A Review on Various Fusion Techniques in Multimodal Biometrics

Dr. M. N. Nachappa
Associate Professor,
Department of Computer Science,
St. Joseph's College (Autonomous),
Langford Road, Shanthinagar,
Bangalore – 560027, India.

A. M. Bojamma
Assistant Professor,
Department of Computer Science,
St. Joseph's College (Autonomous),
Langford Road, Shanthinagar,
Bangalore – 560027, India.

M. C. Aparna
Department of Computer Science,
St. Joseph's College (Autonomous),
Langford Road, Shanthinagar,
Bangalore – 560027, India.

***Abstract*-- Biometrics as the name suggests it is the study of personal identity verification in order to prove or test whether the respected person has been admitted to access the particular confidential system or not. Unimodal biometric systems use the method of authentication by using one biometric modality which leads in a couple of disadvantages like noisy data which is a scar on the finger print, change of voice due to other effects can lead to error in verification. Intra –class variation which means the biometric trait received from a person during enrollment can be different from the sample taken during the verification phase thus causing the difference in matching. Spoof attacks is nothing but biometric traits like signature or voice can be attacked by an intruder which can sometimes be very easy for the attacker thus causing low level security to the system. Unacceptable error rates, this happens mainly due to the distinctiveness. Human faces can be different in most of the cases but in some cases it can be similar thus causing high matching errors. The same happens in voice recognition too. Non universality where every user is expected to agree for a single type of biometric traits, whereas in some cases like finger print verification there are chances of ridges not being prominent thus creating a cause for an error in inappropriate enrollment.[4]**

These limitations can be resolved to a certain extent by using the Multimodal Biometric system. The major purpose of this study is to understand the concept of biometrics and also the concept of modal biometrics and the possible ways to use multimodal biometrics for the verification purposes which will lead us to less number of errors.

I. INTRODUCTION

Controlling access to prohibited areas and protecting important government and civilian properties are among the main activities of national and international security organizations. Usually, person authentication for access control to a prohibited area or for identification in different networks or social services scenarios (e.g., banking, welfare disbursement) is done using biometric systems.

Traditional authentication systems are based on "Data of information you have "example Password or "Data or information that you know "example Personal Identification Number (PIN) whereas biometrics deal with "What you are? No one else can steal it from you" [1]. A biometric system is defined as "a system which automatically distinguishes and recognizes a person as individual and unique through a combination of hardware and pattern recognition algorithms based on certain physiological or behavioural characteristics that are inherent to that person"

Some forms of behavioral *biometric identification* include the following:

1. Keystroke or Typing Recognition
2. Speaker identification or Recognition

Some forms of *physical* biometric identification include the following:

1. Iris
2. Voice
3. Retina
4. Fingerprint
5. Hand Geometry
6. Finger Geometry
7. Facial Proportions
8. Signature/Handwriting

II. TRIATS IN BIOMETRIC SYSTEMS

Traits in biometric system is nothing but the parts of the human body which is unique and can be used an identification tool, like the ones below:

