

# Conceptual model of the face recognition process based on the image of the face and iris of personnel of critical infrastructure facilities\*

Sergey Bushuyev<sup>1,†</sup>, Ihor Tereikovskiy<sup>2,†</sup>, Oleksandr Korchenko<sup>3</sup>, Ivan Dychka<sup>2</sup>, Liudmyla Tereikovska<sup>1</sup> and Oleh Tereikovskiy<sup>3</sup>

<sup>1</sup> Kyiv National University of Construction and Architecture, Kyiv, Ukraine

<sup>2</sup> National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

<sup>3</sup> National Aviation University, Kyiv, Ukraine

## Abstract

Today's challenges determine the need to improve the biometric authentication of personnel of critical infrastructure facilities. Common means of biometric authentication, which are usually based on the use of neural network technologies for facial image analysis, need improvement in the direction of adaptation to the conditions of recognition during the performance by personnel of their functional duties, which are characterized by the influence of interference during video recording and an increase in the probability attacks using dummies. Another area of improvement is determined by the availability of video recording tools, which provide the ability to recognize a person by the iris of the eye and the ability to recognize emotions. It is shown that the first stage of improvement of neural network means of biometric authentication is the development of a formalized description of the recognition process, which takes into account promising areas of improvement. A conceptual model containing a formalized description and criteria for evaluating the effectiveness of the recognition process is proposed. At the same time, for the first time, an approach to determining the parameters of obstacles was proposed, which involves comparing the parameters of obstacles with the location and number of key and control faces that they overlap. Recognition of attacks is proposed to be implemented based on the analysis of the dynamics of basic emotions, the dynamics of eye movement parameters and the environment. The results of this study are important in the context of the development of effective biometric authentication tools, as they provide a formalized description of the requirements for the functional capabilities of the main components of the process of recognizing the identity and emotions of personnel of critical infrastructure facilities.

## Keywords

model, critical infrastructure, face image, iris, neural network, information security


---

Proceedings of the 5th International Workshop IT Project Management (ITPM 2024), May 22, 2024, Bratislava, Slovak Republic

\* Corresponding author.

† These authors contributed equally.

✉ sbushuyev@ukr.net (S. Bushuyev); terejkowski@ukr.net (I. Tereikovskiy); agkorchenko@gmail.com (O. Korchenko); dychka@pzks.fpm.kpi.ua (I. Dychka); tereikovskal@ukr.net (L. Tereikovska); tereikovskiyio@gmail.com (O. Tereikovskiy)

🏠  0000-0003-3412-1639 (S. Bushuyev); 0000-0002-5385-5761 (I. Tereikovskiy); 0000-0002-9421-8566 (O. Korchenko); 0000-0002-9421-8566 (I. Dychka); 0000-0002-9421-8566 (L. Tereikovska); 0000-0002-9421-8566 (O. Tereikovskiy)



© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

## 1. Introduction

In modern conditions, even minor security breaches of critical infrastructure facilities (CIF) can have a significant negative impact on the social and economic spheres of the state, as well as its defence capability and national security. One of the main requirements for a comprehensive information protection system of CIF is to ensure reliable identification and authentication of CIF personnel. For this purpose, a wide range of tools is used, including biometric authentication systems (BA) based on facial images (FI) and iris of the eye (IE) recognition [1, 26]. This is primarily explained by the widespread availability of high-quality video cameras capable of accurately capturing relevant biometric parameters, enabling sufficiently precise identification and authentication of personnel. However, the results [13, 15, 16] and practical experience indicate insufficient accuracy of such authentication systems in terms of face recognition under adverse conditions. Additionally, in modern conditions, for effective performance of duties, CIF personnel must be in a satisfactory psycho-emotional state, which can be monitored both during personnel access to the object and while performing official duties through the analysis of FI and IE. This explains the relevance of research aimed at enhancing CIF security through the development and implementation of BA systems that provide both facial recognition and assessment of the emotional state of personnel.

## 2. Literature Review and Problem Postulation

In the process of analysis of scientific and practical works devoted to the development of means of recognizing a person and the emotional state of a person, attention was focused on the identification of promising solutions that can be used to ensure the effective functioning of the BA systems of the CIF staff.

In [30], the use of MobileSSD technology is described for the selection of human faces in a video stream in real-time. The experiments were carried out under conditions of various obstacles, including the presence of glasses on the face, and the presence of foreign objects on the face that interfere with the fixation of characteristic points of the face. Also, the effectiveness of the technology was determined in different conditions of the lighting level, and the distance from the face to the camera. It was determined that turning the face most often leads to the impossibility of its selection.

In [16], the use of computer vision technologies to solve the problem of recognition of FI, eyes and PEO in real time is defined. It is proposed to use the Blob Analysis approach to identify FI, to use a threshold function for segmentation, and to use the Circle Hough approach to highlight the IE. It is declared that the use of these solutions allows achieving high recognition results on low-quality images.

