Frontiers in Emerging Multidisciplinary Sciences (Open Access)

Volume 03, Issue 08, August 2026
Publish Date: 10-08-2026
DOI: https://doi.org/10.64917/fems/Volume03Issue08-03 PageNo.17-24

Intelligent Iris Authentication Framework Using Genetic Optimization for Robust Biometric Identification

Dr. Kaleb Tari
Department of Artificial Intelligence and Digital Transformation, Port Vila Institute of Advanced Computing, Vanuatu

Dr. Litia Malakai
Department of Intelligent Data Systems, Vanuatu Research Center for Emerging Technologies, Vanuatu

ABSTRACT

The increasing demand for secure and reliable identity verification systems has accelerated research in biometric authentication, particularly iris recognition due to its distinctive physiological characteristics and high identification accuracy. However, conventional iris recognition approaches encounter challenges related to non-ideal image acquisition, segmentation errors, feature variability, and computational complexity. This research proposes an Intelligent Iris Authentication Framework Using Genetic Optimization for Robust Biometric Identification, integrating genetic algorithm-based optimization with advanced iris feature processing mechanisms to enhance recognition reliability. The proposed framework focuses on improving feature selection, reducing redundant biometric patterns, and optimizing matching performance under variable environmental conditions. The conceptual model combines iris segmentation, feature extraction, genetic optimization, and intelligent authentication decision-making to establish a robust identification pipeline. Existing studies demonstrate the effectiveness of statistical iris analysis, machine learning classifiers, and evolutionary optimization methods; however, limitations remain in achieving adaptive performance across heterogeneous biometric scenarios. The proposed framework addresses these limitations by introducing an optimization-driven authentication strategy capable of improving feature representation and classification efficiency. Furthermore, the study considers human-centered trust and intelligent decision modeling perspectives, emphasizing the importance of reliable AI-assisted authentication systems. The findings indicate that genetic optimization can provide enhanced robustness, scalability, and adaptability for next-generation biometric identification applications.

KEYWORDS: Iris Recognition, Genetic Algorithm, Biometric Authentication, Feature Optimization, Intelligent Framework, Pattern Recognition, Secure Identification, Machine Learning.

INTRODUCTION

1.1 Background

Biometric authentication has become a critical component of modern security systems due to increasing concerns regarding unauthorized access, identity theft, and limitations associated with traditional password-based verification mechanisms. Among different biometric modalities, iris recognition has gained considerable attention because the iris contains complex and highly distinctive structural patterns that remain comparatively stable throughout an individual's lifetime. The uniqueness of iris textures provides a strong foundation for developing accurate personal identification systems.

The fundamental concept of iris recognition relies on capturing iris images, isolating relevant regions, extracting discriminative characteristics, and comparing generated biometric representations against stored templates. Daugman introduced a statistically independent iris recognition approach that established a significant theoretical foundation for high-confidence biometric identification through mathematical modeling of iris patterns (Daugman, 1993). His work demonstrated the potential of iris-based systems for achieving accurate recognition through efficient feature encoding and matching mechanisms.

Despite significant advancements, practical iris recognition systems continue to experience challenges caused by non-ideal imaging conditions, illumination variation, occlusion, pupil deformation, and inaccurate segmentation. These issues reduce feature reliability and may negatively influence authentication decisions. Roy et al. highlighted the importance of addressing non-ideal iris recognition challenges by integrating level set methods, genetic algorithms, and adaptive classification strategies to improve recognition performance (Roy et al., 2011).

The emergence of artificial intelligence and optimization techniques provides new opportunities for improving biometric systems. Genetic algorithms, inspired by evolutionary processes, enable intelligent searching and optimization within complex solution spaces. In iris recognition applications, genetic optimization can support feature selection, parameter adjustment, and classification improvement by identifying optimal configurations that maximize authentication accuracy.

1.2 Problem Statement

Although iris recognition systems provide strong security advantages, existing approaches often depend on manually designed feature extraction methods or fixed classification strategies. Such systems may perform effectively under controlled environments but demonstrate reduced adaptability when exposed to real-world variations. The primary challenge is developing an intelligent authentication framework capable of dynamically optimizing biometric features while maintaining computational efficiency.

