The object of study is a comprehensive biometric identification method based on local-texture descriptors HOG and 1DLBP. The task addressed is to determine the impact of adversarial cyberattacks on the accuracy of biometric identification by facial image.

The results under the predefined research conditions were evaluated in terms of the comprehensive method's efficiency, robustness, and stability. Experiments were conducted on six datasets covering controlled and uncontrolled shooting conditions, using a unified set of metrics. The impact was determined in scenarios of full visibility of facial features and in the presence of local occlusive disturbances characteristic of adversarial attacks.

The efficiency retention coefficient of the comprehensive method when used under controlled shooting conditions is 86.84–92.86% with a sensitivity index of 7.14–13.16%; the decrease in accuracy is statistically insignificant for most image sets. Compared with DNNs whose accuracy degradation under the influence of adversarial attacks reaches 26.45–76%, the comprehensive method's identification accuracy decreases by 1.5%. Such results are due to the features of the algorithmic formation of attribute vectors by descriptors and the comprehensive method's absence of sensitivity to perturbations calculated on the properties of DNN methods.

The HOG and 1DLBP descriptors compute the gradient and texture characteristics of local image regions based on deterministic algorithms without using training parameters and the error backpropagation mechanism. As a result, adversarial perturbations optimized for hierarchical nonlinear representations of DNNs have a limited impact on the feature space formed by descriptors. By conducting a study on face images acquired under variable conditions, the limits of the solution's applicability were determined.

The suitability of the comprehensive method for practical application in cybersecurity complexes, in particular in video surveillance, access control, and checkpoint systems, has been established

Keywords: biometric identification, facial recognition, image processing, software, cyber threats, adversarial attacks, local texture descriptors, HOG, 1DLBP, occlusive perturbations

UDC 004.93:004.056
DOI: 10.15587/1729-4061.2026.363911

DETERMINING THE IMPACT OF ADVERSARIAL CYBERATTACKS ON THE PERFORMANCE OF A COMPREHENSIVE BIOMETRIC IDENTIFICATION METHOD BASED ON LOCAL-TEXTURE DESCRIPTORS

Yelyzaveta Zhabska
Corresponding author
Doctor of Philosophy (PhD)*
E-mail: y.zhabska@gmail.com
ORCID: https://orcid.org/0000-0002-9917-3723
Kateryna Merkulova
Candidate of Technical Sciences, Associate Professor*
ORCID: https://orcid.org/0000-0001-6347-5191
Oleksii Bychkov
Doctor of Technical Sciences, Professor*
ORCID: https://orcid.org/0000-0002-9378-9535
*Department of Software Systems and Technologies
Taras Shevchenko National University of Kyiv
Volodymyrska str., 60, Kyiv, Ukraine, 01033

Received 13.03.2026
Received in revised form 26.05.2026
Accepted 04.06.2026
Published 30.06.2026

How to Cite: *Zhabska, Y., Merkulova, K., Bychkov, O. (2026). Determining the impact of adversarial cyberattacks on the performance of a comprehensive biometric identification method based on local-texture descriptors. Eastern-European Journal of Enterprise Technologies, 3 (9 (141)), 26–37. https://doi.org/10.15587/1729-4061.2026.363911*

1. Introduction

Biometric identification methods based on facial recognition are becoming increasingly widespread in modern security systems. This trend is due to the non-invasiveness and speed of identification methods, as well as the high degree of their implementation in the existing digital infrastructure. Facial recognition technologies are actively used in smart homes and offices, banking and finance, industry, medical and educational institutions, public transport, airports, and other various areas [1].

The use of biometric identification methods based on facial images is especially relevant in the context of the Russian-Ukrainian war as it plays an important role in ensuring national security and supporting the processes of solving humanitarian tasks. Such methods can be effectively used to identify individuals at checkpoints in order to detect sabotage and reconnaissance groups, identify the deceased, search for missing persons and illegally deported citizens. Facial recognition technologies are used in the detection and investigation of war crimes by identifying combatants using open source materials, which confirms their practical importance for ensuring the needs of state security.

According to Fortune Business Insights [2], in 2025 the global market for facial recognition technologies was estimated at USD 8.83 billion. According to forecasts, this estimate will increase to USD 10.13 billion in 2026, and to USD 30.52 billion in 2034. The average annual growth rate of 14.80% during the forecast period indicates a high level of trust in facial recognition technologies and determines their rapid development and spread in biometric identification software systems.

The increasing prevalence of biometric identification methods based on facial images is accompanied by an increase in the number and complexity of cyber threats directed against them. The false identification of just one person can pose a serious threat to the cyber environment. However, physical attacks, the effectiveness of which has been proven in real-world applications, can compromise a wide range of implemented security software packages. The data indicate that the consequences of vulnerabilities in biometric identification tools based on facial recognition technologies go beyond individual incidents and pose a threat to the digital infrastructure.

Accordingly, there is a need to conduct research on the effectiveness of biometric identification methods in the context of realistic cyber threats that interfere with the biometric data processing process. The results of studies could identify the limits of the reliability of existing biometric methods in the context of cyber threats, justify the choice of methods that are resistant to partial occlusion and local image disturbances, which determines the practical significance of our work.

Therefore, research into assessing the effectiveness of biometric identification methods based on facial images in the context of modern cyber threats is relevant from a scientific-practical point of view.

2. Literature review and problem statement

The results of research on the classification of attacks on biometric identification systems based on facial images are reported in [3]. It is shown that in the context of facial recognition, it is advisable to categorize basic attacks to reflect different levels of interference in the identification process, namely presentation, template, model, hardware, transmission, or storage attacks. However, issues related to assessing the impact of the aforementioned attack categories on the effectiveness of recognition methods remain unresolved. The reason may be the difficulty of taking into account the specific features of individual identification methods and cyberattack models within a single evaluation methodology. A likely option is to conduct research on the effectiveness of individual classes of recognition methods, taking into account the vulnerabilities inherent in these methods that can be used to implement attacks. That is the approach used in [4], in which it was found that the most common in practice are template attacks, which are carried out at the input to the biometric system, without requiring access to the internal structure.

The cited study was conducted using adversarial attacks, which are a type of template attacks. A benchmark for assessing the impact of adversarial attacks on identification methods based on convolutional neural networks is proposed, the results of which allow the authors to interpret the effectiveness of the attacked methods. A similar approach was used in [5], which investigated the impact of physical adversarial attacks on facial recognition systems using fabric masks. Masks are organically combined with the subject's facial features, which leads to errors in identification systems. Both papers show that classical convolutional neural networks are vulnerable to adversarial attacks, when used in which the effectiveness of the methods is significantly reduced. However, studies [4, 5] do not imply assessing in the same context the effectiveness of methods with an architecture different from neural networks or other artificial intelligence methods. The likely reason is that artificial intelligence methods are usually considered the most accurate and widespread in modern identification systems. As a result, research into architecturally different methods is mostly bypassed in studies of this type.

In [6], the results of devising a simulated adversarial attack in a physical environment using patches created on the basis of random affine transformations, an image pyramid, and a meta-ensemble strategy are reported. It is shown that the proposed method demonstrates high efficiency in experiments on face recognition on 16 basic neural network architectures, the efficiency of which decreases accordingly. However, despite the large number of experimentally studied methods, the issues related to the impact of an adversarial attack on other classes of identification methods have remained unresolved. The likely reason is the attack parameters specifically tuned to the neural network architectures, which does not indicate the absence of an impact of the attack on other identification methods. This confirms the previously noted thesis about the lack of an assessment of the impact of adversarial attacks on approaches alternative to artificial intelligence methods.