In [29], the use of deep learning methods for recognizing human emotions based on FI is considered. Conduct recognition of 7 emotions. A previously trained Haar cascade classifier was used to distinguish the face, eyes, and mouth. A convolutional neural network (CNN) was used to recognize emotions, having previously trained it on the FER-2013 database. Claimed recognition accuracy of 0.62 on the test sample.

In [18], experimental studies were conducted to reveal the dependence of a person's recognition of an actor's emotion based on his facial expression on the presence of a mask on his face. It was found that the presence of a mask worsens the recognition of facial emotions by about 20%.

In [15], in addition to the effect of the presence of a mask, the effect of the presence of sunglasses on the recognition of an actor's emotion and his identification by face is also analyzed. It was found that, unlike the presence of a mask, the presence of sunglasses did not reduce the accuracy of emotion identification and recognition.

A study of the possibilities of such FI and ROO analysis systems as FaceReader from the Noldus Information Technology company, Captemo from the Logic Pursuits company and BioObserver from the Herta company was also conducted.

Although the results of the analysis of scientific and practical robots and known software and hardware solutions indicate the expediency of their application to CIF, these same results testify to the complication of the identification and authentication procedure for FI and IE under the influence of various interferences. It is also possible to conclude the most promising analysis of FI and IE with the help of neural network means (NN means). Another important direction of improvement of BA tools based on FI and IE is the need to increase the effectiveness of protection against attacks with the help of dummies [31, 9, 17].

At the same time, common means of recognizing such attacks are based on the analysis of the quality of the controlled image [4], the analysis of its spatial characteristics [23, 27], the verification of the dynamics of the parameters characteristic of the FI and IE of a living person [3, 5, 26] and the execution by the controlled person of certain commands that cause changing video registration parameters [10, 12]. At the same time, the same works noted the difficulties of effective analysis of the quality of FI and IE under variable conditions of video recording and the difficulty of determining spatial characteristics during video recording with one camera.

Also, the results of the conducted analysis indicate the absence of a formalized holistic description of the BA process of CIF personnel according to FI and IE, which takes into account the presence of typical problems, the possibility of attacks on the BA system with the help of dummies, the need to identify the identity and emotional state of the staff, and so on the mechanism for determining the effectiveness of the BA process.

The main purpose of this study is to develop a conceptual model that provides a formalized holistic description of the process of recognizing a person based on the image of the face and the iris of the eye during biometric authentication of personnel of critical infrastructure facilities using neural network tools, taking into account the need to identify emotions and detect attacks using dummies.

### **3. Conceptual model development**

Designing a conceptual model for face recognition incorporating both facial and iris recognition for critical infrastructure facilities involves several key components. Here's a proposed breakdown:

1. **Image Acquisition.** The process begins with capturing images of personnel using high-resolution cameras placed strategically at entry points or checkpoints within the facility. **Pre-processing.** Raw images undergo pre-processing to enhance quality

and remove noise. This step may involve techniques like normalization, resizing, and filtering to standardize the images.

2. Facial Recognition. Employ algorithms like Haar cascades or deep learning-based methods to locate faces within the images. Feature Extraction. Utilize techniques like Principal Component Analysis (PCA), Local Binary Patterns (LBP), or Convolutional Neural Networks (CNNs) to extract discriminative features from the detected faces. Matching. Compare the extracted features against a database of known personnel using methods such as Euclidean distance, cosine similarity, or deep metric learning.
3. Iris Recognition. Locate and isolate the iris region within the captured face images using techniques like Hough transforms or template matching. Feature Extraction. Extract unique features from the iris pattern using methods like Gabor filters or wavelet transforms. Matching. Compare the extracted iris features against a database of enrolled personnel using algorithms like Hamming distance or phase correlation.
4. Integration. Combine the results from facial and iris recognition modules to increase the overall accuracy and reliability of the identification process. Employ fusion techniques such as score-level fusion or decision-level fusion to integrate the outputs from individual recognition modules.
5. Decision Making. Based on the fused recognition scores, decide the identity of the personnel. Apply thresholding techniques to determine acceptance or rejection based on the similarity scores obtained from the recognition process.
6. Access Control. Grant or deny access to the personnel based on the decision made during the recognition process. Interface with the facility's access control system to activate/deactivate entry mechanisms like doors, turnstiles, or gates.
7. Feedback and Iteration. Provide feedback to the system based on the outcomes of recognition decisions to improve performance over time. Employ techniques such as adaptive learning or retraining of the recognition models using new data to enhance accuracy and robustness.

Also, when developing the conceptual model, the results of [22, 24, 27] were taken into account, which led to the use of the following terms:

- Neural network model - a model that describes the architecture of an artificial neural network and characterizes the neurons that are part of it.
- IE is a colored ring in the front part of the pupil, consisting of muscle and connective tissue and pigment cells, which changes the size of the pupil of the eye.
- FI - the image of the front part of the human head, which is bounded from above by the forehead, below by the lower edge of the chin, and from the sides by the base of the auricles.
- BA - authentication based on the results of the analysis of a person's biometric data.
- Attack using fakes (spoofing) – an attack based on providing a sensor to read fake biometric data.
- Emotion is a mental reflection in the form of a direct, biased experience of the vital meaning of phenomena and situations, determined by the relationship of their objective properties to the needs of the subject.
- Basic emotions - anger, disgust, sadness, fear, surprise, contempt, joy.

