

Ministry of Education and Science of Ukraine

*Odessa National Academy
of Food Technologies*



International Competition of Student Scientific Works

BLACK SEA SCIENCE 2020

Information Technology, Automation and Robotics

Proceedings

Odessa, ONAFT 2020

Editorial board:

Prof. B. Iegorov, D.Sc., Rector of the Odessa National Academy of Food Technologies, Editor-in-chief

Prof. M. Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations, Editor-in-chief

Dr. S. Kotlyk, Ph.D., Assoc. Prof., Director of the P.M. Platonov Educational-Scientific Institute of Computer Systems and Technologies “Industry 4.0”, Editor-in-chief

O. Sokolova – Senior Lecturer of the Department of Advanced and Applied Mathematics, ONAFT, Technical Editor

Black Sea Science 2020: Proceedings of the International Competition of Student Scientific Works. Information Technology, Automation and Robotics. / Odessa National Academy of Food Technologies; B.Yegorov, M. Mardar, S.Kotlyk (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2020. – 365 p.

These materials of International Competition of Student Scientific Works «Black Sea Science 2020» contain the works of the contest participants in the section «Information technologies, automation and robotics» (not winners).

The author of the work is responsible for the accuracy of the information.

Organizing committee:

Prof. Bogdan Iegorov, D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

Prof. Stefan Dragoev, D.Sc., Vice-Rector for Scientific Work and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Mircea Bernic, Dr. habil., Vice-Rector for Scientific Work of Technical University of Moldova (Moldova)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Dr. Mei Lehe, Ph.D., Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Prof. Plamen Kangalov, Ph.D., Vice-Rector for Academic Affairs of “Angel Kanchev” University of Ruse (Bulgaria)

Dr. Alexander Sychev, Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

Dr. Hanna Lilishentseva, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

Prof. Heinz Leuenberger, Ph.D., Professor of the Institute of Ecopreneurship of University of Applied Sciences and Arts (Switzerland)

Prof. Edward Pospiech, Dr. habil., Professor of the Institute of Meat Technology of Poznan University of Life Sciences (Poland)

Prof. Lali Elanidze, Ph.D., Professor of the Faculty of Agrarian Sciences of Iakob Gogebashvili Telavi State University (Georgia)

Dr. V. Kozhevnikova, Ph.D., Senior Lecturer of the Department of Hotel and Catering Business of Odessa National Academy of Food Technologies, Secretary of the Committee

The jury for the section «Information technologies, automation and robotics»

Head of the jury:

Serhiy Kotlyk – Ph.D., Associate Professor, Director of the P.M. Platonov Educational-Scientific Institute of Computer Systems and Technologies “Industry 4.0” of Odessa National Academy of Food Technologies

Members of the jury:

Francisco Augusto – Dr., International Relations Manager of Higher Institute of Information and Communication Technologies (Angola)

Andrey Kuprijanov – Ph.D., Associate Professor of the Department of Software for Computers and Automated Systems of Belarusian National Technical University (Belarus)

Simon Milbert – Vice-President of Xtra Information Management, Inc. (USA)

Ivan Palov – D.Sc., Professor of University of Ruse “Angel Kanchev” (Bulgaria)

Gerard H. Degla – Communications and Training Manager of “MAPCOM solutions informatiques” company group (Benin)

Viktor Khobin – D.Sc., Professor, Head of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies

Valerii Levinskyi – Ph.D., Associate Professor of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies

Viktor Yehorov – Ph.D., Supervisor of the Laboratory of Mechatronics and Robotics of Odessa National Academy of Food Technologies

Valeriy Plotnikov – D.Sc., Professor, Head of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Pavlo Lomovtsev – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Yurii Kornienko – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Sergii Artemenko – D.Sc., Professor, Head of the Department of Computer Engineering of Odessa National Academy of Food Technologies

Serhii Shestopalov – Ph.D., Associate Professor of the Department of Computer Engineering of Odessa National Academy of Food Technologies

Secretary of the jury:

Oksana Sokolova – Senior Lecturer of the Department of Advanced and Applied Mathematics of Odessa National Academy of Food Technologies

