UDC 004.932.72'1
DOI: 10.15587/2312-8372.2017.110868

Nechyporenko O.,
Korpan Y.

ANALYSIS OF METHODS AND TECHNOLOGIES OF HUMAN FACE RECOGNITION

Проаналізовані задачі, методи і технології розпізнавання людини по зображенню обличчя. Визначені вимоги та фактори, що впливають на ознаки і характеристики об'єкта системи біометричної ідентифікації людини по обличчю, проаналізовано особливості класів та властивості задач. Розроблений узагальнений алгоритм автоматичної ідентифікації людини по обличчю, проаналізовані можливості подальшого розвитку таких систем.

Ключові слова: *розпізнавання облич, ідентифікація особистості, система біометричної ідентифікації людини по обличчю.*

1. Introduction

At present, biometric systems of human identification are widely used. Classical identification systems require knowledge of the password, the presence of a key, identification card, or other identifying item, it can forget or lose. In contrast, biometric systems are based on unique biological characteristics of a person that are difficult to forge and which uniquely identify a particular person. Such characteristics include, for example, fingerprints, palm shape, face geometry, iris pattern and retina image [1].

According to the report «Faith in Technology», prepared in May 2017 by HSBC, the countries of Asia and the Middle East are ahead of the West in the introduction of biometric technologies. India tops the list of countries with the greatest distribution of biometric identification tools, whose residents three times (9 %) used «iris recognition» for identification, than residents of any other country (3 %) who participated in the study. The Chinese prefer using fingerprint scanners (40 %). They are followed by Indians (31 %) and residents of the UAE (25 %). At the same time, only 9 % of French and Germans, and 14 % of Canadians used fingerprint scanning technology for identification [2].

At the same time, the regular use of traditional technologies, such as password-based identification, is most common in the West. When it comes to managing money assets, people in India (50 %) and China (48 %) are much more likely to trust computer advice than people, while for Canada and the UK this figure was 18 % and 21 %, respectively [2].

The task of identifying a person's face in a natural or artificial environment and further identification has always been among the top priorities for researchers working in the field of computer vision systems and artificial intelligence. Nevertheless, many studies conducted in leading scientific centers around the world for several decades have not led to the creation of real computer vision systems capable of detecting and recognizing a person in any conditions. Despite the proximity of the tasks and methods used in the development of alternative systems for biometric identification of a person, such as fingerprint identification or iris image, the face image recognition systems are significantly inferior to these systems. Therefore, the issue of research, improvement and development of modern methods and technologies for human face recognition is an urgent task.

2. The object of research and its technological audit

The object of research is the processes of biometric identification and human authentication based on the image of his face for computer vision systems.

Biometric authentication is the process of proving and authenticating through the presentation of a user's biometric image and by transforming this image in accordance with a predefined authentication protocol. Biometric authentication systems are the authentication systems used to verify the identity of people with their biometric data.

Face recognition is the automatic localization of a human face on an image or video and, if necessary, the identification of a person's identity on the basis of available databases (DB).

Biometric systems consist of two parts: hardware and specialized software. The hardware includes biometric scanners and terminals that capture a particular biometric parameter and convert the information received into a digital model available to the computer. And the software processes this data, correlates it with the database and makes a decision as to who appeared before the scanner. For example, [3] provides an analysis of biometric fingerprint sensors for an access control system, and [4] compares the characteristics of specialized biometric access control systems.

In order for the biometric system to be able to further identify the user, it must first register information about its identifiers. Commercial systems (in contrast to systems used by law enforcement and law enforcement agencies) retain not the image of real identifiers, but their digital models. When the user repeatedly accesses the system, the model of his identifier is again formed, and it is compared with the models already entered earlier in the database.

A serious problem facing computer vision systems is the large variability of visual images associated with changes in illumination, color, scale, viewing angles. In addition,

people have a habit of walking around the streets and in the premises dressed, which leads to significant variability in the images of the same person. However, the most difficult task of computer vision is the problem of eliminating the ambiguity that arises when designing 3D real-world objects on flat images. The color and brightness of individual pixels in the image also depends on a large number of hard-to-predict factors. These factors include:

– number and location of light sources;
– color and intensity of radiation;
– shadows or reflections from surrounding objects.

The task of detecting objects on the image is also complicated by the large amount of data contained in the image. The image can contain thousands of points, each of which can be important. Full use of the information contained in the image requires the analysis of each pixel for the belonging of its object or background, taking into account the possible variability of the objects. Such analysis may require large expenditures of the required memory of the computer's performance.

The disadvantages of person recognition by the person image include the fact that in itself such system does not provide 100 % reliability of identification.

