Biometrics: An Overview of the Technology, Issues and Applications

S. Asha
Department of Computer Science & Engineering
Anna University, Chennai

C. Chellappan
Department of Computer Science & Engineering
Anna University, Chennai

ABSTRACT
Biometric identification refers to identifying an individual based on his/her distinguishing physiological and/or behavioral characteristics. As these characteristics are distinctive to each and every person, biometric identification is more reliable and capable than the traditional token based and knowledge based technologies differentiating between an authorized and a fraudulent person. This article discusses the various biometric technologies, the advantages and disadvantages of biometric technologies, the security issues and finally the applications of various biometric technologies in day today life.

Keywords: biometrics, security, identification, applications, issues, technologies.

1. INTRODUCTION
In the ever-changing world of global data communications, inexpensive Internet connections, and fast-paced software development, security is becoming more and more of an issue. Hence it has become more vital to protect the critical infrastructure and provide security for the smooth functioning of the computing solutions from the attackers. One of the ways of protecting is by providing access control to the existing infrastructure. This can be achieved by providing authentication schemes such as secure login with the help of user name and password, pass phrase, smart cards, PIN numbers, biometrics, etc.,

A biometric system is essentially a pattern recognition system that makes use of biometric traits to recognize individuals. The objective is to establish an identity based on 'who you are or what you produce', rather than by 'what you possess' or 'what you know'. The significance of using biometrics has been reinforced by the need for large scale identity management systems. The very purpose of identity management is to accurately determine an individual's identity in the context of several different applications. This new technique not only provides enhanced security but also avoids, in authentication the need to remember several passwords and maintain multiple authentication tokens.

1.1 History of Biometrics
Biometrics is not a new concept; it is the oldest form of identification. Bertillon Systems (1882) took subject's photography, height, the length of one-foot, an arm and index finger. FBI setup a fingerprint identification division in the year 1924. By 1926, law enforcement officials in several U.S. cities had begun submitting fingerprint cards to the FBI in an effort to create a database of fingerprints from known criminals. In the early 1960's the FBI invested a large amount of time and effort into the development of automated fingerprint identification systems. This automation of biometric identification for law enforcement purposes coincided with the development of automated systems for non-forensic applications, such as high-security access control. AFIS installed in 1965 with a database of 810,000 fingerprints. During the 1970's a biometric product based on measuring the geometry of the hand was introduced in a number of access control applications. First face recognition paper was published in the year 1972 (Goldstein et al).

Interest in biometric identification eventually moved from measuring characteristics of the hand to include characteristics of the eye. In the mid-1980's the first system that analyzed the unique patterns of the retina was introduced while, concurrently, work was being performed to analyze iris patterns. In the 1990's, research continues on developing identification systems based on a wide variety of biometric patterns, such as the traditional biometrics mentioned above (i.e. fingerprint, hand geometry, iris, and retina), along with the development of voice, signature, palm print, and face recognition systems. A few new, innovative approaches are also being examined for biometric analysis, such as ear shape, DNA, keystroke (typing rhythm), and body odor.

The computer industry began using biometrics few years ago. However, as with the first computers, biometric systems were massive. Typically created for a specific function, they lacked the adaptability required to integrate into a variety of environments. This resulted in costly solutions that few were able or willing to incorporate. However, over time, as technology advanced and networking and device standards were created, biometric solutions evolved to be widely recognized as viable options to security solutions (Heath, role). Fraud, security breaches, and human administrative error are helping drive the expansion of biometric technology [11].

Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to moderate access to restricted systems. However, security can be easily breached in these systems when a password is revealed to an unauthorized user or an impostor steals a card. Furthermore, simple passwords are easy to guess (by an impostor) and difficult passwords may be hard to recall (by a legitimate user).

The emergence of biometrics has addressed the problems that plague traditional verification methods. Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person [14]. By using biometrics it is possible to establish an identity based on `who you are', rather than by `what you possess' (e.g., an ID card) or `what you remember' (e.g., a password). Current biometric systems make use of fingerprints, hand geometry, iris, retina, face, facial thermograms, signature, gait, palm print and voiceprint to establish a person's identity. While biometric

systems have their limitations they have an edge over traditional security methods in that they cannot be easily stolen or shared. Besides strengthening security, biometric systems also enhance user convenience by alleviating the need to design and remember passwords.

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security [7]. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics is set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and cost effective.

There is a variety of means for identifying a person's identity:

- appearance (how the person looks, e.g. height, gender, weight)
- social behavior (how a person interacts with others)
- name (what the person is called)
- codes (what a person is called by an organization)
- knowledge (what the person knows)
- possession (what the person owns)
- bio-dynamics (what the person does)
- natural physiology (who the person is, e.g. facial characteristics)
- Imposed physical characteristics (what the person is now, e.g. tags, collars, bracelets)

The goal of authentication is to protect a system against unauthorized use. This feature enables also the protection of subscribers by denying the possibility for intruders to impersonate authorized users.

Authentication procedures are based on the following approaches [6]:

- Proof by Knowledge. The verifier known information regarding the claimed identity that can only be known or produced by a principal with that identity (e.g. passport, password, personal identification number (PIN), questionnaire)
- Proof by Possession. The claimant will be authorized by the possession of an object (e.g. magnetic card, smart card, optical card)
- Proof by Property. The claimant directly measures certain claimant properties using human characteristics (e.g. biometrics)

1.2. Biometric Data

Biometric data is different than a password that can be guessed or changed because it relies on a physical or behavioral characteristic of a person. In order for a biometric system to function well, the qualities of the data taken need to be such that all users of the system can be uniquely identified. Fundamental and secondary qualities are listed below.

1.3. Fundamental Qualities

Universality – Must be some trait that can be taken from many people

Uniqueness – Unique per person; quality must not occur in two different individuals

Permanence – Quality must be constant over time (eliminates need for re-enrollment)

Collectability – Characteristic must be able to be measured quantitatively

1.4. Secondary Qualities

- Performance – How well the biometric balances the various requirements of the systems
- Acceptability – The acceptance of the users to present the biometric data
- Circumvention – How easy it is to fool the system

1.5. Biometric System

All biometric systems consist of three basic elements:

- Enrollment, or the process of collecting biometric samples from an individual, known as the enrollee, and the subsequent generation of template.
- Templates, or the data representing the enrollee's biometric.
- Matching, or the process of comparing a live biometric sample against one or many templates in the system's database.

1.5.1 Enrollment

Enrollment is the first stage for biometric authentication because enrollment generates a template that will be used for all subsequent matching. Figure 1 shows the enrollment process.

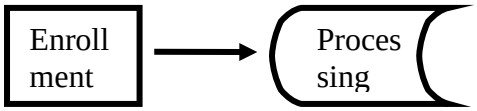


Figure 1 Capturing a biometric sample

Typically, the device takes three samples of the same biometric and averages them to produce an enrollment template. Enrollment is complicated by the dependence of the performance of many biometric systems on the users' familiarity with the biometric device because enrollment is usually the first time the user is exposed to the device. Environmental conditions also affect enrollment. Enrollment should take place under conditions similar to those expected during the routine matching process. In addition to user and environmental issues, biometrics themselves change over time. Many biometric systems account for these changes by continuously averaging. Templates are averaged and updated each time the user attempts authentication.

1.5.2 Templates

As the data representing the enrollee's biometric, the biometric device creates templates. The device uses a proprietary algorithm to extract "features" appropriate to that biometric from the enrollee's samples. Figure 2 shows the

process of storing a sample in a database. Templates are only a record of distinguishing features, sometimes called minutiae points, of a person's biometric characteristic or trait.

