Requirements for the Procedure for Assessing the Operator's Person When Processing Accelerometer Data

A V Grecheneva¹, N V Dorofeev¹, M S Goryachev¹

¹Vladimir State University, Gor’kogo st. 87, Vladimir, 600000, Russian Federation

E-mail: dorofeevnv@yandex.ru

Abstract. The article considers the possibility of biometric authentication based on gait parameters, which are obtained after intelligent processing of the accelerometer data of a wearable device. The article discusses the main trends and trends in the field of biometric authentication, as well as authentication by gait parameters. The developed neural network algorithm and informative parameters are described in the authentication procedure based on the data of a single sensor of a portable device. The practical verification of the proposed approach is carried out on 32 subjects of different physiology. The results of the study show the possibility of distinguishing their own movements in 100% of cases, and the distinction of the subjects is more than 90%. Also, the final part of the article provides the requirements for the authentication procedure when processing accelerometric data of gait biometrics, the level of trust of the developed algorithm is determined.

1. Introduction

Currently, cases of fraud in relation to users personal data and forgery of user biometrics have become more frequent [1]. To increase the reliability of the authentication procedure, cybersecurity experts note special prospects for using dynamic biometric data called behavioral biometrics [2-4]. Since 2017, this direction has been actively developing within the framework of state programs: the Russian project "Unified Biometric System", the American project DARPA, as well as the National Cybersecurity Center of the UK, followed by the largest global and Russian banking and financial structures Visa, MasterCard, Rosbank, Tinkoff Bank, Alfa-Bank, and the flagships of the IT industry Apple Pay, Android Pay, Samsung Pay, Rostelecom.

The concept of behavioral biometrics is based on the provisions that human movements are individual and their analysis allows us to identify the user with a high degree of reliability. The subject of behavioral biometrics analysis is often keyboard handwriting, features of finger movements when working with a mouse, screen, touch panel and other manipulators [5-7], less often features of gait and posture, features of facial expressions. This is due to the insufficient elaboration of taking into account the parameters of the individual norm of movements in existing mathematical models, as well as the insufficient efficiency of algorithms for processing data on the parameters of human movements [8, 9]. It should be noted that a person's gait is a chain of sequentially fixed conditionally reflex motor actions (dynamically changing patterns) that are performed by the human body automatically, i.e. without the participation of consciousness [10-13]. The nature of gait and its features are determined by a combination of individual physiological and psychological factors (anthropometric signs, features of the nervous system, the presence of habits, etc.) [14]. At the same time, attempts to consciously...
control and copy the nature of someone's gait will still lead to changes in its parameters (step length, step base, step speed, step frequency, step cycle, support period, transfer period) and suspicious behavior indicating a deviation from the norm can be recognized by various systems as fraudulent.

The mechanism of user authentication based on the parameters of his gait is based on the task of motion control, represented as a multidimensional model of gait biomechanics, which has three outputs and many inputs for controlling the actuators-muscles [15]. It should be noted that the process of walking is a complex multiparametric process, during which the human body uses a significant number of muscles and ligaments. Therefore, the solved task of analyzing the biomechanics of gait has a large dimension, which allows us to draw conclusions about the uniqueness of the user's gait and to assert the expediency of using the proposed method of user authentication based on biometric gait parameters in practice. In this case, based on the control and analysis of the correspondence of gait parameters to the individual pattern of user movements, it is possible to increase the reliability of authentication in systems with limited personal access.

Currently, in Russia and abroad, there is a tendency to develop the direction of research of gait parameters and individual motor activity according to accelerometers built into mobile devices [16-22]. However, the use of data obtained using motion sensors (accelerometers, gyroscopes) built into personal wearable devices (smartphones, fitness trackers, smart watches) is not common for solving tasks of increased responsibility, which is the task of user authentication. This is due to the insufficient accuracy and reliability of measurements associated with the high noise level of the signals of the motion sensors, exposure to the influence of multiplicative interference, as well as the need to take into account the facts of false movement of personal devices relative to the user.

Therefore, the above facts determine the possibility of using gait parameters as unique biometric identity identifiers, and the technological capabilities of measuring gait parameters using wearable devices and the possibility of intelligent data processing using specialized algorithms that provide the required accuracy and reliability, allow us to judge the possibility of successful implementation of a new technology of enhanced user authentication based on data from wearable devices and smartphones on, what is the current direction in the field of information security.

