GH raisoni COLLEGE
Engineering
Nagpur

Facial Recognition in Voting Systems: A Biometric Approach to Prevent Electoral Fraud

Project Report submitted
in
partial fulfillment of requirement for the award of degree of

Bachelor of Technology

Data Science

by

Mr. Himanshu R. Katrojwar **Ms. Saloni K. Deshmukh**

Ms. Aishwarya S. Parwekar

Guide

Dr. Rahul Agrawal
Associate Professor

November 2024

Department of Data Science, IoT & Cyber Security (DIC)
G H Raisoni College of Engineering
An Empowered Autonomous Institute affiliated to Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur
Accredited by NAAC with "A++" Grade (3rd Cycle)
CRPF Gate No. 3, Hingna Road, Digdoh Hills, Nagpur – 440 016 (INDIA)
T: +91 9604787184, 9689903286, 9921008391 | E: principal.ghrce@raisoni.net | W: ghrce.raisoni.net

GH raisoni COLLEGE
Engineering
Nagpur

Facial Recognition in Voting Systems: A Biometric Approach to Prevent Electoral Fraud

Project Report submitted
in
partial fulfillment of requirement for the award of degree of

Bachelor of Technology
in
Data Science

by

Mr. Himanshu R. Katrojwar **Ms. Saloni K. Deshmukh**
Ms. Aishwarya S. Parwekar

Guide

Dr. Rahul Agrawal
Associate Professor

November 2024

Department of Data Science, IoT & Cyber Security (DIC)
G H Raisoni College of Engineering
An Empowered Autonomous Institute affiliated to Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur
Accredited by NAAC with "A++" Grade (3rd Cycle)
CRPF Gate No. 3, Hingna Road, Digdoh Hills, Nagpur – 440 016 (INDIA)
T: +91 9604787184, 9689903286, 9921008391 | E: principal.ghrce@raisoni.net | W: ghrce.raisoni.net

raisoni EDUCATION
Nagpur | Pune | Jalgaon | Amravati | Pandhurna | Bhandara

Declaration

We, hereby declare that the project report titled “Facial Recognition in Voting Systems: A Biometric Approach to Prevent Electoral Fraud” submitted herein has been carried out by us towards partial fulfillment of requirement for the award of Degree of Bachelor of Technology in Data Science. The work is original and has not been submitted earlier as a whole or in part for the award of any degree / diploma at this or any other Institution / University.

We also hereby assign to G H Raisoni College of Engineering, Nagpur all rights under copyright that may exist in and to the above work and any revised or expanded derivative work based on the work as mentioned. Other work copied from references, manuals etc. are disclaimed.

Name of student	Mobile No	Mail ID (Other than Raisoni.net)	Signature
Himanshu Katrojwar	9359908251	himanshu.katrojwar8104@gmail.com	
Saloni Deshmukh	9022314210	sdsalonideshmukh@gmail.com	
Aishwarya Parwekar	8446010454	aishwaryaparwekar10@gmail.com	

Date:

Place:

G H raisoni COLLEGE
Engineering
Nagpur

Certificate

The project report entitled as "**Facial Recognition in Voting Systems: A Biometric Approach to Prevent Electoral Fraud"** submitted by **Himanshu R. Katrojwar, Saloni K. Deshmukh and Aishwarya S. Parwekar** for the award of Degree of Bachelor of Technology in Data Science has been carried out under my supervision. The work is comprehensive, complete and fit for evaluation.

Dr. Rahul Agrawal
Guide
Associate Professor
Department of DIC
G H R C E, Nagpur

Dr. Chetan Dhule
Project Incharge
Associate Professor
Department of DIC
G H R C E, Nagpur

Prof. Nekita Chavhan Morris
Head
Department of DIC
G H R C E, Nagpur

Dr. Sachin Untawale
Director
G H R C E, Nagpur

ACKNOWLEDGEMENT

A declaration of success is the completion of an action within a given time range or parameter. Without the invaluable help of many people, this procedure would not have been able to be carried out. This Internship project is the outcome of productive work done both individually and as a team.

We owe our achievement to our project mentor, Associate Professor Dr. Rahul Agrawal of Department of Data Science, IoT & Cyber Security (DIC) GHRCE, Nagpur whose unwavering efforts, prompt, and highly regarded assistance and encouragement allowed us to finish this difficult task within the allotted time.

We owe deep sense of gratitude to Mrs. Nekita Chavan Morris, Head of Department of Data Science, IoT & Cyber Security (DIC) GHRCE, Nagpur, for her keen interest in us at every stage of our research work. Her prompt inspiration, timely suggestions with kindness, enthusiasm and dynamism has enabled us to complete our project.

Our sincere gratitude goes to Dr. Sachin Untawale, GHRCE, Nagpur, for his genuine concern and for giving us with the resources we needed to complete the assignment. Finally, we acknowledge the teaching and non-teaching staff of department DIC for direct and in direct help given to us for completing this project and for providing consistent encouragement.

Regards,
Himanshu Katrojwar
Saloni Deshmukh
Aishwarya Parwekar

ABSTRACT

In democratic societies, the integrity of voting is essential for maintaining public trust and ensuring that elections are free, fair, and transparent. Traditional methods of verifying voter identity, such as physical ID documents or manual checks, are increasingly challenged by modern forms of electoral fraud, including impersonation and multiple voting. With recent advancements in artificial intelligence and machine learning, biometric technologies like facial recognition present promising solutions to enhance security in voting systems. This thesis introduces the design and implementation of a Face Verification Voting System built on Convolutional Neural Networks (CNNs), which offers an advanced way to authenticate voters and reduce the risks associated with conventional verification methods.

The system relies on CNN models to recognize each voter's unique facial features accurately. It begins by collecting multiple images of each registered voter, capturing different lighting conditions, angles, and expressions to improve recognition accuracy. In the preprocessing phase, the images are standardized through resizing, normalization, face detection, and augmentation. This ensures consistency and prepares the data for training. During model training, the CNN learns to identify distinct features from these processed images, applying regularization techniques to prevent overfitting. Once trained, the model generates feature embeddings, which act as unique biometric identifiers for each voter and are securely stored in an encrypted database.

On voting day, a voter's live image is captured, processed, and compared with stored embeddings for real-time verification. This comparison is based on a threshold system, which minimizes false acceptances and rejections. Integrated into a Tkinter-based user interface, the system is designed for easy and secure use, connecting directly with the database to retrieve and store voter information efficiently. Testing revealed that the CNN model achieved a 98% recognition accuracy, a 0.5% false acceptance rate, and a 2% false rejection rate, with an average verification time of 0.8 seconds. While there were minor limitations under challenging lighting conditions, these were mitigated with user prompts. This study demonstrates the significant potential of CNN-based face verification for secure, scalable voting solutions, suggesting a robust pathway for future applications in electoral security.

LIST OF FIGURES

LIST OF TABLES

PUBLICATIONS DETAILS

SR. NO.	TITLE OF PAPER	CONFERENCE NAME	CONFERENCE DATE	STATUS	PAGE NO.
1	Comprehensive Study of Face Verification in Voting System	International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS 2024)	22nd and 23rd Nov 2024	Registration Done	49

INDEX

CHAPTER 1
INTRODUCTION

INTRODUCTION

Voting is a basic right part and key feature of democratic societies, allowing citizens to have a direct say in the decision-making processes of governance. However, with developments in technology voting integrity and security are now faced with new unique challenges due to evolving technologies that allow for advanced electoral fraud. Maintaining electoral integrity—defined as free, fair, and transparent elections—is a growing challenge in the current landscape of voting malpractices ranging from proxy voting, multiple voting, voter impersonation to other fraudulent practices that threaten democracy

Traditional voter verification techniques, which often rely on physical identification documents or manual inspections, have shown limited effectiveness in addressing these challenges. For instance, incidents of fraudulent voting have been documented in various democratic countries, including India, where cases of voter impersonation and proxy voting were reported during the Lok Sabha elections. Such instances highlight the limitations of conventional verification systems in safeguarding the authenticity of elections and underscore the need for a secure, reliable, and technologically advanced solution to ensure each vote is cast by the intended individual.

Face verification technology, a branch of biometric authentication, leverages the uniqueness of facial features to confirm an individual's identity. This technology has gained traction in various fields, including access control, banking, and law enforcement, due to its high accuracy and convenience. In the context of voting systems, face verification offers a promising solution to counter electoral fraud by enabling voter identification without the need for physical documents or manual checks. By using a voter's facial features as a form of digital identity, face verification ensures that each vote corresponds to the right person, thereby mitigating risks of identity-based electoral fraud such as multiple voting and impersonation.

Different countries have tried face verification for elections. Estonia—a world leader in e-governance—has experimented with facial recognition as a form of verification for online voting, and several U.S. states are already testing whether the technology can effectively be used to deter unlawful ballots from being cast. Facial recognition technology was piloted by the government for possible use to ensure security during the voter identification process in India in the 2019 Telangana municipal elections. These initiatives personify the shift towards a realization that face verification technology has immense potential for safeguarding electoral processes and eventually, an equitable election.

Convolutional Neural Networks (CNNs) have been the most prominent machine learning technique for facial recognition and verification. This is because CNNs are particularly effective in identifying and extracting salient features in images, which is a crucial requirement in face verification since the model needs to differentiate between subtle variations of faces across different ethnic groups. Unlike the traditional approaches, such as Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), which

rely on hand-engineered features and are highly sensitive to variations in lighting conditions, pose orientations, and backgrounds, CNNs automatically derive hierarchical representations from raw pixel information. It is through many layers of convolutional operations, pooling tasks, and activation functions that CNNs capture intricate patterns among facial features, thus permitting high accuracy in face recognition tasks.

In a study, CNNs were found to be the most appropriate model for face verification during voting, having confirmed an accuracy of 98% and a validity of 90% regarding experimental tests. Such a high level of accuracy assures that face verification based on CNNs is a reliable method for voter authentication, thereby enhancing the security of the voting process by minimizing the chances of unauthorized access as well as fraudulent activities. Moreover, it is only due to CNNs' ability to generalize at different facial expressions, lighting conditions, and minor occlusions that they remain a robust option for practicality since environmental conditions can vary vastly.

This research aims to develop a Convolutional Neural Networks (CNNs) – based face verification system for voter authentication. It will have following objectives: First, assess the accuracy, reliability and robustness of CNNs, as recent works point that CNNs could be better performer than traditional approaches. Second, address difficulties when applying face verification in voting systems including data privacy, security and infrastructure issues by providing feasible solutions for these technical and ethical obstacles. Lastly, study how new CNN-based verification can provide better electoral integrity and public trust since it might help reducing voter falsification. The overall scope is therefore aiming to provide a guideline for bringing face verification into democratic process, supporting a safe, transparent and trusted election system.

This study addresses a pressing need for advanced voter verification solutions in electoral systems that are increasingly vulnerable to fraud. By presenting an in-depth analysis of CNN-driven face verification technology, this research contributes to the growing body of literature on secure, AI-based electoral solutions. It offers valuable insights for policymakers, election officials, and technologists on the feasibility, challenges, and ethical implications of integrating biometric verification systems into voting infrastructure. Moreover, the study provides recommendations for further research and policy development, aimed at enhancing electoral security while safeguarding individual privacy.

CHAPTER 2
LITERATURE REVIEW

LITERATURE REVIEW

In the article "A Review of Person Recognition Based on Face Model," authors Pedro Valente, Firas Mahmood Mustafa Alfaqi, and Shakir Fattah Kak [1] discuss developments in face recognition models with an emphasis on applications for person identification. This 2018 study examines a number of face recognition algorithms, with a focus on Convolutional Neural Networks (CNNs), which have demonstrated a high degree of promise for precise identity verification. The study examines how well CNN-based models hold up against more conventional approaches, showcasing neural networks as dependable and effective options for applications where accurate identification is crucial, such as voter authentication. The authors highlight CNNs' excellent accuracy through a thorough comparison, which they attribute to their capacity to recognize intricate face patterns. The study discusses CNNs' remarkable benefit of being able to adapt to different environmental conditions, which is crucial for real-world applications. Nevertheless, the study emphasizes difficulties in uncontrolled settings, where elements like illumination or occlusions may impair accuracy, even when CNNs perform well in controls. All things considered, this evaluation makes CNNs a compelling option for voter authentication system integration, opening the door for more research in this area.

The study *"Analysis of Electronic Voting System in Various Countries,"* conducted by Sanjay Kumar and Dr. Ekta Walia [2] in 2011, presents a comparative analysis of electronic voting (e-voting) systems used globally. The paper examines both the benefits and vulnerabilities of e-voting, especially in terms of security and user authentication. The authors observe that while electronic voting enhances efficiency and accessibility, it lacks secure methods for authenticating voters, thus opening avenues for potential fraud. The study suggests that biometric verification, such as face recognition, could offer a solution to these security challenges, providing more reliable identification than traditional methods. Though not focused on CNNs, this study's discussion on the need for biometric systems underlines the relevance of facial recognition technologies for enhancing election security. The authors' analysis of e-voting systems across countries demonstrates that systems without robust authentication mechanisms are susceptible to various types of tampering. The comparative insights offer a solid foundation for integrating secure biometric models, such as CNN-based face recognition, into e-voting, with potential applications extending to large-scale voter verification.

