A COMPARATIVE STUDY OF MULTIMODAL BIOMETRICS

Shruthy Poonacha[1], Savitha K.V[2] and A. Radhesh[3]

Lecturer, SBRR Mahajana First Grade College, Mysore
Email: [1]shruthypoonacha@gmail.com, [2]savithakv3@gmail.com, [3]aradesh@gmail.com

ABSTRACT

Unlike the use of other forms of authentication, such as passwords or tokens, biometric recognition provides a strong link between an individual and a claimed identity. Voiceprint unlocks the doors of houses. Iris scan lets you into the corporate offices. You are your own key.

Multimodal biometric system is the best solution to the problem of data leakage and ensures reliable data protection.

Biometric technology uses the measurements of a biological characteristic such as fingerprint, iris pattern, retina, image, face or hand geometry or a behavioral characteristic such as voice, gait or signature are used to identify the individuals automatically. Ideally the characteristic should be universally present, unique to the individual, stable over time and easily measurable. The characteristics that stay constant and that are difficult to fake or change on purpose are used for security. The main aim of this study is to make a comparative study of multimodal biometrics and declare the best effective method of biometrics that offers both security and convenience.

Keywords: Biometrics, Finger print, Palm print, DNA, Iris, Ear, Face.

INTRODUCTION

The word biometric can be defined as "life - measure." A biometric system provides an automated method of recognizing an individual based on the individual's biometric characteristics. The need for reliable user authentication techniques has increased in the wake of heightened concerns about security and rapid advancements in networking, communication and mobility.

A driver's license contains biometric information about an individual. His height, weight, hair color and eye color are all physical characteristics that can easily be checked. However, height changes with age (16 years old drivers get taller, senior citizens get shorter). The hair color changes naturally, weight fluctuates over time. For biometrics usually the consideration of the above factors are avoided.

Biometric systems have now been deployed in various commercial, civilian and forensic applications as a means of establishing identity. These systems rely on the evidence of

fingerprints, hand geometry, iris, retina, face, hand vein, facial thermo gram, signature, voice, etc. to either validate or determine an identity [Ross et al., 2006]. Most biometric systems deployed in real-world applications are unimodal, i.e., they rely on the evidence of a single source of information for authentication (e.g., single fingerprint or face). These systems have to contend with a variety of problems such as:

(a) Noise in sensed data: fingerprint images with a scar or a voice sample altered by cold are examples of noisy data. Noisy data could also result from defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavorable ambient conditions (e.g., poor illumination of a user's face in a face recognition system).

(b) Intra-class variations: These variations are typically caused by a user who is incorrectly interacting with the sensor (e.g., incorrect facial pose), or when the characteristics of a sensor are modified during authentication (e.g., optical versus solid-state fingerprint sensors).

(c) Inter-class similarities: In a biometric system comprising of a large number of users, there may be inter-class similarities (overlap) in the feature space of multiple users. [Golfarelli et al., 1997] state that the number of distinguishable patterns in two of the most commonly used representations of hand geometry and face are only of the order of 105 and 103, respectively.

(d) Non-universality: The biometric system may not be able to acquire meaningful biometric data from a subset of users. A fingerprint biometric system, for example, may extract incorrect minute features from the fingerprints of certain individuals, due to the poor quality of the ridges.

(e) Spoof attacks: This type of attack is especially relevant when behavioral traits such as signature or voice are used. However, physical traits such as fingerprints are also susceptible to spoof attacks. Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity [Anil et al., 2004]. Such systems, known as multimodal biometric systems, are expected to be more reliable due to the presence of multiple, (fairly) independent pieces of evidence [Philips.et al., 2004]. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a 'live' user is indeed present at the point of data acquisition.

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode.