- Key points are points on the face that are used to recognize emotions.
- Control points – points on a person's head that are used to recognize a person.

This conceptual model forms the basis for implementing a comprehensive face recognition system incorporating both facial and iris recognition for securing critical infrastructure facilities.

Taking into account the specifics of the problem of developing NN means BA of CIF personnel, in the base case the proposed model is intended to describe the processes of neural network processing of the registered video stream to recognize the identity of CIF personnel and the presence of an attack using dummies on the BA system by FI and IE:

$$\langle \Theta, \mathbf{C} \rangle \xrightarrow{NR} \langle \mathbf{I}, \mathbf{E}, \mathbf{A} \rangle, \quad (1)$$

where  $\Theta$  is a set of parameters characterizing video recording conditions;  $\mathbf{C}$  is a set of parameters characterizing the content of each frame of the video stream;  $\mathbf{I}$  is a set of parameters describing the result of person recognition;  $\mathbf{E}$  is a set of parameters describing the result of emotion recognition;  $\mathbf{A}$  is the result of recognition of an attack using dummies;  $N, J, K$  – power of sets  $\mathbf{C}, \mathbf{I}, \mathbf{A}$ ;  $NR$  - neural network recognition operator.

Taking [2, 28] into account, it is accepted that the elements of the set  $\Theta$ , which characterize the conditions of video registration, include:  $\theta_1$  – the minimum permissible level of illumination without the use of infrared illumination;  $\theta_2$  – the maximum permissible level of illumination;  $\theta_3, \theta_4$  – viewing angles of the video camera horizontally and vertically;  $\theta_5$  – frame rate;  $\theta_6$  – color gamma format;  $\theta_7$  – video stream resolution;  $\theta_8$  – range of action of infrared illumination;  $\theta_9, \theta_{10}$  – the maximum possible angles of changing the direction of video recording horizontally and vertically when the video camera functions in the object tracking mode;  $\theta_{11}$  – illumination range in the visible range of light (white illumination);  $\theta_{12}$  – distance to the face;  $\theta_{13}, \theta_{14}, \theta_{15}$  – angles between the direction of video recording and the projection of the face onto the planes Oxy, Oxz, Oyz.

The general conditions for using a video surveillance system within one location are as follows:  $\theta_{16}$  – illumination;  $\theta_{17}$  – number of video cameras;  $\theta_{18}$  – the maximum possible number of monitoring objects;  $\theta_{19}$  – the presence of obstacles.

Based on the analysis of standard solutions in the field of video surveillance, it was determined that the parameter  $\theta_5$  can take values from 7 to 60 frames per second. The parameter  $\theta_6$  can be RGB, RGBA, BGR, monochrome or CMYK. The  $\theta_7$  parameter can take the following values: VGA (640x480 - 0.3 MP), HD (1280x720 - 1 MP, 1280x960 - 1.3 MP), FullHD (1920x1080 - 2 MP), UHD (4K-3840x2160 - 8 MP, 8K - 7680x4320 - 33 MP).).

In addition, video surveillance systems provide opportunities for: changing the spatial orientation of the video camera; changes in lighting; issuing commands to clarify the position of the face in space and eliminate obstacles. The corresponding parameters are marked as  $\theta_{20} - \theta_{23}$ . In addition, video surveillance systems provide opportunities for: changing the spatial orientation of the video camera; changes in lighting; issuing commands to clarify the position of the face in space and eliminate obstacles. The corresponding parameters are marked as ( $\theta_{24}$ ) and video data packet reception frequency ( $\theta_{25}$ ) are also taken into account.

Consider the set of parameters characterizing the content of each of the frames of the video stream, the parameters of which are displayed in the elements of the set  $\mathbf{C}$ . Since each of the frames of the video stream is essentially a static monochrome or color image, a separate element of the set  $\mathbf{C}$  can be represented as:

$$c_n = \begin{pmatrix} d_{1,1} & \dots & d_{1,X} \\ \dots & \dots & \dots \\ d_{Y,1} & \dots & d_{Y,X} \end{pmatrix} n = 1 \dots N, \quad (2)$$

where  $n$  is the  $n$ th frame;  $N$  is the number of frames of the video stream;  $X$  – horizontal frame size;  $Y$  is the vertical frame size;  $d_{x,y}$  is the color of the pixel with coordinates  $(x, y)$ .

When defining the set  $\mathbf{I}$ , it is taken into account that each of its elements  $i_j$  is interpreted as the confidence that the  $j$ -th representative of the CIF staff is recognized in the video stream. At the same time,  $0 \leq n_j \leq 1$ . Taking into account the need to determine that an illegitimate person should be recognized in the video stream and there may not be a human object at all, the number of elements  $\mathbf{I}$  is calculated as follows:

$$J = L + 2, \quad (3)$$

where  $L$  is the number of legitimate representatives of the CIF staff.

