한국지능정보시스템학회논문지 제11권 제1호 2005년 6월(pp.1~15)

Biometrics for Person Authentication: A Survey

Ankur Agarwal
Dept. of Computer Science & Engineering,
Florida Atlantic University, USA
(ankur@cse.fau.edu)

A. S. Pandya
Dept. of Computer Science & Engineering,
Florida Atlantic University, USA
(abhi@cse.fau.edu)

Young-Uhg Lho
Dept. of Computer Education, Silla University, Korea
(yulho@silla.ac.kr)

Kwang-Baek Kim
Dept. of Computer Engineering, Silla University, Korea
(gbkim@silla.ac.kr)

As organizations search for more secure authentication methods for user access, e-commerce, and other security applications, biometrics is gaining increasing attention. Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology. In others, it is the only viable approach. Several biometric methods of identification, including fingerprint, hand geometry, facial, ear, iris, eye, signature and handwriting have been explored and compared in this paper. They all are well suited for the specific application to their domain. This paper briefly identifies and categorizes them in particular domain well suited for their application. Some methods are less intrusive than others.

Key words : Biometrics, Personal Authentication, Fingerprints, Iris, Signature

Received: July 2004 Accepted: March 2005 Corresponding Author: Kwang-Baek Kim

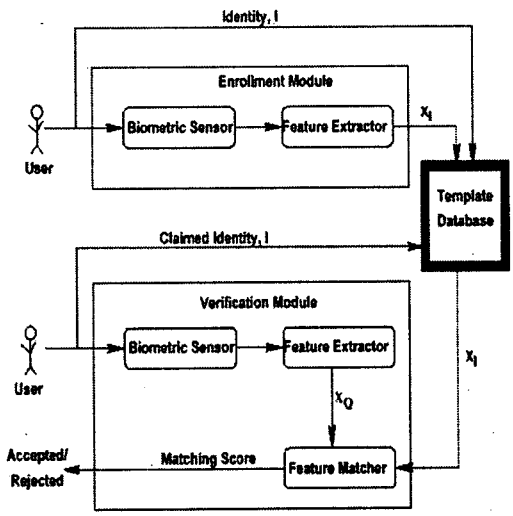
1. INTRODUCTION

Biometrics are the integral and distinctive parts of human beings. As such, they offer a natural convenience and technical efficiency that other authentication mechanisms, which must be mentally remembered or physically produced, do not. For this reason, biometrics can provide identity assurance for countless everyday activities currently protected by traditional means of access control [1,2]. Following the September 11, 2001 terrorist attacks, the U.S. government and other governments and organizations throughout the world became greatly interested in this emerging human recognition technology. For example, on January 7, 2002, the Office of Homeland Security announced its "Specifics of Secure and Smart Border Action Plan," which lists "biometric identifiers" as its first priority. The three basic factors influencing the adoption of biometrics are:

Security, Convenience, cost.

Reliable identification makes life go more smoothly and makes financial and business dealings safer and more efficient, if only by making the participants more accountable for their actions. When we automate the authentication process, we broaden the range of valuable tasks that computers and other devices can perform for us. These automated authentication processes can bring greater security, efficiency, and convenience to our lives. Automated authentication makes it possible to tailor the way that a device responds to different people and to ensure that it confidently responds to people in a correct manner.

In practice, this involves two separate actions: an authentication mechanism verifies the identity, and a separate authorization mechanism ties the appropriate actions to a person's identity. Common biometric verification techniques try to match measurements from an individual's fingerprint [3], hand geometry, eye [4,5], face [6,7,8], signature verification [9,10] or voice [11] to measurements could have been previously collected from them. There are two general applications for this: identification and verification shown in Fig. 1. The biometric authentication process begins with a biometric sensor of some kind. With identification, the biometric system asks and attempts to answer the question, "Who is X?"In an identification application, the biometric device reads a sample, processes it, and compares it against every record or template in the database. This type of comparison is called a "one-to-many" search (1: N). In case of verification, when an individual tries to log in, the sensor collects a biometric reading from them and generates a biometric template from the reading, which becomes the authenticator. The verification procedure essentially measures how closely the authenticator matches the verifier. If the system



[Fig. 1] Biometric verification Process

decides that the match is "close enough," the system authenticates the respective individual; otherwise authentication is denied. The measured properties of the individual's biometric trait serve the role of the base secret in a biometric system [12,13].

