Evaluation of Biometrics

VenkataSubbaReddy Poli **Nagaraja Arcot** **Jyothsna Charapanamjeri**

Department of Computer Science,College of Engineering,S.V.University,Tirupathi-517502, India

Summary

Biometrics is the science of recognizing the identity of a person based on the physical or behavioral attributes of the individual such as face, fingerprints,voice and iris. Data derived from direct measure ment of a part of the human body. Fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition are leading physiological biometrics. An automatic personal identification system based solely on one methodology often cannot meet the system performance requirements. So a combination of two or more methodologies is used to achieve required performance, which is called multibiometrics. In this paper we explained techniques used in biometric system, which includes Iris recognition,Finger print identification,speech recognition,Hand geometry.

Keywords:

BioMetrics,Iris recognition,Finger print identification,speech recognition,Hand geometry.

1. Introduction:

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person. The relevance of biometrics in modern society has been reinforced by the need for large-scale identity management systems whose functionality relies on the accurate determination of an individual's identity in the context of several different applications.

Examples of these applications include sharing networked computer resources, granting access to nuclear facilities, performing remote financial transactions or boarding a commercial flight. The proliferation of web-based services (e.g., online banking) and the deployment of decentralized customer service centers (e.g., credit cards) have further underscored the need for reliable identity management systems that can accommodate a large number of individuals.

The overarching task in an identity management system is the determination (or verification) of an individual's identity (or claimed identity).Such an action may be necessary for a variety of reasons but the primary intention, in most applications, is to prevent impostors from accessing protected resources.

Traditional methods of establishing a person's identity include knowledge based (e.g., passwords) and token-based (e.g., ID cards) mechanisms, but these surrogate representations of identity can easily be lost, shared, manipulated or stolen thereby compromising the intended security. Biometrics offers the identity of an individual may be viewed as the information associated with that person in a particular identity management system [15]. For example, a bank issuing credit cards typically associates a customer with her name, password, social security number, address and date of birth. Thus, the identity of the customer in this application will be defined by these personal attributes (i.e., name, address, etc.).

The term biometric authentication is perhaps more appropriate than biometrics since the latter has been historically used in the field of statistics to refer to the natural and reliable solution to certain aspects of identity management by utilizing fully automated or semi-automated schemes to recognize individuals based on their biological haracteristics.

By using biometrics it is possible to establish an identity based on who you are, rather than by what you possess,such as an ID card, or what you remember, such as a password.

In some applications, biometrics may be used to supplement ID cards and passwords

thereby imparting an additional level of security. Such an arrangement is often called a dual-factor authentication scheme.

Biometric technology is used for dozens of types of applications, ranging from modest to expansive .Depending on the application, the benefit of using or deploying biometrics may be increased security, increased convenience, reduced fraud,or delivery of enhanced services. In some applications, the biometric serves only as a deterrent.In others, it is central to system operation. Regardless of the rationale for deploying biometrics, there are two common elements:

1. The benefits of biometric usage and deployment are derived from having a high degree of certainty regarding an individual's identity.
2. The benefits lead directly or indirectly to cost savings or to reduced risk of financial losses for an individual or institution.

Not withstanding the benefits of biometric technology, biometrics are not suitable for every application and user,

Manuscript received September 5, 2009
Manuscript revised September 20, 2009

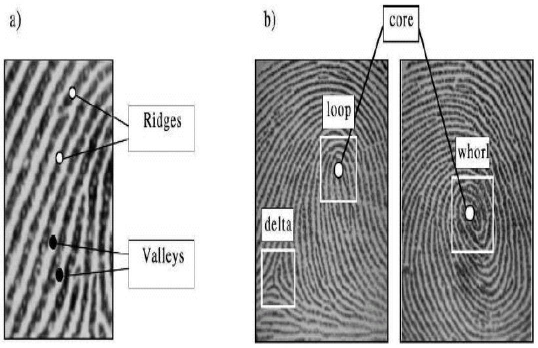
and in some cases biometric authentication is simply the wrong solution. One of the major challenges facing the biometric industry is defining those environments in which biometrics provide the strongest benefit to individuals and institutions, and then demonstrating that the benefits of deployment outweigh the risks and costs. Over time, the increased effectiveness and affordability of biometric technologies has continually broadened the range of applications in which biometrics operate effectively.

What is Biometric Authentication:
Biometric authentication is an automated method whereby an individual's identity is confirmed by examining a unique physiological trait or behavioral characteristic, such as a fingerprint, iris, retina, or signature. Physiological traits are stable physical characteristics, such as finger prints, palm prints and iris patterns. Biometric system is the integrated biometric hardware and software used to conduct biometric identification or verification.

