«Наука и образование: новое время» № 2, 2022

РАЗРАБОТКА И ИССЛЕДОВАНИЕ БИОМЕТРИЧЕСКИХ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Курмашев О.О.

Казахский Агро-Технический Университет им. С. Сейфуллина

Республика Казахстан, г. Нур-Султан

E-mail: qrmashev@gmail.com

Аннотация. Статья раскрывает значение биометрии, ее типы и методы как средство защиты информационных данных. В статье рассматривается разработка метода распознавания формы лица для отображения в веб-ресурсе, рассмотрены возможности фаз идентификации (авторизации, аутентификации).

Ключевые слова: биометрия, распознавание, идентификация, клиент-пользователь, хранилища данных.

DEVELOPMENT AND RESEARCH OF BIOMETRIC METHODS AND MEANS OF INFORMATION PROTECTION

Olzhas O. Kurmashev

Kazakh Agrotechnical University named after Saken Seifullin,

Kazakhstan, Nur-Sultan

E-mail: qrmashev@gmail.com

Abstract. The article reveals the importance of biometrics, its types and methods as a means of protecting information data. The article discusses the development of a facial shape recognition method for displaying in a web resource, the capabilities of identification phases (authorization, authentication) have been reviewed.

Keywords: biometrics, recognition, identification, user client, data warehouses.

Цель работы – исследование биометрии, которая позволит проработать механизм в качестве разработки защиты информации для дальнейшего улучшения сбора хранилища данных.

Объект исследования – процедура идентификации пользователя для входа в хранилища данных.

Предмет исследования – биометрические методы аутентификации и средство защиты информации.

Work objective is to study biometrics, which will allow working out a mechanism as an information security tool for further improving the collection of data storage.

Research object is the user identification procedure for logging onto data warehouses.

Research subject is biometric authentication methods and a means of information protection.

Почти каждый Клиент-пользователь личного устройства (смартфон, планшет) имеет возможность распознавания голоса, отпечатка пальца, формы лица. Это говорит о том, что в условиях стремительного развития технологий люди доверяют разработчикам свои собственные данные для улучшения новых версий смартфонов, браузеров и многих других технологий, где доступны методы распознавания биометрии.

Безопасное хранение данных допустимо при соответствующей фазе авторизации Клиента-пользователя. После этого не понадобится повторно вводить электронный адрес, номер телефона, проходить проверку двухфакторной аутентификацией, что сокращает время, трафик, а главное упрощает вход в базу данных хранилища. Для проникновения злоумышленников понадобятся немалые усилия. Это гарантирует безопасность для клиентов-пользователей.

В нашем мире не существует похожих людей, животных, так как на генетическом уровне по всем признакам они – разные организмы, непохожие друг на друга. Именно распознавание живого объекта имеет весомый аргумент, можно вычислить цвет, размер, температуру, а при длительной съемке и сканировании изображения можно рассчитать действие объекта, количество объек-

тов, состояние объекта. Проводимый анализ поможет в будущем прогнозировать человеческие факторы для удовлетворения потребности в экономии запасов и, в лучшем случае, улучшения системы потребления, в зависимости от места и отрасли ее применения. Развитие технологий распознавания живых объектов (биометрии), в особенности неживых объектов, актуальна. К неживым относится геолокация, астрономические объекты. Ученые подтверждают, что количество любого живого или неживого объекта будет отличаться по типу схожести. Количество населения Земли равно 7 миллиардам, а количество звёзд неизвестно. Известно то, что астрономические объекты не имеют никакой схожести по многим факторам, даже если есть хоть какая-то малейшая схожесть, то она мала, и не превышает 5%, так и с населением людей на Земле.

Биометрические методы

Известно, что биометрия делится на два вида: статические и динамические процессы распознавания. К статическим относится:

- форма лица,
- сетчатка глаза,
- форма ладони,
- отпечаток пальца,
- ДНК
- рисунок вен.

К динамическим относится:

- походка,
- речь,
- голос.

Самое интересное, что данные методы были ранее известны, еще до появления биометрии, ее четко описали в научно-фантастических книгах, в массовой культуре, в разных жанрах фильмов, глянцевых журналах и в других популярных источниках. Например, очень ярко описывают биометрию в фильме "Миссия невыполнима", где спецагенты взламывают систему с помощью физи-

ческого копирования отпечатка пальцев на пластилиновую поверхность, приложив слепок пальцеобразной формы на считыватель сканирования, походку человека отбором копирования похожих людей по весу и росту, а вот для проверки сетчатки глаз уже понадобился взлом базы данных для проникновения, внесение соответствующих корректив в базу пользователей для доступа к хранилищу данных. Во многих похожих источниках в жанре научной фантастики данные системы также не стали исключением.

