O.O. POPOV[1], S. D. ASABASHVILI[1], V.O. ZARITSKYI[1]

Supervisor M.O. PETRYSHCHE[1]

BIOMETRYCZNY SYSTEM KONTROLI DOSTĘPU Z ZASTOSOWANIEM SKANERA ODCISKÓW PALCÓW

Streszczenie: Zwrócono uwagę na pobieranie odcisków palców. Omawiano użycie skaner odcisków palców oraz zestawiono cechy takich jak: cena, jakość i szybkość pracy, aby stworzyć model systemu uwierzytelniania biometrycznego. Dokonano analizy rynku sprzętu biometrycznego i potrzeby stworzenia systemu.

Słowa kluczowe: odciski palców, skaner odcisków palców, identyfikacja, bezpieczeństwo, system

BIOMETRIC FINGER SCANNER ACCESS CONTROL SYSTEM

Summary: Attention was paid to fingerprinting, namely the fingerprint scanner on a set of characteristics such as price, quality and speed of work was chosen to create a model of biometric authentication system. An analysis of the biometric equipment market and the need to create a system have been carried out.

Keywords: Fingerprinting, fingerprint scanner, identification, security system.

1. Annotation

The study designed and developed a universal biometric access system, which comes from a fingerprint scanner for industrial businesses that can be used on a larger advanced security apparatus (requires that they fix the fingerprint scanner on the retina scanner). Specific technical solutions of the software provided with the software are offered.

A functional model for centralization and identification of users based on biometric data has been developed, and a database of these editing functions is described, describing the registered person.

[1] Odesa Państwowa Akademia Regulacji Technicznych i Jakości, Odessa, Ukraina, e-mail: pn11110000@ukr.net

2. Introduction

Today, in an era of rapid development of information technologies and significant proliferation of computer systems, there is a need to ensure fast, convenient and secure access of a person to private property, namely: to personal information, intellectual property, premises, cars and other objects of property.

Along with traditional systems of identification of the person and systems of restriction of access, such as ordinary passwords, pin codes and electronic keys, access systems for biometric parameters are becoming quite popular today. These parameters are fingerprints, retina, DNA and others.

3. Analysis of publications

Currently, fingerprint recognition systems occupy more than half of the biometric market. Many companies are manufacturing access control systems based on fingerprinting. Due to the fact that this area is one of the oldest, it has become the most widespread and is by far the most developed. Fingerprint scanners have come a long way to improve. Modern systems are equipped with various sensors (temperature, pressing forces) that increase the degree of protection against counterfeiting. With each passing day, systems become more comfortable and compact.

4. The purpose of the article is to develop a system of access control through biometric authentication, to implement the storage of this information in the database and to provide the user with the ability to perform certain actions in case of successful passing of the check, registration of information about new users, obtaining statistical information by individual user.

5. Setting objectives

Creation of a system of registration and identification of employees that will be optimal for small and medium-sized enterprises for mass deployment. Creating a versatile, flexible, reliable and inexpensive system.

6. Verification and identification

Verification is a comparison of each other with a biometric template. He verifies that the person is who he pretends to be. Verification is the confirmation of a person by a biometric feature, where the primary authentication was by one of the first two methods mentioned above. The probability that the system will miss an intruder who does not use the remedies is equal to the FAR of the biometric method used. Even for the weakest biometric systems, this probability is very low (Figure 1)[7].

Identification is a one-to-many comparison: after “capturing” biometric data, it connects to a biometric database to determine identity. Identification is successful if the biometric sample is already in the database. Biometric identification is the use of a biometric feature that requires no additional information. The object is searched throughout the database and does not require a previous key. It is clear that the main disadvantage of this is that the more people in the database, the greater the likelihood of wrong access by an arbitrary person. For example, fingerprint systems can hold a base of no more than 300 people and a retina of no more than 3000 people. The main advantage of identification is that all keys will always be with the person, no passwords, no cards, no additional devices are required (Figure 2)[10].

