Network security
By
Biometrics

Presented by

N.ABHILASH 05E81A1201

B.HARI KRISHNA 05E81A1211

III rd B.Tech (C.S.I.T)

ALFA COLLEGE OF ENGG&TECHNOLOGY

ALLAGADDA

EMAIL ID: abhiever_143@yahoo.co.in

Hari.bezawada@gmail.com

CONTENTS:

ABSTRACT

The automated use of physiological or behavioral characteristics to determine or verify identity. To elaborate on this definition, physiological biometrics are based on measurements and data derived from direct measurement of a part of the human body. Fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition are leading physiological biometrics.

Various biometric technologies are fingerprint identification, speaker recognition, facial recognition, hand geometry, signature-scan, keystroke-scan, palm-scan, etc. Among these popular recognition techniques like fingerprint recognition , facial recognition and speech recognition are clearly explained. An automatic personal identification system based solely on one methodology often cannot meet the system performance requirements. So a combination of two or more methodologies is used to achieve required performance, which is called multibiometrics. In this paper we explained an example of multi biometric system, which combines fingerprint identification, speech recognition and facial recognition. A neatly sketched figure is used to describe the process in brief.

Biometrics has wide area applications; Most of them are covered in this paper. Also some of the future applications like ATM machine, workstation and network access, travel and tourism and telephone transactions are mentioned.

INTRODUCTION:

Thousands of years earlier physiological parameters such as scars, complexion, eye color, height, moles, etc are used to identify the individuals. Later, in the nineteenth century physical features and characteristics are used to identify criminals. This resulted in a variety of measuring devices being produced. The idea of measuring individual physical characteristics seemed to stick and the parallel development of fingerprinting became the international methodology among police forces for identity verification.

With this background, it is hardly surprising that for many years a fascination with the possibility of using electronics and the power of microprocessors to automate identity verification had occupied the minds of individuals and organizations both in the military and commercial sectors. After the September 11th terrorist attack, Biometrics has gained prominence as being more reliable than current technologies, for people identification.

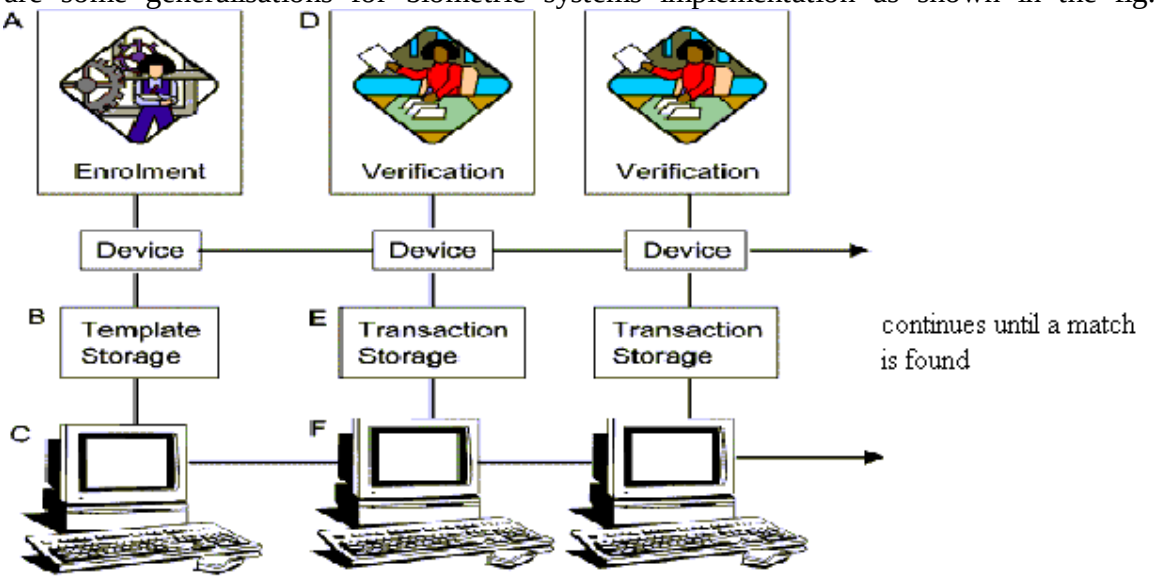
Definition:

Biometrics involves identifying a person based on a unique physical characteristic that is different from any other person. Biometrics can be either 'innate' such as fingerprints, face or iris; or 'behavioral' such as handwriting, gait or typing

Style. Biometric characteristics are measured using sensors that produce data values that can then be processed by a computer using specialized algorithms for analysis and comparison. *Biometric system* is the integrated biometric hardware and software used to conduct biometric identification or verification.