In [7], the results of a quantitative assessment of the impact of adversarial attacks on the accuracy of face recognition in biometric systems based on deep neural networks (DNNs) are reported. It is shown that the fast gradient sign (FGSM) attack reduces the accuracy of the systems from 97.70% to 42.45%, and the projected gradient sign (PGD) attack reduces the accuracy of the systems from 97.70% to 42.45%, and the projected gradient sign (PGD) attack reduces the accuracy of the recognition systems to 21.58%. In general, under the conditions of simulating physical adversarial attacks by digitally applying patches to the image, the accuracy of the recognition systems can degrade to 71.25%. In [8], an attack scenario is proposed under conditions of limited access to the model based on a deep neural network, in which generative adversarial networks (GANs) are used to form local modifications of the image. The generated patches are applied to individual areas of the face image in order to carry out recognition evasion and impersonation attacks. It is important that the patches act locally, overlapping or distorting specific areas of the face, but without changing the image as a whole. The experimental results showed that the formation of targeted local perturbations provides a higher level of attack success and negatively affects recognition methods based on deep networks. The reasons for such results are discussed in [9, 10].

In [9] it is shown that constructed local occlusive perturbations can negatively affect the performance of DNN models even with minimal image changes, which leads to identification errors. This property is due to the architectural features of deep networks, namely their sensitivity to local changes in the high-dimensional feature space. The vulnerability of DNN models justifies the feasibility of researching identification methods built on feature extraction tools with other architectural features.

In [10], an approach to implementing attacks under conditions of full access to the internal structure of the model by applying specially formed stickers to individual areas of the face is described. It is shown that local image modifications can lead to incorrect classification by a neural network even with a slight difference in similarity indicators. This indicates a high sensitivity of face recognition models to local distortions of input data and confirms the possibility of performing incorrect identification with minimal external influence.

The research results above indicate a decrease in the efficiency of recognition methods under the influence of adversarial attacks. However, the cited studies considered only one class of methods, namely neural networks, which demonstrate high accuracy on standard data sets with controlled fixation conditions. However, as shown in the literature [4–10], the efficiency of neural network methods is significantly reduced under the influence of adversarial attacks because even relatively simple physically implemented attacks can reduce the accuracy of the system by more than 76%. Such vulnerability is due to the sensitivity of DNN architectures to local perturbations in the local feature space. All this gives grounds to argue that the high accuracy of DNNs under laboratory conditions does not guarantee their efficiency under conditions of real cyber threats. This trend makes it necessary to study methods with a different architecture from neural networks, using data sets that cover controlled laboratory and shooting conditions close to the real environment. In addition, according to papers [11, 12], biometric identification is becoming increasingly widely used on compact digital devices, which necessitates devising methods with a resource-saving principle of operation.

A comparative analysis of the mathematical models used in [7–10] allows us to distinguish three fundamentally different approaches to the formation of perturbations. Gradient methods, in particular FGSM [7], form perturbations based on the gradient of the loss function. The formalization of the method is defined by expression $x_{adv} = I + eps \cdot \text{sign}(\text{grad}_I(L))$, where I is the input image, eps is the admissible value, L is the loss function, $\text{grad}_I(L)$ is the gradient of the loss function, $sign(\cdot)$ is the sign function. Iterative gradient methods, such as PGD [7], refine the perturbations at each step. In this case, $x_{adv}(it+1) = Proj_{eps}(x_{adv}(it) + alpha \cdot sign(\text{grad}_I(L)))$, where it is the iteration number, $alpha$ is the iteration step, $Proj_{eps}(\cdot)$ is the projection operator onto the admissible set of perturbations. Generative models [8] generate x_{adv} through a trained GAN generator that is optimized by minimizing the loss function L. A common feature of these approaches is that the perturbations are optimized with respect to the loss function and gradients, that is, they are specific to the deep learning architecture. However, perturbations optimized under DNN do not guarantee a similar destructive effect with respect to methods with deterministic feature space.

An alternative approach to biometric identification using facial images is local-texture descriptors. For example, in [13], the effectiveness of information technology for biometric identification using facial images based on local-texture descriptors was demonstrated. The results of improving information technology were considered in [1], which investigated the possibility of creating a single feature space for facial images from different datasets. Compared to neural networks, local-texture descriptors have a number of practically significant advantages, namely, they do not depend on large training sets, are computationally efficient, and operate on local-texture image structures that are formed by deterministic algorithms. The difference in classes of identification methods in the nature of the feature space demonstrates that adversarial perturbations optimized for DNN models may have different effectiveness with respect to local-texture descriptors. Descriptors calculate gradient and texture characteristics of local image regions based on deterministic algorithms without using training parameters and the error backpropagation mechanism. As a result, it can be assumed that adversarial perturbations optimized for hierarchical nonlinear DNN representations will have a limited impact on the feature space formed by descriptors. However, the above hypothesis remains practically unexplored because in most papers tackling the construction of biometric identification methods based on facial images, the object of research is deep learning methods.

Thus, the results of our literature review allow us to state a general unsolved problem. The body of available research does not define the impact of adversarial attacks on the effectiveness of identification methods based on local-textural descriptors. This allows us to argue that it is advisable to conduct a study aimed at eliminating this gap, which involves covering representative sets of images, using unified metrics, and determining the limits of applicability for a biometric identification method.

3. The aim and objectives of the study

The purpose of our study is to determine the impact of local occlusive disturbances characteristic of adversarial cyberattacks and image fixation conditions on the effectiveness of the comprehensive biometric identification method based on a face image according to local-texture descriptors. Results could allow us to substantiate the limits of practical applicability for the comprehensive method and compile recommendations on the feasibility of its use under actual cyberenvironment conditions.

Achieving the goal requires solving the following tasks:

– to assess effectiveness of the comprehensive biometric identification method under variable cyberenvironment conditions using the Rank-1 Identification Rate and Identification Error Rate metrics;

– to investigate robustness of the comprehensive biometric identification method to the impact of adversarial attacks using the Performance Retention Rate, Occlusion Sensitivity Index, and Degradation Slope metrics;

– to assess stability in the functioning of the comprehensive biometric identification method under cyberthreat conditions using the standard deviation and z-test of statistical significance of the decrease in identification accuracy.

4. The study materials and methods

4. 1. The object and hypothesis of the study

The object of our study is a comprehensive biometric identification method based on local-texture descriptors, proposed in [13], which implements a sequential process of image transformations to identify subjects who have a predefined biometric feature.

The principal hypothesis of the study assumes that the use of a comprehensive biometric identification method under conditions of local occlusive disturbances, characteristic of adversarial attacks, could provide a statistically insignificant decrease in efficiency compared to use in the absence of disturbances.

The study assumes that the occlusion of the lower part of the face of the subjects of identification in images is an adequate model of local occlusive disturbances inherent in adversarial cyberattacks in a real cyber environment. At the same time, the degradation of efficiency indicators of the comprehensive method when applied to such images is a consequence of local occlusive disturbances, rather than other factors of image variability.

The study adopts several simplifications. First, the occlusion of the lower part of the face of identification subjects was modeled programmatically at the pre-processing stage. Second, the reference and test samples were formed from the face images of the same number of identification subjects from different data sets, which provided the possibility of comparing the results of evaluating the effectiveness of the comprehensive method.

The experiments were conducted by applying the comprehensive method to samples of reference and test face images from six data sets, characterized by a variety of image parameters depending on the conditions of their acquisition. Two scenarios were envisaged for the experiments. In the first scenario, the comprehensive method was applied to original images with fully visible facial features in the images. The second scenario involved modeling the impact of adversarial cyberattacks on the operation of the comprehensive method, which are performed using masks and patches, forming local occlusive disturbances on the images. As a result of the experiments, the proportion of correctly identified subjects of the test sample relative to the total number of identification subjects was determined. The identification results were evaluated by a unified set of efficiency, robustness, and stability metrics.

