International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 7 Issue 1 –MARCH 2014.

ADVANCED SECURITY WITH ADVANCED BIOMETRICS

K.G.ArunKumar,J.V.Bhavithra and P.Mohanraj
kgarun1983@gmail.com,bhavihravisu@gmail.com,excelmohanraj@gmail.com

Department of Computer Science and Engineering
Excel Engineering College

ABSTRACT:

Up to now, we using PIN's and Password's for identification. But these are not safe. Suppose consider on-line banking here user may open the fake WebPages of bank that are created by hacker. The aim of hacker is to finding password, through this they robs the account of user. Another case former-chief minister of west Bengal jyothi basu, one of servant who knows the password and theft the ATM card drawn 1lakh rupees from ATM account. This kind of problems can be solvable through **biometrics**. The most suitable definition of biometrics is:

"The automated use of physiological or behavioral characteristics to determine or verify identity."

PIN's were one of the first identifiers to offer automated recognition. However, it should be understood that this means recognition of the PIN, not necessarily recognition of the person who has provided it. The same applies with cards and other tokens. A biometric however cannot be easily transferred between individuals. As said in definition, Physiological biometrics is based on measurements and data derived from direct measurement of a part of the human body. Fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition are leading physiological biometrics. Behavioral characteristics are based on an action taken by a person. Behavioral biometrics, in turn, is based on measurements and data derived from an action, and indirectly measure characteristics of

the human body. Voice recognition, keystroke-scan, and signature-scan are leading behavioral biometric technologies.

Biometric system performance varies according to sample quality and the environment in which the sample is being submitted. While it is not possible to definitely state if a biometric submission will be successful, it is possible to locate factors that can reduce affect system performance. To reduce these difficulties we go for **multimodal biometrics**. A multimodal biometric system uses multiple applications to capture different types of biometrics. This allows the integration of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements. There are three types of multimodal biometrics: synchronous, asynchronous, and either/or. In coming days we go for multimodal biometrics for identification.

How is 'BIOMETRICS' Defined?

Biometrics can be used in such a variety of applications; it is very difficult to establish an all-encompassing definition. The most suitable definition of biometrics is:

"The automated use of physiological or behavioral characteristics to determine or verify identity"

To elaborate on this definition, physiological biometrics is based on measurements and data derived from direct measurement of a part of the human body. Fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition are leading physiological biometrics. Behavioral characteristics are based on an action taken by a person. Behavioral biometrics, in turn, are based on measurements and data derived from an action, and indirectly measure characteristics of the human body. Voice recognition, keystroke-scan, and signature-scan are leading behavioral biometric technologies.

SO WHAT WAS WRONG WITH CARDS AND PIN'S?

PIN's (personal identification numbers) were one of the first identifiers to offer automated recognition. However, it should be understood that this means recognition of the PIN, not necessarily recognition of the

person who has provided it. The same applies with cards and other tokens. We may easily recognize the token, but it could be presented by anybody. A biometric however cannot be easily transferred between individuals and represents as unique an identifier as we are likely to see. If we can automate the verification procedure in a user friendly manner, there is considerable scope for integrating biometrics into a variety of processes.

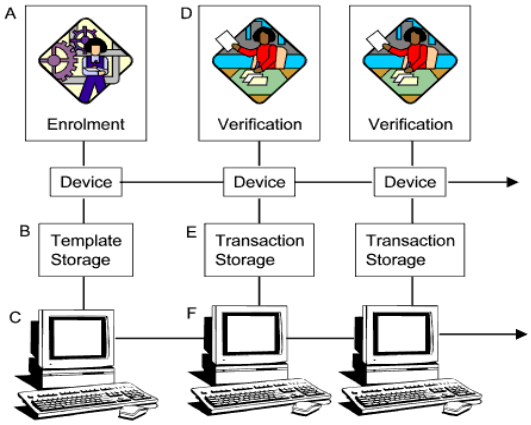
BIOMETRIC BACKGROUND - HOW IT ALL STARTED?

