ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(13), DOI: 10.17485/ijst/2016/v9i13/90545, April 2016* ISSN (Online) : 0974-5645

Estimation of Performance in Multimodal Biometric based Authentication System using Various Clustering

R. Manju* and A. Shajin nargunam

Department of EIE, Noorul Islam University, Kanyakumari – 629180, Tamil Nadu, India;
manjuria.7@gmail.com, shajin@niuniv.com

Abstract

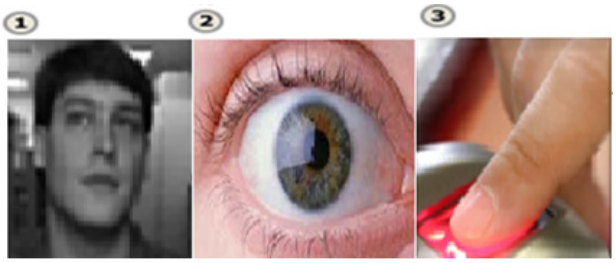
Objectives: A swift growth of awareness in biometric based applications can be currently seen in the world. It includes different approaches to solve problems at hand. **Methods:** In this paper, Rough set with different classifiers are discussed to improve the performance of biometric system based authentication. This paper presents software systems based on rough sets comparing performance evaluation with different classifier techniques, fusion methods, filtering techniques and it provide sophisticated graphical environment. The decision fusion approach of multi modal biometric authentication gives the excellent performance in security system. **Findings:** A special place among different extensions is taken by the loom that replaces imperceptible relation. In the point of many simplification techniques, variant and extension of rough sets in a consistent appearance of the theory and implementation methodology is in place. This paper is meant to fulfil the specified necessitates and various challenges available in multimodal biometric authentication systems. **Applications:** This is used in National Secure the borders, Organizational/Enterprise, Identity and access management, Personal, Preventing impersonation (ID theft).

Keywords: Classifier, Feature Extraction PSO, Median Filter, PCA, Rough Sets

1. Introduction

A biometric verification system is related to automatic recognition of human being, that identifies a person by deciding the validity by, either or both physiological, behavioural feature i.e. Biometric which possessed by that person. Multibiometric is a moderately new approach to biometric knowledge illustration that strives to conquer the problems by fusing the indication presented by multi-biometric inputs. In multibiometric system the following terms such as template requirements, processing time, and computing difficulty are restricted. The main flourishing of multibiometric system is in a most favourable combination proposal, which is needed to merge the details of data offered by multiple domain specialists[1]. The aim of fusion is to conclude the optimum set of practised in a certain problem oriented domain and work out a corresponding task that can optimally merge the conclusions done by the individual specialists[2,3].

This research work provides the application of Fusion at the Matching Score Level. Here three separate unimodal biometric systems are used as virtual input and discuss its efficiency The techniques used as utilization of Principal Component Analysis (PCA) for Feature extraction, Median Filter as Preprocessing, Various clustering techniques like Fuzzy, SVM, Sparse, Neuro-Fuzzy, Rough-Set are used. PSO based Fusion technique is used in the Matching Score Level.



(a)

* Author for correspondence

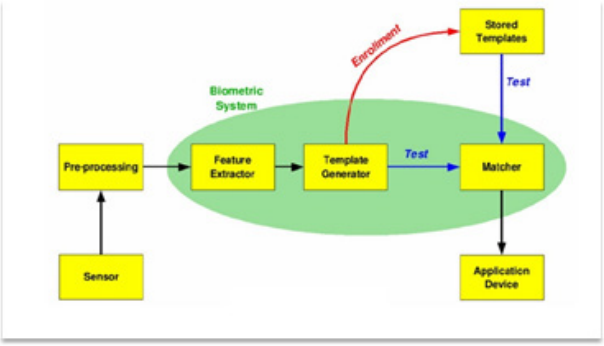
The Three traits used in our system are shown in the above Figure 1a. In this research will focal point in terms used are FAR, FRR, recognition rates, Error Rates (EER), and response times explained in Section 5. The last section gives the information related to discussion and conclusion.

1.1 Features of a Biometric System

The most important of this paper is to enhance the detection presentation of a multi-biometric authentication system by incorporating multiple biometric inputs[4]. Usually, the performance of a biometric system is expressed by some parameters. The system is used to reduce the following two error rates.