However, it's important to recognize that their biometric traits aren't really secrets. An individual often leaves measurable traces of these "secrets" wherever they go, such as fingerprints on surfaces, the recorded sound of their voice, or even video records of their face and body. This "latency"provides a way for attackers to generate a bogus authenticator and use it to trick the system into thinking that the individual is actually present. Moreover, it may be possible to intercept a genuine authenticator collected from the individual and replay it later. Thus, accurate authentication depends in part on whether the system can ensure that biometric authenticators are actually presented by live people. Replication attacks on biometrics try to mimic the personal traits or behaviors that the biometric sensor tries to read. As humans, we all use our natural abilities to recognize people through their voices, faces, and other characteristics. Machines, on the other hand, must be problematically instructed how to use the same observable information to perform human recognition. Technological advances, particularly in biometrics, are helping to close the gap between human perception and machine recognition.

The government's interest in biometric technologies is motivated by the desire to improve the delivery of services to citizens by increasing efficiency and convenience while decreasing costs and fraud [14]. Secure digital identification schemes are becoming increasingly important, as more security applications require identification based on physical characteristics rather than solely on a user's knowledge of a secret cryptographic key or password.

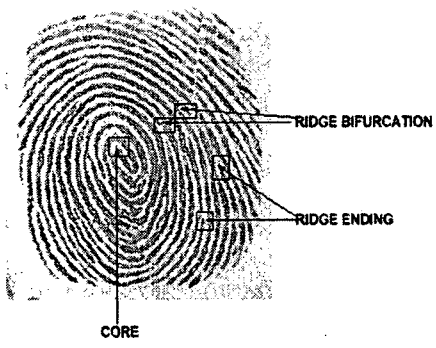
2. BIOMETRIC METHODS

In this section, we shall explore all systems of identification that use measurable biological features. It is desirable that such measurements be non-invasive and simple to perform. The various biometric systems include fingerprints; hand or palm geometry; and retina, iris, or facial characteristics [4-12]. Behavioral characters include signature, voice (which also has a physical component), keystroke pattern, and gait. Of this class of biometrics, technologies for signature and voice are the most developed.

2.1 Fingerprints

Fingerprints are the oldest and most widely recognized biometric markers [Daugman, 1993] due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices. The advent of several novel techniques to acquire fingerprints without the use of ink has taken fingerprint recognition to several civilian applications such as access control; time and attendance; and computer user login. These scanners are known as the "livescan" fingerprint

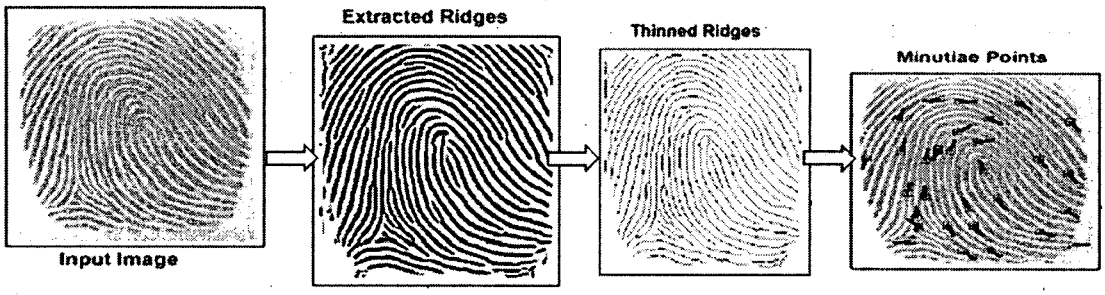
scanners. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows (or valleys)as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending (see Fig. 2). In police and civil applications, the primary interest is in the ridges on the front of the fingers above the end joint. In certain forensic applications, the area of interest is broader and includes all of the friction ridge surfaces on the hands. Within a typical fingerprint image obtained by a live scan device, there is an average of 30-40 minutiae. The Federal Bureau of Investigation (FBI) has shown that no two individuals can have more than 8 common minutiae. The U.S. Court system has consistently allowed testimony based on 12 matching minutiae; in some courts, a lower number of matching minutiae have been allowed.