AUTOMATIC CONTROL SYSTEM FOR TWO-MASS POSITION ELECTRIC DRIVE Author: Mykola Olieinikov Supervisors: Volodymyr Osadchy, Olena Nazarova	135
3D-MODELING OF THE INTERIOR OF THE ROOMS BY CLOUD TECHNOLOGIES Author: Olena Tsybulnyk Supervisor: Svitlana Berezenska	148
RESEARCH AND IMPROVEMENT OF 3D PRINTING WITH ABS PLASTIC USING FDM TECHNOLOGY Author: Daniil Kotlyk Supervisor: Iryna Muntian	160
ANALYSIS OF RELEVANCE OF DEVELOPMENT OF INFORMATION RESOURCE OF WORKFLOW PLANNING FOR BUSINESS ADMINISTRATORS Author: Dmytro Balaban Supervisor: Tatiana Kostirenko	170
IMPROVEMENT OF THE METHOD OF IMPROVING THE INFORMATION SECURITY OF THE INFORMATION AND TELECOMMUNICATION SYSTEM Author: Yana Kmetiuk Supervisor: Volodymyr Barannyk	177
INFORMATION ENTROPY AND FREEDOM OF CHOICE Authors: Maksym Rohach, Mariia Boitsova, Nadiia Bondar Supervisor: Valeriy Shvets	188
CREATION OF INFORMATION TECHNOLOGIES BY THE MULTIMEDIA TRAINING COMPLEX FOR TEACHING STUDENTS OF THE 5TH GRADES OF THE BASICS OF ALGORITHMIZATION AND PROGRAMMING Authors: Anastasiia Khmil, Kateryna Prytkova Supervisors: Iryna Khoroshevska, Iryna Morkvian	197
AUTONOMOUS SOIL MOISTURE MEASUREMENT SYSTEM WITH WIRELESS DATA TRANSMISSION Author: Daniil Smirnov Supervisor: Volodymyr Palahin	211
ONE SEARCH ENGINE BUILT ON A GIVEN DATABASE WITH JSON Authors: Tchanturia Salome, Anjafaridze Besarion, Todria Ucha Supervisor: Kereselidze Nugzar	225
THE USE OF SUPERVISED LEARNING IN ROBOTICS Author: Sophia Serdyuk Supervisor: Maryna Malakhova	235
THE ALGORITHM OF INFORMATION SECURITY RISK ASSESSMENT BASED ON FUZZY-MULTIPLE APPROACH Author: Nataliia Romashchenko Supervisor: Olexander Shmatko	242

**IMPROVEMENT OF THE METHOD OF IMPROVING THE
INFORMATION SECURITY OF THE INFORMATION AND
TELECOMMUNICATION SYSTEM**

Author: Yana Kmetiuk

Supervisor: Volodymyr Barannyk

Ivan Kozhedubi Kharkiv National University of the Air Force (Ukraine)

***Abstract.** The relevance of the topic of identification of a person due to the active informatization of society and an increase in the flow of confidential information. The analysis of modern methods of improving information security shows the obvious movement towards biometric methods due to their convenience, reliability and reliability.*

The task of scientific work is to investigate methods of improving information security.

The research methodology was used. The methods of text analysis based on semantic differential and the method of phonetic analysis of semantic component were used.

It is revealed that the creation of an information security system using biometric methods of user identification will reduce the impact of the "human" factor, which will increase the efficiency of identification and authentication procedures. It is proposed to increase the efficiency of the system to protect information using a steganographic method.

***Keywords:** biotechnology, identification, authentication, verification, access systems, template, mapping, data warehouse.*

I Introduction

Enterprises of different industries have to operate in conditions of high complexity, uncertainty and dynamic environment. There is an urgent need to create not only a single information space, but also an adequate mechanism for organizing information security. This activity is of particular relevance at the present stage, when various forms of hostile competitive influence are being disseminated. Equally important is the provision of information security at the country level.

In today's society, information has become one of the most important strategic resources for further development of the enterprise. That is why information, like other resources, needs special protection. The problem of information security has become especially important in the current context of the widespread use of automated information systems. In view of the growing role of information resources in the life of modern society, as well as the reality of numerous threats, the problem of information security requires constant and considerable attention. The implementation of the latest automation and communication tools require faster and more reliable means and methods of protecting information. Therefore, the use of steganography techniques is necessary to protect information in today's world.

In this paper, information security enhancement methods will be discussed and compared. An analysis of their advantages and disadvantages, the principle of operation, the main characteristics and the best method will be highlighted.

II Analitic review of literature

BIOMETRICS. BASIC METHODS OF DATA RECOGNITION

Biometrics is a collection of automated methods and means of identifying a person based on their physiological or behavioral characteristics.

There are two methods of data recognition: static and dynamic methods.

Static methods:

- fingerprint;
- in the form of a palm;
- the location of the veins on the back of the palm;
- behind the retina;
- behind the iris;
- by face shape;
- by the thermogram of the person;
- DNA;
- using other methods.

Dynamic methods:

- take into account the peculiarities of subconscious movements;
- in handwriting;
- by keyboard handwriting;
- by voice;
- other methods.

To evaluate the performance of a biometric system, there are characteristics that can be easily quantified to determine the reliability of the systems created [1].

