JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 2911 - 2919
https://publishoa.com
ISSN: 1309-3452

Design and Analysis of Multimodal Biometric Authentication System using Machine Learning

Divya Singh[a], Avdhesh yadav[b], Lokendra Singh Umrao[c*], Ravi Ranjan Choudhary[d]
[a,b,c,d]*Department of Computer Science and Engineering, Institute of Engineering and Technology, Dr. Rammanohar Lohia Avadh University, Ayodhya, India*

*Corresponding author Email: lokendrasingh@rmlau.ac.in

ABSTRACT
In this paper, a multimodal biometric identification system based on feature level fusion and machine learning techniques is described. The significance of this study relates to the combination of face and palm print for an individual identification. Machine Learning utilised to improve the performance of a multimodal biometric identification system. The performance evaluation is evaluated based on precision, recognition rate, equal error rate, and numerous evaluation metrics. The suggested multimodal system has an accuracy of 89.96 %, a false acceptance rate (FAR) of 3.32 %, and a false recognition rate (FRR) of 2.92 %. In order to arrive at this result, the multimodal system relies on score level fusion. It is demonstrated that a multimodal system may achieve high accuracy while using minimal FAR and FRR.

INDEX TERMS: Biometric Authentication, Multimodal, Face recognition, Palm Print Recognition, Learning Algorithm

1. INTRODUCTION

The collected biometric is normally processed in two different modes like verification mode and identification mode [9]. To validate an individual, the system performs a one-to-one comparison between a biometric and the biometric database. Enrolment is the initial step for a user of a biometric system. During enrolment, biometric information is taken and saved, and in subsequent steps, biometric information is detected and compared with previously stored information. Therefore, storage and retrieval of these systems are protected provided the system is strong.
In addition to presenting new hurdles for high-security applications, biometric authentication is also natural and quick. Compared to the major established means of identification, such as PIN-codes, passwords, and smart cards, biometrics offers a number of advantages [1].

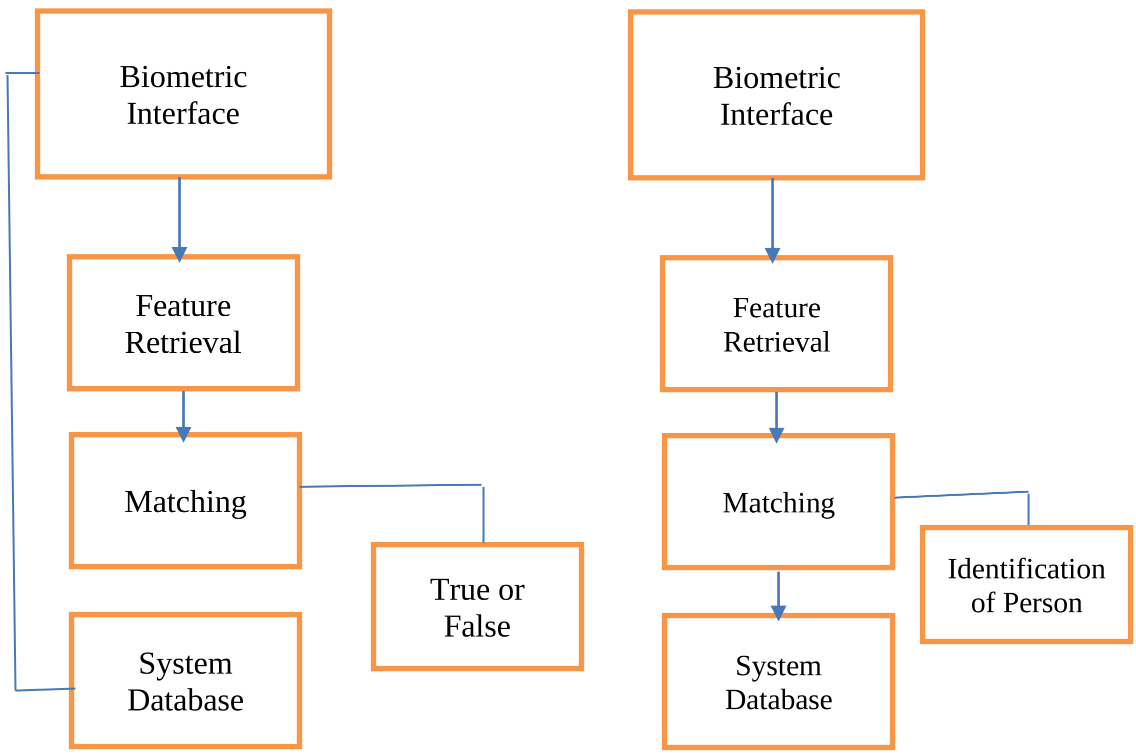
- Unique for each and every person
- Always present Always present
- Unable to copy or transmit
- Low risk of forgetfulness and theft

