A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies

Tiwalade O. Majekodunmi, Francis E. Idachaba

Abstract—**This paper reviews four biometric identification technologies (fingerprint, speaker recognition, face recognition and iris recognition). It discusses the mode of operation of each of the technologies and highlights their advantages and disadvantages.**

Index Terms— **biometric, fingerprint, face recognition, iris recognition, speaker recognition.**

I. Introduction

BIOMETRIC identification, or biometrics, refers to the process of identifying an individual based on his or her distinguishing characteristics. It comprises methods for uniquely recognizing humans based on one or more intrinsic physical or behavioural traits [1], [2].

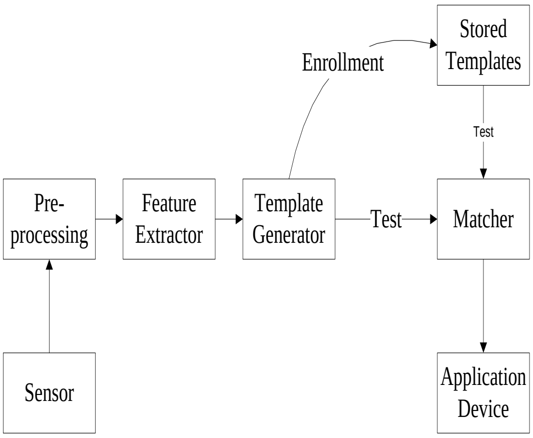

Fig. 1. The basic block diagram of a biometric system

There are three (3) traditional ways of authenticating the identity of an individual, these include possessions (such as keys, passports, and smartcards), knowledge (user ID, passwords and pass phrases), and biometrics. These three modes of authentication can be combined, especially in automated authentication e.g. a password plus a user ID, an ATM card requiring a PIN, a passport with a face picture and signature biometrics, etc. Identity authentication becomes a challenging task when it has to be automated with high accuracy and hence with low probability of break-ins and reliable non-repudiation. The user should not be able to deny having carried out the transaction and should be inconvenienced as little as possible, which only makes the task more difficult [1], [3]. In biometrics, there are two distinct authentication methods and they are:

1. Verification: It is based on a unique identifier which singles out a particular person (e.g. an ID number) and that individual's biometrics. It is based on a combination of authentication modes.
2. Identification: It is based only on biometric measurements. It compares these measurements to the entire database of enrolled individuals instead of just a single record selected by some identifier.

According to [4], there are basically five attributes that biometric data must possess to make it practical and these include:

1. Universality: Every person should have the biometric characteristic.
2. Uniqueness: no two persons should be the same in terms of the biometric characteristic.
3. Permanence: the biometric characteristic should be invariant over time.
4. Collectability: the biometric characteristic should be measurable with some (practical) sensing device.
5. Acceptability: the particular user population and the public in general should have no (strong) objections to the measuring/ collection of the biometric.

It is the combination of all these attributes that determines the effectiveness of a biometric system in a particular application. There is no biometric system that absolutely satisfies any of these properties or one which has all the above mentioned attributes to a completely satisfactorily level simultaneously, especially if acceptability is taken into account. This means that any biometric authentication solution is the result of many compromises

Manuscript received January 19, 2011.

T. O. Majekodunmi is with the Department of Electrical and Information Engineering, Covenant University, Ota, Ogun State, Nigeria. (Phone: +2348062397564;
e-mail: tiwalade.majekodunmi@covenantuniversity.edu.ng).

F.E Idachaba is with the department of Electrical and Information Engineering in Covenant University Ota. He is currently on sabbatical with the Shell Petroleum Development Company in Nigeria. (Phone: +234-8039570321; email:idachabafe@yahoo.com and Francis.Idachaba@shell.com

[1], [5]. This paper seeks to analyse four biometric technologies (fingerprint recognition, speaker recognition, face recognition and iris recognition), their advantages and disadvantages.

