A Study on the Available Biometric Technologies Used in Order to Control Security in Physical Access

RICARDO JANES, AUGUSTO F. BRANDÃO JR, EDUARDO M. DIAS
Departamento de Engenharia e Automação Elétricas - PEA / GAESI
Universidade de São Paulo – Escola Politécnica da USP
Av. Prof. Luciano Gualberto, Travessa 3, nº 158, Sala A2-06 – ZIP Code: 05508-900 – São Paulo
BRAZIL
ricardo.janes@poli.usp.br; brandao@pea.usp.br; emdias@pea.usp.br

Abstract: - The control of the physical access in automated security systems, like banks, ports, airports and military areas, is essential to guarantee the financial security of the institutions and to prevent to the possibility of accomplishment of terrorist acts. To this, a lot of technologies used in security systems can be used, but the choice of a technology depends on some factors, as the level of security related with the financial value to be protected, the entailed cost to the technology implementation related to the level of offered security, and the physical characteristics to the proper installation. This work aims to present the main characteristics of the biometric technologies used currently in the control of physical access, therefore the biometry is known as the measurement technique more insurance currently in the identification of a person. The susceptibility to fraud, involved costs to implementation and installation of the biometric devices, advantages and disadvantages of each technology will be presented in this work. Some technologies have low costs for the implantation, but its use has low acceptance in some countries. Others have high trustworthiness but the cost becomes the prohibitive equipment. This work presents a relation cost-benefit, so that the choice of the technology can be made taking in account the involved cost and the degree of security of the technology to be used.

Key-Words: - Biometric technology. Biometry. Access Control. Smart buildings. Security systems.

1 Introduction

To analyze which the best biometric technology to be used in the control of the physical access in an automated installation, first we must make some considerations on what it is biometry, and its main characteristics, also verifying which parameters of analysis we must use to compare the diverse existing technologies [1].

Biometry can be defined as being the physiological or behavioral mensurations that can be used for verification of person's identity. It aims to identify to a person through the analysis of the individual physical characteristics such as fingerprints, face contours, hand geometry, iris pattern, retina and voice recognition, etc [2].

Behavioral-based methods used to measure the biometric characteristics of an individual person perform the authentication task by recognizing people's behavioral patterns, such as signatures keyboard typing or voice print. The main problem with behavioral methods is that they all have high variations, which are difficult to cope with, per example; the voice can be modifying if the person has flu. On the other hand, while behavioral characteristics can be difficult to measure because of external influences such as stress, fatigue, or illness, they are usually more acceptable to users and generally cost less to implement. Behavioral-based methods are normally used in systems that security level is low, like identification in telephonic systems. Physiological-based methods used to measure the biometric characteristics of an individual person verify a person's identity by means of physiological characteristics such as fingerprint, iris pattern, hand geometry, DNA, or facial features. In general, traits used in the physiological category are more stable than methods in the behavioral category because most physiological features are virtually no alterable without severe damage to the individual, but increase the costs to implement the technology. This method is normally used in systems that the security level is high, like banks and other organizations that aims to protect confidential information [3].

The responsible equipment for effecting the reading of these characteristics and interpreting them, thus recognizing the person who uses the device, generally aims to implement systems of security directed to the access control, that can be divided in two categories:

- ✓ **Control of the physical access** – entrance control of the person in clubs, banks, residences, museums, shopping centers, events, hospitals, arrests, buildings, ports, airports, military areas, and schools;

- ✓ **Control of the logical access** - the access control is mentioned to the computers, mobile nets of computation, telephones, confidential email, data and banking services (computer science).

So that the reading of a behavioral or physiological human characteristic being characterized as biometry, the following criteria must be respected, without exception of each item [4]:

- ✓ **Universality** - each person around the world obligatorily must have the physiological or behavioral characteristic;

- ✓ **Uniqueness** - this characteristic must be enough different between people;

- ✓ **Permanence** - the characteristic must be enough invariant during a certain period of time;

- ✓ **Collectability** - the characteristic can be measured quantitatively, and the measurement can be stored.

Still other factors must be considered in a biometric system, to consider that the technology has a degree of quality, as:

- ✓ **Performance** - the reading of the characteristic, the size of the information measured, its recognition and precision, and the speed of all signal processing, are characteristics that must be considered;

- ✓ **Acceptability** - the level of acceptance of the user is important to choice or not the technology. The most important factor to chose a biometric device is that how much the measurement process is invasive to people. It hopes that the device should be as less invasive as possible;

- ✓ **Security** - the system must be evaluated to identify if fraudulent methods could cause a false identification. In this factor, it could be to characterize an application device, according to the security level. [5]

The verification using biometry technology can be realized in two different methods:

1.1 Authentication - mode 1 : 1

The algorithm receives an identification number (PIN - Personal identification number), through a conventional keyboard, or by reading magnetic cards, by reading of bar codes (cards), smartcards and others, and after identify the person.

