UDC 57.087.1:004:004.651
DOI: 10.7562/SE2011.1.01.07
Review article
www.safety.ni.ac.rs

MILJENKO VRBANEC[1]
FRANJO MAGUŠIĆ[2]

[1]Ministry of Interior of the Republic of Croatia, Police Department međimurska, Čakovec
[2] Ministry of Interior of the Republic of Croatia, Police Academy, Police College, Zagreb

[1] *mvrbanec@mup.hr*
[2]*fmagusic@fkz.hr*

APPLICATION OF BIOMETRIC SYSTEMS IN SAFETY

Abstract: *Development of civil society has created distinctive forms of public security and safety. Worldwide, there is a wide range of biometric systems, which today often come across as a modern approach to increasing public and workplace safety culture and process safety. The paper explains the basic criteria for the differentiation and classification, and the main special features of conventional and multimodal biometric systems, the possibility of comparison of biometric characteristics, the characteristics of alternative multimodal biometric models, building a database of biometric and possible errors, the possibility of stealing and misuse of biometric data. We will stress the police practice in the application of biometric systems.*

Key words: conventional biometric systems, multimodal biometric systems, databases, biometric errors, misuse of biometric data.

INTRODUCTION

Depending on the strategy and mission, there are various forms of safety and protection. For the purposes of this paper, we will get an insight into increased safety of critical infrastructure, "Business intelligence" and "Counterintelligence Business" integrated corporate security and private security using biometric systems. Because of the new strategy of terrorism and modern forms of information gathering and data, there are more biometric system which appear as a safer alternative in public safety and protection.

Corporate companies develop corporate safety while security managers often manage the business processes of corporate security.

Private security jobs can be performed in and around the perimeter of protected object space and around the protected person, within the perimeter security measures and protection as well as VIP (*Very Important Person*) persons, including public areas.

Information Security of the archive of biometric systems is significant, and may be exposed to various security threats and dangers that may threaten its segments and sometimes the entire system. Constitution and international law protect all forms of trade secrets by criminal sanctions.

Security and protection management can operate with different biometric systems and methods with and without the cooperation of people from a distance.

Biometrics can be defined as a model to identify people based on physical and physiological characteristics or behavioral characteristics, and refers to something that a person has or what a person knows to carry out personal identification. Some authors give a more general definition trying to explain how to deal with biometric identification of individuals according to their biological characteristics and behavioral characteristics. It is a sort of a methodology for solving the identification of the above criteria. In the very beginning of the performance and use of biometric systems, priority was given to physical characteristics in relation to behavioral characteristics. It was generally believed that the physical characteristics, in relation to behavioral, have "visibility". According to this view, it was assumed that the physical characteristics are more reliable than behavioral, since they tend to minor differences of variability within the groups and classes, rather than having the behavioral characteristics. Each biometric system has specific implementations that depends on the application of the methods used. The rapid development of technology has increased the need for reliable methods of identification in the field of forensic criminology.

The biometric methods are used in the preparation of identification documents, authorizing the entry and movement of the perimeter of the vulnerable areas and facilities, and in recent times, more and more for identification of persons. Biometric identification is based on the physical and physiological characteristics and peculiarities of behavior of certain persons, on identification patterns and recognition of biometric characteristics.

CONVENTIONAL BIOMETRIC SYSTEMS

Conventional systems use only one biometric method. Although cheaper and easier, these systems are susceptible to errors in identification, because in large populations some biometric characteristics are not unique for everybody. For example, two people can have very similar face. Conventional biometric systems use different measures of the same biometric features, thus trying to improve the performance of biometric

Paper is presented at the "International Conference Safety of Technical Systems in Living and Working Environment", Faculty of Occupational Safety in Niš, October 2011, Niš.

systems. A biometric system is essentially a system for recognizing patterns which use the unique identification to determine the authenticity of some physical and physiological and behavioral characteristics of individuals. System identification can be based either on a single biometric characteristic (one shot), which is a unimodal biometric model, or more biometric characteristics (more shots of biometric features) which is a multi-modal biometric model. Characteristics that should satisfy conventional biometric systems actually refer to only one condition and that is the possibility (impossibility) of fraud of identification systems. In this group of biometric characteristics we may include: fingerprint, iris, retina of the eye, and DNK. What is common for listed characteristic is high durability, permanence and universality, but also a relatively long time required for data processing. Quality conventional biometric system can be improved by using the traditional biometric features. These characteristics have certain qualities about people, but using these features is not possible to distinguish with absolute certainty the person. These are height, weight, gender, hair color and similar. By combining traditional biometric features with conventional biometric system, we get a multimodal biometric system that has characteristics of "strong" biometric features and the speed of traditional biometric features. Disadvantages of conventional biometric systems in relation to multimodal biometric systems are very obvious. The most obvious difference can be seen in the level of application of these systems. Conventional biometric systems can be applied to a "degree" of protection regardless of whether it was a strong, high and low biometric characteristic. Unlike conventional multimodal biometric systems, biometric systems cover the whole range of levels of "strength" which makes them more acceptable in the identification.

