APPLICATION OF FORENSICS TECHNOLOGY IN IDENTIFICATION OF A PERSON

Vyacheslav Tulskikh
APPLICATION OF FORENSICS TECHNOLOGY
IN IDENTIFICATION OF A PERSON

In the man-made world of today, with its nuclear power plants, subways, airplanes, with accumulation of large numbers of people in one and the same place, terrorism (*terror* is Latin for fear and horror) poses serious threat not only to security of a certain state, but also to entire world community. All governmental structures belonging to various departments, bodies and divisions should be effectively involved in struggle against this most dangerous evil.

Outlook for global terrorism is not only unequivocally pessimistic – it is just terrible. Expansion of its social, financial and national base as well as growth of its brutality and aggression and possible use by terrorists of weapons of mass destruction has been widely discussed. "We are all targets of terrorists, our cities are vulnerable, and our values cause hatred of fanatics trying to destroy our society and our way of life". ¹

Many experts having deep knowledge in various fields of social and political activities, criminology and criminal proceedings try to solve problems relating to fight against terrorism. However, no significant reduction in the number of acts of terrorism has been registered insofar.

Thus it suffices to note that the quantity of attacks is annually estimated in several thousands. Some of them are unprecedented in their audacity and cruelty of nature, as was the case with committing of a series of explosions (in Buinaksk, Moscow, Volgodonsk, Beslan and in the Domodedovo Airport in Moscow).

According to several experts, in the world there currently operate about 500 terrorist organizations. Over the past 10 years they have committed 6,500 acts of international terrorism causing death of 5,000 people and injuries to 11,500.

Under these conditions, the measures to be taken against terrorists, including preventive measures, should ever be effective. And the problem concerning efficiency of criminal proceedings (from the point of view of disclosing such crimes) acquires particular importance and urgency in finding out (elimination) of causes and conditions of the crimes to have been committed.

The following ways of committing acts of terrorism are most common in Russia: threats by telephone (telephone terrorism), demonstrative laying of dummy explosives and explosive devices, hidden planting of a bomb at a facility and its subsequent explosion, explosion of a parked car stuffed with explosives, explosion of a moving car with explosives by a suicide bomber, throwing in of trap-mines camouflaged as martial items counting on curiosity and carelessness of citizens, sending of a bomb via mail to a particular recipient, taking and detention of hostages (androlepsy) with the use of weapons and explosive devices (further, ED).

Numerous forums are devoted to problems connected with terrorism, a lot of individuals long to be privy to struggle against it irrespective of their trade and level of competence. Many scientists, including Averjanova T.V., Kirsanov Z.I., Safonov I.I., Belkin R. S, Artamonov I.I., Brusnitsyn V. I, Varchenko I.A., etc. have been involved in this particular issue.

Modern science gives special attention to research in the field of technical and forensic tools and methods to combat terrorism. The use of special knowledge in this area contributes to more careful development of plans to counter terrorist attacks.

In legal terms terrorism is a crime against public security and has several special features. The Criminal Code of the Russian Federation treats terrorism as a set of criminal acts that endanger human lives, causing significant property damage for the purpose of violating public security, frightening the population or part thereof, or exerting influence on decision-making by governmental bodies.²

Terrorism is a crime, the main object of which is public safety, with its additional object being life, health and other interests of the people. It is subject to punishment presumed by Art. 205 ("Terrorism") of the Criminal Code. The main task in fight against terrorism is activity aimed in prevention, revealing and suppression of acts of extremism, creating an effective set of practical preventive measures.

In Israel they use a concept of profiling in fight against terrorism. Profiling is a method of countering acts of unlawful interference by means of psychological techniques. Profiling is the main tool accepted by the psychological service of the Israel Security Agency (ISA).

All the ISA personnel receive special training in the ISA Security Academy. The students are instructed in "classical" methods of search and "elimination" of threats among heaps of people, for example, among passengers of planes,

including methods of inspection, identification and isolation of potentially dangerous individuals.

Thus there must be a different approach to, say, passengers of the plane, a train or a bus, depending on circumstances and behavior of a person.

The ISA professionally trains experts - "selectors" so that they would be able to feel subtle nuances of human behavior, to notice slightest suspicious signs of presence of potential danger. In some cases with their help it was possible to reveal presence of explosives planted in passengers’ luggage even without their permission.

ISA management emphasizes that the prevention of terrorist attacks against Israeli passenger aircraft, especially explosions during flight, is a "top priority" in the work of the agency. Therefore, it has introduced unique standards and methods of work with passengers.

