HAAGA-HELIA
University of Applied Sciences

Biometric Authentication. Types of biometric identifiers

Aleksandra Babich

Bachelor's Thesis

Degree Programme in Business Information Technology

2012

HAAGA-HELIA
University of Applied Sciences

Abstract

Date of presentation

BITE

Author or authors Aleksandra Babich	**Group or year of entry** 2012
Title of report Biometric authentication. Types of biomentric identifiers	**Number of pages** 53
Teacher(s) or supervisor(s) Markku Somerkivi	

The purpose of this thesis was to build clear understanding biometrics and biometrics identifiers and also to look closely on the methods of biometrics.

In this work such methods as data collecting, content analysis were applied. The information is taken from multiple internet resources, TV reports, magazines and newspapers and books.

The study contains information about the history of biometrics and the process of its development, characteristics that people consider to be the advantages and disadvantages of biometrics, and also about two types of biometric identifiers and methods that belong to these types.

The results of the study were the most popular methods of biometrics, their advantages and disadvantages.

Keywords
Biometrics, authentication, identification, verification, physical type of biometrics, behavior type of biometrics

Table of contents

1 Introduction

The most well known and popular situation that everybody of us meet: you come home and find out that the keys from home are lost. What can be done to be sure that this situation will not repeat? The easiest way to open the door is to use what each of us has: voice, hands, eyes, fingerprints.

Nowadays the interest to different systems of biometric identification among users of computer systems grows up. Spheres of use of technologies of identification are not bounded. Government and private organizations are interested in technologies of face recognition as it allows increasing the level of protection of secret and confidential information. Companies that deal in the sphere of information technologies are interested in technologies of fingerprints, face, voice, iris recognition in order to prevent penetration of outside people to their net.

Many famous people point out the increase popularity of biometric systems. Preferences are given to different methods of biometrics. For example, the president of Microsoft Bill Gates stated: "Biometric technologies, those that use voice, will be one of the most important IT innovations of the next several years." (http://www.usfst.com/article/Demystifying-Voice-Biometrics--The-Future-of-Security-is-Available-Today/ cited 21.04.2012)

Even most of the people come up with such a problem of losing the passwords, forgetting them or even worth, when the passports are stolen. People who agitate for using biometrics point out that those problems with password will not be urgent with the use of biometrics. Bill Gates said at the 2007 RSA Conference: "Passwords are not only weak; passwords have a huge problem... If you get more and more of them, the worse it is. Passwords are a headache for everyone, whether at home or the office, on your PC or your cell phone."(http://www.technewsworld.com/story/59728.html cited 13.04.2012)

But even now in different computer nets we can find sites, access to which are regulated by methods of biometrics.

Opportunities to recognise the person basing on his/her biometric characteristics are well-known and widely discussed many years. Nevertheless, many people consider such technique of identification to be the matter of future and sure that it remains the matter of fantastic films because the practical use of biometric methods are too expensive. But there are people who fully support the idea of use biometrics. They find such idea cool and interesting. According to the Global Consumer Biometric Study which was taken by the Ponemon Institute in 2006 about 66% consumers consider biometrics the ideal method to combat with fraud and identity theft. The results of U.S. PC Users Security Survey by Zoomerang in 2005 show that consumers want to have biometric features in their new PCs. (http://www.technewsworld.com/story/59728.html cited 13.04.2012)

So, we have people who do not even come across of biometrics and do not believe of its reality and people who believe that biometrics is rather helpful and will have great future in the sphere of security.

Due to such attitude towards biometrics the main idea of this paper is to build full and understandable picture of biometrics and its methods. People should realize that biometrics is a constant developed science with its pluses and minuses. Each method of biometrics has its strong and weak sides and it depends on the person what method to use.

1.1 Biometric authentication

The word "biometrics" came from Greek and we can divide it into two roots: "bio" means life and "metrics" – to measure.
(http://www.biometrics.gov/documents/biohistory.pdf cited 25.02.2012)

Biometrical authentication or just biometrics is the process of making shure that the person is who he claims to be. Authentication of identity of the user can be done in

three ways: 1) something that person knows(password), 2) something the person has (key, special card), 3) something the person is (fingerprints, footprint).

Biometrics is based on anatomic uniqueness of a person and as follow it can be used for biometric identification of a person. Unique characteristics can be used to prevent unauthorized access to the system with the help of automazed method of biometric contorl which , by checking unique pysiological features or behaviour characteristics identifies the person.(http://en.wikipedia.org/wiki/Biometrics cited 21.02.2012)

1.2 History of Biometrics

The first ideas of biometrics appeared many years ago. In general , it is very difficult to say that biometrics appeared it this place at this time. The ideas to use parts of human body and even the ways to use this ideas appeared all over the world. First evidences of biometrics appeared in 29.000BC when the cavemen used their fingerprints to sign their drawings.

Babylonians used the same very way to sign business transactions which were in the form of clay tablets.(Wikipedia, cited 21.02.2012)

The first recorded evidence of using biometric authentication was in ancient Egypt. One of the administrators , during the construction of great pyramid of Khufu, tried to systemize the process of providing food to workers. He recorded all information about the worker(name, age, work unit, posotion , occupation, etc) . But after the fact that many workers cheated him, the administrator began to record the physical and behavioral characteristics.

In 14th century in China biometric authentication was rather popular among merchants . Technology of early biometrics was rather simple: paper with ink allowed to take palm print s and footprints of children in order to differentiate them from other. It is interesting to point out that in spite of its simplicity this way of bimetric authentication is still in use and is the most popular.

In 1823 Jaonnes Evangelista Purkinje , a Czech physiologist and biologist, published his scientific work where he studied papilary ridges of hands and feet. He was the first who tried to categorize fingerprint pattens.

In 1858 sir William James Herschel, a British officer in India, was the first European who used his fingerprints for identification. Beliving that fingerprints were unique , Herschel used them to sign documents. (Wikipedia, cited 17.2.2012)

In 1870 anthropologist Alphonse Bertillon was looking for the way to identify convicted criminals. He used not only palmprints and footprints but also body movements and all kinds of marks on the body. His ideas, known as Bertillonage, became popuplar in American and British police forces and helped to minimize to circle of suspects. The most interesting fact: fingerprints , the most popular way of biometrics nowadays , were included in Bertillon´s system , but Brtillon himself did not consider it to be important.(About.com Terrorism Issues, 01.03.2012)

In 1880 Henry Fauld wrote a letter to Sir Charles Darwin wherr he tried to explain a system to classify fingerprints, and asked for help. Darwin could not help Fauld but forwarded his letter to Sir Francis Galton. The correspondence between Faulds and Galton was not very intensive, but nevertheless they produced very similar classification systems . Consider, that Faulds was the first European who insisted on the meaning of fingerprints in the identification of criminals. (Wikipedia, cited 10.2.2012 11:08)

In 1892 Sir Francis Galton publish his book " Finger Prints" where three main fingerprints pattens were described : loops, whorls , arches. It should be pointed out that he offerd to use fingerprints from all 10 fingers.

Mark Twain is considered to be the first writer who used biometric in his works. "The Tradegy of Pudd`s head Wilson" is the srory of a man, young lawyer, whose hobby was to collect fingerprints. His relationships with people around him was rather intensive. People did not understand his hobby, considered him to be eccentric. But

knowlegde of the young lawyer helped to save life and freedom of a person who was wrongly accused of murder.

Futher , biometrics began more and more popular:
1903- New York State Prison began systematic use of fingerprints in U.S for criminals. Some defected of Bertillon System was found due to two men, identical twins. According to Bertillon system they had the same measurements and could not differenciate them.

1904-Kansas ans St. Louis Police Departments used fingerprints.
1905 –U.S Army used fingerprints.
1906-U.S Navy used fingerprints.
1908 –U.S Marine Corps used fingerprints.

In 1960s Automated fingerprint identification system was created.Also this time is also known as the starting point of face recognition. W. Bledsoe is the father of face recognition. It was he who insisted to locate eyes, nose, mouth, ears to the photografer.

1965- begnning of automated signature recognition research.

1969- FBI (Federal Bureau of Investigation) tried to automize the process of fingerprint identification.

Goldstein, Harmon and Lesk developed the idea of face recognition in 1980. They used 21 specific subjective makers (color of hair, thickness of lips. etc.) in order to automate face recognition.

Also , at this very time appeared the fist model of behavioral components of speech which was produced by Dr.Joseph Perkell. In his work he used X-rays.

1974- the first hand geometry system appeared . In this very year Standford Research Institute and National Physical Laboratory began to work on a signature recognition.

1980- the term "biometrics" began to be used to describe methods of automated human/person identification.

1983 -the U.S Department of Energy began to test biometrics at Sandia National Lab and the Department of Defense began to test at Naval Postgraduate School.

1985 –the first retinal scanning was created and it was used for secure access to the Defense Department in the Naval Postgraduate School.

In the middle of 80th state Callifornia began to collect fingerprints for driver license applications .

1986 the foundation of the first biometric association was created , International Biometric Association.

1990- the iris recognition technology was created by Daugman of Cambridge University.
1991- Biometric Association was founded in United Kingdom.
1992-the immigration system used fingerprints for the first time.
1994- the U.S. installed the boarding system which was based on hand geometry.
1997- the first Biometric Test Centre was founded
2002- adoption of the first biometric standards.
(National Biometric, cited 22.02.2012)

1.3 Biometric functionality

One of the most asked question: what biological meassuremts is biometrics? The answer is quite simpe and obvious: any. Any characteristic can serve biometrics if it has the following desirable properties:

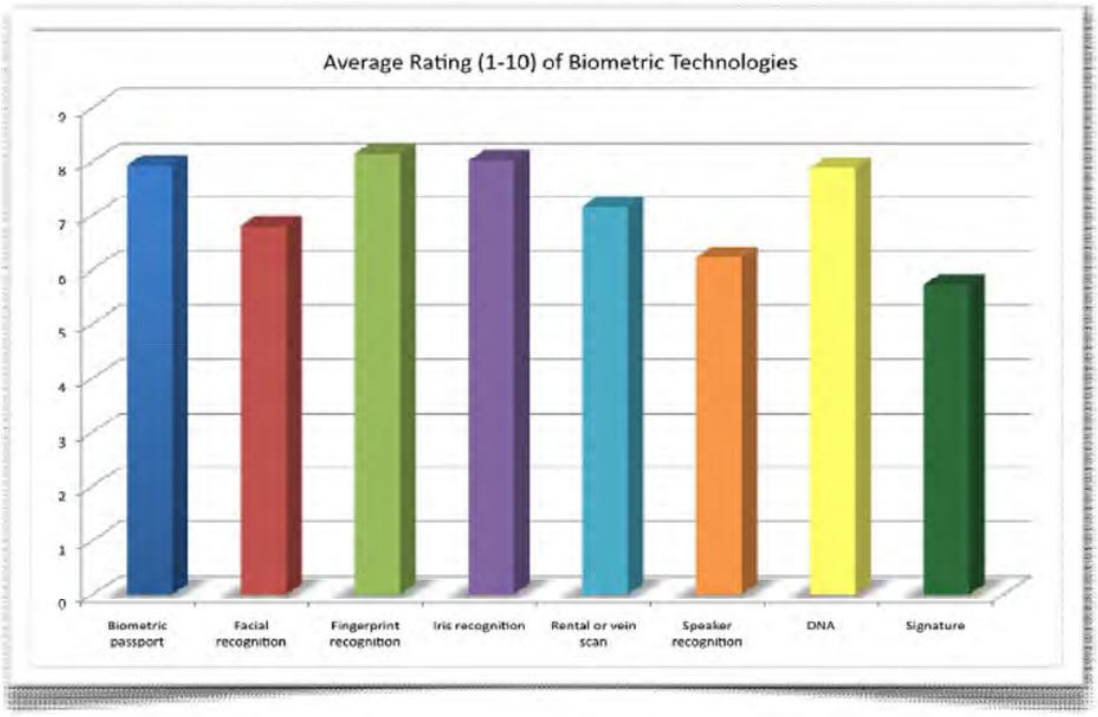
1) Universality- something that each person has
2) Uniqueness- something that separates this very person from others. This means that not all characters can be suitable for biometrics.

