

BIOMETRICS BASED USER AUTHENTICATION

Tanuj Tiwari¹, Tanya Tiwari² and Sanjay Tiwari³

Maheshwari Public School, Kota (Raj), India

¹Department of Electrical & Electronics Engg, Birla Institute of Science & Technology, Pilani (Raj), India
²S.O.S. in Electronics & Photonics, Pt. Ravishankar Shukla University, Raipur (C.G.), India

Abstract : *Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometrics technologies are base for a plethora of highly secure identification and personal verification solutions. It is measurement of biological characteristics – either physiological or behavioral – that verify the claimed identity of an individual. Physiological biometrics include fingerprints, iris recognition, voice verification, retina recognition, palm vein patterns, finger vein patterns, hand geometry and DNA. But there arises a need for more robust systems in order to tackle the increasing incidents of security breaches and frauds. So there is always a need for fool proof technology that can provide security and safety to individuals and the transactions that the individuals make. Biometrics is increasingly used by organizations to verify identities, but coupled with quantum cryptography it offers a new range of security benefits with quantum cryptography where we form a key when we need it and then destroy it. In this paper, we give a brief overview of the field of biometrics and summarize some of its advantages, disadvantages, strengths, limitations, and related privacy concerns.*

Keywords: *Biometrics, identification, multimodal biometrics, recognition, verification, security*

I. Introduction

Reliable user identification is increasingly becoming important in the Web enabled world today and there has been a significant surge in the use of biometrics for user identification. Many corporate heads use laptops and personal digital assistants (PDAs) loaded with sensitive business and personal information. Over 250,000 mobile gadgets are lost or stolen every year, and only 25-30 per cent of these ever make it back to their rightful owners. Such mishaps have created a dire need to ensure denial of access to classified data by unauthorized persons.

Therefore various aspects of everyday life are gradually being digitized as our life experiences and creative efforts are accumulated in personal computers, digital media devices, and mobile devices. People use passwords and other authentication methods to protect these collections of personal and potentially confidential information. Business organizations have been highlighting the importance of ascertaining a user's identity before permitting access to confidential information. Traditional confidentiality and authentication methods (e.g., personal passwords) are less than secure. In addition to requiring the user to remember a variety of passwords, which can result in user error, passwords can be stolen and pure password authentication is vulnerable to unauthorized breach. In a race to improve security infrastructures faster than hackers and stealers can invent to penetrate passwords and firewalls, new technologies are being evaluated to confirm or deny user authentication.

Given the pervasive use of passwords and identification codes for user authentication across all aspects of our daily life, attackers have developed powerful password cracking codes. However, these problems can be resolved through the use of “physiological passwords” through unique personal biometric identification methods such as recognition of the user's face, fingerprints, personal signature, or iris, which are very difficult to either replicate or steal.

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- *Universality:* each person should have the characteristic.
- *Distinctiveness:* any two persons should be sufficiently different in terms of the characteristic.

- *Permanence*: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
 - *Collectability*: the characteristic can be measured quantitatively.
- A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.

Biometrics modes of identification have been found to be the most compelling and intriguing authentication technique. Biometrics are automated methods of recognizing a person based on his physiological or behavioral characteristics. Tokens can be lost, stolen or duplicated and passwords can be forgotten or shared. However, biometrics can authenticate you as you.

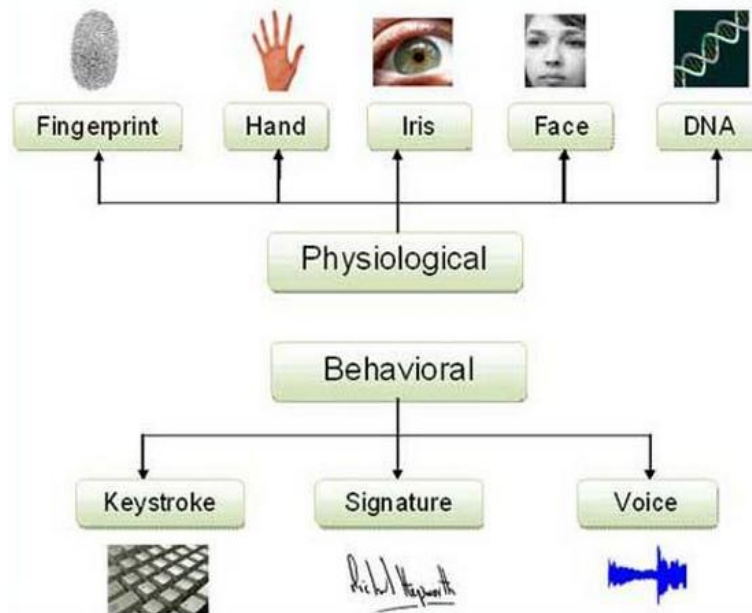


Fig.1 Classification of Biometrics

Biometrics is a means of using parts of the human body as a kind of permanent password. Just as your fingerprints are unlike those of any other person, your eyes, ears, hands, voice, and face are also unique. Technology has advanced to the point where computer systems can record and recognize the patterns, hand shapes, ear lobe contours, and a host of other physical characteristics. Using this biometrics, laptop and other portable devices can be empowered with the ability to instantly verify your identity and deny access to everybody else. It is fundamentally a pattern recognition system that recognizes a person by determining the authentication by using his different biological features i.e. Fingerprint, retina-scan, iris scan, hand geometry, and face recognition are leading physiological biometrics and behavioral characteristic are Voice recognition, keystroke-scan, and signature-scan[1-8].



