ISSN: 2456-9348
Vol (02) _Issue (03) Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

A STUDY ON KEY BIOMETRIC TECHNOLOGIES: CHARACTERISTICS AND APPLICATIONS

[#1]M. Praveen kumar, [#2]S. P. Santhoshkumar, [#3]S. Karthick, [#4]S. Syed shajahaan
Assistant Professor, Dept of IT, Rathinam Technical Campus, Coimbatore, India.
Assistant Professor, Dept of CSE, Rathinam Technical Campus, Coimbatore, India.
Assistant Professor, Dept of CSE, Rathinam Technical Campus, Coimbatore, India.

Abstract:
Over the last few years a new area of engineering science has been established whose products are likely to create a large market in the near future. It has been called "biometrics". The pioneers of this new domain intend to construct devices which would allow identification of a person on the basis of his/her "biological" characteristics: voice, dynamics of movements, features of face and other parts of the body, retina or iris pattern. Nature has made human beings with different characteristics which may vary from one person to another. Biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Several important issues must be considered in designing a practical biometric system. First, a user must be enrolled in the system so that his biometric template can be captured. This template is securely stored in a central database or a smart card issued to the user. The template is retrieved when an individual needs to be identified. Depending on the context, a biometric system can operate either in verification (authentication) or an identification mode. This paper gives an overview of key biometric technologies and basic technique involved. The various opportunities for biometrics are mentioned, followed by the uses, benefits, and applications.

INTRODUCTION

As modern society increasingly depends on systems to provide secure environments and services to people, it becomes paramount to ensure the security of a system through means to identify the validity of an individual requesting access to it. This is usually established by extracting some form of information from the individual to check against information held by the system about valid users.

This ITU-T Technology Watch Report spotlights biometric recognition as a key form of authentication, one which is increasingly used in a wide range of applications made possible by advanced pattern recognition algorithms applied through powerful information and communication technologies (ICT).

Biometric recognition can be described as automated methods to accurately recognize individuals based on distinguishing physiological and/or behavioral traits. It is a subset of the broader field of the science of human identification. Technologies used in biometrics include recognition of fingerprints, faces, vein patterns, irises, voices and keystroke patterns (See Figure 1). In the subfield of telebiometrics, these recognition methods are applied to telecommunications.

In a non-automated way and on a smaller scale, parts of the human body and aspects of human behavior have been used ever since the dawn of mankind as a means of interpersonal recognition and authentication. For example, face recognition has been used for a long time in (non-automated) security and access applications, e.g., as a method to verify that the owner of a passport and the person showing the passport are the same, by comparing the person's face and the passport photo.

The Digital Revolution added ICT as a means to fulfill recognition and authentication processes, often through PCs and computerized telecommunication devices, such as cash dispensers. Users authenticate themselves to the machine by entering a secret knowledge-based authenticator, such as a PIN or passphrase, or by the possession of a token, like a bank card or key, and sometimes authentication requires a combination of knowledge and possession.

The 1960s also saw the first automated biometric recognition applications. However, the biometric industry did not take off at that time, due to high cost, low recognition accuracy and the lack of standards and testing benchmarks with which the different approaches could be compared and quality ensured.

To further the use of biometric systems, issues of security and privacy will need to be carefully addressed, as well as the high levels of expectation in accuracy, reliability, performance, adaptability, and cost of biometric technologies for a wide variety of applications.

Safety, quality and technical compatibility of biometric technologies can be promoted through standards and standardization activities. Standards are essential for the deployment of biometric technologies on large-scale national and international applications.

This Report discusses the advantages of biometric authenticators over their knowledge- and possession-based counterparts, describes different physiology- and behavior-related human traits and how they are used in biometric systems. A choice of biometric recognition applications is highlighted, and an overview of standardization work in the field of biometrics is given.

iJETRM
International Journal of Engineering Technology Research & Management

POSSESS, KNOW, BE – AUTHENTICATION METHODS

Fundamentally, authentication mechanisms that exist today use one or more of the following authenticators (factors):

A. Knowledge-based – an authenticator only the individual knows, which usually refers to PIN, passphrase or an answer to a secret/security question.
B. Possession-based – an authenticator only the individual possesses, which usually refers to keys, smart cards and tokens.
C. Physiology-based or behavior-based – an authenticator only the individual is or can do, referring to biometrics.