We shall present some examples of distinguishing marks of behavior and appearance of the suicide bomber, which govern Israeli "selectors" in their work.

**Behavioral signs:**

1. Concentration. The raised level of a suicide bomber’s concentration can be expressed in absence of reaction to attempts to contact him as well as to other external influences.

2. Mismatch of his behavior to surrounding conditions.

3. When approaching the place of intended attack the person in question can perform ritual prayer, thus making an impression of his talking to someone, or whispering something.

4. Behavior, characterized by lack of interest in the future. For example, buying a one-way ticket, ignoring small change while shopping, leaving valuable items.

5. Stiffness in motion caused by discomfort due to attachment to the explosives closely to body.

6. Presence of hands in pockets – for triggering ED.

7. Abundant perspiration which may indicate potential threat from the person object only in conjunction with a number of other signs.

8. Purposeful movement of the person in question in a straight line towards
an object (target), often paving his way directly through the crowd of people. Upon visual detecting of a target the suicide bomber “switches on” his so-called "Tunnel vision" which would not let him see what is happening around him.

**External signs:**

1. In order to conceal an explosive device (ED), attached to the body, they usually use unnaturally loose clothing, resulting in visual disproportions between head and body sizes. As a mark, there may serve the clothes obviously mismatching current weather conditions (for example, a coat on a hot day). There exists a history of use by suicide bombers of the uniforms of the Police and the Ministry of Defence officers. Visually, in such cases, the uniforms in question may contain a variety of disorders (absence of chevrons, discrepancy between lapel emblems and sleeve chevrons, color of upper and lower parts of the uniform and the headgear).

2. Very often, among elements of clothing (pants, scarf, jacket, etc.) there prevail those of white color, which - according to the Muslim tradition - testifies that the person is willing to commit "sacrifice".

3. For change of appearance the beard may be shaved, and hair, just before day of prospective act of terrorism, may be cut resulting in a marked contrast of the shaved skin color with that of the rest of the parts of the body.

4. Some signs of uneasiness:

   - Eyebrows brought together with their near ends slightly raised;
   - Eyes opened a little wider;
   - Mouth slightly opened or closed and lips firmly set.

5. Some signs of anger:

   - Eyebrows lowered and gathered (frowned).
   - There appear vertical lines (wrinkles) appear between eyebrows.
   - Lower eyelids are strained and can be either lifted or not.
   - Upper eyelids are strained.
   - Eyes are lamped, glance becomes heavy and steadfast.
   - Lips may be in two positions: densely compressed, with the stretched or lowered corners; or opened as if the person is shouting.

In the present work we would like to investigate a possibility of replacement of an Israeli "selector" by intelligent systems of biometric control.

Biometrics of today is a symbiosis of adaptation of new technologies to
methods of criminology developed in the course of many centuries, the most famous of which being dactyloscopy (fingerprint).

But you can detect not only "by fingers". Experts also attribute to biometrical properties the DNA code, shape of face and ears, iris and retinal capillary pattern, hand geometry, voice, handwriting, peculiarities of keyboard operating, and even the pattern of veins on the wrist.

Of course, not all biometric identification methods are equally reliable. Analysis of the DNA structure of DNA takes the leading position in the list of these methods, but it is the most complex and most expensive. The second place is shared by the iris and retina, followed by fingerprint, face and hand geometry, signature, voice, and keyboard "style" complete the list.

Whatever methods of biometric identification you would choose, all of them have their own advantages and disadvantages.

Iris.

Its uniqueness was proved in the middle of the twentieth century.

Specialized cameras and computers with special software are applied for scanning. The eye can be captured from a distance of 1-3 m. The newest devices can provide identification from longer distance and even on the move. For example, the Iris on the Move system produced by the SRI International captures the iris within three meters and can process 30 people per minute. I.e., such systems can be installed, for example, in the subway, airports, on squares and so on. The system works equally well in case when a person’s eye-sight is damaged but his iris is not.

However, its drawbacks include expensive software as well as the influence of age-related changes of iris and nervous system to the measurement result. Undeniable advantage of the iris-based identification technology is its being a non-contact one.

Singapore was the first country in the world to introduce iris biometric check of all those entering the country at a state level (from the middle of the 1990-s).

In the United Arab Emirates (U.A.E.) they have applied similar measures in 2002 - each of 32 boundary check points in the United Arab Emirates is equipped by eye-scanning devices, with the procedure being obligatory for all those who visits the state.
Eye retina.