MULTIMODAL BIOMETRIC SYSTEMS

Multimodal systems use two or more biometric methods of identification [1]. Each method uses the algorithm to calculate the degree of matching identity. The resulting levels are adjusted and the final decision is made. A number of the methods used mean greater accuracy, but higher cost. There is no simple way of selecting a biometric method that will be used in a multimodal system. The methods depend on its use, but in most cases, the best results are achieved with a combination of biometric methods of large and medium accuracy. Disadvantages of multi-modal systems are expensive and compatibility. There is no single standard that would allow easy connection of biometric method, which further increases the cost because of the need to explore and fine-tuning of the system [2]. Multimodal biometrics means combining all of the previously mentioned biometric methods. If the practice uses a larger number of previously listed methods, you can build a secure IT system. In practice, it is a combination of physical characteristics and behaviors that include biometrics verification and identification. In practice they are used in the border police at border crossings to control entry or exit of persons, in the parameter protection to control access to any space, civilian and police identification, network security. Multimodal biometrics is used to support the standard procedures for verifying the identity or if the original documents and records are not possible to obtain sufficient data to describe a person (Figure 1).

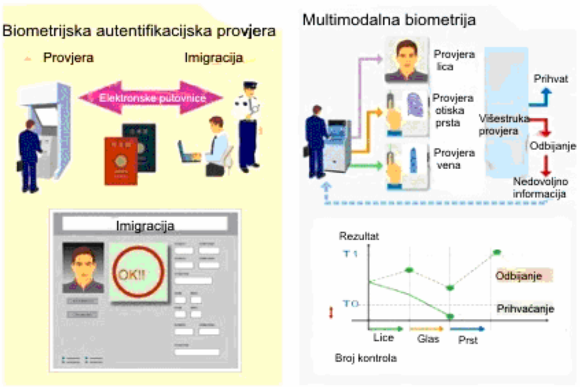

Figure 1. *An example of multimodal biometrics in the customs control [3]*

Recommended is combination of standard security mechanisms and biometric in order to prevent misuse. One example is a fake template fingerprints. If you use only one technique, such as fingerprint matching, it is possible a situation in which a third person has a false fingerprint that performs authentication on behalf of a person, which is questionable safety and security functions. It is evident that unlike conventional biometric system here at their disposal are three more biometric characteristics. As used in this system with biometric features, which are difficult to cheat ,there can also be used biometric characteristics that have some other characteristics which are acceptable according to the manner of collection, costs and capabilities of their storage in databases.

BIOMETRIC SYSTEM HISTORY

This process can be divided into several phases shown in Figure 2. Each biometric system has its own peculiarities of implementation depending on the application of the methods used. There are general features common to all systems. For the user, the first encounter with the system means biometric *enrollment* – registartion of his registration of biometric data and entry into the database.

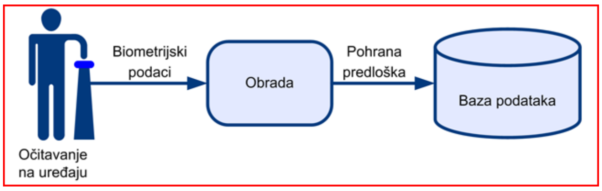

Figure 2. *Biometric enrollment [4]*

According to M. Bači [5], it is desirable to delete biometric data, because it is not advisable that they be be stored in the biometric records, since the identity of the user may be endangered. Each system deletion of biometric data should be carefully planned according to the strategy and goals of biometric systems.

Biometric passports are widely used in the world and the European Union. Deletion of records is governed by a general or special regulations.

In the case of the external borders of the EU, we will analyze a video surveillance system and deletion of their archives (registers) which are defined in the Catalogue of the EU Schengen external border control.

In the Republic of Slovenia, the border police on the basis of the Law on State Border [6] [7] may be in the area of border crossings and other areas along the border, to enable the provision of state border control to install the photography and recording devices. At the border crossing, a person must be warned about the camera and recording devices, according to the Law on Personal Data Protection ZVOP-1-UPB1 [8]. Archive clips and recorded data will be destroyed within one year unless the information is not required in criminal proceedings or proceedings concerning the offense. The Director General of Police issued a technical guidance on the use of video surveillance systems for the protection and supervision of police facilities, premises and surrounding facilities, since 1 January 2008. The instructions included the installation and the use of video surveillance in safety and control of police buildings, spaces and space around the buildings, recording the process of command, control, views and visions, logistics management systems, monitoring the implementation of this guide and how to access the individual images. Instructions are available on the intranet of the police of the Republic of Slovenia.