These characteristics are accompanied by the presence of errors of the first and second kind. Denoted as FRR (False Rejection Rate) - the probability of a mistake of the first kind, that is, the probability of rejecting "one's own".

$$FRR = \frac{NFR}{NAA} \times 100\% , \quad (1.1)$$

where NFR is the number of false deviations;

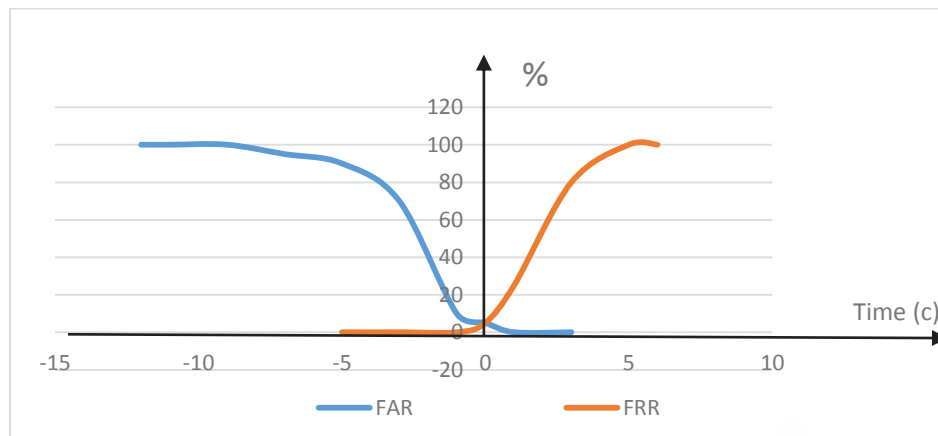
NAA is the time of false deviation.

A second kind of error occurs when comparing "alien" to "alien" when "alien" recognizes "own". Denoted as FAR (False Acceptance Rate) - the probability of a second kind of error, that is, the probability of missing another.

$$FAR = \frac{NFA}{NIA} \times 100\% , \quad (1.2)$$

where NFA is the false approval number;

the NIA is a time of false rejection.



To determine the efficiency of the biometric system is a graph FAR, FRR.

For example, to obtain first-order error statistics, it is necessary to compare pairs of patterns in a single row in order to provide one-to-one comparisons. If the first pattern in a row is compared with all other prints of a row, it turns out $(m - 1)$ comparisons; compare the second pattern in a row with all the patterns that follow it, since it has already been compared to the first pattern, we get a $(m - 2)$ comparison, etc. The penultimate pattern is only compared to the last pattern, one comparison is obtained. Thus, the number of comparisons in the series will be:

$$V_i = \frac{m(m-1)}{2}, \quad (1.3)$$

where m is the number of templates in the database.

To obtain second-order error statistics, comparisons are made in pairs between templates of different rows, to provide comparisons of type "alien" to "alien." the second row of the first row is also compared and more $(n - 1) \times m$ comparisons are obtained. After comparing the first row m patterns with all the other row patterns, we get $m^2 (n - 1)$ comparisons.

The second row templates are compared to the patterns of all $(n - 2)$ rows after it, since they have already been compared to the first row prints, there are still $m^2 (n - 1)$ comparisons. This procedure is carried out to the penultimate row, which is compared only with the only one, the last, close, and there are still m^2 comparisons. This means that the number of possible comparisons of "alien" to "alien" in the base of n samples of m templates each will be:

$$VFAR = \frac{m^2 n(n-1)}{2}, \quad (1.4)$$

where n is the row number.

The use of this method allows to obtain a sufficiently large number of variants of comparisons needed to build characteristics with incomparably smaller amounts of templates in the database [2].

PROSPECTS FOR THE DEVELOPMENT OF BIOMETRIC MARKET AND DIFFERENT TYPES OF BIOMETRIC AUTHENTICATION AND IDENTIFICATION TECHNOLOGY

Biometrics are rapidly acquiring industrial features. The need for standardization and unification is increasing in the world market; Competition is intensifying, mergers and acquisitions are being activated. However, despite the existing differences in the prospective estimation of the volume of the world biometric market, all research and consulting firms believe that the general tendency for further growth of the biometric market will be maintained.

Recent developments in new biometric technologies may have very accurate recognition properties, but at the same time they will require additional data to confirm their uniqueness.

Another fairly significant aspect is how simple ("comfortable") each technology is. The process should be quick and easy, such as standing in front of your camcorder, saying a few words into the microphone, or touching the space in the fingerprint scanner. The main requirement for biometric technologies, which is their major advantage, is quick and easy identification without causing any inconvenience to humans.

Regarding segmentation of the industry market, experts were unanimous in their conclusions that the most popular were and remain systems that implement fingerprint and face identification technologies; third and fourth places share solutions based on the recognition of users by vein pattern and voice.

In the coming years, three major biometrics (fingerprint, face, iris) technologies will retain dominant positions, but overall their share will decline. However, it is assumed that the popularity of rainbow technology will give way only to the popularity of fingerprint identification, and third or fourth place in popularity may come methods of identification of a person by voice.

But the question is: what kind of biometric identification technology is better? It all depends on the specific scope of its application. For example, identification of a person in complete darkness (if necessary) is better done by voice, and techniques using fingerprints are used [3].

