Review of modern biometric user authentication and their development prospects

Z V Boriev¹, S S Sokolov² and A P Nyrkov³

¹ Admiral Makarov State University of Maritime and Inland Shipping, Dvinskaya st. 5/7, St. Petersburg, Russia, 198035
² Admiral Makarov State University of Maritime and Inland Shipping, Dvinskaya st. 5/7, St. Petersburg, Russia, 198035
³ Admiral Makarov State University of Maritime and Inland Shipping, Dvinskaya st. 5/7, St. Petersburg, Russia, 198035

Abstract. This article discusses the possibility of using biometric information technologies in management. Made a brief overview of access control and time attendance. Analyzed biometrics and identification system user. Recommendations on the use of various systems depending on the specific tasks.

Introduction

The use of biometric identification systems these days is becoming more urgent. However, as the reality shows, traditional methods of personal identification and authorization based on the use of passwords or physical media (in the form of pass, passport, driving license, electronic keys and cards), do not meet modern requirements for reliability in the determination of the individual. The password can be forgotten or intercept material carrier - to copy, lose or give to another person. Especially it does not allow the traditional access control systems to ensure an adequate level of reliability. As a result, companies are looking for more efficient ways of ensuring security. One way to solve this problem is to move to biometric identification systems. [1]

1. Information and Control Systems

Effective management requires constant monitoring and planning of all processes in the organization. Planning work is carried out taking into account the fact that it is followed by the monitoring function. A control need timely, accurate information, effective with respect to the cost to develop it. To implement these requirements necessary information management system.

Management Information System (MIS) - a set of hardware and software that allows the company management to obtain timely information necessary for effective decision making.

Daily administration of the enterprise is faced with the decision of questions about payroll, time tracking, providing access to certain resources staff, whose number is constantly changing. By itself, the automation of management processes in the company is not a big problem. These difficulties arise due to the fact that the components of any organization are constantly changing, upgraded or even deleted. Changing environment, changes the structure, process technologies modernized enterprise. If the administration of the organization will be deprived of the opportunity to react promptly to these changes, the consequences for the enterprise can take a serious nature. [2]
2. Access control.

Access control systems (ACS) - an essential component of information management system of any business or office building. ACS is a very complex hardware-software system that is responsible for the registration and restriction of entry and exit of people and vehicles in a certain area through check points (gates, doors). The main objectives of the ACS is to determine the time of admission to the territory and for the identification of objects that are eligible for admission. In addition, the access control system can perform a range of additional features, which include:

- keeping records of working time;
- Conduct payroll employees (if possible integration with the accounting system);
- maintaining a database of visitors and employees.

In any ACS has a email id (key), which is used to determine the rights of the person who owns them. As a key in Access control can be used: barcode, magnetic or smart (smart cards) Plastic cards; "Electronic tablets» (Touch Memory); Wiegand cards; card remote reading (proximity); PIN-code. Moreover, the identifier may be used as the biometric parameters of the person.

"Electronic tablets» (Touch Memory) chip are arranged in a sturdy metal case. The code information recorded in the memory of the circuit. To identify the need to attach the tablet to the reader. Reading Speed - 0.1. Some models allow you to enter information about the user. The advantages are compactness, high resistance to mechanical damage, corrosion, temperature extremes and low cost (comparable to the cost of magnetic stripe cards).

Card with a bar code is a plate coated with a black stripe (strokes). Code information contained in the variable stroke width and the distance between them. Code of the card is read by the optical reader. On a magnetic card code information is recorded on the magnetic strip. The bar code can simply dirty mud. Magnetic card is easily damaged in daily use.

Perforated card is a plate (plastic or metal). The code information is applied to a perforated card as the holes arranged in a specific order. Code card is read by mechanical or optical readers.

Code information on the Wiegand card contains a certain way on the thin metal wires arranged, glued with special glue. Information from the card is read by electromagnetic reader.

Proximity technologies have many advantages - much greater than with other methods of identification reliability and durability, lack of power (in passive cards). Proximity reader constantly sends a radio signal. Map in contact with the zone of the reader takes it in response to radiation and sends a signal containing recorded on a chip code. The distance between the reader and the card depends on the power of the reader varies from 5 cm to several meters. The lack of mechanical contact during operation allows for an arbitrary form identifiers, the identifier can be implanted into the object identification. The advantages are the complexity of forgery, the possibility of using encryption algorithms.

Smart card ("smart card") is a plastic card has an embedded microcontroller with all its attributes (processor, RAM, nonvolatile memory with a file system tools to input additional coprocessors). The main advantages of smart cards - a large memory capacity and high security information from trying to modify and duplication. Drawback - the high cost. Is the standard equipment of appropriate automated systems can be simply implemented in any arbitrary system.