It is more difficult to perform retina scanning. For this purpose they apply weak infra-red radiation to be directed through a pupil to blood vessels onto the back wall of an eye. It requires special and quite expensive camcorder. And, although this system has one of the lowest levels of denial of access to authorized users and almost 0% false permissions, its high cost prevents wide distribution. However, in some countries it is used to control access to specially classified installations. However, certain eye diseases such as cataract, can affect the quality of recognition.

Fingerprint.

At the heart of a method there remains uniqueness of drawing of papillary patterns on fingers. Imprint obtained by using a special scanner or sensor is converted into digital code and compared with previously introduced standard.

The identification process takes seconds. The device itself takes up little space.

The advantages of fingerprint biometrics methods are not only in convenience and reliability of use. It is also important that the fingerprint examination is under a legislative legal basis, and its results can be used as an argument in court.

Hand geometry.

Three-dimensional image of hand is constructed using a special device consisting of a video camera and a set of LEDs (being switched on one by one, they give different projections of the palm). Reliability of such identification is comparable to the reliability of the fingerprint system, but the device itself takes up more space.

Geometry of the person.

There are different systems – some of them produce a digital image of a human face on the basis of two-dimensional images, while others use three-dimensional ones. High-precision synthesis of images is based on dozens of parameters of characteristic elements, such as eyebrows, eyes, nose, lips, their "coordinates" and positional relationship. For "education" of the system they apply hundreds of thousands of images of human faces captured from different angles, under different lighting conditions, in sun-glasses and without them, with various hair styles, etc. “Education” of the system can be "completed" by inputting new images. During such "training" the system takes into account (remembers) process
of natural aging. It becomes possible to successfully identify a person even if the camera angle shooting has been modified (most systems allow rotation up to an angle of 45 degrees). Such systems are widely used to automatically detect the presence of the right person. However, a high-quality video camera is required to obtain good results while scanning takes considerable time (30 seconds). Unlike other biometric systems, face pattern recognition of a person can be used for general surveillance, usually in combination with cameras installed in public places. In the U.S., identification of the person is currently used in two main areas. First, in airports, where the use of such systems was proposed, and in some cases, implemented after the terrorist attacks of September 11. Some airports, including the Logan Airport in Boston, the TF Green in Providence (State of Rhode Island), the international airport of San Francisco and Fresno Airport in California have confirmed having implemented this technology.

Several major sporting events, such as the U.S. Cup football, held in Tampa, where photos of all visitors were captured during their passing into the stadium through the turnstiles and then compared with information contained in a secret database became the second scope of the given technology.

**Voice Recognition.**

Voice recognition is a convenient, but at the same time, not such a reliable way as the other biometric methods. The easiest way to recognize a person resembles that used today for voice dialing applied in cellular phones. A short word (a password) is registered and the user must pronounce this word each time he would like to call. The resulting spectrogram is compared with the one to have been recorded before. Another task is to identify the speaker. It involves more complex algorithms allowing to convert conjoint speech to the certain digital image consisting of information on the underlying tone of voice, rhythmic features of speech and specific features of pronunciation. To advantages of the system one can charge convenience of use, absence of any special equipment (if we don’t regard as such a voice recorder incorporated in many mobile phones of today), and to shortcomings - low recognition accuracy, expensive software, the sensitivity to the voice condition. For example, if you have a cold, or laryngitis, the system may fail to recognize you.

**Signature recognition.**

This technology is becoming a very popular alternative to signing by a pen. Here one can use special pens, or pressure-sensitive pads or their combination. Depending on the required degree of protection the identification algorithm can be simple (degree of coincidence of two images), or complicated, when apart from the images the dynamic signs of a writing are analyzed including degree of pressure, writing speed, distribution of sites with greater and lesser pressure, etc., so that “muscle memory” can be regarded as the subject of Biometric identification in this
case. Reliability of the method is not too high: signatures are still too easy to forge, and in cases of unstable signature system is faltering. However, the hardware is inexpensive, and there is a lot of respective software.

**Keyboard handwriting.**

The main feature used to create an identification code is dynamics of typing the code word. The method requires no special equipment. A standard keyboard is applied.

According to the internationally accepted terminology the biometric monitoring systems are characterized by accuracy of recognition in the following way:

- FAR (False Acceptance Rate) – error (probability) to take "a someone else" for "the user" / i.e. the error to skip a "someone else". This error generally varies from 10⁻³ to 10⁻⁶, although there are solutions and for FAR = 10⁻⁹.
- FRR (False Rejection Rate) - error (probability) to take "the user" for "a someone else" / deny access to "the user". This error is selected to be approximately 0.01, as it is believed that if there is one percent of such failures, it is not very critical, because you can allow for a few touches for users and thus artificially correct the error. In some cases there are special requirements (as in case of a large stream, so that not to create queues) to improve the FRR up to 0.001-0.0001.