After the identification, it makes a reading of some biometric characteristic, as a fingerprint or iris pattern, and then it search in a data base of biometric characteristics, the image previously treated, digitalized and stored, associated to that number, later to compare the images and to determine if they are of the same person.

In this comparison, some statistic algorithms are used, and choose of each case is important to determine the security level.

This method just makes a comparison between two images (digital information about the images) to validate and authenticate the identification, because the person is already identified by the PIN [6], [7].

1.2 Identification - mode 1 : N

The equipment makes reading of any biometric characteristic and a specific algorithm receives the image, and searches in a data base of biometric characteristics previously registered and stored an image that has correspondence with that one received. It’s important to comment that all the images received by the algorithm are digitalized and stored as digital information, and the size of the generated file varies according the adopted algorithm.

When it finds, returns a key that allows the identification of the person. If this method of verification becomes all slower due to search of the similarity of the image in the data base, therefore, the speed of the validation is tied with the amount of stored information.

The algorithms work with taxes of coincidence between two images, that is, from one determined coincidence tax; the algorithm considers that both belong to the same person.

This tax never will be of 100% and is a characteristic of each algorithm.

The determination of this tax is made from the measurement of two parameters: the tax of false acceptance, also known as *False Accept Rate* - ***FAR*** and the tax of false rejection, also known as *False Reject Rate* - ***FRR***.

When it increases the percentage of coincidence, the tax of false acceptance *FAR* falls, but the tax of false rejection *FRR* increases.

The *Error Equal Rate* (***EER***) or the tax of equal error is the point of the curve where the tax of false acceptance is equal to the tax of false rejection.

This is an important parameter in the evaluation of recognition algorithms and biometric identification, therefore how much minor is the ***EER***, better is the algorithm [8], [9].

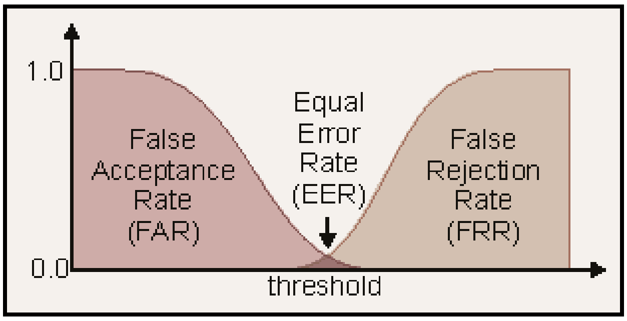


Fig. 1 – Taxes of coincidence

2 Analyzing the characteristics of each biometric system

To analyze the characteristic of each biometric system, it's necessary to define what the main types of biometric technologies are actually used.

The biometric technologies in study, not recognized by the enterprises that sell biometric devices, and the biometric devices that have high cost to implementation, do not analyzed in this paper.

The defined biometric technologies for study as defined by high use in Brazil, and are described below:

- ✓ Fingerprint;
- ✓ Hand geometry;
- ✓ Retinal scan;
- ✓ Iris recognition;
- ✓ Voice recognition;
- ✓ Face recognition;
- ✓ Hand signature.

The hand signature recognition analyzed is this paper is the dynamic case, because the static signature is analyzed only for specialized software used in image treatment, so the importance to characterize as a biometric device is not valid.

2.1 Fingerprint

The main technique of fingerprint identification consists of to capture an image from a fingerprint, through specific equipment (electronic scanners), to storage this image after the digitalizing process, and posterior identification of some characteristics, known as minutiae [10].

The main used readers used to capture the image from a fingerprint are:

- ✓ **Optic**: when placing itself the finger in a glass platform, a light is emitted on the finger, and the image is captured by an optic scanner. The light is generated by a LED (Light emitting diode), and its common to find in the red color;

- ✓ **Ultrasound**: in this equipment, the reading is made by ultrasound emission, and a reader calculates the return time of the emitted signal, transforming these signals into an image;

- ✓ **Capacitive**: the finger is placed directly on a silicon chip, and an electronic circuit catches the minutiae of the finger, generating an image from this detailing.

The analysis consists of verifying the position of the minutiae, such as ridges (or lines) bifurcations and terminations, and also verifying the arcs and returns that appear in the finger, using for this specific algorithms.

The most of the algorithms is based in a technology that identifies the fingerprint minutiae, as delta, core, termination and bifurcation.

After the extraction of this details, is calculated the relation between the distances of these points; each algorithm has your own calculus base, either for analysis of the points between itself or for groupings of points for analysis of triangles similarities with the internal angles.

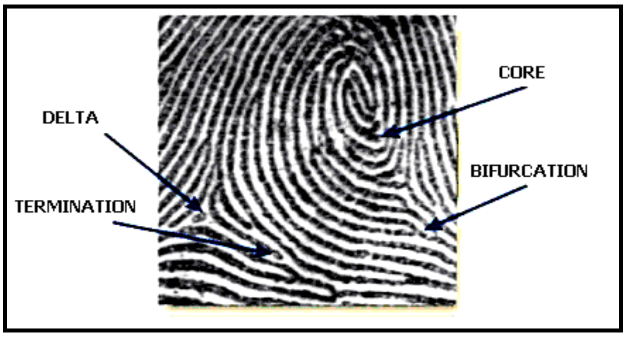


Fig. 2 – Minutiae of a fingerprint

The image of a fingerprint, after to be captured, is treated through specific filters for image treatment, thus generating one template in the black color, by facilitate the next stage of treatment.