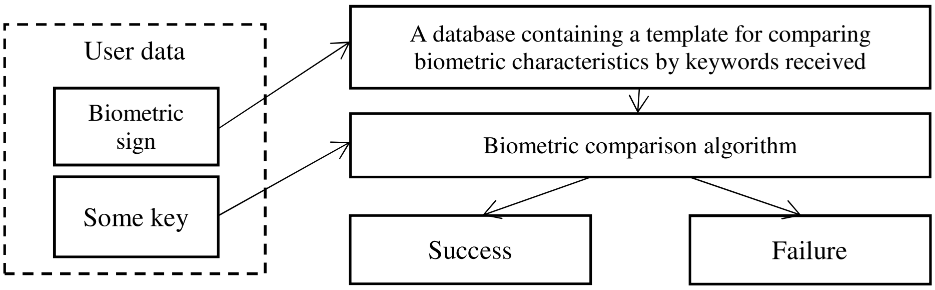

User data
Biometric sign
Some key
A database containing a template for comparing biometric characteristics by keywords received
Biometric comparison algorithm
Success
Failure

Figure 1. Flow chart of biometric system operation in verification mode

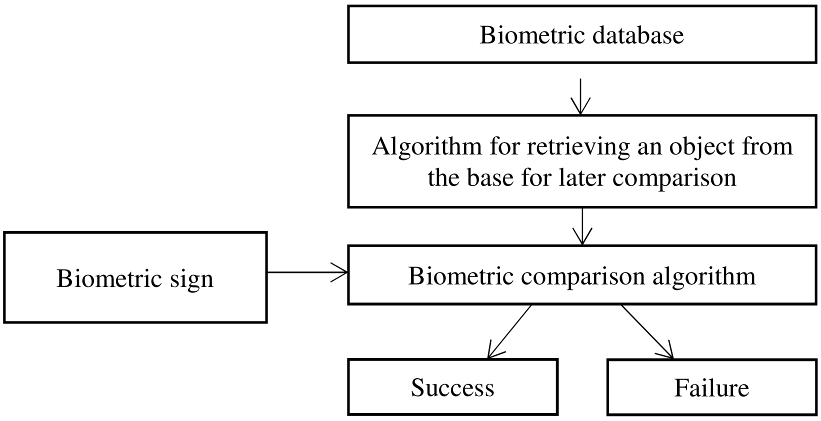

Biometric database
Algorithm for retrieving an object from the base for later comparison
Biometric sign
Biometric comparison algorithm
Success
Failure

Figure 2. Flowchart of biometric identification system operation

Comparing these modes, the following conclusion can be drawn: verification can be performed more quickly as it is known which parameter to compare with, and the likelihood of a check error with all parameters due to the fact that they may be quite similar decreases. As a result, the sensitivity threshold rises. But this mode of operation needs to somehow inform the system that the person wants to be tested, so it is relatively more expensive and difficult to implement. In any mode, reliability can be enhanced by passing multiple validation checks, since the likelihood of error due to the similarity of all of them significantly decreases[9-10].

7. Characteristics of biometric systems

The two main characteristics of any biometric system can be accepted first and second order errors. In the theory of radar, they are usually called "false alarm" or "missing the target", and in biometrics the most common concepts - FAR (False Acceptance Rate) and FRR (False Rejection Rate).

FAR is the error rate, the likelihood of misidentification, that is, the likelihood that the biometric identification system mistakenly recognizes the authenticity of user data (such as fingerprint) that is not logged on to the system.

FMR is the likelihood that the system incorrectly compares an input sample with an incorrect database template.

FRR is the false denial factor - the likelihood that a biometric identification system does not recognize the fingerprint of a registered user.

FNMR - the likelihood that the system will err in determining matches between the input sample and the corresponding database template.