Year	Biometrics	Description
1960	Face	First semi-automatic system for face recognition.
1965	Signature	First project on automatic signature recognition.
1969	Fingerprint	First proposal for fingerprint automatic identification by the FBI.
1970	Face	Further achievements for automatic face recognition.
1974	Hand Geometry	First commercial hand geometry system becomes available.
1976	Voice	First prototype of a speaker recognition system is released.
1977	Signature	Patent awarded for live signature acquisition.
1985	Hand Geometry	Patent for the proposal of hand-based identification is awarded.
1986	Fingerprint	Standard for the exchange of fingerprint minutiae is released.
1986	Iris	Patent for the proposal of iris-based identification is awarded.
1988	Face	Techniques for automatic face recognition are proposed.
1991	Face	Real-time face recognition becomes feasible.
1994	Iris	First Iris identification system is patented.
1998	DNA	DNA indexing system is released by the FBI.
1999	Fingerprint	FBI released the first automated fingerprint identification system.
2000->	Multibiometrics	New biometric systems have been released and more recent techniques combine different biometric traits.

Fig 2 Biometrics traits and history of biometric technology.

II. Principle of working

Once identified, the physical characteristics can be exactly measured and analysed. The statistical use of the characteristic variations in unique elements of living organisms is known as biometrics. Biometrics data of human beings can be collected and analysed in a number of ways, and has been introduced as a mode of personal identification. Biometric systems automatically verify or recognise the identity of a living person based on physiological or behavioural characteristics. Physiological characteristics pertain to visible parts of the human body. These include fingerprint, retina, palm geometry, iris, facial structure, etc. Behavioural characteristics are based on what a person does. These include voice prints, signatures, typing patterns, key-stroke pattern, gait, and so on. A variety of factors, such as mood, stress, fatigue, and how long ago you woke up, can affect behavioural characteristics.

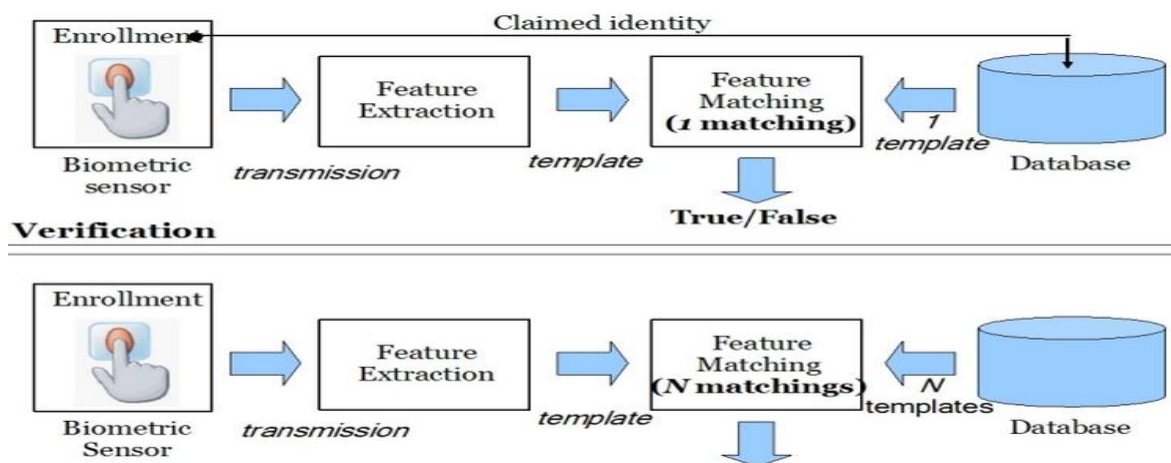
Voice print is a fine series of spectral power density plots that depict how the energy in one's voice at different frequencies varies with time as one vocalises a word or phrase. Voice experts say that sufficient characteristics of one's voice print remain constant under all circumstances, enabling these plots to reliably verify one's identity while physiological traits are usually more stable than behavioural traits, systems incorporating them are typically more intrusive and more expensive to implement

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

Identification - One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against known database.

Verification - One to One: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

Biometric authentication requires to compare a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification process.



Identification

Fig. 3 Block diagrams of enrollment, verification, and identification tasks are shown using the four main modules of a biometric system, i.e., sensor, feature extraction, matcher, and system database.

During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera. The second phase of processing is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed biometric identifier record (sometimes called biometric sample or biometric template). Next phase does the process of enrollment. Here the processed sample (a mathematical representation of the biometric - not the original biometric sample) is stored / registered in a storage medium for future comparison during an authentication. In many commercial applications, there is a need to store the processed biometric sample only. The original biometric sample cannot be reconstructed from this identifier.

III. Advantages of Biometric Technology

Using biometrics for identifying and authenticating human beings offers unique advantages over traditional methods. Tokens, such as smart cards, magnetic stripe cards, and physical keys can be lost, stolen, or duplicated. Passwords can be forgotten, shared, or unintentionally observed by a third party. Forgotten passwords and lost smart cards are a nuisance for users and waste the expensive time of system administrators. In biometrics the concerned person himself is the password, as biometrics authentication is based on the identification of an intrinsic part of a human being. The biometrics technique can be integrated into applications that require security, access control, and identification or verification of users. Biometrically secured resources effectively eliminate risks, while at the same time offering a high level of security and convenience to both the users and the administrators.