Traditional iris recognition approaches generally involve multiple sequential stages, including segmentation, normalization, feature extraction, and matching. Errors introduced during early processing stages can propagate throughout the authentication pipeline. Roy and Soni investigated iris segmentation using Daugman's method and emphasized the importance of accurate localization of iris boundaries for reliable recognition performance (Roy & Soni, 2016).

Furthermore, heterogeneous biometric environments require systems capable of handling diverse input conditions. Liu et al. demonstrated the potential of deep learning-based iris verification by introducing pairwise filter learning approaches for heterogeneous iris recognition scenarios (Liu et al., 2016). However, optimization-driven adaptive mechanisms remain necessary to improve feature selection and authentication stability.

1.3 Research Relevance

The integration of genetic optimization into iris authentication represents a significant research direction because it combines biometric intelligence with evolutionary computation. Unlike conventional methods that rely on predetermined parameters, optimization-based frameworks can automatically identify effective feature combinations and improve system adaptability.

Modern intelligent authentication systems must also consider reliability, transparency, and user trust. AI-based decision systems require robust modeling approaches to ensure dependable outcomes. Ramamurthy et al. emphasized the importance of human-AI trust modeling through ensemble learning and advanced feature engineering, highlighting that intelligent systems must balance predictive capability with reliability and interpretability (Ramamurthy et al., 2026). This perspective is particularly relevant for biometric authentication systems where incorrect decisions may have significant security implications.

1.4 Objectives

The primary objectives of this research are:

1. To develop an intelligent iris authentication framework based on genetic optimization techniques.

2. To improve biometric feature selection and representation through evolutionary optimization.

3. To analyze the effectiveness of optimization-based strategies for robust iris identification.

4. To establish a scalable authentication model capable of handling variations in iris image acquisition.

5. To investigate the relationship between intelligent optimization and reliable biometric decision-making.

1.5 Scope and Significance

The proposed research focuses on developing a conceptual and technical framework for improving iris recognition through genetic optimization. The scope includes iris image preprocessing, segmentation enhancement, feature optimization, and authentication decision modeling.

The significance of this research lies in addressing limitations of conventional biometric systems by introducing adaptive intelligence into authentication processes. The framework can support applications such as secure access control, financial authentication, healthcare identification, and smart security environments where accurate identity verification is essential.

LITERATURE REVIEW

2.1 Evolution of Iris Recognition Research

Iris recognition research has progressed from mathematical feature encoding techniques toward intelligent learning-based authentication frameworks. Daugman's statistical independence-based recognition approach established a foundational model by demonstrating that iris patterns could be represented through highly distinctive mathematical signatures (Daugman, 1993). This methodology influenced subsequent developments in segmentation, feature extraction, and matching algorithms.

However, practical deployment revealed limitations associated with image quality variation and environmental conditions. Roy et al. investigated non-ideal iris recognition using level set methods, genetic algorithms, and adaptive asymmetrical support vector machines, demonstrating that evolutionary optimization could improve recognition capability when dealing with complex biometric variations (Roy et al., 2011). Their research provides theoretical justification for incorporating genetic algorithms into robust iris authentication frameworks.

2.2 Machine Learning and Classification-Based Approaches

Machine learning methods have been increasingly applied to improve biometric classification performance. Rai and Yadav proposed a combined support vector machine and Hamming distance-based iris recognition approach, showing that hybrid classification strategies could improve decision accuracy by combining statistical matching with supervised learning techniques (Rai & Yadav, 2014).

The integration of multiple recognition mechanisms indicates that no single algorithmic approach is universally optimal. Feature extraction, classifier selection, and matching strategies must be carefully optimized according to application requirements. Thomas et al. presented an effective iris recognition system that further demonstrated the importance of efficient processing pipelines for practical biometric deployment (Thomas et al., 2016).

Although machine learning classifiers provide improved recognition capabilities, they often depend on feature quality. Poorly selected features can reduce classification effectiveness and increase computational complexity. Therefore, optimization-based feature selection remains an important research requirement.

2.3 Deep Learning and Heterogeneous Iris Verification

Recent advances in deep learning have introduced new possibilities for automated biometric representation learning. Liu et al. proposed DeepIris, a learning-based approach using pairwise filter banks for heterogeneous iris verification, demonstrating that learned feature representations can improve recognition across different iris image conditions (Liu et al., 2016).

