BIOMETRIC STANDARDS AND METHODS

Ivan A. Tot[a], *Jovan* B. Bajčetić[b], *Boriša* Ž. Jovanović[c], *Mladen* B. Trikoš[d], *Dušan* Lj. Bogićević[e], *Tamara* M. Gajić[f]

[a] University of Defence in Belgrade, Military Academy, Department for Information Systems and Telecommunication Engineering, Belgrade, Republic of Serbia,
e-mail: ivan.tot@va.mod.gov.rs, **corresponding author**,
ORCID iD: https://orcid.org/0000-0002-5862-9042

[b] University of Defence in Belgrade, Military Academy, Department for Information Systems and Telecommunication Engineering, Belgrade, Republic of Serbia,
e-mail: jovan.bajcetic@va.mod.gov.rs,
ORCID iD: https://orcid.org/0000-0002-3070-2594

[c] Serbian Armed Forces, Department of Telecommunications and IT, Center for Applied Mathematics and Electronics, Belgrade, Republic of Serbia,
e-mail: borisa.jovanovic@vs.rs,
ORCID iD: https://orcid.org/0000-0002-9353-724X

[d] University of Belgrade, Faculty of Organizational Sciences, Belgrade, Republic of Serbia,
e-mail: mt20135051@student.fon.bg.ac.rs,
ORCID iD: https://orcid.org/0000-0002-5243-1326

[e] Serbian Armed Forces, Department of Telecommunications and IT, Center for C4 and IT support, Belgrade, Republic of Serbia;
University of Niš, Faculty of Electronic Engineering, Niš, Republic of Serbia,
e-mail: dusan.bogicevic@gmail.com,
ORCID iD: https://orcid.org/0000-0002-4300-2490

[f] University of Belgrade, Faculty of Organizational Sciences, Belgrade, Republic of Serbia;
University of Defence in Belgrade, Military Academy, Belgrade, Republic of Serbia,
e-mail: tamara.gajic@vs.rs,
ORCID iD: https://orcid.org/0000-0002-4386-5608

DOI: 10.5937/vojtehg69-32296; https://doi.org/10.5937/vojtehg69-32296

FIELD: Computer sciences, IT
ARTICLE TYPE: Review paper

ACKNOWLEDGMENT: The authors would like to thank the Military Academy, Unversity of Defence in Belgrade (Project name: Access control management of protected resources in the Ministry of Defence and Serbian Armed Forces computer networks based on multimodal user identification, Project code: VA-TT/3/18-20).

Abstract:

Introduction/purpose: Nowadays, user identification systems play a very important role in modern society. Complex security requirements have led experts to explore ways in which biometric data can be used to identify user identities. This paper presents an overview of biometric standards and methods which can be used to identify users in biometric systems, and therefore to protect information and communication systems.

Methods: This paper deals with the problem of standardization in the field of biometrics. The first part of the paper presents concrete examples of the most widely used biometric standards. The second part of the paper gives an overview of the most used biometric methods.

Results: The obtained results show that the development of biometric systems and biometric sensors contributes to better protection of identity from misuse, because biometric technologies have great potential for improving the security and accuracy of system operation. Biometric systems improve the security of users and also provide much greater precision in establishing identity.

Conclusion: The development of biometric standards should focus on their interconnectivity, as well as on increasing connectivity with other IT standards.

Key words: biometric standardization organizations, biometric standards, biometric sensors, biometric methods.

Introduction

Nowadays, Personal Identification Numbers (PINs) or various passwords are often used for identification purposes. For example, people are asked to identify themselves when withdrawing money at ATMs, logging in on computers, using keys when opening the doors, using codes when entering buildings, typing passwords on the Internet or giving ID, passport or driver's license numbers as proof of identity. All of these methods have various disadvantages (cards and keys can be stolen, passwords can be hacked). In order to precisely identify an individual to minimize current security issues and threats, biometric technics can be used.

Biometrics is a tool that can be used to complement or even replace existing user identification systems based on what the user knows or what he or she possesses. Biometrics is one of the key methods for user recognition because it provides strong security and has great practicality (Ortega-Garcia et al, 2004).

Biometric systems use one's biological and behavioral characteristics which can be distinguished for the purpose of biometric recognition (Jain et al, 2000), (Jain et al, 2004).