In the case where  $j$  lies in the range from 1 to  $L$ ,  $i_j$  represents the confidence that the  $j$ -th CIF personnel representative is recognized in the registered video stream. For  $j = L + 1$ ,  $n_j$  is the confidence that an illegitimate person is recognized in the registered video stream, and for  $j = L + 2$ ,  $n_j$  is the confidence that there are no people in the registered video stream.

The elements of the set  $\mathbf{E}$  describe the emotions of the CIF personnel representative, recognized based on the neural network analysis of the FI. Since in most authoritative works it is accepted that the set of basic emotions includes joy, anger, disgust, fear, sadness, surprise and neutrality, it is appropriate to describe the spectrum of basic emotions using seven parameters. Thus, each of the seven elements of  $\mathbf{E}$  ( $e_i \in \mathbf{E}, 0 \leq e_i \leq 1$ ) is correlated with the manifestation of a basic emotion on the face.

Thus, expressions (1-3) are an analytical representation of the basic variant of the face recognition model for the BA of CIF personnel according to FI and IE. In this case, the model does not reflect the information processing operations performed to determine  $\mathbf{I}$ ,  $\mathbf{E}$  and  $\mathbf{A}$ .

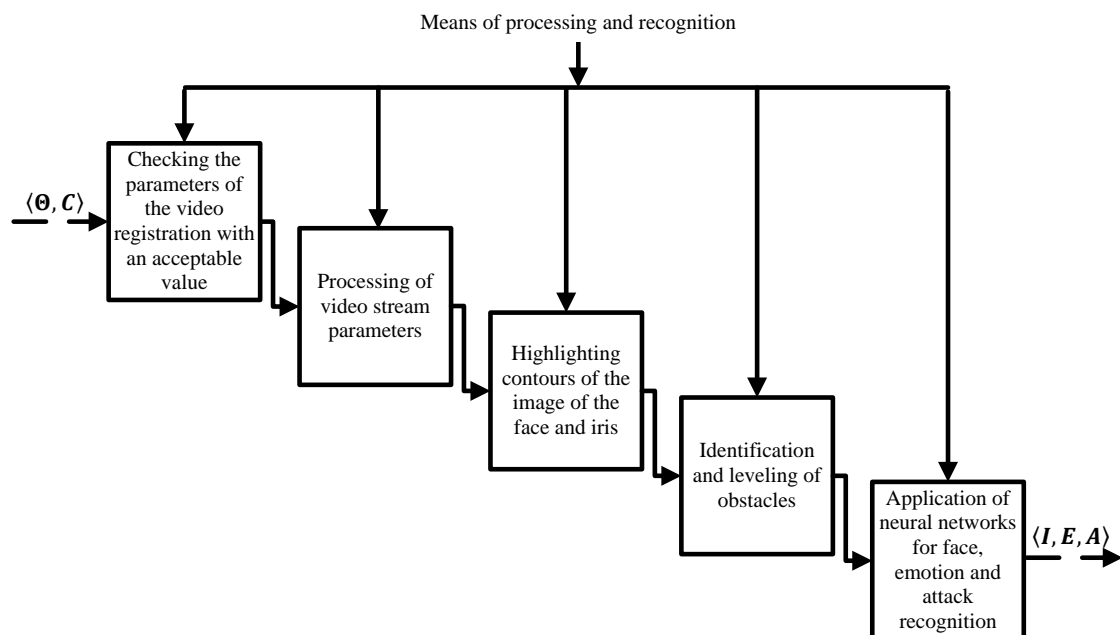
To detail the basic version of the model, the decomposition of face recognition by FI and IE at the BA of CIF personnel was carried out, taking into account the need to recognize emotions and attacks using dummies. According to [23, 27], when decomposing the procedure for recognizing a person, attention is focused on specific operations, the effectiveness of which in modern BA systems of CIF personnel can be considered insufficient. These operations should include:

- Selection of FI and IE in the video stream.
- Detection and leveling of recognition obstacles.
- Attack detection using dummies.

According to [7, 19, 25], the recognition process can be presented as a sequence of the following operations:

- Pre-processing of the image  $\xrightarrow{Pr}$ .
- Selection of contours FI and IE  $\xrightarrow{Sg}$ .
- Determining the coordinates of control points  $\xrightarrow{DtI}$ .
- Determining the coordinates of key points  $\xrightarrow{DtE}$ .
- Leveling of obstacles related to control points  $\xrightarrow{DI}$ .
- Leveling of obstacles that concern key points  $\xrightarrow{DIE}$ .
- Neural network person recognition  $\xrightarrow{NR_I}$ .
- Neural network recognition of emotions  $\xrightarrow{NR_E}$ .
- Neural network recognition of additional parameters to identify attacks using dummy  $\xrightarrow{NR_V}$ .
- Neural network recognition of attacks  $\xrightarrow{NR_A}$ .