Knowledge- and possession-based authentication mechanisms imply that users –in order to be granted access to a system, building, service– need to carry or remember the authenticator. When it comes to comparisons of these traditional authenticators and authentication through biometrics, it is often argued that keys could be lost, stolen or easily duplicated and passphrases could be forgotten. A critical drawback is that the link between the legitimate individual and the authenticator is weak, and the authentication system has no means to distinguish between a designated owner of the authenticator and a thief, impostor or guesser. On the other hand, the general view is that biometric traits have an advantage in that they cannot be stolen, easily guessed or forgotten.

FINGERPRINT, FACE, VOICE – BIOMETRIC TRAITS

Biometrics are commonly categorized as either physiological or behavioral trait. Physiological traits (sometimes called passive traits) refer to fixed or stable human characteristics, such as fingerprints, shape and geometry of face, hands, fingers or ears, the pattern of veins, irises, teeth, as well as samples of DNA. Physiological traits are generally existent on every individual and are distinctive and permanent, unless accidents, illnesses, genetic defects, or aging have altered or destroyed them. Behavioral traits (active traits) measure human characteristics represented by skills or functions performed by an individual. These include gait, voice, key-stroke and signature dynamics.

The following paragraphs describe traits of both categories, which are sometimes evaluated based on such characteristics as:

a. Universality – Each individual should have the biometric trait.
b. Distinctiveness – Any two individuals should be different regarding the trait.
c. Permanence – The biometric should be sufficiently invariant over a certain period of time.
d. Collectibility – The biometric should be quantitatively measurable.

It is argued by some that none of the human biometric traits meets all the above requirements. Although each biometric trait has its strengths and drawbacks; no biometric is “optimal”.

PHYSIOLOGICAL TRAITS

Fingerprint

Fingerprint biometrics is largely regarded as an accurate biometric recognition method. Today, fingerprint scanners are available at low cost and increasingly integrated in laptops and other portable ICT devices.

Most fingerprint recognition systems analyze the unique pattern of ridges and valleys, and the arrangement of small unique marks on the fingerprint, which are known as minutiae. They can be recognized and distinguished by their type, by x- and y-coordinates, and by their direction.

Fingerprint scanners can operate with touch-based or touchless optical systems. The former is to be found in laptops and works in a similar way to digital cameras by capturing a digital image of the fingertip using visible light. While this type of sensor provides a cheap and simple solution, it comes with some drawbacks: when a finger touches or rolls on the scanner surface, the elastic skin deforms. The quality of the captured image strongly depends on amount and direction of pressure applied by the user and the fingerprint may appear different in every capture. In addition, when used in large-scale applications such as an immigration desk, special hygienic care needs to be exercised to avoid dirt being carried from one finger to the other.

By emitting light on or through the finger and capturing the reflected or transmitted signals, fingerprints can be taken without contact between skin and scanner. To avoid fake-finger attacks, some systems employ so-called liveness detection technology, which takes advantage of the sweat activity of human bodies. High-magnification lenses and special illumination technologies capture the finger’s perspiration and pronounce the finger dead or alive.

Application planners need to take into account that fingerprints of a small part of the population cannot be utilized for biometric recognition. This can be due to age (thin skin or senile atrophy of friction skin), accidents, genetic reasons, environmental or occupational reasons (e.g., construction workers may have worn fingerprints or a large number of cuts and bruises on their fingerprints that keep changing).

