UNIVERSITY OF MAURITIUS RESEARCH JOURNAL – Volume 16 – 2010
University of Mauritius, Réduit, Mauritius

Research Week 2009/2010

Trends in Biometric Technology

Nazmeen Bibi Boodoo-Jahangeer *
(MPhil/PhD Student at Faculty of Engineering)
University of Mauritius
Reduit
Email: nazmeen182@yahoo.com

R. K. Subramanian

Sunilduth Baichoo
Faculty of Engineering
University of Mauritius
Reduit
Email: sbaichoo@uom.ac.mu

Paper Accepted on 26 July 2010

Abstract

Biometrics is playing a major role in automating personal identification system deployed to enhance security in several applications including use of passports, cellular telephones, automatic teller machines, computer systems and driver licenses. The use of biometric features for identification purposes requires that a particular biometric factor be unique for each individual, that it can be readily measured, and that it is invariant over time. When used for personal identification, biometric technologies measure and analyze human physiological and behavioural characteristics. A person's physiological characteristics are based on direct measurement of a part of the body such as, fingerprint, hand geometry, facial geometry, and eye retinas and irises. Behavioural characteristics are based on data derived from actions, such as speech and signature. The aim of this paper is to provide an overview of the field of biometrics including the current trends. The commonly-used biometrics have been evaluated and some future research directions have been identified.

Keywords: Biometric, Fingerprint, Face, Iris, Hand, Ear

**For correspondences and reprints*

1. INTRODUCTION

Security is a major issue in the modern world and valuable information ending up in the wrong hands can result in a lot of inconvenience and damage. Traditional methods used to secure valuables and restricted information include passwords, access cards, PIN codes, credit cards, keys, tokens etc. These methods however are not very secure as they are easily transferable and quite easily obtained by any third parties who want unauthorized access to valuables and information (Jain A. et al., 2001). Biometric-based methods easily deal with those problems since users are identified by who they are, not by something they have to remember or carry with them (Choraś M., 2005). Biometric traits are profoundly more difficult to forge, copy, share, misplace or guess (Pankanti, Jain 2008). Biometric system requires the person being authenticated to be present at the time and point of authentication (Pankanti, Jain 2008).

Biometrics refers “to identifying an individual based on his or her distinguishing characteristics” (Bolle et al. 2003). Some examples of common biometric modalities of current interest are Facial features, Voice characteristics, Fingerprints, Handwritten signature ,Iris patterns, Hand shape, Hand vein patterns, Keystroke dynamics, Odour, Ear shape, Gait patterns, Retinal blood vessel patterns (Fairhurst 2003).

The method of biometric identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: The person to be identified is required to be physically present at the point-of-identification or the identification based on biometric techniques obviates the need to remember a password or carry a token or a smartcard (Graevenitz G., 2003).. Along with the rapid growing of this emerging technology, the system performance, such as accuracy and speed, is continuously improved.

The paper has been organised as follows: Section 2 explains the basics of biometrics; Section 3 outlines the existing biometric technologies; Section 4 gives details about the emerging technologies in biometrics; Section 5 discusses the strengths and weaknesses of the main biometric technologies; and last sections include the Conclusion and References.

2. BIOMETRIC SYSTEM

A biometric system (Maltoni D. et al, 2003), is a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the data acquired, and comparing this feature set against the template set stored in the database. A biometric system consists of four main stages (Jain A. et al., 2006):

1. Sensor: It is an acquisition device that captures the biometric data of an individual. For example, an iris sensor images an individual's iris texture.

2. Feature extraction: It is responsible for processing the biometric data to extract a set of discriminatory features. For example, in a hand based biometric system the geometric properties of the hand image are extracted.

3. Matcher: It compares the features extracted against stored templates in the database and generates a matching score. For example, in an iris recognition system, the Iris Codes (features extracted) are compared with Iris code templates in the database. Often the matching stage includes a decision making stage based on the matching score. For example, a subject's claimed identity is confirmed or denied (verification) or a subject's identity is established (identification).

4. Database: It stores the biometric templates of the enrolled users. The enrolment process comprises of capturing the biometric data in digital form, checking the quality of the digital representation and if the quality meets the requirement then the features extracted are stored in the database as templates (compact representation of features extracted).

Any human physiological or behavioural trait can serve as a biometric characteristic as long as it satisfies the following requirements (Prabhakar S., 2003):

- *Universality*: Each person should have the characteristic.
- *Distinctiveness:* Any two persons should be different in terms of the characteristic.
- *Permanence*: The characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
- *Collectability*: The characteristic should be quantitatively measurable.

However, in a practical biometric system, there are a number of other issues that should be considered (Jain, Ross & Prabhakar 2004), including:

- *Performance*, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;

- *Acceptability*, which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;

- *Circumvention*, which reflects how easily the system can be fooled using fraudulent methods.

Biometric measurements may be categorised as either physiological or behavioural (Fairhurst 2003). The first type , examples of which include iris patterns, fingerprints etc, relate to inherent physiological characteristics of an individual, while the second type, such as handwritten signatures, keystroke dynamics, gait patterns, among others, arise from activities carried out by that individual, either those which occur spontaneously or, in some cases, those which are specifically learned. Each biometric trait has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet all of the requirements of all applications (Jain, Ross & Pankanti 2006).

An authentication procedure can be performed in two modes by a biometric system (Jain, Ross & Prabhakar 2004, Gamassi et al. 2004):

(a) Identification: This method consists in selecting the correct identity of an unknown person from a database of registered identities (Figure 1.1). It is called a “one to many” matching process, because the system is asked to complete a comparison between the person’s biometrics and all the biometric templates stored in a database.