To sense the probabilities of FAR and FRR, one can estimate how often there will be erroneous coincidences if you install an identification system on a passing organization with a staff of N people. The probability of a false match obtained by a fingerprint scanner for a database of N prints is FAR N. And every day through the access control, the order of N people also passes. Then the probability of a FAR (N N) working day error. Of course, depending on the purpose of the identification system, the probability of error per unit of time can vary greatly, but if one error is allowed during the working day, then:

$$FAR \times N^2 \approx 1 => N \approx \sqrt{\frac{1}{FAR}} \tag{1}$$

Then we get that stable operation of the identification system at FAR = 0.1% = 0.001 is possible with the number of personnel N ≈ 30 [1, 5].

8. System constituents (devices) and their relationship

The system includes a fingerprint scanner, a device for communication between the scanner and a computer, application software for performing the necessary actions, a database of users, and a device that needs to perform the necessary actions in case of successful authentication (for example, a microcontroller device that controls the electronic lock)(Figure.3).

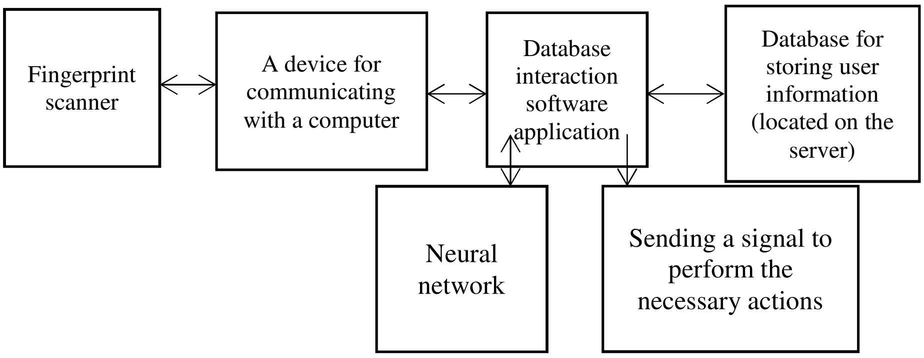

Fingerprint scanner
A device for communicating with a computer
Database interaction software application
Database for storing user information (located on the server)
Neural network
Sending a signal to perform the necessary actions

Figure 3. Block diagram of the system model

The system is designed to allow the user access to the work building (or work space, safe, storage, etc.) at the fingerprint of the user. The system must also generate statistics on user activity, store it in a separate database, and provide the necessary information:

1. Number of registered users;
2. List of users;
3. Detailed information for each user (first name, last name, number of his / her fingerprints in the database, statistics on user activity for all time).

The purpose of this work is to create a model of biometric access control system with fingerprint recognition by a neural network (Figure 3).

Saved fingerprint software in the sensor-based database you use, not identifiers, pinned to specific fingerprints in the memory of the sensor. Also, the software verifies and compares the fingerprints received from the sensors with the reference ones stored in the database, at which point the neural network is used. This solution eliminates the need for fingerprinting in each sensor, thus increasing the security level of the system, since full access to the system is only for the administrator, who deals with the entry of information in the database. With a positive verification result, the software generates and transmits the control signal to the physical equipment that provides access control.

An additional feature of the software is the entry of information about the transfer of persons, current date, time, checkpoints and rights at different levels of access to the database.

9. Fingerprint scanner

Adfruit Industries model FZ1035G was selected as a fingerprint scanner (Fig. 4). According to the principle of operation, the scanner is included in the group "Optical contactless scanners". This model allows you to save up to 162 fingerprints, which is sufficient for the needs of medium-sized companies. The scanner is powered by a data communication device between the scanner and the computer. Data exchange is carried out in the mode of half-duplex serial communication. The standard data rate is 57600 bps. You can also set the baud rate from 9600 to 115200 bps [7, 8, 12].

Figure 4. Appearance of the scanner

There are two parts to fingerprint processing: fingerprint tracking and fingerprint matching (either 1: 1 or 1: N matching). When registering, the user is required to raise the finger twice. The system will create a finger pattern of two images and store it in the local storage. When checking for compliance, the user places his finger on the optical sensor, and the system generates a finger template and compares it with the finger library templates. For a 1: 1 ratio, the system will compare the live finger with the specific pattern indicated in the module. To match 1: N or search, the system will search the entire finger library for that finger. In both cases, the system will return the corresponding result, success or failure[11].