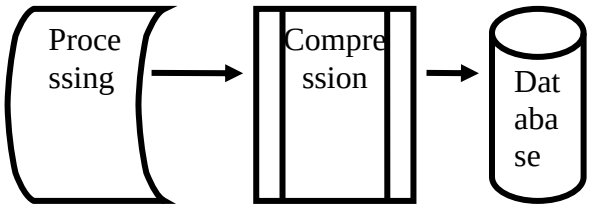


Figure 2 Compression of a biometric sample and storing it in a database

For example, templates are not an image or record of the actual fingerprint or voice. In basic terms, templates are numerical representations of key points taken from a person's body. The template is usually small in terms of computer memory use, and this allows for quick processing. The template must be stored somewhere so that subsequent templates, created when a user tries to access the system using a sensor, can be compared.

1.5.3 Matching

Matching is the comparison of two templates, the template produced at the time of enrollment with the one produced "on the spot" as a user tries to gain access by providing a biometric via a sensor. Figure 3 shows the extraction of live scan and compares it with the biometric template stored in a database to find a match in the stored template

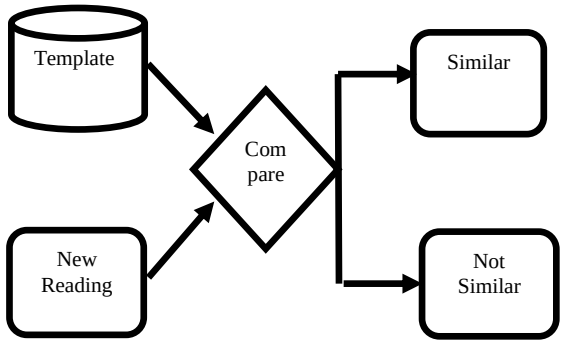


Figure 3 Comparison and evaluation of a biometric sample

There are three ways a match can fail:

- Failure to enroll.
- False match.
- False nonmatch.

Failure to enroll (or acquire) is the failure of the technology to extract distinguishing features appropriate to that technology.

In addition, the possibility of a false match (FM) or a false nonmatch (FNM) exists. These two terms are frequently misled "false acceptance" and "false rejection," respectively, but these terms are application-dependent in meaning. FM and FNM are application-neutral terms to describe the matching process between a live sample and a biometric template. A false match occurs when a sample is incorrectly matched to a template in the database (i.e., an imposter is accepted). A false non-match occurs when a sample is incorrectly not matched to a truly matching template in the database (i.e., a legitimate match is denied). Rates for FM and FNM are calculated and used to make tradeoffs between security and convenience. For example, a heavy security emphasis errs on the side of denying legitimate matches and does not tolerate acceptance of imposters. A heavy emphasis on user convenience results in little tolerance for denying legitimate matches but will tolerate some acceptance of imposters.

1.6. Biometric Systems – Types and Process

All biometric systems fall under two categories, which are familiar to those involved in security systems: identification and verification. The process, applications, and challenges are unique for both these categories because of the system-level differences that exist. An identification system is sometimes referred to as "1:N Matching" because a user presents biometric data to the system and the system attempts to identify if the user is enrolled in the system and who the person is. A verification system is referred to as "1:1 Matching" because a person makes a claim to his or her identity, presents biometric data, and the system compares the presented biometric data to the data on file only for the claimed identity. A helpful way to distinguish between these two types of authentication is the two different questions that users are essentially asking: in identification, "Who am I?"; in verification, "Am I who I claim to be?

The process of using a biometric system is designed to be as transparent as possible. To understand what occurs during the verification or identification process, a few sub-processes need to be defined. Presentation is where the user physically presents to the biometric system the data required for capture, such as a fingerprint, iris, or hand.

Enrollment is the process when a user is initially registered for access to a system. This requires the user to present his or her biometric data (fingerprint, iris, hand, etc.) so that a template can be formed in the system. This template will serve as a basis for comparison when attempting to gain access at later times. Since the template will be used many times in the future, the quality of the biometric data acquired during this stage is critical. This stage of using a biometric system can be the most tedious.

Feature Extraction is an automated process of locating and encoding distinctive characteristics from biometric data to generate a template.

Table 1 Common Biometric Technology

Characteristic	Method	Performance factors	User acceptance	Acquisition Device
Finger prints	Patterns of fingertips are captured and compared	Dryness, dirt, worn, aged fingertips	Medium	Desktop peripheral, PCMCIA card, mouse, chip or reader embedded in keyboard
Face	Facial features are captured and compared	Lighting, age, glasses, hair, environment	Medium	Video camera, PC camera, single-image camera
Retina	Patterns of blood vessels on retina are captured and compared	Glasses, difficult to use	Low	Proprietary desktop or wall-mountable unit
Iris	Patterns of iris are captured and compared	Poor Lighting, movement	High	Infrared-enabled video camera, PC camera
Voice	Cadence, pitch, and tone of vocal tract are captured and compared	Noise, colds, weather, age, equipment, environment	High	Microphone, telephone
Hand Geometry	Dimensions of hand and fingers are measured and compared	Hand injury, age, jewelry	High	Proprietary wall-mounted unit
Signature dynamics	Rhythm, acceleration, and pressure flow of signature are captured and compared	Changing or erratic signatures	High	Signature tablet, motion-sensitive stylus

1.7. Biometric technologies

The function of a biometric technologies authentication system is to facilitate controlled access to applications, networks, personal computers (PCs), and physical facilities. A biometric authentication system is essentially a method of establishing a person's identity by comparing the binary code of a uniquely specific biological or physical characteristic to the binary code of an electronically stored characteristic called a biometric. The various biometric technologies areDNA, Ear, Face, Facial thermogram, Fingerprint, Gait, Hand geometry, Hand Vein, Iris, Keystroke, Odor, Retina, Signature, Voice, Palmprint.

Table 1 gives the summary of some of the common biometric types [7], the method involved, the performance factor, the devices used to acquire the biometric and the user acceptance level.

1.7.1 DNA

Deoxyribonucleic acid (DNA) is the one-dimensional (1–D) ultimate unique code for one's individuality —except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in the context of forensic applications for person recognition. Anil K. Jain et al [1] gives three issues that limit the utility of this biometrics for other applications:

- contamination and sensitivity: it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose;
- automatic real-time recognition issues: the present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert's skills and is not geared for on-line noninvasive recognition; and
- privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, e.g., in hiring practices.

1.7.2 Ear

It has been suggested that the shape of the ear and the structure of the cartilaginous issue of the pinna are distinctive. The ear recognition approaches are based on Anil K. Jain et al [1] matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

1.7.3 Face

In the last decade significant advances have been achieved on biometrics, especially on face recognition (Jain et al., 1999). This technology is considered a natural means of biometric identification since the ability to distinguish among individual appearances is possessed by humans. Facial scan systems can range from software-only solutions that process images processed through existing closed-circuit television cameras to full fledged acquisition and processing systems, including cameras, workstations, and backend processors. With facial recognition technology, a digital video camera image is used to analyze facial characteristics such as the distance between eyes, mouth or nose. These measurements are stored in a database and used to compare with a subject standing before a camera.

The face recognition process has two major parts: detection, locating a human face in an image and isolating it from other objects in the frame, and recognition, comparing the face being captured with a database of faces to find a match.

During detection, the hardware/software combination isolates the facial elements of an image and eliminates extraneous information. The software examines the image for typical facial structures (such as eyes and nose), and once it has found them, it calculates the remainder of the face. It then cuts away background details, leaving a close-up of a face inside a rectangular frame called a binary mask.

Face recognition uses mainly the following techniques:

- Facial geometry: uses geometrical characteristics of the face. May use several cameras to get better accuracy (2D, 3D...)
- Skin pattern recognition (Visual Skin Print)
- Facial thermogram: uses an infrared camera to map the face temperatures
- Smile: recognition of the wrinkle changes when smiling

Facial-scan technology has its advantages and disadvantages.