In the verification mode, the system validates a person's identity by comparing the captured biometric data with his/her own biometric template(s) stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts

a one-to-one comparison to determine whether the claim is true or not typically to check multiple people from using the same identity [Wayman et al., 2001]

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database without the subject having to claim an identity (e.g., "Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who he/she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities [Wayman et al., 2001]. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

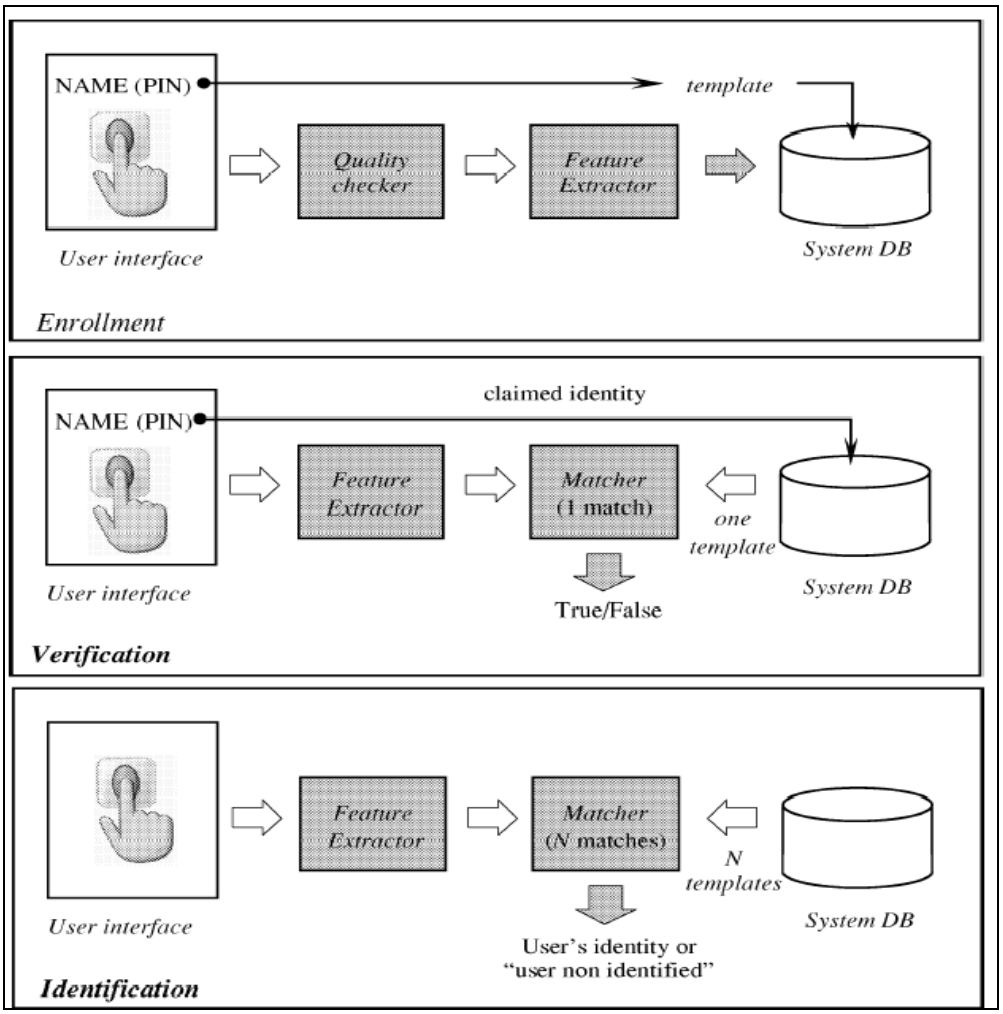


Fig. 1. Block diagrams of enrollment, verification, and identification tasks are shown using the four main modules of a biometric system

Biometric Considerations

While potentially offering significant security benefits, a biometric system is only one of many security tools available. Depending on the application, an environment or circumstance may or may not benefit from a biometric system. Understanding the operational requirements of the situation is necessary to determine if a biometric system can be used to meet a security need. The use of biometrics will not solve all of a system's security problems, but when properly implemented, a biometric system should be one part of overall security architecture.