3. The aim and objectives of research

The aim of research is analysis of the existing tasks, methods and technologies of human face recognition. To achieve this aim, it is necessary to solve the following tasks:

1. To determine the requirements and factors affecting the characteristics and characteristics of the object of biometric face recognition system.

2. To analyze the features of classes and the properties of problems of human face recognition.

3. To develop a generalized algorithm for automatic detection and human face recognition.

4. Research of existing solutions of the problem

The problem of face recognition was considered in the early stages of computer vision. A number of companies for over 40 years are actively developing automated and now automatic systems for recognizing human faces:

– Smith & Wesson (ASID-Automated Suspect Identification System);
– ImageWare (FaceID system);
– Imagis, Epic Solutions, Spillman, Miros (Trueface system);
– Vissage Technology (Vissage Gallery system);
– Visionics (FaceIt system).

Face recognition technologies are used in a wide variety of areas [5]:

– ensuring security in places of large crowds;
– security systems, prevention of illegal intrusion into the territory of the facility, search for intruders;
– face control in the catering and entertainment segment, search for suspicious and potentially dangerous visitors;
– verification of bank cards;
– online payments;
– contextual advertising, digital marketing, Intelligent Signage and Digital Signage;
– photographic equipment;
– forensics;
– teleconference;
– mobile applications;
– photo search in large photo databases;
– mark people on the photo in social networks and many others.

Apple use the face recognition system to unlock the phone – selfie, taken by the owner of the phone on the front camera, will be compared with the pre-loaded photo-standard. Google already uses face recognition in Android, to unlock the device. However, the developers have repeatedly argued that face recognition is not sufficiently protected in comparison with traditional methods. In Europe, the full-scale scientific project Tabula Rasa is being conducted, the main purpose of which is development of fraud protection for biometric identification methods [6].

Human face recognition stands out among biometric systems in that, firstly, no special or expensive equipment is needed. For most applications, a personal computer and a normal video camera are sufficient. Secondly, physical contact with devices is not possible. Do not touch anything or specifically stop and wait for the system to operate. In most cases, it's enough just to pass by or stay in front of the camera for a few seconds [7].

Efficiency of face recognition directly depends on such factors as the stability of the biometric pattern to various kinds of obstacles, distortions in the original photo or video recording [8–10].

With all the variety of different algorithms and methods of image recognition, they have a similar structure. A typical recognition method consists of three components [11]:

– transform the input image into the original representation (can include both pre-processing and mathematical transformations, for example, calculations of the main components);
– highlighting the key characteristics (for example, take the first n main components or the coefficients of the discrete cosine transform);
– classification mechanism (modeling): cluster model, metric, neural network, etc.

In addition, the construction of the recognition method relies on a priori information about the subject area (in this case – the characteristics of the person's face), and is corrected by experimental information that appears during the development of the method.

The tasks of human face recognition are divided into three classes: search in large databases, access control and photo control in documents. These tasks differ both in the requirements provided to the recognition systems and in the methods of solution, and therefore are separate classes. Requirements for errors of the first and second kind for such classes are different. A type I error, a misdetection, is a situation where the object of a given class is not recognized (skipped) by the system. An error of the second kind (type II error, false alarm) occurs when an object of a given class receives an object of another class [12].

There are several approaches to creating a face recognition algorithm: empirical, invariant and face detection using patterns.

The empirical approach was used at the beginning of the development of computer vision. It is based on some rules that a person uses to detect a person. For example, the forehead is usually brighter than the central part of the face, which, in turn, is uniform in brightness and color.

ISSN 2226-3780

Another important feature is the presence of parts of the face in the image – nose, ears, mouth and eyes. To determine the face, a significant reduction in the area of the image is made. These methods are easy to implement, but they are practically unsuitable in the presence of a large number of extraneous objects in the background, several persons in the frame or with a change in perspective.

The following approach uses the invariant features characteristic of the face image. At its basis, as in the previous method, lies the attempt of the system to «think» as a person. The method reveals the characteristic parts of the person, his boundaries, the change in form, contrast, etc., unites all these signs and verifies. This method can be used even when turning the head, but if there are other persons or a non-uniform background of recognition it becomes impossible.

The third approach is detection of the faces using patterns, which are set by the developer. The person is presented to a specific pattern or standard, and the purpose of the algorithm is testing each segment for the presence of this pattern, and the check can be performed for different angles and scales. Such system requires a lot of time-consuming calculations.

For comparison with graphic images-patterns, two main algorithms are used: minimum average correlation energy (MACE) [13] and local binary patterns (LBP) [14].

Local binary patterns (LBPs) use pixel processing on a digital image. The LBP algorithm is popular for recognizing a graphic image in general, and recently it is also used for face recognition. Nonparametric LBP kernel analyzes pixel structure of images. It is invariant to monotonic gray-scale transformations, that is, it is less sensitive to illumination, it is very important.

