Biometric authentication systems

DOMONKOS VARGA, ANDRÁS OLÁH

Budapest University of Technology and Economics, Department of Telecommunications
vargad@hit.bme.hu, olaha@hit.bme.hu

Keywords: personal identification, electronic scanning, security procedures

The security requirements of identification systems have increased considerably recently. This rapid change can partly be explained by the political trends that caused the people to be more and more concerned about their personal or proprietary safety. The conventional security solutions are no longer able to satisfy this demand. Therefore new authentication systems have to be introduced. Amongst these new systems the ones based on biometric authentication may play a decisive role.

Biometrics is one of the various technologies that utilize behavioral or physiological characteristics to determine or verify identity (such biometrics are fingerprint, face, hand geometry, speech, signature, typing dynamics, DNA, iris and retina). During biometric identification personal features are used rather than a conventional code or chip card. In the last decade several solutions were worked out. The motives that ensured the rapid development and spread of biometric systems are as follows [1]:

– the recent increase in the number of passwords causes the security to decrease.
– password management is of extreme cost.
– the importance of authentication required for accessing confidential information has been increasing gradually.
– there is a need for the integration of different security systems, and
– the most up-to-date security system has to be implemented.

Biometric security systems can be divided into two classes. The biometric verification (**BV**) systems make a one-to-one or one-to-few comparison. During verification the newly measured biometric samples are compared to the biometrics stored on disc or card.

The so-called biometric identification (**BI**) systems make a one-to-many comparison. The identity of the target person is determined from a great population. Usually these systems are quite slow as the identification is solely based on the incoming biometric information. Basically these incoming values are compared to the stored data and the most probable identity is chosen. The higher the population, the more complex the search, and the less reliable the result. The **BI** method is very comfortable since there is no need to use supplementary devices. Certain algorithms and special database structures can adequately reduce the time needed for proper identification. By increasing the reliability of the system, however, the false rejection rate may also increase, which in turn might irritate the user. An exact search time cannot be established since it depends on the user population.

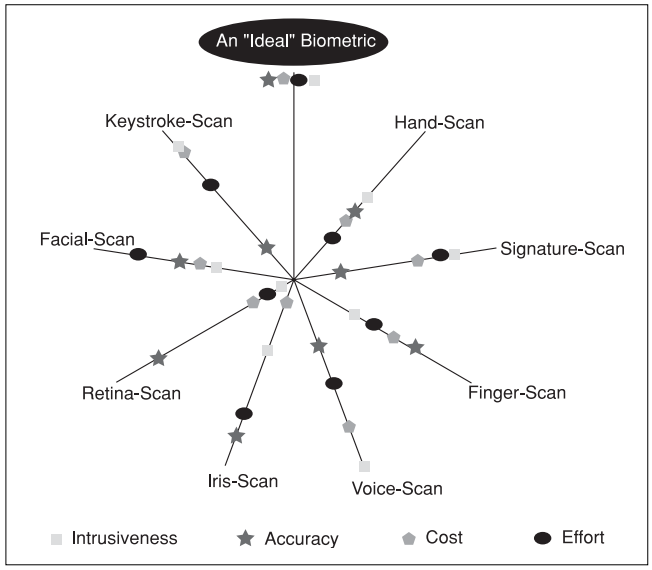
Amongst the advantages of **BV** systems as compared to BI systems are their better price, higher speed and accuracy, as well as their better error properties.

Nowadays the research focuses primarily on the identification systems, because there are several questions that have not been answered yet. One of the major problems is how an identification system can be implemented so that it would be fast and secure enough, and, in the same time, it would operate on large user population.

1. Main objectives

Vendors claim that there is no best biometric technology. A biometric identification technology can be defined as the most accurate, the easiest to use, the easiest to deploy or the cheapest solution, but no system meets all these criteria. For the proper comparison of the different systems an objective measurement tool has to be introduced with which the efficiency of the different implementations can be expressed. This objective tool is the so-called Zephyr chart *(Fig. 1).*

Fig. 1.



