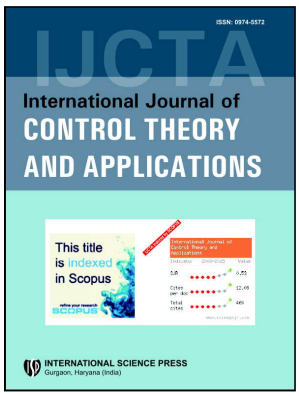

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 6 • 2017

Performance Analysis of Uni-modal and Multimodal Biometric System

Suneet Narula Garg[1], Renu Vig[2] and Savita Gupta[3]

1 Department of Electronics and Communication Engineering UIET,Punjab University, Chandigarh,Punjab, India, Email: suneetgarg1979@gmail.com
2 Department of Electronics and Communication Engineering UIET,Punjab University, Chandigarh, Punjab, India, Email: renuvig@hotmail.com
3 Department of Computer Science and Engineering UIET, Punjab University, Chandigarh, Punjab, India, Email: savita2k8@yahoo.com

Abstract: Now a day's Biometrics is the most acceptable to identify any person. It is an authentication technique which place confidence in measurable individual and physiological characteristics that will be mechanically verified. A biometric system could operate either in identification mode or verification mode. Because the level of security breaches and dealings fraud have increased, the necessity of technologies for extremely secure identification and private verification is changing into apparent. Due to some limitations of unimodal biometric system, multimodal biometrics has been introduced where fusion of the modalities is the bigger challenge. In Multimodal Biometrics, Fusion can be performed on different levels. In this paper, the performance of uni-modal and Multimodal biometric system has been compared. In this work, Iris and fingerprint modalities been used and performance analysis is done on the basis of False Acceptance rate(FAR),False Rejection Rate (FRR) and Recognition Accuracy.

Keywords: Biometrics, Multimodal, Fingerprint, Iris, Fusion.

1. INTRODUCTION

Verification is required when it is important to know whether a man is who they claim to be. It is a technique that includes a man making a case about their personality, and afterward giving confirmation to demonstrate it. This study concentrates on the underlying verification technique that most PC clients are usual to performing when they sign onto a PC framework. For a PC framework the fundamental starting insurance is thought to be confirmation process. It consequently makes sense that this system ought to be made as exact and solid as attainably conceivable. Biometrics alludes an innovation to confirm people via computerized implies that depend on anatomical or behavioral human attributes. Biometric frameworks can possibly do the general population confirmation with a high level of certification. In certifiable application the majority of the sent biometric framework for validation depends on the single wellspring of data (e.g. face, unique mark, voice and so forth.). These frameworks are defenseless against assortment of issues, for example, boisterous information, intra-class varieties, between class similitude, non-

comprehensiveness and ridiculing. It prompts significantly high False Acceptance Rate (FAR) and False Rejection Rate (FRR), constrained separation capacity, upper bound in execution and absence of perpetual quality. For distinguishing proof utilizing different wellspring of data can help in conquering the impediment which comes in uni-modular biometric framework. These frameworks permit the mix of two or more sorts of biometric frameworks known as multimodal biometric frameworks. These frameworks are more dependable because of the nearness of different, autonomous biometrics reliable due to the presence of multiple, independent biometrics. For the increase in accuracy for the process of decision making complimentary information can be provided by the fusion of multiple modalities. For example , for detecting events form a team sports video it can be effective by adding some additional textual information with the fusion of audio and visual features, rather than using single medium. Though with use of multimodal fusion it give efficient results but still there is raise in cost and complexity. While using fusion multiple modalities the first basic step is to select what strategy is be followed. The most considered strategy is known as early fusion i.e. fusing the information at the feature level. Other ways is late fusion or decision level fusion that fuses the information at semantic space. Together these two ways are used as hybrid fusion approach.

1.1. uni-modal Biometric System

The uni-modular biometric utilizes single biometric quality (either physical or conduct characteristic) to distinguish the client Physiological biometrics identifiers incorporate fingerprints, hand geometry, eye designs, ear designs, facial components, and so forth... Behavioral identifiers incorporate voice, signature, writing designs and so forth. While perceiving a man's component, there are chances for the framework to choose a honest to goodness individual as a faker or a sham as a genuine[1].

1.2. Need of Multimodal Biometrics

Numerous biometric frameworks set up so far in various applications, which depend on the proof of single wellspring of data for validation (e.g. unique mark, face, voice and so on.) are uni-modular. These frameworks are perilous because of the event of assortment of issues, for example, uproarious information, intra-class varieties, between class likenesses, non-comprehensiveness and parodying as it prompts constrained separation capacity, upper bound in execution and absence of steadiness. For building up character couple of impediments showed by uni-modular biometric frameworks can be overcome by involving different wellsprings of data. Two or more sorts of biometric frameworks called multimodal biometric frameworks are permitted to incorporate. There unwavering quality relies on upon the nearness of various, autonomous biometrics.

Data and the effectiveness of the general basic leadership procedure can be improved by the combination of different modalities .e.g. effectiveness of distinguishing occasions from a group activities video has just ended up conceivable by combination of varying media highlights alongside other literary information [2] . Multimodal combination is valuable however with a specific expense and trouble in the examination procedure.

