ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20200625120039
Preliminary communication

Automated Fingerprint Identification System: with and without the Possibility of Correction of a Digitalised Image

Natasa PETROVIC*, Snezana STOJICIC, Radovan RADOVANOVIC, Vojkan NIKOLIC, Mina PETROVIC

Abstract: According to the fact that systems for automatic processing of biometric data are constantly advancing in terms of speed and reliability, as well as in terms of adding new processing capabilities, the question of choosing the appropriate system becomes more important. In this paper the idea is to present the technical and technological solutions of the Automated Fingerprint Identification System with different operating principles, with and without the possibility of correction or coding of a digitized image. Comparisons of different systems were performed in test and production environments. The test database with 10 000 records and about half a million records of dactyloscoped persons in the production of database for testing the performance of search was used. The results have shown that there exists a statistically significant difference ($p < 0.001$) between examined systems in face fingerprint search according to latent fingerprint databases (which means indirect verification). In the production environment, it was found that there exists statistically significant difference ($p < 0.001$) in the direct and indirect verification showing advantages and disadvantages of the compared systems.

Keywords: AFIS; dactyloscopy; databases; identification; verification

1 INTRODUCTION

The contemporary systems for support of registration and identification include the system based on dactyloscopic data, AFIS (Automated Fingerprint Identification System), which was originally intended for registration [1], identification, verification of the identity of criminals, as automation in dactyloscopy, and today is increasingly in use in the so-called "civil" sector in terms of security of facilities and persons unambiguous identification of the person of interest. Identification in the AFIS system implies the use of biometric data, i.e. dactyloscopic data, fingerprints or palm prints data, guided by the fact that each fingerprint or palm print is unique and that there aren't two people in the world who have the same prints [2].

Biometric data, fingerprint or palm print, photograph and iris of the eye, are used to determine the identity of a person and verify that identity. The relationship between a person and these data is unambiguous, i.e. the probability of matching in different persons is so small that it can be considered that there are no two persons with identical biometric data of these categories [3]. With the development of information systems and automation of processes as well as the use of modern communications to perform various tasks or transactions, without the personal presence of the person who wants to perform these tasks electronically and the business partner, there is a justified demand for reliable and fast identifying persons [4]. The AFIS systems which have been designed today are divided according to purpose: for the so-called "civil" sector and for the criminal sector. These systems can be designed as independent or connected, in accordance with the purpose, and the legislation as well.

Application in the "civil" sector is aimed at providing unambiguous biometric identification of citizens, in order to establish and/or confirm the identity of citizens using fingerprints, providing preconditions for the production of reliable identification documents and thus preventing identity theft and preventing multiple identities for the same person. Also, it can be applied in business processes related to the protection and security of persons and facilities, i.e. enabling control of entry into facilities and premises with limited access. There is an increasing use of logging in to enable the use of devices and systems, such as mobile devices, laptops, external disks, tablets and mobile phones, replacing the use of passwords with biometric data and reducing the possibility of unauthorized access to data on these devices and media.

The application in the "criminal" sector, i.e. for the prevention and detection of perpetrators of criminal offenses, is to enable an automated procedure for registration and identification of persons on the basis of biometric data. The search itself during the process of verifying the identity of a person can be conducted in two ways, as a direct or indirect verification. Direct verification refers to a type of search where images of latents from the crime scene are searched through a database of fingerprints or palms of indisputably identified persons. Indirect verification refers to the search of fingerprints or palms of a person with an indisputably established identity through a database of latents from the crime scene.

Thanks to AFIS systems, it is now possible to unambiguously identify persons and find the perpetrators of crimes in a short period of time [5]. Such systems enable, through simpler, more reliable, modern and quality work, compliance with international norms and standards. On the other hand, the system offers secure, fast, efficient and automatic biometric identification of the perpetrators of crimes in order to fight terrorism and organized crime as well as other types of serious crime [6]. The reliable identification of persons is the foundation of the national security and safety of every state.