Methods	Description
Face	This method involves analyzing facial characteristics such as the measure of the overall facial structure, including distances between eyes, nose, mouth, and jaw edges.
Fingerprint	This method looks at the patterns found on a fingertip. Patterns are made by the lines on the tip of the finger.
Hand geometry	This method involves analyzing and measuring the shape of a hand.
Iris	This method involves analyzing features found in the colored ring of tissue surrounded the pupil.
Retina	This method involves analyzing the layer of blood vessels situated at the back of the eye.
Vascular Patterns	Vascular patterns are best described as a picture of the veins in a person's hand or face. The thickness and location of these veins are believed to be unique enough to an individual to be used to verify a person's identity.
Voice	This method does not involve the recognition of the user voice, but to convert the voice of the user to text for authentication purposes.
Signature	This method analyzes the way the user signs his/her name, recording signature characteristics such as stroke order, speed, and pressure.



Fig.4. Pattern matching

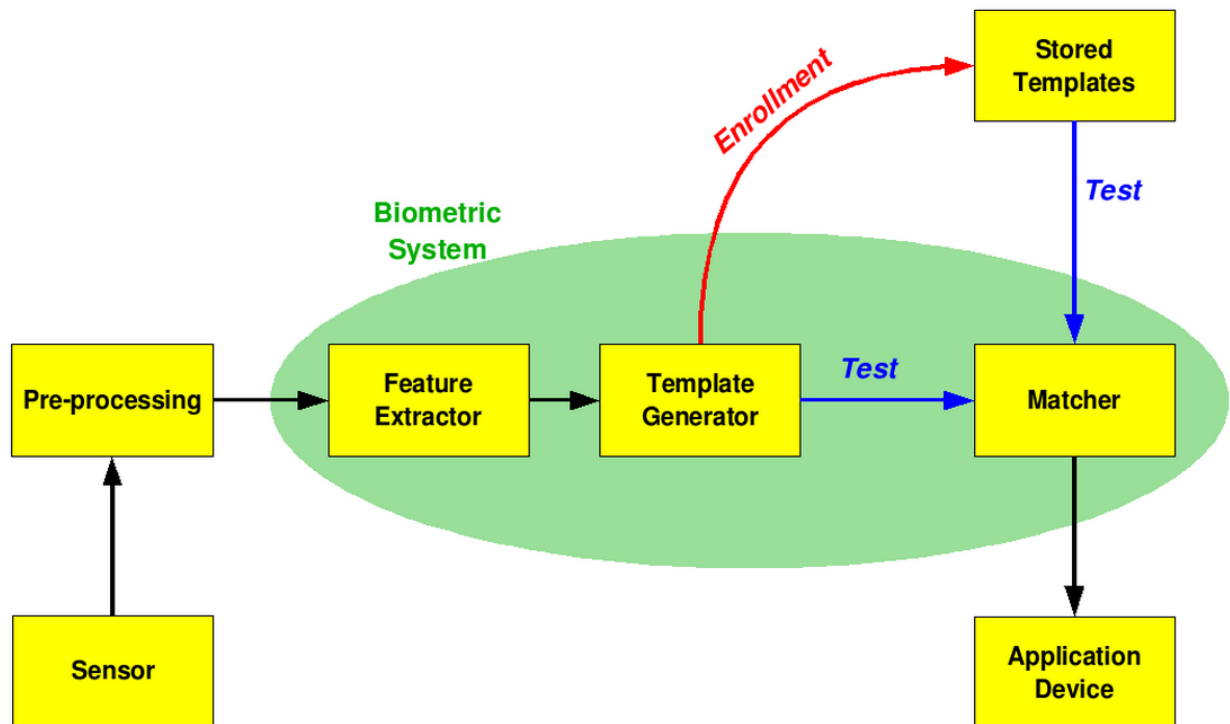


Fig.5 Working of Biometric system

IV. Applications in use

Biometric systems have a powerful potential to provide security for a variety of applications, systems are nowadays being introduced in many applications and have already been deployed to protect personal computers, Banking machines, credit cards, electronic transactions, airports, high security institutions like nuclear facilities, Military Bases and other applications like borders control, access control, sensitive data protection and on-line tracking systems.