There is no single biometric modality that is best for all applications. Many factors must be taken into account when implementing a biometric system including location, security risks, task, expected number of users, user circumstances, existing data, etc. It is also important to note that biometric modalities are in varying stages of maturity and therefore may offer varying levels of security, ease of implementation, and user convenience.

Biometric systems alone do not currently provide adequate security for high assurance applications. When biometric systems are combined with other security mechanisms those systems can provide significant security benefits. However, the biometric system must be implemented correctly for the specific application.

Biometrics Characteristics

Any physical and/or behavior characteristics of a human can be considered as a biometric if it exhibits following characteristics as explained below: [Ross *et al,*.2006]

Each person accessing the biometric application should posses a valid biometric trait i.e. Universality.

The given biometric trait should exhibit distinct features across individuals comprising the population. i.e. Uniqueness.

The biometric characteristics should remain sufficiently invariant over a period of time i.e. Permanence.

The biometric characteristics can be quantitatively measured i.e. Measurability.

The biometric trait should give the required accuracy imposed by the application i.e. Performance.

The chosen biometric trait must be accepted by a target population that will utilize the application i.e. Acceptability.

It is how easily the chosen biometric trait can be fooled using artifacts i.e. Circumvention.

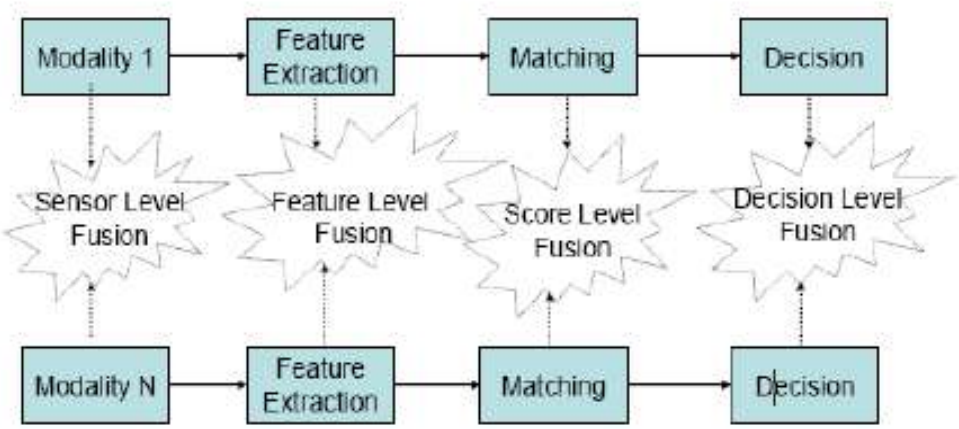


Fig. 2. Block diagram of Multimodal Biometric System

Levels of Fusion

As indicated in fig.2 there are four ways in which information from multiple sources are combined such as sensor level, feature level, match score level and decision level. The amount of the information available for fusion decreases after each level of processing in a biometric system. The raw data represents the richest set of information, while final decision contains just an abstract level of information. Further in many practical multimodal biometric systems, early levels of information such as raw data or feature sets may not be available or even if they are available they may not be compatible for fusion. In such cases information obtained at later levels like match score level or decision level can be employed as it is easy to fuse and all commercial devices provide access to scores and decisions. The brief descriptions of four different levels of fusions are as follows:

Sensor level fusion

Here raw data obtained from different modalities are fused. The sensor level fusion can be performed only if the sources are either samples of same biometric trait obtained from multiple compatible sensors or multiple instances of same biometric trait obtained using a single sensor. Since sensor level fusion combines the information from different sensors, it requires some preprocessing such as sensor calibration and data registration before performing the fusing.

Feature level fusion

Feature level fusion consolidates the features obtained from different sources. If obtained features are structurally compatible then feature concatenation is carried out to fuse the features obtained from different sources otherwise concatenation is not possible. Moreover combining the features will introduce a curse of dimensionality and hence either feature transformation or feature selection can be applied to reduce the dimensionality of the fused feature set.