How Biometric Systems Works?

Biometric devices and systems have their own operating methodology, there are some generalisations for biometric systems implementation as shown in the fig.



[A] *Enrollment*: The process whereby a user's initial biometric sample or samples are collected, assessed, processed, and stored for ongoing use in a biometric system. These samples are referred as templates. A poor quality template will often cause considerable problems for the user, often resulting in a re-enrolment.

[B] *Template storage* is an area of interest particularly with large scale applications which may accommodate many thousands of individuals. The possible options are as follows; Store the template within the biometric reader device or remotely in a central repository or on a portable token such as a chip card. The last one is an attractive option for two reasons. Firstly, it requires no local or central storage of templates and secondly, the user carries their template with them and can use it at any authorized reader position.

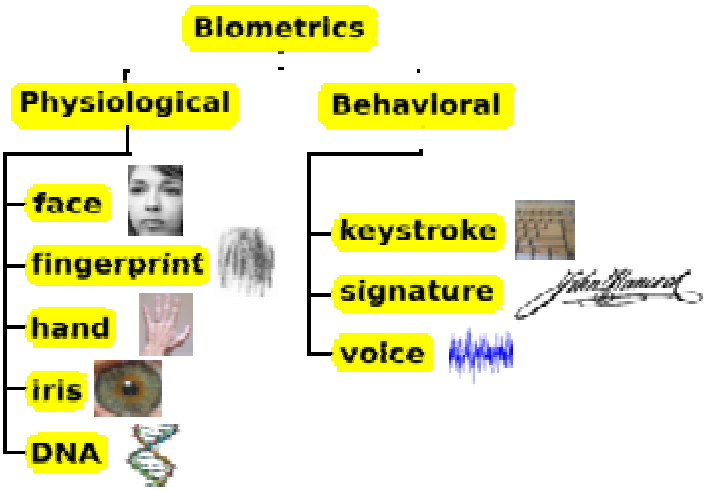
[C] *The network*. Networks may rely on the vendor's systems design and message functionality, together with their own software. Or the user can himself design networking, message passing and monitoring system ,taking advantage of the recent generic biometric API's and accessing the reader functions directly. This provides absolute flexibility and control over systems design.

[*D*] *Verification*: The verification process requires the user to claim an identity by either entering a PIN or presenting a token, and then verify this claim by providing a live biometric to be compared against the claimed reference template. There will be a resulting match or no match accordingly. A record of this transaction will then be generated and stored, either locally within the device or remotely via a network and host (or indeed both).

[E] *Transaction storage:* Some devices will store a limited number of transactions internally, scrolling over as new transactions are received.

[F] *The network (again):* Here the network handles transactions, which is of critical importance in some applications.

Common Human biometric characteristics:



Classification of some biometric traits

Biometric characteristics can be divided in two main classes, as represented in figure on

the right:

physiological are related to the shape of the body. The oldest traits, that have been used for more than 100 years, are fingerprints. Other examples are face recognition, hand geometry and iris recognition.

