ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 12, Issue 06, June 2025

Fingerprint Presentation Attack Detection by Efficient Voting Method

[1] Dharmendra Kaushik, [2] Dr. Alok Kumar Singh Kushwaha, [3] Dr. Vinay Kumar

[1] [2] [3] Department of Computer Science and Engineering, Guru Ghasidas Vishwavidyalaya, Bilaspur - 495009, (C.G.), India
Corresponding Author Email: [1] srnandan.dharam@gmail.com, [2] alokkushwaha@ggu.ac.in, [3] dr.vinaykumar@ggu.ac.in

Abstract*— Fingerprint recognition systems have advanced significantly in recent years. However, existing biometric systems based on fingerprint authentication remain vulnerable to spoofing attacks. Evaluating the effectiveness of fingerprint recognition systems requires large-scale datasets, but collecting such data is costly, time-intensive, and restricted by privacy laws. This study introduces a deep learning-based approach called the Efficient Voting Method (EVM) for fingerprint recognition and compares its performance with three widely used models: Random Forest, Extreme Gradient Boosting (XGBoost), and CatBoost. The proposed method achieves superior recognition accuracy while maintaining lower computational complexity compared to existing techniques. Experimental evaluations were conducted using the Ada Test and Verification System (ATVSFing), CustomFing and Sokoto Coventry Fingerprint (SOCOFing) datasets achieving accuracy rates of 67.25%, 88.79%, and 90.30% respectively.

Index Terms*— Fingerprint PAD, Soft Voting, Binary Classification, Biometric Recognition.

I. INTRODUCTION

Biometric identification is a natural and reliable method for verifying an individual's identity. Traditional authentication techniques, such as passwords, PINs, secret codes, and passphrases, often prove to be temporary, prone to loss, and vulnerable to security threats. These limitations hinder accurate identification, necessitating the development of biometric systems to enhance security, reliability, and efficiency. Biometric identification is categorized into two main types: physiological characteristics and behavioural traits. Physiological characteristics include fingerprints, facial features, palm prints, and iris patterns, while behavioural traits encompass voice recognition, keystroke dynamics, signature verification, and gait analysis. Among these, physiological features are more commonly utilized in biometric systems, with fingerprint recognition being one of the most widely adopted methods for security applications (Agarwal et al., 2020) [1]. Among various biometric identifiers such as face, iris, palm print, and ear, automatic fingerprint recognition systems (AFRS) remain the extreme extensively used, particularly in law enforcement and security applications. Due to its uniqueness, ease of use, and non-transferability, fingerprint authentication has gained widespread adoption in commercial applications (Goyal, 2017; Gafoor, 2018) [2, 3]. However, the increasing reliance on AFRS has led to attempts by criminals to bypass security measures by altering or fabricating fingerprints to evade detection.

Biometric systems play a vital role in various domains, including law enforcement, forensic investigations, personal identification, healthcare, and access control for smartphones and tablets, significantly enhancing security and convenience. However, the rise of sophisticated attack techniques and unpredictable spoofing attempts emphasizes the necessity for presentation attack detection (PAD) systems that can effectively identify previously unseen threats. Fingerprint recognition remains the most widely used biometric trait for identity verification across different sectors, such as access control for smartphones, banking, healthcare, biometric attendance, and visa processing (Jain, 2016; Sharma, 2019) [4, 5]. Presentation attacks (PAs) pose a severe security risk by enabling unauthorized access, potentially allowing intruders to exploit biometric systems for malicious purposes (Tolosana, 2020) [6]. To mitigate these risks, it is essential to develop robust countermeasures that can efficiently detect and prevent fingerprint-based presentation attacks.