Match score level fusion

Match score is a measure of the similarity between the input and template biometric feature vector. In match score level fusion, the match score obtained from different matchers are combined. Since scores obtained from different matchers are not homogeneous, score normalization technique is followed to map the scores obtained from different matchers on to a same range.

Decision level fusion

Decision level fusion involves the fusion of decision obtained from different modalities. Since decision level fusion holds binary values it is also called as abstract level fusion [Ross et al., 2006].

Multimodal Biometrics

A number of biometric characteristics exist and are used in various applications. Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is "optimal." The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic. Commonly used biometrics are as follows:

DNA: Deoxyribonucleic acid (DNA) is the one-dimensional (1–D) ultimate unique code for one's individuality except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in the context of forensic applications for person recognition. Three issues limit the utility of this biometrics for other applications: 1) Contamination and Sensitivity: It is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose.

2) Automatic real-time recognition issues: The present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert's skills and is not geared for on-line noninvasive recognition.

3) Privacy issues: Information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, e.g., in hiring practices.

Ear: It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

Face: Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled "mug-shot" verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport).

The most popular approaches to face recognition are based on either:

1) The location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships.

2) The overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. While the verification performance of the face recognition systems that are commercially available is reasonable [Philips.*et al.,* 2004], they impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple background or special illumination. These systems also have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence [Golfarelli.*et al.,* 1997]. In order for a facial recognition system to work well in practice, it should automatically: detect whether a face is present in the acquired image; locate the face if there is one; and recognize the face from a general viewpoint (i.e., from any pose).

Fingerprint: Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high[Maio.*et al., 2002*]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, a fingerprint scanner costs about U.S.$20 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications.

The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small- to medium-scale identification systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities.

Hand and finger geometry: Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. Commercial hand geometry-based verification systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual's jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops. There are verification systems available that are based on measurements of only a few fingers (typically, index and middle) instead of the entire hand. These devices are smaller than those use d for hand geometry, but still much larger than those used in some other biometrics (e.g., fingerprint, face, voice).

Iris: The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive

information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the iris of identical twins is different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises (e.g., designer contact lenses). Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost effective.

Odor: It is known that each object exudes an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. A whiff of air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of (aromatic) compounds. A component of the odor emitted by a human (or any animal) body is distinctive to a particular individual. It is not clear if the invariance in the body odor could be detected despite deodorant smells, and varying chemical composition of the surrounding environment.

Palm print: The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palm prints are expected to be even more distinctive than the fingerprints. Since palm print scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper [Zhang&Shu, et al., 1999]. Finally, when using a high-resolution palm print scanner, all the features of the palm such as hand geometry, ridge and valley features (e.g., minute and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system.

Retinal scan: The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image acquisition requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these factors adversely affect the public acceptability of retinal biometric. Retinal vasculature can reveal some medical conditions, e.g., hypertension, which is another factor deterring the public acceptance of retinal scan-based biometrics.

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

Voice: Voice is a combination of physiological and behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as a common cold),and emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification.

A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what he/she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel.

A brief comparison of the above biometric techniques based on seven factors is provided in the Table 1. The applicability of a specific biometric technique depends heavily on the requirements of the application domain. No single technique can outperform all the others in all operational environments. In this sense, each biometric technique is admissible and there is no optimal biometric characteristic. For example, it is well known that both the fingerprint-based and iris-based techniques are more accurate than the voice-based technique. However, in a tele-banking application, the voice-based technique may be preferred since it can be integrated seamlessly into the existing telephone system.

