INTRODUCTION

Biometrics (Greek: *bios* ="life", *metron* ="measure") is the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Biometric Authentication - the automatic identification of living individuals by using their physiological and behavioral characteristics; "negative identification can only be accomplished through biometric identification"; "if a pin or password is lost or forgotten it can be changed and reissued but a biometric identification cannot" .

The fields of involvement of Biometric Analysis are as follows:-

DNA\Genetic Fingerprinting - Biometric identification obtained by examining a person's unique sequence of DNA base pairs; often used for evidence in criminal law cases.

Automatic face recognition, face recognition, facial recognition - Biometric identification by scanning a person's face and matching it against a library of known faces; "they used face recognition to spot known terrorists".

Fingerprint - Biometric identification from a print made by an impression of the ridges in the skin of a finger; often used as evidence in criminal investigations

Finger scan, finger scanning - Biometric identification by automatically scanning a person's fingerprints electronically

Iris scanning - Biometric identification by scanning the iris of the eye; "the structure of the iris is very distinctive"

Signature recognition - biometric identification by automatically scanning a person's signature and matching it electronically against a library of known signatures

Retinal scanning - biometric identification by scanning the retina of the eye; "identification by retinal scanning is complicated by eye movements"

Voiceprint - biometric identification by electronically recording and graphically representing a person's voice; "voiceprints are uniquely characteristic of individual speakers"

Identification - evidence of identity; something that identifies a person or thing

In **information technology**, *biometric authentication* refers to technologies that measure and analyzes human physical and behavioural characteristics for authentication purposes. Examples of physical (or physiological or biometric) characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of mostly behavioural characteristics include signature, gait and typing patterns. All behavioral biometric characteristics have a physiological component, and, to a lesser degree, physical biometric characteristics have a behavioral element.

Some researchers, have coined the term **behaviometrics** for behavioral biometrics such as typing rhythm or mouse gestures where the analysis can be done continuously without interrupting or interfering with user activities.

Operation and Performance

In a typical IT biometric system, a person registers with the system when one or more of his physical and behavioural characteristics are obtained. This information is then processed by a numerical algorithm, and entered into a database. The algorithm creates a digital representation of the obtained biometric. If the user is new to the system, he or she enrolls, which means that the digital template of the biometric is entered into the database. Each subsequent attempt to use the system, or authenticate, requires the biometric of the user to be captured again, and processed into a digital template. That template is then compared to those existing in the database to determine a match. The process of converting the acquired biometric into a digital template for comparison is completed each time the user attempts to authenticate to the system. The comparison process involves the use of a Hamming distance. This is a measurement of how similar two bit strings are. For example, two identical bit strings have a Hamming Distance of zero, while two totally dissimilar ones have a Hamming Distance of one. Thus, the Hamming distance measures the percentage of dissimilar bits out of the number of comparisons made. Ideally, when a user logs in, nearly his entire features match; then when someone else tries to log in, who does not fully match, and the system will not allow the new person to log in. Current technologies have widely varying Equal Error Rates, varying from as low as 60% and as high as 99.9%.

Performance of a biometric measure is usually referred to in terms of the false accept rate (FAR), the false non match or reject rate (FRR), and the failure to enroll rate (FTE or FER). The FAR measures the percent of invalid users who are incorrectly accepted as genuine users, while the FRR measures the percent of valid users who are rejected as impostors.

In real-world biometric systems the FAR and FRR can typically be traded off against each other by changing some parameter. One of the most common measures of real-world biometric systems is the rate at which both accept and reject errors are equal: the equal error rate (EER), also known as the cross-over error rate (CER). The lower the EER or CER, the more accurate the system is considered to be.

Stated error rates sometimes involve idiosyncratic or subjective elements. For example, one biometrics vendor set the acceptance threshold high, to minimize false accepts. In the trial, three attempts were allowed, and so a false reject was counted only if all three attempts failed. At the same time, when measuring performance biometrics (e.g. writing, speech etc.), opinions may differ on what constitutes a false reject. If a signature verification system is trained with an initial and a surname, can a false reject be legitimately claimed when it then rejects the signature incorporating a full first name?

Despite these misgivings, biometric systems have the potential to identify individuals with a very high degree of certainty. Forensic DNA evidence enjoys a particularly high degree of public trust at present (ca. 2004) and substantial claims are being made in respect of iris recognition technology, which has the capacity to discriminate between individuals with identical DNA, such as monozygotic twins.

Issues and concerns

As with many interesting and powerful developments of technology, there are concerns about biometrics. The biggest concern is the fact that once a fingerprint or other biometric source has been compromised it is compromised for life, because users can never change their fingerprints. Theoretically, a stolen biometric can haunt a victim for decades.

Identity theft and privacy issues

Concerns about Identity theft through biometrics have not been resolved. If a person's credit card number is stolen, for example, it can cause them great difficulty since this information can be used in situations where the security system requires only "single-factor" authentication; i.e., just knowing the credit card number and its expiration date can sometimes be enough to use a stolen credit card successfully. “Two-factor” security solutions require something you know plus something you have; for example, a debit card and a personal Identification Number (PIN) or a biometric. Some argue that if a person's biometric data is stolen it might allow someone else to access personal information or financial accounts, in which case the damage could be irreversible. But this argument ignores a key operational factor intrinsic to all biometrics-based security solutions; biometric solutions are based on matching, at the point of transaction, the information obtained by the scan of a "live" biometric sample to a prestored, static "match template" created when the user originally enrolled in the security system. Most of the commercially-available biometric systems address the issues of ensuring that the static enrollment sample has not been tampered with (i.e., using hash codes and encryption), so the problem is effectively limited to cases where the scanned "live" biometric data is hacked. Even then, most competently-designed solutions contain anti-hacking routines. For example, the scanned "live" image is virtually never the same from scan-to-scan owing to the inherent plasticity of biometrics; ironically, a "replay" attack using the stored biometric is easily detected because it is too perfect a match.

Marketing of biometric products

Despite confirmed cases of defeating commercially available biometric scanners, many companies marketing biometric products (especially consumer level products such as readers built into keyboards) still claim the products as replacements, rather than suppliments, of passwords. Furthermore, regulations regarding advertising and manufacturing of biometric products are (as of 2006) largely non-existent. Given the low security, consumer level products are most likely to be bought and used by most people, the end result can theoretically lead to large scale economical and social problems associated with biometric identity theft.

Sociological concerns

As technology advances, and time goes on, more and more private companies and public utilities will use biometrics for safe, accurate identification. However, these advances will raise many concerns throughout society, where many may not be educated on the methods. Here are some examples of concerns society has with biometrics:

- Physical - Some believe this technology can cause physical harm to an individual using the methods, or that instruments used are unsanitary. For example, there are concerns that retina scanners might not always be clean.