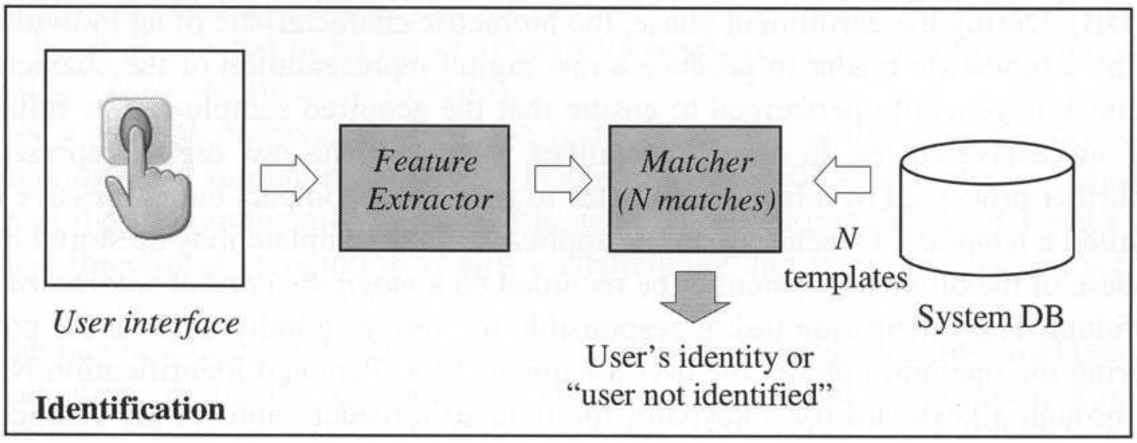

Figure: 1.1 Identification

(b) Verification: This method consists in verifying whether a person is who he or she claims to be (Figure 1.2). It is called a ”one to one” matching process, as the system has to complete a comparison between the person’s biometric and only one chosen template stored in a centralized or a distributed database.

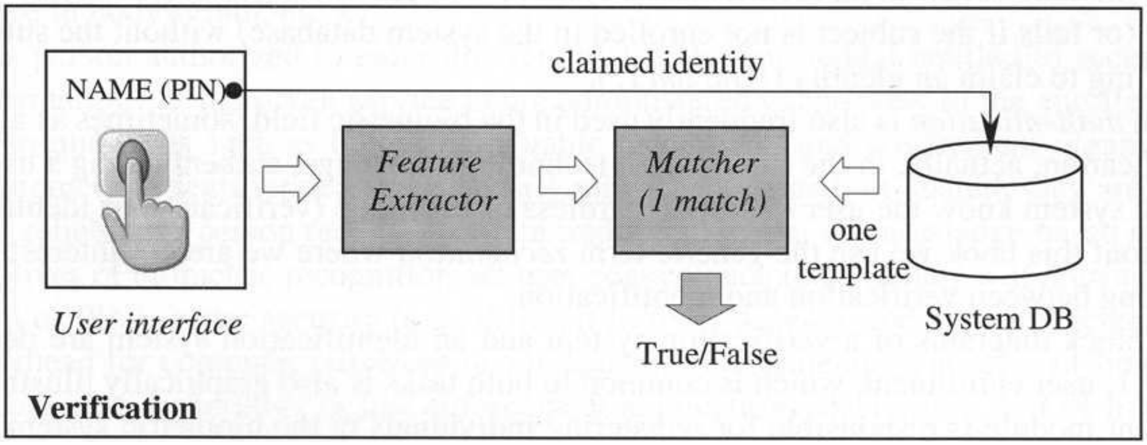

Figure: 1.2 Verification

Due to different positioning on the acquiring sensor, imperfect imaging conditions, environmental changes, deformations, noise and bad user's interaction with the sensor, it is impossible that two samples of the same biometric characteristic, acquired in different sessions, exactly coincide. For this reason a biometric matching systems' response is typically a matching score *s* that quantifies the similarity between the input and the database template representations. The higher the score, the more certain the system is that the two samples coincide (Delac & Grgic 2004). A similarity score *s* is compared with an acceptance threshold *t* and if *s* is greater than or equal to *t* compared samples belong to a same person.

Pairs of biometric samples generating scores lower than *t* belong to a different person. The distribution of scores generated from pairs of samples from different persons is called an *impostor distribution*, and the score distribution generated from pairs of samples of the same person is called a *genuine distribution*, Figure 1.3 (Delac & Grgic 2004).

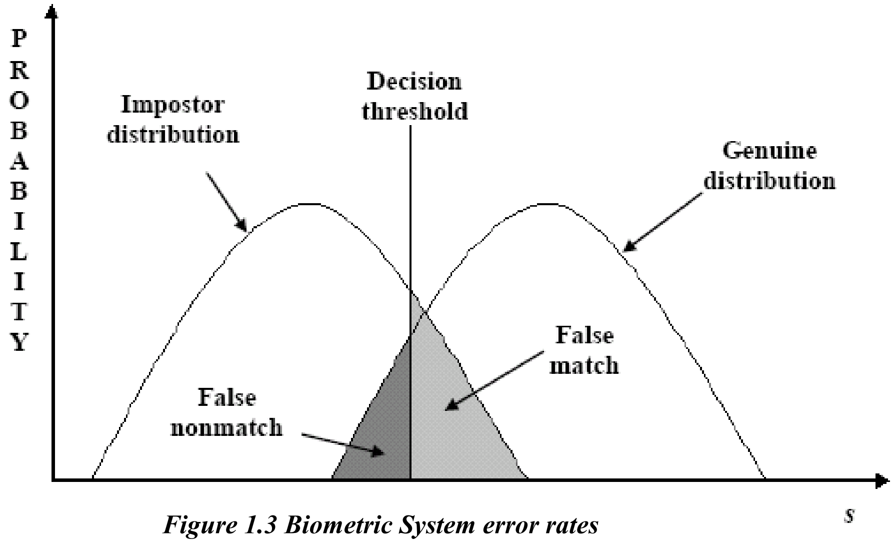

Figure 1.3 Biometric System error rates

3. BIOMETRIC TECHNOLOGIES

In this section, the existing biometric technologies are explained.