3) Permanence- biometric measurement should be constant over time for each person.
4) Measurability (collectability)- it should be easy to measure, should not demand too much time and costs
5) Perfomance- speed, accuracy and robustness
6) Acceptability- how well people accept biometrics
7) Circumvention- how easy it is to fool the system. This becomes very important as the value of information grows rapidly. It gives an opportunity to be ready to two kinds of attacks: 1)privacy attack when the attacker access to the data to which he is not authorized, and 2) subversive attack when the attacker recieves an opportunity to manipulate the system.

The list of these factors were defined by A.K Jain,R. Bolle and S. Pankanti in there book " Biometrics. Personal Identification in Network Society" which was published in 1999. (A Century of Biometrics, cited 21.02.2012)

Students of the Gearge Washington University questioned people about their attitude towards biometric thechnologies and different methods of it.Noteworthy, that more that half of all people that took part in questioning (77%) considered biometric to be rather useful tool for authentication of identity.16%told that they liked some of the advantages that biometrics offers. And only 7% were against of biometrics.

Concerning the methods of biometric, the favorite was fingerprint recognition, the second place- iris recognition. The following picture shows the preferences of common people in choosing the methods of biometrics.



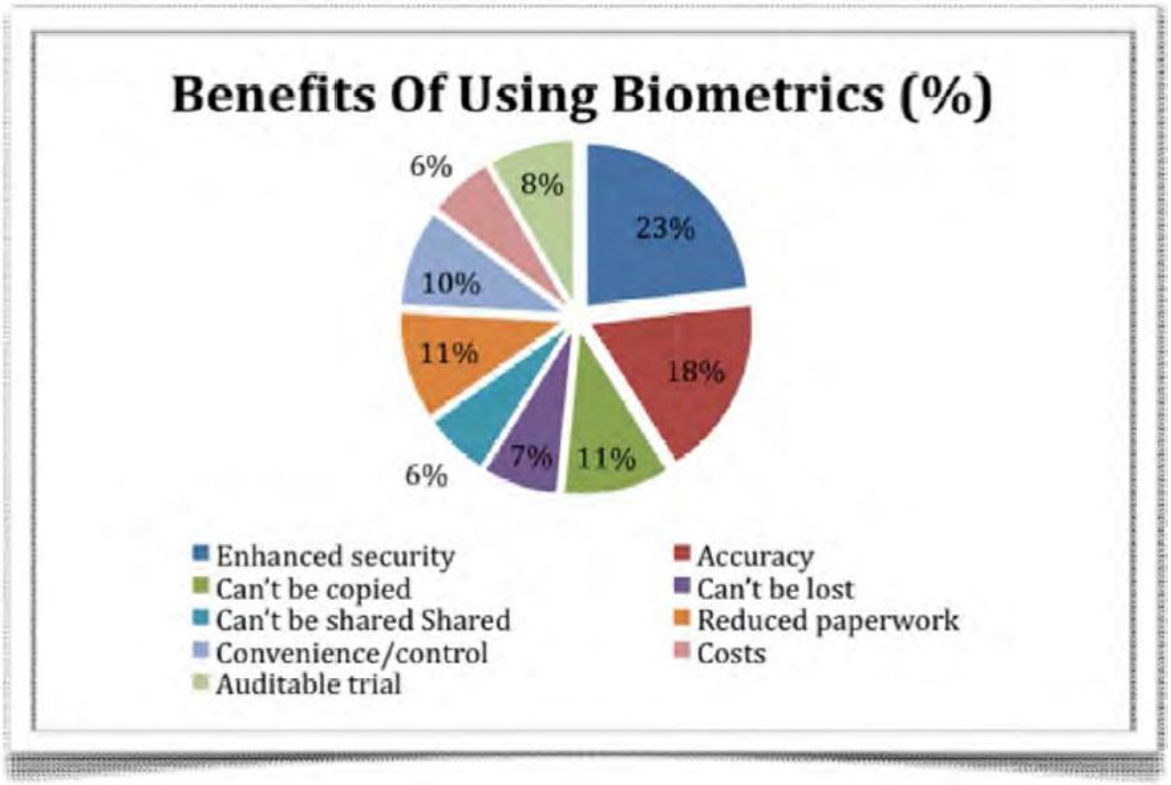
Picture 1. Preferences of common people in choosing the methods of biometrics

Here is the table of advantages and disadvantages of biometrics:

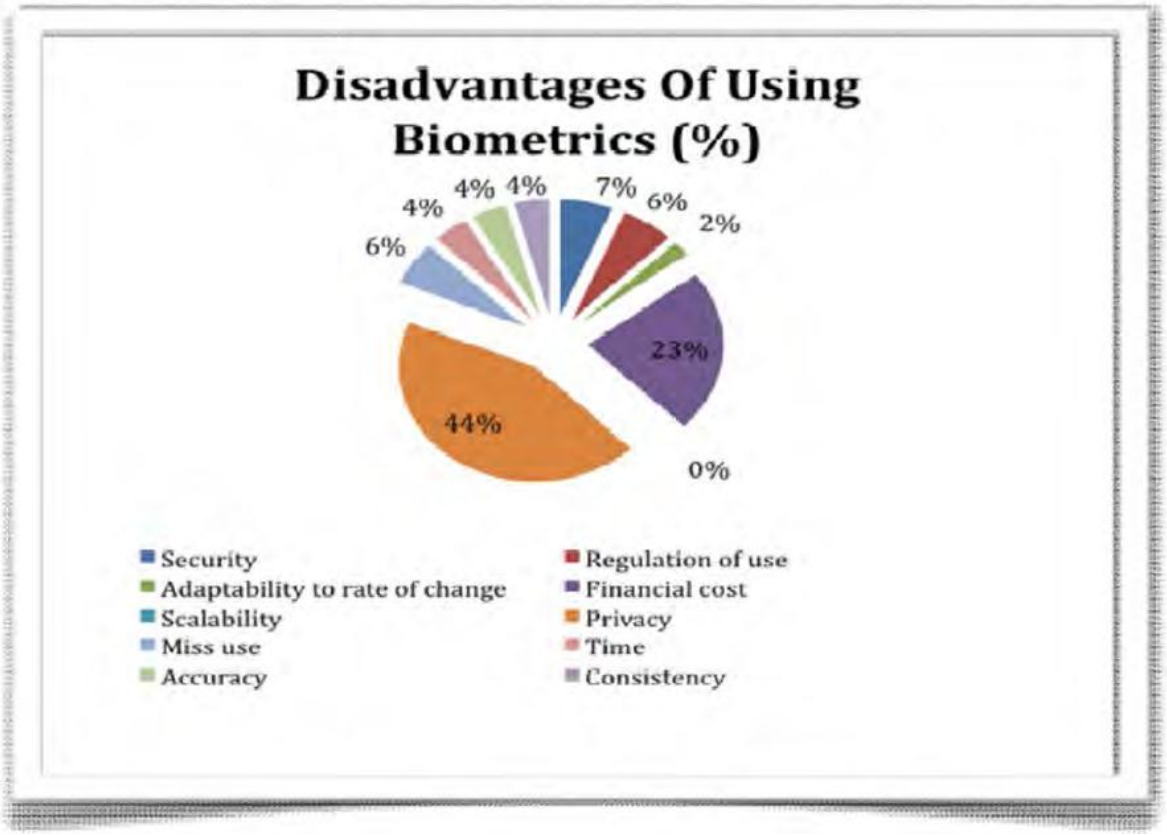
No	Advantages	Disadvantages
1	Increase security	Security
2	Can not be copied	Adaptability to rate of change
3	Can not be shared	Scalability
4	Convinience	Miss use
5	Auditable trial	Regulation of use
6	Accuracy	Accuracy
7	Can not be lost	Financial cost
8	Minimaze paper work	Privacy
9	Costs	Time

Security is considered to be the greatest adavntage of biometrics, on the second position is accuracy.The greatest disadvantages of biometrics are invasion of privacy and costs of implementation.

The second two pictures will show us what people really appreciate in biometrics and what disadvantages they consider to be criticall.



Picture 2. Appreciations of advantages



Picture 3. The critical disadvantages

(TechCast Article Series Use Of Biometrics, cited 01.03.2012)

1.4 Indicators of biometric systems

Different biometric systems diifer according to their indicators:

1) Through-put capacity: characterize by the time that is necessary to serve one user. It depends on condition of work (whether we do authentication or identification). Identification will take more time than authentication as the system needs to compare all examples from database. In condition of authentication user should type personal code and the system will compare it with only one example.
2) Price: one of the most important factors .
3) Reliability of identification: there are two probabilities: a) probbility of " False Reject Rate" when the system does not recognise its user and b) "False Accept Rate"when the system recognise the wrong person as its user. The mistake of "false accept" is more dangerous from the security poin of view that the "false reject" , but the mistake of "false reject" makes the sytem uncomfortable to use as it do not recognise the user from the first time. These two probabilities are connected with each other, and the attempt to minimize one of them encreases the second one. That is why in practice the system should come to compromise. This field is the most difficult in biometrics as the task of the system is to recognise less wrong people and to reject less right users.
4) Simplicity and convinience in use: these indicators determine the consumer characteristic of biometric system. The most popular questions:How easy is it to install this system? Does the system require the active actions of the user or is the receiving of characteristics too difficult? Does the system require additional trainning?
5) Degree of psyhological comfort: shows how different systems and methods can generate negative reaction of the user , fear or doubt.
6) Ability to play tricks with the system: ability to use different " dublicates" such as casts, tape recording, etc. The most vulnerable systems consider to be: systems of voice recognition and face recognition.

7) Method of collation: decide if the user needs to put his finger into the collation, or it will be enough just to say a special phrase or to have a look to the camera. There are two ways of ollation: distant and contact. Thechnology of distant collation allows to increase the through-put capacity and to avoid regular cleaning of collation.
8) Accuracy of authentication: differs from the systems which use passwords.
9) Productivity: depends on such factors as accuracy, price, integration and comfort of use.
10) Expenditures:for many appliations , such as registration in personal computer or network, the additional expanditures for realization of biometric tecnologies are very important. Some applications do not allow large equipment , stimulating minimization of data units. Nowadays a lot of powerful and cheap data units appear and we can use biometrics in new applications for identifiation and this, in its turn , makes it cheaper.
11) Integration: integration of several biometric systems in to one device improve characteristics of the systems . Authentication is not useful when the system can not garantee that the user gives neccessary characteristics.
12) Confidentiality: rises the question: Wherether the biometric data will be used for spying and integration to private life. That is why there is an agreement between the produces that decide to save in database not the picture of a fingerprint but, received from this picture, a key. This key makes impossible to restore the picture of a fingerprint.(SuperMegaOy.ru cited 22.02.2012)

1.5 Difference between biometric authentication and identification

Authentication... Identification... Sometime it is very difficult to understand the difference between these two words and actions they perform.