1.2 Need of Biometric

Any biometric trait may be used to identify an individual. It determines how an individual will be identified. Each biometric characteristic has advantages and disadvantages, based on the following criteria:
Universality: This means that each person should have a distinct personality trait.
Uniqueness: This means that no two people should have the same personality.
Permanence: It means that the characters should not change over time.
Character collectability: This means that the characters can be quantified.
The system may work in two modes, verification mode and identification mode, based on biometric criteria. In general, the biometric system is a pattern recognition system comprised of steps such as data collecting, data pre-processing, data representation, and decision making. Biometric systems have three distinct uses, including

physical access control for barring unauthorised individuals, logical access control for securing networks and computers, and time management for attendance systems. The functionality of the two modes is as follows:
Verification, which confirms a person's claimed identity (Figure 1a). It is a "one-to-one" matching procedure, and the system must perform a comparison between the individual's biometrics and a single template that is maintained in a centralised or distributed database.
Identification, which chooses from a database the accurate identify of an unknown individual (Figure 1b). It is a "one-to-many" matching procedure since the system is tasked with comparing the individual's biometrics to all the biometric templates contained in a database. The method may either select the "best" match or score or rank all potential matches in order of similarity [7].

Any biometric trait may be used to identify an individual. It determines how an individual will be identified. Each biometric characteristic has advantages and disadvantages, based on the following criteria:
Universality: This means that each person should have a distinct personality trait.
Uniqueness: This means that no two people should have the same personality.
Permanence: It means that the characters should not change over time.
Character collectability: This means that the characters can be quantified.
The system may work in two modes, verification mode and identification mode, based on biometric criteria [3]. In general, the biometric system is a pattern recognition system comprised of steps such as data collecting, data pre-processing, data representation, and decision making. Biometric systems have three distinct uses, including physical access control for barring unauthorised individuals, logical access control for securing networks and computers, and time management for attendance systems. The functionality of the two modes is as follows:



(a)
(b) Verification process (b) Identification process
Figure 1: Verification and Identification process

1.3 Multimodal Biometrics
Human identification based on a Multimodal biometric system is an emerging concept that permits the integration of two or more biometric modalities or biometric technologies (such as face recognition, fingerprint and iris

recognition, etc.) to enhance performance [19].
The system determines high security because the user requires one or more identity markers. This approach makes it far more difficult for an intruder to mislead the system by requiring many phoney identities to simultaneously supply data. For instance, a biometric system that combines facial and Palm print features for biometric identification is termed a multimodal system, regardless of whether the face and palmprint pictures are captured by the same or distinct imaging sensors.

2. Literature Review

We have studied many paper in which below papers is selected as base paper for this paper. Ross et al. [21] have discussed an overview of biometrics and fusion in biometrics. Moreover, they have discussed some of the pertinent terminologies necessary to understand this technology. Unar et al. [18] discussed different biometric modalities with their advantages and challenges. It also provides an up to-date review of information regarding feature sets and recognition techniques. The researcher has also provided information about public databases and multimodal biometric system along with fusion techniques and their applications.
E. Yoruk et al. [6] have developed identity verification based on hand biometrics. Several feature schemes are comparatively applied and evaluated. The Independent Component Analysis (ICA) features are found to perform uniformly superior to all other features.

3. Proposed Work

3.1 Dataset Collection and Proposed Objective

This section explores the Proposed work, experimental setup, performance metrics, and results obtained.In this proposed work, OUR Face dataset (http:/ /robotics.csie.ncku.edu.tw/ Databases/ FaceDetect_PoseEstimate.htm) is used for the face modality. This dataset has 90 subjects each with 74 sample images to give a total of 6660 sample images. For the palm modality, the publically available dataset at (www.comp.polyu.edu.hk /~csajaykr/ IITD/Database_Palm) is used. We refer to this dataset as the IITD Palm dataset. It has 230 subjects each with 7 sample images of each left and right hand giving us a total of 3220 sample images [19].

