Volume 2, No. 10, October 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

BIOMETRIC: CASE STUDY

Sushma Jaiswal
Lecturer,S.O.S. in Computer Science,
Pt.Ravishankar Shukla University,Raipur(C.G.)
jaiswal1302@gmail.com

Dr. Sarita Singh Bhadauria
Professor & Head,Department of Electornics Engineering
,Madhav Institute of Technology & Science,Gwalior(M.P.)

Dr.Rakesh Singh Jadon
Professor & Head,Department of Computer Applications
,Madhav Institute of Technology & Science,Gwalior(M.P.)

Abstract:BIOMETRICS is the measurement of biological data. The term biometrics is commonly used today to refer to the authentication of a person by analyzing physical characteristics, such as fingerprints, or behavioral characteristics, such as signatures. Since many physical and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. The word biometrics comes from two Greek words and means life measure. To provide a comprehensive survey, we not only categorize existing boimetric techniques but also present detailed of representative methods within each category.

Any characteristic can be used as a biometric identifier if (1) every person possesses the characteristic, (2) it varies from person to person, (3) its properties do not change considerably over time, and (4) it can be measured manually or automatically. Physical characteristics commonly used in biometric authentication include face, fingerprints, handprints, eyes, and voice. Biometric authentication can be used to control the security of computer networks, electronic commerce and banking transactions, and restricted areas in office buildings and factories. It can help prevent fraud by verifying identities of voters and holders of driver's license or visas. In authentication, a sensor captures a digital image of the characteristic being used to verify the user's identity. A computer program extracts a pattern of distinguishing features from the digital image. Another program compares this pattern with the one representing the user that was recorded earlier and stored in the system database. If the patterns match well enough, the biometric system will conclude that the person is who he or she claims to be.

BIOMETRIC AND AUTHENTICATION

- A biometric is any *measurable*, *robust*, *distinctive*, *physical characteristic* or *personal trait* of an individual that can be used to *identify, or verify* the claimed identity of, that individual.

Measurable means that the characteristic or trait can be easily presented to a sensor and converted into a quantifiable, digital format. This allows for the automated matching process to occur in a matter of seconds.

The *robustness* of a biometric is a measure of the extent to which the physical characteristic or personal trait is subject to significant changes over time. Such changes may occur because of the effects of an individual's exposure to chemicals, aging, or injury. A highly robust biometric is not subject to large changes over time, while a low degree of robustness indicates a biometric that could change considerably over time. For example, iris patterns, which change very little over a lifetime, are more robust than voices.

Distinctiveness is a measure of the variations or differences in the biometric pattern among the general population. The highest degree of distinctiveness implies a unique identifier, while a low degree of distinctiveness indicates a biometric pattern found frequently among the general population. The

purpose of the biometric application determines the degree of robustness and distinctiveness required.

Identification differs significantly from *verification*. Identification is when the device asks and attempts to answer the question, "Who is X?" When biometrics are used to identify an individual, the biometric device reads a sample and compares that sample against every template in the database. This is called a "one-to-many" search (1:N). The device will either find a match and subsequently identify the person or not find a match and fail to identify the person.

Verification is when the device asks and attempts to answer the question, "Is this X?" after the user claims to be X. When biometrics are used to verify the claimed identity of an individual, the biometric device first requires input from the user. For example, the user claims his identity by using a password, token, or user name (or any combination of the three). The device also requires a biometric sample. It then compares the sample against the user-defined template (pointed to by the password, token, and/or user name) in the database. This is called a "one-to-one" search (1:1). The device will either find or not find a match between the two

In general, there are three different approaches to recognizing an individual for security purposes, known as authentication. Presented in order of least secure and convenient to most secure and convenient, the first approach uses something you have, such as a token, card, or key. The second approach uses something you know,

such as a password or PIN. The third uses something you are, a biometric.

Any combination of these three further heightens security, while requiring all three provides the highest level of security.

- Biometric authentication refers to *automated methods of identifying or verifying* the identity of a *living person in real time* based on a *physical characteristic or personal trait*. The phrase, "living person in real time" is used to distinguish biometric authentication from forensics, which does not involve real-time identification of a living individual.

Biometric authentication technologies are used in two ways:

- To prove who you are or who you claim you are.
- To prove who you are not (for example, to resolve a case of mistaken

identity).

Identification vs Verification

There are two categories of Biometric Systems. They are identification and verification. Identification is known as the process that compares a present person to a biometric pattern or database. Verification is a process that validates a person's ID by comparing his/her biometric data with already captured biometric data that is stored in a system. Identification is more complex than the verification process. Identification may generate a one to many matches, where verification generates a one to one match.

An example is a person using biometrics at an airport. During the verification process the passenger would provide a smart card, (already programmed with his/her biometric data). When it is time for the passenger to be scanned, authorization would be verified against both the person and the smart card. This process is extremely straightforward and more easy to use. The identification process is more complicated. Let's take this same passenger, but this time he/she does not have a smart

card. Upon being scanned by the biometric system, the identification process can generate a large number of results based on similar aspects. The results of the database can then be filtered down based on sex, ethnic origin, and other facts. Biometric is a science and technology of authentication. In fact biometric technology is not new technology. Biometric technology is already used since ancient Egyptian times.

Biotechnology is used to identify the persons recording size of recognizable body parts; it is normally used to ensure that the person is the truly him / her. Basically Biometric system was used in security purpose and also used in networking system logically; no one has access without being trusted. Access control technology tries to automate the process of answering two basic questions before offering various types of access.

Where the first question is who are you? And the second question is "Are you really as you say?" The first question

represents the function of identification and the second question represents the function of verification.

Where is the biometric technology first process?

This common approach is to gain access through the use of signs and assumptions that the owner of the sign and the proof identity will match. That kind model is called as single factor security. This technology is mostly used in house keyword system. This technology is also used for the identification purpose. This type of approach has a risk if the sign is lost or stolen. Once any one enters with the key of another person, they could easily enter the house. This also happens with password. It will not be a secret some one else can use it.

To over come this problem go for two factors security is find. This method is most cost and risks. The most common example of automated teller machine (ATM). With a card that shows who you are and PIN which is the mark you as the rightful owner of the card, you can access your bank account. The weakness of this security is that both signs should be at the requester of access. Thus, the card only or PIN only will not work Problems arise when you are forgetful person. Also, you often do not realize that the PIN is very personal thing. Basically, family or close friends may not know. The more sophisticated crime is to steal the PIN data from the source directly.

In this situation, biometric fingerprint scanner can be a solution. , it is pretty exotic technology in the real world. It was basically used in police stations, high security buildings and even on PC keyboards purpose. Using biometric technology you can identify the persons and cards and system.

There is no better way of identifying an individual than using his or her own unique characteristics. Today, with the ever increasing awareness of privacy and data protection, biometrics technology is the safest and the most convenient way in identification which improves individual identification all across the board. Biometrics has now commercial consciousness as laptops, mobiles phones, computers, and other home appliances can now be engaged using this amazing technology.

There are two categories of biometrics technology being used today. One is physiological biometrics which measures characteristics that can be empirically identified such as the face, fingerprint, hand, and iris. Another category is labeled as behavioral which includes signature, voice, and keystroke. As with any type of technology, each of this items under these two categories has its own advantages and disadvantages. Let us get an overview of how each of them works.

Biometric definition is best explained by understanding its nomenclature.

The word "biometrics" is derived from the Greek words 'bios' and ‘metric’; which means life and measurement respectively. This directly translates into "life measurement".

General science has included biometrics as a field of statistical development since the early twentieth century. A very good example is the statistical analysis of data from agricultural field experiments comparing the yields of different varieties of wheat. In this way, science is taking a life measurement of the agriculture to ultimately determine more efficient methods of growth.

Biometrics technologies measure a particular set of a person's vital statistics in order to determine identity.

In the most contemporary computer science applications, the term "life measurement" adapts a slightly different role. Biometrics in the high technology sector refers to a particular class of identification technologies. These technologies use an individual's unique biological traits to determine one's identity. The traits that are considered include fingerprints, retina and iris patterns,facial characteristics and many more.

Types of Biometrics

There are basically two types of biometrics:
1. Behavioral biometrics
2. Physical biometrics

Behavioral biometric definition : Behavioral biometrics basically measures the characteristics which are acquired naturally over a time. It is generally used for verification.

Physical biometric definition : Physical biometrics measures the inherent physical characteristics on an individual. It can be used for either identification or verification.

How does Biometrics work?

No matter what type of biometric scheme is used, all have to go through the same process. The steps of the process are capture, process, and comparison.
• Capture – A biometric scheme is used to capture a behavioral or physiological feature.
• Process – The captured feature is then processed to extract the unique element(s) that corresponds to that certain person
• Comparison – The individual is then enrolled into a system as an authorized user. During this step of the process, the image captured is checked against existing unique elements. This verifies that the
element is a newly authorized user. Once everything is done, the element can be used for future
comparisons.