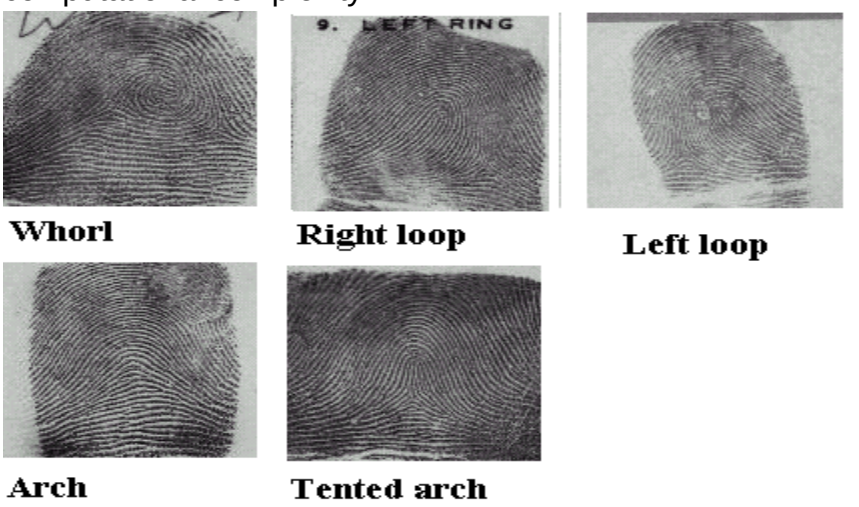
behavioral are related to the behavior of a person. The first characteristic to be used, still widely used today, is the signature. More modern approaches are the study of keystroke dynamics and of voice.
Strictly speaking, voice is also a physiological trait because every person has a different pitch, but voice recognition is mainly based on the study of the way a person speaks,

commonly classified as behavioral.

Popular Biometric Methodologies:

1.Finger Print Identification:

- *Finger Print Matching:* Among all the biometric techniques, fingerprint-based identification is the oldest method, which has been successfully used in numerous applications. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are the locations on your fingerprint where the ridges will stop or split into two, or intersect. Fingerprint matching techniques can be placed into two categories: *minutiae-based* and *correlation based*. In minutiae-based matching a fingerprint is initially enrolled into an archive. Instead of storing the entire image of the fingerprint, only the minutiae points are kept. An algorithm is used to translate the minutiae points into a code, which is called the template. Later, when the person has their fingerprint scanned, the minutiae points are recognized, placed through the algorithm and the code is compared to the template. But it is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Local ridge structures cannot be completely characterized by minutiae. The correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation. So an alternate representation of fingerprints is tried, which will capture more local information and yield a fixed length code for the fingerprint.
- *Fingerprint Classification:* An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database . The input fingerprint is required to be matched only with a subset of the fingerprints in the database to reduce the search time and computational complexity.



An algorithm classifies fingerprints into five classes namely, *whorl, right loop, left loop, arch, and tented arch*, as shown in figure. The algorithm separates the number of ridges present in four directions (0 degree, 45 degree, 90 degree, and 135 degree).

2.Speaker Recognition:

It involves recognizing people based on their voices. Systems plot frequencies that the voice produces every 1/100th of a second to form a "waterfall." The "waterfall" is a three-dimensional image that is a map of the voice for one second. A line graph of curved and straight arrows note the transitions between phonemes, the smallest units of speech. A database stores this information until it is needed. Voiceprint determines resonance of the cavities in the throat with vocal-tract geometry from a voice sample. Different languages, different voice samples, stuffy noses etc cannot fool this method. There are two types of models that have been used extensively in speaker verification and speech recognition systems: *stochastic models* and *template models*. The stochastic model treats the speech production process as a parametric random process and assumes that the parameters of the underlying stochastic process can be estimated in a precise, well-defined manner. The template model attempts to model the speech production process in a non-parametric manner by retaining a number of sequences of feature vectors derived from multiple utterances of the same word by the same person. A very popular stochastic model for modeling the speech production process is the Hidden Markov Model (HMM). The model is a doubly embedded stochastic process where the underlying stochastic process is not directly observable (it is hidden). The HMM can only be viewed through another set of stochastic processes that produce the sequence of observations. Thus, the HMM is a finite-state machine, where a probability density function p(x | s_i) is associated with each state s_i. The states are connected by a transition network, where the state transition probabilities are a_{ij} = p(s_i | s_j). A fully connected three-state HMM is depicted in figure

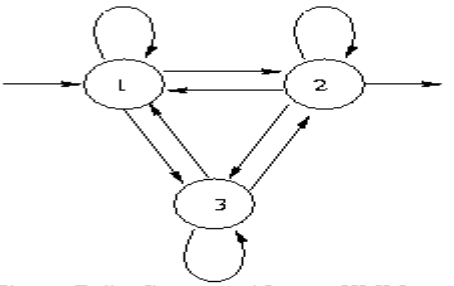


Figure: Fully Connected 3-state HMM

For the Hidden Markov models, the matching score is the probability that the model generated a given set of feature vectors.

