UDC 51-76: 004.7
https://doi.org/10.47533/2024.1606-146X.15

T. SHORMANOV[1], T. MAZAKOV[1,2], SH. JOMARTOVA[1], M. ALIASKAR[1], A. MAZAKOVA[1], A. ZHAKSYMBET[1]*

*[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan;
[2]Research Institute of Mathematics & Mechanics at Al-Farabi Kazakh National University, Almaty, Kazakhstan*

CREATION OF A SOFTWARE AND HARDWARE COMPLEX FOR FINGERPRINT IDENTIFICATION

In this paper, we have studied the following biometric identification of a person by fingerprints. The methodology of the experimental studies is considered, the process of processing the results of identification is described. This paper develops a system of human recognition by fingerprints. The recognition system is designed for data storage, further processing, identification and display of fingerprint images. FPM10A scanner and Arduino microcontroller are used for biometric human identification by fingerprints. The paper considers the Distinguishing features of finger papillary patterns by their structure. Fingerprint matching results with different rotation through the scanner. The article deals with image processing algorithms for biometric identification by fingerprints. Distinguishing features of finger papillary patterns by their structure were investigated, considering different pressures, velocities, directions, ambient temperatures, humidity, etc. levels result in different images. Thanks to various algorithms for Digital image processing and analysis, represented by the SIFT and SURF descriptors, allows for quick characterization of each image.

We used a photographic database obtained from public sources – Fingerprint Verification Competition 2004 (FVC2004). As a result, the graphical representation as well as the number of matching keypoints by fingerprints were investigated. The search for key points is performed using the Hesse matrix. The determinant of the Hesse matrix (Hessian) is maximal at the point where the change in luminance gradient is maximum. Fingerprints were acquired using the "Cross Match V300" optical sensor. In the experiment, the software developed system is invariant to image rotations.

Key words: *Biometrics, fingerprints, identification system, papillary patterns, fingerprint comparison.*

Introduction. There are many ways to protect both information and physical objects, which are used depending on the required level of security for a particular object. One of these methods of protection are biometric systems [1-2], more specifically fingerprint-based identification systems. Such systems have become widespread and have good prospects for further development due to their adaptability. The introduction of biometric technology, and in particular fingerprint recognition, greatly enhances the degree of object security, and significantly increases the quality of identification by eliminating the need for a special card, badge, key, you only need a unique fingerprint, which cannot be forgotten or lost. Systems based on fingerprinting compare the memory print obtained with other prints stored in the system's databases or with the print of a particular person, the method of comparison also depends on the application of this technology [3]. Fingerprints were first addressed in 1877, when the Englishman William Herschel hypothesized the uniqueness and immutability of the papillary pattern on the palms of men [4]. The first mention of the use of fingerprinting techniques for criminal identification dates back to 1902 in Great Britain.

* E-mail корреспондирующего автора: tt007@mail.ru

There is evidence that dactyloscopy was of interest to people long before 1877, as an example of this is chiromancy (an ancient type of divination by the papillary and flexor lines of the palm of a person). Thus, historically, at the initial stage, fingerprints and fingerprints found the greatest use in forensics, and are still relevant, but already on a larger scale.

Research methods

As authentication information in this case are taken into account the original and inherent characteristics of the person. Authentication methods based on the measurement of human biometric parameters provide almost 100% identification, solving the problem of lost passwords and personal identifiers.

The most commonly used ones are:

1) Fingerprints. It is known that they are unique to each person, and do not change throughout life. To scan fingerprints is used the cheapest equipment (compared with other methods of biometric authentication), besides, this method is familiar to users and does not cause any worries. However, it is believed that inexpensive fingerprint scanners can be fooled by a specially made artificial finger.

2) Improving the reliability of identity authentication systems is an urgent scientific and technological challenge. The accuracy of identification (establishment) and identification (confirmation) depends largely on the adequacy of the mathematical model implemented. Theoretical studies of the problems under consideration are devoted to the works of [5-6].

Main part

Algorithms of biometric identification by fingerprints. Due to its forensic value, traces of human hands occupy the first place in the group of methods of identification of persons. This is explained as its frequency of detection, the fact that with its help one can quickly enough identify the person who left the fingerprints, as well as identify the relationship of this person with other incidents in which the same fingerprints were found. Such possibilities are due to the peculiarities of the structure of the skin on the fingers of the hand, namely the uniqueness of the papillary patterns. Fingerprints or parts of the palm provide many opportunities for identification and for limiting the list of suspects.