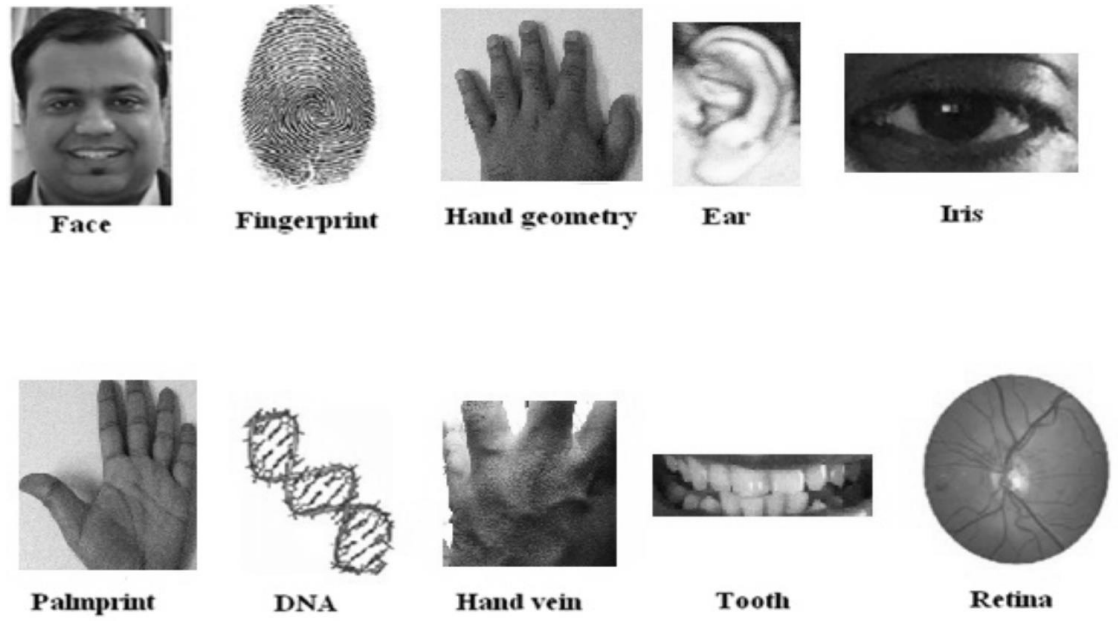


Figure 1:Traits in biometric systems

III. MULTIMODAL BIOMETRICS

The term "multimodal" means combining two or more modals in order to verify or authenticate. The modals are sensed by different sensors. There is also a possibility of combining two different properties of the same modal [2].In orthogonal biometrics different biometric modalities are involved.

Multimodal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. For example, a system combining face and iris characteristics for biometric recognition would be considered a "multimodal" system regardless of whether face and iris images were captured by different or same imaging devices. It is not required that the various measures be mathematically combined in anyway. For example, a system with fingerprint and face recognition would be considered "multimodal" even if the "OR" rule was being applied, allowing users to be verified using either of the modalities.

Multimodal biometric systems are designed to operate in one of the five integration scenarios as below [3]:

- **Multiple Sensors –** The information obtained from different sensors for the same biometric are combined.
- **Multiple Biometric –** Multiple characteristics such as iris and fingerprint are combined. These systems will contain more than one sensor with each sensor sensing different biometric characteristics.
- **Multiple Units of the Same Biometric –** Fingerprints from two or more fingers of a person may be combined or one image each of the same person may be combined.
- **Multiple Snapshots of the Same Biometric -** More than one instance of the same biometric is used for the enrolment and recognition, which includes multiple impression of the same finger, multiple samples of a voice can be combined.
- **Multiple Representations and Matching Algorithms for the same biometrics –** Combining different approaches to feature extraction and matching of the biometric characteristics.
- **Multiple modals of the biometric**-The different samples of the iris, fingerprint, face and voice recognition can be combined.

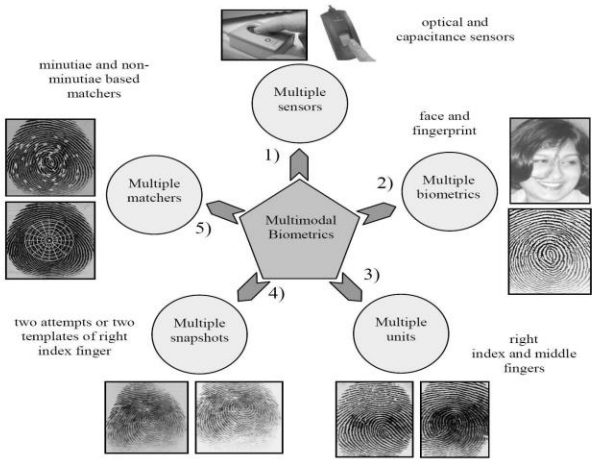


Figure 2: Scenarios of a multimodal biometric system [5].

