iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 Issue: IX Month of publication: September 2024

DOI: https://doi.org/10.22214/ijraset.2024.63926

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IX Sep 2024- Available at www.ijraset.com

Enhanced IRIS Authentication Model - A Gradual Feature Selection Reduction Approach Augmented with Soft Vote Ensemble

Dr Ibharalu F.T, Ajayi A.F, Adebayo A.A, Olukumoro S.O, Akinade A.O
Department of computer science, federal university of agriculture
Department of computer science,Yaba College of technology

Abstract: The issues identified in primary studies showed the need for a reliable user authentication system and thereby constitute low performance metrics. This include the restriction of feature extraction to single image filter thereby returning relative feature vector size of biological traits returns sub-optimal models for a data mining-based authentication system. The aim of this study is to enhance the performance of existing models deploy SqueezeNet embedding for image feature extraction as well as the implementation of synthetic oversampling and employment of vote ensemble model to address the widespread problem of under-fitting and over-fitting observed in literatures. The study further implemented feature engineering technique of feature selection (through information gain and Relief-F) to enhance model performance by eliminating feature redundancy. The user authentication was actualized through Vote ensemble modelling of SMO, MLP, and the DT base learners. Results from the study showed a precision of 75.37%, an accuracy of 83.7%, F-Measure value of 0.781917211 and ROC AUC value of 0.833333333 indicating that the model has a good capability to differentiate between the positive and negative classes.

Keywords: Feature extraction, Feature engineering, SqueezeNet, Vote ensemble, SMO.

I. INTRODUCTION

An authentication system is a security concept which serves as a proactive measure to forestall and prevent unauthorized access to a service or data [33]. Besides what a user knows the identity authentication factors of username and or password, biometrics encapsulates the unique biological traits of users in what is often referred to as *what the user* is [28]. Biometrics have likewise proven to be more efficient than the use of tokens or hardware items (*what a user has)* because of its distinguishing factor of being more of who a person is than any other secondary means of authentication [52]. The performance metrics of biometric systems have been proven to surpass even multi-factor cryptographic authentication systems for access control. The biological, physiological or behavioral characteristic nature of human beings, baring its uniqueness in mind, reliably identifies an individual. Common biometric features used for authentication systems include the fingerprint scans, facial or retina scans, and sometimes voice for voice recognition authentication systems [7]. The same biological attributes are captured for the verification purposes hence discouraging impersonation, identity theft, identity mismatch etc. Upon a successful matching of extracted biological attributes with those in the database, data or service access is granted the user. Biometrics therefore is the science that entails both identification and verification of humans relying on the basis of human measurable traits [7]. A system with the functionality of biometrics could uniquely identify users by their measurable traits before access is granted or denied. Indeed, diversified researches returns iris as one of the most important traits that guarantees higher accuracy, recognition and efficiency in identity recognition [49]. The iris feature is believed to consist more than 250 unique elements, which describes human identity through numeric feature vectors [5]. This study seeks to enhance the performance of existing models in literature. In due course, the study would be enhancing face and iris user authentication systems and increase the performance and accuracy of the model.

II. RELATED WORKS

Authentication systems are security measures established for data or system safety purposes that requires inputs for access or operations [16]. Authentication therefore encompasses techniques and procedures deployed for determining whether someone or something is who or what they claim to be. Authentication systems could also provide for access control by mapping user inputs with information in the database for correlation and verification purposes thereby ensuring a secure process and system [8].

For user identity purposes, user identification number is deployed when user provide credentials such as a password which must match information registered for the user in the database. The authentication system is further explain based on the terms; Knowledge-based factor, Possession-based factor, Inherence-based factor, location-based factor, and time-based factor.

Knowledge-based factor, popularly referred to as *something you know*, consist of authentication credentials that involves information that a user possesses, including individual identification number, user-generated username, a password, answer to a secret question etc.

Possession-based factor is referred to as *something the user has including* item-based credentials that a user owns and carry along such as a hardware device, a security token or even a mobile phone used to text message or to generate a one-time password or PIN.

Inherence-based factor is something a user is, which is characteristically a biometric identification system comprising of fingerprints, facial recognition, thumbprints, retina scan etc.

The location factor is often deployed as an addendum or adjunct *to other factors with the aid of* global positioning systems with relative levels of accuracies. The location factor seldom stands on its own for authentication but it supplements other factors thereby providing means of ruling out some requests. It can for instance prevent an attacker located in a pre-defined remote geographical area from posing as a user. Similar to the aforementioned location-based is the time-based factor which refers to when *you are authenticating.* However, it is often deployed as an addendum mechanism for weeding out attackers who intends to access a resource at a specific time when the said resource is not available to the authorized user. It is often deployed alongside the location-based factor. As aforementioned, several authentication factors are deployable for securing an entity against unauthorized attacks either as a two-factor or a multi-factor authorization access control system. However, an advanced and more reliable method for user authentication is offered by the biometric authentication system. Rather than relying on a shared secret or key, biometric system authentication deploys unique physiological or behavioral features of a person as an attribute for verification and authentication. Hence, genuine users are recognized through distinct characteristic features of fingerprints, ear shapes, irises etc. [7].

