



# Multibiometric technologies in the system of criminalistic registration

Lyudmila YUGAY<sup>1</sup>

Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

## ARTICLE INFO

### *Article history:*

Received 10 august 2020

Received in revised form 20  
august 2020

Accepted 25 august 2020

Available online

August 2020

### *Keywords:*

Fingerprints

Genotypic registration

Physical features

Criminal records.

## ABSTRACT

The article deals with the relevance of human biometric parameters almost in all spheres of social life. Human biometrics is used in the notary, banking and control management access systems. The biometric identifiers used in the system of criminal records are analyzed. The opinions and views of forensic scientists on the choice of optimal biometric parameters are considered. Genotypic and phonoscopic types of registration is proposed to use in forensic registration system, along with fingerprinting and portrait registration in the paper. The advanced foreign experience of using biometric databases in China, Argentina, South Korea, the countries of the European Union, and the USA is highlighted. The author developed proposals on integration of all automated biometric systems, maximum coverage of population and exchange of biometric data, persons on the wanted list, who committed especially serious crimes. Solution of the problem connected with increasing the efficiency of the use of multibiometric records for the detection and investigation of crimes, an integrated approach is required that provides for organizational, methodological and legal aspects. In introducing biometric systems particular importance takes the issues of providing protection of personal data during their receipt, processing, storage and their usage.

2181-1415/© 2020 in Science LLC.

This is an open access article under the Attribution 4.0 International (CC BY 4.0) license (<https://creativecommons.org/licenses/by/4.0/deed.ru>)

<sup>1</sup> PhD, Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Tashkent, Uzbekistan  
Email: [yugay.lyudmila@inbox.uz](mailto:yugay.lyudmila@inbox.uz)

## Криминалистик рўйхатга олиш тизимида мултиметр технологиялар

### **Калит сўзлар:**

Бармоқ излари  
Генотипик рўйхатга олиш  
Ташқи кўриниш  
хусусиятлари  
Криминалистик ҳисобга  
олиш.

### **АННОТАЦИЯ**

Мақолада инсон биометрик параметрларини ижтимоий ҳаётнинг барча жабҳаларида қўллаш долзарблиги очиб берилган. Инсон биометрияси нотариал, банк соҳаларида, бошқарув назорати тизимларида қўлланилади. Шу билан бирга, криминалистик ҳисобга олиш тизимида фойдаланиладиган биометрик идентификаторлар таҳлил қилинган. Мақбул биометрик параметрлар танлови юзасидан криминалист-олимларнинг фикрлари ва қарашлари кўриб чиқилган. Ушбу тадқиқотда криминалистик рўйхатдан ўтказиш тизимида дактолоскопик ва портретли ҳисобга олиш билан бир қаторда рўйхатга олишнинг генотипик ва фоноскопик турлардан ҳам фойдаланиш таклиф этилган. Хитой, Аргентина, Жанубий Корея, Евроиттифоқ мамлакатлари, АҚШдаги биометрик маълумотлар базасидан фойдаланишнинг илғор хорижий тажрибаси ёритиб берилган. Муаллиф томонидан барча автоматлаштирилган биометрик тизимларнинг интеграцияси бўйича, аҳолини максимал даражада қамраб олиш ва ўта оғир жиноят содир этиб қидирувда бўлган шахсларнинг биометрик маълумотлари бўйича тажриба алмашиш таклифлари ишлаб чиқилган. Жиноятларни очиш ва тергов қилиш мақсадида мултибиометрик ҳисобга олишдан фойдаланиш самарасини ошириш муаммоларига ечим топиш учун ташкилий, методик ва ҳуқуқий аспектларни назарда тутадиган комплекс ёндашув зарур. Биометрик тизимларни татбиқ этишда шахсий маълумотларни олиш, ишлов бериш, сақлаш ва фойдаланиш жараёнида уларнинг хавфсизлигини таъминлаш муҳим аҳамиятга эга.

## Мултибиометрические технологии в системе криминалистической регистрации

### **Ключевые слова:**

Отпечатки пальцев  
Генотипическая  
регистрация  
Черты внешности  
Криминалистические  
учеты.