- Personal Information - There are concerns whether our personal information taken through biometric methods can be misused, tampered with, or sold, e.g. by criminals stealing, rearranging or copying the biometric data. Also, the data obtained using biometrics can be used in unauthorized ways without the individual's consent.

Danger to owners of secured items

When thieves cannot get to secure properties, there is a chance that thieves will stalk and assault property owner to gain access. If the item is secured with biometric device, the damage to the owner can become irreversible, and potentially cost more than the secured properties. In 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car.

Uses and initiatives

Biometrics being a wide field of application is being used in several different ways in different countries since the Ethical, Logical, Social Issues vary from country to country. The description of biometric analysis for some countries in which it is applied oftenly for various purposes.

Brazil

Since the beginning of the 20th century, Brazilian citizens have used ID cards. The decision by the Brazilian government to adopt fingerprint-based biometrics was spearheaded by Dr. Felix Pacheco at Rio de Janeiro, at that time capital of the Federative Republic. Dr. Pacheco was a friend of Dr. Juan Vucetich, who invented one of the most complete tenprint classification systems in existence. The Vucetich system was adopted not only in Brazil, but also by most of the other South American countries. The oldest and most traditional ID Institute in Brazil (Instituto de Identificação Félix Pacheco) was integrated at DETRAN [3] (Brazilian equivalent to DMV) into the civil and criminal AFIS system in 1999.

Each state in Brazil is allowed to print its own ID card, but the layout and data are the same for all of them. The ID cards printed in Rio de Janeiro are fully digitized using a 2D bar code with information which can be matched against its owner off-line. The 2D bar code encodes a color photo, a signature, two fingerprints, and other citizen data. This technology was developed in 2000 in order to enhance the safety of the Brazilian ID cards.

At the end of 2005, the Brazilian government started the development of its new passport. The soon to be released new passport will include several security features. Brazilian citizens will have their signature, photo, and 10 rolled fingerprints collected during passport requests. All of the data is planned to be stored in ICAO E-passport standard. This allows for contactless electronic reading of the passport content and Citizens ID verification since fingerprint templates and token facial images will be available for automatic recognition. The project is expected to go into operation phase by the second semester of 2006.

United States

The United States government has become a strong advocate of biometrics with the increase in security concerns in recent years, since September 11, 2001. Starting in 2005, US passports with facial (image-based) biometric data were scheduled to be produced. Privacy activists in many countries have criticized the technology's use for the potential harm to civil liberties, privacy, and the risk of identity theft. Currently, there is some apprehension in the United States (and the European Union) that the information can be "skimmed" and identify people's citizenship remotely for criminal intent, such as kidnapping. There also are technical difficulties currently delaying biometric integration into passports in the United States, the United Kingdom, and the rest of the EU.

These difficulties include compatibility of reading devices, information formatting, and nature of content (e.g. the US currently expect to use only image data, whereas the EU intends to use fingerprint and image data in their passport RFID biometric chip(s)).

The speech made by President Bush on May 15, 2006, live from the Oval Office, was very clear: from now on, anyone willing to go legally in the United States in order to work there will be card-indexed and will have to communicate his fingerprints while entering the country. Many foreigners will have to subject themselves to these procedures, formerly only imposed to criminals and to spies, not to immigrants and visitors, and even less to citizens.

"A key part of that system [for verifying documents and work eligibility of aliens] should be a new identification card for every legal foreign worker. This card should use biometric technology, such as digital fingerprints, to make it tamper-proof." President George W Bush (Addresses on Immigration Reform, May 15, 2006)

The US Department of Defense (DoD) Common Access Card, is an ID card issued to all US Service personnel and contractors on US Military sites. This card contains biometric data and digitized photographs. It also has laser-etched photographs and holograms to add security and reduce the risk of falsification. There have been over 10 million of these cards issued.

According to Jim Wayman, director of the National Biometric Test Center at San Jose State University, Walt Disney World is the nation's largest single commercial application of biometrics. However, the US Visit program will very soon surpass Mickey's kingdom for biometrics deployment.

Germany

The biometrics market in Germany will experience enormous growth until 2009. “The market size will increase from approximately 12 million € (2004) to 377 million €” (2009). “The federal government will be a major contributor to this development”. In particular, the biometric procedures of fingerprint and facial recognition can profit from the government project . In May 2005 the German Upper House of Parliament approved the implementation of the ePass, a passport issued to all German citizens which contain biometric technology. The ePass has been in circulation since November 2005, and contains a chip that initially will hold a digital photo of the holder's face. “Starting in March 2007, fingerprints also will be stored on the chips – one from each hand”. “A third biometric identifier – iris scans – could be added at a later stage”. An increase in the prevalence of biometric technology in Germany is an effort to not only keep citizens safe within German borders but also to comply with the current US deadline for visa-waiver countries to introduce biometric passports. In addition to producing biometric passports for German citizens, the German government has put in place new requirements for visitors for apply for visas within the country. “Only applicants for long-term visas, which allow more than three months' residence, will be affected by the planned biometric

registration program. The new work visas will also include fingerprinting, iris scanning, and digital photos".

Germany is also one of the first countries to implement biometric technology at the Olympic Games to protect German athletes. "The Olympic Games is always a diplomatically tense affair and previous events have been rocked by terrorist attacks - most notably when Germany last held the Games in Munich in 1972 and 11 Israeli athletes were killed".

Biometric technology was first used at the Olympic Summer Games in Athens, Greece in 2004. "On registering with the scheme, accredited visitors will receive an ID card containing their fingerprint biometrics data that will enable them to access the 'German House'. Accredited visitors will include athletes, coaching staff, team management and members of the media".

Identity theft and privacy issues

Concerns about Identity theft through biometrics have not been resolved. If a person's credit card number is stolen, for example, it can cause them great difficulty since this information can be used in situations where the security system requires only "single-factor" authentication; i.e., just knowing the credit card number and its expiration date can sometimes be enough to use a stolen credit card successfully. “Two-factor” security solutions require something you know plus something you have; for example, a debit card and a personal Identification Number (PIN) or a biometric. Some argue that if a person's biometric data is stolen it might allow someone else to access personal information or financial accounts, in which case the damage could be irreversible. But this argument ignores a key operational factor intrinsic to all biometrics-based security solutions; biometric solutions are based on matching, at the point of transaction, the information obtained by the scan of a "live" biometric sample to a prestored, static "match template" created when the user originally enrolled in the security system. Most of the commercially-available biometric systems address the issues of ensuring that the static enrollment sample has not been tampered with (i.e., using hash codes and encryption), so the problem is effectively limited to cases where the scanned "live" biometric data is hacked. Even then, most competently-designed solutions contain anti-hacking routines. For example, the scanned "live" image is virtually never the same from scan-to-scan owing to the inherent plasticity of biometrics; ironically, a "replay" attack using the stored biometric is easily detected because it is too perfect a match.

