## Anita Razafindrakotovao

## Literature review:

Electoral integrity is a cornerstone of democratic governance, yet many countries, including Madagascar, struggle with issues such as electoral fraud, inaccuracies in voter rolls, and barriers to political participation. Traditional voter registration systems often fail to adequately address these challenges, leading to compromised election results and diminished public trust in the democratic process. In response to these issues, the implementation of a biometric voter registration system has emerged as a viable solution. This system leverages biometric identification methods to ensure accurate voter registration and verification, significantly reducing the potential for fraudulent activities. By enhancing the reliability and transparency of elections, such a system not only bolsters democratic integrity but also aligns with Sustainable Development Goal 10, which aims to reduce inequalities and promote inclusive societies. In Madagascar, where marginalized communities frequently encounter obstacles to political participation, the adoption of biometric voter registration is a crucial step towards ensuring equal access to the electoral process for all citizens.

The following section will review existing literature on the implementation of biometric voter registration systems in various contexts, drawing from articles published since 2018. This review provides insights into the methodologies, challenges, and outcomes documented by other researchers and practitioners in the field.

* (SYED SHAHRAM NAJAM, AAMIR ZEB SHAIKH, & SHABBAR NAQVI, 2018) proposes a novel hybrid biometric electronic voting system that integrates fingerprint and facial recognition for voter identification, aiming to enhance accuracy compared to single-method systems. Utilizing the Viola-Jones algorithm and Haar feature selection for facial recognition, coupled with GPCA and K-NN classifiers for verification, the system achieves 91% accuracy under normal lighting conditions. This design, tailored for developing countries like Pakistan, Nepal, and Sri Lanka, includes future plans for enhancing security through encryption algorithms, offering a robust solution for fair and secure general elections.
* (Agarwal, Afreen Haider, & Abhishek, 2020) focuses on developing a fingerprint-based biometric voting system to address issues like booth capturing, rigging, fake voting, and tampering with Electronic Voting Machines (EVMs) in India. The proposed system uses fingerprint sensors linked to the Aadhaar database to authenticate voters and ensure "one person, one vote." The methodology involves registering and verifying voters through a digital template of their fingerprints, and preventing multiple votes with a buzzer system. Case studies demonstrated the system's effectiveness in real-life scenarios, preventing unauthorized voting and immediate result display. The study concludes that this system enhances security and efficiency, recommending its national-level implementation to improve India's election process.
* (Sudeepthi Komatineni & Gowtham Lingala, 2020) proposes a secure electronic voting system combining facial recognition and biometric authentication methods to enhance voter privacy and prevent fraud. It emphasizes the integration of Eigen face-based facial recognition and minutiae-based biometric scanning to ensure robust voter authentication. By leveraging a comprehensive database, the system aims to eliminate duplicate votes and fraudulent activities, thereby improving efficiency and user-friendliness in both online and traditional polling environments. The implementation promises to increase voter turnout and address historical challenges of malpractice in elections, thereby safeguarding democratic processes against errors and voter marginalization.
* (Afolabi, 2020) highlited the issues and problems of the election management in Nigeria and Zimbabwe, both developing democracies with similar historical conditions. Elections and its management are the role of Electoral Management Body (EMB). It also defined the electoral fraud and how and when it can occur, also by whom. Finally it found that BT improved pre-election processes with reliable voter registers and identification but faced limitations due to technical issues, lack of skilled staff, power supply problems, and high costs. Despite these challenges, BT reduced certain types of fraud, though not completely, as post-election manipulations persisted. The study concluded that while BT can help, it is not a complete solution; broader efforts including voter education and changes in attitudes towards electoral democracy are also needed to fully address electoral fraud.
* (Debos, 2021) talked about the introduction of biometrics in Chad as it highlits that the roll-out of electoral biometrics across Africa is framed as a solution to political issues. According to (Debos, 2021), the introduction of biometrics marginally improved the electoral process by making the voter roll more accurate, but it did not eliminate fraudulent and violent practices. The technology also technicalized the voter-state relationship, fostering a procedural and narrow conception of democracy that marginalized other forms of political action. The study argues that while biometrics can standardize elections, it may also support undemocratic political orders and calls for a broader discussion on the political implications of electoral biometrics, beyond just technological and cost-related issues.