How do I select the right biometric system?

Certain questions need to be asked and answered when choosing a biometric system. Below are some of these questions:

1. What level of security is needed?
2. Will the system be attended or unattended?
3. Do you want the system to be resistant to spoofing?
4. What reliability level is wanted?
5. Should this system work 24 hours a day?
6. Does the system require backups?
7. What is the acceptable time for enrollment?
8. Is privacy an issue for your system?
9. What about the storage of the signature?

What is Biometrics?

Biometrics are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioral characteristics.
Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). During **Enrollment**, as shown in the picture below, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison.
Biometric recognition can be used in **Identification** mode, where the biometric system identifies a person from the entire *enrolled* population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching. A system can also be used in **Verification** mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user.

A biometric is any measurable, physical or physiological feature or behavioral trait that can be used to identify an individual or to verify the claimed identity of an individual.3,4 Examples of physiological biometrics include fingerprints, hand geometry, the face, the iris, the retina, the venous networks of the hand and even body odour.

Behavioural biometrics include voice,5 signature, keystroke dynamics (manner of typing on a keyboard) and gait (manner of walking).6 While the range of body features that can be used for biometric recognition has greatly expanded since this technology was first established, not all physiological or behavioural characteristics are suitable for biometric recognition. In order to be considered suitable for use in biometric recognition, a physiological or behavioural characteristic is usually evaluated against a number of criteria: (i) universality, (ii) distinctiveness, (iii) permanence, (iv) collectability, (v) performance, (vi) acceptability and (vii) resistance to circumvention (see Table 1).7,8,9,10 These are sometimes referred to as the "seven pillars of biometrics". While no biometric modality fulfils all seven of the pillars equally well, certain modalities satisfy more of the criteria than others (*e.g.* fingerprint and iris would score better overall than dynamic signature and keystroke dynamics) and would, therefore, be deemed more reliable or "stronger" in terms of their suitability for recognition purposes. In addition, for large-scale applications (*e.g.* in airports) high-speed matching is required and this can favour the selection of one particular biometric modality over another.

Why we Use Biometrics?

Using biometrics for identifying human beings offers some unique advantages. Biometrics can be used to identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember a multitude of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites and so forth. Biometrics hold the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications. There is no one "perfect" biometric that fits all needs. All biometric systems have their own advantages and disadvantages. There are, however, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, for nearly a century, law enforcement has used fingerprints to identify people. There is a great deal of scientific data supporting the idea that "no two fingerprints are alike." Technologies such as hand geometry have been used for many years and technologies such as face or iris recognition have come into widespread use. Some newer biometric methods may be just as accurate, but may require more research to establish their uniqueness.

Another key aspect is how "user-friendly" a system is. The process should be quick and easy, such as

having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner. Low cost is important, but most implementers understand that it is not only the initial cost of the sensor or the matching software that is involved. Often, the life-cycle support cost of providing system administration and an enrollment operator can overtake the initial cost of the biometric hardware. The advantage biometric authentication provides is the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users.

Why is Biometrics terms used?

Traditionally, the identification of an individual or the verification of an individual's claimed identity involved the use of a password, personal identification number (PIN) or cryptographic key ("something you know") or the possession of an identity (ID) card, smart card or token ("something you have"). however, there are a number of problems associated with these security measures. For example, passwords and PINs can be forgotten, shared with others, and lost or stolen, which could compromise the integrity of the system. A biometric trait is part of an individual and as such it offers the third element of proof of identity, *i.e.* "something you are". Consequently, biometric traits are thought to have a number of advantages over the aforementioned security measures: they cannot be lost or forgotten, they are difficult to copy, forge or share and they

require the individual to be present at the time of identification. The use of biometrics also makes it difficult for an individual to repudiate having accessed a physical location or a computer system, or having conducted a particular transaction. In fact, biometric traits are often portrayed as the ultimate form of identification or verification, and are being promoted in many quarters as a means of heightened security, efficiency and convenience and have been proposed as the solution to issues of identity theft and benefit fraud. It is envisaged that biometric systems will be faster and more convenient to use, cheaper to implement and manage and more secure than traditional identification and verification methods. Nonetheless, biometrics also have their limitations, for example, passwords, PINs and ID cards can all be re-issued relatively easily if they become compromised, which is not the case for an individual's fingerprint or iris image. The practical and technological aspects and limitations of biometric recognition systems are discussed in more detail below.

Design of Biometric recognition systems

Although humans have been using certain features (*e.g.* face, voice and gait) to recognize each other for thousands of years, the automated and semi-automated approach used in biometric recognition systems is a relatively recent development from the last few decades.28 While the mechanisms involved and the modalities (characteristics) used may vary, there are four basic stages in biometric systems: (i) enrolment, (ii) storage, (iii) acquisition and (iv) matching. With any biometric system, the individuals required to use the system need to be enrolled. Biometric data, for example a fingerprint, is collected using a sensor to produce a digital representation of the data. The system then extracts salient discriminatory features (*i.e.* feature extraction) from the digital representation and these features are used to generate a template (*i.e.* a feature data set), which is then linked to the user's identity and stored in the system. In basic terms the template takes the form of numeric data. The next time the individual presents his/her fingerprint to the sensor the sample template that is acquired is compared to the enrolled (stored) template using a mathematical algorithm. If they match the individual is accepted.

Why We opt for Biometrics?

There are many benefits of using biometrics including better security. These systems offer low cost and convenient security tier. By using the biometrics, companies can also reduce the frauds related to buddy punching and ID. Biometric systems also take care of the problems related to forgotten passwords, lost IDs by employing physiological attributes. Companies can easily cut down password administration expenses and can replace difficult passwords too. Biometrics technology also provides increased ROI and cost savings in various areas including time and attendance and loss prevention.

We **Choosing the Biometrics Technology**

There is a range biometrics system available in the market. It is important to pick one that suits user profile, interface requirements, application based parameters and environmental conditions. By keeping the following things in mind, one can pick the best biometric technology for use. Choose easy to use technologies unless you are trained for a specific type. It is also important to check the error incidence too. Environmental conditions and time affects accuracy of the biometric information. Vendors generally use two ways for measuring biometric accuracy. False rejection Rate and False acceptance rate are used for rating the accuracy of biometrics. So while buying the biometrics system, think about your requirements and then take an informed decision. Do not forget to analyze user acceptance and cost associated with the technology.

Why the Fingerprints are so *Good* for use in Biometrics?

There are many criteria that must be accounted before a physical or behavioral trait can be considered suitable for use in biometrics. Perhaps the most important criteria are *"Uniqueness"* and *"Permanence"*. Fingerprints have been well proven on both counts.

• **Uniqueness:**

Uniqueness of fingerprint is not an established fact but an empirical observation. Fingerprints have been routinely compared worldwide for more than 140 years. In that time, no two fingerprints on any two persons have been found to be identical. Even identical twins who shared same DNA structure have different finger prints; they tend to have fingerprints that are similar globally, i.e. have the same fingerprint classes (e.g.. whorl, loop, arch, etc) but ridge structures are very different. The true is also holds for the right and left finger and can be anticipated for clones.

• **Permanence:**

Fingerprints are fully formed at about seven months of fetus development and finger ridge configuration do not change throughout the life of an individual except due to accidents such as bruises and deep physical injuries. They simply expand proportionately in all directions as we grow, means fingerprints maintains a proportional scale for its entire existence. The other advantages of fingerprints as a biometric are stated bellow:

• **High Universality:**

Within human population every individual has fingerprint which can be easily used for their authentication.

• **High Indispensability:**

Like token-based authentications fingerprints for human identification does not lead problems of being stolen or lost. On the other hand fingerprints would never be forgotten like PINs, password, or other knowledge-based systems. Actually in most cases, fingerprints would accompany the individual throughout his/her life time unless there is some serious injury to their fingers.

• **High Collectability:**

Fingerprints can be easily collected compared to other biometric samples, such as Retina, DNA, Irish, etc. which require complete cooperation and high cost special equipment to acquire the biometric samples. On the other hand the process of fingerprint acquiring requires minimal or no user training and can be collected easily from both cooperative and non cooperative users.

• **Good Storability:**

The database of fingerprints does not require huge space; it depends on the representation of the templates that can be chosen for the system. Depending on the application and way of representation the size of these templates can be from 52 bytes to several megabytes.

• **High Performance:**

Fingerprints remain one of the most accurate biometric modalities considering both False Accept Rate (FAR) and False Reject Rate (FRR).

• **Wide Acceptability:**

Since the beginning of the twentieth century, fingerprints have been formally accepted as valid personal identification trait and have become a standard routine in forensics.

