Biometric identification

V I Syryamkim, D N Kuznetsov and A S Kuznetsova
Tomsk State University, Tomsk, Russia
E-mail: novorostomsk@gmail.com

Abstract. Image recognition is an information process implemented by some information converter (intelligent information channel, recognition system) having input and output. The input of the system is fed with information about the characteristics of the objects being presented. The output of the system displays information about which classes (generalized images) the recognized objects are assigned to. When creating and operating an automated system for pattern recognition, a number of problems are solved, while for different authors the formulations of these tasks, and the set itself, do not coincide, since it depends to a certain extent on the specific mathematical model on which this or that recognition system is based. This is the task of formalizing the domain, forming a training sample, learning the recognition system, reducing the dimensionality of space.

1. Introduction

The main operations in pattern recognition using the methods discussed are the operations of determining the similarity and difference of objects. The objects in this group of methods play the role of diagnostic precedents. At the same time, depending on the conditions of a particular task, the role of a separate precedent can vary within the widest limits: from the main and decisive to the very indirect participation in the recognition process. In turn, the conditions of the task may require the successful solution of the participation of a different number of diagnostic precedents: from one in each recognizable class to the full sample size, as well as different ways of calculating measures of similarity and distinction of objects. These requirements explain the further division of extensional methods into subclasses.

Table 1.3 contains a brief description of the methods of pattern recognition with respect to the following parameters:

- classification of recognition methods;
- scope of recognition methods;
- classification of limitations of recognition methods.

Table 1. Table of classification of methods of recognition, comparison of their areas application and limitations

Classification of methods recognition		Application area	Restrictions (limitations)
	Methods based on estimates of the distribution densities characteristic values (or similarities and differences of objects)	Problems with the known distribution, as a rule, normal, the need for a set of great statistics	Necessity of search the entire training sample in recognition, high sensitivity to the unrepresentation of the training sample and artifacts

Intensive methods recognition	Methods based on assumptions about the class of decision functions	Classes must be well separated, a system of attributes - orthonormal	The form of the decisive function must be known in advance. The impossibility of taking into account new knowledge about correlations between signs
	Logical methods	problems of small dimension feature spaces	When selecting logical decision rules (conjunctions) is a complete search. High computational complexity
	Linguistic (structural) methods	Tasks of small dimensions of the feature space	Recovery task (definition) of a grammar by a certain set statements (descriptions of objects), is it is difficult to formalize. Unresolved theoretical problems
Extensional methods recognition	Comparison with the prototype	Comparison with the prototype	High dependence the results classification from the measure of distance (metric). Uncertainty optimal metric
	Nearest Neighborhood Method	The method of the nearest neighbors The problem of small dimension by the number of classes and indications	High dependence of results classification from measure distance (metric). The need for a full enumeration of the training sampling in recognition. Computing labor intensity
	Evaluation algorithms (voting) of the ABO	Tasks of small dimension by the number of classes and indications	Dependence of classification results on the measure of distance (metrics). The need for a full enumeration of the training sample when recognition. High technical complexity
	Algorithms estimates (voting)	Tasks of small dimensionality by the number of classes and	Very high technical complexity method, the unsolved

		indications	nature of a number of theoretical problems, the definition of the areas of competence of private methods, and in the particular methods themselves

Neural network, fuzzy-multiple and hybrid models in systems for processing and analyzing multidimensional complex data, their advantages and disadvantages with different approaches to modeling complex systems. Structural and functional possibilities and limitations of individual classes of fuzzy models, neural networks and their compositions dominating under representation and analysis of the corresponding types of models of complex systems and processes.

Biometric systems consist of two parts: hardware and specialized software.

The hardware includes biometric scanners and terminals. They fix one or another biometric parameter (fingerprint, iris, veins on the palm or finger) 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 decides who was before the scanner.

In order for the biometric system to be able to further identify the user, it must first register information about its identifiers. Commercial systems do not store images 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.

Of the total biometrics market, 14.7% are occupied by face identification technologies. Identification by fingerprints incorporated the best that is inherent in biometrics in general. A fingerprint is identified by a fingerprint, unlike the password, the fingerprint can not be forgotten, transferred to another. Modern scanners have learned to establish the belonging of a fingerprint to a living person, and they can not be deceived, imprinting an imprint on paper, gelatin or glass. The probability of erroneous identification is 0.0000003%, and the time required for scanning the print does not exceed a fraction of a second [1–5].

