Application of face recognition technologies in access control and management systems

A N Marenkov, T M Gelagaev, V Yu Kuznetsova
Astrakhan State University, Astrakhan, Tatischeva str., 20A, 414056, Russia

E-mail: arhelia@bk.ru

Abstract. The article shows the relevance of the widespread use of computer vision technology on the example of face recognition as part of the access control and management system. The scheme of access control implementation with face recognition technology is described. The use of this technology makes it possible to increase the level of information security of enterprises and, as a consequence, reduce the possible financial damage from the implementation of attacks on their assets from illegitimate penetration into the protected area through the access control system using passes of legal users.

Keywords: security; access control and management system; face recognition; neural networks; safety.

1. Introduction
The use of computer vision in the field of security provides a huge impetus for the improvement of access control systems (ACS). Representatives of medium and large businesses that use access control systems at their facilities provide information that every fiftieth passage through the turnstile is carried out in violation of security requirements - to enter the territory with limited access, cards of legal users or fake access cards are used. Face recognition technologies are systematically introduced into many technological processes, including security systems. ACS with the use of face recognition technology helps to detect situations when an attacker uses a legal user's card for passage, by comparing the face of the cardholder from the organization's database with the portrait of the one who is trying to enter the protected area. Improving the access control system in this way will increase the level of information security of enterprises and, as a result, reduce the possible financial damage from the implementation of attacks on their assets. In addition, contactless identification of users by recognizing their faces is relevant in an unfavorable epidemiological situation.

2. The principle of operation of a classic ACS
The access control and management system is one of the most popular and effective systems for protecting areas with limited access. ACS restricts the passage to the protected area, while not interfering in any way in the business processes of the organization. In addition, the system monitors the movements of employees within the organization and records their hours worked, which contributes to violations of the work schedule.

Main functions:
• restriction of access to the premises of the protected object;
• keeping time records of working hours for each employee;
• fixing the time of arrival and departure of visitors;
• personal and temporary control over the opening of internal premises;
• control over the movement of employees around the facility;
• registration and notification of cases of attempts to enter the protected premises;
• integration and interaction between video monitoring and security and fire alarm systems.

The classic principle of ACS operation is as follows: it is an access system based on key cards with RFID tags.

The abbreviation RFID is derived from the term Radio Frequency Identification, which means radio frequency identification in Russian. An RFID tag consists of three components:
• a chip that stores identification information and is responsible for communication with the reader;
• Antenna that allows information to be transmitted between the tag and the reader;
• shell or body.

![Figure 1. The classic scheme of access control at the enterprise](image)

Currently, RFID systems can be found absolutely everywhere, starting with public transport (paying for travel by means of a card tied to a user's account), staying at a hotel (a smart card is a key to enter the room), ending with a foreign passport (new generation), which can be obtained with an electronic contactless RFID chip [3].

Practice shows that this type of access control has a number of disadvantages that can provoke vulnerabilities associated with unauthorized access to the information resources of the protected object. The most striking example of such a drawback is the use of someone else's cards to enter a protected area, for example, this is possible if an employee has forgotten the card of the house and asked his colleague to “lend” him a card for the passage, or, worse, an attacker used a lost or stolen card to pass through.

Also, a significant problem for ACS is the widespread cloning of keys and access cards. In the press and on ad sites, you can often see information about services for cloning access keys for anyone, for example, door phone users often turn to such a service. However, the use of such keys in an access control system significantly reduces the effectiveness of ensuring security in an organization. Many access control systems do not prevent the simultaneous use of several identical keys or access cards. The cloned key not only allows access to the enterprise but also opens all internal doors that were allowed for the authentic key.

Most often, this problem is solved by installing biometric scanners (fingerprints, retina, etc.), however, in an unfavorable epidemiological situation, these systems are becoming less in demand. At the same time, contactless fingerprint reading systems show poor performance. According to a report by the American National Institute of Standards and Technology (NIST), the accuracy of contactless devices when recognizing one finger was relatively low - only 60-70%.


3. Face recognition for security purposes

Face recognition is one of the most promising methods of biometric contactless identification of a person by face. According to analysts from Future Market Insights, the global market for contactless biometric technologies will grow at an average annual rate of 17.4% from 2020 to 2030 and will reach $70 billion by 2030. It is expected that contactless technology will be more in demand due to the coronavirus pandemic in the world and surface hygiene problems such as contact fingerprint scanners [4].