INTRODUCTION

"Biometrics" are automated methods of recognizing an individual based on their physical or behavioral characteristics. Some common commercial examples are fingerprint, face, iris, hand geometry, voice and dynamic signature. These, as well as many others, are in various stages of development and/or deployment. The type of biometric that is "best " will vary significantly from one application to another. These methods of identification are preferred over traditional methods involving passwords and PIN numbers for various reasons: (i) the person to be identified is required to be physically present at the point-of-identification; (ii) identification based on biometric techniques obviates the need to remember a password or carry a token. Biometric recognition can be used in identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match.

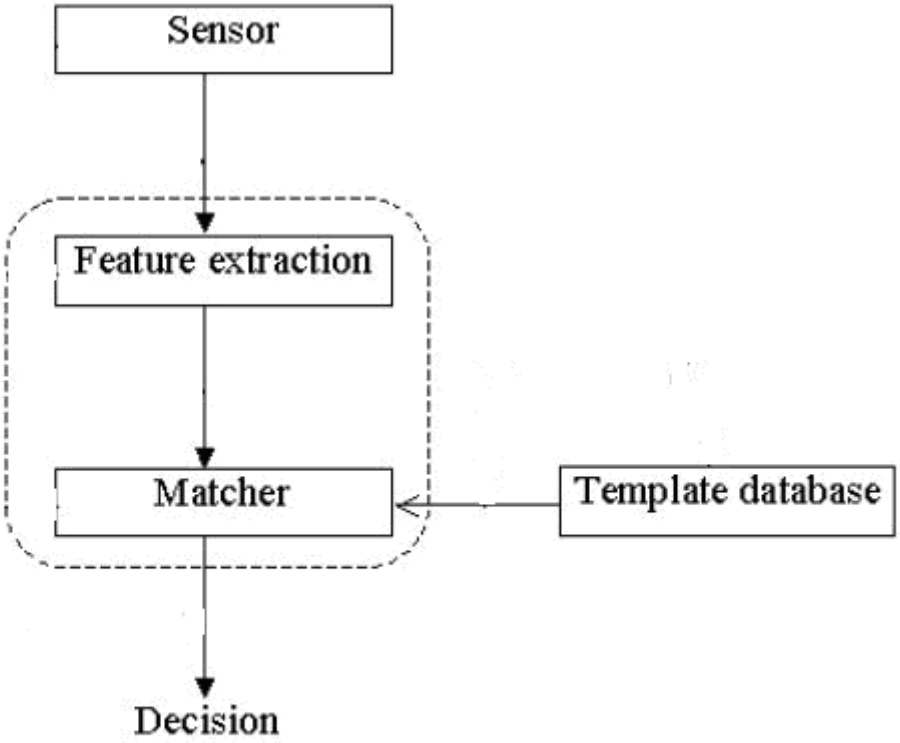
A BIOMETRIC SYSTEM

All biometric systems consist of three basic elements:

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

Enrollment

Enrollment is the crucial first stage for biometric authentication because enrollment generates a template that will be used for all subsequent matching. Typically, the device takes three samples of the same biometric and averages them to produce an enrollment template. Enrollment is complicated by the dependence of the performance of many biometric systems on the users' familiarity with the biometric device because enrollment is usually the first time the user is exposed to the device. Environmental conditions also affect enrollment. Enrollment should take place under conditions similar to those expected during the routine matching process. For example, if voice verification is used in an environment where there is background noise, the system's ability to match voices to enrolled templates depends on capturing these templates in the same environment. In addition to user and environmental issues, biometrics themselves change over time. Many biometric systems account for these changes by continuously averaging. Templates are averaged and updated each time the user attempts authentication.



Templates

As the data representing the enrollee's biometric, the biometric device creates templates. The device uses a proprietary algorithm to extract "features" appropriate to that biometric from the enrollee's samples. Templates are only a record of distinguishing features, sometimes called minutiae points, of a person's biometric characteristic or trait. For example, templates are not an image or record of the actual fingerprint or voice. In basic terms, templates are numerical representations of key points taken from a person's body. The template is usually small in terms of computer memory use, and this allows for quick processing, which is a hallmark of biometric authentication. The template must be stored somewhere so that subsequent templates, created when a user tries to access the system using a sensor, can be compared. Some biometric experts claim it is impossible to reverse-engineer, or recreate, a person's print or image from the biometric template.

Matching

Matching is the comparison of two templates, the template produced at the time of enrollment (or at previous sessions, if there is continuous updating) with the one produced "on the spot" as a user tries to gain access by providing a biometric via a sensor. There are three ways a match can fail:

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

Failure to enroll (or acquire) is the failure of the technology to extract distinguishing features appropriate to that technology. For example, a small percentage of the population fails to enroll in fingerprint-based biometric authentication systems. Two reasons account for this failure: the individual's fingerprints are not distinctive enough to be picked up by the system, or the distinguishing characteristics of the individual's fingerprints have been altered because of the individual's age or occupation, e.g., an elderly bricklayer.

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

BIOMETRIC TECHNOLOGIES

The function of a biometric technologies authentication system is to facilitate controlled access to applications, networks, personal computers (PCs), and physical facilities. A biometric authentication system is essentially a method of establishing a person's identity by comparing the binary code of a uniquely specific biological or physical characteristic to the binary code of an electronically stored characteristic called a biometric. The defining factor for implementing a biometric authentication system is that it cannot fall prey to hackers; it can't be shared, lost, or guessed. Simply put, a biometric authentication system is an efficient way to replace the traditional password based authentication system. While there are many possible biometrics, at least eight mainstream biometric authentication technologies have been deployed or pilot-tested in applications in the public and private sectors and are grouped into two as given,

- fingerprint,
- hand/finger geometry,
- Palm Print Recognition
- dynamic signature verification, and
- keystroke dynamics.
- facial recognition,
- voice recognition
- iris scan,
- retinal scan.
- others

For the purpose of this study, a biometric technology that requires an individual to make direct contact with an electronic device (scanner) will be referred to as a contact biometric. Given that the very nature of a contact biometric is that a person desiring access is required to make direct contact with an electronic device in order to attain logical or physical access. Because of the inherent need of a person to make direct contact, many people have come to consider a contact biometric to be a technology that encroaches on personal space and to be intrusive to personal privacy.

A contactless biometric can either come in the form of a passive (biometric device continuously monitors for the correct activation frequency) or active (user initiates activation at will) biometric. In either event, authentication of the user biometric should not take place until the user voluntarily agrees to present the biometric for sampling. A contactless biometric can be used to verify a persons identity and offers at least two dimension that contact biometric technologies cannot match. A contactless biometric is one that does not require undesirable contact in order to extract the required data sample of the biological characteristic and in that respect a contactless biometric is most adaptable to people of variable ability levels.

Fingerprint

Human beings have used fingerprints for personal identification for centuries, and they have used them for criminal investigations for more than 100 years. The validity of fingerprints as a basis for personal identification is thus well established.

A fingerprint is the pattern of ridges and furrows on the surface of a fingertip. No two persons have exactly the same arrangement of patterns, and the patterns of any one individual remain unchanged throughout life. Fingerprints are so distinct that even the prints of identical twins are different. The prints on each finger of the same person are also different.

The level of detail in fingerprint images scanned into a biometric system depends on several factors. They include the amount of pressure applied to the fingertip during image scanning, the presence of any cuts or other deformities on the fingertip, and the dryness of the skin. Therefore, any unusual or prominent features on a fingertip, the endings of the fingerprint ridges, and ridge bifurcations, or branches—collectively known as minutiae—are all used in a biometric system based on fingerprint identification.

The development of solid-state sensors for fingerprint scanning may soon make the cost of incorporating a fingerprint-based biometric device affordable in many applications, such as laptop computers and cellular telephones. Consequently, researchers expect fingerprint identification to be the leading biometric technique in the near future. One problem with fingerprint technology is its acceptability in society, because fingerprints have traditionally been associated with criminal investigations and police work. Another problem is that the fingerprints of a small fraction of the population may be unsuitable for automatic identification because the prints may be deformed as a result of aging, some genetic condition, or environmental reasons.

The fingerprint biometric is an automated digital version of the old ink-and-paper method used for more than a century for identification, primarily by law enforcement agencies. The biometric device involves users placing their finger on a platen for the print to be read. The minutiae are then extracted by the vendor's algorithm, which also makes a fingerprint pattern analysis. Fingerprint template sizes are typically 50 to 1,000 bytes. Fingerprint biometrics currently have three main application arenas: large-scale Automated Finger Imaging Systems (AFIS) generally used for law enforcement purposes, fraud prevention in entitlement programs, and physical and computer access.

Advantages

- Matured technology based on years of research & understanding
- Do not change naturally
- Has wide acceptance in the security community
- The equipment is relatively low-priced compared to other biometric system

Disadvantages

- Can be altered / worn out over time
- Vulnerable to noise and distortion brought on by dirt and twists.
- Some people may feel offended about placing their fingers on the same place where many other people have continuously touched.