II. RELATED WORK

Feng et al. (2010) [7] proposed a technique that separates the ridge orientation field into singular and continuous orientation components. By examining irregularities in the continuous ridge orientation field, these features are utilized to train a support vector machine (SVM) classifier to distinguish real fingerprints from fake ones. Yoon et al. [8] introduced a classification approach that integrates ridge orientation with minutiae distribution. Likewise, Tiribuzi et al. 2012 [9] designed new features, such as minutiae density maps and ridge orientation entropy, to improve fingerprint classification. However, double-identity fingerprints do not exhibit disruptions in ridge orientation fields or extra minutiae, as their alignment and weighted combination process prevents such inconsistencies. Consequently, existing fingerprint alteration detection methods (Askarin, 2018) [10] struggle to identify this form of attack. In recent years, deep learning has become increasingly prominent in biometrics research due to its capability to capture complex data patterns and model intricate nonlinear relationships. Significant progress in fingerprint authentication has been

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 12, Issue 06, June 2025

achieved through convolutional neural networks (CNNs), which are used for feature extraction, fingerprint matching, liveness detection, spoof detection, and handling low-quality fingerprints (Tertychnyi et al. [11]). Jiang et al. [12] introduced a patch-based CNN approach to extract minutiae features, utilizing two CNNs—one to determine whether a region contains a minutia and another to precisely locate it. Similarly, Jang et al. [13] proposed a deep CNN model based on VGG for fingerprint pore extraction, demonstrating improved performance compared to traditional feature-based techniques.

Moreover, Nogueira et al. [14] developed a CNN-based model for fingerprint liveness detection. Liveness Detection (LivDet) is an international competition series designed to evaluate and benchmark Presentation Attack Detection (PAD) technologies. The LivDet-2023 Noncontact Fingerprint competition [15] marks the first edition dedicated to noncontact fingerprint PAD, assessing algorithms and systems within this domain. This competition serves as a critical benchmark by providing: (a) an independent evaluation of the latest advancements in noncontact fingerprint PAD for both algorithms and systems, (b) a standardized evaluation framework featuring diverse Presentation Attack Instruments (PAIs) and live finger photos for biometric research, and (c) a comparative analysis of cutting-edge algorithms from academia and industry, tested on both older and newer Android smartphones (Purnapatra et al., 2023) [16]. The authors utilized Syn-CoLFinGer, a synthetic fingerprint generation technique developed by Priesnitz et al. (2022) [17], which simulates and creates finger photos based on contact-based fingerprint impressions. However, these artificial live patterns can be visually illustrious from real fingertips with relative ease. In 2023, Purnapatra et al. [16] introduced a PAD dataset that adhered to standard Presentation Attack Instrument (PAI) creation protocols. This dataset featured three difficulty levels, incorporating various materials and PAI textures designed to replicate real skin tones. Despite the progress, there remained a need for standardized model comparisons and evaluation benchmarks across academia and industry to enhance performance. The LivDet-2023 Noncontact Fingerprint Algorithm and System competition was the first LivDet event dedicated to noncontact fingerprint-based PAD. It was co-organized by Clarkson University (USA) and the University at Buffalo (USA). Previously, the LivDet series had hosted multiple liveness detection competitions covering fingerprint, face, and iris recognition. Additional details on past competitions can be found in the LivDet Team records. The primary aim of LivDet-2023 was to assess the effectiveness of cutting-edge noncontact fingerprint PAD algorithms and systems in detecting both traditional and novel PAIs. The competition was divided into two categories: Algorithms and Systems. Participants had the opportunity to compete in one or both categories, and institutions from both academia and industry were encouraged to take part. Unlike the Algorithm competition, where participants were provided with training data to ensure standardized evaluation, the System competition did not offer an official training dataset. Competitors in the System category were allowed to use proprietary or publicly available datasets for training their models. The Algorithm competition focused on single-fingertip-based models and included six different PAI types: printed finger photos on glossy paper, ecoflex, playdoh, wood glue, latex, and high-quality synthetically generated fingertip images.