Face

iJETRM
International Journal of Engineering Technology Research & Management

Humans distinguish and recognize faces based on location, size and shape of facial features, such as eyes, eyebrows, lips, nose, cheekbones, chin and jaw. The corresponding automated approaches to face recognition are summarized as geometry feature-based methods. Other approaches are based on image templates and compute the correlation between a locally captured face and one or more model templates to estimate similarity.

Most vendors of automated face recognition systems use proprietary algorithms to generate biometric templates. The algorithms are kept secret and cannot be reverse-engineered to create a recognizable facial image from the template. Consequently, face recognition templates are not interoperable between vendors and therefore the original captured photograph has to be kept, instead of a ready-to-use template. In the case of machine-readable passports, the original captured photograph is stored on the RFID (radio-frequency identification) chip. When passing a border or immigration desk, the receiving state uses its own vendor algorithm to compare the passport bearer's facial image captured in real time with the data read from the chip. To be recognized accurately at many borders, it is important that the template image on the chip makes visible a number of facial features and is taken under certain light and contrast conditions.

Face recognition is a non-intrusive method and can be performed with digital cameras or in combination with closed-circuit television (CCTV), incorporating remote video surveillance cameras. However, today's technology may recognize accurately from full front faces or from images taken in small angles, with simple background and special illumination, but not from different viewing angles, under poor light conditions, or if hair, sunglasses, or hats cover the person's face. These limitations became apparent in larger field tests at airports and train stations.

Iris patterns

The idea of recognizing an individual by using iris patterns was proposed by an ophthalmologist in 1936. Later, the idea appeared in some action movies, including 1983's James Bond "Never Say Never Again", but at that time it remained science fiction. In 1994, the first automated iris pattern recognition algorithms were developed by physicist and computer-vision expert John Daugman and patented, and continue to be the basis of all current iris recognition systems and products.

Before extracting and analyzing an iris pattern, the iris has to be located within an image. Landmark features, such as the outer iris boundaries and the pupil in the center of the eye help to mark the iris' borders. Once located, the iris is captured with the help of a high quality camera, which in many cases emits infrared light to illuminate the eye without causing harm to the eye or discomfort. A digital representation of the iris features (orientation, spatial frequency, position) is computed (the IrisCode), stored and –in the application– compared.

It is extremely difficult to surgically tamper the texture of the iris, and spoof attacks (e.g., with prepared contact lenses) are detectable rather easily. On the downside, iris recognition is difficult to perform from distances further than a meter and it requires active user participation.

DNA

At present, there exists no technology to allow for instant and automated recognition of DNA samples. DNA analysis and profiling (genetic fingerprinting) requires a lab environment and at least several hours. However, significant R&D efforts are underway to develop this technology, and also to enable governments to better use the millions of DNA profiles collected and archived in DNA databases.

BEHAVIORAL TRAITS

Voice print

Behavioral traits can be learned or acquired, but also include physiological elements. For instance, the human voice is influenced by the physiological characteristics of lungs, tongue, throat, etc. and its behavioral features evolve and change over time. They can be influenced by factors such as age, illnesses, mood, conversational partner or surrounding noise.

Individuals (speakers) can be recognized by their voice print, the set of measurable characteristics of a human voice. Speaker recognition and speech recognition –a similar technology that focuses on the content of the spoken input rather than on who is speaking– rely on resource-intensive algorithms, including frequency estimation, vector quantization and hidden Markov models. These are applied in text-dependent, text-prompted or text-independent speaker recognition systems, as explained below:

a. Text-dependent systems: The user is requested to speak a word or phrase, which was saved earlier during the enrollment process. The spoken input is represented by a sequence of feature vectors and compared with previously recorded input vectors, to calculate the degree of similarity.
b. Text-prompted systems: The user is prompted to repeat or read a word or phrase from a pre-recorded vocabulary displayed by the system (e.g., "Please say the numbers 8 2 2 1!").
c. Text-independent systems: These systems have no initial knowledge/vocabulary, but need to be trained by the user to recognize accurately. In the training phase, reference templates are generated for different phonetic sounds of the human voice, rather than samples for certain words. In operation mode, the system matches the

acquired phonetic templates and those from arbitrary input text. Text-independent systems are more difficult to design, but offer higher protection against impostors and fraud.

