System, Method, and Apparatus for Robust and Secured Locker Access via Liveness Detection-based Biometric Authentication

Presented By: Lomesh Wagh, Yash Waghmare, Bhumika Patil, Disha Magar **Guided By:** Prof. Dr. Sudeep D Thepade

Pimpri Chinchwad College of Engineering, Pune
NBA Accredited | NAAC Accredited with 'A' Grade | An Autonomous Institute |
AICTE Approved | ISO 9001 : 2015 Certified | Permanently Affiliated to SPPU, Pune

Patent Number:

Kshitij 2024

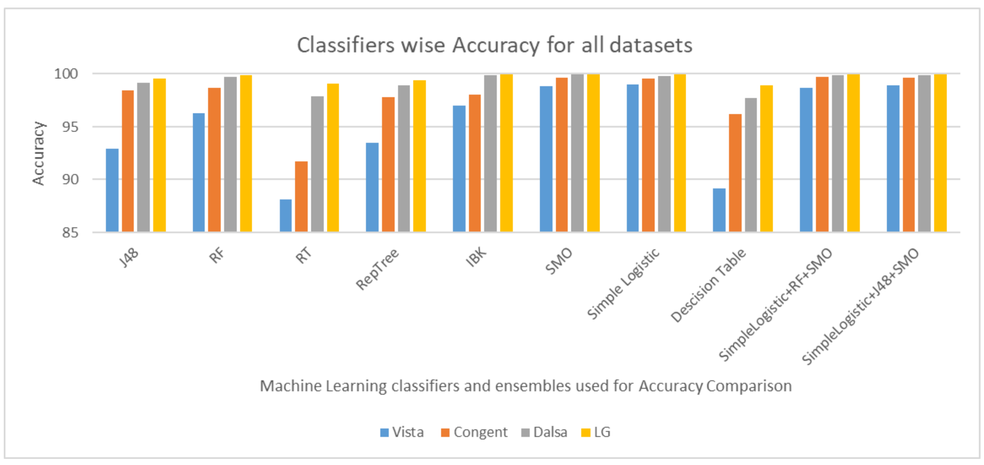
INTRODUCTION

Securing personal data is more crucial than ever. Traditional iris recognition systems, while accurate, are susceptible to spoofing attacks. To address this vulnerability, a new approach has emerged: the integration of auto-extracted and explicitly defined features. Auto-extracted features leverage artificial intelligence algorithms to automatically identify and extract unique characteristics from iris images. On the other hand, explicitly defined features are localized traits computed using predefined mathematical formulas. By combining these distinct feature sets, a novel composite feature set is generated. This amalgamation of features serves as the foundation for a cutting-edge biometric liveness detection system. This system is designed to discern between authentic, live biometric traits and fraudulent, spoofed representations.

OBJECTIVES

- To improve system robustness to identify genuine and fake biometric trait.
- To utilize both auto-extracted and explicitly defined features to accurately classify iris patterns as either fake or live.
- To reduces the risk associated with spoofing attacks by adding a new layer that checks liveness in biometric trait.
- To enhance institutional capabilities by integrating reliable biometric security measures, focusing on iris liveness detection