Tanuj et al. (2024) [18] introduced a contactless fingerprint recognition system incorporating spoof images fabricated using various materials. Taneja et al. (2016) [19] assessed the effectiveness of different texture signifiers, including Local Binary Patterns (LBP), Locally Uniform Comparison Image Descriptor (LUCID), and Dense Scale-Invariant Feature Transform (DSIFT), in combination with Support Vector Machine (SVM) for non-contact fingerprint Presentation Attack Detection (PAD). They developed a spoof fingerprint database using six photo attack techniques and two print attack methods. Their findings revealed that LBP-based features performed the best, achieving an Equal Error Rate (EER) of 3.7%. Zhang et al. (2016) [20] proposed a 2D fake fingerprint detection method tailored for smartphones. This approach integrated Convolutional Neural Networks (CNNs) with two local descriptors, LBP and Local Phase Quantization (LPQ). To evaluate their algorithm, they created a dataset of 2D printed fingerprints captured using a capacitive fingerprint scanner. Wasnik et al. (2018) [21] introduced a smartphone-based PAD technique that utilized the convolution of second-order Gaussian derivatives at multiple scales. Their experiments were conducted on a self-compiled database containing different Presentation Attack Instruments (PAIs), including display, print-photo, and replay attacks. Marasco et al. (2021) [22] compared various CNN models using the IIITD Smartphone Finger-Photo database, which includes spoofed data from printouts and display-based attacks. Their findings suggested that the PAD system based on AlexNet exhibited greater robustness against different spoofing techniques.

III. DATASET

The research on fingerprint spoofing detection utilizes three datasets: ATVSFing, CustomFing, and SOCOFing. These datasets contain fingerprint images labeled as either live or fake, aiding in the development and evaluation of detection algorithms. ATVSFing, the Ada Test and Verification System, is a well-established benchmark for assessing the robustness of fingerprint recognition systems against presentation attacks. It includes a diverse collection of counterfeit fingerprint images created using various materials and techniques. The CustomFing, is a balanced collection containing 3,000 real and 3,000 fake fingerprint images. With an equal number of samples in both categories.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

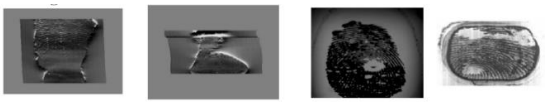
Vol 12, Issue 06, June 2025

Each image is clearly labeled as either "live" or "fake," making it suitable for supervised learning and classification tasks. The SOCOFing dataset offers additional metadata, including gender, hand orientation, and finger identification, with all subjects being 18 years or older. Like ATVSFing, it includes various spoofed fingerprint images produced using different materials and techniques.

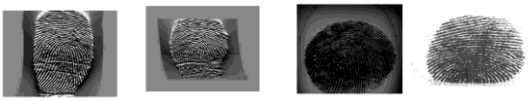
(a)Fake

(b) Live

Fig. 1. Sample Fingerprints of ATVSFing Dataset1



(a)Fake



(b) Live

Fig. 2. Sample Fingerprints of Custom Dataset2

(a)Fake

(b) Live

Fig. 3. Sample Fingerprints of SOCOFing Dataset3

IV. PROPOSED METHOD

The soft voting ensemble classifier integrates predictions from Random Forest, XGBoost, and CatBoost models. Each classifier is trained separately, and their predictions are averaged to enhance overall accuracy. The performance is assessed using multiple evaluation metrics, including accuracy, ROC curves, and precision-recall curves, with results visualized for better analysis. By combining the strengths of these individual models, the ensemble approach aims to improve predictive performance. This method effectively utilizes Random Forest, XGBoost, and CatBoost classifiers to enhance classification accuracy. The working of the soft voting ensemble model is given below:

1. **Model Training:** Each model is trained independently on the same training dataset (x_{train}, y_{train}).

Random Forest Classifier: RF model $\leftarrow Train(RandomForestClassifier, x_{train}, y_{train})$

XGBoost Classifier: XGB model $\leftarrow Train(XGBClassifier, x_{train}, y_{train})$

CatBoost Classifier: CatBoost mode $\leftarrow Train(CatBoostClassifier, x_{train}, y_{train}, params)$