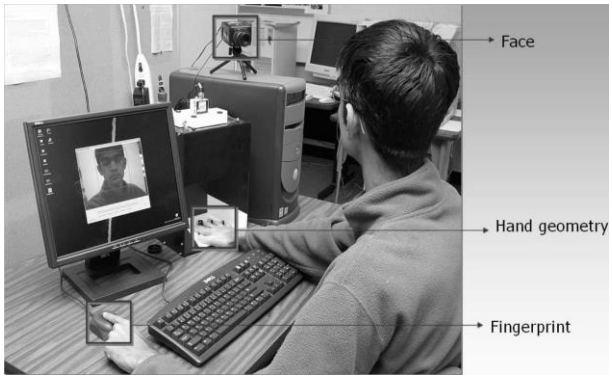


Figure 3: Typical prototype of multimodal biometric system.

IV DIFFERENT LEVELS OF FUSION IN MULTIMODAL BIOMETRIC SYSTEMS:

Since we use more than a single biometric modality, we need more than one decision channels. In order to join two or more biometric traits a method called as "fusion" is used. The design process that can combine the classified results from every biometric channel is called as a biometric fusion.

Multimodal biometric fusion is done in order to combine the different biometric samples in a better way in order to enhance the strength and also to reduce the error rates which occur during the verification process.
In this section we present different scenarios of fusion used in the multimodal biometrics.
It is worth nothing that the multimodality does not involve the use of multiple biometric modalities in the strict sense of the term, but its meaning is broader defined in the following by the various scenarios of fusion .
Biometric features which are suited to fusion: [5]

1) Iris, Face
2) Ear form, Voice
3) Fingerprint, Face
4) Voice, Hand geometry
5) Voice, Lips movement
6) Facial thermo gram, Face
7) Fingerprint, Face, Voice
8) Palm print, Hand geometry
9) Voice, Face, Lips movement
10) Fingerprint, Face, Hand geometry
11) Fingerprint, Voice, Hand geometry

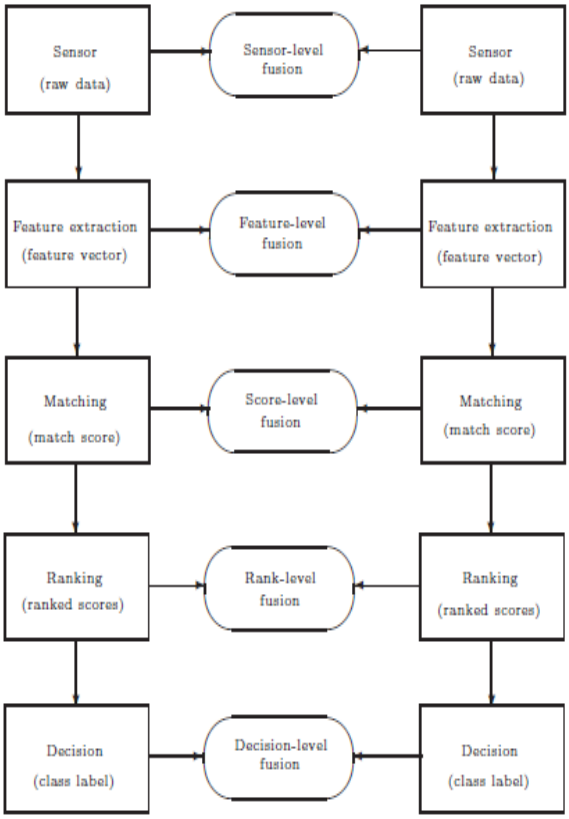


Figure 4: Levels of fusion.

V MULTIMODAL BIOMETRICS WITH VARIOUS LEVELS OF FUSION :

According to[A.K.Jain], "Information fusion can be defined as an information process that associates, correlates and combines data and information from single or multiple sensors or sources to achieve refined estimates of parameters, characteristics, events and behaviours".

A good information fusion method allows minimizing the influence of unreliable sources compared the better reliable ones. Since, multimodal biometric systems rely on the evidence presented by multiple sources of biometric information, information fusion is essential for analysis, indexing and retrieval of such information. There are numbers of fusion techniques for any particular information. Choosing appropriate fusion techniques for any specific information depends on the necessity of the application and the performance of the fusion techniques proven by previous research.