- This experimentation follows three objectives:-

- Performance evaluation of unimodal face recognition on OUR Face dataset
- Performance evaluation of unimodal palm recognition on IITD Palm dataset
- Performance evaluation of multimodal face+palm recognition using score level fusion

Datasets are segregated into training and testing datasets in such a way that a batch of images can be made containing 50,100,150 and 200 sample images of 10 virtual personalities created out of these two datasets. For example, to make a batch of 50 sample images, we can take 10 virtual personalities with each personality having 3 face images and 2 palmprint images (1 left palm+1 right palm).
In this work, three classifiers trained and tested are Random Forest (RF), Support Vector Machine Classifier (SVM), and Artificial Neural Network (ANN). The reason to select these three classifiers is to look for a better performing approach in supervised multiclass classification tasks concerning SVM is superior in hyperplane separation in multidimensional data, RF is the promising ensemble approach in feature extraction, and ANN is capable of obtaining better features automatically. Combining the best for the multimodal systems enhances the overall performance [10].
To get everything done on WEKA simulation tool, first, we need to have all the images with their label converted into SCV file format. Then these files have to be converted into the .arif file format required by the WEKA tool.

3.2 EXPERIMENTAL SETUP

In this work WEKA (version 3.8.5) simulation tool is used undertheWindows10OSwithhardwareconfiguration–IntelCorei5CPU@1.60GHz.8GBRAM. It is a similation tool developed by the University of Waikato, New Zealand, and has implementations for many algorithms including predictive modeling and visualizations.

3.3 EVALUATION CRITERIA

The confusion matrix and its components are generally utilized for the computation of other well-known metrics for the better evaluation of multiclass classification tasks.
These componentsof the confusionmatrix are -
True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). TP represents the number of

correct classifications while FP represents the number of the wrong classification that the model predicts as correct classification. A similar theory but in reverse is also true for the TN and FN.

In this work, we achieve multimodal biometric authentication as a multi-class classification. Hence TP and TN are calculated with one vs rest. Here, one refers to class of concern and rest is for the group of remaining classes. For example, say, the four users are – User1, User2, User3, and User4. Therefore, TP for "User1" is all "User1" instances predicted correctly as "User1". TN is instances of the remaining 3 user classes predicted correctly as instances of those respective classes only. For the multi-class and unbalanced dataset, accuracy alone is not enough, and other metrics such as FPR, Precision, TPR/Recall/Sensitivity, F1-Score, MCC, ROC-AUC, Kappa are calculated.

4.Result and Discussion

In this work WEKA (version 3.8.5) simulation tool is used undertheWindows10OSwithhardwareconfiguration–IntelCorei5CPU@1.60GHz.8GBRAM. Result of work is displayed in Table 1 and Table 2.

TABLE 1: Performance Evaluation on OUR FACE dataset (WEKA Simulation)

Image Batch Size	**Classifier**	**FPR =1-Specificity**	**Precision**	**TP Rate /Recall /Sensitivity**	**F1 Score**	**MCC**	**ROC AUC**	**Accuracy**	**Kappa**
50	RF	0.105	0.821	0.809	0.800	0.718	0.882	80.848	0.689
100		0.083	0.870	0.846	0.840	0.782	0.901	84.568	0.751
150		0.098	0.862	0.835	0.827	0.762	0.888	83.503	0.731
200		0.085	0.875	0.851	0.844	0.790	0.915	85.100	0.758
50	SVM	0.098	0.852	0.825	0.816	0.752	0.879	82.443	0.714
100		0.148	0.769	0.755	0.740	0.633	0.879	75.530	0.596
150		0.173	0.683	0.702	0.690	0.536	0.852	70.210	0.518
200		0.171	0.697	0.706	0.699	0.546	0.848	70.636	0.527
50	NN	0.093	0.880	0.818	0.800	0.728	0.892	81.940	0.679
100		0.097	0.872	0.835	0.829	0.772	0.900	86.560	0.789
150		0.161	0.861	0.814	0.825	0.762	0.898	87.890	0.710
200		0.088	0.778	0.765	0.812	0.732	0.879	89.300	0.690

TABLE 2: Performance Evaluation on IITD Palmprint dataset (WEKA Simulation)

Image Batch Size	**Classifier**	**FPR =1-Specificity**	**Precision**	**TP Rate /Recall /Sensitivity**	**F1 Score**	**MCC**	**ROC AUC**	**Accuracy**	**Kappa**
50	RF	0.095	0.921	0.799	0.901	0.617	0.883	80.959	0.790
100		0.073	0.970	0.836	0.941	0.681	0.902	84.679	0.852
150		0.088	0.962	0.825	0.928	0.661	0.889	83.614	0.832
200		0.075	0.975	0.841	0.945	0.689	0.916	85.211	0.859
50	SVM	0.088	0.952	0.815	0.917	0.651	0.880	82.554	0.815
100		0.138	0.869	0.745	0.841	0.532	0.880	75.641	0.697
150		0.163	0.783	0.692	0.791	0.435	0.853	70.321	0.619
200		0.161	0.797	0.696	0.800	0.445	0.849	70.747	0.628

