Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Fingerprint analysis (AFIS) and biometric system of identification by fingerprints: issue of artificial papillary pictures

Vitali KIRVEL[1]

Academy of Public Administration under the aegis of the President of the Republic of Belarus

ARTICLE INFO

Article history:
Received September 2020
Received in revised form
15 October 2020
Accepted 15 November
2020
Available online
31 December 2020

Keywords:
Fingerprinting,
Fingerprint examination,
Fingerprinting records,
Automated fingerprint
identification systems
(AFIS),
Falsification of fingerprints,
Artificial papillary patterns,
Biometric technologies,
Biometric identification
systems by fingerprints,
Verification,
Identification.

ABSTRACT

The article discusses the theoretical and applied aspects, as well as prospects for the development of fingerprint examination, fingerprint records (automated fingerprint identification systems-AFIS) in the disclosure and uncovering of crimes, as well as biometric identification systems by fingerprints to protect personal data, control access to corporate and personal information, time tracking in the information sector of the economy.

The paper presents methods form an ufacturing models with artificial papillary patterns (falsification of papillary patterns of fingerprints), the results of experiments that consisted in creating a model (dummy) of the nail phalanx of the finger with an artificial papillary pattern and verification of a biometric scanner using biometric technologies.

[1]Ph.D. (Juridical Sciences), Associate Professor, Academy of Public Administration under the aegis of the President of the Republic of Belarus, Minsk, Republic of Belarus
Member of the Lithuanian Association of Criminalists, Vilnius, Republic of Lithuania
E-mail: kirvit@tut.by

Дактилоскопическая экспертиза (АДИС) и биометрические системы идентификации личности по отпечаткам пальцев рук: проблема искусственных папиллярных узоров

Ключевые слова:
Дактилоскопия,
дактилоскопическая экспертиза,
Дактилоскопические учеты,
Автоматизированные дактилоскопические идентификационные системы (АДИС),
Фальсификация следов пальцев рук,
Искусственные папиллярные узоры,
Биометрические технологии,
Биометрические системы идентификации личности по отпечаткам пальцев рук,
Верификация,
Идентификация.

АННОТАЦИЯ

В статье рассматриваются теоретические и прикладные аспекты, а также перспективы развития дактилоскопической экспертизы, дактилоскопических учетов (автоматизированных дактилоскопических идентификационных систем) в раскрытии и расследовании преступлений, а также биометрических систем идентификации личности по отпечаткам пальцев рук для защиты персональных данных, контроля доступа к корпоративной и личной информации, учета рабочего времени в информационном секторе экономики.

В работе представлены способы изготовления моделей с искусственными папиллярными узорами (фальсификация папиллярных узоров следов пальцев рук), результаты экспериментов, которые заключались в создании модели (муляжа) ногтевой фаланги пальца с искусственным папиллярным узором и верификации биометрического сканера с использованием биометрических технологий.

INTRODUCTION

The relevance of the issue of effective detection, uncovering, preliminary research, removal and expert research of finger prints in the course of revealing and investigation of crimes is due to the growing public need to create an effective mechanism for combating crime, to ensure proper protection of the person, rights and freedoms of citizens, to strengthen the rule of law, and to increase public confidence in the authorities and management. In order to resolve the issue successfully, it is necessary to constantly improve the scientific and technical means, techniques and methods used by law enforcement agencies in the course of detection and crime investigations. For this purpose, modern technical means, scientifically based methods and techniques aimed at improving the effectiveness of detection, preliminary research, seizure and expert investigation of traces of crimes should be constantly introduced into law enforcement activities.

Annually, the State Committee of Forensic Examinations of the Republic of Belarus (hereinafter referred to as the SCFE) conducts an average of about 30-40% of fingerprint examinations of all conducted forensic examinations. Belarusian forensic experts use the automated fingerprint identification system (hereinafter – AFIS) «Dakto–2000» to establish more than 12 thousand matches on handprints taken during the inspection of the scene, identify about 500 unidentified corpses, about 800 persons who are unable to report any information about themselves or who have reported false personal data. [1]

Such wide spread use of human handprints by law enforcement officials during the disclosure and crime investigations, as well as AFIS «Dacto – 2000», as an accurate and reliable method of identifying a person, causes interest in persons involved in illegal

activities in terms of their falsification. It should be noted that modern technologies make it possible to create models (dummies) on which artificial papillary patterns (hereinafter - APP) of the fingers of a certain person are reproduced with a high degree of accuracy.

Taking into account the foregoing, we suppose that the public danger of falsifying finger prints consists in obstructing the establishment of truth in the case on the basis of a comprehensive, complete and objective examination, misleading the preliminary investigation authorities and court regarding the actual circumstances of the case included in the subject of proof, which may lead to the imposition of unfair sentences, when the perpetrator of the crime is not brought to justice.

A brief review of the literature on the issue under consideration indicates the following facts 1) studying the APP issue (falsification of fingerprints) during fingerprint examination and the use of AFIS by foreign and domestic researchers: T. Ley [2], O.Ya. Baev [3], S.S. Samishchenko [4], A.G. Sukharev [5], O.A. Sokolova [6, 7, 8], N.V. Efremenko [9, 10], N.S. Taletski [11] et al., 2) studying the AFIS issue, BSPI by fingerprints and APP by foreign and domestic researchers: Ya.N. Imamverdiev [12], T. van der Putte [13], T. Matsumoto [14], M. Sandstrom [15], V.S. Zubakha [16], R.V. Bondarenko [17], R.E. Demina [18] and others who created theoretical background for the study of the issue, as well as resolving certain practical issues of detecting, identifying, preliminary investigation, seizing and expert investigation of falsified fingerprints during the disclosure and investigation of crimes, as well as resolving certain practical issues of verification AFIS Software, fingerprint and biometric scanners using the model (dummy) of the nail phalanx of the finger with APP.

It should be noted, that the studies conducted by Belarusian scientists and practitioners are not systematic and final, and concern only the issue statement and certain practical issues of detecting, identifying, preliminary research, removal and expert examination of falsified fingerprints in law enforcement practice, concern only the problem setting and certain issues of fingerprint accounting using AFIS and verification of biometric scanners using a model (dummy) of the guttural phalanx of the finger with APP did not exhaust the possibilities of studying the whole range of aspects of this issue, that arise in the conditions of scientific and technological progress, dynamic development of forensic science, forensic science and law enforcement practice.