PIN-code. Carrier code information is the memory of man. User independently from the keyboard code and it gives the signal for the end device. [3]

3. Biometric identification systems. Legislative regulation

In the Russian Federation in the field of protection of human subjects of personal data biometric data given special attention. Article 11 of the Federal Law "On Personal Data" gives the following definition of biometric data - a "data that characterize the physiological and biological characteristics of the person on the basis of which it is possible to establish his identity (biometric personal data) and are used by the operator to identify the subject of personal data can be processed only with the consent in writing of the subject of personal data, except as specified in paragraph 2 of this Article. "

[3]
Part 2 of Article 11 of the Federal Law "On Personal Data" states that the processing of biometric personal data can be carried out without the consent of the subject of personal data in connection with the implementation of international treaties of the Russian Federation on readmission, in connection with the administration of justice and all that is connected with it.

By passing this law provides specific requirements for material media biometric personal data and storage technologies such data is personal data information systems.

Material carrier must provide:
• protection against unauthorized re-entry and additional information after its removal from the information system of personal data;
• access to recorded material carrier on biometric personal data carried out by the operator and persons authorized in accordance with the legislation of the Russian Federation to work with biometric PD;
• the ability to identify personal data information system, which was implemented biometric record of PD, as well as the operator, to carry out such a record;
• preventing unauthorized access to biometric personal data contained in a tangible medium.

The operator of biometric data used is personal data information systems, must:
• maintain records of the number of copies of material carriers;
• Provide appropriate material carrier of a unique identification number that allows the operator to accurately determine, to record biometric personal data on the material carrier.

4. Biometric identification systems. Hardware and software
Biometric identification systems are most effective because they cannot recognize the physical media, and the unique physical characteristics of a human. Access and protection of information, based on such technologies are not only the most reliable but also the most user-friendly to date. All biometric devices have specific requirements for hardware and software. In any system user identification must first be registered. Many biometric systems allow users to do it themselves.

Biometric Access control, allow to organize an efficient, reliable and cost-effective system of access control. The use of biometric technology avoids problems such as loss, re-release and transfer to third parties badges.

Timesheet is no less important issue for the management of the companies. Time tracking system supplies reporting data corresponding to the time of arrival and departure at the workplace staffing, delays in the workplace, processing and defects. The presence of such information allows, in turn, greater flexibility to manage the distribution of wages, bonuses, penalties, increases discipline in the enterprise and, of course, translates into economic benefits. Importantly, the time tracking system constructed on the basis of biometric identification allows, compared to conventional systems, to eliminate instances of intentional abnormality associated with the lack binding - e.g., the magnetic card to a specific person, whereby the card can easily be transferred from one person to another.

Identify several ways of accessing the necessary resources:
1. The verification based on biometrics and unique identifier that identifies a particular person (eg, ID number), ie, This method is based on a combination of identification and authentication techniques.
2. Authentication, which in turn is based only on the biometric measurements. The measured parameters are compared with all entries from the database of registered users, rather than one of them selected on the basis of that ID. [4]

Generally, both methods are used equally. Select the Authentication method is carried out directly on the basis of security requirements, as well as funds allocated for these purposes. But the reliability of access depends not only on the way of authentication. An important factor in this regard is the same biometric selection parameters based on which will be accessed.

5. Biometric parameters
There are a number of biometric parameters, on which the identification and authentication of identity. These include:
Every year there are more biometric parameters, which can identify and authenticate identity. But to study them, and find ways of processing algorithms takes a lot of time and money. Therefore, the degree of scrutiny of biometric parameter directly affects the extent of its use.

The most-used options today is the fingerprint. This is due to the fact that fingerprinting got its spread in the late 19th and early 20th century. The cost of fingerprint scanners every day more and more reduced, and the number of additional parameters, such as temperature finger pressing force and the like, increases. We can say that in the near future by the scanner manufacturer reached the limit of opportunities in this area.

The most statistically robust and resistant to forgery access parameters are iris and veins in the arms. But the process of collecting and processing parameters such takes a bit longer than the processing of fingerprint or face shape. Reliability indices are such features as false rejection and false access access. Biometric data for a false denial of access tends to 0%, and a false access does not exceed 1-2%. [7]

Despite all the differences between the biometric parameters, as the basic characteristics of biometric systems was made to use the False Acceptance Rate (FAR) and False Rejection Rate (FRR). Obviously, the smaller these ratios, the stronger or the other option. These factors help to decide whether to use a particular method of identification and authentication, depending on the task.