### **АННОТАЦИЯ**

В статье раскрывается актуальность использования биометрических параметров человека практически во всех сферах социальной жизни. Биометрия человека применяется в нотариальной, банковской сферах, системах контроля управления доступом. Анализируются биометрические идентификаторы, используемые в системе криминалистических учетов. Рассматриваются мнения и взгляды ученых-криминалистов по поводу выбора оптимальных биометрических параметров. В работе предлагается использовать в системе криминалистической регистрации, наряду с дактилоскопическими и

портретными учетами, генотипические и фоноскопические виды регистрации.

Освещается передовой зарубежный опыт использования биометрических баз данных в Китае, Аргентине, Южной Корее, странах Евросоюза, США. Автором разработаны предложения по интеграции всех автоматизированных биометрических систем, максимальному охвату населения и обмену биометрическими данными, лиц находящихся в розыске, совершивших особо тяжкие преступления. Для решения вопросов повышения эффективности использования мультибиометрических учетов в целях раскрытия и расследования преступлений необходим комплексный подход, предусматривающий организационные, методические и правовые аспекты. При внедрении биометрических систем особую важность приобретают вопросы обеспечения защиты персональных данных при их получении, обработке, хранении и использовании.

## INTRODUCTION

All over the world, interest is growing to the usage of human biometric characteristics almost in all spheres of social life. These include control management access systems (CMAS), records of operating time control systems, identity verification during banking, notarial and payment operations. Since 2020 identification of personality of applicants for passing entrance exams to higher educational establishments by fingerprints and facial features has been carried out in the Republic of Uzbekistan. Besides, biometric indicators are applied in the field of crime prevention, operational and comprehensive crime detection and border control as well.

In developed countries of the world, active research on usage and improvement of security of modern biometric system is being carried out. In particular, Milan Adamek, Miroslav Matýsek, Petr Neumann (Czech Republic) [1, p. 169-176], Rodrigo de Luis-Garcia, Carlos Alberola-López, Otman Aghzout, Juan Ruiz-Alzola [6, p. 2539-2557], S. Ayeswarya and Jasmine Norman [3, p. 67-99], Paweł Krotewicz, Wojciech Sankowski, Piotr Stefan Nowak [11, p. 69-81], Raymond T. Moor [16, p. 107-110], Nalini Kanta Ratha, Ruud Bolle [14, p. 458], Henry C. Lee, Robert E. Gaensslen [12, p. 444], Christophe Champod, Chris J. Lennard, Pierre Margot [4, p. 285], Itiel E. Dror, Jennifer L. Mnookin [10, p. 46-47], Peter Komarinski [15, p. 312] and other scientists devoted their work to the study of biometric characteristics. In these studies, special importance take the issues of usage of biometric systems on mobile platform, as well as ensuring the security of personal data.

In the legal system of the republic, large-scale reforms are being carried out related to the effective introduction of innovative modern technologies in disclosure and investigation of crimes. In particular, in our country, among the main tasks in this area, the dynamic development of forensic activity, widespread introduction of automated information retrieval systems and computer programs, electronic databases in forensic establishments are determined [24].

The aim of the work is to identify the most perspective biometric parameters for forensic registration, as well as development of proposals and recommendations on improvement of measures for the use of biometric systems in the field of combating crime.

## MATERIALS AND METHODS

The analysis of law-enforcement practice in the Republic of Uzbekistan for 6 months of 2020 shows that from all the studies conducted by the forensic departments of the organs of internal affairs, biometric (fingerprinting, portrait and handwriting) composed 97.9%. At the same time, in comparison with 2019, over the same period of time, growth was observed from this kind of conducted research by 2.26% [26]. Abovementioned indicators testifies the importance of the obtained biometric information as a significant source of evidentiary information in disclosure and investigation of crime.

Today, in the forensic departments of the organs of internal affairs, fingerprinting records and physical feature records are used. Records of fingerprints and handprints taken from the scene are widely used.

It should be noted that since 2011, biometric passports have been introduced in the Republic of Uzbekistan, which contain a chip with biometric information. The electronic chip stores information about the fingerprints and features of the passport holder.