Fusion before matching category contains sensor level fusion and feature level fusion, while fusion after matching contains match score level fusion, rank level fusion and decision level fusion.

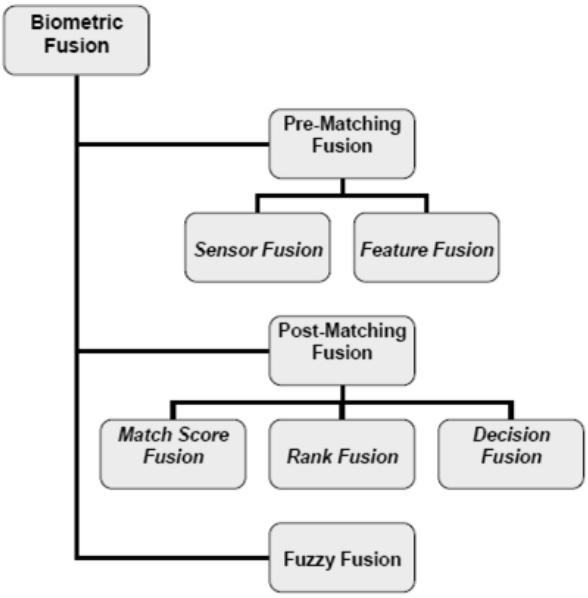
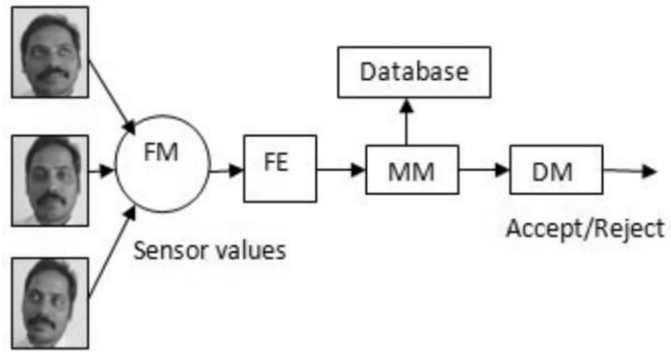


Fig 5: Biometric fusion classification

1. Sensor level:

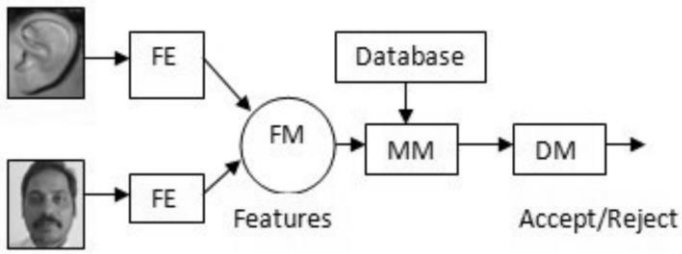
It is defined as "The consolidation of evidence presented by multiple sources of raw data before they are subjected to feature extraction" It is a type of fusion where it combines biometric traits from different sensors in order to provide an accurate result. It uses direct combination of images for fusion. For example authors combined multiple instances of faces captured using a single camera by mosaicking method to obtain better recognition performance. The raw data, acquired from sensing the same biometric characteristic with two or more sensors, is combined. An example of the sensor fusion level is sensing a speech signal simultaneously with two different microphones. Sensing a speech signal concurrently with two various microphones may be fused and then be subjected to feature extraction and matching. The raw data obtained from multiple sensors can be practiced and merged to generate new biometric data from which trait can be extracted. Biometric traits from different sensors like fingerprint, video camera, iris scanner, digital signature etc, are fused to form biometric trait for processing.