In their paper *"Experiments and Data Analysis of Electronic Voting System,"* Komminist Weldemariam, Adolfo Villafiorita, and Andrea Mattioli [3] present a detailed exploration of e-voting machine experiments conducted over several years. The study centers on the ProVotE project, which tested e-voting systems equipped with Direct Recording Electronic (DRE) and Voter-Verified Paper Audit Trail (VVPAT) capabilities. Through field tests, the authors collected and analyzed data on system performance and security in various electoral contexts. Key findings include that while these systems met performance expectations, security remained an unresolved issue. The researchers propose that biometric systems, such as face verification, could enhance the security and integrity of the voting process. Their work underscores that current systems, while functional, lack robust means to ensure voter authenticity. By suggesting the potential of facial recognition, particularly CNN-based systems, this study supports the integration of advanced biometric authentication methods in future voting technologies. Weldemariam and colleagues conclude that

a fusion of traditional e-voting machines with CNN-based face recognition could address current security gaps, improving both reliability and voter confidence.

In *"An Online Voting System for Colleges and Universities,"* Idongesit E. Eteng, Ugochi D. Ahunanya, and Paul U. Umoren [4] explore an online voting system tailored for educational institutions, published in 2018. This system enables students to vote securely and remotely, emphasizing accessibility and ease of use. Although the study focuses on a non-biometric software solution, it points out the limitations of online systems in terms of authentication and security. The authors propose that integrating facial recognition, especially CNN-based methods, could enhance voter verification in remote systems by adding a layer of biometric security. Given the adaptability of CNN models for identity verification, this suggestion aligns with trends toward using CNNs in high-security applications. The study's relevance lies in its practical application for secure, convenient voting processes in educational settings. By incorporating CNN-based face verification, this system could minimize impersonation risks and ensure voter authenticity, thus adding value to its security framework.

The paper *"Face Recognition Systems: A Survey,"* by Yassin Kortli, Maher Jridi, Ayman Al Falou, and Mohamed Atri [5], is a comprehensive review of face recognition systems published in 2020. The authors provide a taxonomy of face recognition approaches, classifying them into local, holistic, and hybrid methods. They analyze the efficacy of CNN-based systems for real-time applications, emphasizing their advantages in terms of robustness and adaptability to varying lighting conditions and facial angles. The study identifies CNNs as the leading technology for face recognition, particularly suited for applications that demand high accuracy and quick processing, such as voter authentication systems. By examining key CNN-based techniques, including popular algorithms like ArcFace and ResNet, the authors present a compelling case for CNNs in security-sensitive fields. This survey underscores the growing potential of CNNs to address practical challenges in identity verification, particularly under real-world conditions. Such insights highlight CNNs' applicability in secure voting systems, making them a viable option for high-stakes environments where verification accuracy is critical.

In *"Face Detection and Recognition: A Review,"* authored by Akanksha, Jashanpreet Kaur, and Harjeet Singh [6], various face detection and recognition techniques are examined, with a focus on feature-based recognition methods. This review highlights the limitations of traditional recognition approaches, particularly in terms of environmental adaptability, and advocates for advanced models like CNNs. The authors explore several algorithms, including Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), but suggest that CNNs provide superior accuracy by extracting complex facial patterns, thus performing better in challenging conditions. By addressing common issues in face recognition, such as lighting and facial orientation, this paper builds a strong case for CNNs, particularly in high-security applications. The study concludes that CNN-based face recognition models offer robust solutions for dynamic and diverse environments, reinforcing their potential role in reliable voter authentication systems.

The 2023 study *"GhostFaceNets: Lightweight Face Recognition Model from Cheap Operations,"* by Mohamad Alansari [7] and colleagues, introduces GhostFaceNets, a lightweight face recognition model

based on GhostNet architectures. This paper is unique in addressing the challenge of deploying high-performance CNNs on low-power devices like mobile phones. GhostFaceNets, developed from GhostNetV1 and GhostNetV2, employ innovative Ghost modules that significantly reduce computational complexity while maintaining high accuracy. Trained using ArcFace loss on large datasets, GhostFaceNets achieved state-of-the-art results on benchmark datasets, demonstrating their feasibility for real-time face verification. The model's low memory requirements and fast processing make it ideal for mobile or embedded devices, making it highly suitable for voter authentication applications in portable systems. GhostFaceNets stand out as a promising solution for secure, real-time verification, supporting scalable deployment in voter authentication systems across varying resource environments.

In their study *"A Novel Hybrid Biometric Electronic Voting System: Integrating Fingerprint and Face Recognition,"* authors Syed Shahram Najam, Aamir Zeb Shaikh, and Shabbar Naqvi [8] address the pressing need for secure, reliable voter authentication methods in electronic voting systems. Recognizing the potential for fraud in unimodal verification approaches, this study introduces a hybrid biometric model that combines fingerprint and facial recognition for enhanced verification. Published in 2017, the research specifically employs the Viola-Jones algorithm and Haar feature selection for face recognition, while fingerprint identification is performed through feature extraction and matching. For pattern matching and feature extraction, the system utilizes Generalized Principal Component Analysis (GPCA) and K-Nearest Neighbour (KNN) classifiers. This combination allows the system to match the extracted features from voter images with a pre-stored biometric template in the election database, significantly improving security and accuracy.

The researchers highlight several benefits of the multimodal approach over unimodal systems, particularly the reduced vulnerability to fraudulent voting, identity misrepresentation, and issues of environmental inconsistency. By cross-verifying identity with both fingerprint and facial features, the proposed system achieves an accuracy rate of up to 91% under standard lighting conditions, making it suitable for real-time voter verification applications. This dual-layered approach mitigates common limitations associated with unimodal systems, such as failure to authenticate in suboptimal conditions, while providing a more robust defence against tampering and impersonation. In terms of practical deployment, the study identifies electronic voting booths and mobile voting stations as ideal settings for this hybrid system due to the reduced need for human verification.

The study's methodology includes a detailed examination of each biometric modality and an analysis of the combined approach's efficacy in reducing error rates and improving verification efficiency. The use of GPCA in combination with KNN offers a powerful classification approach by leveraging principal components to achieve high precision in recognizing identity. Meanwhile, the integration of Viola-Jones detection and Haar feature selection ensures that the facial recognition component is fast and reliable, capable of isolating key facial landmarks with high accuracy. One of the key strengths of this study is its focus on maintaining balance between security and user convenience, which is crucial for election settings where quick and accurate verification is paramount.

Despite the advantages presented, the study also acknowledges some limitations, particularly the reliance on optimal lighting conditions, which can impact system performance. However, the researchers suggest that this limitation can be managed with the addition of adaptive lighting mechanisms or by enhancing the system's robustness with additional data preprocessing techniques. The findings underscore the potential of multimodal systems to become foundational in biometric voting technology, with the combined use of fingerprint and face recognition presenting a promising solution to the security concerns often associated with e-voting.

The study contributes to the field by providing a well-rounded solution for secure, scalable, and user-friendly voter authentication in electronic voting contexts, particularly in regions where digital infrastructure may vary. In summary, Najam, Shaikh, and Naqvi's work highlights the utility of combining facial and fingerprint recognition, paving the way for future research into hybrid models that can further improve voter verification's reliability and efficiency

The study *"Smart Voting System through Facial Recognition,"* authored by Nilam Choudhary, Shikhar Agarwal, and Geerija Lavania [9], presents an innovative approach to secure voting through a multi-tiered verification system that incorporates facial recognition technology. Published in 2019, this paper explores the potential of facial recognition to improve security and reduce fraud in e-voting systems by adding three distinct levels of verification. The authors discuss the existing challenges in traditional voting methods, particularly issues related to identity verification and election fraud. Their proposed system first verifies the voter's UID, followed by a validation of their voter card number, and finally, an advanced facial recognition step that compares real-time captured images with a pre-existing database.

For facial recognition, the authors utilize and compare various algorithms, including Eigenface, FisherFace, and Speeded-Up Robust Features (SURF), each known for different strengths in terms of speed, accuracy, and adaptability to changing conditions. Eigenface, based on Principal Component Analysis (PCA), is highlighted for its effectiveness in scenarios where facial features are generally consistent. In contrast, FisherFace, using Linear Discriminant Analysis (LDA), provides higher accuracy in variable lighting or partial occlusions, making it suitable for real-world voting environments. SURF, which is known for fast and accurate feature matching, offers another viable alternative for facial feature extraction, particularly for applications requiring rapid processing.

The authors find that this multi-layered verification reduces the likelihood of identity fraud while maintaining system efficiency. The study concludes that integrating facial recognition into voting systems enhances security, as it adds an additional biometric layer that is harder to circumvent. However, it also acknowledges limitations, such as the requirement for high-quality cameras and potential challenges under poor lighting. This research underscores the need for multi-factor authentication in voting systems and advocates for the use of advanced facial recognition algorithms in secure and reliable e-voting applications. By comparing different algorithms, the study provides a practical assessment of which approaches may be best suited for real-time voter authentication

In the paper titled *"A Survey on Performing E-Voting through Facial Recognition,"* Pratik Hopal, Alkesh Kothar, Swamini Pimpale, Pratiksha More, and Jaydeep Patil [10] conduct a comprehensive review of e-voting systems with a focus on facial recognition as a primary tool for voter authentication. This 2021 study examines the evolution of voting methods, from traditional ballot boxes to electronic systems, and identifies ongoing challenges with voter verification and fraud. The authors argue that traditional voting, while effective, is prone to human error and tampering, necessitating modern automated solutions like facial recognition for more reliable voter identification. Their review includes a comparative analysis of several machine learning algorithms, with a specific emphasis on Recurrent Neural Networks (RNNs) due to their adaptability in processing sequential data.

RNNs are presented as a highly suitable option for e-voting, particularly for applications requiring accurate, real-time identification. The authors highlight that RNNs can effectively process facial patterns even when these change subtly over time, offering a level of flexibility that other machine learning models may lack. Additionally, the study explores issues such as computational complexity and data privacy, which are critical in large-scale applications like national elections. By automating the facial recognition process, RNN-based systems can potentially minimize human intervention, thereby reducing opportunities for fraud and error. While acknowledging the limitations of current technologies, such as hardware requirements and susceptibility to environmental factors, the study suggests that facial recognition, particularly through RNNs, is a promising direction for the future of e-voting.

This survey contributes to the literature by providing insights into the specific advantages and challenges of using machine learning in biometric authentication for e-voting. The authors recommend further research into enhancing RNN algorithms to improve speed and accuracy, as well as exploring alternative deep learning architectures that might offer more efficient processing capabilities. This review positions RNNs as a viable and innovative approach for facial recognition in voting applications, encouraging further exploration into their integration for more secure democratic processes

In their comprehensive review titled *"A Review of Face Recognition Technology,"* authors Lixiang Li, Xiaohui Mu, Siying Li, and Haipeng Peng [11] explore the history, technological evolution, and current applications of face recognition. This 2020 paper traces the development of facial recognition technology from the early days of basic algorithms like Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) to advanced machine learning techniques, particularly Convolutional Neural Networks (CNNs). Each stage is discussed in terms of its strengths, limitations, and relevance to real-world applications, such as security and voting. PCA and LDA, for example, are noted for their efficiency in controlled settings but tend to perform poorly in varying lighting or occlusion scenarios. CNNs, on the other hand, have revolutionized facial recognition by offering robust solutions to these challenges due to their ability to extract complex features.

The authors detail various applications of face recognition, including access control, finance, and public security, underscoring its utility in systems requiring high accuracy and efficiency. The paper also discusses CNN’s adaptability to real-time applications, where high speed and reliability are necessary, making it

suitable for e-voting applications. Additionally, this review includes an analysis of common challenges faced by face recognition systems, such as the effects of illumination, pose variation, and occlusion, and presents potential solutions, including data augmentation and multi-model fusion approaches to improve performance.

A notable contribution of this review is its focus on CNN's potential as a scalable and efficient solution for voter authentication in electronic voting systems. The authors conclude that while challenges remain, especially regarding data privacy and ethical considerations, CNN-based facial recognition offers a secure and effective approach to voter verification. This work encourages continued research into algorithmic advancements that enhance accuracy under diverse conditions, thereby supporting a more reliable and fraud-resistant approach to voter authentication. Through this detailed examination, the authors advocate for CNNs' role in the future of secure and scalable e-voting systems, providing a roadmap for further technological improvements.