Certain applied aspects for the production of finger models (dummies) with APP, individual theoretical and applied aspects for verification of biometric scanners, BSPI for fingerprints to protect personal data, to control access to information and to track time using finger models (dummies) with APP, remained out of sight of domestic researchers.

MATERIALS AND METHODS.

The purpose of the research is to learn the patterns, that are the basis of the theory and practice of using human fingerprints in detection and investigation of crimes, in identifying promising areas of development of fingerprint examination and fingerprint records (AFIS), biometric systems for person identification (hereinafter – BSPI) on fingerprints in order to gain access to personal data, corporate and personal information, accounting of working hours in the information sector of the economy, their issues, offering solutions to some theoretical and applied aspects, as well as the formation of a single set of knowledge based on them, adequate to the modern development of

fingerprinting as an integral direction in forensic science, law enforcement practice and in the information sector of the economy.

The object of study is public relations that arise, develop and cease in the process of law enforcement agencies in detecting, identifying, preliminary investigation, seizure and expert investigation of falsified fingerprints in the process of disclosing and investigating crimes, as well as when using biometric methods of protecting personal data, control access to corporate and personal information, time tracking in the information sector of the economy, etc.

When studying the subject of research, the following **methods** were used: 1) the universal dialectic research method; 2) general scientific methods: analysis and synthesis, induction and deduction, analogy and abstraction, generalization and systems approach, statistical methods, modeling, observation, experiment, comparison, description, measurement; and 3) special methods: fingerprinting, sociological, etc.

The results of a brief review of the literature on the study of APPs issues (falsification of fingerprints) during fingerprint examination and the use of AFIS in the detection and investigation of crimes.

Tang Lei, a graduate student of Voronezh state University, was the first in the territory of the former Soviet Union, who considered the issue of APP in solving and investigating crimes in 1991. Under the guidance of Professor O. Ya. Baev, the graduate student, investigating the prognostic functions and possibilities of forensic examination, drew attention to a number of issues that experts may face in the future due to the use of scientific and technological progress by criminals. «As one of the issues, the author for the first time in the Soviet and Chinese forensic literature covers in sufficient detail the issue of artificial papillary patterns (APP), which has already arisen in a number of Western European countries, and offers a system of scientifically based recommendations for recognizing APP» [2, p. 20].

Later on, the Russian forensic scientist O.Ya. Baev, while considering the directions of the development of forensic technology, first of all highlights the development and implementation in practice of law enforcement agencies of new ways of identifying a person by the traces found at the scene and scientifically based methods for recognizing various falsifications of evidence. He writes that «an issue has already arisen in foreign forensics (I believe, unfortunately, that if it has not already become, then in the near future it may become relevant for our subjects to process investigation of crimes) of the recognition of APP- artificial papillary patterns» [3, p. 51-52].

Russian criminologist S. S. Samishchenko considered the issue of APP in the detection and investigation of crimes, in particular, the analysis of methods of forgery and forgery of handprints, as well as methodological recommendations for establishing the fact of falsification of this kind of material evidence in the dissertation study on the theory, practice and trends in the development of modern fingerprinting (2003) [4, p. 27].

Also, the issue of APP (falsification of fingerprints) at the experimental level was considered in their works by the Russian and Belarusian researchers: A.G. Sukharev et al. «Artificial papillary patterns as negative aspects of fingerprint registration» (2011) [5], O.A. Sokolova «Features of revealing signs of falsification of traces of papillary patterns of hands in fingerprint examinations (experimental research)» (2018) [8] and N.V. Efremenko «About the possibility of falsifying traces of hands» (2014) [10] and others.

In 2011, Russian scientists A.G. Sukharev, A.V. Stalmakhov and R.Yu. Trubitsyn in their study examined current issues related to the possibility of falsification of human papillary patterns, and also cited the results of experiments using dummies of the nail phalanges of fingers with APP from impression material made using laser engraving on elastic polymer plates and photolithography for verification of the AFIS software «Papillon and Autonomous biometric identification AGESES cards» [5, p. 64-72].

In 2014, Belarusian researchers N.V. Efremenko and A.V. Bashilova in their study «analyzed the most common methods (technologies) used to make models for the purpose of falsifying images of papillary patterns of fingers, systematized the group of specific signs of images of papillary patterns identified during numerous experiments and comparative studies, methods for their detection and research, and suggested recommendations for improving the methodology for conducting a comprehensive study of fingerprints» [9, p. 175].

In 2018, Russian researcher O.A. Sokolova examined the features of identifying signs of falsification of papillary hand patterns during fingerprint examinations, and in the course of experimental studies revealed signs indicating a household (simplified) method of falsification of papillary patterns [8, p. 112-116].

Thus, **the relevance, scientific and practical significance** of the APP issue for law enforcement bodies of the Republic of Belarus is due to the already existing expert methodology for recognizing APP in Russia. Based on the foregoing, we can conclude that this issue was relevant and had practical significance for the law enforcement agencies of Russia, and their scientists developed appropriate guidelines. Since the borders of the Union State of Belarus and Russia, the CIS are porous for the movement of people, it can be assumed that the issue of APP is relevant not only for the Russian Federation, but also for the Republic of Belarus.

As we noted above, there are very few works by Belarusian researchers to study this issue, and the results of interviewing employees of operational, forensic and investigative departments have shown that they did not encounter the issue of APP in their practical activities, although they are partially conversant with it.[2]

The previous theoretical and experimental studies of the author were also devoted to the issue of APP (falsification of fingerprints) [19, 20, 21, 22].

RESULTS AND ITS DISCUSSION.

Experiment 1

Belarusian researchers N.V. Efremenko and A.V. Bashilov point to six methods used to create models for falsifying images of papillary patterns of fingers (any part of the palm): 1) using plastics, 2) photolithography method, 3) photopolymer method, 4) laser engraving on rubber, 5) flash-technology; 6) vulcanization of rubber from matrices based on the use of solid photopolymer compositions. Further, they refer to their own experiments and comparative studies, during which two groups of specific falsification signs of images of natural papillary lines of human fingers were identified.