Advantages

- No contact required
- Commonly available sensors (cameras)
- Large amounts of existing data to allow background and/or watch list checks
- Easy for humans to verify results

Disadvantages

- 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

One major advantage is that facial-scan technology is one of the biometric capable of identification at a distance without subject complicity or awareness. Another advantage of facial-scan technology is the fact that static images can be used to enroll a subject. The main advantage of facial recognition systems is the lack of user interaction needed to perform scans. While users may be required to stand still, facial recognition systems are without a doubt one of the least intrusive on the market. In addition facial recognition is suited to environments where there is significant dirt or potential pathogens, as there is no physical contact required between users and systems.

The disadvantages include acquisition environment and facial characteristic changes that effect matching accuracy and the potential for privacy abuse. Images are most accurate when taken facing the acquisition camera and not sharp angles. The users face must be lit evenly, preferably from the front. Changes in hairstyle, makeup or the wearing of a hat or sunglasses may pose a problem during the verification process. Facial-scanning technology has a poor record in verifying a subject who has had plastic surgery to alter their appearance. The fact that a biometric facial scan can take place without the knowledge or consent of a subject raises privacy concerns among many. Facial-scan technologies have unique advantages over all other biometrics in the areas of surrounding large groups and the ability to use preexisting static images. Its disadvantages include the falsely non-matching folks when subject appearances change during verification.

Andrea F. Abate, et al [2] discusses the five key factors that significantly affect system face recognition performances.

- Illumination variations due to skin reflectance properties and due to the internal camera control. Several 2D methods do well in recognition tasks only under moderate illumination variation, while performances noticeably drop when both illumination and pose changes occur.

- Pose changes affect the authentication process, because they introduce projective deformations and self-occlusion. Even if methods dealing with up to 32_ head rotation exists, they do not solve the problem considering that security cameras can create viewing angles that are outside of this range when positioned.

- On the contrary, with exception of extreme expressions such as scream, the algorithms are relatively robust to facial expression.

- Another important factor is the time delay, because the face changes over time, in a nonlinear way over long periods. In general this problem is harder to solve with respect to the others and not much has been done especially for age variations.

- At last, occlusions can dramatically affect face recognition performances, in particular if they are located on the upper-side of the face, as documented in literature.

1.7.4 Facial thermogram

Facial thermogram requires an (expensive) infrared camera to detect the facial heat patterns that are unique to every human being. 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 (visible spectrum) photograph. The technology could be used for covert recognition. A thermogram-based system does not require contact and is noninvasive, but image acquisition is challenging in uncontrolled environments, where heat-emanating surfaces (e.g., room heaters and vehicle exhaust pipes) are present in the vicinity of the body. A related technology using near infrared imaging is used to scan the back of a clenched fist to determine hand vein structure [1]. Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermograms.

1.7.5 Fingerprint

Fingerprinting technology is the oldest of the biometric sciences and utilizes distinctive features of the fingerprint to identify or verify the identity of individuals [1]. All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a unique fingerprint is matched for verification and authorization. These unique fingerprint traits are termed “minutiae” and comparisons are made based on these traits. On average, a typical live scan produces 40 “minutiae”. The Federal Bureau of Investigation (FBI) has reported that two individuals can share no more than 8 common minutiae.

There are five stages involved in finger-scan verification and identification: fingerprint image acquisition, image processing, location of distinctive characteristics, template creation and template matching. A scanner takes a mathematical snapshot of a user's unique biological traits. This snapshot is saved in a fingerprint database as a minutiae file.

Fingerprint authentication mechanisms rely on the identification of minutiae in the fingerprints - discontinuities in the flow of a user's fingerprints that can come in the form of deltas, pores, islands, and other characteristics. Once systems have isolated the minutiae of a fingerprint, the precision of the matching is based on the numbers of minutiae, which are used to create a positive match.

Fingerprint verification has emerged as one of the most reliable means of biometric authentication due to its universality, distinctiveness, permanence and accuracy [4]. Fingerprint biometrics has a number of benefits. They enjoy good acceptance rates in the general public, and have a positive image. The mechanism is not overly intrusive, and is generally trusted. The mechanism is quite flexible for failure rates, as fingerprints have a high number of potential areas to be mapped for identification. Thus if desired, fingerprint based rollouts can be highly secure.

As a popular and precise mechanism, fingerprinting does have drawbacks. Fingerprinting systems will struggle in areas where users are likely to have either injured or dirty hands. Similarly, the elderly and those with dry skin may struggle to register and make use of these biometrics systems. Finally fingerprinting systems are the most commonly targeted systems for attempts to falsify credentials. A number of methods used to counter this are available, and mechanisms such as liveness testing should be considered when using fingerprinting.

Advantages

- 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 watch list 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

Disadvantages

- Public Perceptions
- 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

1.7.5.1 Issues with use of fingerprints

For a system that uses a fingerprint as its biometric data, it has been found by multiple groups that the use of “gummy fingers” (artificial fingers made from gelatin) can spoof a biometric system. One such study found that it was possible to create a gummy finger from a latent fingerprint, enroll into the system and then verify using the same gummy finger against a live enrolled template.

1.7.6 Gait

Gait is the peculiar way one walks and is a complex spatio-temporal biometric. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications. Gait is a behavioral biometric and may not remain invariant, especially over a long period of time, due to fluctuations in body weight, major injuries involving joints or brain, or due to inebriety. Acquisition of gait is similar to acquiring a facial picture and, hence, may be an acceptable biometric. Since gait-based systems use the video-sequence footage of a walking person to measure several different movements of each articulate joint, it is input intensive and computationally expensive.

1.7.7 Hand geometry

Among a number of biometric techniques that are used for frequent human identification tasks, hand shape and hand shape-based biometry is an emerging new technique, with certain advantages over the more established competitor techniques. First, human hand data acquisition is less cumbersome, user-friendlier. Furthermore, it is much less susceptible to intrinsic variations and environmental artifacts [1]. Hand-based identification/verification systems provide an attractive and growing alternative biometric scheme [10].

Hand geometry employs measurements of various aspects of the hand including width, length, and width and length of fingers. Because of the relatively basic nature of this mechanism, it is suitable for authentication, but not identification.

Most people are willing to use their hands and bring a fresh perspective to this technology (as opposed to fingerprint recognition systems, which are associated with criminals being booked).

Hand geometry authentication offers several advantages. Hand geometry verification systems use geometric measurements of hand as the features for the verification of individuals. Hand geometry measurements are easy to collect and non intrusive. The hardware requirements imposed by such a system are not severe. The system just requires properly placed camera that can get the image of the hand. Furthermore, with back illumination the measurements can be made very robust against ambient lighting conditions. Hand geometry acquisition and verification is extremely fast and accurate enough for verification. It is very well suited for integration with other biometrics and in particular with fingerprints. It is very easy to envision a system that simultaneously acquires hand geometry and fingerprint images.

Hand geometry, however, does have some negatives. First, hand geometry systems should not be considered for identification purposes, since hands are not unique and accuracy rates cannot be as high as other biometric readers. Rather, they are best used for verification purposes and coupled with a PIN for extra security. Hand geometry systems have been well accepted to date, and can be configured to be quite reliable. They have been deployed in several major areas with no major issues of public acceptance, possibly due to the lack of potential for identification with this mechanism. While hand geometry systems can struggle with equipment issues in dirty environments, authentication should not be an issue as the attributes to be measured are far less detailed than those used for fingerprinting.

Hand geometry systems come at a higher cost. The hardware used for such scanning is dedicated, and systems are proprietary. Different manufacturers employ different mapping standards based on different attributes, so potential buyers would be advised to obtain field results on failure types and enrolment issues.