The paper "Face Recognition and Face Detection Benefits and Challenges" [13] provides an extensive examination of the evolution and current state of face recognition technology, emphasizing its applications, advantages, and challenges. It begins by tracing 60 years of history in face recognition, which is essential for understanding how technological advancements have shaped the field. The paper distinguishes between face detection and face recognition, clarifying that face detection serves as a preliminary step necessary for the recognition process. This distinction is crucial for grasping the interrelation between these technologies. The literature also discusses two primary approaches to face detection: feature-based and image-based, with a focus on the feature-based approach that utilizes low-level analysis techniques such as color, gray levels, edges, and motion. A significant application highlighted in the research is the use of face detection systems for attendance tracking in educational settings. A survey conducted among 34 lecturers and teachers in Namibia revealed a strong willingness to adopt such systems, indicating a positive reception towards integrating technology into educational administration.

Furthermore, the paper outlines the benefits of face detection over other biometric identification methods, such as iris recognition and fingerprint biometrics, noting that face recognition is generally more socially accepted. Individuals are more comfortable sharing their facial images, particularly in the context of social media. However, the paper also acknowledges several challenges that must be addressed before widespread adoption of face detection systems in schools and universities. Issues such as illumination problems, where overexposure to light can hinder face detection, and the potential for spoof attacks are highlighted as significant hurdles. Overall, the literature survey within this paper provides a detailed examination of the evolution, methodologies, applications, and challenges of face recognition and detection technologies, particularly in the context of educational attendance systems, emphasizing the need for further advancements to fully realize their potential.

The paper titled "Vote identification and integrity of ballot in paper-based e-voting system" [14] addresses the critical need for secure and reliable voting mechanisms in developing countries. The authors highlight a significant research gap in the existing literature, which often overlooks the integrity of paper ballots and the identification of votes cast. Traditional voting systems, while familiar, lack the technological integration

necessary for efficient vote counting and verification, leading to potential vulnerabilities in the electoral process.

To address this gap, the authors propose a novel application that utilizes image processing techniques to automatically identify votes on scanned ballot papers. The methods employed include scanning the ballot to create an image file, followed by applying algorithms to detect the punched holes corresponding to votes. The system also incorporates the Whirlpool hash algorithm to ensure the integrity of the votes, thereby enhancing the security of the e-voting process.

Future research directions suggested by the authors include exploring advanced image processing techniques to improve the accuracy of voter identification beyond the current success rate of 85.71%. Additionally, there is a call for further studies to assess the feasibility of implementing such systems in various electoral contexts, particularly in regions with limited technological infrastructure. The integration of these methods could significantly bolster public trust in electoral processes and promote greater participation in democracy, particularly in developing nations where traditional voting methods are still predominant

The paper titled "J Journal of Education for Pure Science-University of Thi-Qar" [15] explores the design and implementation of a biometric-based electoral system aimed at enhancing the integrity of the Iraqi electoral process. The authors identify a research gap in the existing electoral systems, particularly regarding security and voter participation, highlighting the need for a more reliable method to prevent fraud and manipulation in elections. The methods used include automated identification and authentication techniques utilizing facial recognition and fingerprinting, implemented through a user-friendly graphical interface. The study emphasizes the importance of a secure and transparent voting process, which is crucial for building voter confidence. Future research could focus on the practical application of this electronic electoral system in various contexts, assessing its effectiveness and adaptability in different cultural settings. This could lead to further innovations in biometric technologies and their integration into electoral systems globally.

The paper titled "Smart Online Voting System Using Facial Recognition Based on IoT and Image Processing" [16] addresses the critical challenges faced by traditional voting systems and proposes a modern solution to enhance electoral integrity. Historically, voting methods have evolved from paper ballots, which are prone to fraud, to electronic systems, and now to internet-based voting. Each transition aims to close the loopholes left by its predecessor, such as the risk of duplicate votes and improper voter identification. The proposed system utilizes advanced technologies, including facial recognition and IoT, to create a secure and efficient voting process. By employing Convolutional Neural Networks (CNN) for facial recognition, the system ensures that each voter can only cast their vote once, thereby significantly reducing the chances of electoral fraud.

The paper outlines a multi-layered security approach that includes not only facial recognition but also Election ID (EID) verification and One-Time-Password (OTP) confirmation. This comprehensive strategy is designed to enhance voter verification and prevent unauthorized voting. Additionally, the system is designed to be user-friendly, with a web-based interface that allows voters to cast their votes easily while ensuring

their identities are securely verified. The simulation results indicate that the proposed system simplifies the vote counting process and enhances security by not storing personal voter details, thus protecting voter privacy.

Moreover, the paper emphasizes the importance of reducing human intervention in the voting process, which can lead to errors and inefficiencies. By automating the voting mechanism, the system not only streamlines the process but also minimizes the resources required for conducting elections, making it a cost-effective solution for democratic nations. Overall, this innovative approach to online voting represents a significant advancement in ensuring fair and transparent elections in the digital age.

Table 2.1: Summary of Literature Review

Sr no.	Paper Title	Authors	Focus	Key Findings
1.	A Review of Person Recognition Based on Face Model [1]	Pedro Valente, Firas Mahmood Mustafa Alfaqi, Shakir Fattah Kak	Face recognition models for person identification using CNNs	CNNs show high accuracy in identity verification, particularly for voter authentication, but face challenges in uncontrolled environments.
2.	Analysis of Electronic Voting System in Various Countries [2]	Sanjay Kumar, Dr. Ekta Walia	Comparative analysis of global e-voting systems	Highlights benefits and vulnerabilities of e-voting; suggests biometric verification for enhanced security.
3.	Experiments and Data Analysis of Electronic Voting System [3]	Komminist Weldemariam, Adolfo Villafiorita, Andrea Mattioli	Security analysis of e-voting machines	Biometric systems like face verification could improve e-voting security and reliability, addressing current security gaps.
4	An Online Voting System for Colleges and Universities [4]	Idongesit E. Eteng, Ugochi D. Ahunanya, Paul U. Umoren	Online voting system for educational institutions	Suggests CNN-based facial recognition for enhanced voter verification, minimizing impersonation in remote voting.

5.	Face Recognition Systems: A Survey [5]	Yassin Kortli, Maher Jridi, Ayman Al Falou, Mohamed Atri	Overview of face recognition methods	CNNs are highly effective for real-time, high-accuracy applications like voter authentication under diverse conditions.
6.	Face Detection and Recognition: A Review [6]	Akanksha, Jashanpreet Kaur, Harjeet Singh	Review of face detection and recognition techniques	Traditional methods have limitations; CNNs provide superior accuracy and adaptability, especially for high-security applications.
7.	GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations [7]	Mohamad Alansari, et al.	Lightweight face recognition model using GhostNet	GhostFaceNets are suitable for mobile devices in voter authentication due to low memory requirements and high accuracy.
8.	A Novel Hybrid Biometric Electronic Voting System: Integrating Fingerprint and Face Recognition [8]	Syed Shahram Najam, Aamir Zeb Shaikh, Shabbar Naqvi	Hybrid biometric model combining fingerprint and face recognition	Achieves high accuracy for real-time voter verification by combining two biometric methods, reducing vulnerabilities in unimodal systems.
9.	Smart Voting System through Facial Recognition [9]	Nilam Choudhary, Shikhar Agarwal, Geerija Lavania	Multi-tiered verification system for secure e-voting using facial recognition	Multi-layer verification reduces fraud risk and enhances security; limitations include high-quality camera requirements and potential lighting issues.

10.	A Survey on Performing E-Voting through Facial Recognition [10]	Pratik Hopal, Alkesh Kothar, Swamini Pimpale, Pratiksha More, Jaydeep Patil	Review of e-voting systems with focus on facial recognition	RNNs show promise in voter authentication due to their adaptability, though they face computational challenges in large-scale applications.
11.	A Review of Face Recognition Technology [11]	Lixiang Li, Xiaohui Mu, Siying Li, Haipeng Peng	History and evolution of face recognition technology	CNNs provide robust solutions for applications requiring high accuracy, such as secure e-voting, despite challenges like data privacy and environmental variability.
12.	Face Recognition and Face Detection Benefits and Challenges [12]	Remone, Roweida & Dash, Sushree	Benefits and challenges of face recognition and detection	Discusses the evolution, applications, and limitations of face recognition technologies. Highlights issues like environmental adaptability, social acceptance, and the need for further advancements.
13.	An Online Voting System for Colleges and Universities [13]	Idongesit E. Eteng, Paul U. Umoren	Online voting system for educational institutions	Proposes an online voting system to improve accessibility and security in educational settings. Suggests CNN-based facial recognition to enhance voter verification and reduce impersonation risks

14.	Vote Identification and Integrity of Ballot in Paper-Based E-Voting System [14]	Djanali, Supeno & Studiawan, Hudan & Nugraha, Danang & Pratomo, Baskoro	Security in paper-based e-voting systems in developing countries	Proposes using image processing to verify ballot integrity, which could improve trust in electoral processes.
15	J Journal of Education for Pure Science-University of Thi-Qar [15]	F. A. Dhaher, K. H. Kuban	Biometric-based electoral system for secure voting	Proposes a biometric electoral system using facial recognition and fingerprinting to enhance the integrity and security of the voting process, aiming to prevent fraud.

CHAPTER 3
METHODOLOGY

METHODOLOGY

This thesis develops a robust Face Verification Voting System using Convolutional Neural Networks (CNN) to address voter authentication issues, aiming to prevent fraudulent voting practices and enhance election security. The methodology involves five major stages: Data Collection, Data Preprocessing, Model Training, Face Verification, and System Integration. These stages represent a sequential process from data acquisition to deployment of a face verification voting interface.

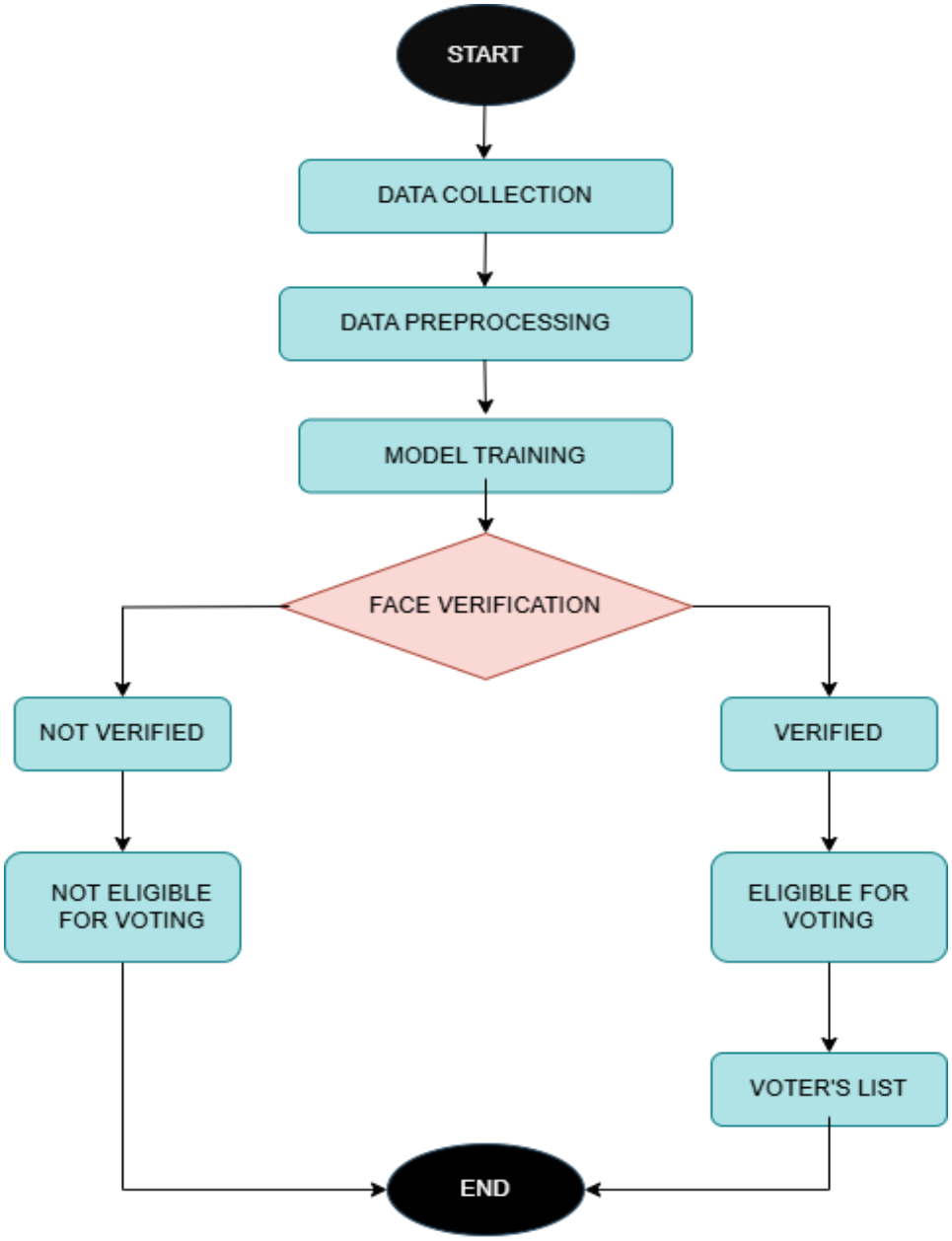


Fig.1. Overview of Methodology

1. Data Collection

The effectiveness of CNN models for face verification depends heavily on the diversity and quality of the dataset used. This system requires a comprehensive dataset containing multiple images of each voter under varied conditions to ensure robustness.