Biometric characteristics:
1. Universality: Every individual accessing the application should possess the trait.
2. Uniqueness: The given trait should be sufficiently different across individuals comprising the population.
3. Permanence: The biometric trait of an individual should be sufficiently invariant over a period of time with respect to the matching algorithm. A trait that changes significantly over time is not a useful biometric.
4. Measurability: It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause undue inconvenience to the individual. Furthermore, the acquired raw data should be amenable to processing in order to extract representative feature sets.
5. Performance: The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.
6. Acceptability: Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.
7. Circumvention: This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g., fake fingers), in the case of physical traits, and mimicry, in the case of behavioral traits.

Popular Biometric Methodologies:
1. Fingerprint Recognition:
Fingerprint images can be broadly classified into three categories, namely, (i) rolled/full, (ii) plain/flat and (iii) latent [10, 12, 14] . Rolled fingerprint images are obtained by rolling a finger from one side to the other ("nail-to-nail") in order to capture all the ridge-details of a finger. Plain impressions are those in which the finger is pressed down on a flat surface but not rolled. While plain impressions cover a smaller area than rolled prints, they typically do not have the distortion introduced during rolling.
Rolled and plain impressions are obtained either by scanning the inked impression on paper or by using live-scan devices. Since rolled and plain fingerprints are acquired in an attended mode, they are typically of good quality and are rich in information content. In contrast, latent fingerprints are lifted from surfaces of objects that are inadvertently touched or handled by a person through a variety of means ranging from simply photographing the print to more complex dusting or chemical processing [9, 13]. It is the matching of a latent fingerprint against a database of rolled prints or latent prints (reference prints) that is of utmost importance in forensics to apprehend a criminal.

For storing in to database we use the fallowing techniques:
Feature extraction:
In a fingerprint image, ridges (also called ridge lines) are dark whereas valleys are bright (see Figure a). Ridges and valleys often run in parallel; sometimes they bifurcate and sometimes they terminate. When analyzed at the global level, the fingerprint pattern exhibits one or more regions where the ridge lines assume distinctive shapes. These regions (called singularities or singular regions) may be classified into three typologies: loop, delta, and whorl (see Figure b). Singular regions belonging to loop, delta, and whorl types are typically characterized by ∩, ¢ , and O shapes, respectively. The core point (used by some algorithms to pre-align fingerprints) corresponds to the center of the north most (uppermost) loop type singularity.



a) Ridges and valleys in a fingerprint image;
b) singular regions (white boxes) and core points (circles) in fingerprint images.

At the local level, other important features, called *minutiae* can be found in the fingerprint patterns. Minutia refers to the various ways in which the ridges can be discontinuous. For example, a ridge can abruptly come to an end (termination), or can divide into two ridges (bifurcation) (Fig below).

Although several types of minutiae can be considered, usually only a coarse classification (into these two types) is adopted to deal with the practical difficulty in automatically discerning the different types with high accuracy.

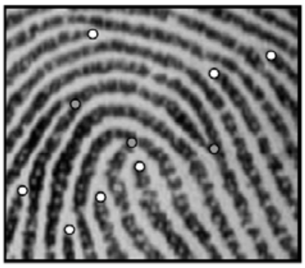
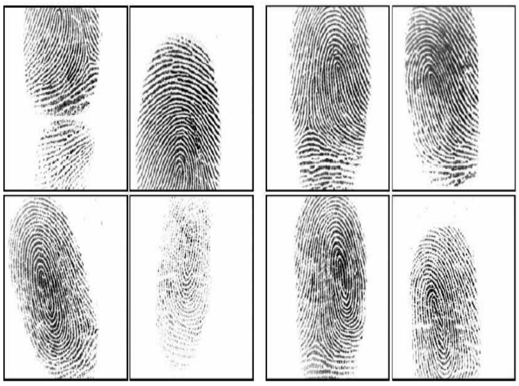


Fig: Termination (white) and bifurcation (gray) minutiae in a sample fingerprint.

MATCHING:

Matching high quality fingerprints with small intra-subject variations is not difficult and every reasonable algorithm can do it with high accuracy. The real challenge is matching samples of poor quality affected by: i) large displacement and/or rotation; ii) non-linear distortion; iii) different pressure and skin condition; iv) feature extraction errors. The two pairs of images in Figure visually show high variability (large *intra-subject* variations) that can characterize two different impressions of the same finger. On the other hand, as it is evident from Figure b, fingerprint images from different fingers may sometimes appear quite similar



a) Each row shows a pair of impressions of the same finger, which were falsely non-matched by most of the algorithms

b) each row shows a pair of impressions of different fingers, which were falsely matched by some of the algorithms

The large number of existing approaches to fingerprint matching can be coarsely classified into three families:

i) correlation-based matching,
ii) minutiae-based matching and
iii) ridge feature-based matching.