Speaker recognition systems are a useful choice for telephone-based applications. Individuals are used to speaking on the telephone and recognition systems can be easily integrated into telephone networks.

Signature dynamics

Biometric signature recognition systems measure and analyze the physical activity of signing. Important characteristics include stroke order, the pressure applied, the pen-up movements, the angle the pen is held, the time taken to sign, the velocity and acceleration of the signature. Some systems additionally compare the visual image of signatures, though the focus in signature biometrics lies on writer-specific information rather than visual handwritten content. While it may appear trivial to copy the appearance of a signature, it is difficult to mimic the process and behavior of signing.

However, a person's signature changes over time as well as under physical and emotional influences. Therefore, signature recognition works most effectively when used regularly, and when the biometric template is regularly updated to reflect gradual changes. Since a signature is one of the most accepted means of asserting identity, main uses of signature biometrics include limiting access to restricted documents and contracts, delivery acknowledgement and banking/finance related applications.

Signature data can be captured via pens that incorporate sensors or through touch-sensitive surfaces which sense the unique signature characteristics. Touch-sensitive surfaces are increasingly being used on ICT devices such as screens, pads, mobile phones, laptops and tablet PCs.

Keystroke dynamics

The recognition of keystroke dynamics is the process of analyzing the way an individual types at a terminal by monitoring the keyboard inputs thousands of times per second in an attempt to recognize the individual based on habitual typing rhythm patterns. Keystroke dynamics are described by speed (the time a key is pressed, the time between keys pressed), rhythm, precision, keys used (e.g., left Shift key or right Shift key, Caps Lock), and other typing characteristics.

Similar to other active traits, an individual's keystroke rhythm evolves over time, for instance by switching from two finger typing to touch typing. Subjects can become tired or distracted during the course of a work day, which in turn affects the typing rhythm. Recognition accuracy would be very limited if only a small number of variables were considered. The longer the text entered the more characteristics revealed and the more accurate recognition can be. The ultimate aim is to be able to continually check the identity of an individual typing on a keyboard.

The equipment requirements are minimal (keyboard) and give information about the huge field of possible applications. For instance, Psylock, a keystroke recognition system developed at University of Regensburg (Germany), uses a JavaScript function to capture the user's keystroke dynamics on the client side (using a web browser), transmits the data on an encrypted connection (SSL) to an authentication server, which replies to authentication requests. The university successfully used the system to authenticate users for service desk tasks (password reset); it was also proposed as an alternative to transaction authentication numbers (TAN) in home-banking applications.

CAPTURE, COMPARE, DECIDE – BIOMETRIC SYSTEMS

In addition to selecting a feasible biometric for an application, its interplay with a biometric system is a crucial factor for deployment decisions. The following desired quality factors may influence the choice of a specific biometric for an application:

- Performance – The measurement of the biometric trait is robust, accurate, fast and efficient.
- Acceptability – The extent to which individuals are willing to accept the use of a particular biometric trait in an application.
- Circumvention and Reliability – Extent to which the system can be manipulated by using fraudulent methods.
- Cost.

It is obvious that some of these factors are intangible and may depend on the perception of each user. For instance, the question of whether a biometric application is acceptable or not may be linked to the user's cultural background, attitude to privacy and to technology, etc. Accuracy and performance, however, can be quantified and compared. This section describes biometric systems, its components, operation modes and rates that measure its performance.

A biometric system is a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the data acquired, and comparing this sample against an earlier registered template. Depending on the type of application the template may be stored in the system's database or on a token, such as a smart card.