2. Denial of passwords

Denial of passwords was made through the introduction of a fingerprint scanner into a smartphone. No matter how they scolded the Touch ID function, opponents of biometric data collection, the technology is actively used not only for simple unlocking of a smartphone, but also for making purchases or using services.

In the future, some large banks are also considering the possibility of switching to a fingerprint scanner as a way of authentication. Moreover, the companies are working on a prototype of the iris scanner, which will be used in the online payment service. Despite openness to the perception of a new one, buyers are more inferior to more invasive technologies, such as face recognition software, that could be used to identify them by an employee during a shopping trip.

Assessing fingerprint recognition technology in the process of paying for goods, almost half (42.4%) of respondents would welcome this technology if it also allowed them to automatically receive a home delivery service (Figure 1).

Figure 1. Fingerprint.

In addition, 57% of the buyers surveyed want to have the ability to scan the product from their devices to see reviews and recommendations for other products that they might like, while 48% of buyers do not object to the function of pop-up offers starting to arrive on their mobile device at the entrance to the store.

3. Cydercrime

On the black market, there are at least 14 vendors offering skimmers who can steal data from fingerprints, and at least three researchers who are working on technologies that can break systems for recognizing the pattern of veins on the wrist and iris. On the black market pre-sale testing of the first versions of biometric skimmers has already been carried out. Then several errors were found, but the main problem was the use of GSM modules for transmitting biometric data - they could not cope with large volumes of information, which means that new versions of such skimmers will use other, faster data transfer technologies [2]. In the communities of cybercriminals actively discussing the development of mobile applications that allow to mask human faces [2]. Such programs help to use photos of real people posted on social networks to deceive the face recognition system. Unlike passwords or PIN-codes, which can be easily changed in case of hacking, fingerprints or the image of the iris of the eye can not be changed. Accordingly, if biometric data is once in the hands of others, their continued use will pose a serious risk. That's why they need exceptionally reliable methods of protection. The danger lies also in the fact that they are introduced into modern electronic passports and visas, which means that the theft of such documents leads to the fact that in the hands of the attacker is virtually all information on which the identity of a person can be established. "

4. Voice biometry

Voice biometrics is one of the technologies that develops very quickly and allows different companies to use its solutions to identify customers. In the biometric system, individual behavioral, psychological and some other characteristics are used to determine or confirm the personality. There are many biometric measurements, including scanning the iris, fingerprints, face recognition, voice, signature, etc..

Voice biometry allows, by examining the voice characteristics of a person, to identify a person. It is a relatively simple and economical way to solve a number of practical problems. Voice biometry is a highly developed technology that can be used to improve the quality of a service to such an extent that a person can experience this improvement. The developer must provide the person with automated service, and speech technologies can help in this.

Nobody forces people to wait, does not redirect and does not offer to use the menu. Voice communications are convenient for a person.

The system understands the person and is able to test his words. He may not even remember the password or the number. The biometry of the voice, which is used during the conversation, allows you to determine who is calling. This reduces the talk time. So the client does not need to be presented and name the password. His password is his voice! At the same time, he feels that his call is important and the developers immediately make a decision [3–7].

The most widely used technology is applied in the banking sector, in insurance companies, in telecom. Airlines are showing considerable interest. The market of mobile applications for cell phones is also promising, where speech technologies are in full demand. In the automotive industry, voice systems allow you to use navigation devices along the way, are able to turn on music, air conditioning, help, without distracting from the control of the car, write down and send SMS, etc.

In medicine, speech technologies are used to record information about clients, create electronic patient maps. This allows you to optimize the work of doctors and creates clear benefits for customers. The doctor does not use the computer keyboard, he just dictates the medical indicators and diagnosis. The speech recognition system translates the voice into text and writes it down [8–15].

Bank contact centers successfully use voice technology. If the client needs basic information, then it is given to him freely. But if he wants to conduct a financial operation or some operation with his account, then his [status] should be checked. Voice biometry is one of the types of human verification, with which it is possible to identify whether a person is alive, or a speech record is broadcast (Figure 2).

Figure 2. Vois biometry.

The voice biometry system can reveal the need for additional verification of a person. You can also create a `blacklist 'of client votes, seen in fraud or in attempts to unauthorized access to the accounts of other customers. This allows you to ensure the safety of banking operations.

5. Smell Detection

The ability to identify individuals using body odor as a method of unique human identification. Changing the smell can be evidence of a substitution.