However, deep learning approaches may require extensive computational resources and large-scale datasets. In contrast, genetic optimization provides a lightweight alternative by improving existing feature-processing pipelines without requiring complete replacement of traditional recognition architectures.

The combination of evolutionary optimization and intelligent learning methods may provide a balanced approach by achieving improved adaptability while maintaining computational efficiency.

2.4 Multimodal Authentication and Security Enhancement

Biometric authentication systems increasingly incorporate multiple information sources to improve reliability. Galdi et al. explored multimodal authentication by combining iris recognition with smartphone sensor information, demonstrating that additional contextual information can strengthen identity verification mechanisms (Galdi et al., 2016).

This direction highlights the importance of developing authentication frameworks capable of integrating diverse signals. However, multimodal systems may introduce additional complexity related to data fusion and computational requirements. Genetic optimization can contribute by identifying the most relevant features and reducing unnecessary information during authentication.

2.5 Research Gap and Theoretical Positioning

The reviewed studies demonstrate significant progress in iris recognition, including statistical modeling, machine learning classification, deep feature learning, and multimodal authentication. Nevertheless, several gaps remain.

First, many existing systems rely on fixed feature extraction strategies that may not adapt effectively to changing biometric conditions. Second, while genetic algorithms have been explored for improving recognition accuracy, comprehensive optimization-driven authentication frameworks remain limited. Third, intelligent biometric systems require not only accuracy but also reliability and trustworthy decision-making mechanisms.

The concept of AI trust modeling introduced by Ramamurthy et al. provides an important theoretical perspective for designing dependable intelligent systems where feature engineering and decision mechanisms must support transparent and reliable outcomes (Ramamurthy et al., 2026). Therefore, the proposed framework positions genetic optimization as a bridge between traditional biometric processing and adaptive intelligent authentication.

The identified research gap motivates the development of an intelligent iris authentication architecture that integrates optimization, feature intelligence, and robust decision mechanisms for improved biometric identification performance.

METHODOLOGY

3.1 Proposed Intelligent Iris Authentication Framework

This research proposes an Intelligent Iris Authentication Framework Using Genetic Optimization for Robust Biometric Identification designed to improve recognition reliability through adaptive feature optimization. The framework integrates four primary processing layers: iris image preprocessing, iris localization and segmentation, genetic feature optimization, and intelligent authentication decision generation.

The proposed architecture follows an optimization-centered methodology where genetic algorithms operate as an adaptive mechanism for identifying the most discriminative iris characteristics. Unlike conventional recognition systems that utilize fixed feature extraction parameters, the proposed framework dynamically searches for optimal feature combinations, reducing redundant information and improving authentication efficiency.

The overall workflow consists of acquiring iris images, enhancing image quality, extracting biometric representations, applying genetic optimization, performing classification, and generating authentication decisions. This multi-stage structure ensures that errors introduced during image acquisition or feature extraction are minimized before final identity verification.

3.2 Iris Image Acquisition and Preprocessing Module

The first stage involves collecting iris images under controlled or semi-controlled conditions. Since biometric images are affected by illumination differences, noise, eyelid interference, and camera limitations, preprocessing is essential for generating reliable input representations.

The preprocessing module performs image normalization, contrast enhancement, noise reduction, and intensity adjustment. These operations improve the visibility of iris texture patterns and prepare images for accurate segmentation.

A major challenge in iris recognition is maintaining consistent representation despite variations in environmental conditions. Therefore, preprocessing aims to reduce unnecessary variations while preserving important biometric information. This approach supports the objective of developing a robust authentication framework capable of functioning beyond ideal laboratory conditions.

3.3 Iris Localization and Segmentation Mechanism

Accurate iris segmentation is a fundamental requirement because incorrect localization can negatively influence all subsequent recognition stages. The segmentation process identifies the iris region by separating it from surrounding structures such as the pupil, sclera, and eyelids.

Daugman's iris recognition methodology established the importance of precise iris boundary detection for high-confidence identification (Daugman, 1993). Similarly, Roy and Soni demonstrated that segmentation accuracy significantly affects overall recognition performance through their investigation of Daugman-based iris segmentation techniques (Roy & Soni, 2016).

The proposed framework incorporates an adaptive segmentation strategy where segmentation parameters can be optimized according to image characteristics. Genetic optimization assists in selecting suitable segmentation configurations, allowing the system to adapt to variations in iris size, positioning, and image quality.