There are several biometric technologies that have been used so far: fingerprint- (Lalović et al, 2019), face-, iris-, or vein arm-based (Kumar & Prathyusha, 2009), (Wang & Wang, 2017), electroencephalograms (EEGs), electrocardiograms (ECGs) (Chun, 2016), (Odinaka et al, 2012), and multispectral skin photometrics (MSP). Each of these biological characteristics uses specific biometric sensors.

The development of biometrics for user authentication has led to the development of standards for biometrics. These standards should provide the set of specifications to ensure interoperability with other biometric systems and products (Prabhakar et al, 2003).

This paper gives an overview of the most applied biometric standards as well as biometric methods that can be used to resolve security issues and threats.

Biometric standardization organizations

Each standard should be based on proven results of science, technology (technology) and experience.

Standardization organizations are divided into: formal and informal.

Formal Standardization Organizations (FSOs) develop "de jure" standards, and they form official national standards bodies and internationally recognized bodies. The examples of formal organizations for standardization are:

At the International Development Standard (SDOs) level:

- IEC - International Electrotechnical Commission,
- ISO - International Organization for Standardization, and
- ITU - International Union of Telecommunications.

At the regional level:

- CENELEC - European Committee for Standardization in Electrical Engineering,
- CEN - European Organization for Standardization, and
- ETSI - European Institute for Standardization in Telecommunications.

At the national level:

- JISC - Committee on Japanese Industrial Standards,
- ANSI - US National Standards Institute, and
- BSI - British Standards Institution.

"De facto" standards are developed by informal standardization organizations, usually by business associations and consortia. Some of them are W3C (World Wide Web Consortium), Internet Engineering Task Force and OASIS. JavaCard Forum, BioAPI Consortium and Voice XML Forum represent informal standardization organizations that deal with biometric data.

Formal standardization organizations

JTC1 ("Join Technical Committee 1") is the ISO and IEC technical committee for information technology standards. It has a subcommittee with the task of development of generic biometric standards SC37 ("SubCommittee 37").

This subcommittee has six working groups WG ("Working Group") with a specific area of work:

WG1 - Harmonized Biometric Vocabulary,
WG2 - Biometric Technical Interfaces,
WG3 - Biometric Data Interchange Formats,
WG4 - Biometric Profiles,
WG5 - Biometric Performance Testing and Reporting, and
WG6 - Cross-Jurisdictional and Societal Aspects of Biometrics.

ISO has other technical committees with task of dealing with biometric data. These are TC68 for financial services, JTC1 SC32 for data management and exchange, JTC1 SC17 for cards and personal identification, JTC1 SC29 for encoding audio, image, multimedia and hypermedia records, JTC1 SC24 for computer graphics and images, JTC1 SC27 for IT security techniques, JTC1 SC31 for automatic identification and data acquisition techniques, JTC1 SC36 for IT for learning, education and training, ITU-T SG17.

Informal standardization organizations

The BioAPI consortium is an example of informal organization for biometric standards. It was responsible for development of a common biometric application programming interface. The ANSI standard and the ISO standard are the most famous specifications of this group.

Biometric standards

There are different ways of collection and reproduction of biometric data so the safety of biometric data is crucial (Unar et al, 2014).

The financial sector was the first sector that used biometric standards. However, the development of biometric systems has led the organizations for standardization to introduce new biometric standards which are related to the security of biometric applications and biometric systems.

Nowadays, there are a lot of studies in the field of biometrics such us biometric transaction security and protection of biometric data.

The most popular biometric technical standards founded by SC37 are the Biometric Application Programming Interface (BioAPI) and the Common Biometric Exchange Format Framework CBEFF).

BioAPI

The BioAPI (Biometric Application Programming Interface) standard determines biometric application interfaces, devices and algorithms for distinguishing biometric data and device types.

This standard introduces basic functions of biometric systems, i.e. Enrollment, Verification and Identification. It also introduces an API (Application Program Interface) and an SPI (Service Provider Interface) for programmers and developers. Figure 1 gives the BioAPI's Application Program Interface/Service Provider Interface model.