Authentication and identification are closely connected with verification and authorization.

Biometric Identification is the automatic identification of living individuals by using their physiological and behavioral characteristics; "negative identification can only be

accomplished through biometric identification"; "if a pin or password is lost or forgotten it can be changed and reissued but a biometric identification cannot.

For example, there is a database where all the photos of users are collected. Suddenly, somebody comes to you and greets you. You want to know who it is, and put the picture of this person to the system. The system is looking for the match. When the match is found the system represents the full information about this person.

Verification means verifying person's identity. A guy comes to you and tells his name, Bill. You take the picture of Bill and put it to the system. The system finds the Bill's file and tries to match the pictures. If the result is positive the system indicates that this guy is really Bill, is negative it indicates that it is not Bill.

Authentication is the same as verification, its task to verify if the user is actually who he claims to be.

Authorization means whether the user has a right to access to the system.
In practice it looks like the same as if you come to the cinema. You should buy a ticket, because you know that a person who checks the tickets will not allow you to see the movie without a ticket. There is no identification or verification process.

The same situation is with fingerprint based computer system. In order to access to the system the user should place the finger to the fingerprint scanner. The scanner will capture the fingerprint and compare the given example with all the fingerprints of all the users. If it finds the match- the user has a permission to access the system. If not, the access will be denied. When the user places his finger to the scanner, the process of verification starts. Authorization happens when the system return a definite answer to the question: If this person has a permission to access the system or not? (360 Biometrics, cited 04.03.2012)

1.6 Biometrics in different countries

Biometrics is the constantly developed branch of science. More and more convenient and reliable technologies allow using biometrics in common life making it easier and interesting.

Almost every country in the world has so called biometric passport, by not everyone knows what information it contains, for what purpose it is used for. Sometimes people cannot find information about such kind of passport. When biometric passport appeared people began to use for the word "biometrics", it became a bit closer and not so awful as it seemed before.

European Union: biometric passports in European Union are planned to have digital imaging and fingerprints places on chip. These measures should increase the level of security and protection against of fake identification paper documents. Such passports should be available in all countries of Schengen zone, except United Kingdom and Ireland, and also three of Association Trade countries- Iceland, Norway and Switzerland. These countries are obliged to have and implement machines readable facing images for passports.

British biometric passports have only digital image, but there is no fingerprints. German biometric passports have fingerprints from two hands and digital image. Romania has the same very type of biometric passport as Germany. Netherlands also include fingerprints to the biometric passport and plans to store them.

Albania has biometric passports since 2009. The passport contains fingerprints and digital photo and all other information as in ordinary passport.

Armenia does not have biometric passports yet but they plan to produce them in September 2012. Biometric passports will replace the ordinary passports. Biometric passport will be of two parts: the first part, ID card with electronic signature, will be used locally and the second part, biometric passport itself, will be for international travelling. Biometric passport will contain such information as: digital image of the owner, type

(is it for local use of for international use) country code, the number of the passport, surname and given names, nationality, date of birth, sex, country of birth, date of issue , date of expiry, authority code, chip with fingerprints. All the information will be in Armenian and in English.

Australia has biometric passport since 2009. This passport contains microchip with all personal information and digital photo. It should be notices that this passport take into consideration the desire of intersex people and instead of traditional female/male, the person can choose "X" and supported it with the statement from doctor. For transgender individuals can select gender without any statements.

Brasilia began to issue biometric passport at the end of 2010, only in the capital area and Goiaz state. But it took one year and biometric passports were all over the country. Passports contain the common set of personal information, digital photo, fingerprints.

Canada before the end of 2012 will have ePassports which will incorporate biometric passport. There will be a chip, with all personal information, as well as information found in machine -readable zone. Also the chip will include a specific signature that will prove that the passport was issued by the Government of Canada. The government also paid attention to the safeness of the information the chip contains: the information can be read only by holding the chip within 10 centimetres of the reader unit.

China began to use biometric passports in 2011. Passport contains digital photo of the owner, fingerprints and all other biometric features of the holder.

Croatia used biometric passport since 2009. The chip contains two fingerprints (from both hand) and digital photo.

In Egyptian biometric passport contactless chip is embedded in the cover of passport and contains the digital photo of the holder and personal data. Besides of standard set

of personal information there are two new columns: military status and barcode (machine readable code+ number of the passport + issuing office number).

The first biometric passports in India were issued in 2008. The 64KB chip contains personal information, digital photo, fingerprints. The passport was tested with passport readers and the results were quite good: it took 4 seconds for the reader to show the information. The only thing is the passport should not be carried in metal jacket for security reason as it should be passed through the reader, after which the access keys are generated to unlock the chip with information. Indian biometric passport also contains information about parents of the holder, the number of old passport.

In Japan biometric passports appeared in 2006. Also there is a chip with all personal information.

Concerning biometric passport in Kosovo, which were issued in 2011, personal information include citizenship, place of birth, height, eye colour and personal number.

Like United States and Australia, New Zealand has biometric passport since 2005 and it is based on the face recognition. It has two levels of defence: small symbol on the front cover that indicates the presence of a chip and the polycarbonate leaf on the front.

Norway also used biometric passports since 2005.Personal information also included information about the height. The information is presented in English and in Norwegian.

2006 biometric passports appeared in Russia. Generally speaking biometric passports are made for travelling abroad but not for the internal use. Foreign passport has two zones: visual and machine readable. In the visual zone there is a digital photo of the holder, data about the passport and also data about the holder. The personal information is the same as in other countries.

In the U.S variant of biometric passport there is a contactless chip, digital image, but no fingerprints. There is an opportunity for facial recognition if the holder of the passport has such desire. (Wikipedia, cited 19.03.2012)

2 Types of Biometric Identifiers

Biometric characteristics of a person are unique. Most of such keys are impossible to copy and exactly produce. Theoretically these are ideal keys. But by using biometric identification a lot of spesific problemes appear.

All biometric identifiers can be divided into two big groups:

1) Physiological
2) Behavior

Though behaviour biometrics is less expensive and less dangerous for the user, physiological characteristics offer highly exact identification of a person. Nevertheless, all two types provide high level of identification than passwords and cards.

Spheres of use:

- Criminalistics (biometric identifiers are used to recognise victims, unidentified body and protection of children against kidnapping.)
- Marketing (methods of biometrics are used to identify owners of loyal cards)
- Time accounting systems at work, schools, etc
- Security systems (are use to control the access to the rooms and control access to internet resources)
- Voting system (during the functionality of voting system identification/authentication of people, that take part in voting is demanded)
- According to actual international demands (for example, according to the standard of ICAO there should be biometric part in passport.)
- Biometric identifiers are used for registration if immigrants and foreign workers. It allows identifying people even without documents.
- For organisation of distribution of social help.

Methods of biometric authentication differ according their degree of safeness:

- DNA
- Iris recognition

- Fingerprint
- Face recognition
- Voice
- Typing Rhythm

2.1 Physiological Type of Biometrics

Physiological systems are considered to be more realible as individual features of a person, that are used by these systems, do not change by influence of psychoemotional state. Physiological systems of identification deal with statistical characteristics of a person : fingerprints, iris recognition, hand geiometry, DNA, face recognition, palm print.

2.1.1 Fingerprints

Today fingerprints consider being one of the oldest and popular among other bio-metric technologies.

Fingerprint identification is also known as dactyloskopy or also hand identification is the process of comparing two examples of friction ridge skin impression from human fingers, palm or toes.

Picture 4. Example of fingerprint

Method of fingerprinting helps police to investigate crimes during long period of time. The most amazing fact how many details about person can be known using only his/her fingerprints.

Human skin has two layers: epidermis and dermis. Dermis has also two layers: papillary и reticulated layer. In papillary layer find themselves in pairs pyramidal formations that are called papillary. Each pair of papillary is divided by channels of sweat glands. Such pairs make a row and covered by the layer of epidermis build comb of papillary lines. Papillary lines are situated chaotically but as streams. When three streams are near each other they build triangle which is called delta.

Papillary pattern is flexible. It means that there are no two similar papillary patterns in the world. Each person has its own unique papillary pattern. Each papillary pattern has its own unique details of structure: beginning and end of lines, merging and separation of lines, bends and breaks, ridges, eyes and hooks, breaks of papillary lines and oncoming places of their beginnings and ends.

Besides uniqueness, papillary pattern is also stable. Age changes do not influence on papillary pattern and it is considered that papillary pattern remains stable during all period of life.

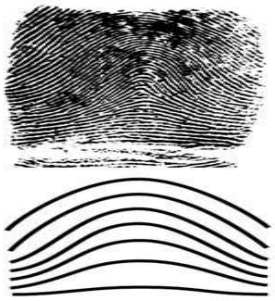
Papillary pattern is reflected. Person can leave his/her fingerprints at any thing whether he/she wants it or not. This happens because of physiological peculiarity of human skin- our skin is always covered by secretions of sweat and fat.

Also papillary pattern has an ability to restore. If the finger is not badly damaged the picture of papillary pattern is fully restored in time without any changes.

One of the most important things concerning papillary pattern is that it can be divided into three groups that are called types. The division is based on quantity, form and arrangement of papillary streams, availability, quantity, form and arrangement of deltas at

the nail phalange. The opportunity to classify papillary patterns gives the basic to theoretical and practical works which are used for fighting with criminality.

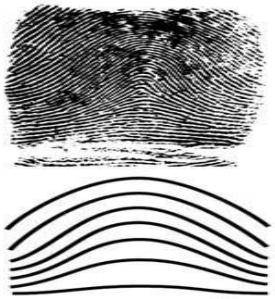
The first type of papillary pattern is arch papillary pattern. They are simplest in their structure and according to the frequency of meeting – 5%. They consists of not more than two streams of papillary lines that starts at one side end and go to another end , making in the middle of the pattern arcing figures. There are no inner picture and delta in this pattern.



Picture 5.Example of arch pattern

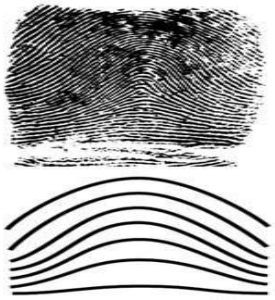
This type can be divided into 3 subtypes: plain arch, tented arch and, central pocket loop.

The second type is loop papillary pattern. This type is the most popular; about 60%-65% of people have this type of pattern. The picture is built by three streams of lines. The central picture consists of one or more loops, lines start at the end of the pattern and going up, come to the same end. The loop has its head, feet and open part. This type has its own subtypes, which are differ according to the quantity of loops, place o f start and end of feet: plain arch, tented arch, loops (radial and ulnar).



Picture 6.Examle of loop pattern

The third type is whorl, is met at about 30% of people. The inner picture can be made by papillary lines as ovals, spirals, loops, or their combinations. The characteristic feature of this type is not less than two deltas, one of which is situated on the left side, another- on the right side from inner part of the pattern. As the previous types, this type is also subdivided into tree subtypes: plain whorls, accidental whorls, double loop whorls, central pocket loop whorls.