In Croatia, under the Law on State Border Protection [9], the border police has been authorized to supervise the state border for the purpose of searching, finding and determining the identity of the offender and the crime, do photography, imaging and video surveillance, and apply other technical aids. These devices can be automatic. Devices placed on the border crossings must be visible and people in such areas must be warned of such devices. When the border crossing record personal information, it is necessary to destroy such recordings within one year, unless they are required to prosecute perpetrators of an offense.

In the Republic of Serbia, Border Police is authorized to apply effective border safety activities, under the Law on State Border Protection [10], and to collect personal data and use this data in the records. The collection can be done by applying technical and other means. Technical and other means can be automatic, when used for photography, filming and video surveillance. At border crossings, equipment must be placed at a visible position with a visible warning sign. The archives of recordings of personal data collected by these devices and equipment are destroyed after five years, from the day of recording, unless they are required for criminal and misdemeanor proceedings.

In the Republic of Bosnia and Herzegovina, under the Law on Border Control [11] Border Police is authorized to take photographs, to record and use video surveillance, and apply other technical aids during the border control, with the aim of searching, finding or determining the identity of the perpetrators of crimes and offenses. Devices placed on the border crossings must be visible and people must be warned of such devices. If you are using the devices and other technological aids to capture personal data, archive recordings of these data must be destroyed within one year from the date of recording, unless it is necessary to prosecute perpetrators of an offense. The data collected during the reading of documents border are used in the form of records [12]. Also, it is allowed to collect, store and process other kind of data: fingerprints, palm prints and information about other physical identification marks, if they exist. These data records are kept for five years after entry into the records.

Modern identification documents contain biometric characteristics that the police use in criminal forensics to identify a person [2].

In the archives of the biometric systems, biometric features distinguish the following:

- **physical and physiological characteristics*:*** face, fingerprint, iris, retina of the eye, facial thermogram, body and hands, ears, DNK and
- **behavioral characteristics**: walk, smell, voice and signature.

In the very beginning of execution and use of biometric systems, priority was given to physical and physiological characteristics in comparison to behavioral characteristics. It was generally believed that physical and physiological characteristics in relation to behavioral have the "visibility. Physical and physiological characteristics are more reliable from behavioral since they differ within the groups. Today, there are a dozen biometric technologies that are being used or will be used soon [13].

PHYSICAL-PHYSIOLOGICAL CHARACTERISTICS

Face recognition

Face recognition is the most natural way of identification among the people. Nowadays, it is used as a method of biometric authentication, where the computer compares the user's current face image with the face stored in the register. There are two-dimensional and three-dimensional algorithms to compare faces.

Among the two-dimensional, the most famous algorithms are the algorithms of the face and facial metrics, used to solve the problems of face recognition. The algorithm -*eigenface* (*possible faces of human beings*) -compares the characteristic of facial feature with already existing images of human faces, usually with 100 to 150 faces. For each eigenface the degree of overlap with the user's face is calculated then the matrix of matching degrees stored as a user template that takes up very little disk space. The algorithm of facial metric analyzes the positions and relative distances between parts of the user's face (nose, mouth and eyes), and the information about them is written in the template. Two-dimensional algorithms can be easily fooled by a false image. The quality of recognition depends on the angle of light which falls on the face of the user and the change of the viewing angle of the camera. The problem is the change of face caused by aging, different hairstyles, makeup, facial expression and wearing glasses. Three-dimensional algorithms analyze and store 3D features and size of the parts of the face (Figure 3).

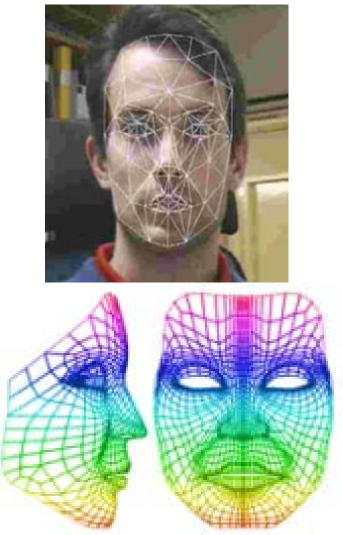

Figure 3. *Biometric face recognition pattern [3]*

This method avoids the problems that characterize the properties of two-dimensional methods, since three-dimensional model does not depend on facial expression, makeup or rotation of the head. A 3D method is so accurate that it can analyze the iris scan. Algorithms used to compare faces are faster than those for the comparison of the iris, and cameras for the retrieval of facial images are easier to handle.