- Some people have damaged or eliminated fingerprints

Hand/Finger Geometry

A variety of measurements of the human hand can be used as biometric characteristics. These include hand shape, the lengths and widths of the fingers, and the overall size of the hand. Biometric devices based on hand geometry have been installed at many locations around the world. Hand-reader systems are used at some prisons in the United States and the United Kingdom to track the movement of inmates. The United States Immigration and Naturalization Service uses hand-reader systems at several major U.S. airports for the rapid admittance of frequent foreign travelers into the United States. The hand-geometry technique is simple, relatively easy to use, and inexpensive. The main disadvantage of this technique is that it does not distinguish well between the hands of different people. In other words, the system can easily determine if a particular hand shape belongs to a specified individual but cannot reliably determine if a particular hand shape belongs to one of several individuals. Hand geometry information may vary over the lifespan of an individual, especially during childhood, when rapid growth can drastically change hand geometry. In addition, the presence of jewelry or limited dexterity as a result of arthritis may make it difficult for a system to extract correct hand geometry information. Biometric systems based on hand geometry are large in size, so they cannot be used in applications with limited space, such as laptop computers.

Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers. Neither of these methods takes actual prints of the palm or fingers. Only the spatial geometry is examined as the user puts his hand on the sensor's surface and uses guiding poles between the fingers to properly place the hand and initiate the reading. Hand geometry templates are typically 9 bytes, and finger geometry templates are 20 to 25 bytes. Finger geometry usually measures two or three fingers. Hand geometry is a well-developed technology that has been thoroughly field-tested and is easily accepted by users.

Advantages	Disadvantages
Easy to use	Injury or trauma degradation can make the print hard to read.
Easy to integrate	The hand itself is not unique. It is the parameters that make it unique.
Does not significantly change after ageing	Does not work well for people with arthritis
Used to improve security, accuracy, and convenience for access control, time, and attendance.	Accuracy is low
Can work with dirty hands	Fairly expensive

Palm print recognition

The palms of the hand have patterns of ridges and valleys, similar to those found in fingerprints, which can be used for biometric recognition. These systems use a number of different sensor types, *i.e.* optical, capacitance, ultrasound and thermal. Depending on the resolution of the sensor, the captured images can contain all the features of the palm including the ridge and valley features, the principal lines and wrinkles, as well as hand geometry measurements. Similarly to fingerprint recognition the systems extract minutiae and/or pattern details, which are used to create a template. The template can be representative of the entire palm surface or it can be confined to specific smaller regions of the palm surface, depending on the performance requirements. The matching process can involve minutiaebased matching, correlation-based matching or

ridge-based matchingThe use of palm print recognition technology is increasing in commercial and law enforcement applications.

Similarly to fingerprints, palm prints are not universal and they are susceptible to the same problems of wear and tear. however, because a palm represents a larger area than a fingerprint, these features are considered to be even more distinctive than fingerprints. In addition, the minutiae characteristics of palms are more distinctive than the ridge characteristics. The collection of palm prints can be assisted through user feedback, for example, regarding the positioning of the hand. Palm print recognition is considered to be highly accurate, though the quality of the images can affect the error rates. Minutiae-based matching is more accurate than correlation-based matching, but it can take longer. however, system speed can be assisted by partitioning the database into different sections. It has been suggested that palm print recognition accuracy will improve with further technological advances, though independent testing will be needed to corroborate these results.

From a practical perspective, palm print sensors are larger and, consequently, more expensive than fingerprint sensors.Decisions to implement palm print recognition systems must balance the need for accuracy against the cost and the interoperability issues associated with this technology

Vein pattern recognition

In vein pattern recognition systems a high resolution camera and infrared light are used to capture the pattern and structure of blood vessels visible on the back of an individual's hand or finger . The algorithm registers the vascular pattern characteristics (*e.g.* blood vessel branching points, vessel thickness and branching angles) and stores these as a template for comparison with subsequent samples from the enrolled individual. This technology has the potential to be linked with existing recognition systems such as fingerprint and palm recognition sensors. vein pattern recognition systems are increasingly being used in order to access ATM cash dispensers and banking services, and for physical access to hospitals and universities as well as for residential access, particularly in Japan.These recognition systems are also being used for high security network access and in point of sale terminals.

The random pattern of blood vessels under the skin is relatively distinct and stable, thus enabling its use for some forms of biometric recognition.Sensors are non-contact and relatively easy to use, though additional guidance brackets may be used to facilitate correct hand positioning. Images cannot be collected at a distance and since the systems are noncontact no latent images are left behind after sensing, which encourages acceptance. System performance is quite accurate and because it is difficult to counterfeit blood vasculature, vein recognition is seen as a secure biometric modality.

Advantages	ar Disadvantages
Veins do not change during a person's life	Fairly new- so the effect by a person's heart attack or medical problems is not clear
Highly secure due to being hard to copy or even read.	

Dynamic Signature Verification

Each person has a unique style of handwriting and, therefore, a unique signature. One problem with signature recognition is that the signature of a particular individual may vary somewhat. Despite the variations, researchers have designed a few successful systems for signature-based authentication. Biometric devices based on signature verification are reasonably accurate, but not accurate enough to recognize specific individuals in a large population. However, signature verification is reliable enough to be used in place of a PIN in accessing automated teller machines (ATMs).

There are two approaches to identification based on signature verification: static and dynamic. Static signature verification uses only the geometric (shape) features of a signature, such as the degree of slant, breadth and height of letters, and space between lines, letters, and words. Dynamic signature verification uses both geometric features and dynamic features, such as the speed a person writes and the pressure of the writing implement. Dynamic verification requires a special pen. It is resistant to forgery, as it is virtually impossible for a forger to replicate both the shape of a signature and the speed and pressure with which another person signs his or her name. An inherent advantage of a signature-verification system is that the signature is already an acceptable form of personal identification. It can therefore be incorporated easily into existing business processes, such as credit card transactions.

Dynamic signature verification is an automated method of examining an individual's signature. This technology examines such dynamics as speed, direction, and pressure of writing; the time that the stylus is in and out of contact with the "paper"; the total time taken to make the signature; and where the stylus is raised from and lowered onto the "paper." Dynamic signature verification templates are typically 50 to 300 bytes.

Advantages

- Reasonably accurate
- Easy to user

Disadvantages

- Systems can be fooled by imitation signatures

Keystroke Dynamics

Keystroke dynamics is an automated method of examining an individual's keystrokes on a keyboard. This technology examines such dynamics as speed and pressure, the total time of typing a particular password, and the time a user takes between hitting certain keys. This technology's algorithms are still being developed to improve robustness and distinctiveness. One potentially useful application that may emerge is computer access, where this biometric could be used to verify the computer user's identity continuously.

Advantages

- User friendly
- Fairly unique between per methods
- More suitable for verification
- Low cost

Disadvantages

- A person may hack in and get the users password.
- Less suitable for identification

Facial Recognition

The most familiar biometric technique is facial recognition. Human beings use facial recognition all the time to identify other people. As a result, in the field of biometrics, facial recognition is one of the most active areas of research. Applications of this research range from the design of systems that identify people from still-photograph images of their faces to the design of systems that recognize active and changing facial images against a cluttered background. More advanced systems can recognize a particular individual in a videotape or a movie.

Researchers base the patterns used for facial recognition on both specific and general features. The specific features include the location and shape of facial attributes such as the eyes, eyebrows, nose, lips, and chin. More generally, they employ an overall analysis of the facial image and a breakdown of the image into a number of component images. Researchers are unsure whether the face itself, without any additional information, is sufficient for the accurate recognition of one person in a large group of people. Some facial recognition systems impose restrictions on how the facial images are obtained, sometimes requiring a simple background or special lighting.

Facial recognition records the spatial geometry of distinguishing features of the face. Different vendors use different methods of facial recognition, however, all focus on measures of key features. Facial recognition templates are typically 83 to 1,000 bytes. Facial recognition technologies can encounter performance problems stemming from such factors as no cooperative behavior of the user, lighting, and other environmental variables. Facial recognition has been used in projects to identify card counters in casinos, shoplifters in stores, criminals in targeted urban areas, and terrorists overseas.

S.Jaiswal et.al.[2010] given a comprehensive literature on Image Based human and machine recognition of faces during 1987 to 2010. Machine recognition of faces has several applications. As one of the most successful applications of image analysis and understanding, face recognition has recently received significant attention, especially during the past several years. In addition, relevant topics such as Brief studies, system evaluation, and issues of illumination and pose variation are covered. In this paper numerous method which related to image based 3D face recognition are discussed. S.Jaiswal et.al.[2008] described an efficient method and algorithm to make individual faces for animation from possible inputs. Proposed algorithm reconstruct 3D facial model for animation from two projected pictures taken from front and side views or from range data obtained from any available resources. It is based on extracting features on a face in automatic way and modifying a generic model with detected feature points with conic section and pixalization. Then the fine modifications follow if range data is available. The reconstructed 3Dface can be animated immediately with given parameters. Several faces by one methodology applied to different input data
to get a final Animatable face are illustrated.