10. A device for communicating between a scanner and a computer

The Arduino Uno microcontroller board is used as the communication device (Figure 5). The power to the scanner comes from the 5V output of Uno, and the power to the Uno comes from a standard USB cable that connects the board to the computer. The Uno board is also connected to the scanner with two TX / RX wires for data exchange. The Uno data exchange with the computer is done via the virtual COM port [2-3,6].

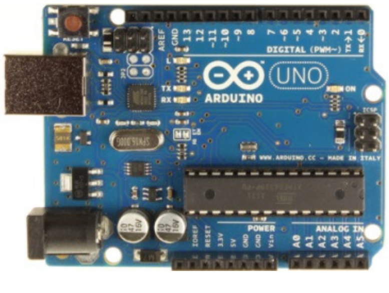
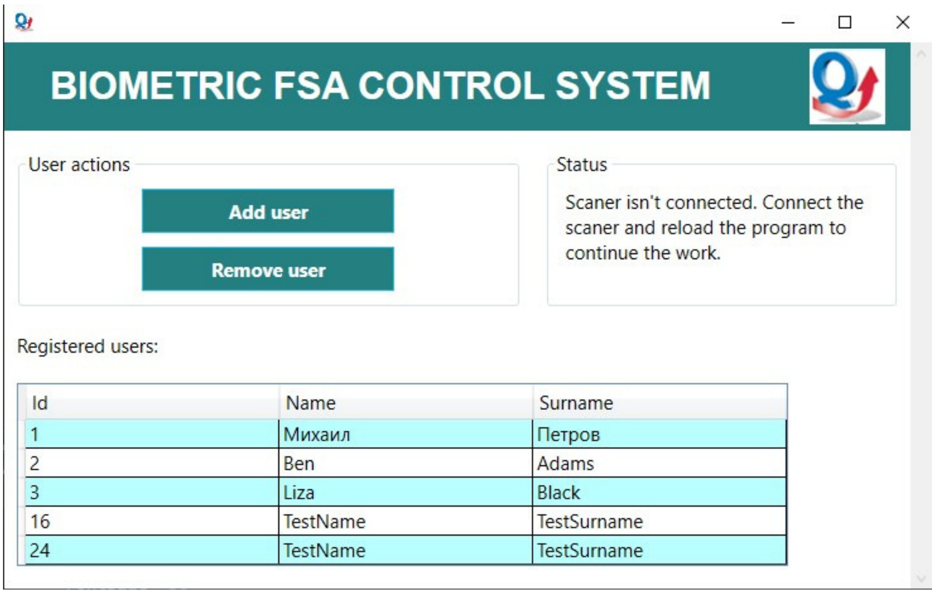


Figure 5. Appearance of the Arduino Uno board

The Arduino Uno is a device based on the ATmega328 microcontroller. The Arduino Uno can be powered by USB or an external power source - the source type is selected automatically. An external AC power source (NOT USB) may use an AC/DC network adapter or a battery / battery.

11. Sample software

Because the system administrator must have access to the activity database of all users and analyze this information, a special application software was developed using WPF .NET. In addition to the standard features to get the information you need from the database, it also has the ability to connect a fingerprint scanner through a data exchange device to simulate basic operations: adding a fingerprint and authentication [11].



Scaner isn't connected. Connect the scaner and reload the program to continue the work.