Face recognition is the process of matching the facial images of people caught in the camera lens with photographs from a database of previously saved facial images of reference standards, for example, employees of an organization. According to the structural implementation of the face recognition system, there are 3 schemes:

- **Analysis of the video stream on the server** - the IP camera sends the entire video stream to the server for processing and analysis. On the server, specialized software searches for a face in the video sequence and compares the images of faces obtained from the video stream with the base of reference faces.

  The disadvantages of such a scheme will be high network load, high cost of the server, even the most powerful server can be connected to a limited number of IP cameras, i.e. the larger the system, the more servers. The advantage is the ability to use an existing video surveillance system.

- **Analysis of the video stream on the IP camera** - the images will be produced on the camera itself, and the processed metadata will be transmitted to the server.

  Disadvantages - special cameras are needed, the choice of which is extremely small at the moment, the cost of cameras is higher than that of conventional ones. Also, in systems of different manufacturers, the issue of storage and size of the database of recognized faces of standards will be solved in different ways, as well as issues of interaction between the software on the camera and software on the server.

  Advantages - connection of an almost unlimited number of cameras to one server.

- **Analysis of the video stream on the access control device** - the camera is built into the access control device, which, in addition to face recognition, which occurs on the device, performs the functions of access control, usually through a turnstile or an electric lock installed on the door. The database of reference faces is stored on the device, and usually no longer in the form of photographic images.

  Disadvantages - as a rule, all such devices are produced for indoor use. Advantages - Low cost of systems compared to video surveillance systems used for face recognition.

  As a rule, all the proposed methods of face recognition are mainly implemented using 2D images, since Despite the development of three-dimensional models, the base of such standards is still rather scarce, and the equipment for organizing this kind of recognition is expensive.

Analysis of face recognition approaches. Despite the variety of existing approaches, it is possible to define a general algorithm for face recognition.

The main stage of the described process is the face recognition itself, which is ensured by calculating features and identifying the similarity or dissimilarity of photographs. Let's consider several methods that can be applied in the face recognition algorithm.

**Flexible comparison method on graphs.** The essence of this method is reduced to graph matching. Faces are represented as graphs with weighted vertices and edges. At the stage of recognition, one of the graphs - the reference one - remains unchanged, while the other changes in order to best fit the first. In such recognition systems, graphs can represent both a rectangular lattice and a structure formed by characteristic (anthropometric) points of the face. The difference (distance) between two graphs is calculated using a certain price deformation function that takes into account both the difference between the values of the features calculated at the vertices and the degree of deformation of the edges of the graph [5].

**Neural networks.** Currently, there are about a dozen types of neural networks (NN). Neural networks are trained using a set of training examples. The essence of training comes down to adjusting the weights of intraneuronal connections in the process of solving an optimization problem using the gradient descent method. In the process of learning the neural network, key features are automatically extracted, their importance is determined and relationships between them are built. It is assumed that a trained NN will be able to apply the experience gained in the learning process to unknown images due to
generalizing abilities. The best results in the field of face recognition (according to the results of the analysis of publications) were shown by the convolutional neural network [7].

Hidden Markov models. One of the statistical methods of face recognition is hidden Markov models (HMM) with discrete time. HMM uses the statistical properties of signals and takes into account their spatial characteristics directly. The elements of the model are a set of hidden states, a set of observed states, a matrix of transition probabilities, an initial probability of states. Each has its own Markov model. When recognizing an object, the Markov models generated for a given base of objects are checked and the maximum observable probability is sought that the sequence of observations for a given object is generated by the corresponding model.

4. Prototype development
In the developed prototype, it is proposed to use a neural network, which will be trained with a teacher. The neural network will be trained on two images, where the result of comparison will be true or false (the person in the photographs is the same person or not). In addition, face recognition can be carried out using standard libraries [9].

The teacher creates a dataset containing at least two photographs of one person from many others [9].

Reasons for choosing this approach:
• the neural network is retrainable;
• the neural network can be "retrained" by adding new data sets;
• a trained neural network gives quick answers (within the framework of the problem being solved "similar / not similar");
• you can always increase or decrease the similarity threshold.

The following structure of an ACS prototype with face recognition technology is proposed:
• Arduino Mega to control RFID readers and turnstiles;
• RFID readers;
• IP cameras for capturing images;
• a computer with the ACS application installed;
• server with database.

Arduino Mega. Arduino electronic devices have long established themselves in the programmable electrical engineering market as a high-quality, multifunctional and inexpensive product. Therefore, in this project, this electronic device of the Mega model will be used, which in turn has 256 KB of flash memory and 8 KB of RAM in its arsenal.