The basic principles of biometric verification were understood and practiced somewhat earlier. Thousands of years earlier to be precise, as our friends in the Nile valley routinely employed biometric verification in a number of everyday business situations. There are many references to individuals being formally identified via unique physiological parameters such as scars, measured physical criteria or a combination of features such as complexion, eye colour and height and so on. Of course, they didn't have automated electronic biometric readers and computer networks (as far as we know), and they certainly were not dealing with the numbers of individuals that we have to accommodate today, but the basic principles were similar. Later, in the nineteenth century there was a peak of interest as researchers into criminology attempted to relate physical features and characteristics with criminal tendencies. This resulted in a variety of measuring devices being produced and much data being collected. The results were not conclusive but the idea of measuring individual physical characteristics seemed to stick and the parallel development of fingerprinting became the international methodology among police forces for identity verification.

In parallel, other biometric methodologies such as fingerprint verification were being steadily improved and refined to the point where they would become reliable, easily deployed devices. In recent years, we have also seen much interest in iris scanning and facial recognition techniques which offer the potential of a non contact technology, although there are additional issues involved in this respect.

HOW THINGS WORK - TYPICAL DEVICE / SYSTEMS PROCESS MAP:

Whilst individual biometric devices and systems have their own operating methodology, there are some generalizations one can make as to what typically happens within a biometric systems implementation. The following diagram depicts the process pictorially and the accompanying notes provide a more detailed explanation:



[A] Obviously, before we can verify an individual's identity via a biometric we must first capture a sample of the chosen biometric. This 'sample' is referred to as a biometric template and is the reference data against which subsequent samples provided at verification time are compared. A number of samples are usually captured during enrolment (typically three) in order to arrive at a truly representative template via an averaging process. The template is then referenced against an identifier in order to recall it ready for comparison with a live sample at the transaction point.

[B] Template storage is an area of interest, particularly with large scale applications which may accommodate many thousands of individuals. The possible options are as follows;

1) Store the template within the biometric reader device.

2) Store the template remotely in a central repository.

3) Store the template on a portable token such as a chip card.

[C] The network. There are possible variations on a theme with regard to networks. Some devices have integral networking functionality, often via RS485 or RS422 with a proprietary protocol. This may enable you to network a number of devices together with no additional equipment involved, or maybe with a monitoring PC connected at one end of the network.

[D] Verification. The verification process requires the user to claim an identity by either entering a PIN or

presenting a token, and then verify this claim by providing a live biometric to be compared against the claimed reference template. There will be a resulting match or no match accordingly .A record of this transaction will then be generated and stored, either locally within the device or remotely via a network and host (or indeed both).With some systems, the reference template is automatically updated upon each valid transaction. This allows the system to accommodate minor changes to the users live sample as a result of ageing, local abrasions etc. and may be a useful feature when dealing with large user bases.

[E] Transaction storage. This is an important area as you will certainly wish to have some sort of secure audit trail with respect to the use of your system. Some devices will store a limited number of transactions internally, scrolling over as new transactions are received. This is fine as long as you are confident of retrieving all such transactions before the buffer fills up and you start losing them. In practice, this is unlikely to be a problem unless you have severe network errors. In some cases, you may wish to have each biometric device connected directly to a local PC which may in turn be polled periodically (over night for example) in order to download transactions to a central point. In either case, you will probably wish to adopt a local procedure to deal with error and exceptional conditions, which will in turn require some sort of local messaging. This may be as simple as a relay closure in the event of a failed transaction activating an annunciator of some description. You may wish to analyze it via an existing reporting tool (if it is in a suitable format) or perhaps write a custom application in order to show transactions in real time as well as write them to a central database.

[F] The network (again). How the network handles transactions may be of critical importance in some applications. For example, you may have multiple terminals distributed within a large facility, each of which requires a real time display of information. This will require fast and reliable message transmission. Each terminal user may wish to ‘hold’ a displayed transaction until a response has been initiated. This will require a separate local message buffer and possibly a message prioritization methodology to ensure that

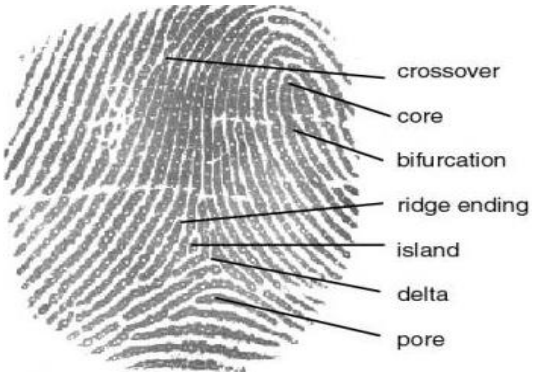
critical messages are dealt with promptly.