[2]To determine the awareness of law enforcement officials on the issue of APP in 2015, an interview was conducted with the staff of the SCFE, the Investigative Committee and the Interior Affairs Department of the X-region. The survey results showed that 38% of employees are conversant with the issue of APP. Of these, 36% respondents learned about the existence of APP from a colleague, 22% from the educational and scientific literature on forensic technology, 17% from the media (including the Internet), 13% from seminars and conferences, 12% found difficulty in replying.

It should be noted that the first two methods were proposed by Japanese researchers Tsutomu Matsumoto and colleagues in 2002. Unfortunately, Belarusian researchers do not describe the technology of manufacturing models themselves, but give the result of only a comparative study. It seems to us that the essence of the experiments not only in the above methods and the established signs of falsification, but also in the technologies themselves, in their reproducibility. For example, N.V. Efremenko and A.V. Bashilova indicate that in the first method they used plastic mass from the kit «Mikrosil TM» [9, p. 177-180]. The question arises: *«So, how were the models obtained for subsequent comparative research?»* (highlighted by the Author).

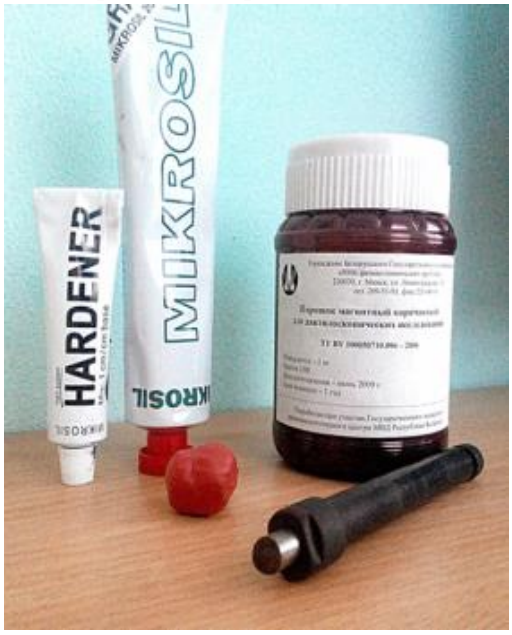

Photo 1.Materials used for manufacture of APP

In order to dispel the myth of the impossibility of creating an APP by an ordinary citizen and to fill the gap in the experiments of these researchers, the author and student N.V. Chichko decided to repeat the experiment of Matsumoto T., A.G. Sukharev and to create a model (dummy) of the nail phalanx of the finger with APP. To make a model (dummy) of the nail phalanx of the finger with APP, we used the plasticine needed to obtain a fingerprint, a set of Mikrosil pastes to obtain a texturized (three-dimensional) impression of the finger, as well as brown magnetic powder and a magnetic brush to detect and identify traces fingers of hands (Photo 1).

To obtain a texturized trace of a finger, we made a lump from plasticine, pressed a finger on it and, as a result, got the texturized trace of a finger (Photo 2). To obtain a three-dimensional dummy from the fingerprint, a set of Mikrosil pastes was used. After mixing, a homogeneous gray mixture was obtained, with which we filled in the texturized fingerprint made from plasticine (Photo 3).

After that, we got a volumetric dummy of the finger with APP[3] (Photo 4). Then, we decided to compare the obtained APP with the natural fingerprint of the donor's hand. To do this, we left a trace of the papillary pattern, which was displayed in the model, and the donor's fingerprint on the glass surface(Photo 5).

The obtained fingerprints were provided for a comparative study by experts of the expert-forensic division of the SCFE X-Department. In the course of a comparative study, they found a coincidence of fingerprints based on: 1) general features: a) the type of papillary pattern, b) the direction and steepness of the flow of papillary lines, their presence, location and disposition, as well as on 2) specific features of the papillary pattern: a) the beginning and end of papillary lines, b) the branching and merging of papillary lines, c) the presence of islets.

To illustrate a comparative study of coincident features, a shot of the donor's fingerprint and a footprint obtained using a dummy with APP was made. The coinciding structural details of the papillary patterns are marked with the same numbers and lines:

[3] In order to prevent crime, the technology of obtaining a model (dummy of the nail phalanx of the finger with APP) is presented in a simplified form.

1) beginning of the papillary line - No. 1, 2; 2) end of the papillary line - No. 5, 6, 7, 9, 11, 12; 3) branching papillary lines - No 10; 4) merging papillary lines - No. 3, 8; 5) islet - No. 4 (Photo 6).