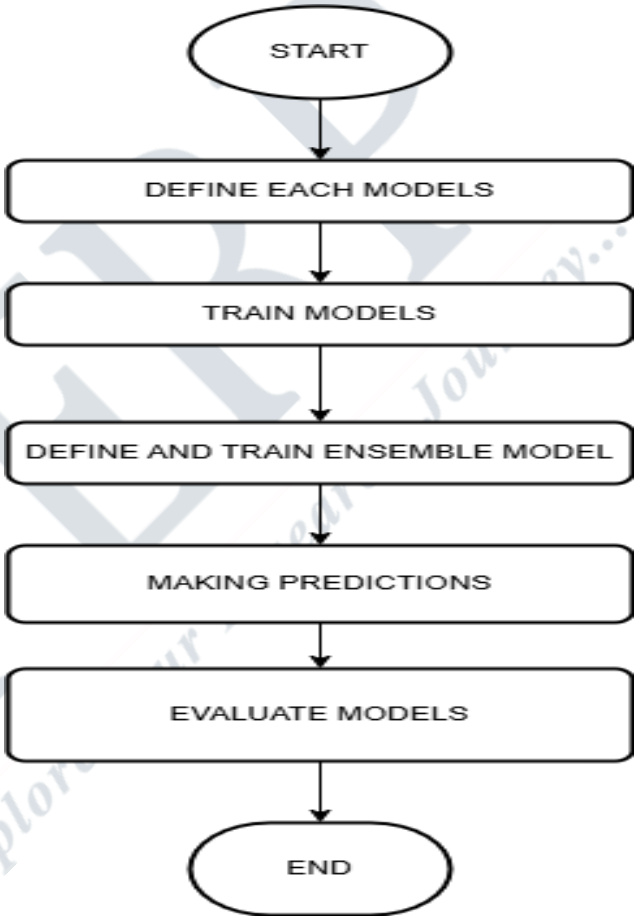


Fig. 4. Flowchart of the proposed model

2. **Prediction Generation:** Each model generates predictions for the testing dataset X_{test}. Random Forest: $\hat{y}_{RF}$ = RF_model.predict(X_{test})

XGBoost: $\hat{y}_{XGB}$ = XGB_model.predict(X_{test})

CatBoost: $\hat{y}_{CatBoost}$ = CatBoost_model.predict(X_{test})

3. **Soft Voting Ensemble:** Soft voting involves averaging the predictions from each classifier. For each sample i in the testing dataset, the ensemble prediction $\hat{y}_i$ is determined by:

$$\hat{y}_i = \frac{1}{3}(\hat{y}_{RF,i} + \hat{y}_{XGB,i} + \hat{y}_{CatBoost,i}) \quad (1)$$

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 12, Issue 06, June 2025

where

$\hat{y}_i$ = final predicted probability for sample i

$\hat{y}_{RF}$ = the probability predicted by the Random Forest classifier

$\hat{y}_{XGB}$ = the probability predicted by the XGBoost classifier

$\hat{y}_{CatBoost}$ = the probability predicted by the CatBoost classifier

A threshold (usually 0.5) is used to convert the averaged prediction into a binary class label. If the average is greater than or equal to 0.5, the sample is classified as 1, otherwise as 0 as given below:

$$\hat{y}_i = \begin{cases} 1 \ if \ \frac{1}{3}(\hat{y}_{RF,i} + \hat{y}_{XGB,i} + \hat{y}_{CatBoost,i}) \geq 0.5 \\ 0 \ otherwise \end{cases} \quad (2)$$

V. RESULT ANALYSIS

The performance of the model is assessed using evaluation metrics such as APCER, BPCER, F1-score, precision, and recall. Tables 1, 2, and 3 provide a comparative analysis between the proposed method and recent algorithms.

Table I: Performance of models on ATVSFing Dataset1

Model/Parameters	F1-Score	Precision	Recall	BPCER	APCER	Accuracy
Random Forest	0.70245	0.63636	0.78385	0.44792	0.21615	0.66797
XGBOOST	0.71245	0.62366	0.83073	0.50130	0.16927	0.66471
CATBOOST	0.70673	0.61710	0.82682	0.51302	0.17318	0.65690
HVMethod	**0.71274**	**0.63479**	**0.81250**	**0.46745**	**0.18750**	**0.67253**

Table 2: Performance of models on CustomFing Dataset2

Model/Parameters	F1-Score	Precision	Recall	BPCER	APCER	Accuracy
Random Forest	0.86347	0.90103	0.82891	0.08523	0.17109	0.87326
XGBOOST	0.87447	0.88500	0.86419	0.10511	0.13581	0.88004
CATBOOST	0.60317	0.68032	0.54173	0.23828	0.45827	0.65536
HVMethod	**0.87513**	**0.94860**	**0.81222**	**0.04119**	**0.18778**	**0.88793**