Table 1 shows the average values for the various biometric systems:

|                | Fingerprint | Geometry face | Iris     |
|----------------|-------------|---------------|----------|
| FAR, %         | 0.001 %     | 0.1 %         | 0.00001 %|
| FRR, %         | 0.8 %       | 7 %           | 0.10 %   |

6. Structure of biometric systems of access control

In the majority of ACS and the system of working hours are networked distributed systems with the access rights of users who need to build, open to integration with other manufacturers' equipment. At the points of passage set by the controller connected to the control PC or server via USB or LAN Ethernet.

User registration is performed using special software. To register a fingerprint reader applies a control that connects via the USB port of a personal computer. Users can also register independently at the terminals of the system using specific procedures.
As seen in figure 1, the ACS has a modular structure. This allows the system to be scalable and more stable. In the event of failure of one of the elements, the system continues to work, of course, in limited functionality mode. Software in most cases consists of two modules "working time control system" and "access control system". Time tracking system works with personnel shifts, schedules, events, or obtained automatically entered in manual mode allows you to build reports. Access control program is responsible for connecting and configuring devices, setting the rights of passage and time zones, synchronization of data between the database and terminals.

7. Comparative evaluation of biometric systems.

Select several empirical characteristics for assessing the quality of the system:

1. Resistance to forgery.
2. Stability of Environment - characteristic estimating system stability under various environmental conditions, such as changing the lighting or room temperature.
3. Ease of use - shows how difficult it is to use a biometric scanner whether it is possible to identify "on the fly".
4. The speed of the
5. The cost of the system

Below is a comparative evaluation of biometric systems for the ten-point scale.

|                  | Resistance to forgery | Resistance to environment | Ease of use | Speed | Cost | Stability characteristic cost Time |
|------------------|-----------------------|---------------------------|------------|-------|-----|-----------------------------------|
| Iris             | 10                    | 9                         | 8          | 7     | 10  | 10                                |
| Fingerprinting   | 6                     | 10                        | 9          | 10    | 10  | 9                                 |
| 2D face          | 4                     | 6                         | 6          | 10    | 10  | 8                                 |
| 3D face          | 9                     | 8                         | 10         | 5     | 7   | 10                                |
| An arm vein      | 10                    | 7                         | 9          | 7     | 8   | 7                                 |
| Retina           | 10                    | 10                        | 6          | 3     | 6   | 9                                 |

It can be concluded that the resistance to forgery or that the biometric parameter is inversely proportional to the speed of its processing by the system.
Summary
Opting for the use of a parameter when accessing or working hours accounting depends on the system requirements. The most statistically robust and resistant to forgery access systems are the systems of admission iris and veins hands. The least expensive and easiest to use, but having good statistics are of tolerance on one hand. Tolerance on 2D face is convenient and cheap, but it has a limited range of applications due to poor statistics.

In addition to combining the use of biometrics, it is possible to combine the parts of the body from which the parameters are removed. Since Iris can increase the accuracy of the system is almost quadratic, lossless time if complicate the system, making it two eyes. For fingerprint method - by combining several fingers, and recognition of the veins, by combining the two hands, but in this case, the improvement is only possible by increasing the time of human interaction with extractors.

Summarizing the results of the methods that can be said that for medium and large objects as well as objects with maximum safety requirement should be used as an iris biometric access and possibly recognize hand veins. For objects with the number of staff to several hundred people will be optimal access fingerprint. Recognition system for 2D face image is very specific. They may be required in cases where the detection requires the absence of physical contact, but to put the system on the iris control is not possible. For example, if authentication is required for a person without his participation, hidden camera, camera or external detection, but this is only possible with a small number of subjects in the database and a small stream of people shoot camera.

References
[1] Boreyscho A A Biometrics and software features of modern ACS J Security of Business Information 59 (2005) 40-43
[2] Aleshin A P Maintenance business security Dashkov & Co Moscow 2008
[3] Balle R M Pankanti S Ratha N K Senior A W Guide to Biometrics Springer Science+Business Media New York 2004
[4] Information on http://habrahabr.ru/post/126144/
[5] Kharitonov A V Overview of biometric identification methods J Cybernetics and programming 2 (2013) 12-19
[6] Korobeynikov A G Gatchin Y A Application for Determination of Mail Document Spam Level World Applied Sciences Journal 30 (2014) 165-169
[7] Chernyi S Zhilenkov A Sokolov S Titov I Self-contained drilling rig automatic control system efficiency improvement by means of assuring compatibility and integration methods development Metallurgical and Mining Industry 2015 No 3 P 66-73