Advantages

- Easy to capture
- Believed to be a highly stable pattern over the adult lifespan

Disadvantages

- Use requires some training
- Not sufficiently distinctive for identification over large databases; usually used for verification of a claimed enrollment identity
- System requires a large amount of physical space

1.7.8 Hand Vein

Vein patterns are within you, people don't leave them around (like fingerprints) nor can they be easily observed like Iris patterns or faces. Vein structures are not easily covertly captured or reproduced like other biometric traits.

Vein recognition technology is an emerging biometric technology with great promise. But vein recognition is not without its faults. The technology could be seen as invasive by many people, particularly in the US, where fears surrounding the long-term damage of such internal readings are paramount. In addition, it faces an uphill battle against other biometric technologies that have existed far longer than vein recognition.

1.7.9 Iris

Penny Khaw [9] in his article says that the iris has many features that can be used to distinguish one iris from another. One of the primary visible characteristic is the trabecular meshwork, a tissue which gives the appearance of dividing the iris in a radial fashion that is permanently formed by the eighth month of gestation. During the development of the iris, there is no genetic influence on it, a process known as chaotic morphogenesis that occurs during the seventh month of gestation, which means that even identical twins have differing irises. The iris has in excess of 266 degrees of freedom, i.e. the number of variations in the iris that allow one iris to be distinguished from another. The fact that the iris is protected behind the eyelid, cornea and aqueous humour

means that, unlike other biometrics such as fingerprints, the likelihood of damage and/or abrasion is minimal. The iris is also not subject to the effects of aging which means it remains in a stable form from about the age of one until death. The use of glasses or contact lenses (coloured or clear) has little effect on the representation of the iris and hence does not interfere with the recognition technology.

Advantages

- No contact required
- Protected internal organ; less prone to injury
- Believed to be highly stable over lifetime
- Highly protected, internal organ of the eye
- Externally visible; patterns imaged from a distance
- Iris patterns possess a high degree of randomness
- Changing pupil size confirms natural physiology
- Pre-natal morphogenesis (7th month of gestation)
- Limited genetic penetrance of iris patterns
- Patterns apparently stable throughout life
- Encoding and decision-making are tractable
- Image analysis and encoding time: 1 second
- Decidability index (d-prime): d' = 7.3 to 11.4
- Search speed: 100,000 IrisCodes per second on 300MHz CPU

Disadvantages

- Difficult to capture for some 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
- Lack of existing data deters ability to use for background or watch list checks
- Cannot be verified by a human
- Small target (1 cm) to acquire from a distance (1 m)
- Moving target ...within another... on yet another
- Located behind a curved, wet, reflecting surface
- Obscured by eyelashes, lenses, reflections
- Partially occluded by eyelids, often drooping
- Deforms non-elastically as pupil changes size
- Illumination should not be visible or bright
- Some negative (Orwellian) connotations

1.7.10 Keystroke Dynamics

Keystroke dynamics is a biometric method that tries to identify in the typing of different keyboard users. This 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 of typing a particular password, and the time a user takes between hitting certain keys. This technology's algorithms are still being developed to improve robustness and distinctiveness. Any person knowing the username and password of another user cannot gain access rights for computer system due to the difference of their keystroke patterns. On the other hand, unlike the other biometric methods, Keystroke analysis does not require the aid of extra special tools [1]. Just keyboard and analysis software are sufficient for the biometric analysis. Therefore it is cheaper than biometric authentication methods. However, user authentication via keystroke dynamics remains a difficult task. Because, physiological features such as face, retinal, palm print and fingerprint remains stable over time. But behavioral properties such as keystroke patterns may vary according to the users' skill, illness and tiredness.

1.7.11. Odor

It is known that each object exudes an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. A whiff of air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of (aromatic) compounds. A component of the odor emitted by a human (or any animal) body is distinctive to a particular individual. It is not clear if the invariance in the body odor could be detected despite deodorant smells, and varying chemical composition of the surrounding environment [1].

1.7.12. Retina

Retina-scan technology makes use of the retina, which is the surface on the back of the eye that processes light entering through the pupil. Retinal Scan technology is based on the blood vessel pattern in the retina of the eye. The principle behind the technology is that the blood vessels at the retina provide a unique pattern, which may be used as a tamper-proof personal identifier. Since infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue, it is used to illuminate the eye retina. Analysis of the enhanced retinal blood vessel image then takes place to find characteristic patterns.

Retina-scan technology is still in a prototype development stage and still commercially unavailable. Retina-scan technology image acquisition is difficult in that the retina is small and embedded, requiring specific hardware and software. The user positions his eye close to the unit's embedded lens, with the eye socket resting on the sight. In order for a retinal image to be acquired, the user must gaze directly into the lens and remain still; movement defeats the acquisition process requiring another attempt. A low intensity light source is utilized in order to scan the vascular pattern at the retina. This involves a 360 degree circular scan of the area taking over 400 readings in order to establish the blood vessel pattern. This is then reduced to 192 reference points before being distilled into a digitized 96 byte template and stored in memory for subsequent verification purposes. Normally it takes 3 to 5 acceptable images to ensure enrollment. Because of this, the enrollments process can be lengthy. Enrollments

can take over 1 minute with some users not being able to be enrolled at all.

After image acquisition, software is used to compile unique features of the retinal blood vessels into a template. Retina-scan technology possesses robust matching capabilities and is usually configured to do one-to-many identification against a database of users, however, this technology requires a high quality image and will not enroll a user unless a good image is acquired. For this reason, there is a moderately high false reject rate due to the inability to provide adequate data to generate a match template.

Retina-scan technology has its advantages and disadvantages.

Its advantages are it is resistance to false matching or false positives because of the fact that the pupil, like the fingerprint remains a stable physiological trait throughout ones life. The retina is unaltered by any environmental or temporal condition. Its resistance to false matching is due to the fact that retinal scans produce patterns that have highly distinctive characteristics, sufficient to enable identification. Well-trained users find retina scan capable of reliable identification. Like fingerprints, retina traits remain stable throughout life.

Disadvantages are the technology is difficult to use, users claim discomfort with eye-related technology in general and the fact that retina scan technology has limited uses. Retina-scan enrollments take longer than both iris-scan and fingerprinting. Users claim discomfort with the fact that they must position their eye very close to the device and fear that the device itself or the light inside the device can harm their eyes in some way. Other biometrics can provide most if not all the benefits of this technology without the problems. If future technology allows for retina scanning being easier to use and allow users to enroll from a greater distance from the imaging device, its future will be bright.

Popularized in various science fiction and action movies, it is interesting to note that retinal scans are based on very old theories related to the uniqueness of patterns of blood vessels in the human eye. Clearly the image of retinal scans is one of a technology which is much more invasive than any other alternative to date. Public perceptions of retinal scanning include concerns around potential eye damage. Combining this with the invasive reputation, retinal scanning technology may not have an ideal image for rollout to the public. Hardware costs are high, and systems are not particularly mobile, limiting their use in a field environment or at user desktops.

1.7.13. Signature Verification

Signature verification technology utilizes the distinctive aspects of the signature to verify the identity of individuals. The technology examines the behavioral components of the signature, such as stroke order, speed and pressure, as opposed to comparing visual images of signatures. Unlike traditional signature comparison technologies, signature verification measures the physical activity of signing. While a system may also leverage a comparison of the visual appearance of a signature, or "static signature," the primary components of signature verification are behavioral.

The signature along with the variables present during the signing process, is transmitted to a local PC for template generation. Verification can take place against a local PC or a central PC, depending on the application. In employee-facing signature verification applications such as purchase order authentication, local processing may be preferred; there may be just a single PC used for such authorization. For customer-facing applications, such as retail or banking authentication, centralized authentication is likely necessary because the user may sign at one of many locations.