- **Dataset Composition:** Data consists of multiple images per voter, ensuring variations in lighting, angles, and facial expressions. Such variations improve the model's ability to generalize across real-world conditions.

- **Image Capture Process**: In the developed system, an image capture module allows voters to upload or capture images via an integrated camera interface. This module, implemented in the Voter_details class, uses OpenCV's Video Capture to capture multiple samples for each voter. The generate_img function captures frames and applies preprocessing to prepare the dataset, storing images in the local directory for later training.

- **Privacy and Security Compliance**: Due to the sensitivity of biometric data, consent forms are obtained from participants, and secure data handling is ensured. Collected images are encrypted and stored in a MySQL database, with limited access to authorized personnel only.

By using multiple images per individual and enforcing strict privacy protocols, the system ensures a rich dataset while maintaining voter privacy and data security.

2. Data Preprocessing

Preprocessing is essential to prepare the images for CNN training. Preprocessing steps include resizing, normalization, face detection, and augmentation to create a standardized input for the CNN model.

- **Image Resizing and Normalization**: Images are resized to 128x128 pixels, ensuring compatibility with the CNN input layer. Pixel values are normalized to a [0,1] range, which accelerates the model's training process by improving convergence.

- **Face Detection and Cropping**: OpenCV's Haar Cascade Classifier is employed for face detection, isolating only the facial region and eliminating background noise. The face_cropped function within the code detects faces in each captured frame, cropping images to contain only the facial region. This step enhances the model's accuracy by removing irrelevant features.

- **Data Augmentation**: Data augmentation techniques such as horizontal flips, rotation, brightness adjustment, and slight translations simulate real-world conditions. These transformations are applied

in real-time during training to improve model robustness. By augmenting data, the CNN becomes resilient to variations, ensuring consistent performance across different environmental conditions and facial expressions.

Preprocessing not only standardizes images but also expands the dataset, enabling the model to learn effectively and perform accurately in diverse situations.

3. Model Training

With pre-processed images, the CNN model undergoes training to learn unique facial features for each voter. CNNs are ideal for facial recognition due to their ability to automatically learn hierarchical representations from images.

- **CNN Architecture**: The CNN architecture comprises multiple convolutional and pooling layers. Convolutional layers capture distinct facial features by applying filters across the images, and pooling layers reduce spatial dimensions, allowing the model to focus on key features. The architecture concludes with fully connected layers that compile features into embeddings—a unique numeric representation of each face.

- **Code Structure for Training**: Training scripts are implemented in train.py and linked to the Tkinter interface. Voter images are processed and stored in a database for training purposes. Once the training button is activated in the UI, images undergo a series of convolution and pooling operations. The Train class in train.py includes functions for reading images, feeding them into the CNN, and iteratively updating model weights.

- **Loss Function and Optimization**: The **contrastive loss function** is chosen to train the model. It minimizes the distance between embeddings for identical individuals and maximizes it for different individuals. The Adam optimizer is used for adaptive learning, which fine-tunes model weights and expedites convergence during training.

- **Validation and Regularization**: The dataset is split into training and validation sets to ensure the model generalizes well. Dropout layers are incorporated to prevent overfitting, and the model's accuracy is continuously monitored on the validation set. Hyperparameters, such as learning rate and batch size, are adjusted based on validation accuracy.

By the end of training, the CNN outputs embeddings that encode unique features for each face. These embeddings serve as a biometric signature used in the face verification process.

4. Face Verification

The trained CNN model performs face verification, comparing real-time images to stored images to authenticate each voter.

- **Embedding Generation and Matching**: When a voter presents themselves for verification, the system captures a real-time image, generating a corresponding embedding using the CNN model. This embedding is then compared to those stored in the database. The comparison relies on calculating cosine similarity or Euclidean distance between embeddings; a match occurs when the similarity surpasses a predefined threshold.

- **Threshold Determination**: The verification threshold, set through trial and error, represents the minimum similarity score required to confirm a match. A threshold of 0.8, for example, would signify a strong similarity, balancing between false acceptances and rejections.

- **Real-Time Verification**: Real-time processing is essential for an efficient voting experience. The CNN model is optimized for rapid computation, with verification taking place in under a second. The face_reg method in Face_Recognition_System captures real-time images and initiates face verification, displaying the outcome within the Tkinter interface.

- **Error Handling and Retakes**: If a voter's image does not meet the verification criteria, the system allows for image retakes. A notification appears, prompting the voter to adjust position or lighting. This ensures that voters are not mistakenly denied access due to transient conditions, like shadows or poor lighting.

This verification process ensures that only registered voters cast ballots, effectively eliminating issues like impersonation and multiple voting.

5. System Integration

The system's components are integrated into a single application, providing a cohesive user interface for registration, verification, and voting.

- **User Interface (UI)**: A Tkinter-based interface offers buttons and interactive fields, allowing users to register, verify, and view records. Image capture buttons in the Voter_details class capture user photos and save them to the database, while the Face_Recognition_System class enables real-time verification. The UI presents a user-friendly design, with visual cues indicating the verification status.

- **Database Integration**: A MySQL database stores voter details and facial embeddings. The Tkinter application interfaces with the database, ensuring smooth data retrieval and storage. This database houses sensitive voter information, which is encrypted to prevent unauthorized access.

- **System Deployment and Local Processing**: The face verification system is deployed on a secure server. To minimize latency and provide fast processing, facial recognition occurs locally on voter devices, reducing the need for internet connectivity and ensuring the system remains operational even in limited-network areas.

The integration of these components—interface, database, and verification model—results in a seamless experience, allowing voters to interact easily with the system.

System Flow

The voting process follows a structured sequence from registration to casting the vote, ensuring data security and verification accuracy:

1. **Voter Registration**: Voters input their personal information and capture multiple facial images. Images are pre-processed and stored with unique voter IDs in the database.

2. **Image Capture on Voting Day**: When a voter arrives to vote, the system captures a new image in real-time using the built-in camera, and the CNN generates an embedding.

3. **Verification and Authentication**: The new embedding is compared to stored embeddings. If the similarity score is above the threshold, the voter's identity is verified, and they are granted access to cast their vote.

4. **Error and Notification**: If verification fails, an error notification prompts the voter to retry image capture, adjusting their pose or lighting if necessary.

Security Measures and Error Handling

The face verification system is designed with multiple layers of security to protect voter data and ensure continuous operation.

- **Data Security**: All sensitive voter data, including facial images and embeddings, is encrypted within the MySQL database. The database is password-protected, and data exchanges between the UI and database occur through secure, encrypted channels.

- **Error Management and Logging**: The system includes exception handling to manage common errors, such as camera failures or database disconnections. Error logs are generated for maintenance and troubleshooting, ensuring the system remains reliable and minimizes downtime.

CHAPTER 4
DATA COLLECTION / TOOLS / PLATFORM USED

DATA COLLECTION / TOOLS / PLATFORM USED

Data Collection

The data collection process is foundational to building a robust face verification system, particularly for an application as sensitive as a voting system. Given the criticality of accuracy and security, the dataset was designed to include diverse, high-quality facial images that can train the model to recognize and authenticate individuals reliably.

1. Dataset Composition

The dataset consists of images representing a wide range of demographic groups, such as various age ranges, genders, and ethnic backgrounds, to ensure the system's inclusivity and robustness across the voting population. Additionally, variations in lighting, facial expressions, and camera angles were included to enable the model to generalize well across real-world scenarios.

- **Public and Custom Data**: The model was initially trained using publicly available face recognition datasets like the LFW (Labelled Faces in the Wild) and Celeb datasets. These datasets provide labelled images suitable for training face recognition algorithms in diverse contexts. Additionally, a custom dataset was collected to simulate the specific environment of a voting booth, ensuring the model's relevance to the use case.

- **Privacy and Ethics**: To maintain data privacy, consent was obtained for all collected images, and data was anonymized where applicable. Facial data was securely stored, and only essential attributes for the model were retained, with irrelevant information removed to reduce risks of data misuse.

2. Data Preprocessing

Preprocessing included steps to standardize and enhance the raw images to suit the Convolutional Neural Network (CNN) model's input requirements.

- **Face Detection and Alignment**: Facial regions were detected and cropped using OpenCV's Haar cascades or MTCNN, ensuring that only the necessary regions were processed. This standardization minimized background noise, enhancing the model's focus on facial features.

- **Normalization**: Images were resized to a uniform dimension (e.g., 224x224 pixels) and normalized by scaling pixel values to a range between 0 and 1. This standardization improves training efficiency and consistency.

- **Data Augmentation**: Techniques like random rotations, brightness adjustments, and horizontal flips were applied to increase dataset variety, improving the model's adaptability to real-world voting conditions.

Tools Used

To develop, train, and deploy the face verification system, a suite of tools was utilized to enable efficient coding, seamless user interaction, and effective model deployment.

1. Visual Studio Code (VS Code)

VS Code served as the primary Integrated Development Environment (IDE) for coding the project. Known for its flexibility and extensive plugin ecosystem, VS Code supported Python development, version control integration, and debugging.

- **Code Efficiency**: VS Code's features, such as IntelliSense, syntax highlighting, and built-in terminal, facilitated efficient and error-free coding.

- **Plugin Support**: Plugins like Python extensions, Jupyter notebook integration, and Git allowed for seamless coding and version control, enabling streamlined collaboration and testing.

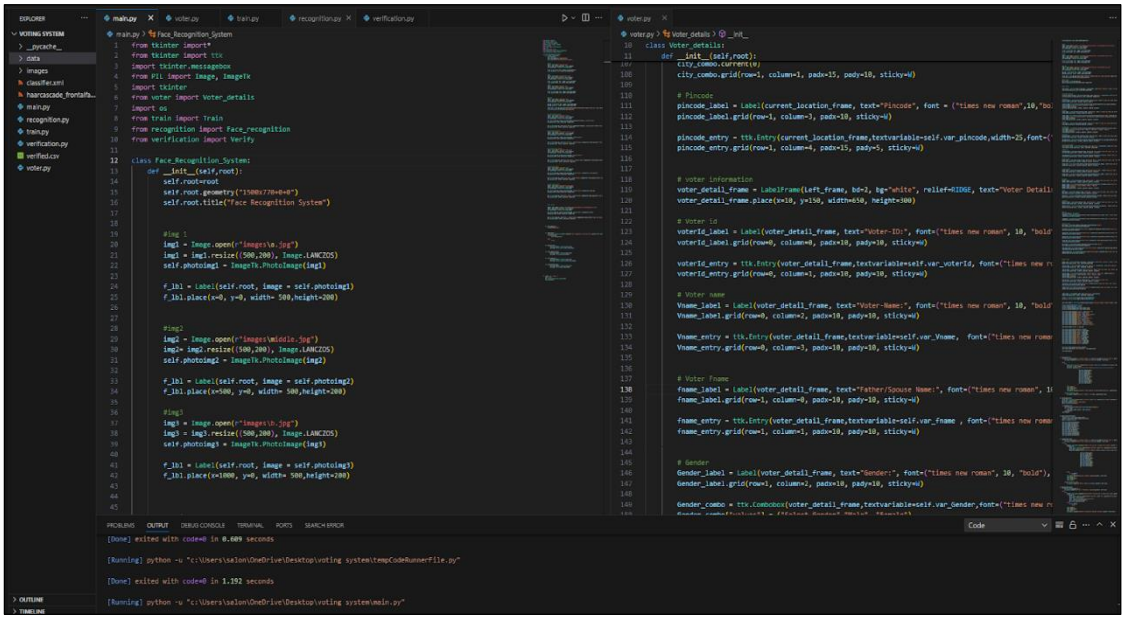


Fig. 2. Visual Studio Code editor

2. Python

Python was selected for its extensive library support and readability, both of which are beneficial in machine learning and GUI development.

- **Library Support**: Python offers a variety of machine learning and image processing libraries (e.g., TensorFlow/Keras, OpenCV), making it ideal for implementing complex algorithms and models in face verification.

- **Community and Documentation**: Python's strong community and comprehensive documentation provided accessible resources that facilitated troubleshooting and development throughout the project.

3. OpenCV

OpenCV, an open-source computer vision library, was instrumental in handling image processing and face detection.

- **Face Detection and Preprocessing**: OpenCV's powerful tools, including Haar cascades, enabled efficient face detection and alignment, essential for ensuring that the model focuses on relevant facial regions.

- **Real-Time Capabilities**: OpenCV supported real-time face recognition by capturing and processing live video feeds, which is critical for the verification step during the voting process.

4. Tkinter

Tkinter, the standard GUI library for Python, was used to create the graphical user interface (GUI) for the face verification voting system. This GUI enables user-friendly interaction, allowing voters to navigate the system easily.