POPULAR BIOMETRIC METHODOLOGIES - WHAT ARE THEY?

Fingerprint recognition:

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. 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 as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

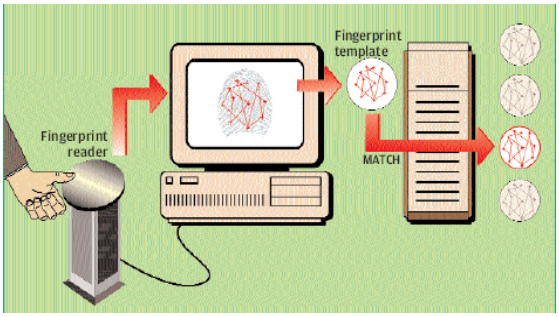
Fingerprint scanning is the acquisition and recognition of a person's fingerprint characteristics for identification purposes. This allows the recognition of a person through quantifiable physiological characteristics that verify the identity of an individual.



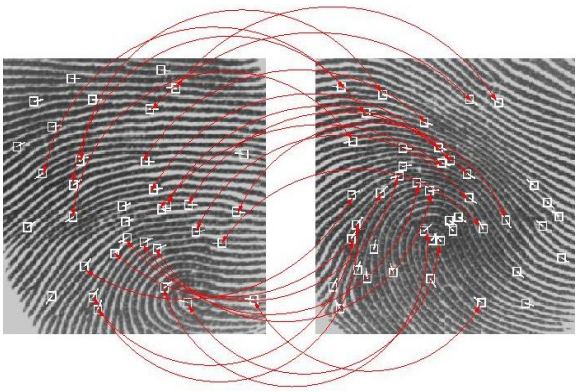
There are basically two different types of finger-scanning technology that make this possible.One is an optical method, The other uses a semiconductor-generated electric field to image a finger. There are a range of ways to identify fingerprints. They include traditional police methods of matching minutiae, which starts with a visual image of a finger.

straight pattern matching, moiré fringe patterns and ultrasonics.

Fingerprint matching techniques can be placed into two categories: minutiae- based

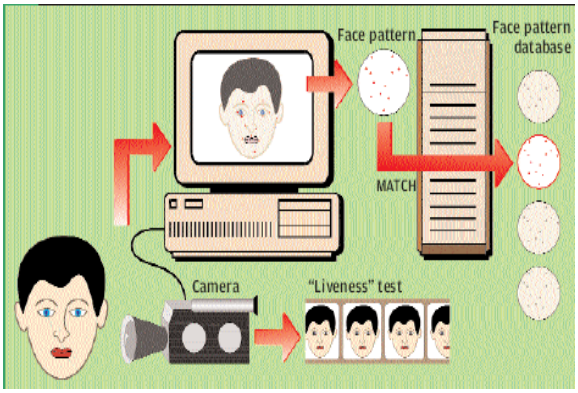


low quality. Also this method does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.



Face recognition:

Facial recognition systems are built on computer programs that and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of analyze images of human faces for the purpose of identifying them. The programs take a facial image, measure characteristics such as the distance between the eyes, the length of the nose, and the angle of the jaw, and create a unique file called a "template." Using templates, the software then compares that image with another image and produces a score that measures how similar the images are to each other. The user 'claims' an identity through a login name or a token, stands or sits in front of the camera for a few seconds, and is either matched or not matched. This comparison is based on the similarity of the newly created match template against the reference template or templates on file. The point at which two templates are similar enough to match, known as the threshold, can be



chin. The system generally needs to match between 14-25 nodes in order to obtain a positive ID. Now, obviously, there are a lot of people coming in and out of the place where this system is set up. The real challenge is to recognize a face instantaneously. To facilitate this, a database is created with the help of an algorithm, which goes through the characteristics of the faces and stores them as a string of numbers. This string is called a face print. The following are the board steps utilized by facial recognition software:

Face detection: The camera pans around looking for a face. The minute it encounters a face, it starts scanning it and proceeds to identifying the various nodes and taking measurements if possible.

Detection of orientation: Once the face is detected, the system determines the heads size and position. Generally, a face needs to be around 40 degrees adjusted for different personnel, PC's, time of day, and other factors. When the image of human face was entered software divides the face into 80 nodes, some of the common one being distance between eyes, width of nose, and depth of eye sockets, cheekbones, jaw line, and towards the camera for the system for register and analyze it.