4. 2. Concept of a comprehensive biometric identification method

The comprehensive method involves image transformation by sequentially applying the Viola-Jones methods, anisotropic diffusion, Gabor wavelet transform, histogram oriented gradient descriptors (HOG), and one-dimensional local binary patterns (1DLBP), as well as the square Euclidean distance metric. The input data for the comprehensive method is the face image matrix of the identification subject I.

At the stage of face detection in the image, the Viola-Jones method [14, 15] is used based on a cascade of classifiers, each of which checks a certain area of the image brightness matrix for the presence of facial features. The image matrix is scanned by a sliding window, in which the values of the Haar feature sequence are calculated. When applying the cascade to each classifier, a weighted sum of the Haar feature values is calculated. If at a certain stage the weighted sum of feature values exceeds a threshold value, the image region is classified as potentially containing facial features. The face image luminance matrix I_H is passed to the preprocessing stage using the anisotropic diffusion method [16].

First, the values of gradients in the brightness matrix I_H of the image are calculated, which are determined using a one-way difference scheme. Next, the conductivity gradients are calculated, which determine the change in the conductivity coefficient depending on the brightness gradient of the image matrix. The resulting values of conductivity gradients are used to calculate the diffusion flux, which describes how the brightness values of the elements change in different directions of the image matrix. The diffusion flux has smaller values at the boundaries of the contours that define facial features [14]. After applying anisotropic diffusion, the I_{AD} matrix is formed, the values of which are calculated by adding the diffusion flux values to the initial values of the matrix elements.

The I_{AD} matrix is then processed by the Gabor wavelet transform [17, 18]. The elements of the $GW(i_{GW}, j_{GW})$ matrix of the GW Gabor filters are calculated from the following formula

$$GW\left(i_{GW}, j_{GW}\right) = \\ = \exp\left(-\frac{1}{2}\left[\frac{i'^2_{GW} + g^2 j'^2_{GW}}{s^2}\right]\right)\cos\left(2\pi\frac{i'_{GW}}{l} + ph\right), \quad (1)$$

where $i'_{GW} = i_{GW}\cos o + j_{GW}\sin o$ and $j'_{GW} = -i_{GW}\sin o + j_{GW}\cos o$, o are the orientation of the normal to the parallel bands of the Gabor function in degrees, g is the spatial aspect ratio that determines the ellipticity of the Gabor function carrier, s is the standard deviation of the Gaussian kernel, l is the wavelength of the sinusoidal component, ph is the phase shift of the sinusoidal function.

The I_{AD} matrix is processed by f Gabor filters [GW_1, GW_2, ..., GW_f] using the convolution operation, thereby forming the resulting matrix I_G

$$I_G = I_{AD} * GW_f. \quad (2)$$

The I_G matrix is processed separately by each local texture descriptor to extract feature vectors. Histogram of Oriented Gradients (HOG) [19, 20] involves computing orientation gradients for each region of the image after its decomposition. The gradients in the horizontal direction $G_i(i, j)$ and in the vertical direction $G_j(i, j)$ are calculated as:

$$G_i\left(i,j\right) = \left|I_G\left(i,j+1\right) - I_G\left(i,j-1\right)\right|, \quad (3)$$

$$G_j\left(i,j\right) = \left|I_G\left(i+1,j\right) - I_G\left(i-1,j\right)\right|. \quad (4)$$

The magnitude $m(i, j)$ and orientation $O(i, j)$ of the gradients in the pixel with indices (i, j) are calculated from the following formulae:

$$m\left(i,j\right) = \sqrt{G_i^2\left(i,j\right) + G_j^2\left(i,j\right)}, \quad (5)$$

$$O\left(i,j\right) = \arctan\left(\frac{G_j\left(i,j\right)}{G_i\left(i,j\right)}\right)\cdot\frac{180°}{pi} \bmod 180°. \quad (6)$$

The matrix I_G is divided into small spatial regions, for each of which a local one-dimensional histogram of gradient orientations for all pixels within the region is accumulated. The histogram of regions of the matrix h_t is formed as an array where each value corresponds to the sum of the gradient values of pixels in regions whose orientation falls within the corresponding interval

$$h_t = \sum_{(i,j)\in C} m\left(i,j\right)\cdot mu_t\left(i,j\right), \quad (7)$$

where the weight coefficients mu_t are defined as

$$mu_t\left(i,j\right) = 1 - \frac{\left|O\left(i,j\right) - \Delta O\left(t + ½\right)\right|}{\Delta O}. \quad (8)$$

The histogram of cell C is determined by vector $\overrightarrow{H_C}$, having the form $\overrightarrow{H_C} = \left[h_1, h_2, \ldots, h_T\right]$, where T is the number of orientation intervals, and the histogram of the image block Q takes the form $H_Q = [H_{C1}, H_{C2}, ..., H_{Cr}]$, where r is the number of cells in the block. The V_{HOG} feature vector is formed by concatenating the normalized histograms of the image blocks.

Feature vector extraction by the descriptor of local binary patterns in one-dimensional space (1DLBP) [21] involves the decomposition of the I_G matrix into blocks, each of which is

transformed into one-dimensional space by inverting the pixel values and calculating their sum S_i in each i-th row

$$S_i = \sum_{j=1}^{M} B_{inv}(i,j), \quad (9)$$

where j is the index of matrix columns in the general sequence $j = [1, 2, ..., M]$, and M is the number of columns of the inverted brightness matrix B_{inv} of block B.

From the values of sums of the brightnesses of the inverted brightness matrix, the projection vector V_{pr} is formed

$$V_{pr} = (S_1, S_2, ..., S_M). \quad (10)$$

Each element of projection vector V_{pr} is compared with 8 neighboring values. All neighbors receive the value 1 if they are greater than or equal to the central element, 0 otherwise. The results of the comparison form $\vec{c}$ for elements of the projection vector, where $\vec{c} = [c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7]$. Next, weight coefficients are formed, which are set as $w_n = 2^n$, where n corresponds to the positions of elements $\vec{c}$. A separate value of the resulting $\vec{E}$ is calculated from the following formula

$$e = \sum_{n=0}^{7} c_n \cdot w_n. \quad (11)$$

The one-dimensional representation of the local binary patterns of a block in the matrix is defined by the resulting feature vector $\vec{E}$, of the form $\vec{E} = [e_1, e_2, ..., e_M]$, where M is the number of elements in the vector, which is equal to the number of columns in block B.

The feature vector V_{1DLBP} is formed as

$$V_{1DLBP} = [E_1, E_2, ..., E_B], \quad (12)$$

where B is the number of blocks of the input matrix formed as a result of decomposition.

The global face image feature vector is formed by concatenating the normalized V_{HOG} and V_{1DLBP} feature vectors, then compared with the reference feature vectors and classified by determining the least squared Euclidean distance. The result of the proposed comprehensive method is the identifier of the subject whose face is recorded on the input image I.

Thus, the comprehensive method of biometric identification is implemented by the sequence of stages of facial image transformation given in Table 1.

Table 1

Stages of implementing a comprehensive biometric identification method

Stage	Method	Input data	Output data	Goal
1	Viola-Jones	I	I_H	Face detection
2	Anisotropic diffusion	I_H	I_{AD}	Preprocessing
3	Gabor wavelet transform	I_{AD}	I_G	Image processing
4	HOG	I_G	V_{HOG}	Feature vector extraction
	1DLBP		V_{1DLBP}	
5	Squared Euclidean distance	Global feature vector [V_{HOG}; V_{1DLBP}]	Subject identifier	Feature vector classification

Stage 4 is the only parallel stage, as the HOG and 1DLBP descriptors process the same matrix, independently forming two feature vectors that are combined before the classification stage.