[Fig. 2] Fingerprint image with the core and four minutiae points marked on it

Fingerprint matching techniques can be placed into two categories: Minutiae-based and correlation based. Minutiae-based techniques attempt to align two sets of minutiae points and determine the total number of matched minutiae. Correlation-based techniques, on the other hand, compare the global pattern of ridges and furrows to see if the ridges in the two fingerprints align. Virtually every published method of feature extraction computes the orientation field of the fingerprint image, which reflects the local ridge direction at every pixel. (See Fig. 3).

An authenticate function has to compensate for (i) translation, (ii) rotation, (iii) missing features, (iii) additional features, (iv) spurious features and, more importantly, (v) elastic distortion between a pair of feature sets. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties in extracting the minutiae points accurately when the fingerprint is of low quality and this method does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings, which requires the precise location of a registration point and is affected by image translation and rotation. Fingerprint matching based on minutiae has problems in matching different sized (unregistered) minutiae patterns. Local ridge structures can not be completely characterized by minutiae.



[Fig. 3] steps for a biometric fingerprint recognition system.

2.1.1 Finger-print Classification

An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database (FBI database contains approximately 70 million fingerprints!). Often storage and transmission of fingerprint images involves compression and decompression of the image. Standard compression techniques often remove the high frequency areas around the minutia features.

2.2 Face

Facial recognition is the most natural means of biometric identification; this method of distinguishing one individual from another is an inherent ability of virtually every human. Since the advent of photography it has been institutionalized as a guarantor of identity in passports and identity cards. In the 1990s, automatic-face-recognition technology moved from the laboratory to the commercial world largely because of the rapid development of the technology, and now many applications use face recognition. These applications include everything from controlling access to secure areas to verifying the identity on a passport. In general, face recognition systems proceed by detecting the face in the scene, thus estimating and normalizing for translation, scale and in-plane rotation. Approaches then divide into appearance-based and geometric approaches, analyzing the appearance of the face and the distances between features respectively. Appearance based methods can be global, where the whole face is considered as a single entity, or local, where many representations of separate areas of the face are created. Many systems use a process to detect a person's head and locate the face automatically. Facial recognition technology has recently developed into two areas of study; facial metrics and eigenvalues. Facial metrics technology relies on the measurement of specific facial features (e.g., the distance between the inside corners of the eyes, etc.) and the relationship between these measurements. Local feature analysis refers to a class of algorithms that extract a set of geometrical metrics and distances from facial images and uses those features as a basis for

representation and comparison. Local feature analysis (LFA) locates facial features and extracts them to represent there size, position and general outline shape. Faces can then be compared on the basis of their similarity to their ingredient features. Faces using LFA are represented as less abstract vector based features. Another group of researchers is involved in an investigation that tries to categorize faces according to the degree of fit with a set of "eigenvalues". Eigenvalues, is a vast spectrum containing algorithms that represent and compare faces on the basis of a palette of abstraction images. The images are collected and the faces are then expressed as a as a weighted sum of these archetypal faces. The desired similarity or likeness between faces can then be expressed as a numerical distance on the basis of these weights.

Another innovative technology is facial thermography, or imaging the face with infrared sensors. It extends to 2D face recognition based on normal, visible light imaging techniques. It is based upon the underlying vascular structure and heat properties of the human face, and it is relatively reliable as these properties cannot be disguised.

The face recognition systems should successfully address the following three categories of changes. (1) Physical changes: expression change; aging; personal appearance (make-up, glasses, facial hair, hair style, disguise). (2) Acquisition geometry changes: change in scale, location and in-plane rotation of the face (facing the camera) as well as rotation in depth (facing the camera obliquely). (3) Imaging changes: lighting variation; camera variations; channel characteristics (especially in broadcast, or compressed images). No current system can claim to handle all of these problems well. The most recent major evaluations of this technology took place between September 1996 and March 1997 using the Ferret tests [8]. These groups were tested on a sequestered set of images, which required the participants' systems to process 3,816 images. The Ferret evaluation measured performance for both identification and verification, and provided performance statistics for different image categories. Each of the following three categories became progressively more difficult, with the final category consisting of images taken at least a year and a half apart. The first category consisted of images taken on the same day under the same incandescent lighting. This category represented a scenario with the potential for achieving the best possible performance with face recognition algorithms. The majority of face recognition algorithms appear to be sensitive to variations in illumination, such as those caused by the change in sunlight intensities throughout the day. The second category involved the facial position. Changing facial position can also have an effect on performance. A 15-degree difference in position between the query image and the database image will adversely affect performance. At a difference of 45 degrees, recognition becomes ineffective.