The dynamics of growth of the world biometric market, from 2007 to 2018, is shown in Fig. 2.1.

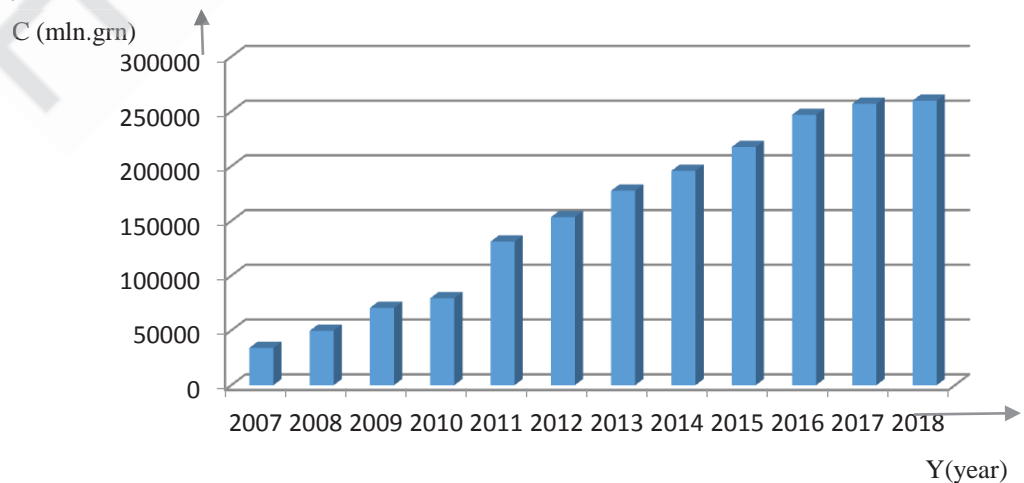


Figure 2.1 - Dynamics of the global biometric market

III Object, subject and methods of research

The scientific and applied task is to increase information security with respect to demarcated access to information resources.

The purpose of the work is to develop an identification method using image hiding methods.

The object of the study - methods of improving information security.

Research Methods - Determine the most effective method of enhancing information security.

IV Work results

PROBLEMS OF FACE IDENTIFICATION BASED ON THE IRIS Iris Identity has a very high degree of reliability and accuracy, but there are a number of problems. First of all, it is the change in the size of the pupil as the lighting level changes. The rest of the problems are related to the features of the human eye structure and are shown in Fig. 3.1.

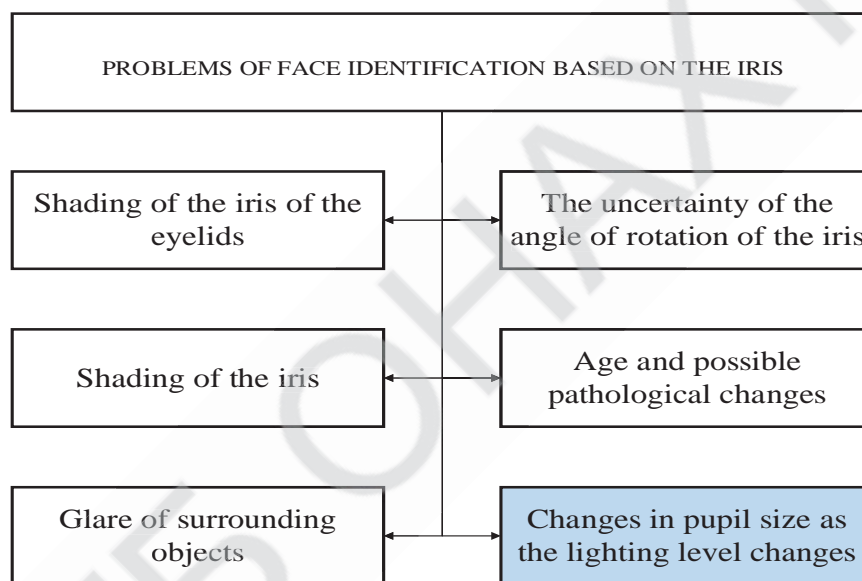


Figure 3.1 - Iris-based identification problems

- shading of the cornea eyelids. This problem can be solved with a special algorithm for searching the eyelids or rejecting parts of the image when comparing consecutive frames;

- shading of the cornea with lashes sticking down. The algorithm of search of eyelids on such pictures works successfully and with great confidence, the area allocated to it, is not suitable for recognition. The problem can be solved by the algorithm of rejecting the sequence of images. The cornea and eyelids with the eyelashes move relative to each other, so those parts of the image where the eyelashes and eyelids hang over the cornea are constantly changing (the eyelashes alternately close different parts of the cornea). On the contrary, the corneal open areas in the normalized image are relatively stable;