II. Fingerprint Recognition

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. The fingerprint is scanned electronically and a reference template created accordingly. This template may be derived from either minutiae element, the pattern of the fingerprint, or simply the image of the fingerprint. The inside surfaces of the hands and feet of all primates contain minute ridges of skin, with furrows between each ridge. The purpose of this skin structure is to facilitate exudation of perspiration, enhance sense of touch, and provide a gripping surface. Fingerprints are part of an individual’s phenotype and hence are only weakly determined by genetics. Fingerprints are distinctive to a person. It is shown in [6], that identical twins have fingerprints that are quite different. Within the forensic community it is widely believed that no two people have identical ridge details. The belief in the uniqueness of fingerprints led to their widespread use in law-enforcement identification applications and also civilian applications such as access control, time and attendance tracking, and computer user login. Fingerprinting for person identification had an advantage over most other biometrics in that fingerprint acquisition has been possible for centuries in the form of impressions of inked fingers on paper and direct impressions in materials like clay. Many novel techniques have been developed over the last decade to acquire fingerprints without the use of ink. The basic principle of the ink - less methods is to sense the ridges on a finger, which are in contact with the surface of the scanner. The acquired image is called a “livescan” and the scanners are known as “livescan” fingerprint scanners [1, 7, and 8]. The livescan image acquisition systems are based on four technologies:

1. Frustrated Total Internal Reflection (FTIR) and other optical methods: A camera acquires the reflected signal from the underside of a prism as the subject touches the top of the prism. The typical image acquisition surface of 1 inch x 1 inch is converted to 500 dpi images using a CCD or CMOS camera. The issue with reflection technologies is that the reflected light is a function of skin characteristics; a wet or dry skin, will give a fingerprint impression that can be saturated or faint, respectively, and hard to process but this can be overcome to some extent by using ultrasound instead of visible light [9,10, and 11].
2. CMOS capacitance: The ridges and valleys of a finger create different charge accumulations when the finger touches a CMOS chip grid. This charge is converted to an intensity value of a pixel with suitable electronics. These CMOS devices are sensitive to electrostatic discharge and mechanical breakage. These devices image at 500 dpi and provide about 0.5 inch x 0.5 inch of fingerprint surface scan area, this can be a problem as two impressions of the same finger acquired at two different times may have little overlap and the images also tend to be affected by the skin dryness and wetness [12].
3. Thermal Sensing: The sensor is fabricated using pyroelectric material, which measures temperature changes due to ridge-valley structure as the finger is swiped over the scanner and produces an image. This works on the basis that skin is a better thermal conductor than air and thus contact with the ridges causes a noticeable temperature drop on a heated surface. This technology is claimed to overcome the dry and wet skin issues of optical scanners and can sustain higher static discharge. The resultant images, however, are not rich in gray values, i.e. dynamic range [13].
4. Ultrasound sensing: An ultrasonic beam is scanned across the finger surface to measure directly the depth of the valleys from the reflected signal. Dry, wet and oily skin conditions do not affect the imaging and the images better reflect the actual ridge topography. These units however tend to be bulky and they require longer scanning time than the optical scanners [14].

There is a property that is peculiar to automatic fingerprint recognition systems - the process of acquiring the biometric data involves touching some input device with the pattern, this makes the actual pattern that is being sensed distorted during the acquisition. Non- contact fingerprint scanners are used to avoid the problems associated with the elastic distortion of the skin pattern caused by the touch sensing methods [15]. A fingerprint authentication system reports some degree of similarity or difference between two fingerprint images but it should report these measures accurately and reliably, irrespective of imaging problems associated with the matching techniques discussed below. Ideally the similarity between two impressions of the same finger should be large or the difference between the two images should be small. Hence the similarity or difference between two impressions of the same finger should be invariant to translation, rotation, applied pressure and elastic distortion between the impressions due to the elasticity of the finger skin [1]. There are three classes of matching techniques:

1. Image techniques: This class includes both optical as well as numerical image correlation techniques. These techniques are most effective when the area of the finger that is sensed is small (e.g. as with CMOS sensors).
2. Feature techniques: This class extracts interesting features from the fingerprint and develops different machine representations of it from the features. This is the most widely used technique.
3. Hybrid techniques: This technique combines both the image and feature techniques or uses neural networks to improve accuracy.

Human experts use details of the ridge flow pattern to determine if two impressions are from the same finger [1].

Fig. 2 shows a piece of thinned fingerprint structure with some of these features: ridge endings, ridge bifurcations , independent ridge, etc. the most commonly used fingerprint features are the ridge bifurcations and ridge endings which are collectively known as minutiae and are extracted from the digitized print.