Первый метод в биометрии – это отпечаток пальца. Еще раньше для криминалистов было проще находить преступников по совпадению отпечатков пальцев на месте преступления. Фактом является то, что после отбора подозреваемого, схожесть была равна 98-99%, но ученые до сих пор не доказали и не обосновали саму теорию дактилоскопического способа. Отпечатки можно спокойно подделать. Метод распознавания формы руки относится к дактилоскопическому способу вычисления. Английского основателя, выдвинувшего гипотезу еще в 1877 году «О неизменности папиллярного рисунка ладонных поверхностей кожи человека», звали Уильям Гершель.

Для обхода системы распознавания нужен грим или различные пластические операции, а солнцезащитные очки или головной убор вовсе недопустимы, так как снижают точность распознавания, по крайней мере надетая медицинская маска распознается, ведь основной содержательной частью лица являются глаза. Также могут повлиять на распознавание биометрических данных малые физические изменения в ракурсе. Deep Fake – технология машинного обучения (Machine learning), обманывает сканер отпечатка пальцев и выдает себя за чужое лицо. Deep Fake или, как его еще называют Deep Learning, опасен подделками реальных людей на видео, созданием многочисленных аудио сообщений благодаря нейронной сети, генерирующей подделку материала даже в транслируемом онлайн режиме. Биометрия считывается на основе некоторых алгоритмов, таких как Алгоритм Виолы-Джонса, Сверточной нейросети и Гистограм-

мы направленных градиентов. Каждый из алгоритмов по-своему особенный и годен для разработки безопасной платформы.

Алгоритм Виолы-Джонса представляет собой распознавание изображения в реальном времени. Данный метод разработан Паулом Виолой и Майклом Джонсоном в 2001 году. Основной задачей при его создании было обнаружение лиц.

Алгоритм Сверточной Нейросети работает в реальном времени и производит поиск на рисунке изображения для сходства объекта или нескольких объектов. При регулируемом движении объектов алгоритм производит сетку, на которой находит схожую разметку. Процесс изначально производит свертку путем фильтрации, таким образом на рисунке закрашивается в числовое значение 1, а какую-то часть в 0. Фильтрация свертки происходит по нескольку раз, то есть до фильтрации коэффициенты между собой перемножаются для конечного результата целой финальной сетки-матрицы рисунка. В конечном итоге получаем – “вектор”.

Алгоритм Гистограммы направленных градиентов – это дескрипторы особых точек, которые применяются в компьютерном обучении, обработка изображений с целью распознавания объектов. Данная техника основана на подсчете количества направлений градиента в локальных областях изображения. Метод отличается от предыдущих методов тем, что вычисляется на плотной сетке равномерно распределенных ячеек и использует нормализацию перекрывающегося локального контраста для увеличения точности.

Разработка функции распознавания формы лица

Благодаря OpenCV, библиотеке алгоритмов компьютерного зрения и обработки изображения, нам удается заполучить, то самое распознавание, которое мы программируем на языке Python, JavaScript, Matlab. Библиотека разработана компанией Intel на языках C и C++.

Машинное обучение на основе библиотеки TensorFlow, разработанная Google, где пользователям была предоставлена возможность создавать продукт

распознавания посредством биометрических методов. Данная библиотека разработана на языке Python, C++, CUDA. Для подключения данной технологии потребуется веб-камера. Смотреть результат ниже на рис. 1.

Первоначально создаются файлы .py в среде программирования PyCharm. Отобразить процесс поможет создание DNS – локального сервера (призываем на языке Django). Также с помощью Терминала (с подключением Django) возможно создавать файлы, как .html, .css, .js на языке программирования Python. Скрипт tfjs (tensor flow) написан на JavaScript и предназначен для языка гипертекстовой разметки таким образом:

- <script src="https://cdn.jsdelivr.net/npm/@tensorflow/tfjs"></script>

Скрипт blazeface или facemesh модели машинного обучения предназначены для быстрого определения лиц и ключевых точек:

- <script src="https://cdn.jsdelivr.net/npm/@tensorflow-models/blazeface"></script>

Локальный сервер служит общей связью файлов для отображения веб-файла, а также загрузки и выгрузки файловых данных. Особо значимые файлы .js играют важную роль в биометрии, ведь без него он не будет работать.