Sensor Level Fusion

2. Feature level Fusion:

The feature sets are extracted from different biometric channels can be fused using specific fusion algorithm to form a composite feature set. The feature collections of different modalities agree to extract a minimal feature set from the high-dimensional feature vector. The feature vectors extracted from the face and ear modalities can be fused is an example of multimodal system. The feature level fusion is the extraction of correlated feature from the different modalities and in course identifies a prominent set of features that can improve recognition accuracy. The feature level fusion is likely to achieve superior result in comparison with score level and decision level fusion can be applied to the extraction of different features from the same modality or different multimodalities. An example of a unimodal system is the fusion of instantaneous and transitional spectral information for speaker recognition. On the other hand, concatenating the feature vectors extracted from face and fingerprint modalities are an example of a multimodal system. It is stated that fusion at the feature level is expected to perform better in comparison with fusion at the score level and decision level. The main reason is that the feature level contains richer information about the raw biometric data. However, such a fusion type is not always feasible. For example, in many cases the given features might not be compatible due to differences in the nature of modalities. Also such concatenation may lead to a feature vector with a very high dimensionality. This increases the computational load. It is reported that a significantly more complex classifier design might be needed to operate on the concatenated data set at the feature level space.



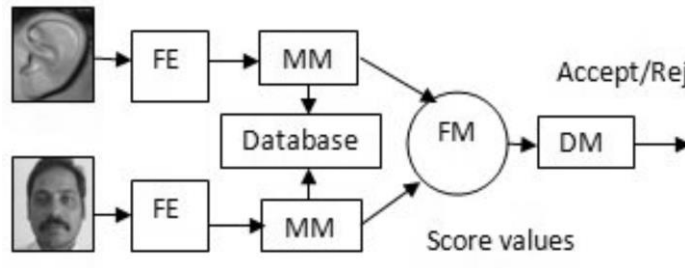
Feature level fusion

3. Matching score level fusion:

Rather than combining the feature vector, we process them separately and individual matching score is found, then depending on the accuracy of each biometric matching score which will be used for classification. As different matching scores from different algorithms may not share the same underlying properties or the score range, score normalization is necessary in match score level fusion methods. Min-max, decimal scaling, z-score, median absolute deviation, double sigmoid, tanh-estimator; median are some examples of score normalization technique. Such scores are obtained, for example, on the basis of the proximity of feature vectors to their corresponding reference material .The overall score is then sent to the decision module. Currently, this appears to be the most

useful fusion levels because of its good performance and simplicity this fusion level can be divided into two categories: combination and classification. In the former approach, a scalar fused score is obtained by normalizing the input matching scores into the same range and then combining such normalized scores. In the latter approach, the input matching scores are considered as input features for a second level pattern classification problem between the two classes of client and the Impostor.

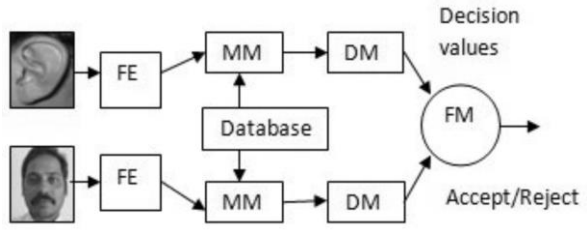
Feature vectors are generated separately for each modality. Extracted feature vectors compared with the templates residing in the database individually for each biometric trait to generate match scores. Depending on the accuracy of each biometric channel, output set of match scores which are fused to create composite matching score. As an example, face and hand modalities match score may be combined by the use of simple sum rule in order to obtain a new match score which is then sent to the decision module.



Match score level fusion

4. Decision level fusion:

Each modality is first pre-classified independently. Decision level fusion method consolidates the final decision of single biometric matchers to form a consolidated decision. When each matcher outputs its own class label (i.e., accept or reject in a verification system, or the identity of a user in an identification system), a single class label can be obtained by employing techniques, such as, "AND"/"OR", majority voting, weighted majority voting, decision table, Bayesian decision and Dempster-Shafer theory of evidence. Many biometric systems can only output the final decision, thus decision level fusion is very appropriate for those biometric systems. The available information for this fusion method is binary (yes/no in most cases), which allows very simple operations for fusion.