1.3. Multimodal Biometric System

To decide a man's confirmation two or more components of a man to be perceived together are consolidated in a multimodal biometric framework. To enhance populace scope, stopping parody assaults, expanding the degrees of opportunity, and diminishing the inability to-enlist rate, Multi modular biometric frameworks can prominently enhance the acknowledgment execution . The interest of uni-modular biometric framework can be lower than that of the capacity prerequisites, preparing time, and computational requests of a multimodal biometric framework .Advantages displayed by the multimodal biometric framework are more than that of the uni-modal biometric framework and these are:

- As compared to that of unimodal system, multimodal biometric system obtains more than one type of information and it also provides a substantial improvement in the matching accuracy. By satisfying a

wide population of users, Multimodal biometric systems are able to address the non universality issue. User can enter into a system by using another valid biometric trait .If he doesn't have a single valid biometric trait still. Perhaps only a subset of acquired traits is requested for verification and also a certain degree of flexibility can be obtained by enrolling the user by acquiring his multiple traits[3].

- It is very difficult to hoax the legitimate user enrolled in multimodal biometric system as they are less delicate to imposter attacks.
- When information acquired from the single biometric trait is falsified by noise , another trait of the same user can be used to perform the verification as Multimodal biometric systems are insensitive to the noise on the sensed data.
- When a single biometric trait is not enough in continuous monitoring or tracking the person in situation these systems can prove helpful e.g. tracking a person using face and gait simultaneously[4].

2. SYSTEM DESIGN AND ANALYSIS

2.1. Image dataset

This model spotlights on enhancing the effectiveness of the framework and is actualized for all intents and purposes utilizing MATLAB 7.11.0 environment. A database of 100 specimens of both iris and unique mark comprising of Test set and Training sets are utilized. From the 50 known persons preparing set comprise of test of 100 iris and unique finger impression. Each individual contributes two specimens. Test set comprise of test of 100 iris and unique mark comprising of 50forged and 50 authentic specimens. The acquired result has diminished the FRR and additionally FAR and there is expansion in execution of the framework. There is an expansion in the precision of the multimodal biometric of a Training Set and Test Set is utilized. Preparing Set comprises of 50 honest to goodness tests from IITD database. Every Person contributes 2 tests.

2.2. Basic Block Design

For creating tests a multimodal biometric framework constitutes of iris and unique finger impression obtaining gadget. Straightforward framework engineering is picked as appeared in Figure 1 where both surges of information utilizing demonstrating apparatuses and highlight extraction are displayed autonomously. The element vectors are then perceived utilizing grouping technique and choice can be framed utilizing choice level combination.

2.3. Algorithm Level Design

The algorithm design involves:

- Data Acquisition
- Feature Extraction
- Recognition(Iris and Fingerprint)
- Decision Level Fusion

Results are discussed in this work.

3. IRIS RECOGNITION SYSTEM

It is a generally new branch of biometric acceptance. The human iris is the annular part amongst understudy and sclera. It has unmistakable component, for example, spots, crowns, stripes, wrinkles et cetera. Iris recognition favored as a result of the accompanying reasons:

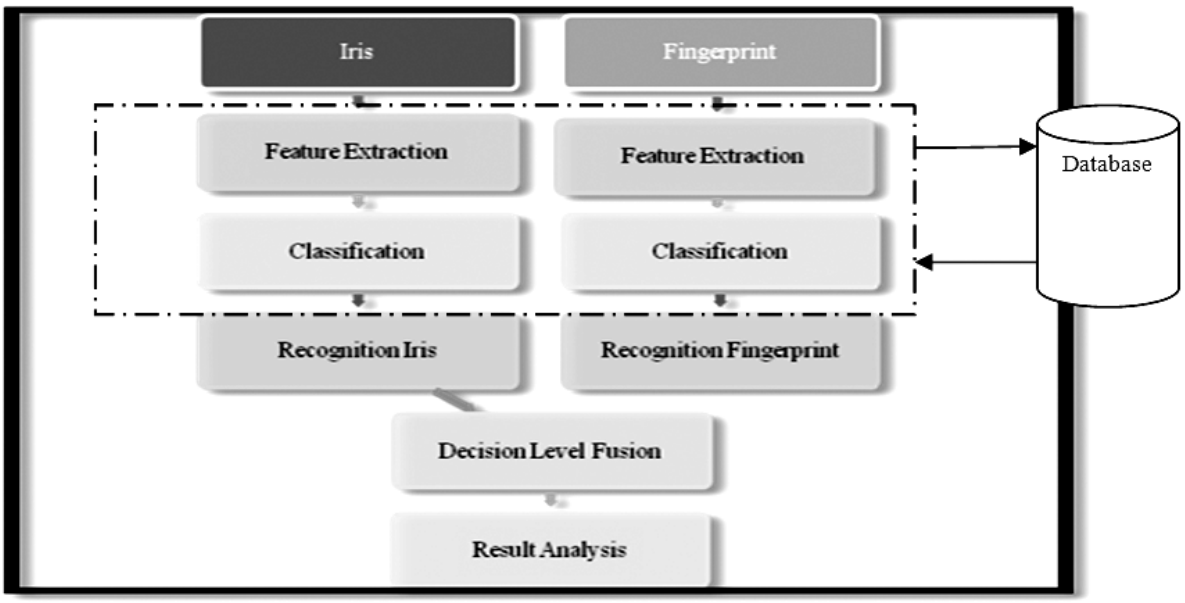

Figure 1: Basic Design of Multimodal Biometric System

Uniqueness: The likelihood of two persons' irises being the same is lower than $10^{"35}$. Despite the fact that they are twins, their irises are entirely distinctive. This is the motivation behind why we utilize iris to perceive individual identity [8].

Reliability: iris is an internal organ in our eyes and ensured by eyelid, lash and cornea. Not at all like finger and palm, it is from time to time hurt and the blunder of acknowledgment brought on by scar will never happen. In this sense, iris acknowledgment is greatly improved than unique finger impression and palm-print recognition[11].

Real strides of iris recognition are given after:

Segmentation: A method is required to disconnect and prohibit the antiquities and in addition finding the round iris area. The inward and the external limits of the iris are ascertained.

Normalization: Iris of various individuals might be caught in various size, for the same individual additionally size may change in light of the variety in brightening and different variables. This procedure will produce iris areas having same steady measurements so that under the diverse conditions the two photo of same iris will have Characteristic components at the same spatial area.

Feature extraction: For making the examination between the formats, from the iris critical element must be encoded. For making biometric layout numerous iris acknowledgment framework use band pass disintegration of iris pictures. Iris gives rich composition data. a component vector is framed which comprises of the requested grouping of elements separated from the different representation of the iris pictures.

Matching of an Image: To confirm by means of recognizable proof (one-to-numerous layout coordinating) or (balanced format coordinating), a layout made by imaging the iris is contrasted with a put away esteem format in a database. A positive distinguishing proof is exact just If the Hamming separation is beneath the choice limit, e.g. a hamming separation would bring about an exact match.

Localization: In the entire iris acknowledgment framework, Iris confinement is a vital stride. Exact result can be acquired just when one section iris accurately from the first iris picture. Iris confinement can be characterized as a way to distinguish the area of iris' inward and external limits.

Figure 2 shows the basic design of the Iris Recognition System prepared in MATLAB. This Iris recognition System is based on canny based method. Here first Training Sample is selected & prepare template of these sample. Here Image sample is segmented & then features can be extracted by using canny based methods. This template is matched with the testing sample. If both samples matched gets a message 'image matched' as shown in Figure 3.