The television program Mythbusters attempted to break into a commercial security door equipped with biometric authentication as well as a personal laptop so equipped. While the laptop's system proved more difficult to bypass, the advanced commercial security door with "live" sensing was fooled with a printed scan of a fingerprint after it had been licked. Assuming the tested security door is representative of the current typical state of biometric authentication, that it was so easily bypassed suggests biometrics may not yet be reliable as a strong form of authentication.

Facial recognition system

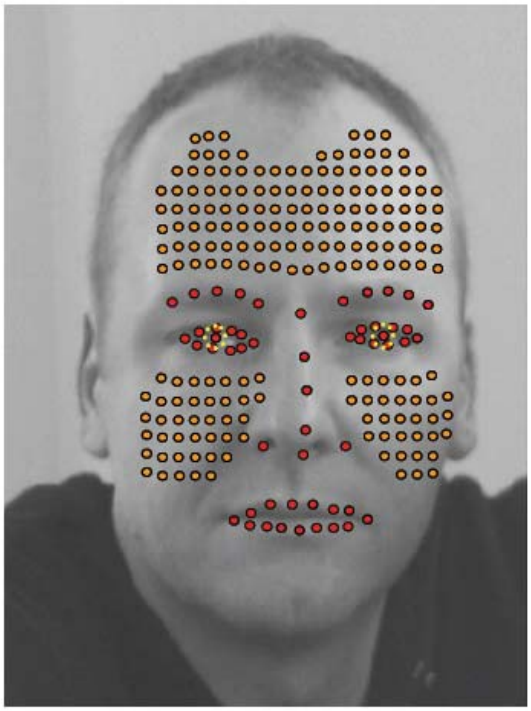
A **facial recognition system** is a computer-driven application for automatically identifying a person from a digital image. It does that by comparing selected facial features in the live image and a facial database.

It is typically used for security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.

Popular recognition algorithms include eigenface, fisherface, the Hidden Markov model, and the neuronal motivated Dynamic Link Matching. A newly emerging trend, claimed to achieve previously unseen accuracies, is three-dimensional face recognition. Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. Tests on the FERET database, the widely used industry benchmark, showed that this approach is substantially more reliable than previous algorithms.

SIMBA™

Single-Image Multiple Biometric Analysis



- 2D high resolution images allow the seamless integration of **Facial Feature**, **Skin Texture** and **Iris** Analysis into a single recognition engine
- Required resolution in pixels between the eyes:
  - Facial feature >25*
  - Skin texture >80*
  - Iris >600*

(6 Megapixel Camera)

Uses of Face Recognition System

In addition to being used for security systems, authorities have found a number of other applications for facial recognition systems.

At Super Bowl XXXV in January 2000, police in Tampa Bay, Florida, used FaceIt to search for potential criminals and terrorists in attendance at the event.(it found 19 people with pending arrest warrants)

In the 2000 presidential election, the Mexican government employed facial recognition software to prevent voter fraud. Some individuals had been registering to vote under several different names, in an attempt to place multiple votes. By comparing new facial images to those already in the voter database, authorities were able to reduce duplicate registrations. Similar technologies are being used in the United States to prevent people from obtaining fake identification cards and driver's licenses.

There are also a number of potential uses for facial recognition that are currently being developed. For example, the technology could be used as a security measure at ATM's; instead of using a bank card or personal identification number, the ATM would capture an image of your face, and compare it to your photo in the bank database to confirm your identity. This same concept could also be applied to computers; by using a webcam to capture a digital image of yourself, your face could replace your password as a means to log-in.

Criticisms of the Face recognition System

Efficacy

Critics of the technology complain that the London Borough of Newham scheme has, as of 2004, never recognised a single criminal, despite several criminals in the system's database living in the Borough and the system having been running for several years. "Not once, as far as the police know, has Newham's automatic facial recognition system spotted a live target." This information seems to conflict with that given by Identix's press release of April 2001, where they claim the system was credited with a 34% reduction in crime - which better explains why the system was then rolled out to Birmingham also.

An experiment by the local police department in Tampa, Florida, had similarly disappointing results.

"Camera technology designed to spot potential terrorists by their facial characteristics at airports failed its first major test at Boston's Logan Airport"

Privacy concerns

Despite the potential benefits of this technology, many citizens are concerned that their privacy will be invaded. Some fear that it could lead to a "total surveillance society," with the government and other authorities having the ability to know where you are, and what you are doing, at all times.

Early developments

Pioneers of Automated Facial Recognition include: Woody Bledsoe, Helen Chan Wolf, and Charles Bisson.

During 1964 and 1965, Bledsoe, along with Helen Chan and Charles Bisson, worked on using the computer to recognize human faces (Bledsoe 1966a, 1966b; Bledsoe and Chan 1965). He was proud of this work, but because the funding was provided by an unnamed intelligence agency that did not allow much publicity, little of the work was published. Given a large database of images (in effect, a book of mug shots) and a photograph, the problem was to select from the database a small set of records such that one of the image records matched the photograph. The success of the method could be measured in terms of the ratio of the answer list to the number of records in the database. Bledsoe (1966a) described the following difficulties:

This recognition problem is made difficult by the great variability in head rotation and tilt, lighting intensity and angle, facial expression, aging, etc. Some other attempts at facial recognition by machine have allowed for little or no variability in these quantities. Yet the method of correlation (or pattern matching) of unprocessed optical data, which is often used by some researchers, is certain to fail in cases where the variability is great. In particular, the correlation is very low between two pictures of the same person with two different head rotations.

This project was labeled man-machine because the human extracted the coordinates of a set of features from the photographs, which were then used by the computer for recognition. Using a graphics tablet (GRAFACON or RAND TABLET), the operator would extract the coordinates of features such as the center of pupils, the inside corner of eyes, the outside corner of eyes, point of widows peak, and so on. From these coordinates, a list of 20 distances, such as width of mouth and width of eyes, pupil to pupil, were computed. These operators could process about 40 pictures an hour. When building the database, the name of the person in the photograph was associated with the list of computed distances and stored in the computer. In the recognition phase, the set of distances was compared with the corresponding distance for each photograph, yielding a distance between the photograph and the database record. The closest records are returned.

Field Identification Issues

- Problem
  - Positive identification of people is time consuming and often inaccurate
  - Processing people at a booking station is expensive
  - Mistaken identity can lead to false arrests
- Solution
  - Fast, in-field identification of persons and vehicles using a handheld device
  - Multi-biometrics guarantees positive ID (face, skin, iris, fingerprint)
  - Embedded database of identities or wireless connection to background servers to ensure widest match

This brief description is an oversimplification that fails in general because it is unlikely that any two pictures would match in head rotation, lean, tilt, and scale (distance from the camera). Thus, each set of distances is normalized to represent the face in a frontal orientation. To accomplish this normalization, the program first tries to determine the tilt, the lean, and the rotation. Then, using these angles, the computer undoes the effect of these transformations on the computed distances. To compute these angles, the computer must know the three-dimensional geometry of the head. Because the actual heads were unavailable, Bledsoe (1964) used a standard head derived from measurements on seven heads.