The principle of MACE filter operation is based on determining the average degree of correlation with preprepared images; the correlation coefficient is zero on the entire image, except for areas that coincide with the patterns, that is, in these areas the correlation degree is greater. To work, it is necessary a pattern database to calculate the correlation degree. To ensure greater reliability in the database, it is necessary to have a relatively large number of facial images, under different lighting conditions and changes in facial expressions.

5. Methods of research

The basis of any face recognition system is the method of its coding. In some cases, an analysis of individual local characteristics is used to represent the general image of a person in the form of statistically valid, standard data blocks. This method is used by Viscionics Corporation in its Facelt system. This mathematical method is based on the possibility of obtaining a person with a representative sample using modern statistical techniques. They cover the facial image pixels and universally represent the face shapes. In fact, there are much more elements in the construction of a person than the number of parts of it. The identity of a person is determined not only by the characteristic elements, but also by the method of their geometrical unification (their relative positions are taken into account). The obtained complex mathematical code of individual identity – the Faceprint pattern-contains information that distinguishes a person from millions of others with high accuracy. The pattern depends on changes in lighting, skin tone, presence or absence of glasses, facial expressions, hair, is resistant to change in angles up to 35″ in any directions.

Facelt system automatically evaluates the image quality for face recognition and, if necessary, is able to improve it. It also creates a face image from the data segments, generates a numeric code or internal pattern unique to each individual. The system incorporates a time tracking mode, as well as the compression of a face image to a size of 84 bytes for use in smart cards, barcodes and other devices with a limited storage size.

A person is a fairly simple object for recognition (when compared with other classes of objects). However, on the other hand, the face recognition systems have strict requirements for reliability, accuracy and stability of the allocation in the presence of various obstacles and changes in shooting conditions. The stability and accuracy of the recognition of facial elements on images in modern systems already exceed these characteristics for an expert person.

Typically, an image of a person is presented on an ambient background, which is not homogeneous (interior or exterior). The main stage of the face recognition system consists in determining the local area of the person's image according to its characteristic features (color components, local features of the points of the face and their relative position, shape). Allocation and evaluation of these characteristics underlies a whole class of algorithms aimed at solving the task of detecting faces on static images and video sequences [15–18].

The choice of algorithm that is used to human face recognition also depends on the specific conditions for its application. For example, the task of identifying a particular person in a crowd requires the use of sophisticated methods to reduce the level of false alarms. In the initial stages of the work, the identification system must cut off candidates that are not suitable and use the many candidates that remain to make the final decision on identification.

6. Research results

Solution to the problem of detecting objects on the face image is in correctly selection of the description of the objects for which the system is created and recognized. The description of the object must take into account its characteristic features and be sufficiently representative to distinguish this object from other elements of the surrounding scene.

To avoid subjectivity when choosing the desired description, one can use methods of automatic selection of the corresponding characteristics of the object, which are realized in genetic algorithms and in the training of artificial neural networks. At the same time, there are a number of parameters in the description of the object that the researcher currently has to select, developing a detection and recognition system. This choice includes:

– selection between 2D and 3D view of the scene and object. Algorithms that use the 2D representation are usually simpler than 3D algorithms, but at the same time require a large number of different descriptions, corresponding to the representation of the object under different observation conditions;

– choice between describing the object as a whole or as a system consisting of a certain number of interrelated elements;

– choice between the system of characteristics, based on geometric or other characteristics, describing the specifics of the object.

Let's analyze the features of the distribution of problems of human face recognition to classes.

For a class of image search tasks in large databases, one solution is to store small sets of predefined key characteristics in the database, as much as possible characterize the images. First of all, this method belongs to the method of principal components (the method of «own persons») [19–22]. Development of the method of principal components based on neural networks is described in [23, 24]. [25] also showed the possibility of using the features formed on the later layers of a specialized neural network for the classification of images by the nearest neighbor method.

By configuring the system, it automatically solves the problems of access control, it is possible to control the conditions for obtaining images that will be stored in the database, and to achieve their compliance with the conditions in which identification of a person will be carried out. Under the term «conditions» in this case, it is possible to mean both the person's light exposure when shooting, and its position in front of the camera (angle, distance to the lens), facial expressions, etc. To reduce the probability of incorrect identification, when creating a classifier, it is possible to use several images belonging to one person (with variations), up to comparison of video sequences of certain specific head movements and facial muscles of the face. In addition, when solving a problem of this kind, there arises the problem of physicians' age-related changes (search and selection of time-invariant characteristics). Typically, the system developer is able to provide an update of the image database in the event of an increase in the number of false access denials.