In principle, the best algorithms already provide the following levels of errors:
- "let a someone else go" (FAR) - not more than 1 per billion;
- "do not miss the user" (FRR) - not less than 1 per 1,000.

Video surveillance systems have already become a familiar attribute of public places including the underground, railway stations, airports and big marts. With the help of these systems, the public security agencies and special investigative bodies have been monitoring the "facial streams" (a professional term) in order to detect well-known criminals and terrorists. Airlines provide for investigation of airport facilities to prevent intruders on board the aircraft. One may think of other scope of application of such systems for law enforcement agencies, special services and military units. Research show that accuracy of detection by an operator of famous people in the facial video stream, even in the best case, does not exceed 20%. Moreover, this level drops significantly with reducing of the period of the persons presence in the frame, load growth and fatigue of the operator. One must take into account that boredom and monotony of such work can not but adversely tell on the level of attention. The use of biometrics will increase the efficiency of standard video surveillance systems by 4-4.5 times.
Upon having received some video from the camera the automatic biometric system can detect suspicious persons by emotions expressed on their faces, "recognize" in the crowd already known terrorists whose data had been entered into the Ministry of Interior (MI) database. The program will be able to identify a criminal by his … gait.

For example, we need to establish surveillance of all the entrances to an airport. For this purpose we shall need to attach a few cameras at each entrance and connect them to one computer serviced by an operator on duty. He will not have to observe a dozen zones himself- it is the computer which - in case of detection of a suspicious passenger – will sound the alarm and will show his enlarged portrait on the screen. At the same time it will be possible to display the entry number or other area or the ground floor, where the "client" had been found. After that the operator will only pass the information over to guards so that they could detain the suspect and double-checked him with a frame-detector, gas analyzer or just search him after all.

It is possible to input into the program all the nuances of the human psyche which can only be reflected on the person’s face in case of evil intent, fear in anticipation of something awful, even if it is a sole move of an eyebrow, or a wrinkle to have suddenly formed on his forehead. The system can be thinking exactly in the same as a psychologist - "selector" would do when selecting a suspicious person. As for the gait, if the computer did not recognize its owner on the basis of the information which had been previously entered, it can signal about the danger in case it detects a creeping person or a citizen carrying a very heavy object, etc.

Application of biometric technology in CCTV is just a matter of time. Use of video surveillance abroad is regulated by law. For example:

**In Germany:**

Law prohibits any kind of secret surveillance over citizens. Public video surveillance is permitted. At that the cameras and their models should be clearly marked, and citizens must know where they are installed. An absolute ban is imposed on the secret phone-tapping of citizens, as well as on their e-mail inspection. In addition, a complete taboo is imposed on data gathering about citizens and personal shadowing of employees wherever it occurs - within the walls of the enterprise, outdoors or at home. All these activities can be conducted only in one case - a suspected criminal offense or a serious breach of official duties.

**In Israel**

Secret installing of video-cameras is prohibited.
In France

Installing of video-cameras and other technical means in France is strictly regulated. Video-surveillance is permitted in the country. However, prior to installation of a video-camera one must submit an application to the National Commission on Informatics and Freedoms.

In the Russian Federation there is no any Federal Law on the use of video surveillance and biometric control systems linked with the need for video surveillance over the places that may be subjected to a terrorist attack. We strongly believe that such a law is necessary and it should reflect the following provisions:

- First and foremost the law must reflect the provisions of the ETS Convention № 181 “On Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows” ³, which spelled out the provisions of protection of rights and freedoms of individuals in the processing of personal data including rights to privacy, personal and family secrets.

- Depersonalization of personal data – i.e. the actions that result in impossibility to determine appurtenance of any personal data to a particular subject of personal data;

- Confidentiality of personal data – i.e. a requirement mandatory for compliance by the operator or any other person to have got access to personal data to prevent their spread their distribution without consent of the subject of personal data or the presence of other lawful basis;

- Processing and use of biometric personal data can be carried out without consent of the subject of personal data in connection with administration of justice, as well as in the cases stipulated by Russian legislation on safety, Russian legislation concerning investigative activities, Russian legislation on public service, the penal legislation of the Russian Federation, the legislation of the Russian Federation on the Procedure for Exit from the Russian Federation and Entry in the Russian Federation;

- Use and storage of biometric personal data outside the information systems of personal data may only be carried out on such material data carriers and with application of such a technology of its storage, which would provide for protection of the data against unauthorized or accidental access, as well as from destruction,