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 2911 - 2919
https://publishoa.com
ISSN: 1309-3452

50	NN	0.083	0.980	0.808	0.901	0.627	0.893	82.051	0.780
100		0.087	0.972	0.825	0.930	0.671	0.901	86.671	0.890
150		0.151	0.961	0.804	0.926	0.661	0.899	88.001	0.811
200		0.078	0.878	0.755	0.913	0.631	0.880	89.411	0.791

We are getting the below result after simulation-

Other optiomal metrics measurement forRandomForestare*FPR=0.073,Precision=0.975,Recall=0.841,F1Score=0.945,MCC=0.0.689*.Comparativelyless performanceachievedbySVMwhere average *Accuracy= 74.78%* and *Kappa= 0.815* . The other metric soresfor SVM are *FPR = 0.088, Precision = 0.952, Recall =0.815,F1Score=0.917,MCC=0.651*. The optimal result are shonw by NN with average *Accuracy= 86.5%* and other measuerments stats are *FPR = 0.078, Precision = 0.980, Recall =0.825,F1Score=0.926,MCC=0.627*.
Sensitivity is the ratio of true positives & truepositives + false negatives and a value close to 1 isdesirable.Forthe*<RF,SVM,NN>*theobservedandstabilizedmeasurement for this metric is *<0.841,0.815,0.825>*. Similarly,specificity is a measurement of the ratio of true negatives&true negatives + false positives. Consequently, this should alsobe very near to 1. The score for our trio *<RF,SVM,NN>*is *<0.927,0.912,0.923>*.

TABLE3:Comparison with unimodal systems

Biometric System	**FAR**	**FRR**	**Avg Accuracy**
Face	10.52%	10.98%	81.54
Palmprint	12.36%	11.91%	81.65
Proposed Multimodal (Face+Palmprint)	**3.32%**	**2.92%**	**89.96**

TABLE4:Comparison of recognition rate

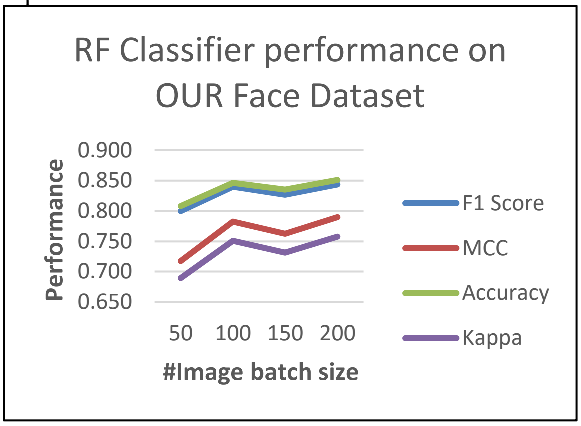
Approach	**Recognition rate %**		**Average**
	OUR FACE	**IITD Palmprint**	
RF	83.5	83.61	83.555
SVM	74.75	74.81	74.78
NN	86.42	86.53	86.475
Proposed Multimdoal	88.96	89.21	89.085

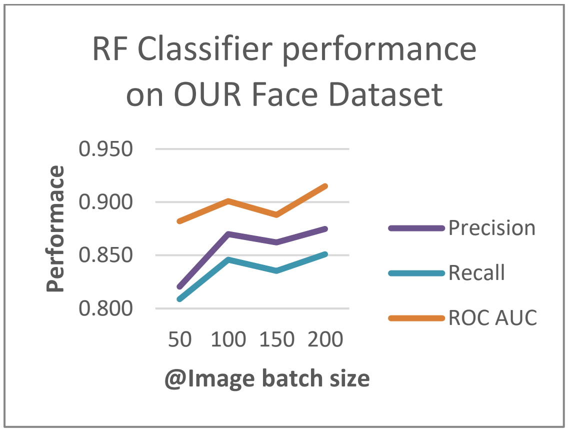
Best Peforming Model The analysis of table 3 & table 4 shows that the proposed Multimodal approach performs better compared to corresponding unimodal systems. The average *Accuracy* achieved 89.96%. While observing the average accuracy for individual unimodals systems Random Forest and NN are performing equally while SVM degraded comparatively.

Performance Representation through Box Plots Thevariability of the performance score for *RF*, *SVM*, and *NN* can be observed in Figures 1(a & b). Box plots show that the RF and NN are consistent over both the datasets while these show some skewness in IITD palm datasets. SVM has a considerably large variation in accuracy score in both datasets.