Identification signs of finger teat patterns are usually divided into global and local signatures [7].

Global Signatures you can see with the naked eye include. Such features include Type and type of capillary pattern, direction and steepness of capillary line flow, structure of the central pattern, structure of delta, number of capillary lines from center to delta, and many other features.

Another feature is that local. Also called minutiae (features, special points). Unique features that are unique to a particular print and determine the points of change in the structure line's (termination, division, breakage, etc.), the direction of the line, and the coordinates at these points. A single print may contain up to 70 or more miniatures.

Several types of descriptors were used in this study: SIFT, SURF, and ORB [8]. An analysis of the effectiveness and speed of technologies and algorithms for facial biometrics leads to the following conclusions.

Using the approach based on the allocation of key points in the image for biometric identification by fingerprints, allows to create on its basis a software system for rapid recognition of fingerprints and the subsequent search.

SURF/SIFT algorithms have better classification abilities when solving domestic search problems on textured images. Both algorithms require more hardware and are suitable for other computer vision tasks. Both algorithms are patented, and commercial use is prohibited without the consent of the copyright holders. "Overpowered" in the fingerprinting task.

ORB algorithm has higher speed compared with the above algorithms SIFT / SURF methods and is more suitable for fingerprint biometric identification tasks. The ORB algorithm descriptor is a binary descriptor and checking for a match for such descriptor, the sum of the Hamming distances for each byte of the descriptor is. The application of this algorithm is suitable for search tasks due to the fact that it is not a complete fingerprint.

Analysis based on comparison of local features - minutiae are the most common approach for identification due to the widespread belief that they are the most legible and reliable features [9-10]. However, this method creates serious problems related to the large distortions caused by matching fingerprints with different rotations. An example of such a match is shown below (Image 1) Distortions from the FVC2004 DB1 database (102_3.tif and 102_5.tif). Fingerprints look too similar to each other to fit standard image searches.

Fingerprints of the same person never look the same on two readings. Different pressure, speed, direction, ambient temperature, skin moisture/humidity, etc. will result in different images. Also, in [11] there is an example of age-related changes in fingerprints, with age fingerprints become less clear and can change.

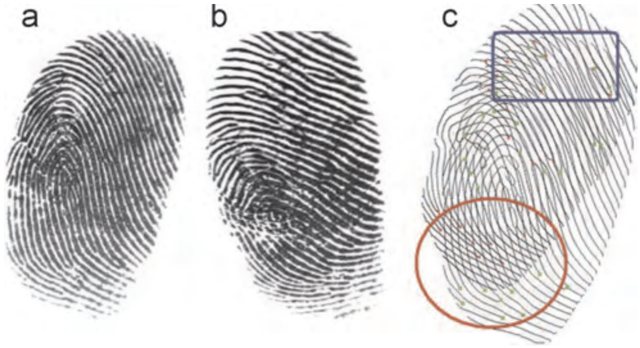


Image 1 – Results of matching fingerprints in different rotations

The task of biometric identification by fingerprints refers to one of the problems solved by modern image processing algorithms. We used a photographic data base obtained from public sources – Fingerprint Verification Competition 2004 (FVC2004) [12], and the result of the work: a graphic image of matching number of matches between keypoints and fingerprint keypoints. In FVC2004, the emphasis is on distortion, and on imaging dry and wet fingerprints. Fingerprints areacquiredwith an optical sensor "CrossMatch V300".

There are certain correlations between discriminative features of the structure of the nipple pattern of the same person obtained at different times, which need to be established. For this purpose, we use a so-called precedent, i.e., a set of fingerprint images that have already been identified using this algorithm.

Such a precedent is called a training sample. Based on them, the most appropriate processing and classification algorithm is chosen. Several types of descriptors were considered and used in this study, including SIFT, SURF, and ORB descriptors.

Analysis of search algorithms and identification by image showed that for the task of identification by fingerprint is effective to use the key point descriptors, due to the fact that they provide a high degree of accuracy fingerprint classifier (descriptor), and also have a good function of identification by partial fingerprint, an example of displays a 30-item evaluation in Figure 2.

Experimental study of biometric identification by fingerprints, the developed software system, created based on the proposed method of finding key points, was shown to be invariant to image rotation. Capable of operating in a wide range of light varies up to 50-70% of the light intensity in the image and is invariant to changes in scale and minor distortions.