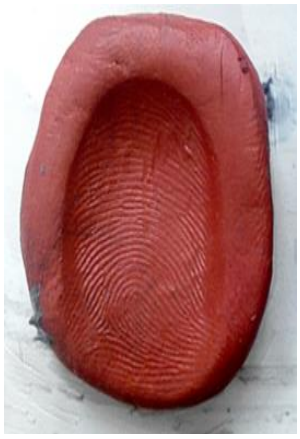

Photo 2. Texturized trace of the thumb of the right hand

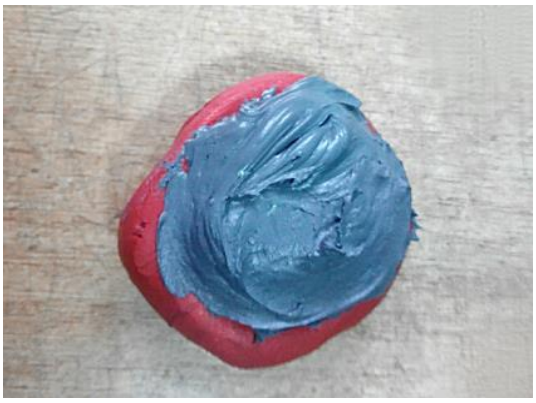

Photo 3. Obtaining a three-dimensionalmodel of the thumb of the right hand

Photo 4. Three-dimensional model with APP

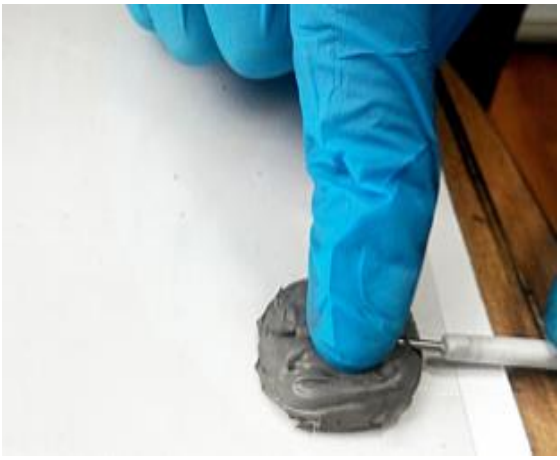

Photo 5. Obtaining a fingerprint using dummy with APP

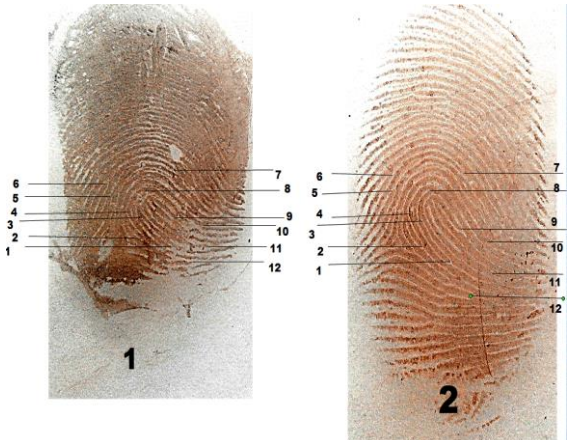

Photo 6. Papillary patterns of the thumbs obtained using dummy (No. 1) and the donor's fingerprint (No. 2) / Comparative study of fingerprints obtained using dummy (No. 1) and the donor's fingerprint (No. 2)

We asked the forensic expert: «If you received a piece of tape with a fingerprint on it, that was left using a dummy fingerprint and a dactocard of X suspect, whose papillary pattern was reproduced using a dummy with APP, then while conducting a comparative

study, could you distinguish between them?» We received the following answer: *«No! The identity of the two prints would be established»* (emphasized by the Author).

Thus, on the basis of the foregoing, it can be concluded that the development of modern technologies allows the creation of models (dummies) of fingerprints of a person's hand with an APP by an ordinary citizen without the use of special equipment. Our experiment definitely showed the existence of an APP issue during fingerprint examinations in the detection and investigation of crimes at the present stage.

The results of a brief review of the literature on the study of the issue of verification of AFIS software, fingerprint and biometric scanners using the model (dummy) of the nail phalanx of the finger with APP.

In 2012, Ya.N. Imamverdiev, a member of staff of the Institute of Information Technologies of the National Academy of Sciences of Azerbaijan, proposed an effective method for detecting fingerprint APP based on a modified model of orientation field coherence, since he believes that «one of the urgent issues related to the security of biometric technologies is the detection of false and artificially modified papillary fingerprint patterns» [12, p. 86].

An analysis of the literature of far abroad countries on this topic showed that in a number of European countries and Japan the topic of APP is also not new and there is a certain amount of research. It should be noted that these publications are mainly devoted to biometric systems for protecting personal data and controlling access to corporate and personal information.

In 2000, at the conference on research of smart cards and advanced technologies in Bristol (UK), researchers from the Netherlands Tonom van der Putte and Jeroenom Keuningom presented the report «Biometric fingerprint recognition: do not burn your fingers» [13]. Dutch researchers presented the results of an experiment on biometric fingerprint recognition. By creating finger models (dummies) with APP, they proved that *all tested commercial scanners recognized them as real fingerprints at the first or second attempt* (highlighted by the Author), which contradicted the manufacturer's information about the possibility of their recognition.

In 2002 Japanese researchers Tsutomu Matsumoto and his colleagues from Yokohama National University conducted a study in the field of cryptography: «The effect of artificial fingers made of polymer materials on fingerprint recognition systems» [14]. They presented it at the Optical Security Conference on methods of preventing falsification. Japanese researchers described in their report the creation of two APP manufacturing technologies, which they used to trick fingerprint sensors that are used in security systems. *Depending on the applied method of manufacturing APPs and the type of scanners, the frequency of false recognitions according to their data ranged from 70 to 95%* (highlighted by the Author).

Swedish researcher from Linkoping University Marie Sandstrom outlined universal research directions in her monographic work: «Vulnerability Detection in Fingerprint Recognition Systems» (2004) [15]. The author explains the importance of her research by the fact that in the near future it is planned to use biometric passports with owners' fingerprints, as well as to use it in border control systems. *Consequently, law enforcement agencies need to be prepared for use the APP by representatives of transnational crime for falsifying biometric passports* (highlighted by the Author).

We consider vulnerability of using fingerprints in everyday activities (a biometric method for protecting personal data and access to information) on the following examples.

Fingerprints of the German Minister of Defense Ursula von der Leyen were obtained with a help of an ordinary camera in a smartphone, the available «Veri Finger» software[4]. Hacker «Starbug» (Ja. Chrisler) announced this at the congress of the largest European hacker association Chaos Computer Club (2014) [23]. According to his words, fingerprints can be easily obtained during a public event using an ordinary camera. J. Krissler explained that he took fingerprints of the Minister of Defense from a close-up photograph of her palms made during a press conference (Photo 7). Other pictures taken from different angles at other events helped him to compile a complete papillary pattern. He also believes that *the massive use of this method can be a serious blow to personal safety of those, who chose fingerprints as a biometric method for protecting personal data and access to personal information* (highlighted the Author), and he recommends to high-ranking officials always wear gloves at public events, because the collected biometric information can be used to authenticate a person.[5]

In April 2017, the **Master Card** International Payment System introduced the first bank card with a built-in fingerprint sensor (Photo 8). According to the staff of **Master Card**, the fingerprint scanner will allow you to replace the PIN code and make the payment confirmation procedure more convenient and safe. At the same time, experts in the field of information security note that biometric protection does not guarantee absolute protection, since the fingerprint can be copied and reproduced using a printer [24].

Photo 7. Close-up photo of the palms of Ursula von der Leyen

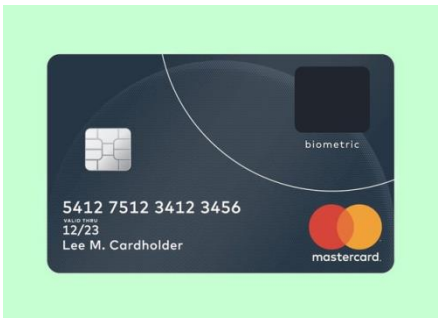

Photo 8. MasterCard card with a built-in fingerprint sensor

It should be noted that the IDEX study conducted in 2018 showed that 56% of consumers trust fingerprint protection rather than PIN codes. 76% of smartphone owners use a fingerprint scanner on devices, and 23% use biometrics for mobile payments [25].