One of the biological means of uniquely identifying a user is through their facial attributes through the instrumentality of technology [31]. A facial identification system uses biometrics for a 1-1 mapping of facial features from an image or video. The extracted features from the image is compared with the information on the database of pre-registered faces to purposely find a match. Identity is therefore verified for access purposes [19]. The process of using visible plus near-infrared light to capture a high contrast photograph of an individual’s iris for verification purposes is referred to as iris recognition [46]. In the same category as face or fingerprint recognition technologies, iris recognition is a biometric system use case for the purpose of user authentication. Practitioners compare iris of suspects with pre-registered set in the database through a scanning technology to ascertain or confirm the user’s identity [46].

III. METHODOLOGY

The proposed bimodal authentication is a six-phase biometrics based user verification system that combines iris and facial pattern recognition attributes for the purpose of training a machine learning model. The training set is made up of iris and facial images of both authentic and unauthentic users, which is then fitted by a Vote ensemble learner algorithm for the purpose of building the artificial intelligent authentication system. Feature vectors are extracted from the input data through knowledge transfer technology of image embedding functionality and are consequently concatenated for the ensuing phase of feature engineering. The output of the feature engineering makes up the ideal training set for the consecutive machine learning phase.

The supervised machine learning training produces the proposed intelligent model which could uniquely recognize biological patterns from a user who intends to gain access through the machine learning testing phase. The result of the authentication determines if access is granted or denied at the sixth phase of the proposed methodology.

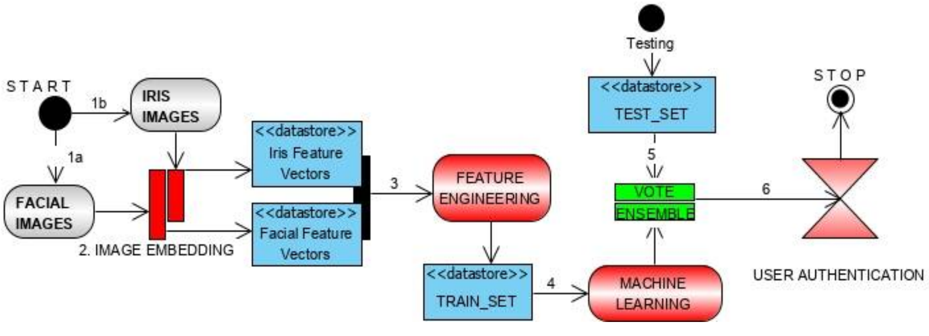

Fig. 1 Proposed bimodal authentication framework

The first phase of the framework is the image acquisition phase when dual image inputs of iris and facial is captured for instance on the dataset as shown in Fig.1. The images belong to authorized users' category and the non-authorized users, each having a pair of facial and iris representations. Instances for each data feature has more than one representation on the dataset to avail the predictive model an armful opportunity to robust pattern recognition. The sizes of the images notwithstanding, two sets are prepared for this study including the training set and test set.

Table I: Summary of existing work

S/N	Author	Methodology	Strength	Limitation
1.	(Joseph *et al.*, 2020) [25]	AES, Blowfish, DES	i. Multimodal approach of the methodology through cryptography ensemble ii. The bio-cryptography approach of the study	i. No optimal feature selection task is implemented ii. Non-implementation of image enhancement tasks
2.	(Ibtehaz, *et al.*, 2021) [20]	Deep Learning	i. Incorporation of deep machine leaning ii. Robust enrollment and evaluation dataset iii. Synthetic minority oversampling of training set	i. Vulnerability of the biometric system ii. No feature selection mechanism
3.	(Sharma, *et al.*, 2021) [47]	Quality of minutiae points	i. Optimization of the minutiae point system ii. Homogeneous nature of the dataset	i. Single factor authentication system ii. Ensemble of machine learning with biometrics would return better efficiency
4.	(Raja *et al.*, 2015) [42]	SIFT and BSIF	i. Implementation of the robust OSIRIS v4.1 on Android operating systems is novel ii. Multimodal approach of the methodology	i. Non-deployment of feature selection ii. Infusion of biometrics and machine would be better
5.	(Yang, *et al.*, 2020) [55]	Feature-adaptive methodology	i. Compatibility nature of proposed system based on the heterogeneous nature of dataset ii. The feature-adaptive nature of the proposed model for the generation of the projection matrix	i. Vulnerability of the biometric-only methodology ii. No feature selection scheme incorporated into the methodology
6.	(Jahan, *et al.*, 2018) [22]	Fast stereo matching algorithm with fingerprint	i. Reduction of computational cost in biometric matching ii. The fast stereo algorithm enhanced speed performance	i. No feature selection mechanism ii. Machine learning would be a better complement with biometrics