2.3 Hand geometry

Hand geometry is based on the fact that

virtually every person's hand is shaped differently than another person's hand and that the shape of a person's hand (after a certain age) does not significantly change its shape. Hand geometry based authentication is limited in scalability but it is an extremely user-friendly biometric. Various methods are used to measure the hand; these methods generally fall into one of two categories - mechanical or image-edge detection. Either method produces estimates of certain key measurements of the hand (length of fingers and thumb, widths, etc.); this data are used to "categorize" a person. As the computation is also fairly easy, a standalone system is easy to build. As this biometrics is not seen to compromise user privacy, it is quite widely accepted. However, hand geometry based authentication systems are less accurate than fingerprint-based authentication techniques.

2.4 Eyes

Eyes are made up of two distinct components: the iris and the retina. Depending upon the type of identification purpose needed either of the two are used for identification purposes. A retina-based biometric involves analyzing the layer of blood vessels situated at the back of the eye. An established technology, this technique involves using a low intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. Retinal Scan technology is based on the blood vessel pattern in the retina of the eye. An infrared light source is used to illuminate the retina of the eye; the infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue. The image of the enhanced blood vessel pattern of the retina is analyzed for characteristic points within the pattern. A typical system which is involved in this type of recognition uses the filtered infrared spectrum off the beam of flashlight bulb and uses it to do a circular scan of the retinal pattern on the back of the eyeball.

An iris-based biometric, on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil. The colored part of the eye bounded by the pupil and sclera is the iris which is extremely rich in texture. Like fingerprints, this biometric results from the developmental process and is not dictated by genetics. So far in the literature, there has been only a couple of iris recognition systems described. The primary reason being the difficulties in designing a reliable image acquisition stage. In the Daugman system for iris recognition, the texture of the iris is represented using Gabor wavelet responses and the matcher is an extremely simple and fast Hamming distance measure. Iris scanning, undoubtedly the less intrusive of the eye-related biometrics, uses a fairly conventional camera element and requires no close contact between the user and the reader. In addition, it has the potential for higher than average template matching performance. Controlled lighting is essential to high performance.

2.5 Signature

Signature has a long pedigree before the advent of computers, with considerable legal recognition and wide current usage in document authentication and transaction authorization in the form of checks and credit card receipts. Signature verification analyzes the way a user signs his/her name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape but they may or may not be available, depending on the sensing modality. Signature verification enjoys a synergy with existing processes that other biometrics do not. The literature on signature verification is quite extensive [9,10] and is divided into two main areas of research: offline and online systems. Offline systems deal with a static image of the signature; online systems capture the position of the pen tip as a function of time. Online signature recognition can be based on the dynamics of making the signature, i.e., acceleration rates, directions, pressure, stroke length, etc., rather than a direct comparison of the signature after it has been written. On-line or 'dynamic' signatures are written with an electronically instrumented device and the dynamic information (pen tip location through time) is usually available at high resolution, even when the pen is not in contact with the paper. Some on-line signature capture systems can also measure pen angle and contact pressure, providing a much richer signal than is available in the on-line case, and making the identification problem correspondingly easier. These additional data make on-line signatures very robust to forgery. Signature verification devices are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted identifier.

2.6 Visual Speech

Despite the inherent technological challenges, voice recognition technology's most popular applications will likely provide access to secure data over telephone lines. Voice recognition has already been used to replace number entry on certain Sprint systems. The speech recognition technology can be interpreted as what the speaker says and speaker recognition technology verifies the speaker's identity. Speaker recognition systems fall into two basic types: text-dependent and text-independent [11]. In text-dependent recognition, the speaker says a predetermined phrase. This technique inherently enhances recognition performance, but requires a cooperative user. In text independent recognition, the speaker need not say a predetermined phrase and need not cooperate or even be aware of the recognition system. Speaker recognition suffers from several limitations. Different people can have similar voices, and anybody's voice can vary over time because of changes in health, emotional state, and age. Furthermore, variation in handsets or in the quality of a telephone connection can greatly complicate recognition. Current NIST speaker-recognition evaluations measure verification performance for conversational speech over telephone lines.6 in a recent NIST evaluation, the data we used consisted of speech segments for

several hundred speakers [15]. To measure performance under different conditions, it is important to recorded several samples on many lines. This is due the fact that differences among telephone handsets can severely affect performance. Handset microphones come in two types, either carbon-button or electret. It seems that the performance is better when the training and testing handsets are of the same type.

