ISSN: 2321-7782 (Online)

Volume 3, Issue 4, April 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Next Generation Secure Computing: Biometric in Secure E-transaction

Manaswini Pradhan
Lecturer,
P.G Department of Information and Communication Technology,
Fakir Mohan University, Balasore,
Odisha, India

Abstract: To establish identity of an individual is becoming critical in our heavy interconnected society. The need for reliable user authentication techniques has increased heightened concerns about security and rapid developments in networking, communication, and mobility. Biometrics, described as the science of recognizing an individual or the person based on his or her physical or behavioral traits. Biometric technologies are crucial components of secure personal identification and verification systems and today beginning to gain acceptance as a legal step for determining an individual's identity. Biometric systems have now been deployed in various commercial, civilian and forensic applications sectors as a means of establishing identity helping to protect information and automate transaction in information technology. In this chapter, an overview of biometrics and some issues are addressed for making biometric technology an effective tool for providing information security which includes examining applications where biometrics serves as a focal point to solve issues pertaining to development, testing, evaluation and application of biometric based personal identification and verification technology. Information security, enumerating the fundamental challenges encountered by biometric systems in real world applications and solutions to address the scalability and security in large scale authentication system are the issues in today's ever concerned world.

Key Words: Biometrics, information security, digital rights management, grand challenge. Public key infrastructure (PKI)

I. INTRODUCTION

The issue of information security lies in the protection of information elements, e.g. multimedia data, ensuring that only authorized users are able to access the contents available in digital media. The owners of contents, such as, authors and authorized distributors, are losing billions dollars revenue due to illegal copying and sharing of digital media. In order to address this problem, digital rights management (DRM) systems are being introduced and forced to regulate the duplication and dissemination of digital content [1]. The critical component of a DRM system is user authentication which determines whether a certain individual is an authorized to access the content in a particular digital medium. In a generic cryptographic system, the user authentication method is procession based, which means, the procession of the decrypting key is sufficient to establish the authenticity of the user. Since cryptographic key are long and random e.g. 128 bits for the advanced encryption standard (AES) [2] [3], they are difficult to memorize. As a result, these keys are stored somewhere on a computer or a smart card and released based on some alternative authentication mechanism, like password. Most passwords are so simple that they can be easily guessed especially based on social engineering methods or broken by simple dictionary attacks [4]. The most commonly used password is the word "password". Thus, multimedia data protected by a cryptographic algorithm are only as secure as the password and is the weakest link used to release the correct decrypting key(s) that can be used for establishing user authenticity. Simple passwords are easy to guess and comprise security. Complex passwords are difficulty to remember and are expensive to maintain. Some users tend to "store" complex passwords at easily accessible locations. Further, most people use the same password across different applications; therefore upon determination of s single password can access multiple applications.

Finally, in a multiuser account scenario, password are unable to provide non repudiation (i.e., when a password is divulged to a friend, it is impossible to determine who the actual user is. This may eliminate the feasibility of countermeasures such as holding legitimate users account in a court of law.

Problems with this security system based on Passwords, or ID/Swipe cards:1) Can be Lost. 2) Can be forgotten and 3) Worse! Can be stolen and used by a thief/intruder to access your data, bank accounts, car etc….

The biggest problem for network security is the authentication system. For most systems, they mainly use and rely on passwords which is a combination of letters, characters and/or numbers. However, passwords need to be renewed within a certain period of time to maintain a high level of security. Moreover, it might be copied and used by unauthorized users. To fix that problem, biometrics security system can be applied. The most use of biometrics security system in network is the logical access control method. It will verify person's identification for secure workstation logon or network logon to get access control to the system. Frauds in industry happen in the following situations like safety deposit boxes and vaults, bank transaction like ATM withdrawals, access to computers and emails, credit card purchase, purchase of house, car, clothes or jewellery, getting official documents like birth certificates or passports, obtaining court papers, drivers licence, getting into confidential workplace, writing Checks. To prevent stealing of possessions that mark the authorised person's identity e.g. security badges, licenses, or properties. Biometric applications are needed to prevent fraudulent acts like faking ID badges or licenses and to ensure safety and security, thus decrease crime rates

With increasing use of IT technology and need to protect data, there is a possibility that a person have multiple accounts/passwords.We can only remember so many passwords, so we end up using things we know to create them (birthdays, wife/girlfriends name, dog, cat…). Its is easy to crack passwords, because most of our passwords are weak!.If we create strong passwords (that should be meaningless to us) we will forget them! And there is no way to remember multiple such passwords

A number of limitations associated with the use of password can be lessened by the incorporation of better methods for user authentication. More traditional means of access control include token-based identification systems (such as driver’s license or passport) and knowledge-based identification systems (such as a password or personal identification number). Biometric authentication or, simply biometric identifiers [5] [6] [7] , refers to establishing identity based on the *physical* and *behavioral* characteristics (also known as trait or identifiers) of an individual such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc. These metrics are all related to human characteristics. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods. Since September 11, 2001, our national requirements strengthen homeland security have been taken as a serious issue and being intensified , stimulating government and industry interest in applying biometric technologies to the automated verification of the identity or individuals as this technologies raises privacy concerns about the ultimate use of the information. Biometric technologies control access to valuable information, to economic assets and to parts of national infrastructure. Many law enforcement, health and social service activities are biometric based used to identify and verify system support information based economy by enabling secure financial transactions and online sales. Biometric techniques are automated methods for identifying an individual or verifying the person’s identity based on the person’s physiological or behavioural characteristics. *Physiological attributes* include fingerprints, hand geometry, and facial recognition, DNA, voice, iris, retinal features palm veins all *related to the shape of the body*. *Behavioural attributes* include the dynamics of signatures, keystrokes, typing rhythm, gait and voice *all related to the pattern of behaviour of a person*. These techniques capture and process a person’s unique characteristics, and then authenticate that individual or the person based on comparison of the record of captured characteristics with a biometric sample presented by the person to be authenticated. Due to continuous development and progress in the research in the field of biometric technologies, reliable and cost-effective systems were established and were acceptable to customers and are user friendly. Novel applications of biometrics are successfully implemented in secure modern travel system documents, visas, and personal identity verification cards. These applications help to safeguard valuable assets and information, strengthen homeland security, contributing to safety and secured automated transactions

Public and private sectors are looking for reliable, accurate and practical methods for the automated authentication of identity, and are using biometric technologies in a wide range of applications including areas like health, defense, social service programs, driver licenses, passport, electronic banking, investing, retail sales and law enforcement.