Fingerprint

Fingerprint is the oldest and the most popular method of authentication. As a method for secure identification, it was known in ancient China, and since 1896 it has been used for criminal identification. Therefore, the identification of fingerprints has been inconvenient to users for a long period of time. Since this method became more popular, it also became more accepted. Fingerprint reader ca be found everywhere, and they can even be installed on PCs.

From the loaded images of prints, samples can be extracted by various methods. The method detailed analysis explains the relative positions of individual characteristics such as fingerprint ridge endings, bifurcations (places where two lines merge into one), points (a very short line) and the places where two lines intersect (Figure 4).

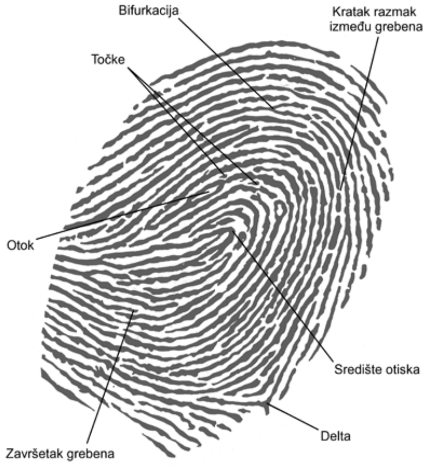

Figure 4. *Fingerprint and corresponding characteristics [2]*

The method of analyzing details has recently become very popular, but its main drawback is that it does not take into account the entire structure of the fingerprint, but only the position and direction of the characteristic points. These problems tend to improve the method of correlation, where one seeks to compare the entire sample prints. However, the method of correlation has a major drawback – it is overdependence on the position and rotation of the finger. The template obtained by this method is 2-3 times higher than the previously mentioned methods. Fingerprint has great potential to identify individuals. It is characterized by speed and accuracy and is suitable for rapid identification process in real time, this advantage is recognized by police practice for fast criminal processing. Reader prints available in the market are very cheap, but usually have no possibility of hardware fingerprint comparison.

Iris

The iris is the colored part of the eye surrounding the pupil. It consists of a network of radial lines (Figure 5) that is unique, the time fixed for each person and does not depend on the genetic parameters.

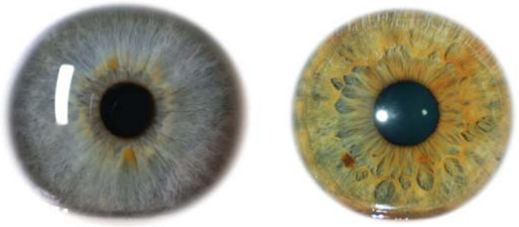

Figure 5. *The appearance of the iris of two different people [4]*

Reliable automatic identification of persons has long been an elusive goal. As with all pattern recognition, a key issue is the relationship between class and within-class variability: objects can be reliably classified only if the variability between different instances of the same class is less than the variability between different classes [14]. For example, in face recognition, difficulties arise from the fact that the face is a changing organ displaying a variety of expressions, as well as being a 3D object whose image depends on the viewing angle, position, lighting, equipment used, and age. Studies have shown that faces painted in a range of at least one year have errors, even the best current algorithms the 43% to 50% of errors. In contrast to this intra-class, variability between classes is limited because different faces possess the same basic set of features, in the same canonical geometry. For all these reasons, iris patterns become interesting as an alternative approach to the reliable recognition of persons when the picture is taken at distances of less then one meter and are more reliable especially when there is a need to search very large databases without the need for solving a large number of false matches. Although small in size (11 mm), and sometimes problematic to image, the iris has the great mathematical advantage that is pattern variability among different persons. As an additional benefit, because the inner part of the iris of the eye, it is well protected from the environment and stable over time. As a planar object its image is relatively insensitive to angle of illumination, a change in viewing angle cause only affine transformations; not even related to the deformation pattern caused by papillary dilation that is readily reversible. Finally, the ease of localizing eyes in faces, and the distinctive annular shape of the iris, facilitate reliable and precise isolation of this feature and the creation of a size-invariant representation. The iris begins to form around the third month of pregnancy. The structures and patterns that give it identity is formed by the eighth month, although pigment accretion can continue up to one year after birth. Its complex structure contains many different features such as arching ligaments, furrows, tops, rings, shells, freckles and so on. Iris color is determined mainly by the density of melanin pigment [15] in the front of her coat, and blue irises resulting from an absence of pigment: long wavelengths of light penetrate and are absorbed by the pigment epithelium, while shorter wavelengths are reflected and scattered are more reliable from the iris stroma.