The main difficulty in automating the task of control of photographs in documents is the complete absence of any a priori information when comparing the images of the presenter received from the video camera and the photo scanned from the document. A significant complication is also possible a difference in the age of the person depicted on the document and the person facing the camera (the validity of the passport can be from 5 years to 55).

In addition, the problem is obtaining more or less the same (in terms of brightness) of the compared digital images. If the process of obtaining a high-quality image of the presenter of the document now does not cause any special problems, the digitization of the photo-portrait, glued to the document, is complicated by several factors. First of all, the quality will be lost due to the fact that not the object itself (the original) but its two-dimensional photo image is used to obtain the digital image, and also because it is impossible to control the initial conditions for obtaining this copy [26].

Distortion of digital images is due to the presence on modern documents of anti-counterfeiting tools. The imposition of varying degrees of complexity of patterns and seals on documents is used in many states and can serve as an additional complication in the analysis of the image and the allocation of signs for recognition.

The solution of the passport control problem requires the use of recognition methods, based on the comparison of only two images. The main difficulty of its solution lies in finding a sufficient number of common or distinctive features on the compared images for a confident answer to the question of the identity of objects. To determine the necessary minimum of such signs, based only on a couple of photos and often not being able to use any a priori information about the objects depicted on them, is a difficult task. Therefore, researchers working in this direction proposed methods based on the deformation of one image with the aim of transforming it into another and evaluating the «efforts» required for its implementation [21].

The results of the analysis of the properties of human face recognition problems are given in Table 1.

Having analyzed the requirements and peculiarities of the problems of human recognition by the person, let's develop a generalized algorithm for solving such problems.

The currently existing methods of automatic detection and human face recognition realize a scheme consisting (in the general case) of the following steps (Fig. 1):

1) identification of the presence of a person on the stage;
2) highlighting the figure of a person;
3) separation of the head;
4) determination of the head position (full face, profile);
5) separation of a person and his characteristics (attributes);
6) tracking the movement of a person by frames (for video images);
7) quality evaluation of the selected image;
8) comparison with standards and identification;
9) creation of an entry for the database.

Depending on the specific conditions, the structure and implementation of individual steps of the algorithm may differ. In the most difficult case, the person's face detection and identification system is used in a highly variable environment, with a large flow of input data. For example, work on city streets with heavy traffic, in the metro, airports, etc. To achieve satisfactory results of the algorithm, the use of maximum available information is required.

The algorithm should be able to effectively perform such actions:

– cut off static and slowly changing elements of the scene;
– work in different lighting conditions;
– recognize the figure of a person from different angles;
– track the movements of a large number of people;
– automatically select the time that is suitable for performing the identification of this person.

To provide such capabilities of the algorithm, a certain hardware saturation of the system is necessary. It includes multi-camera review and analysis of the scene with the possibility of selecting a 3D-structure. Also, resources are required for high-speed video stream input with filtering of scene elements with motion parameters and using color to highlight scene elements. In addition, cameras with high resolution and good optics are needed to provide the greatest possible range of reliable identification. In simple cases, with a static scene and a limited flow of events, it is possible to use a simpler hardware structure and algorithm. For example, a stereopair or a single camera and a pre-prepared scene model may be sufficient to reliably determine the fact that a person is in the control zone, highlighting his figure, and identifying him.

ISSN 2226-3780

Table 1

Analysis of the properties of human face recognition problems

Class	Requirements	Description	Algorithm
The task of finding images in large databases	Comparison of the «one-to-many» type. High requirements for an error of the first kind – the recognition system must find images corresponding to this person. A small number of other people are allowed in the resulting sample. Requirements for accuracy are not as critical as in access control and documentation control tasks	In a large database, it is necessary to find the image that is most similar to the specified one. The search should be conducted in a reasonable time. The applied methods: the method of the main components (the method of «own persons»), the development of the method of principal components on the basis of neural networks and the method of the nearest neighbor	The surveillance system takes pictures of a person. With the help of a neural network, the face area is searched. It is highlighted, the brightness and the contrast of the image are optimized, then the normalized photo portrait goes to the processing of another neural network that recognizes the entrance portrait and makes a choice from similar photos stored in the database
The task of access control	Comparison of the «one-to-few» type. The requirements for errors of the second kind are critical. The system should not recognize strangers, perhaps even by increasing the errors of the first kind. It is necessary high reliability of recognition. The system should work in real time. In the process of operation, the system is rapidly being trained	The system should recognize a group of faces and open access to a specific room. People who are not in this group, the system do not miss. There are no restrictions on the methods used here, but all of them agree that there is a training set of images of faces of a given group of people to which the system accesses during the recognition process or is tuned to it in the training process	On the door there is a photo or video camera that fixes the person at the entrance. The photograph shows the area of the face, then it is recognized. If the person corresponds to the portrait stored in the database, then additional information is read: name, age, position, etc. On the basis of this data, the system opens or closes access to objects
The task of controlling a photo in documents	Comparison of the «one-to-one» type. To formulate the requirements for errors of the first and second kind as to the recognition system is incorrect. It is desirable that the system does not make mistakes when comparing. Taking into account all possible differences in the learning process or setting up the system is complex. Great influence is exerted by age and other changes in the face	It is necessary to compare the received image of a person's face, with a photograph from the document in real time in the absence of a priori information about the analyzed photo portraits. The system determines whether these persons are one person or not. The methods are applied with special adaptation, for example, they use methods based on deformation of the image with the purpose of its transformation and evaluation of the «efforts» required for its implementation	The surveillance system takes a photo of a person. With the help of a neural network, the area of the face in the photograph is searched. The face area is analyzed, the signs for recognition are highlighted, after which this photo portrait is compared with the photo from the document. For this, the photo is scanned and the features for recognizing are allocated