Virtually, all authentication systems are characterized by three factors (Figure 1)

1. Password, PIN, A memory "unique: to oneself : Something that the person know
2. Token of Identification(ID) like Key/Card/ badge: Something the person have
3. Biometric(Physiological/Behavioural)-Fingerprints/Facial pattern: Something that the person is

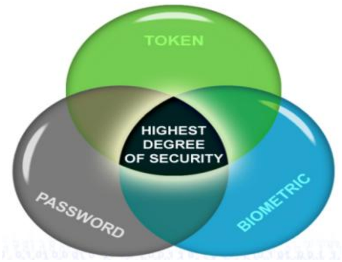


Fig 1: Levels of Authentication

The systems that incorporate all three above mentioned factors are stronger than those that use only one or two factors. Biometric authentication is used in systems to identify and access control. Authentication as a biometric factor helps to reduce identity theft. In this scenario, the need to remember passwords or to carry documents can be counterfeited and ignored. When the biometric attributes are used with one or two other factors, it is possible to achieve new and highly secured identity applications. It is used to identify individuals in groups that are under surveillance. The biometric factor is stored in a physical device and a smart card is used to verify the identification of an individual or the person. Biometric identifiers are the distinctive, measurable characteristics used to describe individuals and label them. The identification cards issued to employees for accessing the buildings or to enter into his or her own organization, and related to concern information, the card used by the person for financial transaction, often include biometric information.

Biometric factors are used with encryption keys and digital signatures to enhance secure authentication. Biometric information use public key infrastructure (PKI) system to incorporate encryption to help make the system more tamper free and resistant. The National Institute of Standards and Technology (NIST) help to develop the guidelines for the development of measurements, standards, and tests for biometrics. The Information Technology Laboratory (ITL) of NIST does in the research frontiers to investigate in the area of fingerprints, face recognition, iris recognition, and speech recognition. NIST support the development of voluntary industry standards and the development of conformance tests, reference implementations, and evaluation procedures to facilitate the implementation of standards in the biometric products. NIST works in close cooperation with industry, nation and international standards groups and federal state, and local government organizations for the advancement in the development of measures and standards for biometrics. For e.g., recent legislation directed NIST to work with other federal agencies to develop standards needed for the biometric authentication of applicants for U.S. visas. NIST activities support biometric standards and measurements and update the ITL Bulletin issued in May 2001 detailing NIST's biometric technology and standards activities: *Biometric-Technologies for Highly Secured Personal Authentication*, by Fernando L. Podio, Information about NIST, industry and standard activities.

II. Biometrics Technology

The term "*biometric*" is derived from the Greek words bio (stands for life) and metric (is measure). For our use, biometric refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics. These characteristics are unique to individuals, hence can be used to verify or identify a person.

Biometrics is the science and technology of measuring, analyzing, identifying or verifying the identity of a person based on physiological or behavioural characteristics gathered based on the biological data. In information technology, biometric proved to be very efficient, more natural and easy for users than traditional methods of human identification. Biometrics refers to patter recognition systems and technologies for measuring and analyzing human body characteristics, like DNA, fingerprints, eye retinas and iris, voice patterns, facial patterns and hand geometry for authentication purposes. In today's world security plays a very important role in organizations and particularly computer systems. To make the systems more reliable and secure, several biometric techniques that exploit physiological and behavioral traits of people have been developed for verification and identification of the individuals. The wide spread use of fingerprints are now in information and news. For taking the fingerprints of a person for identification purpose scanners are used which measure the unique, complex swirls on a person's fingertip which can even accommodate cuts being characterized and produced as a template. Literature and news informs that countries in the world that uses fingerprint technology includes California, Los Angels, Spain to reduce welfare fraud by using it for social security card and it's expended for use in handing out pension, unemployment and health benefits.

Definition: A biometric system is a identification system which makes a personal recognition by determining the authenticity of a specific physiological or behavioural characteristic processed by the user. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

- » The person to be identified is required to be physical present at the point of identification
- » Identification based on biometric techniques eliminates the need to remember a password or carry an identity

Depending on the context on which a biometric system works, it can be either classified as an *identification system* or a *verification* (authentication) system. *Identification involves establishing a person's identify* whereas in *verification involves confirming or denying a person's claiming identity*. (Table I)

The factors used when accessing the suitability of any trait for use in biometric authentication includes 1) *Universality* mean that every person using a should possess the trait. 2) *Uniqueness* means the trait should be sufficiently different for individuals in the relevant population. 3) *Permanence* relates to the manner in which a trait varies over time. 4) *Measurability/collectability* relates to the ease of acquisition or measurement of the trait. 5) *Performance* relates to the accuracy, speed , and robustness of technology used 6) Acceptability relates to how well individual in the relevant population accepts the technology and 7) Circumvention relates to the ease with which a trait might be imitated using an artefact or substitute.

Table I: Identification Vs. authentication

Identification	Authentication
It determines the identity of the person	It determines whether the person is indeed who he claims to be
No identity claim Many to one mapping Cost of computation id infinite number of record of users	Identity claim from the user One to one mapping The cost of computation is independent of the number of records of users
Captured biometric signatures come from a set of known biometric feature stored in the system	Captured biometric signatures may be known to the system

Recently an adaptive biometric system is becoming more popular and this field is gaining usage and its application because it aims to auto-update the model to the intra-class variation of the operational data. Firstly, with this system one no longer needs to collect a large number of biometric samples during the enrolment process. Secondly, it no longer required to re-enrol or retain the scratch in order to cope up with the changing environment of the system. These advantages of the system help to solve the problem arising due to limited training data and tracking the temporary variations of the input data through adaption. There are several open challenges involved associated with these adaptive biometric systems ,like for misclassification error i.e. false acceptance by the biometric system, cause adaption using impostor sample.