The next stage consists of digitalize the image (white and black pixels), making with that the lines are reduced to only one pixel of width.

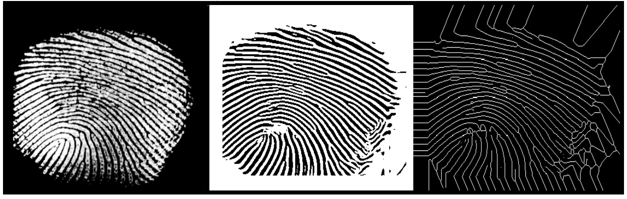


Fig. 3 – Three stages of a fingerprint analyses

With this last image, the algorithm now locates the points of minutiae, analyzing each pixel to verify if this is black or white. If there is a white pixel without neighbors, the algorithm interprets that a terminal point exists. In case that a white point has three neighboring points at the same color, the algorithm interprets that a bifurcation exists.

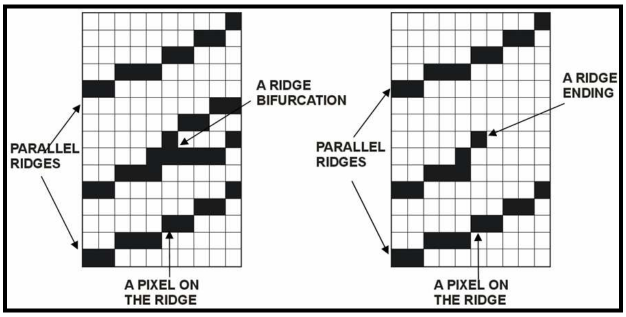


Fig. 4 – A fingerprint separated in bits

After analyzed the entire image, it must be compared the points of minutiae previously found with the points registered in stored registers, in the data base, for similarity verification between the images. A fingerprint has fifty points of minutiae on average, and is necessary about thirteen points in common so that the algorithm validates the reading.

The problems that can occur in the biometric verification characteristics of the fingerprint are tied with the quality of the generated image in the reading, and this can be: finger rotation at the moment of the reading, small wounds in the finger, scars proceeding from wounds caused by small accidents, after the cadastre of the fingerprint, drying of the skin, dirt in the reader, among others factors [11], [12]. The main advantages of the reading systems of fingerprint are high velocity and data interpretation, low entailed cost to the technology, reduced size of the readers and low level of intrusion to the users. The disadvantages are in the variation of the reading of the finger, causing “false negatives”, and mainly in the vulnerability of the system.

2.1.1 Use of the electronic and biometric ballot boxes in Brazil – a case study

In a democratic system of voting, the security of the vote is necessary for the exercise of the citizenship.

Therefore, aiming at to guarantee this right, some technologies have been developed for Brazilian Electoral Justice. Between them, it deserves prominence the development of Biometric Ballot boxes that will process the vote from the biometric identification of the voter.

The electronic ballot box with biometric reader was tested in three cities, being one of the Region North (Colorado of the West-RONDONIA), another one of Center-West (Fatima of the South-MATO GROSSO DO SUL) e, the last one, of the South Region (São João Batista), both in Brazil. By means of this system, the country will not only have the voting more informatized as well as more the insurance, since it will not have doubts how much to the identity of each voter.

The new system beyond registered the images of the fingerprints of all the fingers of the hands the photograph. In the day of the voting, after the presentation of documents for the voter, the identity of the voter was ratified by means of the biometric recognition of its fingerprint. Below, the image of the reader used in this process:

Fig. 5 – A fingerprint reader in use

In case that the board member has doubts with regard to the voter, or its digital one is not recognized for the biometric system, that one will have, to its disposal, the leaf of voting with the photos of all the voters of that section, which will be able to appeal for confirmation of the identity of the voter.

The objective of this biometric cadastre is to exclude the possibility of a person to vote for other, becoming impracticable the fraud the voting procedure.

The expectation is of that, in ten years, all the states of the Country have ballot boxes with biometrics readers.[13]

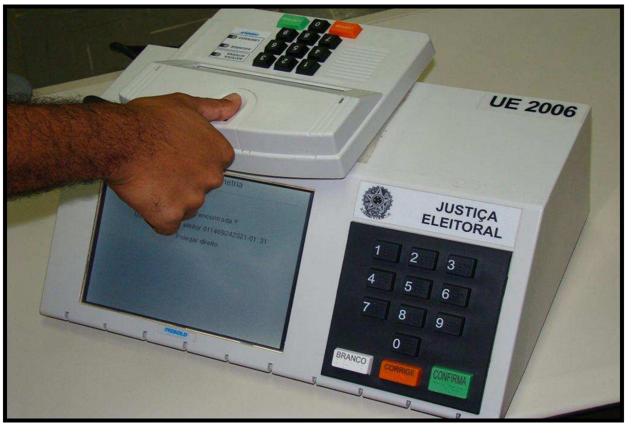


Fig.6 – Brazilian ballot box with biometric reader

The identification process will have to confirm the identity of each voter all, comparing the data supplied with the available data base.