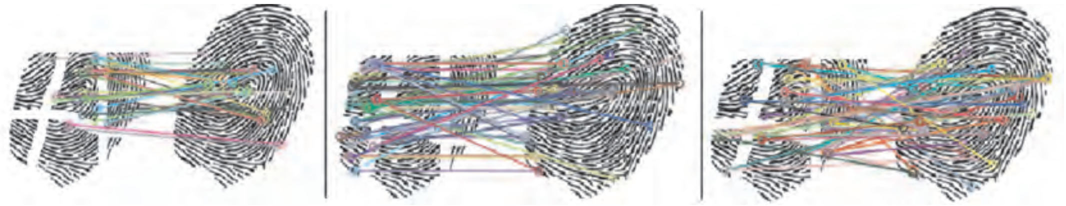
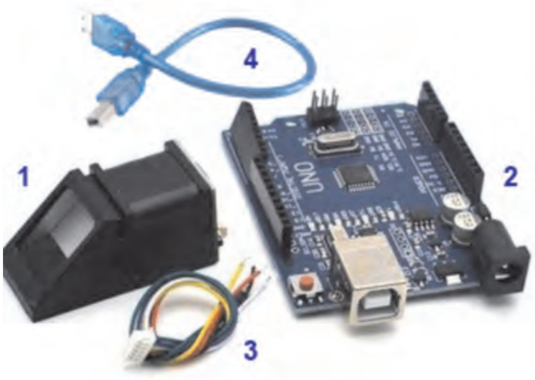


Figure 2 – Evaluation of 30 keypoint descriptors ORB (left), SIFT (center), SURF (right)

Discussion

Practical implementation. Secure systems can be accessed through passwords and keys, both of which can be inconvenient and easily forgotten. FPM10A module with Adafruit Arduino library was used to create a block of biometric system for human identification by fingerprints [13-14].

Figure 3 shows the elements of the image acquisition and fingerprint identification unit. The specified unit is implemented based on the Arduino UNO controller.



1 – FPM10A optical fingerprint scanner; 2 – Arduino UNO;
3 – wires to connect the scanner to the Arduino; 4 – USB cable for Arduino
Figure 3 – Fingerprint scanner

Arduino is a device based on the ATmega 328 microcontroller [15-16]. It contains everything needed for simple microcontroller operation: 14 digital I/Os (6 of which can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal pickup, a USB connector, a power connector, an on-chip programming socket (ICSP) and a reset button. To start working with the device, simply power it up with an AC/DC adapter or battery or connect it to a computer via a USB cable.

Optical fingerprint scanner - a module that can be used with Arduino and other microcontrollers [15]. Capable of storing fingerprints (1000 fingerprints) with their further identification. Used in places of strict secrecy, as a kind of password key access, based on scanning and verification of fingerprints from a database.

Another function of fingerprints is general matching. Like everything in the human body, the finger pattern is formed through a combination of genetic and environmental factors. The genetic code in DNA forms the general basis of skin patterning [17].

FPM10A Fingerprint Scanner Specifications:

- power supply voltage from 3.6 to 6 volts DC.
- operating current up to 120mA, peak current - 140 mA.
- fingerprint scanning time of up to 1 second.
- scan window size: 14 x 18 mm.
- interface: UART (TTL logical level) or USB2.0/USB1.1.
- interface: UART (TTL logical level) or USB2.0/USB1.1.
- temperature working environment from - 20C to + 50C.
- relative humidity 40 % RH to 85 % RH (no condensation).
- size: 56 x 20 x 21.5 mm.
- weight: up to 40 gr.
- Chinese production.

When using the fingerprint sensor, there are two basic steps. First, the data is written to the sensor memory, that is, a unique ID is assigned to each fingerprint, which will be used for comparison later. After recording, you can proceed to "Search" while comparing the image of the current print with the image recorded in the sensor memory [18-19].

To record fingerprints included software for Windows (this is the easiest and most convenient option because can see in the pictures that are taken) or sketch for Arduino (relevant for those who do not have Windows).

Recording new prints through a Windows program

As mentioned above, the easiest way to write new data to the optical fingerprint sensor memory is through a Windows program. Unfortunately, there is no software for other operating systems.