The Zephyr chart examines the different technologies from four main points of views, namely the ease-of-use, the cost, accuracy and the perceived intrusiveness. The further the parameter from the center, the better the property of that biometry [1].

1.1. Accuracy

There are two parameters for the measurement of accuracy:

- False Acceptance Rate (**FAR**) – that is the probability of the acceptance of unauthorized individuals.
- False Rejection Rate (**FRR**) – which is the probability that the system rejects an authorized individual.

From the security point of view the emphasis is on keeping as low false acceptance rate as possible. From the user point of view, however, it is just as important to establish fast and accurate recognition. (It is certainly not so fascinating to be able to get access just in the tenth trial.) The FAR for average biometric systems is between 1/100000 and 1/1000000.

1.2. Cost

At the beginning biometric systems were solely used in situations where providing extreme security was of great importance. Thanks to the decreasing costs biometrics is becoming more and more wide-spread. (Areas where biometrics has been gaining ground were computer system authentication, door control, work hour registration, alarm systems, etc.) A considerable part of the costs comes from the control and management software. The price of the installed peripheral devices may also vary between wide ranges. The overall cost of the systems, however, has been gradually decreasing.

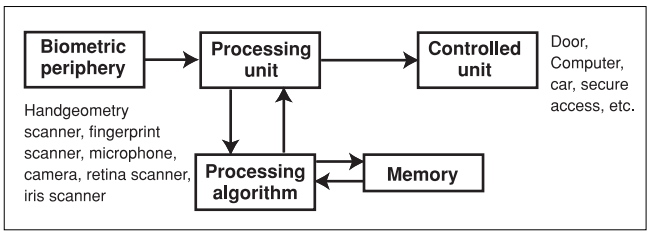
1.3. Effort

The usage of biometric systems needs to be user friendly as well as easy to learn.

1.4. Intrusiveness

There are certain factors other than technical ones that have to be taken into account during the design process. One of the most important non-technical feature is trust, i.e. whether the user can accept that the system reliably identifies them and only them. The other such feature is ergonomics, i.e. how comfortable it is to use the system in long term and how much effort is needed for the every day usage.

Fig. 2.



In the following section an overview of a general system is presented which helps to understand how the different biometric identification techniques work. (Of course there are other possible schemes as well.) The main functional blocks are depicted on *Fig. 2.*

- The role of the biometric peripheral device is to read biometric parameters and to convert them to digital signals so that they can be understood by the processing unit. The cost of this peripheral device largely depends on the sampled biometric parameter. (The price of a simple microphone or camera is just a tiny fraction of that of a fingerprint reader.)
- The processing unit controls the entire system, and also interacts with the user. It informs both parties whether the identification is successful and whether or not access can be granted for the examined person.
- The processing algorithm performs identification and recognition by comparing the original and the actual samples. The original samples are stored in memory. Although the memory is expandable, its maximum size is limited. This is mainly because the larger the memory the larger the population. High population means higher error probability and in case of identification systems the processing time also increases. If the population exceeds a certain limit it is more feasible to store the original samples in personal chip cards than in the memory of a central mainframe. This arrangement retains speed and security but has one major drawback: a card is needed for the identification. Further problems might arise if this card was lost.
- The controlled unit can be anything that requires security. In practice it is usually a computer system or a door lock system of a building.

In the next section the most common biometric identification systems are introduced.

2. The types of biometric identification systems

2.1 Face recognition

Face recognition systems are not that successful in practice. There are several features which the recognition can be based on. Usually the target person is identified by the contour of their face [1,2]. The geometric features of the face (the distance of the eyes from the edge of the face or from each other, nose length, mouth width, eye width), together with its profile or its thermogram are also used [1].

There are smaller systems for home use which can be utilized in smaller, family-size populations. Also, there exits larger systems that can cope with bigger population. The latter is for in hospital or in bank use and is for identifying patients or customers respectively.

The only way face recognition systems can be successful is when they either work on small population or they are combined with other solutions [1].