- glare from surrounding objects on the cornea. The cornea acts as a spherical mirror, reflecting the outside world. These reflections (especially reflections of light sources, patches of sunlight and areas of the daytime sky) can be several times brighter and more completely suppress corneal details. To solve this problem, high intensity in the narrow area of the illumination spectrum is used (far exceeding the solar illumination, most often use infrared radiation) and image registration in the same area of the spectrum;

– different size of pupil under variable shooting conditions. As noted above, the affine transformation of the corneal image to a standard size solves this problem only in the first approximation, since the corneal stretch obeys a nonlinear, too complicated law. To solve this problem, it is suggested, for example, to remember the size of the human pupils when registering in the system, and to recognize the accommodation (expansion or narrowing) of the pupils to this size by manipulating the brightness of a special visible light source;

– pathological and age-related changes. The cornea very clearly reflects the state of the body, including various pathologies (diseases, injuries, poisoning). In this regard, the question arises about the stability (over time) of the recognition of the object subject to these changes. However, there are a significant number of birthmarks and signs that remain unchanged throughout the life of the cornea. It is almost impossible to separate congenital and acquired traits, but even a small number of traits can be recognized by a person. The required minimum is 30%, and even so, the probability of a false tolerance does not exceed 10-64;

– uncertainty of corneal angle of rotation. There is no problem with the corneal registration system or the corneal-face combination system. For the so-called "one-eyed" system, you can determine the angle on the configuration of the eyelids, the pupil decentralization or on some important characteristic of the cornea. All of these signs may change over time. In this case, it is necessary to iterate over the angles of rotation (significantly increases the operating time of the system) or to calculate signs that are invariant to rotation (such signs are ten times less, therefore, greatly reduces the reliability of the system). In addition to all of the above biometric identification systems should be resistant to the use of fakes. For iris-based identification systems, either a corneal volumetric photograph or a mockup of the eye can be used as a fake, as well as the alienation of biometric features (in this case, a "torn" eye) [4].

There are two ways to solve this problem:

Method 1 - Corneal Reflection Spectrum. The cornea of the "living" eye is constantly moisturized, the "dead" eye quickly dries. The reflectance spectra of wet and dry corneas differ.

Method 2 is by the reaction of the eye to illumination. The pupil reacts to external stimuli (flash of light, loud sound, etc.) in a certain way and with some delay, and this reaction is controlled by the brain.

Iris scanning, electronic fingerprints and signature recognition are definitely better than the password on a piece of paper attached to the monitor. However, according to researchers, biometric information is easy to steal or copy. "In this regard, it is desirable to develop such an identification device, when working with which you would not need to make a secret of biometric data," - they say.

In an article in the International Journal of Biometrics, scientists led by Masakutsu Nishigaki and Daisuki Arai of the University of Shizuoka write that they have been able to develop an alternative method of authentication based on the unique reflex response of the human eyeball. Nishigaki and Arai use as a biometric identifier the unintentional reaction of the eyeball to an external action, measured in conjunction with the calculation of its dead zones, also called blind zones.

Blind spot is a visual projection of the optic disc. This rounded eye area of about 1.9 mm in size cannot form a visual image. Human eyes have an area of blind spot, however, due to binocular vision, the blind spot remains unnoticed, as these areas are superimposed when comparing images of the right and left eyes. Even with one eye closed, seeing a blind spot is not easy. The brain compensates for the missing visual information and the blind spot goes unnoticed. Increasing the size of the blind spot can indicate a number of eye diseases and is a diagnostic criterion in ophthalmology.

Each vertebrate eye has a dead zone where the optic nerve moves away from the retina. This visual gap is not perceived visually as the field of view of the other eye overlaps this dead zone. Scientists use this dead zone to detect eye movement. A person is shown a visual image, both within and beyond, and measures the reaction time of the eye until the moment of movement of the eyeball. Other options for using this method, such as dead man positions and pupil constriction time, are also offered.

Nishigaki especially draws attention to the fact that using only the dead zone position as an identifier is by no means safer than using a scan of the iris, since in this case it is possible to use contact lenses or even surgery.

DEVELOPMENT OF PERSONAL IDENTIFICATION METHOD USING STEGANOGRAPHIC TRANSFORMATION

The method of face recognition by iris and human eyeball response to stimuli consists of the following steps:

a) a request for an identification process, that is, to determine the identity of a person and determine his or her rights to perform certain actions. The person who wants to access the data should bring the face closer to the scanner, fix its position and look at the special mark on the scanner display. Then the camera takes pictures at a rate of ten frames per second, and the resulting images are processed by a special program. The beam incident on the curved surface is bent - the greater the curvature of the surface, the stronger the bend of the beam. Initially, a visible light source was used. Then visible light will be replaced by infrared.

b) the input of the key (password) by the person. The key is the rule for steganographic conversion of a snapshot taken by the system. The key is a certain sequence of letters / numbers known to the system, the person requesting identification, and the system administrator. With this system, the system places data on the container, so that the attacker will not know which blocks of the container are steganographically changed. User must enter 2 keys:

- the first to close information;
- second for steganographic placement in the container.