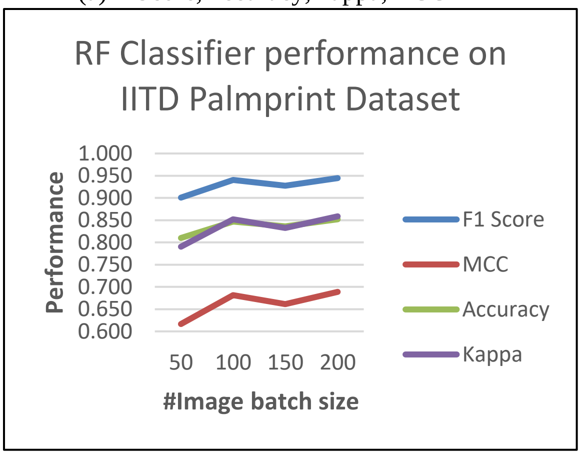
PerformanceRepresentationthroughlineCharts In the line chart so f Figures 2 to 4, for RF and NN, almost all the metrics show an increasing trend as the number of images in batch increases except *FPR* which shows downward progress. This is highly recommended in authentication and we achieve 2.92% After theslight initial increase, these upward progressing lines show constant progress with as minimum as 5 features onward.

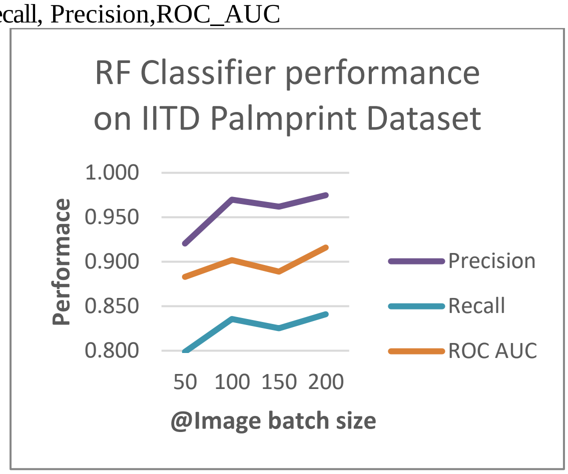
SVM classifier's performance is depicted in Figure 3and it is observed that almost all the metrics show decreasing trend as the number of images in the batch increases except *FPR* whichshowsalittleconstantprogress.Graphical representation of result shown below.





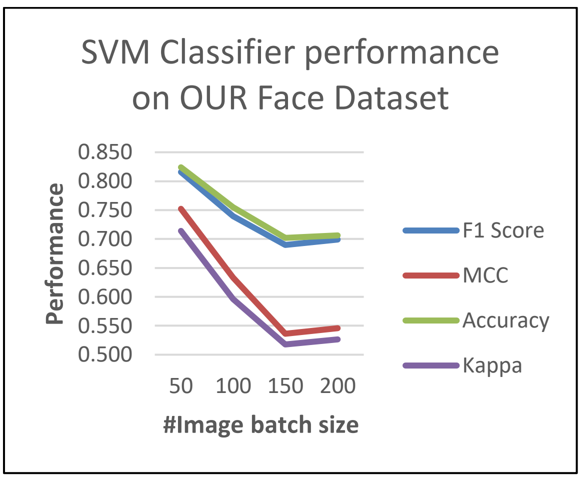
(a)F1Score,Accuracy,Kappa,MCC b)Recall, Precision,ROC_AUC

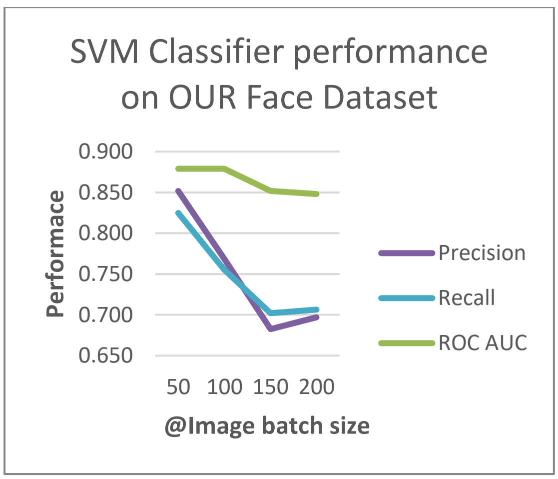




(c)F1Score,Accuracy,Kappa,MCC (d)Recall, Precision,ROC_AUC

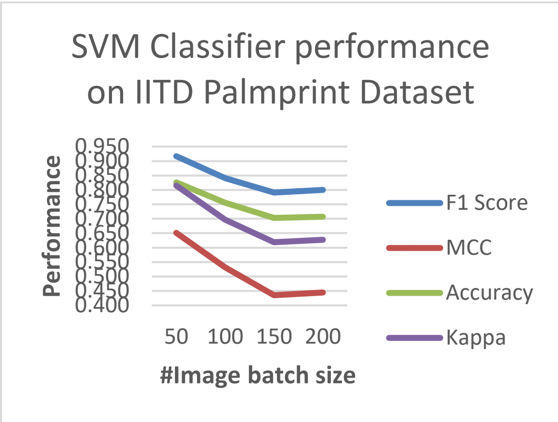
FIGURE2:PerformanceofRandomForestforNumberofSelectedImages (batch).

