In [14] is also noted that the corresponding standard PPG waveform contains the specified characteristics.

In addition to the above characteristics, it is proposed to use the width or value of one pulse wave period. It is also proposed to consider the first, second and third derivatives of the HPG signal, namely their transition points through zero, which are the key. Another unique characteristic of the pulse wave for each person is the rate of pressure reduction from the systolic peak to the dicrotic surge.

In [15], the pulse wave characteristics are distinguished taking into account the region to which they belong - the time and frequency regions. The following characteristics are distinguished from the time domain: the full amplitude of all turning points, the area under the pulse wave curve, the positive and negative speed of wave change, and the positive and negative slope of each pulse wave. In the frequency domain, the following characteristics are distinguished such characteristics as the magnitude (amplitude) and the value of the power spectral density (PSD) in the ranges from 0.5 to 5 Hz, from 5 to 10 Hz, from 10 to 15 Hz, from 15 to 25 Hz.

This paper proposed a method based on the use of a hydrocuff for fixing the pulse wave, which also consists in identifying key characteristics that will be used for identification and authentication of the individual in the future. Taking into account the research results provided in the studied sources, which contain a description of the PPG used key characteristics, it is necessary to determine the pulse wave key characteristics set for identification and authentication using hydrocuff technology. The key characteristics set of the pulse wave determined during the research will be further refined based on the results obtained during the databases formation on field experiments basis.

Studying the pulse wave characteristics allows to identify a greater number of characteristics. However, despite the increased identification accuracy, an increase in the number of characteristics will increase the processing time of such a set and increase the complexity of training neural networks that are proposed to be used in identification and authentication procedures.

Based on the sources review results that provide PPG characteristics proposed for identification and authentication, as well as taking into account the pulse wave noted characteristics, the following key characteristics are proposed in this paper: amplitude, area under the pulse wave curve, positive and negative rate of wave change, the pulse wave positive and negative slope, the value (amplitude) and the spectral power density value in the range from 0.5 to 5 Hz, from 5 to 10 Hz, from 10 to 15 Hz, from 15 to 25 Hz.

At research conducting, the possibility of characteristics number changing to reduce the amount of training data for the neural network and reduce the neural network training time is evaluated. Also, the PW characteristics set used for biometric authentication is determined based on the user recognition reliability (the number of errors of the 1-st and 2-nd kind).

3. Results

Pulse wave signals were received using the "Hemodin 2" device. The pressure signal processing algorithm is implemented as a virtual instrument using LabVIEW software. The graphic processing was performed using MATLAB R2015b software, the participant’s age and health status were taken into account. Participants were divided into groups based on their age. The results of measuring the participant's pressure were also taken into account. During the research, a group of participants with normal pressure parameters was identified, as well as groups of participants with increased and reduced values. A similar approach was used in the study described in [15]. Such a division into groups is necessary due the participants state affects the results obtained.

In this regard, another problem related to the collected data processing should be noted. The data collected from participants contains information about their health status. People are very sensitive to the collection and processing of such information and often do not want it to become known to others.
or used to achieve any results. Therefore, at information collecting, the consent to its collection and processing must be obtained.

In addition to the ethical side of the problem, there is also a legal one. In many countries, there are regulatory legal documents that establish requirements for the personal data collection and processing, which include the personal PWCHC characteristics. There are national laws worldwide "on personal data" and a large number of other normative legal documents that define the procedure for collecting and processing personal data, as well as requirements for ensuring their security. Compliance with all established requirements leads to the need to implement a large number of measures (organizational and technical). This requires significant costs to implement such measures. When processing special personal data categories, which include pulse wave characteristics (personal health data), the requirements are tightened. With a large volume of raw data collected, significant efforts will be required to comply with the provisions of existing regulatory documents. Starting from the consent receiving of the established content personal data processing and up to the personal data destruction when the processing purpose is achieved.

These problems can be partially solved by reducing the amount of raw data collected by reducing the number of participants from whom this data is collected. Persons interested in conducting research and obtaining its results can be involved in the data collection process. This will partially reduce the amount of work aimed at meeting the requirements of regulatory legal documents that establish requirements for the processing and protection of personal data. In this case, there is a problem with the research results reliability, since the more source data is used, the higher the obtained research results reliability. However, this problem can be solved by using artificial (synthetic) source data.

4. Conclusion

As the conducted research result, it is concluded that the hydrocuff technology and the hydroplethysmogram being removed allows to form a PW contour with increased amplitude-time characteristics values, which significantly increases the signal-to-noise ratio, and as a result, a better the pressure curve contour representation.

One possible way to solve problems related to the raw data collection (pulse waves) is to use synthetic biometric images. Such images do not belong to specific individuals, so there is no need in consent obtaining and resolving other issues related to the personal data collection and processing. The task of forming synthetic images occurs when they are formed.

It is necessary to take into account both the age and features of the individual condition, when generating synthetic images. Namely, when using algorithms allowing to create synthetic images based on natural biometric images of two people, it is needed to choose images of two people in the same age group as initial images. Also, their cardiovascular system state should be the same, or have no significant differences (diseases and abnormalities).

The obtained synthetic biometric images will be used for training an artificial neural network and evaluating the required data amount for the image of the information system registered user.

References

[1] Website of Public company “XCom” Retrieved from: https://www.xcomspb.ru
[2] Website of Public company “IT-Trade” Retrieved from: https://cryptostore.ru
[3] Tarang Chugh, Kai Cao and Anil K Jain 2018 Fingerprint Spoof Buster: Use of Minutiae-Centered Patches Information Forensics and Security IEEE Transactions on 13(9) 2190-202
[4] Alizar A 2014 Fingerprinting based on photographs of hands Retrieved from: https://xakep.ru
[5] Ruiz-Blondet M V, Jin Z and Laszlo S 2016 CEREBRE: A Novel Method for Very High Accuracy Event-Related Potential Biometric Identification in IEEE Transactions on Information Forensics and Security 11(7) 1618-29
[6] Yokota T et al. 2020 A conformable imager for biometric authentication and vital sign measurement Nat Electron 3 113-21
[7] Sarkar A Abbott A L and Doerzaph Z 2016 Biometric authentication using
photoplethysmography signals 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems 1-7

[8] Petros S, Jiexin G and Dimitrios H 2011 Feasibility study of photoplethysmographic signals for biometric identification 17th International Conference on Digital Signal Processing 1-5

[9] Sancho J, Alesanco Á and Garcia J 2018 Biometric authentication using the ppg: a long-term feasibility study Sensors 18(5) 1525

[10] Gu Y Y, Zhang Y and Zhang YT 2003 A novel biometric approach in human verification by photoplethysmographic signals, in information technology applications in biomedicine 4th International IEEE EMBS Special Topic Conference 13-4

[11] Jianchu Yao, Xiaodong Sun and Yongbo Wan 2007 A pilot study on using derivatives of photoplethysmographic signals as a biometric identifier, in Engineering in Medicine and Biology Society EMBS 29th Annual International Conference of the IEEE 4576-9

[12] Kavsağlu A R, Polat K and Bozkurt M R 2014 A novel feature ranking algorithm for biometric recognition with PPG signals Computers in Biology and Medicine 49 1-14

[13] 2017 Gerashchenko M S and Gerashchenko S I Electronic tonometer Pat. of the Russian Federation 2652070

[14] Francesco Rundo et al. 2018 Advanced bio-inspired system for noninvasive cuff-less blood pressure estimation from physiological signal analysis Sensors (Basel) 18(2) 405

[15] Xiaomi Ma Non-invasive blood pressure measurement algorithm for all age groups Retrieved from: https://openrepository.aut.ac.nz