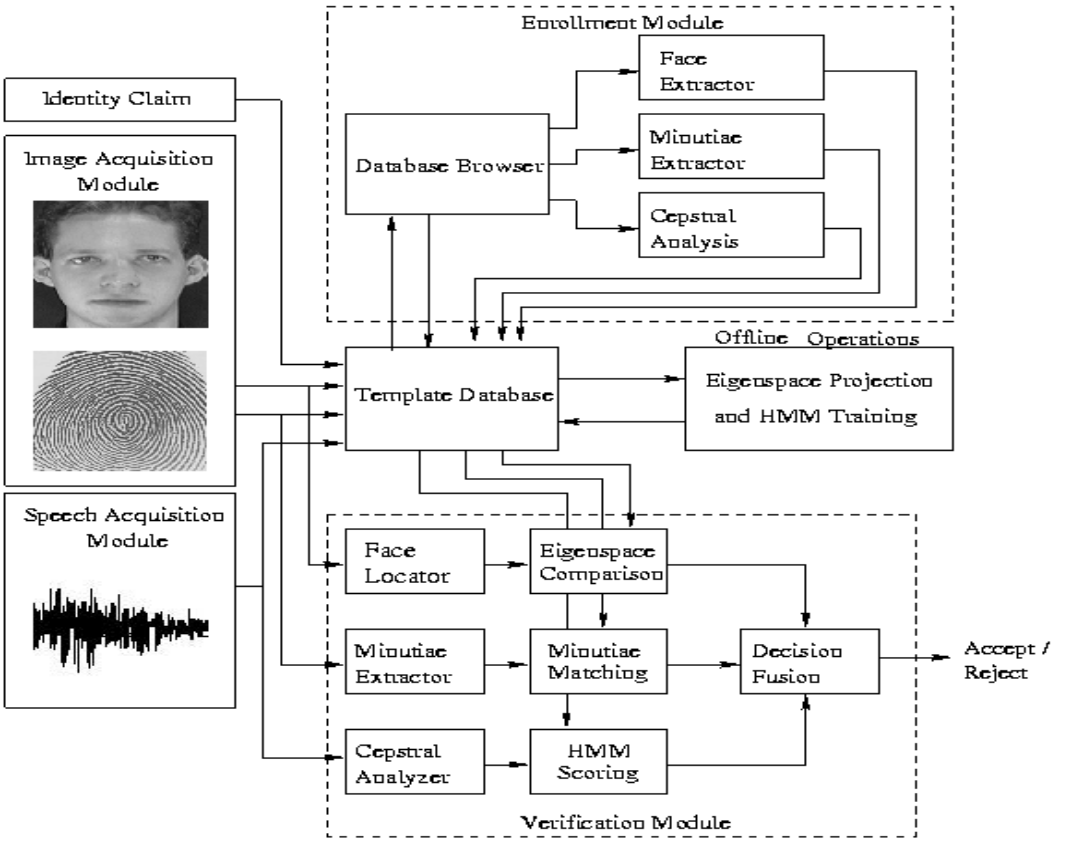
3.Facial Recognition:

- *Eigenfaces:* Developed by Visage Technology. First, a camera captures the image of a person. The face is mapped into a variety of coefficients depending on the features, which becomes 128 digits, otherwise called a "vector." The vector is the code for the person. When the person presents him/herself later to be identified, he/she must present a PIN or bar code and then allow the camera to take a picture. The difference between the face's vector and the database's vector for the PIN or bar code are placed on a coordinate system called "face space" and the differences between the two of them are

determined.If distance between the images is small enough, access is granted, else denied

- *Local Feature Analysis*: Local Feature Analysis (LFA) is another algorithm. First, the camera takes a picture of the face and cuts out the background and other faces. LFA is based on idea that all faces are made of building blocks. However, every face uses different building blocks and puts them together in a unique manner. LFA translates the building blocks into a code called "face print." The "face print" is stored in a database for identification. LFA is also used for verification.
- *Neural Networks*: Neural Networks is a slight bit more complicated than the "eigenfaces" method. A series of neurons, or processing units, are connected together. A programmer sets the rules of how the neurons recognize patterns. If the actual output is greatly different than the computed output, then the neurons will adjust itself to fit the situation. More situations lead to more shifts in neurons, which lead to better results.

