2. Приложение к свидетельству №64901 об утверждении типа средств измерений «ОПИСАНИЕ ТИПА СРЕДСТВА ИЗМЕРЕНИЙ. Хромато-масс-спектрометры газовые GCMS-QP2020». – 5 л.

3. Крылов, В.А. ХРОМАТОМАСС- СПЕКТРОМЕТРИЧЕСКИЙ МЕТОД АНАЛИЗА: учебное пособие / В.А. Крылов, П.В. Мосягин. – Нижний Новгород: Нижегородский госуниверситет, 2021. – 88 с.

УДК 349.98

A. E. Serada, I. I. Luzgin
(*Belarusian State University, Minsk*)

PROSPECTS OF AUTOMATED FACIAL RECOGNITION (AFR) AS A TOOL IN SOLVING AND PREVENTING CRIMES

The article deals with the prospects of automated facial recognition in terms of investigating and solving crimes in the Republic of Belarus. Main problems of its implementation are being looked into and the solutions as to how to enhance its efficacy are suggested.

Since time immemorial, human beings have been using facial features to recognize one another. Interestingly, the practice of authorities and police utilizing the body features and characteristics to identify people, foes and friends alike, has a long recorded history dating back to the mid-1800 (and, in some instances, even further). Previously, there has also been ways to use one's body features to that effect – as, for example, the ancient Chinese way of signing documents with a person's fingerprint (even back then, it was known that this characteristic is distinctive).

The most recent history which has been recorded in terms of scientific advances and practical usages knows the following steps into the new territory that later would be known as «biometrics» («bio» meaning «life», «metrics» meaning «to measure» in Greek):

1) one trigger for the systematic use of biometric traits to recognize a person was the enactment of the Habitual Criminal Act in 1869 in the United Kingdom. This Act made it mandatory to maintain a register of all persons convicted of a crime in the UK along with appropriate evidences of identity [1, c. 85];

2) in order to identify repeat offenders, a French police officer named Alphonse Bertillion introduces a system of person identification based on a set of anthropometric measurements. Additionally, he utilized multiple descriptive attributes such as eye color, scars, and distinctive marks in order to recognize an individual [1, c. 85];

3) the Bertillion's approach was quickly discarded as insufficiently efficient in favor of a more accurate approach involving manual comparison of human fingerprints. This was made possible by the pioneering works of Henry Faulds, William Herschel, and Sir Francis Galton, who established uniqueness of certain features in a fingerprint ridge pattern such as minutia points [1, c. 85].

As a result, in the 1980s, the term «biometrics» began to be used to describe automated or not-so-much systems of human recognition then being developed. In the 1970s, however, the most promising field had been known as «Automated Personal Identification».

What has changed with more recent developments in biometrics is that these practices are now being extensively and thoroughly digitalized, which includes the use of complex algorithms designed to read collectedly bodily data and the use of biometric technologies in conjunction with growing and widespread networks of surveillance. Of all the available body features to distinguish one person from another face clearly stood out in that it was susceptible to so many algorithms developed in order to identify a person. Additionally, in comparison with other biometric features, the face has a number of advantages that make it one of the most preferred features for identifying a person [2, c.159]:

1) lack of physical contact: unlike collecting fingerprints and scanning the iris, images of faces can be obtained at a distance without physical contact. The facial recognition system can collect biometric data in a way convenient for the researcher;

2) no need for cooperation: compared to iris and fingerprints, face recognition requires less interaction with persons;

3) the presence of signs significant for identification: a person has a number of unique (distinctive) physical characteristic significant for the identification. These physical attributes are easily measurable and most visible to the researcher (as opposed to capillaries on the fingertips or blood type and DNA sequence among other things).

The research on enabling computers to recognize human faces commenced in the mid-1960s by Woodrow W. Bledsoe and his colleagues at Panoramic Research. The matching was then done automatically based on 20 normalized distances derived from these facial landmarks (e.g., width of the mouth, width of eyes, etc.). A system capable of automatically extracting such facial landmarks was also proposed in Takeo Kanade's Ph.D. thesis published in 1973, which can be considered to have presented the first fully automated face recognition system [1, c. 88].

While the earliest face recognition systems were based on geometric features, the Eigenface approach (the Eigenface technology creates matrices of human faces and uses complex mathematical equations to generate templates for individual features that are digitally stored. The library of Eigenfaces can be superimposed over raw facial images when searching for a facial identification) popularized by Turk and Pentland in 1991 was based on holistic facial appearance. Holistic appearance-based techniques generate a compact representation of the entire face region in the acquired image by mapping the high-dimentional face image into a lower dimentional sub-space. This sub-space is defined by a set of representative basis vectors, which are learned using a training set of images. The local feature analysis method of Penev and Atick and the Fisherface method of Belfumeur et al. are other examples of holistic appearance-based face recognition [1, c. 89].