2 MATERIAL AND METHODOLOGY

The system represents a complete solution in the field of digital collection (acquisition) of identification data (alphanumeric and biometric data), for processing the data and integration with existing databases and systems for recording crimes, as well as systems for personalization of identification documents, and search and exchange of all types of data [7]. The paper compares the results of work with two AFIS systems which are in parallel production

work, chosen by the authors who had the opportunity and privilege to work with them. For assessment was used test and production environment. A test environment was designed for these two systems for training and verification of declared functionalities and system performance. For both systems considered production databases were approximately the same size and quality in terms of the dactyloscopic data. The images of prints were taken partly through ink and paper and then entered into the database by scanning, and mostly directly through the "Live" scanner. Latents have been processed and entered by scanning on flatbed scanners. The bases of the AFIS test systems are identical and have a capacity of 10000 people and 1000 latents from the crime scene. Data on persons and latents were taken at random, except for 100 latents from criminal acts and 100 persons who were identified as perpetrators of those acts. The data consist of valid fingerprints of all 10 fingers, palms and edges, obtained by registration of persons, latents from the crime scene and the same data that were entered in both systems during the one-year period of work. Analysis of the system performance was conducted using statistical methods for frequency of positive results comparison (χ^2 test) with level of significance $p < 0.05$.

3 SCANNER/IMAGE RECORDING

Due to the direct dependence of the image quality and the reliability of the AFIS system, it is important to define the acquisition methods and the types of scanners used in accordance with the purpose [8]. Identifying and verifying a person's identity using dactyloscopic data via the AFIS system with individual fingerprints, regardless of the technology used, require three general steps: image creation/capture, image digitization and image format standardization according to the existing dactyloscopic database. The quality of the search directly depends on the image quality, so it is necessary to analyse in detail the characteristics of the scanner performing the prints [9]. There are different types of scanners depending on the sensors used and the way the fingerprints and/or latents are acquired. For the acquisition of a fingerprint images can be said to be the most common so-called "Live" scanners. The number of details of unique fingerprint characteristics increases by increasing the quality of the generated image. This is correlated with scanner resolution, i.e. high-resolution scanners enable identification of the largest number of characteristics of papillary fingerprint lines and thus affect search results [10]. The size of the area where the fingerprint image is taken, also affects the accuracy and speed of identification or verification [11].

3.1 Original Paper Ink Technique

Prior to the use of scanners for the acquisition of fingerprint images, for persons of interest to the police, acquisitions were made on dactyloscopic cards, on the basis of which dactyloscopic collections were created or on the basis of fingerprints collected at the crime scene. This method requires that a person's fingers are covered with ink and pressed or rolled on a fingerprint card. The collected images of fingerprints and latents were manually compared by forensic experts on existing dactyloscopic cards from dactyloscopic collections. Disadvantages of this technology include the possible smearing of the fingerprint image with ink, which leads to the inability to notice the characteristics, the required training and experience of the person taking the fingerprints, and the relatively low speed in achieving work results (Fig. 1).

Today to improve the search speed and verifying the match results the prints are converted to digital format. Images digitized in this way can be synchronized with an existing database, then analysed and compared using a high-speed matching algorithm. To meet the certification requirements, scanned images must have a minimum resolution of 500 dpi [10]. Scanning of such acquired prints is done with ordinary flatbed scanners.

Figure 1 Images of prints taken with ink on paper

3.2 Scanners with Sensor System Live Scanners

Sensor-scanned scanners allow working with hard-to-read fingerprints, such as dry, wet, or dirty fingers. They contain algorithms that adjust and optimize the generated images. Acquisition of a dry, wet or dirty fingerprint often is not feasible, but an AFIS system that has scanners configured with this type of sensor in the first few frames (less than one second) adjusts and captures a clear, complete and uniform high quality fingerprint image [12]. The scanners, that the authors have the opportunity to work with, are scanners with a sensor system with electroluminescent films (LES) and optical sensors that use TIR (Total Internal Reflection) technology [9]. The difference between the clarity of the images of the prints taken by the scanners with this type of sensor is shown in Fig. 2. The left print is obtained with using TIR technology, and the right with LES (The left and right thumb prints of one of the authors are shown).