After Bledsoe left PRI in 1966, this work was continued at the Stanford Research Institute, primarily by Peter Hart. In experiments performed on a database of over 2000 photographs, the computer consistently outperformed humans when presented with the same recognition tasks (Bledsoe 1968). Peter Hart (1996) enthusiastically recalled the project with the exclamation, "It really worked!"

Comparative study

Among the different biometric techniques facial recognition may not be the most reliable and efficient but its great advantage is that it does not require aid from the test subject. Properly designed systems installed in airports, multiplexes, and other public places can detect presence of criminals among the crowd. Other biometrics like fingerprints, iris, and speech recognition cannot perform this kind of mass scanning. However, questions have been raised on the effectiveness of facial recognition software in cases of railway and airport security.

Three-dimensional face recognition

Three-dimensional face recognition (3D face recognition) is a modality of facial recognition methods in which the three-dimensional geometry of the human face is used. It has been shown that 3D face recognition methods can achieve significantly higher accuracy than their 2D counterparts, rivaling fingerprint recognition.

3D face recognition achieves better accuracy than its 2D counterpart by measuring geometry of rigid features on the face.[citation needed] This avoids such pitfalls of 2D face recognition algorithms as change in lighting, different facial expressions, make-up and head orientation. Another approach is to use the 3D model to improve accuracy of traditional image based recognition by transforming the head into a known view.

The main technological limitation of 3D face recognition methods is the acquisition of 3D images, which usually requires a range camera. This is also a reason why 3D face recognition methods have emerged significantly later (in the late 1980s) than 2D methods. Recently commercial solutions have implemented depth perception by projecting a grid onto the face and integrating video capture of it into a high resolution 3D model. This allows for good recognition accuracy with low cost off-the-shelf components.

Currently, 3D face recognition is still an open research field, though several vendors already offer commercial solutions.

Iris recognition

Iris recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the irides of an individual's eyes. Not to be confused with another less prevalent ocular-based technology, retina scanning, iris recognition uses camera technology, and subtle IR illumination to reduce specular reflection from the convex cornea to create images of the detail-rich, intricate structures of the iris. These unique structures converted into digital templates, provide mathematical representations of the iris that yield unambiguous positive identification of an individual.

Iris recognition efficacy is rarely impeded by glasses or contact lenses. Iris technology has the smallest outlier (those who cannot use/enroll) group of all biometric technologies. The only biometric authentication technology designed for use in a one-to many search environment, a key advantage of iris recognition is its stablity, or template longevity as, barring trauma, a single enrollment can last a lifetime.

Breakthrough work to create the iris recognition algorithms required for image acquisition and one-to-many matching was pioneered by John G. Daugman, Ph.D, OBE (University of Cambridge Computer Laboratory), who holds key patents on the method. These were utilized to effectively debut commercialization of the technology in conjunction with an early version of the IrisAccess system designed and manufactured by Korea's LG Electronics. Daugman's algorithms are the basis of almost all currently (as of 2006) commercially deployed iris-recognition systems. It has a so far unmatched practical false-accept rate of zero; that is there is no known pair of images of two different irises that the Daughman algorithm in its deployed configuration mistakenly identifies as the same. (In tests where the matching thresholds are – for better comparability – changed from their default settings to allow a false-accept rate in the region, the IrisCode false-reject rates are comparable to the most accurate single-finger fingerprint matchers.

Iris Recognition Channel
Final Step

- To achieve optimal integration Neven Vision will develop proprietary iris analysis
- Key questions revolve around optimal wavelength regimes

Operating principle

An iris-recognition algorithm first has to identify the approximately concentric circular outer boundaries of the iris and the pupil in a photo of an eye. The set of pixels covering only the iris is then transformed into a bit pattern that preserves the information that is essential for a statistically meaningful comparison between two iris images. The mathematical methods used resemble those of modern lossy compression algorithms for photographic images. In the case of Daugman's algorithms, a Gabor wavelet transform is used in order to extract the spatial frequency range that contains a good best signal-to-noise ratio considering the focus quality of available cameras. The result are a set of complex numbers that carry local amplitude and phase information for the iris image. In Daugman's algorithms, all amplitude information is discarded, and the resulting 2048 bits that represent an iris consist only of the complex sign bits of the Gabor-domain representation of the iris image. Discarding the amplitude information ensures that the template remains largely unaffected by changes in illumination and virtually negligibly by iris color, which contributes significantly to the long-term stability of the biometric template. To authenticate via identification (one-to many template matching) or verification (one-to one template matching) a template created by imaging the iris, is compared to a stored value template in a database. If the Hamming Distance is below the decision threshold, a positive identification has effectively been made.

A practical problem of iris recognition is that the iris is usually partially covered by eye lids and eye lashes. In order to reduce the false-reject risk in such cases, additional algorithms are needed to identify the locations of eye lids and eye lashes, and exclude the bits in the resulting code from the comparison operation.

Advantages

The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons:

It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor.

The iris is mostly flat and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae), which control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face.
The iris has a fine texture that – like fingerprints – is determined randomly during embryonic gestation. Even genetically identical individuals have completely independent iris textures, whereas DNA (genetic "fingerprinting") is not unique for the about 1.5% of the human population who have a genetically identical monozygotic twin.
An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person to be identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against finger-print scanners, where a finger has to touch a surface, or retinal scanning, where the eye can be brought very close to a lens (like looking into a microscope lens).
Some argue that a focused digital photograph with an iris diameter of about 200 pixels contains much more long-term stable information than a fingerprint.
The only currently commercially deployed iris recognition algorithm, John Daugman's IrisCode, has an unprecedented false match rate (better than 10-11). Not a single false match has ever been reported for this algorithm, which has already been used to cross-compare more than 200 billion combinations of iris pairs as part of the immigration procedures in the United Arab Emirates.
While there are some medical and surgical procedures that can affect the colour and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identification have succeeded over a period of about 30 years.

]Disadvantages

Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into finger-print recognition.
Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera.
As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates. [4]
As with other identification infrastructure (national residents databases, ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will.

Security considerations

Like with most other biometric identification technology, a still not satisfactorily solved problem with iris recognition is the problem of "live tissue verification". The reliability of any biometric identification depends on ensuring that the signal acquired and compared has actually been recorded from a live body part of the person to be identified, and is not a manufactured template. Many commercially available iris recognition systems are easily fooled by presenting a high-quality photograph of a face instead of a real face, which makes such devices unsuitable for unsupervised applications, such as door access-control systems. The problem of live tissue verification is less of a concern in supervised applications (e.g., immigration control), where a human operator supervises the process of taking the picture.