The elastic bunch graph matching approach of Wiskott et al. was a pioneering work in model-based face recognition. Model-based techniques try to derive a pose-independent representation of the face images by building 2D or 3D face models. These schemes typically require the detection of several fiducial or landmark points in the face (e.g. corners of yes, tip of the nose, corners of the mouth, and the chin), which leads to increased complexity compared to appearance-based techniques. The morphable model proposed by Blanz and Vetter advanced the use of 3D models in face recognition by exploiting both facial texture and shape features. Since appearance-based schemes use the raw pixel intensity values, they are quite sensitive to changes in ambient lighting and facial expressions. Therefore, texture-based methods like «Scale Invariant Feature Transform» and «Local Binary Patterns» were developed. These methods use more robust representations that characterize the texture of an image using the distribution of local pixel values. Sparse representation coding and face recognition based on deep learning are some of the more notable advances in the area of face recognition in the last decade [1, c. 89].

Most of the face recognition techniques assume that faces can be aligned and properly normalized (both geometrically and photometrically). The alignment is typically based on the location of the two eyes in the face. The face detection scheme developed by Viola and Jones is considered a milestone because it enabled faces to be detected in real-time even in the presence of background clutter, a situation commonly encountered in applications such as surveillance. Even though the Viola-Jones face detector has demonstrated excellent performance in real-time applications, it is still challenged when confronted with non-frontal facial poses, illumination changes, occlusion, etc.

Consequently, real-time face recognition has been made feasible in a wide range of applications where the user is cooperative and the face image is acquired in a controlled environment. However, solutions to unconstrained face recognition such as in surveillance applications were still in development and some of them proved to be quite effective, while others certainly didn't.

The development, of course, didn't stop there. In 2014, Facebook launched the «DeepFace» service, which determines whether two photographed faces belong to the same person with an accuracy of 97.25%. In 2015, Google also presented its development called the «FaceNet» face recognition system. Owning to the enormous array of data collected by Google services, «FaceNet» achieved significant accuracy at that time – 99.63%. In particular, this technology is used in the «Google Photo» application to sort images and automatically mark people on them [3].

The police in the USA implemented face recognition system called "FACE" (Facial Analysis, Comparison, and Evaluation) which is based on algorithms that scan more than 30 million images from copyright and photographs. In addition, companies such as «Clearview AI», «Vigilant Solutions» and «Accuant FaceID» are also working on their face recognition systems for the purpose of solving crimes and holding the perpetrators accountable. As of 2020, the AFR technology was used in 98 countries; banned in 3; its implementation was planned in 13 more. In 2022, about 109 countries are using facial recognition systems in one or another area of their society. According to a 2019 study called "Facial Recognition Market", the global facial recognition market was estimated at 3.2 billion US dollars. The forecast for 2024 is 7 billion US dollars (with an annual growth of 16%) [3].

Not surprisingly, automated facial recognition technology nowadays can be found in many things: from "Apple Face ID" to the automatic tagging function in Facebook and biometric passport checkpoints at international airports. However, the most profound achievement that this technology has scored is that AFR now is either fully or partially implemented in applications such as border control, forensics, surveillance, de-duplication, and chain-of-custody. The examples of successful using AFR in forensics and law enforcement activities are the following:

1) the implementation of the state program "Safe City" in Moscow in 2020 contributed to the solving of more than 5 thousand crimes. The facial recognition system, massively introduced in Moscow in January 2020 and deployed in 10 other Russian cities, currently plays a significant role in 70% of crime investigations (there are already more than 189,000 cameras with the ability to recognize faces in the capital and more than 12,300 installed in subway trains) [4];

2) by the end of 2018, there were about 4,000 CCTV cameras with a facial recognition system in Minsk, thanks to which about 500 crimes were solved in the same year. In Belarus, the «Synesis» company's product "Kipod" is used, which recognizes from 15 to 25 persons in the frame [4];

3) in China, the «Dragonfly Eye» facial recognition system is used to maintain public order. In the first three months of using this technology, 567 violators were detained in Shanghai [10]. As a result, the level of pickpocketing in Chinese cities has fallen by almost a third [5, 6];

4) in the Czech Republic, the use of face recognition since 2018 has contributed to the prosecution of 160 offenders at the airport in Prague alone [5];

5) American law enforcement actively used facial recognition in the investigation of mass riots at the Capitol on January 6, 2021. Thanks to this technology, it was possible to bring to justice more than 500 people who took part in the riot. Facial recognition is now bein used by the FBI in criminal investigations. In addition, the FBI dropped the use of their Integrated Automated Fingerprint Identification Systems (IAFIS) in favor of The Next-Generation Identification System (NGIS), which pertains heavily to biometrics and relies on facial recognition as well.

There were about 4,000 surveillance cameras installed in Minsk by the end of 2018 as part of the Republican Public Security Monitoring System (hereinafter referred to as RSMOB). In order to maintain law and order, a product developed by «Synesis» called «Kipod» was deployed, which allows setting up a biometric system for identification and recognition of persons, as well as identification and recognition of vehicle registration numbers (the accuracy of face recognition is about 94.21%, and registration numbers around 97.46%). Depending on the location of the CCTV camera, «Kipod» easily recognizes approximately up to 25 persons in a crowd.