Table 1. Comparison of Biometric Techniques based on characteristics with High (H=3), Medium (M=2) &Low (L=1)

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention	Scores	Rank
DNA	H	H	H	L	H	L	L	15	3
Ear	M	M	H	M	M	H	M	16	2
Face	H	L	M	H	L	H	H	16	2
Fingerprint	M	H	H	M	H	M	M	17	1
Iris	H	H	H	M	H	L	L	16	2
Odor	H	H	H	L	L	M	L	14	4
Palm Print	M	H	H	M	H	M	M	17	1
Retina	H	H	M	L	H	L	L	14	4
Signature	L	L	L	H	L	H	H	13	5
Voice	M	L	L	M	L	H	H	13	5

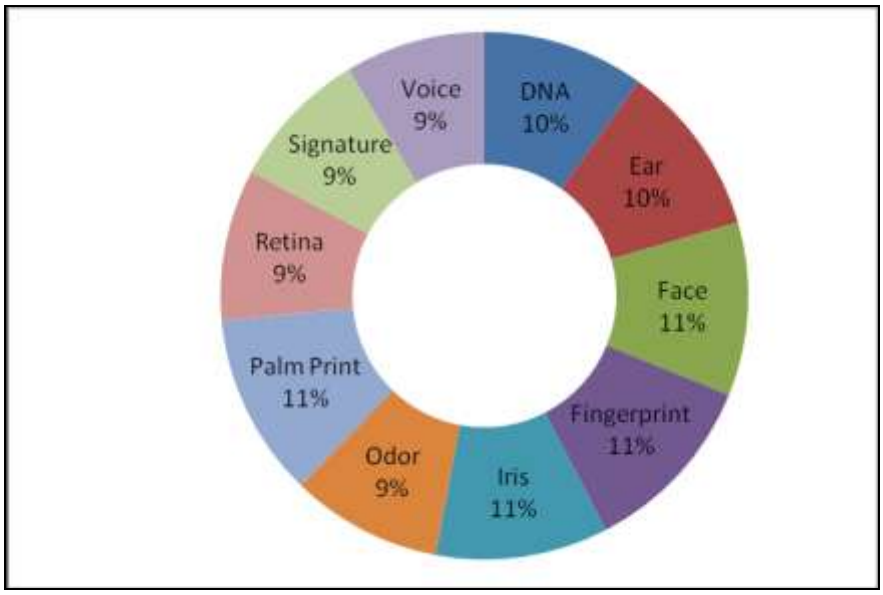


Fig. 3. Comparison of Biometric Techniques

Factors of Evaluation

False Accept Rate (FAR) and False Match Rate (MAR): It is the probability that the system incorrectly declares a successful match between the input pattern and a no 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.

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 Tradeoff (DET), which is obtained using normal deviate scales on both axes

Equal Error Rate (EER): The rates at which both accept and reject errors are equal. ROC or DET plotting is used because how FAR and FRR can be changed. When quick comparison of two systems is required, the ERR is commonly used. 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.

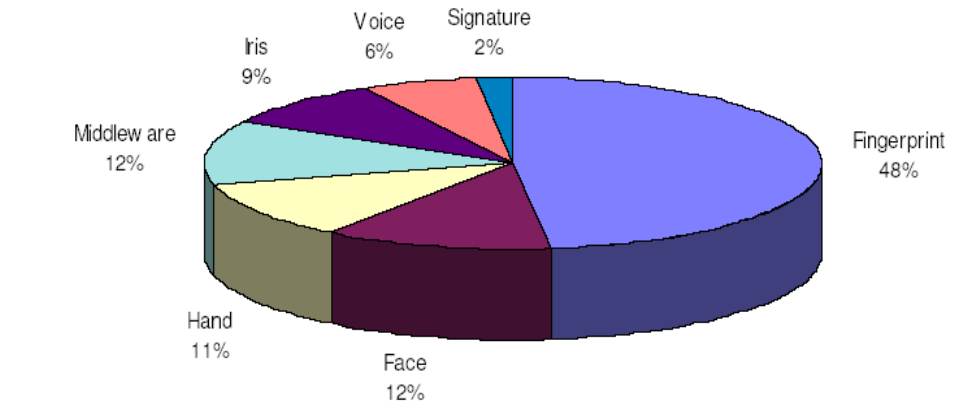
Failure to Capture Rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly is generally treated as FTC.

Template Capacity: It is defined as the maximum number of sets of data which can be input in to the system.