First, the sensor must be connected to the computer using a USB-to-serial converter (Figure 4). Loading the "blank sketch" on the Arduino:

```
// this sketch gives us a way around the Atmega chip
// and connect the fingerprint sensor directly to the USB/Serial converter
// Red is connected to +5V
// Black connects to Ground
// white is connected to Digital 0
// Green is connected to Digital 1
voidsetup() {}
voidloop() {}
```

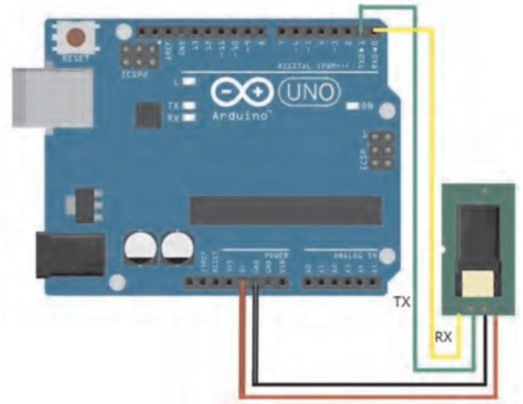
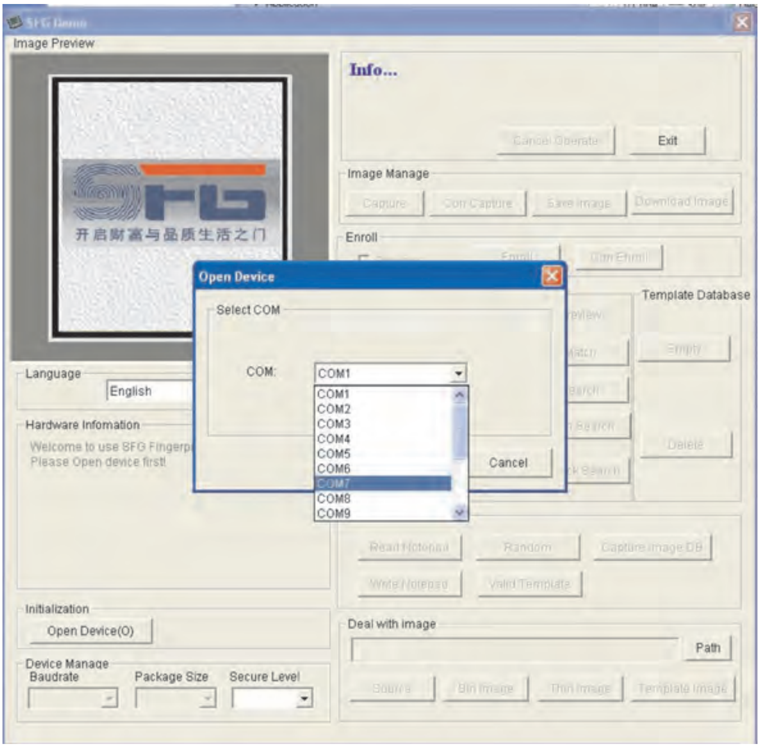


Figure 4 – Diagram for connecting the scanner to the Arduino

Using the SFGDemo program (Figure 5) and ArduinoIDE, new fingerprints are loaded, assigning each one a new ID #. All uploaded fingerprint images are encrypted (Figure 6).