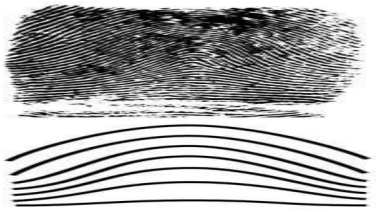
Picture 7.Example of whorl pattern

An interesting fact: one of the Russians scientists compared the fingerprints of maniacs and came to the conclusion that such people have a rare papillary picture.

As it was discussed earlier fingerprints can be taken with the help of ink and common white sheet of paper. The surface of fingerprint should be covered by ink and after that should be applied to the sheet of paper.

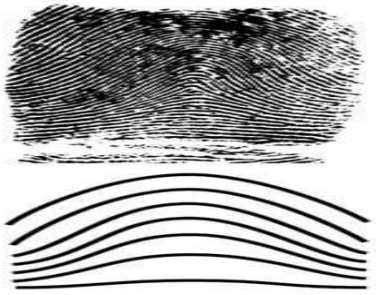
Besides of common classification of fingerprints that is based on uniqueness of papillary pattern fingerprints can differ according to the pace the fingerprint was taken or where it will be used:

1) Examplar prints, known prints, are deliberately collected in order to use them for different purposes: to enrol to the system, also when a person is under arrest. It should be noticed that the method of taking fingerprints with the help of ink and sheet of white paper is commonly used here. Also the system Live Scan can be used here.



Picture 8.Example of examplar print that is taken using ink and sheet of white paper

2) Latent prints are prints that are accidentally left on any surface. Electronical, chemical, physical technologies make latent invisible print visible.



Picture 9. Example of latent print

3) Patent prints are visible to the human eyes because of transferring foreign material from the finger to the surface. Because of their visibility there is no need for extra technologies.
4) Plastic prints are prints that are left in the material that remains their shape. They are visible and do not require any additional technologies.
5) Electronic recording: Nowadays much news about "clever "technique appear. Stolen mobile phones and notebooks send signals to the police with exact co-ordinators and photos of criminals, parts of hands and body.

Let's have a look on how the process of biometric technology with the help of fingerprints takes place.

There are different types of fingerprint readers but they all have one and the same goal: to measure the physical difference between the ridges and the valleys.
All methods can be grouped in two groups:

1) Solid state fingerprint readers
2) Optical readers

The procedure of taking the fingerprint using a sensor consists of rolling and touching with the finger the sensing area. This sensing area captures the difference between ridges and valleys according to the physical principles. But the results of such procedure can be an inconsistent, non-uniform image because of the difference direction and quantity of pressure, skin condition.

To make the results more reliable, new touchless fingerprint scanners have been developed in 2010. 3D fingerprint scanners use the digital approach of pressing or rolling the finger. Scanners model the distance between neighbouring points and the image of fingerprint is created. The quality of such image is good enough to record all the necessary details.

For authentication it is necessary to receive the picture of papillary pattern of one or several fingers with the help of special readers. Further, this picture is processed and special characteristics such as bifurcation of lines, end of lines or crossing the lines are found. For each characteristic relative arrangement and other parameters are dated. The sum of such special features and their characteristics build the template of biometric characteristic. The process of identification and verification is built on comparison of early received template with the given one. Based on the definite level of accord the conclusion about identification of templates is made and the verification or identification of a finger takes place.

As it was mention above the area of using fingerprinting is big enough but special meaning fingerprinting place in criminalistics. Fingerprints can point to the criminal; prove quilt or innocence of a person. Almost each country in the world has its own databases where fingerprints of criminals are collected. For example, United States has the Integrated Automated Fingerprint Identification System where above 51million of fingerprints of criminals are recorded and about 1, 5 million of civil fingerprints. The use of such databases makes the work easier and allowed to minimize the rime of investigations.

The method of fingerprint is considered to be the most reliable method. The pluses of such method are: low cost of equipment, low time of procedure. But it has some minuses: papillary picture of the finger can easily be damaged; the system can be broken because of the high quantity of staff, some scanners "do not like "dry skin and it makes difficult for old people to use this method. The producers of scanners try their best to approve the quality of their goods.(Uchebnik cited 05.03.212 , Kriminalistika, cited 18.03.2012)

2.1.2 Face Recognition

During the whole history of humanity, people used face to distinguish one person from the other. Facial (face) recognition is a computer application that automatically identifies or verifies a person with the help of a digital image or a video frame from a video source. One of the ways to do this is to compare the given example with the examples in the database.

The face of a person has a numerous distinguishable characteristics. Face IT has 80 nodal points and some of these points can be measured by software:

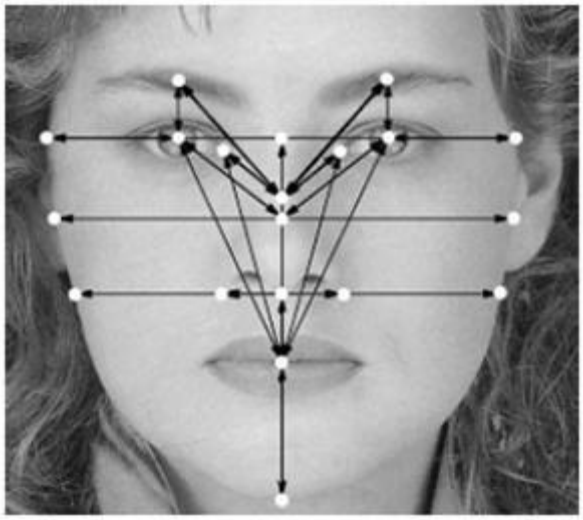
- Distance between eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

By measuring these nodal points a special numeric code is created. This code is called a face print, and it is this code that represents the face in the database.

Facial recognition technologies can be divided into two ways:

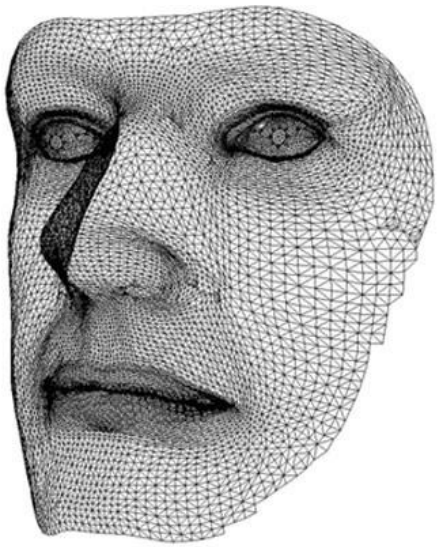
1. 2-d: it is the most ineffective way of biometrics. This method was mostly used in criminalistics. Now the computer version of this method appeared making it more reliable. This method does not need any expensive equipment, but reliability is very low. Method strongly depends on the light. Problems may occur if

the person has glasses, beard, etc. Person should look straight to the camera, the expression of the face should be neutral.



Picture10. Example of 2-d technology

2. 3-D there is a lot of methods for3-D face recognition. These methods cannot be compared because all of them use different scanners and databases. The advantage of this method is that there is no need for contact, the low sensitivity to such factors as: beard, glasses, another form of hair, colour of hair. Also 3D show high degree of reliability that can be compared with fingerprinting. But the negative side of the method is the expensive equipment, change of face expression reduces the statistical reliability of the method.



Picture11. Example of 3-d technology

Between 2D and 3D methods there is so called transitional method which has the features of 2-D and 3D, realizes the information about the face. The method has better characteristics as 2D and also uses only one camera. The camera makes a picture of a person who looks directly at the camera, after this he turn his head and algorithm connect images together.

The classical method of facial recognition is the creation of projection template of the face. First we project a face onto the elastic grid. Further, camera makes 10 photos in a second and these photos are worked up with the special program. The ray falls to the crooked surface starts bending. At the beginning visible light was used, but soon it was changed to the infra-red. At first stage the program deletes all the photos where the face cannot be seen at all, or if there are some extra things. After this the 3D model of the face can be constructed. Beard, glasses and all other unnecessary things can be deleted. The second stage is the analysis of the 3D model: different anthropometrical characteristics are found and constructed to the unique code.

The face recognition process normally consists of four phases:

1. Detecting a face: It is not difficult for people to differential one person from another just look at his/her face. This task is more difficult for computer. The task of the computer is to decide what the part of the image is and what is not. The task is easier with the photos with white background, but it becomes more difficult if there are some other colours, things on the background.
2. Normalization: when the face is found it should be normalized, it should be standardize in terms of position, size relative to the image in the database. The system locates the facial landmarks. With the help of these landmarks the system can create a slight variation of the image. Using the facial landmarks is the key to all systems. If facial landmarks cannot be located, the recognition process cannot take place and fail.
3. Feature extraction and recognition: biometric template is generated with a help of recognition algorithms. These algorithms differ by the ways they transform or translate the face image to a simplified mathematical representation in order to perform a recognition task. This template is stored in the database and it is

the basis of any recognition task. It is important that maximum of information should be retained for successful recognition. If this condition fails, the algorithm will not have ability for successful recognition and the task will failed.

4. Recognise face image: here we can have different purposes, whether it is identification or verification. If verification takes place the image will match to only one image in data base. If it is identification the image will be compared with all images in the database.

Facial recognition is not a perfect method of biometrics. As all other methods it has its own weak sides and strong sides. Dependence on the light, low resolution, sometimes form of hair, facial expression make the weak side of face recognition. The strongest side of the method is that it is not required aid from the test subject.(rukovodstvo po biometrii, cited 24.02.2012)

2.1.3 DNA

Not long ago Russian show business was full of rumours that one of the popular Russian singers has two fathers and each father tried his best to influence on the son. Special programmes were created and the situation was discussed but only one thing was interested to public: who was the real father of the singer. The singer himself was confused. In one of the programs the singer and both of his fathers decide to take DNA test.

DNA or Deoxyribonucleic acid is the part of a cell that contains genetic information unique for each person. DNA typing is a method of biometrics that measures and analyses DNA to distinguish people with some degree of probability.

This method of biometrics is rather popular in criminalistics. It should be mentioned that DNA is the only method of biometrics that is not automated and it takes hours to make the DNA test. But this method is considered to be one of the most reliable methods and due to it many unsolved crimes were solved. Most of the methods of biometrics are based on the unique parts of the person (finger prints, iris), the method

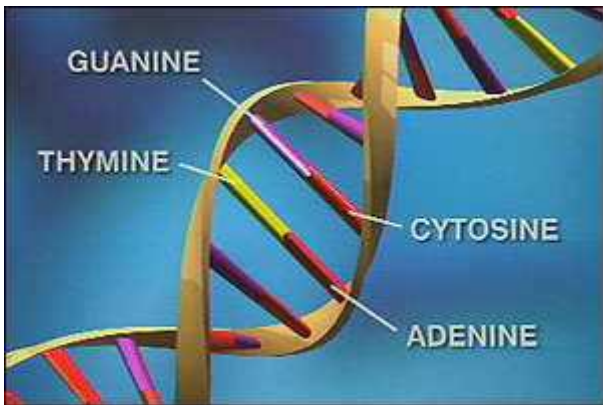
of DNA has one exception: DNA of the twins can be the same. As a finger prints DNA is unique and it will not change in time.