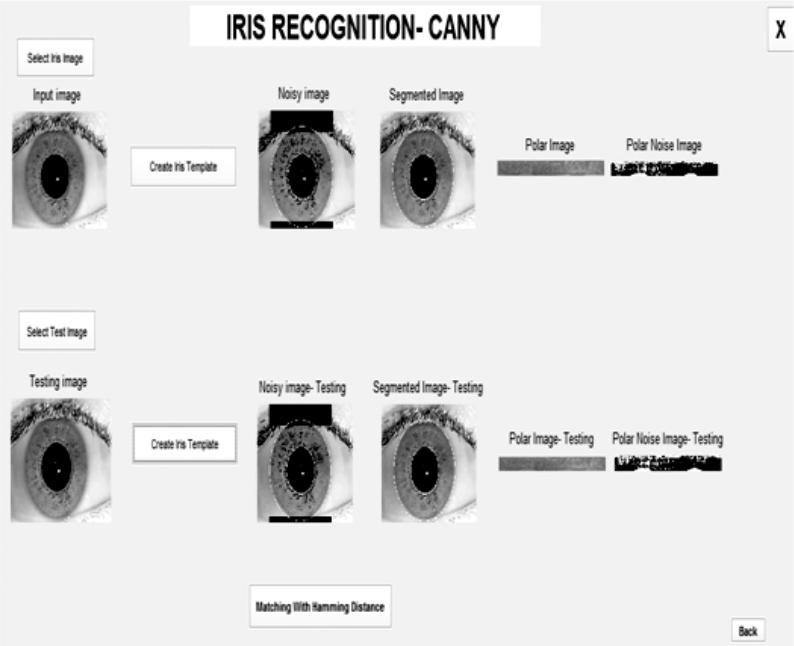

Figure 2: Iris Recognition System

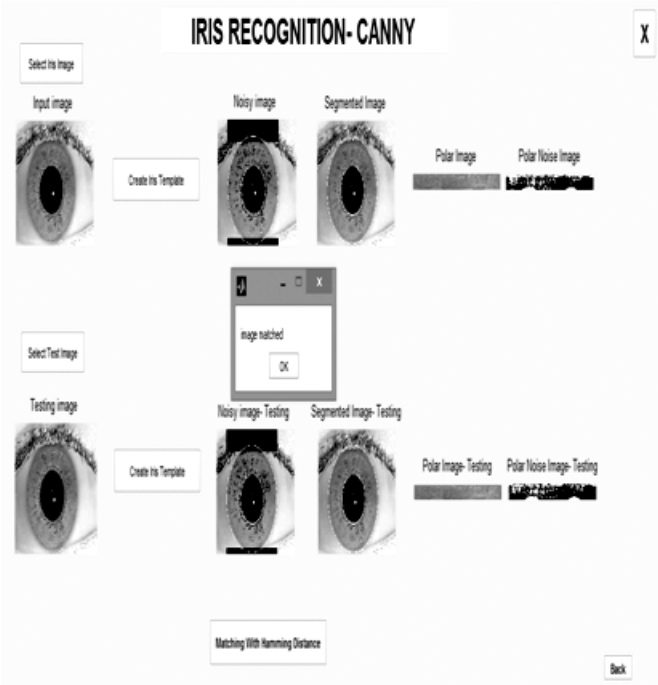

Figure 3 : Testing Phase of Iris Recognition System

4. FINGERPRINT RECOGNITION

One of the most publicized and well known biometrics is fingerprint identification. Due to their consistency and uniqueness over the time for identification purpose fingerprints are used over the century, and due to enhancement in computing capabilities it has become more automated. Due to inherent ease in acquisition fingerprint identification have become popular as for collection there are many source (ten fingers) available and their established use and collections by law enforcement and immigration [13].

4.1. Fingerprint patterns: Basic patterns

The three essential examples of unique mark edges are the curve, the circle, and the whorl. A curve is an example where the edge enters one side of the finger, then ascents in the inside framing a curve, and exits on the opposite side of the finger. With a circle the edge enters one side of the finger, then structures a bend, and exits on the same side of the finger from which it entered. Circles are the most widely recognized example in fingerprints. At last a whorl is the example you have when edges frame circularly around a focal point[10].

4.2. Minutiae highlights

Particulars allude to particular focuses in a unique mark, these are the little subtle elements in a finger impression that are most essential for finger impression acknowledgment. There are three noteworthy sorts of details elements: the edge finishing, the bifurcation, and the dab (likewise called short edge). The edge closure is, as demonstrated by the name, the spot where an edge closes. A bifurcation is the spot where an edge parts into two edges. Spots are those unique mark edges that are essentially shorter than different edges. Figure 4 shows the basic design of the Fingerprint Recognition System prepared in Matlab.