S.Jaiswal et.al.[2007] the proposed study, 2D photographs image divided into two parts; one part is front view (x, y) and side view (y, z). Necessary condition of this method is that position or coordinate of both images should be equal. We combine both images according to the coordinate then we will get 3D Models (x, y, z) but this 3D

model is not accurate in size or shape. In defining other words, we will get 3D animatable face, refinement of 3D animatable face through pixellization and smoothing process. Smoothing is performed to get the more realistic 3D face model for the person.

2D Facial Recognition

Advantages

- Needs lesser storage space for identification templates (as compared to 3D)
- Faster in identification process, requires lesser memory

Disadvantages

- 2D images contain limited information
- Sensitive to illumination, orientation, facial expressions and make ups
- Will not work when using a mask of other face-covering veils

3D Facial Recognition

Advantages

- With the ability to capture and store more information, 3D provides more accurate representation of the face
- Much better handling of illumination and orientation-related readings

Disadvantages

- Higher computational cost due to need for processing large amount of data
- Will not work when using a mask of other face-covering veils

Facial thermography

Facial thermography measures the amount of thermal radiation (heat) emitted from an individual's face. It has been suggested that the pattern of heat radiated by the human face (or body) is suitable for recognition purposes. An infrared camera is used to capture the heat images and analyse them for anatomical information, which is considered to be invariant to temperature changes, for example, the patterns of superficial blood vessels. The most likely applications of facial thermography are similar to those employing 2D- and 3D-based facial recognition. For example, this technology could be employed to secure computer and network access, at ATM cash dispensers and point of sale terminals and in e-passports. however, it has also been suggested that facial thermography recognition could potentially be used in the medical field for triage, diagnosis and monitoring treatments.

All individuals produce facial thermograms and the complexity of blood vasculature underlying these thermograms is thought to be distinctive enough to permit recognition. however, facial thermograms can be affected by a number of different factors including the ambient temperature, the ingestion of certain substances (*e.g.* vasodilators and vasoconstrictors), extensive facial surgery, sinus problems, inflammation, arterial blockages, incipient stroke, soft tissue injuries and other physiological conditions. The collection of this biometric is unobtrusive, can be done at a distance and is possible under varying lighting conditions, including darkness. Despite this, difficulties can arise in capturing facial thermogram images in uncontrolled environments containing other heat sources. Other factors can also reduce system performance such as the presence of glasses

and even severe sunburn. Nonetheless, preliminary accuracy results seem promising and they are expected to improve. As the facial thermograms are generated from blood vessels below the surface of the skin, this technology is resistant to circumvention using disguises. Moreover, attempts to change the pattern of blood vessels to alter the resulting thermogram can also be detected. Liveness detection is another possible security measure, for example, a number of image frames could be taken and analysed for small thermal variations caused by the heart rate and respiration. user acceptance of facial thermography is high owing to the non-contact, non-invasive nature of image collection and the fast throughput speed. Some concerns have been raised regarding the potential to infer certain medical conditions from the vascular patterns. In addition, because the images can be collected covertly, privacy concerns relating to surveillance have been raised.

Voice Recognition

voice is often classified as a combination of a behavioural and a physiological biometric because certain features of an individual's voice are based on the shape and size of their vocal tracts, mouth, nasal cavities, lips, *etc*. From a biometrics perspective there are basically two different types of voice/speaker recognition system, *i.e*. text dependent and text independent systems. In a text dependent system the user speaks a particular, predetermined, pass phrase, for example, a sequence of numbers. When enrolling in such a system, the user may be required to repeat the pass phrase a number of times, to enable the algorithm to take account of any intra-class variation. Consequently, the enrolment process lasts longer, but this is thought to result in increased accuracy. In a text independent system the user's voice is recognised regardless of what he/she is saying. Such systems are said to offer greater security against abuse than text dependent systems, but they are more difficult to design.443 In general, sound waves from the individual's voice recording are calculated as feature vectors, which are then modelled as a voiceprint (template) for that individual. During the recognition process, the sequences of feature vectors from the sample and enrolled voiceprints are compared using pattern analysis, *i.e*. the system *does not* compare the voice itself. If these patterns are sufficiently similar, a match is given.

Like signature, speech is mostly a behavioral characteristic. However, speech has some biological aspects that make speech characteristics similar for all people. These similarities are due to the relatively similar shape and size of individuals' vocal tracts, mouths, nasal cavities, and lips, all of which help produce the sounds of speech. The speech of a specific individual is distinctive but may not contain sufficient information to be of value in large-scale recognition.

Voice recognition is based on either a text-dependent speech input or a text-independent speech input. A text-dependent system verifies the identity of an individual on the basis of the utterance of a fixed predetermined phrase, such as the person's name. A text-independent system verifies the identity of a speaker regardless of what he or she says. Text-independent voice recognition is more difficult than text-dependent verification but offers more protection against fraud. Speech-based features are sensitive to factors such as background noise and the emotional and physical state of the speaker. In addition, some people are extraordinarily skilled at mimicking other people's voices. This popular perception of the

vulnerability of voice recognition may be a reason why speech-based authentication is not widely used in high-security applications.

Voice or speaker recognition uses vocal characteristics to identify individuals using a pass-phrase. Voice recognition can be affected by such environmental factors as background noise. Additionally it is unclear whether the technologies actually recognize the voice or just the pronunciation of the pass-phrase (password) used. This technology has been the focus of considerable efforts on the part of the telecommunications industry and NSA, which continue to work on improving reliability. A telephone or microphone can serve as a sensor, which makes it a relatively cheap and easily deployable technology.

Advantages

- Non-invasive
- Distinctive in terms of vocal chords, vocal tract, sinuses, and mouth tissues
- Vocal tract is not affected by a cold.
- Can be used with telephones
- Low invasiveness

Disadvantages

- Easily corrupted with noise, so may not be suitable for use in public places
- Probability of High false rates (positive and negative) due to physical ailments (cold & cough, sinus problems, etc.)
- Local acoustics can throw off the biometric system
- Illness and age can be some of the factors that effect voice biometrics.
- High false non-matching rates

Ear Geometry Biometrics

This form of biometric recognition is based on analyses of the shape of the outer ear, the ear lobes and bone structure, and both 2D and 3D methodologies are used. A sensor (*e.g.* a camera) collects a side profile image of the user's head, from which the system automatically locates the ear and isolates it from the surrounding hair, regions of the face, and the user's clothes. The algorithm uses a combination of colour and depth analysis to first localise the ear pit, then generates an outline of the visible ear region. The algorithm has to account for differences in skin tone (caused by lighting variation), as well as differences in ear size, ear shape, hair occlusion, and the presence of earrings.

From a biometric perspective, ears present good universality and it has been suggested that the rich structure of the ear is unique enough to permit its use as a biometric. however, others have questioned the level of distinctiveness of ear geometry, particularly for recognition purposes. In the main, apart from injury, the structure of the ear is quite stable and undergoes only small, predictable changes over time, which can be accounted for in recognition systems. This is not the case, however, for very young individuals (*i.e*. 4 months to 8 years old) and the elderly (*i.e*. those over 70 years of age), for whom ear geometry exhibits more marked changes. Collectability is relatively straightforward, quick and non-invasive, which contributes to its high acceptability. In addition, while ear geometry can be collected passively, the overall performance is improved if the users are given feedback regarding their distance from the camera, their position and angle of exposure and their pose. Performance is also

affected by a number of other factors including the occlusion of the ear by hair, clothing or earrings, and differences in illumination, which can increase specularity and shadowing of the ear structures. The 3D methodologies appear to cope better with some of these issues and preliminary results suggest that performance is improving. Overall, ear geometry recognition systems exhibit moderate resistance to circumvention.

Iris Scan

The iris is the colored part of the eye. It lies at the front of the eye, surrounding the pupil. Each iris is unique, and even irises of identical twins are different. The complex structure of the iris carries distinctive information that is useful for identification of individuals. Early results of research on the accuracy and speed of iris-based identification have been extremely promising. These results indicate that it is feasible to develop a large-scale recognition system using iris information. Furthermore, the iris is more readily imaged than the retina.Iris scanning measures the iris pattern in the colored part of the eye, although the iris color has nothing to do with the biometric. Iris patterns are formed randomly. As a result, the iris patterns in your left and right eyes are different, and so are the iris patterns of identical-cal twins. Iris scan templates are typically around 256 bytes. Iris scanning can be used quickly for both identification and verification Applications because of its large number of degrees of freedom. Current pilot programs and applications include ATMs ("Eye-TMs"), grocery stores (for checking out), and the few International Airports (physical access).