Methods that have been suggested to provide some defence against the use of fake eyes and irises include:

Changing ambient lighting during the identification (switching on a bright lamp), such that the pupillary reflex can be verified and the iris image be recorded at several different pupil diameters
Analysing the 2D spatial frequency spectrum of the iris image for the peaks caused by the printer dither patterns found on commercially available fake-iris contact lenses
Analysing the temporal frequency spectrum of the image for the peaks caused by computer displays
Using spectral analysis instead of merely monochromatic cameras to distinguish iris tissue from other material
Observing the characteristic natural movement of an eyeball (measuring nystagmus, tracking eye while text is read, etc.)
Testing for retinal retro-reflection (red-eye effect)
Testing for reflections from the eye's four optical surfaces (front and back of both cornea and lens) to verify their presence, position and shape
Using 3D imaging (e.g., stereo cameras) to verify the position and shape of the iris relative to other eye features

A 2004 report by the German Federal Office for Information Security noted that none of the iris-recognition systems commercially available at the time implemented any live-tissue verification technology. Like any pattern-recognition technology, live-tissue verifiers will have their own false-reject probability and will therefore further reduce the overall probability that a legitimate user is accepted by the sensor.

Deployed applications

A U.S. Marine Corps Sergeant uses an iris scanner to positively identify a member of the Baghdaddi city council prior to a meeting with local tribal figureheads, sheiks, community leaders and U.S. service members. One of three biometric identification technologies internationally standardized by ICAO for use in future passports (the other two are fingerprint and face recognition)
At Schiphol Airport, Netherlands, iris recognition has permitted passport free immigration since 2001
United Arab Emirates border control at all 17 air, land and seas ports since 2001
UK's IRIS - Iris Recognition Immigration System
Used to verify the recognition of the "Afghan Girl" (Sharbat Gula) by National Geographic photographer Steve McCurry.
In several Canadian airports, as part of the CANPASS Air program that facilitates entry into Canada for pre-approved, low-risk air travellers.

Iris recognition in fiction

Steven Spielberg's 2002 science fiction film Minority Report depicts a society in which what appears to be a form of iris recognition has become daily practice. A main character has an eye transplant in order to change his identity.

Retinal scan

A retinal scan is a biometric technique that uses the unique patterns on a person's retina to identify them.

The human retina is stable from birth to death, making it the most accurate biometric to measure. It has been possible to take a retina scan since the 1930s, when research suggested that each individual had unique retina patterns. The research was validated and we know that the blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person. A retinal scan involves the use of a low-intensity light source and coupler that are used to read the blood vessel patterns, producing very accurate biometric data. It has the highest crossover accuracy of any of the biometric collectors, estimated to be in the order of 1:10,000,000.

Development of the technology has taken longer than expected and for many years the process of taking a retinal scan was measured in tens of seconds. New technology is capable of capturing a retinal scan in less than 1 second.

Some biometric identifiers, like fingerprints, can be fooled. This is not the case with a retina scan. The retina of a deceased person quickly decays and cannot be used to deceive a retinal scan. It is for this reason that retina scan technology is used for high end access control security applications.

As of 2006, some parts of the American Department of Energy were using retinal scanners for identification purposes.

DNA Fingerprinting and its Applications in Biometric Analysis.

The chemical structure of everyone's DNA is the same. The only difference between people (or any animal) is the order of the base pairs. There are so many millions of base pairs in each person's DNA that every person has a different sequence.

Using these sequences, every person could be identified solely by the sequence of their base pairs. However, because there are so many millions of base pairs, the task would be very time-consuming. Instead, scientists are able to use a shorter method, because of repeating patterns in DNA.

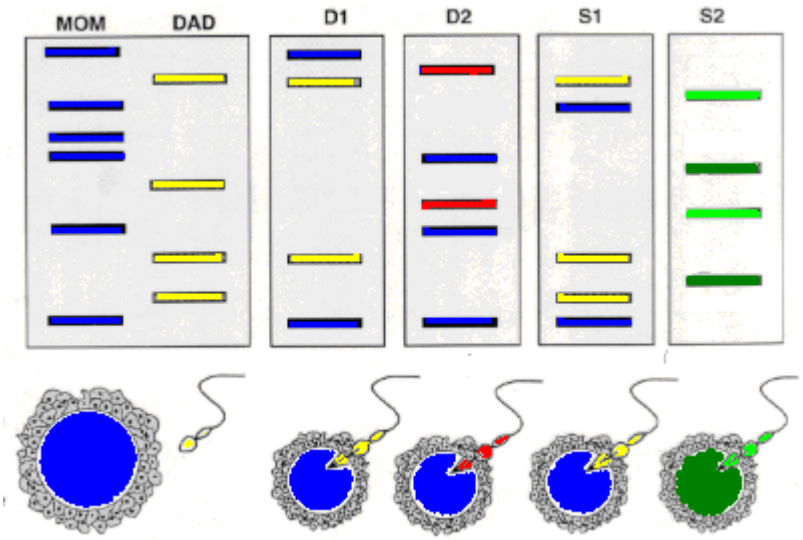
These patterns do not, however, give an individual "fingerprint," but they are able to determine whether two DNA samples are from the same person, related people, or non-related people. Scientists use a small number of sequences of DNA that are known to vary among individuals a great deal, and analyze those to get a certain probability of a match.

How is DNA Fingerprinting done?

Every strand of DNA has pieces that contain genetic information which informs an organism's development (exons) and pieces that, apparently, supply no relevant genetic information at all (introns). Although the introns may seem useless, it has been found that they contain repeated sequences of base pairs. These sequences, called Variable Number Tandem Repeats (VNTRs), can contain anywhere from twenty to one hundred base pairs.

Every human being has some VNTRs. To determine if a person has a particular VNTR, a Southern Blot is performed, and then the Southern Blot is probed, through a hybridization reaction, with a radioactive version of the VNTR in question. The pattern which results from this process is what is often referred to as a DNA fingerprint.

A given person's VNTRs come from the genetic information donated by his or her parents; he or she could have VNTRs inherited from his or her mother or father, or a combination, but never a VNTR either of his or her parents do not have. Shown below are the VNTR patterns for Mrs. Nguyen [blue], Mr. Nguyen [yellow], and their four children: D1 (the Nguyens' biological daughter), D2 (Mr. Nguyen's step-daughter, child of Mrs. Nguyen and her former husband [red]), S1 (the Nguyens' biological son), and S2 (the Nguyens' adopted son, not biologically related [his parents are light and dark green]).



Because VNTR patterns are inherited genetically, a given person's VNTR pattern is more or less unique. The more VNTR probes used to analyze a person's VNTR pattern, the more distinctive and individualized that pattern, or DNA fingerprint, will be.