7.	(Yang, *et al.*, 2019) [54]	Steganography and PKI	i. Diffusion of record multiplicity-based attacks ii. Deployment of cancelable biometric methodology	i. Vulnerability of the biometric system is not mitigated ii. Vulnerability of the single factor system
8.	(Ying & Nayak, 2019) [56]	Self-certified Public Key Cryptography and Elliptic Curve Cryptography	i. Self-certification of the public key is an advantage ii. The public key cryptography	i. Ensemble with biometrics authentication system would be better ii. Non mitigation of cryptography vulnerability
9	(Sajjada, *et al.*, 2019) [44]	Fingerprint with Convolutional Neural Network	i. Multimodal authentication system ii. Multi-factor input system	i. Homogeneous nature of data ii. No over-fitting and under-fitting tradeoff
10	(P.Punithavathi, *et al.*, 2019) [39]	Biometric system	i. Ensemble of machine learning with cryptography ii. cancelable biometric system	i. Limitation of the machine learning approach due to homogeneous nature of data ii. Prevalent under-fitting and over-fitting tradeoff

Feature engineering concepts adopted in this study includes the information gain feature selection and the synthetic minority oversampling technique. The feature selection phase is to ensure all variables encapsulated in the dataset are useful for the machine learning modelling. Inclussion of reduncdant variables reduces the generalization ability of the model which will eventually reduce the performance metrics of the chosen classifier. Therefore, the goal of the feature selection technique is to find and deploy the best dataset of features that helps to build an accurate model.

Recently, a surge of deployment is witnessed in studies with Support Vector Machines (SVM) as SVM have empirically shown to return good generalization performance on different problems [40] including character recognition [29], face detection, pedestrian detection [38], and text categorization [23]. However, the SMO was introduced as an improved variant of the SVM which is theoretically simple, easy to execute, faster, and with better scaling properties for difficult problems than the traditional SVM training algorithm [40]. The SMO is an optimized variant of the traditional secure vector machine (SVM) majorly conceptualized to address the optimization problem of the secure vector machine. It is an effective method for training SVM on classification tasks reputable for sparse data sets and it is different from SVM algorithms as it does not entail a quadratic programming solver.

Research showed that SVMs can be optimized via the decomposition of a large quadratic programming problem into smaller mini-problems. Optimizing individual mini-problem therefore minimizes the initial quadratic programming problem once no further progress is possible on all of the sub-problems. The original quadratic programming problem is thereby solved. Since individual sub-problem can have stable magnitude, optimization through decomposition is possible with a permanent size. Decomposition in SMO therefore is far more efficient than the quadratic programming approach of SVM. Since SMO deploys a sub-problem of dual size, each sub-problem therefore has a methodical solution. While other methods towards solving the quadratic programming problem of SVM hold great promise, SMO is the only optimizer that explicitly exploits the quadratic form of the objective function and simultaneously uses the analytical solution which is therefore applied in this methodology for a better result.

Algorithm: The Sequential Minimal Optimization Algorithm

```
Input: Ground truth labels ($x_t$, $y_t$), t = 1, ..., n, and a small constant f.
Output: optimal output μ.
$i \leftarrow -1; j \leftarrow -1$
$\tilde{\nabla} f(\mu) \leftarrow 0$
while μ is not optimal do
    Unsystematically permute samples.
    $for\ t \leftarrow 1 \ldots n\ do$
        $\tilde{\nabla} f(\mu)_t = w^T x_t - y_t$
        if $\tilde{\nabla} f(\mu)_t < \tilde{\nabla} f(\mu) - f$ and $t \in I_{low}$ then        ⊿ $I_{low}$ is defined in (4).
            $\tilde{\nabla} f(\mu)i \leftarrow \tilde{\nabla} f(\mu)_t$
            $i \leftarrow t$
        $else\ if$ $\tilde{\nabla} f(\mu)_t > \tilde{\nabla} f(\mu) + f$ and $t \in I_{up}$ $then$        ⊿ $I_{up}$ is defined in (4).
            $\tilde{\nabla} f(\mu)_j \leftarrow \tilde{\nabla} f(\mu)_t$
            $j \leftarrow t$
        $end\ if$
        $if\ i \neq -1\ and\ j \neq -1\ then$
            update $\mu_i$and $\mu_j$ according to (13)
            update w according to (14)
            update $\tilde{\nabla} f(\mu)$ according to (18)
            $i \leftarrow -1; j \leftarrow -1;$
        end if
    end for
end while
```

Information gain is used to compute the entrophy reduction during the transformation of a database. It is used for feature selection by evaluating the information gain of each variable within the context of the target variable. Information is computed for a split by finding the difference between entropies of each branch from the original entropy. Therefore, the entropy of a random variable X is calculated thus: X_i

$$= \sum [p(Xi) \times log2(Xi)] \qquad (1)$$

where X_i represents each possibility of (i^{th}) of value X, and $p(X_i)$ is the probability of a particular posible value of X.