4. 3. Data sets

The impact of adversarial attacks on the effectiveness of the comprehensive biometric identification method was determined using image samples from six data sets covering a wide range of shooting conditions. From each data set, reference and test samples of images captured under controlled laboratory conditions and uncontrolled conditions close to the real environment of biometric identification were formed. The characteristics of the selected data sets are given in Table 2.

Table 2

Characteristics of face image sets

Dataset	Shooting conditions	Variability characteristics
The Database of Faces [22]	Controlled	Variations in lighting, facial expressions and occlusal elements, head rotation angles
FERET [23]	Controlled	Range of poses between frontal and profile, variations in facial expressions, changes in lighting between sessions, shooting intervals of more than 2 years
SCface [24]	Controlled	Fixation by video surveillance cameras, variability in distances between cameras and subject, different quality of camera sensors
AgeDB [25]	Uncontrolled	Large variability in age, variety of poses, facial expressions, and lighting
CFP [26]	Uncontrolled	Extreme variations in head position, natural changes in lighting and facial expressions
LFW [27]	Uncontrolled	Variations in pose, lighting, facial expressions, scale, and background

Objectivity and comparability of the research results between the datasets was ensured by limiting the number of identification subjects to 40 individuals, which corresponds to the number of subjects in the smallest dataset – The Database of Faces. In the test samples, 1 face image was stored for 1 identification subject, in the reference samples – from 2 to 5 images.

4. 4. Setting up and conducting experiments

In order to perform experimental studies, software was developed that implements a comprehensive biometric identification method and provides automated experiments for both scenarios on samples from each set of images.

The parameters of the comprehensive method are defined as follows. For the anisotropic diffusion method: conductivity value – 20, diffusion rate – 0.1, number of iterations – 10. For Gabor filters: filter size – 7 × 7 pixels, number of orientations o – 16 with a step of pi / 16, wavelength l – from pi with a step of pi / 10, standard deviation s – from pi with a step of pi / 10, phase shift ph – pi / 2, spatial aspect ratio g – 0.24. For the HOG descriptor: the number of orientations is 8, the block size is 16 × 36 pixels, the normalization region is 1 × 1, the vector dimension is 512 values. For the 1DLBP descriptor: the block size is 16 × 32 pixels, the vector dimension is 512 values. The global feature vector has a dimensionality of 1024. The software activity diagram is shown in Fig. 1.

The choice of scenarios for conducting experiments is determined by the purpose of our study.

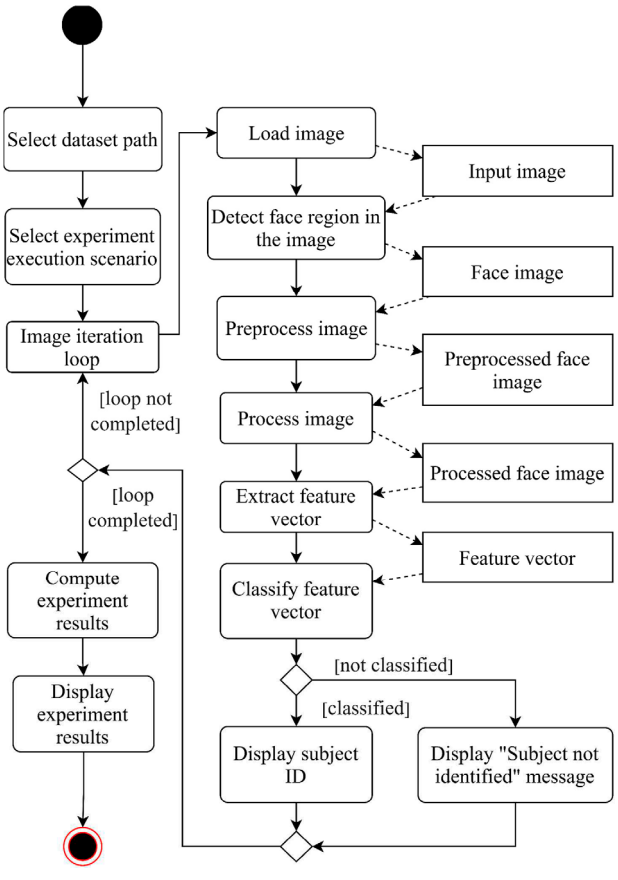

Fig. 1. Diagram of software activity and experiment execution process

Scenario 1 involved evaluating the effectiveness of the comprehensive biometric identification method under conditions of full visibility of facial features in the images. This scenario is defined as the base one, which corresponds to the conditions of the absence of adversarial cyberattacks.

Scenario 2 involved evaluating the effectiveness of the comprehensive method in the presence of local occlusive disturbances of the central and lower areas of the face, modeling a realistic vector of adversarial cyberattacks using patches overlapping these areas. The implementation of scenario 2 was ensured by transforming facial images at the pre-processing stage by software extraction of the central and lower areas containing adversarial elements.

In both scenarios, the reference and test image samples were identical. That is, the difference between the experimental scenarios was the additional technique of pre-processing images in Scenario 2, which ensured a correct comparison of the results.

4. 5. Evaluation metrics

The comprehensiveness of evaluation of the comprehensive method in experimental scenarios was enabled by a set of metrics that covered three aspects: the effectiveness of biometric identification, resistance to changes in operating environment conditions, and stability of functioning under input data variability.

Rank-1 Identification Rate (IR) was used as the basic metric for evaluating the effectiveness, which determines the accuracy of identification as the proportion of correctly identified subjects relative to the total number of identification subjects in the test sample. This metric directly reflected the probability of correctly determining the subject identifier for each test sample and was calculated from the following formula

$$IR = \frac{N_{correct}}{N_{total}}, \tag{13}$$

where $N_{correct}$ is the number of correctly identified subjects, N_{total} is the total number of subjects identified.

The Identification Error Rate (IER) characterized the proportion of incorrectly identified or unidentified subjects relative to the total number of subjects in the test sample, determining the probability of false identification at the Rank-1 level

$$IER = \frac{N_{total} - N_{correct}}{N_{total}}. \tag{14}$$

Degradation Slope (DS) measured the average decrease in accuracy per level of difficulty. Data sets were ranked from easiest to most difficult according to their identification accuracy value. The slope was equal to the accuracy range divided by the number of intervals between data sets

$$DS = \frac{IR_{\max} - IR_{\min}}{N-1}, \tag{15}$$

where $IR_{\max}$ is the highest identification accuracy, $IR_{\min}$ is the lowest identification accuracy, and N is the number of datasets. A smaller slope indicates a smoother degradation of performance and a higher robustness of the comprehensive method to the complexity of the identification conditions.

The Performance Retention Rate (PRR) determined the fraction of the identification performance under conditions of full visibility of facial features in the image (Scenario 1) that was retained in the presence of local occlusive disturbances (Scenario 2). By normalizing the performance for each dataset separately, PRR provided a robustness assessment independent of the accuracy level, which allowed for a correct comparison of results between datasets with different accuracy values

$$PRR = \frac{IR_{C2}}{IR_{C1}} \cdot 100\%, \tag{16}$$

where IR_{C1}, IR_{C2} are the identification accuracy indicators in Scenario 1 and Scenario 2.

Occlusion Sensitivity Index (OSI) is a metric complementary to PRR, which reflects the loss of identification accuracy in the presence of local occlusive disturbances relative to the accuracy indicator under conditions of full visibility of facial features

$$OSI = \frac{IR_{C1} - IR_{C2}}{IR_{C1}} \cdot 100\%. \tag{17}$$

The degree of dispersion in the identification accuracy values relative to the mean value was determined by the standard deviation (*std*)

$$SD = \sqrt{\frac{IR(1-IR)}{N_{total}}}. \tag{18}$$

The low value of *std* indicated stability of the comprehensive method in both scenarios of the experimental study.