Some Concerns on the Measurement for Biometric Analysis and Applications

Some concerns of measurement for biometric analysis and synthesis are investigated. This research tries to reexamine the nature of the basic definition of measurement of distance between two objects or image patterns, which is essential for comparing the similarity of patterns. According to a recent International Workshop on Biometric Technologies: Modeling and Simulation at University of Calgary, Canada [Yanushkevich et al., Eds. (2004)], biometric refers to the studies of analysis, synthesis, modeling and simulation of human behavior by computers, including mainly recognition of hand printed words, machines printed characters, handwriting, fingerprint, signature, facial expression, speech, voice, emotion and iris etc.The key idea is the measurement that defines the similarity between different input data that can be represented by image data. This paper deals with the very fundamental phenomena of measurement of these studies and analysis. Preliminary findings and observations show that the concepts of segmentation and disambiguation are extremely important, which have been long ignored. Even while computer and information professionals and researchers have spent much effort , energy, and time, trying very hard and diligently to develop methods that may reach as high as 99.9999 % accuracy rate for character and symbol recognition, a poorly or ill considered pre-designed board poster or input pattern could easily destroy its effectiveness and lower the overall performance accurate rate to less than 50%. The more data it handles, the worse the results. Its overall performance accuracy rate will be proportionally decreasing.

Overview (Introduction)

We first briefly review what's happening in biometric research and their results. According to [Int. biometric group (2003)], a majority of biometric studies fall into the categories of fingerprint, facial and symbol analysis and recognition, about 74%. It can be shown in the Fig. 3.1.

Inverse methods in analysis examples are shown in [Plamondon and Srihari (2000)], [Popel (2006)], [Yanushkevich et al.(2005)] (Fig. 3.2):
(a) Modeling, or tampering (e.g. signature forgery in the task of signature recognition)

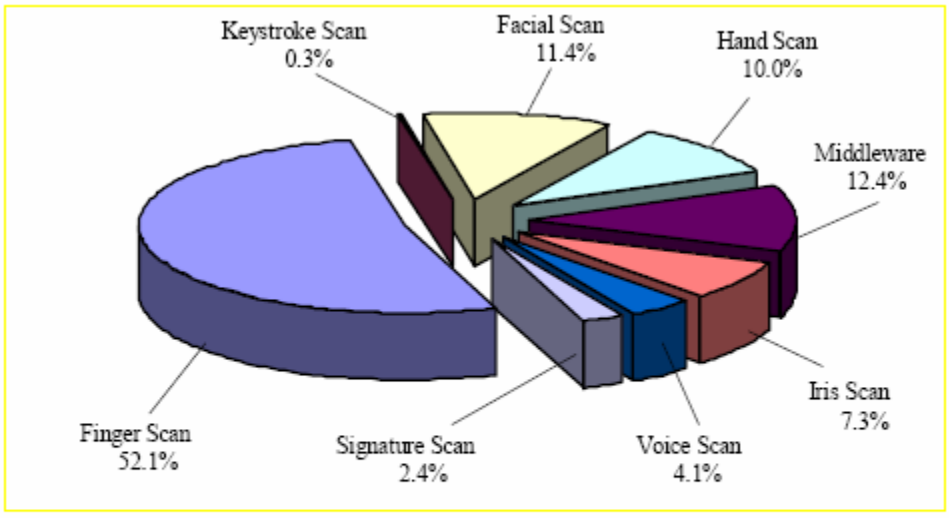


Fig. 3.1 Percentage of Biometric Applications in real life [Int. biometric group (2003)], in which *biometrics* are defined as automated methods of recognizing a person based on the acquired physiological or behavioral characteristics

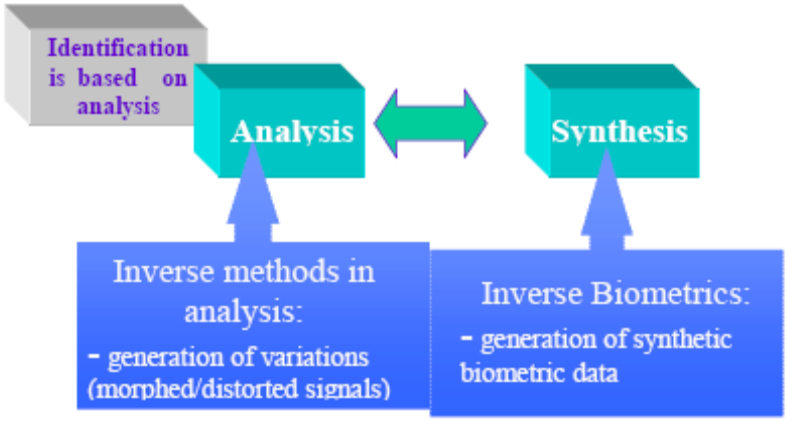


Fig. 3.2 Analysis and Synthesis of biometric images

(b) Voice synthesis (telecommunication services), and
(c) Facial image synthesis (animation, \talking heads").
There are also some developments of generating synthetic biometric data, using computer graphics, computational geometry methodologies, with applications to the following fields, which are being implemented successfully [Jain et al. (2005)], [Jain and Uludag (2003)], [Ma et al. (2005)], [Ratha et al. (2001)], ?? [Zhang et al. (2004)], [Zhang et al. (2001)]:
(a) Collecting large databases for testing the robustness of identification systems,
(b) Training personnel on a system that deploys simulation of biometric data,
(c) Cancelable biometrics,
(d) Biometric Data Hiding, and
(e) Biometric Encryption.
Further, according to a most recent book regarding advanced aspects of biometrics Handbook of Multibiometrics [Ross et al. (2006)], consistent advances in biometrics help to address problems that plague traditional human recognition methods and offer significant promise for applications in security as well as general convenience. In particular, newly evolving systems can measure multiple physiological or behavioral traits and thereby increase overall reliability that much more. Multimodal Biometrics provides an accessible, focused examination of the science and technology behind multimodal human recognition systems, as well as their ramifications for security systems and other areas of application. After clearly introducing multibiometric systems, it demonstrates the noteworthy advantages of these systems over their traditional and unimodal counterparts. In addition, the work describes the various scenarios possible when consolidating evidence from multiple biometric systems and examines multimodal system design and methods for computing user-specific parameters. In another book about general biometrics systems which was published by Springer [Wayman et al.(2005)], which provides an overview of the principles and methods needed to build reliable biometric systems. It covers 3 main topics: key biometric technologies, testing and management issues, and the legal and system considerations of biometric systems for personal verification/identification. It focuses on the four most widely used technologies - speech, fingerprint, iris and face recognition. It includes: (a) In-depth coverage of the technical and practical obstacles which are often neglected by application developers and system integrators and which result in shortfalls between expected and actual performance,
(b) Detailed guidelines on biometric system evaluation, and
(c) Protocols and benchmarks which will allow developers to compare performance and track system improvements.
The book of Biometric Systems - Technology, Design and Performance Evaluation is intended as a reference book for anyone involved in the design, management or implementation of biometric systems.
According to a recent paper regarding metric learning for text documentation analysis and understanding [Lebanon (2006)], many algorithms in machine learning rely on being given a good distance metric over the input space. Rather than using a default metric such as the Euclidean metric, it is desirable to obtain a metric based on the provided data. We

consider the problem of learning a Riemannian metric associated with a given differentiable manifold and a set of points. Their approach to the problem involves choosing a metric from a parametric family that is based on maximizing the inverse volume of a given data set of points. From a statistical perspective, it is related to maximum likelihood under a model that assigns probabilities inversely proportional to the Riemannian volume element. We discuss in detail learning a metric on the multinomial simplex where the metric candidates are pull-back metrics of the Fisher information under a Lie group of transformations. When applied to text document classification the resulting geodesic distance resemble, but outperform, the tfidf cosine similarity measure.