The diagram of the decomposition of the procedure of recognition of the person according to FI and IE at the BA of the CIF staff, taking into account the need to determine emotions and detect attacks using dummies, is shown in Fig. 1.



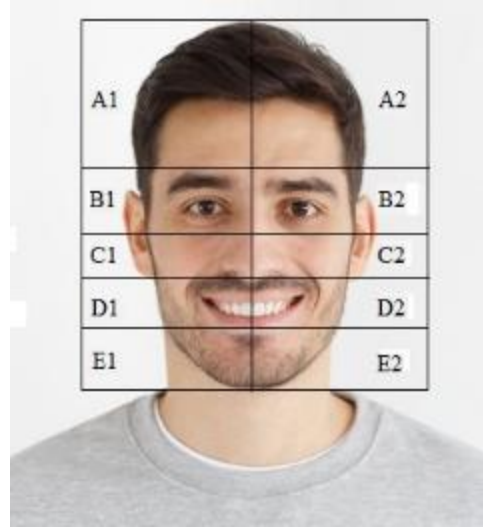
**Figure 1:** Decomposition diagram of the person recognition procedure.

Taking into account the generally accepted technology of neural network analysis of a video stream, the parameters of the model  $(\widetilde{C})$  relating to the selection of FI and IE contours should include the parameters that describe these contours in the pre-processed video stream. By analogy with (2), the frame of the processed video stream is described as follows:

$$\tilde{c}_k = \begin{bmatrix} \tilde{d}_{1,1} & \dots & \tilde{d}_{1,\tilde{X}} \\ \dots & \dots & \dots \\ \tilde{d}_{\tilde{Y},1} & \dots & \tilde{d}_{\tilde{Y},\tilde{X}} \end{bmatrix}, \quad k = 1 \dots K, \quad (4)$$

where  $k$  is the  $k$ th frame of the video stream;  $K$  is the number of frames of the input video stream;  $\tilde{X}$  – horizontal frame size;  $\tilde{Y}$  is the vertical frame size;  $\tilde{c}_{\tilde{x},\tilde{y}}$  is the color of the pixel with coordinates  $(\tilde{x}, \tilde{y})$ .

The presence of obstacles is intended to be described using the set  $\mathbf{Z}$ . Note that the data [6, 22] indicate the absence of a generally accepted approach to determining the parameters of interference. Therefore, to describe obstacles related to the visibility of key and control points, an approach is proposed that involves comparing the parameters of obstacles with their location and the number of key and control points that they overlap. It is assumed that the obstacle may overlap one or more zones shown in Fig. 2.



**Figure 2:** Areas of possible location of obstacles.

Zone A corresponds to the upper part of the human head, zone B to the eyes, zone C to the nose, D to the mouth, and E to the lower part of the face. Index 1 corresponds to the left part of the face, and index 2 to the right part. The intensity of the disturbance localized in a certain area of the face is suggested to be compared with the number of key and control points that it overlaps. The intensity of interference on the IE is correlated with the area covered by this interference. Note that the proposed approach allows you to adapt the interference intensity to use in models with different numbers of key and control points. Thus

$$\mathbf{Z} = \{z_1, z_2, \dots, z_{12}\}, \quad (5)$$

where  $z_1, \dots, z_{10}$  – a parameter that determines the intensity of interference localized in the area of the face image A1, A2, B1, B2, C1, C2, D1, D2, E1, E2, respectively;  $z_{11}, z_{12}$  – a parameter that determines the intensity of interference on the IE of the left and right eye.

$$z_m = \frac{1}{W_m} \sum_{w=1}^{W_m} r_w, \quad 0 \leq r_w \leq 1, \quad (6)$$



where  $m$  – the number of the corresponding area of the face image;  $W_m$  – the number of control/key points in the zone  $m$ ;  $r_w$  – the degree of reduction in the visibility of the  $w$ -th control/key point in the  $m$ -th area of the face due to the effect of interference.

Based on the results [8, 20, 24], approaches to detect attacks on the BA system based on the use of human face and eye dummies are proposed. The first approach involves the detection of an attack based on the results of the analysis of parameters characterizing the image of the environment, and the second - the detection of an attack based on the results of the analysis of the dynamics of FI and IE parameters, which describe the basic emotions of the CIF staff representative and additional parameters describing the dynamics of eye movements. Therefore, the set  $\Gamma$ , which contains additional parameters used to recognize attacks using dummies, includes:

- Change of gaze direction.
- Change in the size of the pupil of the eye.
- The presence of pulsations of blood vessels on the image of the eye.
- Eye blinking.

When using the second approach, the set  $\Gamma$  includes the parameters describing:

- The limits of the dummy demonstration device;
- Characteristic changes in the quality of FI plots;
- Objects that are recorded in typical video recording conditions;
- Distance from video camera to FI.