2.2. Identification based on iris patterns

The iris is the colored ring that surrounds the pupil. Iris biometric technologies analyze the complex pattern of the iris. The cornea, crypts, filaments, freckles, pits, radial furrows and striations make up such a complex system that cannot easily be duplicated and that possesses more than 400 different measurable parameters [3]. Even the irides of identical twins are different. Amongst all biometric systems this one is the most secure. The method can even distinguish between live and dead people's irides. The recognition process starts with the localization of the edge of the iris. It is followed by image capture. Then the artifacts caused by the shadowing effects of the eyelid and glimmering are compensated. The recognition itself is performed on this preprocessed image.

Performing the above steps results in a so called IrisCode record that serves as a reference for future recognitions. The system is so reliable that it can accurately recognize millions of people [1,3].

2.3. Identification by signature

The development of signature verification systems started a long time ago. Signature verification systems extract and measure a number of characteristics, such as the velocity and acceleration of the signature, the pressure exerted when holding the pen or the number of times the pen is lifted from the paper [4,5]. Two platforms were developed to measure these parameters. The first one is a special pen that is connected to the processing unit via a special cable [6]. The other one is a special plate [7]. The two platforms may also be combined.

Signature verification methods are very accurate with low false acceptance rate. Their use is optimal in situations where signature is a common and accepted way of identification.

It should be noted that making the signature recognition process adaptive is a key point since signature might drastically change by time. [4].

2.4. Identification by keystroke dynamics

Keystroke dynamics are also referred to as typing rhythms. This method analyzes the way a user types at a terminal by continuously monitoring the keyboard input. It has been shown that the typing can serve as biometrics. It is a security method only used in connection with computer systems.

The typing rhythm is checked a thousand times per second. Obviously, keystroke dynamics are behavioral and evolve over time as users learn to type and develop their own unique typing pattern. Although the security level of keystroke dynamic verification systems is not very high, it has got one main advantage: the target people are continuously monitored during their work [1].

2.5. Identification by retinal scan

The artificial duplication of the retina is impossible due to its unique properties. Retinal biometric technologies utilize low intensity infrared light together with an optical coupler to scan the blood vessel system pattern in the back of the eye ball known as fovea. The blood vessel system pattern changes with death, and it is impossible to remove it.

Although the retinal identification system is quite secure, it has a major disadvantage. Its use is uncomfortable, because the user has to look into a receptacle and focus on a given point, and their head must be held still for a couple of seconds [1].

2.6. Identification by voice recognition

Since the human voice has some unique characteristics it can also be used for identification. Voice recognition biometric technologies are based on sampling the spectrum (or rather cepstrum) of human voice and comparing it to the stored pattern.

Identification by voice is a plausible method. Some implementations use sensors attached to walls, while others are implemented as small devices that can be placed in conventional telephone receivers.

Voice verification biometrics is currently used in security control or as a door lock mechanism [1].

2.7. Identification by fingerprint verification

Two biometric property sets are used for identification by fingerprints:

Minutiae – these are the crossings, discontinuities, loops, marks, junctions, and bridges in fingerprints.

Pattern – patterns can be grouped into the following main classes: common arc, common loop, double loop, random line, sharp arc, and spiral.

By the appropriate analysis of the above characteristics the identification can be very accurate. About 100 such characteristics can be analyzed. (Even the fingerprints of identical twins differ to some extent.) A considerable part of biometric identification systems belongs to the so-called Automatic Fingerprint Identification Systems (ASIF). These are utilized by national, international, or federal institutions (FBI, INTERPOL, police etc.) in more than 30 countries.

Some implementations simply emulate the AFIS techniques (with the help of optical or capacitive sensors), others are based on pattern recognition or use ultrasonic scan to identify thresholds [1,8]. There are devices that can even determine whether the scanned fin-

gerprint belongs to a live or a dead person. Presently, fingerprint biometrics is the most widely adopted biometric technologies in the industry.