In the rest of this section, the representation of the fingerprint acquired during enrollment is denoted as the *template* (T) and the representation of the fingerprint to be matched is denoted as the *input* (I). In case no feature extraction is performed, the fingerprint representation coincides with the grayscale fingerprint image itself.

Advantages:

- Low cost biometric technology
- Low volume, low throughput openings
- High security environments

Application: *Access Contro*

2. Hand Geometry:

Associating an identity with an individual is called personal authentication. The person can be recognized by what he knows (e.g. password, PIN, or piece of personal information), by what he owns (e.g. card key, smart card, or token like a SecurID card) or by his human characteristics (biometrics). Biometric methods of person authentication belong in modern approaches in field of access security. The main advantage of biometric is that human characteristics cannot be misplaced or forgotten [1].

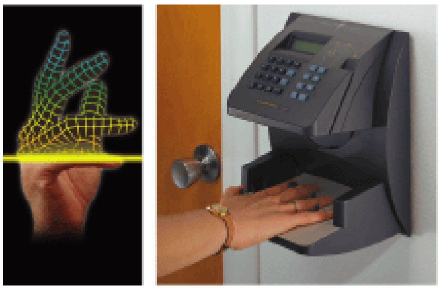


Fig 1. System Architecture

Typical architecture of all biometric systems consists of two phases:

- enrollment,
- recognition.

In the phase of enrollment, several images of hand are taken from the users. The images, called templates, are preprocessed to enter feature extraction, where a set of measurement is performed. Final model depends on the method used for recognition. Models for each of the users are then stored in the database. In the phase of recognition,a single picture is taken, preprocessed, and features are obtained. In the proposed system, the process of verification is used, where the input template is compared only with the model of claimed person. The feature vector is compared with features from the model previously stored in the database. The result is the person is either authorized or not authorized.

To evaluate a biometric system's accuracy the most commonly adopted metrics are the False Rejection Rate (FRR) and False Acceptance Rate (FAR). FRR is the percentage of authorized individuals rejected by the systemand FAR is the percentage that unauthorized persons are accepted by the system [1]. The point where FAR and FRR have the same value is called Equal Error Rate (ERR).

The proposed system is dedicated for verification and therefore requires the user to claim identity through an artificial ID (e.g., magnetic card or PIN) before the system can start process of enrollment or authentication. Due to assistance of artificial IDs, verification systems require considerable less computational resources but the FRR may increase slightly. This Is because the combined FRR for a system that uses both artificial IDs and biometric is:

(1) On the other hand, the combined FAR can be greatly reduced with artificial identities.

(2) Gaussian Mixture Model

In order to obtain better results than in previous approaches,technique of Gaussian mixture models (GMM) has been implemented for recognition block. GMM is pattern recognition technique that uses an approach of the statistical methods [6]. The vector of each hand measurement can be described by normal distribution, also called Gaussian distribution. Each hand measurement may be then defined by two parameters (for our case, where measurement vector is one dimensional): mean (average) and standard deviation (variability).

Technology

When a user presents a biometric sample, hand geometry systems follow the same basic steps as other biometric devices: capturing the sample, processing the raw sample into a biometric template, and comparing the observed template to a reference template in the enrollment database. Most hand geometry systems also incorporate the optional step of updating the reference template in the enrollment database after a successful verification. These processes are illustrated in below fig

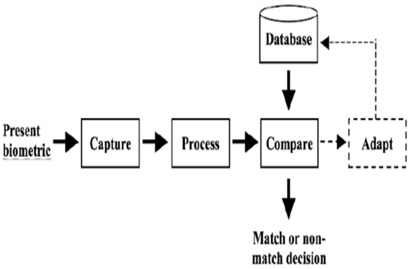


Fig: Hand geometry recognition

Hand Capture:

Capturing the biometric sample is often achieved by a standard optical camera or a flat-bed scanner. Some units rely only on ambient light, but most provide their own illumination, generally in the near infrared. Because hand geometry is based on analyzing the contours of the hand, these systems binarize the captured grayscale image into a black-and-white silhouette (Fig below).

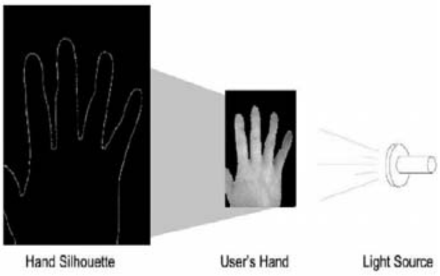


Fig: Depiction of hand casting a shadow.