Electoral Justice will have the care to collect given referring to all the fingers of the hand of the voter. Thus, in the case of the reading of the ballot boxes of the TSE, the possibility of a voter to vote in substitution to another one is practically nulled. The possibility of an authentic voter to be denied by the biometric system is real, even so very rare.

This occurs because the fingerprints of a person can temporarily disappear because of use of chemical products or several scaling off in the palm of the hand. In case that this situation occurs, the board members will have other resources to make to be valid the vote of the Brazilian voter: the confirmation for the photo, the constant data in the electoral heading, or other procedures in the law.

To create the new register in cadastre on the basis of biometric voters, Electoral Justice goes to present a kit (Kit Bio) in the electoral sections of the three cities selected for the project-pilot.

The calls “Kit Bio" they are one composites the box and a great folder. They fit a portable computer (laptop), a digital camera, a reader biometric scanner and a photographic mini-studio with seat. [14], [15].

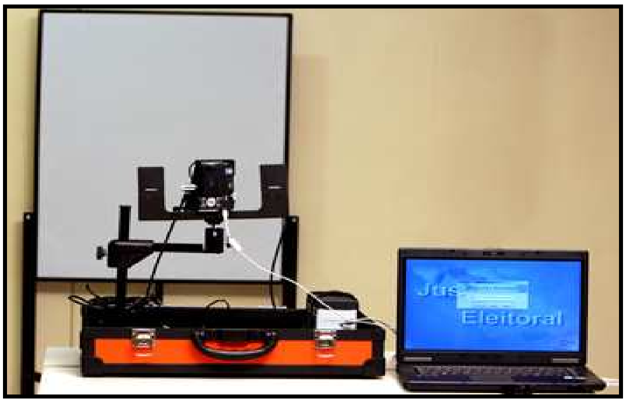


Fig. 7 – Kit Bio to collect biometric characteristics

2.2 Hand geometry

This technology has for purpose the reading of the physical characteristics of the hand of a person, being based on the fact of do not exist two people with identical hands and of that the hand do not suffer to significant changes certain age after.

The reading is carried through of three-dimensional form, however, the only characteristics can vary due the diverse factors as change of weight or diseases, and dirt in the hands or cuts, and for this reason, this technology is not used for identification, just use for authentication, having characterized the biometric verification mode 1:1. The hand dimensions, as the size of the finger, width and area are the main characteristics used in the analysis. For this, the equipment leads about two seconds capturing the image of a hand and producing the resultant analysis. The captured image occupies little space for storage, therefore, the number of people registered in cadastre in unique equipment is raised, making with this technology wide is used in places of great movement and access such as university, clubs, etc. The main problem in the use of this technology is in the correct hand positioning, preventing itself thus the improper rotation, and for this, they exist, in the equipment, alignment bolts or pins that induce the user to correctly place its hand in the interior of the reader. For the capture, the user locates its hand in the reader, lining up the fingers with aid of the pins, and a chamber located above of the hand captures the image. Some equipments use a set of mirrors to capture the three-dimensional image of the hand. Three-dimensional measures of selected points are taken and the system extracts the information to determine length, width, thickness and bending of the hand and the fingers and translates this information for a numerical standard, creating an only mathematical identification in the creation of the model. A typical model requires about nine bytes of storage. The security against frauds in this system if bases on the fact of that it is practically impossible to private get information on the geometry of the hand of a person, the least that has its cooperation. About the stability, it must be considered that geometry of the hand changes in accordance with the age and, occasionally, with the loss or profit of weight [16].

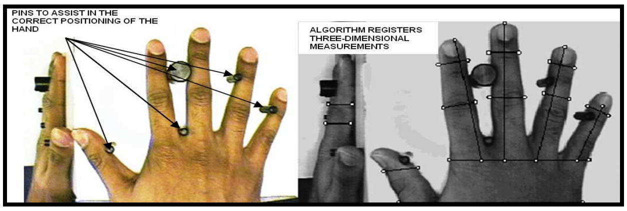

PINS TO ASSIST IN THE CORRECT POSITIONING OF THE HAND
ALGORITHM REGISTERS THREE-DIMENSIONAL MEASUREMENTS

Fig. 8 – Hand positioned in the equipment

2.3 Retinal scan

The biometry of the retina is based on the layer analysis of the sanguineous vases in the eyes base (deep). For this, it uses a light of low intensity normally proceeding from a laser, and a camera, so that sweepings are carried through, to find the singular standards of the retina, therefore the trustworthiness of this method if must to the fact of the structure of the sanguineous vases be related with the personal vital signals, and thus, the reading device will not obtain to define the standard of the retina of a person if this will be without life.