In today's world for *biometric security* there is the need for effective security being implemented efficiently. Individuals are identified to allow or restrict access to secure and protected areas or to enable them to use a computer system, personal digital assistant (PDA), or mobile smart phone. Biometric signatures or just biometrics are used to identify individuals by analysing and measuring unique physical and behavioural characteristics.

Biometric System Components include:

» *Sensor*: Collects data and converts the information to digital format

» *Signal processing algorithm*: Perform quality control activities and develop the biometric template

» *Data Storage*: Keeps information that new biometric templates will be compared to

» *Matching Algorithms*- Compares the new biometric template to one or more templates in data storage

» *Decision process*- Uses the results from the matching component to make a system-level decision(either automated or human assisted)

All the biometric technologies are implemented using *a sensor* to acquire raw biometric data from the individual or a person. Subsequently, *feature extraction* process is adopted to process the acquired data to develop a set of features that represent the biometric traits. Next *pattern matching* is done to compare the extracted feature-set against the stored templates in a database and finally *decision-making* is carried out whereby a user's claimed identity is obtained in terms of authentication or rejection. (Figure 2)

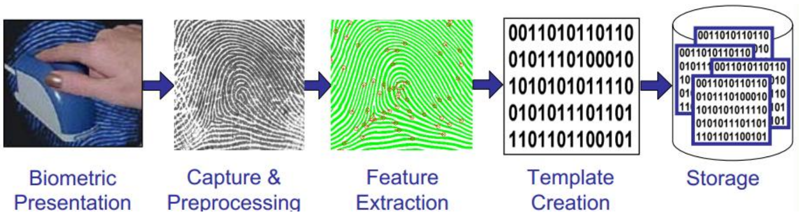


Fig. 2: Working of Biometrics

Biometric based authentication systems offer several advantages over traditional authentication schemes. They are inherently more reliable than password based authentication as biometric traits cannot be lost or forgotten (passwords can be lost or forgotten). Biometric traits are difficult to copy, share and distribute. Passwords can be announced in hacker websites and they require the person being authenticated to be present at the time and point of authentication, conniving users can deny that they have shared the password. It is difficult to forge biometrics. It requires more time, money, experience, access privileges and it is unlikely for a user to repudiate having accessed the digital content using biometrics. Thus, a biometrics based authentication scheme is a powerful alternative to traditional authentication schemes. In sometimes instances. In some instances, biometrics can be used in conjunction with passwords (or tokens) to enhance the security offered by the authentication system.

Biometrics technology is popular the following reasons:

» It is most definitive, real-time tool available today

» Can be combined with other tools to form more secure, easier to use verification solutions

» Recognizes individuals definitively

» It is based on physiological and behavioural characteristics

Biometric readings, range from several hundred bytes to over megabytes, have the advantage that their information content is usually higher than that of a password or a pass phrase. Simply extending the length of passwords to get equivalent bit strength presents significant usability problems. It is nearly impossible to remember a 2K phrase, and would take an annoyingly long time to type such a phrase (especially without errors). Fortunately, automated biometrics can provide the security advantages of long passwords while retaining the speed and characteristics simplicity of short passwords.

Even though automated biometrics can help alleviate the problem associated with the existing methods of user authentication, hackers will still find there are weak points in the system, vulnerable to attack. Password systems are prone to brute force dictionary attacks. Biometric systems, on the other hand, require substantially more effort for mounting such an attack. Yet there are several new types of attack possible in the biometric domain. This may not apply if biometrics is used as a supervised authentication tool. But in remote, unattended applications, such as Web based e-commerce applications, hackers may have the opportunity and enough time to make several attempts, or even physically violate the integrity of a remote client before detection.

III. Biometric Functionalities

Biometrics in no doubt a fascinating pattern recognition problem but , if carefully used, could also be an enabling technology with the potential to make our society safer, reduce fraud, and lead to user convenience , user friendly man machine interface by broadly providing the following three functionalities:

» ***Verification***

Biometrics helps to verify with high certainty the authenticity of a claimed enrolment based on the input biometric sample. It's the task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates. For example, a person claims that he or she is Peter Paul within the authentication system and offers his or her fingerprint. The system must match and compare his/hers biometrics with Peter Paul's stored Biometrics. The system then either accepts or rejects the claim based on a comparison performed between the offered pattern and the enrolled pattern associated with the claimed identity. If they match, then user is 'verified' or authenticated that he is indeed 'Peter Paul'. The question is: "Is this person truly Peter Paul?" It's an access control application scenarios. Typically, referred as 1:1 matching(Figure 3). Commercial applications such as computer network logon, electronic data security, ATMs, credit card purchases, physical access control, cellular phones, personal digital assistants(PDAs), medical records management, and distance learning are sample authentication applications. Authentication applications are typically cost sensitive with a strong incentive for being user friendly.

Fig 3: Referred as 1:1 matching

» ***Identification***

A submitted biometric sample is collected, searched and compared to all the templates in a database for reference matching. Match a person's biometrics against a database to figure out his identity by finding the closest match. Commonly referred to as 1: N matching (Figure 4). 'Criminal Watch-list' application scenarios

In a given input biometric sample, identification determines if the input biometric sample is associated with any of a large number e.g., millions of enrolled identities. The question is: "Is this person in the database?" Typically identification applications include welfare disbursement, national ID cards, border control, voter ID cards, driver's license, criminal investigation, corpse identification, parenthood determination, missing children identification etc. These identification applications require a large sustainable throughput with as little human supervision as possible.