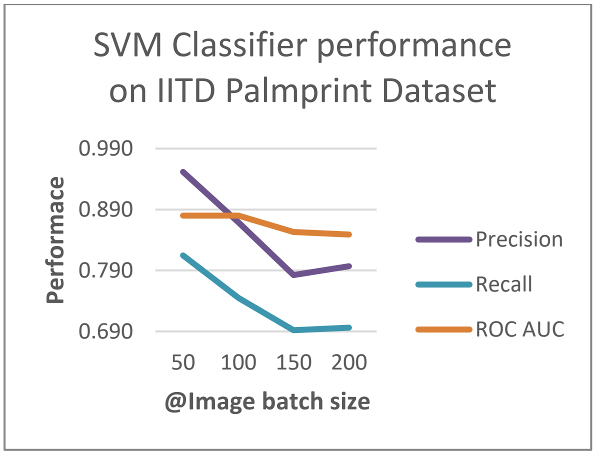




(a)F1Score,Accuracy,Kappa,MCC (b)Recall, Precision,ROC_AUC

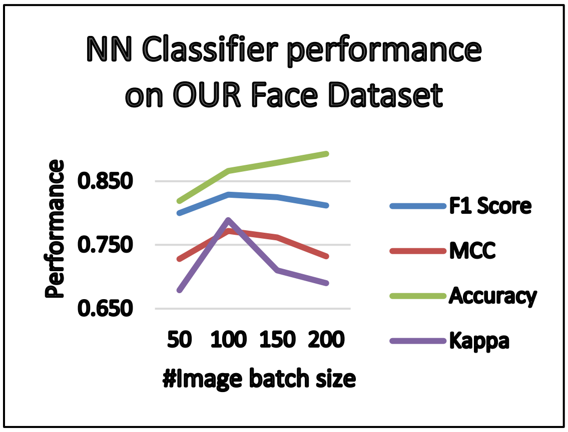
JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 2911 - 2919
https://publishoa.com
ISSN: 1309-3452

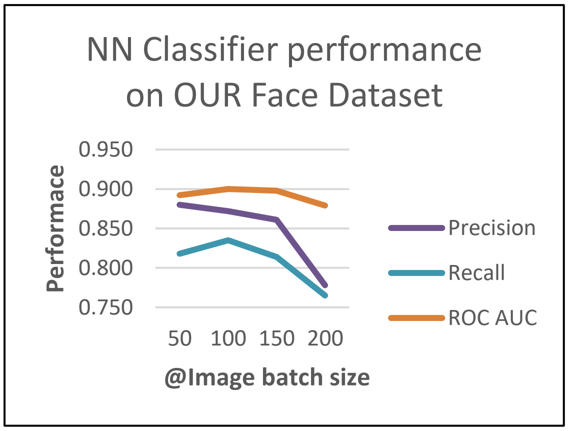




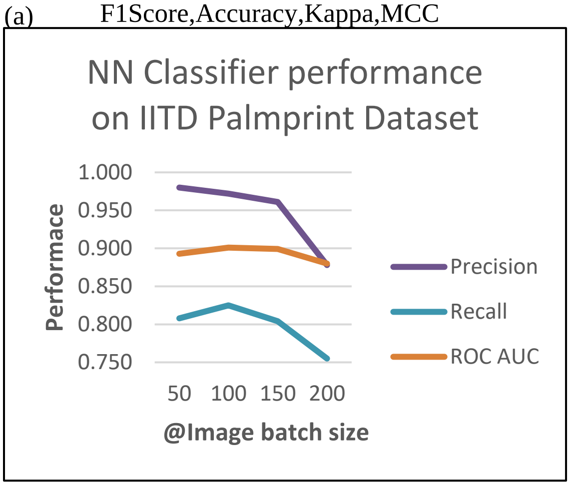
(c)F1Score,Accuracy,Kappa,MCC (d)Recall, Precision,ROC_AUC