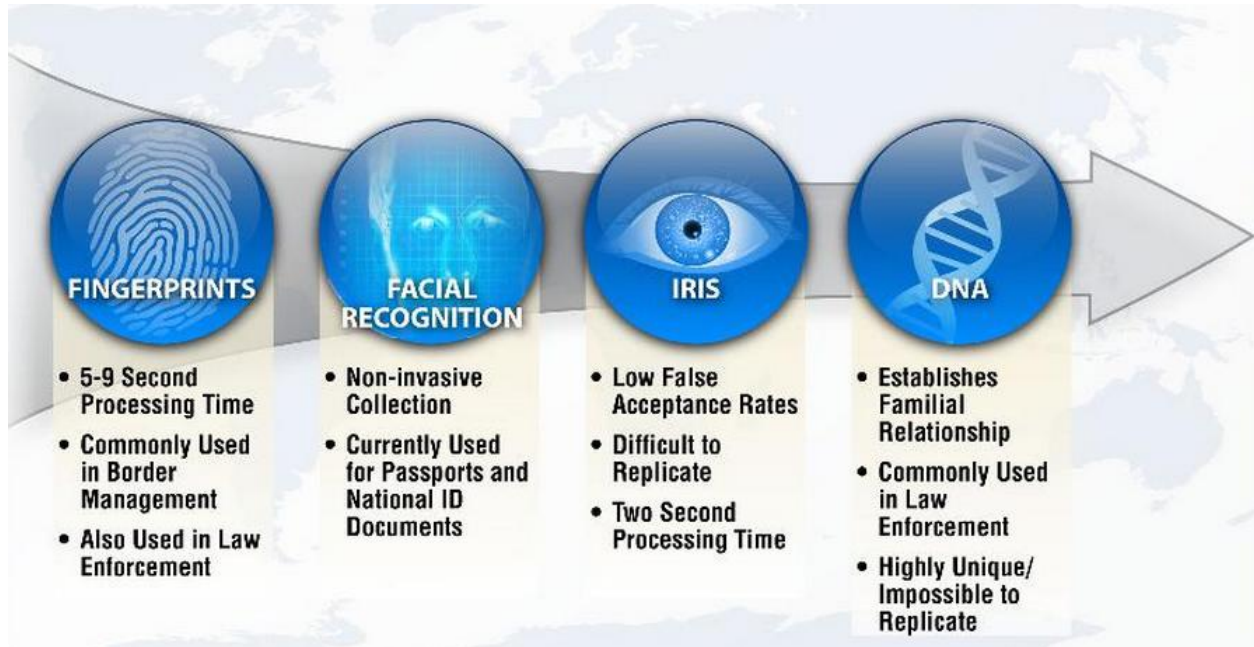


Fig.6 Biometric traits

Nationwide Building Society, the UK, has incorporated an iris recognition system at ATMs. A camera takes a digital record of each user's iris. The iris print is stored in a database to verify personal identity during transactions.

Biometric Comparison Chart						
Sr. No	Characteristics	Fingerprint	Iris	Face	Palm Print	Voice Recognition
1	<u>Speed</u>	Medium/Low	Medium	Medium	Medium	Medium
2	<u>FTE Rate</u>	Medium/Low	Low	Low	Low/Medium	Medium
3	<u>Standards</u>	High	Medium	High	High	Low
4	<u>Uniqueness</u>	High	High	Medium	High	Medium
5	<u>Maturity</u>	High	Medium	Medium	Medium	Low
6	<u>Durability</u>	High	High	Medium	High	Low
7	<u>Invasiveness</u>	High	Medium	Low	High	Low
8	<u>Overtness</u>	High	Medium	High	Low	Low
9	<u>Range</u>	Low	Low	Medium	Low	High
10	<u>Template Size</u>	Medium (250-1,000 bytes) (per finger)	Medium (688 bytes)	High (84-2,000 bytes)	Medium (250-1000 bytes)	High (1,500-3,000 bytes)
11	<u>Age Range</u>	High	High	High	High	Medium
12	<u>Universality</u>	High	Medium	High	High	High
13	<u>Stability</u>	High	High	Medium	High	Low
14	<u>Skill</u>	Medium	Medium	Low	High	Low
15	<u>Accuracy</u>	Medium-High	High	Medium	High	Low
16	<u>Hygienic Level</u>	Low	High	High	Low	High
17	<u>Performance</u>	High	High	Low	High	Low
18	<u>Cost</u>	Low	High	Low	High	Low

Iris recognition subsystem is also being incorporated into ATMs in Japan. Siemens Nixdorf, Germany, is incorporating facial recognition mode into ATM systems. Standard Bank, South Africa, scans the fingerprints of its customers, instead of using a personal identification number (PIN), when they wish to withdraw cash. Basically, the biometrics security technique acts as a front end to a system that requires precise identification before it can be accessed or used. The system could be a sliding door with electronic locking mechanisms, an

operating system (OS), or an application where individual users have their own rights and permissions. Imagine unlocking your house or withdrawing money from your bank with just a blink of an eye, a tap of your finger, or just showing your face. Kelly Gates of Iris Scan is developing an authentication system, wherein users only have to open their eyes and look towards the camera lens for a few seconds to be identified.

Keystroke biometrics provides a foolproof authentication solution. The gap between consecutive keystrokes when typing the access code and typing rhythm are unique to a user, so even if an unauthorized person discovers the access code, he can't access the system unless he knows the user's typing rhythm also.

A multi-application travel card would enable the holders to participate in various frequent flier and border control systems as well as pay for air ticket, hotel room, etc. all with one convenient token.

A biometric chip reader incorporated into a PC can facilitate secure Internet based online transactions. Applications that are being developed to accept biometric data include computer networks, cars, cellular phones, and hoards of other types of embedded systems. Biometrics could authenticate e-mail and other documents transmitted via computer networks.

In hospitals, biometric techniques could replace ID bracelets to establish patients' identities, for instance, during blood administration.

With existing voice-transmission technology, voice recognition biometric techniques can function over long distances using the ordinary telephone. A well conceived and properly implemented voice based security system could provide a greater safety to financial transactions conducted over the telephone.

Biometrics on the move

Immigration and naturalization passenger accelerated service systems (INP ASS) allow international airports to use hand geometry scanners to verify the identity of travelers. Airports are testing face recognition scanners to help weed out terrorists.

One of the most hotly pursued applications of biometrics is handheld. Researchers are working on means to integrate eye scanners, fingerprint readers, and voice recognition systems into mobile phones, PDAs, and laptops. Scanners are getting smaller, cheaper, and more accurate, and can be used in mobile gadgets without sprucing up the size, cost, and power consumption. Not only biometrics renders handheld and laptops worthless to would-be stealers, it could also eliminate fraudulent transactions. Mobile manufacturers and wireless operators are incorporating voice and fingerprint scanning techniques in their devices.