The stability of the comprehensive method was assessed by the z-test, which determined whether the decrease in accuracy when switching between image sets and study scenarios was statistically significant or due to random sampling variation with a constant number of subjects. The z-test values were calculated from the following formula

$$z_i = \frac{IR_{C1,i} - IR_{C2,i}}{\sqrt{std^2_{C1,i} + std^2_{C2,i}}}. \quad (19)$$

where IR_{C1}, IR_{C2} are the identification accuracy indicators in Scenario 1 and Scenario 2, and std_{C1}, std_{C2} are the standard deviation in the identification accuracy values relative to the mean in Scenario 1 and Scenario 2.

5. Results investigating the effectiveness, robustness, and stability of the comprehensive method

5. 1. Evaluation of effectiveness

Table 3 gives the results of evaluating the effectiveness of the comprehensive biometric identification method under variable cyber environment conditions according to Scenarios 1 (C1) and 2 (C2) of conducting experiments, obtained using the Rank-1 Identification Rate (IR) and Identification Error Rate (IER) metrics, calculated from (13), (14).

It has been found that the effectiveness of the comprehensive method varies significantly depending on the set of images and their shooting conditions. In Scenario 1, the value of the IR metric is in the range of 0.450–0.950, while for sets of images recorded under uncontrolled conditions, lower identification accuracy rates are observed compared to data sets characterized by controlled shooting conditions. The IER metric repeats the IR trend in a complementary form.

In the presence of local occlusive disturbances in the images (Scenario 2), a decrease in the IR metric indicators was found for all data sets. The greatest degradation of identification accuracy is recorded for image sets LFW ($\Delta IR = 0.300$), AgeDB ($\Delta IR = 0.200$), and CFP ($\Delta IR = 0.100$), where ΔIR defines the difference in IR values between Scenarios 1 and 2. A smaller drop in accuracy is recorded for image sets with controlled shooting conditions: SCface ($\Delta IR = 0.125$), FERET ($\Delta IR = 0.075$), The Database of Faces ($\Delta IR = 0.050$). Overall, Scenario 2 retains the relative hierarchy of efficiency but is accompanied by an overall decrease in IR and an increase in IER.

The radar chart (Fig. 2) demonstrates that the transition from Scenario 1 to Scenario 2 is accompanied by a noticeable narrowing of the efficiency profile.

Table 3

Results of our experimental study on the effectiveness of the biometric identification comprehensive method

Dataset	Reference sample	Test sample	Number of identified subjects		IR_{C1}	IR_{C2}	ΔIR	IER_{C1}	IER_{C2}
AgeDB	174	40	18	10	0.450	0.250	0.200	0.550	0.750
CFP	202	40	24	20	0.600	0.500	0.100	0.400	0.500
LFW	125	40	22	10	0.550	0.250	0.300	0.450	0.750
The Database of Faces	120	40	28	26	0.700	0.650	0.050	0.300	0.350
FERET	99	40	29	26	0.725	0.650	0.075	0.275	0.350
SCface	160	40	38	33	0.950	0.825	0.125	0.050	0.175

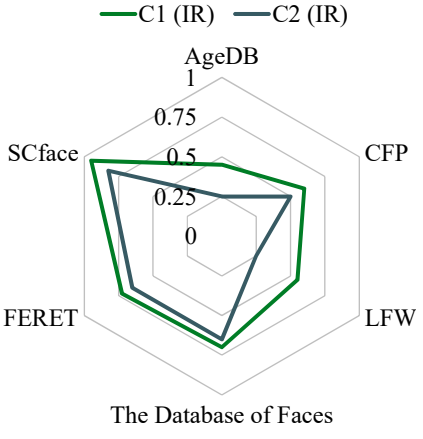

Fig. 2. Radar chart for identification accuracy of the comprehensive method

Our results reflect different degrees of degradation between data sets and indicate the variability of the effectiveness of the comprehensive method depending on the conditions of image acquisition.

5. 2. Results of robustness assessment

The robustness of the comprehensive method to the influence of adversarial attacks was assessed using the degradation slope index (DS), performance preservation ratio (PRR), and occlusion sensitivity index (OSI), calculated according from (15) to (17). Table 4 gives values of the DS metric.

Table 4

Indicators of the slope of degradation in identification accuracy for the comprehensive biometric identification method

Scenario	IR_{max}	IR_{min}	N	DS
C1	0.950	0.450	6	10%
C2	0.825	0.250	6	11.5%

The degradation slope indicator in Scenario 2 shows a slight increase compared to Scenario 1. The difference in indicators, which is 1.5%, indicates the absence of a significant impact of local occlusive disturbances on the nature of the decrease in the efficiency of the comprehensive method. Fig. 3 demonstrates that in both scenarios, similar dynamics of identification accuracy degradation are observed, which indicates the resistance of the comprehensive method to the influence of adversarial attacks.

Table 5 gives results of calculating the PRR and OSI metrics. In the general case, PRR values above 85% and OSI below 15% are considered indicators of high resistance of the comprehensive method to local occlusive disturbances, which is consistent with typical approaches to assessing resistance in biometric identification tasks. Analysis of the PRR and OSI indicators reveals a significant differentiation of the resistance of the comprehensive method depending on the conditions of data set formation. For image sets with controlled shooting conditions, the PRR is from 86.84% to 92.86%, which exceeds the established threshold value of 85%. At the same time, OSI values that are in the range of 7.14–13.16% do not exceed the threshold level of 15%. Accordingly, both indicators meet the criteria for a high level of resistance

of the comprehensive method to the influence of adversarial attacks due to the presence of local occlusive disturbances in the images.

Table 5

Efficiency retention coefficients and occlusion sensitivity indices of the comprehensive method

Dataset	PRR (%)	OSI (%)	Robustness Rating
AgeDB	55.56	44.44	Low
CFP	83.33	16.67	Moderate
LFW	45.45	54.55	Low
The Database of Faces	92.86	7.14	High
FERET	89.66	10.34	High
SCface	86.84	13.16	High

The metrics for the image sets with uncontrolled shooting conditions are outside the range of acceptable PRR and OSI values, indicating a low level of robustness. However, it is worth noting that the CFP data set yielded metrics close to the metric thresholds, so the robustness rating is set to moderate.

Fig. 4 illustrates the distribution of PRR and OSI values for the image sets.

Visual representation of PRR and OSI values allows us to clearly assess the distribution of robustness levels of the comprehensive method and confirm the identified patterns.

5. 3. Stability assessment results

The stability of the comprehensive method under cyberthreat conditions was assessed using the standard deviation *std* (18) and z-test scores (19) to test the statistical significance of the decrease in identification accuracy between the two study scenarios. The resulting values of these two scores are given in Table 6. A statistically insignificant result ($|z| < 1.96$) means that the observed change does not differ from chance, which indicates statistical confirmation that the comprehensive method is stable under the studied conditions.

Table 6

Results of stability assessment of the comprehensive method

Dataset	std_{C1}	std_{C2}	z	Rating
AgeDB	0.079	0.068	1.918	Stable
CFP	0.077	0.079	0.904	Stable
LFW	0.079	0.068	2.877	Unstable
The Database of Faces	0.072	0.075	0.478	Stable
FERET	0.071	0.075	0.726	Stable
SCface	0.034	0.060	1.805	Stable

The z-test results demonstrate that the decrease in identification accuracy when moving from Scenario 1 to Scenario 2 is statistically significant ($|z| > 1.96$) only for the LFW dataset ($z = 2.877$), as depicted in Fig. 5.