Figure 2 Quality of images of prints taken from different scanners

Scanners with LES technology have the ability to clean parts of image prints, such as accidental touches, dirt left over from previous users, after each recording, but have the ability to ignore everything except the region that is important for search (Fig. 3). This allows high-band width (fast input and verification) of high-quality prints. They are suitable for large data entry or verification, frequent, multiple identity checks, such as for smartphones.

Figure 3 Example of residual random contact

Optical sensors with TIR technology have ability to directly capture a fingerprint placed on the upper surface of the glass prism of the "Live" scanner. Until recently, optically based sensors were the only practical technology to achieve the level of image quality required to meet FBI standards of 500 dpi image size (Fig. 4) [9].

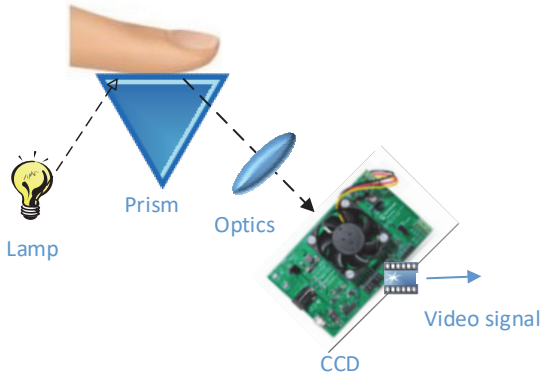

Figure 4 Optical sensor

Some scanners have ability to capture multiple images and the appropriate algorithm can select the best image or combine images to achieve high quality matching [10].

4 DATABASES AND TYPES OF DATA

The AFIS systems enable dactyloscopic facial data to be stored in database management systems in digital form and enable efficient searches and connections to other databases for the purpose of rapid and efficient facial identification. Databases can be divided by the type of data they contain, i.e. those that contain all ten fingerprints for a person whose identity has been indisputably established, palms, latents of unidentified persons from unresolved cases containing fingerprints, unresolved fingerprints containing palm prints and a database with personal information about the person [13-15].

The paper presents those AFIS systems that contain the specified types of data, i.e. indisputable fingerprints as well as latents from the crime scene and which can be connected to other databases via identifiers [16].

5 OBJECTIVES OF CONSIDERATION

Technological development has led to the fact that today a large number of systems exist for identification of persons on the basis of dactyloscopic data, thus asking questions which of them is appropriate or allows efficient identification and identification of latents from the crime scene, especially bearing in mind that they can be related to legally based consequences. When it comes to the work of investigative bodies in order to combat crime, it should have been noted that the focus is not on the speed of the system and reliability in terms of stability, but only in relation to the accuracy of comparison algorithms and search results. To interpret the results of comparing available dactyloscopic data to databases, it is necessary to clearly define the terms used, as well as the procedures used in converting fingerprints into digital form. Only the consideration and comparison of search results of the different AFIS systems is conditioned by the growing need for fast and reliable identification of persons, modernization of equipment for acquisition of dactyloscopic data and improvement of search algorithms.

The systems were selected based on the experience of authors who have been administering production and testing of new AFIS systems on offer for 15 years, and noting that the AFIS systems they encountered can be classified according to the manner and results of work in one of these two.

5.1 Types of Searches on AFIS Systems

The aim of the research is to see whether the systems will be able to identify all 100 persons by direct and indirect verifications (Fig. 5). The quality of prints is defined by categories of excellent quality, good and bad, and prints of unsatisfactory quality as rejected [12]. The quality is determined by the size, clarity of the papillary lines and the number of minutiae that the impression contains.

The samples of databases used in our study, observed from the aspect of data quality assessment, have 0.79% of prints of excellent quality, 72.93% of good quality, 19.48% of prints of poor quality and 6.80% of prints that were "rejected". Interestingly, the largest percentage of prints of excellent quality is from the thumb of the left hand, 50.96%, and the largest number of "rejected" is from the index finger of the left hand, 8.44%. The average number of minutions on the prints is 66, which shows that both samples are of very good quality for the needs of dactyloscopic comparison [10]. The samples of the database of test systems that were isolated and on which the accuracy of the search was considered are the same in terms of volume, size and type of data.