Considering (1-6), individual operations of the recognition process are represented as follows:

$$if ((\forall \theta \in \Theta) \theta \in \theta_{ent}) \wedge ((\forall c \in C) c \subset c_{ent}) \rightarrow \langle \Theta, C \rangle_{check} \text{ else } \mathbf{stop}, \quad (7)$$

$$\langle \Theta, C \rangle_{check} \xrightarrow{Pr} C_{pr}, \quad (8)$$

$$\langle \Theta, C_{pr} \rangle \xrightarrow{Sg} \tilde{C}, \quad (9)$$

$$\langle \Theta, \tilde{C} \rangle \xrightarrow{DtI} \langle \tilde{C}_I, Z_I \rangle, \quad (10)$$

$$\langle \Theta, \tilde{C} \rangle \xrightarrow{DtE} \langle \tilde{C}_E, Z_E \rangle, \quad (11)$$

$$\langle \tilde{C}_I, Z_I \rangle \xrightarrow{DU} \langle \tilde{C}_{crI}, Z_{crI} \rangle, \quad (12)$$

$$\langle \tilde{C}_E, Z_E \rangle \xrightarrow{DIE} \langle \tilde{C}_{crE}, Z_{crE} \rangle, \quad (13)$$

$$\langle \tilde{C}_{crI}, Z_{crI} \rangle \xrightarrow{NR_I} I, \quad (14)$$

$$\langle \tilde{C}_{crE}, Z_{crE} \rangle \xrightarrow{NR_E} E, \quad (15)$$

$$\langle \tilde{C}_{crI}, \tilde{C}_{crE}, Z_{crI}, Z_{crE} \rangle \xrightarrow{NR_\Gamma} \Gamma, \quad (16)$$

$$\langle E, \Gamma \rangle \xrightarrow{NR_A} A, \quad (17)$$

where  $\theta_{ent}$  - is the set of permissible values for  $\theta \in \Theta$ ;  $c_{ent}$  - set of admissible values for  $c \in C$ ;  $\langle \Theta, C \rangle_{check}$  - a tuple consisting of sets of  $\Theta, C$ , that have passed the verification of compliance of video registration parameters with permissible values;  $C_{pr}$  - a set of pre-

processed video stream parameters;  $\tilde{\mathbf{C}}_I, \tilde{\mathbf{C}}_E$  - sets of parameters of control and key points;  $\mathbf{Z}_I, \mathbf{Z}_E$  - sets of interference parameters;  $\tilde{\mathbf{C}}_{crI}, \tilde{\mathbf{C}}_{crE}$  - sets of parameters of control and key points after leveling of obstacles;  $\mathbf{Z}_{crI}, \mathbf{Z}_{crE}$  - sets of parameters of the interference.

Also, according to [11, 21, 14], the conceptual model includes a set of criteria for assessing the accuracy of the recognition process. For operations  $\xrightarrow{NR_I}, \xrightarrow{NR_E}, \xrightarrow{NR_\Gamma}, \xrightarrow{NR_A}$ , which are related to the classification of objects, the specified criteria include Accuracy, Recall, Precision and F1-score. For the operations  $\xrightarrow{Sg}, \xrightarrow{DtI}, \xrightarrow{DtE}, \xrightarrow{DII}, \xrightarrow{DIE}$ , which are related to semantic segmentation, the Dice criterion was used:

$$Dt = 2 \sum_{k=1}^K (y_{t,n} y_{m,n}) / \left( \sum_{k=1}^K y_{t,n}^2 + \sum_{k=1}^K y_{m,n}^2 \right), \quad (18)$$

where  $K$  - is the number of points describing the selected object;  $y_{m,n}$  is the value characteristic of the  $n$ th pixel of the selected object;  $y_{t,n}$  - is the value characteristic of the  $i$ -th pixel of the expected output signal.

Using the proposed conceptual model of recognition (7-18) in the development of NN means, it is necessary to take into account the level of development of technologies of neural network analysis of the video stream and the criteria for evaluating the effectiveness of BA tools.

Let's look at the benefits of using a conceptual model.

The conceptual model of facial and iris recognition offers several benefits for critical infrastructure security. Enhanced Security. This approach offers a stronger layer of security compared to traditional methods like keycards or passwords. Facial and iris recognition are unique biometric identifiers that are difficult to forge or replicate. Multimodal Authentication. By combining facial and iris recognition (multimodal approach), the system adds an extra layer of verification. Even if someone manages to spoof a face, a mismatch in the iris recognition would deny access. Improved Access Control Efficiency. Facial and iris recognition systems can automate the access control process, reducing wait times and streamlining entry for authorized personnel. Reduced Reliance on Physical Credentials. Physical access cards can be lost, stolen, or copied. Facial and iris recognition eliminates the need for physical credentials, minimizing the risk of unauthorized access. Potential for Deterrence. The very presence of a sophisticated facial and iris recognition system can deter potential intruders, knowing they face a significant hurdle to gain access. Auditability. The system can maintain a record of access attempts, allowing for easier identification and investigation of suspicious activity. The conceptual model provides a framework for a secure and efficient access control system that leverages the unique identification capabilities of facial and iris recognition technology.