The metric used in the study include Precision, F-Measure**,** Received Operating Characteristic (ROC)**,** Area Under the ROC Curve (AUC)**,** False Positive Rate (FPR)**,** True Negative Rate (TNR)**,** False Negative Rate (FNR) and Accuracy.

IV. IMPLEMENTATION

The feature extraction, data mining and feature engineering phases of the framework were implemented using Orange data mining toolkit composed of python libraries. The acquired iris and facial images are uploaded on the application to extract image embedding, which are numeric vectors representing the genetic representations of each image (iris and facial) instance. The Orange widgets are presented and their resulting outputs. The Jupyter notebook of the Anaconda navigator used for the machine learning phases are also presented. The implementation and testing was performed on Lenovo e-450 intel processor 1.65 GHz, 4GB RAM and 148 GB Hard Disk running Microsoft Windows 10 Operating System.

The data mining and feature extraction phases of the implementation was executed on the integrated development environment of the Orange data mining tool [12], while the machine learning functionalities were implemented using python programming on the Anaconda navigator environment [43]. The various python libraries employed in the coding of the three base learners are discussed, as well as the Vote ensemble implementation.

V. RESULTS

The public data employed for this study is acquired from the public repository, Kaggle. The data [21] consist of two folders including the image folder and another folder for the labels of each image. Each of the individuals captured in the database (103 of them, presented in Figure 5) has 12 images each, showing different parts of their facials.

Therefore, there are 1236 image instances in the acquired dataset. The activity overview of the data indicates there has been 2879 views, 85 downloads for research purposes, and a 0.03 download per view metric. Download rate peaks in November, 2022, May 2023 till July 2023, and in September 2023, showing a growing interest in the training dataset. For the purpose of this study, each of the image signals are preprocessed to extract the iris of each instance represented in the dataset.