The analysis of the reliability of searches for the purpose of reaching a conclusion on the confirmation of the identity of a person on the basis of dactyloscopic data was based on the types of searches (Fig. 5) which refer to:

Accuracy of the search in relation to all ten fingerprints of the newly entered person according to the database of fingerprints of persons whose identity has been indisputably established.

This is a procedure for verifying or establishing the identity of each person whose dactyloscopic data are entered into the AFIS system. This determines whether biometric data for that particular person exist in the AFIS system and if so, under which identity the person is registered, i.e. whether he provided false information about himself during registration.

Accuracy of the search in relation to all ten fingerprints of the newly entered person according to the database of unresolved latents from the site that contain fingerprints as dactyloscopic data.

Basically, this means determining whether the person for whom dactyloscopic registration is performed is the perpetrator of a crime for which data-latents already exist in the system. It gives the possibility of resolving several criminal acts of the same perpetrator. The type of search according to the previously entered latents from the place is indirect verification.

The accuracy of the search in relation to the palms of the newly entered person according to the base of LV latents from a crime scene containing the palm prints, and this type of search is indirect verification.

Accuracy of the search of the LV fingerprints or palms from the crime scene towards the bases with indisputable fingerprints or palms.

This is a procedure for identifying the perpetrator of a crime for which latents of fingerprints on the crime scene are collected by forensics. The type of search for latents from the place according to the database with indisputable fingerprints is direct verification.

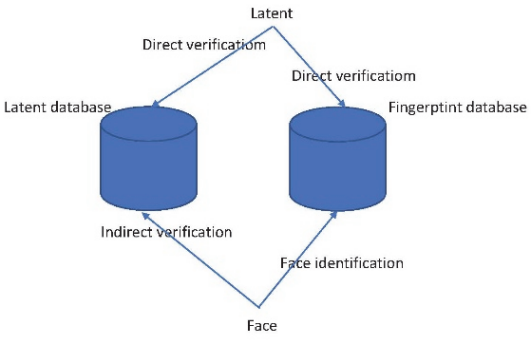

Figure 5 Direct and indirect verification

5.2 Methodology Used in Consideration

The aim of the analysis presented in this paper is to examine the degree of reliability of comparison with and without the possibility of correction or coding of a digitized image between two conceptually different systems of the same purpose-identification using dactyloscopic data, fingerprints and palms, over samples of approximately the same size and data type and quality. It should also be noted that the results of the work of the system created for the affairs of the criminal police due to the greater complexity in terms of types of searches were analysed.

In both systems, the original image of the print is transformed into binary form, the so-called digitization of the image, which is suitable for the system to search. In the first step, a region of importance is extracted from the original image of the print and thus the analysis of parts of the image that are not part of the print is avoided. The orientation of the papillary lines is determined, the lines are separated and a thin or skeleton image of the print is created (the name depends on the system manufacturer, but it is the same type of image) in which each papillary line is one pixel thick. Based on such an image, the AFIS system now sets the minutions and makes comparisons. Also, the accuracy of the search depends on the quality and accuracy of the image selected in this way.

The first system, without the possibility of image correction, but with the possibility of manually encoding the digitized image (setting and deleting the minutes themselves), is marked in the text as system A, in order to avoid stating the names of systems and manufacturers. In accordance with the subject of the paper, only aspects related to the efficiency of comparison with and without the inclusions of the possibility of image corrections are considered. The system A performs fully automatic processing of biometric data and as such sends them for search according to the appropriate databases. The forensic scientists are not allowed to change the image of the print, but only the manipulation with the characteristic points-minutes (Fig. 6). The circle indicates the position of the minutia, and the dash the direction of the papillary line.