Mapping: The facial image is scaled down to the level of the images in the database and is then rotated and otherwise adjusted to match the formatting to the images in the database.

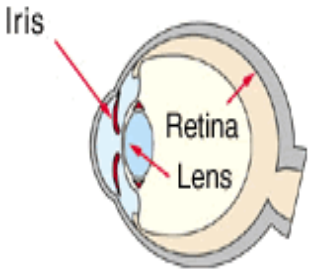
Encoding: The algorithm then converts the face into a face print based on the pre-defined criteria programmed into the algorithm.

Matching: This new data is then used as a filter to sort through the database of faces at super fast speeds to come up with a match.

Since it uses a variety of nodes, simple alteration of the face will not fool it; however, twins might; so the system is certainly not infallible.

IRIS RECOGNITION:

Iris scan biometrics employs the unique characteristics and features of the human iris in order to verify the identity of an individual. The iris is the area of the eye where the



pigmented or coloured circle, usually brown or blue, rings the dark pupil of the eye.

The iris-scan process begins with a photograph. A specialized camera, typically very close to the subject, no more than three feet, uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. This process takes only one to two seconds and provides the details of the iris that are mapped, recorded and stored for future matching/verification. Eyeglasses and contact lenses present no problems to the quality of the image and the iris-scan systems test for a live eye by checking for the normal continuous fluctuation in pupil size. The inner edge of the iris is located by an iris-scan algorithm which maps the iris' distinct patterns and characteristics. An algorithm is a series of directives that tell a biometric system how to interpret a specific problem. Algorithms have a number of steps and are used by the biometric system to determine if a biometric sample and record is a match.

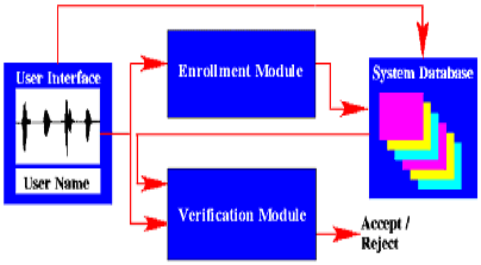
Iris' are composed before birth and, except in the event of an injury to the eyeball, remain unchanged throughout an individual's lifetime. Iris patterns are extremely complex, carry an astonishing amount of information and have over 200 unique spots. The fact that an individual's right and left eyes are different and that patterns are easy to capture, establishes iris-scan technology as one of the biometrics that is very resistant to false matching and fraud. The false acceptance rate for iris

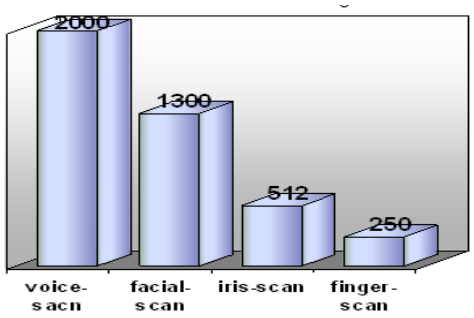
recognition systems is 1 in 1.2 million. The real benefit is in the false-rejection rate, a measure of authenticated users who are rejected. This technology is still not in the public domain and is used only to secure highly sensitive security areas.

VOICE RECOGNITION:

Voice Recognition is a technology which allows a user to use his/her voice as an input device. Voice recognition may be used to dictate text into the computer or to give commands to the computer (such as opening application programs, pulling down menus, or saving work). Older voice recognition applications require each word to be separated by a distinct space. This allows the machine to determine where one word begins and the next stops. These kinds of voice recognition applications are still used to navigate the computer's system, and operate applications such as web browsers or spread sheets. Newer voice recognition applications allow a user to dictate text fluently into the computer. These new applications can recognize speech at up to 160 words per minute. Applications that allow continuous speech are generally designed to recognize text and format it, rather then controlling the computer system itself.

Voice recognition technology utilizes the distinctive aspects of the voice to verify the identity of individuals. Voice recognition is occasionally confused with speech recognition, a technology which translates what a user is saying (a process unrelated to authentication). Voice recognition technology, by contrast, verifies the identity of the individual who is speaking. Two technologies are often bundled – speech recognition is used to translate the spoken word into an account number, and voice recognition verifies the vocal characteristics against those associated with this account. Voice recognition can utilize any audio capture device, including mobile and land telephones and PC microphones. Performance of voice recognition systems can vary according to the quality of the audio signal as well as variation between enrollment and verification devices, so acquisition normally takes place on a device likely to be used for future verification.