The sample of DNA can be taken from different sources: paper or plastic cups, sweat T-shirt, glass, ear wax, socks, chewed gun, hair, nails, blood, urine, etc.

DNA consists of four bases:

- Adenine (A)
- Guanine (G)
- Cytosine (C)
- Thymine (T)

which all together make DNA code. These bases combine in specific sequence to form base pairs that determine the anatomy and physiology of the organism. Each base pair with sugar and phosphate creates a nucleotide. Nucleotides form two long strands connected by the base pairs (in the ladder like form) and form the spiral , which is known as double helix.



Picture 12. Double helix

There are about 3 million bases, 99% of wich are the same from person to person, and only 1% is unique. It is this 1% that makes DNA a method of biometrics.
The cell of DNA contains genetic information. This information is shared through chromosomes. There are 23 pairs chromosomes. The total amount of chtomosomes is 46, 23 from mother and 23 from father. 99,7% of DNA human is shared with his/her parents and only 0,3% is the unique code(repetitive coding) that serves for DNA biometrics. (DNA as a Biometric Identifier, cited 15.03.2012)

Generally, DNA recognition uses so genetic profiling or, in other words, genetic fingerprints for isolation and identification of repetitive DNA redions. In 1980s only several repetitive DNA regions were discovered. Nowadays there 13 of such regions.

The main steps of DNA profiling are:

1. Isolate the DNA sample from different types of samples
2. Section DNA sample into shorter segments which contain known variable number tandem repeats(VNTRs)- identical repeat sequences of DNA.
3. Organize the DNA sample by size with the help of agarose gel electrophoresis. A replica of the gel with DNA fragments is received by using this gel with special chemicals that cause the DNA to denature.
4. Compare the DNA segments from various samples.

The more repeats of the seguences the more accureate the DNA comparison is.

Two methods can be used for DNA fingerprinting:

- Restriction fregment length polymorphism (RFLP). This method requires at least 50 nanograms of the sample.
- Polymerase chain reaction (PCR) This method is used when the sample of DNA is too small and is not suitable for RFLP method. This method produces millions of copies of the given sample. PCR is faster than RFLP.

There are four main methods of extraction:

1. Organic: here phenol, chloroform and several centifuge steps are used to separate DNA cellular debris. The procedure will take 2-3 hours.
2. Chelex™ : DNA is bound with the help of boiling step and iminodiacetic beads. The process is rather quick and will take less than an hour.
3. FTA™paper: the sample is placed on the paper and is washed several times. After this the paper is proceed to amplificatopn reaction. The whole process will take less than an hour.
4. Alkaline: DNA can be removed with the help of filtering. This process is the longest and can take several hours.

One of the main advantages of DNA is that it allows to detect specific types of deseases, to identify the predisposition to different types of breast cancer. Also DNA is indispensable in identifing unknown bodies.

But the main disadvantage is that the sample of DNA can be easily stolen. Conerning the future of DNA testing in such fields as physical and network security everything depends on the experts and their ability to make the method more cost efficient. Nowadays DNA test is rather expensive.(DNA as a Biometric Identifier, cited 15.03.2012)

2.1.4 Palmprint

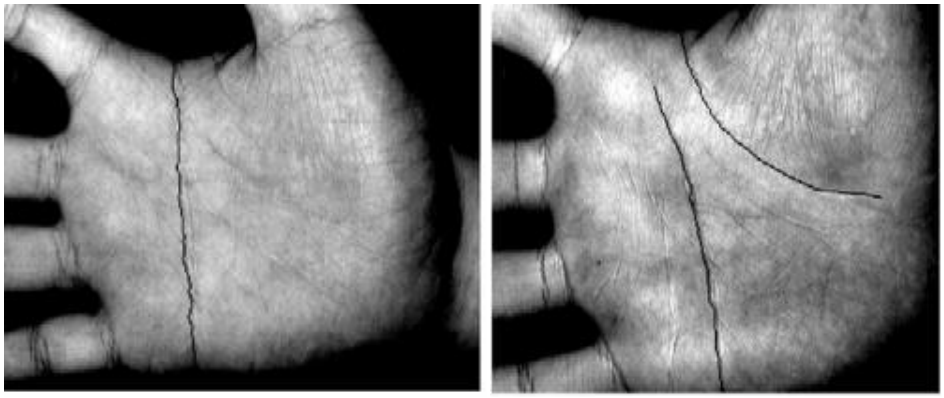
Palmprint refers to an image required of the palm region of the hand.

As a method of biometrics palmprint is often mentioned with such methods as fingerprints and iris recognition. Palmprint is also distinctive and can easily be captured with low resolution devices. The devices are not expensive. They are similar to those which are used for taking fingerprints but their size is bigger and this makes the limitation of use in mobile devices. Palmprint is suitable for everyone and besides it has one big plus: it does not require personal information.

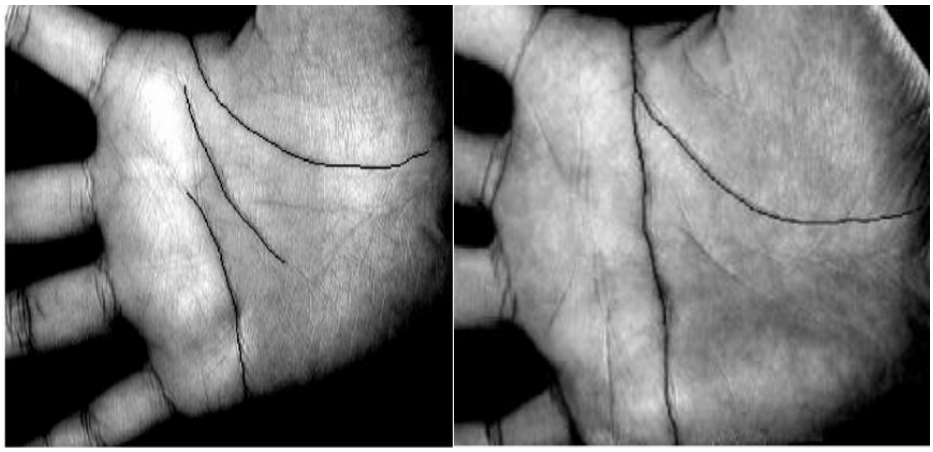
The palm of each person consists of principle lines, wrinkles secondary lines and ridges. Palm also contains such information as texture, indents and marks which are used during the comparison of one palm with another.

Classification of palmprints is based on the different principle lines and number of intersection. This classification was offered by X.Wu, D.Zhang, K.Wanfg and B.Huang in their book “Palmprint classification using principle lines”.

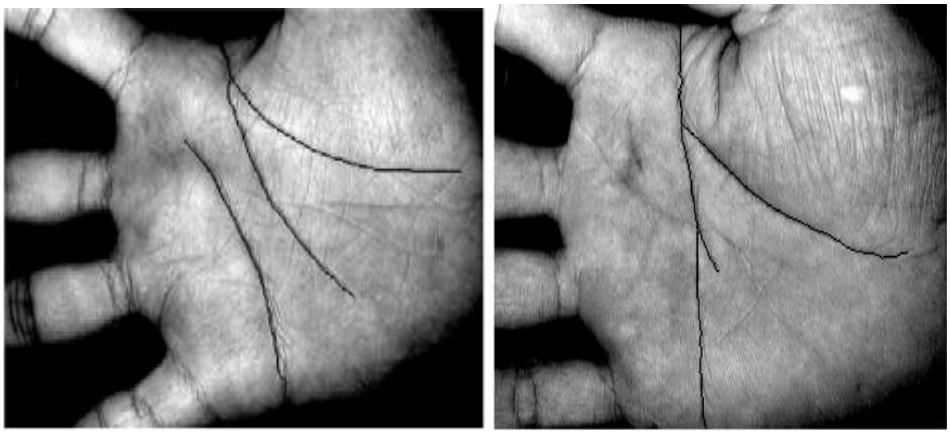
According to this classification there are 6 categories of palmprints:



Category 1 Category 2



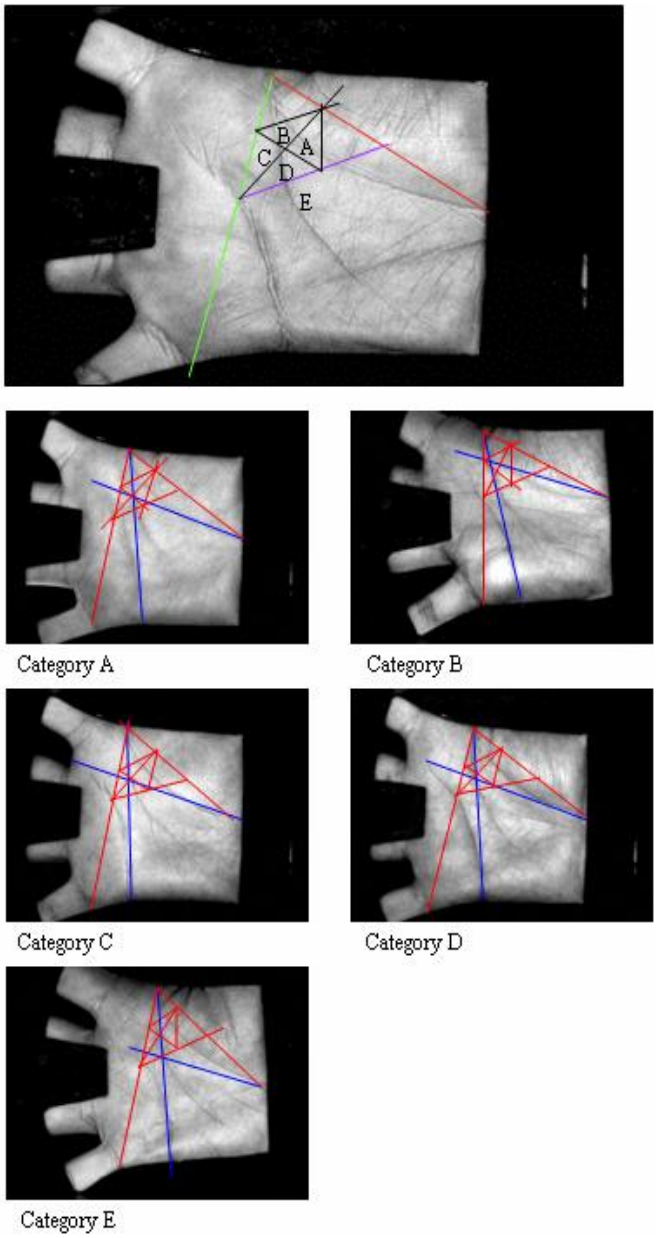
Category 3 Category 4



Category 5 Category 6

Picture 13. 6 categories of palmprint

The category 5 is the most widespread. This category is further divided into 5 subcategories:



Picture 14. Division of the category 5

The process of taking palmprint can be described in the following way:

1. The process starts when the palmprint capture device captures the image of the palm
2. The system classifies the image using the category of 6 patterns. Here there can be 2 variants of the process. First, the palm print can belong to the categories 1,2,3,4,6. In this case the system just saves/compares the image in the database. If the image belongs to the category5 , the system continues the process of classification using subcategories. After the process ends and the category and

subcategory is given the system saves/compares the image.(Palmprint Classification, cited 28.03.2012)

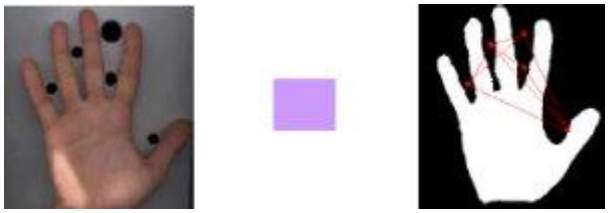
Palmprinting has its own advantages comparing with other methods of biometrics.