Voice is an obvious preference for mobile phones. Since it doesn't require any extra hardware in the device, it is naturally integrated into the way people use phones. All the processing is done on the mobile phone system that stores the reference voiceprints, which are as unique as a fingerprint, looking for particular patterns of tone, inflection, and behaviour in a voice. This ensures that a real person, not a tape recording, is on the line.

V. Characteristics of Biometric system

A number of biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires that the biometric characteristics satisfy the following characteristics:

1. **Universal:** Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.
2. **Invariance of properties:** They should be constant over a long period of time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.
3. **Measurability:** The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.
4. **Singularity:** Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.
5. **Acceptance:** The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.
6. **Reducibility:** The captured data should be capable of being reduced to a file which is easy to handle.
7. **Reliability and tamper-resistance:** The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.
8. **Privacy:** The process should not violate the privacy of the person.
9. **Comparable:** Should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.
10. **Inimitable:** The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

IV. The biometric model

A generic biometric model consists of five subsystems, namely, data collection, transmission, signal processing, decision making, and data storage. Data collection involves use of sensors to detect and measure an individual's physiological or behavioural characteristics.

The measured biometric must be unique and repeatable over multiple measurements. However, technical parameters of the sensor, as well as the ergonomics of the device and the manner in which the biometric characteristic is presented to effect the measurement, could eventually impact the outcome of the system. For instance, background noise and acoustics of the environment may impact a speech recognition system, while the pressure applied to a fingerprint scanner might also affect the data. The data collection subsystem most directly impacts the user. Sensor specifications determine the intrusiveness of the system. Intrusiveness is the degree to which the user feels that the measurement process violates his personal space, and is often correlated to how close the user has to be near the sensor. For instance, a retinal scan, which requires close proximity to the camera, is considered far more intrusive than a voice recognition system.

Not all biometric systems process and store data on the measuring device. Often measurement is made using a relatively simple device to a computer or server for processing and/or storage. Depending on the system, the data may be relatively large and thus would need to be compressed for quick transfer. The compression algorithm needs to be selected carefully, otherwise it may introduce some artifacts that could impact the decision process

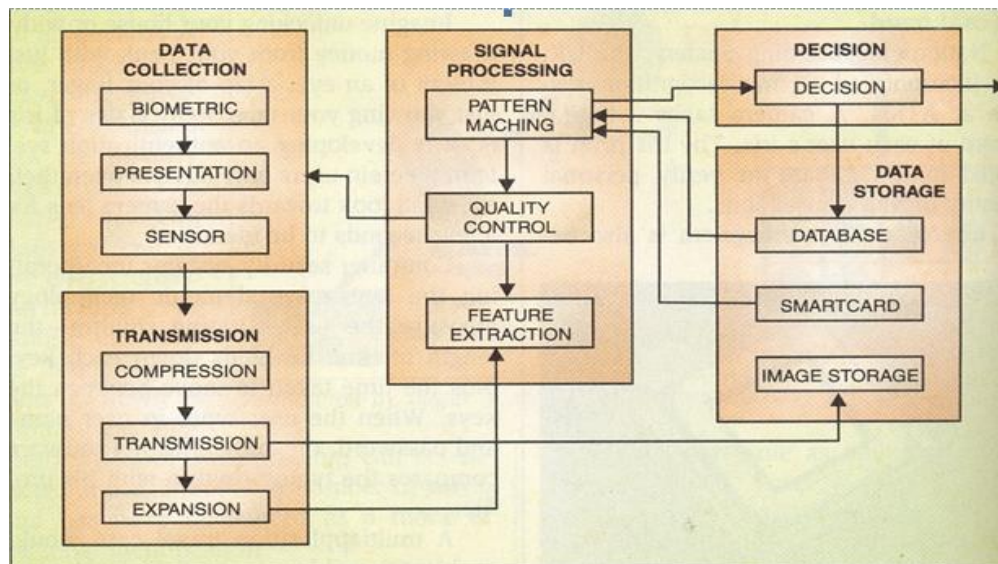


Fig. 7 Block diagram of a biometric model

In fingerprint scanning systems, wavelet scalar quantisation is often preferred to JPEG compression due to the blockings that the latter produces at high compression ratios. The data can also be transmitted to the database for storage as raw data. The signal processing subunit uses feature extraction algorithms to extract true biometric information from the sample in the presence of noise introduced during data collection and transmission. Additional measurements are made if any flaw or corruption is noted, to ensure good quality. Pattern matching involves comparing the feature sample to a stored sample. (Biometric data can be stored locally on the biometric device, some central database/ server, or on a smart card issued to users.) The result of comparison is sent to the decision system to determine the match. The decision subsystem uses statistical methods to confirm authentication if the variance between the sample and template data is within a certain threshold.

System quality The quality of a biometrics authentication algorithm is specified in terms of false rejection rate (FRR) and false acceptance rate (FAR). FRR indicates the percentage of instances an authorized individual is falsely rejected by the system. FAR states the percentage of instances an unauthorized individual is falsely accepted by the system. FRR and FAR are diametrically opposed, therefore increasing the FAR will lower the FRR, and vice-versa. FRRs and FARs can be adjusted according to the needs of a given security system.

The biometric system should be able to account for permanent/semi-permanent changes in authorized / unauthorized users. For instance, a user's biometric characteristics, even if these are physiological, can change over time. People can grow beards, injure their hands, change their accent become better typists, change their hairstyles, and so on. Robust biometric systems are able to meet these contingencies by slightly modifying the template for accepted authentication situations. The user's profile in the database adapts to changes in the user's biometric features.