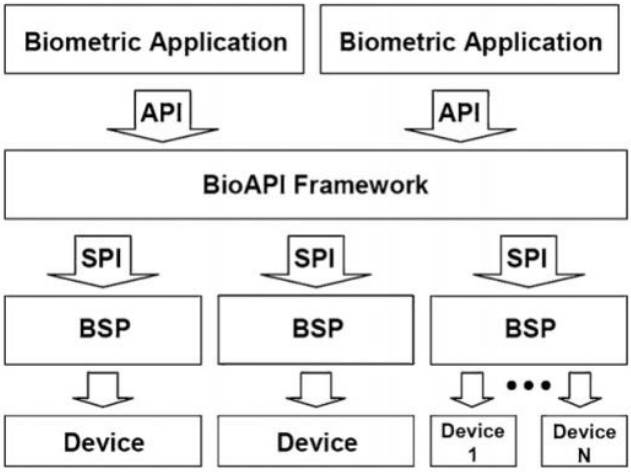

Figure 1 – BioAPI's API/SPI model (Thevenot et al, 2001)
Рис. 1 – BioAPI API/SPI модель (Thevenot et al, 2001)
Слика 1 – Модел BioAPI API/SPI (Thevenot et al, 2001)

CBEFF

The CBEFF (Common Biometric Exchange Format Framework) introduces a set of data elements needed to support biometric technologies in order to provide interoperability between biometric programs and biometric systems made by different manufacturers.

Figure 2 refers to the basic data structure for face, iris, fingerprint, palm, etc.

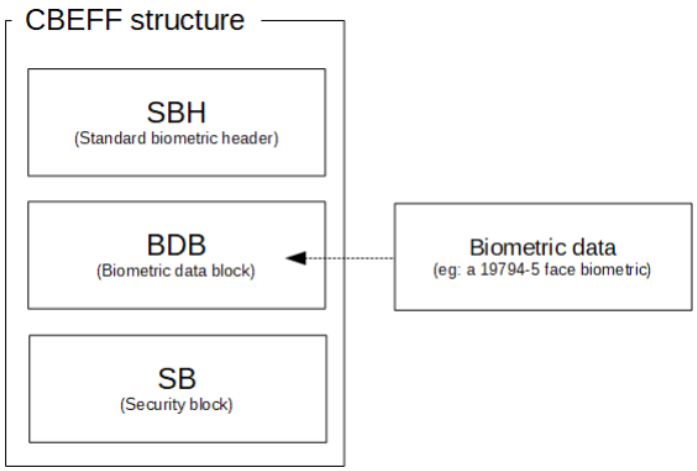

Figure 2 – CBEFF basic data structure (Thevenot et al, 2001)
Рис. 2 – CBEFF базовая структура данных (Thevenot et al, 2001)
Слика 2 –Основна структура података CBEFF (Thevenot et al, 2001)

ACBio

In order to ensure the integrity and confidentiality of transactions, the ACBio standard uses data encryption and digital certificates. It specifies the structure of data for a remote biometric verification.

In the ACBio model, a biometric transaction represents a number of processes executed by the Biometric Process Unit - BPU (e.g. sensor, smart card, comparison device, software running on a personal computer, etc.). Each of them sends relevant security information as a data block called the ACBio instance generated by the BPU.

Biometric sensors

In order to reach the phase of user identification, in terms of protection of information and communication systems, it is necessary to

collect biometric data through biometric sensors that will be compared with the already existing data registered in the system itself.

A sensor is a device that measures physical quantities and converts them into a signal readable by an observer or an instrument. The measured signal can be light, heat, movement, humidity, pressure or any other environmental phenomenon. The output is usually a legible signal to the observer or instrument at the sensor location itself or can be transmitted electronically over the network for reading and further processing.

Sensors have a wide application in virtually all aspects of life, including safety, security, surveillance, monitoring and detection in general (Ortega-Garcia, 2004). Sensors in the industry occupy a central place in process control, monitoring and security. In medicine, sensors also occupy a primary place because they are used to diagnose and monitor physiological changes in patients.

There are several sensor classifications by different authors and experts (Thevenot et al, 2001). Some are very simple and some very complex. According to one classification of sensors, they are divided into active and passive ones. Active sensors are those that require an external excitation signal or power signal, while passive sensors, on the other hand, do not require any external power signal and directly generate a signal response. The second type of classification is based on the means of detection used in the sensor. Some of the detection methods are electrical, biological, chemical, radioactive, etc. The following classification is based on the phenomenon of conversion, i.e. input and output. Some of the common conversion phenomena are photoelectric, thermoelectric, electrochemical, electromagnetic, thermo-optical, etc. (Maček et al, 2015). Finally, sensors can be classified into analog and digital ones. Analog sensors produce an analog output, i.e. a continuous output signal. Digital sensors, unlike analog sensors, work with discrete or digital data. The data in digital sensors used for conversion and transmission are digital in nature (Lalović, 2018).