The pattern of the iris is taken by monochrome camera hidden behind the mirror. Respondent in the mirror looks at a reflection of their own eye, and so allows the camera to grab an image of the iris. The camera automatically focuses and, if necessary, includes additional light. The resulting image is processed in a way that extracts the iris from the pupil and the rest of the eye. As width of the iris is not constant because it changes depending on the light or the radius of the pupil final image should be transformed before analysis. From this picture a special algorithm encodes the features and gets IrisCode record that occupies 512 KB. Such records are quickly and easily compared using the Hamming distance. The computer can compare millions of records in seconds and iris identification is therefore highly suitable. Because of its unique characteristics, iris is extremely difficult to forge, and due to rapid decomposition after death, using someone else's iris is nearly impossible.

Retina of the eye

The retina is a thin tissue of nerve cells and is located in the back of the eye (Figure 6). It is unique for each person in a network of blood capillaries which are steeped. It does not change throughout life, except in the case of glaucoma and diabetes. Retinal image is obtained by directing an infrared laser light into the interior of the eye. The reflected light contains information about the position of the capillaries.

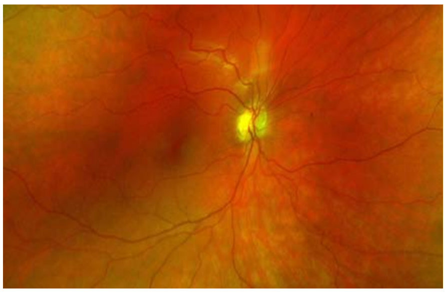

Figure 6. *Retina of the eye [4]*

The size of the form is 96 kB, the data are discriminatory and can be used for identification. Negative aspect of this method is its aversion, since it requires the penetration of laser light around the person against whom is done testing for identification. A trained operator to manage these complex systems is often needed.

Facial thermogram

Thermogram of the face is a new and promising biometric method that has not been used in an appropriate manner. The face of every human being is pervaded by an extensive network of blood vessels. The network is unique for every person, even for twins. The heat spreading can be read using infrared camera (Figure 7). The uniqueness of the obtained sample is large, and unlike in the methods of facial recognition, the image can be sampled regardless of the surrounding lighting. Its advantage is the fact that a respondent is required only to look at the camera.

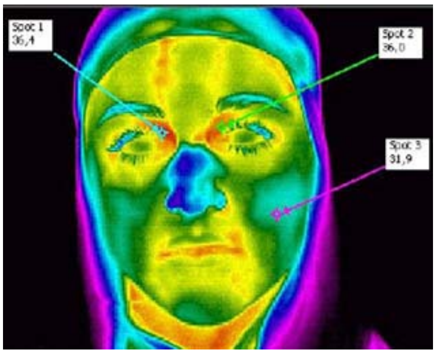

Figure 7. *Facial thermogram [4]*

Recognition works regardless of age, facial expression and aesthetic modifications. Due to high accuracy and speed, the method is suitable for identification. The reason it has not been used is the cost of necessary equipment and infrared cameras.

Thermograms of hand and body

Thermograms of hand and body have very similar features to facial thermogram (Figure 8 and 9). The images obtained by infrared camera describe the positions of blood vessels and veins that are unique to each person. Unlike facial thermogram, research method of thermogram hand and the body is still in its initial phase. Subcutaneous blood vessels on the human face and body products have the unique features, while the heat which penetrates through the tissue radiates out from the skin.

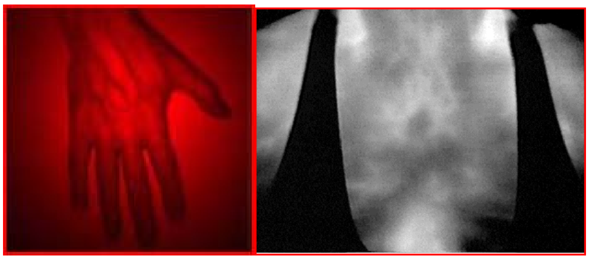

Figure 8. *Palm thermogram hand and body [4]*

Thermogram of face and body can be obtained from recording of the face and body by an infrared camera. It is believed that the thermogram of the face and body is unique for each person. Thermograms of the face and body are stable single biometric characteristic as they can be changed only by the surgery. There is the influence of ambient temperature, alcohol, drugs and medicines on thermogram image of the face and body. The disadvantage of this method is the price of infrared cameras, and thus obtained pictures take up a lot of spaces; therefore, this method is not suitable for large databases. Thermogram face and body gives us the possibility of classification, recognition and identification of faces and body parts (Figure 9).