3.1 Fingerprint

Fingerprints are oriented texture patterns present on the surface of the finger consisting of interweaved ridges and valleys. At about seven months of prenatal development, fingerprints are fully formed (Maltoni D. et al, 2003). The finger ridge configuration of the individual does not naturally change. However cuts and bruises affect the ridge pattern. In context of digital images of fingerprints, the dark areas called ridges and the bright areas called valleys are the most important characteristics of the fingerprint structure. The ridge lines have a high curvature in certain regions when the fingerprint image is analyzed at a global level, lending the ridge lines a distinct shape. These regions are called singularities (Maltoni D. et al, 2003). Such singular regions can be classified into `loop', `delta' and `whorl'. Most fingerprint matching techniques align two fingerprints on the basis of a registration point called the `core', which corresponds to the centre point of the north most `loop' type singularity. For fingerprints that do not contain `loop' singularities, defining the core becomes difficult. In such cases, the `core' is associated with point of maximum ridge line curvature. Unfortunately, due to image acquisition issues and large intra class variability of fingerprints, it is difficult to define the `core' reliably.

When the fingerprint is analyzed at the local level, minutiae (small details) can be found in the fingerprint pattern. In 1892, Sir Francis Galton introduced the minutiae features for fingerprint matching. Minutia describes the discontinuity in the ridges (e.g., termination, bifurcation, crossover, spurs etc.). Some common minutiae types are shown in Figure 3.1. However, only a few of these minutiae types are used in practice due to practical difficulty in identifying the minutia type reliably. For instance, the FBI minutia model consists of only terminations and bifurcations (Maltoni D. et al, 2003). In this model, each minutia is denoted by its location in the spatial domain, and the angle between the horizontal axis and the tangent to the ridge line at the minutia location.

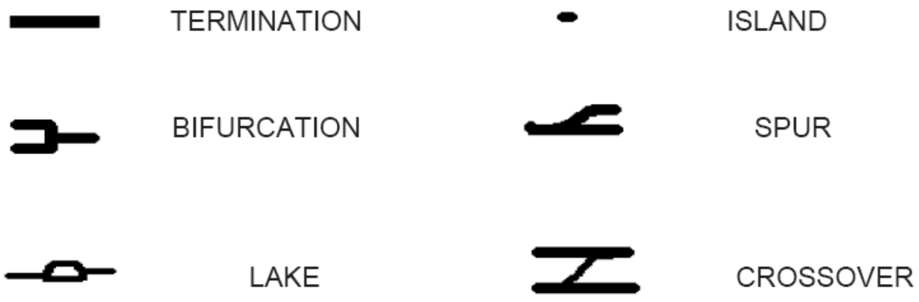

Figure 3.1: Some common minutiae types

If a fingerprint image is acquired at higher resolution, it is possible to capture the `sweat pores' present on the ridge lines. These pores have highly distinctive features like number, location, shape, etc. but the ability to extract such information is dependent on the availability of high resolution scanners and good quality fingerprint images. Figure 3.2 shows some important characteristics of fingerprints.

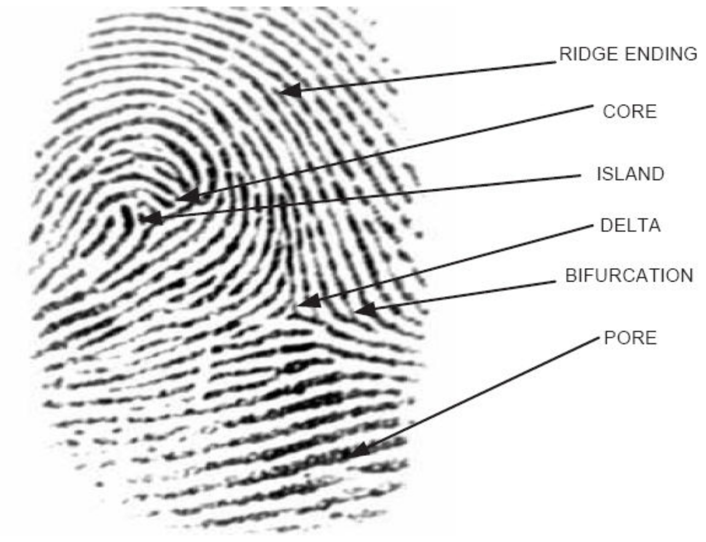

Figure 3.2: Fingerprint characteristics

On the basis of the extracted features from fingerprints, fingerprint matching can be categorized into three types namely correlation based matching, ridge feature based matching and minutiae based matching (Maltoni D. et al, 2003).

1. Correlation based matching: The fingerprint images are superimposed on each other and the correlation between the corresponding pixel intensities is computed for different alignments.

2. Minutiae based matching: This is the most popular technique whereby minutiae points are extracted from the two fingerprints to be matched and their location and ridge orientations are stored. The matching process comprises of determining the alignment between the template and input minutiae set that result in the maximum number of minutiae pairings. For low quality fingerprint images the minutiae extraction process can be difficult.

3. Ridge feature based matching: Since pixel intensities and minutiae locations are features of the ridge pattern, they can be considered to be sub-categories of the ridge features. In ridge feature based matching, the texture information, local orientation, frequency and ridge pattern are used to match two fingerprints.

3.2 Face Recognition

Face recognition is currently highly researched area of computer vision and pattern recognition (Zhao W. et al., 2003). While many algorithms are being developed, they are usually compared to existing ones quite superficially and only simple comparisons are reported. Given the numerous theories and techniques that are applicable to face recognition, it is clear that detailed evaluation and benchmarking of these algorithms is crucial. Effort done by FERET researchers in their evaluations (Phillips P. J. et al., 2000) pushed face recognition algorithm comparisons to the next level.