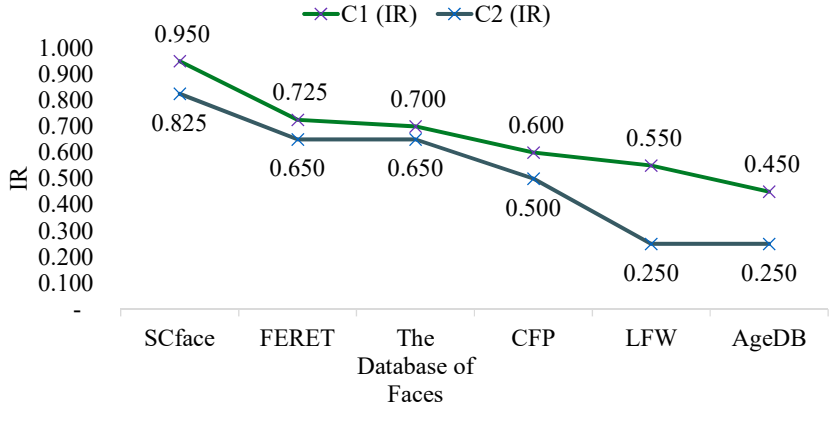

Fig. 3. Degradation curves for identification accuracy of the comprehensive method

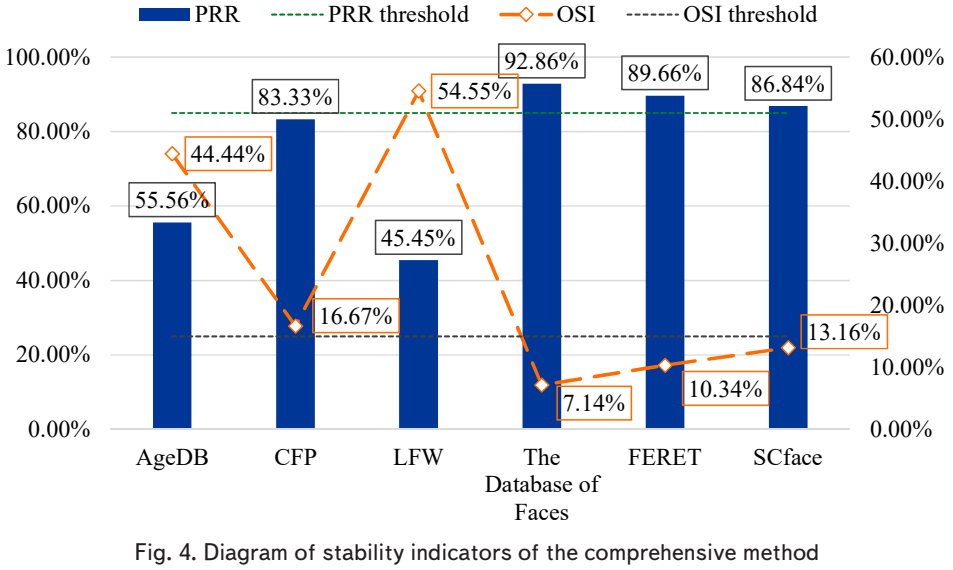

Fig. 4. Diagram of stability indicators of the comprehensive method

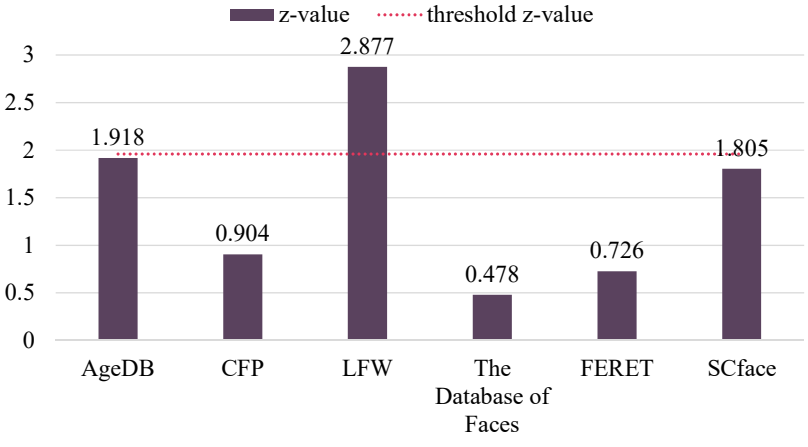

Fig. 5. Diagram of stability indicators for the comprehensive method

For the remaining datasets, the accuracy degradation is statistically insignificant ($|z| < 1.96$), which indicates stability in the performance of the comprehensive biometric identification method regardless of the application scenario.

6. Discussion of results based on investigating the comprehensive method; comparative analysis

The results of our study should be interpreted in the context of the properties of the input images and practical scenarios of adversarial cyberattacks, under which the effectiveness of the comprehensive biometric identification method was assessed.

The established dependence of the identification accuracy on the conditions of the data set formation (Table 3) is due to the features of the feature space formed by the local-texture descriptors HOG and 1DLBP according to (3) to (12). When applied to images obtained under controlled shooting conditions, the descriptors ensure the formation of stable and discriminative feature vectors, which is confirmed by the IR values in the range of 0.700–0.950 in Scenario 1. However, for image sets obtained under uncontrolled conditions, the IR indicator decreases to the range of 0.450–0.550, which reflects a decrease in the informativeness of the formed feature vectors with an increase in the variability of the input images. The degradation of efficiency in Scenario 2 is also differentiated depending on the conditions of image set formation, namely for images with uncontrolled shooting conditions ΔIR is 0.200–0.300, while for controlled sets – 0.050–0.125. This pattern is explained by the cumulative nature of the influence of two factors. The high intraclass variability of input images, inherent in uncontrolled shooting conditions [28], significantly reduces the discriminative capability of feature vectors in Scenario 1. At the same time, additional face occlusion in Scenario 2 enhances this effect due to the reduction in the volume of texture and gradient characteristics of images available for analysis. At the same time, the relative hierarchy of efficiency between data sets is preserved in both scenarios (Fig. 2), which confirms the stable nature of the implementation of the comprehensive method under variable cyber environment conditions.

Analysis of the degradation slope indicators (Table 4) reveals the preservation of the nature of the degradation of the efficiency of the comprehensive method when switching between the research scenarios. The increase in the DS indicator is 1.5%, which is confirmed by the similar dynamics of the degradation curves (Fig. 3). This result indicates that the influence of adversarial attacks due to the presence of local occlusive disturbances does not violate the general hierarchy of the efficiency of the comprehensive method between the data sets, but only evenly shifts the accuracy profile. The values of PRR in the range of 86.84–92.86% and OSI in the range of 7.14–13.16% for the controlled data sets that meet the criteria for a high level of stability (Table 5, Fig. 4) are explained by the volume of discriminative texture information in the upper part of the face that does not contain occlusion, which is sufficient for correct identification. The lower PRR values in the range of 45.45%–83.33% for the uncontrolled sets are a consequence of the cumulative effect described above, in which the already reduced discriminative capability of the descriptors due to the variability of the imaging conditions is further reduced due to occlusion [29]. At the same time, the upper limit of the PRR range, close to the threshold value, indicates a significant potential for increasing the robustness of the comprehensive method under the conditions of application in uncontrolled cyber environments.