Because of this, hand geometry systems are insensitive to changes in surface features such as tattoos, hair, cuts, scrapes, burns, dirt, or other contaminants that may affect other biometric modalities.

Processing:

Some hand geometry units rely on finger-positioning guides to aid in repeatable placement of the hand. For these systems, a pre-processing step is required to remove the positioning pins from the image. While this increases processing at the image level, it may decrease the overall computational power required for the algorithm, as the algorithm is no longer required to account for hand rotation or hand deformation due to varying hand placement [2]. As will be discussed in a following section, a significant number of researchers are investigating pin-free hand geometry systems, as they are seen as more user friendly than systems with pins. Others feel that the tactile feedback provided by the pins is a positive feature that enhances ease of use as well as performance.

Processing the captured image varies greatly for different types of hand geometry systems. Commercial systems and most academic systems begin by measuring geometric features in the binarized hand-image. Measurements typically include finger lengths, widths, surface areas, angles between landmarks, and ratios of those quantities. See Fig below.

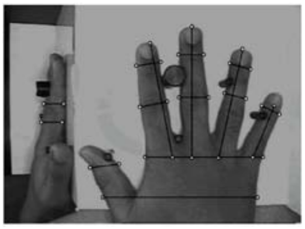


Fig: Example top-view image with side-mirror, showing measurements for length, width, and thickness

3. Facial Technology:

Recognition Systems' face recognition readers analyze faces based on the found face and eyes position. The method involved in this is as follows:

- Any kind of data source is used for input it is either a still image, a video stream or a connection to a face image database.
- Normalization: based on the found face and eyes position, the image is scaled, rotated and finally presented at a fixed size.
- Preprocessing: standard techniques applied like histogram equalizations, intensity normalization
- The images are analyzed to determine the position and size of one or more faces.
- The eyes centers are located and marked. Images including eyes positions are taken as Primary Facial Data.
- Characteristics of the face are extracted and represented as a vector inn-dimensional spaces are similarity of faces is the distance of two vectors. The vectors represent the Secondary Facial Data and are used for fast comparisons.
- Secondary Facial Data can be stored in a central database or on a token storage device, like a smartcard.
- In case the Secondary Facial Data is stored on a smartcard, only verification is possible.

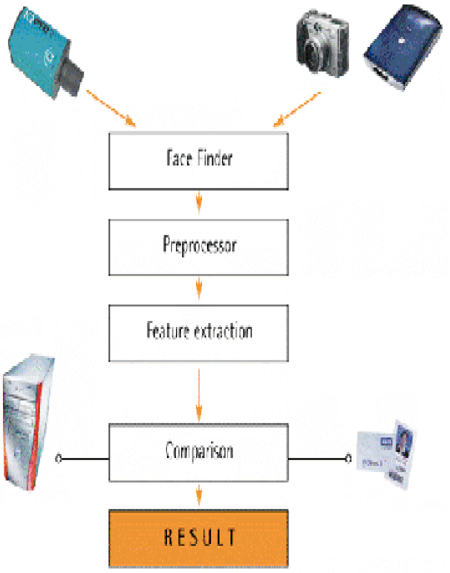


Fig: face recognition system architecture

Face Recognition Techniques

Law enforcement agencies have built, over time, very large databases of facial images of offenders. Digital face images are becoming prevalent in government issued documents (e.g., passports and driver licenses). This is due to the high compatibility of face biometric in machine readable travel document systems based on a number of evaluation factors among the six major biometric modalities [6].

The non-intrusiveness characteristic of face biometric often ompensates for its relatively lower accuracy, which has made it popular in applications dealing with official documents.

As a result, a number of critical security and forensic applications require automatic identification or verification capability based on facial images. A major problem that various government and law enforcement agencies face is to detect “multiple enrollments” in the facial database that they maintain (such as mugshot, driver license photos or passport pictures). To address this problem, we need to develop face recognition systems invariant to images of the same user captured at different times. Many offenders will commit crimes at different periods in their lives, often starting as a young adult - or even before - and continue throughout their lives. It is not unusual to encounter a time difference of many years between enrollment and verification in some applications. Ling et al. [10] studied how age differences affect face recognition performance in a real passport photo verification task. Their results show that the aging process does increase the difficulty, but it does not surpass the influence of illumination or expression. However, as these latter issues, namely, illumination and expression, are being successfully addressed by incorporating 3D models, aging process will continue to be a major obstacle for performance improvement [20] [19].