RESULTS OF EVALUATION

The evaluations of various techniques using the above parameters are presented in a tabular format.

Biometric	EER	FAR	FRR	Subjects	Comments
face	NA	1%	10%	37437	varied light, indoor /outdoor
finger print	2%	2%	2%	25000	rotation and exaggerated skin distortion
Iris.	.01%	94%	.99%	1224	indoor environment
voice	6%	2%	10%	30	text dependent and multilingual



Source: International Biometric Group

Fig. 4. Commonly Used Biometric Technologies

Table 2. Comparison of the biometric methods based on their characteristics, accuracy, cost and social acceptability

	Eye-Iris	**Eye-Retina**	**Fingerprint**	**Hands Geometry**	**Writing signature**	**Voice**
Reliability	Very-high	High	High	High	High	High
Easiness of the users use	Average	Low	High	High	High	High
Attack's precaution	Very-high	Very-high	High	High	Average	Average
Acceptance	Average	Average	Average	High	Very-high	High
Stability	High	High	High	Average	Average	Average
Identification and Authentications	Both	Both	Both	Authentication	Both	Authentication
Standards			ANSI / NIST / FBI			SVAPI
Interference	Glasses	Irritations	Dirtiness, Injury, Roughness	Arthritis, Rheumatism	Changeable or easy signatures	Noise, Cold
Use	Nuclear installations, medical services penitentiary centers	Nuclear installations, medical services penitentiary centers	Police, Industrial	General	Industrial	Remote access in banks or database
Price($)	5000	5000	1200	2100	1000	1200

Table 3. Advantages and disadvantages, usage and cost of installation of Biometrics

Technique	**Advantages**	**Disadvantages**	**Usage**	**Cost**
Fingerprint Scanning	• Better security • Can accommodate cuts • Less Expensive • Small • Easy to adapt • Widely accepted • Small storage space required	• Each finger only has 50 discriminators • 2% of the population Have poor fingerprints	• Law enforcement • Corporate database	$50-$1,200
Facial Recognition	• Video camera equipment is inexpensive • Unobtrusive/Passive • Allow for audits from stored face images	• Awkward lighting in the image can affect authentication • Subject to spoofing attempts	• General	$200-$3,000

Table 3. Advantages and disadvantages, usage and cost of installation of Biometrics (Contd…)

Technique	Advantages	Disadvantages	Usage	Cost
Iris	• The iris remains unchanged throughout a person's life • The left and the right irises are different • Each iris has 170 discriminators • Very accurate • The iris's image can be captures from a distance	• More expensive • Subject to user motion • Large template • 15% of the population cannot have their iris scanned	• Access control • ATM • Airport	$200-$3,000
Voice Print	• Less expensive • Can be used remotely • PCs already have the necessary hardware	• Less accurate • Susceptible to rejections • Susceptible to forgery	• Industrial	$120-$1,000

Comparing All the Factors in the Tables above Us We Can Deduce That the Most Adequate Methodology Is the Fingerprint Authentication

A software algorithm searches the finger print image for the location of "minute" which are points where a ridge ends or splits in two. In addition, some algorithms categorize the overall patterns of the fingerprint into one of five standard classes, such as a whorl or an arch. Because fingerprints have fewer degrees of freedom than irises (about 40 versus more than 200), automated fingerprint identification has generally not achieved the same level of accuracy as iris scans. In fact, the false rejection rate—the frequency with which a valid identification is erroneously rejected—is 1% in most systems. False acceptance rates, however, are extremely low, which makes imposture almost impossible. So fingerprint-image systems are being widely adopted for social welfare purposes. Using prints from two fingers has reduced false rejection rates. In addition, Identic, Inc. (Sunnyvale, CA), the largest provider of fingerprint scanning hardware and software, is marketing its device as a computer security aid to replace the use of passwords. Here, the scanner is placed on a pad next to the computer, incorporated into the mouse, or built into the keyboard.