Advantages

- Very high accuracy
- Does not change over time
- Does not require intimate contact with the reader
- Higher average for matching performance
- Convenient for people who wear glasses
- Chances of a false positive are very low
- Almost unaffected by environment sue to being protected by the cornea and the aqueous humor.
- Left and right iris patterns a certain person are different, including those of.identical twins.

Disadvantages

- Acquiring image requires proper alignment and positioning
- Result may get affected due to pupil size change
- Not easy to use
- Not easy to integrate with other systems
- The position of the eye can be problematic
- Require specialized devices, so can be expensive

Retinal Scan

The retina is the innermost layer of the eye. The pattern formed by veins beneath the surface of the retina is unique to each individual. This pattern is a reliable biometric characteristic.

Researchers acquire digital images of retinal patterns by projecting a low-intensity beam of visible or infrared light into a person’s eye and scanning an image of the retina. For a fixed portion of the retina to be used for identification, the person undergoing the scan must gaze into an eyepiece and focus on a

predetermined spot. The amount of user cooperation required for a retinal scan makes this technique unacceptable in many applications. On the other hand, a large number of biometric devices based on retinal scans have been installed in prisons and other highly secure environments. The primary disadvantage of this biometric technique is that retinal scanners are expensive.

Retinal scans measure the blood vessel patterns in the back of the eye. Retinal scan templates are typically 40 to 96 bytes. Because users perceive the technology to be somewhat intrusive, retinal scanning has not gained popularity with end-users. The device involves a light source shined into the eye of a user who must be standing very still within inches of the device. Because the retina can change with certain medical conditions, such as pregnancy, high blood pressure, and AIDS, this biometric might have the potential to reveal more information than just an individual's identity.

Advantages

- Accurate
- Impossible to forge a human retina
- Lower error rate of 1 in 10,000,000 compared to fingerprint identification (1 in 500)
- Low false acceptance rate and low false rejection rate

Disadvantages

- Not very convenient for people who wear glasses
- Uncomfortable for users
- Fairly new, so not many are using retina
- biometric devices

EMERGING BIOMETRIC TECHNOLOGIES

Many inventors, companies, and universities continue to search the frontier for the next biometric that shows potential of becoming the best. Emerging biometric is a biometric that is in the infancy stages of proven technological maturation. Once proven, an emerging biometric will evolve in to that of an established biometric. Such types of emerging technologies are the following:

- Brainwave Biometric
- DNA Identification
- Vascular Pattern Recognition
- Body Odor Recognition
- Fingernail Bed Recognition
- Gait Recognition
- Handgrip Recognition
- Ear Pattern Recognition
- Body Salinity Identification
- Infrared Fingertip Imaging & Pattern Recognition
- Odour

DNA (Deoxyribonucleic acid)

Each individual human is identifiable by genetic variation found in his/her DNA, which is contained in the nucleus of almost every cell as well as mitochondria. DNA serves as a unique genetic code, half of which comes from each parent. Identical twins are the exception to this rule since they have the same genetic code.486 DNA is a long double stranded molecule that is composed of four bases: (i) adenine, (ii) guanine, (iii) cytosine and (iv) thymine. In the case of humans, there are approximately three billion bases, 99 per cent of which are the same from person

to person. The variations, or order of the bases, in the remaining 1 per cent are the

means by which DNA becomes unique to each individual. This remaining 1 per cent can be used to identify or verify the identification of a given individual. As there are so many bases in a person's DNA, the task of analysing all of them would be impracticable, thus, scientists use a small number of sequences of DNA (short tandem repeats) that are know to vary greatly among individuals to ascertain identity. Despite the fact that DNA profiling is recognised as the most consistently effective method of establishing a permanent record of identity (statistical sampling shows a one in six billion chance of two people having the same profile), its role as a method of identity verification currently remains limited. This is largely because the process of producing a DNA profile is not automatic and cannot be conducted in real time, *i.e*. it takes a few hours. Moreover, unlike other biometrics, DNA profiling requires the removal of material from the body itself rather than feature extraction or template generation and this inevitably raises issues in relation to bodily integrity. Thus, the differences between traditional biometrics and DNA are at this point in time distinct and make a full discussion of DNA as a biometric identifier outside the scope of the current report. Nonetheless, the level of accuracy of DNA, as indicated by its use in forensic applications (*e.g.* for law enforcement) and for paternity testing, suggest that it

could potentially be used for biometric recognition in the future and therefore merits a limited discussion.

Forensic DNA identification is based on the process of DNA profiling. This involves the analysis of the numbers of tandemly repeating sequences of non-coding DNA, *i.e.* regions of DNA that are not part of genes and are, generally, not considered to have any specific function, from a given locus on the human genome. Depending on the exact methodology used, a particular number of loci may be targeted, which are from different parts of the DNA

Advantages

- The genome is unique to each person.
- Accurate

Disadvantages

- Not fast and automated
- Matching not done in real-time
- Intrusive

Gait

gait is a complicated spatio-temporal biometric, which relates to the specific way an individual walks. Moreover, humans have been shown to identify and recognise people on the basisof their gait. In terms of biometric recognition of gait, a video camera is used to capture the specific repeating pattern produced by an individual as he/she walks. An algorithm is used to determine the mathematical relationship between each point of movement of the body and to create a signature pattern (template) necessary for recognition. Biometric gait recognition can utilise the shape and/or the dynamics of the body as it moves and these are predominantly assessed through silhouette matching. Other factors such as stride length, cadence and stride speed as well as static body movements may also be assessed. gait is not a universal biometric trait, since not all individuals are able to walk. In addition, gait is not regarded to be very distinctive across large populations, but it is considered sufficiently distinguishable for recognition purposes in low security applications.426

While an individual's gait is influenced by his/her musculo-skeletal structure it is a behavioural trait, and is prone to variation over time, for example, due to changes in body weight, pregnancy, injuries (especially to the legs or feet) and even drunkenness. An individual's gait can be collected from a distance and from a number of angles, even using a low resolution video camera. Collection can also be achieved with or without the user's cooperation or knowledge. While the ability to examine an individual's gait covertly and at a distance may raise some concerns relating to surveillance, gait recognition systems are generally widely accepted. however, this type of system is not considered to offer very high performance overall. While indoor applications of gait recognition have shown somewhat better performance levels, this technology is most likely to be employed outdoors, where changing environmental conditions, for example, illumination and the presence of shadows, can affect recognition accuracy adversely. Furthermore, it has been shown that performance is also particularly susceptible to differences in footwear, clothing, walking surface, walking speed, whether or not the individual was carrying something, whether image collection occurred indoors or outdoors, and the time elapsed since the individual last used the system. research is ongoing to try to overcome some of these issues and also to try and identify aspects of gait that are not affected by these factors. While it has been suggested that it could be difficult for an individual to mask his/her own gait pattern while posing as someone else, the current level of performance of these systems would leave it open to circumvention.

Advantages

- Non-invasive
- Can discriminate using various actions such as walking, jogging, running)
- Can be obtained from a distance
- Can be used to determine medical illnesses

Disadvantages :

- Can be altered by observation
- May not be applied to smaller devices such as mobiles or desktops
- Still under research
- Can be obtained from a distance – invasion of pr

Odour recognition

These systems are based on the recognition of characteristic components of odour emitted by a given individual. Since odour is emitted from pores all over an individual's body, these systems operate by circulating air around the body part being analysed (*e.g.* the back of the hand, the arm or the neck) and over an array of chemical sensors. Each of these sensors is sensitive and receptive to certain groups of aromatic compounds of the individual's smell, which are extracted and classified into a template.

All individuals emit an odour, components of which are considered to be distinctive. While the odour profile itself is considered permanent, it can be affected by certain foods and medications. While body odour can be collected from non-intrusive parts of the body, currently available sensors have difficulties in distinguishing the invariant components of body odour, which limits system performance. In addition, performance can also be affected by the use of deodorants and perfumes435

and contamination or odour transfer between different people.

Keystroke Dynamics

It has been suggested that individuals have a characteristic way of typing on a keyboard, which is sufficient for use in biometric recognition systems. This technology can assess an individual's keystroke dynamics (*e.g.* speed and pressure), the total typing time for a specific password and the time taken between hitting certain keys. Keystroke dynamic systems are moderately resistant to circumvention, but they are usually used for low security app lications,*e.g*. for controlling and monitoring access to computer systems and networks.

While not considered unique to a given individual, it has been suggested that keystroke dynamics are distinctive enough to verify an individual's identity. however, not all individuals can exhibit keystroke dynamics, for example, due to insufficient literacy levels or competence in using computers. As a behavioural biometric trait, keystroke dynamics are inherently variable over time. This variation, combined with the limited distinctiveness of this biometric, results in poor system performance, which limits the implementation of this technology to small-scale applications. This trait can be collected quite easily and unobtrusively, which may assist in the acceptance of this method of recognition.

Dental

Dental biometric schemes analyze dental radiographs for human identification.