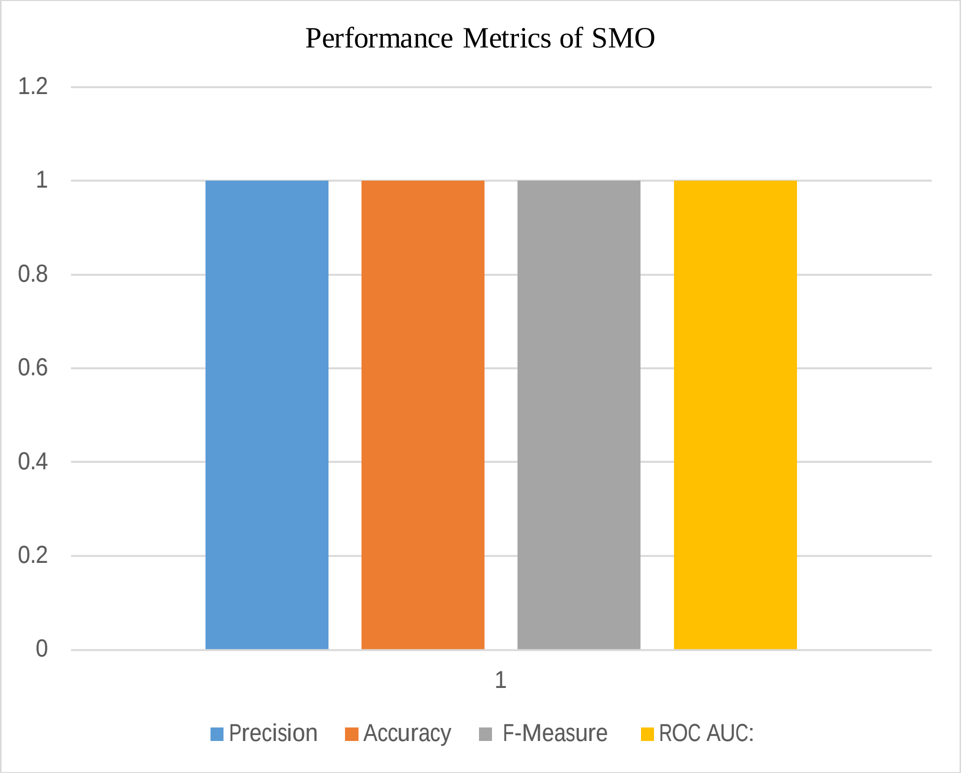

Fig. 2 Performance metrics of the SMO

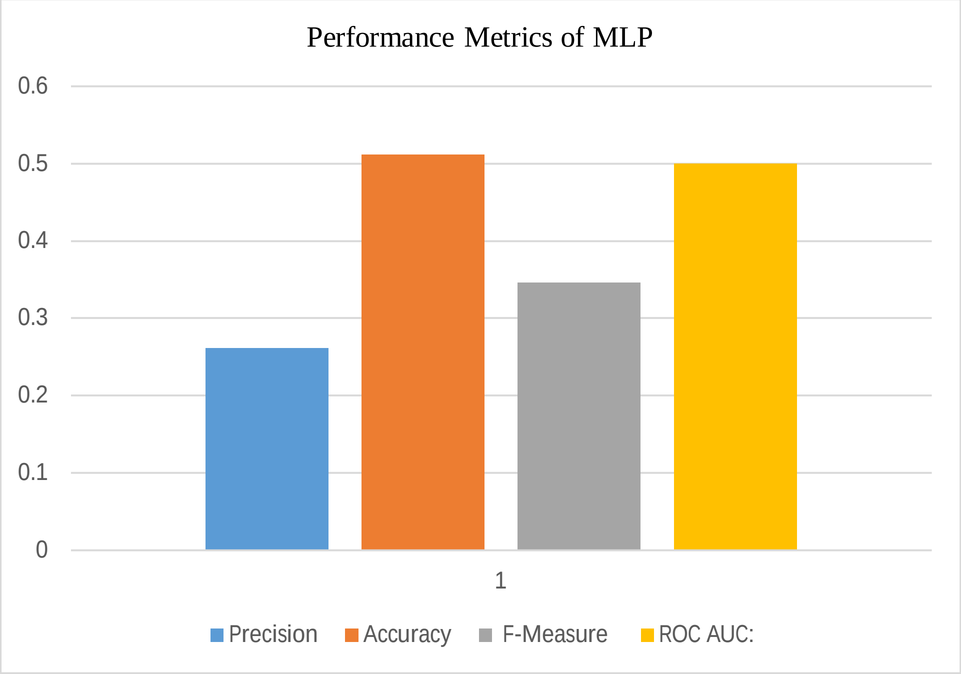

Fig. 3 Performance metrics of the MLP

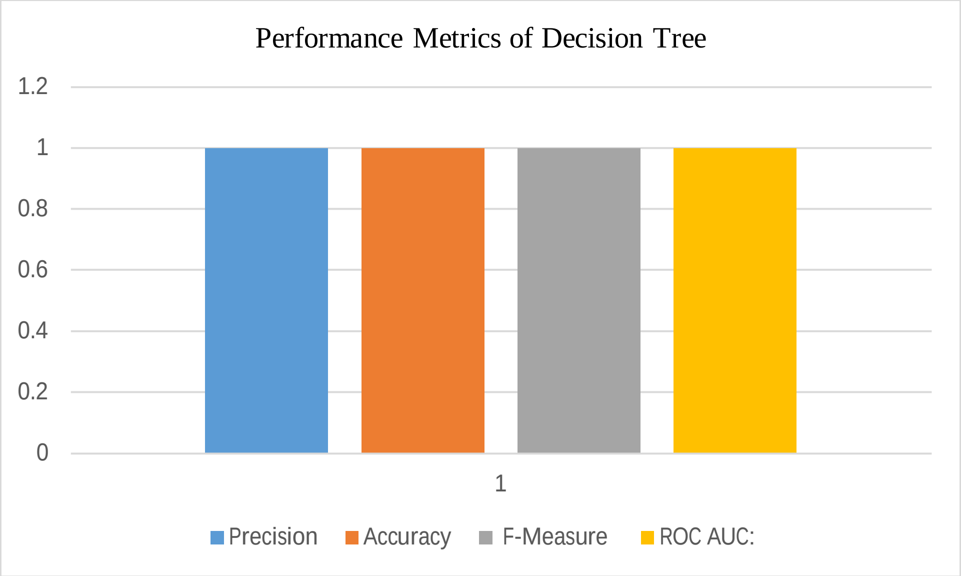

Fig. 4 Performance metrics of the DT

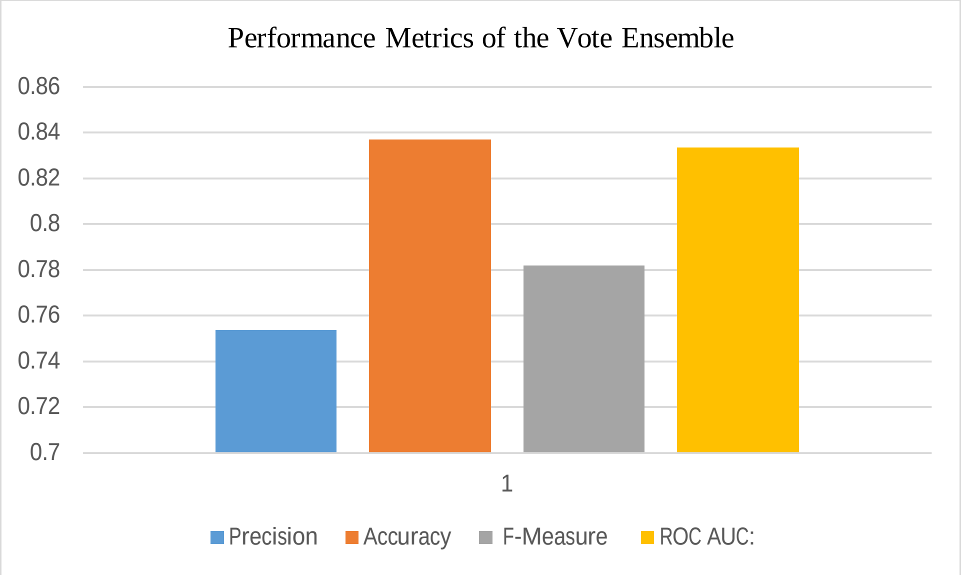

Fig. 5 Performance metrics of the Vote ensemble

Table II: Vote ensemble, the performance metrics

METRIC	VALUE
Precision	75.37%
Accuracy	83.70%
F-Measure	0.781917211
ROC AUC	0.833333333

The classification results are shown the Table II as well as in Fig. 2 to Fig. 5. The Fig. 2 depicts the classification results using Sequential Minimal Optimization (SMO). The Fig. 3 depicts the classification results using Multi-Layer Perceptron (MLP). The Fig. 4 depicts the classification results using Decision Tree (DT). While the Fig. 5 depicts the classification results using Vote ensemble.
The Support Vector Machine (SMO) exhibited impeccable performance with perfect precision, accuracy, F-measure, and ROC AUC.

In contrast, the Multilayer Perceptron (MLP) demonstrated lower precision, accuracy, F-measure, and ROC AUC, highlighting the challenges associated with its application. The Decision Tree (DT) model also achieved outstanding performance with perfect precision, accuracy, F-measure, and ROC AUC. Furthermore, the Vote ensemble model yielded commendable results, showcasing competitive precision, accuracy, F-measure, and ROC AUC values, indicating its robustness in predictive capabilities.

The study encountered some issues related to class imbalance and enhance the model's predictive capabilities. Similarly, there is the need to identify the most relevant and significant attributes for user authentication as well as the need for a vast range of datasets to assess the generalizability and scalability of the proposed model. Furthermore, the study needs a deeper insight into the decision-making process of the model to improve the interpretability and transparency of the authentication system.

VI. CONCLUSION

The study successfully accomplished its objectives, which included the deployment of SqueezeNet embedding for feature extraction, the implementation of synthetic oversampling, the utilization of feature selection techniques, and the development of a Vote ensemble model for user authentication. The Support Vector Machine (SMO) exhibited impeccable performance with perfect precision, accuracy, F-measure, and ROC AUC. In contrast, the Multilayer Perceptron (MLP) demonstrated lower precision, accuracy, F-measure, and ROC AUC, highlighting the challenges associated with its application. The Decision Tree (DT) model also achieved outstanding performance with perfect precision, accuracy, F-measure, and ROC AUC.