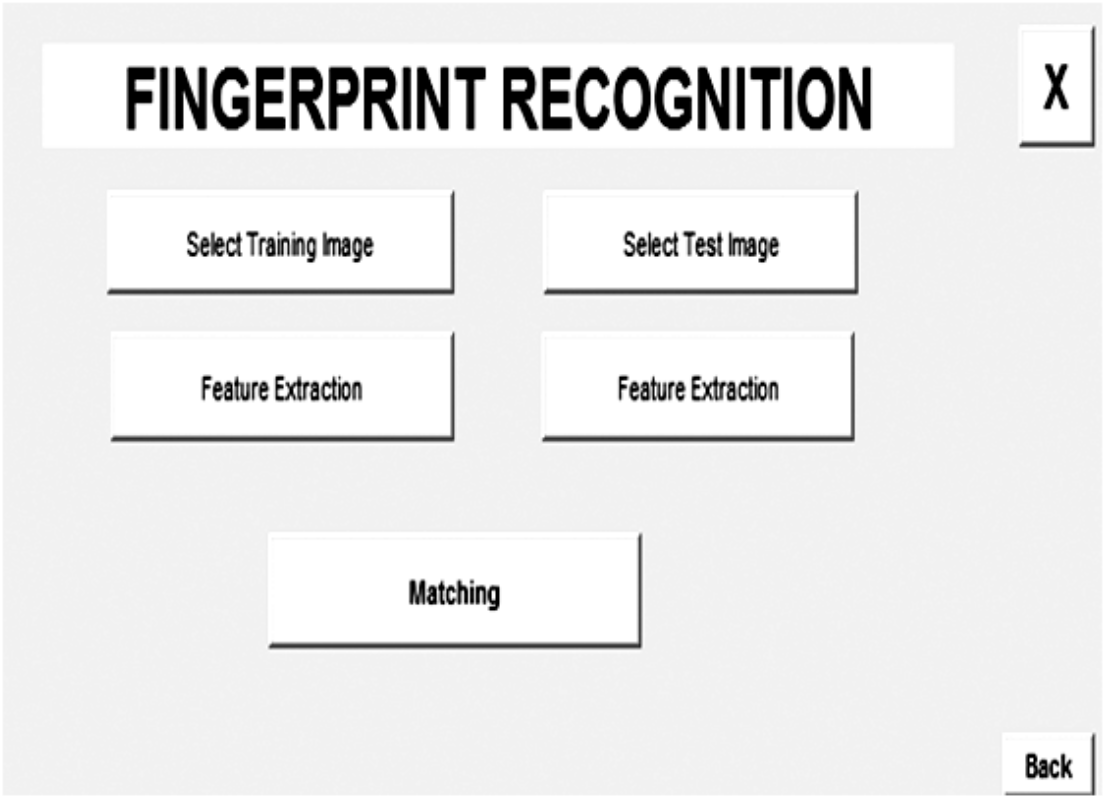

Figure 4: Fingerprint Recoginition System

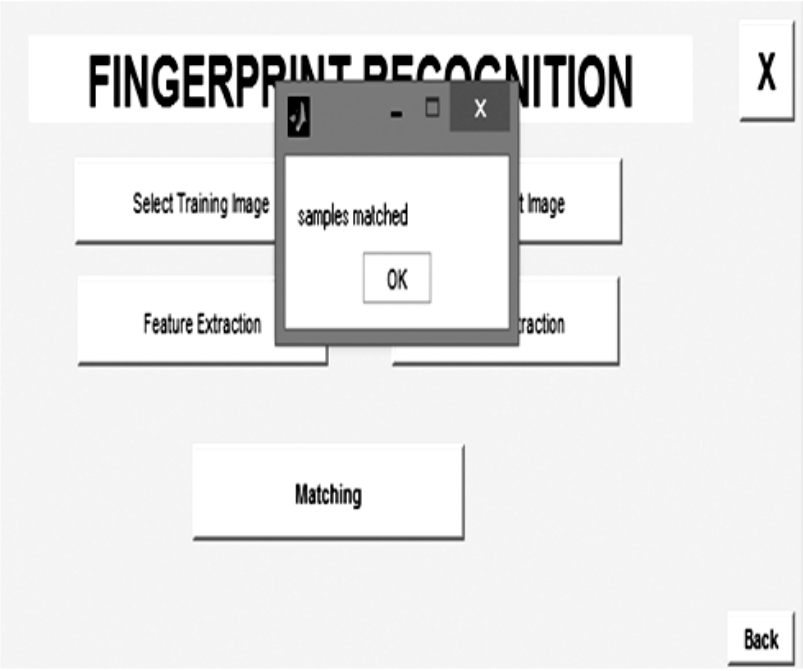

Figure 5: Testing Phase of Fingerprint Recognition

This Fingerprint recognition System is based on core point Detection method. Here first Training Sample is selected & then features can be extracted by detecting their core points. These features will be matched with the testing sample. If both samples matched gets a message 'sample matched' as shown in Figure 5.

5. IRIS AND FINGERPRINT BASED MULTIMODAL BIOMETRICS SYSTEM

Iris & Fingerprint traits are here combined together for the analysis of Multimodal Biometric System. This paper describes the architecture which uses wavelet & texture based feature extraction method.

This Multimodal Biometric System is for all intents and purposes executed utilizing MATLAB 7.11.0 environment. In this, a database of 100 Iris and Fingerprint tests comprising of a Training Set and Test Set is

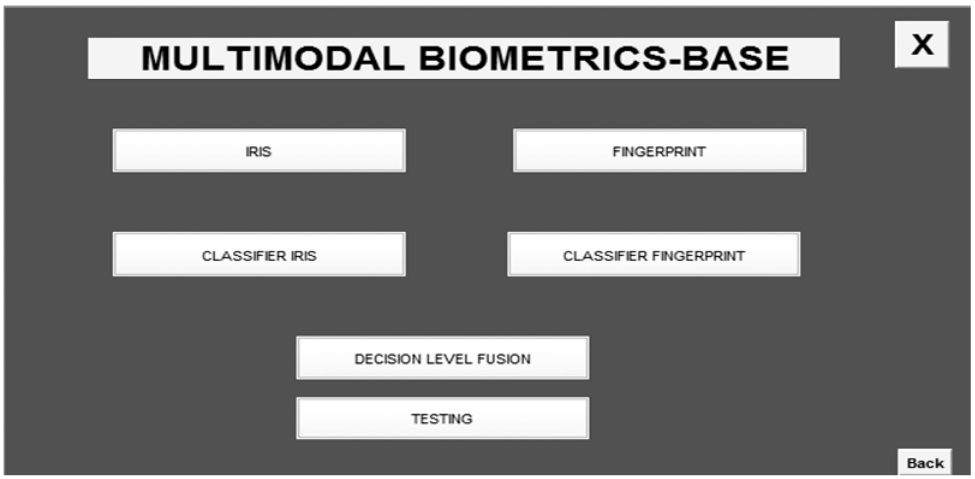

Figure 6: Multimodal Biometric System

utilized. Preparing Set comprises of 50 honest to goodness tests from IITD database. Every Person contributes 2 tests. Test Set comprises of 100 tests which comprise of 50 honest to goodness and 100manufactured examples. The result obtained has been measured by calculating FAR as well as FRR. This system uses two biometrics traits that are iris and fingerprints. For both traits, the process flow is as: first capture the biometric trait sample where no. of samples has been collected for both, preprocessing phase where each sample has been normalized and converted into gray scale as required and feature extraction using hybrid wavelets[15]. Here hybrid wavelets [12bp] are generated from Walsh and Kekre [2bp] transforms. The feature vector for the enrolled dataset in given to neural classifier. The decisions of the classifiers are then fused together using decision fusion[4][12][16].