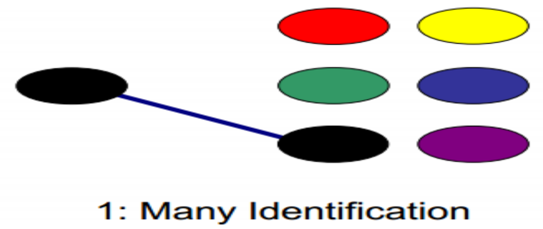


Fig 4: Referred to as 1: N matching

Broadly identification is categorized into

1. Closed-set identification: The person is known to exist in the database
2. Open-set identification: The person is not guaranteed to exist in the database. System determines if the person is in the database.

» **Screening**

Screening applications determine whether a person belongs to a watch list of identities. The question is: “Is this a wanted person?” Example of screening applications could include airport security, security at public events and other surveillance applications. The screening watch list consists of moderate e.g., a few hundred number of identities. The screening applications:

1. Do not have a well defined *user* enrolment phase
2. Can expect only minimal control over their subjects and imaging condition.
3. Requires large sustainable throughput with as little human supervision as possible.

Screening cannot be accomplished without biometrics e.g., by using token based or knowledge based identification. Now-a-days biometric systems are therefore increasingly being deployed in civilian applications that have several thousand enrolled users.

» ***Biometric Characteristics***

A number of biometric characteristics have been in use for different applications [8].Each biometric trait has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet all of the requirements (e.g., accuracy, practicality, and cost) of all applications (e.g., DRM, access control, and welfare distribution). No biometric is *optimal* although a number of them are *admissible*. The suitability of a specific biometric for a particular application is determined depending upon the requirements of the application and properties of the biometric characteristics. Traits such as voice and keystroke lend themselves more easily to a challenge response mechanism that may be necessary in applications like telebanking. The main types of biometrics include Finger prints, Retina Scans, Iris Scans, Voice recognition, Face recognition. Other forms of emerging biometrics are thermal scans, DNA (actually actively used in forensics), Signatures, hand geometry, ear structure, and heart rhythm (Figure 5).

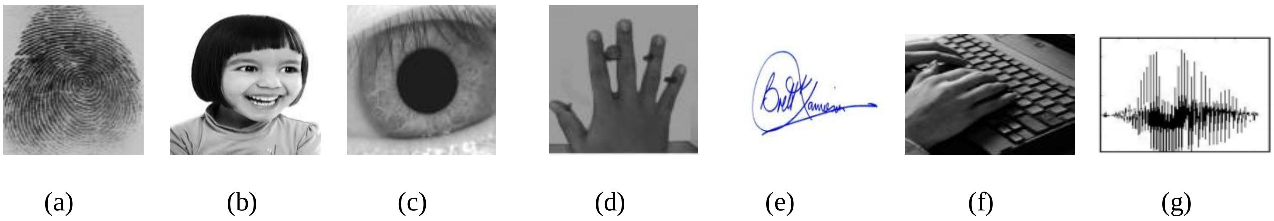


Fig 5: Examples of biometric characteristics: (a) fingerprint, (b) face, (c) iris, (d) hand geometry, (e) signature (f) keystroke, and (g) voice

Commonly used biometrics is given below:

A. Fingerprint:

Human fingerprint is made of a number of ridges and valley on the surface of finger that are unique to each human. "Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form two minutiae points: ridge endings-where the ridges end, and ridge bifurcations-where the ridges split in two. (Figure 6)The uniqueness of a fingerprint can be determined by the different patterns of ridges and furrows as well as the minutiae points. A fingerprint is the pattern of ridges and valleys on the surface of fingertips, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person.

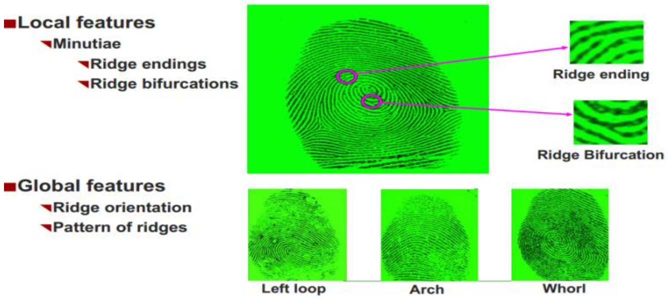


Fig 6: Fingerprint Biometric

There are five basic patterns which make up the fingerprint: the arch such as tented and plain arch covers 5% of fingerprint; left and right loop covers 60% of fingerprints; whorl covers 34% of fingerprints and accidental whorls covers 1% of fingerprints (Figure 7).Minutiae based fingerprint matching is one of the most commonly used algorithms for extracting features that characterizes a fingerprint (Figure 8).The different Minutiae feature locations and types can identify different individuals. These are what are stored in the Biometric template. Image & Signal processing used to process fingerprint images. Humans have used fingerprints for personal identification for many decades and the matching (i.e., identification) accuracy using fingerprints has been shown to very high [9]. The accuracy of the currently available fingerprint recognition systems is adequate for authentication system involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large scale identification involving millions of identities. One problem with the current fingerprint recognition system is that they require a large amount of computational resources, especially when operating in the identification mode. Today, the marginal cost of embedding a fingerprint based biometric in a system e.g., laptop, computer which has become affordable in a large numbers of applications. Fingerprints of a small fraction of the population may be unsuitable for the automatic identification because of genetic factors, aging, environmental, or occupational reasons, e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing.