RESULTS



METHODS

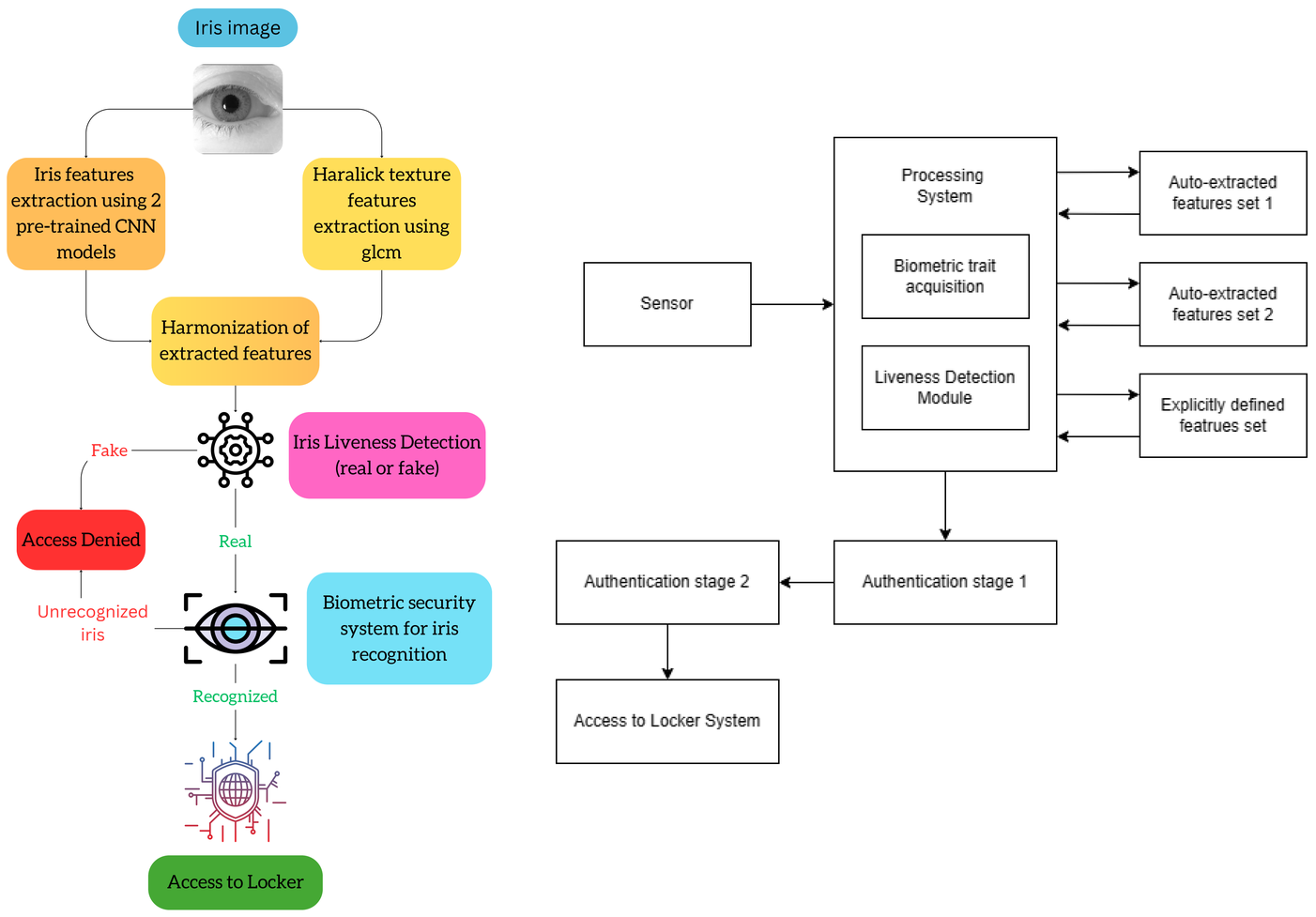


Fig: ILD method for Biometric access control system using a fusion of Haralick texture features and ResNet50 & DensNet121 global features.

Results by ensemble SimpleLogistic + SMO + J48

DATASET	% ACCURACY	% ACER
Vista	98.7179	1.19921
Congent	99.7039	0.30329
Dalsa	99.8832	0.08613
LG	99.92	0.04762

CONCLUSION

- Minimum ACER and maximum accuracy achieved by ensemble SimpleLogistic+SMO+J48.
- The ACER rates for IIITD and Clarkson are 0.675% and 0.067%, respectively.
- In terms of accuracy, IIITD achieved 99.2109%, while Clarkson reached 99.9016%.
- The proposed methodology results in superior performance compared to the existing state-of-the-art approaches, as it enhances accuracy and reduces ACER.

SUSTAINABLE DVELOPMENT GOALS

- **Goal 9:** Industry, Innovation, and Infrastructure
  - Emphasizing innovation in biometric security for advanced infrastructure.
- **Goal 11:** Sustainable Cities and Communities
  - Promoting secure authentication for sustainable urban development.
- **Goal 16:** Peace, Justice, and Strong Institution
  - Strengthening institutions with reliable biometric security measures.
- **Goal 17:** Partnerships for the Goals
  - Collaborating for enhanced cybersecurity and biometric authentication.

REFERENCES

- Dewan, J. H., & Thepade, S. D. (2021, April). Image retrieval using weighted fusion of GLCM and TSBTC features. In 2021 6th International Conference for Convergence in Technology (I2CT) (pp. 1-7). IEEE.
- Huang, Gao, et al. "Densely connected convolutional networks." Proceedings of the IEEE conference on computer vision and pattern recognition. 2017.
- He, Kaiming, et al. "Deep residual learning for image recognition." Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.