TECHNOLOGY COMPARISON:

Method	Coded Pattern	Misidentification rate	Security	Applications
Iris Recognition	Iris pattern	1/1,200,000	High	High-security facilities
Fingerprinting	Fingerprints	1/1,000	Medium	Universal
Facial Recognition	Outline, shape and distribution of eyes and nose	1/100	Low	Low-security facilities
Voiceprinting	Voice characteristics	1/30	Low	Telephone service

Biometric system performance varies according to sample quality and the environment in which the sample is being submitted. While it is not possible to definitely state if a biometric submission will be successful, it is possible to locate factors that can reduce affect system performance.

Fingerprint- Cuts to fingerprint, angle of placement, cold finger, dry/oily finger, pressure of placement, manual activity that would mar or affect fingerprints.

Facial recognition- Change in facial hair, change in hairstyle, lighting conditions, adding/removing hat , adding/removing glasses and change in facial aspect, change in weight.

Iris-scan- Too much movement of head or eye, glasses, colored contacts.

Voice recognition- Cold or illness that affects voice, speaking softly, variation in background noise, quality of capture device, different enrollment and

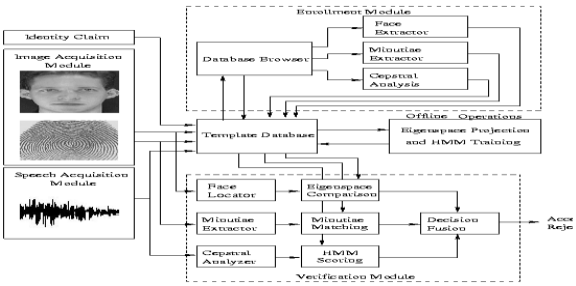
HOW LARGE ARE BIOMETRIC TEMPLATES?

The memory (in bytes) occupied to store template in different technologies are shown below.

verification environments (inside vs. outside)

A MULTIMODAL BIOMETRIC SYSTEM USING FINGERPRINT, FACE AND SPEECH:

We introduce a multimodal biometric system, which integrates face recognition, fingerprint verification, and speaker verification in making a personal identification. This system takes advantage of the capabilities of each individual biometric. It can be used to overcome some of the limitations of a single biometrics. Preliminary experimental results demonstrate that the identity established by such an integrated system is more reliable than the identity established by a face recognition system, a fingerprint verification system, and a speaker verification system.



REFERENCE:

1. M. Abdel-Mottaleb, J. Zhou, Human Ear Recognition from Face Pro¯le Images,ICB 2006, pp. 786 - 792.
2. A. H. M. Akkermans, T. A. M. Kevenaar, D. W. E. Schobben, Acoustic EarRecognition for Person Identi¯cation, Fourth IEEE Workshop on Automatic Identi¯cation Advanced Technologies (AutoID'05) pp. 219-223
3. L. Alvarez, E. Gonzalez, L. Mazorra, Fitting ear contour using an ovoid model,Proc. of 39 IEEE International Carnahan Conference on Security Technology,2005, pp. 145- 148.
4.Paul J. Besl, Neil D. McKay, A method for registration of 3-D shapes, IEEE Trans. Pattern Anal. Machine Intell., pp. 239-256, 1992.
5. M. Burge, W. Burger, Ear biometrics in: Jain, Bolle and Pankanti (Eds.), Biometrics: Personal Identi¯cation in Networked Society, Kluwer Academic, Dordrecht, 1998, pp. 273-286.
6. Burge, M., and Burger, W., Ear biometrics in computer vision, Proc. ICPR 2000, pp. 822-826, 2002
7. A. Bertillon, La photographie judiciaire, avec un appendice sur la classi¯cation et l'identi¯cation anthropometriques, Gauthier-Villars, Paris, 1890.
8. K. Chang, K.W. Bowyer, S. Sarkar, B. Victor, Comparison and combination of ear and face images in appearance-based biometrics, IEEE Trans. PAMI, 2003, vol. 25, no. 9, pp. 1160-1165.
9. H. Chen, B. Bhanu, R. Wang, Performance evaluation and prediction for 3D ear recognition, Proc. International Conference on Audio and Video based Biometric Person Authentication, NY, 2005.

