UDC 004.93
DOI: 10.31733/2078-3566-2019-5-198-201

Andrii HREBENIUK©
Cand. of Eng-g, Ass. Prof.
(Dnipropetrovsk State University of Internal Affairs)

USE OF THERMAL IMPORTER FOR BIOMETRIC IDENTIFICATION OF HUMAN

Андрій Гребенюк. ЗАСТОСУВАННЯ ТЕПЛОВІЗОРА ДЛЯ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ЛЮДИНИ. Розглянуто сучасні технології біометричної ідентифікації людини, що застосовуються як для охоронних систем так і для систем контролю і управління доступом, які існують в різних країнах світу і використовуються на практиці різними установами і організаціями у тому числі правоохоронними органами.

Основними перевагами біометричної ідентифікації є складність підробки ідентифікаційного параметра, практична неможливість втрати ідентифікатора, неможливість передачі ідентифікатора іншій людині. Зчитування біометричних параметрів вимагає від системи надійності обчислювальних алгоритмів, а також високого швидкодії. В іншому випадку залишається ймовірність виникнення помилок, які бувають двох основних типів: помилковий відмова в доступі або помилкова ідентифікація. Для біометричних систем необхідно враховувати ймовірність виникнення помилок FAR / FRR.

Най частіше в системах контролю доступу використовується така біометрична характеристика, як відбитки пальців. Однак в місцях, що вимагають більшого рівня безпеки, наприклад, в охоронюваних приміщеннях аеропортів, урядових будівлях і т.д., використовується сканування сітківки ока і технологія розпізнавання облич.

Інтерес до цих систем дуже великий в зв'язку з широким колом завдань, які вони вирішують. В даний час популярність технології розпізнавання осіб в різних сферах діяльності зростає. Технології розпізнавання облич застосовуються в найрізноманітніших сферах.

Головний недолік технології розпізнавання облич – це погіршення якості розпізнавання при погіршенні освітленості або зміні положення голови і ракурсу. Для зменшення помилкових відмов і хибних ідентифікацій стали застосовувати тепловізійні відеокамери. Основна конкурентна перевага відеокамер з тепловізором – ефективна робота в будь-яких погодних умовах. При снігу, в пургу, під час дощу, вітер, такі камери знаходять мету навіть якщо вона сховалася за густим листям дерев.

Розглянуто також особливості використання телевізора для біометричної системи так як на даний момент вважається перспективним напрямом, який дозволяє прибрати всі недоліки, які існують при використанні звичайних відеокамер.

***Ключові слова**: ідентифікація людини, тепловізійні відеокамери, біометрична автентифікація, контроль доступу.*

Problem statement. Currently, there are a number of methods and technologies that allow you to produce identification of a person according to his biological parameters. All of them are based on the fact that each of us has an individual combination of physiological, psychosomatic, personal and other characteristics.

The use of biometrics in access control and management (ACM) systems seems natural and logical. However, the practical implementation of this idea was not so simple. Only now, biometrics is becoming an integral part and an important factor in the ACM market.

The development of computer technology has made it possible to create devices that are able to quickly and reliably process biometric data using special algorithms. They have become widely used in access control systems. The parameters read by the biometric access control system are divided into two broad classes:

1. Static – permanent or slightly variable throughout life (outline of the face, fingerprints, capillaries of the fingers, drawing of the iris, DNA code and more);

2. Dynamic – behavioral or psychosomatic, which are prone to major changes depend-

© Hrebeniuk A., 2019
ORCID iD: https://orcid.org/0000-0002-6529-683X
k_inf@dduvs.in.ua

ing on age and environment (handwriting or tone of voice).

The main advantages of biometric identification are the complexity of tampering with the identification parameter, the practical impossibility of losing the identifier, the inability to pass the identifier to another person.

Reading biometric parameters requires a reliable system of computational algorithms, as well as high performance. Otherwise, there are two main types of errors: false denial of access or false identification.

For biometric systems, the probability of FAR / FRR errors should be considered. Where FAR is the False Acceptance Rate (False Reception Rate) and FRR is the False Rejection Rate. It is necessary to take into account the relationship of these indicators: artificially reducing the level of sensitivity of the FAR system, we usually reduce the percentage of FRR errors, and vice versa. [1,3]

To date, all biometric technologies are likely, none of them capable of guaranteeing the complete absence of FAR / FRR errors.

Analysis of publications that started solving this problem. The problem of biometric identification is devoted to many publications including the following authors: Lavrukhin A.I., Ivanitsky G.R., Deyev A.A., Khizhnyak E.P., Khizhnyak L.N., Selyanichev A.L., Zakharov V.P., Rudeshko V.I., Lavrukhin A.I., Selyanichev O.L. and others [1 – 4]. The importance of scientific achievement and contribution to the theory and practice of information security of these scientists can hardly be overestimated.