RFID reader. These readers are needed to read UID (User identifier) from smart cards.

IP camera. For better system operation, you will need IP cameras with certain characteristics:
1. The presence of WDR (Wide Dynamic Range) - this parameter that affects the illumination.
2. The number of frames per second - the more frames per second the camera takes, the higher the probability that the camera will take the desired picture. This task requires a minimum of 20 frames per second.
3. Resolution of the video surveillance camera - higher resolution will provide higher detail. High resolution will have a positive effect on the process of identifying markers by the neural network in the resulting image.
4. Varifocal lens - a lens where it is possible to change the focal length.

A computer. Minimum requirements for the normal operation of the ACS application:
• processor 2 cores, frequency 1.1 GHz;
• Windows 7 and newer;
• RAM 2 GB;
• installed .NET Framework 4.8;
• 150 MB of free space.

Server with a database. The server must have SMSS from Microsoft installed.

The conceptual model of the ACS operation is shown in Figure 2.
Figure 2. Conceptual scheme of ACS operation

5. The scenario of using ACS with face recognition technology
The owner of the smart card must bring the smart card to the reader. The reader receives the UID of the presented card and sends it (the UID of the smart card) to the Arduino electronic device. The Arduino, in turn, sends the UID of the read smart card and the ID of the reader from which the UID was received to the computer (with the ACS application installed) via the COM port. On the computer, the ACS application sends a request to the database in order to check the presence of this smart card in the database, if the UID of the smart card does not exist, then we have an attacker. When a card is detected, an image bound to the UID of the read smart card is unloaded from the database. The ACS application analyzes the coincidence of the face image obtained from the database with the image obtained from the IP camera. If the probability of a match is below a certain predetermined threshold, it means that we are facing an attacker and the system will deny him access. If the probability of image coincidence is higher than the threshold value, the ACS application will send the turnstile ID and the “open” command to the Arduino electronic device, and the Arduino, in turn, will send the “open” command to the required turnstile.

The block diagram of the proposed solution is shown in Figure 3.

Figure 3. Flowchart of the process
6. Conclusion

- Face recognition technologies are systematically introduced into many technological processes, including security systems. ACS with the use of face recognition technology helps to detect situations when an attacker uses a legal user's card for passage by comparing the face of the cardholder from the organization's database with the image of a person trying to enter the protected area.
- The paper proposes a general scheme of the access control and management process using face recognition technology and demonstrates a conceptual diagram of the proposed hardware solution.
- Improving the access control system will improve the level of information security of enterprises and, as a result, reduce the possible financial damage from attacks on their assets.
- Contactless identification of users by recognizing their faces is relevant in an unfavorable epidemiological situation.
- Potential users of this system can be both government and commercial organizations interested in ensuring the confidentiality regime on their own territory.

References

[1] Vorozheikin M R, Chernova S V 2019 General information about the face recognition system (Publishing house “Sputnik +” № 47) p 35-37.
[2] Rudinskaya E A, Paringer R A 2019 Development of a face detection algorithm using combinations of Haar cascades (Proceedings of ITNT-2019 Publishing house: Novaya tekhnika) p 6-12.
[3] RFID tags - the ultimate guide to choose [site]: URL: https://securityrussia.com/blog/rfid-metki.html
[4] Site of the news service "Kiosksoft" [site] URL: https://kiosksoft.ru/news/2020/05/28/tochnost-beskontaktnoj-identifikacii-otpetchatkov-palcev-poka-ostaetsya-nizkoj-71797
[5] Vlasenko A V, Dzoban P I, Zhuk R V 2020 Overview of machine learning tools and their use in the field of cyber security (Caspian Journal: Management and High Technologies №1) p 144-155.
[6] Marenkov A N, Prikhodko A A, Kuznetsova E O 2019 Intelligent video surveillance systems: problems and functionality (Problems of increasing the efficiency of scientific work in the military-industrial complex of Russia, 2nd All-Russian scientific practical conference)
[7] Marenkov A N, Demin K S 2020 Methods for recognizing human movements using technologies of neural networks (Mathematical methods in engineering and technology – MMTT).
[8] Viola P, Jones M J 2004 Robust real_time face detection (International Journal of Computer Vision vol. 57, № 2) pp. 137-154.
[9] Bradski G, Kaebler A 2008 Learning OpenCV (Published by O'Reilly Media), p 495-512.
[10] Adelson E H and Bergen J R 1986 The Extraction of Spatio-Temporal Energy in Human and Machine Vision (Proceedings of Workshop on Motion: Representation and Analysis) p. 151-155.