The system, developed by the scientists of Madrid, is able to identify people by the smell emanating from the body. The researchers argue that the body of each person has permanent distinct "odor patterns", which are not affected by disease, diet, or age. Researchers have created a sensor that can recognize the "unique patterns" of the smells of the human body and identify their carrier with an accuracy of 87%. The sensor was tested on 11 volunteers, of which eight were men and five were women. Scientists took thirty samples of smell from cleanly washed hands of each of the subjects at different times of the day.

According to the developers, the sensitivity of the sensor was so high that it was difficult to deceive with soap, deodorant, cologne or other attempts to change the smell. In the official statement of the university, scientists express confidence that this opens the possibility for creating "less aggressive" ways of identifying a person than what exists at the present time. Despite the fact that the recognition of the iris and fingerprint gives high accuracy of identification, in the mass consciousness, these technologies are closely associated with forensic science, which causes distrust and protest, the scientists state [4,16].

Recognition of persons at the current stage of development gives too high a level of errors. Thus, the development of odor sensors, allowing to identify a person passing by them, opens the possibility for the development of more comfortable and inconspicuous methods of identification with a sufficiently high level of accuracy. Researchers are confident that such technologies can be used at airports, at checkpoints on the border and in any other situations where identification is currently applied on the photo. Identification by smell is one of the oldest methods used to find and identify people, but now forensic experts use specially trained dogs for this. The development of methods for effective recognition of the smell of man using electronic devices started relatively recently.

The most original and unusual method of identifying an individual in our opinion is to implant chips or swallow microcomputers. This will solve the problem of authorization radically and forever. Chips and microcomputers will analyze the pulse, the composition of the gastric juice and other internal biometric information. This, in turn, will ensure the security of Russia and the world.

Summarizing the results of this article, it can be argued that neural networks technologies for biometric authentication of users of open systems are technically feasible at the modern level of knowledge. Accordingly, for the creation of neural network technologies for biometric authentication, it is necessary to borrow the symmetrization of the problem of identifiable Volterra nuclei.

Acknowledgments

The article is prepared within the framework of Competitiveness Enhancement Programme of National Research Tomsk State University

References

[1] Yazov Yu K, Volchihin V I, Ivanov A I, Funtikov V A, Nazarov I G 2012 *Neural network protection of personal biometric data* (Moscow, Radio technics)

[2] Akhmetov B S, Ivanov A I, Funtikov V A, Bezyaev A V, Malygina E A 2014 *The technology of using large neural networks to convert fuzzy biometric data into the code of access key* (Almaty, LEM Publishing house)

[3] Bekhtin Yu S, Klestov S A, Kutsov M S, Syryamkin V I, Titov D V 2016 *Theoretical foundations of digital image processing in build-in vision systems* (Tomsk, STT Publishing house)

[4] Syryamkin V I 2017 *Intellectual robotic and mechatronic systems: textbook* (Tomsk, STT Publishing house)

[5] Kuznetsov D 2018 *Matec Web of Conferencec* **155** 01018 doi: 10.1051/matecconf/201815501018

[6] Syryamkin V I *et al.* 2009 *Devices and systems of automatic control of high accuracy*. – (Tomsk, Publishing house Tom. University)

[7] Syryamkin V I 2010 *Correlation-extreme radio navigation systems* (Tomsk, Publishing house Tom. University)

[8] Syryamkin V I *et al.* 2012 *Cognitive systems for monitoring and forecasting the scientific and technological development of the state* (Tomsk, Publishing house Tom. University)

[9] Syryamkin V I 2013 *Regional problems of public security* (Tomsk, Publishing house Tom. University)

[10] Syryamkin V I 2012 *Medical diagnostic and therapeutic systems. Principles of designing and building medical hardware and software systems* (Germany, LAP LAMBERT Academic Publishing)

[11] Syryamkin V I 2013 *Recognition of complex oil and gas deposits based on neuro-fuzzy portraits* (Germany, LAP LAMBERT Academic Publishing)

[12] Syryamkin V I, Bureev A Sh, Zhdanov D S 2009 A method for diagnosing the state of human or animal organs and the device for its implementation. Patent for invention № 2429979 from July 22, the Russian Federation

[13] Syryamkin V I 2014 *Neuro-fuzzy methods in intelligent systems for processing and analyzing multidimensional information* (Tomsk, Publishing house Tom. University)

[14] Titov V S *et al.* 2012 *Methods and systems for digital processing of aerospace images* (Novosibirsk, Science)

[15] Serikov M Z *et al.* 2017 *Proceedings – 2016 11th International Forum on Strategic Technology, IFOST 2016, 510*

[16] Yurchenko A V *et al.* 2015 *IOP Conf. Ser.: Mater. Sci. Eng.* **81** 012112