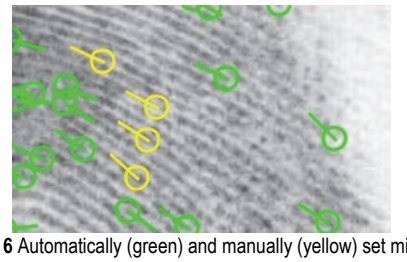

Figure 6 Automatically (green) and manually (yellow) set minutiae

Another system with the possibility of image corrections, here signed as system B, performs automatic processing of dactyloscopic data, with the possibility of a higher degree of change in the digitized image itself, but without the possibility of manual coding (setting minutions). Here, it is possible to "fix" the initial digitized image of the fingerprint in terms of correcting or drawing papillary lines using the knowledge and experience of experts on the flow and mutual position of papillary lines on fingerprints and / or palms (Fig. 7). Minutes are automatically determined by the system each time after a change, based on papillary lines that are automatically drawn or manually redesigned.

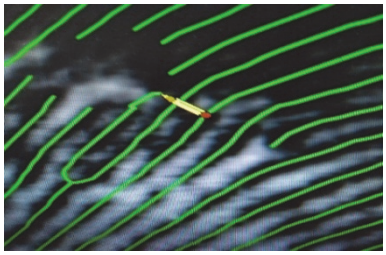

Figure 7 Correction of papillary lines

It should be noted that the algorithms are very complex and represent results of many years of research. They are also incorporated into different solutions from different manufacturers.

5.3 Outcome of Comparison of Search Results in Systems A and B

The comparison of search results in system A and system B was performed in two different environments, production and test. In the first phase, the search results in production systems were considered on a sample database of about 500000 faces and 100000 latents. In this case, the fingerprints as well as the latents are of the same type, without favouring any type of fingerprints or palm prints in number or quality.

5.3.1 Comparison of Search Results in a Production Environment

The analysis of the work of production systems was performed on the data entered into the databases, which were created in real situations, during the commission of criminal acts. The system A contained 531371 face prints and 88181 latents from the crime scene in the database. During one year, the other 13903 face prints and 20405 latents were entered. For the same period, in the system B, the database contained 459922 fingerprints and 110087 latents, and in one year, the other 14018 face prints and 21714 latents were entered (Tab. 1, Fig. 8).

Table 1 Description of the volume of data in the observed databases

	System A	System B
Database size		
Faces Latents	531371 88181	459922 110087
One year records		
Personal data	13903	14018
Latents	20405	21714

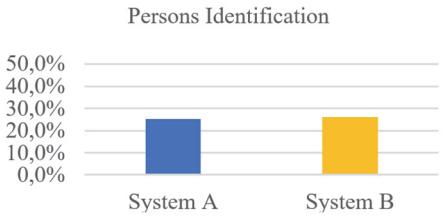

Figure 8 Identification of person

The accuracy of searches in direct and indirect verifications of fingerprints and latents, and verification of fingerprints of persons registered with the fingerprints of persons in the database, were analysed (Fig. 9).

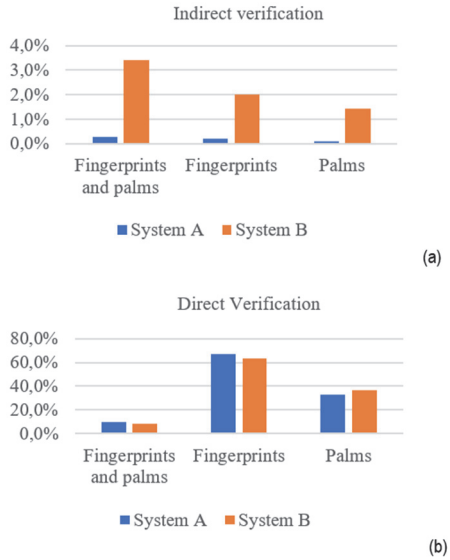

Figure 9 Distribution of indirect (a) and direct verification (b)

The same calendar year was observed for both systems. The result of the accuracy of the comparison during these searches is presented in Tab. 2.The accuracy assessment was performed based on the number of latents entered in a year in relation to the latents identified. The same logic was used to identify the person. As a percentage, the success of both systems in the identification of persons is approximately the same because they are fingerprints of persons who were fingerprinted by experts. The input data used for analysis, in this sample, were of good quality. When it comes to latents from crime scene, we do not have many choices, but we enter all the latents, even those of poorer quality. It means that these are images that do not have clearly visible papillary lines, as well as partial images of prints. Therefore, considered types of searches are relevant for the accuracy results of the AFIS system, while the identification of persons is in second place.