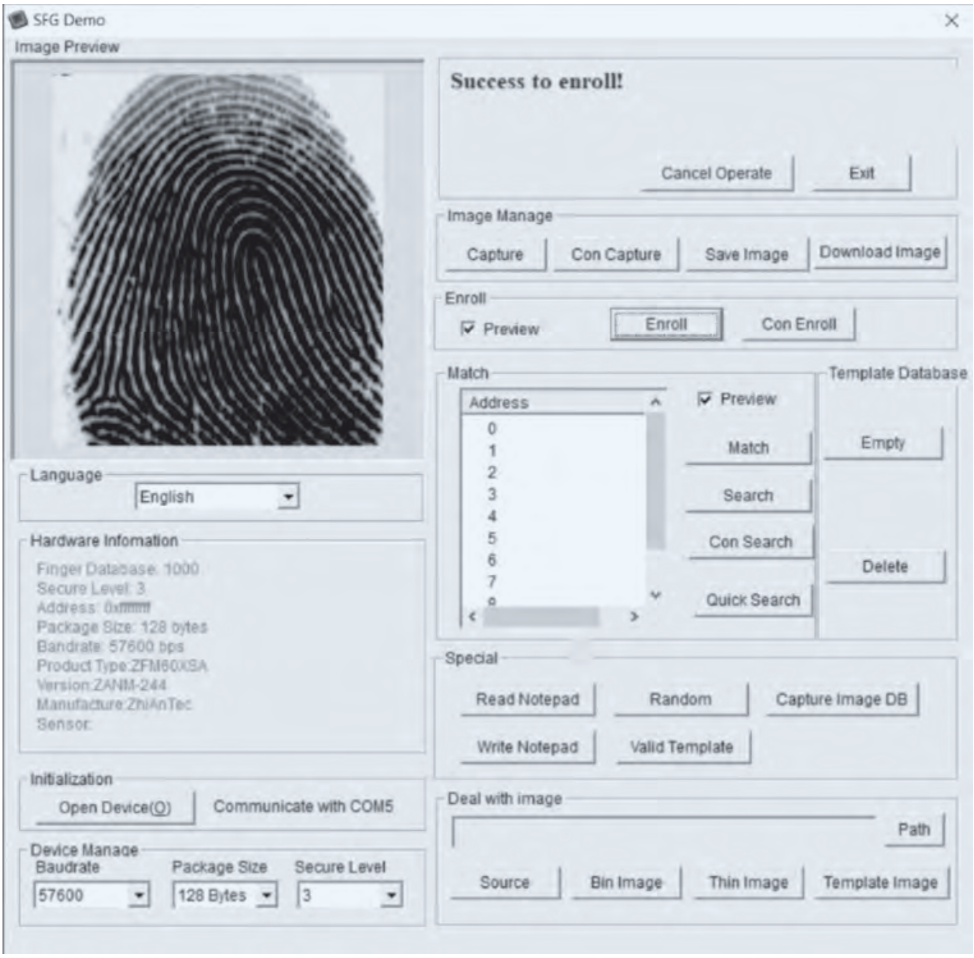
Language: English

Hardware Infomation

Welcome to use SFG Fingerp
Please Open device first!

COM: COM1

Figure 5 – SFGDemo program



SFG Demo

Image Preview

Success to enroll!

Language: English

Hardware Infomation

Finger Database: 1000
Secure Level: 3
Address: 0xffffffff
Package Size: 128 bytes
Bandrate: 57600 bps
Product Type:ZFM60XSA
Version:ZANM-244
Manufacture:ZhiAnTec
Sensor:

Initialization

Communicate with COM5

Device Manage

Baudrate: 57600
Package Size: 128 Bytes
Secure Level: 3

Enroll

☑ Preview

Match

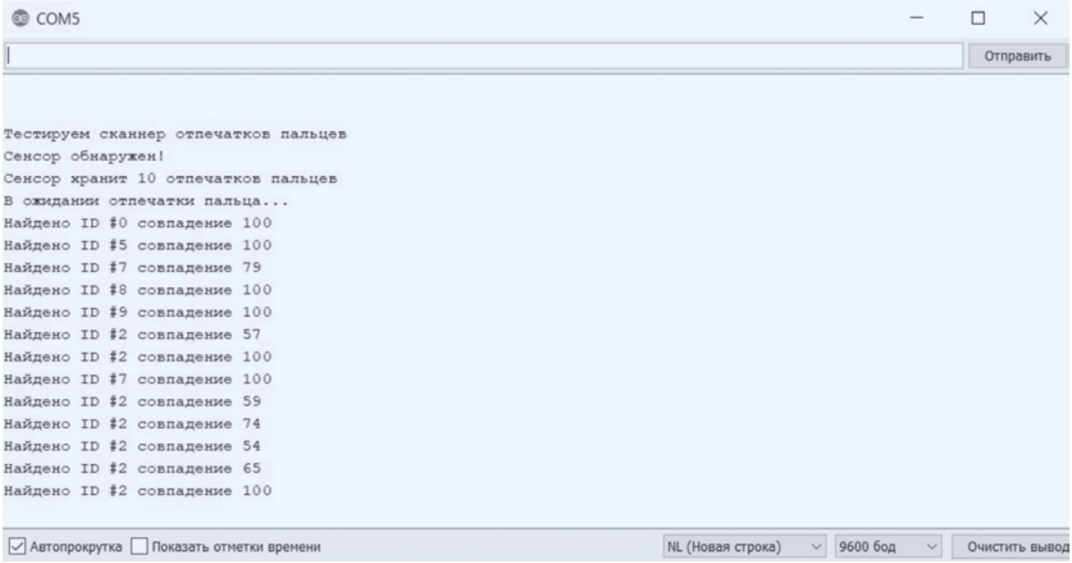
☑ Preview

Figure 6 – Uploading fingerprints to the database

After loading the fingerprints into the base, disconnect the green and white contacts and connect the green conductor to contact digital 2, and the white conductor to digital 3. Using the "Adafruit_Fingerprint" library, load an example "fingerprint" sketch onto Arduino IDE. Open the serial monitor window by setting the baud rate to "9600 baud" and, when prompted, put your finger on the fingerprint sensor [20].

In Figure 7 you can see the percentage of matching. Fingerprints that do not match the fingerprints stored in the database are ignored by the scanner.

Conclusion. During this work the following tasks were investigated: the methodology of the experimental studies was analyzed, the process of processing the results using a biometric scanner for human identification by fingerprints was described. A promising area of use of the FPM10A module with the Adafruit Arduino library is the addition of software products for search by non-full fingerprints are often only part of the actual fingerprint to be searched for a match. Using the approach based on the allocation of key points in this image is for biometric authentication by fingerprint, allows to create on its basis a software



```
Тестируем сканнер отпечатков пальцев
Сенсор обнаружен!
Сенсор хранит 10 отпечатков пальцев
В ожидании отпечатки пальца...
Найдено ID #0 совпадение 100
Найдено ID #5 совпадение 100
Найдено ID #7 совпадение 79
Найдено ID #8 совпадение 100
Найдено ID #9 совпадение 100
Найдено ID #2 совпадение 57
Найдено ID #2 совпадение 100
Найдено ID #7 совпадение 100
Найдено ID #2 совпадение 59
Найдено ID #2 совпадение 74
Найдено ID #2 совпадение 54
Найдено ID #2 совпадение 65
Найдено ID #2 совпадение 100
```

Figure 7 – Fingerprint recognition

system for rapid recognition of fingerprints and the subsequent search. SURF/SIFT algorithms have better classification abilities when solving domestic search problems on textured images. Both algorithms require more hardware and are better suited to other computer vision tasks, and both algorithms are patented and prohibited for commercial use, without the consent of the copyright holder. For fingerprint identification tasks, they are "overpowered". ORB algorithm has higher speed compared with the above algorithms SIFT / SURF, and more suitable for the task of biometric identification by fingerprints. The descriptors of the ORB algorithm are binary descriptors, and the check for matching such descriptors is the sum of the Hamming distances of each byte of the descriptor. The application of this algorithm is suitable for search tasks by not a complete fingerprint. Numerical studies performed on the model problem showed the effectiveness of human recognition by fingerprints.

This study used a photographic database-Fingerprint Verification Competition 2004 (FVC2004)-obtained from a public institution. In this context, we examined the graphical display of matching key points and the number of key points matched by fingerprints. The search for key points is performed with the help of the Hesse matrix. The determinant of the Hesse matrix (Hessian) is maximal at the point where the change in luminance gradient is maximum. Fingerprints were acquired using the Crossmatch V300 optical sensor. Experiments showed that the developed software system is invariant to image rotation.

Funding. The work was carried out at the expense of the Research Institute of Mathematics and Mechanics at Al-Farabi Kazakh National University and grant funding for scientific research for 2023-2025 under the project AP19678157 “Development of a hardware and software complex for monitoring the state of the occupancy level of a reservoir”.

REFERENCES

1 Zadorozhny V.V. (2004). Identification by fingerprints. PC Magazine. *Russian Edition*, *1*, 5.

2 Makeev, S. C. (2000). BIOMETRY? BIOMETRY. BIOMETRY! Science-intensive technologies and intelligent systems in XXI century. *Collection of scientific works of youth scientific-technical conference*, 102-105.

3 Larina E. A., Glushko A. A. (2016). Scanning methods for obtaining fingerprints. *Young Scientist*, *27*, 97-107.

4 Herschel William J. (1916). The Origin of Fingerprinting. *Oxford University Press*.

5 Katorin Y. F., Razumovsky A. V., Spivak A. I. (2012). Information protection by technical means. SPb: *NRU ITMO,* 416.

6 Shangin V. Ф. (2012). Complex protection of information in corporate systems. M.: *Forum Publishing House,* 592.

7 Гололобов В. Н. (2019). Arduino для любознательных. СПБ.: *Наука и техника,* 240.