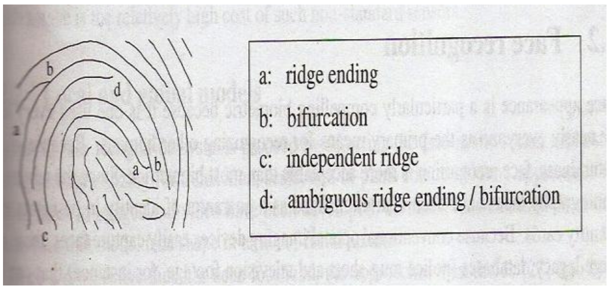

Fig. 2. Ridge patterns of individual fingers have minute details, known as minutiae that distinguish one print from another [1].

The process of feature extraction typically starts with examination of the quality of the input image then computing the orientation of the flow of ridges, which reflect the local ridge direction at each pixel. The local ridge orientation is used to tune filter parameters for image enhancement and ridge segmentation. A thinned image, Fig. 2 is computed from the segmented ridges to locate the minutia features. A minutia post-processing stage cleans up several spurious minutiae resulting from fingerprint imperfections (dirt, cuts), enhancement, and ridge segmentation or thinning artefacts [1]. The machine representation of a fingerprint is critical to the success of the matching algorithm. A minimal representation of a processed fingerprint is a set $\{(x_i, y_i, \Theta_i)\}$ of minutiae, i.e., a set of points (x_i, y_i), expressed in some coordinate system with a ridge direction at point, Θ_i [16]. Jain et al in [17] used a string representation in which matching is performed through string matching algorithms.

Advantages

1. Fingerprint is practical in forensic investigation.
2. Ease of collecting samples using low technology means. There is a continuous decline in the size and price of fingerprint readers. The conversion of fingerprints into digital images is getting easier, better and cheaper.
3. There are large legacy databases of fingerprints in existence.

Disadvantages

1. There is a large variation of the quality of the fingerprint over the population. The appearance of a person's print depends on age, grease, and cut or worn fingers, i.e., on occupation and lifestyle in general.
2. Elastic distortion of the skin of the finger due to touch sensing methods and potential problems with cleanliness of the sensor and public hygiene.
3. In some very rare cases, there are people without fingers, or without a full set of fingers. Obviously, these individuals cannot be fingerprinted.

III. Speaker Recognition

This is the process of automatically recognising an individual through his speech by using speaker-specific information included in speech waves to verify the identity being claimed. It is sometimes referred to as voiceprint recognition or voice recognition. It attempts to identify individuals by how they sound when speaking [1]. The dynamics of vocal annunciation are partly a product of our vocal tract, mouth and nasal cavities, and general physiological "architecture". In speaker recognition, these characteristics are captured and a representative template created for subsequent comparison with a live sample [7]. Speaker identity is correlated with physiological and behavioural characteristics of the speech production system of an individual speaker. These characteristics derive from both the spectral envelope (vocal tract characteristics) and the supra-segmental features (voice source characteristics) of speech [18]. Speaker recognition can be classified into speaker identification and speaker verification. Speaker identification is the process of determining from which of the registered speakers a given utterance comes. Here, a speech utterance from an unknown speaker is analyzed and compared with speech models of known speakers. The unknown speaker is identified as the speaker whose model best matches the input utterance. Speaker verification is the process of accepting or rejecting the identity claimed by a speaker. Here, an identity is claimed by an unknown speaker, and an utterance of this unknown speaker is compared with a model for the speaker whose identity is being claimed. If the match is good enough, that is, above threshold, the identity claim is accepted. The fundamental difference between identification and verification is the number of decision alternatives. In identification, the number of decision alternatives is equal to the size of the population, whereas in verification there are only two choices, acceptance or rejection, regardless of the population size [18]. Speaker recognition is different from speech recognition. Although they often share the same front-end processing, in speech recognition it is the words, not the speaker that must be determined. Speaker recognition is attractive because of its prevalence in human communication and human day-to-day use. Voice is a behavioural biometric but it is dependent on underlying physical traits which govern the type of speech signals we are able and likely to utter. Properties like the fundamental frequency (a function of the vocal tract length), nasal tone, cadence, inflection, etc., all depend on the identity of the speaker [1].