The acceptability of the technology is low because it requires that the user looks in a viewfinder and focuses one definitive point.

Some medical specialists in eyes affirm that characteristics of the retina is not steady and that some illnesses exist that can modify its format, therefore, still studies exist to analyze the use of this type of technology in the access control.

The analysis carried through for specific algorithm, hides 900 points distinct; therefore, the technology has an excellent precision, if compared with the analysis of about 50 points of the biometry for identification of fingerprint, and the analysis of about 400 points the biometry for identification the Iris [17].

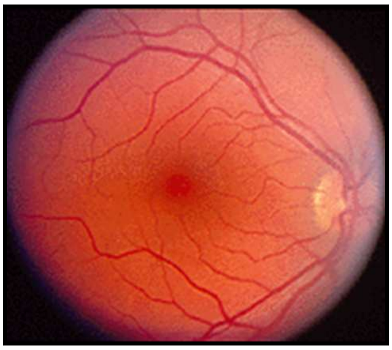


Fig. 9 – Retina and sanguineous vases

2.4 Iris recognition

The Iris is the ring colorful that surrounds the pupil of the eye, and although to be external visible, it is an internal component of the eye. Each iris contains an only structure, characterizing a complex standard. She can be a combination of specific characteristics as crown, gland, filaments, radial and stretch marks, ridges. These characteristics are highly complex and unique, and the probability of two Irises to be identical is esteem in about 1 in 10^{78}. The recognition process initiates with the acquisition of a photograph of the iris taken off under an infra-red illumination, therefore the Irises of dark pigmentation disclose to greater complexity when under this type of illumination, although to be possible to use a visible light [18], [19].

The resultant photograph is analyzed using specific algorithms, normally patented, that locates the Iris and extracts the necessary information to create a biometric sample.

The system can be used by people who use contact lenses, for not being invasive, this technology has better acceptance for the user, and therefore it requires a lesser interaction of the user. The Iris cannot be modified by cosmetic surgery.

The identification for analysis of the Iris generates 600 points approximately, whereas the average of minutiae generated for a fingerprint is of 50, therefore, this process is more necessary, however, the cost still is raised to a use on a large scale.

The process of reading of the Iris consists of:

- ✓ To locate the presence of the eye in the image;
- ✓ To locate the exterior and interior limits of the Iris;
- ✓ To detect and to exclude eyelids, if these will be able to induce errors on readings;
- ✓ To define a system of coordinate 2D, where is mapped the Iris standard and generate these code;
- ✓ The Code of the Iris can be stored in hexadecimal code in a data base or another type and media. A time in the data base, the code is used as base for the comparison against the captured Iris for the camera in the process of identification of a person.

Below, the detailing of a human eye can be seen in the figure. The Iris is the bluish green area. The other visible structures are the pupil (black circle in the center) and sclera (white part of the eye) around of the Iris. The cornea is present in this photo, but it is not possible to see it, for being transparent.

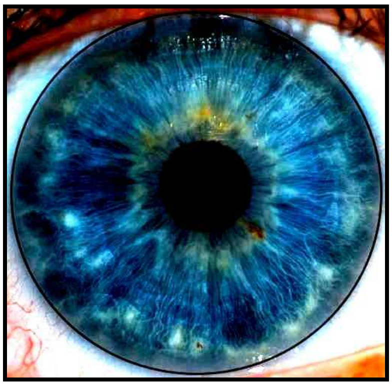


Fig. 10 – Human Iris

2.5 Voice recognition

The sound of the human voice is generated by the resonance in the vocal fold. The length of the vocal fold, the format of the mouth and nasal sockets are important things in the determination of the voice of a person. The sound is measured when affected for these specific characteristics.

The technique of measurement of the voice can use as dependent methods of text or not. That is, the voice can be captured with a user speaking a specific password of combined phrases, words or numbers (dependent), or any form of phrase, words or numbers (independent).

Currently, the dependent techniques of text are dominant in the available commercial systems of identification of speak.

Noises and interferences in the environment where the equipment of reading and interpretation is installed could to diminish the performance of all the system to voice recognition. The basic process to voice recognition is:

- ✓ Capture: the user must speak in a microphone, a phrase previously selected (dependent) or a random phrase (independent). This process generally is repeated some times to construct to a profile of the voice, thus eliminating some noises;

- ✓ Extraction: biometric equipment extracts the only signal of the voice and then one template is created;

- ✓ Comparison: the verification one-to-one is the preferential method. The user speaks in a microphone; the new example of voice then is compared with template stored. The waveform of the phrases is measured using Fourier analyses to find the specter of frequencies that show the characteristics of the voice, and after that, the comparison is based on the two characteristic from the human waveforms voice:

Cepstral analysis - analysis that allows representing the similarities between two waves of voice as a simple Euclidean distance that will be converted into one “match score”;

HMM score - probability of a wave to have been generated for the same source that one another form of wave template.