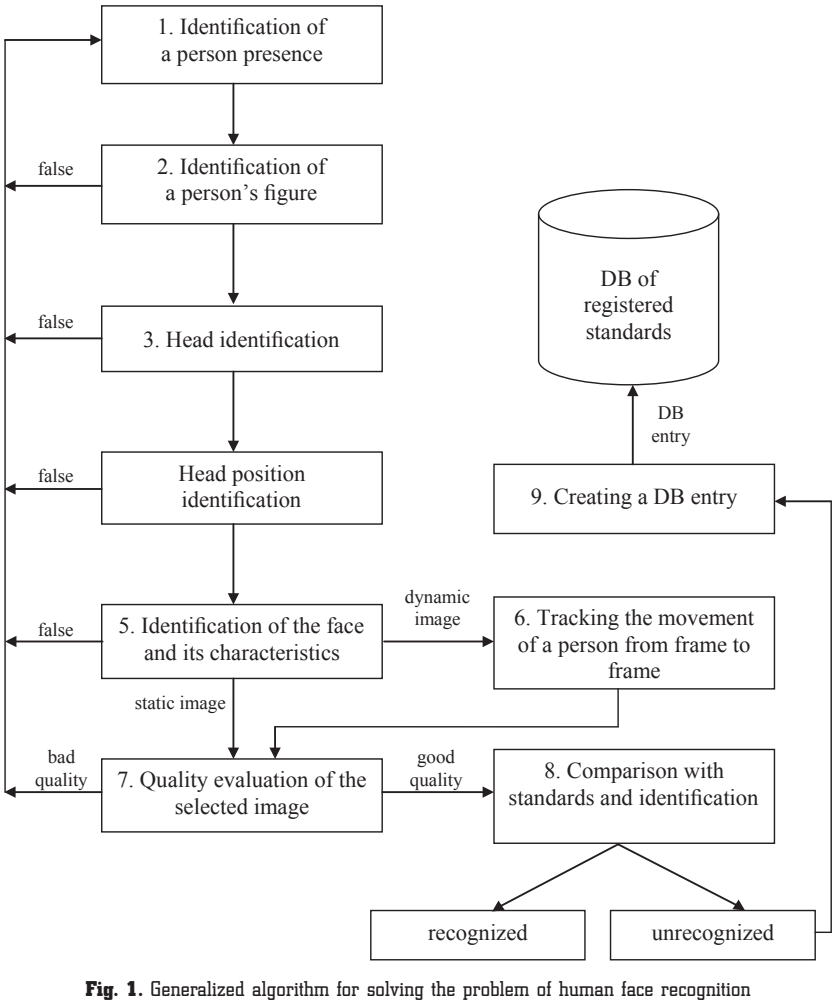

Fig. 1. Generalized algorithm for solving the problem of human face recognition

The task of determining the presence of a person on the stage requires an algorithm of a certain level of intelligence. It does not have to be a system, it reacts simply to the fact of the scene change. The human detection algorithm should not give false alarms when changes in illumination, the movement of shadows from static objects, the appearance in the control zone of animals, etc. In the case where this is necessary, the problem of creating an adequate description of the scene arises. This description may represent a three-dimensional model of a scene, a probable model for distributing colors or brightness of scene elements or a system of features, distinguishes the scene elements from recognition objects. Relationships between scene elements that are considered as backgrounds or foreground elements may change. The same human figure, if its image is less than a certain limiting value determined by the ability of the optical system, can be attributed to the background elements, since its analysis is unproductive for the fulfillment of the basic task of human identification.

When identifying a person moving in the field of view of a human camera, it is necessary to track the movements of the person from frame to frame. Having several images of one person in different angles, the program chooses the most successful frame from its point of

view and stores it in the database. By processing several images of one person in different angles, it is possible to achieve a very high percentage of recognition accuracy.