Palmprint is hardly affected by age(the problem of age is the main problem for face recognition). Palmprints contains more information and can use low resolution devices(in comparison with fingerprinting). Palmprinting can not make harm to the health of people, and many people prefer palmprinting to iris recognition based on this very reason.

Palmprinting is a rapidly developed method of biometrics. One of the variants of palmprinting is the recognition based on the veins of palm. Infra-red camera makes the image of inner or external side of the hand. Haemoglobin absorbs infra-red light and veins can be seen as black lines. This method is contactless and reliable. The main minus of this method is that there should be no light near the scanner.

2.1.5 Hand Geometry

Hand geometry is the use of geometric shape of the hand for recognition purposes. This method was rather poopular 10 yeares ago but nowadays it is seldom used. The method is based on the fact that the shape of the hand of one person differs from the shape of the hand of another person and does not change after certain age. But it is not unique. The main characteristics for this method are measuring and recording the height, length of the fingers, distance between joints, shape of the knuckles, surface area of the hand. (GlobalSecurity.org. cited 10.03.2012)



Picture 15. Hand geometry measure

There are two kinds of principles that can be used for measurement of the hand:

1. Mechanical
2. Optical

Optical scanners can also be divided into two subcategories: devices that belong to the first subcategory create black and white bitmap image. These devices use 2D characteristics of the hand. The second subcategory offers a bit more complicated devices. They have two (vertical and horozontal) sensors to measure the hand shape. These devices use 3D characteristics.

There are scanners that produce the video signal with hand shape. Computer digitalizes and process the image.

Scanners uses a charge couple device camera, infrated light emitting diodes with mirrors and reflectors for capturing the black and white image of the hand silhouette. For hand geometry method there is no need to record surface details, fingerprints, lines, scars and color. The hand scanner just records the silhouette of the hand. Due to the use of mirror and reflector, the optics produce two distinct images, from the top and from the side. Scanner takes 96 measurements of the hand. Mictoprocessor converts these measuremnts to the 9byte template that is ready to be stored in database. This process is also known as enrollment. During the process the person is asked to place the hand on the scanner platen three times. Platen is used as a reflactive surface that allows to project the silhouette of the hand.

For verification the person should enter his personal PIN code and place the hand to the platen. The system makes common procedures and compares the given template with the template stored in the database.

The method of hand geometry has its own advantages and disadvantages. The main advantages of this method are its simplicity, easiness of use. Scanners are not expensive. Also its is easy to collect hand geometry data that differs this method from fingerprinting . Environmental factors (dry skin) can not influence on the results.

Among disadvantages of the method it should be mentioned that hand geometry cannot be used in identification system . Hand geometry is ideal for adults but not for growing children as their hand characteristics can change in time. And data size is too large .(360 Biometrics, cited 29.03.2012)

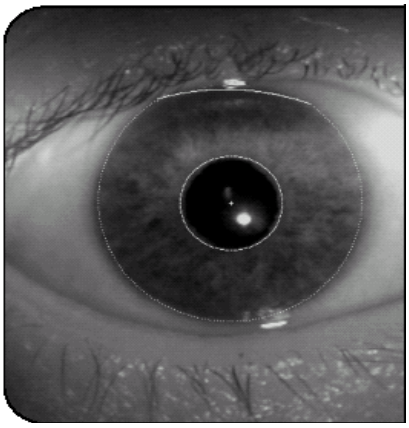
2.1.6 Iris Recognition

Iris is a unique characteristic of a person. The primary visible characteristic of iris is the trabecular meshwork, that makes possible to divide the iris in a radial fashion. It is formed in the eighth month of gestation. Iris is stable and does not change during the whole life.

Iris recognition is considered to be one of the exact methods of biometrics. Iris is protected by eyelid, cornea and aqueous humour that makes the likelihood damage minimal unlike fingerprinting.

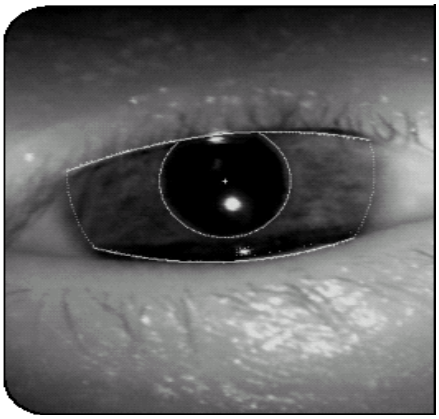
Some sources divide the process of iris recognition into two steps, some into three:

1. Capturing the image: The image can be captured by a standard camera using both visible and infrared light. The procedure can be manual or automated. In the manual procedure the iris should be in focus and the length between the camera and iris shoulld be within six and twelve inches , while in automated procedure the length is between three and a half inces and one metre. In automated procedure the camera automatically locates the face and iris into the focuse and make the process rather easy and friendly.
2. Define the location of the iris and optimising the image: when the iris is in focuse , the iris recognition system just identifies the image with the best focus and clarity. The image is analyzed. The purpose of the analysis is to identify the outer boundary of the iris where it meets with white clera of the eye, the pupillary boundary and the centre of pupil. The result of the analysis is the precise location of the circular iris



Picture 16. Circular iris location

Iris recognition system tries to identify the areas suitable for feature extraction and analysis: removing areas covered by the eyelids, deep shadows, reflective areas. This attempt is known as optimisation of the image.



Picture 17. Optimisation of the image

3. Store and compare the image: the process of division , filtering and maping segments of the iris into hundreds of vectors(phasors) takes place. The process is also known as 2-D Gabor. 2-D Gabor phasor can be easily understand as "what" and "where" of the image. Even after this procedure there are still 173 degrees of freedom to identify the iris. 2-D Gabor takes into consideration the changes that may occur with an iris. Iris image is saved as so-called IrisCode® , 512-byte record. The record is stored in a database. (Reading Room Sans, Iris Recognition Technology , cited 8.03.2012)

When there is a need in comparison the same process takes place but in stead of storing the system compares the given sample with the record stored in the database.

Iris recognition system is used for enrolment, making the process quick and safe. The person who wears glasses should remove them during the initial enrolment in order to avoid reflection. People who wear contact lenses should not remove them because they will not influence on the process, they have no reflection.

Among the advantages of iris recogniton method the first place is taken by fact that iris remains stable during the whole life. There is no diricet contact between the user and camera. The laser does not used, just video technology. The high level of accuracy put the method in one row with fingerprinting. The method is remarkable for its high speed, scalability.

In spite of the big amount of advantages, the method has also some disadvantage. The iris is a small organ and it is impossible to take the process of scanning from a distance. For people with such eye problems as blindness and cataracts, it will be very difficult to take part in the process of recognition as it is very difficult to read the iris. Without correct amount of illumination it is difficult to capture image.

2.1.7 Odour/Scent

A human has many unique characteristics: figerprints, palmprint, DNA, eyes. One more unique factor is odour/scent. Each person has his/her own , unique,scent. This characteristic is very useful for dogs. They have very keen nose that allows them to differentiate one person from another. Even twins have diferent scents.

Scent belongs to five main senses: sight, smell, taste, hearing and touch. The main pecularity of scent is that it is difficult to find word for description. Scent plays very important part in our life. Pleasant smell can arouse good memories, smile. Unpleasant smell can make people feel themselves uncomfortably, can react on their behaviour. But in spite of its importance , people do not poccess so keen nose as animals.

Human has about 40 million of olfactory nerves. Due to such big amount people can detect slight traces of chemical components.

In the basis of all systems connected with the task of biometric identification using the odour is the human mecanism of olfaction.

The process of human olfaction can be divided into 5 parts:

1. Sniffing: the odorants are mixed into an unifirm concentation and in the form of mixtures delivered to the mucus layer in the upper part of nasal cavity. Here, molecules are dissolved and transported to the cilia of the olfactory receptor neurons.
2. Reception: olfactory molecules are binded to the olfactory receptors. Molecules are binded to the proteins which transport them across the receptor membrane. During this the stimulation of receptors is taking place which in its turn creates chemical reaction. Chemial reaction produced electrical stimulus. Such signals are transported to the olfactory bulb.
3. Detection: electrical signals from olfactory bulb are further transported to the olfactory cortex.
4. Recognition: the information, that olfactory cortex received, is further transmitted to the cerebral cortex.
5. Cleansing: removing olfactory molecules from olfactory receptors.

The main task of each odour recognition system is to create model similar to the nose of the person.Electronic/artificial noses(ENoses) were created.

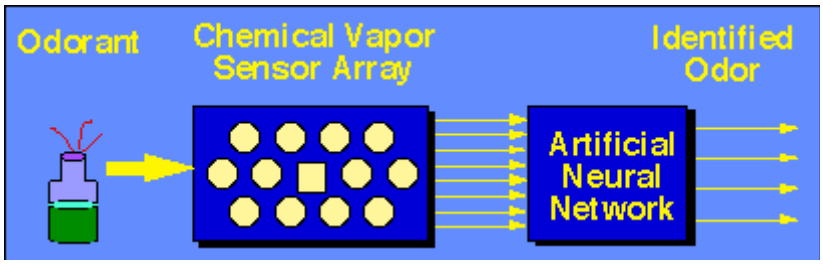
ENoses is a combination of two components:

1. Sensing system: receive the odour from the environment. The system can consists of single device, an array of chemical sensors or the combination of two of them.
2. Pattern recognition system: the main task is to build recognition system for classification or clustering each odorant through the automated identification. Several approaches can be used in this component: statistical,ANN, and neuromorphic.

Statistical approach includes principal component analysis,partial least squares, discriminant and cluster analysis.

Atrificial neutral network (ANN is the information processing system that has certain performance characteristics in common with biological neutral netwok) trains a pattern classifier to categorize sensor values using specific odour labels.