It is certainly not surprising that due to their low cost, small weight and integrability fingerprint identification systems are used in computer jobs [1], in which the population is limited. Such systems are capable of replacing tradition passwords on computers and make it possible to use fingerprint information instead [8].

2.8. Identification based on hand geometry

Identification by hand geometry is the analysis of the hand geometry including the fingers. The scanned parameters make the hand geometry a useful and applicable identification system (more than 90 different parameter can be analyzed). The analysis is just as detailed as the micro-injuries of the hand would not affect the results of identification [9].

The hand geometry biometric system performs 3D scan to measure the physical characteristics of the hand and the fingers. The identification is based on the comparison of the geometric properties of the palm, or one or two fingers with the stored sample. (The three versions might also be combined.)

The hand geometry analysis is fast, accurate and easy to use. The method can be used well in case of large user population or if the users are with inexperienced [1]. The security provided by the system is not only high, but also allows for flexible acceptance level and easy configuration.

Hand geometry systems are widely used, especially in work hour registration [1,9]. They can easily be integrated with other systems through which a more secure system is formed.

2.9. Complex biometric identification systems

Each biometric identification system has its advantages and disadvantages. Although some of these systems are easy to use, they would not be able to guarantee adequate level of security in standalone mode. By combining three or four such biometric methods complex biometric systems are formed to provide for higher security and to utilize the advantages of the individual subsystems [10].

The overall uncertainty of the complex system is the product of the uncertainty of the subsystems. So if three systems were combined all of which had a false acceptance rate of 1/100, the combined system would have a FAR value of 1/1000000 [10]. And this means a significant increase in security.

3. Summary

Thanks to their ease-of-use and high reliability biometric systems now serve as a measure in the field of authentication applications. The overall cost of such systems varies between wide ranges. A part of the costs comes from the peripheral devices, from the processing unit, and form the memory, and a considerable part is needed to cover the expenses of the software.

The memory requirements also has an effect on the spread of the different biometric systems (the chart bellow depicts the typical memory sizes for the leading biometric technologies) [1].

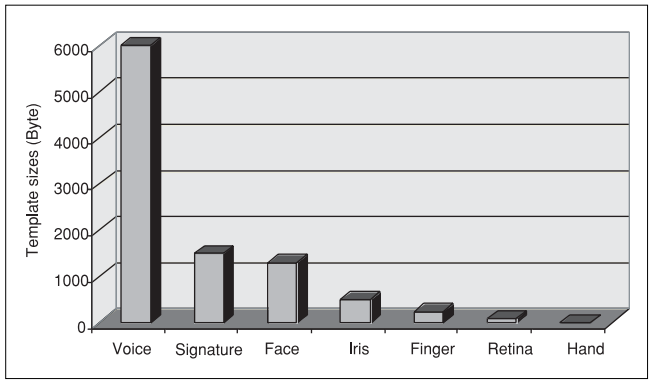


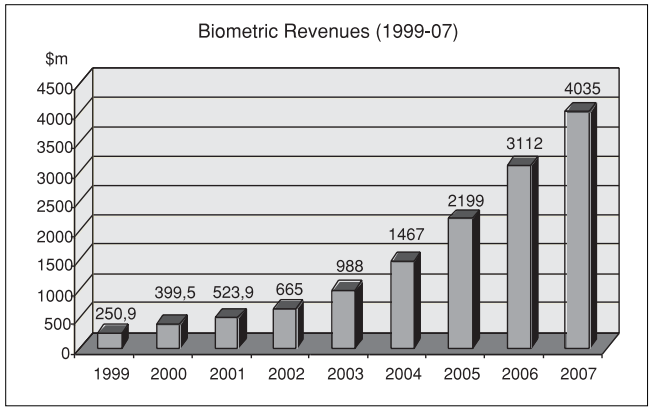
Fig. 3.

The presence of biometric systems in the civil sphere has been growing dynamically. This development is due to the great decrease in price and rapid advancements in technology. At the beginning the sophisticated (finger, iris and retina) solutions are expected to spread. This is followed by the spread of the easy-to-use techniques, because they are already part of our life. Such biometrics methods are voice and signature based identification systems.