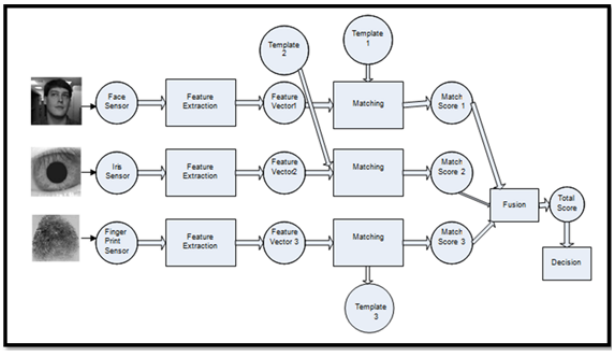
False Acceptance Rate (FAR): is defined as possibility of a fake being allowed as a real personality. It is computed as the small part of fake score surpassing the threshold value.

False Rejection Rate (FRR): is defined as the possibility of an actual personality being discarded as a fake. A little amount of FRR typically leads to a tubby FAR, although a little FAR typically involves a higher FRR[5]. Normally, the modal requirements are indicated by using the terms of FAR. If there is a zero of FAR, that means there is no fake data's are acknowledged as an actual personality. In Genuine Accept Rate (GAR), is used to compute the performance of an authentication system[6,7]. It is calculated as the small parts of genuine achieve surpassing the threshold value GAR = 1- FRR.

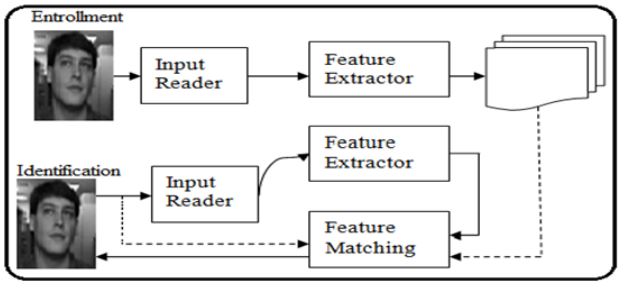


(b)

Figure 1b and 1c shows the fusion unit to enhance the identification performance and Figure 1d shows the Architecture of generic biometric system.



(c)



(d)

Figure 1. (**a**) Three traits used in our system (**b**) Block diagram of the unimodal biometric system (**c**) Block diagram of the Multimodal biometric system (**d**) Architecture of generic biometric system.

2. Proposed Work

2.1 Preprocessing

For noise removing in a nonlinear digital filtering technique as median filter is used, frequently used to remove noise by using Median filtering[8]. Its broadly used because of it protects edges while eliminating noise. The median filtering technique is shown in the Figure 2

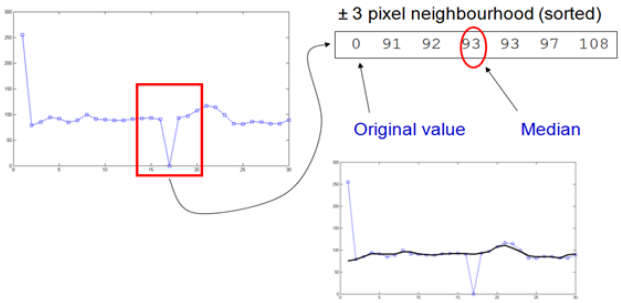


Figure 2. Median Filtering Technique

The goal and steps of the median filter as follow,

- It center pixel is replaced by the value of the median of the intensity significances in the neighborhood of that pixel.
- For a nonlinear operation Median filtering is often used in image processing which reduce "salt and pepper" noise. A median filter aim is to concurrently decrease noise and protect edges.
- Median filters are mostly efficient for existence of *impulse noise*, also called '***salt – and – pepper***' noise due to its manifestation in terms of white and black dot lay over on the image.
- For every pixel encountered 3x3 as center is judged. The median value is replaced in the center value pixel using median filter.

3. Feature Extraction

3.1 Principal Component Analysis (PCA)

PCA is an *n*-dimensional data analysis algebraic method. Eigenimage method has a dense depiction, an image of biometrics like face; iris and fingerprint[9] can be quickly characterized by using few components with the trait vector. For extracting features in an effective way PCA is used in this research. The steps followed in this algorithm as follow:

- Read the images
- Calculation of mean
- Subtracting the mean from the data
- Covariance for this difference is calculated
- Eigen vectors, values are calculated for this covariance
- The Eigen values are sorted in descending order
- Only most significant information is considered.