Further research work is required to examine the utilization of additional oversampling techniques and ensemble methods to comprehensively address issues related to class imbalance and enhance the model's predictive capabilities.

Performing an in-depth research into more sophisticated feature selection techniques and investigate their impact on model performance to identify the most relevant and significant attributes for user authentication is required for further study.

Further studies are required to perform extensive experiments with diverse datasets to evaluate the generalizability and scalability of the proposed model, thereby ensuring its applicability to a wide range of real-world biometric authentication scenarios.

Future study could explore the implementation of explainable AI methodologies to provide insights into the decision-making process of the model and enhance the interpretability and transparency of the authentication system.

VII. ACKNOWLEDGMENT

This is to acknowledge Dr ibharalu and other contributors for their assistance and support for the successful completion of this paper we sincerely appreciate all your efforts.

REFERENCES

[1] Abbas, A., Abdelsamea, M. M., & Gaber, M. M. (2021). Classification of COVID-19 in chest X-ray images using DeTraC deep convolutional neural network. Applied Intelligence, 854–864.

[2] Abo-Zahhad, M., Ahmed, S. M., & Abbas, S. N. (2016). A new multi-level approach to EEG based human authentication using eye blinking. Pattern Recognition Letters, 216-225.

[3] Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two factor authentication using mobile phones. 2009 IEEE/ACS International Conference on Computer Systems and Applications (pp. 641-644). IEEE.

[4] Alsaadi, M. I. (2015). Physiological biometric authentication systems, advantages, disadvantages and future development: A review. International Journal of Scientific & Technology Research, 285-289.

[5] Ammour, B., Boubchir, L., Bouden, T., & Ramdani, M. (2020). Face-Iris Multimodal Biometric Identification System. Electronics , 1-18.