Table 3: Performance of models on SOCOFing Dataset3

Model/Parameters	F1-Score	Precision	Recall	BPCER	APCER	Accuracy
Random Forest	0.82303	1.00000	0.69928	0.00000	0.30072	0.84964
XGBOOST	0.89279	0.99888	0.80707	0.00091	0.19293	0.88225
CATBOOST	0.77260	0.77901	0.76630	0.21739	0.23370	0.77446
HVMethod	**0.86653**	**1.00000**	**0.76449**	**0.00000**	**0.23551**	**0.90308**

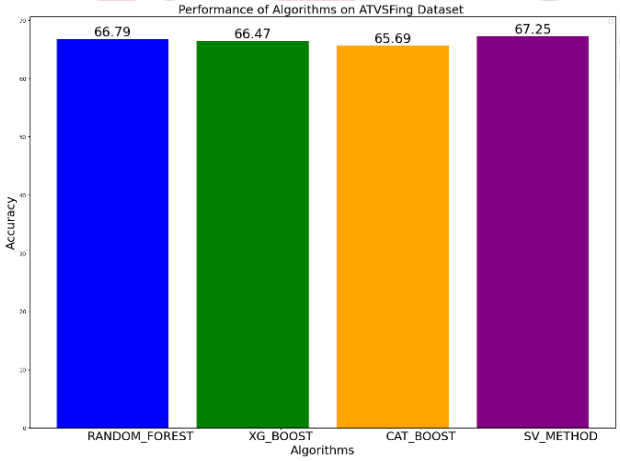


Fig. 5. Performance of the Models on ATVSFing Dataset1

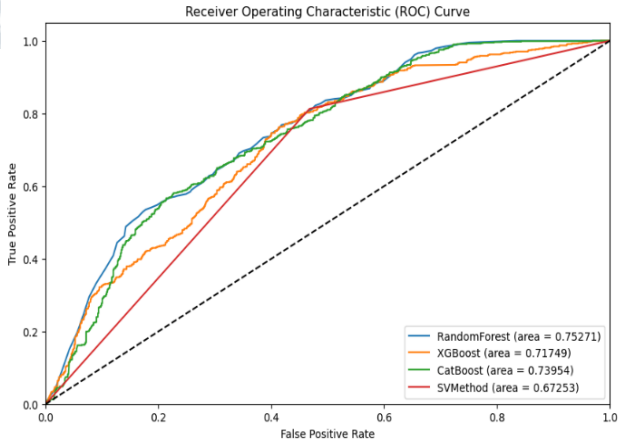


Fig. 6. ROC Curve for ATVSFing Dataset1

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 12, Issue 06, June 2025

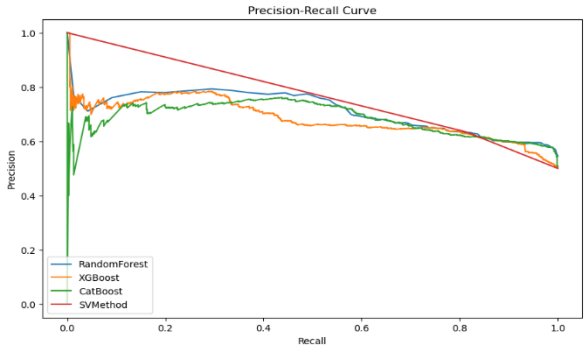


Fig. 7. Precision-Recall Curve for ATVSFing Dataset1

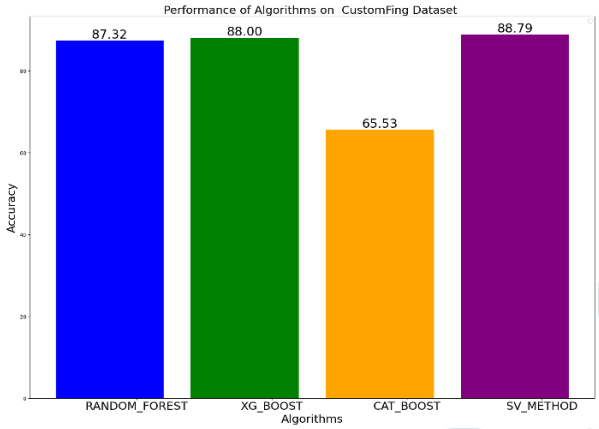


Fig. 8. Performance of the Models on CustomFing Dataset2

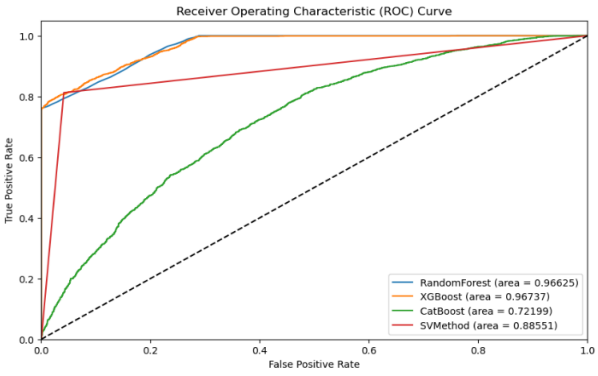


Fig. 9. ROC Curve for CustomFing Dataset2

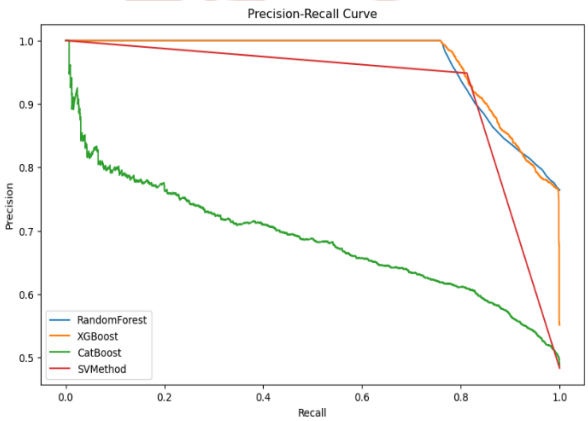


Fig. 10. Precision-Recall Curve for CustomFing Dataset2

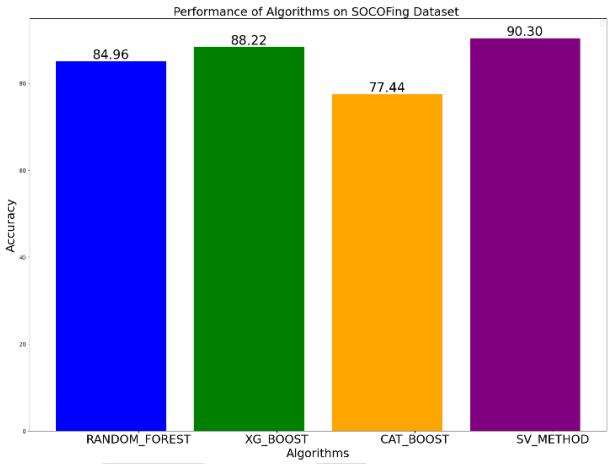