Eigenimage performance for the iris sub images available in the virtual database input[10, 11]. Set of training input images are given in the starting time in the template. From this Eigenvalue and Eigenvectors are to be calculated. Then the covariance matrixes found from these images are utilized in appropriate algorithms[12]. From the eigenvectors (Eigenimages) that are created, in these steps, need to choose a subset of the highest eigenvalues. For the elevated eigenvalue, the enhanced features of a virtual images eigenvectors are illustrates[13]. For Eigenimage having small eigenvalues are to be rejected in computation. These can explains for a few amount of performance features of the input image. Either an AR (Acceptance Rate) or RR (Rejection Rate) can be computed using their threshold value. For the remaining procedures are based on the threshold value match.

4. Classifier

Clustering means finding similarities in data and putting similar data into groups. Here Fuzzy C means Clustering is used. The demerits and restrictions of unimodal system can be reduced by this research work. Instead of using a classifier to conclude the performance of evaluation[14], in this research work multi-classifiers used to identify individual's score. The different classifiers used in this research work as follow,

- Fuzzy
- SVM
- Sparse
- Neuro-Fuzzy
- RoughSet Fuzzy

4.1 Fuzzy

It's a data clustering algorithm in which each data point is associated with a cluster. An object can belongs[15, 16] any number of clusters but to different membership degrees. The steps used as follow,

- The number of clusters is initialized
- The partition matrix U is initialized rc x N
- The cluster centers are calculated by $C^{*}_{i} = (\Sigma^{N}_{K=1} (\mu_{ik})^{m} X_{k}) / (\Sigma^{rc}_{i=1} (\mu_{ik})^{m})$
- The Euclidean distance is calculated between the data and cluster centers d_{ik}
- The membership function is calculated by $\mu^{*}_{ik} = 1/(\Sigma^{rc}_{i=1}(d_{ik}/d_{ij})^{2/(m-1)}$
- Based on the new membership value and cluster centers the data is clustered.

4.2 SVM

Support Vector Machine Algorithm is an efficient classifier to analyse the performance of the individual inputs. The Steps involved as follow;

- First prefer a kernel task of condition
- Prefer a assessment for *C*
- work out quadratic programming problem (there are numerous software packages are existing)
- Then create the Discriminant function by using support vectors .

4.3 Sparse

Sparse method makes use of this detail by means of a matrix. There is a set of nonzero parts and its corresponding location as specified by row and column inside the matrix. Sparse method of clustering is additional proficient, if there are sufficient zero-part functions in the opaque form is give additional time need to locate and work on matrix parts in the sparse appearance meaningful.

4.4 Neuro-Fuzzy

A hybrid neural net computationally identical to Sugeno-type fuzzy reasoning. Where,

$\mathbf{F}_{n}$ - Arranged set of neurons with size of n ´ 1, as an input field element.

$\mathbf{F}_{m}$ - Output field element.

An arranged set of neurons with size of m ´ 1 is to be used as neuro-fuzzy input vector, Î Â^{n}, which is match ups to input of neuron i from the input elements.

F_{x} - Fuzzy output vector, Î Â^{m}, which is related to the output function of neuron i in the output element.

F_{y}, **A**: Â^{n}®Â^{m} – The association function.

L Í **A** - Set of learned association

f: Â^{k}®Â - Activation function of Neuron.

4.5 RoughSet Fuzzy

The ultimate aim of the rough set based clustering method is to select a smallest amount of attribute subset. That has a similar spirit of power in the complete attribute set. The dependency is dependent upon the selection of attributes. Generally twice prior troubles are occurring while creating feature selection based clustering algorithm. These are described as follow,

- How to estimate the elected attributes.
- How to find for a high-quality attribute subsets.

In this research work used dependence function can be introduced to evaluate the goodness of selected features.

4.6 Matching Score Level Fusion

All the input scores are mingled in matching score stage by using PSO technique. In this, the virtual test images corresponds to the Eigen space, and compute the space of the position related to the unknown image eigenspace and the template image position from the eigenspace[17, 18].