- How does the dental technology work?

Postmortem radiographs, (PM), are those radiographs that are acquired after a person's death.

Antemortem radiographs, (AM), are acquired while a person is alive. Dental biometrics can be broken into two categories: feature extraction and matching.

Images are enhanced and dental work is segmented in the feature extraction stage. The matching stage can be further broken into three steps: tooth-level matching, computation of image distances, and subject identification.

- Tooth-level matching – Using a shape registration method, the tooth contours are matched. Dental work is also matched on overlapping areas in this stage.
- Computations of image distances – Distance between the two radiographs is measured based on the corresponding teeth.
- Subject identification – All of the distances between the given PM and the AM are combined to establish the identity of the person.

The database containing both AM and PM radiographs are used to analyze one of the radiographs against the other.

Advantages

- Radiographs can be used on living and non-living people

Disadvantages

- Not an automated method
- Variation of dental structure between AM and PM

Rhythm/Tapping Sequence

In the early days of telegraphy, operators could identify each other by recognizing the way in which they tapped out messages. This simple idea has been used as a type of biometric, using newly

developed polymer thick-film pressure sensors that can detect the unique cadence of a tapped rhythm and verify identity. This method exploits the differences with which individuals tap out a rhythm, capturing the pattern of taps on a single sensor rather than the pattern of keystrokes on a keyboard (such as keystroke dynamics). A tapping sequence can have both waveform and rhythm features. Waveforms are studied for unique charachterisics, such as height and duration. Like sound waves, pressure points provide measurable wavelenths. Recognition by rhythm is so simple it may be possible to implement on devices such as smartcards and PDAs by screen-printing a sensor onto a thin layer of Mylar that is bonded onto the device.

Keypad pressure sensors may run up against many of the same obstacles as the early keystroke-pattern recognition systems. A user must apply the sensors with a substantial amount of initial input in order to train the sensors to recognize the individual's unique waveform signature. Biological responses like fatigue can change the pattern of the user's input in the course of such a test. Factors such as posture or position relative to the sensor pad can also affect the user's pressure "signature.

Skull Resonance

Skull resonance is a developing form of biometric identification by which sound waves are passed through the head of a subject to produce a unique sonar profile.

Body Salinity (Salt)

This developmental system works by exploiting the natural level of salinity, or salt, in the human body. This is accomplished by using an electric field and salt's natural conductivity to measure a tiny electrical current that is passed through the body. The electrical current that is used is approximately one-billionth of an amp (nanoamp), which is less than the natural currents already present in the body. Speeds equivalent to a 2400-baud modem have been claimed, yielding a data transfer rate of up to 400,000 bits per second. Applications for this kind of biometric technology could include the interaction (data transfer) between communication devices carried on the body, such as watches, mobile phones, and pagers. Also, applications could include "waking up" household appliances/devices as one enters a room.

SECURITY ISSUES

The most common standardized encryption method used to secure a company's infrastructure is the Public Key Infrastructure (PKI) approach. This approach consists of two keys with a binary string ranging in size from 1024-bits to 2048-bits, the first key is a public key (widely known) and the second key is a private key (only known by the owner). However, the PKI must also be stored and inherently it too can fall prey to the same authentication limitation of a password, PIN, or token. It too can be guessed, lost, stolen, shared, hacked, or circumvented; this is even further justification for a biometric authentication system. Because of the structure of the technology industry, making biometric security a feature of embedded systems, such as cellular phones, may be simpler than adding similar features to PCs. Unlike the personal computer, the cell phone is a fixed-purpose device. To successfully incorporate Biometrics, cell-phone developers need not gather support from nearly as many groups as PC-application developers must.

Security has always been a major concern for company executives and information technology professionals of all entities. A biometric authentication system that is correctly implemented can provide unparalleled security, enhanced convenience, heightened accountability, superior fraud detection, and is extremely effective in discouraging fraud. Controlling access to logical and physical assets of a company is not the only concern that must be addressed. Companies, executives, and security managers must also take into account security of the biometric data (template). There are many urban biometric legends about cutting off someone finger or removing a body part for the purpose of gain access. This is not true for once the blood supply of a body part is taken away, the unique details of that body part starts to deteriorate within minutes. Hence the unique details of the severed body part(s) is no longer in any condition to function as an acceptable input for scanners.

The best overall way to secure an enterprise infrastructure, whether it be small or large is to use a smart card. A smart card is a portable device with an embedded central processing unit (CPU). The smart card can either be fashioned to resemble a credit card, identification card, radio frequency identification (RFID), or a Personal Computer Memory Card International Association (PCMCIA) card. The smart card can be used to store data of all types, but it is commonly used to store encrypted data, human resources data, medical data, financial data, and biometric data (template). The smart card can be access via a card reader, PCMCIA slot, or proximity reader. In most biometric-security applications, the system itself determines the identity of the person who presents himself to the system. Usually, the identity is supplied to the system, often by presenting a machine-readable ID card, and then the system asked to confirm. This problem is "one-to- one matching." Today's PCs can conduct a one-to-one match in, at most, a few seconds. One-to-one matching differs significantly from one-to-many matching. In a system that stores a million sets of prints, a one-to-many match requires comparing the presented fingerprint with 10 million prints (1 million sets times 10 prints/set). A smart card is a must when implementing a biometric authentication system; only by the using a smart card can an organization satisfy all security and legal requirements. Smart cards possess the basic elements of a computer (interface, processor, and storage), and are therefore very capable of performing authentication functions right on the card.

The function of performing authentication within the confines of the card is known as 'Matching on the Card (MOC)'. From a security prospective MOC is ideal as the biometric template, biometric sampling and associated algorithms never leave the card and as such cannot be intercepted or spoofed by others (Smart Card Alliance). The problem with smart cards is the public-key infrastructure certificates built into card does not solve the problem of someone stealing the card or creating one. A TTP (Trusted Third Party) can be used to verify the authenticity of a card via an encrypted MAC (Media Access Control).

ADVANTAGES OF BIOMETRIC TECHNOLOGIES

Biometric technologies can be applied to areas requiring logical access solutions, and it can be used to access applications, personal computers, networks, financial accounts, human resource records, the telephone system, and invoke customized profiles to

enhance the mobility of the disabled. In a business-to-business scenario, the biometric authentication system can be linked to the business processes of a company to increase accountability of financial systems, vendors, and supplier transactions; the results can be extremely beneficial.

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

DISADVANTAGES OF BIOMETRIC TECHNOLOGIES

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

Performance measurement

Errors and Error Rates

No biometric system can recognize a person absolutely. While it appears to give a simple yes or no answer, it is, in fact, measuring how similar the current biometric data is to the record stored in the database and makes a decision according to the probability that the biometric sample comes from the same person that provided the stored biometric template. While there are several types of errors that occur in biometric systems, there are two major classes of errors that relate to the system's accuracy; *comparison errors* and *decision errors*

The errors discussed below have error "rates" associated with them. Thus, a False Match has a False Match Rate (FMR) associated with it, a False Non-Match a False Non- Match Rate (FNMR) and so on. These rates are established by extensive testing, and are nothing more than how often these errors have been shown to occur during testing. Expressed mathematically, a rate is the expected

probability that this error will occur in this biometric system.

These rates provide quantifiable metrics that allow one to compare the effectiveness of various technologies and the various products therein.

Comparison errors are erroneous matches or nonmatches that could be considered "machine

functions," or more semantically correct, machine malfunctions.

A *false match* is an erroneous conclusion by the biometric system that a template stored in its database is from the same person that has just presented a biometric sample, when in fact, it is not.

A *false non-match* is an erroneous conclusion by the biometric system that a template stored in its database is not from the same person that has just presented a biometric sample, when in fact, it is.

Decision errors are erroneous conclusions arising from comparison errors. The definitions of decision errors depend upon the application (the premise by which a subject uses the system).

A *false accept* in an application such as access control, where the subject makes a "positive" claim of enrollment ("I am enrolled as Pat") is an erroneous conclusion by the biometric system that a template stored in its database is from the same person that has just presented a biometric sample, when in fact, it is not.

A false accept rate (FAR), is the expected probability that this will occur in this particular biometric system, in this application. In a positive identification application, false accept is the
same as false match.

A *false reject* in a positive identification application such as access control is an erroneous conclusion by the biometric system that a template stored in its database is not from the same person that has just presented a biometric sample, when in fact, it is.

A false reject rate (FRR),
is the expected probability that this will occur in this particular biometric system, in this application. In a positive identification application, false reject is the same as false non-match.

A *false accept* in a negative identification application where a "negative" claim of enrollment (such as watch lists, or benefits entitlements, where a person claims "I am not enrolled in the system") is an erroneous conclusion by the biometric system that no template stored in its database is from the same person that has just presented a biometric sample, when in fact, one is. A false accept rate (FAR) is the expected probability that this will occur in this particular biometric system, in this application.