7. SWOT analysis of research results

Strengths. Methods of biometric identification and human face authentication are used in multimodal biometric systems. Multimodal biometric systems built on the combination of several biometric technologies, such as fingerprint recognition, facial features, voice, etc., are characterized by high efficiency of detecting unauthorized access to self-service banking devices. And also to the devices of the healthcare system database, mobile devices and a large number of online and offline applications. Therefore, the introduction of multimodal biometric systems in such sectors as healthcare, banking, financial sector, securities and insurance sector, transport sector, automobile transport, and also in the public sector will have a positive impact on the market of biometric face recognition technologies.

Weaknesses. To increase the identification accuracy, one can use images of human blood vessels. Images of blood vessels are the most stable and difficult to change sign of a person. By scanning the face image in infrared light, a unique temperature map of the face is created – a thermogram. Identification of the thermogram provides indicators that are comparable to fingerprint identification indicators, but to operate such system it is necessary to use expensive equipment. Installation, calibration and subsequent operation of such equipment require the involvement of highly qualified specialists.

Opportunities. A study of the possibilities for further development of biometric identification systems in the face shows that with an increase in the reliability of electronic identification documents (ID cards), it is possible to predict the quality equalization of the compared images. This is due to the fact that the information on such documents is presented in digital form, that is, the process of comparison of the generated digital image of the card presenter and the identifier recorded on it is simplified (with the allowance for video camera characteristics and shooting conditions).

Allied Market Research (USA) predicts the growth of the market for face recognition systems at 9.6 billion by 2022, with an average growth rate of 21.3 % per year. The market leader, according to forecasts, will be the United States. 3D technologies will occupy most of the market compared to 2D, and the software market will grow by 23.9 % annually until 2022 [6].

Manufacturers invest heavily in research and development of biometric identification systems in the face. It is expected that this will greatly accelerate the development of such systems by identifying the qualitative parameters of the face (scars, nose length, ear shape, facial expression, age or sex of a person).

In connection with the growing need to increase the level of security in Europe, a steady increase in the use of biometric identification systems in the face is expected. According to the marketing company GIA (USA), the volume of the world market for identification technologies by face and voice can reach up 2.9 billion dollars up to 2018 and according to MarketsandMarkets agency – 6.5 billion dollars

GIA analysts believe that the growing need for biometrics (including face and voice identification technologies) will contribute to increasing interest in ensuring security and resisting terrorist attacks, racially and ethnically motivated violence, crime and other unlawful acts. For the biometric identification technology segment in the face, the global CAGR will be 19 % (according to GIA) and 27.7 (MarketsandMarkets estimates).

Analysts of MarketsandMarkets believe that first of all the needs of state structures will contribute to the market's progress, as well as the continued spread of video surveillance systems. In addition, according to the authors of the work, good opportunities are opened by the application of the technologies considered in consumer electronics devices and mobile gadgets. It is possible that further development will receive «cloud» services based on biometric identification in the face [2].

Threats. Despite the current level of photo and video equipment, the face recognition systems are significantly inferior to fingerprint analysis systems or iris images.

8. Conclusions

1. Requirements and factors influencing the performance and characteristics of the object of the biometric face recognition system are defined. First of all, it is the variability of visual images, the design of three-dimensional objects, the number and location of light sources, the color and intensity of radiation, shadows or reflections from surrounding objects. The solution to the problem of detecting objects on the image lies in the correct choice of the description of objects, for the detection and recognition of which the system is created. This choice includes:

– the choice between 2D and 3D representation of the scene and object;

– the choice between describing an object as a whole or as a system;

– the choice between the system of characteristics that describe the specifics of the object.

2. The features of classes and properties of human face recognition problems are analyzed. For a class of image search tasks in large databases, one solution is to store small sets of predefined key characteristics in the database, as much as possible characterize the images. When adjusting the system, it automatically solves the problems of access control, to reduce the probability of incorrect identification, one can envisage the use of several images belonging to one person (with variations), up to comparing the video sequences of certain specific head movements and face facial muscles. The solution of the passport control problem requires the use of recognition methods based on the deformation of one image in order to turn it into another and to evaluate the «efforts» required for its implementation.

3. A generalized algorithm for automatic face detection and recognition is developed. The presented scheme of the generalized algorithm consists of nine simple steps and takes into account the identification features using photo and video images. The advantage of the algorithm is the simplicity of implementation, it allows already at the design stage of the identification system, to quickly evaluate the system's operability by analyzing the internal interaction of its elements.