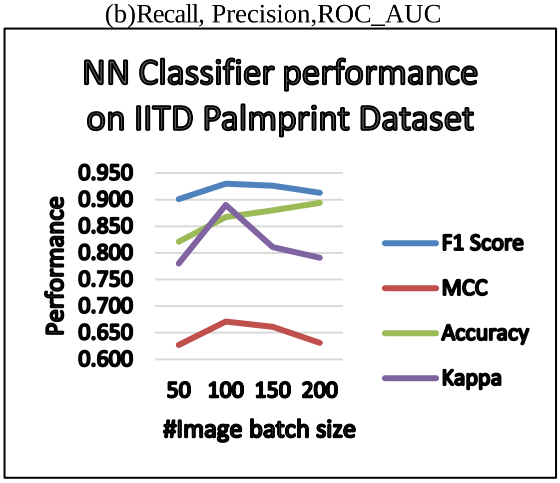
FIGURE3:PerformanceofSVMwithRespecttoNumberofSelectedImages (batch).





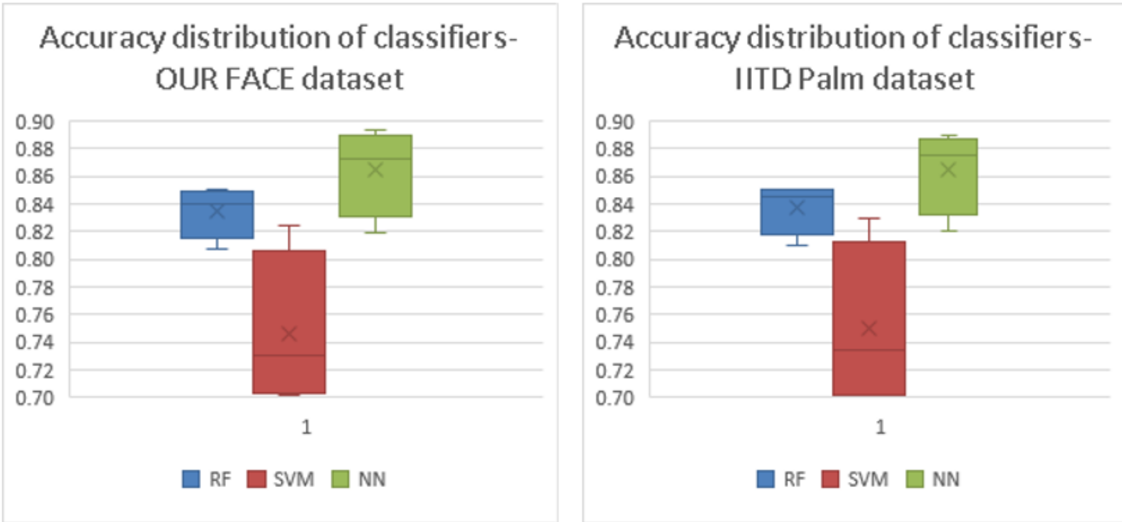
(a) F1Score,Accuracy,Kappa,MCC (b)Recall, Precision,ROC_AUC





(c)F1Score,Accuracy,Kappa,MCC (d)Recall, Precision,ROC_AUC

FIGURE4: PerformanceofNNwithRespecttoNumberofSelectedImages (batch).



(a) OUR FACE Dataset-Accuracy (b) IITD Palm Accuracy

5. CONCLUSIONS AND FUTURE WORK

The proposed work presents the biometric authentication system employing face and palmprint biometric traits.For the face OUR FACE dataset is used while palmprint dataset is available from IITD. The average accuracy, FAR , and FRR obtained through the the experimentation done on WEKA simulation tool for face are 81.54%, 10.52%, and 10.98% respectively. Similarly for palmprint these measuers obtained are 81.65%, 12.36%, and 11.91%. emphasizing that the performance with the parlmprint has a little improvement than that of with face but with the the higher cost of FAR and FRR. Combining these two independent system together to achieve multimodal system the performance achieved is considerably good in all three performance parameters. The accuracy, FAR and FRR for the proposed multimodal system are 89.96%, 3.32% , and 2.92% respectivevly.

The resultant multimodal system uses score level fusion to achieve this score. Here in this work the multimodal system is built and its performance copared with the individual components systems (e.g. face, palmprint) and achieved very high accuracy with minimum cost of FAR and FRR. For the future work deep learing is proposed to impletement such a similar system with improvement on the performance. Deep learning removes the burder of hand-crafeted feature extracton (or selection) and leads to more accuracy. Optimization for the optimum parameters is the other future objective.