The Face Recognition Grand Challenge (FRGC, 2006) evaluation showed that substantial progress has been made in face recognition [16]. Results of FRGC demonstrated that the performance improved by an order of magnitude over Face Recognition Vendor Test (FRVT 2002). However, automatic face recognition in unconstrained situations remains a challenging problem. The difficulties come from potentially large variations in face images from the same subject due to differences in pose, lighting, expression, age and occlusion, leading to drastic performance degradation [11]. The FRVT report estimated a decrease in performance by approximately 5% for each additional year of age difference. Therefore, the development of age correction capability remains an important issue for robust face recognition. The use of 3D face models and 3D range images has helped in achieving pose and expression invariance [11][13]. 3D face matching is intrinsically pose-invariant, and a deformable model can achieve robustness to expression variation. However, although range scanners and other Studies on face verification across age progression [19] have shown that:

(i) simulation of shape and texture variations caused by aging is a challenging task, as factors like life styles and weather contribute to changes in addition to biological factors.

(ii) the aging effects can be best understood using 3D scans of human heads, and

(iii) the few existing aging databases are not only small but also contain uncontrolled external variations.

Due to these reasons, the effect of aging in facial recognition has not been as extensively investigated as other factors of intra-individual variations in facial appearance. A few studies on aging process can be found in biological sciences, e.g. in [23, 18]. These studies have shown that cardioidal strain is a major factor in aging of facial outlines. Such results have also been used in psychological studies, e.g. introducing aging by caricatures generated by shifting 3D model parameters [12].

A few image-based approaches in 2D have already been proposed to simulate both growth and adult aging, e.g. [20, 22]. These seminal studies demonstrated the feasibility of improving face recognition accuracy by simulated aging.

There are also some developments in the related area of age the face images such as normalizing faces for rotation, scale and illumination compensation.

IDENTIFICATION MODE: The presented data is used to scan a data base for most similar faces the most similar reference data is taken as an evidence of the person's identity.

VERIFICATION MODE: The presented facial data is compared to data read from the database or token, based on the similarity threshold the identity is confirmed.

Robust face recognition systems should be able to handle the variations that occur under practical operational scenarios. This means having the ability to handle any and all of face variations under different lighting, pose, expressions, and other variation factors such as low resolution face acquisition from a distance. To improve the performance and address each variation, numerous new algorithms have been proposed aiming at generalization to unseen people, multiple factor analysis and hidden structures of the faces. In case of low resolution faces, pre-processing methods that can enhance the resolution of face images have been detailed. Small pose variations can be handled and trained by different classifiers; however large pose variations can only be modelled

by methods such as Tensorfaces and our proposed extensions.

4. Iris Recognition:

Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity. Biometric authentication requires only a few seconds, and biometric systems are able to compare thousands of records per second. Finger-scan, facial-scan, iris-scan, hand-scan and retina-scan are considered physiological biometrics and voice-scan and signature-scan are considered behavioral biometrics. A distinction may be drawn between an individual and an identity; the individual is singular, but he may have more than one identity, for example ten registered fingerprints are viewed as ten different identities [1].

Iris recognition is the most powerful biometric technology. The iris is the plainly visible, colored ring that surrounds the pupil. It is a muscular structure that controls the amount of light entering the eye, with intricate details that can be measured, such as striations, pits, and furrows. The iris is not to be confused with the retina, which lines the inside of the back of the eye as shown in Fig 1.

Fig 1:

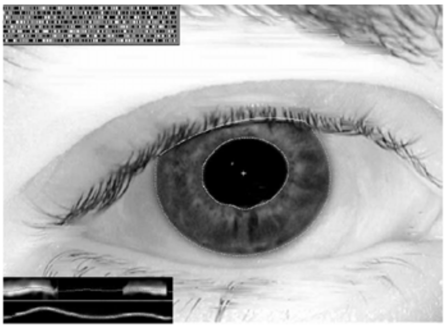
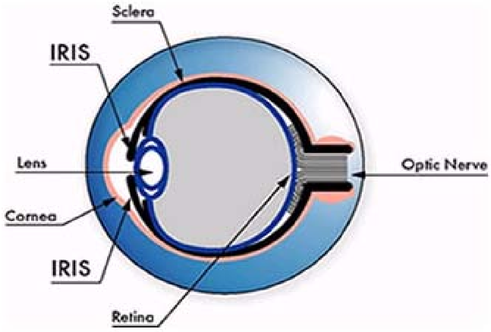


Fig2:



Data acquisition begins with reliable means of establishing a visible iris, and then its boundaries are precisely located by a circular edge detector algorithm. Extracting textural characteristics are based in 2-D Gabor phasor coefficients which are computed, providing high orientational and spatial-frequency resolution as well as the information of its 2-D position. Zones of analysis are established on the iris in a projected polar coordinate system, dimensionless, in order to maintain reference to the same regions of the iris regardless of constriction of iris (pupillary size), distance to eye and video zoom factor. Each bit in an iris code can be regarded as a coordinate of a vertice in a unit square of the complex plane from the coordinate system described above, forming a 256 bytes code, which is used for comparisons [5].