VII. Vulnerability to attacks

Biometric systems, like all security systems, have vulnerabilities. This entry provides a survey of the many possible points of attack against traditional biometric systems [9-12]. Biometric system security is defined by its absence: a vulnerability in biometric security results in incorrect recognition or failure to correctly recognize individuals. This definition includes methods to falsely accept an individual (spoofing), to decrease overall system performance (denial of service), or to attack another system via leaked data (identity theft)[13-14]. In a biometrics based authentication system, there are five points vulnerable to attacks by invaders as shown in the figure 8.

Bio Enable Technologies, Pune, is a software company that develops biometric products to cater to the tough Indian working conditions and environments. The firm has developed intelligent biometric solutions for physical access control, banking transaction, timing, and attendance applications.

Bio Enable has introduced a fingerprint-based identification terminal for use in factories, defence installations, public Kiosks, offices, retail outlets, etc. The fingerprint system translates illuminated images of fingerprints into digital code. The digital code is subjected to system software code for verification/ authentication of requested users and enrollment/registration of new users' fingerprints.

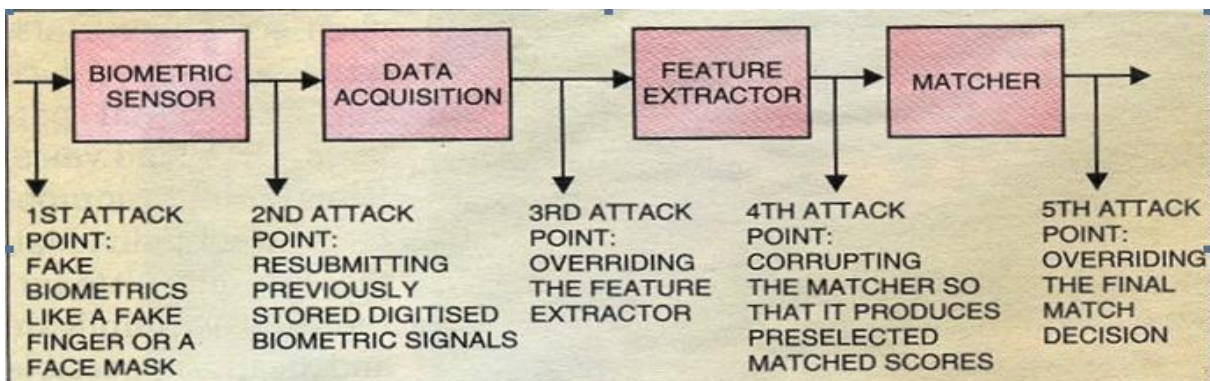



Fig.8 Five point vulnerable to attacks in biometric based authentication system

- > RBI wants multi-factor authentication for card transactions
- > Besides the card's presence and signature/PIN, it wants an additional fraud-proof feature
- > The security feature should be usable by customers who are only numerically literate

WHAT ARE THE CONCERNS?

- > Biometric authentication will push up hardware and telecom costs significantly
- > In fact, bankers say



machines will require 3G speeds to send scanned images for verification

- > Aadhaar itself has not yet been made mandatory

Fig.9 Looking for more security

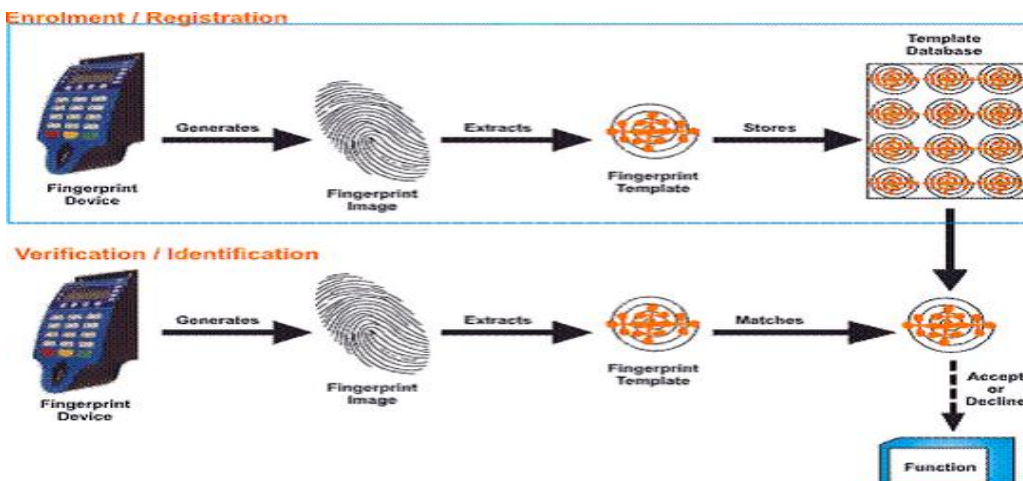


Fig.10 Bio enabled fingerprint recognition system

CMOS image sensors capture high-contrast, high-resolution fingerprint images that are virtually distortion-free. Powerful algorithms developed by Bio enabled extract minutiae data from the images to map the distinguished characteristics of fingerprint ridge ends, bifurcation, loops, splits, and upper and lower cores. The data is then converted into a template and stored in the database. To identify or verify, the algorithm compares the new template with the extracted minutiae points from the stored sample. The entire matching process takes roughly one second.

Siemens Information Systems Ltd (SISL), Bangalore, has developed a text independent autonomous speech recognition system to identify and authorize a speaker by analyzing his voice. Central Forensic Science Laboratories, Chandigarh, uses this system to track down and identify criminals by comparing their voice samples using SISL software.