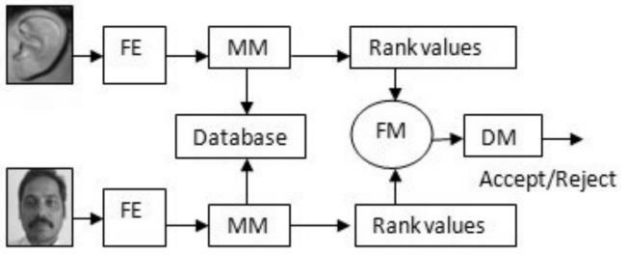


Decision level fusion

5. Rank level fusion:

It is nothing but the combination of multiple ranking lists which helps in the establishment of the final decision. Sometimes, only the final ranked outputs from a biometric system are available. Furthermore, in some biometric systems, the matching scores from the matchers are not suitable for fusion. Thus rank level fusion is a feasible solution in such systems. This type of fusion is relevant in identification systems where each classifier associates a rank with every enrolled identity. Rank level fusion method, however is a relatively new approach compared to others and still remains understudied. Very limited research has been conducted on fusion at this level which has the potential of efficiently consolidating rank information in multimodal biometric identification system.Rank level fusion consolidates multiple ranking lists obtained from several biometric matchers to form a final ranking list which would aid in establishing the final decision. This type of fusion is relevant in identification systems where each classifier associates a rank with every enrolled identity. Techniques such as Borda count may be used to make the final decision. Among the available fusion methods, pre-matching fusion approaches, such as sensor level fusion and feature level fusion methods have not been used extensively due to limited access to the information. Match score level fusion methods are very popular with developers and also has been extensively investigated by biometric researchers as some of the earlier methods. But match score fusion approach needs normalization of the outcomes of unimodal matchers which is computationally extensive. Moreover inappropriate choice of normalization technique can degrade the system performances. Decision level fusion approaches are too abstract and used primarily in the commercial biometric system where only the final outcomes are available for processing. Fuzzy logic based fusion is another impressive information fusion approach which has been successfully applied in many different applications for the past years, such as automatic target recognition, biomedical image fusion and segmentation, gas turbine power plants fusion, weather forecasting, aerial image retrieval and classification, vehicle detection and classification and path planning. Further, with the fuzzy logic based fusion, we can obtain the level of confidence for the final recognition outcome which can be very important in some security critical biometric applications. Rank level fusion is a new fusion approach where each classifier associates a rank with every enrolled identity.

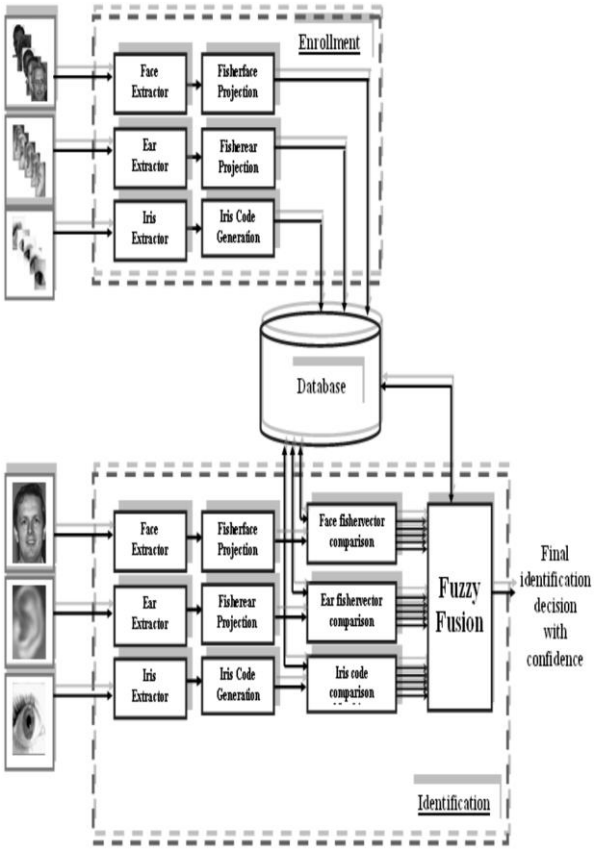
Fusion involves consolidating the rank output by individual biometric subsystems and determining a new rank that would support in establishing the final decision. However, these fusions have one weakness. In multimodal biometric, more different identities output from two or three matching modules which are designed to appear some identities of only one matcher. In this case, the rank level fusion shows the risk of wrong results [11].