There are, to our knowledge, no scientific papers describing medical procedures interfering in biometric data in iris recognition, there are reports in fingerprinting though No two irises are alike. There is no detailed correlation between the iris patterns of even identical twins, or the right and left eye of an individual. The amount of information that can be measured in a single iris is much greater than fingerprints, and the accuracy is greater than DNA. This method an iris recognition camera takes a black and white picture from 5 to 24 inches away, depending on the type of camera. The camera uses non-invasive, near-infrared illumination that is barely visible and very safe. Unlike other biometric technologies that can be used in surveillance mode, iris recognition is an opt-in technology. In order to use the technology you must first glance at a camera.

Iris Code:

The picture of an eye is first processed by software that localizes the inner and outer boundaries of the iris, and the eyelid contours, in order to extract just the iris portion. Eyelashes and reflections that may cover parts of the iris are detected and discounted.

Sophisticated mathematical software then encodes the iris pattern by a process called Demodulation. This creates a phase code for the texture sequence in the iris, similar to a DNA sequence code. The Demodulation process uses functions called 2-D wavelets that make a very compact yet complete description of the iris pattern, regardless of its size and pupil dilation, in just 512 bytes.

The phase sequence is called an Iris Code template, and it captures the unique features of an iris in a robust way that allows easy and very rapid comparisons against large databases of other templates. The IrisCode template is immediately encrypted to eliminate the possibility of identity theft and to maximize security.

Iris Recognition:

In less than a few seconds, even on a database of millions of records, the IrisCode template generated from a live image is compared to previously enrolled ones to see if it matches any of them. The decision threshold is automatically adjusted for the size of the search database to ensure that no false matches occur even when huge numbers of Iris Code templates are being compared with the live one. Some of the bits in an IrisCode template signify if some data is corrupted (for example by reflections, or contact lens boundaries), so that it does not influence the process, and only valid data is compared. Decision thresholds take account of the amount of visible iris data, and the matching operation compensates for any tilt of the iris. A key advantage of iris recognition is its ability to perform identification using a one-to-all search of a database, with no limitation on the number of IrisCode records and no requirement for a user first to claim an identity, for example with a card.

APPLICATIONS:

The practical applications of biometric technologies are diverse and expanding, as new needs are identified. Some areas where Biometrics can be used are

Banks: ATMs, VPNs, Automated branches, Cash Dispensing, Point of Sale, Access Control.

E-Business: B2B Trading exchanges, Payment gateways, Call centers, Data Centers.

Networksecurity: Enterprise Intranet, Extranet, VPNs.

These applications can be categorized into three main groups (see Table 1.1):

1. Commercial applications such as computer network login, electronic data access control, mobile phone, PDA, medical records management, distance learning, etc.
2. Government applications such as national ID card, managing inmates in acorrectional facility, driver's license, social security, welfare-disbursement,
border control, passport control, etc.
3. Forensic applications such as corpse identification, criminal investigation,
parenthood determination, etc.

Future Applications:

- ATM machine use: Most of the leading banks have been experimenting with biometrics for ATM machine use and as a general means of combating card fraud.
- Workstation and network access: Many are viewing this as the application, which will provide critical mass for the biometric industry and create the transition between sci-fi device to regular systems component, thus raising public awareness and lowering resistance to the use of biometrics in general.
- Travel and tourism: There are multi application cards for travelers which, incorporating a biometric, would enable them to participate in various frequent flyer and border control systems as well as paying for their air ticket, hotel room, hire care etc.
- Telephone transactions: Many telesales and call center managers have pondered the use of biometrics.

Benefits:

- ✓ No more forgotten passwords, lost cards or stolen pins. You are your own password.
- ✓ Positive Identification-It identifies you and not what you have or what you carry.
- ✓ Highest level of security.
- ✓ Offers mobility.
- ✓ Impossible to forget.
- ✓ Serves as a “Key” that cannot be transferred or coerced.
- ✓ Non-intrusive.
- ✓ Safe & user friendly.
- ✓ Increased security when controlling access to confidential data and IT systems.
- ✓ Reduced risk of fraudulent use of identity by employees.

Demerits:

- ➢ An automatic personal identification system based solely on fingerprints or faces is often not able to meet the system performance requirements.
- ➢ In case of face recognition, face will sometimes change with time or injury, and that poses a problem
- ➢ Fingerprint verification is reliable but inefficient in database retrieval.
- ➢ Some voice recognition systems has some problems since the voice changes with a human’s mood and illness and background noise poses some problems.