The results of signature verification comparisons must be tied into existing authentication schemes or used as the basis of new authentication procedures. For example, in a transactional authentication scenario, the "authorize transaction" message might be sent after a central PC acquires a signature. When signature verification is integrated into this process, an additional routine requires that the signature characteristics be successfully matched against those on file in order for the "authorize transaction" message to go forward. In other applications, the results of a signature verification match may simply be noted and appended to a transaction. For example, in document authentication, an unsuccessful comparison may be flagged for future resolution while not halting a transaction. The simplest example would be a signature used for handheld device login: the successful authentication message merely needs to be integrated into the login module, similarly to a PIN or password.

As one of the biometric authentication methods, signature has been widely accepted in our real life, because it is user-friendlier than fingerprint, iris, retina and face. On-line signatures are acquired using digitizing tablet that captures both temporal and spatial information, such as coordinates, pressure, inclinations, etc. It is not possible to reproduce the online features even if a person's handwriting is copied from an already existing document. Therefore it is significantly more difficult to circumvent online handwriting and signature verification systems. However, two aspects pose challenges in the field of online signature verification. Firstly, intra-personal variation can be large. Our recent study about the distinctiveness of signature features indicate that the speed, pressure and inclinations pertaining to the signatures made by the same person can differ greatly making it quite challenging to extract consistent features. Secondly, we can only expect few samples from one person and no forgeries in practice. This makes it difficult to determine the consistency of extracted features.

1.7.14. Voice recognition

Voice or speaker recognition uses vocal characteristics to identify individuals using a pass-phrase. Voice recognition can be affected by such environmental factors as background noise. Additionally it is unclear whether the technologies

actually recognize the voice or just the pronunciation of the pass-phrase (password) used. This technology has been the focus of considerable efforts on the part of the telecommunications industry and NSA, which continue to work on improving reliability. A telephone or microphone can serve as a sensor, which makes it a relatively cheap and easily deployable technology.

Voice authentication is a fairly simple process. To register, a user records sample(s) of their voice which are stored in the authenticating system and become known as their 'voiceprint'. Then, to access this resource subsequently, they supply a sample of their voice to the system, and it decides if it matches their voiceprint before allowing them access.

Voice authentication is best used for identifying persons over the phone or in an environment that can control background noise; however, today's solutions are better equipped to handle background noise than they were a few years ago. Mobile phone conversations are less of an issue, and the migration to voice over IP (VoIP) will help with the integration. The technology, however, has taken a back seat to other initiatives such as enhanced voice identification and routing systems.

Advantages

- Public acceptance
- No contact required
- Commonly available sensors (telephones, microphones)

Disadvantages

- Difficult to control sensor and channel variances that significantly impact capabilities
- Not sufficiently distinctive for identification over large databases

Voice biometrics offer major advantages over other types of authentication techniques in terms of usability, cost, easy of deployment and user acceptance, since it is the most non-intrusive amongst the many biometrics that are being used. Apart from the content of speech and identity of the user, information such as accent, gender, age and other soft biometric traits of the individual can also be inferred from his speech signal.

The disadvantages of voice biometric are when deciding whether or not to employ a voice authentication system it is important to consider the application. The elements of any voice authentication system need to be analyzed and it must be ensured that individually and collectively, the probability of a vulnerability arising is low, and the potential for an individual or group to exploit the vulnerability unlikely. a sample voice print is shown in the figure 18 which is nothing but analog signals.

1.7.15. Palmprint

The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the fingerprints [1]. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper. Finally, when using a high-resolution palmprint scanner, all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system.

1.8. Emerging Biometric Technologies

- Brainwave Biometric
- Vascular Pattern Recognition
- Fingernail Bed Recognition
- Handgrip Recognition
- Body Salinity Identification
- Infrared Fingertip Imaging & Pattern Recognition

1.9. Comparison of various biometric technologies

Amit Mhatre and et al [3], Anil K. Jain et al [1] discusses the comparison of various biometric technologies. Table 2 shows the results of the comparison.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	**H**	**H**	**H**	**L**	**H**	**L**	**L**
Ear	**M**	**M**	**H**	**M**	**M**	**H**	**M**
Face	**H**	**L**	**M**	**H**	**L**	**H**	**H**
Facial Thermogram	**H**	**H**	**L**	**H**	**M**	**H**	**L**
Fingerprint	**M**	**H**	**H**	**M**	**H**	**M**	**M**
Gait	**M**	**L**	**L**	**H**	**L**	**H**	**M**
Hand geometry	**M**	**M**	**M**	**H**	**M**	**M**	**M**
Hand vein	**M**	**M**	**M**	**M**	**M**	**M**	**L**
Iris	**H**	**H**	**H**	**M**	**H**	**L**	**L**
Keystroke	**L**	**L**	**L**	**M**	**L**	**M**	**M**
Odour	**H**	**H**	**H**	**L**	**L**	**M**	**L**
Retina	**H**	**H**	**M**	**L**	**H**	**L**	**L**
Signature	**L**	**L**	**L**	**H**	**L**	**H**	**H**
Voice	**M**	**L**	**L**	**M**	**L**	**H**	**H**
Palmprint	**M**	**H**	**H**	**M**	**H**	**M**	**M**

Table 2: Comparison of various biometric techniques

H- High, M – Medium, L – Low

2. ISSUES OF BIOMETRICS

While biometric systems can offer greater levels of security, various attacks exist to gain unauthorized access to a system that is protected by biometric authentication. The various issues of the biometric system are dealt here.

2.1. System design issues

Biometrics is invariably associated with security; hence the biometric system itself should be reasonably secure and trustworthy. Some of the biometric security issues are

- Rogue sensors and unauthorized acquisition of biometric samples
- Communications security between sensors, matchers and biometric databases
- Accuracy
- Speed
- Scalability
- Resilience
- Cost
- Privacy

2.2. Authentication or Identification?

The various key issues to be considered during the examination of biometrics for authentication systems are discussed here. First we need to identify whether the system is meant for identifying users, or simply authenticating users. Identification of a user is a much more difficult task.

Authentication is the verification that a user is who they claim to be [3]. For such a situation, the user provides a possible range of users of one. The authentication mechanism then compares the expected credentials for the claimed identity to the credentials it finds on the claimant. If there is a match, the user is authenticated. This is known as a one to one test.

In contrast, identification does not involve a claim of identity at all. Instead, the system is presented with a set of (ideally complete) credentials, and asked to compare this set of credentials against the users it knows of, returning a result, which identifies the user, in question. This is known as a one to many test, and it should be evident that this type of test is both more labour intensive for the system, and more reliant on having a wide range of attributes to compare users with.

2.2.1 Failure Rates

Failure rates are a critical consideration in the configuration and day to day running of a biometrics system. Two types of failure rates must be considered; false acceptance rates, and false rejection rates. These failure rates are a function of how precisely the system attempts to verify each user against the characteristics registered for them. Thus, a system, which is configured, to be very precise and have very low false acceptance rates will almost invariably be performing a higher number of false rejection rates, relative to a balanced system. Similarly a system, which involves lower value access, will likely be granted to be less precise to ensure that the positive customer experience is delivered.

A security professional will tend to move immediately towards a configuration with low false acceptance rates and ignore the false rejection rates. This is not a practical option in all cases, and the configuration depends strongly on the environment in which the biometrics-based system is to be deployed. In a high security military-style setting where security is paramount, users, or at least their administrators will be more accepting of a high false rejection rate which is in support of a low false acceptance rate. In a commercial setting, there will often be less scope for the acceptance of delays and difficulties associated with false rejection rates.

2.2.2. Liveness

A number of attacks on biometrics systems have been proposed over the years, and a number have been quite successful. Fingerprinting systems were originally entirely reliant on fingerprints for authentications, meaning that moulded synthetic fingers with imprints of fingerprints could be used to authenticate users. Similarly, hand geometry systems were entirely reliant on superficial physical attributes.