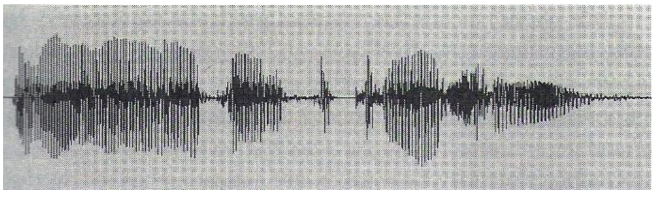

Fig. 3. A segment of a voice amplitude signal (e.g. voltage measured across a microphone) as a function of time [1].

Speaker authentication systems can be categorised depending on requirements for what is spoken, this also determines the sophistication of algorithms used. The categories of speaker authentication systems are:

1. Fixed Text: The speaker says a predetermined word or phrase, which was recorded at enrolment. The word may be secret, so acts as a password, but once recorded a replay attack is easy, and re-enrolment is necessary to change the password.
2. Text-Dependent: The speaker is prompted by the authentication system to say a specific thing. The machine aligns the utterance with known text to determine the user. For this, enrolment is usually longer, but the prompted text can be changed at will.
3. Text Independent: The speaker authentication system processes any utterance of the speaker. Here the speech can be task-oriented, so it is hard to record and replay speech that also accomplishes the impostor's goal. Monitoring can be continuous, and the system's confidence in the identity of the user is greater. Such systems can even authenticate a person when they switch language. The advent of trainable speech synthesis [19], [20] might enable attacks on this approach.
4. Conversational: During authentication, the speech is recognised to verify identity by inquiring about knowledge that is secret, or at least is unlikely to be known or guessed by an impostor. FAR (False Acceptance Rates) below 10^{-12} are claimed to be possible by this combination of biometric and knowledge, making conversational biometrics very attractive for high-security applications [21], [22].

Speaker recognition is traditionally used for verification, but more recent technologies have started to address identification protocols particularly in audio and video indexing. Conversational biometrics which combines "voiceprint" recognition with the exchange of knowledge in an interactive authentication provides higher accuracy [21, 22, and 23]. The processing of the speech signal requires that the output of the microphone be digitised then the speech and non-speech portions (such as silence) in the signal are separated. After this, most speaker recognition systems extract some form of frequency-based features similar to those used in speech recognition systems. For instance, the use of short-term spectral analysis with 20 ms windows placed every 10 ms to compute Fourier coefficients are typical. These magnitude spectra are then converted to cepstral features (a method for extracting the spectral envelope independent of the voicing signal). The cepstral features are further processed to compensate for channel mismatch before being used to generate or match models of individual speakers. Matching techniques in speaker recognition vary because many of the features used in the representation are algorithm-specific [1]. According to [24], the matchers can be classified into four categories, namely:

1. Template Matching: Here, a fixed text utterance is used to generate a stored reference which is then compared to the newly acquired feature vector to generate a matching score.
2. Dynamic Time Warping (DTW): This is an optimisation technique. It is used to obtain the best alignment between the two signals. In a variation of DTW, called *nearest-neighbour matching*, the match score is computed as the sum of distances between the query vector and the *k* nearest neighbours (reference templates) corresponding to the speaker's purported identity.
3. Neural Network-based Matchers: These essentially develop more precise and statistically accurate decision boundaries but require extensive data-driven training to discriminate between the speakers.
4. Hidden Markov Models (HMMs): This is a common technique in speech recognition. It encodes the feature vectors and the evolution of features over the course of an utterance. It can also compensate for statistical variation of the features but require large amounts of training data.

Advantages

1. Voice is a natural biometric (one that people use instinctively to identify each other) under certain circumstances (phone) and machine decisions can be verified by relatively unskilled operators.
2. The voice biometric requires only inexpensive hardware and is easily deployable over existing, ubiquitous communications infrastructure (the telephone system). Voice is therefore very suitable for pervasive security management.
3. Voice allows incremental authentication protocols. For example, the protocol prescribes waiting for more voice data when a higher degree of recognition confidence is needed.

Disadvantages

1. With the improvement of text-to-speech technology improving, it becomes possible to create non-existent identities with machine voices (when enrolment and authentication are remote) and trainable speech synthesis may make it possible to create an automatic system that can imitate a given person saying anything [20].
2. Voice recognition is dependent on the quality of the captured audio signal. Speaker identification systems are susceptible to background noise, channel noise (from phone lines, wireless transmission, or severe compression) and unknown channel or microphone characteristics.
3. Speech characteristics can drift away from models with age.