5.1. Feature Extraction phase

Iris feature extraction: In this a feature extraction phase is a separate phase. Here first a sample feature has been selected it then converted into grey scale then perform localization and texture features has been extracted. The features values have been saved in .mat file ands extremes, centroid and area features has been extracted as shown in Figure 7.

Fingerprint feature extraction: In this a feature extraction phase is a separate phase. Here first a sample feature has been selected it then converted into grey scale then texture features has been extracted [17]. The features values have been saved in .mat file & extrema, centroid, perimeter, convex hull, maxima and minima features has been extracted as shown in figure 7.

Fingerprint feature extraction: In this a feature extraction phase is a separate phase. Here first a sample feature has been selected it then converted into grey scale then texture features has been extracted [18]. The features values have been saved in .mat file and extrema, centroid, perimeter, convex hull, maxima and minima features has been extracted as shown in Figure 8.

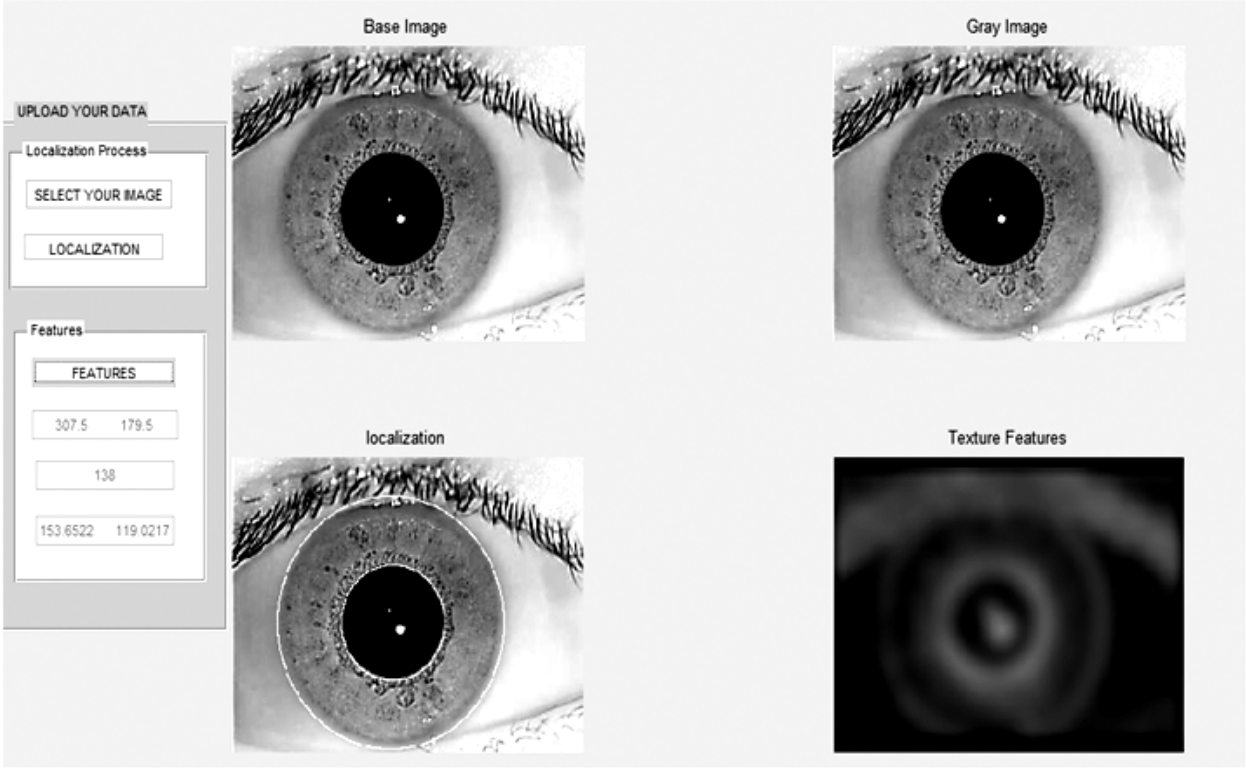

Figure 7: Iris Feature Extraction

6. RESULT ANALYSIS

Execution of the biometric frameworks is measured by their exactness in ID, which is ascertained utilizing false dismissal rate and false acknowledgment rate. As appeared in the Table 1, the Accuracy is figured utilizing all examples on the premise of false dismissal rate and false acknowledgment rate. Tests are keep running on the dataset of 50 clients. Exactness is computed for iris acknowledgment, unique finger impression acknowledgment and for both. Total Number of Samples in the database=100

6.1. False Acceptance Rate or False Match Rate (FAR or FMR)

The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

$$FAR = \frac{\text{Number of Samples that Falsely accepted}}{\text{Total Number of Samples} - \text{Number of Samples that Falsely accepted}} \times 100 \quad (1)$$

6.2. False Non-Match Rate or False Rejection Rate (FNMR or FRR)

The probability that the system fails to detect a match between the matching template in the database and input pattern. It measures the percent of valid inputs which are incorrectly rejected.