All biometric systems use common main functional components, which include: Storage entity with the biometric data samples (templates) of the enrolled individuals that is linked or integrated in a database with the identity information of the corresponding individuals.

iJETRM
International Journal of Engineering Technology Research & Management

a. Biometric sensor device and pre-processing capacities to capture the biometric sample data from an individual as input data.
b. Comparison process evaluating the similarity between reference template and captured data sample, and then calculating a matching score.
c. Decision function that decides if the data sample matches the reference template.

In addition, the communications channels between these components are of great importance. In telebiometrics, these can include wired or wireless telecommunication environments, and private or public networks, including the Internet.

The matching decision is a fundamental element of the biometric system. It is made on the basis of the matching score and a threshold value. The matching score is typically a single number on a scale from low to high, measuring the success that a biometric probe record (the individual being searched for) matches a particular gallery record (a previously enrolled individual). The threshold value is a benchmark score above which the match between the stored biometric and the individual is considered acceptable or below which it is considered unacceptable.

APPLICATIONS

Advances in ICT, increased performance and availability of equipment at lower cost have smoothed the way for automated biometric recognition.

Biometric applications may be categorized into three main groups:

a. Forensic applications, in criminal investigations, e.g., for corpse identification, parenthood determination, etc.
b. Government applications, including personal documents, such as passports, ID cards and driver's licenses; border and immigration control; social security and welfare-disbursement; voter registration and control during elections; e-Government.
c. Commercial applications, including physical access control; network logins; e-Commerce; ATMs; credit cards; device access to computers, mobile phones, PDAs; facial recognition software; e-Health.

This order generally reflects the emergence and use over time of biometric recognition systems. Initially found mainly in the field of criminology and forensics, biometrics underwent a market breakthrough when governments started to integrate biometric access control mechanisms in personal documents. While access control and authentication have remained the primary purpose, other fields of application are taking off.

Google's photo organizer software Picasa and social-networking site Facebook have integrated face recognition algorithms to make it easier to search and display all photos featuring a certain person. Picasa is available as an application for several operating systems, while its photo sharing web site (Picasa Web Albums) and Facebook provide face recognition online. Biometric systems embedded in cars of a vehicle fleet can help to identify the driver, adjust seat, rear mirrors, and steering wheel to meet individual preferences. A number of other applications are presented in Box 1.

Commercial and government applications are likely to overlap in some fields. Future e-commerce, e-health and e-government services may require authentication with the help of biometric personal documents issued by governments, as soon as they are used by a large enough part of the population. Some developing countries have used biometrics for voter registration in the run-up to elections in order to avoid out-dated voter lists and election fraud.

Market forecasts on biometric spending are generally optimistic. Growth is expected especially in commercial and government applications, where the biometrics industry and the related smart card chip industry benefit from government decisions toward the adoption of electronic personal documents and biometrics. From an estimated US$ 3 billion spent on biometric technologies in 2008, market researchers forecast investment of US$ 7.3 billion by 2013.

Alongside fingerprints, which will remain the dominant biometric traits, face, iris, hand and speech recognition systems are expected to emerge and be widely adopted in biometric applications.

SECURITY AND PRIVACY

Biometrics can play an important role in authentication applications, since they are strongly linked to the holder, and difficult to forget, lose or give away. It is important that biometric systems be designed to withstand attacks when employed in security-critical applications, especially in unattended remote applications such as e-commerce.

In an often-cited paper published in the IBM Systems Journal in 2001 the authors identify eight vulnerable points in biometric systems (illustrated and described in Box 2), which are also critical for local and remote (tele-) biometric applications.

The strong link between biometrics and the holder also guarantees that the characteristics cannot be influenced or altered by its holder, without harm. It appears to be difficult to deny or hide one's biometrics. Privacy concerns exist wherever uniquely identifiable data relating to an individual are collected, stored or processed. Some argue that the ubiquitous use of biometrics in large-scale commercial applications, the ease to create biometric templates and the accumulation of biometric profiles in huge databases could devalue classic forensic applications.

iJETRM
International Journal of Engineering Technology Research & Management

A number of provisions and techniques have been proposed to safeguard security and privacy in biometrics.