The main limitations in the use of this technology are that the voice changes during the time due to some factors, such as natural ageing, stress, cooled, and that the system can be deceptive by a previously recorded voice.

The average time for make a register of voice is of three minutes, and the verification is carried through in about half minute, showing as soon as the technology is fast to use.

The level of intrusion to the user is low, but the use in environments with level of raised noise must be prevented, therefore the same it influences in the reading of the voice [20], [21].

2.6 Face recognition

The technology of face recognition has for purpose to recognize the identity of people through the analysis of the face. Making specific use of software and mathematical algorithms, a computer locates faces human beings in data visual field through cameras and compares with one definitive database previously constructed.

To recognize the face of a person, the programs technically trace the geometry and the ratios of the face. Then some delimiters points in the face are registered, which allow defining ratio, distances and form of each element of the face and, on the basis of these data, to initiate the comparisons.

The main points are: eyes, nose, and chin, high cheek bones, ears, lips, mouth, eyebrow, and the relation between them.

The technology of face recognition considerer that he measures of the face that never changes, exactly that the person is submitted to the cosmetic surgeries.

The basic measures are: Distance between the eyes; Distance between the mouth, nose and the eyes; Distance between eyes, chin, mouth and line of the hair. The camera captures a photograph of the human face that is mapped in a series of 128 numbers, known as coefficients.

These are processed of form to compose a bi-dimensional arrangement only and, of the disposal of clear and dark areas of the face.

Also an optional test of face expressions can be made, to diminish the possibility of frauds [22], [23].

The face recognition in 2D has some limitations, to the level of the images that it captures, therefore can confuse the person through the face expressions. However, with the development of the technology in 3D, many of these difficulties leave to exist.

Main characteristics of the technology:

- ✓ High acceptability, therefore the photograph is accepted in a general way in diverse places as identification form;
- ✓ Low level of intrusion to user - the user does not have interact with the equipment during a period of significant time;
- ✓ Can be created face templates without the physical presence of the individual, in the case of the technology in 2D;
- ✓ The verification human being of biometric template against the person/existing photograph is relatively simple and habitual for the responsible entities for the control of borders.

It must be considerate, before the choice of this technology, that the cost still is raised, had to the use of automated systems of high technology, has low trustworthiness and the time of reading and research are raised [24], [25].

2.7 Hand signature - dynamic recognition

The biometric systems that analyze the written by hand signature verify the act to write, the pressure, the speed and the rhythm of the writing, therefore the simple signature, of static form, is easy to copy, although to exist biometric systems that carry through this type of analysis.

These systems also register the sequence of the writing, in the method as the letters are formed, as if they add to points and traces when writing or the existing pause enters the writing of two words.

To make the reading, is normally used a scanner composed for sensors that recognize the angle, pressure and direction of the writing, carried through on a specific area of the equipment.

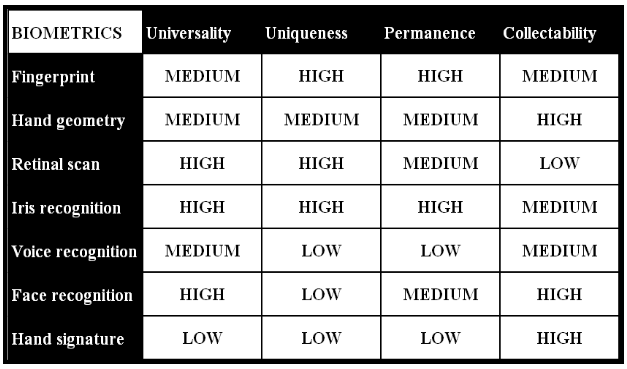
As comment before, the static recognition of hand signature is not analyzed because is easily copied, and the process for identification is only to use specialized software to image recognition.

A specific mathematical algorithm analyzes the writing with one previously template stored, and then it makes the comparison, validating or not using it [26].

3 Results

Analyses of cost for the implementation of the technology, efficiency based on the security offered for the system and advantages and disadvantages of each technology they had been carried through in this work.

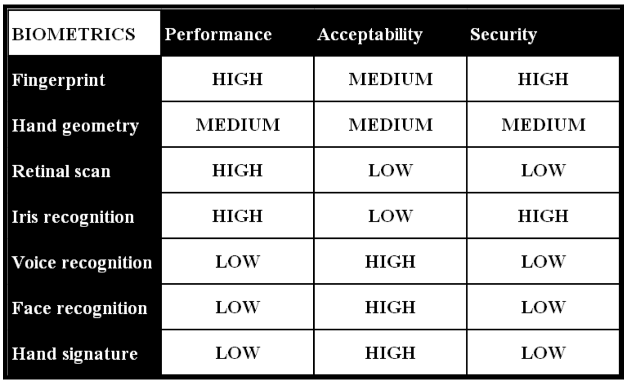
The following table shows a comparison of existing biometric systems in terms of the parameters that it characterizes as biometry, as universality, uniqueness, permanence and collectability.