$$FRR = \frac{\text{Number of Samples that Falsely rejected}}{\text{Total Number of Samples} - \text{Number of Samples that Falsely rejected}} \times 100 \quad (2)$$

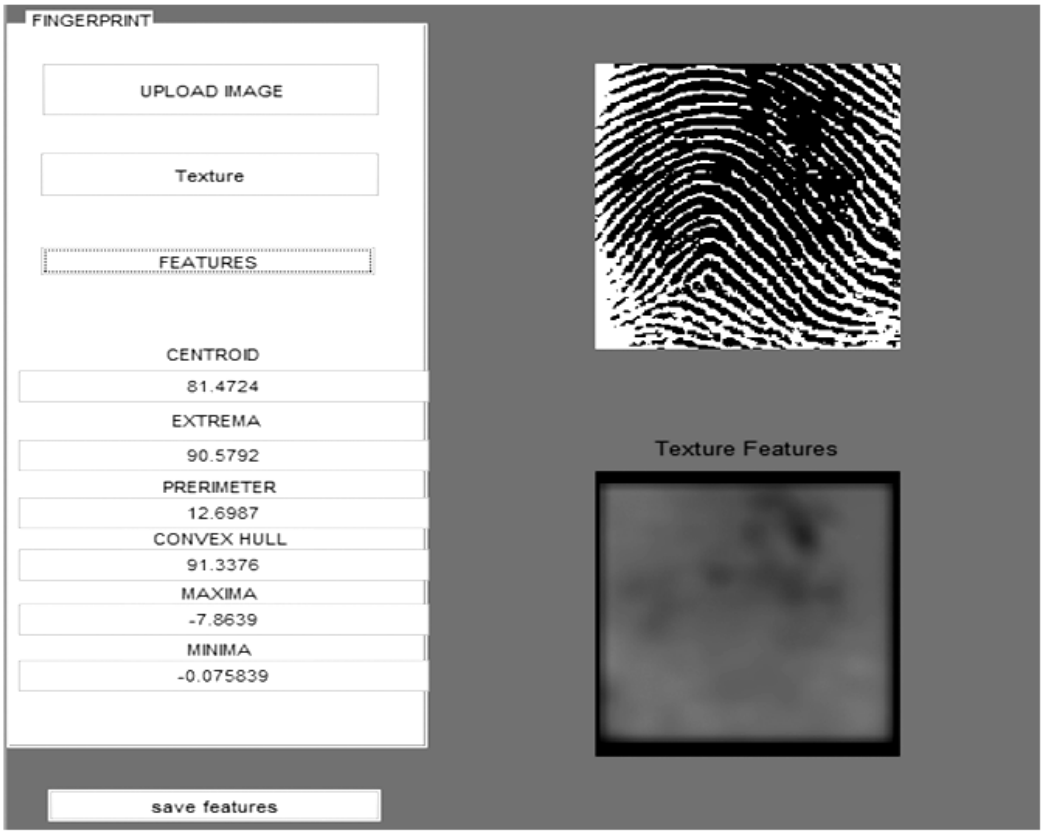

Figure 8: Fingerprint Feature Extraction

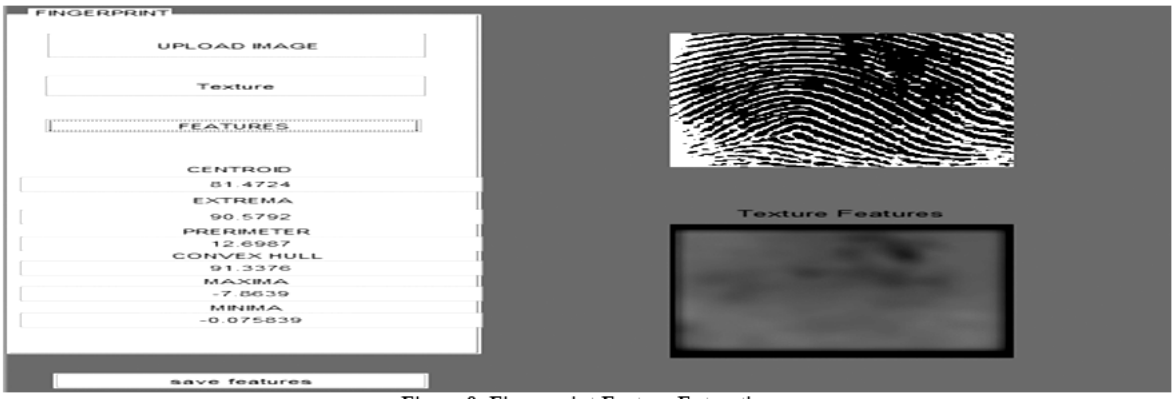

Figure 9: Fingerprint Feature Extraction

6.3. Recognition Accuracy

As shown in the Table 1, the FAR & FRR are calculated with different methods. On the dataset of 50 users the test is done. Feature vector are made for both genuine users and intruder, after this feature vectors are fused using different techniques describe in table. Results are given in the form of FRR and FAR which are deduced for different methods. Accuracy is calculated for all the methods.