The most common AFIS in the territory of the post-Soviet space today are the Russian AFIS «Papillon» [26] and Sonda [27], as well as the Belarusian AFIS «Dacto-2000» [28].

The software and the mathematical apparatus (hereinafter referred to as «MA») of modern AFIS allows displaying fingerprints in the form of a mathematical model. The basis of

[4]In 1998, «Neurotechnology» company developed a fingerprint identification technology for biometric system integrators. «VeriFinger» scans fingerprints from a flat surface and transfers them (rotation, deformation of distorted fingerprints) for biometric data monitoring and protection systems.
[5]The procedure of authentication in information technology.

the software and MA functioning is the theory of forensic identification, theory of probability, information theory, set theory, theory of mathematical logic, theory of algorithms, etc.

The Russian company «Papilon» JSC is positioning itself as a manufacturer of reliable, selective and accurate biometric fingerprint identification systems: AFIS, fingerprint scanners («Live Scanner») and biometric terminals, as well as iris identification systems and habitoscopic systems, setting them as equal, because their functioning is based on certain theoretical principles and mathematical algorithms.

According to the statement of Russian developers, when creating a search mathematical model, not only the flow directions and structural details of the papillary pattern are described, but also the topological characteristics of the ridge structure - the relative position of neighboring features across and along the flow of papillary lines. A topological approach ensures search selectivity, superior selectivity of systems that describe only the integral structure of the pattern and / or the position and direction of small features [26].

The Russian company «Sonda Technology» is positioning it self as a manufacturer of reliable, high-speed and accurate biometric fingerprint identification systems: AFIS, biometric scanners and terminals, as well as working time control systems, also setting them as equal, because their functioning is also based on some theoretical principles and mathematical algorithms [27].

The Belarusian company LTD «Todes» is a manufacturer of AFIS «Dacto – 2000» and fingerprint scanners («Live Scanner»).

AFIS «Dacto – 2000» is designed for fingerprint records and checks on the basis of hands traces taken from unsolved crimes, on fingerprint arrays of individuals, who are persons registered on fingerprint records in forensic units, as well as operational reference fingerprint records of information units of law enforcement agencies. AFIS can also be used for fingerprint registration of citizens and in identification systems for various purposes.

AFIS «Dakto–2000» (vercion 4.0) was successfully tested according to the methodology of the Forensic Center of the Ministry of Internal Affairs of the Russian Federation and the State Scientific Research Forensic Center of the Ministry of Internal Affairs of Ukraine.

The developed mathematical algorithms for fingerprint information processing allowed to obtain high search reliability indicators: 1) «Trace – Trace» - 100%; 2) «Trace – Dactocard» - 90%; 3) «Dactocard – Trace» - 85.5%; 4) «Dactocard – Dactocard» - 100% [28].

Thus, based on the foregoing, we can state that the fingerprint scanner, as a registration and control tool, which is a mandatory part of any modern AFIS, operates on the same theoretical principles and mathematical algorithms as biometric scanners of personal identification systems.

In 2004, Russian researcher V.S. Zubakha examined in his dissertation «The Current State and Issues of Automation of Fingerprint Records» [16], issues of structural organization and the principles of functioning of AFIS, issues of automation of fingerprint records, criteria for evaluating the effectiveness of modern AFIS and the reliability of the results obtained during verification by AFIS.

In particular, V.S. Zubakha introduced AFIS as a typical classifier, because in the search process it performs an encoded image identification of the fingerprint from the database with the request fingerprint. He considered the probability of a coincidence index

and the effect of the search mode and request fingerprint parameters on the frequency function nature of the «stranger» pairs of fingerprints index matches.

When examining the dependence of the coincidence index on the search mode, the author states that when having many request fingerprints, accounting the type of pattern and integral characteristics for prints from data bases do not affect the distribution density of the coincidence index, and data bases of limited volume when removing control by the type of pattern and integral characteristics, the number of prints with a nonzero match index increases. The author also examined the dependence of the display frequency distribution of "stranger" fingerprints on the features of the request fingerprint (on number of signs).

The analysis conducted by Zubakha V.S. shows that the probability of coincidence for «stranger» and «native» fingerprints depends on *the quality of the AFIS software and the subjective errors of the operator, as well as on the features of the request fingerprints and the search mode* (highlighted by the Author). Therefore, when evaluating the characteristics of the AFIS, it is very important, that the frequency of the request fingerprints with particular features to the AFIS input should correspond to the frequency of their appearance under the actual operating conditions of the AFIS.

In 2011, Russian scientists A.G. Sukharev, A.V. Stalmakhov and R.Yu. Trubitsyn examined in their study current issues related to the possibility of falsification of human papillary patterns, and also presented the results of experiments using dummies of nail phalanges of fingers with APP from impression material made by laser engraving on elastic polymer plates and photolithography for verification of «Papillon» AFIS software and the «Autonomous Biometric Identification AGESES Card» [6, p. 64-72].

One of the main features of modern AFIS should be noted. *The authors state that the currently used AFIS is not originally intended for recognizing signs of APP when checking fingerprints* (highlighted by the Author). In this case, the AFIS operator can, if necessary, correct the distortions in the trace in manual mode. All this leads to the fact that traces of dummies are recognized by such systems as traces of natural papillary patterns [5, p. 67].

To support this, the authors conducted an experiment using the «Papillon» AFIS. Dummies with APP were made in two ways: from silicone compounds and using laser engraving on various materials. During the experiment with a help of dummies superficial traces of papillary finger patterns of the several individuals' hands were left. These fingerprints had previously been entered into the AFIS database. When checking these tracks on an array of more than 900 thousand fingerprints in the recommendation list, on the first place was always the information on the participant of the experiment, whose artificial track was checked. This situation is objectively explainable and is associated with the absence of the task of recognizing APP traces in the «Papillon» AFIS software, as mentioned above.