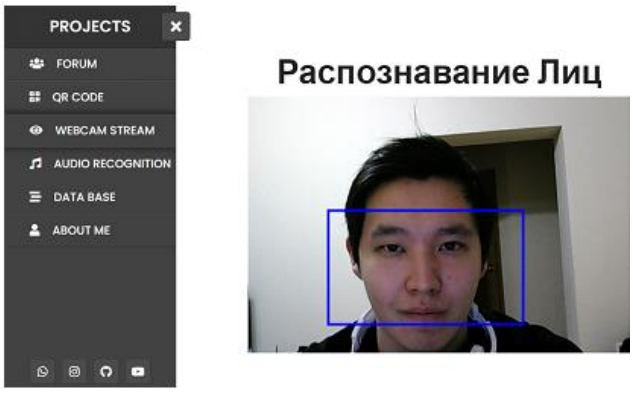


Рисунок 1. Изображение функции распознавания формы лица в реальном времени

Как сообщалось ранее, данная функция распознавания формы лица, может распознавать лица с надетыми головным убором, медицинскими масками, а солнцезащитные очки или маски, закрывающие лица не могут быть распознаны.

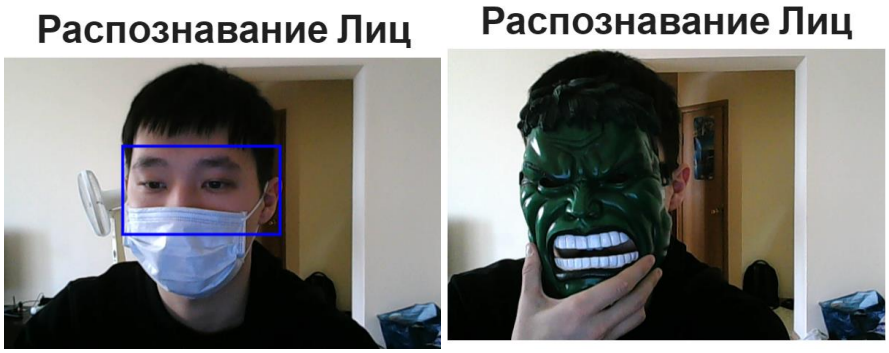


Рисунок 2. Сравнение функции распознавания лица в полузакрытой и закрытой части лица

Архитектура создания биометрии в визуальном режиме заняла небольшое количество времени. Для создания Базы данных была построена система архитектуры:

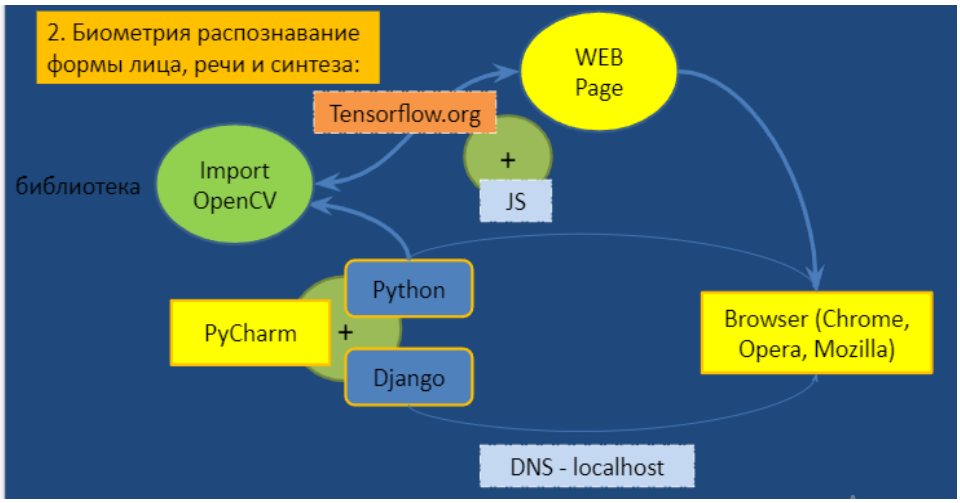


Рисунок 3. Архитектура создания биометрии

Список использованной литературы

1. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Из-во Пензенского государственного университета, 2000. – 188 с.