Other innovations of SISL include fingerprint identification and management system (FIMS), language-independent speech recognition system, and optical character recognition system. SISL is developing low-cost chips that can be fitted into cars and toys. These chips will store fingerprint of the user and allow selective access to devices and homes.

Axis Software, Pune, deals in fingerprint, iris, and face recognition technology and is planning to add voice recognition technology to its range of authentication products and systems. The Axis system stores biometric records in an record by itself is of no use to a stealer and cannot be reconstructed to reveal , person's identity to someone else.

Biometric Society of India (INBIOS), affiliated to the International Society of Computational Biology (ISCB), provides innovative professional solutions and services dedicated to bioinformatics.

Global developments

Internet security. Litronix, USA, a leading provider of public key infrastructure (PKI)based Internet security solutions, has developed biometric identification techniques for use in electronic data applications such as digital networks and smart cards. Apart from iris, voice and handwritten signature recognition can be used for authentication purposes when digitally signing a document or obtaining access to secure WebPages. The smart card, integrating voice and handwritten functions, incorporates the appropriate biometric template to deliver the final match and authorization.

The company plans to incorporate capture, manipulation, enrollment, and extraction features in the smart card reader also.

Biometric smart cards. Polaroid and Atmel have developed secure identity cards that merge ultra-secure smart cards, fingerprint verification, biometric identification, and digital imaging. These cards will be used in e-commerce, online, remote access, and any IT environment where authentication is required.

The information stored in the card is protected by circuits inside the card that perform encryption/decryption of the data in the card. The tiny smart card circuits in these ID cards are actually integrated circuits, called smart card ICs, supplied by Atmel. Atmel's smart card ICs can perform critical encryption; decryption functions within the card and are able to securely identify the person or system reading the card.

Biometrics cellulars. Fujitsu Microelectronics has developed an innovative fingerprint identification system that combines sweep sensor technology with advanced algorithms to provide a powerful, dependable, easy-to-use authentication for PDAs, cell phones, and other mobile devices. The sensor measures just 1.28x0.20 cm and is powered by sophisticated algorithms that generate unique minutiae templates that correspond to specific fingerprint features. A single-fingerprint sweep across the sensor captures fingerprint features to rapidly authenticate users of cell phones and PDAs.

Cyber security. Cyber SIGN, USA, has built-in signature security management features of Adobe Acrobat 4.0 software. This software enables the handwritten signature to be included as an electronic signature in any Acrobat portable document format (PDF) file on the Web. Anyone can online use his handwritten signature to authorize and sign electronic Acrobat documents. Costs involved in businesses are reduced, as signed documents and forms are available online, and productivity and security are increased when vendors and suppliers can quickly access signed, secure, and trusted electronic documents.

8. Challenges for Biometrics

Imagine a world without keys, passwords, pins or passports, where you interact seamlessly with technology, where personalization is ubiquitous and devices recognise who you are in order to make life more convenient. And it is all implemented properly, with due consideration to privacy.

Customer behavior is changing with transactions moving more and more to the digital world. Fraud and cyber-attacks are on the increase which demand more controls to be put in place. User name and password are clearly outdated. Is this the right time to try to invest into making the customer journey more seamless? Where do biometrics fit in the future?

As usernames and passwords are so regularly compromised, we are rapidly moving to a new form of digital identity authentication. Digital signatures and sign-ons, enabled by mobile and biometrics, are becoming standard, but where does this take us in the longer term?

Identity management in government applications remains a popular topic and we will continue the debate from last year looking at different countries and how they address this issue – including an update on the use of biometrics in developing economies such as identity systems and voter registration

Privacy on trial! Customer authentication and identification are on the increase in the cyber world. We are being validated by people connected to us. We even are prepared to give up some privacy to receive certain benefits in return. “Selfies” are being advertised as the password for transactions on mobile devices but while this offers great convenience, are there any risks to be considered?

Biometric vulnerability assessments are now being recognised as an important part of the implementation of biometrics and the international standards community is also addressing presentation attacks. With a high demand of smaller and faster scanners for mobile devices, the question about vulnerability becomes even more important.

IX. Multibiometrics

Multibiometrics is a system, which implements two or more biometric systems and performs the function of verification or identification. For instance, multibiometrics can combine fingerprint recognition and hand geometry with iris recognition and speaker verification to give foolproof identification. In fact, a multimodal biometric system has been introduced, which integrates face recognition, fingerprint recognition, and speaker verification in making a personal identification.

Multimodal Biometric Systems

Multimodal biometric systems are those that utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked to as a means of

1. Reducing false non-match and false match rates,
2. Providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and
3. Combating attempts to fool biometric systems through fraudulent data sources such as fake fingers.

A multimodal biometric verification system can be considered as a classical information fusion problem i.e. can be thought to combine evidence provided by different biometrics to improve the overall decision accuracy. Generally, multiple evidences can be integrated at one of the following three levels.

- Abstract level: The output from each module is only a set of possible labels without any confidence value associated with the labels; in this case a simple majority rule may be used to reach a more reliable decision.
- Rank level: The output from each module is a set of possible labels ranked by decreasing confidence values, but the confidence values themselves are not specified.
- Measurement level: the output from each module is a set of possible labels with associated confidence values; in this case, more accurate decisions can be made by integrating different confidence values.

X. Mobile Biometrics

MOBIO concept is to develop new mobile services secured by biometric authentication means. Scientific and technical objectives include robust-to-illumination face authentication, robust-to-noise speaker authentication, joint bi-modal authentication, model adaptation and scalability.