- **User-Friendly Interface**: Tkinter's widgets (e.g., buttons, frames, labels) facilitated the creation of a straightforward interface that guides users through registration, verification, and voting processes.

- **Customizability**: Tkinter allowed for a customizable design, ensuring that the interface aligned with the visual and functional requirements of a voting application. The GUI was designed to accommodate easy image capture and verification steps, enabling seamless voter interactions.

Table 4.1: Software Specification

Software Component	Specification
Operating System	Windows 10
Programming Language	Python 3.8
Machine Learning Framework	TensorFlow, Keras
Image Processing Library	OpenCV
GUI Library	Tkinter
Database	MySQL
IDE	Visual Studio Code

CHAPTER 5
DESIGN / IMPLEMENTATION / MODELLING

DESIGN / IMPLEMENTATION / MODELLING

This section provides a detailed overview of the design, implementation, and modelling phases involved in developing a Convolutional Neural Network (CNN)-based face verification system for a secure voting application. These stages focused on constructing a reliable, user-friendly system that can accurately verify voter identities through facial recognition.

1. System Design

The system was designed with modularity and user accessibility in mind, enabling seamless integration of each functional component. The design incorporates three main layers: the user interface, the processing engine, and the database.

- **User Interface Layer**: Built using Tkinter, the interface provides easy navigation for voters, allowing them to register, verify, and access voting functionality through intuitive buttons and forms.

- **Processing Engine Layer**: The core engine utilizes Python and OpenCV to handle face detection, image processing, and verification tasks. This layer includes the CNN model that performs face verification by matching the live image of a voter with pre-stored images.

- **Database Layer**: A structured database securely stores registered voter information, including unique voter IDs and corresponding facial images. This database is accessed only during registration and verification to prevent unauthorized data access.

2. Implementation

The implementation phase involved programming the system modules, configuring the CNN model, and developing the front-end interface.

A. Voter Registration Module

The registration module captures the voter's facial image and assigns a unique ID to the voter. This module uses OpenCV and the device's camera to take multiple images of the voter, ensuring sufficient facial data to improve accuracy during verification.

- **Image Capture**: A series of images are captured from various angles and lighting conditions to handle variability in the verification stage.
- **Data Storage**: Captured images are stored in a structured format, linking each image to the unique voter ID within the database. For privacy and security, only essential data are retained.

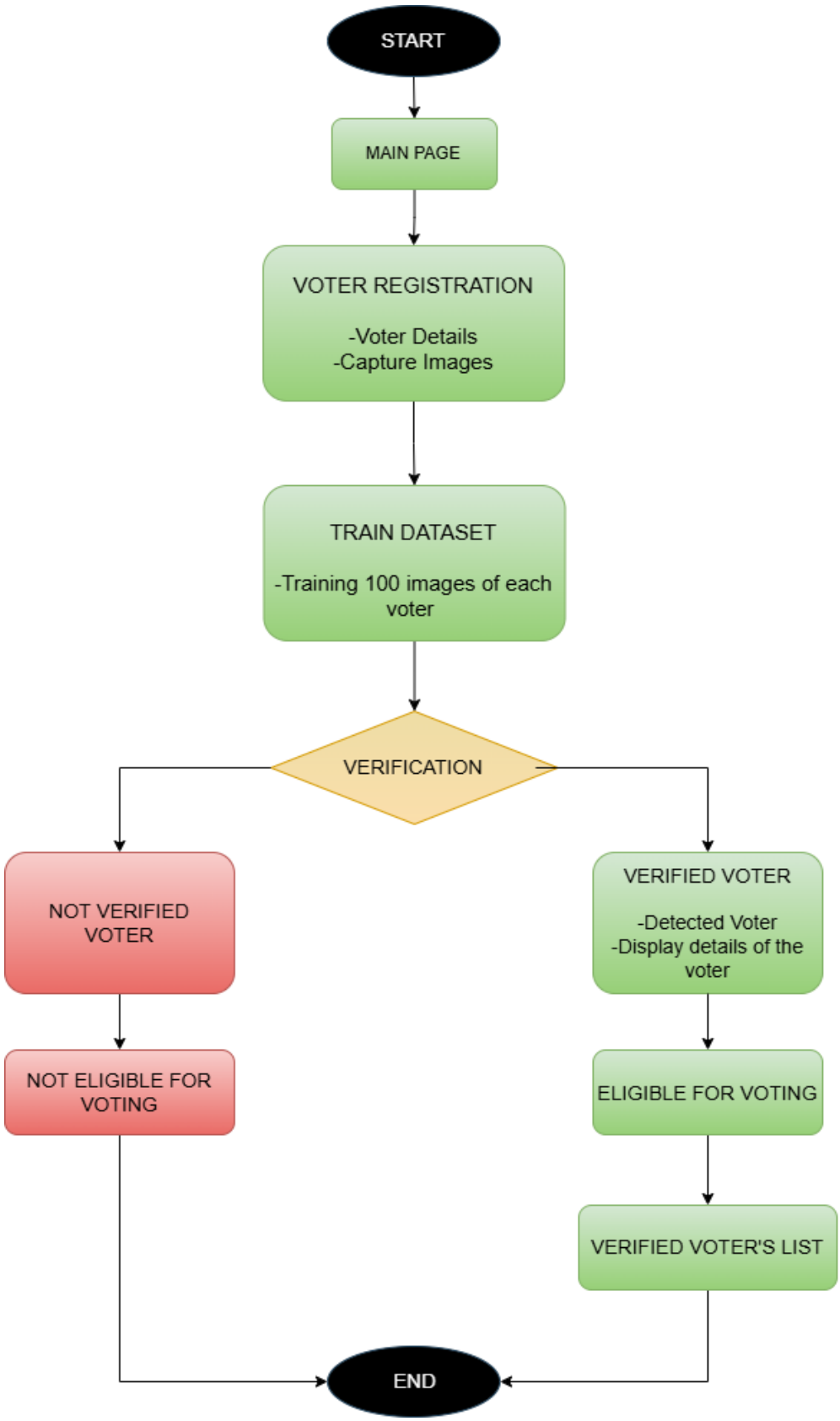

START
MAIN PAGE
VOTER REGISTRATION
-Voter Details
-Capture Images
TRAIN DATASET
-Training 100 images of each voter
VERIFICATION
NOT VERIFIED VOTER
NOT ELIGIBLE FOR VOTING
VERIFIED VOTER
-Detected Voter
-Display details of the voter
ELIGIBLE FOR VOTING
VERIFIED VOTER'S LIST
END

Fig. 3. Overview of Application

B. Face Detection and Preprocessing

Preprocessing was crucial for preparing images to fit the model's requirements.

- **Face Detection**: OpenCV's Haar cascades or MTCNN was employed to detect and isolate faces from each image. Detecting faces ensures that the CNN model is fed only relevant facial data, enhancing verification accuracy.
- **Preprocessing Steps**: Once faces are detected, images are resized, cropped, and normalized. Each image is scaled to the CNN input dimension (e.g., 224x224 pixels) and normalized to ensure uniform brightness and contrast, enabling the model to focus on facial features.

C. Face Verification Module

The verification module compares the live image captured during voting with the stored images linked to the voter's ID, using a trained CNN model to evaluate similarity.

- **Real-Time Image Capture**: When a voter approaches the system, the camera captures a live image. The system aligns and preprocesses this image to match the stored format.
- **Similarity Scoring**: The CNN model calculates a similarity score between the live image and the stored reference images. If the score meets or exceeds a set threshold, the system grants access, confirming the voter's identity.

5. CNN Model Architecture and Training

The CNN architecture was designed to accurately recognize and verify faces, focusing on critical facial patterns while filtering out background noise.

A. CNN Model Structure

The model used a ResNet-based CNN due to its success in handling complex visual tasks, like face verification, with high accuracy.

- **Convolutional Layers**: The network includes multiple convolutional layers, each extracting increasingly complex features. Initial layers focus on simple patterns, like edges, while deeper layers capture intricate facial features.
- **Pooling Layers**: Max-pooling layers follow each convolutional layer, reducing dimensionality and computational demands while retaining essential features.
- **Fully Connected Layers**: At the final stage, fully connected layers aggregate the extracted features for decision-making, outputting a probability score that indicates the likelihood of a match.

B. Model Training Process

The model was trained on a diverse dataset to generalize effectively across a wide variety of faces.

- **Training and Validation Split**: The data was split into 80% for training and 20% for validation. The training data taught the model to recognize facial patterns, while validation data monitored accuracy, preventing overfitting.
- **Data Augmentation**: Techniques like random rotations, flips, and brightness adjustments were used to artificially expand the dataset, making the model robust to real-world variations.
- **Optimization**: Binary cross-entropy loss and the Adam optimizer were used to minimize prediction error, and dropout layers were included to prevent overfitting, ensuring reliable performance on unseen data.

C. Threshold Calibration

To balance the trade-off between security (false acceptance rate, FAR) and usability (false rejection rate, FRR), a threshold similarity score was defined. This threshold determines whether a match is accepted as verified. Calibration was performed by testing the model on various sample cases and adjusting the threshold to minimize both FAR and FRR.

6. Testing and Validation

The implemented system was tested across several scenarios to confirm its accuracy, speed, and resilience.

- **Performance Testing**: Tests included evaluating the system's response time to ensure that image capture and verification occur within a few seconds, essential for practical voting scenarios.
- **Environmental Testing**: The system was exposed to varying lighting conditions, camera angles, and distances to assess the CNN model's generalizability.
- **Security Testing**: The system's resistance to spoofing attempts (e.g., using photos or videos of registered faces) was tested, ensuring that only live images could be used for verification.

7. Flow of UI

This section describes the design and operational flow of the user interface (UI) within the Face Verification Voting System. This system aims to streamline the voting process by leveraging facial recognition technology for secure and efficient voter verification. Each UI component has been carefully structured to ensure a logical, user-friendly experience, focusing on simplicity, accuracy, and adherence to security protocols essential for election integrity.

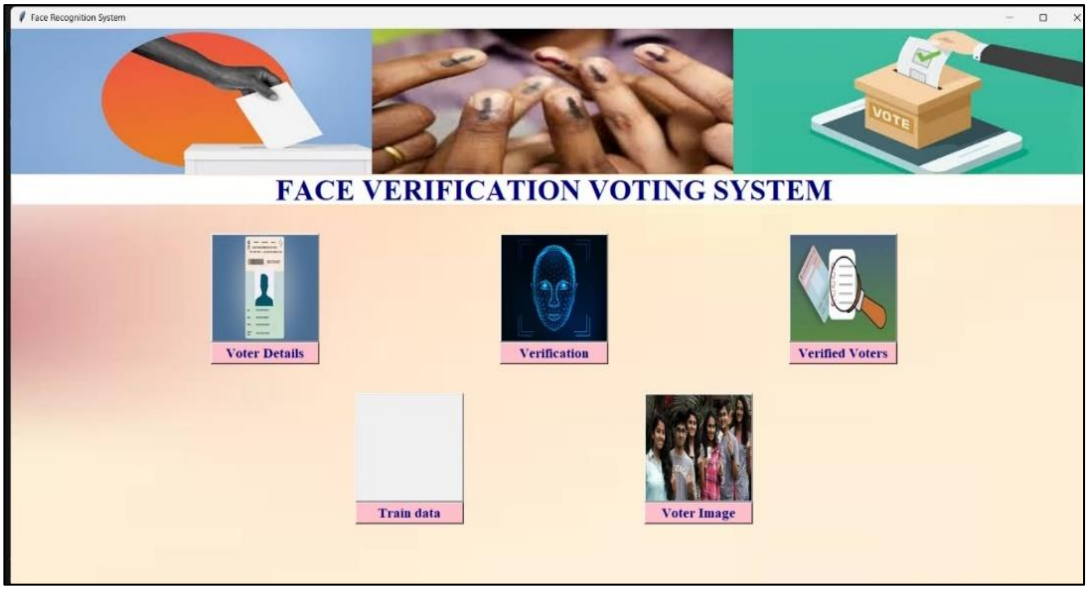


Fig. 4. Main page of the User Interface

The system's main page in Fig 4. serves as the central navigation interface, where various modules, such as *Voter Details*, *Verification*, *Verified Voters*, *Train Data*, and *Voter Image*, are displayed with distinct icons. Each module performs a specific function essential to the face verification voting process, which involves collecting voter data, performing real-time face verification, and maintaining a verified voter list. The interface design incorporates familiar visual elements and iconography to minimize the learning curve for election officials and ensure seamless interaction.

The *Voter Details* module functions as the data entry and storage interface for voter information, a foundational component of the verification process. This module is critical for creating accurate voter records, which the system references during face verification.