Research and development of biosensors is becoming an increasingly developed discipline, because simple, fast, cheap, highly sensitive and highly selective biosensors contribute to progress in all aspects of life. For example, in a new generation of medicine, such as individualized medicine and ultrasound detection, an on-site sensor marks diseases. Some of the conventional biosensors and biosensing techniques from the point of view of smart biomaterials are: biosensors based on SPR (surface plasmon resonance), biosensors based on FRET

(fluorescent glucose biosensors) and biosensors based on AuNP (gold nanoparticles).

Research related to biosensors is interdisciplinary. For example, advances in surface chemistry provide new methods for designing target molecule recognition systems. In the future, advances in nanofabrication technologies promise not only the construction of new transducers, but also the miniaturization and integration of high-bandwidth biosensors. Therefore, the development of innovative biosensors requires interdisciplinary efforts outside conventional specialties. The combination of a lot of interdisciplinary knowledge will accelerate the development of biosensors and contribute to the revolution in the biomedical fields.

Biosensors are analytical devices that convert biological signals into electrical signals. Essentially, biometric sensors are highly specific, independent of physical parameters such as pH and temperature, and must be reusable.

The development of biosensors, as well as biosensor materials, transduction devices and immobilization methods, requires multidisciplinary research in chemistry, biology and engineering. The materials used in biosensors are categorized into three groups based on their mechanisms: a biocatalytic group containing enzymes, a bioaffinity group including antibodies and nucleic acids, and microorganisms containing microorganisms.

Biometric methods

Biometric devices perform data acquisition by receiving data from one of the sensory receptors in the form of a sensation that occurs in or on the human body and converts it into analog or digital signals that are used for further processing (Lalović et al, 2017). The data thus collected can be used to identify people. Individual biometric data are unique for each person and can be used to identify persons, both in the civil sector, e.g. in health care, educational institutions, companies, as well as in military, police and state institutions in order to protect their own resources. Biometric authentication (i.e. real authentication) is used in information technologies as a form of user identification and access control to protected resources.

Verification involves performing a one-on-one biometric comparison to provide access to either physical assets, such as a room or building, or digital assets, such as a smartphone, computer application, computer network, or database. For this purpose, biometric data is increasingly used as a replacement for traditional passwords and PIN codes to

improve access control. By comparing a living biometric sample of an individual with one reliable stored sample, the identity of the person is determined (Lalović et al, 2015). This saved sample can be located either in a central database, a smartphone, or as a token on a credential, such as an ID smart card (Lalović et al, 2016a).

There are different methods for biometric data acquisition and user authentication. Each of the methods of biometric identification has something specific:

Face recognition - Of the various methods of biometric identification, face recognition is one of the most flexible, even when the subject is not aware of the scan. This method of identification can search masses of people who have spent only a few seconds in front of a “scanner” - that is, an ordinary digital camera. Facial recognition systems work by systematically analyzing specific features that are common to all - the distance between the eyes, the width of the nose, the position of the cheekbones, the line of the jaw, the chin and so on. These numerical quantities are then combined into one code that uniquely identifies each person (Al-Maadeed et al, 2016).

Fingerprint identification - Fingerprints remain constant throughout life. In more than 140 years of comparing fingerprints around the world, it has not been discovered that two fingerprints are similar, even in identical twins. Fingerprint scanners are installed in PDAs, mobile phones and laptops, so scanning technology is also simple. Fingerprint identification includes comparison of ridge and groove fingertip samples, as well as minutiae (ridge characteristics that occur when the ridge splits in two, or ends) with biometric fingerprint samples in the database (Bhardwaj et al, 2017), (Lalović et al, 2016b).

Palm geometry biometrics – Palm geometry readers work in more extreme environments, do not require clean conditions and form a small data set. It is a common method of authentication in industrial environments.

Retinal scan - There is no way to fake the retina in the literature. The pattern of blood vessels on the back of the eye is unique and remains the same throughout life. However, it takes about 15 seconds of careful concentration for the scan to be of good quality. Retinal scanning is standard in the military and government sectors.

Iris Scanning - Like retinal scanning, iris scanning also provides unique biometric data that is very difficult to fake and remains unchanged throughout life. There are ways to encode biometric data to scan the iris in such a way that it can be securely transmitted in the “barcode” format (Belcher & Du, 2008).