10. H. Chen, B. Bhanu, Contour matching for 3-D ear recognition, Proc. IEEE Workshop on Applications of Computer Vision, Colorado, 2005.
11. B. Bhanu, H. Chen, Human ear recognition in 3-D, Proc. Workshop on Multimodal User Authentication, Santa Barbara, CA, 2003, pp. 91-98.
12. H. Chen and B. Bhanu, Shape Model-based ear detection from side face range images, Proc. of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) - Workshops, 2005, vol. 3, p. 122.
13. M. Choras, Ear Biometrics Based on Geometrical Feature Extraction, Electronic Letters on Computer Vision and Image Analysis (Journal ELCVIA), 2005, vol. 5, no. 3, pp. 84-95.
14.www.timesonline.co.uk/article/0,1-973291,00.html Man convicted of murder by earprint is freed, January 22, 2004
15. Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993).
16. C. Dorai and A. Jain, COSMOS-A representation scheme for free-form surfaces, Proc. IEEE Conf. Computer Vision, 1995, pp. 1024-1029.
17. L. Meijermana, S. Shollb, F. De Contic, M. Giaconc,C. van der Lugtd, A. Drusinic, P. Vanezis, G. Maata, Exploratory study on classi¯cation and individualisation
of earprints, Forensic Science International 140 (2004) 91-99 18. Hurley, D. J., Nixon, M. S. and Carter, J. N. Force Field Energy Functionals for Image Feature Extraction. Proc. 10th British Machine Vision Conference, 1999, pp. 604-613 The Ear as a Biometric 19
19. D. J. Hurley, M. S. Nixon, J. N. Carter, A New Force Field Transform for Ear and Face Recognition. In Proceedings of the IEEE International Conference on Image Processing ICIP2000,, 2000, pp. 25-28.
20. D. J. Hurley, M. S. Nixon, J. N. Carter, Force Field Energy Functionals for Image Feature Extraction, Image and Vision Computing, Special Issue on BMVC 99, 2002, vol. 20, No.5-6, pp. 311-317
21. D. J. Hurley, M. S. Nixon, J. N. Carter, Automatic Ear Recognition by Force Field Transformations. In Proceedings of IEE Colloquium: Visual Biometrics (00/018), 8/1-8/5.
22. D. J. Hurley, Force Field Feature Extraction for Ear Biometrics. PhD Thesis 2001, Electronics and Computer Science, University of Southampton.
23. D. J. Hurley, M. S. Nixon, J. N. Carter, Force ¯eld feature extraction for ear biometrics, Computer Vision and Image Understanding, 2005, vol. 98, pp. 491-512.
24. D. J. Hurley, M. S. Nixon, J. N. Carter, Ear Biometrics by Force Field Convergence, Proc. AVBPA 2005, pp. 386-394
25. A. Iannarelli, Ear Identi¯cation, Paramount Publishing Company, Freemont, California, 1989
26.K. Iwano, T. Hirose, E. Kamibayashi, S. Furui, Audio-Visual Person Authentication Using Speech and Ear Images, Proc. of Workshop on Multimodal User Authentication, 2003, pp.85-90.
27. I. T. Jolli®e, Principal Component Analysis (New York: Springer), 1986
28. STATE v. David Wayne KUNZE, Court of Appeals of Washington, Division 2. 97 Wash. App. 832, 988 P.2d 977, 1999
29. K. Messer, J. Matas, J. Kittler, J. Luettin, G. Maitre, XM2VTSDB: The

Extended M2VTS Database, Proc. AVBPA'99 ,Washington D.C., 1999

30. B. Moreno, A. Sanchez, On the Use of Outer Ear Images for Personal Iden-ti¯cation in Security Applications, IEEE 33rd Annual Intl. Conf. on Security Technology, 1999, pp. 469-476.

31. Z. Mu, L. Yuan, Z. Xu, D. Xi, S. Qi, Shape and Structural Feature Based Ear Recognition1, Sinobiometrics 2004, LNCS 3338, 2004, pp. 663-670.

32. J. L. Northern, M. P. Downs, Hearing in Children, Lippincott Williams & Wilkins, Fifth Edition, 2002

33. K. Pun, Y. Moon, Recent advances in ear biometrics, Proc. of the Sixth International Conference on Automatic Face and Gesture Recognition, 2004, pp. 164-169.

34. www.biometrics.org

35. www.biometricsinfo.org

36. www.bioapi.org