- For fusion PSO is used in this research work.

Input: Initialize the algorithm parameters (c1, c2, w, vmax, Swarm_Size, Max_Iter, r1, r2).

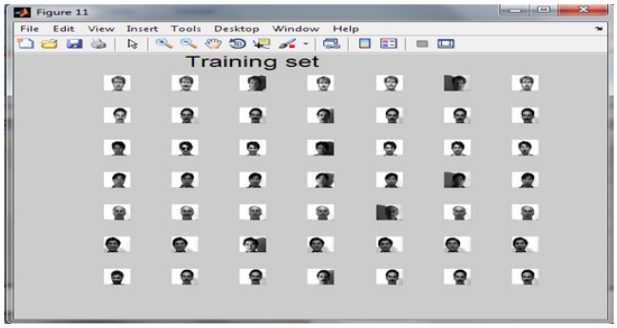
Output: The optimization having the highest fitness by using PSO.

- **Step 1:** Randomly generate the initial particles and velocities to construct a swarm.
- **Step 2:** Compute the fitness gathering of individual components.
- **Step 3:** From the position of the particles to decide the position like, update the particles to shows this fact.
- **Step 4:** Find the best particle of the swarm. Update the positions of the particles by using the above steps (1) and (2).
- **Step 5:** If there is upper limit of repetitions go beyond the optimum, then proceed the step 6 or else proceed the Step 2.
- **Step 6:** Facsimile the optimum value and exit.

5. Results and Discussions

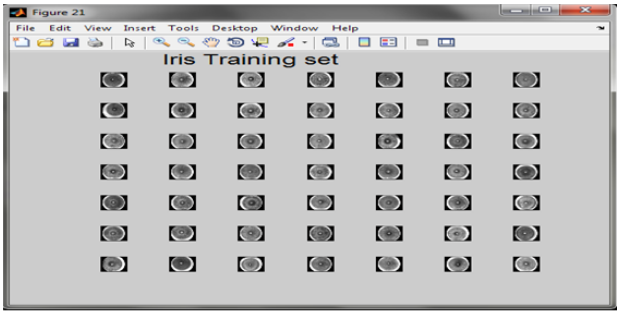
5.1 Processed Experimental Data

In this work have used a true database which contains three unimodal databases for face, iris, and finger print respectively.

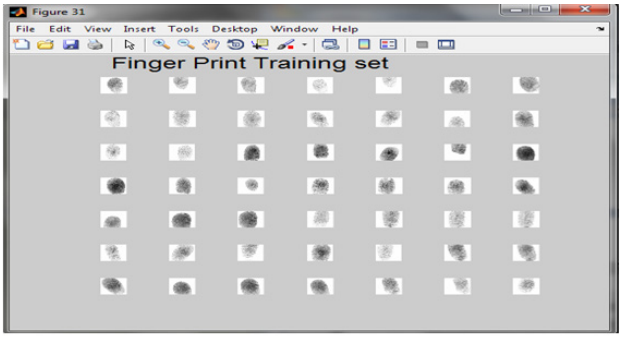


(a)

The face training set is given in the Figure 3a. The Databases of iris is shown in Figure 3b.

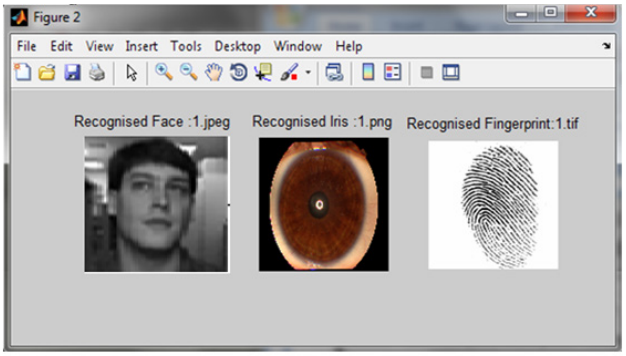


(b)



(c)

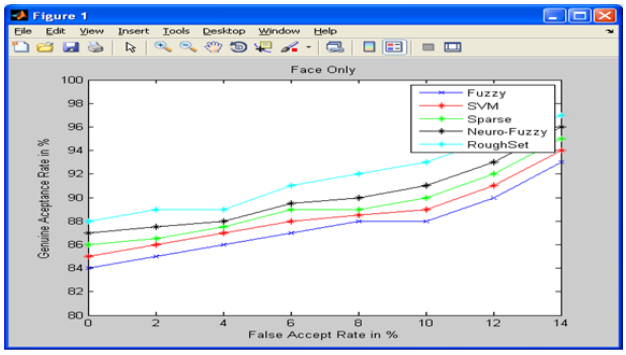
In this research work virtual database are used for training dataset. For iris verification/ identification databases and some private licensed databases like IIT's databases are accessible for testing. Among that Nist ice database is the prime general database are available.