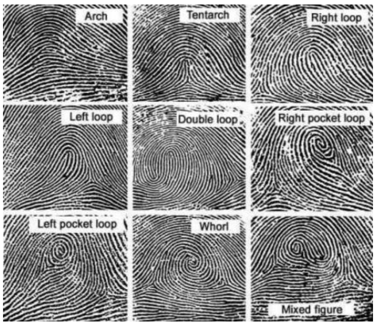
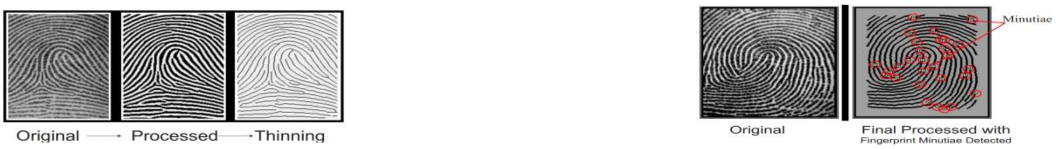


Fig 7: Fingerprint types. (Source: http://www.FINGERPRINTS.TK[Lazaroff,2004])

There are several benefits of using fingerprint recognition systems. This system is easy to use and install. It requires cheap equipment which generally has low power consumption. However, there are some disadvantages in this system. If the surface of the finger gets damaged and/or has one or more marks on it, identification becomes increasingly hard. Furthermore, the system requires the users' finger surface to have a point of minutiae or pattern in order to have matching images. This will be a limitation factor for the security of the algorithm. Fingerprint security system is used widely in different applications such as: cell phones, laptops, USB flash drives and others devices. It is also used in judicial systems in order to record users' information and verify one person's identity



(a) *(b)*

Fig 8: Fingerprint Minutiae Extraction

B. Face:

Face recognition detector technique capture a facial image, which is then transformed into a unique face print .The image is transformed using a technique called "elastic graph matching". Algebraic algorithms are used to make a perfect match. Images are sent to a back-end database for comparison and possible matches. Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristics used by humans to make personal recognition. The most popular approaches for face recognition [10] are based on:

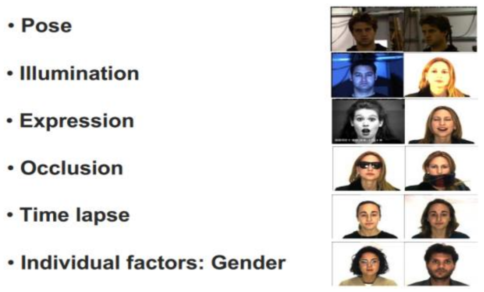
» The location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their special relationships

» The overall (global) analysis of the face images that represents a face as a weighted combination of a number of canonical faces.

The authentication performance of the face recognition systems are commercially available is reasonable [11]. They impose a number of restrictions on how the facial images are obtained, often requiring a fixed and simple background or special illumination. These systems also have difficulty in matching face images captured from two drastically different views and under different illumination conditions i.e., varying temporal contexts. It is to be confirmed that the face itself, without any contextual information, is sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence. For a facial recognition system to work well in practice, it should automatically detect whether a face is present in the acquired image, locate the face if there is one and recognize the face from a general viewpoint i.e., from any pose. It will measure the overall structure, shape and proportion of features on the user's face such as: distance between eyes, nose, mouths, ears, jaw, size of eyes, mouth and others expressions. Facial expression is also counted as one of the factors to change during a user's facial recognition process. Examples include, smiling, crying, and wrinkles on the face. There are various challenges faced during the face recognition like pose, illumination, expression, occlusion, time-lapse, individual factors like gender-male or a female etc. (Figure 9(a) and Figure 9(b))

Future of face recognitions can be depends the wide use of tools like Neural Nets to improve accuracy and predictions. Wearable computing will make face recognition ubiquitous. Hybridized techniques would be used with face recognition like thermal scans, voice recognition of digitized images

Future of face recognitions can be depends the wide use of tools like Neural Nets to improve accuracy and predictions. Wearable computing will make face recognition ubiquitous. Hybridized techniques would be used with face recognition like thermal scans, voice recognition of digitized images



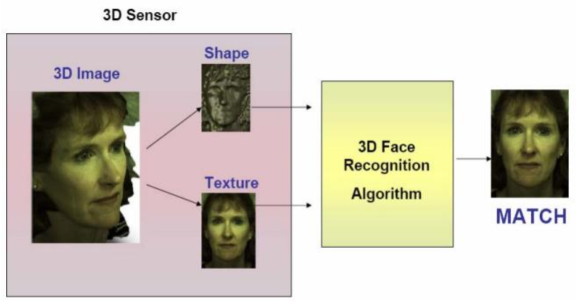


Fig 9(a): Challenges in Face recognition

Fig 9(b): 3D Face matching

Source: http:// www.frvt.org/FRGC/FRGC_Phillips.pdf

Eigen faces is a very well known Face Recognition algorithm in the research community. It has become a baseline for comparing new algorithms and manner in which they perform better. This uses Linear Algebra math to decompose a 'basis' vectors which can describe training face data. These basis vectors are called 'Eigenvectors' or 'Eigen faces' since these vectors look like faces (Figure 10)

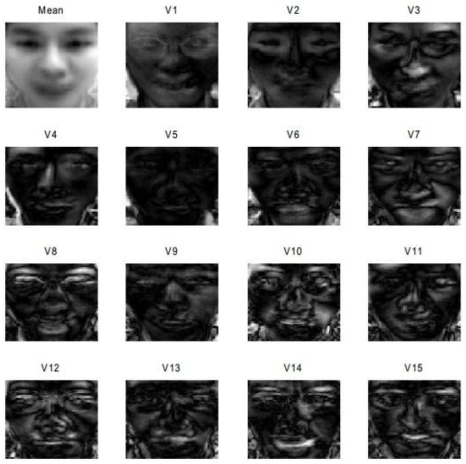


Fig 10: Eigen vectors look alike

Source: Dr. Matios Savvides, Lecture Notes in Pattern Recognition Course, Electrical & Computer Engg, Carnegie Mellon University

As the human face is one of the easiest characteristic this can be used in biometric security system to identify a user. Face recognition technology, is very popular and is used more widely because it does not require any kind of physical contact between the users and device. Cameras scan the user face and match it to a database for verification. Furthermore, it is easy to install and does not require any expensive hardware. Facial recognition technology is used widely in a variety of security systems such as physical access control or computer user accounts. However, it is still not as unique as its counterparts such as retinal, iris or DNA. Therefore, it is normally used with other characteristics in the system. On the other hand, time is the most negative affective factor with face recognition technology because as the user ages will change over time. Biometric face recognition systems will collect data from the users' face and store them in a database for future use.