In 2015, Belarusian researcher N.S. Taletsky in the publication «Falsification of fingerprints of papillary finger patterns as the main way to overcome identification biometric security systems» considered the possibility of changing, replacing and falsifying fingerprints of papillary finger patterns of persons engaged in illegal activities. He believes, that the danger of falsification of fingerprints of papillary finger patterns lies, first of all, in the possibility of bypassing BSPI in order to obtain secret and other information, access to personal data of citizens and commercial «secrets» of companies, penetration into protected objects, etc. Also the use of fake fingerprints of papillary hand patterns in order to prevent the establishment of truth in the case under investigation, misleading the bodies

of preliminary investigation, inquiry and the court regarding the real circumstances of the incident cannot be excluded [11, p. 230].

Experiment 2

Based on the assumption that the fingerprint scanner and biometric scanner, which is used in the information sector of the economy, use the same theoretical principles and mathematical algorithms, we conducted the following experiment in the framework of the study.

Currently there are many biometric devices on the market aimed at protecting information, controlling working hours, recording users and performing other functions based on biometric data. Their developers guarantee a sufficiently high degree of protection due to the use of appropriate technologies. For the experiment we selected the **submitted for the experiment** by the «BioLinkBel» company (Belarus), the demo version of the «**BioTime**» biometric registration system for time tracking and access control, and the USB optical scanner: «BioLink S-Match 1F, Russia» (terminal). As noted by Russian developers, the probability of errors in such a device is minimal.

It should be explained that biometric scanners, like any other devices, can cause errors. There are 2 levels of errors. Errors of the first type, when we have an erroneous rejection of verification (False Reject Rate, hereinafter - FRR), i.e. the scanner cannot recognize a registered user, and errors of the second type consist in the erroneous acceptance of the verification (False Accept Rate, hereinafter - FAR), i.e. an unregistered user is defined by the scanner as registered.

Errors of the first type (FRR) are not so critical for the security system, although they create inconvenience, since it is necessary to pass verification for a second time. And reliability of the system of protection against unauthorized access depends on the number of errors of the second type (FAR), as a result of which an attacker can gain access to the system. The appearance of FRR and FAR errors is determined by such characteristics as quality and resolution of scan, scan area, mathematical algorithms used to compare fingerprints, number of details that are used for comparison.

Typically, the frequency of occurrence of FRR errors is higher than the frequency of occurrence of FAR errors. So, *the probability of occurrence of FRR errors is usually less than 2%, and the probability of FAR errors* **is less than 0.0001%** [29].

Technical support of the experiment: 1) **BioTime Biometric time attendance and access control system** («BioLink Solutions», Russia, 2015) [30], 2) terminal («BioLink S-Match 1F, Russia» Biometric USB Fingerprint Optical Scanner), Photo 9), 3) model (dummy) of the nail phalanx of the finger with APP (made using plasticine and a set of pastes «Mikrosil», Photo 4).

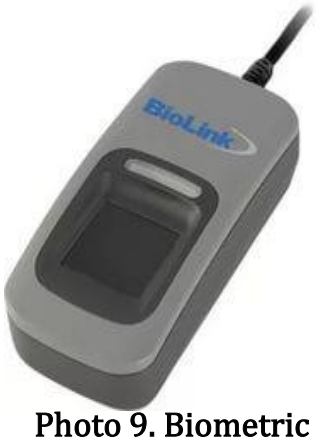

Photo 9. Biometric USB Optical Scanner

It should be noted that today there is a discrepancy in the content of the terms that are used by specialists in technology and law.

Let's explain. So, in accordance with GOST ISO/IEC 24713-1-2013 «Information technology. Biometric profiles for interoperability and data interchange. Part 1. Overview of biometric systems and biometric profiles»[31], under:

identification in biometrics means the function of a biometric system that performs a one-to-many search (paragraph 3.25);

verification means a function of a biometric system that searches for a query sample with a specified template stored in the system in a one-to-one

mode and returns the result in the form of a coincidence index or a decision about a coincidence (paragraph 3.35). In forensics, identification means the process of establishing the identity of an object or person by entirety of general and particular features, carried out with the aim of deciding whether this object is sought [32, p. 27].

Verification in the logic and methodology of science (from Latin verificatio - proof, confirmation) means as the process of establishing the truth of scientific statements as a result of their empirical verification. To verify is to directly or indirectly confirm the truth of scientific statements using empirical observation or experiment procedures [33].

Thus, the purpose of the experiment was to verify the «**BioTime**» software for biometric registration of time tracking and access control by means of empirical verification, as well as user identification based on a combination of general and particular features, in order to establish identity.

Two women and three men aged from 20 to 40 years and 5 dummies of their nail phalanges of right-hand thumb with APP were users of the software for biometric registration of time tracking. Basic data of the persons participating in the experiment were depersonalized and presented as users with numbers from 1 to 5. Models (dummies) of their nail phalanges of thumbs were indicated from M1 to M5.

Verification of the terminal and software through the use of dummies of the nail phalanx of thumb of right hand was planned in 10 procedures.

On the 7th verification procedure of the M4 dummy, software identified the registered user No 4! The experiment was stopped.

In our experiment, we observed an error of the second type, which consists in false acceptance of verification (FAR), so an unregistered user M4 was indicated by the terminal and software as a registered user No. 4. The terminal manufacturer («BioLink S-Match 1F», (Russia)) the probability of a FAR error is declared as less than 0.0001%.

In the experiment, the error of the second type (FAR) was 0.0294% (7 procedures x 5 models = 35 procedures – 1 (M5) = 34, i.e. 1/34). Thus, the probability of a second type of error (FAR) declared by the terminal manufacturer does not correspond to the indicated characteristics and exceeds it almost in 300 times (294 times)!

Our experiment convincingly showed the presence of an APP issue for BSPI on fingerprints with the aim of protecting personal data, controlling access to corporate and personal information, accounting for working hours in the information sector of the economy, and also for fingerprinting using AFIS (the work of which is based on the same theoretical principles and mathematical algorithms) in order to disclose and investigate crimes at the present stage.

It should be noted that, the next achievement of scientific and technological progress – 3D bioprinter, which is capable of printing human skin, may be the next issue in forensic science and biometric technology[6] [34].