BIOMETRICS	Universality	Uniqueness	Permanence	Collectability
Fingerprint	MEDIUM	HIGH	HIGH	MEDIUM
Hand geometry	MEDIUM	MEDIUM	MEDIUM	HIGH
Retinal scan	HIGH	HIGH	MEDIUM	LOW
Iris recognition	HIGH	HIGH	HIGH	MEDIUM
Voice recognition	MEDIUM	LOW	LOW	MEDIUM
Face recognition	HIGH	LOW	MEDIUM	HIGH
Hand signature	LOW	LOW	LOW	HIGH

Tab. 1 – Parameters of a biometry technology

The following table shows other parameters that can be considered to choice a biometric technology, as performance of the system, acceptability by users and security level:



BIOMETRICS	Performance	Acceptability	Security
Fingerprint	HIGH	MEDIUM	HIGH
Hand geometry	MEDIUM	MEDIUM	MEDIUM
Retinal scan	HIGH	LOW	LOW
Iris recognition	HIGH	LOW	HIGH
Voice recognition	LOW	HIGH	LOW
Face recognition	LOW	HIGH	LOW
Hand signature	LOW	HIGH	LOW

Tab. 2 – Parameters of quality of each technology

The advantages and disadvantages (limitations) of each biometric technology, studied is this work, is described below.

3.1 Fingerprint

Advantages: convenient and easy to use, low cost to implementation, low dimension, due to the use of silica sensor, ideal for all applications.
Limitations: connotation of criminal justice, performance is affected dry, oily, dirty or healed fingers, contact is considered unhygienic in some Asian countries. Files require approximately 1kB to storage the template.

3.2 Hand geometry

Advantages: convenient and easy to use, file require 9 bytes to storage the template, not affected for skin conditions, ideal for access control. **Limitations:** high size, high cost, contact considered unhygienic in some Asian countries.

3.3 Retinal scan

Advantages: very high taxes of precision. **Limitations:** medium-high infrastructure, discomfort with the light generated by the equipment in the eye, requirement of 96 bytes to storage the template.

3.4 Iris recognition

Advantages: high precision tax, bigger than the DNA identification, high speed, ideal in ports, airports and security areas.
Limitations: high cost, discomfort to the user, requirement of 512 bytes to storage the template.

3.5 Voice recognition

Advantages: low cost, ideal for telephony applications.
Limitations: low precision, noises can be affect the reading, requirement of 1500 to 3000 bytes to storage the template.

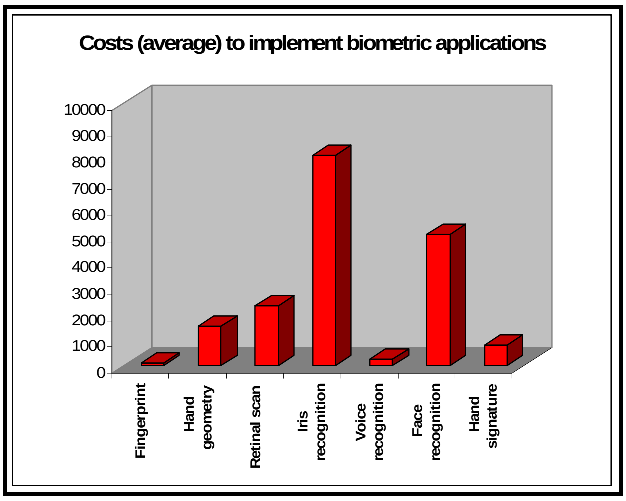
3.6 Face recognition

Advantages: ideal for monitoring intentions can be used without knowledge for user.
Limitations: adequate illumination and controlled environment to install the equipment, requirement of 500 to 1500 bytes to storage the template.

3.7 Hand signature

Advantages: it can be used in any device with a sensible touch screen as PDAs, and smart phones, effective cost, socially acceptable.
Limitations: low precision, requirement of 1000 bytes to storage the template.

The following graphic shows the costs to implement technology. The costs are an average of some equipment manufacturers, and esteem in accordance with the Brazilian market, therefore, the estimates cannot be applied to other countries.



Graph. 1 – Costs of implementation of biometric applications

4 Conclusion

This paper has presented a preview about the main biometric technologies used in automated installation, to improve the security systems for the access control. The costs and the security level are the main characteristics that can be considered to make the choice. In some cases, the user profiles it's more important that the other characteristics.
With the data about biometric technologies exposed in this paper, it's possible to planed multimodal biometric systems, according to the automated installation, creating integrated strategies that can be adopted to fuse information and improve overall system accuracy. It's necessary to be careful when choosing biometry as a technology to control physical access, because in some countries, all the devices that need to be touched do not have high acceptance, so the security level or the costs are not the most important criteria to the choice.
The most used device in Brazil is the fingerprint recognition, because offers a certain level of security with the low cost to implementation.
In some banks, the iris recognition is the preferential device to application. In the Santos port (the biggest port of Brazil), the hand geometry technology is used.