#### 4. Conclusion

As a result of the analysis of scientific and practical works, it is shown that to build effective NN means of person recognition based on FI and IE of CIF personnel, it is necessary to supplement the methodological base by developing a conceptual model that will provide a formalized description of the recognition process.

It was determined that the recognition procedure includes the operations of checking the admissibility of the video registration parameters, refining the parameters of the video stream, selecting FI and IE contours, detecting and leveling interference, and applying NN means. For each of the specified operations, a list of efficiency assessment criteria adapted to the characteristics of modern means of implementation is substantiated.

For the first time, approaches to determining the parameters of obstacles for recognizing faces and emotions and recognizing attacks using dummies are proposed. The approach to determining the parameters of obstacles involves comparing the parameters of obstacles with the location and number of key and control faces that overlap. Approaches to the recognition of attacks with the help of dummies involve the detection of such attacks based on the analysis of the dynamics of basic emotions, eye movement parameters, and the environment during video recording.

Analytical expressions have been developed that provide a formalized description of each of the operations, and together, determined by the accuracy assessment criteria, form a conceptual model of the process of recognizing a person by FI and IE at the BA of CIF personnel using NN means, taking into account the need to determine emotions and detect attacks using dummies.

With the use of the developed recognition model, the prospects of improving NN means BA systems due to the use of the proposed approaches to parameter determination were determined obstacles and recognizing attacks using dummies. The development and implementation of a face recognition system integrating both facial and iris recognition technologies offer a robust solution for enhancing security at critical infrastructure facilities. By following the conceptual model outlined and the subsequent steps, organizations can Improved Security, Enhanced Efficiency Increased Reliability Adaptability and Scalability, and Continuous Improvement.

In essence, the implementation of a face recognition system incorporating facial and iris recognition technologies represents a proactive approach to security management, fostering a safe and secure environment for critical infrastructure facilities and their personnel.

## References

- [1] Ali, M., Thakur, K., & Tappert, C. (2015). User authentication and identification using neural network. *I-manager's Journal on Pattern Recognition*, (2), 28-39.
- [2] Bagitova, K., Tereikovskiy, I., Babayev, I., Tereikovska, L., & Tereikovskiy, O. (2023). Model for processing images of online social networks used to recognize political extremism. *Journal of Mathematics, Mechanics and Computer Science*, 119(3), 91-103. doi:10.26577/JMMCS2023v119i3a8.
- [3] Batista, J. C., Albiero, V., Bellon, O. R., & Silva, L. (2017). AUMPNet: Simultaneous Action Units Detection and Intensity Estimation on Multipose Facial Images Using a Single Convolutional Neural Network. *In 12th IEEE International Conference on Automatic Face & Gesture Recognition* (pp. 866-871).
- [4] Callet, P., Viard-Gaudin, C., & Barba, D. (2006). A Convolutional Neural Network Approach for Objective Video Quality Assessment. *IEEE Transactions on Neural Networks*, 17(5), 1316-1327.

- [5] Chandrani, S., Washef, A., Soma, M., & Debasis, M. (2015). Facial Expressions: A Cross-Cultural Study. *In Emotion Recognition: A Pattern Analysis Approach* (pp. 69-87). Wiley Publ. doi:10.1002/9781118910566.
- [6] Connaughton, R., Bowyer, K. W., & Flynn, P. J. (2013). Fusion of Face and Iris Biometrics. *In Handbook of Iris Recognition* (pp. 219-237). Springer.
- [7] Dychka, I., Chernyshev, D., Tereikovskiy, I., Tereikovska, L., & Pogorelov, V. (2020). Malware Detection Using Artificial Neural Networks. In Z. Hu, S. Petoukhov, I. Dychka, & M. He (Eds.), *Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing* (Vol. 938, pp. 3-12). Springer, Cham. doi:10.1007/978-3-030-16621-2\_1.
- [8] Held, G. (2003). *Securing wireless LAN's*. Macon, Georgia, USA: Publisher.
- [9] Linartz, J.-P., & Tuyls, P. (2003). New shielding functions to enhance privacy and prevent misuse of biometric templates. *In Proceedings of 4th International Conference on Audio And Video Based Biometric Person Authentication* (pp. 393-402).
- [10] Lu, X., & Jain, A. K. (2011). Deformation modeling for robust face matching. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 30(8), 1347-1358.
- [11] Ma, X., Fu, M., Zhang, X., Song, X., Becker, B., Wu, R., Xu, X., Gao, Z., Kendrick, K., & Zhao, W. (2022). Own Race Eye-Gaze Bias for All Emotional Faces but Accuracy Bias Only for Sad Expressions. *Frontiers in Neuroscience*, 16, 1-11. doi:10.3389/fnins.2022.852484.
- [12] Matusugu, M., Katsuhiko, M., Yusuke, M., & Yuji, K. (2003). Subject independent facial expression recognition with robust face detection using a convolutional neural network. *Neural Networks*, 16(5-6), 555-559.
- [13] Mian, A. S., Benamoun, M., & Owens, R. (2011). Keypoint detection and local feature matching for textured face recognition. *International Journal of Computer Vision*, 80(1), 1-13.
- [14] Nazarkevich, M., Vozniy, Ya., & Nazarkevich, G. (2021). Development of a machine learning method for biometric protection with new filtering methods. *Cyber Security: Education, Science, Technology*, 3(11), 16-30. doi:10.28925/2663-4023.2021.11.1630.
- [15] Noyes, E., Davis, J., Petrov, N., Gray, K., & Ritchie, K. (2021). The effect of face masks and sunglasses on identity and expression recognition with super-recognizers and typical observers. *Royal Society Open Science*, 8(3), 201169. doi:10.1098/rsos.201169.
- [16] Ranjith, G., Pallavi, K., & Mahendra, V. (2023). Human Face, Eye and Iris Detection in Real-Time Using Image Processing. In J.K. Mandal, M. Hinchey, & K.S. Rao (Eds.), *Innovations in Signal Processing and Embedded Systems. Algorithms for Intelligent Systems* (pp. 101-116). Springer, Singapore. doi:10.1007/978-981-19-1669-4\_34.
- [17] Ratha, N., Connelli, J., & Bolle, R. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3), 614-634.
- [18] Rinck, M., Primbs, M. A., Verpaalen, A. M., & Bijlstra, G. (2022). Face masks impair facial emotion recognition and induce specific emotion confusions. *Cognitive Research: Principles and Implications*, 7(1), 83, 203-217. doi:10.1186/s41235-022-00430-5.
- [19] Royer, J., Blais, C., Charbonneau, I., Déry, K., & Tardif, J. (2018). Greater reliance on the eye region predicts better face recognition ability. *Cognition*, 181, 12-20. doi:10.1016/j.cognition.2018.08.004.