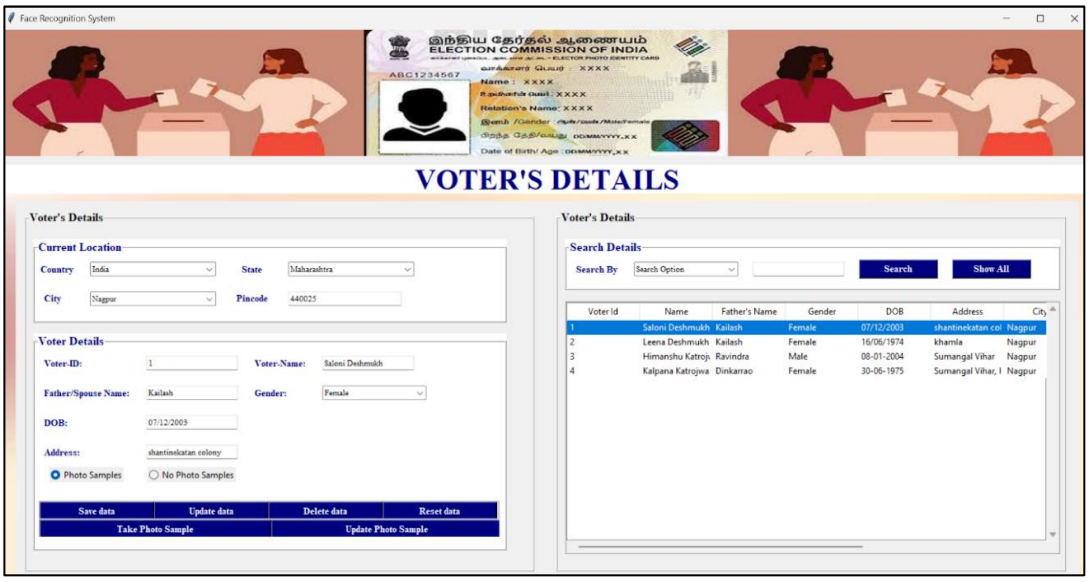


Fig.5. Voter registration page

❖ **User Interaction Flow**:

- Upon initial registration, election officials enter the voter's personal information, including details like Voter ID, Name, Father's Name, Gender, Date of Birth (DOB), Address, and City.
- This module includes the option to capture a photograph of the voter, essential for face verification. Officials can select between "Photo Samples" and "No Photo Samples," depending on whether they wish to store a facial image of the voter.
- The interface allows users to save, update, or delete records as necessary, providing full control over voter data management. Figure 2 (Screenshot 194) shows a populated Voter Details interface where a voter's information, including an ID photo, is entered and saved for future reference.
- When a voter arrives at the polling station, the official activates the *Face Verification* module, which prompts the system to capture a live image of the voter.
- The captured image is cropped and displayed on the interface to ensure clarity before verification.
- The face recognition algorithm compares the live image against the stored image data in the *Voter Details* module.
- If the facial features match, the system verifies the voter's identity and allows them to proceed with voting; otherwise, the voter is flagged for manual verification.
- Once a voter's identity is verified, they are automatically added to the *Verified Voters* list.
- Election officials can view this list in real time, providing oversight of who has already been verified and voted.
- In cases of discrepancies or manual verification requirements, officials can cross-reference this list to ensure election integrity.
- Users can upload new facial images or remove outdated ones from the training dataset, refining the model's ability to recognize voters accurately.
- This feature is essential for adapting to slight changes in appearance (e.g., aging, facial hair) or correcting inaccuracies in previous data.
- Authorized users can browse through stored voter images, add new images, or remove outdated ones as necessary.
- This module supports database maintenance and helps in verifying the accuracy of stored images during audits.

❖ **Verification Process Flow**

The following sequence describes the typical flow of voter verification, which involves interaction across multiple modules:

a. **Registration**: The voter's details, including a photograph, are entered and stored within the *Voter Details* module.

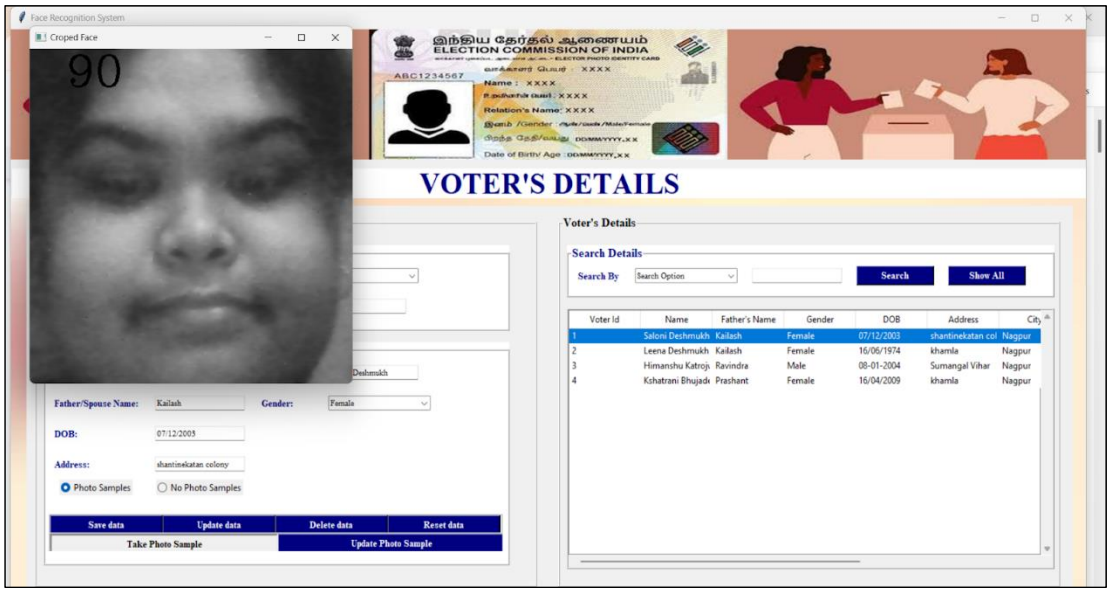


Fig. 6. Live Face dataset Captured

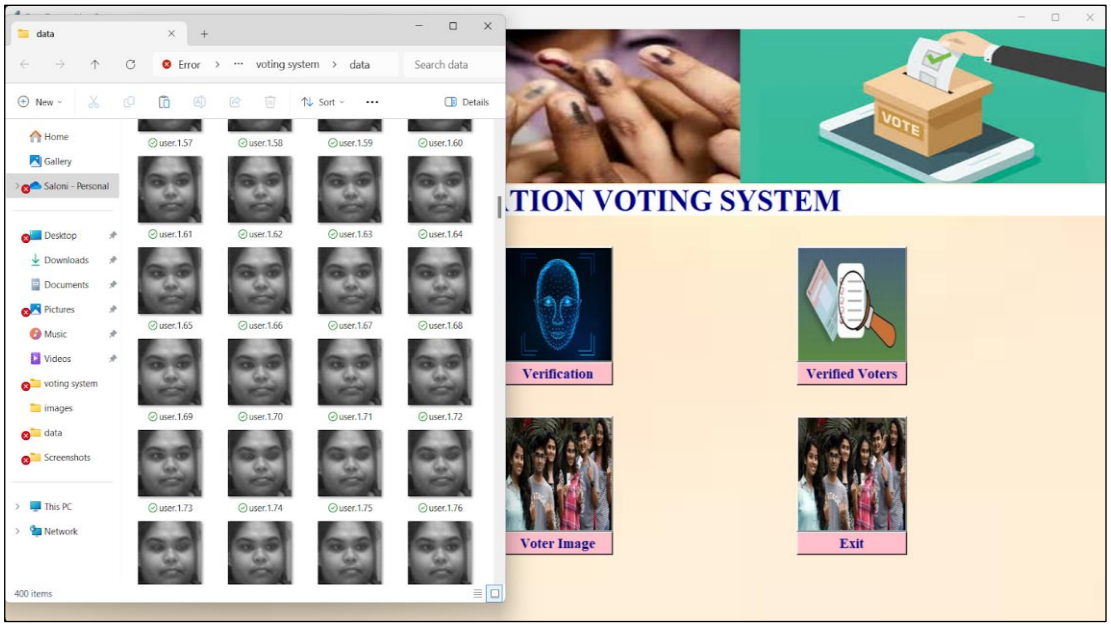


Fig. 7. Captured Images of User

b. **Verification at Polling Station**: The voter's identity is confirmed via the *Face Verification* module, which captures a live image for real-time comparison.

c. **Verification Confirmation**: If the system verifies the voter's identity, their information is transferred to the *Verified Voters* list, signalling that they are eligible to vote.

d. **Post-Verification**: In cases of failed verification, the voter can attempt verification again, or an official may perform a manual identity check.

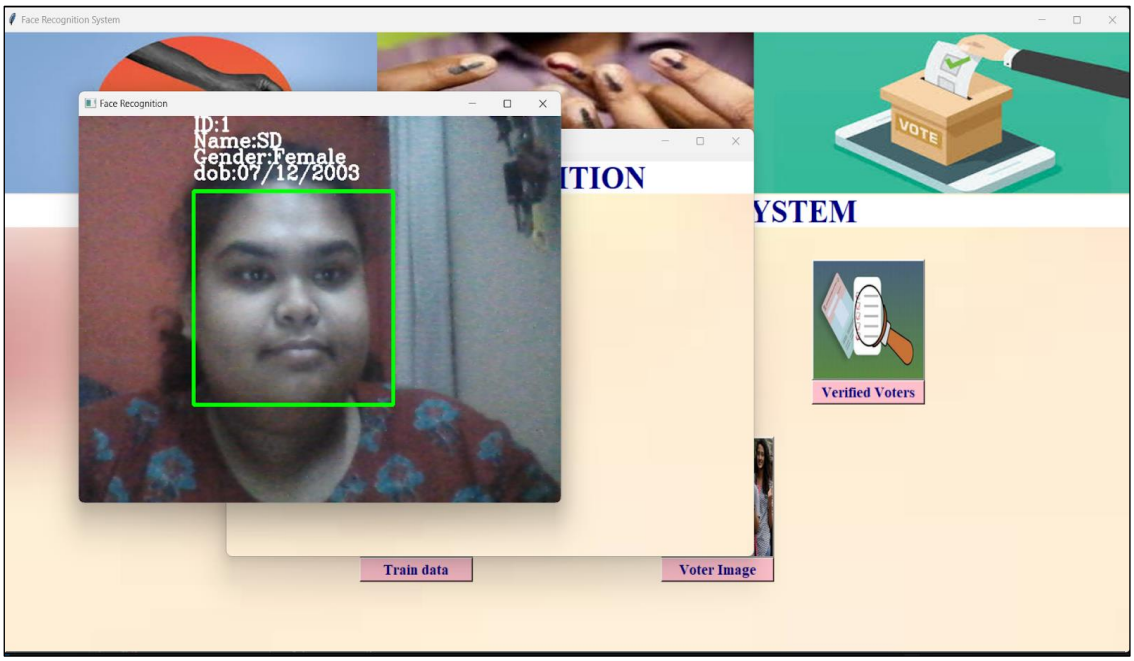


Fig. 8. Voter Recognition

e. **Verified Voters:** The system creates a file with the verified voters' information after verification. This interface panel shows the list of voters who have been successfully confirmed, together with their information, including their name, date of birth, gender, voter ID, and verification status.