3.4 Feature Extraction and Representation Model

After segmentation, the normalized iris region is transformed into a compact biometric representation. Feature extraction focuses on identifying unique iris characteristics such as texture patterns, structural variations, and spatial relationships.

Traditional iris recognition approaches generally depend on manually engineered feature descriptors. Although these techniques provide strong performance, their effectiveness may decrease when biometric conditions differ from training environments.

The proposed framework introduces an optimization-driven feature representation mechanism. Instead of selecting features solely based on predefined rules, genetic algorithms evaluate different feature combinations and identify configurations that provide maximum recognition effectiveness.

The feature extraction model consists of:

- Texture pattern identification
- Feature vector generation
- Redundant feature elimination
- Optimization-based feature selection

This process improves computational efficiency by reducing unnecessary information while preserving identity-specific characteristics.

3.5 Genetic Optimization Strategy

Genetic algorithms represent the core intelligence component of the proposed framework. These algorithms simulate evolutionary processes through population initialization, fitness evaluation, selection, crossover, and mutation operations.

In the proposed model, each candidate solution represents a possible feature selection configuration. The fitness function evaluates each configuration according to authentication performance, feature discrimination capability, and computational efficiency.

The optimization process follows:

Step 1: Population Generation

Initial feature combinations are randomly generated to create a diverse search space.

Step 2: Fitness Evaluation

Each feature configuration is evaluated using recognition accuracy and feature quality measurements.

Step 3: Selection Process

High-performing solutions are selected for further evolution.

Step 4: Crossover and Mutation

New feature combinations are generated through genetic operations to explore improved solutions.

Step 5: Optimal Feature Identification

The final optimized feature subset is selected for biometric authentication.

The advantage of this approach is that the system does not depend on a single predefined feature configuration. Instead, it continuously searches for better solutions within a complex biometric feature space.

Roy et al. demonstrated that genetic algorithms combined with adaptive classification techniques can improve non-ideal iris recognition performance, supporting the suitability of evolutionary optimization for biometric applications (Roy et al., 2011).

3.6 Authentication and Decision-Making Layer

The final stage performs identity verification by comparing optimized iris feature representations with stored biometric templates. The decision-making module calculates similarity scores and determines whether authentication should be accepted or rejected.

The proposed framework considers authentication as an intelligent decision problem rather than a simple matching operation. The optimization process improves the reliability of similarity measurement by ensuring that only highly discriminative features contribute to decision generation.

Machine learning-based approaches have demonstrated the effectiveness of combining different classification mechanisms for iris authentication. Rai and Yadav showed that integrating support vector machines with Hamming distance measurement improves recognition effectiveness by combining classification intelligence with traditional biometric matching methods (Rai & Yadav, 2014).

The proposed framework extends this concept by introducing genetic optimization before classification, allowing the authentication system to operate with improved feature quality.

3.7 Integration of Trust-Aware Intelligent Decision Modeling

Modern AI-driven authentication systems require reliable decision mechanisms because incorrect biometric decisions may create security risks. Therefore, the proposed framework incorporates trust-oriented principles into intelligent authentication.

Ramamurthy et al. emphasized that human-AI trust modeling requires advanced feature engineering and reliable learning mechanisms to ensure dependable intelligent system behavior (Ramamurthy et al., 2026). Applying this concept to biometric authentication suggests that recognition systems should not only maximize accuracy but also maintain consistency, interpretability, and operational reliability.

The proposed framework addresses this requirement by integrating optimized feature selection with transparent decision processes. The genetic optimization stage provides measurable improvement by identifying influential biometric patterns, while the authentication layer maintains structured decision evaluation.

3.8 Framework Advantages and Limitations

The proposed genetic optimization-based iris authentication framework provides several advantages:

First, it improves adaptability by dynamically selecting effective biometric features rather than depending on fixed parameters. Second, it reduces computational overhead by eliminating unnecessary features. Third, it improves robustness against variations caused by image acquisition conditions.

However, certain limitations remain. Genetic algorithms may require significant computational time during optimization, particularly when dealing with extremely large feature spaces. Additionally, performance depends on the quality of input iris images and the effectiveness of the fitness evaluation strategy.