In the literature, there is another recent book regarding some guidance to biometrics published in 2004 [Bolle et al. (2004)]. This complete, technical guide offers some rather detailed descriptions and analysis of the principles, methods, technologies, and core ideas used in biometric April 10, 2006 22:48 WSPC/Book Trim Size for 9in x 6in Main_WorldSc_IPR_SAB Some Concerns on the Measurement for Biometric 21 authentication systems. It explains the definition and measurement of performance and examines the factors involved in choosing between different biometrics. It also delves into practical applications and covers a number of topics critical for successful system integration. These include recognition accuracy, total cost of ownership, acquisition and processing speed, intrinsic and system security, privacy and legal requirements, and user acceptance. From above investigations, it can be seen that most recent development and applications largely rely on the fundamental definition of pattern matching, which in turn depends on the measurement of distances between two input images. It has been observed that the concept of ambiguity plays a very important fundamental roles of all these distance measurement and image pattern processing in both learning (analysis) and recognition (synthesis), which is also the most difficult obstacles of essentially all recognition problems in the real daily life. Therefore in the next section, we are going to discuss these problems and how input images (patterns) can and should be disambiguated in dealing with real life problem applications.

Biometrics perspectives for IT Sector

IT security biometrics is the study on person recognition methods based on the sensing of a person's biological characteristics, measuring of the captured or scanned biometric characteristics (raw data and sensor system calibration data), computing of biometric signatures and biometric templates, and verifying and identifying against biometric templates and (hashed) biometric signatures with regard to the mathematical definitions of metrics and metric spaces. The (hashed) biometric signatures are used for authentication purposes against and identification and surveillance purposes by IT systems within ICT infrastructures.

Privacy : Privacy is everyone's fundamental human right, which is documented in the Universal Declaration of Human Rights by the General Assembly of the United Nations [16]. In this paper a definition of privacy by Westin from is used: "Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others". Fischer-Hfubner formulates in [14] basic privacy principles, which summarize the most essential privacy requirements. Concerning the analysis of risks for privacy in biometric IT systems, the discussion focusses on the privacy principles of purpose binding and necessity of data collection. The principle of purpose binding limits the subsequent use of personal data to the specified purposes. The principle of necessity of data collection means to avoid or at least to minimize personal data within an ICT system.

A biometric authentication system is defined as a set of hardware components, processes, algorithms, data structures, and databases fulfilling internal and/or external communication between the elements for the purpose of biometric authentication.

A threat to biometric authentication technology is the potential of a circumstance or an action that causes loss of security, degradation of the technology's reliability or performance, or the harm to a person's privacy. The vulnerability of biometric authentication technology is a flaw or weakness that makes it possible for a threat to biometric authentication technology to occur.

A security risk of biometric authentication technology is an expectation of loss expressed as the probability that a specific threat to biometric authentication technology will be exploited against a specific vulnerability of biometric authentication technology with potentially hazardous consequences and effects.

Biometric enrollment is the process of training a person's biometric(characteristics|patterns) into a biometric person recognition system and storing of the biometric data in a biometric database. Biometric authentication is the process of verifying a person's claimed identity by comparison of a computed biometric signature from the person's biometric (characteristics|patterns) against a stored biometric template. Biometric derollment is the process of detraining a person's biometric (characteristics|patterns) from a biometric person recognition system and removal of the biometric data from a biometric database.

In the broader sense a biometric(enrollment | authentication | derollment) algorithm is an algorithm for the enrollment, authentication, or derollment of a person's biometric characteristics against a biometric (authentication|identification system or abortion of an attempt. In the narrower sense a biometric algorithm is a biometric signal processing algorithm used within (en|de)rollment and authentication.

A biometric signature is a (binary coded representation of biometric characteristics for (distributed) computing systems. A biometric template is a biometric signature (class|cluster) representing a set of biometric signatures. Biometric signatures/templates can be hashed which results in hashed biometric signatures templates.

Biometric Databases.
A biometric database is a database which holds data about biometric characteristics, biometric signatures, and personal data. A biometric database which subsumes biometric characteristics (raw data and calibration data), biometric signatures, personal data, and a rule-based access control mechanism is defined to be a complete biometric database. A partial biometric database represents a subset of a complete biometric database.

Biometric Communication Channels. A threat for biometric authentication via insecure networks is given by replay attacks. A concept of a technical solution for this problem is presented in Figure 2 by using an active sensor system with an emitter for security information, which is controlled over a control channel by a biometric authentication server. The biometric raw data with the added security information is captured and transferred to the server over the data channel. The server accepts received biometric raw data, if the expected and valid security information is included. The cryptographic secured control and data channels, the active sensor system and security information enhanced biometric raw data are defined together as secure biometric communication channels.

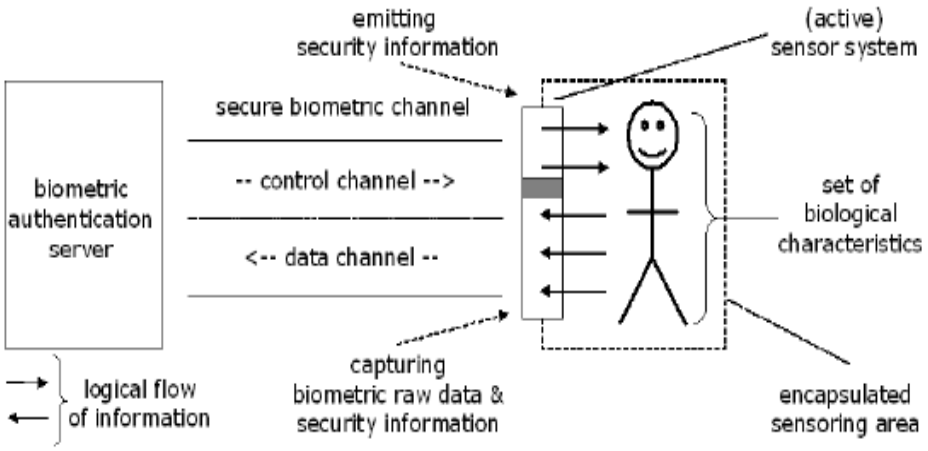


Figure 2: Secure biometric communication channel (biochannel)