In addition, the Republic of Uzbekistan provides for the introduction of identification cards (hereinafter referred to as ID-card), which should replace a number of identity documents [25]. ID-card data contains a single identification number of a person, personal data and it will also be used for identification and verification of personality too. Taking into consideration foreign experience, in order to increase the level of data protection, ID-cards include several biometric parameters of its owner. These include fingerprint data and physical features.

Information about the facial features of the owners of biometric documents is stored in the database of the automated personal identification system.

Fingerprint data is integrated into automated fingerprint identification systems.

In our opinion, the used methods of biometric identification of a person in the forensic registration system currently require revision. Fairly reliable and time-tested biometric identifiers exist. Biometric parameters are divided into static and dynamic. Static parameters include fingerprints, facial thermogram, iris, retinal capillaries, facial features, hand geometry, hand vein patterns, etc. Dynamic features include signs of handwriting, signs of signature, voice, gait, typing features on keyboard and etc.

V.A. Vorona and V.O. Kostenko point to the possibilities of such static methods as identification by the subungual layer of the skin, by the volume of fingers indicated for scanning of fingers, shape of ear, body odor and dynamic - identification by lip movement when saying a code word, by the dynamics of turning a key in a door lock, and etc. [19, p. 224-241].

According to V.G. Bulgakov, the functional-motor (functional-dynamic) complex of a person, motor stereotypes have serious prospects for further use in the theory and practice of forensic personality identification [18, p. 143].

A study of the latest literary sources shows the correctness of this statement. Active scientific research is being conducted on personal identification by gait, gestures, facial expressions, articulation.

At the same time, biometric identification systems are being actively introduced abroad as well. The United States is successfully implementing the FBI Next Generation Identification (NGI) system, which uses the most innovative technologies and improved search for fingerprints and their traces taken from the scene is considered to be one of the world's largest and most effective electronic database of biometric and criminal information [5].

The NGI system includes the Advanced Fingerprint Identification Technology (AFIT), the National Palm Print System (NPPS), the International Photo System, the ability to identify by face, iris, etc.

In addition, the Eurodac biometric system (European Dactyloscopy System) operates in Europe is the world's largest automated fingerprint identification system, serving 32 countries. Eurodac is a database of fingerprints of asylum seekers in the EU, as well as fingerprints of persons detained as a result of illegal border crossings [2].

Under the Eurodac system, participating States are required to promptly fingerprint every asylum seeker over the age of 14. These fingerprints are then compared with the fingerprint data transmitted by other participating States, stored in the AFIS central database. If Eurodac shows that the fingerprints have already been registered, the asylum seeker can be sent back to the country where their fingerprints were originally taken. [9]

Besides it, at the end of November 2017, the European Council approved the future Entry / Exit System (EES). It will replace the existing system of traditional stamping on passports with electronic registration of name, type of travel document, biometric data (4 fingers and face), as well as dates and places of entry and exit of third-country nationals visiting the Schengen area for short visits.

Facial recognition will be the main component of this system, as each Schengen country will have a national biometric database as well. These central and national biometric databases should be established by 2020 [7].

In 2011, Argentina created SIBIOS (Sistema Federal de Identificación Biométrica para la Seguridad) - Federal biometric identification system for security. The country's fingerprint database includes more than 40 million prints of the entire population.

The Argentinean SIBIOS system is integrated with other functioning databases in the country. Besides the biometric information and photographs, SIBIOS stores complete information from the time of birth of a person. Since 2012, in maternity hospitals in Argentina, electronic prints of fingers and toes are taken from all newborns, and a snapshot of the face is done as well [23, p. 88].

Since 2017, China has been collecting fingerprints from all foreigners between the ages of 14 and 70 at checkpoints across the country. The storage of biometric information of people entering and leaving borders is an important border control measure [17].

In the Republic of Korea, fingerprints are collected from every citizen over the age of 18 and up to the age of 18 with the consent of their parents. The government database currently contains fingerprints and photographs of over 3.5 million children under the age of 18, over 81,000 patients with mental disorders and over 62,000 patients with dementia, making for 39.8% of the more than 9.3 million citizens subject to mandatory fingerprinting registration.