Signature - A signature is another example of biometric data that is easy to collect and not physically intrusive. Digitized signatures are sometimes used, but usually do not have sufficient resolution to ensure authentication.

Voice Analysis - Like face recognition, voice biometrics provides a way to authenticate an identity without the subject's knowledge. But it has a big drawback, because it is easy to fake.

EEG authentication - uses an electrophysiological system to monitor brain activity. This technology is very popular and can be used without any side effects on the brain (Chen et al, 2016), (Tot et al, 2021), (Nakamura et al, 2017).

Conclusion

Given the significant advances in science and technology, such as basic developments in micro / nanotechnology, wireless communications, information technology and biomedical sciences over the past few years, there has been a transformation in this area of biometric systems, and models have been designed and built in a wide range of biosensors and load-bearing sensors.

The development of biometric systems and biometric sensors contributes to better protection of identity from misuse, because biometric technologies have great potential for improving the security and accuracy of system operation. The application of biometric systems improves the security of users, and such systems also provide much greater precision in establishing identity.

Due to the importance of establishing identity, it is necessary to constantly work on improving the system for precise identification, i.e. on improving their performance, either through the development of biometric sensors, or through the improvement of biometric data acquisition methods.

References

Al-Maadeed, S., Bourif, M., Bouridane, A. & Jiang, R. 2016. Low-quality facial biometric verification via dictionary-based random pooling. *Pattern Recognition*, 52, pp.238-248. Available at: https://doi.org/10.1016/j.patcog.2015.09.031.

Belcher, C. & Du, Y. 2008. A Selective Feature Information Approach for Iris Image-Quality Measure. *IEEE Transactions on Information Forensics and Security*, 3(3), pp.572-577. Available at: https://doi.org/10.1109/TIFS.2008.924606.

Bhardwaj, I., Londhe, N.D. & Kopparapu, S.K. 2017. A spoof resistant multibiometric system based on the physiological and behavioral characteristics of fingerprint. *Pattern Recognition*, 62, pp.214-224. Available at: https://doi.org/10.1016/j.patcog.2016.09.003.

Chen, Y., Atnafu, A.D., Schlattner, I., Weldtsadik, W.T., Roh, M.C., Kim, H.J., Lee, S.W., Blankertz, B. & Fazli, S. 2016. A High-Security EEG-Based Login System with RSVP Stimuli and Dry Electrodes. *IEEE Transactions on Information Forensics and Security*, 11(12), pp.2635-2647. Available at: https://doi.org/10.1109/TIFS.2016.2577551.

Chun, S.Y. 2016. Single pulse ECG-based small scale user authentication using guided filtering. In: *International Conference on Biometrics (ICB)*, Halmstad, Sweden, pp.1-7, June 13-16. Available at: https://doi.org/10.1109/ICB.2016.7550065.

Jain, A., Hong, L. & Pankanti, S. 2000. Biometric identification. *Communications of ACM*, 43(2), pp.90-98. Available at: https://doi.org/10.1145/328236.328110.

Jain, A. K., Ross, A. & Prabhakar, S. 2004. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), pp.4-20. Available at: https://doi.org/10.1109/TCSVT.2003.818349.

Kumar, A. & Prathyusha, K.V. 2009. Personal Authentication Using Hand Vein Triangulation and Knuckle Shape. *IEEE Transactions on Image Processing*, 18(9), pp.2127-2136. Available at: https://doi.org/10.1109/TIP.2009.2023153.

Lalović, K. 2018. Patent overview: Device for fingerprint identity guarantee. Vojnotehnički glasnik/Military Technical Courier, 66(2), pp.366-379. Available at: https://doi.org/10.5937/vojtehg66-15868.

Lalović, K., Anđelić, S. & Tot, I. 2017. How to guarantee baby identity based on fingerprint biometry. In: *The Ninth International Conference on Business Information Security (BISEC-2017)*, Belgrade, pp.1-4, October 18 [online]. Available at: http://bisec.rs/files/2017/16-k-lalovic-s-andjelic-i-tot-bisec-2017.pdf [Accessed: 20 February 2021].

Lalović, K., Maček, N., Milosavljević, M., Veinović, M., Franc, I., Lalović, J. & Tot, I. 2016a. Biometric Verification of Maternity and Identity Switch Prevention in Maternity Wards. *Acta Polytechnica Hungarica*, 13(5), pp.65-81. Available at: https://doi.org/10.12700/APH.13.5.2016.5.4.