Table 2 Search results according to the observed systems

Search for latents	System A	System B
It has been confirmed that the data on the person already exist in the database, i.e. that it is already registered.	3519/13903 (25.31%)	3656/14018 (26.08%)
Search of fingerprints according to the database of latents indirect verification.	57/20405 (0.28%)	742/21714 (3.42%)
Criminal perpetrators found in the database of latent fingerprints.	40/20405 (0.2%)	432/21714 (1.99%)
Identified criminal perpetrators in the base of nn (not known) palm latents.	17/20405 (0.08%)	310/21714 (1.43%)
According to the latent, the perpetrators of the criminal search were identified according to the database of fingerprints or palms direct verification.	1967/20405 (9.64%)	1732/21714 (7.98%)
Identified by latent fingerprints.	1326/1967 (67.41%)	1099/1732 (63.45%)
Identified by palm latents.	641/1967 (32.59%)	633/1732 (36.55%)
Total identified perpetrators of crimes for one year.	2024/20405 (9.92%)	2474/21714 (11.4%)

Results presented in Tab. 2 show that as both systems have respectable size, there is no significant difference in number of searches for latents that has been confirmed meaning that the data on the person already exist in the database, i.e. that it is already registered. For the search of fingerprints according to the database of latents-indirect verification there was significant difference ($p < 0.001$). Generally, in the analysed sample, in an indirect verification better results were found in the System B, as well as for the searches related to the criminal perpetrators regarding the database of latent fingerprints ($p < 0.001$), and identified criminal perpetrators regarding the database of palm latents ($p < 0.001$). For the search, according to the latent, the perpetrators of the criminal search that were identified according to the database of fingerprints or palms-direct verification in the analysed simple there was significant difference ($p < 0.001$). Generally, in analysed sample, better results were found in System A, related to direct verification, as well as for the search for latents that were identified by latent fingerprints ($p < 0.001$), but for the search related to identification through palms there was no significant difference found. Furthermore, from the total identified penetrators of crime searched in presented sample for one year period of time, the System B has

shown better results with 11.4% identified penetrators ($p < 0.001$).

5.3.2 Comparison of Search Results in a Test Environment

On a test base of a total of 10000 individuals and 1000 latents from the crime scene, both systems (A and B) were considered over the same data sets. The consideration concerned only the identification of the perpetrators by fingerprints. In both systems, 9900 persons were entered with rolled fingerprints of 10 fingers, control prints and palm prints. Then, 100 persons were entered for whom we previously identified with the help of clues, regardless of the consideration that was conducted, that is, from the cases that were resolved in the previous period. 900 arbitrarily taken latents were entered into the database of latents and the other 100 latents that are known to belong to persons who were previously recorded in the database. Due to such a small number in the databases, the search for fingerprints of newly entered persons according to the database of fingerprints of persons with indisputably established identity is not tested, and because of that the result would not provide any useful information.

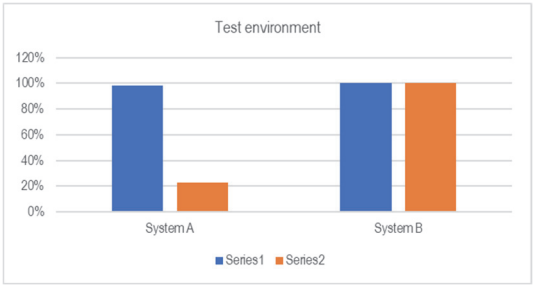

Figure 10 Searching in test environment

Within the obtained results, the position of the fingerprint for which the search is performed was registered, which is also a useful data in relation to the accuracy of the search. The results are presented in Fig. 10 and Tab. 3. Comparing systems A and B in a test environment performed on the same sample regarding search results it was found that in direct verification, search for latents according to the person database, there was no significant difference, but in the case of indirect verification, there was a significant difference ($p < 0.001$) in comparison with face print search according to the latent database.