Research in automatic face recognition dates back at least until the 1960's (Bledsoe W., 1964). A survey of face recognition techniques has been given by Zhao et al., (2003). In general, face recognition techniques can be divided into two groups based on the face representation they use:

(a) Appearance-based, which uses holistic texture features and is applied to either whole-face or specific regions in a face image;

(b) Feature-based, which uses geometric facial features (mouth, eyes, brows, cheeks etc.) and geometric relationships between them.

Kirby and Sirovich were among the first to apply principal component analysis (PCA) to face images, and showed that PCA is an optimal compression scheme that minimizes the mean squared error between the original images and their reconstructions for any given level of compression (Kirby M. and Sirovich L., 1990). Turk and Pentland popularized the use of PCA for face recognition (Turk M. and Pentland A., 1991). They used PCA to compute a set of subspace basis vectors (which they called "eigenfaces") for a database of face images, and projected the images in the database into the compressed subspace. New test images were then matched to images in the database by projecting them onto the basis vectors and finding the nearest compressed image in the subspace (eigenspace).

Researchers began to search for other subspaces that might improve performance. One alternative is Fisher's linear discriminant analysis (LDA, a.k.a. "fisherfaces") (Swets D. and Weng J., 1996). For any N-class classification problem, the goal of LDA is to find the N-1 basis vectors that maximize the interclass distances while minimizing the intra-class distances. At one level, PCA and LDA are very different: LDA is a supervised learning technique that relies on class labels, whereas PCA is an unsupervised technique.

One characteristic of both PCA and LDA is that they produce spatially global feature vectors. In other words, the basis vectors produced by PCA and LDA are non-zero for almost all dimensions, implying that a change to a single input pixel will alter every dimension of its subspace projection. There is also a lot of interest in techniques that create spatially localized feature vectors, in the hopes that they might be less susceptible to occlusion and would implement recognition by parts. The most common method for generating spatially localized features is to apply independent component analysis (ICA) to produce basis vectors that are statistically independent (Bartlett M. S, 2001.) .

3.3 Iris Recognition

Automated iris recognition is receiving increased attention among other biometrics for non-invasive verification and identification of people. First of all, that is because of its high reliability (the probability of finding two people with identical iris pattern is almost zero); in addition compared to fingerprint or face, the iris is well protected from the environment (behind the cornea and the eyelid) and stable over time (neither subject to aging nor to variability in appearance). Like the fingerprint and the face, the iris can be acquired by a non-invasive device; moreover, differently to the other two biometric characteristics, the iris is relatively insensitive to angle of illumination, changes in viewing angle and distortions, thus it is more suitable for the creation of a size-invariant representation that makes possible an automated recognition with high degree of accuracy, based on currently available machine vision technologies.

One of the most well known systems for iris recognition is based on phase code using Gabor filters and has been developed in the first 90s by Daugman (1993) and patented by IriScan Inc. Other works proposed later are the following: Wildes et al (1996) proposed a system based on Laplacian pyramid constructed with four different resolution levels for representing iris texture and used the normalized correlation as similarity measure; Boles and Boashash (1998) used zero-crossing representation of 1-D wavelet transform for feature extraction; Sanchez-Reillo et al. (1999) used Gabor filters as feature extractor and a statistical matcher; finally Ma et al. (2002) adopted texture analysis methods to capture the iris details.

In general, the process of iris recognition can be divided into four steps (Figure 3.3):

(a) Localization of the iris
(b) Normalization of the iris to a fixed size
(c) Feature Extraction
(d) Matching

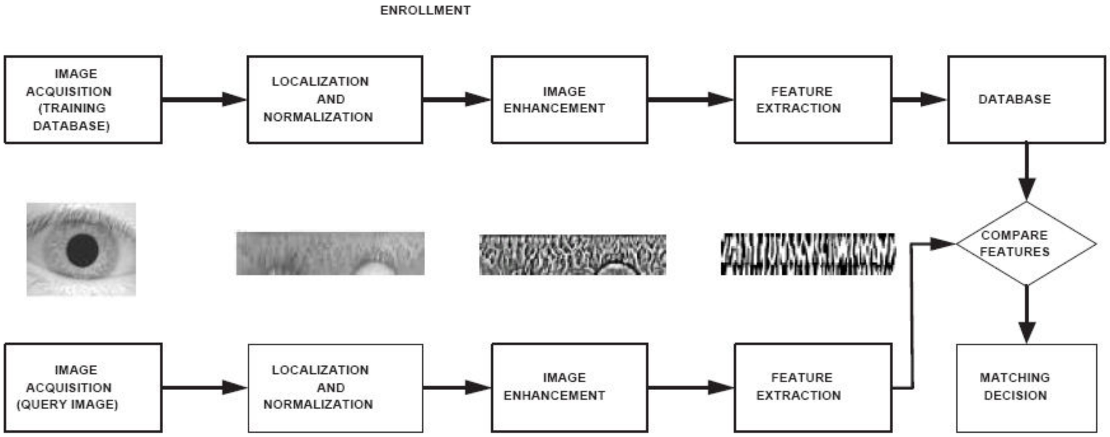
ENROLLMENT
IMAGE ACQUISITION (TRAINING DATABASE)
LOCALIZATION AND NORMALIZATION
IMAGE ENHANCEMENT
FEATURE EXTRACTION
DATABASE
COMPARE FEATURES
IMAGE ACQUISITION (QUERY IMAGE)
LOCALIZATION AND NORMALIZATION
IMAGE ENHANCEMENT
FEATURE EXTRACTION
MATCHING DECISION

Figure 3.3: A typical iris recognition system

3.4 Hand Geometry

The hand image is obtained using a camera looking from the top when the user placed his or her hand at a specified surface. The hand can be aligned using pegs or reference marks. Two views are usually taken in a single image, the top view and the side view. The side view is usually taken by the top camera as well using a side mirror. From the hand image, the fingers are located and the length, width, thickness, curvatures and their relative geometry measured.