Multimodal biometric systems

It is now recognized that biometric recognition can be better performed when multiple measurements are involved–an approach described as multimodal, multibiometric or biometric fusion. The five different operational scenarios of the multimodal approach are described in Box 3. This approach addresses the issue of non-inclusiveness due to non-universality of certain biometric traits, since sufficient population coverage can be ensured using multiple traits.

A. Template-on-token

Storing biometric authenticator and identity data of an individual on a token, such as a smart card, represents a two factor authentication with the following security-/ privacy-enhancing features:

a. Avoidance of knowledge-based authenticators;
b. Avoidance of a centralized database storing biometrics or other personal information;
c. Two authenticators, biometric and token, are required for successful authentication;
d. Prevention of unauthorized read-out or manipulation of the content stored on the token through access control mechanisms possible.

In this approach, the user retains control over its biometrics, and would be able to hand them out only to trustworthy services and devices. However, once a communication partner is deemed trustworthy, the personal information leaves the token and the controlled area of the user.

Match-on-token

This approach extends template-on-token to the extent that only the final matching decision leaves the token, or activates it. In addition to the biometric template being stored, the token integrates a biometric sensor and a comparator with sufficient processing power.

Data-hiding techniques

In telebiometric applications, digital representations of biometrics are transmitted in a compressed format over the communication network. For instance, the Wavelet Scalar Quantization (WSQ) image compression scheme proposed by the American FBI is the de facto standard used for compressing fingerprint images, because its low image distortion characteristics even at a high compression ratio have advantages over other formats including JPEG. However, being an open format, WSQ-compressed fingerprint bitstreams can be intercepted and decrypted, saved and fraudulently used, for instance in replay attacks.

Data-hiding techniques embed additional information in fingerprint images–an approach similar to hiding digital watermarks in image or audio data to ensure data integrity. If the embedding algorithm remains secret, a service provider (e.g., e-commerce) can investigate the received fingerprint image for the expected standard watermark to ensure it has been sent from a trusted sensor. One-time templates are generated by embedding a different verification string provided by the service provider into the fingerprint image, and are only valid for one transaction.

Cancelable biometrics

One advantage of knowledge- and possession-based authenticators over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version, an option not readily available for biometrics. Cancelable biometrics perform an intentional and repeatable distortion of the original biometric signal by applying a chosen noninvertible transform, which is applied in the same way during the enrollment and authentication process. Every biometric application may use a different transform to render cross-matching of biometrics impossible. If one variant of transformed biometric is compromised, this representation can be "canceled" and replaced by a biometric generated with a new transform. The original biometric remains secret and cannot be reconstructed from compromised representations.

CONCLUSION

Within a fairly short period of time, biometric recognition technology has found its way into many areas of everyday life. Citizens of more than 50 countries hold machine-readable passports that store biometric data–a facial image and in most cases a digital representation of fingerprints–on a tiny RFID chip, to verify identity at the border. Law enforcement agencies have assembled biometric databases with fingerprints, voice and DNA samples, which make their work more efficient and manageable. Commercial applications use biometrics in local access control scenarios, but also increasingly in remote telebiometric deployments, such as e-commerce and online banking, and complement or replace traditional authentication schemes like PIN and passwords.

Biometrics-based authentication clearly has advantages over these mechanisms, but there are also vulnerabilities that need to be addressed. No biometric trait can be applied universally, it may be a good choice for a given application, but unfeasible in another.