As an example of the effective use of fingerprinting data, one may consider the accident on a tourist boat on the Danube River in Budapest, which occurred on May 29, 2019. Thanks to the practice of fingerprinting in South Korea of all its citizens, 11 South Korean citizens were identified out of 28 people who died. [13].

Furthermore, the Republic of Korea has introduced a new biometric regulation that requires all foreigners entering Korea to be fingerprinted as part of their immigration registration from January 1, 2012.

Moreover, Korean airports are equipped with biometric stalls for fingerprint scanning of fingerprints from Integrated Biometrics' in the framework of automated



immigration checks. Fingerprint scanners allow to compare fingerprints with fingerprint databases of known terrorists and criminals.

Since 2007, Japan has introduced the practice of fingerprinting foreigners entering the country as part of its anti-terrorism policy. Fingerprints are compared with international and domestic lists, and anyone who is listed as a terrorist or refuses to undergo fingerprint scanning will be denied entry and face deportation. Since 2019, in accordance with an international agreement, law enforcement bodies in Japan and the United States have begun to exchange fingerprint data in order to combat terrorism and organized crime.

The bilateral agreement allows the Japan National Policy Agency and US law enforcement bodies such as the FBI and the Ministry of Interior Security to work more closely together. The automatic fingerprint identification system is installed in both countries, and the requested party's database will automatically reply if there is a match. The AFIS database in Japan contains fingerprints of nearly 11 million people who have been taken into custody [8].

In France, in 1990, automation of all bases of the Ministry of Internal Affairs regardless of the level of the unit was implemented. Since 1991, a new National Police Computing Center PNK-2 (Police National Center) has been functioning in the UK. Since 2004, Russia has been implementing the Program of the Unified Information Telecommunication System of Internal Affairs Bodies [22, p. 118-121].

One of the sources of information about the crime event and creation of the evidence base are biological samples obtained from the scene of the incident (blood, saliva, nails, skin particles, bone fragments, teeth, etc.). As a result of DNA research, the perpetrators of these crimes can be identified based on samples obtained from the places of intended murder, rape, from suspects.

The method of DNA analysis and registration of DNA profiles of suspects, accused and convicted persons have been tested by time and are successfully applied in the law enforcement practice of foreign countries (Great Britain, USA, Canada, Japan, China, Malaysia, Singapore, Thailand, Chile, Colombia, New Zealand, etc.).

In its turn I.S. Dubrovin notes that «in the presence of appropriate DNA databases, search for persons who are carriers of the seized biological object can be carried out even in the absence of comparative samples, by comparing the genetic characteristics of the investigated object and stored in the database of DNA profiles» [21, p. 16].

This type of record is very promising in Uzbekistan and it is advisable to form it on the basis of the Main Forensic Center of the Ministry of Internal Affairs of the Republic of Uzbekistan. It is planned to create a genomic database of DNA profiles of those convicted persons of crimes against sexual inviolability and sexual freedom of the individual, unidentified persons and unidentified corpses.

Genomic registration is new and still understood incompletely direction for Uzbekistan in the forensic registration system, however, further improvement of legislation in this area, integration with other types of forensic records allow significantly increase the efficiency of crime detection and investigation.

Phonoscopic records are relevant in registration of persons who are reported to commit terrorist acts and mining of buildings. Voice is a biometric identifying feature allowing to identify personality. Foreign experience shows the effectiveness of these records.

Today, we consider fingerprint, portrait, genotyposcopic (DNA) and phonoscopic records to be the most basic directions for multibiometric registration in crime detection activities.

We support the opinion of R.E. Demin [20], who emphasizes the expediency of creating unified automated network, which include a system of departmental data banks with forensically significant information, in which piled up, systematized and processed information about various registration objects in order to provide information support for the investigation and disclosure of crimes.

Reasoning from above mentioned opinions and taking into account current trends towards the integration of various types of accounting, it is necessary to combine various types of biometric accounting to create the possibility of parallel verification of the personal data of a particular person, fingerprint data, determination of physical features, criminal records, genomic data, etc.