Global 2004 industry revenues of 1467m USD are expected to reach 4.04b USD by 2007, driven by large-scale public sector biometric deployments, emergence of transactional revenue models, and the adoption of standardized biometric infrastructures and data formats.

The increase in biometric revenues is due to the rapid growth of PC/Network access and e-commerce. Although in the last decades biometric systems see-

Fig. 4.



med to be secure, the R&D corporations had to face new challenging difficulties. New techniques were developed for hacking biometric security systems. In conventional systems the security was assured by passwords or keys, which could be stolen. In case of biometrics, however, the key point is replicating the characteristics of a person, which obviously is a more difficult task.

Today the main problem is how to prevent the biometric security systems from being hacked. The fraud of a system is something completely different from the cracking of other security systems. (It is not known whether the system can be hacked as long as it is not deceived.) For example a vendor made an optical biometric identification system that identified only living finger. The system seemed secure until someone has breathed on the optical sensor. The system identified the breath together with the fingerprint still present on its sensor (the fingerprint of the previous person who gained access) as a living finger; and provided access. In another case a photocopy of a valid fingerprint was enough to fraud the system.

Until now the exact and fast identification was in the focus of the research, but as technology spreads, several new difficulties have to be taken into account. Until all the technological questions are answered biometric systems must be used very cautiously. For example in the case when one does not have count with the fake of security system because the identification is made under supervision (such situations can be when a security guard or camera is watching).

In the following years, biometric security systems are expected to spread further because identity verification has never been so important, as it has become recently. After September 11, 2001 fingerprint verification systems were set up in US airports. The EU also plans to install a global biometric verification system for identifying anyone entering the Union. Thanks to their decreasing price and increasing reliability, biometric systems have never been so popular, as in the last few years.

References

[1] International Biometric Group, http://www.biometricgroup.com
[2] Xiaguang J., "Extending the feature set for automatic face recognition", thesis for the degree of doctor of philosophy, 1993.
[3] Iridian Technologies, http://www.sensar.com
[4] R. K. Abbas, "A prototype system for off-line signature verification usig multilayered feedforward neural network", thesis, 1994.
[5] T. Wessels, C. W. Omlin, "Hybrid system for Signature Verifivation", 1999.
[6] H. S. M. Beigi, "An overview of handwriting recognition", 1994.
[7] CIC, http://www.cic.com
[8] ActiveCard, http://www.activcard.com/ /activ/products/other/biometrics/index.html
[9] A. Ross, "A prototype hand geometry-based verification system", Biometrics Research, http://biometrics.cse.msu.edu
[10] BioID, http://www.bioid.com

News

NEC Corporation and Japan Science & Technology Agency have jointly succeeded in realizing 150-km-long single-photon transmission. This transmission enables secure network communication supported by the principles of quantum mechanical physics. Due to wide-area coverage (up to 150 km), this system can realize quantum cryptography transmissions in optical networks in metropolitan areas, and is expected to contribute to the realization of an optical fiber network system requiring advanced safety levels. The main features of this system are as follows:

- Stable one-way photon transmission which reduces the noise of backscattered photons.
- Suppression of the deterioration in photon-detection sensitivity that occurs due to the widening of the photon-pulse width.
- Tenfold increase in signal-to-noise ratio as compared with current systems.

The **Plenipotentiary Conference** creeated a Group of Specialists to review the management of the Union (the „GoS"). In October 2003, the ITU Council decided to mandate an external consultant to develop a plan for the implementation of the recommendation made by the Group of Specialists following this review. Based on the recommendations of the GoS, Dalberg staff worked from ITU premises to produce their report for consideration by the Council. The workshops and meetings were variously aimed at bringing together elected officials, representatives of the membership, ITU managers and staff to develop common approaches to the implementation of new processes. The consultants´ report includes various proposals with regard to information systems and management processes. The common view was to work objectives for the future, enhanced communication and information flows. What more suitable goal for an organization so deeply involved in helping the world to communicate?