[6]Spanish scientists, together with colleagues from the «BioDan Group», have developed a 3D bioprinter capable of printing human skin. The skin printed on such a printer completely repeats the structure of a real human one, with an external protective layer of the epidermis and an internal layer of the dermis, which contains fibroblasts that produce collagen - a protein that makes the skin firm and supple at the same time. Unlike an usual printer, this printer does not use ink cartridges, but injectors with biological components. The printer can print the skin from allogeneic (stranger) cells, for research purposes, and from the patient's cells for transplantation. Developers say that the finished product can be transplanted to patients or used for commercial needs, to test the chemical, cosmetic or pharmaceutical products in the

Photo 10.3D bioprinter and printed «artificial» skin

CONCLUSION:

1) the creation and use of APP is not regulated by the legislation of the Republic of Belarus, which creates the prerequisites for their use for illegal purposes: a) for the falsification of fingerprints during fingerprint examinations and the use of AFIS in the detection and investigation of crimes; b) for access to personal data, corporate and personal information, falsification of time tracking in the information sector of the economy, etc.;

2) to prevent the possibility of using APP for criminal purposes, we consider it appropriate and justified: a) to develop theoretical and applied provisions and methodological recommendations for their detection, identification, preliminary investigation, seizure and expert investigation of falsified fingerprints during the disclosure and investigation of crimes, b) to develop theoretical and applied provisions and guidelines for countering the use of APP in BSPI for fingerprints in order to gain access to personal data, corporate and personal information, time tracking in the information sector of the economy, as well as in biometric passports with fingerprints of the owner[7], c) to train expert personnel in the framework of advanced training; d) to organize a study of this issue in the form of a separate topic for employees of preliminary investigation bodies, the Prosecutor's Office and judges;

3) at the present stage of development of society and scientific and technological progress, a promising direction for the development of fingerprint examinations and fingerprint records based on AFIS, BSPI on fingerprints in order to gain access to personal data, corporate and personal information, and accounting for working hours in the information sector of the economy is a solution the issue of APP, because it is possible to establish the fact of falsification of the papillary pattern, if there is a combination of established signs and only during a dactyloscopy examination, as well as improving the quality of AFIS software and biometric scanners.

In conclusion, it should be noted that the author does not make a claim for the indisputability of the opinions and conclusions expressed. He believes that the article will arouse interest among readers and invites theoreticians and practitioners to the discussion, and also proposes a joint comprehensive scientific and practical study of this issue.

References:

1. *Povyshenie effektivnosti vedeniya kriminalisticheskikh uchetov – v tsentre vnimaniya kollegii Gosudarstvennogo komiteta sudebnykh ekspertiz.* [Improving the effectiveness of forensic records - the focus of the board of the State Forensic Examination Committee] Available

right quantities, quickly and at the right price. A 3D printer for skin printing, created by Spanish scientists, is currently being tested by European regulatory authorities, who are responsible for introducing such technologies into medical and research practice.

[7]The creation of the Belarusian integrated service and payment system for the use of biometric passports is planned in 2019. Active users: Ministry of internal Affairs, Ministry of foreign Affairs, State Border Committee of the Republic of Belarus, etc.

at: http://www.pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti prava/2016/november/21803/ (accessed:19 December 2020).

2. Tang Lei. *Sudebnaya ekspertiza v ugolovnom protsesse KNR i SSSR : (opyt sravnitelnogo issledovaniya). Avtoreferat dissertatsii. Voronezhskiy gosudarstvennyy universitetim. Leninskogo komsomola.* [Forensic examination in the criminal process of the PRC and the USSR: (experience of comparative research). Thesis]. Voronezhskij gosudarstvennyj universitet. Voronezh, 1991. 20 p.

3. 3.Baev O. Ya. *Osnovy kriminalistiki : Kurs lektsiy.* [Fundamentals of Criminalistics: a course of lectures]. Moscow, Examen Publ., 2003. 320 p.

4. Samishchenko S. S. *Sovremennaya daktiloskopiya : teoriya, praktika i tendentsii razvitiya* .[Modern fingerprint analysis: theory, practice and tendencies of development]. Akademiya upravleniya vnutrennikh del Rossiyskoy Federatsii. Moscow, 2003. 35 p.

5. Sukharev A. G., Stalmakhov A. V., Trubistyn R. Yu. *Iskusstvennye papilljarnye uzory kak negativnye aspekty daktiloskopicheskoy registracii i verifikacii* [Artificial Papillary Patterns as Negative Aspects of Fingerprint Registration and Verification]. Sudebnyja ekspertiza, 2011. No 1. pp. 64-72.

6. Sokolova O. A. *Falsifikatsiya sledov i otpechatkov ruk cheloveka* [Falsification of traces and fingerprints of human hands]. Sudebnyja ekspertiza, 2012, No. 4 (32). pp. 56-71.

7. Sokolova O. A. *K voprosu o sovershenstvovanii metodiki proizvodstva daktiloskopicheskikh ekspertiz v svyazi s vozmozhnoy fal'sifikatsiey papillyarnykh uzorov* [On the issue of improving the production methods of fingerprint examinations in connection with the possible falsification of papillary patterns] Vestnik Moskovskogo universiteta. 2017, No 2. pp. 125-128.

8. Sokolova O. A., Lapteva A. L. *Osobennosti vyyavleniya priznakov falsifikatsii sledov papillyarnykh uzorov ruk pri proizvodstve daktiloskopicheskikh ekspertiz (eksperimental'nye issledovaniya).* [Features of revealing signs of falsification of traces of papillary patterns of hands in fingerprint examinations (experimental research)]. Vestnik ekonomicheskoy bezopasnosti. 2018, No 1, pp. 112-116.

9. Efremenko N. V., Bashilova A. S. *Ustanovlenie fakta falsifikatsii sledov paltsev ruk.* [Establishment of falsification of fingerprints]. Vestnik Polotskogo universiteta. 2014. No. 13. pp. 175 - 182.

10. Efremenko N. V., Bashilova A. S. *O vozmozhnosti falsifikacii sledov ruk*. *Aktualnye voprosy sovershenstvovaniya sudebno-ekspertnoy deyatelnosti: tezisy dokladov mezhdunarodnoy nauchno prakticheskoy konferencii, Minsk, 23-24 oktjabrja 2014 g. Gosudarstvennyy komitet sudebnykh ekspertiz Respubliki Belarus. Minsk: GKSJe*. [About the possibility of falsifying traces of hands. Actual issues of improving forensic activity: thesis. Int. scientific-practical conf., Minsk, October 23-24. 2014. State Forensic Examination Committee of the Republic of Belarus]. Minsk. 2014. pp. 61-63.