(d)

5.2 Results

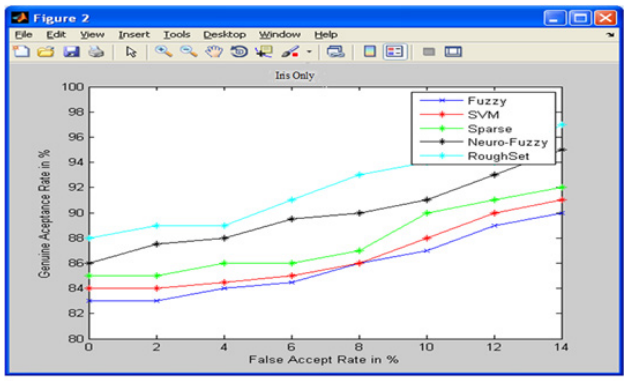
In this research various classification techniques have compared in terms of FAR and GAR. The results are shown by the Recognised output Figure 3d and graph Figure 3h, it is clear that rough set performance better than previous methods.



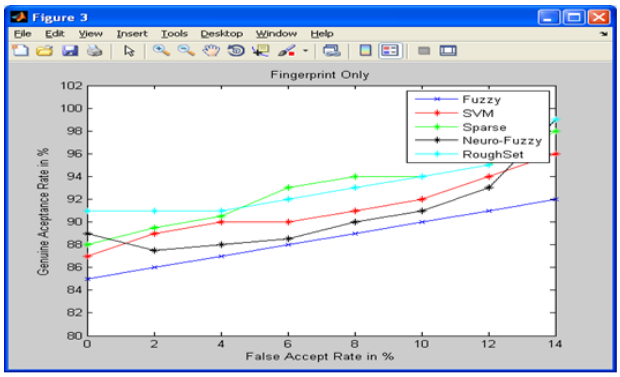
(e)

The Output Response of Face, iris and finger print are shown in Figure 3e, Figure 3f Figure 3g respectively[19, 20]. In biometric authentication method primarily general parameters used for evaluating system performance includes the False Acceptance Rate (FAR), this is a levy of the number of possible impostors shown by the Figure 3h.

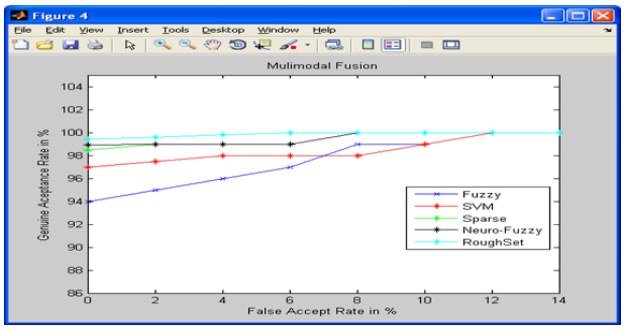
These two factors are normally represented in the graphical manner like - single curve as the Receiver Operating Characteristic (ROC)[21]. Figure 3i shows the acquired ROC curve of the proposed system.



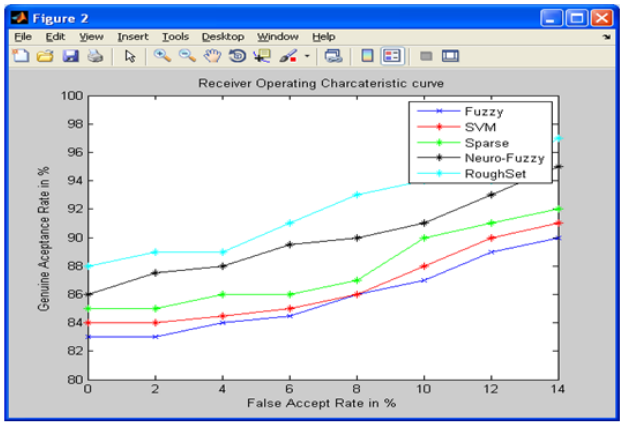
(f)



(g)



(h)



(i)

Figure 3. (**a**) Databases of Face, (**b**) Databases of iris (**c**) Databases of fingerprint (**d**) Recognized Output (**e**) Output Response of Face (**f**) Output Response of Iris (**g**) Output Responseof Finger print (**h**) Output performance of multimodal fusion (**i**) ROC curve for different Classifier Methods.