MultiBiometrics:



A biometric system, which relies only on a single biometric identifier in making a personal identification, is often not able to meet the desired performance requirements.

We introduce a multimodal biometric system, which integrates face recognition, fingerprint verification, and speaker verification in making a personal identification. This system takes advantage of the capabilities of each individual biometric. A multimodal biometric system integrates face recognition, fingerprint verification, and speaker verification in making a personal identification as shown in figure.

Applications:

- Time Attendance
- Access control
- Identification card and Immigration checks
- Police records, Patient management in hospitals
- Customer identification, Loyalty programs
- Security systems and Preventing identity theft
- Membership management in clubs, libraries etc.

Future Applications:

v ATM machine use: Most of the leading banks have been experimenting with biometrics for ATM machine use and as a general means of combating card fraud.

v *Workstation and network access:* Many are viewing this as the application, which will provide critical mass for the biometric industry and create the transition between sci-fi device to regular systems component, thus raising public awareness and lowering resistance to the use of biometrics in general.

v *Travel and tourism:* There are multi application cards for travelers which, incorporating a biometric, would enable them to participate in various frequent flyer and border control systems as well as paying for their air ticket, hotel room, hire care etc.

v *Telephone transactions*: Many telesales and call center managers have pondered the use of biometrics.

Real-time Application:

U.K Airport Tests Passenger Eye ID's: Heathrow is the first UK airport to carry out a large-scale trial of the iris recognition technology, which examines a passenger's eye, rather than their passport as they go through immigration control. The aim is to speed up the movement of passengers through the terminal and detect illegal immigrants. Each passenger will have an image of one of his or her eye's iris stored on computer. Instead of showing their passport on arrival they will go into a kiosk where in seconds a camera will check that the pattern of their iris matches computer records. It is hoped the technology could have future security benefits, with UK airports still on alert following 11 September. The entire procedure only takes a few seconds and there is no contact with the body or with lasers or other potentially harmful light sources. Passengers taking part are being asked to carry their passports during the trial period should immigration officials want to check their details.

Benefits:

- ü Increased security when controlling access to confidential data and IT systems
- ü Reduced risk of fraudulent use of identity by employees
- ü Enhanced user convenience
- ü Increased costs savings due to reduced password maintenance costs
- ü User convenience due to no passwords to remember or reset and faster login
- ü Privacy – ability to transact anonymously

Demerits:

- ✖ An automatic personal identification system based solely on fingerprints or faces is often not able to meet the system performance requirements.
- ✖ In case of face recognition, face will sometimes change with time or injury, and that poses a problem
- ✖ Face recognition is fast but not reliable.
- ✖ Fingerprint verification is reliable but inefficient in database retrieval.
- ✖ Some voice recognition systems has some problems since the voice changes with a human's mood and illness and background noise poses some problems.

Biometrics In Future:

In future with Biometrics, one can go to shopping without money purse or credit card. It just needs to place his/her finger on the reader device and can debit money from their bank accounts. In credit cards system if a mother and daughter have a joint account, then they cannot know how much each one uses. But with biometrics mother will know her daughter secretly buying beer bottles. The biometrics market is expected to grow to $1.8 billion by 2004.

Conclusion:

Biometrics makes automated use of physiological or behavioral characteristics to determine or verify identity. Finger biometrics are most popular and one of the most accurate and cost effective solutions. Hand geometry, signature-scan, keystroke-scan, palm-scan are some more biometric technologies in use. With Biometrics there is no problem of ID being stolen. Many institutions and organizations are trying to use this technology.