These days, portable personal devices such as PDAs or mobile phones are indeed widely used. They provide the mobile worker or the customer with portable computing and wireless access to Telecom networks and to the Internet. It is then possible to provide anywhere anytime a natural access to any service, such as PIN code replacement, phone card reloading, remote purchase, telephone banking or voice-mail. Most of these services involve micro payments that can currently be done only using PIN codes or passwords.

Efforts to develop and evaluate bi-modal (face and voice) biometric authentication (BMBA: Bi-modal biometric authentication) technologies in the context of portable and networked devices are in progress. Although biometric authentication is a complex problem, and is still not reliable enough to be widely accepted, it has also been shown that the use of multiple modalities increases the performance of biometric systems. However, most of the current multi-modal biometric systems simply perform fusion and do not actually take advantage of temporal correlations between modalities. As a matter of fact, very little work in the research community has been done on joint multi-modal fusion to perform joint authentication of several modalities (in our case face and voice).

XI. Social, Ethical, and Legal Issues

The success of a biometric-based identification system depends to a large extent on human itself. If a biometric system is able to measure the characteristic of an individual without contact, such as those using face, voice, or iris, it may be perceived to be more user-friendly and hygienic[15]. Biometrics, has various implications that have to be considered. Some of the social issues are that some people are wary of this new technology. The fear of having your personal belongings and data stolen (such as a car, banking accounts, assets, and even social

security number) maybe be very negative, but can be reversible with effort and over time. The fear associated with the use or rather misuse of biometrics is to ultimately lose what defines you as who you are. Ethical and legal implications also come into consideration. All biometric systems must comply with the European Convention of Human Rights, as well as the Data Protective Directive. Ethically, biometrics sits in the grey area pertaining to the privacy of individuals' personal lives. People are sensitive to the release of their personal information, even for legitimate uses. Biometrics requires the release of intimate information about the user. By having biometric information about users and individuals in a database, there is a fear that this collection of personal data would be tempting for those who would steal it and use it for personal gains. The Data Protective Directive places legal restrictions pertaining to data access systems, stating that the data gathered and used in biometric systems must be fair, regulated, and limited to specify purposes

XII. Conclusions

Biometrics, or biometric authentication, consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. Biometrics is a pervasive technology, which has been widely used in forensics, secured access and prison security. Biometric-based systems also have some limitations that may have adverse implications for the security of a system. While some of the limitations of biometrics can be overcome with the evolution of biometric technology and a careful system design.

Biometrics does have a promising future in the next generation authentication and security systems. Attempts should be made to standardize common software interfaces to enable sharing of biometric templates and to permit the effective comparison and evaluation of different biometric technologies. It is the right time to boost the biometric capabilities and also invest in research & development pertaining to Biometrics keeping the demands of the industry in mind.

References

- [1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy Mag.*, vol. 1, no. 2, pp. 33–42, 2003.
- [2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer-Verlag, 2003.
- [3] A. K. Jain, R. Bolle, and S. Pankanti, Eds., *Biometrics: Personal Identification in Networked Society*. Norwell, MA: Kluwer, 1999.
- [4] (2002) Schiphol Backs Eye Scan Security. CNN World News. [Online]. Available: <http://www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/>
- [5] J. Daugman, "Recognizing persons by their Iris patterns," in *Biometrics: Personal Identification in a Networked Society*, A. K. Jain, R. Bolle, and S. Pankanti, Eds. Norwell, MA: Kluwer, 1999, pp. 103–121.
- [6] L. O'Gorman, "Seven issues with human authentication technologies," *Proc. Workshop Automatic Identification Advanced Technologies (AutoID)*, Tarrytown, NY, Mar. 2002, pp. 185–186.
- [7] E. d. Os, H. Jongebloed, A. Stijssiger, and L. Boves, "Speaker verification as a user-friendly access for the visually impaired," in *Proc. Eur. Conf. Speech Technology*, Budapest, Hungary, 1999, pp. 1263–1266.
- [8] A. Eriksson and P. Wretling, "How flexible is the human voice? A case study of mimicry," in *Proc. Eur. Conf. Speech Technology*, Rhodes, 1997, pp. 1043–1046.
- [9] J. K. Lee, S. R. Ryu AND K. Y. Yoo. Fingerprint-based remote user authentication scheme using smart cards. *Electronics Letters*. 2002;38(12):554–555.
- [10] W. C. Ku, S. T. Chang AND M. H. Chiang: Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards. *Electronics Letters*. 2005;41(5):240–241.
- [11] M. K. Khan and J. Zhang "An efficient and practical fingerprint-based remote user authentication scheme with smart cards", *Information Security Practice and Experience*. 2006;3903:260–268.
- [12] A. Baig, A. Bouridane, F. Kurugollu and G. Qu "Fingerprint-Iris fusion based identification system using a single hamming distance matcher" *International Journal of Bio-Science and Bio-Technology*. 2009;1(1):47–58.
- [13] Shin-Yan Chiou "Secure Method for Biometric-Based Recognition with Integrated Cryptographic Functions" *Biomed Res Int*. 2013; 2013: 623815.
- [14] Andy Adler and Stephanie A. C. Schuckers, "Biometric Vulnerabilities: Overview", Living Reference Work Entry, Encyclopedia of Biometrics, 2014, pp 1-11
- [15] Anil K. Jain, Arun Ross, and Salil Prabhakar, An Introduction to Biometric Recognition *IEEE Transactions On Circuits and Systems For Video Technology*, Vol. 14, No. 1, 2004, 4-17