REFERENCES

1. Abaza, A. and Harrison, M.A.F., Ear recognition: a complete system. In Biometric and Surveillance Technology for Human and Activity Identification, Vol. 8712, pp. 87120, 2013.
2. 1. Jung, Ho Yub, Yong Seok Heo, and Soochahn Lee. "Fingerprint Liveness Detection by a Template-Probe Convolutional Neural Network." IEEE Access 7 (2019):118986-118993.
3. Ghorbani, Mohammadjavad, Mahdi Alizadeh, Alireza Esfahani Omran, and Morteza Modarresi Asem. "An Investigative Review of Human Authentication Based on Fingerprint." In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1359-1366. IEEE, 2018.
4. Zhang, Yong, Dapeng Li, and Yujie Wang. "An indoor passive positioning methodusingCSIfingerprintbased onAdaboost." IEEESensorsJournal 19, no. 14(2019):5792-5800.
5. Khan, Muhammad Jamil, Muhammad Ali Riaz, Humayun Shahid, Mansoor Shaukat Khan, Yasar Amin, Jonathan Loo, and Hannu Tenhunen. "Texture representation through overlapped multi-oriented tri-scale local binary pattern."IEEEAccess7 (2019):66668-66679.
6. Yörük, E., Dutağaci, H. and Sankur, B., Hand biometrics. Image and vision computing, Vol. 24(5), pp. 483-497, 2006.
7. Chlaoua, Rachid, Abdallah Meraoumia, Kamal Eddine Aiadi, and Maarouf Korichi. "Deep learning for finger-knuckle-print identification system based on PCANetandSVMclassifier."EvolvingSystems10, no.2 (2019):261-272.

8. Yan, Wei Qi. "Biometrics for surveillance." In Introduction to Intelligent Surveillance, pp.127-153.Springer, Cham, 2019.
9. Zerdoumi, Saber, Aznul Qalid Md Sabri, Amirrudin Kamsin, Ibrahim Abaker Targio Hashem, Abdullah Gani, Saqib Hakak, Mohammed Ali Al-Garadi, and Victor Chang. "Image pattern recognition in big data: taxonomy and open challenges: survey." Multimedia Tools and Applications 77, no. 8 (2018): 10091-10121.
10. Wani, M. Arif, Farooq Ahmad Bhat, Saduf Afzal, and Asif Iqbal Khan. "Supervised Deep Learning in Fingerprint Recognition." In Advances in Deep Learning, pp.111-132.Springer, Singapore, 2020.
11. Win, Khin Nandar, Kenli Li, Jianguo Chen, Philippe Fournier Viger, and Keqin Li. "Fingerprint classification and identification algorithms for criminal investigation:Asurvey."FutureGenerationComputerSystems (2019).
12. Belciug, Smaranda, and Florin Gorunescu. "Data Mining-Based Intelligent DecisionSupport Systems." In IntelligentDecision SupportSystems—AJourney toSmarterHealthcare, pp.103-258.Springer, Cham, 2020.
13. Uhl, Andreas. "State of the Art in Vascular Biometrics." In Handbook of VascularBiometrics,pp.3-61.Springer,Cham,2020.
14. Miikkulainen, Risto, Jason Liang, Elliot Meyerson, Aditya Rawal, Daniel Fink, Olivier Francon, Bala Raju et al. "Evolving deep neural networks." In Artificial Intelligence in the Age of Neural Networks and Brain Computing, pp. 293-312. AcademicPress, 2019.
15. Obaidat, Mohammad S., Issa Traore, and Isaac Woungang, eds. BiometricBasedPhysicalandCybersecuritySystems.Vol.368.Springer, 2019.
16. Meng, Fanzhi, Yunsheng Fu, and Fang Lou. "A network threat analysis method combined with kernel PCA and LSTM-RNN." In 2018 Tenth International Conference on Advanced Computational Intelligence (ICACI), pp. 508-513. IEEE,2018
17. Abaza, A., Ross, A., Hebert, C., Harrison, M.A.F. and Nixon, M.S., A survey on ear biometrics, ACM computing surveys (CSUR), Vol. 45(2), pp. 22, 2013.
18. Unar, J.A., Seng, W.C. and Abbasi, A., A review of biometric technology along with trends and prospects, Pattern recognition, Vol. 47(8), pp. 2673-2688, 2014..
19. Ahuja, M.S. and Chabbra, S., A survey of multimodal biometrics. International Journal of Computer Science and its Applications, Vol. 1, pp. 157-160, 2011.
20. Alaraj, M., Hou, J. and Fukami, T., A neural network based human identification framework using ear images, In TENCON 2010-2010 IEEE Region 10 Conference IEEE, pp. 1595-1600, 2010.
21. Anil K. Jain, Arun Ross and SalilPrabhakar, An Introduction to Biometrics, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14(1), 2004.