Id	Name	Surname
1	Михаил	Петров
2	Ben	Adams
3	Liza	Black
16	TestName	TestSurname
24	TestName	TestSurname

Figure 6. The main program window

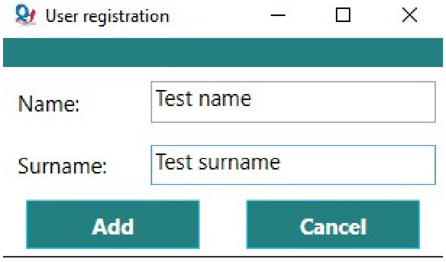
There are several logical sections in the main window:

- Work with users: operations to add a user to the database and remove the user from the database;

- System status;

- Registered users spreadsheet for downloading data for all users (Figure 6).

Tap on the Add User button will display another window where you can enter your first and last name (Figure 7):


User registration

Name: Test name

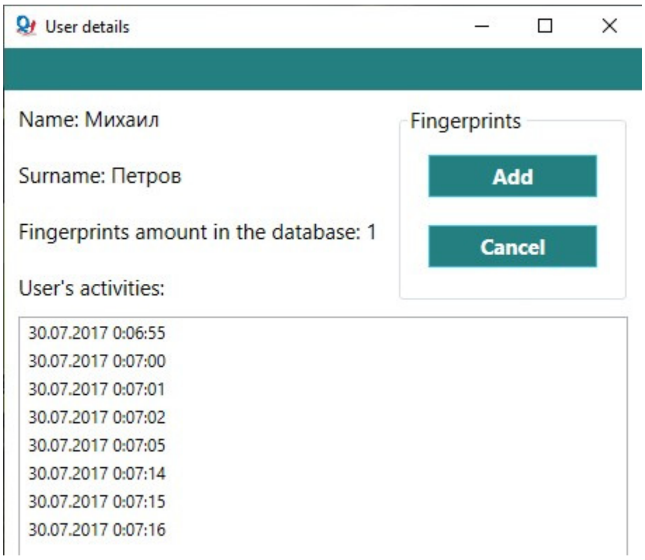
Surname: Test surname

Figure 7. User registration form

After entering all the data, the system will ask the user to put their finger on the scanner, will try to save the fingerprint in the scanner storage and in the activity database. If successful, the user will receive a corresponding standard message. In case of failure - also.

Double tap on a row in the user table will bring up another window with details about the user. The administrator will be able to see the name, last name, number of prints in the database and a list of its activity over all time (Fig. 8).

Also, the same window gives the user the ability to add another fingerprint or remove the extra one. Tap on these buttons will also display a standard message asking the user to attach a finger to the scanner. The transaction will then be transmitted and the results will be reported.


User details

Name: Михаил

Surname: Петров

Fingerprints amount in the database: 1

User's activities:

30.07.2017 0:06:55
30.07.2017 0:07:00
30.07.2017 0:07:01
30.07.2017 0:07:02
30.07.2017 0:07:05
30.07.2017 0:07:14
30.07.2017 0:07:15
30.07.2017 0:07:16

Figure 8. Details window for individual user

12. User activity database

A free version of Microsoft SQL Server 2016 was selected as the DBMS for creating, maintaining, and operating the database.

Microsoft SQL Server is a relational database management system (DBMS) developed by Microsoft. The main query language used is Transact-SQL, created jointly by Microsoft and Sybase. Transact-SQL is an implementation of the ANSI / ISO standard Structured Query Language (SQL) extension. Used to work with databases ranging from personal to large enterprise-wide databases (Figure 9)[4].

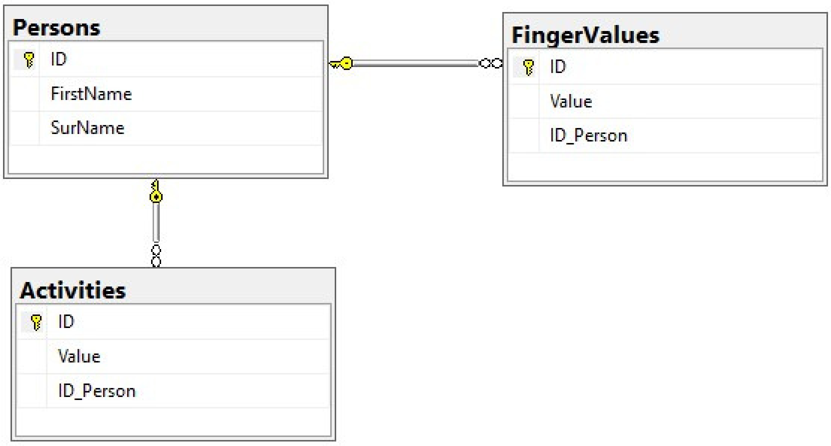


Figure 9. Diagram of the user database

The database consists of three relationships: Persons, Activities, FingerValues.