The results of stability assessment (Table 6, Fig. 5) indicate that for five of the six studied data sets, the decrease in identification accuracy when moving from Scenario 1 to Scenario 2 is statistically insignificant ($|z| < 1.96$), which confirms the stability of functioning of the comprehensive method under the conditions of cyber threats. The only exception is the LFW image set ($z = 2.877$), which is characterized by a combination of the widest range of image characteristics obtained under uncontrolled conditions and the largest absolute decrease in accuracy, as a result of which the influence of local occlusive disturbances becomes systematic and reproducible, going beyond the limits of natural variability of the sample.

Taking into account the revealed patterns, the limits of applicability of the comprehensive biometric identification method have been determined. The comprehensive method provides the highest values of efficiency and resistance to adversarial cyberattacks under controlled conditions with constant lighting, a fixed distance between the subject and the camera, and limited variability of pose and head position. Application under uncontrolled conditions of the environment, which is characterized by uneven lighting, variable distance, age variability, and a wide range of poses, is limited due to a significant decrease in accuracy and stability and requires additional image normalization mechanisms.

The most balanced overall results among the studied scenarios for evaluating the comprehensive method were obtained when applied to the SCface image set, which simulated video surveillance conditions from different distances and angles. The comprehensive method provides high accuracy values ($IR = 0.950$ under conditions of full visibility of facial features and 0.825 in the presence of local occlusive disturbances in the image at a low level of errors, and the efficiency degradation index between scenarios ($\Delta IR = 0.125$) is one of the lowest among all image sets. The robustness of the comprehensive method when applied to the SCface set is evidenced by the metrics $PRR = 86.84\%$

and $OSI = 13.16\%$ (Table 5), which meets the criteria for a high level of stability ($PRR > 85\%$, $OSI < 15\%$). From the point of view of stability, the value $z = 1.805$ was obtained for the SCface set (Table 6, $|z| < 1.96$), which indicates a statistically insignificant decrease in accuracy between the experimental scenarios. The standard deviation *std* varies in the range 0.034–0.060 (Table 6), which is the lowest indicators in both application scenarios among all sets, which indicates the stable functioning of the comprehensive method. The combination of all indicators confirms the suitability of the comprehensive method for practical application in video surveillance systems, access control, and checkpoints.

Analysis of the characteristics of images from the SCface dataset allows us to formulate the following requirements for the input data of the comprehensive method. The most effective comprehensive method is performed when applied to images in JPG format with a resolution of 91 to 144 pixels in height with automatic calculation of the width while maintaining the aspect ratio. The subject's head can be rotated up to 45 degrees. Lighting conditions – without excessive darkening or lighting of individual areas. The distance from the subject to the camera can be from 1 m to 4.2 m. The time interval between capturing images of one subject should not exceed 2 years. Minor variability in facial expression is allowed, in particular, open or closed eyes, the presence or absence of a smile.

No direct comparison of the effectiveness of biometric identification methods based on local texture descriptors with deep learning methods under identical local occlusive disturbances has been carried out in available scientific papers. However, a comparison is possible based on the results of studies in which similar disturbances were applied to DNN systems. The comprehensive biometric identification method demonstrates a significantly lower sensitivity to local occlusive disturbances compared to methods based on deep learning. In contrast to [8], in which it was recorded that adversarial attacks reduce the accuracy of the DNN system from 97.70% to 71.25% (–26.45%) under the condition of applying adversarial patches to the image, the degradation of the effectiveness of the comprehensive method under similar conditions on controlled data sets does not exceed 12.5% ($\Delta IR = 0.125$, Table 3). The higher efficiency of the comprehensive method is also confirmed by the results in [5, 9], in which it is stated that adversarial attacks reduce the efficiency of DNN methods by 76%. The data indicate a high vulnerability of DNN to local occlusive disturbances and a better stability of the approach based on local-texture descriptors in solving the problem of biometric identification under the influence of adversarial attacks. This becomes possible due to the differences in the processes of image transformation by deep neural networks and local-texture descriptors. DNN architectures build hierarchical nonlinear representations of images and are sensitive to small, coordinated disturbances in high-dimensional space. Local-texture descriptors form feature vectors algorithmically based on the texture, gradient, and orientation characteristics of the image. That is, the descriptors show a lower impact of gradient-optimized attacks designed for the properties of neural networks.

The results of our experiments and the evaluation of effectiveness partially confirm the hypothesis of this study for the image sets obtained under controlled shooting conditions and partially refute it for the image sets formed under uncontrolled conditions. Our study bridges the gap identified in our review of related literature. The experiments were conducted using a comprehensive method based on local-texture descriptors to image samples from six representative data sets. The impact of adversarial attacks on the effectiveness, robustness, and stability of the comprehensive method was quantitatively assessed using a unified set of metrics; the limits of practical applicability of the comprehensive method were determined based on the obtained indicators.

Several limitations must be taken into account in practical application and further research. First, local occlusive perturbations of the lower part of the face are modeled programmatically, and not by physical adversarial masks or patches, while physical attacks can introduce unreproducible spatial heterogeneity of features. Second, the evaluation is limited to 40 subjects per dataset, which does not allow us to assess the significance of findings for large-scale identification systems. Third, only one type of occlusion was investigated, namely the lower face, so adversarial attacks targeting the periocular region or the entire face require separate investigation.

The disadvantage of the study is the lack of direct comparison with deep learning methods under identical experimental conditions, which makes it impossible to quantitatively confirm the superiority in efficiency.

Further research involves a wider coverage of occlusive elements and dynamic perturbations, investigation of methods for increasing robustness under uncontrolled conditions, and scaling by increasing the number of identification subjects in order to expand the scope of applicability of the comprehensive method.

7. Conclusions

1. We have established that in the absence of adversarial cyberattacks, the comprehensive method provides identification accuracy in the range of 0.700–0.950 for image sets with controlled shooting conditions and 0.450–0.600 under uncontrolled conditions. In the presence of local occlusive disturbances, the degradation of accuracy is differentiated depending on the conditions of data set formation: for controlled sets ΔIR = 0.050–0.125, for uncontrolled ones – ΔIR = 0.100–0.300, while the relative hierarchy of efficiency between the sets is preserved in both scenarios. This pattern is due to the algorithmic nature of feature vector formation by local-textural descriptors HOG and 1DLBP. This feature enables stable selection of gradient and texture characteristics within the visible area of the face. The identified differentiation indicates the dependence of effectiveness of the comprehensive method on the conditions of obtaining images in a real cyber environment.

2. It has been found that for image sets with controlled shooting conditions, the PRR values are 86.84–92.86% and OSI – 7.14–13.16%, which meets the criteria for a high level of resistance of the comprehensive method to adversarial attacks, while for image sets with uncontrolled shooting conditions, the PRR is 45.45–83.33%, which indicates a low or moderate level of resistance. The degradation slope index in the presence of local occlusive disturbances increases by 1.5%, which confirms the preservation of the general nature of the efficiency degradation regardless of the presence of occlusion. The revealed robustness of the comprehensive

method is explained by the sufficient amount of discriminative texture information in the face region that does not contain occlusion, and the lack of sensitivity of the method to gradient-optimized perturbations calculated on the properties of DNN methods, the accuracy degradation of which under similar occlusive conditions reaches 26.45–76%.

3. It has been established that the decrease in identification accuracy in the presence of local occlusive disturbances is statistically insignificant ($|z| < 1.96$) for five of the six image sets studied, which indicates stability of the comprehensive method. The exception for the LFW data set is explained by the cumulative effect of the widest range of characteristics of the uncontrolled environment and the largest absolute drop in accuracy, as a result of which the disturbance acquires a systematic and reproducible character, going beyond the limits of natural sample variability.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study and the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

All data are available in the main text of the manuscript.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

Authors' contributions

Yelyzaveta Zhabska: Conceptualization, Methodology, Software, Formal analysis, Investigation, Writing – original draft, Visualization; **Kateryna Merkulova:** Conceptualization, Methodology, Validation, Formal analysis, Resources, Writing – review & editing, Project administration; **Oleksii Bychkov:** Writing – review & editing, Supervision.