Typical applications using hand geometry include access control where dirt, grease, ink or other debris would reduce the reliability of fingerprint identification, for example, oil refineries or manufacturing plants. Hand geometry is also widely used to control access to nuclear plants.

Hand geometry has several advantages, including: Ease of use. The technology is simple to use and has been in widespread use for many years. It does not carry the negative perceptions of fingerprints and is perceived to be less intrusive than iris and retinal scans. Most users have sufficient dexterity to easily use the devices, thus reducing user error rates. Hand Geometry is resistant to spoofing. The principal spoofing technique is a cast or latex model of a hand which is difficult to execute, particularly if simple physical security measures are in place. Other spoofing techniques such as gloves or other devices are unreliable and more likely to be rejected. Also, Hang Recognition uses small template size. Compared to other biometrics such as fingerprints, hand scan and iris scans, hand geometry is extremely small and can be accommodated on a variety of devices including magnetic stripe cards. The small template size allows fast processing, important where large volumes of users are processed. The readers of hand geometry are durable and able to process large volumes of users of several years without undue reader failure. They can also withstand wide temperature ranges and operate in hostile (such as high temperature and dusty) environments. The technology has been in use for many years and has proved reliable.

The main disadvantage of hand geometry is the cost. Hand geometry scanners are relatively large and expensive and palm and hand scanners are equally or more costly. The size of the devices precludes use in portable applications or small devices such a computer mouse. While the basic structure of the hand changes little over time, injuries, swelling or diseases such as arthritis can obscure this structure and cause recognition difficulties. It is interesting to note that students need re-enrolment once or twice in their scholastic lives to accommodate growth. Hand geometry is not sufficiently distinctive to allow 1-to-many searches and is generally limited to 1-to-1 authentication uses. It’s use is therefore limited to identity verification rather than identification of an individual from a database. This is, however, considered and advantage by privacy advocates. Hygiene is another issue arising from multiple users touching the reader.

3.5 Voice

Voice authentication or speaker recognition uses a microphone to record the voice of a person. The recorded voice is digitised and then used for authentication. The speech can be acquired from the user enunciating a known text (text dependent) or speaking (text independent). In the former case, the text can be fixed or prompted by the system. The text can also be read discretely or the entire text read out continuously. The captured speech is then enhanced and unique features extracted to form a voice template. There are two types of templates: stochastic templates and model templates. Stochastic templates require probabilistic matching techniques such as the popular Hidden Markov Model and results in a measure of likelihood of the observation given the template. For model templates, the matching techniques used are deterministic. The observation is assumed to be similar to the model, albeit some distortion. Matching result is obtained by measuring the minimum error distance when the observation is aligned to the model. The matching techniques popularly used for model templates include Dynamic Time Warping algorithm, Vector Quantisation and Nearest Neighbours algorithm (Campbell J. P., 1997).

As voice is a common means of communication, and with an extensive telephone network, a microphone becomes rather common and as such the cost of voice authentication can be very low and compact. Furthermore, it is relatively easy to use. However, voice varies with age and there can be drastic change from childhood to adolescence. Also illness and emotion may affect the voice as well as room acoustics and environmental noise. Variation in microphones and channel mismatch (use of different type and quality of microphones) is also a major problem for the widespread use of this biometric technology.

3.6 Palm

As with finger, palms of hands and soles of feet have epidermal ridges, thought to provide a friction surface to assist with gripping and object of surface. The biometric use of palm prints uses ridge patterns to identify an individual. Similar in many respects to fingerprint identification, palm print identification systems measure and compare ridges, lines and minutiae found on the palm.

The are three groups of marks which are used in palmprint identification (Wei Shu and David Zhang, 2009):

(a) Geometric features, such as the width, length and area of the palm. Geometric features are a coarse measurement and are relatively easily duplicated. In themselves they are not sufficiently distinct;

(b) Line features, principal lines and wrinkles. Line features identify the length, position, depth and size of the various lines and wrinkles on a palm. While wrinkles are highly distinctive and are not easily duplicated, principal lines may not be sufficiently distinctive to be a reliable identifier in themselves; and

(c) Point features or minutiae. Point features or minutiae are similar to fingerprint minutiae and identify, amongst other features, ridges, ridge endings, bifurcation and dots. Palm creases and ridges are often superimposed which can complicate feature extraction

As with fingerprint recognition, there are three principal palm matching techniques. These are:

(a) Minutiae-based matching, the most widely used technique,
(b) Correlation-based matching, and
(c) Ridge-based matching.

Palm Recognition encounters certain reading difficulties. Where users hands do not fully contact the palm readers, there made be some difficulty in obtaining a clear image. A complicating factor here is a change in scale caused by increasing or varying the distance between the reader and palm. Another difficulty is in capturing a clear image of the hollow of the palm which may not fully contact the reader. Other difficulties have been caused by shifting position, closing fingers or placing the hand on different parts of the reader when registering.

3.7 Retina

Retinal scans measure the blood vessel patterns in the back of the eye. The device involves a light source shined into the eye of a user who must be standing very still within inches of the device. Because users perceive the technology to be somewhat intrusive, retinal scanning has not gained popularity; currently retinal scanning devices are not commercially available.

3.8 Signature

The use of written signature as a means to acknowledge the identity of a person has been used for long. Dynamic signature verification is an automated method of measuring an individual’s signature. This technology examines such dynamics as speed, direction, and pressure of writing; the time that the stylus is in and out of contact with the paper, the total time taken to make the signature; and where the stylus is raised from and lowered onto the paper.

3.9 DNA

DNA sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample. This method of capture still has to be refined. So far, DNA analysis has not been sufficiently automatic to rank it as a biometric technology. The analysis of human DNA is now possible within 10 minutes. If the DNA can be matched automatically in real time, it may become more significant. At present, DNA is very entrenched in crime detection and will remain in the law enforcement area for the time being

4. EMERGING TRENDS

Emerging trends in biometric technologies use diverse physiological and behavioural characteristics and are in various stages of development. Each technique's performance can vary widely, depending on how it is used and its environment in which it is used.