The regulatory legal act of the Republic of Belarus, which was a prerequisite for the creation of the RSMOB, is Presidential Decree No. 527 of 2013. The main characteristic of this regulatory legal act is that it provides for the creation of a video surveillance system in the country. The application contains a list of objects that needed to be connected in the first place (transport hubs, sports complexes, hotels and administrative buildings). In May 2017, the President of the Republic of Belarus also signed Decree No. 187 "On the Republican public Security monitoring system", according to which the main tasks of the monitoring system are monitoring the state of public security in order to ensure public order, prevention, detection (disclosure) and suppression of crimes, other offenses, search for persons who committed them and persons missing (disappeared), prevention and liquidation of emergency situations, as well as prompt information about recorded events».

According to the decree of the Ministry of Internal Affairs of the Republic of Belarus dated July 2, 2019, the software for the RSMOB should provide for integration with third-party information databases and systems that store photos of people. In accordance with this, some critics of the «Kipod» system, a video surveillance and face recognition system used in the Republic of Belarus, believe that it is integrated with the automatic identification systems «Passport» and «Traffic Police Center».

As part of the use of facial recognition systems in the investigation of crimes, such problematic aspects have so far been identified as: the accuracy – this indicator may have a programmatic nature (depends on the algorithm), as well as a technical one (depends on the quality and capabilities of the technical means used in recognition); variability of the distinctive characteristics of people – deformation of facial features due to age-related changes or surgical intervention, for example; the legislative aspect is that the use of facial recognition technology may raise objections from human rights defenders in terms of the admissibility of evidence obtained as part of a criminal investigation. For the successful application of facial recognition technology in the investigation and prevention of crime in the Republic of Belarus, it seems appropriate to implement the following measures:

1) installation of video surveillance cameras with a facial recognition system in places of potential interest to participants and organizers of mass riots and unauthorized mass events;

2) creation of training programs for specialists in the field of working with current facial recognition technologies and the development of new, more sophisticated algorithms for their functioning;

3) the use of 3D facial recognition software in crime investigation, which is not as easily misled due to tricks or technical problems as 2D prototypes. The reliability of the result of using this equipment in poor light conditions is much higher and turning a person's head is an uncritical aspect. By adding a parameter like "depth" to the equation, a 3D face print can include contours, curves, and finer distance shapes;

4) widespread informing of citizens that a facial recognition system is being used;

5) the existing format of video surveillance cameras, intended as a cost-effective means for surveilling large areas, does not meet the requirements for the effective use of face recognition technology. To optimize their application, improved standards in the technology and configuration of video surveillance systems are required;

6) taking into account the fact that some changes (for example, aging) can radically change a person's appearance, it is advisable to: a) create data banks related to gender, age and ethnicity, which provide background information for a variety of diagnostic, clinical and judicial procedures; b) develop and use an algorithm that is able to take into account the approximate age change of a person after a certain time.

The successful application of this technology in solving crimes implies overcoming existing contradictions in legislation, resolving existing issues regarding accuracy, security and confidentiality of data. The accuracy of these systems is of particular importance, since specialists have no right to make mistakes – any erroneous detention can distract from the capture of a criminal, or mislead the investigation. Thus, the development of facial recognition technology and its use in the detection and investigation as well as preventing of crimes is gaining priority in the context of exponential development of information technology and contributes to the effective implementation of the National Security program of the Republic of Belarus. In particular – ensuring public safety and the safety of the population, reducing crime and criminalization of society; as well as compliance with the basic principles of criminal law.

Список использованной литературы

1. Jain, K. 50 years of biometric research: Accomplishments, challenges, and opportunities / K. Jain, K. Nandakumar, A. Ross // Pattern Recognition Letters. – 2016. – № 79. – С.80 – 105.

2. Saferstein, R. Criminalistics: an Introduction to Forensic Science / R. Saferstein. – New York: Pearson, 2020. – 558 с.

3. Facial Recognition Market by Component, Application, Vertical and Region – Global Forecast to 2025 [Электронный ресурс]. – Режим доступа: https://www.marketsandmarkets.com/pdfdownloadNew.asp?id=995. – Дата доступа: 19.02.2022.

4. Yi Zeng Responsible Facial Recognition and Beyond [Электронный ресурс] / Y. Zeng, E. Lu, Y. Sun, R. Tian. – Режим доступа: https://arxiv.org/ftp/arxiv/papers/1909/1909.12935.pdf. – Дата доступа: 17.02.2022.

5. Можно немного хромать: BYPOL ответил, как защититься от распознавания камерами на уличных акциях [Электронный ресурс]. – Режим доступа: https://www.the-village.me/village/city/news-city/287555-kak-zashititsja. – Дата доступа: 21.02.2022.

6. Распознание лиц: почему в Китае не скрыться даже в 60-тысячной толпе [Электронный ресурс]. – Режим доступа: https://www.bbc.com/russian/news-43751391. – Дата доступа: 08.02.2022.

7. В Китае научились распознавать 95% лиц в масках [Электронный ресурс]. – Режим доступа: https://www.forbes.ru/newsroom/biznes/395425-v-kitae-nauchilis-raspoznavat-95-lic-v-maskah. – Дата доступа: 10.02.2022