8 X. Tan and B. Bhanu. (2002). Robust fingerprint identification. *Proceedings of the 2002 International Conference on Image Processing, Rochester*. *NY, USA, 1*, 1-277. https://dblp.org/db/conf/icip/index: 14.03.2023

9 Rosten, Edward, Tom Drummond. (2006). Machine learning for high-speed corner detection, 9th European Conference on Computer Vision (ECCV), *430 – 443*.

10 Michael Calonder, Vincent Lepetit, Christoph Strecha, Pascal Fua. (2010). "BRIEF: Binary Robust Independent Elementary Features", 11th European Conference on Computer Vision (ECCV), *778–792*.

11 Biometric Systems Lab. (2004). Pattern Recognition and Image Processing Lab. Biometric Test Center [Online]. Available: http: // bias.csr.unibo.it/ fvc2004/.

12 Zitova B., Flusser J. (2013). Image registration methods: a survey // Image and Vision Computing, *21, 977–1000*.

13 Larina E. A., Glushko A. A. (2016). Scanning methods for obtaining fingerprints. *Young Scientist, 27,* 97-107.

14 Petin V. A. (2016). Projects using Arduino controller. SPb: *BHV-Peterburg,* 464.

15 Boxell, J. (2017). Learning Arduino. 65 projects with your own hands. SPb: *Peter,* 400.

16 Belov A. B. (2018). Arduino. From the basics of programming to creating practical devices. SPb: *NIT,* 480.

17 Lowe D. G. (2009). Object recognition from local scale-invariant features // Proc. Intl. Conference on Computer Vision, *1150–1157*.

18 Mazakov T.O., Jomartova Sh. A., Shormanov T. S., Ziyatbekova G. Z., Amirkhanov B. S., Kisala P. (2020). The image processing algorithms for biometric identification by fingerprints. News of the national academy of sciences of the Republic of Kazakhstan. *Series of Geology and Technical Sciences, 1(439)*, 14-22.

19 Aliaskar, T. Mazakov, A. Mazakova, S. Jomartova and T. Shormanov. (2022). Human voice identification based on detection of fundamental overtones. *IEEE 7th International Energy Conference (ENERGYCON),* 1-4. doi: 10.1109/ENERGYCON53164.2022.9830471.

20 Soweon Yoon and Anil K. Jain. (2015). «A longitudinal study of fingerprint identification» *PNAS*, 8555-8560.

Т. С. ШОРМАНОВ*[1]*, Т. Ж. МАЗАКОВ*[1,2]*, Ш. А. ДЖОМАРТОВА*[1]*,
***М. С. ӘЛИАСҚАР*[1]*, Ә. Т. МАЗАҚОВА*[1]*, А. Т. ЖАҚСЫМБЕТ*[1]

[1]*әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан;*
[2]*әл-Фараби атындағы Қазақ ұлттық университетінің Математика және механика ғылыми-зерттеу институты, Алматы, Қазақстан*

САУСАҚ ІЗІ БОЙЫНША СӘЙКЕСТЕНДІРУГЕ АРНАЛҒАН БАҒДАРЛАМАЛЫҚ-АППАРАТТЫҚ КЕШЕН ҚҰРУ

Мақала саусақ іздері арқылы адамның биометриялық сәйкестендіруін зерттеуге арналған. Эксперименттік зерттеулердің әдістемесі қарастырылып, сәйкестендіру нәтижелерін өңдеу үдерісі сипатталған. Бұл жұмыста саусақ іздері арқылы адамды тану жүйесі жасалған. Тану жүйесі деректерді сақтауға, оны әрі қарай өңдеуге, саусақ іздерінің суреттерін анықтауға және көрсетуге арналған. Адамды саусақ ізімен биометриялық анықтау үшін FPM10A сканері және Arduino микроконтроллері қолданылады. Жұмыста саусақтардағы папиллярлық өрнектер құрылымының сәйкестендіру белгілері қарастырылған. Саусақ іздерін әр түрлі айналдыру арқылы сәйкестендіру сканер нәтижесінде пайда болады. Мақалада саусақ ізін биометриялық сәйкестендіруге арналған кескінді өңдеу алгоритмдері қарастырылады. Әр түрлі қысым, жылдамдық, бағыт, қоршаған орта температурасы және ылғалдылық деңгейі алуан түрлі кескіндерге әкелетінін ескере отырып, саусақтардағы папиллярлық үлгілердің құрылымының сәйкестендіру белгілері зерттелді. Кескінді сандық өңдеу мен талдаудың әртүрлі алгоритмдерінің арқасында, мысалы: SIFT тұтқасы (дескрипторы), сондай-ақ ең жақын бәсекелес SURF тұтқасы, әр кескіннің бірегей сипаттамаларын жылдам алу мүмкіндігі пайда болды.