IV. Face Recogntion

Face recognition is a process of automatically identifying or verifying a person from a digital image or a video frame from a video source. An image of the face is captured and analysed in order to derive a template. This analysis may take various forms from plotting geometric points to grey-scale analysis of pixels to determine boundaries, etc [7], [25]. Face recognition was introduced in the 1960s. The US government hired a man named Woodrow W. Bledsoe to create the very first semi-automated face recognition system. The machine located key features on the face and calculated the ratios between them for identification. A decade later, three men named Goldstein, Harmon and Lesk joined forces to enhance the existing machines. They developed a 21-point check for the machines to identify and calculate the ratios between these facial structures. The 21 points included very intricate features of the face such as thickness of the lips and colour of the hair [26]. Some recognition algorithms identify faces by extracting landmarks, or features from an image of the subject's face. For example, an algorithm may analyse the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalise a gallery of face images and then compress the face data, only saving the data in the image that is useful for face detection. A probe image is then compared with the face data. One of the earliest, successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation [25]. Recognition algorithms can be divided into two main approaches:

1. Geometric, this looks at distinguishing features, and
2. Photometric, which is a statistical approach that distils an image into values and comparing the values with templates to eliminate variances.

Face recognition systems are often required to deal with a wide variety of image acquisition modes. The National Institute of Standards and Technology (NIST) proposed a recommended set of guidelines for face image acquisition [27], and they include:

1. Single Image: Optical methods include digitizing hardcopy documents using optical scanners. This is important because legacy data is mostly available in the form of still photographs, either black-and –white or coloured. Analogue and digital cameras may also be used for live face image acquisition. Generally, images are taken cooperatively (as in the case of driver's licenses) and under well-controlled lighting conditions in order to normalise the appearance of samples in the database.
2. Video Sequence: Surveillance cameras acquire video sequences, often including face images. Regular camera has not proved to be very useful for face recognition because the spatial resolution is too low. Even using hyper-resolution technique, where detail is built up by integrating successive frames, has not borne much fruit because the frame rates for many surveillance systems are quite low (1 – 4 frames per second) and hence very few good images of a face are acquired from a moving target. Tracking techniques in conjunction with a pan-tilt-zoom (PTZ) camera might be used to improve the resolution by physically zooming in on suspected faces (at the cost of diminishing the overall view).
3. 3D Image: Many new face recognition techniques are based on skin or skull geometry and require 3D images of the face instead of a 2-D image. Techniques for acquiring such images include but are not limited to stereo, structured light, and phase-based ranging.
4. Near Infrared: Low-power infrared illumination (invisible to the human eye) can be used to obtain robust images under poor lighting conditions.

In general, face recognition systems proceed by detecting the face in the scene, thereby estimating and normalising for translation, scale and in-plane rotation. Many approaches to finding faces in images and video have been developed and they are all based on weak models of the human face that model the shape of the face in terms of facial texture [1]. After the localisation of a prospective face, the approaches then divide into two categories [28]:

1. Face Appearance: the essence of these approaches is to reduce a facial image containing thousands of pixels to a handful of numbers and capture the distinctiveness of the face without being overly sensitive to "noise" such as lighting variations. To achieve this, a face image is transformed into a space that is spanned by basis image functions, just like Fourier transform projects an image onto basis images of the fundamental frequencies. In its simplest form, the basis functions, known as eigenfaces, are the eigenvectors of the covariance matrix of a set of training images as shown below in Fig. 3.

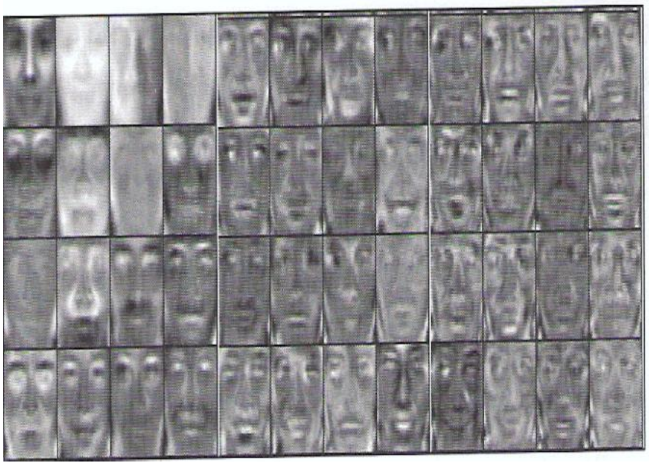

Fig. 4. A face image decomposed as a sum of weighted eigenfaces; the first eigenface (top left) is considered as "beauty" and the other eigenface deviations from "beauty" are considered as caricatures [1].