Lalović, K., Milosavljević, M., Tot, I. & Maček, N. 2015. Device for Biometric Verification of Maternity. *Serbian Journal of Electrical Engineering,* 12(3), pp.293-302. Available at: https://doi.org/10.2298/SJEE1503293L.

Lalović, K., Nikolić, J., Tot, I. & Lalović, Ž. 2016b. Software algorithm of device for biometric identification of parenthood. In: The Eighth International Conference on Business Information Security (BISEC-2016), Belgrade, pp.66-71, October 15 [online]. Available at: https://www.metropolitan.ac.rs/files/2016/10/BISEC2016_Conference-Proceedings.pdf#page=67 [Accessed: 20 February 2021].

Lalović, K., Tot, I., Arsić, A. & Škarić, M. 2019. Security Information System, Based on Fingerprint Biometrics. *Acta Polytechnica Hungarica*, 16(5), pp.87-100. Available at: https://doi.org/10.12700/APH.16.5.2019.5.6.

Maček, N., Đorđević, B., Gavrilović, J. & Lalović, K. 2015. An Approach to Robust Biometric Key Generation System Design. Acta Polytechnica Hungarica, 12(8), pp.43-60. Available at: https://doi.org/10.12700/APH.12.8.2015.8.3.

Nakamura, T., Goverdovsky, V. & Mandic, D.P. 2017. In-ear EEG biometrics for feasible and readily collectable real-world person authentication. *IEEE Transactions on Information Forensics and Security*, 13(3), pp.648-661. Available at: https://doi.org/10.1109/TIFS.2017.2763124.

Odinaka, I., Lai, P-H., Kaplan, A.D., O'Sullivan, J.A., Sirevaag, E.J. & Rohrbaugh, J.W. 2012. ECG Biometric Recognition: A Comparative Analysis. *IEEE Transactions on Information Forensics and Security*, 7(6), pp.1812-1824. Available at: https://doi.org/10.1109/TIFS.2012.2215324.

Ortega-Garcia, J., Bigun, J., Reynolds, D. & Gonzalez-Rodriguez, J. 2004. Authentication gets personal with biometrics. *IEEE Signal Processing Magazine*, 21(2), pp.50-62. Available at: https://doi.org/10.1109/MSP.2004.1276113.

Prabhakar, S., Pankanti, S. & Jain, A.K. 2003. Biometric recognition: Security and privacy concerns. *IEEE Security and Privacy*, 1(2), pp.33-42. Available at: https://doi.org/10.1109/MSECP.2003.1193209.

Thevenot, D.R., Toth, K., Durst, R.A. & Wilson, G.S. 2001. *Biosensors and Bioelectronics*, 16(1-2), pp.121-131. Available at: https://doi.org/10.1016/S0956-5663(01)00115-4.

Tot, I., Trikoš, M., Bajčetić, J., Lalović, K. & Bogićević, D. 2021. Software Platform for Learning about Brain Wave Acquisition and Analysis. *Acta Polytechnica Hungarica*, 18(3), pp.147-162. Available at: https://doi.org/10.12700/APH.18.3.2021.3.8.

Unar, J.A., Seng, W.C. & Abbasi, A. 2014. A review of biometric technology along with trends and prospects. *Pattern Recognition*, 47(8), pp.2673-2688. Available at: https://doi.org/10.1016/j.patcog.2014.01.016.

Wang, J. & Wang, G. 2017. Quality-Specific Hand Vein Recognition System. *IEEE Transactions on Information Forensics and Security*, 12(11), pp.2599-2610. Available at: https://doi.org/10.1109/TIFS.2017.2713340.