2. Иванов А.И. Компьютер Вас узнает / А.И. Иванов, И.А. Сорокин, С.Н. Шумкин // Безопасность, достоверность, информация (БДИ). – № 1. – 996. – С. 18-21.

3. Барсунов В.С. Биометрическая защита информации // Защита информации. Конфидент.- 2000. – № 1. – С. 45-52.

4. Тельных А. Идентификация личности. Как это делается / А. Тельных, А. Коган. // Компьютерра. – 1999. – №10. – С. 39-41.

5. Уиллес Д. Шесть биометрических устройств идентификации отпечатков пальцев. / Д. Уиллес, М. Ли. // Сети и системы связи. – 1998. – №9(31). – СЛ46-155.
6. Уиллес Д. Пусть Ваши пальцы зарегистрируются сами // Сети и системы связи. – 1998. – №9(31). – С. 156-160.
7. Филлипс П. Дж. Введение в оценку биометрических систем / П. Дж. Филлипс, Э. Мартин, С.Л. Пржибоски // Открытые системы. – 2000. – №3. – С. 21-27.
8. Пентланд А. Распознавание лиц для интеллектуальных сред. /А. Пентланд, Т. Чаудхари, // Открытые системы. – 2000. – №3. – С. 28-33.
9. Белоцерковский О.М. Компьютерное распознавание человеческих лиц. /О.М. Белоцерковский, А.С. Глазунов, В.В. Щенников // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. – 1997. – №8. – С. 3-14.
10. Глазунов А. Компьютерное распознавание человеческих лиц // Открытые системы. – 2000. – №3. – С. 43-47.

Курмашев Олжас Ойратович – студент, Казахский Агро-Технический Университет им. С. Сейфуллина
Республика Казахстан, 010000, г. Нур-Султан ул. Т. Бигельдинова, 6
Kurmashev Olzhas Ayratovich – student, S. Seifullin Kazakh AgroTechnical university
Republic of Kazakhstan, 010000, Nur-Sultan, T. Bigeldinov street, building 6

Introduction

Almost every user client engaging with a personal device (smartphone, tablet) has the capability to recognize voice, fingerprint, facial shape. This suggests that with the rapid development of technology, people entrust developers with their own data to improve new versions of smartphones, browsers and many other technologies, which enable biometric recognition methods.

Safe storage of data is allowed at a corresponding phase of a user client authorization. After that, one does not need to re-enter the email address, phone number, pass a two-factor authentication check, which saves time, traffic, and, most importantly, simplifies logging onto the data warehouse database. It will take a lot of intruders' efforts to infiltrate. This guarantees security for user clients.

In our world, there are no similar people, animals, because at the genetic level, according to all signs, they are different organisms, unlike each other. It is the recognition of a living object that has a weighty argument, you can calculate the color, size, temperature, and with long-term shooting and image scanning, you can calculate the action of the object, the number of objects, the state of the object. The analysis carried out will help in the future to predict human factors to meet the need to save stocks and, at best, improve the consumption system, depending on the place and industry of its application. The development of technologies for recognizing living objects (biometrics), especially non-living objects, is relevant. The non-living include geolocation, astronomical objects. Scientists confirm that the amount of any living or non-living object will differ in the type of similarity. The population of the Earth is 7 billion, and the number of stars is unknown. It is known that astronomical objects have no similarity in many factors, even if there is at least some slightest similarity, then it is small, and does not exceed 5%, and the same goes with the population of people on the Earth.

Biometric methods

It is known that biometrics is divided into two types: static and dynamic recognition processes. The static ones are:

- face shape,
- retina,
- palm shape,
- fingerprint,
- DNA
- pattern of veins.

The dynamic ones are:

- gait,
- speech,
- voice.

The most interesting thing is that these methods had been previously known, even before the advent of biometrics, it was clearly described in science fiction books, in popular culture, in various genres of films, glossy magazines and in other popular sources. For example, the biometrics is very vividly described in the movie "Mission Impossible", where special agents hack into the system by physically copying a fingerprint onto a plasticine surface, attaching a finger-shaped impression to a scanning reader, a person's gait by selecting copies of similar people by weight and growth, but to check the retina of the eye, it already took a database hack to penetrate, making appropriate adjustments to the user database to access the data warehouse. In many similar sources in the science fiction genre, these systems are also no exception.