Rank level fusion

6. Fuzzy fusion:

The fuzzy fusion method can be employed in both before matching or after matching stages. When this fusion method is applied in before matching stage, usually it is to reduce the size of the dataset for comparison or matching. This fusion can also be employed in after matching stage to increase the recognition performance and to obtain the level of confidence of the final outcomes.



VI PERFORMANCE METRICS FOR BIOMETRIC SYSTEM:

- **False acceptance rate or false match rate (FAR or FMR):** the probability that the system cannot match the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is an unauthorized template in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FAR.
- **False rejection rate or false non-match rate (FRR or FNMR):** the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
- **Receiver operating characteristic or relative operating characteristic (ROC):** The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FAR but increase the FRR. A common variation is the *Detection error trade-off (DET)*, which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- **Equal error rate or crossover error rate (EER or CER):** the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.
- **Failure to enroll rate (FTE or FER):** the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
- **Failure to capture rate (FTC):** Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- **Template capacity**: the maximum number of sets of data which can be stored in the system.

VII ISSUES AND CONCERNS:

A. Privacy and discrimination: It is possible that data obtained during biometric enrollment may be used in ways for which the enrolled individual has not agreed. For example, biometric security that utilizes an employee's DNA profile could also be used to screen for various genetic diseases or other 'unwanted' traits.

There are three categories of privacy concern:

1. Unintended functional scope: The authentication goes further than authentication, such as finding a defect in the person's profile such as tumor.
2. Unintended application scope: The authentication process correctly identifies the subject when the subject did not wish to be identified.
3. Covert identification: The subject is identified without seeking identification or authentication, i.e. a subject's face is identified in a crowd.

B. Danger to owners of secured items:

When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. For example, in 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car. [17]

C. Cancelable biometrics:

One advantage of passwords over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics.

If someone's face is compromised from a database, they cannot cancel or reissue it. Cancelable biometrics is a way in which to incorporate protection and the replacement features into biometrics. It was first proposed by Ratha et al. [18]
Several methods for generating new exclusive biometrics have been proposed. The first fingerprint-based cancelable biometric system was designed and developed by Tulyakov et al. essentially, cancelable biometrics perform a distortion of the biometric image or features before matching. The variability in the distortion parameters provides the cancelable nature of the scheme. Some of the proposed techniques operate using their own recognition engines, such as Teoh et al and Savvides et al. whereas other methods, such as Dabbah et al., take the advantage of the advancement of the well-established biometric research for their recognition front-end to conduct recognition. Although this increases the restrictions on the protection system, it makes the cancellable templates more accessible for available biometric technologies.

D. Soft biometrics:

Soft biometrics traits are physical, behavioural or adhered human characteristics, which have been derived from the way human beings normally distinguish their peers (e.g. height, gender, hair color). Those attributes have a low discriminating power, thus not capable of identification performance; additionally they are fully available to everyone which makes them privacy-safe.

E. International sharing of biometric data:

Many countries, including the United States, are planning to share biometric data with other nations.
In testimony before the US House Appropriations Committee, Subcommittee on Homeland Security on "biometric identification" in 2009, Kathleen Kraninger and Robert A Mocny commented on international cooperation and collaboration with respect to biometric data, as follows:

> *To ensure we can shut down terrorist networks before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defenses. Just as we are improving the way we collaborate within the U.S. Government to identify and weed out terrorists and other dangerous people, we have the same obligation to work with our partners abroad to prevent terrorists from making any move undetected. Biometrics provides a new way to bring terrorists' true identities to light, stripping them of their greatest advantage—remaining unknown.*

According to an article written in 2009 by S. Magnuson in the National Defense Magazine entitled "Defense Department under Pressure to Share Biometric Data" the United States has bi-lateral agreements with other nations aimed at sharing biometric data. To quote that article:

> *Miller [a consultant to the Office of Homeland Defense and America's security affairs] said the United States has bi-lateral agreements to share biometric data with about 25 countries. Every time a foreign leader has visited Washington during the last few years, the State Department has made sure they sign such an agreement.*

F. Governments are unlikely to disclose full capabilities of biometric deployments:

Certain members of the civilian community are worried about how biometric data is used but full disclosure may not be forthcoming. In particular, the Unclassified Report of the Defense Science Board Task Force on Defense Biometrics states that it is wise to protect, and sometimes even to disguise, the true and total extent of national capabilities in areas related directly to the conduct of security-related activities. This also potentially applies to Biometrics. It goes on to say that this is a classic feature of intelligence and military operations. In short, the goal is to preserve the security of 'sources and methods'.