Other biometric techniques have significantly greater error rates than either iris scanning or fingerprint imaging. Hand dimensions remain relatively stable but are not sufficiently unique to distinguish people in a large population. There has been considerable research on facial recognition, but faces vary depending on expression and are too easy to alter and disguise. Voice identification is desirable for remote access applications; however, a person's voice varies with emotion, age, and health, so this approach has not reached the application stage. In some systems, several identification methods are used in combination with fingerprinting.

In the Connecticut welfare program, for example, ID cards contain a photograph and signature as well as an encoded fingerprint.

Global Biometrics Market: Recent reports estimates that the global biometrics market grew from $1.95 billion to $2.7 billion between 2006 and 2008, a 21.3 percent increase. A further projected annual growth rate of 21.3 percent would bring the annual revenue to $7.1 billion by 2012. The fingerprint market alone is projected to grow from $427.4 million in 2004 to $6.3 billion in 2012. This growth rate implies recognition of the importance of biometric security systems.

CONCLUSION

Biometrics is a unique identity management approach that offers the combination of user convenience, cost-effective provisioning and a non-repudiated compliance audit trail for the system operator.

Biometrics-based authentication clearly has advantages over these mechanisms, but there are also vulnerabilities that need to be addressed. No biometric trait can be applied universally, it may be a good choice for a given application, but unfeasible in another.

The fingerprint system would provide higher level of security, non-repudiated identification for internal control and regulatory compliance, and increased user convenience and productivity without the costs associated with physical credentials. A properly designed and implemented fingerprint biometric system is a viable way to accomplish all the objectives.

ACKNOWLEDGEMENT

First and the foremost our gratitude to Prof. K.V. Prabhakara, Principal, and SBRR Mahajana First Grade College for his constant encouragement, support and for the research grants for this minor project.

We extend our gratitude to Dr. Shankar. P. Hosmani, Professor and Head, Biotechnology also the convener for the Research Cell, SBRR Mahajana First grade College for his guidance, and timely help rendered during the course of the project work.

We wish to record our thanks to Mr. Mohammed Imran, Research scholar, DOS in Computer Science, Manasagangothri, Mysore, for his technical suggestions during our work.

Finally we thank one and all who have directly and indirectly assisted us during the course of this project work.

REFERENCES

1. Anil K. Jain, *Fellow, IEEE*, Arun Ross, *Member, IEEE*, and Salil Prabhakar, *Member, IEEE,* 2004,An Introduction to Biometric Recognition.
2. Chris Roberts November 2005 – Biometrics
3. Debnath Bhattacharyya, Rahul Ranjan1, Farkhod Alisherov A.2, and Minkyu Choi3. Biometric Authentication: A Review- International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009
4. Eric J. Lerner February 2000: Biometric Identification © American Institute of Physics
5. Golfarelli M., D. Maio, and D. Maltoni, July 1997 On the error-reject tradeoff in biometric verification systems, *IEEE Trans. Pattern Anal. Machine Intell.* vol. 19, pp. 786

796Http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20Disadvantages%20of%20technologies

6. Karine Pellerin , 2004, Increasing Accuracy in Multimodal Biometric Systems
7. Maio D, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, 2002: Fingerprint verification competition," in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Quebec City, QC, Canada, Aug. 2002, pp. 744–747.
8. Philips P. J., P. Grother, R. J.Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone. 2002: Overview and Summary. [Online]. Available: http://www.frvt.org /FRVT2002/documents.htm
9. Ross A., K.Nandakumar, and A.K. Jain, 2006 Handbook of Multi biometrics, Springer-Verlag edition.
10. Wayman J. L., 2001, Fundamentals of biometric authentication technologies, Int. *J.* Image Graphics.
11. Voice Biometrics as a Natural and Cost-Effective Method of Authentication Zivbarzilay, CTO and Founder, cellmax Systems Ltd.
12. Zhang D and W. Shu, , 1999 "Two novel characteristic in palm print verification: Datum point invariance and line feature matching," *Pattern Recognition.*, vol. 32, no. 4, pp. 691– 702.