5. Conclusion:

Biometrics makes automated use of physiological or behavioral characteristics to determine or verify identity. Finger biometrics are most popular and one of the most accurate and cost effective solutions. Hand geometry, signature-scan, keystroke-scan, palm-scan are some more biometric technologies in use. With Biometrics there is no problem of ID being stolen. Many institutions and organizations are trying to use this technology.

References: Iris

[1] Nanavati S, Thieme M, Nanavati R: Biometrics: identity verification in a networked world.". New York: John Wiley & Sons, Inc 2002.

[2] Daugman J: Wavelet demodulation codes, statistical independence, and pattern recognition. *In: Institute of mathematics and its applications* Cambridge: Horwood 2000, 244-60.

[3] Daugman J: How iris recognition works. *The Computer Laboratory, University of Cambridge.* [Acessed 2003 Jan 23 at http://www.CL.cam.ac.uk/users/jgd1000 *webcite*]

[4] Ronald AllenL, Duncan MillsW: *In: "Signal analysis: time, frequency, scale, In: "Signal analysis: time, frequency, scale, and structure."* New York: IEEE Press, John Wiley & Sons Inc 2004, 338-351.

[5] Daugman JG: High confidence visual recognition of persons by a test of statistical significance. *IEEE Trans Pattern Anal Machine Intell* 1993, 1148-61.

References: Finger Print

[1] Case Profile, Innocence Project. http://www.innocenceproject.org/Content/73.php.

[2] Neurotechnology Inc., Verifinger. http://www.neurotechnology.com.

[3] CDEFFS: the ANIS/NIST Committee to Define an Extended Fingerprint Feature Set. http://fingerprint.nist.gov/standard/cdeffs/index.html.

[4] Evaluation of latent fingerprint technologies 2007. http://fingerprint.nist.gov/latent/elft07/.

[5] A review of the FBI’s Handling of the Brandon May-field Case. Office of the Inspector General, Special Report, March 2006. http://www.usdoj.gov/oig/special/s0601/PDF_list.htm.

[6] Conclusion of circuit court judge Susan Souder - grants motion to exclude testimony of forensic fingerprint examiner capital murder case: State of Maryland v. Bryan Rose, October 2007. http://www.clpex.com/Information/STATEOFMARYLAND-v-BryanRose.doc.

[7] http://fingerprint.nist.gov/latent/elft07/phase1_aggregate.pdf.

[8] D. Ashbaugh. Quantitative-Qualitative Friction Ridge Analysis.

[9] P. M. Christophe Champod, Chris Lennard and M. Stoilovic,editors. Fingerprints and Other ridge Skin Impressions. CRC Press, 2004.

[10] V. N. Dvornychenko and M. D. Garris. Summary of NIST latent fingerprint testing workshop. NISTIR 7377, November 2006. http://fingerprint.nist.gov/latent/ir_7377.pdf.

[11] J. Feng. Combining minutiae descriptors for fingerprint matching. Pattern Recognition, 41(1):342–352, 2008.

[12] P. Komarinski, editor. Automated Fingerprint Identification Systems (AFIS). Elsevier Academic Press, 2001.

[13] H. C. Lee and R. E. Gaensslen, editors. Advances in Fingerprint Technology. CRC Press, New York, 2001.

[14] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. Handbook of Fingerprint Recognition. Springer-Verlag, 2003.

References: Face Recognition

[1] FG-NET Aging Database, http://www.fgnet.rsunit.com.

[2] V. Blanz and T. Vetter. A morphable model for the synthesis of 3d faces. In SIGGRAPH ’99: Proc. 26th annual conference on Computer Graphics and Interactive Techniques, pages 187–194, New York, NY, 1999.

[3] T. F. Cootes, G. J. Edwards, and C. J. Taylor. Active appearance models. IEEE Trans. on Pattern Anal. and Mach. Intell., 23(6):681–685, 2001.

[4] L. G. Farkas, editor. Anthropometry of the Head and Face. Lippincott Williams & Wilkins, 1994.8th IEEE Int'l Conference on Automatic Face and Gesture Recognition.

[5] X. Geng, Z.-H. Zhou, and K. Smith-Miles. Automatic age estimation based on facial aging patterns. IEEE Trans. Pattern Anal. Mach. Intell., 29:2234–2240, 2007.

[6] R. Heitmeyer. Biometric identification promises fast and secure processing of airline passengers. ICAO Journal, 55(9),2000.1

[7] A. Lanitis, C. Draganova, and C. Christodoulou. Comparing different classifiers for automatic age estimation. IEEE Trans. SMC-B, 34(1):621–628, February 2004.