4.1 Vein Pattern

Vein pattern identification uses an infrared light source to scan for haemoglobin in the blood. De-oxygenated haemoglobin appears as a black pattern with the hand or finger showing as a lighter colour or white. The device then captures an image of vein patterns in wrist, palm, back of the hand, finger or face. This is similar to the technique used to capture retinal patterns. The backs of hands and palms have a more complex vascular patterns than fingers and provide more distinct features for pattern matching and authentication.

As with other biometric identification approaches, vein patterns are considered to be time-invariant and sufficiently distinct to clearly identify an individual. The difficulty is that veins move and flex as blood is pumped around the human body

The main advantage of vein pattern biometrics is that it is perceived as secure as it incorporated “liveness” detection. Being contact less, it is also perceived as being hygienic and does not carry the stigma associated with fingerprints. The human vascular structure is individually distinct. Even identical twins have different and distinct vascular patterns. Vein patterns are not easily spoofed, observed, damaged, obscured or changed. Vein pattern recognition requires simple low resolution imaging devices. The technology is reliable in that is shows little performance degradation in harsh environments, such as mines, manufacturing and construction sites as well as heavy traffic areas such as schools, military bases and dormitories.

4.2 Keystroke Dynamics

Keystroke dynamics is an automated method of examining an individual’s keystrokes on a keyboard. This technology examines such dynamics as speed and pressure, the total time taken to type particular words, and the time elapsed between hitting certain keys. This technology’s algorithms are still being developed to improve robustness and distinctiveness. One potentially useful application that may emerge is computer access, where this biometric could be used to verify the computer user’s identity continuously.

4.3 Nail bed identification

This technology is based on the distinct longitudinal, tongue-in-groove spatial arrangement of the epidermal structure directly beneath the fingernail. This structure is mimicked in the ridges on the outer surface of the nail. When an interferometer is used to detect phase changes in back-scattered light shone on the fingernail, the distinct dimensions of the nail bed can be reconstructed and a one-dimensional map can be generated.

4.4 Gait

Gait is an attractive biometric feature for human identification at a distance. Human Gait is a spatio-temporal phenomenon and typifies the motion characteristics of an individual (Nandini C. and Ravi Kumar C. N., 2008). A person's gait can be hard to disguise because a person's musculature essentially limits the variation of motion. Compared with traditional biometric features, such as face, iris, plam print and finger print, gait has many unique advantages such as non-contact, non-invasisve and perceivable at a distance. Several algorithms have been proposed for gait recognition. However, there is a need to evaluate them to variations such as view angle, clothing, shoe types, carrying conditions, illumination and time.

4.5 Lip

Human Lip recognition is an interesting emerging method of human identification that originated from the criminal and forensic practice. Abdulla et al. (2009) have used Lip Tracking to enhance Speaker recognition system. While the person is speaking, visual images are extracted from a sequence of the speaker’s lips. The shape and the pixel intensities around the edge of the lips are the required features. A recognition rate of 82.8 % for speaker identification was achieved.

4.6 Facial, hand, and hand vein infrared thermogram:

According to A. K. Jain et al. (2004), the pattern of heat radiated by human body is a characteristic of an individual and can be captured by an infrared camera in an unobtrusive way much like a regular photograph. The technology could be used for covert recognition. The advantages of facial thermography over other biometric technologies are that it is not intrusive, no physical contact is required. Every living person presents a usable image, and the image can be collected on the fly. Also, unlike visible light systems, infrared systems work accurately even in dim light or total darkness. Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermograms.

4.7 Odour

Each object exudes an odour that is characteristic of its chemical composition and this could be used for distinguishing various objects (A. K. Jain et al. 2004). The body odour biometrics is based on the fact that virtually every human’s smell is unique. The smell is captured by sensors that are capable of obtaining the odour from non-intrusive parts of the body, such as the back of the hand. The scientific basis is that the chemical composition of odours can be identified using special sensors. Each human smell is made up of chemicals known as volatiles. They are extracted by the system and converted into a template. The use of body odour sensors broaches on the privacy issue, as the body odour carries a significant amount of sensitive personal information. It is possible to diagnose some disease or activities in last hours by analyzing body odour.

4.8 Blood pulse

Blood pulse biometrics measure the blood pulse on a finger with infrared sensors. This technology is still experimental and has a high false match rate, making it impractical for personal identification.

4.9 Skin elements

The exact composition of all the skin elements is distinctive to each person. For example, skin layers differ in thickness, the interfaces between the layers have different undulations, pigmentation differs, collagen fibres and other proteins differ in density, and the capillary beds have distinct densities and locations beneath the skin. Skin pattern recognition technology measures the characteristic spectrum of an individual's skin. A light sensor illuminates a small patch of skin with a beam of visible and near-infrared light. The light is measured with a spectroscope after being scattered by the skin. The measurements are analyzed, and a distinct optical pattern can be extracted.

4.10 Multi- biometrics

Although most biometric systems deployed in real-world applications are unimodal, so they rely on the evidence of a single source of information for authentication, these systems have to contend with a variety of problems such as noise in sensed data, intra-class variations, inter-class similarities, non-universality, and spoof attacks. Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. These systems allow the integration of two or more types of biometric systems. Integrating multiple modalities in user verification and identification leads to high performance (Jain A.K., Ross A., 2004).

Integration of information in a Multimodal biometric system can occur in three main levels, namely feature level, matching level or decision level (Ross A., Jain A.K., 2004). At feature level, the feature sets of different modalities are combined. Fusion at this level provides the highest flexibility but classification problems may arise due to the large dimension of the combined feature vectors. Fusion at matching level is the most common one, whereby the scores of the classifiers are usually normalized and then they are combined in a consistent manner. At fusion on decision level each subsystem determines its own authentication decision and all individual results are combined to a common decision of the fusion system.