This paper presents the results of a scientific research aimed at developing a technology for enhanced user authentication based on data from wearable devices and smartphones based on intelligent processing of biometric gait parameters.

2. Personality assessment
To assess the levels of rigor and determine the requirements for the authentication technology being developed based on gait parameters recorded using a single accelerometer sensor built into the wearable device, it is necessary to assess the probability of errors of the first and second kind of authentication algorithm.

During the preliminary analysis, informative parameters were established: the duration of movement and the shape of the accelerometer signal, the standard deviation, the composition of the frequency spectrum.

For each user, movement patterns are selected and a neural network classifier is trained. The duration of the maximum time of the template is taken as the value of the time window. All patterns are normalized in amplitude and supplemented with zeros up to the duration of the maximum pattern (time normalization). Further, during the operation, the data read from the phone's accelerometer is processed within the time window. Each component (axis) of the accelerometer is processed separately. This makes it possible to bring the dependence of the data on the sensor orientation to zero.

The read data located within the time window is normalized. The average value and the standard deviation of the time window data are estimated. After that, the correlation value of the time window data and each of the templates is evaluated. If the correlation value exceeds the set threshold of 0.8, a neural network classifier is launched. A multilayer direct propagation network is chosen as the basic structure for a neural network. It is proposed to use cross-entropy as an optimization criterion. The
activation function of the hidden layer is a sigmoid, and the output layer is a normalized exponential function.

Further, in the case of selecting the subject's template from the time series using an intelligent algorithm, an additional comparison is made with the data stored in the personal information map of movements. After that, the probability of risk is calculated using a digital model of the frequencies of the initial gait signs. As a result of the assessment of the compliance of the obtained value of the risk probability with the established threshold, a decision is formed on the positive or negative passage of the authentication process by the user.

The level of rigor and requirements for the developed technology are supposed to be chosen in accordance with the new generation standards in the field of authentication [23-25].

3. Practical verification
The practical test was carried out on 32 male and female subjects of different ages, gender, weight and posture. To complicate the experiment, the subjects were divided into subgroups (according to similar physiological characteristics) of 4 people. The volume of the training sample was formed from the movements that were performed with different clothes and the location of the phone in it. Basic movements: walking, and without on a flat and inclined surface on a light and with a straight line and stairs with a load (a bag with a laptop weighing 3.5 kg) and without it. Thus, the research reflected the main movements performed in a person's daily life. The level of rigor of the proposed algorithm can be appreciated by Figure 1. As can be seen from the figure, the proposed algorithm allows you to distinguish your own movements in 100% figure 1a, to distinguish the subjects when performing different movements in more than 90% of cases figure 1b.

4. Conclusions
Thus, in the course of the research, it was found that the use of a single accelerometric sensor of a mobile phone allows you to distinguish between both individual human movements and movements made by different people. According to the developed technology, the daily user biometrics reading and the identification of unique gait signs will be carried out in the background of personal wearable devices, which will allow training intelligent algorithms with a high degree of accuracy. It is also supposed to take into account the dynamics of daily activity and its time frame (for example, every

![Figure 1. Example of the authentication result.](image-url)
day at a certain time of the day an office employee walks in order to get to a vehicle, then for a certain number of hours he is in a sitting position, etc.), as well as personal characteristics of heart rhythms.

The user authentication process will be carried out at the active request of the user (with an existing statistical database about the user), in case of successful completion of which, together with other authentication methods, the system will be granted access to high-responsibility operations. At the same time, for successful authentication, it is enough for the user to perform a simple action. It should be noted that in order to increase the level of confidence in the gait authentication procedure, it is necessary to conduct studies on a larger number of subjects. In this regard, at this stage, the level of trust in this authentication technology in accordance with international standards is correlated as low. This corresponds to the recommendations of international standards regarding resistance to selection attacks – 10 to 1000 with a minimum key length of 4 to 10 bits. However, it is possible to improve this indicator in the "biometrics-code" conversion procedure by increasing the effective key length to 30% or more of the biometric key length. In general, with an increase in the duration of the analyzed time window, the probability of a successful selection on the first attempt will be less than 10-10. With multi-factor authentication, as well as improvements to the proposed authentication algorithm, the level of trust can correspond to medium or high.