Fig. 11. Performance of the Models on SOCOFing Dataset3

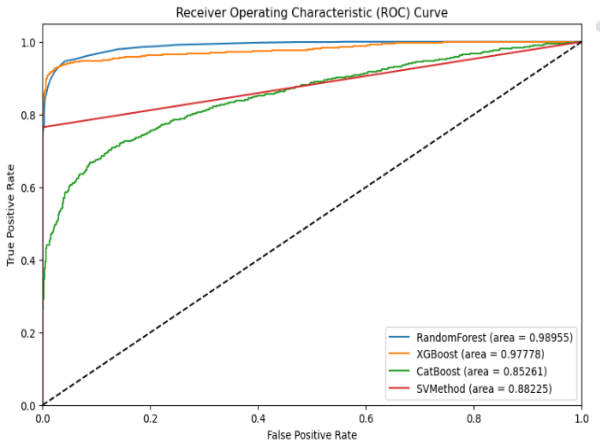


Fig. 12. ROC Curve for SOCOFing Dataset3

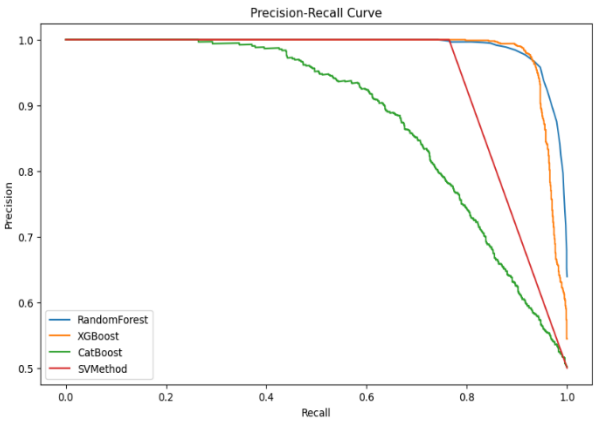


Fig. 13. Precision-Recall Curve for SOCOFing Dataset3

For the SOCOFing fingerprint dataset3, our method achieved the highest performance with an accuracy of 90.30%. On the dataset2, our method demonstrated strong consistency, attaining an accuracy of 88.79%. Additionally, the method yielded an impressive accuracy of 67.25% on the dataset3. These results highlight the robustness and effectiveness of the proposed approach across various datasets in fig. 14.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 12, Issue 06, June 2025

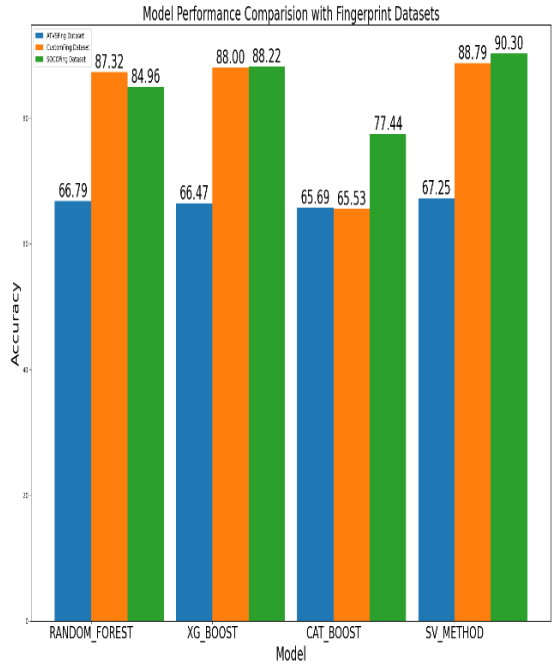


Fig. 14. Performance Comparison of Models with the datasets

VI. CONCLUSION

Our proposed Efficient Voting Method (EVM) demonstrated outstanding performance, achieving accuracy rates of 67.25 % on the ATVSFing dataset1, 88.79% on the CustomFing dataset2, and 90.30% on the SOCOFing dataset3. These results underscore the method's effectiveness in handling diverse datasets and its potential for real-world applications requiring precise classification. The findings confirm that our method is robust and reliable for classification tasks, making it a valuable tool for applications that demand high accuracy. Future research could explore the integration of other biometric modalities, such as iris and facial recognition, to enhance anti-spoofing capabilities further.

REFERENCES

[1] R. Agarwal, A. S. Jalal, and K. V. Arya, "A review on presentation attack detection system for fake fingerprint," *Mod. Phys. Lett. B*, vol. 34, no. 5, pp. 1–26, 2020, doi: 10.1142/S021798492030001X.

[2] V. S. Sanket Goyal and P. Desai, "Multi-level security embedded with surveillance system," *IEEE Sensors J.*, vol. 17, no. 22, pp. 7497–7501, Nov. 2017.

[3] M. Ghafoor, S. Iqbal, S. A. Tariq, I. A. Taj, and M. N. Jafri, "Efficient fingerprint matching using GPU," *IET Image Process.*, vol. 12, no. 2, pp. 274–284, 2018.