ISSN 2226-3780

References

1. Jain, A. K. Biometrics: Personal Identification in Networked Society [Text] / ed. by A. K. Jain, R. Bolle, S. Pankanti. – Springer US, 1999. – 411 p. doi:10.1007/b117227
2. Biometricheskaia identifikatsiia (mirovoi rynok) [Electronic resource] // Tadviser. – May 29, 2017. – Available at: \www/URL: http://www.tadviser.ru/index.php/Статья:Биометрическая_идентификация_(мировой_рынок)
3. Lukashenko, V. M. Systemnyi analiz biometrychnykh datchykiv vidbytkiv paltsia dlia systemy upravlinnia dostupom lazernoho tekhnolohichnoho kompleksu [Text] / V. M. Lukashenko, T. Yu. Utkina, O. S. Verbytskyi, D. A. Lukashenko, S. A. Mitsenko, O. V. Nechyporenko // Visnyk ChDTU. – 2012. – No. 4. – P. 29–34.
4. Lukashenko, V. M. Sravnitel'nyi analiz spetsializirovannyh sistem upravleniia dostupom na baze biometirii [Text] / V. M. Lukashenko, O. S. Verbitskii, S. A. Moshchenko, Yu. Yu. Tereshchenko, E. P. Lukatskaia // Materialy VI Miedzynarodowej naukowi-praktycznej konferencji «Nauka i wyksztaicenie bez granic – 2010», 7–15 grudnia 2010, Przemysl, Poland. – Przemysl: Nauka i studia, 2010. – Vol. 22. – P. 9–12.
5. Ionova, A. Tehnologii raspoznavaniia lits ili feiskontrol' po-umnomu [Electronic resource] / A. Ionova // Novosti Interneta veshchei. – February 28, 2017. – Available at: \www/URL: https://iot.ru/gorodskaya-sreda/tekhnologii-raspoznavaniya-lits-ili-feyskontrol-po-umnomu
6. Tehnologii biometricheskoi identifikatsii [Electronic resource] // Tadviser. –August 25, 2017. – Available at: \www/URL: http://www.tadviser.ru/index.php/Статья:Технологии_биометрической_идентификации
7. Kuharev, G. A. Metody obrabotki i raspoznavaniia izobrazhenii lits v zadachah biometrii [Text] / G. A. Kuharev, E. I. Kamenskaia, Yu. N. Matveev, N. L. Shchegoleva; ed. by M. V. Hitrov. – Saint Petersburg: Politehnika, 2013. – 388 p.
8. Hrulev, A. Sistemy raspoznavaniia lits. Sostoianie rynka. Perspektivy razvitiia [Electronic resource] / A. Hrulev // Sistemy bezopasnosti. – 2012. – No. 1. – Available at: \www/URL: http://secuteck.ru/articles2/videonabl/sistemi-raspoznavaniya-lic
9. Korpan, Ya. V. Metody filtratsii shumu pry obrobtsi tsyfrovoho zobrazhennia [Text] / Ya. V. Korpan, O. V. Nechyporenko // Materialy XII Miedzynarodowej naukowi-praktycznej konferencji «Dynamika naukowych badan – 2016», 07–15 lipca, 2016, Przemysl, Poland. – Przemysl: Nauka i studia, 2016. – Vol. 13. – P. 17–21.
10. Korpan, Ya. V. Analiz vykorystannia tekhnolohii zmenshennia shumiv na zobrazhenni pry identyfikatsii i avtentyfikatsii obiekta [Text] / Ya. V. Korpan, O. V. Nechyporenko // Zbirka naukovykh prats IV Naukovoi konferentsii «Fundamentalni ta prykladni doslidzhennia u suchasnii nautsi», 30 zhovtnia 2016, Kharkiv, Ukraine. – Kharkiv: Technology Center, 2016. – P. 90.
11. Tropchenko, A. A. Metody vtorichnoi obrabotki i raspoznavaniia izobrazhenii [Text]: Handbook / A. A. Tropchenko, A. Yu. Tropchenko. – Saint Petersburg: Universitet ITMO, 2015. – 215 p.
12. Glazunov, A. Komp'iuternoe raspoznavanie chelovecheskih lits [Electronic resource] / A. Glazunov // Otkrytye sistemy. – 2000. – No. 3. – Available at: \www/URL: https://www.osp.ru/os/2000/03/177945/
13. Savvides, M. Face Verification using Correlation Filters [Text] / M. Savvides, B. V. K. V. Kumar, P. Khosla // CMU Electrical & Computer Engineering. – Available at: \www/URL: http://www.ece.cmu.edu/~kumar/Biometrics_AutoID.pdf
14. Marcel, S. On the Recent Use of Local Binary Patterns for Face Authentication [Text] / S. Marcel, Y. Rodriguez, G. Heusch // International Journal of Image and Video Processing, Speci Al Issue on Facial Image Processing. – 2007. – Available at: \www/URL: http://www.idiap.ch/~marcel/professional/publications/marcel-ijivp-2007.pdf