All relationships must have ID attributes that represent the primary key to uniquely identify each tuple within the corresponding relationship.

The Persons relationship must have FirstName, SurName attributes, which store information about the User's First and Last Name.

The FingerValues relationship has an ID_Person attribute for organizing one to many Persons relationships and a Value attribute for storing fingerprint information. This information is consistent with the fingerprint scanner repository.

The Activities relationship has an ID_Person attribute for organizing a one-to-many relationship with Persons and a Value attribute for storing the date and time of the user's activity, such as the date and time when the user was authenticated.

The database is in its third normal form, so it is securely protected from anomalies with data such as anomalies when adding, modifying, and deleting data. If you need to store additional user information, the database can be easily expanded by adding new relationships or adding new attributes to existing relationships. Expanding the database will not cause anomalies with the data.

13. Conclusion

As a result of this work, the optimal model of the scanner model, which works in identification mode, was selected for use in the demonstration model.

1. A system outline has been developed which, in addition to providing normal authentication, stores information about the activity of system users.

2. A microcontroller was programmed to connect the fingerprint scanner to this system.

3. A software product was created to monitor user activity using NET WPF technology.

4. A relational data repository has been created to store the required user information and is hosted on the MS SQL SERVER server.

The system created is quite flexible: if necessary, any server can be selected to maintain the database; the monitoring terminal can be created as a mobile or WEB service; any scanner that is best suited to the specific situation can be selected. Thus, the system created can meet the needs of a large number of diverse customers, both firms and organizations, and individuals.

REFERENCES

1. MAILIS N.P. Fingerprinting: Textbook. - M. Publishing house "Shield-M", 2008.
2. BLOOM J. Learning Arduino: tools and methods of technical magic: Per. from English — SPb.: BHV-Petersburg, 2015.
3. EVSTIFEEV A.V. Microcontrollers AVR family Mega. User's manual. - M .: Dodeka-XXI Publishing House, 2007. Pages: silt (Series "Programmable Systems").
4. Microsoft SQL Server: [Electronic resource] www/URL: *https://uk.wikipedia.org/wiki/Microsoft_SQL_Server.*
5. VELICHKO O.M., KOLOMIЄTS L.V., GORDINKO T.B. Metrology, technical regulation and secure care. Volume 5: Recording of statistical methods. Pidruchnik. - Odesa: WWII, 2014.
6. Arduino Uno: [Electronic resource] www/URL: http://arduino.ua/ru/hardware/Uno.
7. Fingerprint scanners. Classification and implementation methods: [Electronic resource] www/ URL: *https://geektimes.ru/post/116458.*
8. What are and how do fingerprint scanners work: [Electronic resource] www/ URL: *http://china-review.com.ua/6339-vse-chto-nuzhno-znat-o-skanerah-otpechatkov-palcev.html*
9. Modern biometric identification methods: [Electronic resource] www/URL: *https://habrahabr.ru/post/126144.*
10. Biometric identification: technology reliability: [Electronic resource] www/URL: *https://habrahabr.ru/post/86530.*
11. Fingerprint Sensor and Arduino: [Electronic resource] www/URL: *http://arduino-diy.com/arduino-datchik-otpechatka-paltsa.*
12. Adafruit Optical Fingerprint Sensor: [Electronic resource] www/URL: *https://cdn-learn.adafruit.com/downloads/pdf/adafruit-optical-fingerprint-sensor.pdf.*