4.11 Ear

Ear recognition has received considerably less attention than many alternative biometrics, including face, fingerprint and iris recognition. Ear-based recognition is of particular interest because it is non-invasive, and because it is not affected by environmental factors such as mood, health, and clothing (Saleh M. et al., 2006). Also, the appearance of the auricle (outer ear) is relatively unaffected by aging, making it better suited for long-term identification.

The main drawback of ear biometrics is that they are not usable when the ear of the subject is covered (A. Iannarelli, 1989). In the case of active identification systems, this is not a drawback as the subject can pull his hair back and proceed with the authentication process. The problem arises during passive identification as in this case no assistance on the part of the subject can be assumed. In the case of the ear being only partially occluded by hair, it is possible to recognize the hair and segment it out of the image.

5. EVALUATION OF BIOMETRIC TECHNOLOGIES

There is no single biometric technology that can serve all applications. Each biometric has its own strengths and weaknesses as shown in Table 5.1, while Table 5.2 (Anil K. et al., 2006) shows the comparison of the commonly-used biometric technologies.

Technology	Strengths	Weaknesses
Fingerprint	• Subjects have multiple fingers. • Easy to use, with some training • Some systems require little Space. • Large amounts of existing data to allow background and/or watchlist checks. • Has proven effective in many large scale systems over years of use. • Fingerprints are unique to each finger of each individual and the ridge arrangement remains permanent during one's lifetime.	• Privacy concerns of criminal implications • Health or societal concerns with touching a sensor used by countless individuals • Collection of high quality nail-to-nail images requires training and skill, but current flat reader technology is very robust • An individual's age and occupation may cause some sensors difficulty in capturing a complete and accurate fingerprint image
Face	• No contact required • Commonly available sensors (cameras) • Large amounts of existing data to allow background and/or watchlist checks • Easy for humans to verify results	• Face can be obstructed by hair, glasses, hats, scarves,etc. • Sensitive to changes in lighting, expression, and pose • Faces change over time • Propensity for users to provide poor-quality video images yet to expect accurate results
Iris	• No contact required	• Difficult to capture for some

	• Resistance to false matching • Protected internal organ; less prone to injury • Believed to be highly stable over lifetime	individuals • Easily obscured by eyelashes, eyelids, lens and reflections from the cornea • Public myths and fears related to “scanning” the eye with a light source • Acquisition of an iris image requires more training and attentiveness than most biometrics • Cannot be verified by a human
Voice	• Public acceptance • No contact required • Commonly available sensors (telephones, microphones) • Synergy with speech recognition	• Difficult to control sensor and channel variances that significantly impact capabilities • Perception of low accuracy • Large template size
Hand Geometry	• Easy to capture • Believed to be a highly stable pattern over the adult lifespan • Ability to operate in challenging environment	• Use requires some training • Not sufficiently distinctive for identification over large databases • System requires a large amount of physical
Signature	• Resistant to impostors • Leveraging existing processes, supplement to the standard signing process • Perceived as non-invasive • Users can change signatures, other biometrics cannot be changed	• Inconsistent signatures lead to increased error rates • Limited applications
Keystroke	• Leverages existing	• Retains many flaw of

	hardware • Leverages common authentication process in addition to password creation • Username and passwords can be changed	password-based system

Table 5.1: Strengths and weaknesses of biometric systems

Biometric Technology	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
Facial Thermograms	High	High	Low				

Table 5.2 Comparison of biometric technologies

Future Research Directions

Performance

The Performance of a biometric system is crucial for its implementation in commercial applications. All biometric systems exhibit non-zero error rates (Ross et al., 2006). Thus, more research works need to be done in this direction to make biometric systems having negligible error rates.

Biometric Template Security

Though biometric is more reliable than passwords, there is the concern that it violates the privacy and personal rights of individuals. These issues include possibility of fraud and identity theft. The problem here is that once a biometric trait has been compromised, it has been compromised forever, that is it cannot be ever used. It is important to find proper ways in storing the biometric traits.

Emerging Traits

As mentioned above, there are many new biometric technologies that are under development. There is a need to evaluate their effectiveness as biometric and make a comparison with the existing state-of-art biometric technologies.

New Databases

There are just a few databases exist for experimentation. Examples include FERET face database, NIST fingerprint database and CASIA iris database, among others. However, there is a need of standard databases for many biometric traits, especially for the emerging biometric technologies.

Multi-biometric systems

Though several multi-biometric systems have been developed by researchers to increase system performance, there are not yet commercial applications developed yet. There is a need to evaluate the multi-biometric systems on common dataset to test their reliability for commercial applications.

6. CONCLUSION

Biometric authentication is the use of physiological characteristics such as a fingerprint, hand shape, face map, voice, or iris to determine the identification of the user. This type of identification is more reliable in comparison to traditional verification methods such as possession of a key or swipe card, or the knowledge of a password or login, because the person is required to be physically present at the time of identification. Reliable personal identification is important in everyday transactions ranging from ATM withdrawals to restricted building access.

This paper has given an overview of the different biometric technologies, including the technologies still under development. Also, the strengths and weaknesses of commonly-used biometrics have been outlined. Lastly, some future research directions have been proposed.

REFERENCES

ABDULLA, W. H., YU, P. W. T., CALVERLY, P. (2009), Lips Tracking Biometrics For Speaker Recognition, *International Journal of Biometrics*, Vol. 1, No. 3, pp 288-306

ANIL K. J., ARUN R., SHARATH P. (2006) Biometrics: A Tool for Information Security, *IEEE Transactions on Information Forensics and Security*, Vol. 1, No.2.

BARTLETT, M. S. (2001) *Face Image Analysis by Unsupervised Learning*. Kluwer Academic Publishers.

BLEDSOE, W. W. (1964). *The model method in facial recognition*, Technical Report, PRI 15, Panoramic Research, Inc., Palo Alto, California.

