

Andrij Soroka

Criminalistic Requirements to Biometric Technologies as Means of Protection from Document Forgery

Abstract: The article deals with the topical issues of using capabilities of biometrics for protection against forging of documents which are used to identify a person considering criminalistics requirements to such technology.

Keywords: Biometrics, biometric technologies, criminalistics, identification.

Biometric technologies in passports and identification cards are recently widely applied which is caused mostly by threats of acts of terror which are performed in different countries, illegal people smuggling across the border, human trafficking, other trans-border crimes.

Biometrics is no longer a science fiction but a modern technology which has acquired new, specific meaning. At present, biometric technologies are defined as automatic or automated methods of people's identification by their biological characteristics or features.

In this article «biometric technologies» are understood as a set of methods and means constituting them which main purpose consists in identification of a person by his or her specific features, including appearance, which are attributable to a person as to a biometric object. Such features as voice, fingerprints, structure of a retina of an eye are unique characteristics of a person by which they can be identified. There are also other characteristics of biological object, for example his or her portrait in infra-red range, an electromagnetic portrait, gene structure, etc.

Biometric technologies continue to be implemented into life of citizens of majority of the states of the world and appear in all spheres of their public life. Ukraine is not an exception here: a program of creation of national biometric passports is underway.

The main functions of biometric system consist in identification, verification and authentication of a person. For the purposes and tasks of criminalistics the most important function is identification of a person.

Identification under any biometric system has four stages: recording (physical or behavioural sample which is recorded and stored by a system); allocation (unique information which is taken out from a sample and constitutes the biometric pattern); comparison (stored sample is compared to the presented one); match/mismatch (if there is a match of biometric samples the system gives positive result, if there is a mismatch - the result is negative).

Biometric samples are physiological and behavioural characteristics of a subject. Examples of physiological characteristics are fingerprints, form of a hand, layout of blood vessels of a hand, characteristic features of face, eye retina. A signature, voice, dynamics of pressing of keys relate to behavioural characteristics.

From the point of view of criminalistics biometric technologies, as a part of system of protection against forging of documents, should meet certain requirements.

First, biometric technologies should meet the following general requirements: high accuracy of identification of a person (low level of statistical errors of the first and second types of decision-making); high sensitivity; simplicity and convenience of use; high processing speed (number of objects identified per one second); reliability, etc.

Secondly, biometric technologies which are used in documents, should meet the requirements of means of protection from document forgery.

Such requirements include:

- Complete reproducibility of protective system (here we mean reproduction of identical properties of one and the same object; identity of material properties used in a batch, series of devices; display by devices of unique properties of the equipment or features of technology used in their production, and degree of durability of these features);

- Impossibility of the system deception by means of the inexact or distorted input of the information about features of a person (for example, input of an image of a fingerprint instead of a real fingerprint);

- Non-dependence from the conditions that influence general operational factors of a document over time, durability and indestructibility during the attempts of unauthorized use;

- Impossibility of disclosure of a security element (anti-counterfeit feature) by other means (concerning biometric technologies the important questions are: how unique is the equipment, used for production of objects; is the technology being used unique; are there any restrictions as to the selling, acquisition or relocation of the equipment and technologies which are used; is there any control over these issues from special services of a state where they are produced as well as from the manufacturer; is it possible to decode or change the information);

- Non-keeping (losing) by a security element (means) some of its specific properties in case of interfering with the document for the purpose of its partial falsification (this feature is very important from the point of view of solving criminalistics task of revealing and fixing of traces of tampering with a document);

- Independence of protected documents from each other. In other case disclosing of one element of protection (anti-counterfeit feature) will cause disclosing of all the whole system;

- Controllability of an anti-counterfeit feature (possibility to establish authenticity).

Criminalistic practice testifies that quite often objects which are subject to the research, are subjected to some changes due to various influences. However, irrespective of an object condition it is necessary to solve a question concerning its authenticity and its origin: whether properties of a device change after it is influenced; whether a device suitable for criminalistic identification after such influences (whether an object was made with the equipment with use of materials of a particular company); whether it is possible to establish the authenticity of a document in case of its partial damaging.

First of all, it is necessary to specify the list of signs of authenticity which are available in an object during its operation and matter at different levels of control: the manufacturer; forensic services; special services which supervise circulation of documents; persons who are engaged in such circulation. As practice shows, controlling of last two levels is the most difficult. Failure at these levels results in uncontrollable circulation of documents. Maximum efficiency of counteraction against forgery is provided if the services of the third level have the means of operative control.

Secondly, biometric technologies which are used in documents should be specially developed or adapted for the documents used.

Finally, the information concerning a person who is a holder of a biometric document should have the same format as the information in corresponding national and interstate databases of criminals or other category of persons.

At the same time, it is necessary to notice that from the perspective of manufacturers the question about testing, certification and standardization of biometric systems seems to be solved, while from the viewpoint of the court practice the question concerning acknowledgement of correctness of such procedures, as well as withdrawal of signs and their processing remains open.

Thus, it is vitally necessary to consider the approaches to the choice of biometric technologies offered by the author during the production of biometric documents.

References

Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус // Закон України від 20 листопада 2012 р. № 5492-VI.

МОРОЗ А.О. Біометричні технології ідентифікації людини. Огляд систем / А.О. Мороз // Математичні машини і системи. № 1. – Київ: – 2011. С. 39-45.

БАРКОВСКАЯ Е.Г. Криминалистика и биометрия: проблемы интеграции научного знания / Е.Г. Барковская // Философия права. № 3. – Ростов-на-Дону: – 2011. С. 27-31.

Проблеми та перспективи використання біометричних технологій [Електронний ресурс]. – Режим доступу: <http://donlegion.com/index.php?aid=42>.

Кľúčové slová: biometria, biometrické technológie, kriminalistika, identifikácia.

Súhrn

Článok sa zaoberá aktuálnou problematikou využitia možnosti biometrie na ochranu proti falšovaniu dokumentov, ktoré sa používajú na zistenie totožnosti osoby vzhľadom na kriminalistické požiadavky na tieto technológie.

Doc. Soroka Andrij, CSc.

Senior lecturer of the department of criminal process and criminalistics

National academy of the State border guard service of Ukraine named after B.

Khmelnytskyi,

major of justice, candidate of jurisprudence.

E-mail: ander.sor@yandex.ru