Countries applying multimodal biometrics are :
Australia, Brazil, Canada, China, Gambia, Germany, India, Iraq, Israel, Italy, Netherlands, New Zealand, Norway, Ukraine, United Kingdom, and United States.

CONCLUSION

The results of this study show that multimodal biometrics is better than the unimodal biometrics. The error rates which occur in unimodal biometrics are way more than the multimodal biometrics. An additional advantage of multimodal biometrics is that the problem of wrong verification is less. Since every invention which has its own advantages will also be having its own disadvantages multimodal biometrics fall under the same category but the disadvantages of multimodal biometrics are not very dangerous to cause too much damage. Future scope is to investigate the different levels of fusion in detail and also compare the different levels to come up with the best fusion level by reviewing the biometric result based on different fusions.

IX REFERENCES

1. P. S. Sanjekar and j. B. Patil, an overview of multimodal biometrics, an international journal (sipij) vol.4, no.1, february 2013.
2. Prof. V. M. Mane and prof. (dr.) D. V. Jadhav, international journal of biometrics and bioinformatics (ijbb), volume 3, issue 5
3. feature level fusion of multimodal biometrics and two tier security in atm system international journal of computer applications (0975 – 8887) volume 70– no.14, may 2013
4. overview of multimodal biometrics v.sireesha, k.sandhyarani research scholar, professor: dept of computer science s.p.m.v.v, tirupati, andhra pradesh
5. Multimodal biometrics: an overview arun ross and anil k. Jain. Appeared in proc. Of 12th european signal processing conference (eusipco), (vienna, austria), pp. 1221-1224, september 2004.
6. Multimodal biometric systems overview ,eugen lupu petre g. Pop,technical university of cluj-napoca ,volume 49, number 3, 2008
7. a.k. jain and a. Ross, "learning user-specific parameters in a multibiometric system," proc. Ieee int'l conf. Image processing, pp. 57-60, sept. 2002.
8. a multimodal biometric system using fingerprint, face and speech. By anil jain ,ling hong and yathin kulkarni.
9. A. Ross and a.k. jain, "information fusion in biometrics," pattern recognition letters, vol. 24,no. 13, pp. 2115-2125, 2003.
10. Multimodal biometric systems:applications and usage scenarios, michael thieme, director of special projects, international biometric group ,biometric consortium conference 2003 ,arlington, va.
11. Review of multimodal biometrics: applications, challenges and research areas, prof. Vijay m. Mane , assistant professor ,department of electronics engineering, vishwakarma institute of technology, pune (india).
12. Multimodal biometric systems ,study to improve accuracy and performance, k.sasidhar1, vijaya l kakulapati2, kolikipogu ramakrishna3 & k.kailasarao4
13. Multimodal biometrics: an overview and some recent developments kar-ann tohbiometrics engineering research center school of electrical & electronic engineering ,yonsei university, seoul, korea
14. score level fusion based multimodal biometric identification fingerprint & voice, youssef elmir ,leesi laboratory ,computer science dept. Ahmed draia african university
15. A. K. Jain, a. Ross and s. Prabhakar, "an introduction to biometric recognition". Ieee transactions on circuits and systems for video technology, vol. 14, pp. 4–20, jan, 2004.
16. A.k. jain, a. Ross, "multibiometric systems". Communications of the acm, vol. 47, pp. 34-40, 2004. Australia, brazil, canada, china, gambia, germany, india, iraq, i srael, italy, netherlands, new zealand, norway, ukraine, united kingdom, and united states.