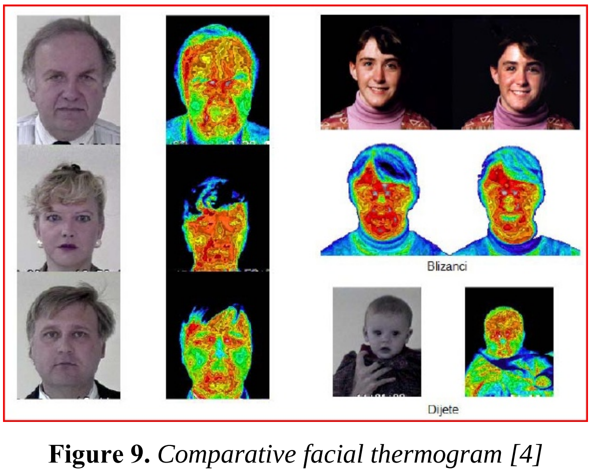

Figure 9. *Comparative facial thermogram [4]*

It can be used in medicine to detect certain diseases. It is used in situations when you need to make a rapid identification, extracting the desired person from the group. Identification can be performed under various lighting conditions, including in the dark. This method allows the detection without the cooperation of people and shooting from a distance.

Ear

Embossed ear shape and structure of crispy tissue on the surface of the ear are different among individuals (Fig. 10). Ear is not expected to have features unique to each person. Approaches to identify the ear based on the overlapping of the vectors of length of the convex points on the surface are more reliable from site boundary signs on the ear.

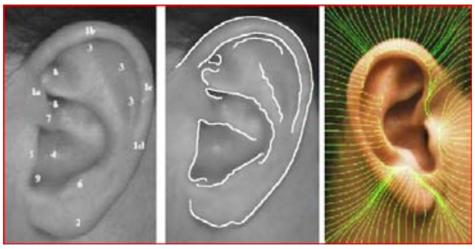

Figure 11. *Biometric characteristics of the ear [4]*

This method belongs to a group of intrusive techniques. Although this method gives promising results, we need additional research to answer the question:

- can ear feature extraction can be done on different conditions but with satisfactory reliability?
- If an ear is covered with hair, this method is inapplicable. It is necessary to find an answer: whether it is it possible to achieve a partial identification, and whether the use of thermogram can solve the problem.

DNA

DNA is a unique one-dimensional label for a person's individuality, used in forensics and identification (Figure 12). Most human DNA is identical for the entire human population, and only a relatively small number of specific locations on DNA presents individual variations.

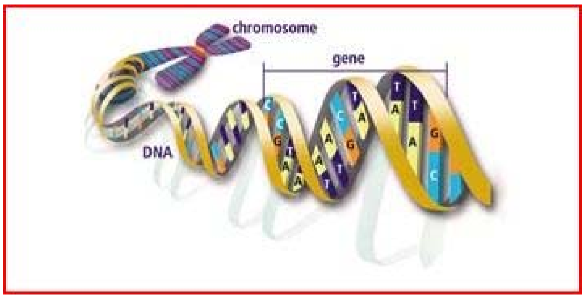

Figure 12. *Biometric characteristics of the DNA sample [2]*

These variations are represented either in the number of repetitions of basic block flow or less dysfunctional disorders of primary flow. The processes involved in the identification based on DNA determine whether two DNA samples derive from the same or different individuals.

BEHAVIOURAL CHARACTERISTICS

From the behavioral characteristics we have chosen: the dynamics of walking and voice.

Dynamic of walking

Human walking is a complex spatio-temporal behavior of biometrics. Its characteristic is that it is unique to each individual, but its distinctive characteristics make it possible to verify the identity according to the character, situation in which a person can be found and personal health. Walk is not fixed, especially in long periods of time, since people get tired. The sample is obtained from video recording made by a video camera (Figure 13).

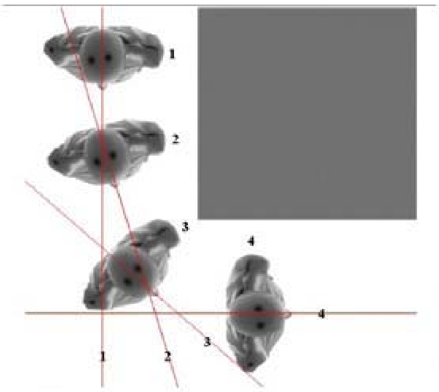

Figure 13. *Display angle under which a person avoids obstacles [3]*

All the checks of dynamics of walking are based on the personalities of several different movements of each joint when performing certain actions. Walk is a complex spatiotemporal behavior of biometrics. It is not unique to each individual, but it is sufficiently distinctive to enable authentication. Walk is a biometric characteristic of the behavior and must remain immutable, especially over a long period of time. Characteristics of walking are derived from analyzing video material (it is necessary to record a person walking). Inspection is based on a typical journey of a sequence of images used by people walking, and the verification is based on the characterization of several different movements of each articulated joint.

Voice

Characteristics of the human voice are completely determined by vocal tract, mouth, nasal cavity and other mechanisms for creating the voice of the human body (Figure 14). Since these characteristics are not sufficiently unique, they are not expected to enable identification of individuals from a large database of identity.