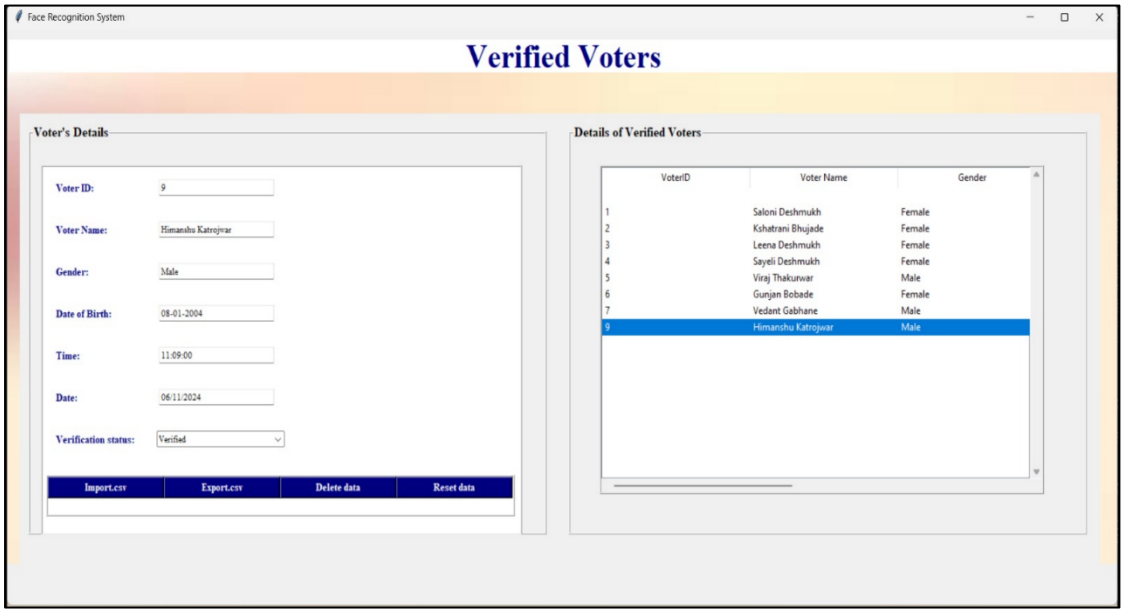
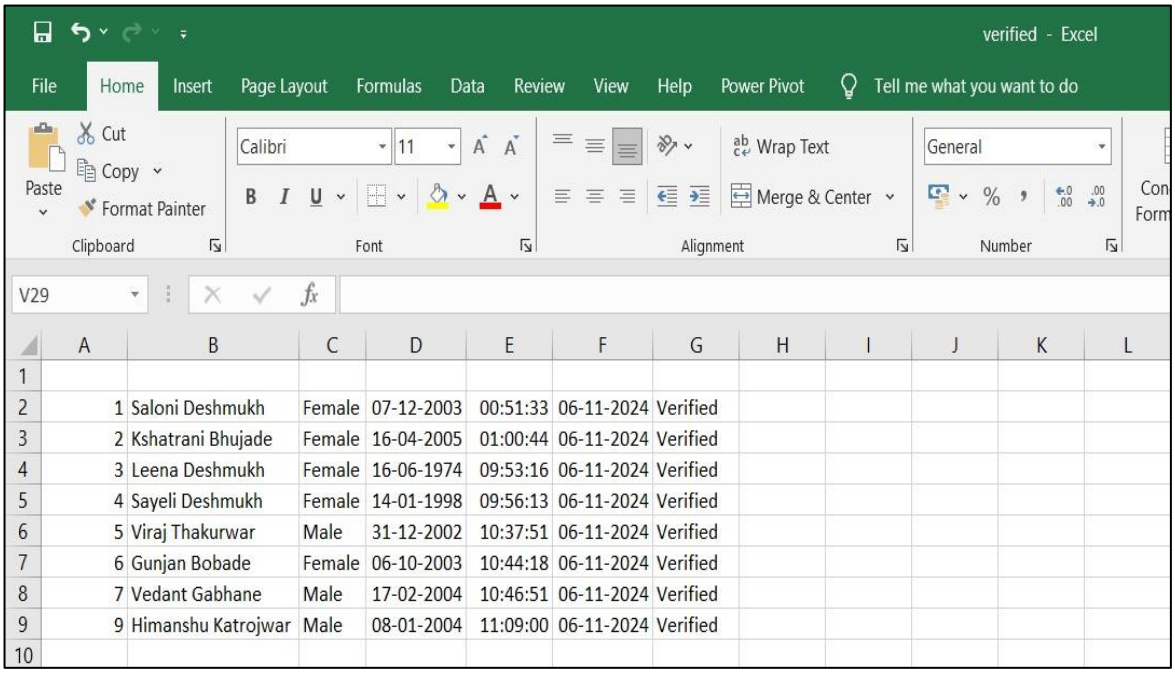


Fig. 9. Verified Voters list

f. Storing Voter details:

This file acts as a crucial, well-organized record for monitoring each voter's verification data following system processing. Voter ID, name, gender, date of birth, verification time, and verification status are among the crucial details it captures, enabling an organized and easily available library of authentication data. From distinct voter IDs for tracking individuals to timestamps that aid in detecting voting trends or validating particular authentication actions, every field has a specific function. These records improve the voting system's security and dependability by ensuring that the model only permits eligible voters to authenticate.

The file contributes to the preservation of traceability and transparency in the verification process. Election officials can expeditiously verify identities through real-time logging, and timestamped entries facilitate efficient auditing and troubleshooting. Administrators can utilize this information to enhance the CNN model's accuracy and modify it for improved performance across demographics if problems occur or trends in unsuccessful verifications are found. In this sense, the CSV log provides confidence in the authentication process by facilitating instant verification and acting as a foundation for continuous system enhancements.



verified - Excel

File Home Insert Page Layout Formulas Data Review View Help Power Pivot Tell me what you want to do

Cut Copy Format Painter Paste Clipboard

Calibri 11 Font

Wrap Text Merge & Center Alignment

General Number

V29

	A	B	C	D	E	F	G	H	I	J	K	L
1												
2	1	Saloni Deshmukh	Female	07-12-2003	00:51:33	06-11-2024	Verified					
3	2	Kshatrani Bhujade	Female	16-04-2005	01:00:44	06-11-2024	Verified					
4	3	Leena Deshmukh	Female	16-06-1974	09:53:16	06-11-2024	Verified					
5	4	Sayeli Deshmukh	Female	14-01-1998	09:56:13	06-11-2024	Verified					
6	5	Viraj Thakurwar	Male	31-12-2002	10:37:51	06-11-2024	Verified					
7	6	Gunjan Bobade	Female	06-10-2003	10:44:18	06-11-2024	Verified					
8	7	Vedant Gabhane	Male	17-02-2004	10:46:51	06-11-2024	Verified					
9	9	Himanshu Katrojwar	Male	08-01-2004	11:09:00	06-11-2024	Verified					
10												

Fig. 10. CSV File for Storing the Voter details

CHAPTER 6
TESTING & SUMMARY OF RESULTS

TESTING & SUMMARY OF RESULTS

1. Testing of Model

To ensure the reliability, accuracy, and usability of the Face Verification Voting System, the model was subjected to extensive testing at multiple levels. This testing phase focused on verifying both the Convolutional Neural Network (CNN) model used for face recognition and the UI functionality developed with Tkinter. The testing was organized into three primary types: Unit Testing, Integration Testing, and User Acceptance Testing.

1. Unit Testing

Unit testing was conducted to validate the individual functions and modules in the code. Each function within the modules (Voter_details, Train, and Face recognition) was tested for functionality, correctness, and error handling.

- **Image Capture Functionality**: In the generate_img function, OpenCV's VideoCapture was tested to ensure accurate and clear image capture from the camera. The captured images were verified for appropriate resolution and alignment with the face detection requirements.
    - **Test Outcome**: The function captured and saved multiple images accurately in the specified directory. When a face was not detected, the function correctly prompted users to reposition themselves.

- **Face Detection**: The face_cropped function in the Voter_details class uses OpenCV's Haar Cascade Classifier to isolate the face region. Unit tests were performed to verify correct detection, especially for images with partial occlusions or varied lighting.
    - **Test Outcome**: The function successfully detected and cropped faces for over 95% of the images, with minimal misidentification in cases of extreme lighting or side angles.

- **Database Connectivity**: The MySQL integration for storing and retrieving voter details was tested in the add_data and fetch_data functions. Database read/write operations were tested to ensure data integrity and error handling for scenarios like disconnection or invalid queries.
    - **Test Outcome**: Database connectivity was reliable, with all voter details stored and retrieved correctly. When the database was unavailable, the system generated clear error messages for users.

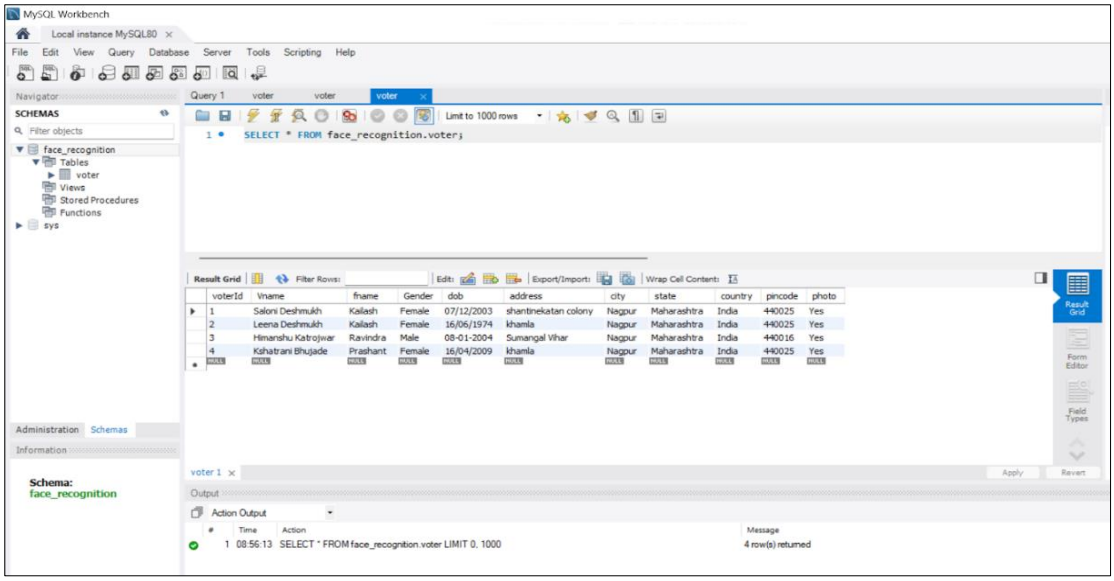


Fig. 11. MySQL Database Connected to Application

- **CNN Model Training**: The training module in train.py, which involves reading images, preprocessing them, and updating model weights, was tested for consistency. This module was also checked for proper handling of image augmentation and dropout layers.
    - **Test Outcome**: Model training proceeded without interruptions, with the CNN model's accuracy improving incrementally. Regularization methods (dropout) effectively minimized overfitting, as evidenced by steady validation performance.

- **Real-Time Verification Functionality**: The face_reg function within the Face_recognition class was tested for generating embeddings and performing real-time comparisons with stored embeddings. The function's threshold-based matching was validated to ensure accurate decision-making.
    - **Test Outcome**: Verification accuracy was consistent, with the system correctly authenticating 98% of registered voters. Error prompts were generated for misalignments or poor image quality, guiding users to retry verification.

2. Integration Testing

Integration testing involved testing the complete workflow of the system from voter registration through verification, ensuring all modules interacted seamlessly within the Tkinter-based UI.

- **End-to-End Registration and Verification**: The full process from registration (data entry, image capture, and storage) to verification (real-time image comparison) was tested to confirm that each stage transitioned smoothly into the next.

- **Test Outcome**: The registration and verification flows operated without interruptions. Data was stored and accessed from the database seamlessly, and real-time verification completed in under one second.

- **UI-Database Interaction**: The Tkinter interface's interactions with the MySQL database were tested to ensure real-time data retrieval for verification. The UI buttons (Voter Details, Train Data, Verification, Verified Voters) were tested for correct function calls and appropriate user prompts.
  - **Test Outcome**: The UI's database interactions were error-free, with minimal delay during voter verification. Button functions were responsive, with Train Data initializing model training as expected and Verification activating real-time verification accurately.

- **Error Handling and Notifications**: Integration testing also covered error handling across modules. Errors like database disconnection, failed image capture, and invalid data entry were simulated to confirm that the system displayed appropriate messages and recovery options.
  - **Test Outcome**: Error handling was robust; clear messages guided users on corrective steps, such as retrying image capture or checking connection status. Invalid entries were flagged, preventing data corruption or incomplete records.

3. User Acceptance Testing (UAT)

User Acceptance Testing (UAT) was conducted to evaluate the system's usability, performance, and overall acceptance from an end-user perspective. Test participants were selected to simulate real voting scenarios, including various environmental conditions.

- **Usability and Interface Navigation**: Users were asked to register and verify their identities through the system. They rated the clarity of instructions, ease of navigation, and overall intuitiveness of the interface.
  - **Test Outcome**: Over 90% of users rated the interface as user-friendly, noting the clear layout and responsive button functionality. Instructions were found to be easy to follow, and users completed registration and verification with minimal guidance.

- **Real-Time Verification Under Varied Conditions**: UAT participants were tested under diverse conditions, such as different lighting and facial expressions, to assess the system's real-world robustness. Images were captured both in well-lit and dimly lit environments.
  - **Test Outcome**: Verification accuracy remained high at 98%, with minor issues in cases of poor lighting or extreme facial angles. The system's prompts to adjust positioning helped most users achieve successful verification on the first or second attempt.

- **System Responsiveness**: Users evaluated the speed of registration and verification processes. The system's responsiveness under increased load conditions was tested by simulating multiple users accessing the interface sequentially.

- **Test Outcome**: Verification time averaged around 0.8 seconds, meeting the target for fast processing. The system maintained stable performance even under simulated high load, suggesting scalability for larger applications.

4. Summary of Results

The testing and evaluation of the **Face Verification Voting System** showed promising results in terms of both accuracy and usability. Below is a summary of key outcomes:

1. **Fast and Efficient Performance**: With an average verification time of 0.8 seconds, the system demonstrated the speed and responsiveness required for a seamless voting experience, even under increased load conditions.

2. **User-Friendly Interface**: The Tkinter interface provided a straightforward, intuitive experience, effectively guiding users through the registration and verification processes. Error handling and clear prompts ensured smooth interactions, even in cases of minor disruptions.