15. Li, S. Z. Handbook of Face Recognition [Text] / S. Z. Li, A. K. Jain. – London: Springer, 2011. – 699 p. doi:10.1007/978-0-85729-932-1
16. Jafri, R. A Survey of Face Recognition Techniques [Text] / R. Jafri, H. R. Arabnia // Journal of Information Processing Systems. – 2009. – Vol. 5, No. 2. – P. 41–68. doi:10.3745/jips.2009.5.2.041
17. Viola, P. Rapid object detection using a boosted cascade of simple features [Text] / P. Viola, M. Jones // Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001. – Kauai, Hawaii, USA, 2001. – Vol. 1. – P. 511–518. doi:10.1109/cvpr.2001.990517
18. Papageorgiou, C. P. A general framework for object detection [Text] / C. P. Papageorgiou, M. Oren, T. Poggio // Sixth International Conference on Computer Vision (IEEE Cat. No.98CH36271). – Narosa Publishing House, 1998. – P. 555–562. doi:10.1109/iccv.1998.710772
19. Nechyporenko, O. V. Biometrychna identyfikatsiia i avtentyfikatsiia osoby za heometriieiu oblychchia [Text] / O. V. Nechyporenko, Ya. V. Korpan // Visnyk KhNU. – 2016. – No. 4. – P. 133–138.
20. Samal, D. I. Vybor priznakov dlia raspoznavaniia na osnove statisticheskih dannyh [Text] / D. I. Samal, V. V. Starovoitov // Tsifrovaia obrabotka zobrazhenii. – 1999. – P. 105–114.
21. Samal, D. I. Algoritmy identifikatsii cheloveka po fotoportretu na osnove geometricheskih preobrazovatelei [Text]: PhD thesis / D. I. Samal. – Minsk: ITK NANB, 2002. – 167 p.
22. Chellappa, R. Human and machine recognition of faces: a survey [Text] / R. Chellappa, C. L. Wilson, S. Sirohey // Proceedings of the IEEE. – 1995. – Vol. 83, No. 5. – P. 705–741. doi:10.1109/5.381842
23. Bryliuk, D. Application of Recirculation Neural Network and Principal Component Analysis for Face Recognition [Text] / D. Bryliuk, V. Starovoitov // The 2nd International Conference on Neural Networks and Artificial Intelligence. – Minsk: BSUIR, 2001. – P. 136–142. – Available at: \www/URL: http://neuroface.narod.ru/files/npca.pdf
24. Kong, H. Generalized 2D principal component analysis for face image representation and recognition [Text] / H. Kong, L. Wang, E. K. Teoh, X. Li, J.-G. Wang, R. Venkateswarlu // Neural Networks. – 2005. – Vol. 18, No. 5–6. – P. 585–594. doi:10.1016/j.neunet.2005.06.041
25. Samaria, F. S. Face Recognition Using Hidden Markov Models [Text]: PhD thesis / F. S. Samaria. – Engineering Department, Cambridge University, 1995. – Available at: \www/URL: https://www.repository.cam.ac.uk/handle/1810/244871
26. Samal, D. I. Metodika avtomatizirovannogo raspoznavaniia liudei po fotoportretam [Text] / D. I. Samal, V. V. Starovoitov // Tsifrovaia obrabotka zobrazhenii. – Minsk: Institute of Technical Cybernetics of the National Academy of Sciences of Belarus, 1999. – P. 81–85.

АНАЛИЗ МЕТОДОВ И ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ ЛЮДЕЙ ПО ИЗОБРАЖЕНИЮ ЛИЦА

Проанализированы задачи, методы и технологии распознавания человека по изображению лица. Определены требования и факторы, влияющие на признаки и характеристики объекта системы биометрической идентификации человека по лицу, проанализированы особенности классов и свойства задач. Разработан обобщенный алгоритм автоматической идентификации человека по лицу, проанализированы возможности дальнейшего развития таких систем.

Ключевые слова: распознавание лиц, идентификация личности, система биометрической идентификации человека по лицу.

Nechyporenko Olga, *PhD, Associate Professor, Department of Robotics and Specialized Computer Systems, Cherkassy State Technological University, Ukraine, e-mail: olne@ukr.net, ORCID: http://orcid.org/0000-0002-3954-3796*

Korpan Yaroslav, *PhD, Associate Professor, Department of Robotics and Specialized Computer Systems, Cherkassy State Technological University, Ukraine, e-mail: populusdocti@gmail.com, ORCID: http://orcid.org/0000-0002-1455-5977*