This increases the complexity of accessing the system for unauthorized users [5].

c) forming a template based on the shot. In the first stage of processing, the image is deleted, where the face is not visible at all or there are foreign objects that interfere with identification. The resulting images restores a 3-D model of the person, which stands out and removes unnecessary obstacles (hairstyle, beard, mustache and glasses). Then the model is analyzed - anthropometric features are distinguished. The pupil "circle" is selected from the general image of the eyeball and the blind areas are selected. Measures the reaction time of the human eyeball to stimuli.

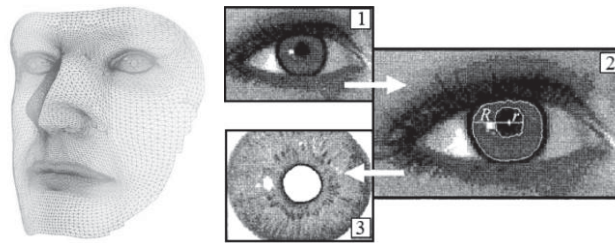


Figure 3.1 - Forming a 3-D pattern for face recognition and getting a "pupil" circle
 d) forming the contour of the image. Contours are lines that extend across homogeneous areas. The elements $z_{i, j}$ of the space-time representation of the image, the values of which do not exceed a certain threshold, form homogeneous regions. This is determined by the following condition:

$$|z_{max} - z_{min} \leq 1|, \quad (3.1)$$

where z_{max} is the element of the largest image area that is defined based on the following expression:

$$z_{max} = \max_{1 \leq i \leq x} \{z_{i,j}\} \text{ при } j = \overline{1, y}, \quad (3.2)$$

where y the allowed number of elements of the image;

z_{min} is the element of the smallest value image area is determined by the formula:

$$z_{min} = \min_{1 \leq i \leq x} \{z_{i,j}\} \text{ при } j = \overline{1, y}, \quad (3.3)$$

where 1 is the threshold for the detection of homogeneous regions.

The most common and practically applied approaches for contour detection are gradient methods. Gradient methods are based on the determination at each point of an array of values of brightness increase (gradient) and the directions of their greatest change, with further determination of maximum values of brightness gradient, their statistical processing and division into thresholds (levels).

The most common way to find outlines is to process the image with a sliding mask. It is a square matrix with coefficients. The matrix-based image processing process is filtered or masked and is given by the following functional $f(Z, K)$ (Figure 3.1):

$$M = f(Z, K), \quad (3.4)$$

where M is the image obtained by processing the image Z based on the mask K .

The filtering process is based on the gradual spatial movement of the filter mask from element to element of the image. Analysis of Figure 3.1 shows that the value of the element $m_{i,j}$ (filter response) is calculated using the values of the previous and next elements in the two-dimensional plane.