11. Taletsky N. S. *Falsifikaciya otpechatkov papillyarnykh uzorov paltsev ruk kak osnovnoy sposob preodoleniya identifikacionnykh biometricheskikh system zaschity.* [Falsification of fingerprints of papillary finger patterns as the main way to overcome identification biometric security systems]. Visnik Pivdennogo regional'nogo centru Nacional'noy akademii pravovih nauk Ukraini, 2015. No 5. pp. 228-234.

12. Imamverdiev Ya. N. *Metod obnaruzheniya iskusstvennogo izmeneniya papillyarnykh uzorov otpechatkov paltsev naosnove kogerentnosti polyaorientatsiy* [Method for detecting

artificial changes in papillary fingerprint patterns based on the coherence of the orientation field]. Shtuchniy intelekt, 2012. No 1. pp. 86-96.

13. Van der Putte, Ed. T. Biometrical fingerprint recognition. Don't get your fingers burned. Ed. T. van der Putte, J. Keuning. – Kluwer Academic Publishers, 2000, pp. 289-303. Available at: http://cryptome.org/fake-prints.htm (accessed: 19 December 2020).

14. Tsutomu Matsumoto. Impact of Artificial «Gummy» Fingers on Fingerprint Systems. Ed. T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino. Optical Security and Counterfeit Deterrence Techniques IV, Thursday-Friday 24-25 January 2002. Available at: http://cryptome.org/gummy.htm (accessed: 19 December 2020).

15. Sandström Ed. M. Liveness detection in fingerprint recognition systems. Ed. M. Sandström. – Linköping University, 2004, p. 129. Available at: http://liu.diva-portal.org/ (accessed: 19 December 2020).

16. Zubakha V. S. *Sovremennoe sostoyanie i problem avtomatizatsii daktiloskopicheskikh uchetov.* [The current state and issues of automation of fingerprint surveys]. Saratov, 2004, 22 p. Available from: http://www.dissercat.com/content/sovremennoe-sostoyanie-i-problemy-avtomatizatsii - daktiloskopicheskikh-uchetov#ixzz5gHkzP1Ev (accessed: 19 December 2020).

17. Bondarenko R. V. *Primenenie informatsionnykh tekhnologiy v issledovani isledov ruk pri raskrytii i rassledovanii prestupleniy.* [Application of information technology in the study of handprints in the disclosure and investigation of crimes]. Moscow, 2003, 26 p.

18. Demina R. E. *Informatsionnoe obespechenie raskrytiya prestupleniy: puti optimizatsii*. [Information support for the disclosure of crimes: ways of optimization].Vestnik Povolzhskoy akademii gosudarstvennoy sluzhby, 2008. No. 3, pp. 83-87.

19. Kirvel V. K., Bashilova A. S. *Iskusstvennye papillyarnye uzory : mif ili realnost* [Artificial papillary patterns: myth or reality]. Vestnik Akademii MVD Respubliki Belarus, 2010. No 2 (20), pp. 118–121.p

20. Chemeris E. V. *Perspektivy razvitiya daktiloskopicheskoy ekspertizy v Respublike Belarus.* [Prospects for the development of fingerprint expertise in the Republic of Belarus. XXI Respublikanskiy konkurs nauchnykh rabot student]. Minsk, 2014, 49 p.

21. Chichko N. V. *Iskusstvennye papillyarnye uzory.* [Artificial papillary patterns]. Academy of public Administration under the President of the Republic of Belarus. Minsk, 2016. 61 p.

22. Kirvel V. K. *Biometricheskie tekhnologii: verifikaciya opticheskikh skanerov.* [Biometric Technologies: Verification of Optical Scanner] Available from: http://cb.aercom.by/программа (accessed 19 December 2020).

23. *Khaker skopiroval otpechatki paltsev po obychnoy fotografii.* [Hacker copied the fingerprints from a regular photo]. Available from: http://www.vesti.ru/doc.html?id=2272876 (accessed: 19 December 2020).

24. *Master Card vypustila kartu so skanerom otpechatka paltsa.* [Master Card has released a card with a fingerprint scanner]. Available from: http://newsroom.mastercard.com/ru/press-releases/mastercard-представляет-банковскую-карту (accessed: 19 December 2020).

25. *Otpechatok vmesto PIN: kak ustroeny biometricheskie bankovskie karty.* [Fingerprint instead of PIN: how are biometric bank cards arranged]. Available from: https://psm7.com/card/biometricheskie-bankovskie-karty.html (accessed: 19 December 2020).

26. *Sovremennye biometricheskie resheniya ot AO «Papilon»* [Modern biometric solutions from JSC «Papilon»]. Available from: http://www.papillon.ru/rus/42 (accessed: 19 December 2020).

27. *Biometricheskie sistemy identifikacii po otpechatku paltsa: ADIS, ... skanery, terminaly.* [Biometric fingerprint identification systems: AFIS, ... scanners, terminals]. Available from: https://www.sonda.ru/product/afis/. (accessed: 19 December 2020).

28. *ADIS «Dakto – 2000»* Todes. [AFIS «Dakto – 2000»Todes]. Available from: https://www.todes.by/dactoru/ (accessed: 19 December 2020).

29. Pakhomov S. Otpechatok paltsa vmesto parolya. [Fingerprint instead of password]. Available from: http://compress.ru/article.aspx?id=10423 (accessed: 19 December 2020).

30. *Biometricheskiy uchet rabochego vremeni i kontrol dostupa: sistema «BioTime»*. [Biometric time tracking and access control: «BioTime» system]. Available from: http:// biotime.ru (accessed: 19 December 2020).

31. *Informacionnay asistema MEGANORM.* [MEGANORM Information System]. Available from:http://meganorm.ru/Index2/1/4293774/4293774788.htm (accessed: 19 December 2020).

32. Belkin R. S. *Kriminalisticheskaya enciklopediya.* [Forensic encyclopedia]. Moscow: Megatron XXI. 2000. 334 p.

33. *Filosofiya: enciklopedicheskiy slovar.* [Philosophy: Encyclopedic Dictionary]. Moscow: Gardariki. 2004. 1072 p. Available from: https://dic.academic.ru/dic.nsf/enc_philosophy/198/VERIFIKACIJa. (accessed: 19 December 2020).

34. 3-D bioprinter to print human skin – Science Daily Available from: http:// www.sciencedaily.com/releases/2017/01/170123090630.htm. (accessed: 19 December 2020).