Figure 14. *Digitized voice sample [16]*

The aim of identification is to determine the voice of the speaker, comparing a stored pattern with the current pattern. It relies on the characteristics of the voice, not the pronunciation of individual words. Vocal characteristics depend on the structure of the vocal cords, throat and mouth, but also acquired characteristics (tempo and style of speech). To be able to do the comparison, it is necessary to identify "undeniable" voice (the voice of strangers) and compare it with the spoken voice.

BUILDING ALTERNATIVE MULTIMODAL BIOMETRIC MODELS

Each biometric system has four main modules, namely:

- sensor module which is responsible for the exclusion of features from raw data,
- feature extraction module whose task is to extract data from the a set of characteristics that best represent the characteristics of the raw data,
- module that provides a comparison of classification and comparison of secreted along with the feature templates and
- decision module whose task is to identify the information or the person.

According to the targeted needs of a biometric system and the BM (biometric) coefficients [5] [16], our practice is to order ITS multimodal biometric models.

SAFETY OF BIOMETRIC SYSTEMS

An information security management system is accompanied by the standard ISO / IEC 27001:2005, and ISO / IEC 27001:2005, which describes the implementation of certain measures of the previous standards and the ISO / IEC 27005: 2008 which describes the risk assessment in the field of information security.

Corporate companies develop a corporate security for the achievement of the company's success.

Private [17] [18] and corporate security will be adjusted to control risks in the company by the international standard ISO 31000: 2009 (Risk Management Guidelines on principles and implementation of risk management).

By K. Antoliš [19] a special hazard may be information security of wireless network transmission of biometric information and data.

As it is the case with many technologies that have recently experienced strong growth and achieved interesting advances, there are some effects that provoked some criticism, fear and concern for the personal health in public, regarding biometry. According to the research by M. Vrbanac [20], biometrics can be associated with serious violations of justice, if the infatuation possibilities of new technology, hence the minimum extent of information security and civil control.

In practice, we can see that:

- DNA can be found at the crime scene,
- other people identities can be connected with their biometric characteristics, under false pretenses without inducing doubt
- biometric data archive can be used for criminal acts.

Identity theft

Questions about identity theft through biometrics use have not yet been resolved. If a credit card number is stolen from an individual, this can cause many problems. In case when this person has a scan of the iris of the eye stolen, and it is used by an unknown person to "identify" as someone who is not (change of identity), then the damage done may be irreparable. It is often the case that the amount of biometric technology used in the public are without the adequate security and protection measures that would protect the collected personal information about individuals. It should be noted also that the biometric solutions for identity theft is as good as the information in a database that is used to verify identity. The problems of obtaining accurate and useful initial information confirmed by the current troubles with the so-called "No Fly List" U.S. Dept. of Homeland Security. Specifically, the assumption is that after the correct storage of the initial information, any future computer error or vandalism (hacking) prevent the biometrics of 100% resistance to identity theft.

Privacy

Although biometrics is often given as a tool in order to fight crime, privacy rights defenders say fears that biometrics could be used for a denial of personal liberty and law abiding citizens. The development of a number of new technologies in addition of biometrics such as digital video, infrared, X-ray, wireless technology, GPS, image scanning, voice recognition, DNA and monitoring of brain waves - are provided by government agencies a host of new ways to "search" individuals and collect endless archives database of information about law abiding citizens.

Sociological questions

As time progresses and technology advances, there are more and more private companies and public services that use biometrics for safe and accurate identification. However, this progress generates many questions in the society where great number of people may not be familiar with the procedure itself. Here are some ethical issues that the society assigns to biometrics:

- Integrity of the body. Some believe that this technology could cause body injury to an individual, when tools and methods that are not healthy for humans are used. For example, scanning, the use of the thermogram, etc.
- Privacy of personal information. There are concerns whether our personal information taken through biometric methods will be abused, tampered with, sold to interest groups, stolen and made public, unauthorized reallocated or in copied from biometric database. Also, data collected using biometrics can be used in an unauthorized manner without the consent of the individual.

As safety culture becomes more and more familiar with the procedures in biometrics and its widespread usage, these issues will become increasingly apparent. The design technology used at border crossings that have electronic readers can read the chip in the card and thus confirm the information present in the card and the passport. This procedure allows the increased efficiency and accuracy of identification of people at border crossings. The example is a system called CANPAS currently used at several major airports in the United States. For this purpose, special units have been placed at the airports and they are used for taking digital photographs of the human eye, for the purpose of identification.

Some biometric techniques can be forged by a copy:

- rubber fingerprints in latex,
- modified recording of a voice of a person,
- mask or facial photographs and
- contact lens or photography of an iris.

CONCLUSION

Modern computer systems are being overwhelmingly used, but the special attention should be paid to the use of biometric system. In the area of safety and protection, they can be found in the perimeters of critical infrastructure, business intelligence and business counterintelligence, integral corporate security, private security, insurance, public performances, events and gatherings, the surveillance of public areas, the use of archives for telecommunications providers, monitoring traffic roads and other needs.