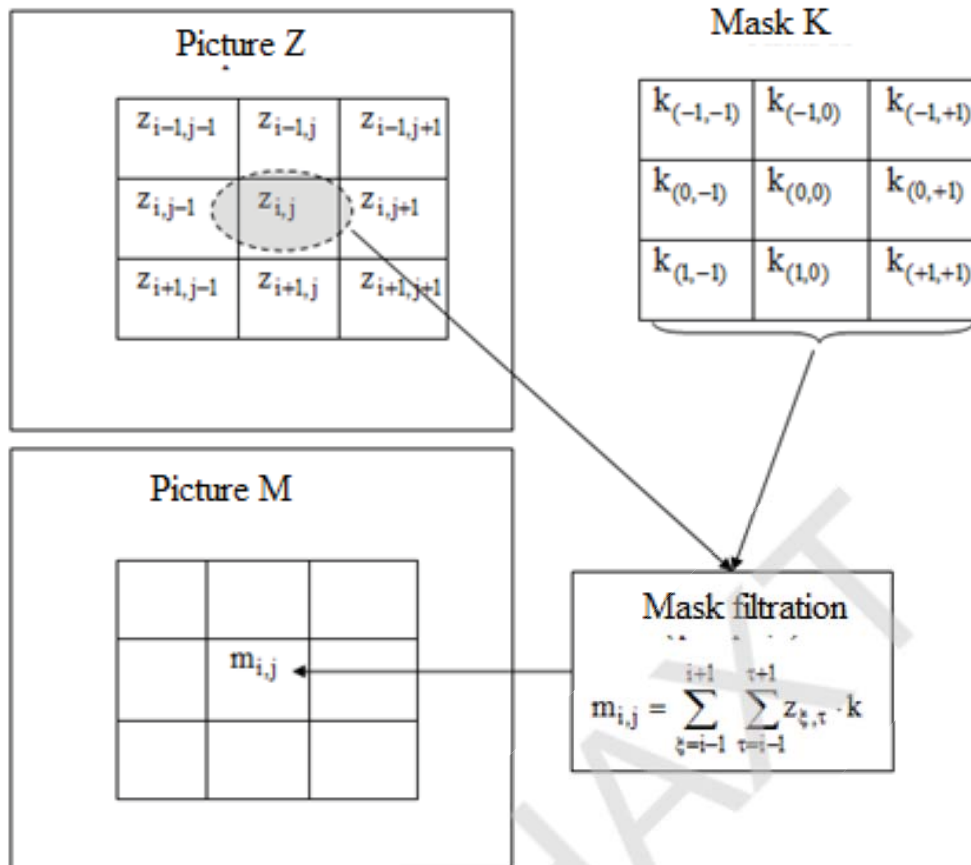


Figure 3.2— Scheme of masking an image based on a variable mask

e) embedding the data in the least significant bits (NZB) of the spatial representation of the image. The NSA is selected with the second key entered by the user in step 2. The embedding of the message occurs in the lower bit of the image, which carries the least information.

In fact, NZB is noise, so it can be used to embed a secret message. In spatial-temporal representation, image embedding is based on the properties of the 24-bit representation of the image.

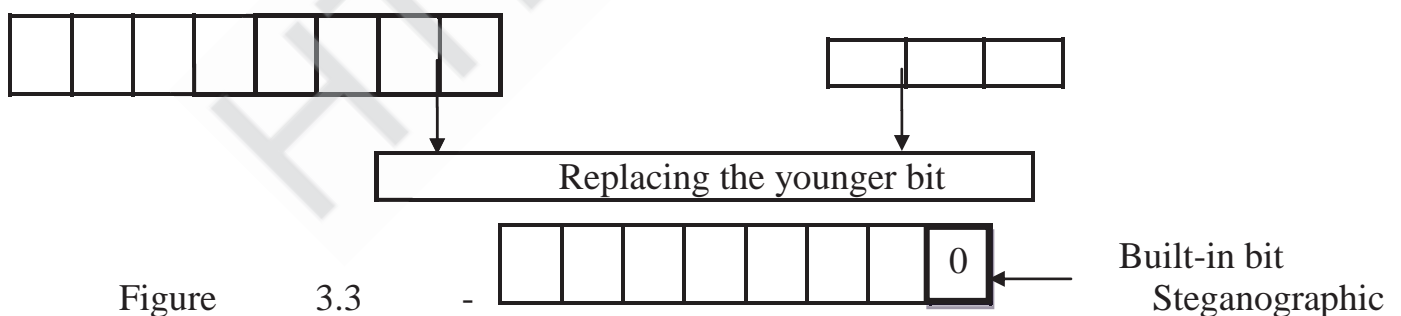


Figure 3.3 - embedding in the least significant bit

24-bit color in computer graphics is a method of presenting and saving an image that allows you to display a large number of colors, undertones and tones. Color is represented using 256 levels for each of the three components of the RGB model: red (R), green (G) and blue (B), resulting in 16 777 216 (224) different colors.

Usually, when encoding a pixel, one byte is assigned to each of the channels (red, green, blue channels); the fourth byte (if used) is usually assigned either to store alpha channel data or simply ignored.

The size of the embedded message can be 1/8 of the total volume of the container. For example, a 512x512 image can embed 32kBytes of information. If you modify the two smallest bits, the bandwidth can be doubled.

The method of embedding data in the spectral region is somewhat more complicated than embedding the message in the spatial-temporal region of the image. Embedding information occurs after a discrete-cosine transform (DCT) of the image.

The DCT coefficients (transformants) are ordered according to their importance, for example according to the contribution to information content, so that transformants with small information content can be omitted (discarded). Other transformants are quantized, coded and transmitted or memorized. The importance of coefficients can be compared, for example, visually (subjectively), according to their contribution to the picture of the brightness of the reconstructed image on the display; thus, you can work around the issue of image element correlation and evaluate the result of compression. The archiving is considered to be excellent, in which it is impossible to distinguish between the original and unpacked (restored) image on the eye, good - when the difference is visible only for a number of these images. With further increase in the degree of compression, as a rule, there are noticeable side effects characteristic of the compression algorithm used.