The article's objective is to consider the most promising areas for the development of biometric technologies and effective existing biometric systems, based on their effectiveness. But the possible introduction of human identification using a thermal imager to ensure the reliability of face recognition and in all weather conditions.

Basic content. Biometric systems consist of two parts: hardware and specialized software. Hardware includes biometric scanners and terminals. They capture a particular biometric parameter (fingerprint, iris, vein drawing on the palm or fingers) and turn the information received into a digital model available to the computer. And the software tools process this data, correlate with the database and make decisions about who is in front of the scanner.

In order for the biometric system to be able to identify the user in the future, it is necessary to first register information about its user. Commercial systems (unlike those used by law enforcement and law enforcement) do not store real IDs but their digital models. When a user re-accesses the system, the model of his / her ID is re-formed and compared to the models already stored in the database.

Any biometric access control system includes an access control device – a reader or scanner. This is a device that reads information, then this information is analyzed and compared with the personal information of the person recorded earlier. If the data is the same, the person is authenticated. If the authenticated user is allowed to stay in this room for that period of time, the device beeps and opens an electronic lock.

Most often, biometric characteristics such as fingerprints are used in access control systems. However, in places requiring a higher level of security, such as in secure areas of airports, government buildings, etc., retinal scans and face recognition technology are used.

Face recognition technology works on a similar principle to the human brain. After all, we first see the image, in this case a person, pay attention to the features of his/her face and process them in our head. The same with technology: the system must look for faces in the image and highlight the desired area.

Different algorithms are used for this purpose. Sometimes the system determines the similarity of proportions, selects the contours in the image and compares them with the contours of individuals or distinguishes symmetry through neural networks.

Now such technologies are available in different countries, because with their help it is possible to solve many problems in different spheres, including in the sphere of security, forensics, face-control.

Facial recognition is the automatic localization of a human face in an image or video and, if necessary, the identification of a person's identity based on available databases. The interest in these systems is very high because of the wide range of tasks they solve. Currently, the popularity of face recognition technology in various fields of activity is increasing.

Facial recognition technologies are used in various fields [1, p. 5]:

- providing security in places of large crowds;
- security systems, avoid illegal entry into the territory of the object, search for intruders;

- "face-control" in the segment of catering and entertainment, search for suspicious and potentially dangerous visitors;
- verification of bank cards;
- online payments;
- contextual advertising, digital marketing, Intelligent Signage and Digital Signage;
- phototechnics;
- forensic science;
- teleconferences;
- mobile applications;
- photo search in large photo bases;
- tagging people in photos on social networks and more.

Face recognition (as well as other related operations) is a fairly common task. Therefore, many companies provide ready-made services in the form of cloud APIs (software intermediaries between applications) to qualitatively solve these problems. In addition to IT giants like Microsoft and Google, specialized companies are also involved in face recognition. Their products are rapidly evolving and provide even more fun features such as identifying faces and silhouettes in a crowd.

The main disadvantage of face recognition technology is the deterioration of recognition quality when the illumination is diminished or the head and angle are changed.

Thermal imaging cameras have been used to reduce erroneous failures and false identifications. The main competitive advantage of cameras with thermal imaging is efficient operation in all weather conditions. In snow, in blizzards, in the rain, in the wind, such cameras find a purpose, even if it is hidden behind the thick leaves of trees.

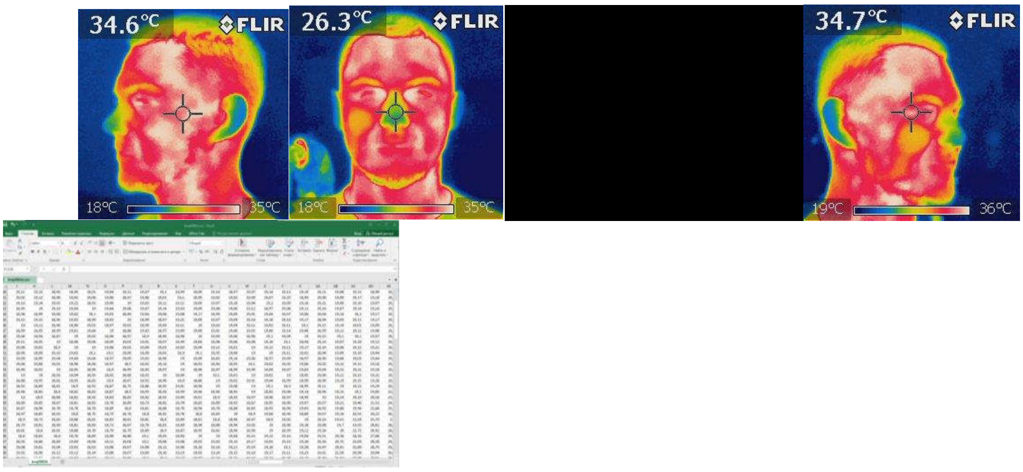

Fig. 1

Generation of a three-dimensional face surface is performed using the 3D Basel Face Model (BFM) tool in Matlab language using the data of images of a thermal imaging camera Fig. 1. For this purpose, a vector α of 199 components is created, where α1 ∈ N (0, 1) is a random variable with normal distribution and all other values are zero. The first factor is responsible for the shape of the face, so changing it allows you to generate identical faces with different shapes. The resulting vector is used to generate faces using the standard BFM tool feature. [2, p. 4]

Conclusion. The use of thermal imaging cameras, for face recognition purposes, is currently considered a promising direction, which allows to remove all the disadvantages that exist when using humble video cameras.