БИОМЕТРИЧЕСКИЕ СТАНДАРТЫ И МЕТОДЫ

Иван А. Тот[а], **корреспондент**, *Йован* Б. Байчетич[а], *Бориша* Ж. Йованович[б], *Младен* Б. Трикош[в], *Душан* Л. Богичевич[г], *Тамара* М. Гайич[д]

[а] Университет обороны в г. Белград, Военная академия, кафедра телекоммуникаций и информатики, г. Белград, Республика Сербия

[б] Вооруженные силы Республики Сербия, Управление телекоммуникаций и информатики, ЦПМЕ, г. Белград, Республика Сербия

[в] Белградский университет, Факультет организационных наук, г. Белград, Республика Сербия

[г] Вооруженные силы Республики Сербия, Управление телекоммуникаций и информатики, ЦКИСИП, г. Белград, Республика Сербия;
Нишский университет, Факультет электроники, г. Ниш, Республика Сербия

[д] Белградский университет, Факультет организационных наук, г. Белград, Республика Сербия;
Университет обороны в г. Белград, Военная академия, г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 50.00.00 АВТОМАТИКА. ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА:
50.41.00 Программное обеспечение вычислительных машин, комплексов и сетей
ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: Системы идентификации пользователей играют весьма важную роль в современном обществе. Сложные требования безопасности побудили экспертов изучить способы использования биометрических данных для идентификации личности пользователя. В данной статье представлен обзор биометрических стандартов и методов, которые могут использоваться для идентификации пользователей в биометрических системах, а следовательно и для защиты информационных и коммуникационных систем.

Методы: В данной статье рассматривается проблема стандартизации в области биометрии. В первой части статьи представлены конкретные примеры наиболее широко используемых биометрических стандартов. Во второй части статьи приведен обзор наиболее часто используемых биометрических методов.

Результаты: Полученные результаты показали, что прогресс биометрических систем и биометрических датчиков способствует лучшему удостоверению личности и предотвращает неправомерное использование идентичности другими лицами, поскольку биометрические технологии обладают большим потенциалом повышения безопасности и точности работы системы. Биометрические системы повышают безопасность пользователей, а также обеспечивают гораздо большую точность при установлении личности.

Выводы: При разработке биометрических стандартов следует сосредоточить внимание на их внутреннюю взаимосвязанность, а также на улучшении их взаимосвязи с другими ИТ-стандартами.

Ключевые слова: организация биометрической стандартизации, биометрические стандарты, биометрические датчики, биометрические методы.

БИОМЕТРИЈСКИ СТАНДАРДИ И МЕТОДЕ

Иван А. Тот[а], **аутор за преписку,** *Јован* Б. Бајчетић[а],
Бориша Ж. Јовановић[б], *Младен* Б. Трикош[в],
Душан Љ. Богићевић[г], *Тамара* М. Гајић[д]

[а] Универзитет одбране у Београду, Војна академија, Катедра телекомуникација и информатике, Београд, Република Србија

[б] Војска Србије, Управа за телекомуникације и информатику, ЦПМЕ, Београд, Република Србија

[в] Универзитет у Београду, Факултет организационих наука, Београд, Република Србија

[г] Војска Србије, Управа за телекомуникације и информатику, ЦКИСИП, Београд, Република Србија;
Универзитет у Нишу, Електронски факултет, Ниш, Република Србија

[д] Универзитет у Београду, Факултет организационих наука, Београд, Република Србија;
Универзитет одбране у Београду, Војна академија, Београд, Република Србија

ОБЛАСТ: рачунарске науке, информационе технологије
ВРСТА ЧЛАНКА: прегледни рад

Сажетак:

Увод/циљ: У данашње време системи за идентификацију корисника имају веома важну улогу. Сложени захтеви који се односе на сигурност навели су експерте да разматрају начине на које би биометријски подаци могли бити коришћени за идентификацију корисника. У раду је представљен преглед биометријских стандарда и метода који се могу користити за идентификацију корисника у биометријским системима, чиме би се остварила заштита информационих и комуникационих система.

Методе: Разматрају се проблеми у стандардизацији на пољу биометрије. У првом делу рада наводе се конкретни примери најчешће коришћених биометријских стандарда, а у другом даје преглед биометријских метода које се најчешће употребљавају.

Резултати: Прикупљени резултати показују да развој биометријских система и биометријских сензора доприноси бољој заштити идентитета од погрешне употребе, с обзиром на то да биометријске технологије имају велики потенцијал за побољшање заштите и тачности системских операција. Примена биометријских система повећава заштиту корисника, као и

омогућава бољу прецизност приликом успостављања идентитета.

Закључак: Развој биометријских стандарда треба да се фокусира на њихову међусобну повезаност, као и на чвршћу везу са осталим ИТ стандардима.

Кључне речи: организације за биометријску стандардизацију, биометријски стандарди, биометријски сензори, биометријске методе.

Paper received on / Дата получения работы / Датум пријема чланка: 18.05.2021.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 29.09.2021.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 30.09.2021.