2. Face geometry: this approach seeks to model a human face in terms of particular face features, such as eyes, mouth etc., and the geometry of the layout of these features. Face recognition is then a matter of matching feature constellations as in Fig. 4.

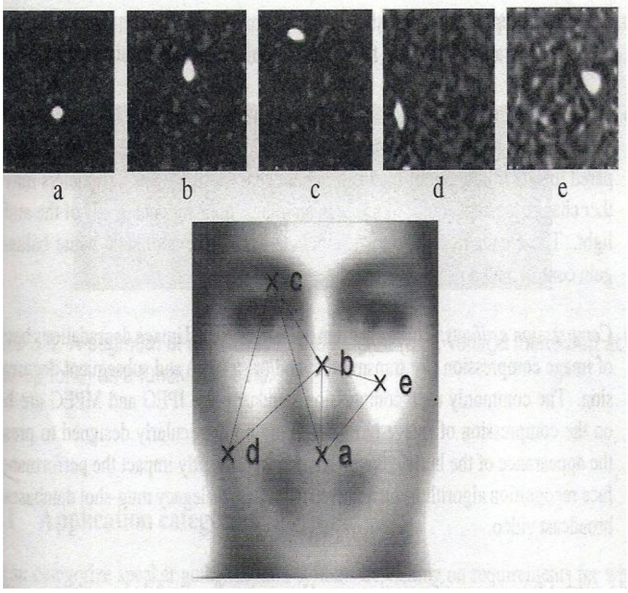

Fig. 5. Feature-based face recognition: a - e: Local feature detection and localisation. The face image below shows the local features and geometric relations (courtesy J.J. Atick (Identix Inc.) & [29].

Fig. 5 shows an approach to face recognition that is based on face features. Features like the rim of the nose and the cheeks of the subject are detected and their geometric relationships are used for recognition of the face. Local face feature appearance models are often similar to the eigenface models for complete faces like that shown in Fig. 4 and these are then called "eigen-eyes", "eigen-noses," etc [1]. Turk and Pentland [30] popularised the eigenface approach. Kirby and Sirovich [31], [32] introduced similar face image transformation for representing and compressing face images and they also developed a computationally efficient matrix computation of the transform.

Advantages

1. Face recognition systems are the least intrusive from a biometric sampling point of view because they neither require contact nor the awareness of the subject.
2. The biometric works with legacy photograph databases, video tape and other image sources.
3. It is a fairly good biometric identifier for small-scale verification application.

Disadvantages

1. A face needs to be well-lit by controlled light sources in automated face authentication systems.
2. Face is a poor biometric for use in a pure identification protocol, it performs better in verification.
3. There is some criminal association with face identifiers since this biometric has long been used by law enforcement agencies ("mug-shots").

V. Iris Recognition

Iris recognition is a method of biometric authentication that uses pattern-recognition techniques based on high-resolution images of the irises of an individual's eyes. The iris is captured via an infrared imaging process, which distinguishes the iris from the pupil and sclera portions of the eye. A template is then derived from an analysis of the detail within the trabecula meshwork of the iris [7], [33]. Iris recognition technology uses camera technology, with subtle infrared illumination reducing specular reflection from the convex cornea to create images of the detail-rich, intricate structures of the iris. These images are converted into digital templates to provide mathematical representations of the iris that yield unambiguous positive identification of an individual. John G. Daugman of the University of Cambridge's Computer Laboratory pioneered this breakthrough work to create the iris recognition algorithms required for image acquisition and one-to-many matching. These algorithms were used to effectively debut commercialisation of the technology in conjunction with an early version of the IrisAccess system designed and manufactured by Korea's LG Electronics. Daugman's algorithms are the basis of most of the currently commercially deployed iris recognition systems [33]. An iris recognition algorithm first has to identify the approximately concentric circular outer boundaries of the iris and the pupil in a photo of an eye. The set of pixels covering only the iris is then transformed into a bit pattern that preserves the information that is essential for a statistically meaningful comparison between two iris images. The mathematical methods used are similar to those of modern lossy compression algorithms for photographic images. In the case of Daugman's algorithms, a Gabor wavelet transform is used in order to extract the spatial frequency range that contains a good best signal-to-noise ratio considering the focus quality of available cameras. The result is a set of complex numbers that carry local amplitude and phase information of the iris image. All amplitude information is discarded (to ensure the template remains largely unaffected by changes in illumination and virtually negligibly by iris colour, which contributes significantly to the long-term stability of the biometric template) and the resulting 2048 bits that represent an iris consist of only the complex sign bits of the Gabor-domain representation of the iris image. To authenticate via identification (one-to-many template matching) or verification (one-to-one template matching), a template created by imaging the iris is compared to a stored value template in a database. A Hamming distance (between the live and stored templates) below the decision threshold indicates a positive identification [33].