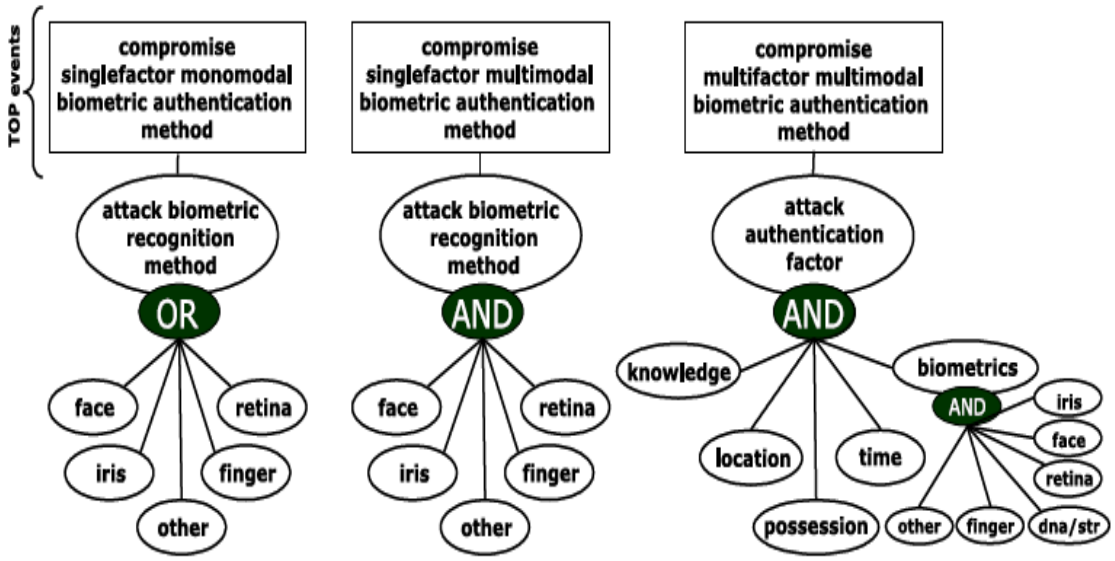


Figure 4: General attack trees for (single|multi)factor (mono|multi)modal biometric authentication methods

---

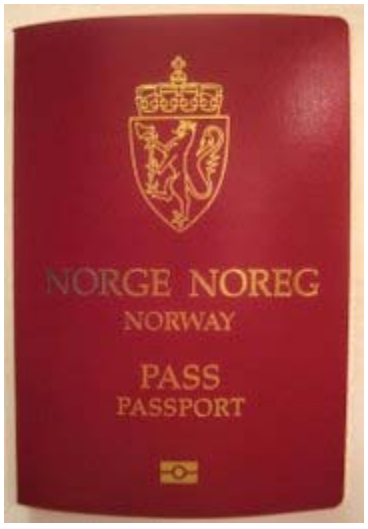
By studying security risks of biometric authentication methods, researchers come to more secure and reliable prototypical research solutions like presented for instance with multimodal biometric methods (biometric fusion techniques) by Hong and Jain in and with multifactor multimodal biometric authentication methods by Br¨omme in Based on adapted fault trees for security analyses, introduced by Schneier in as attack trees, a general attack tree for different types of biometric methods can be constructed showing a security risk analysis in a qualitative way (Figure 4).

Some other Applications of Biometric Analysis

In addition to its extensive use in forensic sciences, biometrics technology is rapidly being adopted in a wide variety of security applications such as electronic and physical access control, electronic commerce, digital rights management, background checking, homeland security, and defense. Security systems demand high accuracy, high throughput, and low cost from their biometric sub-systems. Although biometric systems have made great strides especially over recent years, there is continued need for vigorous research to solve many outstanding challenging problems. The goal of this special issue is to document the current state-of-the-art, the latest breakthroughs achieved by the scientists working in the area of biometric recognition, and to identify future promising research areas. We invite original contributions that provide novel solutions to challenging problems. Submitted papers can address theoretical or practical aspects of the progress and directions in biometrics research. Topics of interest include, but are not limited to:

- ✓ Estimation of biometric individuality (information content).
- ✓ Statistical performance evaluation.
- ✓ Temporal interclass and intraclass variability in biometric characteristics.
- ✓ Verification and identification systems; tracking, indexing, and classification.
- ✓ Biometric cryptosystems; template protection; privacy protecting techniques; liveness detection.
- ✓ Multimodal biometrics; information fusion.

A **biometric passport** is a combined paper and electronic identity document that uses biometrics to authenticate the citizenship of travelers. The passport's critical information is stored on a tiny RFID computer chip, much like information stored on smartcards. Like some smartcards, the passport book design calls for an embedded contactless chip that is able to hold digital signature data to ensure the integrity of the passport and the biometric data.



Norwegian biometric passport

The current staged biometrics for this type of identification system is facial recognition, fingerprint recognition, and iris scans. The International Civil Aviation Organization defines the biometric standards to be used in passports. ICAO does not currently have plans to use retinal scanning. Only the digital image (usually in jpeg format) of each biometric feature is actually stored in the chip. The biometric algorithm is computed outside of the passport chip by electronic border control systems (e-borders). To store biometric data on the contactless chip, it includes a minimum of 32 kilobytes of EEPROM storage memory, and runs on an interface in accordance with the ISO 14443 international standard, amongst others. These standards ensure interoperability between the different countries and the different manufacturers of the passport books.

Symbol for biometric passports, usually printed on the cover of the passports.

CONCLUSION

This paper presents a systematic approach for a holistic security risk analysis of biometric authentication technology based on the high-level component & process model for integrated security risk analysis of biometric authentication technology also proposed here. The processes and components used within this model are developed together with a terminology for biometric authentication technology for the research field of IT security biometrics, which is comprehensively presented here for the first time.

Current approaches for risk analysis of biometric authentication technology are limited to enrollment and identification/ verification processes with biometric algorithms mainly considered as black-boxes, only.

By using the biometric authentication risk matrices introduced here it is shown that more than seven thousand single possible risk effect classes can be identified, which should be examined for an overall holistic security risk analysis of biometric authentication technology.

With the systematic discovery of such a large amount of possible risk effect classes in this paper, it can be concluded that current biometric authentication technology contains inherent holistic security risks, which are not systematically explored. For this reason, the specific risk analysis approach presented here has a strong advantage in comparison with other evaluation and risk analysis approaches in this area. More generally speaking, the presented approach is a significant contribution on the way to the possible development of more (holistic) secure biometric authentication technology.

REFRENCES

1. **www.answers.com**
2. **www.biotech.com**
3. **www.ccs .neu.edu**
4. **articles from "TIMES OF INDIA"**