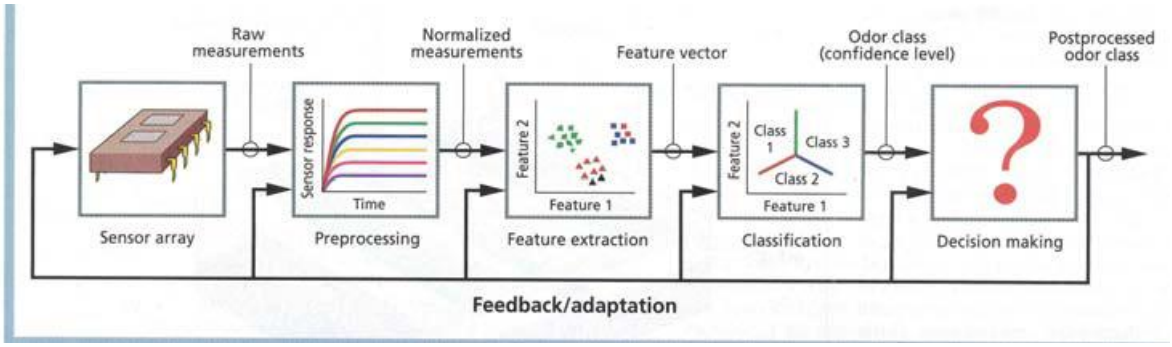
Neuromorphic builds the models of olfactory based on biology



Picture 18. Scematic diagram of ENose
(Biometric Pesron Authentication: Odour, cited 16.03.2012)

The main purpose of ENose is to identify the odour sample and to estimate its concentaration. It means signal processing and pattern recognition system.But, it is necessary to remember that the sample of the odour should be already in the database. So, the process can be divided into several steps:

1. Preprocessing: compresses the response of the sensor array and reduces variations.
2. Feature extraction: reduces measurement space, extracts information for pattern recognition.
3. Classification: some similarity with brain function which interprets th responses from olfactory sensors.
4. Decision making: gives the class of the sample



Picture 19. Signal Processing andPattern recognition system stages
((Biometric Pesron Authentication: Odour, cited 16.03.2012)

2.2 Behavior Type of Biometrics

Behaviour methods of identification pay attention to the actions of a person, giving the user an opportunity to control his actions. Biometrics based on these methods takes into consideration high level of inner variants (mood, health condition, etc), that is why such methods are useful only in constant use. Behaviour or sometimes called psychological characteristics such as voice, gait, typing rhythm are influenced on psychological factors. Because of the ability to change during the time period, such characteristics should be renewed constantly. Behaviour characteristics are influenced by controlled actions and less controlled psychological factors.

As behaviour characteristics can be changed in time, registered biometric sample should be renewing every time of use.

2.2.1 Typing Rhythm

Nowadays, our world is fully computerized. Almost every house has so important part of the world. Computer is used not only for work, but also for entertainment, communication, education and so on. Keyboard- is an inalienable part of computer. It can be a separate device, or attached inside the laptop or smart phone. Keyboard- is the part that helps us to communicate with computer. People use keyboard in different ways. Some people type fast, some slow. The speed of the typing also depends on the mood of a person and a time of a day.

Biometric keystroke recognition – is a technology of recognising people from the way they are typing. It is rather important to understand that this technology does not deal with "what" is written but "how" it is written.

Keystroke recognition is considered to be a natural choice for computer login and network security.

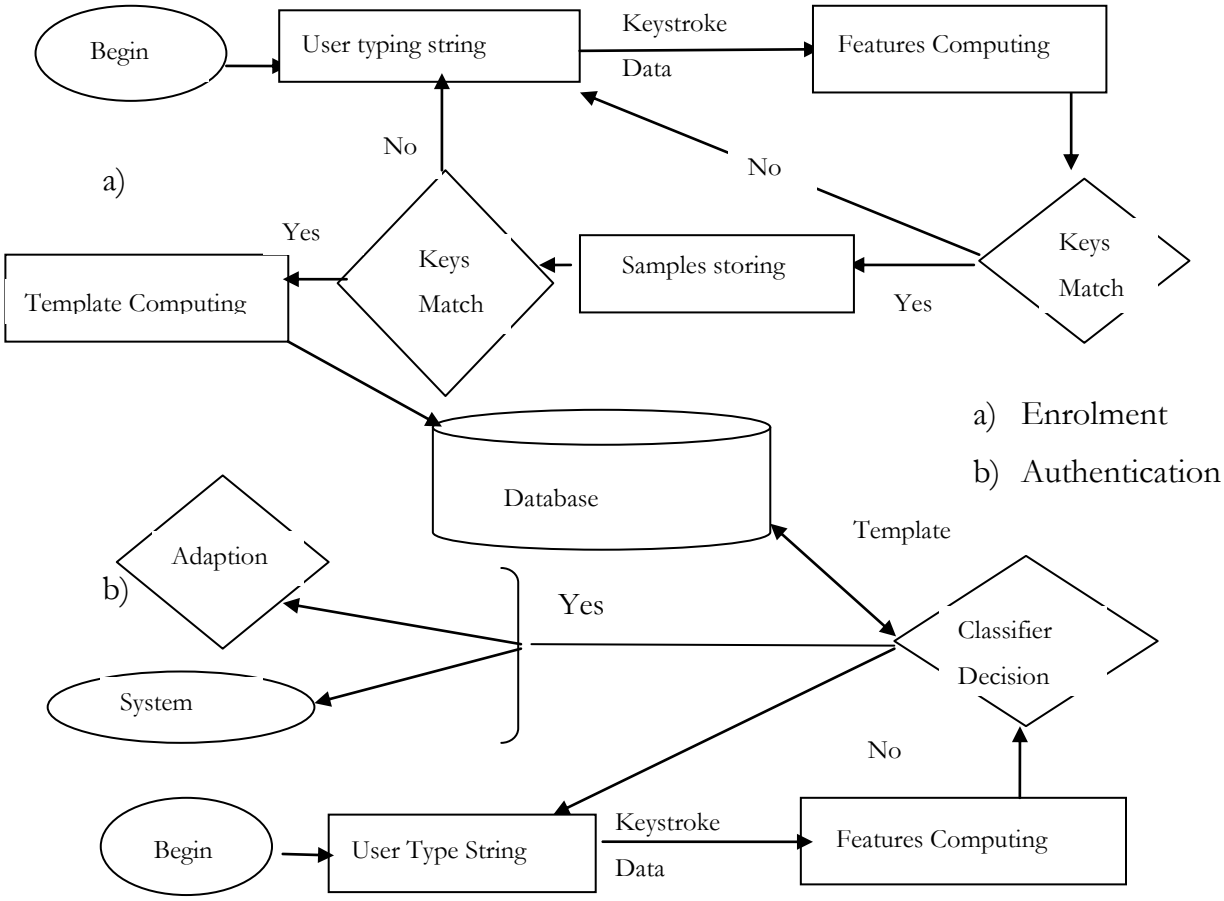
The main features that are used to describe typing pattern of a user are:

- Latencies between successive keystrokes – is the time between the release of the first key and the depression of the second.
- Duration of each keystroke – is a time that the user holds the key down
- Finger placement
- Pressure applied on the keys
- Overall typing speed

There are four key press latencies:

1. P-P (Press-Press) – the time interval between successive key press, the speed of the typing
2. P-R (Press-Release) - the time interval between the press and release of the key, how much efforts the user should make to type the key.
3. R-P (Release –Press) – the interval between the releasing one key and pressing another.
4. R-R (Release-Release) – the time interval of releasing two successive keys.(Biometric authentication using random distributions, cited 27.03.2012)

When user wants to access to a system, he selects an account and types target strings (login, password, first name, last name).Keystroke data is captured and the sample is created. The sample will contain the features (duration of the key and keystroke latency) of that are calculated using the data. If it is a new account, a template is created. A sample will be stored in the case of key code features matching. In the case of authentication the sample will be analyzed by the classifier and compared with template.



Picture 20. Flowchart of a) Enrolment b) Authentication
(User Authentication Through Typing Biometric Features, cited 05.04.2012)

There are two types of keystroke dynamics: static and continuous. Also the process of adaptation or re-enrolment takes place for maintaining the templates update.

In static dynamics the keystrokes can be analyzed only at a specific period of time, for example during the procedure of login. From one hand static dynamics can provide more robust user verification in comparison with the simple passwords. But this method does not be able to provide continuous security.

In continuous dynamics, keystrokes can be analyzed during the whole session.

As all methods, typing has its advantages and disadvantages. The main advantages of the typing are its non intrusive and wide acceptance, minimum training and no need in additional hardware. But the main disadvantages are high level of false reject rate, dependence on the physical condition of a user, narrow range applications.

2.2.2 Gait

How often we have a chance to identify a person only recognizing the way he/she walks?

Gait biometrics is a biometrics that is based on the way the person walks. It should be mentioned that gait is not affected by the speed of the person's walk.

Some scientists differentiate gait from gait recognition, pointing out that gait can be considered as a cyclic combination of movements that results in human locomotion and gait recognition is recognition of some property style of walk, pathology, etc. (Biometric Gait Recognition, cited 30.03.2012)

The common parameters of gait analysis are:

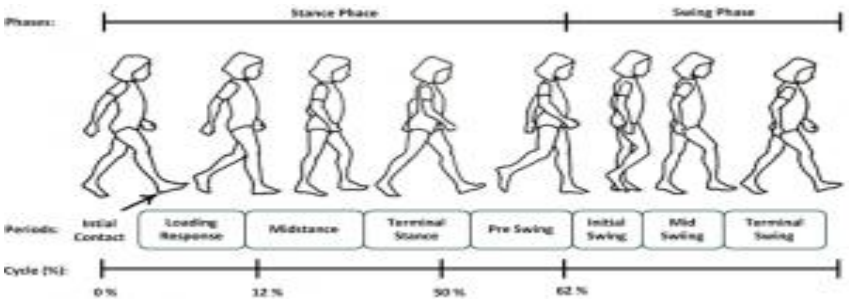
- Kinematic parameters such as knee, ankle movements and angles.
- Spatial-temporal parameters as length and width of steps, walking speed.
- Correlation between parameters.

Long time ago psychologists paid attention to this human metric. Johansson found out that a person can identify another person in less than one second.

According to Bertenthal and Pinto there are 3 important properties of human perception of gait:

1. Frequency entertainment: various components of the gait share a common frequency.
2. Phase locking: the relationships among the components of the gaits remain stable.
3. Physical plausibility. (Bertenthal, B.I., Pinto, 209–239 cited 10.04.2012)

Such characteristic of human being as the ability to identify a person by analyzing the manner of walk is very important for biometrics as it offers more reliable and efficient means for identity verification.



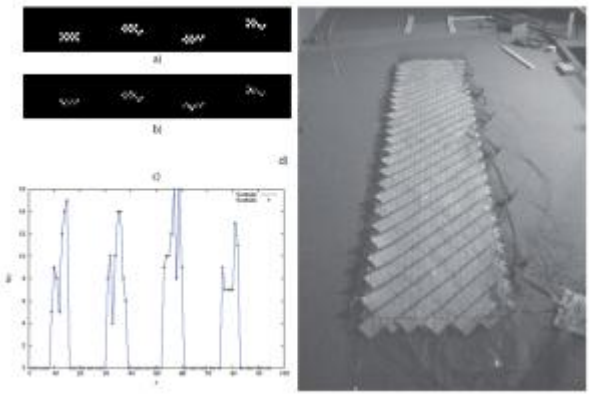
Picture 21. Division of the gait cycle into five stances phase periods and two swing phase periods

There are three gait recognition approaches:

1. Machine Vision Based: this approach includes several digital or analog cameras with suitable optics that are used to acquire the gait data. The image is converted into black and white image, the feature is extracted from the background, and the system counts light and dark pixels.

Picture 22. Machine Vision Based approach (Background segmentation for extracting the silhouette picture)

2. Floor Sensor: sensors are situated on a mat along the floor. Walking across the mat the ground measurements starts, also the process is known as GRF (Ground Reaction Force)



Picture 23. Floor Sensor

Gait collection by floor sensors a) footsteps recognized, b)time spent at each location in a), c) footsteps profiles for heels and toe strikes, d) picture of floor sensor carpet.

3. Wearable Sensor Based: the new "word" in gait recognition. The approach is based on special motion recoding sensor that a person wears on the body. The sensor can: 1) measure acceleration, 2) measure rotation and number of degrees per second of rotation, 3) measure the force of walking. This approach is used in mobile phones.