[8] A. Lanitis, C. J. Taylor, and T. F. Cootes. Toward automatic simulation of aging effects on face images. IEEE Trans. Pattern Anal. Mach. Intell., 24(4):442–455, 2002.

[9] W.-S. Lee, Y.Wu, and N. Magnenat-Thalmann. Cloning and aging in a vr family. In VR '99: Proc. IEEE Virtual Reality,page 61, Washington, D.C., 1999. 3

[10] H. Ling, S. Soatto, N. Ramanathan, and D. Jacobs. A study of face recognition as people age. In IEEE International Conference on Computer Vision (ICCV), 2007.

[11] X. Lu and A. K. Jain. Deformation modeling for robust 3d face matching. In IEEE Conf. Computer Vision and Pattern Recognition (CVPR), pages 1377–1383, Washington, D.C.,2006.

[12] A. OT'oole, T. Vetter, H. Volz, and E. Salter. Threedimensional caricatures of human heads: distinctiveness and the perception of facial age. Perception, 26:719–732, 1997.

[13] U. Park, H. Chen, and A. K. Jain. 3d model-assisted face recognition in video. In CRV '05: Proc. 2nd Canadian Conference on Computer and Robot Vision, pages 322–329,Washington, D.C., 2005. 1, 3

[14] E. Patterson, K. Ricanek, M. Albert, and E. Boone. Automatic representation of adult aging in facial images. In IASTED '06: Proc. 6th International Conference on Visualization,Imaging, and Image Processing, pages 171–176,2006. 2

[15] E. Patterson, A. Sethuram, M. Albert, K. Ricanek, and M. King. Aspects of age variation in facial morphology affecting biometrics. In BTAS '07: Proc. First IEEE International Conference on Biometrics: Theory, Applications, and Systems, pages 1–6, 2007. 2

[16] P. J. Phillips,W. T. Scruggs, A. J. O'Toole, P. J. Flynn, K.W.Bowyer, C. L. Schott, and M. Sharpe. FRVT 2006 and ICE 2006 Large-Scale Results. Technical Report NISTIR 7408, National Institute of Standards and Technology.

[17] F. Pighin, R. Szeliski, and D. H. Salesin. Modeling and animating realistic faces from images. Int. J. Comput. Vision,50(2):143–169, 2002. 4

[18] J. B. Pittenger and R. E. Shaw. Aging faces as viscal-elastic events: Implications for a theory of nonrigid shape perception. J.

[19] N. Ramanathan and R. Chellappa. Face verification across age progression. In IEEE Conf. Computer Vision and Pattern Recognition (CVPR), volume 2, pages 462–469, 2005. 1, 2

[20] N. Ramanathan and R. Chellappa. Modeling age progression in young faces. In IEEE Conf. Computer Vision and Pattern Recognition (CVPR), volume 1, pages 387–394, 2006. 1, 2

[21] K. J. Ricanek and T. Tesafaye. Morph: A longitudinal image database of normal adult age-progression. In FGR '06: Proc.7th International Conference on Automatic Face and Gesture Recognition, pages 341–345, Washington, D.C., 2006. 3

[22] J. Suo, F. Min, S. Zhu, S. Shan, and X. Chen. A multiresolution dynamic model for face aging simulation. In IEEE Conf. Computer Vision and Pattern Recognition (CVPR),2007. 2, 3

[23] D. W. Thompson. On Growth and Form. New York: Dover, 1992. 2

[24] J. Wang, Y. Shang, G. Su, and X. Lin. Age simulation for face recognition. In ICPR '06: Proc. 18th International Conference on Pattern Recognition, pages 913–916, 2006.27

References: Handgeometry

[1] KUNG, S. Y., MAK, M. W., LIN, S. H. Biometric Authentication. Published as Prentice Hall Professional Technical Reference. New Jersey: First Printing, September 2004.

[2] VARCHOL, P., LEVICKY, D. Implementation of Gaussian mixture models for biometric security system. In Proceedings Komunikacne a informacne technologie, Tatranske Zruby(Slovak Republic), 2007.
RADIOENGINEERING, VOL. 16, NO. 4, DECEMBER 2007 87

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

[4] SANCHEZ-REILLO, R. Biometric identification through hand geometry measurements. IEEE Transactions on Pattern Analysis and Machine Intelligence. ISSN: 0162-8828. Washington, 2000.

[5] JAIN, A., ROSS, A. A prototype hand geometry-based verification system. In Proceedings of 2nd Int. Conference on Audio- and Videobased Biometric Person Authentication. Washington (USA), 1999.

[6] YOUNG, S. The HTK Book (for HTK Version 3.2). First published December 1995, Revised for HTK Version 3.2 December 2002.