$$\text{Recognition Accuracy} = 100 - (\text{FAR} + \text{FRR}) \tag{3}$$

Table 1
Comparison of Performance

	Iris Recognition	*Fingerprint Recognition*	*Multimodal Biometrics*
FAR	9.9	17.6	3.1
FRR	13.6	12.4	16.3
Accuracy	76.5%	70%	80.6%

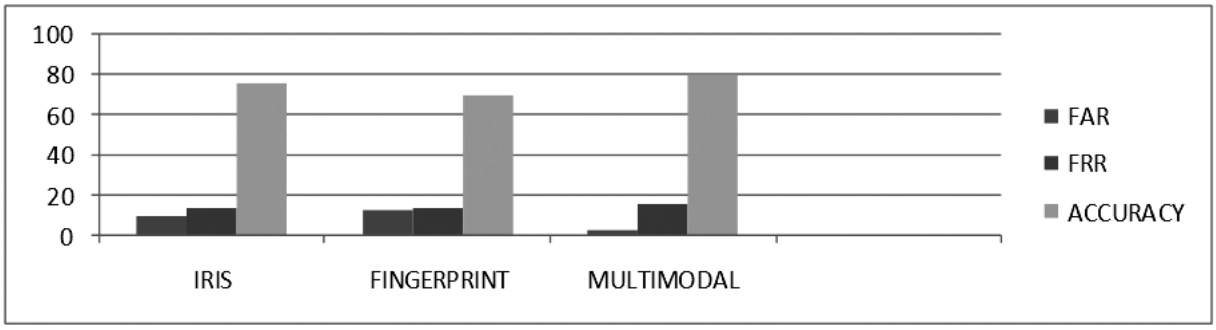

Figure 10: Performance Measure

7. CONCLUSION

In this work we check the effectiveness of the multimodal biometric framework and contrast it and unimodal biometric framework. In this shrewd based components are removed for Iris and center focuses are separated for Fingerprint. Here choice level combination is utilized as a part of multimodal framework after grouping of extricated components. The exactness of given framework is 80.6% for multimodal framework and 76.5% and

70% for iris and unique mark separately. This implies a multimodal biometric framework works proficiently than uni-modular framework. Future works could go toward utilizing more strong procedures against frauds and crossover combination level can be utilized. Likewise, the framework ought to be tried on a bigger database with loud examples to approve the fervor of the model.

REFERENCES

[1] S. Pankanti, R.M. Bolle and A. Jain, "Biometrics - The future of Identification", *IEEE Computer*, Volume 33, No. 2, pp. 46-49, February 2002.

[2] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication", *Proceedings of the IEEE*, Vol. 91, No. 12, pp. 2019-40, Dec. 2003.

[3] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security & Privacy Concerns*", IEEE Security and Privacy Magazine*, Vol. 1, No. 2, pp. 33-42, March-April 2003.

[4] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*, New York, Springer, 2006.

[5] Anil K. Jain, Arun Ross and Sharath Pankanti, "Biometrics: A Tool for Information Security*", IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 2, pp. 125-143, June 2006.

[6] Anil K. Jain and Arun Ross, "Multibiometric Systems". *Communications of the ACM*, *Special issue on Multimodal Interfaces*, 47(1):34-40, January 2004.

[7] J. D. Woodward, Biometrics: Privacy's foe or privacy's friend? *Proceedings of the IEEE (Special Issue on Automated Biometrics)*, Vol. 85, pp.1480–1492, September 1997.

[8] BelCn Ruiz-Mezcua , D.G. Plaza, C.Fernandez , P.D.Garcia and F.Fernandez, "Biometrics verification in a real environment" Security Technology,1999. Proceedings. *IEEE 33rd Annual 1999 International Carnahan Conference.*

[9] L. Hong, Y. Wan, and A. K. Jain, "Fingerprint image Enhancement :Algorithm and performance evaluation,"*IEEE Trans. Part. Anal. Machine Intell.*, Vol. 20, pp. 777-789, Aug. 1998.

[10] A.K. Jain, S. Prabhakar, and L. Hong, "A multichannel approach to fingerprint classification",*PAMI*, 21 (4):348-359, 1999.

[11] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, "Is independence good for combining classifiers?,"*In Proc. of Int'l Conf. on Pattern Recognition (ICPR*), Vol. 2, (Barcelona, Spain), pp. 168-171, 2000.

[12] K.I. Chang, K. W. Bowyer, P. J. Flyrn, and X. Chen, "Multibiometrics Using Facial Appearance, Shape and Temperature", *In Sixth IEEE International Conference on Automatic Face and Gesture Recognition*, pages 43-48, Seoul, Korea, May 2004.

[13] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman, "Biometrics: A Grand Challenge", *in the Proceedings of International Conference on Pattern Recognition*, Cambridge, UK, Aug. 2004.

[14] N. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength,"*In Proc. Int. Conf. Audio and Video-based Biometric Person Authentication*, Halmstad, Sweden, pp. 223-228, Jun. 2001.

[15] S.Ben-Yacoub, Y.Abdeljaoued, and E.Mayoraz, "Fusion of Face and Speech Data For person Idenity Verification" .*IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(5):616-622, May 2003.