3. SELECTING A BIOMETRIC TECHNOLOGY

Biometric technology is one area that no segment of the IT industry can afford to ignore. Biometrics provides security benefits across the spectrum, from IT vendors to end users, and from security system developers to security system users. All these industry sectors must evaluate the costs and benefits of implementing such security measures. Different technologies may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters. There are different methods to rate the accuracy offered by the biometric system like False Rejection Ratio (FRR), false Acceptance rate (FAR). Both methods focus on the system's ability to allow limited entry to authorized users. However, these measures can vary significantly, depending on how you adjust the sensitivity of the mechanism that matches the biometric.

For example, you can require a tighter match between the measurements of hand geometry and the user's template (increase the sensitivity). This will probably decrease the false-acceptance rate, but at the same time can increase the false-rejection rate. Since FAR and FRR are interdependent, it is more meaningful to plot them against each other. Each point on the plot represents a hypothetical system's performance at various sensitivity settings. With such a plot, you can compare these rates to determine the crossover error rate. The lower the CER, the more accurate is the system. Generally, physical biometrics is more accurate than behavioral biometrics.

For wide acceptance of biometrics, standards for interfaces and performance evaluation are necessary. Several standards are in the process of being developed and promoted. BioAPI [16] is a standard for the application programmer interface allowing the decoupling of biometrics-technologies from the applications that use them. The US Dept. of Defense runs the FERET face recognition test. NIST in USA has been playing an important role in designing several fingerprint databases and conducting speaker verification tests. However, each institution planning to employ a person authentication system must perform its own evaluation based on its needs. We shall discuss the important issues below and then provide a comparison in Table 1.

Ease of use: This aspect is associated with the user-friendly environment offered by the device.

Error incidence: Biometrics may be affected

by the changes in environment and the individual's age. These are the primary cause for the concern of Biometric applications. Two primary causes of errors affect biometric data: time and environmental conditions. Biometrics may change as an individual ages. Environmental conditions may either alter the biometric directly (for example, if a finger is cut and scarred) or interfere with the data collection (for instance, background noise when using a voice biometric).

Cost: Cost includes various aspects from hardware used to capture biometrics, its processing unit, testing and verification of result, to the installation, mounting of biometric equipment and its maintenance.

User acceptance: Generally speaking, the less intrusive the biometric, the more readily it is accepted. However, certain user groups some religious and civil-liberties groups have rejected biometric technologies because of privacy concerns.

Long-term stability: Organizations should consider a biometrics' stability, including maturity of the technology, degree of standardization, level of vendor and government support, market share, and other support factors. Mature and standardized technologies usually have stronger stability. Table 1 below provides a comparison of various biometric technologies. Retinal Scan has high accuracy but also has high data collection error rate and low user acceptability. Iris Scan is unobtrusive and, as such, is generally accepted by clients. The Iris Scan image capture may be impaired by dark glasses, eye disease, and the

<Table 1> Table showing the Comparison of Different Characteristics of Biometrics

Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of use	High	High	Low	Medium	Medium	High	High
User Acceptance	Medium	Medium	Low	Medium	High	Very High	High
Collectability	Medium	High	Low	Medium	High	High	Medium
Accuracy	High	High	Very High	Very High	High	High	High
Sensor Cost	$100	$200	$5,000	$3,000	$25	$300	$10
Data Size (template)	200 bytes	10 bytes	256 bytes	256 bytes	2 K bytes	100 bytes	2 K bytes
Barriers to universality	Dryness, dirt worn ridges, finger impairment age	Hand injury age	Visual impairment	Lighting visual impairment	Lighting glasses, age hair	Changing signatures, age	Colds, noise, weather, speech impairment
Distinctiveness	High	Medium	High	High	Low	Medium	Low
Potential for Circumvention	Low	Medium	Low	Low	High	High	High
Maturity	Very High	Medium	High	High	Medium	Medium	Medium