- [20] Stallings, W., & Brown, L. (2022). *Computer security: principles and practice (4th ed.)*. Pearson.
- [21] Tariq, U., Lin, K., Li, Z., Zhou, Z., Wang, Z., Le, V., Huang, T. S., Lv, X., & Han, T. X. (2012). Emotion recognition from an ensemble of features. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 42(4), 1017–1026.
- [22] Tereikovskiy, I., Hu, Z., Chernyshev, D., Tereikovska, L., Korystin, O., & Tereikovskiy, O. (2022). The method of semantic image segmentation using neural networks. *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, 14(6), 1-14. doi:10.5815/ijigsp.2022.06.01.
- [23] Tereikovska, L., Tereikovskiy, I., Ayt Khozhaeva, E., Tynymbayev, S., & Imanbayev, A. (2017). Encoding of neural network model exit signal, that is devoted for distinction of graphical images in biometric authenticate systems. *News of the National Academy of Sciences of the Republic of Kazakhstan Series of Geology and Technical Sciences*, 6(426), 217–224.
- [24] Toliupa, S., Kulakov, Y., Tereikovskiy, I., Tereikovskiy, O., Tereikovska, L., & Nakonechniy, V. (2020). Keyboard Dynamic Analysis by Alexnet Type Neural Network. In *IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering* (pp. 416-420). doi:10.1109/TCSET49122.2020.235466.
- [25] Toliupa, S., Tereikovskiy, I., Dychka, I., Tereikovska, L., & Trush, A. (2019). The Method of Using Production Rules in Neural Network Recognition of Emotions by Facial Geometry. In *3rd International Conference on Advanced Information and Communications Technologies (AICT)* (pp. 323–327). doi:10.1109/AIACT.2019.8847847.
- [26] Vinette, C., Gosselin, F., & Schyns, P. (2004). Spatio-temporal dynamics of face recognition in a flash: it's in the eyes. *Cognitive Science*, 28, 289–301. doi:10.1016/j.cogsci.2004.01.002.
- [27] Viola, P., & Jones, M. (2005). Fast Multi-view Face Detection. *Mitsubishi Electric Research Laboratories Technical Report TR2005-097*, 67.
- [28] Viola, P. (2005). Robust real-time face detection. *International Journal of Computer Vision*, 58(2), 137–155.
- [29] Viswanath Reddy, A., et al. (2021). Facial Emotions over Static Facial Images Using Deep Learning Techniques with Hysterical Interpretation. *Journal of Physics: Conference Series*, 2089, 1-17. doi:10.1088/1742-6596/2089/1/012014.
- [30] Vysotska, O., Davydenko, A., & Khrystevych, V. (2022). Segmentation of a person's face in a video stream to monitor employees' compliance with safety conditions during work and training. *Information Security*, 24(2), 94-107. doi:10.18372/2410-7840.24.16934.
- [31] Zhuravlov, D., & Polshakova, O. (2023). Detection of face spoofing attacks on biometric identification systems. *Interdepartmental scientific and technical collection "Adaptive automatic control systems"*, 1(42), 108-114.