References

1. Martsenyuk, V., Bychkov, O., Merkulova, K., Zhabska, Y. (2023). Exploring Image Unified Space for Improving Information Technology for Person Identification. IEEE Access, 11, 76347–76358. https://doi.org/10.1109/access.2023.3297488
2. Facial Recognition Market Overview and Future Outlook (No. FBI101061) (2026). Fortune Business Insights. Available at: https://www.fortunebusinessinsights.com/industry-reports/facial-recognition-market-101061
3. Leyva, R., Gregory, E., Maple, C. (2025). Attack Vectors for Face Recognition Systems: A Comprehensive Review. ACM Computing Surveys, 58 (1), 1–37. https://doi.org/10.1145/3736753
4. Wang, M., Zhou, J., Li, T., Meng, G., Chen, K. (2026). A survey on physical adversarial attacks against face recognition systems. Neurocomputing, 669, 132485. https://doi.org/10.1016/j.neucom.2025.132485
5. Zolfi, A., Avidan, S., Elovici, Y., Shabtai, A. (2023). Adversarial Mask: Real-World Universal Adversarial Attack on Face Recognition Models. Machine Learning and Knowledge Discovery in Databases, 304–320. https://doi.org/10.1007/978-3-031-26409-2_19
6. Liu, X., Shen, F., Zhao, J., Nie, C. (2024). EAP: An effective black-box impersonation adversarial patch attack method on face recognition in the physical world. Neurocomputing, 580, 127517. https://doi.org/10.1016/j.neucom.2024.127517
7. Ma, T. (2025). Research on The Security of Face Recognition Systems Based on Digital and Physical Counterattacks. ITM Web of Conferences, 78, 2003. https://doi.org/10.1051/itmconf/20257802003
8. Hwang, R.-H., Lin, J.-Y., Hsieh, S.-Y., Lin, H.-Y., Lin, C.-L. (2023). Adversarial Patch Attacks on Deep-Learning-Based Face Recognition Systems Using Generative Adversarial Networks. Sensors, 23 (2), 853. https://doi.org/10.3390/s23020853
9. Guesmi, A., Hanif, M. A., Ouni, B., Shafique, M. (2023). Physical Adversarial Attacks for Camera-Based Smart Systems: Current Trends, Categorization, Applications, Research Challenges, and Future Outlook. IEEE Access, 11, 109617–109668. https://doi.org/10.1109/access.2023.3321118
10. Zheng, X., Fan, Y., Wu, B., Zhang, Y., Wang, J., Pan, S. (2023). Robust Physical-World Attacks on Face Recognition. Pattern Recognition, 133, 109009. https://doi.org/10.1016/j.patcog.2022.109009
11. Birgisdóttir, E. L., Kunkel, M. I., Pleva, L., Papaioannou, M., Choudhary, G., Dragoni, N. (2025). Exploring the Security of Mobile Face Recognition: Attacks, Defenses, and Future Directions. Applied Sciences, 15 (24), 13232. https://doi.org/10.3390/app152413232
12. Abidi, S. M. H., Hassan, S. A., Raza, S. M., Beliatis, M. J. (2026). Advances in Face Recognition: A Comprehensive Review of Feature Extraction and Dataset Evaluation. Electronics, 15 (2), 338. https://doi.org/10.3390/electronics15020338
13. Bychkov, O., Merkulova, K., Zhabska, Y. (2020). Information Technology of Person's Identification by Photo Portrait. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 786–790. https://doi.org/10.1109/tcset49122.2020.235542
14. Perona, P., Malik, J. (1990). Scale-space and edge detection using anisotropic diffusion. IEEE Transactions on Pattern Analysis and Machine Intelligence, 12 (7), 629–639. https://doi.org/10.1109/34.56205
15. Obaida, T. H., Jamil, A. S., Hassan, N. F. (2022). Real-time face detection in digital video-based on Viola-Jones supported by convolutional neural networks. International Journal of Electrical and Computer Engineering (IJECE), 12 (3), 3083. https://doi.org/10.11591/ijece.v12i3.pp3083-3091

16. Xia, R., Cheng, Y., Tang, Y., Liu, X., Liu, X., Wang, L., Jiang, P. (2025). S-Diff: An Anisotropic Diffusion Model for Collaborative Filtering in Spectral Domain. Proceedings of the Eighteenth ACM International Conference on Web Search and Data Mining, 70–78. https://doi.org/10.1145/3701551.3703490
17. Merkulova, K., Zhabska, Y. (2023). Input Data Requirements for Person Identification Information Technology. Proceedings of the 1st International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2023), 3468, 24–37. Available at: https://ceur-ws.org/Vol-3468/paper3.pdf
18. Wang, H., Jing, J., Li, N., Zhang, W. (2023). Multiscale and Multidirectional Gabor Filters for Image Corner Detection. 2023 9th International Conference on Mechanical and Electronics Engineering (ICMEE), 396–405. https://doi.org/10.1109/icmee59781.2023.10525496
19. Dalal, N., Triggs, B. (2005). Histograms of Oriented Gradients for Human Detection. 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), 1, 886–893. https://doi.org/10.1109/cvpr.2005.177
20. Legarda, D., Pérez, K., Muñoz, D. M. (2025). A comparative hardware implementation of histogram of oriented gradients as a descriptor in embedded tracking of swarm robots. Journal of Parallel and Distributed Computing, 198, 105026. https://doi.org/10.1016/j.jpdc.2024.105026
21. Benzaoui, A., Boukrouche, A., Doghmane, H., Bourouba, H. (2015). Face recognition using 1DLBP, DWT and SVM. 2015 3rd International Conference on Control, Engineering & Information Technology (CEIT), 1–6. https://doi.org/10.1109/ceit.2015.7233002
22. The Database of Faces. Available at: https://cam-orl.co.uk/facedatabase.html
23. Face Recognition Technology (FERET). Available at: https://www.nist.gov/programs-projects/face-recognition-technology-feret
24. Grgic, M., Delac, K., Grgic, S. (2009). SCface – surveillance cameras face database. Multimedia Tools and Applications, 51 (3), 863–879. https://doi.org/10.1007/s11042-009-0417-2
25. Moschoglou, S., Papaioannou, A., Sagonas, C., Deng, J., Kotsia, I., Zafeiriou, S. (2017). AgeDB: The First Manually Collected, In-the-Wild Age Database. 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 1997–2005. https://doi.org/10.1109/cvprw.2017.250
26. Sengupta, S., Chen, J.-C., Castillo, C., Patel, V. M., Chellappa, R., Jacobs, D. W. (2016). Frontal to profile face verification in the wild. 2016 IEEE Winter Conference on Applications of Computer Vision (WACV), 1–9. https://doi.org/10.1109/wacv.2016.7477558
27. Huang, G. B., Ramesh, M., Berg, T., Learned-Mille, E. (2007). Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. University of Massachusetts. Available at: https://people.cs.umass.edu/~elm/papers/lfw.pdf
28. Chethana, H. T., Nagavi, T. C., Mahesha, P., Ravi, V., Al Mazroa, A. (2025). Face Recognition in Unconstrained Images Using Deep Learning Model for Forensics. Security and Privacy, 8 (2). https://doi.org/10.1002/spy2.70012
29. Vu, H. N., Nguyen, M. H., Pham, C. (2021). Masked face recognition with convolutional neural networks and local binary patterns. Applied Intelligence, 52 (5), 5497–5512. https://doi.org/10.1007/s10489-021-02728-1