percentage of the iris area that is exposed with the eyelid open in a "natural," static environment. There is some question as to whether a low light condition (that increases the size of the pupil thus decreasing the total area of the iris) may affect the proper imaging of the iris. An iris scan produces a high data volume, which equates to a high discrimination rate (identification rate). Iris scan technology may be more acceptable to user than retinal scans and, as opposed to retinal scan, it does not use an infrared light source to highlight the biometric pattern in the iris. Facial Recognition is still in the research stage does not seem to be a dependable technique to establish identity because the error rates for this biometric appear to increase with time, angle of the image captured, lighting, and facial expression. Hand geometry, as compared to some other means of biometric identification (notably fingerprints), does not produce a large data set. Therefore, given a large number of records, hand geometry may not be able to distinguish one individual from another who has similar hand characteristics. The problems with signature recognition lie in the means of obtaining the measurements used in the recognition process and the repeatability of the signature.

The instrumentation cannot consistently measure the dynamics of the signature. Also, a person does not make a signature in a fixed manner; therefore, the data obtained from any one signature from an individual has to allow for a range of possibilities. Signature recognition has the same problem with match discrimination (i.e., finding a match in a large database) as does hand geometry.

The Fingerprint biometric has a low data collection error rate and high user acceptability. Fingerprint images contain a large amount of data. Because of the high level of data present in the image, it is possible to eliminate false matches and quickly reduce the number of possible matches to a small number, even with large database sizes. Because of the fact that Fingerprint Imaging Systems use more than one finger image in the match process, the match discrimination process is geometrically increased. Today in the criminal justice Automated Fingerprint identification System application, the fingerprint identification process has a 98%+ identification rate and the false positive identification rate is less than 1%.

A retinal scan can produce almost the same volume of data as a fingerprint image analysis. Based on the fact that a high data volume equates to a high discrimination rate (identification rate),it would seem that retinal scan may be an alternative to fingerprint identification. However, Retinal scan technology has several drawbacks that are not common to fingerprint imaging technology; 1) the retinal scan is more susceptible to disease (notably cataracts, etc.) that change the characteristics of the eye; 2) the method of obtaining a retinal scan is personally invasive - a laser light (or other coherent light source) must be directed through the cornea of the eye. Finally, the Fingerprint biometric has the highest acceptance in the identification community and virtually every large biometric system in operation today uses the fingerprint biometric. Notwithstanding its

association with "criminal" applications, the fingerprint biometric is generally accepted by clients.

4. CONCLUSION

With the increased concerns in security and other privacy issues, any biometric which proves better in usage towards security applications for the computer visions and the machines gets highly enhanced and widely accepted. At present there is an opportunity for dual or multiple biometrics to be used at the same time. The applications are varied and diverse from security control against terrorists at airports to the privacy issues for a bank or criminal records. Reliable personal recognition is critical to many business processes. Since conventional knowledge-and token-based methods rely on surrogate representations of a person's identity to establish personal recognition, any system assuring reliable positive personal recognition must necessarily involve a biometric component. In fact, a sound personal recognition system design must incorporate many biometric and non-biometric components. Although the evolution of biometric technology will surely overcome some limitations, it is important to understand that foolproof personal recognition systems simply do not exist and perhaps never will. Security is a risk-management strategy that identifies controls, eliminates, or minimizes uncertain events that can adversely affect system resources and information assets. A system's security requirements depend on the application's requirements (the threat model) and the cost-benefit analysis. In our opinion, properly implemented biometric systems are effective deterrents to perpetrators.

Finally, the use of biometrics indeed raises several privacy concerns. A sound trade-off between security and privacy might be necessary; but we can only enforce collective accountability and acceptability standards through common legislation. On the positive side of the privacy issue, biometrics provides tools to enforce accountable logs of system transactions and to protect individuals' right to privacy. As biometric technology matures interaction will increase among applications, the market, and the technology. The technology's value, user acceptance, and the service provider's credibility will influence this interaction. It is too early to predict where and how biometric technology will evolve and which applications will ultimately embed it. However, it is certain that biometric-based recognition will profoundly influence the way we conduct our daily business.

REFERENCES

[1] U. Feige, A. Fiat and A. Shamir, "Zero Knowledge Proofs of Identity", Journal of Cryptology, Vol.2, pp.77-94, 1998.