Since these attacks have been proposed, a new area of biometrics has arisen which focuses entirely on determining whether the authenticating attributes being measured are in fact the attributes of a living being, as opposed to a recording or a synthetic imitation. The mechanisms are varied, relying on things such as prompted user actions to smile for facial recognition. In the area of fingerprinting systems have been developed to measure both perspiration and the pulse of the authenticating user. Hence, liveness testing is becoming a vital part of biometrics systems.

Methods have been proposed to make spoofing biometric systems more difficult. The method that is considered here is the determination of liveness. To determine whether or not a person is live when they present their biometric data to a system can be a difficult task to automate in a fashion that is acceptable to users, and feasible to implement. Many methods exist, such as temperature sensing, detection of pulse in fingertip, pulse oximetry, electrocardiogram, dielectric response, and impedance. Each of these methods have their own challenges in being able to automate and integrate into systems in the most transparent way possible. For example, the extra equipment required to perform some of these tests, such as electrocardiogram, can be expensive and inconvenient for the user.

2.3. Physically Challenged Non-Registrable Users

During the rollout and use of a system based on biometrics, it is inevitable that some users will be found who cannot register for a given system due to their physical characteristics. Thus, a secondary authentication mechanism is always needed for biometric systems. Care must be taken to ensure that the use of biometrics does not mean the complete exclusion of a given group of users.

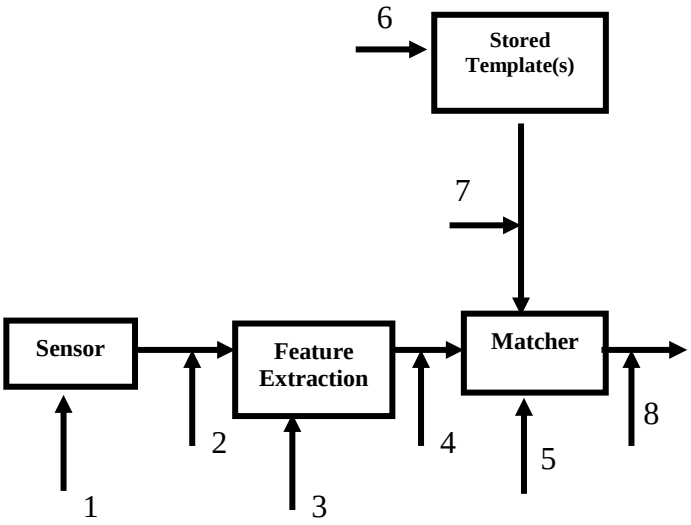
The mechanics of non-registrable users varies depending on the biometric mechanism being used. Even without actual physical injury, some mechanisms can suffer in particular sections of the population. When examining fingerprinting, for example, it has been found that the elderly often have either very dry skin, or very weak fingerprints simply as a result of aging skin.

2.4. Circumvention

It is key that when rolling out a biometrics system, the view of a system as a chain is maintained, along with the understanding that a system is only as secure as the weakest part of that chain. Biometrics offer a strong means to authenticate users for systems, however attackers will tend to attack systems at their weakest point, not their strongest.It is vital that biometrics serve a supporting role in well designed, properly secured systems. Installing biometrics into a fundamentally weak system is a waste of both resources and time.

2.5. Scalability

There are general concerns related to the scalability of biometrics systems - it is key that any solutions vendor be pressed to prove that the solution offered is going to be appropriately scalable.



1	Fake biometric	2	Replay old data
3	Override feature extractor	4	Synthesized feature vector
5	Override matcher	6	Modify template
7	Intercept the channel	8	Override final decision

Figure 5 Vulnerabilities of a biometric system

While it is highly recommended that test pilots be performed for rollouts of biometrics systems, the issue of scalability is a more difficult one to tackle. Biometrics rollouts across very large user populations may not scale well. Research into this area is lacking at present, and unfortunately the larger rollouts of biometrics to date have involved organizations that are less likely to wish to discuss their authentication mechanisms in depth.

Biometrics come with a complex set of issues which need careful consideration. The issues above illustrate a number of potential pitfalls, and hopefully give an indication of the consequences of ill-considered biometrics deployments.

N.K.Ratha et al [11] identified eight places in the generic biometric system (Figure 4) where attacks may occur.

3. GUIDELINES FOR BIOMETRIC TECHNOLOGY

3.1. Checklist of things to consider when choosing a biometric

- Physical contact and durability
- Usage and durability
- Flexible packaging
- Infrastructure and interoperability
- Enrolment
- Standards
- Security
- Proven technology
- Reliability
- Accuracy
- Capture
- Liveness
- User friendliness
- Intrusiveness
- Context of application
- Convenience
- Cost

3.2. Authentication guidelines

Before enrolling a new user, the system must establish to a proper degree of certainty that a new user is indeed who they claim to be. Without sufficiently strong authentication during the enrolment step, a biometrics authentication system is effectively useless, no matter how strong the actual mechanisms employed.

Authentication for enrolment will always ideally be performed in-person with well-trained and examined staff. The verification process should be explicitly defined in terms of the identification required, and the steps, which must be taken to verify this identification. When possible, authentication should be a two-stage process to diminish the likelihood of insider attacks resulting in deliberately incorrect authentication of new users.

In some models, an in-person verification may not be possible, or may not be seen as necessary for user authentication. For example, a bank rolling out biometrics devices for authentication across the Internet may wish to mail out devices and incorporate their enrolment process into the next session the user establishes through the historic authentication mechanisms. In such cases, additional remote mechanisms must be found to ensure that enrolment is secure. If the chain of authentication to establish biometric authentication credentials contains a step with authentication of a lower strength than the biometrics layer, then an attacker will simply move one layer down and attack systems at the initial authentication/enrolment stage.

3.3. Enrollment Guidelines

Once authentication has been performed and the user is to authenticate, the system and those administering it must ensure that the user credentials gathered from the mechanism are sufficient to identify the new user accurately. Biometrics systems assemble their views of users through sets of measurements, as described in the techniques section. The precise location of each measurement and number of measurements taken for each user may vary slightly, as each user will have different characteristics to compare. The biometrics system that is used must be configured and employed such that all user credential sets contain a minimum number of points of reference to identify or authenticate that user.

As an example, if a fingerprint based system typically relies on fifteen points of reference, and attempts to enroll a user with worn fingers, the system may simply not be able to enroll this user. If only ten points of reference are found, this must result in a failed enrolment, not simply a weaker profile for this user. Similarly, a user attempting to enroll with damaged fingerprints might enroll with a set of characteristics, which are both temporary and potentially reproducible. Enrolment officers must be qualified to judge both potential cases, and must have clearly defined procedures to deal with these issues.

Similarly, enrolment officers must be accustomed to dealing with equipment and its failures. In the case of mechanisms such as fingerprint authentication, sensors can wear out over time, leading to issues of either complete failure, or repeated generation of user information sets lacking the detail to form a proper authentication set.

3.4. Administration & Maintenance

Biometrics systems will ideally be as low-maintenance as possible. If stored locally, the integrity of both authentication data and authentication mechanisms must be maintained. Role separation and tamper proof systems auditing are both controls to be strongly considered.

Table 3: Advantages and drawbacks of the different protection techniques

Technique	Advantages	Drawbacks
Liveness Detection	Resists spoofing attacks	Increases cost for the extra hardware and software, user inconvenience and increased acquisition time.
Watermarking	Prevents replay attacks and provide integrity of the stored templates	Problem of image degradation and lack of algorithms to deal with it.
Soft biometrics	Provides improved performance through filtering and tuning of parameters	Lack of techniques for automatic extraction of soft biometric techniques
Multimodal biometrics	Improves performance, resists spoofing and replay attacks and provides high population coverage	Increased system complexity, computational demands and cost

If systems do require regular maintenance by administrative staff, role-based access controls should be considered to ensure that staff maintaining systems do not have access to either the data, logic, or logs of the systems. Similarly, auditing personnel should not have access to the system whose logs they examine. Maintaining clear separations of both roles and data access will ensure that data and logic functions are kept as securely as possible.