³ ETS Convention № 181 “On Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows” // Strasbourg, November 8, 2001
modification, blocking, copying or distribution;

- Personal data on race or ethnic origin, political opinions, religious beliefs, health condition and sexual life can be automatically processed only in cases where national law provides appropriate guarantees. The same rule applies to any personal data relating to convictions ⁴;

- Security of personal data in the course of their being processed in information systems shall be provided by means of a system of protection of personal data, including institutional measures and means of information security products (including encryption (cryptographic) devices, means to prevent unauthorized access, information leakage via technical channels, software-and-technical impacts on technical equipment designed for processing personal data), as well as the IT means applied in the information system. Hardware and software must match the requirements stipulated by the Russian Federation legislation on protection of information.

- In the existing Federal Law № 781 "On approval of Regulations on securing personal data being processed in personal data systems" ⁵ the matters concerning collection and further processing of biometric personal data, which are most sensitive to a person have not been properly reflected. Meanwhile, backed by some sub-legislative departmental regulations as well as by some local regulations there expands the use of biometric personal data for various purposes, including the data being a part of a new generation of identification documents (such as passport and visa documents, pass-entry documents used in automated systems of access control), which are generated in government and in nongovernmental organizations, with inclusion in these documents of electronic data carriers, into which, in addition to commonly used information about the individual, a variety of biometric personal data concerning the owners of these documents have been entered, with subsequent processing of such data in respective information systems.

Operators creating information systems with application of biometric personal data face considerable difficulties in connection with absence in the Russian Federation of legislative regulation of use of the majority of the biometric personal data which are recommended by International Civil Aviation Organization and are widely applied in foreign countries in passport and visa and other certifying documents of new generation. Russian law currently governs application of only one type of biometric personal data, i.e. personal fingerprint

⁴ Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data //Strasbourg, January 28, 1981.

⁵ Government Resolution № 781 dated 17.11.2007 "On approval of Regulations on securing personal data being processed in personal data systems" //Rossiyskaya Gazeta, №260 of 21.11.2007.
data, and only in limited spheres of activities of the state authorities. As a result, development of information systems with application of biometric personal data in government agencies and non-governmental agencies is conducted on the basis of sub-legislative departmental regulations and local regulations, thus failing to meet the requirements of federal law.

Lack of adequate legal regulation in this area creates additional opportunities for invasion of privacy and abuses in this area.

In furtherance of the Federal Law the Russian Government released a number of laws and regulations, namely:

Russian Federation Government Resolution No. 687 dated 15 September 2008 “On enactment of provisions on particulars of processing of personal data without automated means” 6;

Russian Federation Government Resolution № 512 dated July 6, 2008 "On enactment of requirements to tangible media of biometric personal data and technologies of storage such data outside the information systems of personal data” 7;

Russian Federation Government Resolution № 781 dated November 17, 2007 "On approval of Regulations on securing personal data being processed in personal data systems".

By the Rossvyazkomnadzor (Federal Supervision Agency for Information Technologies and Mass Communications) order № 42 dated February 18, 2009 there was approved a sample form for notification on processing of personal data. 8


7 Russian Federation Government Resolution № 512 dated July 6, 2008 "On enactment of requirements to tangible media of biometric personal data and technologies of storage such data outside the information systems of personal data".

8 Order by Federal Supervision Agency for Information Technologies and Mass Communications dated February 18, 2009 № 42 whereby a sample form for notification on processing of personal data was approved // Has not been published.
Also in pursuance to paragraph 3 of the said Ordinance of FSTEC Russia and within its competence, there was approved a package of documents, containing "Technique for determining actual threats to securing personal data being processed in personal data systems" "Reference model of threats to securing personal data being processed in personal data systems" and also "Key activities on organization and maintenance support of securing personal data being processed in personal data systems"

Simultaneously, pursuant to the same point of the Ordinance by the FSS of Russia, there were approved "Typical requirements for organization and maintenance of encryption (cryptographic) means designed for protection of information that does not contain information classified as state secrets, in case of their application for securing personal data being processed in personal data systems" and "Guidelines for maintenance of security of personal data being processed in the personal data information systems by using automation tools, with the help of the cryptographic means".

In general, these sub-legislative regulations are aimed at protecting basically personal data and not the rights of citizens on obtaining and processing of their personal data in information systems, that does not meet the basic trends in the development of legislation on personal data in European countries within the framework of realization of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Keywords:
- Forensics
- Criminal procedure
- Biometric control
- Biometric identification (recognition)
- Iris recognition
- Counter-terrorism
- Personal data
- Automated data processing
- Protection of personal data
- Information systems