[2] D. Chaum, "Security without identification: Transition systems to make big brother Obsolete," Communications of the ACM, Vol.28, pp.1035-1044, 1985.

[3] A. K. Jain, L. Hong, S. Pankanti and E. Bolle, "An Identity Authentication System Using Fingerprints", Proceedings of IEEE, Vol.85, No.9, pp.1365-1388, 1997.

[4] J. G. Daugman, "High Confidence Visual Recognition of Person by a Test of a Statistical Independence", IEEE Transactions of Pattern Analysis and Machine Intelligence, Vol.15, No.11, pp.1148-1161, 1993.

[5] R. Hill, A. Jain, R. Bolle and S. Pankanti, Retina Identification, Biometric Person Identification in Networked Society, Kluwer Academic, 1999.

[6] H. Wechsler et al, "Face recognition Theory to Application", Springer-Verlag, Berlin, 1998.

[7] R. Chellappa, C. Wilson and S. Sirohey, "Human and Machine Recognition of Faces: A Survey", Proceedings of IEEE, Vol.83, No.5. pp.705-740, 1995.

[8] P. J. Phillips, H. Moon, A. Rizvi and P. J. Rauss, "The Ferret Evolution Methodology for Face-Recognition Algorithm", IEEE Transaction, Pattern Analysis and Machine Intelligence, Vol.22, No.10, pp.1090-1104, 2000.

[9] F. Leclerc and R. Plamondon, "Automatic Signature Verification", International Journal of Pattern Recognition and Artificial Intelligence, Vol.8, No.3, pp.643-660, 1994.

[10] R. Plamondon and G. Lorette, "Automatic Signature Verification and Writer Identification the State of the Art", Pattern Recognition, Vol.22, No.2, pp.107-131, 1989.

[11] J. P. Cambell, "Speaker Recognition: A Tutorial", Proceedings of IEEE. Vol.85, pp.1437-1462, 1997.

[12] Simon Liu and Mark Silverman, "A Practical Guide to Biometric Security and Technology", Proceedings of IEEE Conference of IT Professional, Vol.3, Issue 1, pp.27-32, 2001.

[13] Podio F.L. "Personal Authentication through Biometric Technologies", Proceedings of IEEE International Workshop on Network Appliances, pp. 57-66, 2002.

[14] P. J., Martin A, Wilson C.L., Przyboci M., "An Introduction Evaluating Biometric Systems", IEEE Transactions on Computer, Vol.33, Issue 2, pp. 56-63, 2000.

[15] Dugelav J. L., Jungua J. C., Kotropoulos C., Perronnin F., Pitas I., "Recent Advances In Biometric Person Authentication," Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Vol.4, pp.4060-4063, 2002.

[16] BioAPI http://www.bioapi.org.

요약

개인 인증을 위한 생체인식시스템 사례 및 분류

안큐 아가와*, 어비짙 판디야*, 노영욱**, 김광백***

어떤 조직에서 사용자 접근이나 e-Commerce 또는 다른 보안 응용에서 사용하기 위해 보안이 뛰어난 인증 방법을 찾을 때 생체인식시스템이 최근에 보다 많은 주목을 받고 있다. 생체인식시스템은 개인 인식에서 전통적인 방법보다 뛰어난 보안성과 편리성을 제공한다. 생체인식시스템은 어떤 응용 분야에서는 기존의 기술을 대체하거나 보조하고, 다른 응용 분야에서는 사용할 수 있는 유일한 접근방법이 되고 있다. 본 논문에서는 지문, 손 모양, 얼굴, 귀, 홍채, 서명과 필적을 포함한 여러 생체인식 방법들을 조사하고 비교하였다. 이들 방법들은 특정 응용 분야에서 매우 적합하다. 본 논문에서는 특정 응용 분야에 적합한 생체 인식 방법들을 찾아서 분류하였으며, 어떤 방법은 다른 방법에 비해 침입하기가 어려운 것으로 나타났다.

Keywords : 생체인식시스템, 개인 인증, 지문 인식, 홍채 인식, 서명 인식

* 플로리다 애틀란틱 대학교 컴퓨터공학과
** 신라대학교 컴퓨터교육과
*** 신라대학교 컴퓨터공학과