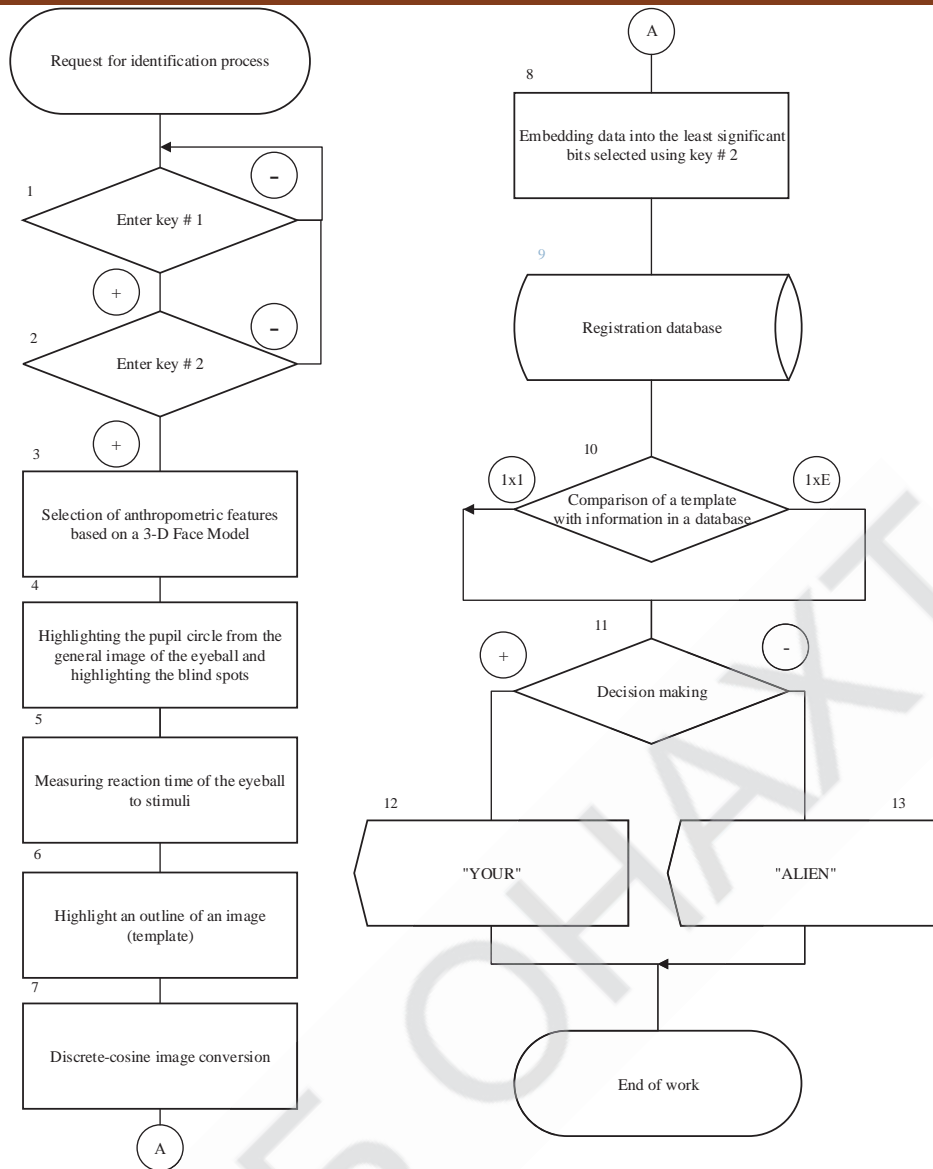
The embedding is done by bit: one bit of information into one value of the low-frequency DCT factor. For this purpose, information bits are transformed into polar form.

e) sending a steganographically converted image to the database. Each biometric system has a storage subsystem - a registration database that serves to store templates.

g) comparison of the template with the information in the registration database. The resulting verification template is compared with the stored one to determine if these patterns match. This technology uses the user's installation data (keys entered by the user) as a pointer to retrieve the stored subscriber's account and verify one-to-one (authentication or verification) between the template or one-to-many received during verification biometric parameters, and a template that already exists for that username. Otherwise (identification procedure), the biometric metric parameter template that is being presented is compared to the entire set of stored templates.

g) decision making by the system ("one's own" / "another's").

Scheme of operation of the iris identification system and the response of the human eyeball to stimuli using steganographic transformation:



V List of references

1. Barannik V. Steganographic Method Based On The Modification Of Regions Of The Image With Different Saturation/ V. Barannik, A. Lekakh, A. Bekirov, D. Barannik / Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (S5). – 2018. – p. 81-85.
2. Wang J. Electronics, electrical Engineering and Information Science / J. Wang, L. Xiaolong — World Scientific, 2015 — 210 p.
3. Nyadets T. Biometrics: strengths and weaknesses. Monograph / T. Hnidets, N The hum. - L.: Lviv State University of Internal Affairs, 2014. - 326 p.
4. Moroz A. Biometric technologies for human identification. Systems overview. Monograph / A. Moroz, K. Chernov. - K: Peter, 2016 - 184 p.
5. Kmetyuk Y. A method of increasing the efficiency of delimiting access to automated special purpose control systems / Y. Kmetyuk, M. Parkhomenko, V. Dimchuk, D. Zhuykov // Radio electronics and informatics. - 2019. №4 (87). Kh.: KNURE, 2019.