5.3 Accuracy

The proper verification should be done, when using biometric system compare to existing methodology. The foremost factor which affects the performance of biometric systems is improper biometric input data. It's occurs when a noisy fingerprint input image captured, which contains smear, remaining deposits, etc. In addition that unclear iris image due to out of focus and lighting.

In this research work, it's avoided by using tested virtual data base as for iris UBIRIS data base is used. From the figure getting images/impressions of a user's finger. If the images ridge details are worn-out then noise present in acquired input data. This is happen because of faulty or improper sensor units. These are the factors affecting face, finger print and iris images. This leads to reduce the recognition accuracy of biometric system. Biometrics input is high sensitive to quality of input and the strident data can leads to variation of GAR of biometric system.

Biometric traits for enrollment and identification are to be use in the universal. The basic conditions for a biometrics are, all the biometric traits are not really same. The NIST has presents that it is not possible to obtain a fine quality fingerprint from around 2% of the population (people with hand related to hand using labors which contains cuts and bruises on their fingertips, and people with very oily or dry fingers)[22]. It's very difficult to enroll such persons. Similarly, people have lengthy eye-lashes and those pains from eye abnormality or diseases like glaucoma, cataract, aniridia, and nystagmus, from that getting a good quality iris image is difficult. Non-universality leads to high FTER and FTCR in a biometric system[23].

For face, Olivetti Research Lab Database is used, which is containing 49 images of 7 for every 7 different subjects. For Iris UBIRIS data base is used. For finger print - DB1: "V300"is used, it's collected by using the optical sensor technologies[24, 25]. These databases are giving an accurate response it's being tested and accepted virtual databases from IIT Delhi and other labs.

5.4 Security Analysis

The biometric based security systems in tenures of the min-entropy of the helper data. Min-entropy of a random variable A is need as $H1(A) = ¡\log (maxaP(A = a))$: (5.5). Note that all the logarithms in this section are of base 2. If the obscurity in guessing is considered as A. Now consider a pair of random variables A and B. In entropy of A given B as,

$H1(AjB) = ¡\log (maxaP(A = ajB = b))$

and the average min-entropy of A given B as ,

$H\ 1(AjB) = ¡\log (EbÃB\ [maxaP(A = ajB = b)])$

$= ¡\log^{3} EbÃB\text{h}2¡H1(AjB)\text{i}$

In this research work scrutinizes the security using roughest Algorithm. By the usage of PSO fusion techniques to reduce the training and reorganization time.

6. Conclusion

This research work is specifically focused on considerate the multipart mechanisms employ to find a high-quality by combining of multibiometric features and various clustering methods to get the optimal verification outcome. In this research present a comparison between various clustering, used in multimodal biometric based system performance and variations of the results obtained in different stages of applying PSO based fusion. For instance, the virtual databases used in these methods demonstrated enhanced identification presentation, although the preparation time was slightly privileged than that of the eigenimage technique.

7. References

1. Hong L, Jain A. Integrating faces and fingerprints for personal identification. IEEE Transactions on Pattern Analysis Machine Intelligence. 1998; 20(12):1295–307.