Advantages

1. Iris recognition has the smallest outlier (those who cannot use/enrol) group of all biometric technologies.
2. Template longevity is a key advantage of this technique as barring trauma, a single enrolment can last a lifetime.
3. The iris has a fine texture that is determined randomly during embryonic gestation. Even genetically identical individuals (twins) have completely independent iris textures, whereas

DNA (genetic “fingerprinting”) is not unique for the about 0.2% of the human population who have a genetically identical twin [33].

4. John Daugman’s IrisCode, which is the originally commercially deployed iris recognition algorithm, has an unprecedented false match rate (FMR) better than 10^{-11} [33].

Disadvantages

1. There are few legacy databases.
2. The small size of the iris makes sampling of the iris pattern require a great deal of user cooperation or complex, expensive input devices.
3. The performance of iris authentication may be impaired by glasses, sunglasses and contact lenses.
4. The iris biometric is not left as evidence on crime scene so it is not useful for forensic applications.

VI. Conclusion

Fingerprint has a long tradition of its use as an immutable identification in law enforcement and its samples can be collected with ease. Speaker recognition is attractive because of its prevalence in human day-to-day communication and conversational biometrics provides higher accuracy and flexibility. Face recognition uses low-power infrared illumination to obtain robust images under poor lighting conditions, its systems are the least intrusive from a biometric sampling point of view and it is a fairly good biometric identifier for small-scale verification applications. Iris recognition has the smallest outlier group of all biometric technologies, it is well-suited for one-to-many identification because of its speed of comparison and template longevity is a key advantage of this technology.

References

[1] Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, and Andrew W. Senior, *Guide to Biometrics*. Springer Science + Business Media, Inc, NY 10013, USA, 2004, pp 3 – 6, 31 – 45, 146 – 148.

[2] (2010, August 10). Biometrics – Wikipedia, the free encyclopaedia [Online]. Available: http://en.wikipedia.org/wiki/Biometrics

[3] B. Miller, “Vital Signs of Identity,” IEEE *Spectrum*, vol. 31, no. 2, pp. 22-30, 1994.

[4] R. Clarke, “Human Identification in Information Systems: Management Challenges and Public Policy Issues,” *Information Technology & People*, vol. 7, no. 4, pp. 6 – 37, December 1994.

[5] A. K. Jain, R. M. Bolle, and S. Pankanti (Eds.), *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers, Boston, MA, 1999.

[6] S. Pankanti, S. Prabhakar, and A.K. Jain, “The Individuality of Fingerprints,” in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Kauai, Hawaii, December 2001, pp. I: 805 -812.

[7] Julian Ashbourn, *Practical Biometrics: From Aspiration to Implementation*. Springer-Verlag London, 2004, p. 2.

[8] (2010, August 10). Fingerprint recognition – Wikipedia, the free encyclopaedia [Online]. Available: http://en.wikipedia.org/wiki/Fingerprint_recognition

[9] D.T. Follette, E. B. Hultmark, and J. G. Jordan, “Direct Optical Input System for Fingerprint Verification,” *IBM Technical Disclosure Bulletin*, April 1974.

[10] N.J. Harrick, “Techniques To Improve Binary Joint Transform Correlator Performance For Fingerprint Recognition,” *Applied Optics*, vol. 33, 1962.

[11] *Data sheet 8: Frustrated Reflection Fingerprinting*, Harrick Scientific Products Inc., Pleasantville, New York 10570, circa 1970.