The approaches proposed within the framework of the project and the results obtained will not only provide a solution to the problem of increasing the reliability of user digital operations and procedures performed through information authentication systems, but also to obtain new dependencies of the dynamics of spatial and temporal gait parameters necessary for research in the field of medical orthopedics and diagnostics, as well as bionic robotics.

5. References
[1] Chaos Computer Clubs breaks iris recognition system of the Samsung Galaxy S8 URL: https://www.ccc.de/en/updates/2017/iriden
[2] YampolskiyVenu R and Govindaraju V Int. J. of Biometrics 1 83-113
[3] Schumacher G Behavioural 2012 Second Generation Biometrics: The Ethical, Legal and Social Context vol 11, ed E Mordini and D Emilio (Netherlands: Springer) p 354
[4] Dovgal V A and Dovgal D V 2017 Bull. of the Adyghe State Univer. Series 4: Natural-Mathem. and Tech. Sci. 3 139-42
[5] Krutokhvosot D S and Khitsenko V E 2017 Cybersecurity 5 91-9
[6] Sulavko A E and Shalina E V 2019 App. Informatics 14 39-5
[7] Faundez-Zanuy M, Fierrez J, Ferrer M A, Diaz M, Tolosana R and Plamondon R 2020 Cognitive Computation 12 940-53
[8] Dorofeev N V and Grecheneva A V 2020 IOP Conf. Series: Materials Sci. and Engin. 873 1-7
[9] Dorofeev N V, Grecheneva A V and Buzhinsky V S 2021 Biomedical Engin. 2 11-4
[10] Skvortsov D V 1996 Clinical analysis of movement. Gait analysis (Ivanovo: Publishing house SPC - "Stimulus") p 344
[11] Stolyarov A. Yu. 2015 Bull. of the Volga State University. Series 1: Math. Physics 1 47-51
[12] Izholdina V V, Budkov V Yu and Denisov A V 2018 Sci. Result Inf. Techno. 4 48-62
[13] Zhang R, Vogler C and Metaxas D N 2006 Gait Recognition Using Hidden Markow Model vol 4221, ed Changhong C, Jimin L, Heng Z and Hu H (Berlin: Springer) pp 399-407
[14] Shenderov V A, Kitaev N N and Negreeva M B 2007 Rus. J. of Biomechanics 2 75-8
[15] Khodashinsky I A, Savchuk M. V., Gorbunov I V and Meshcheryakov R V 2011 Reports TUSUR 2-3 236-48
[16] Erokhin A L and Lednev S N 2017 Vestnik NTU KHP 1 54-64
[17] Kazantseva A G and Lavrov D N 2011 Math. Structures and Modeling 23 31-7
[18] Helvas A V, Belyankina N G, Gilya-Zetinov A A, Chernikova D D, Shabunin V M and Yapruntsev E O 2017 Proceedings of MIPT 2(34) 164-75
[19] Chen Y 2016 Int. Conf. on Artificial Intell.: Technol. and Applications (Bangkok: Springer
Nature) pp 50-3

[20] Anguita D, Ghio A, Oneto L, Parra X and Reyes-Ortiz J L IWAAL 2012 Ambient Assisted Living and Home Care (Bruges: CCO Public Domain) pp 216-223

[21] Teh P S, Zhang N, Tan S-Y, Shi Q, Khoh W H and Nawaz R 2020 Journal of Ambient Intelligence and Humanized Computing 11 4019-39

[22] Zhang X, Yao L, Huang C, Gu T, Yang Z and Liu Y 2020 ACM Transactions on Intelligent Systems and Technology 11 1-24

[23] GOST R 2020 58833-2020 is the national standard of the Russian Federation Information protection Identification and authentication General provisions Information protection Identification and authentication General (Moskow: Gostroy)

[24] 2021 Unified identification and authentication system Methodological recommendations for the use of a Unified identification and authentication system (Moskow: Gostroy)

[25] GOST R 2006 52633.0-2006 The national standard of the Russian Federation Information protection Information security techniques Requirements for highly reliable biometric authentication tools (Moskow: Gostroy)

Acknowledgments
This work was supported by the grant of the President of the Russian Federation No. MK-1558.2021.1.6.