C. Iris:

The iris is the colored portion of the eye surrounding the pupil. Its pattern results from a meshwork of muscle ligaments, and its color and contrast are determined by pigmentation. The iris is the annular region of the eye bounded by the pupil and the sclera, is white of the eye, on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of the file.

Advantages of Iris as biometric

» Thought to be very unique, potentially more discriminate than fingerprints

» Remains stable over an individual’s lifetime

» For cooperating subjects, iris pattern is captured quickly in an image

The complex iris texture carries very distinctive information useful for personal recognition. [12] [13] [14]. The accuracy and speed of currently deployed iris based recognition system is promising and points to the feasibility of large scale identification systems based on iris information. Each iris is believed to be distinctive and like fingerprints even the irises of identical twins are expected to be different. It is extremely difficult to surgically tamper the texture of the iris. The ability to detect artificial irises e.g., designer contact lenses, has been demonstrated in the literature. Although the early iris based recognition system required considerable user participation and were expensive, the newer systems have become more user friendly and cost effective. While iris systems have a very low false accept rate (FAR) compared to other biometric traits, the false reject rate (FRR) of these systems can be high [15]

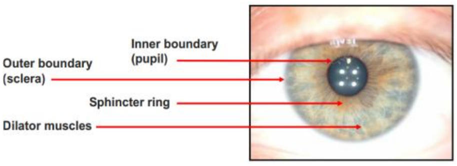
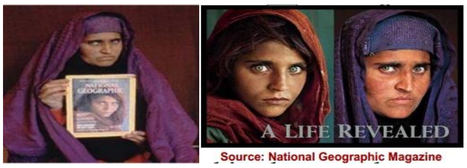


Fig 7: Iris as Biometric

Iris recognition security systems are considered as one of the most accurate security system nowadays. It is unique and easy to identify a user. Even though the system requires installation equipment and expensive fees, it is still the easiest and fastest method to identify a user. There should be no physical contact between the user and the system during the verification process. During the verification process, if the users are wearing accessories such as glasses and contact lenses, the system will work as normal because it does not change any characteristics of the user's iris. Theoretically, even if users have eye surgery, it will have no effect on the iris characteristics of that individual

Iris Biometric got really famous in the lost Afghan girl story......

In 1994 National Geographic photographer Steve McCurry took a picture of a little Afghan girl called Sharbat Gula in refugee camp in Pakistan. Her photo (she had amazing green eyes) made it to National Geographic 100 best Pictures! McCurry later tried to trace and find the girl, until finally 17 years later he located a girl with those same haunting green eyes.

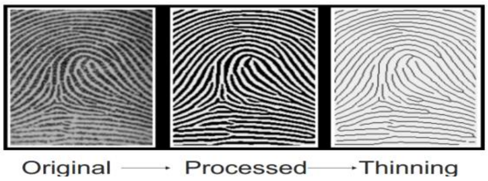


Source: National Geographic Magazine

http://news.nationalgeographical.com/news/2002/03/0311_020312_sharbat.html

17 years passed…how to verify if this was the same girl?

Hard-ship changed the girl’s appearance. But she had those same haunting green eyes…The Explorer team got verification using U.S.FBI iris scanning technology. They used iris image from old taken photograph and compared to the new one. Iris code declared a ‘match’! This was indeed the same girl! Iris biometric made it possible to verify this.



D. Hand Geometry:

Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and length and width of the fingers [16]. Commercial hand geometry based authentication systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effect on the authentication accuracy of hand geometry based systems. The geometry of the hand is not known to very distinctive and hand geometry based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry information may not be invariant during the growth period of children.

One of the recent biometric technologies invented is the vein recognition system. Veins are blood vessels that carry blood to the heart. Each person's veins have unique physical and behavioural traits. Taking advantage of this, biometrics uses unique characteristics of the veins as a method to identify the user. Vein recognition systems mainly focus on the veins in the users hands. Each finger on human hand has veins which connect directly with the heart and it has its own physical traits. Compared to the other biometric systems, the user's veins are located inside the human body. Therefore, the recognition system will capture images of the vein patterns inside of users' fingers by applying light transmission to each finger. For more details, the method works by passing near-infrared light through fingers, this way a camera can record vein patterns. Vein recognition systems are getting more attention from experts because it has many other functions which other biometrics technologies do not have. It has a higher level of security which can protect information or access control much better. The level of accuracy used in vein recognition systems is very impressive and reliable by the comparison of the recorded database to that of the current data. Furthermore, it also has a low cost on installation and equipment. Time which is taken to verify each individual is shorter than other methods averaging 0.5second.

An individual’s jewellery e.g., rings or limitations in dexterity e.g., from arthritis, may pose further challenges in extracting the correct hand geometry information. The physical size of a hand geometry based system is large and it cannot be embedded in certain devices such as laptops. There are authentication systems available that are based on measurements of only a few fingers typically index and middle finger instead of the entire hand. These devices are smaller than those used for hand geometry, but are still much larger than those used in some other biometrics e.g., fingerprint, face and voice.

E. **Keystroke:**

It is hypothesized that each person types on a keyboard in a characteristic way. This behavioural biometric is not expected to be unique to each individual but it is expected to offer sufficient discriminatory information that permits identity verification [17]. Keystroke dynamics is a behavioural biometrics for some individuals; one may expect to observe large variations in typical typing patterns. The keystrokes of a person using a system could be monitored as that person is keying in information. This biometric permits *continuous verification* of an individual over a period of time.

F. Signature:

The way a person signs his or her name is known to be characteristic of that individual [18]. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal and commercial transactions as a method of authentication. Signatures are a behavioural biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially even successive impressions of their signature are significantly different. Professional forgers may be able to reproduce signatures that fool the system.