Picture 24. Wearable sensor

Gait as a method of biometrics has its own advantages and disadvantages. Among the main advantages is the ability to identify the person from a distance spending less that a second. Also, gait analyzis can be taken even if the resolution is low and even if the illumination is poor.

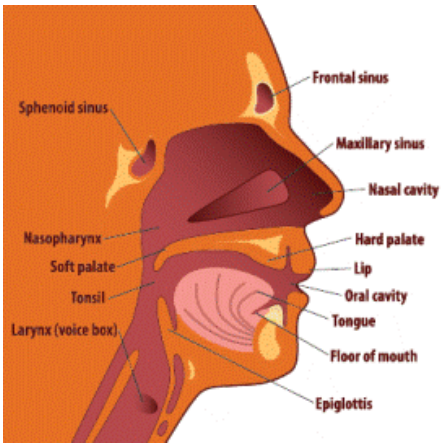
Among disadvantages of gait recognition is that sometimes it depends on the surface , downhill, uphill and if the person wears something that can influence on his style of walking.(Derawi Biometrics, cited 03.04.2012)

2.2.3 Voice

Voice, like many other characteristics that are used for biometric methods, is unique. Like style of gait, it takes quite little time to analyze the voice and to identify the person.

Voice in biometrics, or"voice print" is presented as a numerical model of the sound. (Authentify Voice Biometrics, cited 02.04.2012)

Voice is often compared with fingerprints, because like fingerprints, due to their unique form serve for biometric authentication, so the voive does. The uniqueness of the voice is achieved due to the different phisical components of a human throat and mouth. To produce a sound, air leaves the body of a human being through resonators: larynx, the oral cavity(mouth), nasal cavity (nose). The form , tone of the sounds are depended on the size of the stream, obstractions. Obstractions may include tongue, gums, teeth, lips, their position and size.



Picture 25.Human Speech Production System

Voice has more than 100 separate characteristics that make voice biometrics to be one of the most reliable.

To identify the person with the help of voice print, a sample of speech should be taken. This sample is analyzed. Different multiple measurements are taken and the results are presented in the form of the algorithm. Common delusion is that the voice itself is

stored in the database. No, the output from the algorithm is stored in the database. For verification, another sample of the speech is taken. As in identification process the second sample is analysed, and measured. If the results match, the identity can be verified.(Salmat Speech, cited 22.04.2012)

How often in the cinema we can see how good and clever heroes, sometimes criminals play tricks with the voice print system with the help of little electronic devices where the sample of the voice needed is recorded. And the question that everybody asks himself: is it so simple? If nothing can be done to prevent it? If everyone can do it? But nowadays, the system of voice print has a special step that can be added to the process of verification. Liveliness test is a real answer to all the questions. The system asks the user to repeat a random phase or sequence of numbers. The recorded voice will not be able to repeat all this and the test will fail.

For voice verification two types of system can be used:

- Text-dependent when the decision is made using speech corresponding text
- Text-independent when there is no use in speech.

Voice print systems differ from each other:

1. Fixed password system: all users have one and the same password sentence.
2. User-specific text –dependent system: each user has his/her own password
3. Vocabulary-dependent system: password is made from fixed vocabulary
4. Machine –driven text-independent system: unique text should be pronounced
5. User-driven text-independent system: user is free to produce any speech he/she wants.

The first three systems belong to text-dependent type of the system, the last two- to the text-independent.(Voice Based Biometric Security System 20.04.2012)

3 Conclusion

Making conclusions of the first two chapters it should be mentioned that:

1) Biometrics has a long history that starts from the ancient time and is widely used in our days. This is very important because most of young people think that biometrics as a science appeared not long ago and just used in criminalistics. Although many people even do not realize that biometrics has many different methods.
2) Biometrics has its own functionalities: universality, uniqueness, permanence-measurability (collectability), perfomance, acceptability. Most of the people think that biometrics is rather helpful and useful. Among the main advantage of biometrics is security, that proves how accurate and attentively people treat their private information. One of the most popular methods of biometrics is fingerprinting.
3) Biometrics is wide spread among the population of different countries. The main confirmation of this is biometric passports. But in some countries people do not have clear understanding about what information this kind of passport contains and how this passport works. In most of the countries biometric passports contain the same kind of information: digital image of the owner, type, country code, number of the passport, surname and given names, nationality, date of birth, sex, date of issue, date of expiry.
4) Biometric identifiers can be of two types: physiological and behaviour. Physiological type includes such methods as: fingerprinting, iris recognition, DNA, palm printing, hand geometry, odour, and face recognition. Behaviour type includes: gait, voice, typing rhythm. Each method is based on the uniqueness of the measured part of the body/function of the body.
    a) Fingerprinting: is one of the oldest and most popular method of biometrics, is widely used in criminalistics. The main idea of the method is that the picture of papillary pattern is unique for each person. The sample of papillary pattern can be easily taken from any surface that the person touches. It is also considered that fingerprints are the most popular evidences in the places of crime.

b) Iris recognition is considered to be one of the most exact methods of biometrics, is based on the scanning of the iris.

c) Palm print is often mentioned with such methods as fingerprinting and iris recognition. There are 6 categories of palm and the category 5 has its own subdivisions.

d) DNA, as fingerprinting, is often used in criminalistics. This method is not automated, and this fact differs this method from another. Many people trust this method because of its exactness.

e) Hand geometry is not popular nowadays as it was 10 years ago.

f) Face recognition: the system produce the digital image of the person. Two technologies can be used: 2-d and 3-d.

g) Odour: production of so called ENoses allows this method to develop. It simulates the nose of a person to distinguish odours.

h) Voice is one of the fastest ways to identify a person.

i) Like voice, gait is also served for identification of a person, and like voice people can easily identify the person just spending less than a minute.

j) Typing rhythm: it is difficult to believe that even the way we typing can be unique. It is very important to understand and to remember that no matter "what" we write, the main idea is "how "we do it.

It should be noticed that in spite of the high level that each method of biometrics received, further investigations continue in order to achieve better results and to protect the information. Methods improve every day. But in spite of it produces try their best to make the systems easy to use, generally available and cheap. All this factors influence on the choice of the buyers and ability to competition.

4 References

360 Biometrics, What is a Hand Geometry, URL: http://360biometrics.com/faq/Hand-Geometry-Biometrics.php (cited 29.03.2012)

360 Biometrics, Difference Between Identification and Authentication, URL: http://www.360biometrics.com/blog/difference-between-identification-authentication/ (cited 04.03.2012)

About.com Terrorism Issues. History of Biometrics URL: http://terrorism.about.com/od/issuestrends/tp/History-of-Biometrics.htm (cited 01.03.2012)

A Century of Biometrics, URL http://www.cnil.fr/fileadmin/documents/en/AR-22-biometrics_VA.pdf (cited 21.02.2012)

Authentify Voice Biometric Authentication URL: http://www.authentify.com/solutions/voice_biometrics.html (cited 02.04.2012)

Bertenthal, B.I., Pinto, J.: Complementary processes in the perception and production of human movements. In Smith, L.B., Thelen, E., eds.: A Dynamic Systems Approach to Development: Applications. MIT Press, Cambridge, MA (1993) 209–239 cited 10.04.2012

Biometric authentication Using Random Distribution, Varun Kacholia, Shashank Pandit URL: http://shashankpandit.com/papers/bioart/paper.pdf (cited 27.03.2012)

Biometric Gait recognition, Jeffrey E.Boyd, James J.Little, URL: http://course.ku.ac.th/lms/files/resources_files/2512/157917/gait_10.1.1.110.9741.pdf (cited 30.03.2012)

Biometric Person Authentication: Odour, Zhanna Korotkaja URL: http://www2.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf (cited 16.03.2012)

Biometrics History, URL:http://www.biometrics.gov/documents/biohistory.pdf (cited 25.02.2012)

Biometrics in the Here and Now URL: http://www.technewsworld.com/story/59728.html (cited 21.04.2012)

Demistifying Voice Biometrics: The Future of Security is Available Today URL: http://www.usfst.com/article/Demystifying-Voice-Biometrics--The-Future-of-Security-is-Available-Today/ (cited 21.04.2012)

Derawi Biometrics: Research on Different Biometric Modalities, Gait, URL: http://biometrics.derawi.com/?page_id=38 (cited 03.04.2012)

DNA as A Biometric Identifier, URL: http://www.cse.msu.edu/~cse891/Sect601/CaseStudy/DNABiometricIdentifier.pdf (cited 15.03.2012)

Global Security.org, Hand Geometry and Handwriting, URL: http://www.globalsecurity.org/security/systems/biometrics-hand.htm (cited 10.03.2012)

Kriminalistika, uchebnik pod obshei redakciei professora A.G. Filippova, 4 izdanie, pererabotannoe i dopolnennoe Moskva, Visshee obrazovanie 2009, str 93-94 (cited 01.03.2012

National Biometric,history of biometric technology development URL: http://www.nationalbiometric.org/about_history.php (cited 22.02.2012)

Palmprint Classification, Li Fang, Maylor K.H.Leung URL: http://www3.ntu.edu.sg/SCE/labs/forse/PDF/palmprintClass.pdf (cited 28.03.2012)

Reading Room Sans, Iris Recognition Technology URL: http://www.sans.org/reading_room/whitepapers/authentication/iris-recognition-technology-improved-authentication_132 (cited 8.03.2012)

Rukovodstvo po biometrii ,Boll R.M., Konnel G.X., Pankanti Sh. 2007 (cited 24.02.2012)

Salmat Speech, 06.07.2010, what is a Voice Biometric URL: http://speech.salmat.com.au/be-educated/what-is-a-voice-biometric (cited22.04.2012)

SuperMegaOy.ru Protection of nets with the help of biometric systems URL: http://www.supermegayo.ru/compterr/43.html(cited 22.02.2012)

TechCast Article Series Use Of Biometrics, Vivian Chu and Gayathru Rajendran 2009 URL: http://www.techcast.org/Upload/PDFs/634122830612738824_Biometrics-VivianandGayathrilo-res.pdf (cited 01.03.2012)

Uchebnik, D.N Balashov, N.M Balashov, S.V Malikov. Kriminalistika 2 izdanie. Moskva, INFRA 2009, str58-64 (cited05.03.2012)

User Authentication Through Typing Biometric Features, Livia C.F., Luiz H.R 2.02.2005 URL: http://ai.pku.edu.cn/aiwebsite/research.files/collected%20papers%20-%20others/User%20authentication%20through%20typing%20biometrics%20features.pdf (cited 05.04.2012)

Voice Based Biometric Security System, Abhishek Mitra, Saurabh Bisht, 2002, URL: http://alumni.cs.ucr.edu/~amitra/bio_rep.pdf (cited 20.04.2012)

Wikipedia, Biometric Passport, URL:
http://en.wikipedia.org/wiki/Biometric_passport (cited 19.03.2012)

Wikipedia: History of Biometrics URL :
http://en.wikipedia.org/wiki/Biometrics#History_of_Biometrics (cited 21.02.2012)

Wikipedia Sir William Herschel, 2nd Baronet URL:
http://en.wikipedia.org/wiki/Sir_William_Herschel,_2nd_Baronet (cited 10.2.2012)