2. Toh KA, Jiang D, Yau WY. Exploiting global and local decisions for multi-modal biometrics verification. IEEE Transactions on Signal Processing. 2004; 52(10):3059–72.
3. Snelick R, Uludag U, Mink A, Indovina M, Jain AK. Large scale evaluation of multimodal biometric authentication using state-of the-art systems. IEEE Transactions on Pattern Analysis Machine Intelligence. 2005; 27(3):450–55.
4. Jain AK, Ross A, Pankanti S. Biometrics: A tool for information security. IEEE Transactions on Information Forensics Security. 2006; 1(2):125– 43.
5. Punidha R, Anisha Vincy S, Mary Judith. Remote Service Access using Biometrics. Indian Journal of Science and Technology. 2016 Jan; 9(1). DOI: 10.17485/ijst/2016/v9i1/85786
6. Bhattacharyya D, Ranjan R, Alisherov F Choi M. Biometric Authentication: A Review. International Journal of u-and e-Service, Science and Technology. 2009; 2 (3):13 –28.
7. Zdenek Ríha, Václav Matyáš. Biometric Authentication Systems. International Journal of Computer Applications (0975 – 8887). 2010 Nov; 9(10).
8. Angeline Prasanna G, Anandakumar K, Bharathiar University, Coimbatore - 641 046, Tamil Nadu, India. Bannari Amman Institute of Technology, Sathyamangalam - 638 401, Tamil Nadu, India. Indian Journal of Science and Technology. 2015 December; 8(34). DOI:10.17485/ijst/2015/v8i34/70767.
9. Bhattacharyya D, Ranjan R, Das P, Hoon Kim T, Bandyopadhyay K, Biometric Authentication Technique and Its Future probabilities. IEEE Trans International Conference on Computer and Electrical Engineering. 2009. p. 652–55.
10. Kisku DR, Gupta P, Sing JK. Fusion of Facial Features using DS Theory for Face Recognition. International Journal of Recent Trends in Engineering. Academy Publishers; 2010; 4(2):139 –141.
11. Jain AK, Kumar A. Biometrics of Next Generation: An Overview. 2nd Generation Biometrics Springer; 2010. p. 1–36.
12. Bhatnagar J, Kumar A, Saggar N. A novel approach to improve biometric recognition using rank level fusion. Proc. IEEE Conference on Computer Vision Pattern Recoginition. Minneapolis: MN CVPR'07; 2007. p. 1– 6.
13. Jain A, Nandakumar K, Ross A. Score normalization in multimodal biometric systems. Pattern Recognition. 2005; 38 (12):2270–85.
14. You J, Li W, Zhang D. Hierarchical Palmprint Identification via Multiple Feature Extraction. Pattern Recognition. 2002; 35(4):847–59.
15. Kumar A, Passi A. Comparison and combination of iris matchers for reliable personal identification. Pattern Recognition. 2010; 43(3):1016 –26.
16. Kumar A, Wu C. Automated human identification using ear imaging. Pattern Recognition. 2012; 41(5):956–68.
17. Kumar A, Wong DCM, Shen HC, Jain AK. Personal verification using palmprint and hand geometry biometric. Audio-Video-Based Biometric Person Authentication. Springer: Berlin Heidelberg; 2003. p. 668–78.
18. Wang Y, Tan T, Jain AK. Combining face and iris biometrics for identity verification. Audio-Video-Based Biometric Person Authentication. Springer: Berlin Heidelberg; 2003. p. 805–13.
19. Frischholz RW, Dieckmann U. BiolD: A multimodal biometric identification system. Computer. 2000; 33(2):64–68.
20. Ross AA, Nandakumar K, Jain AK. Handbook of Multibiometrics. Springer-Verlag: New York. 2006.
21. Podio FL, Dunn JS. Biometric Authentication Technology: From the Movies to Your Desktop. The Biometric Consortium. 2002. p. 1–8.
22. Fierrez-Aguilar J, Ortega-Garcia J, Garcia-Romero D, Gonzalez- Rodriguez J. A comparative evaluation of fusion strategies for multimodal biometric verification. Proc. 4th Int. Conf. Audio-Video-Based Biometric Person Authentication; 2003. p. 830–37.
23. Ross AA, Govindarajan R. Feature level fusion using hand and face biometrics. Proc. SPIE 2nd Conference on Biometric Technology Human Identification. Orlando: FL. 2005. p. 196 –204.
24. Kumar A. Incorporating Cohort Information for Reliable Palmprint Authentication. 6th Indian Conference on Computer Vision, Graphics and Image Processing; ICVGIP'08; Bhubaneswar. 2008. p. 583–90.
25. Ross A, Govindarajan R. Feature level fusion using hand and face biometrics, Proc. SPIE 2nd Conference on Biometric Technology Human Identification; Orlando: FL. 2005. p. 196 –204.