The first method in biometrics is a fingerprint. Even earlier, it was easier for forensic scientists to find criminals by matching fingerprints at the crime scene. The fact is that after the selection of the suspect, the similarity was 98-99%, but scientists still have not proven and substantiated the very theory of the fingerprint method. They can be easily faked. The hand shape recognition method refers to the fingerprint calculation method. William Herschel, an Englishman, who put forward a hypothesis back in 1877 "On the invariability of the papillary pattern of the palmar surfaces of human skin", is considered its founder.

To bypass the recognition system, make-up or various plastic surgeries are needed, and sunglasses or a hat are completely unacceptable, as they reduce recognition accuracy, at least a medical mask worn is recognized, because the main meaningful part of the face is the eyes. Small physical changes in perspective can also affect the recognition of biometric data. Deep Fake is a machine learning technology that deceives the fingerprint scanner and impersonates some other person. Deep Fake or, as it is also called Deep Learning, is dangerous by the possibility of creating fakes of real people on videos, also by creating numerous audio messages thanks to a neural network that generates fake material even in broadcast online mode. Biometrics is read based on some algorithms such as Viola-Jones Algorithm, Convolutional Neural

Network and Directional Gradient Histograms. Each of the algorithms is special in its own way and suitable for developing a secure platform.

The Viola-Jones algorithm is a real-time image recognition. This method was developed by Paul Viola and Michael Johnson in 2001. The main task in its creation was the detection of faces.

The Convolutional Neural Network algorithm works in real time and searches for an image in the whole picture for the similarity of an object or several objects. With the controlled movement of objects, the algorithm produces a grid, on which it finds a similar markup. The process initially performs convolution by filtering, so in the figure it is painted over with a numerical value of 1, and some part with 0. Convolution filtering occurs several times, that is, before filtering, the coefficients are multiplied among themselves for the final result of the entire final grid-matrix drawing. In the end, we get – a "vector".

The algorithm of Histograms of directional gradients are descriptors of singular points that are used in computer learning, image processing for the purpose of object recognition. This technique is based on counting the number of gradient directions in local areas of the image. The method differs from previous methods in that it is computed on a dense grid of uniformly distributed cells and uses overlapping local contrast normalization to increase accuracy.

Development of facial shape recognition function

Thanks to OpenCV, a library of computer vision and image processing algorithms, we are able to obtain the very recognition that we program in Python, JavaScript, Matlab. The library was developed by Intel in C and C++.

Machine learning based on the TensorFlow library developed by Google, where users were given the opportunity to create a recognition product through biometric methods. This library is developed in Python, C++, CUDA. To connect this technology, you need a webcam. See the result below in pic. 1.

The .py files are initially created in the PyCharm programming environment. The creation of a DNS - a local server (we summon it in the Django language) will

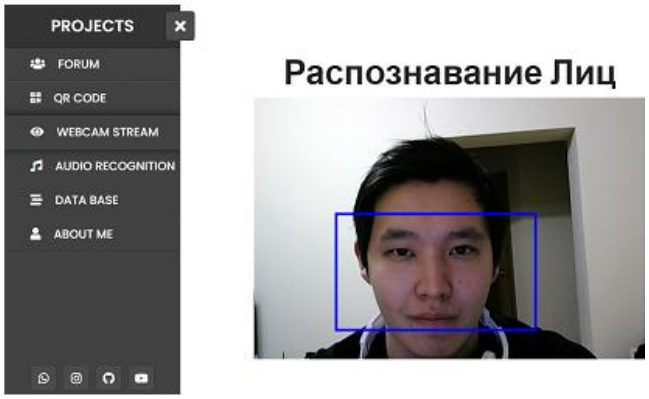
help to display the process. Also, using the Terminal (with Django connection) it is possible to create files like .html, .css, .js in the Python programming language. The tfjs (tensor flow) script is written in JavaScript and is intended for hypertext markup language in this way:

● <script src="https://cdn.jsdelivr.net/npm/@tensorflow/tfjs"></script>

Script blazeface or facemesh machine learning models are designed to quickly identify faces and key points:

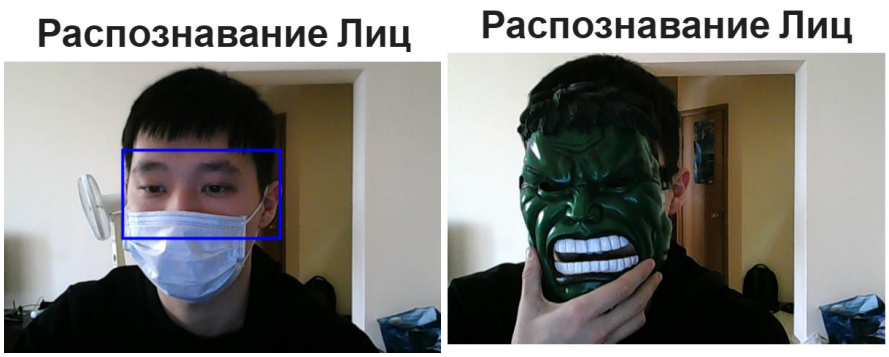
● <script src="https://cdn.jsdelivr.net/npm/@tensorflow-models/blazeface"></script>

The local server serves as a shared file link for displaying a web file and uploading and downloading file data. The especially important .js files play an important role in biometrics because it won't work without it.



Picture 1. Real-time facial shape recognition function image

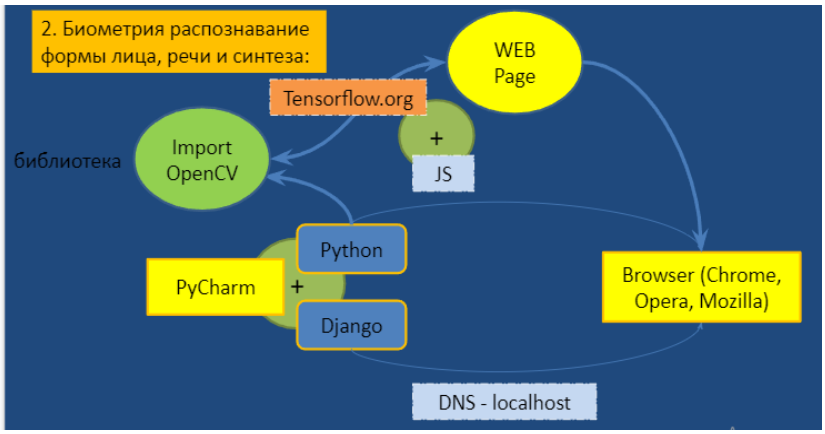
As previously reported, this facial shape recognition function can recognize faces wearing headgear, medical masks, but sunglasses or masks that cover the face cannot be recognized.



Picture 2. Comparison of the face recognition function in the semi-closed

and closed part of the face

The architecture for creating biometrics in visual mode took a small amount of time. To create the Database, a system of architecture was built:



Picture 3. Architecture of biometrics construction

List of used literature

1. Ivanov A.I. Biometric identification of a person by the dynamics of subconscious movements. – Penza: Penza State University, 2000. – 188 p.

2. Ivanov A.I. The computer recognizes you /A.I. Ivanov, I.A. Sorokin, S.N. Shumkin //Security, reliability, information (BDI). – №1. – 1996. – Pp. 18-21.

3. Barsunov B.C. Biometric information protection // Information protection. Confidential. – 2000. – No. 1. – Pp. 45-52.

4. Telnykh A. Identification of personality. How it is done. / A. Telnykh, A. Kogan. // Computerra. – 1999. – №. 10 – P. 39-41.

5. Willes D. Six biometric fingerprint identification devices. / D. Willes, M. Lee. // Networks and communication systems. – 1998. – №9(31). – SL 46-155.

6. Willes D. Let your fingers register themselves. //Networks and communication systems. – 1998. – №9(31). – Pp. 156-160.

7. Phillips P. J. Introduction to the evaluation of biometric systems. /P. J. Phillips, E. Martin, S.L. Przyboski // Open systems. – 2000. – No. 3. – Pp. 21-27.

8. Pentland A. Face recognition for intelligent environments. / A. Pentland, T. Chaudhary, //Open Systems. – 2000. – No. 3. – P. 28-33.

9. Belotserkovsky O.M. Computer recognition of human faces /O.M. Belotserkovsky, A.C. Glazunov, V.V. Schennikov // Foreign radio electronics. The successes of modern radio electronics. – 1997. – №8. – P. 3-14.

10. Glazunov A. Computer recognition of human faces //Open systems. – 2000. – № 3. – Pp. 43-47.