G. Voice:

Voice is a combination of physical and behavioural biometrics. The features of an individual's voice are based on the shape and size of the appendages e.g., vocal tracts, mouth, nasal cavities and lips, that are used in the synthesis of the sound [19]. These physical characteristics of human speech are invariant for an individual, but the behaviour part of the speech of a person changes over time due to age, medical conditions such as common cold, emotional state etc. Voice is also not very distinctive and may not be appropriate for large scale identification. A text dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text independent voice recognition system recognizes the speaker independent of what he or she speaks. A text independent system is more difficult to design than a text dependent system but offers more protection against fraud. A disadvantage of voice based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone based applications but the voice signal over phone is typically degraded in quality by the communication channel. Example of commonly used representation schemes and matching algorithms for five different biometric traits are as below:

Table II: List of the commonly used representation and matching schemes for biometric traits

Modality **(Biometric Trait)**	**Representation Scheme**	**Matching Algorithm**
Fingerprint	Minutiae distribution	String matching
Face	Principal Component Analysis(PCA)	Euclidean distance, Bunch graph matching
Iris	Texture analysis, Key point extraction	Hamming distance
Hand	Length/Width of fingers/palm	Euclidean distance
Voice	Mel-Cepstrum	Hidden Markov model, Gaussian mixture model

IV. Pros and Cons of Biometric Systems

The different biometrics has different properties.1) *Fingerprint's* uniqueness can be defined by analyzing the minutiae of a human being. Two individuals having the same fingerprint is less than one in a billion. 2) To identify any person, generally look at face and eyes in particular seem to tell a story how the person feels. Face recognition is a kind of electronic unmasking 3) Iris is thin membrane on the interior of the eyeball. Iris pattern remains unchanged after the age of two and does not degrade overtime or with the environment. Iris patterns are extremely complex than other biometric patterns. The iris-scan process begins with a photograph. A specialized camera, typically very close to the subject, not more than three feet, uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. This process takes 1 to 2 seconds. The picture of eye first is processed by software that localizes the inner and outer boundaries of the iris. And it is encoded by image-processing technologies. In less than few seconds, even on a database of millions of records, the iris code template generated from a live image is compared to previously enrolled ones to see if it matches to any of them. An iris recognition camera takes a black and white picture from 5 to 24 inches away. The camera uses non-invasive, near-infrared illumination that is barely visible and very safe. And this iris recognition cannot take place without the person permission 4) The person to be identified is usually pronounce a designated password or phrase, which facilitates the verification process. But has the weakness of technology. 5) This is done by analyzing the shape, speed, stroke, pen pressure and timing information during the act of signing. Dynamic signature verification is a replacement. 6) The image of the hand is collected and the feature vectors are extracted and compared with the database feature vectors.

Properties of biometric identifiers are as below:

- Universality- Do all people have it?
- Distinctiveness- Can people are distinguished based on an identifier?
- Permanence-How permanent are the identifiers?
- Collectable-How well can the identifiers be captured and quantified?

Attributes of biometric systems are as below:

- Performance-Matching speed and accuracy
- Acceptability-Willingness of people to accept
- Circumvention-Foolproof

The most widely used biometrics and associated advantages are described below: (Table 3)

Table III: Advantages of Biometric Security System

Biometrics	Advantages
Fingerprints	» 5-9 second processing time » Commonly used in boarder management » Used in law enforcement
Facial Recognition	» Non-invasive collection » Currently used for passports and National ID documents
Iris	» Low False Acceptance rates » Difficult to replicate » Two seconds processing time » Accurate » Stability » Fast » Scalable
DNA	» Establishes familial relationship » Commonly used in Law enforcement » Highly unique/impossible to replicate

Advantages

1. The first advantage of using this new technology is the uniqueness and it is also the main characteristic which allows biometrics technology to become more and more important in our lives. With uniqueness of biometrics technology, each individual's identification will be single most effective identification for that user. A chance of two users having the same identification in the biometrics security technology system is nearly zero.
2. Secondly, the highly secure way of identifying users makes this technology less prone for users to share access to highly sensitive data. For example, users can share their fingerprints, iris and so forth allowing other users access to secure information. Each trait used during identification is a single property of that user. In other words, it is extremely hard or impossible to make duplicate or share biometrics accessing data with other users. This makes it ever more secure allowing user information and data to be kept highly secure from unauthorized users

3. Lastly, this identification of users though biometrics cannot be lost, stolen or forgotten. This aspect of biometrics technology allows it to become more popular in its use. This method of identifying and giving access to user makes user identification a lot easier. Finally, most biometrics security systems are easy to install and it requires small amount of funding for equipment (except modern biometrics technology such as: DNA/retinal/iris recognition)

Disadvantages

Even though, there are many advantages of biometrics security system, it still has many flaws in its system.

1. Each biometrics application method has weaknesses which can cause problems for its users. For example, if the biometrics security system uses fingerprints to identify its users and an accident causes a user to lose his/her finger then it can be a problem during the verification process. For voice recognition methods, illnesses such as strep throat can make it hard for authorized users to get access to their information. Another factor that can influence voice recognition systems is the continuous aging of its users. Noise in an environment where voice recognition is used to identify its users can also make it hard for users to be identified
2. For iris or retinal scanning applications, users may find it very intrusive. Users may also have the concern for the safety of their eyes during the iris or retinal scan. Furthermore, databases used to store user identification data will be very large which might form a potential threat. For scanning retinal/iris characteristics and storing large amount of database, biometrics system requires new and modern technology. Therefore, the cost for equipment is also expensive.

Finally, lots of people are still concerned about biometrics technology in different aspects such as: security, adaptability to rate of change in life, scalability, accuracy, privacy and others.