These studies collectively underscore the promising role of biometric technologies in electoral reform. While biometrics offer robust tools for enhancing voter authentication and reducing certain types of electoral fraud, they also highlight the necessity for comprehensive approaches. Integrating technological advancements with broader institutional reforms, such as improved election management bodies and enhanced voter education, is crucial to bolstering electoral integrity and promoting democratic participation globally. By addressing technical challenges, ensuring secure implementation, and fostering public trust through education, these integrated approaches can mitigate risks associated with electoral malpractice and support more transparent, inclusive electoral processes. As biometric systems continue to evolve, their effective integration into electoral frameworks requires not only technological innovation but also strategic planning and stakeholder engagement to uphold democratic principles and ensure equitable electoral outcomes across diverse contexts.

## Data Research

Facial recognition technology has rapidly advanced in recent years, becoming a cornerstone in various applications from security systems to personalized user experiences. This data research project focuses on exploring and analyzing datasets relevant to biometric technologies, specifically for voter registration purposes. The project seeks to investigate datasets that facilitate the development and validation of biometric models, particularly in facial recognition, within the context of electoral systems.

Facial recognition datasets have evolved significantly, offering diverse resources for advancing technology in biometrics. Key datasets like Digi-Face 1M emphasize synthetic, privacy-conscious approaches, while VGG Face2 and UMDFaces provide extensive, varied datasets for large-scale training and evaluation. Specialized datasets such as CelebA and Wider Face cater to specific applications like attribute annotation and face detection under challenging conditions. Open data initiatives like MS-Celeb-1M promote collaboration and transparency in research. These datasets collectively support innovations in facial recognition, addressing scalability, diversity, and ethical considerations, thereby enhancing the reliability and applicability of biometric technology across different domains.

For our project of Biometric Voter Registration system, the first part implementation is planned to be the facial recognition and Digi-Face dataset is chosen to be used to training the model.

### DigiFace-1M Dataset

The DigiFace-1M dataset is a collection of over one million diverse synthetic face images for face recognition. (Gwangbin Bae, Martin de La Gorce, & Tadas Baltruˇsaitis, 2022)

It was introduced in our paper DigiFace-1M: 1 Million Digital Face Images for Face Recognition and can be used to train deep learning models for facial recognition.

The dataset contains 720K images with 10K identities (72 images per identity). For each identity, 4 different sets of accessories are sampled and 18 images are rendered for each set.

(DataGen, 2024) Like other state-of-the-art methods, DigiFace1M is evaluated on a benchmark dataset, (LFW), which consists of 13k images of 5.7k people.

It was found that:

* The model trained on synthetic data only outperforms that trained on real-world data only, when only a small number of real face images are available.
* The best results are obtained when the facial recognition model is trained on synthetic data, then fine-tuned with real-world data.

Impressively, the best model achieved a whopping 99.33% accuracy on the Labeled Faces in the Wild benchmark. This is when the model is trained on DigiFace and then fine-tuned with real faces.

**The challenges of DigiFace-1M:**

Admittedly, DigiFace-1M is not foolproof. The pipeline does not comprehensively close the domain gap. In particular, it cannot generate the same person at different ages. Since an identity always has the same hairstyle, DigiFace-1M also lacks variation in hairdos or haircuts. Further, it does not generate accessories that cover parts of the body like jewelry and tattoos.

Identities of DigiFace-1M also lack demographic labels. As a result, there could be a potential bias towards certain demographic profiles. Thus, it cannot be used to alleviate the biases of existing models, which is done by adding identities of the underrepresented demographic groups to the training dataset. To address this weakness of DigiFace-1M, the authors could consider generating identities with demographic labels.

## 3. Technology review

The implementation of a biometric voter registration system using machine learning holds significant importance in modernizing electoral processes worldwide. By integrating advanced technologies such as fingerprint verification and facial recognition, this system aims to enhance voter authentication, reduce fraud, and ensure ethical conduct of elections.

The proposed Biometric Voter Registration systems leverages two primary technologies:

### Fingerprint Verification:

Fingerprint recognition typically employs minutiae-based algorithms. These algorithms analyze unique features of fingerprints such as ridge endings, bifurcations, and ridge counts. The matching process involves comparing captured fingerprints with stored templates to authenticate individuals.