In a Negative identification application, false accept is the same as a false non-match, although the rates may be different depending upon the number of comparison attempts made in reaching the "accept" decision.

A *false reject* in a negative identification application (such as watch lists, or benefits entitlements) is an erroneous conclusion by the biometric system that a template stored in its database is from the same person that has just presented a biometric sample, when in fact, it is not. A false reject rate (FRR), is the expected probability that this will occur in this particular biometric system, in this application. In a negative identification application, false reject is the same as false match, although their rates may be different depending upon the number of comparisons required to make a "reject"
decision.

This somewhat confusing distinction is the result of new, non-traditional applications that have been developed for biometric systems. Historically, FAR and FRR have been used synonymously with FMR and FNMR respectively. However, with the emergence of negative identification systems, usually 1:N identification systems, they are no longer synonymous.

In traditional access control applications (positive ID systems), the premise of the user was always "I am in the system and entitled to enter." A false acceptance occurred when the subject was an impostor and not entitled to entry, but as the result of a false match, he was allowed entry. Likewise, subjects who were legitimately enrolled in the systems became victims of a false rejection when

there was a false non-match. In today's negative identification systems such as watch lists, correctional facilities, and detection of double dippers in benefits entitlement programs, the premise of the user is "I'm not in the system and never have been." In these applications, a false accept occurs when the system commits a false non-match error, and a false reject occurs when the system commits a false match error.

Comparison and Comparison Errors

Comparison is the act of comparing one (or more) acquired biometric sample to one (or more) stored biometric templates to determine whether they "match," that is, come from the same source. In essence, there are three ways a mistake can be made:

- Failure to enroll and failure to acquire .
- False acceptance (FAR)
- False rejection (FRR)

Both failure to enroll and failure to acquire (during the comparison process) mean the system is unable to "extract" and distinguish the appropriate features of the user's biometric. For example, a small percentage of the population cannot enroll a fingerprint, either because their fingerprints are not distinctive enough or the characteristics have been altered due to age or occupation. Failure to enroll and/or failure to acquire indicate this person's biometric characteristics may not be of sufficient quality to be used for recognition. In access control systems, a false acceptance occurs when a sample is incorrectly matched to a different user's template in a database (in the case of an access control system, an impostor is allowed in the building). A false rejection occurs when a sample is incorrectly not matched to an otherwise correct matching template in the database (in the case of an access control system, a legitimate enrollee is falsely rejected). In most biometric systems, the false acceptance and false rejection thresholds can be adjusted, depending upon the level of security required. For example, in a high security access control application, the system can be adjusted to err on the side of denying legitimate matches and not tolerating impostors. Alternatively, a conveniencefocused application could be adjusted to offer little or no denial of legitimate matches, while allowing some minimal acceptance of impostors.

- **False Accept Rate (FAR) or False Match Rate (FMR):**

  The probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database. It measures the percent of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people.

- **False Reject Rate (FRR) or False Non-Match Rate (FNMR):**

  The probability that the system incorrectly declares failure of match between the input pattern and the matching

template in the database. It measures the percent of valid inputs being rejected.

- **Receiver (or relative) Operating Characteristic (ROC):**

In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems the FAR and FRR can typically be traded off against each other by changing those parameters. The ROC plot is obtained by graphing the values of FAR and FRR, changing the variables implicitly. A common variation is the *Detection error trade-off (DET)*, which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

Equal Error Rate (EER):

The rate at which both accept and reject errors are equal. ROC or DET plotting is used because how FAR and FRR can be changed, is shown clearly. When quick comparison of two systems is required, the ERR is commonly used. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.

- **Failure To Enroll Rate (FTE or FER):** The percentage of data input is considered invalid and fails to input into the system. Failure to enroll happens when the data obtained by the sensor are considered invalid or of poor quality.
- **Failure to Capture Rate (FTC):**

Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly.

- **Template capacity**:

The maximum number of sets of data which can be input in to the system.

BIOMETRIC APPLICATIONS

Most biometric applications fall into one of nine general categories:

- Increase security - Provide a convenient and low-cost additional tier of security.
- Reduce fraud by employing hard-to-forge technologies and materials. For e.g.Minimise the opportunity for ID fraud, buddy punching.
- Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. Prevent unauthorised use of lost, stolen or "borrowed" ID cards.
- Reduce password administration costs.
- Replace hard-to-remember passwords which may be shared or observed.
- Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access

- Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN! Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance.
- Unequivocally link an individual to a transaction or event.

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

CONCLUSION

Recent advances in biometric technology have resulted in increased accuracy at reduced costs, biometric technologies are positioning themselves as the foundation for many highly secure identification and personal verification solutions. Today's biometric solutions provide a means to achieve fast, user-friendly authentication with a high level of accuracy and cost savings. Many areas will benefit from biometric technologies. Highly secure and trustworthy electronic commerce, for example, will be essential to the healthy growth of the global Internet economy. Many biometric technology providers are already delivering biometric authentication for a variety of web-based and client/server based applications to meet these and other needs. Continued improvements in technology will bring increased performance at a lower cost.

Currently, there exist a gap between the number of feasible biometric projects and knowledgeable experts in the field of biometric technologies. The post September 11 th, 2002 attack (a.k.a. 9-11) on the World Trade Center has given rise to the knowledge gap. Post 9-11 many nations have recognized the need for increased security and identification protocols of both domestic and international fronts. This is however, changing as studies and curriculum associated to biometric technologies are starting to be offered at more colleges and universities. A method of closing the biometric knowledge gap is for knowledge seekers of biometric technologies to participate in biometric discussion groups and biometric standards committees.

The solutions only needs the user to possess a minimum of require user knowledge and effort. A biometric solution with minimum user knowledge and effort would be very welcomed to both the purchase and the end user. But, keep in mind that at the end of the day all that the end users care about is that their computer is functioning correctly and that the interface is friendly, for users of all ability levels. Alternative methods of authenticating a person's identity are not only a good practice for making

biometric systems accessible to people of variable ability level. But it will also serve as a viable alternative method of dealing with authentication and enrollment errors.

Auditing processes and procedures on a regular basis during and after installation is an excellent method of ensuring that the solution is functioning within normal parameters. A well-orchestrated biometric authentication solution should not only prevent and detect an impostor in instantaneous, but it should also keep a secure log of the transaction activities for prosecution of impostors. This is especially important, because a great deal of ID theft and fraud involves employees and a secure log of the transaction activities will provide the means for prosecution or quick resolution of altercations.

REFERENCES:

[1.] Pankanti S, Bolle R & Jain A, Biometrics:The Future of Identification

[2.] Nalwa V, Automatic on-line signature verification

[3.] Biometric Consortium homepage, http://www.biometrics.org

[4.] International Biometric Group website,http://www.biometricgroup.com/biometric_technology_overview.htmISO/IEC JTC1/SC17 N1793, "Usability of Biometrics in Relation to Electronic Signatures v1.0."

[5.]] R. Chellappa et al., "Human and Machine Recognition of Faces: A Survey", Technical report CAR-TR-731, University of Maryland Computer Vision Laboratory, 1994.

[6.] MIT Media Lab Website, http://web.media.mit.edu/~jebara/uthesis/node8.html.

[7.] M. Turk and A. Pentland, "Eigenfaces for Recognition", Journal of Cognitive Neuroscience,

[8.] Vol. 3, pp. 72-86, 1991.

[9.] Visionics website, http://www.visionics.com/faceit/tech/lfa.html

[10.] L. Wiskott, J.M. Fellous and C. von der Malsburg, "Face Recognition by Elastic Bunch Graph

[11.] Matching", IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 19, pp. 775-779, 1997.

[12.] Biometric Systems Lab website, Bologna , University:http://bias.csr.unibo.it/research/biolab/bio_tree.html.

[13.] A Jain, R. Bolle, S. Pankanti, "Biometrics: Personal Identification in Networked Society", Kluwer, 1999.

[14.] International Biometric Group "Biometric Market Report 2003" website: http://www.ibgweb.com/reports/public/market_report.html Sushma Jaiswal, Sarita Singh Bhadauria, Rakesh Singh Jadon and Tarun Kumar Divakar,Brief description of image based 3D face recognition methods ,Volume 1, Number 4, 1-15, DOI: 10.1007/3DRes.04(2010)02.\

[15.] Sushma Jaiswal , Sarita Singh Bhadauria , Rakesh Singh Jadon “Creation 3D Animatable Face Methodology Using Conic Section-Algorithm”,Information Technology Journal, ISSN:18125638,pages no.292-298,2007.

[16.] Sushma Jaiswal , Sarita Singh Bhadauria , Rakesh Singh Jadon,”Automatic 3D Face Model from 2D Image-Through Projection” Journal: Information Technology Journal Year: 2007 Vol: 6 Issue: 7 Pages/record No.: 1075-1079.