At the moment, a mobile verification system based on fingerprint databases is being tested in Tashkent. The mobile complex ADIS is located in a specially equipped vehicle that drives to the crime scene and allows to carry out an audit on the databases directly from the crime scene and accelerates the process of identifying a person by traces of papillose tracery. It would be advisable to organize an automatic parallel mobile check for facial features.

Today, fingerprint and portrait databases in the Republic of Uzbekistan function in separate information systems.

We consider it expedient to create in the near future an integrated multibiometric information system that will unite fingerprinting, habitoscopic, genotypic, phonoscopic, and other types of records. On this bases, found a bank of biometric information, which consist of general and special registration. The database of special biometric records contain information regarding persons who have committed crimes, as well as related to the crime. The base of general biometric records combine data about persons, information about which was obtained in connection with obtaining biometric documents or at their will.

It should be noted that cameras are becoming a necessary phenomenon of modern life, providing first of all, safety of population, protection of public order, detection of crimes in hot pursuit and much more. We observe them at banks, airports, posts, streets, parking lots, etc. Thanks to video cameras, crimes are solved, wanted persons are detained, and a kind of passive crime prevention is carried out.

## **RESULTS AND DISCUSSIONS**

The successful implementation and operation of these multibiometric systems is realized by solving a set of legal, technical, organizational and methodological issues. It is not possible to cover all of them within the framework of this article. However, an analysis of foreign experience and law enforcement practice in combating crime determines the following measures to improve the efficiency of these databases:

- integration of several types of biometric records, allowing automatically check it for other types of records in checking one type;
- maximum coverage of population. The more prints there are in the database, the more significant the result will be. In Argentina, collection of fingerprints and photography

of newborns are carried out already in maternity hospitals. In Belarus, all conscripts undergo fingerprinting;

- to introduce the possibility of carrying out checks on biometric databases on mobile complexes installed on official vehicles throughout the territory of the Republic of Uzbekistan;

- use at border control to identify wanted persons, persons with fake passports;

- to establish interstate exchange of biometric data of wanted persons and much more.

Conclusions. Biometric registration systems have its supporters, and at the same time its opponents, who point to the risk of violation of confidentiality, constitutional rights and freedoms of citizens and total control by the state. However, in our opinion, in modern conditions it is better to pay for security than to pay for its absence later. It is impossible to stop the process of informatization of all spheres of society. But to ensure the protection of the rights and freedoms of an individual and citizen, it is necessary to work out in detail the legal framework and provide technical security of personal information in its receipt, processing, storage and use.

### References:

1. Adamek, M., Matýsek, M., Neumann, P., 2014. Security of Biometric Systems // 25th DAAAM International Symposium on Intelligent Manufacturing and Automation 2014: 26-29 November 2014, [Vienna, Austria, During the DAAAM International Week] – p.169-176.
2. Automated Fingerprint Identification System (AFIS) – a short history. Retrieved August 10, 2020, from <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history>
3. Ayeswarya, S., Norman, J. A survey on different continuous authentication systems. // Int. J. Biometrics. – 2019. – №11 (1). – P. 67-99.
4. Christophe Champod, Chris J. Lennard, Pierre Margot. Fingerprints and other ridge skin impressions. – N-Y.: CRC LLC, 2004. – P. 285.
5. Criminal Justice Information Services Division. (n.d.). Retrieved August 10, 2020, from <https://archives.fbi.gov/archives/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/criminal-justice-information-services.pdf>
6. De Luis-Garcia, R., Alberola-López, C., Aghzout, O., Ruiz-Alzola, J. Biometric identification systems // Signal Processing. – 2003. – №83 (12). – P. 2539-2557.
7. Detect the guilty, protect the innocent. Retrieved August 10, 2020, from <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history>
8. Eric Johnson, Staff Writer. Japan-U.S. law enforcement fingerprint data-sharing pact kicks off, raising privacy concerns. Retrieved August 10, 2020, from [https://www.japantimes.co.jp/news/2019/01/28/reference/japan-u-s-law-enforcement-fingerprint-data-sharing-pact-kicks-off-raising-privacy-concerns/#.XUQiQ\\_L7Tcc](https://www.japantimes.co.jp/news/2019/01/28/reference/japan-u-s-law-enforcement-fingerprint-data-sharing-pact-kicks-off-raising-privacy-concerns/#.XUQiQ_L7Tcc).
9. Eurodac. Retrieved August 10, 2020, from [https://ec.europa.eu/home-affairs/content/eurodac\\_en](https://ec.europa.eu/home-affairs/content/eurodac_en)
10. Itiel E.Dror, Jennifer L. Mnookin. The use of technology in human expert domains: Challenges and risks arising from the use of automated fingerprint identification systems in forensics // Law, Probability and Risk (Law Probab Risk) – Oxford University Press – 2010. – 9. – P. 47-67.