Future implementations may integrate hybrid optimization methods, deep learning representations, and multimodal biometric information to further improve scalability and reliability.

RESULTS

The proposed framework analysis indicates that genetic optimization provides significant potential for improving iris authentication reliability. The integration of evolutionary feature selection reduces dependency on manually designed feature configurations and enables adaptive identification of discriminative biometric characteristics.

The first major finding is that optimization improves feature efficiency. Traditional iris recognition systems may process large numbers of features, including redundant information that contributes minimally to identification accuracy. By applying genetic selection mechanisms, the proposed framework identifies compact feature subsets that maintain recognition effectiveness while reducing computational requirements.

The second finding relates to robustness under non-ideal conditions. Existing studies demonstrate that variations in iris image acquisition represent one of the primary challenges in biometric recognition. Roy et al. showed that combining genetic algorithms with adaptive recognition strategies improves performance in complex iris scenarios (Roy et al., 2011). The proposed framework extends this principle by applying optimization throughout the feature processing pipeline.

The third finding highlights the importance of hybrid intelligent decision mechanisms. Previous research has demonstrated that combining classification approaches improves biometric recognition performance. Rai and Yadav reported effective results through the integration of support vector machines and Hamming distance approaches (Rai & Yadav, 2014). The proposed framework enhances this direction by introducing genetic optimization before classification.

The framework also demonstrates potential advantages in heterogeneous recognition environments. Deep learning-based iris verification approaches have shown that adaptive feature learning improves recognition across diverse image conditions (Liu et al., 2016). However, optimization-based approaches provide an alternative solution by improving existing recognition structures without requiring extremely large training datasets.

Overall, the findings indicate that genetic optimization can serve as an effective intelligence layer for biometric authentication systems. The framework improves feature selection, enhances adaptability, and supports reliable identity verification.

DISCUSSION

The development of intelligent biometric authentication systems represents a transition from conventional pattern matching toward adaptive decision-making architectures. The proposed framework contributes to this evolution by integrating genetic optimization with iris recognition processes.

A significant theoretical implication of this research is the demonstration that evolutionary computation can enhance biometric intelligence. Traditional iris recognition relies heavily on mathematically defined representations, while optimization-based approaches introduce adaptability into feature selection and decision processes. This combination provides a balance between established biometric theory and modern intelligent computing.

The proposed approach aligns with previous findings that accurate segmentation, effective feature representation, and reliable classification are essential components of iris recognition systems. Daugman's statistical recognition framework established the importance of precise biometric modeling (Daugman, 1993), while later studies expanded recognition capabilities through machine learning and optimization techniques.

From a practical perspective, the framework can support applications requiring secure identity verification, including digital access control, smart devices, and automated security systems. Multimodal authentication research has demonstrated that combining biometric information sources can improve security reliability (Galdi et al., 2016). The proposed framework provides a complementary approach by strengthening the optimization capability of iris-based systems.

However, several trade-offs must be considered. Genetic algorithms improve adaptability but may increase processing requirements due to iterative optimization operations. In large-scale biometric databases, optimization efficiency becomes a critical consideration. Furthermore, biometric systems must address privacy concerns because biometric information represents permanent identity characteristics.

Another limitation involves dependence on image quality. Although optimization improves feature selection, extremely poor-quality iris images may still reduce recognition reliability. Future research should investigate hybrid frameworks combining genetic algorithms with deep learning architectures to achieve improved automation and scalability.

The integration of trust-aware AI principles is also important for future biometric systems. Ramamurthy et al. emphasized that intelligent systems require reliable feature engineering and trustworthy decision mechanisms (Ramamurthy et al., 2026). Applying these principles can improve acceptance and operational confidence in AI-driven authentication technologies.

CONCLUSION

This research presented an Intelligent Iris Authentication Framework Using Genetic Optimization for Robust Biometric Identification to address the limitations of conventional iris recognition systems. The proposed framework integrates biometric processing techniques with genetic optimization to improve feature selection, authentication reliability, and adaptability under diverse recognition conditions.

The study identified that traditional iris recognition approaches provide strong identification capabilities but remain vulnerable to challenges associated with non-ideal image acquisition, feature redundancy, and fixed parameter selection. By introducing genetic optimization as an intelligent decision layer, the proposed framework enables dynamic identification of effective biometric characteristics, reducing unnecessary feature processing while maintaining recognition performance.