[6] Banyal, R. K., Jain, P., & Jain, V. K. (2013). Multi-factor authentication framework for cloud computing. 13th International Conference on Computational Intelligence, Modelling and Simulation. IEEE.

[7] Bolle, R. M., Connell, J. H., Ratha, S., K., N., & W., A. (2013). Guide to biometrics. Springer Science & Business Media.

[8] Burrows, M., Abadi, M., & Needham, R. M. (2009). A logic of authentication. Proceedings of the Royal Society of London, (pp. 233-271).

[9] Chen, S., Pande, A., & Mohapatra, P. (2014). Sensor-assited facial recognition: an enhanced biometric authetication system for smartphones. 12th annual international conference on Mobile systems, applications, and services, (pp. 109-122).

[10] Conklin, A., Dietrich, G., & Walz, D. (2004). Password-based authentication: a system perspective. 37th Proceedings of the Annual Hawaii International Conference on System Sciences (pp. 1-10). IEEE.

[11] Crepeau, C. R. (2001). Super Bowl XXXV and Its Excesses .

[12] Demšar, J., & Zupan, B. (2012). Orange: Data mining fruitful and fun. Inf. Družba IS, 1-486.

[13] Gandhi, V. (2019). A comprehensive guide to Ensemble learning . Retrieved from Kaggle: https://www.kaggle.com/vipulgandhi/a-comprehensive-guide-to-ensemble-learning

[14] Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perception of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers and Security, 208-220.

[15] Hodashinsky, I. A., Kostyuchenko, E. Y., Sarin, K. S., Anfilofev, A. E., Bardamova, M. B., Samsonov, S. S., & Filimonenko, I. V. (2018). IMAGE PROCESSING, PATTERN RECOGNITION. Computer Optics, 657–666.

[16] Hosseinzadeh, M., Vo, B., Ghafour, M. Y., & Naghipour, S. (2021). Electrocardiogram signals-based user authentication systems using soft computing techniques. Artificial Intelligence Review , pages667–709.

[17] Huang, X., Xiang, Y., Chonka, A., & Deng, J. Z. (2010). A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. IEEE Transactions on Parallel and Distributed Systems, 1390-1397.

[18] Huang, Y., Huang, Z., Zhao, H., & Lai, X. (2013). A new one-time password method. IERI Procedia, (pp. 32-37).

[19] Ibrahim, A., & Ouda, A. (2017). A hybrid-based filtering approach for user authentication . 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering. Canada: IEEE.

[20] Ibtehaz, N., Chowdhury, E. H., Khandakar, A., Kiranyaz, S., Rahman, M. S., Tahir, A., . . . Rahman, T. (2021). EDITH : ECG biometrics aided by Deep learning for reliable Individual auTHentication. arXiv:2102.08026v1, 1-23.

[21] Ivan, E. (2011, January 10). GI4E - Gaze Interaction for Everybody. Retrieved September 30, 2023, from Kaggle: https://www.kaggle.com/datasets/masurte/gi4e-gaze-interaction-for-everybody

[22] Jahan, S., Chowdhury, M., & Islam, R. (2018). Robust user authentication model for securing electronic healthcare system using fingerprint biometrics. International Journal of Computers and Applications, 233-242.

[23] Joachims, T. (2017). Text Categorization with Support Vector Machines. LS VIII Technical Report, No. 23, University of Dortmund. Retrieved from ftp://ftp-ai.informatik.unidortmund.de/pub/Reports/report23.ps.Z

[24] Jordan, M. I., & Mitchell, T. M. (2019). Machine learning: Trends, perspectives, and prospects. In Science (pp. 255-261). Washington: American Association for the Advancement of Science.

[25] Joseph, T., Kalaiselvan, S. A., Aswathy, S. U., Radhakrishnan, R., & Shamna, A. R. (2020). A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. Journal of Ambient Intelligence and Humanized Computing , 1-9.

[26] Kanade, S., Petrovska-Delacretaz, D., & Dorizzi, B. (2010). Obtaining cryptographic keys using feature level fusion of iris and face biometrics for secure user authentication . 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (pp. 138-145). IEEE.

[27] Kim, D., & Shin, J.-I. (2016). Design of a secure biometric authentication framework using PKI and FIDO in fintech environments. International Journal of Security and its Applications, 69-80.

[28] Krishnmaoorthy, S., Rueda, L., Saad, S., & Elmiligi, H. (2018). Identification of user behavioral biometrics for authentication using keystroke dynamics and machine learning . 2018 2nd International Conference on Biometric Engineering and Applications , (pp. 50-57).

[29] LeCun, Y., Jackel, L. D., Bottou, L., Cortes, C., Denker, H., Drucker, J., . . . Vapnik, V. (2015). Learning Algorithms for Classification: A Comparison on Handwritten Digit Recognition. Neural Networks: The Statistical Mechanics Perspective, 261-276.