[12] S. Jung, R. Thewes, T. Scheiter, K.F. Gooser, and W. Weber, “A Low-Power and High-Performance CMOS Fingerprint Sensing and Encoding Architecture,” in *IEEE Journal of Solid-State Circuits*, vol. 34, no. 7, July 1999, pp. 978-984.

[13] J. F. Mainguet, M. Pegulu, and J.B. Harris, “Fingerchip™: Thermal Imaging and Finger Sweeping in a Silicon Fingerprint Sensor,” in *Proceedings of AutoID 99*, October 99, pages 91 -94.

[14] W. Bicz, Z. Gurnienny, and M. Pluta, “Ultrasound Sensor for Fingerprints Recognition,” in *Proceedings of SPIE*, vol. 2634, Optoelectronic and Electronic Sensors, June 1995, pp. 104 – 111.

[15] *Non-Contact Fingerprint Scanner*, Digital Descriptor Systems Inc., Available: http://www.ddsi-cpc.com/products.htm.

[16] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, “A Real-time Matching System for Large Fingerprint Database,” in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 18, no. 8, August 1996, pp. 799 – 813.

[17] A. K. Jain, L. Hong, and R. M. Bolle, “On-Line Fingerprint Verification,” in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, April 1997, pp. 302 – 313.

[18] (2010, August 28). Speaker Recognition – Scholarpedia [Online]. Available: http://www.scholarpedia.org/article/Speaker_recognition

[19]R. Donovan, “ Trainable Speech Synthesis,” Ph.D. thesis, Engineering Department, Cambridge University, Cambridge, UK, 1996.

[20] R.W. Sproat, “Multilingual Text-to-Speech Synthesis: The Bell Labs Approach,” Lucent Technologies Staff, Bell Laboratories, Lucent Technologies, Murray Hill, NJ, USA. Kluwer Academic Publishers, Boston, MA, October 1997.

[21] S. H. Maes, J. Navratil, and U. V. Chaudhari, “Conversational Speech Biometrics,” in *E-Commerce Agents, Marketplace Solutions, Security Issues, and Supply Demands*, Berlin: Springer-Verlag, 2001, pp. 166 -179.

[22] G.N. Ramaswamy, “Conversational Biometrics: The Future of Personal Identification,” Technical report, IBM Research Division, Yorktown Heights, NY, September 2001.

[23] H. S. M. Beigi, S. H. Maes, U. V. Chaudhari, and J. S. Sorensen, “IBM Model-Based and Frame-By-Frame Speaker Recognition,” *Speaker Recognition and its Commercial and Forensic Applications, Avignon*, April 1998.

[24] D. A. Reynolds, “Automatic Speaker Recognition: Current Approaches and Future Trends”, in *Proceedings of IEEE AutoID 2002*, Tarrytown, NY, March 2002, pp. 103 – 108.

[25] (2010, August 10). Facial recognition system – Wikipedia, the free encyclopaedia [Online]. Available: http://en.wikipedia.org/wiki/Face_recognition

[26] (2010, August 10). Facial Recognition Biometrics – MIS Biometrics [Online]. Available: http://misbiometrics.wikidot.com/face

[27] *NIST, American National Standard for Information systems – Data Format for the Interchange of Fingerprint, Facial, and Scar Mark and Tattoo (SMT) Information*, ANSI-ITL 1- 2000 (NIST Special Publication 500-245), September 2000.

[28] R. Brunelli and T. Poggio, “Face Recognition: Features Versus Templates,” in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 10, October 1993, pp. 1042 -1052.

[29] P. S. Penev, “Local Feature Analysis: A Statistical Theory for Information Representation and Transmission,” PhD thesis, The Rockefeller University, 1998.

[30] B. Victor, K. W. Bowyer, and S. Sarkar, “An Evaluation of Face and Ear Biometrics,” in *Proceedings of the International Conference on Pattern Recognition*, August 2002, pp. I: 429 – 432.

[31] M. Kirby and L. Sirovich, “Application of the Karhunen-Loève Procedure for the Characterisation of Human Faces,” in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12, no. 1, January 1990, pp. 103 – 108.

[32] L. Sirovich and M. Kirby, “Low – Dimensional Procedure for the Characterisation of Human Faces,”*Optical Society of America*, vol. 4, 1987, pp. 519 – 524.

[33] (2010, August 10). Iris Recognition – Wikipedia, the free encyclopaedia [Online]. Available: http://en.wikipedia.org/wiki/Iris_recognition