iJETRM
International Journal of Engineering Technology Research & Management

Significant progress has been made recently in the capabilities of biometric sensors, algorithms and procedures. Due to the availability of ever-increasing processing power at low cost, the accuracy of biometric systems has improved to a degree which in some scenarios may exceed the recognition accuracy of humans. In addition, sensors have decreased in size, allowing biometric applications to increasingly appear on mobile devices, which could outsource the processing-intensive parts of biometric recognition to the cloud. Scientific and technical challenges remain in achieving accuracy in recognition under uncontrolled illumination and environment conditions and in the recognition of moving objects.
Since biometrics rely on highly sensitive personal information, the handling of biometric information needs to be given special attention and protective measures need to be put in place to safeguard privacy and avoid compromise of biometric data.
Some approaches to improve security and ensure privacy when deploying biometric recognition have been described in this Report and are increasingly reflected in international biometric standards. Insecure biometric systems may not only have negative consequences for a specific application or its users, but may also result in loss of public trust and lack of acceptance of biometric recognition technologies as a whole. The accelerated development of biometric standards in recent years has facilitated the enhancement and increasing use of biometric applications. As more international standards become available, it is likely that these systems will be used in an ever-widening range of applications.

REFERENCES

[1] A.K. Jain, A. Ross, S. Prabhakar: An Introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1):4-20, 2004.
[2] G. Parziale: Touchless fingerprinting technology. Advances in biometrics, 25-48, 2008.
[3] Y. Adini, Y. Moses, S. Ullman: Face recognition: the problem of compensating for changes in illumination direction. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7):721-732, 1997.
[4]S. Murphy, H. Bray: Face recognition devices failed in test at Logan. The Boston Globe, September 2003. http://www.boston.com/news/local/articles/2003/09/03/face_recognition_devices_failed_in_test_at_logan/
[5] National Science and Technology Council: Introduction to biometrics. 2007. http://www.biometrics.gov/documents/biofoundationdocs.pdf
[6] A.K. Jain, A. Ross, S. Prabhakar: Biometrics: a tool for information security. IEEE Transactions on Information Forensics and Security, 1(2):125-143, 2006.
[7] J.P. Campbell: Speaker recognition: a tutorial. Proceedings of the IEEE, 85(9):1437-1462, 1997. See Jain et al.: Biometrics: a tool for information security.
[8] J. Ortega-Garcia, J. Bigun, D. Reynolds, J. Gonzalez-Rodriguez: Authentication gets personal with bio-metrics. IEEE Signal Processing Magazine, 21(2):50-62, 2004.
[9] M. Gifford, N. Edwards: Trial of dynamic signature verification for a real-world identification solution. BT Technology Journal, 23(2):259-266, 2005.
[10] F. Monrose, A.D. Rubin: Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems, 16(4):351-359, 2000.
[11] D. Bartmann: On the design of an authentication system based on keystroke dynamics using a predefined input text. International Journal of Information Security and Privacy, August 2006.ISO/IEC: Information technology – Biometrics tutorial. ISO/IEC TR 24741:2007(E). 2007. See Jain et al.: An Introduction to biometric recognition.
[12] J. Daugman: How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technol-ogy, 14(1):21-30, 2004.
[13] P.J. Phillips et al.: Face Recognition Vendor Tests 2006 and Iris Challenge Evaluation 2006: Large-scale results. 2007. http://frvt.org/FRVT2006/docs/FRVT2006andICE2006LargeScaleReport.pdf. Biometrics faces rosy future says pundits. Biometric Technology Today, 16(9):4-5, 2008.
[14] A. Pfitzmann: Biometrie: wie einsetzen und wie keinesfalls. Informatik-Spektrum, 29(5):353-356, 2006. (German).See Jain et al.: An Introduction to biometric recognition.
[15] N.K. Ratha, J.H. Connell, R.M. Bolle: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3):614-634, 2001.
[16] N.K. Ratha, J.H. Connell, R.M. Bolle, S. Chikkerur: Cancelable biometrics: a case study in fingerprints. ICPR '06: Proceedings of the 18th International Conference on Pattern Recognition, 370-373, 2006.
[17] R. Ryan: The importance of biometric standards. Biometric Technology Today, 17(7):7-10, 2009.
[18] F. Deravi: Biometrics standards. Advances in biometrics, 473-489, 2008.
[19] C. Tilton: Biometric standards – an overview. 2009. White paper available at http://www.daon.com/. See R. Ryan: The importance of biometric standards.