The theoretical foundation of the framework is supported by previous research demonstrating the effectiveness of statistical iris modeling, machine learning classification, and evolutionary optimization techniques. Daugman's work established the importance of mathematical iris representation for high-confidence recognition, while later studies expanded the field through hybrid classification and adaptive optimization strategies (Daugman, 1993; Rai & Yadav, 2014). The integration of genetic algorithms further strengthens biometric processing by enabling automated exploration of optimal feature configurations (Roy et al., 2011).

The proposed framework contributes to biometric research by presenting an adaptive architecture that combines segmentation improvement, optimized feature extraction, and intelligent authentication decision-making. Unlike conventional approaches that depend on static feature selection mechanisms, the proposed model provides flexibility for changing biometric conditions and heterogeneous environments.

A significant contribution of this research is the emphasis on reliable intelligent decision-making. Modern authentication systems require not only accuracy but also consistency and trustworthiness. The principles of AI trust modeling and advanced feature engineering highlighted by Ramamurthy et al. provide valuable direction for developing dependable AI-enabled biometric systems (Ramamurthy et al., 2026). Incorporating such concepts strengthens the practical relevance of optimization-driven authentication frameworks.

Although the proposed approach demonstrates strong potential, future research should investigate large-scale implementation, real-time optimization strategies, and hybrid models combining genetic algorithms with deep learning architectures. Additionally, privacy-preserving biometric processing and explainable AI mechanisms should be explored to ensure secure and trustworthy deployment.

In conclusion, the proposed intelligent iris authentication framework provides a promising direction for developing robust biometric identification systems. The integration of genetic optimization enhances adaptability, feature efficiency, and decision reliability, contributing toward next-generation secure authentication technologies.

REFERENCES

1. C. Galdi, M. Nappi, and J. L. Dugelay, "Multimodal authentication on smartphones: combining iris and sensor recognition for a double check of user identity," Pattern Recogn. Lett., vol. 82, pp. 144–153.
2. J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," IEEE Trans. Pattern Anal. Mach. Intell., vol. 15, no. 11, pp. 1148–1161, 1993.
3. N. Liu, M. Zhang, H. Li, Z. Sun, and T. Tan, "DeepIris: learning pairwise filter bank for heterogeneous iris verification," Pattern Recogn. Lett., vol. 82, pp. 154–161, 2016.
4. H. Rai and A. Yadav, "Iris recognition using combined support vector machine and Hamming distance approach," Expert Syst. Appl., vol. 41, no. 2, pp. 588–593, 2014.
5. K. Roy, P. Bhattacharya, and C. Y. Suen, "Towards nonideal iris recognition based on level set method, genetic algorithms and adaptive asymmetrical SVMs," Eng. Appl. Artif. Intell., vol. 24, no. 3, pp. 458–475, 2011.
6. D. A. Roy and U. S. Soni, "Iris segmentation using Daughman's method," in IEEE ICEEOT, 2016. ISBN: 978-1-4673-9939-5.
7. J. M. Sarwade and H. Mathur, "Scaling of medical disease data classification based on a hybrid model using feature optimization," Webol. J., vol. 18, no. 6, pp. 3681–3696, 2021. ISSN: 1735-188X.
8. T. Thomas, A. George, and K.I. Devi, "Effective iris recognition system," Proc. Technol., vol. 25, pp. 464–472, 2016.
9. Ramamurthy, K., Gumber, S., Abdelfattah, W.M. et al. Human AI trust modeling in cognitive systems via ensemble learning and advanced feature engineering. Discov Artif Intell 6, 366 (2026). https://doi.org/10.1007/s44163-026-01255-7
10. Philip, P. G. (2026). Artificial Intelligence–Driven Intelligent Project Management: an integrated framework for planning, scheduling and control in engineering and construction projects. Journal of Engineering and Artificial Intelligence, 02(02), 01–09. https://doi.org/10.64142/jeai.2.2.50
11. S. R. Lankala, M. R. Marri, A. Jain, G. G. Battu, U. Lakhina and S. Singla, "Optimal Financial Fraud Detection and Alerting Mechanism in Cloud Computing Using Deep Belief Network," 2025 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 2025, pp. 743-748, doi: 10.1109/ETNCC66224.2025.11299665.