3.5. Increased Security and Perception

Biometrics has a real potential to boost some areas of security in a system, though clearly they are not a magical bullet for all security issues. Biometrics can play a real role in systems where identity theft is an issue, ensuring that each individual user is only present once on a system. Clearly though, this is still limited, as the first user to claim an identity on a given system is then the "owner" of this identity. While biometrics can be used to cut down on account hijacking, issues around fraudulent accounts fall back onto registration procedures, just as is the case with any other authentication system.

On the perception side, it has been suggested that in the casino trade, the use of facial recognition to monitor card counters and the like has been split regarding identifying culprits, and deflecting potential cheats.

3.6. Methods to overcome the Biometric Attacks

3.6.1 Liveness Detection:

Liveness detection refers to the ability of the system to distinguish between a sample feature provided by a live human being and a copy of a feature provided by an artifact. Liveness detection can be implemented using software or hardware means.

- Using extra hardware to acquire life signs like temperature, pulse detection, blood pressure etc for fingerprints and movements of the face for face recognition. Iris recognition devices can measure the involuntary papillary hippos (Constant small constrictions and dilations of the pupil caused by spontaneous movements of the Iris). The drawback is that extra hardware makes the system expensive and bulky.
- Using the information already captured to detect life signs. The only researched method is using information about sweat pores. For this a sensor that can acquire a high-resolution image is required. It is difficult to reproduce the exact size and position of the pores on an artificial mold.
- Using liveness information inherent to the biometric being obtained. For fingerprints, using a side impression

near the nail, which has been enrolled earlier, can do this. The advantage is that people do not leave side impressions as latent prints and no major changes in the scanner is needed to acquire this additional information. A system that uses multiple instances of the same biometric can be used for liveness detection by asking the user to provide a random subset of biometric measurements.

3.6.2. Steganographic and Watermarking Techniques

Steganography means secret communication. It involves hiding critical information in unsuspected carrier data. Steganography based techniques can be suitable for transferring critical biometric information from a client to a server.

Ratha [6] proposes a water marking technique applicable to fingerprinting images compressed with WSQ wavelet-based scheme. The discrete wavelet transform coefficients are changed during WSQ encoding by taking into consideration possible image degradation. This method is used to secure biometric authentication systems for commercial transactions against replay attacks. To achieve this, the service provider issues a different verification string for each transaction. The string is mixed with the fingerprint image before transmission. When the image is received by the service provider it is decompressed and the image is checked for a one-time verification string. Here, the message is not hidden in a fixed location, but is deposited in different places on the structure of the image so that it cannot be easily recovered.

4. MULTI-MODAL BIOMETRIC SYSTEMS

Multi-modal biometric systems can be used to resist spoofing attacks (attacks at point 1). These systems can address the problem of non-universality since multiple traits can ensure sufficient population coverage. They can be used to counteract spoofing attacks, since it is difficult for a hacker to simultaneously spoof multiple biometric traits of a legitimate user. The choice and the number of biometric traits is decided by the nature of the application, the computational demands and costs introduced, and the correlation between the traits considered.

4.1 Multi-algorithm

One step beyond a "simple" biometric is what we might call a multi-algorithm approach. This approach still employs a single sensor, and acquires a single biometric sample. Two or more different algorithms process the single sample, and the individual results are fused to obtain an overall recognition result.

4.2 Multi-sample

Another approach might be called "multi-sample" or "multi-instance." Multiple samples of the same biometric are sensed, the same algorithm processes each of the samples, and the individual results are fused to obtain an overall recognition result.

4.3 Multi-modal: "orthogonal"

One common category of multi-modal biometrics might be called "orthogonal." By "orthogonal" we mean to indicate that the biometric sources are different; that is, different parts of the body are involved. An example would be face recognition and fingerprint used together.

4.4 Multi-modal: "independent"

Another category of approach to multi-modal biometrics might be called "independent." By "independent" we mean to indicate that the individual biometrics are processed independently of each other. It would seem that orthogonal biometrics are processed independently by necessity. But when the biometric source is the same and different properties are sensed, then the processing may be independent, but there is at least the potential for gains in performance through collaborative processing.

4.5 Multi-modal: "collaborative"

A less common approach to multi-modal biometrics might be called "collaborative." By "collaboration" we mean the degree to which the processing of one biometric is influenced by the results of processing another biometric.

4.6 Challenges to Multi-Modal Biometrics

A number of challenges and issues confront multimodal biometrics research.

- An important practical issue is that appropriate datasets does not exist to support research in multi-modal biometrics.
- Best fusion methods are not available. Almost every research report in multi-modal biometrics considers several possible ways of fusing the results. However, it seems that no fusion approach has emerged that generally achieves a statistically significant improvement over a simple sum of scores.
- Some research results that suggest that a multi-sample approach using "enough" samples can out-perform a multi-modal approach.
- It is very difficult to choose a best set of N samples for a particular biometric.

5. SOFT BIOMETRICS

Soft biometrics can be used to thwart attacks at the attack points 1 and 8 (attacks on the sensor and decision maker). Most of the biometric systems collect ancillary information about the users during enrollment, which is stored either in the database or in the smart card possessed by the user. The ancillary information collected together with the matching scores will lead to the correct identification of the user, which in turn prevents spoofing. The factors like age, gender, color, etc can affect the performance of a biometric system. The use of soft biometric traits helps to filter a large biometric database to get a reduced number of templates to do the comparison with, which in turn, will improve the speed and efficiency of the biometric system. Soft biometric traits can also be used for tuning the parameters of a biometric system

like the threshold on the matching score in a unimodal system, and the thresholds and weighing of different modalities in a multi-modal biometric system to obtain the optimum performance for a particular user or class of users. Incorporating soft biometrics will reduce FAR and FRR errors which in turn prevents spoofing.

6. ADVANTAGES OF BIOMETRIC TECHNOLOGIES

A major motivation for using biometrics is the ability to authenticate the true identity of an individual [1]. Biometric technologies can be applied to areas requiring logical access solutions, and it can be used to access applications, personal computers, networks, financial accounts, human resource records, the telephone system, and invoke customized profiles to enhance the mobility of the disabled. In a business-to-business scenario, the biometric authentication system can be linked to the business processes of a company to increase accountability of financial systems, vendors, and supplier transactions; the results can be extremely beneficial.

The global reach of the Internet has made the services and products of a company available 24/7, provided the consumer has a user name and password to login. In many cases the consumer may have forgotten his/her user name, password, or both. The consumer must then take steps to retrieve or reset his/her lost or forgotten login information. By implementing a biometric authentication system consumers can opt to register their biometric trait or smart card with a company's business-to-consumer e-commerce environment, which will allow a consumer to access their account and pay for goods and services (e-commerce). The benefit is that a consumer will never lose or forget his/her user name or password, and will be able to conduct business at their convenience. A biometric authentications system can be applied to areas requiring physical access solutions, such as entry into a building, a room, a safe or it may be used to start a motorized vehicle. Additionally, a biometric authentication system can easily be linked to a computer-based application used to monitor time and attendance of employees as they enter and leave company facilities. In short, contactless biometrics can and do lend themselves to people of all ability levels.