Бұл зерттеуде ашық көздерден алынған фотосуреттер базасы қолданылды – Fingerprint Verification Competition 2004 (FVC2004). Жұмыс нәтижесінде сәйкес келетін негізгі нүктелердің графикалық бейнесі, сондай-ақ саусақ іздері бойынша сәйкес келетін негізгі нүктелердің саны зерттелді. Негізгі нүктелерді іздеу Гессе матрицасы арқылы жүзеге асырылады. Гессиан матрицасының детерминанты жарық градиентінің максималды өзгеру нүктелерінде экстремумға жетеді. Саусақ іздері "Cross Match V300"оптикалық сенсорының көмегімен алынды. Эксперименттік зерттеу нәтижесінде әзірленген бағдарламалық жасақтама жүйесі кескінді бұруға инвариантты екендігі анықталды.

Түйін сөздер: *биометрия, саусақ іздері, сәйкестендіру жүйесі, папиллярлық өрнектер, саусақ іздерін салыстыру.*

Т. С. ШОРМАНОВ*[1]*, Т. Ж. МАЗАКОВ*[1,2]*, Ш. А. ДЖОМАРТОВА*[1]*,
***М. С. ӘЛИАСҚАР*[1]*, Ә. Т. МАЗАҚОВА*[1]*, А. Т. ЖАҚСЫМБЕТ*[1]

[1]*Казахский национальный университет имени аль-Фараби, Алматы, Казахстан;*
[2]*Научно-исследовательский институт математики и механики Казахского национального университета им. аль-Фараби, Алматы, Казахстан*

СОЗДАНИЕ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДЛЯ ИДЕНТИФИКАЦИИ ПО ОТПЕЧАТКАМ ПАЛЬЦЕВ

Статья посвящена исследованию биометрической идентификации человека по отпечаткам пальцев. Рассмотрена методика экспериментальных исследований, описан процесс обработки ре-

зультатов идентификации. В данной работе разработана система распознавания человека по отпечаткам пальцев. Система распознавания предназначена для хранения данных, дальнейшей её обработки, идентификации и отображении снимков отпечатков пальцев. Для биометрической идентификации человека по отпечаткам пальцев использован сканер FPM10A и микроконтроллер Arduino. Рассмотрены идентификационные признаки строения папиллярных узоров на пальцах. Получен результат совпадении отпечатков пальцев с различным вращением через сканер. В статье рассматриваются алгоритмы обработки изображений для биометрической идентификации личности по отпечаткам пальцев. Исследованы идентификационные признаки строения папиллярных узоров на пальцах с учетом того, что различное давление, скорость, направление, температура окружающей среды и уровень влажности приводят к разным изображениям. Благодаря различным алгоритмам цифровой обработки и анализа изображении таким как дескриптор SIFT, а также ближайший конкурент – дескриптор SURF, появилась возможность быстрого получения уникальных характеристик по каждому изображению.

В данном исследовании использовалась база данных из фотографий, полученная из открытых источников – Fingerprint Verification Competition 2004 (FVC2004). В результате работы исследованы графическое изображение совпадающих ключевых точек, а также количество совпавших ключевых точек по отпечаткам пальца. Поиск ключевых точек производится с помощью матрицы Гессе. Детерминант матрицы Гессе (гессиан) достигает экстремума в точках максимального изменения градиента яркости. Отпечатки пальцев были получены с помощью оптического датчика «Cross Match V300». Проведенное экспериментальное исследование показало, что разработанная программная система обладает инвариантностью к поворотам изображения.

Ключевые слова: *биометрия, отпечатки пальцев, система идентификации, папиллярные узоры, сравнение отпечатков пальцев.*