Biometric characteristics can be documented by conventional and multimodal biometric systems. Conventional systems use a single biometric method while multi-modal systems use two or more biometric methods.

Archives of biometric information and data require special security and competencies regarding archiving (recording) and deleting. The period of data storage and the user guides should be designed for all users; people privacy should be maintained and the abuse of biometric characteristics should be prevented.

The following physical and physiological biometric features were selected: identification of the face, fingerprint, iris, retina of the eye, facial thermogram, palm and body thermogram, ear, and DNA. For each feature, we tried to discuss economic viability, development, implementation in the biometric systems, reliability, the consent of the person, and for some of them, even the size of the memory (in kB).

The behavioral characteristics that have been explained are walk dynamic and voice with its features.

The applicability of biometric information and data does not depend on the alternative platforms of multimodal biometric models.

Information security develops information security management using recognizable and binding international standards. Nowadays, it is extremely important to emphasize the wireless network security in the transmission of biometric information and data.

Society, project management and each individual should develop and comply with IT security culture and develop transparent measures of surveillance equipment, biometric devices and systems that do not make the detrimental consequences on the health of our citizens and employees in public and private sectors.

REFERENCES

[1] Cert.Carnet: Biometrija, CCert-Pubdoc-2006-09-167

[2] Arhiva Ministarstva unutarnjih poslova Republike Hrvatske, 2004-2008, Zagreb

[3] B. Pavišić, D. Modly, P. Veić: Kriminalistika (Knjiga I), Golden marketing-Tehnička knjiga, 2006, Zagreb

[4] L. Nimac: Pregled biometrijskih metoda identifikacije-Seminar, MUP RH, 2004, Zagreb

[5] Miroslav. Bača, Marko. Antonić, Franjo. Magušić: Upgrading Existing Biometric Security Systems by Implementing the Concept of Cancelable Biometrics, 19thCentral Europen Conference on Information and Intelligent Systems, September 24-26, 2008, Varaždin, Croatia, pp. 421-425

[6] Zakon o nadzoru državne meje, Uradni list RS št. 60/2007. i 35/2010, oznaka zakona ZNDM-2-UPB-1, Ljubljana: Uradni list RS, 2007, 2010.

[7] Pravilnik o izvajanju Zakon o nadzoru državne meje, Uradni list RS št. 116/2007, Ljubljana: Uradni list RS, 2007.

[8] Zakon o vartsvu osebnih podatkov ZVOP-1-UPB1, Uradni list RS št. 94/2007, Ljubljana: Uradni list RS, 2007.

[9] Zakon o nadzoru državne granice, NN 173/04, 141/06, 08/07, 146/08, Zagreb: Narodne novine

[10] Zakon o zaštiti državne granice, Sl. Glasnik 97/08, Beograd: JP Službeni glasnik

[11] Zakon o graničnoj kontroli, Sl. Glasnik 53/09, Sarajevo: JP NIO Službeni list BiH

[12] Zakon o graničnoj kontroli, Sl. Glasnik 54/10, Sarajevo: JP NIO Službeni list BiH

[13] I. Vasiljević: Biometrija- Seminar, MUP RH, 2007, Zagreb

[14] M. Bača: Odabrane teme iz biometrije, poglavlje 4, FOI, 2005, Varaždin

[15] Identification in Networked Society, Kluwer Academic Publishers Jan, A., Bolle, R., Pankanti,S., „Biometrics“, Kluwer Academic Publisher, 1999.

[16] L. Gyergyek, i dr: Uvod u raspoznavanje uzoraka, Tehnička knjiga , 1988, Zagreb

[17] Nemet,Charles P. Private security & public safety/ Charles Nemeth, K.C.Poulin-1. st ed. P.cm., Pearson Education,Inc.Upper Saddle River, New Jersey 07458

[18] http://www.coess.org/pdf/final-study.PDF (26.06.2011.)

[19] K. Antoliš, Simona. Strmečki, F. Magušić: Informacijska sigurnost i inteligentni transportni sustavi, Suvremeni promet, Vol.28 N° 5, 2008, pp. 353-355

[20] M. Vrbanec: Izgradnja biometrijskog kriminalističko identifikacijskog modela, Magistarski rad, FOI, 2008, Varaždin

BIOGRAPHY

Miljenko Vrbanec was born 1970. in Čakovec, Croatia. He got his Master's degree from Faculty of Organisation and Informatics in Varaždin in the field of social sciences information sciences, and received Master of Science degree of from University of Zagreb.

His main research interests include biometric indentification models and application biometric system to security procedures. He works as chief of police station of the Croatian Ministry of interior.