[30] Lee, H. J., Ullah, I., Wan, W., Gao, Y., & Fang, Z. (2019). Real-time vehicle make and model recognition with the residual SqueezNet architecture . Sensors .

[31] M., M. V., Alex, O., & Terzopoulos, D. (2002). Multilinear image analysis for facial recognition. Object recognition supported by user interaction for service robots , IEEE.

[32] Manchev, N. (2021, May 20). SMOTE Oversampling Technique. Retrieved from Domino DataLab: https://blog.dominodatalab.com/smote-oversampling-technique

[33] Mihajlov, M., Jerman-Blazic, B., & LLievski, M. (2011). ImagePass-Designing graphical authentication for security. 2011 7th International Conference on Next Generation Web Services Practices (pp. 262-267). IEEE.

[34] Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. Decision Support Systems, 1-14.

[35] Olaleye, T. O., & Vincent, O. R. (2020). A Predictive Model for Students’ Performance and Risk Level Indicators Using Machine Learning. 2020 International Conference in Mathematics, Computer Engineering and Computer Science (pp. 1-7). Lagos: IEEE.

[36] Olaleye, T., Arogundade, O., Adenusi, C., Misra, S., & Bello, A. (2021). Evaluation of Image Filtering Parameters for Plant Biometrics Improvement Using Machine Learning. icSoftComp (pp. 301-315). Springer.

[37] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography.

[38] Oren, M., Papageorgious, C., Sinha, P., Osuna, E., & Poggio, T. (193-199). Pedestrian Detection Using Wavelet Templates. Proc. Computer Vision and Pattern Recognition, 2017.

[39] P.Punithavathi, S.Geetha, Karuppiah, M., Islamc, S. H., Hassand, M. M., & Choo, K.-K. R. (2019). A lightweight machine learning-based authentication framework for smart IoT devices. Information Sciences, 255-268.

[40] Platt, J. C. (2018). Sequential Minimal Optimization: A Fast Algorithm for Training Support Vector Machines. Microsoft Research, 1-22.

[41] Rahman, M. N., Rahman, A. A., Seyal, A. H., & Kamarudin, N. (2014). Facial recognition using eigenfaces approach. International Conference on Global Economy, Commerce and Service Science .

[42] Raja, K. B., Raghavendra, R., Stokkenes, M., & Busch, C. (2015). Multi-modal Authentication System for Smartphones Using Face, Iris and Periocular. ICB 2015 (pp. 143-150). IEEE.

[43] Rolon-Mérette, D., Ross, M., Rolon-Mérette, T., & Church, K. (2016). Introduction to Anaconda and Python: Installation and setup. Quant. Methods Psychol, 16(5), S3-S11.

[44] Sajjada, M., Khan, S., Hussain, T., Muhammad, K., Sangaiahc, A. K., Castiglioned, A., . . . WookBaik, S. (2019). CNN-based anti-spoofing two-tier multi-factor authentication system. Pattern Recognition Letters, 123-131.

[45] Satpathy, S. (2020, October 6). Home page. Retrieved from Analytics Vidhya: http://www.analyticsvidhya.com/blog/2020/10/overcoming-class-imbalance-using-smote-techniques

[46] Schwartz, N. A. (2019, October 25). Iris Recognition. Retrieved from Electronic Frontier Foundation: https://www.eff.org/pages/iris-recognition

[47] Sharma, U., Tomar, P., Ali, S. S., Saxena, N., & Bhadoria, R. S. (2021). Optimized Authentication System with High Security and Privacy . Electronics , 1-23.

[48] Symanovich, S. (2021, August 20). What is facial recognition? How facial recognition works. Retrieved from Norton: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

[49] Szymkowski, M., Jasiński, P., & Saeed, K. (2021). Iris-based human identity recognition with machine learning methods and discrete fast Fourier transform. Innovations in Systems and Software Engineering, 309-317.

[50] Vazquez-Fernandez, E., & Gonzalez-Jimenez, D. (2016). Face recognition for authentication on mobile devices. Image and Vision Computing, 31-33.

[51] Velasquez, I., Angelica, C., & Rodriguez, A. (2018). Authentication schemes and methods: A systematic literature review. Information and Software Technology, 30-37.

[52] Wilson, P. (2001). Importance of Biometrics to Business .

[53] Wilson, W. B. (1964). Facial recognition project report. Panoramic research inc.

[54] Yang, W., Wang, S., Hu, J., Ibrahim, A., Zheng, G., Macedo, M. J., . . . Valli, C. (2019). A Cancelable Iris- and Steganography-Based User Authentication System for the Internet of Things. MDPI.

[55] Yang, W., Wang, S., Shahzad, M., & Zhou, W. (2020). A cancelable biometric authentication system based on feature-adaptive random projection. Journal of Information Security and Applications, 1-9.

[56] Ying, B., & Nayak, A. (2019). Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography. Journal of Network and Computer Applications , 66-74.