7. DISADVANTAGES OF BIOMETRIC TECHNOLOGIES

Some people, especially those with disabilities may have problems with contact biometrics. Not because they do not want to use it, but because they endure a disability that either prevents them from maneuvering into a position that will allow them to make use the biometric or because the biometric authentication system (solution) is not adaptable to the user. For example, if the user is blind a voice biometric may be more appropriate. Some of the disadvantages are listed below:

- Biometric systems are very expensive because, not only the costs for the acquisition of the software and hardware costly but the integration of these in the networks are even more costly. These high costs are coupled with the fact that the returns aren't highly encouraging. So, people are not ready to pool in so much money to utilize the latest technology that is available in the market.
- It is an "all or none" technology, i.e. we set up biometric authentication features etc but if we permit the person for a remote login then there is no use incorporating this technology in the network.
- Like every new technology, Biometrics has a low user acceptance rate.
- People consider it to be an invasion of their privacy and thus, it hasn't been exploited to its full potential. They don't realize the fact that a Biometric system does not copy their fingerprints or any other attributes but goes for a mathematical representation of these attributes that are unique to each person.
- Even though full secrecy is maintained regarding these attributes, even if they get leaked out once, they can be used in exploiting various other areas, like to get credit card and medical information, in banking security systems etc. Even though different biometric systems are highly incompatible with each other, their exploitation may ruin the life of the person who trusted this technology.
- Sometimes, a genuine person maybe restricted access to the network and this is very commonly seen in voice recognition patterns where something as small as cold could have the person's access rejected.
- Like all systems, even a Biometric system is not foolproof and has its own flaws and can sometimes allow a person who has assumed a fake identity into the network.
- Biometric template data consume more space than the conventional user ID/password combinations.

8. LIMITATIONS OF BIOMETRICS

The main reason for introducing biometric systems is to increase overall security. However, biometric identification is not perfect it is never 100% certain, it is vulnerable to errors and it can be 'spoofed'.

The biometric system is only one part of an overall identification or authentication process, and the other parts of that process will play an equal role in determining its effectiveness. That is a biometric sample may be used to authenticate a person before logging into a system, or it may be used in lieu of login. Also in some cases it may be used to verify a person after logging into to the system.

Biometric identification is a statistical process. Variations in conditions between enrolment and acquisition as well as bodily changes (temporary or permanent) mean that there is never a 100% match. For a password or a PIN, the answer given is either exactly the same as the one that has been stored, or it is not – the smallest deviation is a reason for refusal; for a biometric, there is no clear line between a match and a non-match. Whether a match exists depends therefore

not only on the two data sets to be compared, but also on what margin of error is deemed tolerable.

A 90% probability of a match may or may not be considered acceptable, depending on the implementation of the biometric in question and the application security requirements. Fraudulent reproduction of biometric data is possible; this depends heavily on the modality, application and resources being considered and availability of the data to be reproduced.

Biometric data may be stored on portable media such as smart cards if they will be used in verification mode. This ensures that the data cannot be used without the user's own authorization, contrary to what happens with data stored in a central database. Biometric verification/ identification can also be realized through remote access, by transmission of the biometric image or template through a network to the device that will process the decision step. This requires a highly secure connection. Watermarking could be used in this case to ensure that the transmitted data have not been corrupted.

Of course, smart cards can be lost or stolen. For this reason, the data they contain must be encrypted and backed-up. However, if the information is stolen, it is necessary to be able to revoke it and to produce another template which could be used for further identification. Revocation is easy when dealing with pin codes or passwords but not with biometric traits as we cannot change our irises or our fingerprints.

Cancellable biometrics [1] is a new research field and some preliminary propositions have been made. It is possible to generate new facial images for a person by filtering the original image.

9. BIOMETRIC APPLICATIONS

Most biometric applications fall into one of nine general categories:

- Financial services (e.g., ATMs and kiosks).
- Immigration and border control (e.g., points of entry, precleared frequent travelers, passport and visa issuance, asylum cases).
- Social services (e.g., fraud prevention in entitlement programs).
- Health care (e.g., security measure for privacy of medical records).
- Physical access control (e.g., institutional, government, and residential).
- Time and attendance (e.g., replacement of time punch card).
- Computer security (e.g., personal computer access, network access, Internet use, e-commerce, e-mail, encryption).
- Telecommunications (e.g., mobile phones, call center technology, phone cards, televised shopping).
- Law enforcement (e.g., criminal investigation, national ID, driver's license, correctional institutions/prisons, home confinement, smart gun).

10. CONCLUSION

Biometrics is a promising and exciting area, where different disciplines meet and provide an opportunity for a more secure and responsible world. There are a number of popular biometrics mechanisms currently deployed, some with strong histories, and some relatively new mechanisms. Each mechanism has its own strengths and weaknesses. When properly applied, biometrics can be used to combat fraud, and ensure that timekeeping systems are honest and accurate.

Using one biometric feature can lead to good results, but there is no reliable way to verify the classification. To achieve robust identification and verification two different biometric features can be combined. A multimodal biometrics can provide a more balanced solution to the security and convenience requirements of many applications

Recent advances in biometric technology have resulted in increased accuracy at reduced costs; biometric technologies are positioning themselves as the foundation for many highly secure identification and personal verification solutions.

Despite the tremendous progress made over the past few years, biometric systems still have to reckon with a number of problems, which illustrate the importance of developing new biometric processing algorithms as well as the consideration of novel data acquisition techniques. Undoubtedly, the simultaneous use of several biometrics would improve the accuracy of an identification system. For example the use of palmprints can boost the performance of hand geometry systems. Therefore, the development of biometric fusion schemes is an important area of study. The possibility of using biometric information to generate cryptographic keys is also an emerging area of study. Thus, there is a definite need for advanced signal processing, computer vision, and pattern recognition techniques to bring the current biometric systems to maturity and allow for their large-scale deployment.

11. REFERENCES

[1] A.K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for Video Technology 14 (1) (2004) 4–20.

[2] Andrea F. Abate, Michele Nappi, Daniel Riccio, Gabriele Sabatino, "2D and 3D face recognition: A survey", www.elsevier.com, 2007.

[3] Amit Mhatre, Srinivasa Palla, Sharat Chikkerur and Venu Govindaraju, "Efficient search and retrieval in biometric database", SPIE, Defence and Security Symposium, 2005.

[4] Davide Maltoni. Handbook of Fingerprint Recognition. Springer Verlag, 2003.

[5] Edmund Spinella, "Biometric Scanning Technologies: Finger, Facial and Retinal Scanning", SANS GSEC, Original Submission, San Francisco, CA Dec 2002, 28 May 2003.

[6] N. K. Ratha, J. H. Connell, R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems",IBM SYSTEMS JOURNAL, VOL 40, NO 3, 2001, pp 614- 634.

[7] Michael Zimmerman, "Biometrics And User Authentication".

[8] Patrick A. Wittich, "Biometrics: Are YOU the Key to Security?" Information Security Reading Room, SANS Institute 2003.

[9] Penny Khaw, "Iris Recognition Technology for Improved Authentication", As part of the Information Security Reading Room, SANS Institute 2002.

[10] R.L. Zunkel, Hand geometry based verification, in: A. Jain, R. Bolle, S. Pankanti (Eds.), Biometrics, Kluwer Academic Publishers, Dordrecht, 1999, pp. 87–101.

[11] S. Nanavati, M. Thieme, R. Nanavati, Biometrics: Identity Verification in a Networked World, pp. 123–131, Wiley, New York, 2002.

[12] Struif, Use of biometrics for user verification in electronic signature smartcards, E-smart 2001, Lecture Notes in Computer Science, Vol. 2140, Springer, Berlin, 2001, pp. 220–227.

[13] Tricia Olsson, "Strengthening Authentication with Biometric Technology", GSEC Practical, August 2003.

[14] Wayne Penny, "Biometrics: A Double Edged Sword - Security and Privacy", GSEC Certification Practical - Version 1.3.

[15] W.S. Wijesoma, K.W. Yue, K.L. Chien, T.K. Chow, Online Handwritten Signature Verification for Electronic Commerce over the Internet, WI 2001, LNAI 2198, 2001, pp. 227–236.