Table 3. Search results in a test environment

System	System A	System B	p
BP size Faces Latents	 10 000 1 000	 10 000 1 000	 / /
Direct verification			
Search for latents according to the person database	98/100 (98%)	100/100 (100%)	NS
Indirect verification			
Face print search according to latent database	23/100 (23%)	100/100 (100%)	$p < 0.001$

6 CONCLUSION

Today, the development of information technologies transfers business to the digital platform, the use of the Internet and social networks, in which the other party we communicate or do business with cannot be determined with certainty, especially, in the fight against terrorism, cross-border crime and illegal migration. Effective identification is crucial to the security and efficient functioning of any society. This paper presented the results of research that included the application of different AFIS systems, i.e. fingerprint identifications, which is still one of the most reliable methods for establishing the identity of a person, as a framework for solving this problem.

By analysing the search algorithms of two different AFIS systems that are in use in most countries of the world, we came to the conclusion that still, although automated, the accuracy of dactyloscopic comparison depends on the human factor. It also remains to be noted that the accuracy of search algorithms directly depends on the image quality of the print, i.e. the higher the image quality, the better the search results.

Particular emphasis should be placed on the part of the paper in which the test results are presented. They confirm that although the degree of automation is lower and additional expert work is needed to work with prints, systems that have additional capabilities to manually enhance the digitized image are a better choice for working on identifying perpetrators and identifying persons in general.

In real work with system A, one must wait for the person who is registered dactyloscopically to commit a new crime that will be of a later date in relation to the date of registration in order to be identified as the perpetrator, i.e. high probability (77%) that the person will not be identified for the act he has already committed even though the data exist in the database. This allows the offender to avoid sanctions for the act committed and, of course, leaves the possibility for the act to be repeated.

During the dactyloscopic registration of the perpetrator, System B will automatically detect whether the person is the perpetrator of a criminal offense for which records in the database exist. We see that in direct verification the system achieved 7.98% of identifications, and in indirect verification 3.42%, which according to the data we had for production of the B system, means that 742 works will be clarified, although there was no additional information that would help to resolve them.

From the production work we can see that the System B in the overall performance has a 1.42% better result, which in total during the analysed year represents 450 solved crimes more than the System A. Taking into account the importance of solving each crime, having in mind the material and non-pecuniary damage suffered by the injured party as well as the possibility that the perpetrator is a returnee and preventing him from repeating the crime, this number certainly favours this type of AFIS system.

The results of comparison in test environment on the same sample have shown that between examined systems exist statistically significant difference ($p < 0.001$) in indirect verification. The results conducted in production environment have shown that for the search of fingerprints according to the database of latents-indirect verification there was statistically significant difference ($p < 0.001$), for the fingerprint and palms either. For the search, according to the latent, the perpetrators of the criminal search that were identified according to the

database of fingerprints or palms-direct verification in the analysed simple there was significant difference ($p < 0.001$), with significant difference in fingerprint comparison, and without significant difference in palms cooperation.

At the same time, new biometric technologies - including iris and facial recognition - mean that the AFIS is rapidly transforming into the ABIS (Automated Biometric Identification System), providing law enforcement agencies with an even more powerful tool.

With the new generation of ABIS software, fingerprint examiners can process multiple complex biometric transactions with high accuracy and link face recognition to fingerprint or iris recognition [17].

7 REFERENCES

[1] MoI (2003). *Requirements Specification for MoI AFIS and FIIS.*

[2] Champod, C. & Chamberlain, P. (2009). *Fingerprints from*. Handbook of Forensic Science Routledge, Accessed on.