Common algorithms include:

* **Minutiae-based Recognition:** This approach identifies and matches minutiae points (points where ridges end or split) between captured and stored fingerprints.
* **Pattern Recognition:** Utilizes ridge patterns and ridge shapes to distinguish and verify identities.
* **Machine Learning Techniques:** Recent advancements integrate machine learning, such as Support Vector Machines (SVM) or neural networks, to enhance accuracy and efficiency in fingerprint matching.

Implementation of fingerprint verification systems requires specialized hardware and software tools:

* **Fingerprint Sensors:** Devices like the MANTRA MFS 100 capture high-resolution fingerprint images.
* **Software Development Kits (SDKs):** SDKs facilitate integration of fingerprint recognition algorithms into applications, providing APIs for capturing, processing, and matching fingerprints.
* **Database Management:** Systems manage fingerprint templates securely, ensuring rapid and accurate retrieval during verification processes.

Comparison with other biometric modalities reveals:

* **Strengths:** High accuracy and reliability, resistance to spoofing, and widespread acceptance.
* **Challenges:** Cost of hardware and software deployment, sensitivity to environmental factors affecting image quality, and the need for continuous database management and updates.

### Facial Recognition:

Facial recognition technology has emerged as a powerful tool in biometric authentication, leveraging machine learning for precise identification.

This involves several stages:

* **Face Detection:** Locating and extracting facial regions from images or video frames.
* **Feature Extraction:** Identifying distinctive features such as eyes, nose, and mouth.
* **Matching:** Comparing extracted features with stored templates to verify identity.

Common algorithms used in facial recognition include:

* **Convolutional Neural Networks (CNNs):** Deep learning models that excel in feature extraction and pattern recognition from images.
* **Eigenface Approach:** Uses principal component analysis (PCA) to represent faces as vectors in a high-dimensional space, enabling efficient matching.
* **Local Binary Patterns (LBP):** Analyzes texture patterns in facial images for identity verification.

Implementing facial recognition systems requires:

* **High-Resolution Cameras:** Capture clear facial images suitable for analysis.
* **Machine Learning Frameworks:** Platforms like TensorFlow or PyTorch for training and deploying CNN models.
* **Face Recognition Libraries:** OpenCV for face detection and recognition tasks, facilitating integration into voting system applications.

Comparing facial recognition with other biometric modalities:

* **Strengths:** Non-intrusive, rapid identification, suitable for large-scale applications, and capable of handling diverse demographic groups.
* **Challenges:** Privacy concerns, potential biases in recognition accuracy, and sensitivity to image quality and angle variations.

In conclusion, the review underscores the critical role of biometric technologies, such as fingerprint and facial recognition coupled with encryption, in modernizing voter registration systems. These technologies not only enhance security and accuracy but also promote transparency and trust in electoral processes. By adopting these tools, the project aims to revolutionize voter registration and authentication, contributing to fairer and more efficient democratic practices globally.

# References

Afolabi, O. S. (2020). Biometric Technologies, Electoral Fraud and the Management of Elections in Nigeria and Zimbabwe. *Strategic Review for Southern Africa, 42*, 205-229.

Debos, M. (2021). Biometrics and the disciplining of democracy: technology, electoral politics, and liberal interventionism in Chad. *DEMOCRATIZATION, 28*(8), 1406-1422.

Agarwal, S., Afreen Haider, & Abhishek, J. (2020). Biometric Based Secured Remote Electronic Voting System. *IEEE 7th International Conference on Smart Structures and Systems ICSSS 2020* (pp. 1-10). Online: IEEE.

SYED SHAHRAM NAJAM, AAMIR ZEB SHAIKH, & SHABBAR NAQVI. (2018). A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition. *Mehran University Research Journal of Engineering & Technology, 37*, 59-59.

Sudeepthi Komatineni, & Gowtham Lingala. (2020). Secured E-voting System Using Two-factor Biometric Authentication. *Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020)* (pp. 245-249). Online: IEEE.

Tazaeen Ilyas Shaikh, Hritika Kamalakar Ranadhir, Suyash Santosh Gugale, Vrushali Prakash Patil, & Omkaresh Kulkarni. (2022). *Biometrics Based Secured Online Voting System Using Machine Learning Method.* India: EasyChair.

Gwangbin Bae, Martin de La Gorce, & Tadas Baltruˇsaitis. (2022). *DigiFace-1M: 1 Million Digital Face Images for Face Recognition.* Microsoft.

DataGen. (2024). From https://datagen.tech/blog/digi-face-1m/