11. Krotewicz, P., Sankowski, W., Nowak, P. Face recognition based on 2D and 3D data Fusion. // International Journal of Biometrics. - 2015. - №7 (1). - P. 69-81.
12. Lee, Henry C., Gaensslen, R. E. Advances in fingerprint technology. – Boca Raton, London New, York Washington, D.C., 2001. – P.444.
13. Marton Dunai. Korea's fingerprint practice helps experts identify Danube boat disaster victims/ Retrieved August 10, 2020, from <https://www.thestar.com.my/news/world/2019/06/06/koreas-fingerprint-practice-helps-experts-identify-danube-boat-disaster-victims#GSy0DqF6Y3YR05ds.99>.
14. Nalini Kanta Ratha, Ruud Bolle. Automatic fingerprint recognition systems. – 2004. – P. 458.
15. Peter Komarinski. Automated Fingerprint Identification Systems (AFIS). – Published December 27th 2004 by Academic Press (first published January 20th 2004). – 312 p.
16. Raymond T. Moor. Why Identifications are likely to score in rank one in AFIS latent fingerprint searches against large files // J. Forensic Ident. – 1991. – 41 (2). –P. 107-110.
17. Sidney Leng. China to store all foreigners' fingerprints upon entry – with new rule starting in Shenzhen. Retrieved August 10, 2020, from <https://www.scmp.com/news/china/policies-politics/article/2069440/china-store-foreigners-fingerprints-upon-entry-new-rule/>
18. Bulgakov V.G. Methodological foundations of forensic identification and diagnosis of a person based on his dynamic characteristics. - M.: Yurlitinform, 2014. – P. 143
19. Vorona, V.A., Kostenko V.O. Biometric identification technologies in access control and management systems // Computational nanotechnology. - 2016. - No. 3. - P. 224-241.
20. Demina, R.E. Problems of forensic registration and its use in crime investigation: Author's abstract. dis. ... cand. law sciences. - Saratov, 2001 - P. 26
21. Dubrovin I.S. Information retrieval systems of domestic, foreign and international services of law enforcement agencies in the fight against crime: Author's abstract. dis. ... cand. law sciences - M., 2007. - P. 16.
22. Karimov, V.Kh. Regularities of the development of criminalistic registration in Russia // News of the Altai State University. - 2017. - No. 3 (05). - P. 118-121.
23. Lebedenko, Yu.I. Biometric security systems. - M., 2013. - P. 88.
24. Resolution of the President of the Republic of Uzbekistan No. PP-4125 «On measures to further improve forensic expertise» dated January 17, 2019 // National database of legislation, January 19, 2019, No. 07/19/4125/2510.
25. Resolution of the President of the Republic of Uzbekistan No. PR-3673 «On organizational measures for the accelerated integration of departmental integration systems and the implementation of innovative projects» dated April 28, 2018 // National database of legislation, April 18, 2018, No. 07/18/3673 / 1084; Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 421 «About additional measures to improve the procedure for the provision of public services to the population through the further introduction of modern information and communication technologies» dated May 20, 2019 // National database of legislation, 05/23/2019, No. 09 / 19/421/3172.
26. Statistical indicators of the Ministry of Internal Affairs of the Republic of Uzbekistan for 6 months of 2020.