References:

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Sec. Privacy Mag., Vol.1, Nº.2, pp. 91-98.
[2] A. K. Jain, A. Ross, S. Prabhakar, An Introduction to Biometric Recognition, *IEEE*

Transactions on Circuits and Systems for Video Technology, Special Issue on Image an Video-Based Biometrics Vol.14, Nº1, pp. 04-20.

[3] VARCHOL, P., LEVICKY, D. Access security based on biometric. In Proceedings Research in Telecommunication Technology. NoveMesto na Morave (Slovak Republic), 2006.

[4] Z. Riha, V. Matyas, *"Biometric Authentication Systems"*, FI MU Report series, 2000.

[5] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*. Norwell, MA: Kluwer, 1999.

[6] J.Ortega-Garcia, J.Bigun, D.Reynolds, J.Gonzales-Rodriguez, "Autentication gets personal with biometrics", *IEEE Signal Processing Magazine,* March 2004, pp. 50-62.

[7] Ross A., Nandakumar K., and Jain A. *Handbook of Multibiometrics.* Springer, 2006.

[8] V. Matyàs and Z. Rìha, *"Biometric authentication - Security and usability,"* in Proc. 6th IFIP TC6/TC11 Conf. Commun. Multimedia Security, 2002, pp. 227–239.

[9] G. Bleumer, *"Biometric Authentication and Multilateral Security"*, AT&T Labs-Research, 2000.

[10] D. Maltoni, D. Maio, A.K. Jain e S. Prabhakar, *"Handbook of Fingerprint Recognition"*, Springer, 2003.

[11] A. K. Jain, L. Hong, S. Pankanti, R. Bolle. "An Identity-Authentication System Using Fingerprints". P*roceedings of the IEEE,* Vol. 85, Nº. 9, September 1997.

[12] Jain, L.C., Halici, U., Hayashi, I., Lee, S.B., Tsutsui, S.: *Intelligent Biometric Techniques in Fingerprint and Face Recognition,* CRC Press LLC, (1999).

[13] Camarão, Paulo César Bhering. *O Voto Informatizado: Legitimidade Democrática*. – São Paulo: Empresa das Artes, 1997.

[14] Ferreira, Pinto. *Código Eleitoral Comentado*. - São Paulo: Editora Saraiva, 1991.

[15] Brunazo Filho, Amilcar. *Fraudes e defesas no voto eletrônico* - São Paulo. ALL-Print Editora, 2006.

[16] R. Sanchez-Reillo, A. Gonzáles-Marcos. "Access Control System with Hand Geometry Verification and Smart Cards". *IEEE Aerospace and Eletronic Systems Magazine,* Vol. 15, Nº. 2, Feb. 2000. pp. 4.

[17] H. Korves, L. Nadel, B. Ulery, and D. Masi, *"Multi-biometric Fusion: From Research to Operations"*, Sigma, Mitretek Systems, Summer 2005.

[18] J. G. Daugman, *"Biometric personal identification system based on iris analysis,"* U.S. Patent 5,291,560, Mar. 1, 1994. U.S. Pat. Off., Washington, DC.

[19] R. Wildes, "Iris Recognition: an emerging Biometric technology" *Proc. IEEE,* Vol. 85, Sept.1997, pp 1348-1363.

[20] M. Faundez-Zanuy, E. Monte-Moreno, "State-of-the-art in Speaker Recognition," *IEEE Aerospace and Electronic Systems Magazine,* 20 (5) (2005) pp. 7-12.

[21] L.R. Rabiner, R.W. Schafer, *Digital Processing of Speech Signals*, Prentice-Hall, Englewood Cliffs, NJ, 1978.

[22] B. Achermann, X. Jiang, and H. Bunke, "Face recognition using range images", in *Proc. of International Conference on Virtual Systems and MultiMedia* (VSMM97), Geneva, Switzerland, Sep. 1997, pp. 129-136.

[23] T. Ko and R. Krishnan, "Fingerprint and Face Identification for Large User Population", *Journal of Systemics, Cybernetics and Information,* Vol.1, No. 3, pp. 87-92, 2003.

[24] B. Victor, K. Bowyer, S Sarkar. "An Evaluation of Face and Ear Biometrics". In: *Proc. Of International Conference on Pattern Recognition.* 2002, pp. 429–432.

[25] K. Chang, K. W. Bowyer, S. Sarkar, B. Victor. "Comparison and combination of ear and face images in appearance-based biometrics". *IEEE Transactions on Pattern Analysis and Machine Intelligence.* Vol. 25, No. 9, 2003, pp. 1160–1165.

[26] R. Plamondon and M. Parizeau, "Signature verification from position, velocity and acceleration signals: A comparative Study," Proceedings of the 9th Int. *Conf. on Pattern Recognition (ICPR'88),* Vol. 1, 1988, Rome, Italy, pp. 260-265.