[4] Anil K. Jain, Karthik Nandakumar, and Arun Ross. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79:80–105, 2016.

[5] Ram Prakash Sharma and Somnath Dey. Fingerprint image quality assessment and scoring using minutiae centered local patches. *Journal of Electronic Imaging*, 28(1):013016, 2019.

[6] Ruben Tolosana, Marta Gomez-Barrero, Christoph Busch, and Javier Ortega-Garcia. Biometric presentation attack detection: Beyond the visible spectrum. *IEEE Transactions on Information Forensics and Security*, 15:1261–1275, 2020.

[7] J. Feng, A. K. Jain, and A. Ross, "Detecting altered fingerprints," in *Proc. 20th Int. Conf. Pattern Recognit.*, 2010, pp. 1622–1625.

[8] S. Yoon, J. Feng, and A. K. Jain, "Altered fingerprints: Analysis and detection," IEEE *Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 3, pp. 451–464, Mar. 2012.

[9] M. Tiribuzi, M. Pastorelli, P. Valigi, and E. Ricci, "A multiple kernel learning frame- work for detecting altered fingerprints," in *Proc. 21th Int. Conf. Pattern Recognit.*, 2012, pp. 3402–3405.

[10] M. M. Askarin, K. Wong, and R. C. Phan, "Planting attack on latent fingerprints," *IET Biometrics*, vol. 7, no. 5, pp. 396–404, 2018.

[11] P. Tertychnyi, C. Ozcinar, and G. Anbarjafari, "Low-quality fingerprint classification using deep neural network," *IET Biometrics*, vol. 7, no. 6, pp. 550–556, 2018.

[12] L. Jiang, T. Zhao, C. Bai, A. Yong, and M. Wu, "A direct fingerprint minutiae extraction approach based on convolutional neural networks," in *Proc. Int. Joint Conf. Neural Netw.*, 2016, pp. 571–578.

[13] Jang et al. "DeepPore: Fingerprint Pore Extraction Using Deep Convolutional Neural Networks." *IEEE Signal Processing Letters, Vol. 24, No. 12, December 2017.*

[14] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 6, pp. 1206–1213, Jun. 2016.

[15] LivDet Organizing Team, "Livdet website," available at: http://livdet.org/.

[16] S. Purnapatra, C. Miller-Lynch, S. Miner, Y. Liu, K. Bahmani, S. Dey, and S. Schuckers, "Presentation attack detection with advanced cnn models for noncontact-based fingerprint systems," *arXiv preprint arXiv:2303.05459*, 2023.

[17] J. Priesnitz, C. Rathgeb, N. Buchmann, and C. Busch, "Syncolfinger: Synthetic contactless fingerprint generator," *Pattern Recognition Letters*, vol. 157, pp. 127–134, 2022.

[18] Tanuj et al. "An evaluation study of non-contact fingerprint presentation attack detection." *2024 IEEE International Conference on Computer Vision and Machine Intelligence (CVMI)* | 979-8-3503-7687-6/2 DOI: 10.1109/CVMI61877.2024.10782562, 2024

[19] Archit Taneja, Aakriti Tayal, Aakarsh Malhotra, Anush Sankaran, Mayank Vatsa, and Richa Singh. Fingerphoto spoofing in mobile devices: A preliminary study. In *IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–7, 2016.

[20] Yongliang Zhang, Bing Zhou, Hong-Tao Wu, and Conglin Wen. 2d fake fingerprint detection based on im- proved cnn and local descriptors for smart phone. In *Chinese Conference on Biometric Recognition*, pages 655–662, 09 2016.

[21] Pankaj Wasnik, Raghavendra Ramachandra, Kiran Raja, and Christoph Busch. Presentation attack detection for smartphone based fingerphoto recognition using second order local structures. In *14th International Conference on*

Signal-Image Technology and Internet-Based Systems (SITIS), pages 241–246, 2018.

[22] Emanuela Marasco and Anudeep Vurity. Fingerphoto presentation attack detection: Generalization in smartphones. In *IEEE International Conference on Big Data (Big Data)*, pages 4518–4523, 2021.