BOLES, W., & BOASHASH, B. (1998). A human identification technique using images of the Iris and Wavelet transform, *In: Proceedings of IEEE Transactions on Signal Processing*, Vol. 46, No. 4, pp. 1185-1188.

BOLLE, R. M., CONNELL, J. H., PANKANTI, S., RATHA, N. K. & SENIOR, A. W. (2003). *Guide to Biometric*: Springer-Verlag, New-York.

BOODOO B. N. & SUBRAMANIAN R. K. (2009). Robust Multi-biometric Recognition Using Face and Ear Images*, International Journal of Computer Science and Information Security*, Volume 6 No.2, pp. 164-169.

CAMPBELL, J.P. (1997). Speaker Recognition: A Tutorial. Proceedings *of The IEEE*, Vol. 85, No. 9, pp. 1437 - 1462.

DAUGMAN, J. (1993), High confidence visual recognition of persons by a test of statistical independence, *In: IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148-1161.

DELAC K., GRGIC M. (2004), A Survey Of Biometric Recognition Methods. *In: 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June, Zadar, Croatia*

FAIRHURST, M.C. (2003), Document Identity, Authentication and Ownership The Future of Biometric Verification. *In: Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR 2003),* vol. 2, pp. 1108-1116.

GAMASSI, M., LAZZARONI, M., MISINO, M., PIURI, V., SANA, D. & SCOTTI F. (2004), Accuracy and Performance of Biometric Systems. *In: Instrumentation and Measurement Technology Conference, Como, Italy, 18-20 May*.

GRAEVENITZ, G.A.V. (2003), *Introduction to Fingerprint technology*, Bergdata Biometrics GmbH, Bonn, Germany published in A&S International, Volume 53, Taipei, pp. 84-86

IANNARELLI, A. (1989). *Ear Identification. Forensic Identification Series*. Paramont Publishing Company, Fremont, California.

JAIN, A. K., ROSS, A. & PANKANTI, S. (2006). Biometrics: A Tool for Information Security. *In: Proceedings of IEEE Transactions on Information Forensics and Security,* Vol. 1, No. 2, pp. 125-143.

JAIN, A., ROSS, A., PRABHAKAR, S. (2001), Fingerprint Matching Using Minutiae and Texture Features. *In: Proceedings of the International Conference on Image Processing*, pp 282-285, Thessaloniki, Greece.

JAIN, A.K., ROSS, A. & PRABHAKAR, S. (2004), An introduction to biometric recognition*. In: Proceedings of IEEE Transactions on Circuits and Systems for Video Technology*, Special Issue on Image- and Video-Based Biometrics, vol. 14, no. 1, pp. 4–20.

KIRBY, M. & SIROVICH, L.(1990). Application of the Karhunen-Loeve Procedure for the Characterization of Human Faces. *In: Proceedings of IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 12, pp. 103-107.

MA, L., WANG, Y., & TAN, T. (2002). Iris recognition based on multichannel Gabor filtering. *In: Proceedings of the 5th Asian Conference on Computer Vision*, pp. 279-283.

MALTONI, D., MAIO, D., JAIN, A. K. & PRABHAKAR, S. (2003), *Handbook of fingerprint recognition*, 1st ed. New York, Berlin Heidelberg: Springer-Verlag, 2003

MRAK, M., GRGIĆ, S., GRGIĆ, M. (2003). Picture Quality Measures in Image Compression Systems. *In: Proceedings of the Eurocon 2003 conference*, pp. 233-237, Ljubljana, Slovenia.

NANDINI, C. & RAVI KUMAR, C. N. (2008), Comprehensive framework to gait recognition, *International Journal of Biometrics*, Vol. 1, No.1, pp. 129 – 137.

PANKANTI, S. & JAIN, A. K. (2008), *Beyond Fingerprinting*, Scientific American, pp. 78-81.

PHILLIPS, P.J., MOON, H., RIZVI, S.A., RAUSS, P.J. (2000). The FERET Evaluation Methodology for Face Recognition Algorithms, *In: Proceedings* *of IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 22, No. 10, pp. 1090-1104

PRABHAKAR, S., PANKANTI, S. & JAIN, A. K. (2003), Biometric Recognition: Security and Privacy Concerns, *IEEE Security and Privacy Magazine*, Vol. 1, No. 2, pp. 33-42

ROSS, A., JAIN, A.K. (2004). Multimodal Biometrics: An Overview. *In: Proceedings of the 12th European Signal Processing Conference (EUSIPCO), Vienna, Austria*, pp. 1221 - 1224.

SANCHEZ-REILLO, R., SANCHEZ-AVILA, C., & MARTIN-PEREDA, J. A. (1999). Minimal template size for iris recognition, *In: Proceedings of the First Joint BMES/EMBS Conference*, Vol. 2, pp. 972.

ROSS, A., NANDAKUMAR, K., JAIN, A.K. (2006), Handbook of Multibiometrics, Springer.

SHU, W. & ZHANG, D. (2009) Palmprint Verification: An implementation of Biometric Technology, Retrieved on 26 February 2009, From: http://ccrma.stanford.edu/~jhw/bioauth/palm/00711120.pdf,

SWETS, D. & WENG, J. (1996). Using Discriminant Eigenfeatures for Image Retrieval. *In: IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 18, pp. 831-836.

TURK, M., & PENTLAND, A. (1991). Eigenfaces for Recognition, *Journal of Cognitive Neuroscience*, Vol. 3, pp. 71-86.

WILDES R., ASMUTH J., GREEN G., HSU S., KOLCZYNSKI R., MATEY J., & MCBRIDE S. (1996), A machine-vision system for Iris recognition. *Machine Vision and Applications*, pp. 1-8.

ZHAO, W., CHELLAPPA, R. PHILLIPS, J., &. ROSENFELD, A. (2003). Face Recognition in Still and Video Images: A Literature Survey, *ACM Computing Surveys*, Vol. 35, pp. 399-458.