[3] Zaeri, N. (2011). Minutiae-based Fingerprint Extraction and Recognition, *Arab Open University, Kuwait*. https://doi.org/10.5772/17527

[4] Grubor, G., Heleta, M., Ristić, N., & Barać, I. (2016). Integrated management model of the corporate digital forensic investigation. *Technical gazette*, *23*(6), 1591-1600. https://doi.org/10.17559/TV-20141121105105

[5] Feng, J. (2017). *Fingerprint Recognition, Department of Automation*. Tsunfhua University, IAPR/IEEE Winter School on Biometrics.

[6] Nadine, C. (2020). *Keeping biometric data on the same page with new International Standards*. https://www.iso.org/

[7] Council Decision 2008/616/JHA, Official Journal of the European Union, L 210/12, 2008.

[8] Smart, A. (2002). *Card Alliance White Paper*. Secure Personal Identification Systems: Policy, Process and Technology Choices for a Privacy-Sensitive Solution.

[9] Seewww.integratedbiometrics.com

[10] Mohammad, A. A., Al-Alem, F., Al-Ayyoub, M., Jararweh, Y., & Gupta, B. (2019). Impact of digital fingerprint image quality on the fingerprint recognition accuracy. *Multimedia Tools and Applications*, *78*(3), 3649-3688. https://doi.org/10.1007/s11042-017-5537-5

[11] Regodić, M., Gigović, Lj., Bajić, Z., & Vasiljević, S. (2017). Contrast enhancement of color digital images. *Technical gazette*, *24(3),* 935-941. https://doi.org/10.17559/TV-20150410194409

[12] Orandi, S., Libert M., J., Grantham, D. J., Lepley, M., Bandin, B., Ko, K., Lindsay, M. P., Stephen, S. W., Stephen, G. H. (2013). *Examination of Downsampling Strategies for Converting 1000 ppi Fingerprint Imagery to 500 ppi.* National Institute of Standards and technology, U.S., Department of comerce. https://doi.org/10.6028/NIST.IR.7839

[13] Makinana, S., Khanyile, N., & Khutlang, R. (2016). Latent fingerprint wavelet transform image enhancement technique for optical coherence tomography. *Conference: Third International Conference on Artificial Intelligence and Pattern Recognition (AIPR).* https://doi.org/10.1109/ICAIPR.2016.7585203

[14] Meuwly, D. (2009). Forensic Evidence of Fingerprint. *Encyclopaedia of Biometrics,* 528-535. https://doi.org/10.1007/978-0-387-73003-5_181

[15] Beslay, L. Galbally, J., & Haraksim, R. (2018). Automatic fingerprint recognition: from children to elderly. *Technical report by the Joint Research Centre (JRC).*

[16] Sahu, S., Mishra, T. S., & Rao, P. (2015). Fingerprints based gender classification using Adaptive Neuro Fuzzy Inference System. *International Conference on Communications and Signal Processing (ICCSP).* https://doi.org/10.1109/ICCSP.2015.7322700

[17] http://thalesgroup.com/en/markets/digital-identity-and-security/goverment/biometrics/biometric-software/automated-biometric-identification-system/

Contact information:

Nataša PETROVIĆ, Msc, Forensic expert
(Corresponding author)
Ministry of the Interior,
Kneza Miloša 101, Belgrade, Serbia
E-mail: natasa.petrovic@mup.gov.rs

Snežana STOJČIĆ, Msc, IT expert
Ministry of the Interior,
Kneza Miloša 101, Belgrade, Serbia
E-mail: snezana.stojcic@mup.gov.rs

Radovan RADOVANOVIĆ, PhD, Full Professor
Criminal Police University,
Cara Dušana 196, Belgrade, Serbia
E-mail: radovan.radovanovic@kpa.edu.rs

Vojkan NIKOLIĆ, PhD, Assistant Professor
Criminal Police University,
Cara Dušana 196, Belgrade, Serbia
E-mail: vojkan.nikolic@kpa.edu.rs

Mina PETROVIĆ, IT manager
Faculty of Organisational Science, University of Belgrade
Jove Ilića 154, Serbia
E-mail: mina.petrovic.vp@gmail.com