• Face recognition in total darkness and in low light conditions;

• Face recognition with makeup, different hairstyles, beard, hat, glasses;

• Allow to recognize twins

There are two areas that are being developed in other countries:

1. Identification by a pre-created thermogram of the identified persons.

2. Identification of a person by images obtained from a thermal imaging camera, and as a person of standards the database of ordinary two-dimensional images is used. This problem is solved by using deep neural networks.

References

1. Захаров В. П., Рудешко В. І. Використання біометричних технологій правоохоронними органами у XXI столітті: наук.-практ. посібник. Львів: ЛьвДУВС, 2009. 440с.

2. Зачек О. І. Можливості застосування біометричного методу ідентифікації за геометрією обличчя в системах відеоспостереження правоохоронних органів. *Науковий вісник Львівського державного університету внутрішніх справ*. 2014. №1, с. 343-351.

3. Lavrukhin A. I., Selyanichev O. L. The geometrical model thermovision image of rawmaterials' surface charged into the blast furnace. *Bulletin of the Cherepovets State University*, 2017, no. 1, pp. 48–55.

4. Иваницкий Г. Р., Деев А. А., Хижняк Е. П., Хижняк Л. Н. Анализ теплового рельефа на теле человека. *Технологии живых систем*. 2007. Т.4, №5-6. С. 43-50.

Received to editorial office 05.12.2019

1. Zakharov, V. P., Rudeshko, V. I. (2009) Vykorystannya biometrychnykh tekhnolohiy pravookhoronnymy orhanamy u XXI stolitti [The use of biometric technologies by law enforcement agencies in the XXI century]: nauk.-prakt. posibnyk. L′viv: L′vDUVS, 440 s. [in Ukr.]

2. Zachek. O. I. (2014) Mozhlyvosti zastosuvannya biometrychnoho metodu identyfikatsiyi za heometriyeyu oblychchya v systemakh videosposterezhennya pravookhoronnykh orhaniv [Possibilities of use of biometric method of identification by face geometry in video surveillance systems of law enforcement agencie]. *Naukovyy visnyk L'vivs'koho derzhavnoho universytetu vnutrishnikh sprav*.. №1, s. 343-351. [in Ukr.]

3. Lavrukhin, A. I., Selyanichev, O. L. (2017) The geometrical model thermovision image of rawmaterials' surface charged into the blast furnace. *Bulletin of the Cherepovets State University*, no. 1, pp. 48–55. [in Eng.]

4. Yvanitskiy, G. R., Deyev, A. A., Khizhnyak, E. P., Khizhnyak, L. N. (2007). Analiz teplovogo rel′efa na tele cheloveka [Analysis of thermal relief on a human body]. *Tekhnologii zhyvykh sistem*. T.4, №5-6. S. 43-50. [in Russ.]

SUMMARY

The article deals with modern technologies of biometric identification of the person, which are used both for security systems and for access control and management systems, which actually exist in different countries of the world and are used in practice by various institutions and organizations including law enforcement agencies. Features of the use of the TV for the biometric system are also considered.

Keywords: *human identification, thermal imaging cameras, biometric authentication, access control.*

UDC 343.55
DOI 10.31733/2078-3566-2019-5-201-206

Aleksey KOVALCHUK©
Ph.D, Ass. Prof.
*(Academy of the Ministry of Internal Affairs
of the Republic of Belarus)*

IMPROPER FULFILLMENT OF RESPONSIBILITIES FOR MAKING THE SAFETY OF CHILDREN'S LIFE AND HEALTH OF: ISSUES FOR IMPROVING CRIMINAL LAWS

Алексей Ковальчук. НЕНАДЛЕЖАЩЕЕ ИСПОЛНЕНИЕ ОБЯЗАННОСТЕЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЖИЗНИ И ЗДОРОВЬЯ ДЕТЕЙ: ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА. Предметом исследования статьи являются уголовно-правовые нормы, устанавливающие ответственность за ненадлежащее исполнение обязанностей по обеспечению безопасности жизни и здоровья детей (ст. 165 Уголовного кодекса Республики Беларусь). Значительное внимание в статье уделяется научному толкованию признаков данного вида преступления. На основе проведенного

ORCID https://orcid.org/0000-0003-2343-551X
info@amia.by