V. BIOMETRIC TIMELINE

Biometrics was used during prehistoric times. Chinese used fingerprinting in the 14th Century for identification. In the 17th century fingerprinting was used to seal official documents**.**

- 1858 -First systematic capture of hand images for identification purposes is recorded
- 1870 – Bertillon develops anthropometrics to identify individuals
- 1892- Gatton develops a classification system for fingerprints
- 1896- Henry develops a fingerprint classification system
- 1936- Concept of using the iris pattern for identification is proposed
- 1960s- Face recognition becomes semi-automated
- 1960- First model of acoustic speech production is created
- 1965- automated signature recognition research begins
- 1969-FBI pushes to make fingerprint recognition an automated process
- 1974- First commercial hand geometry systems become available
- 1986- Exchange of fingerprint minutiae data standard is published
- 1988- First semi-automated facial recognition system is deployed
- 1992- Biometric consortium is established within US Government
- 1997- First commercial , generic biometric interoperability standard is published
- 1999- FBI's IAFIS major components become operational

» 2002- M1 Technical Committee on Biometrics is formed

» 2003-Formal US Government coordination of biometric activities begins

» 2004- US-VISIT program becomes operational

» 2004- DOD implements ABIS

» 2005- US patent on iris recognition concept expires

VI. Conclusion

Biometrics technology provides us with great number of new inventions which improves both the quality and the longevity of our lives. Nowadays, biometrics technology is considered one of the best protection methods of user information, data, etc. Basically, biometrics technology method will collect and measure data of human physiology and behaviour. There are several ways to collect and measure data of users such as: scanning the unique characteristics of the person (retinal, finger-print, facial expression, etc.) or analyzing the unique behaviour of human (signature, keyboard typing styles, etc.). The main purpose of biometric system is to identify and verify a person's identity. Biometrics technology is more convenient than other protection technologies of identity authentication. Biometrics security system has bigger applications in our lives and in recent years, scientists have developed higher stages of identifying a user's identity. Our main application is facial recognition technology. With this technology, we can recognize any person in a crowded group; therefore, we can verify their identification. We can also use this method of biometrics technology to detect previously identified criminals and terrorists in society. This will help us to reduce the crime rate in the world.

Biometrics technology is applied in a variety of ways and different fields of practice. For example, we can see that it is applied in hospitals to verify the identity of patients and to protect their privacy. Furthermore, biometrics technology has been used at airports to verify the identity of people. By using this technology, it helps governments keep track of people going in and out of country. It also helps to identify criminals and terrorists. Other example of this technology which is applied in our daily lives is voice recognition; voice recognition systems are applied in homes to verify identities of authorized users. This technology is not only used for security sections, but it also can be applied in the other aspects of life. It has been used in businesses such as e-commerce and shipping sections.

Biometrics technology is a new technology for most of us because it has only been implemented in public for short period of time. There are many applications and solutions of biometrics technology used in security systems. It has many advantages which can improve our lives such as: improved security and effectiveness, reduced fraud and password administrator costs, ease of use and makes live more comfortable. Even though the biometrics security system still has many concerns such as information privacy, physical privacy and religious objections, users cannot deny the fact that this new technology will change our lives for the better.

References

1. G. Oestreicher-Singer and A. Sundararajan, “Are digital rights valuable? Theory and evidence from the eBook industry, “ in Proc. 25th Int. Conf. Information Systems, Washington, D.C. , Sep. 2004, pp. 533-545
2. Advanced encryption standard (AES), Federal Information Processing Standards Publication 197 National Institute of Standards and Technology, 2001 [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
3. W. Stallings, “Cryptography and Network Security: Principles and Practices”, 3rd ed. Upper Saddle River, NJ: Prentice-Hall, 2003, Guest Editorial, S. Pankanti, R. Bolle, A. K. Jain (Guest Editors)Special Issue of IEEE Computer on Biometrics, Feb. 2000
4. D. V. Klein, “Foiling the cracker: a survey of, and improvements to, password security,” in Proc. 2nd USENIX Workshop Security, 1990,pp. 5–14.
5. A. K. Jain, R. Bolle, and S. Pankanti, Biometrics: Personal Identification in Networked Society, Norwell, MA: Kluwer, 1999
6. A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Trans. Circuits Syst. Video Technology, Special Issue Image- and Video-Based Biomet.”, vol. 14, no. 1, pp. 4–20, Jan.2004
7. R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, Guide to Biometrics. New York: Springer, 2004.

8. J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds., Biometric Systems: Technology, Design and Performance Evaluation. NewYork: Springer Verlag, 2005

9. D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York: Springer Verlag, Jun. 2003

10. S. Z. Li and A. K. Jain, Eds., Handbook of Face Recognition. New York: Springer Verlag, 2004

11. P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, FRVT 2002: Evaluation Report March 2003 [Online].Available: http://www.frvt.org/FRVT2002/documents.htm

12. J. Daugman,, " The importance of being random: statistical principles of iris recognition, " Pattern Recognit., vol. 36, no. 2, pp. 279-291, 2003

13. L. Ma, T. Tan, D. Zhang, and Y. Wang, "Personal identification based on iris texture analysis, "IEEE Trans. Pattern Anal. Mach, Intell., vol. 25, no. 12,pp. 1519-1533, Dec. 2003.

14. R. Wides, " Iris recognition: an emerging biometric technology," Proc. IEEE, vol. 85, no. 9, pp. 1348-1363, Sep.1997

15. International Biometric Group, " Independent Testing of Iris Recognition Technology May 2005 [online]. Available : http://www.biometric-group.com/reports/public/reports/ITIRT_report.htm

16. R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos,"Biometric identification through hand geometry measurements," IEEE Trans. Pattern Anal. Mach. Intell., vol. 22, no. 10, pp. 1168-1171, Oct. 2000

17. F. Monrose and A. Rubin, " Authentication via keystroke dynamics, " in Proc. 4th ACM Conf. Computer and Communications Security, Apr. 1997,pp.48-56

18. V.S. Nalwa, " Automatic online signature verification, " Proc. IEEE, vol. 85, no. 2, pp. 213-239, Feb. 1997.

19. J.P. Campbell, " Speaker recognition: a tutorial, " Proc. IEEE, vol. 85, no. 9, pp. 1437-1462, Sep. 1997

AUTHOR(S) PROFILE

Manaswini Pradhan is a Lecturer in the P G Dept. of Information & Communication Technology, Fakir Mohan University, Balasore-756019, Odisha.