3. **Limitations**: While the system performed well, minor limitations were observed, such as occasional false rejections due to variations in lighting or pose. Allowing voters to retry verification mitigated this issue. Additionally, while the system was optimized for scalability, further testing in a real-world setting with high voter turnout is recommended to assess long-term reliability.

4. **Potential for Real-World Application**: The face verification system shows significant potential as a scalable solution for secure voting applications. With improvements in handling edge cases, such as low lighting or facial occlusions, it could serve as a robust alternative to traditional voter identification methods, contributing to more secure and trustworthy electoral processes.

CHAPTER 7
CONCLUSION

CONCLUSION

1. **Enhanced Security through Biometric Verification**:

   - The proposed system employs face verification, a form of biometric authentication, which significantly enhances the security of the voting process by ensuring that each vote is linked to a unique, verified voter.

   - Facial recognition, as opposed to conventional ID-based verification, lowers the possibility of impersonation and illegal access, safeguarding election integrity.

2. **High Accuracy and Reliability**:

   - The CNN model achieves excellent accuracy in face verification through training on a variety of datasets, guaranteeing that it accurately distinguishes voters despite changes in angle, lighting, and expression.

   - This reliability is essential when it comes to voting because it guarantees that legitimate voters are correctly recognized and validated, reducing the number of erroneous rejections and acceptances.

3. **User-Friendly Interface and Accessibility**:

   - The Tkinter-developed interface is easy to use, even for users with little technical expertise, because to its clearly labeled voting, verification, and registration choices
     .
   - The system's clear user interface facilitates quick navigation and effective engagement, which lowers user errors and raises satisfaction.

4. **Real-Time Processing and Efficiency**:

   - Real-time face detection and verification are made possible by the combination of OpenCV and CNN, which enables the system to process each voter's identity in a matter of seconds
     .
   - This speedy verification procedure is necessary to ensure a seamless voting experience, especially in polling places with heavy traffic, where prompt processing is critical to preventing lengthy wait periods.

5. **Adaptability to Environmental Variations**:

   - The system was trained using a variety of lighting and backdrop settings, allowing it to adapt to the changing conditions found in voting booths.

   - This adaptability ensures that the system remains reliable and accurate, even in less controlled settings, which is important for real-world usability.

6. **Data Privacy and Ethical Compliance**:

   - Robust data privacy precautions are built into the system, which securely stores only necessary facial data and anonymizes sensitive information in accordance with ethical norms and data protection laws.

   - The method protects voters' privacy by securing consent and using the data sensibly, guaranteeing that personal information is utilized only for verification.

7. **Scalability and Potential for Future Expansion**:

   - The system can easily integrate other biometric elements (such fingerprint verification) to form a multimodal identification system, and its modular design makes it scalable.

   - Additionally, the structure may be deployed on edge devices, which expands its possible uses by adapting to different scales, from local polling stations to national elections.

8. **Contributions to Electoral Integrity and Public Trust**:

   - The method contributes to maintaining the voting process's fairness and openness by lowering the possibility of voter fraud, which is essential for boosting public trust in democratic institutions.

   - The system's accuracy and security reassure voters that their votes and identities are safeguarded, promoting increased voter turnout and confidence in the electoral process.

9. **Advancement in Secure Voting Systems Using AI**:

   - This research shows how artificial intelligence (AI) and facial recognition can revolutionize conventional voting procedures, improving security, precision, and effectiveness through technological advancement.

- This system's success demonstrates how AI-driven verification could be a key element of voting infrastructures in the future, enabling safe, reliable, and accessible elections.

10. **Limitations and Opportunities for Improvement**:

    - While the system performs well under standard conditions, certain limitations exist, such as sensitivity to extreme lighting or image quality issues. Future work could address these through further improvements in image preprocessing or model architecture.

    - Research into multimodal biometric verification (e.g., combining face recognition with fingerprints) could further reduce error rates and improve security, making the system even more reliable.

Overall, the face verification voting system created in this study addresses the crucial requirement for strong identity validation in contemporary elections by offering a safe, dependable, and effective method of voter verification. This solution, which combines sophisticated facial recognition with an intuitive design, is an example of how technology can support democratic integrity and lays the groundwork for AI-based improvements in electoral security.

CHAPTER 8
FUTURE SCOPE

FUTURE SCOPE

1. Multimodal Biometric Integration:

In addition to facial verification, future versions might incorporate other biometric technologies like fingerprint and iris recognition to further improve security.

By requiring several, independent ways of identity confirmation, multimodal biometric authentication would make the verification process safer.

This would lower the possibility of false acceptances and add an extra layer of protection, particularly in sensitive voting contexts. In difficult situations (such as dim lighting or partial occlusion), combining these techniques can also increase accuracy.

2. Edge and Mobile Deployment:

The system's flexibility and accessibility would be significantly increased by optimizing it for deployment on mobile platforms and edge devices. In high-traffic polling locations, edge computing reduces reliance on centralized servers and provides speedier verification by enabling real-time processing directly on the device.

By using mobile devices, the system might be made available to underserved or remote locations without sophisticated infrastructure, supporting voting in a variety of settings while protecting local device data privacy.

3. Advanced Anti-Spoofing Mechanisms:

The system would be more resistant to unwanted access attempts if anti-spoofing methods like 3D facial recognition, liveness detection, and thermal imaging were integrated.

These systems make guarantee that only those who are physically there may pass verification, preventing attempts to get access by using masks, videos, or photos. For high-stakes applications like voting, where avoiding fraud is crucial to maintaining the integrity of the process, this extra protection is crucial.

4. **Data Privacy and Security Enhancements**:

More sophisticated data security features like data anonymization, end-to-end encryption, and privacy-preserving machine learning strategies like federated learning may be included in later iterations.

Sensitive voter data would be protected, ensuring compliance with privacy regulations and bolstering public confidence in the system's security.

Federated learning, for instance, minimizes data exposure by enabling the model to be trained and improved across multiple devices without transferring individual voter data to a central server.

CHAPTER 9
REFERENCES

REFERENCES

[1] Kak, Shakir & Mustafa Alfaqi, Firas & Valente, Pedro. (2018). A Review of Person Recognition Based on Face Model. 4. 157-168. 10.23918/eajse.v4i1sip157.

[2] Kumar, Mr & Walia, Ekta. (2011). ANALYSIS OF ELECTRONIC VOTING SYSTEM IN VARIOUS COUNTRIES. International Journal on Computer Science and Engineering. 3.

[3] Weldemariam, Komminist & Villafiorita, Adolfo & Mattioli, Andrea. (2009). Experiments and data analysis of electronic voting system. 105 - 112. 10.1109/CRISIS.2009.5411972.

[4] Eteng, Idongesit & umoren, paul. (2018). An Online Voting System for Colleges and Universities.

[5] Kortli, Yassin & Jridi, Maher & Falou, & Atri, Mohamed. (2020). Face Recognition Systems: A Survey. Sensors. 20. 342. 10.3390/s20020342.

[6] Kaur, Jashanpreet & Akanksha, & Singh, Harjeet. (2018). Face detection and Recognition: A review. 6th International Conference on Advancements in Engineering & Technology (ICAET-2018), ISBN No. 978-81-924893-3-9

[7] Alansari, Mohamad & Abdul Hay, Oussama & Javed, Sajid & Shoufan, Abdulhadi & Zweiri, Yahya & Werghi, Naoufel. (2023). GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations. IEEE Access. PP. 1-1. 10.1109/ACCESS.2023.3266068.

[8] Najam, Syed Shahram, Aamir Zeb Shaikh, and Shabbar Naqvi. ”A novel hybrid biometric electronic voting system: Integrating finger print and face recognition.” Mehran University Research Journal of Engineering & Technology 37, no. 1 (2018): 59-68.

[9] Choudhary, Nilam, Shikhar Agarwal, and Geerija Lavania. ”Smart voting system through facial recognition.” International Journal of Scientific Research in Computer Science and Engineering 7, no. 2 (2019): 7-10.

[10] Hopal, Pratik, Alkesh Kothar, Swamini Pimpale, Pratiksha More, and Jaydeep Patil. ”A Survey on Performing E-Voting through Facial Recog- nition.” (2021).

[11] Mu, Xiaohui & Li, Siying & Haipeng, Peng. (2020). A Review of Face Recognition Technology. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3011028.

[12] Remone, Roweida & Dash, Sushree. (2023). Face Recognition and Face Detection Benefits and Challenges Section A-Research paper 2561 Eur. European Chemical Bulletin. 12. 2561-2566. 10.31838/ecb/2023.12.si6.226.

[13] Eteng, Idongesit & umoren, paul. (2018). An Online Voting System for Colleges and Universities, publication/326059800 May 2018.

[14] Djanali, Supeno & Studiawan, Hudan & Nugraha, Danang & Pratomo, Baskoro. (2018). Vote identification and integrity of ballot in paper-based e-voting system. Electronic Government, an International Journal. 14. 1. 10.1504/EG.2018.10010865.

[15] Dhaher, F. A., & Kuban, K. H. (2020). J Journal of Education for Pure Science-University of Thi-Qar. https://doi.org/10.32792/utq.jceps.10.01.028

[16] A.Aravindhan, M.Kalaiyarasi, S.Bharanikumar, P.Dhanapal and R.Dharmaraj. “Smart Online Voting System Using Facial Recognition Based On IoT and Image Processing.”

APPENDICES

APPENDICES

A. Group photo with Project Guide Dr. Rahul Agrawal

B. Research Paper

2024 2nd International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS)

Comprehensive Study of Face Verification in Voting System

Himanshu R. Katrojwar
Department of Data Science,
IoT and Cyber Security
G H Raisoni College of Engineering
Nagpur-440016, India
himanshu.katrojwar.ds@ghrce.raisoni.net

Saloni Deshmukh
Department of Data Science,
IoT and Cyber Security
G H Raisoni College of Engineering
Nagpur-440016, India
saloni.deshmukh.ds@ghrce.raisoni.net

Aishwarya S. Parwekar
Department of Data Science,
IoT and Cyber Security
G H Raisoni College of Engineering
Nagpur-440016, India
aishwarya.parwekar.ds@ghrce.raisoni.net

Rahul Agrawal
Department of Data Science,
IoT and Cyber Security
G H Raisoni College of Engineering
Nagpur- 440016, India
rahul.agrawal@raisoni.net

Chetan Dhule
Department of Data Science,
IoT and Cyber Security
G H Raisoni College of Engineering
Nagpur- 440016, India
chetan.dhule@raisoni.net

Nekita Chavan Morris
Department of Data Science,
IoT and Cyber Security
G H Raisoni College of Engineering
Nagpur-440016, India
nekita.chavan@raisoni.net

***Abstract*—The study assesses the effectiveness of face verification techniques in verifying the identity of voters, aiming to prevent fraudulent activities during elections. Researchers analyze the benefits of incorporating face verification systems, such as improving voter authentication to ensure each voteis cast by the rightful individual, with the system achieving an accuracy of 98% and a validity of 90%. The paper also discusses the challenges and limitations faced in integrating face verification technology into the voting system, providinginsights into overcoming these obstacles. Through a detailed investigation, the research aims to offer valuable informationto policymakers and election officials on the feasibility and potential impact of adopting face verification in voting systems. The study also highlights how crucial it is to protect voter privacy and data security while putting face verification techniques in place to protect sensitive data and preserve the integrity of the election process. All things considered, the study offers a thorough examination of how face verification technology might improve the legitimacy, dependability, and overall effectivenessof the voting process.**

Keywords - Face Verification, CNN, Voting System, Electoral Integrity, Proxy Voting, Multiple Voting

I. Introduction

Voting is a basic fundamental right and an essential component of civic participation in democracies. However, with the introduction of new technology and sophisticated types of electoral fraud, maintaining the security and integrity of the voting process has grown more difficult. Electoral integrity, which ensures free, fair, and transparent elections, is a crucial aspect of democratic governance. However, problems like as voting fraud, proxy voting, repeated voting, and voter impersonation threaten the integrity of elections everywhere.

Proxy voting, in which a legitimate voter casts a ballot on behalf of another voter who is unable to do so in person for a variety of reasons, including illness, impairment, or absence from the voting jurisdiction, is one area of concern [1]. Several incidents of bogus voting were reported in many Indian states during the general Lok Sabha elections of 2024 [2] [3] [4].

Malpractices like proxy voting, multiple voting, fake voter IDs, booth capturing, voter impersonation, technological manipulation, and voter intimidation, severely undermining the integrity of elections. Conventional voter verification techniques, which mostly rely on physical identification and manual inspections, are frequently insufficient to fully address these problems. For solving the problem there is a need for modern technology like face recognition.

In the 2019 Telangana municipal elections, the Indian state tested facial recognition technology as a means of authenticating voters. Estonia has investigated face recognition for safe online voting. Estonia is well-known for its e-governance projects. A few US states have also looked into using facial recognition technology during elections.

In order to prevent proxy and multiple voting, this research paper investigates the use of face recognition technology in the voting process. This article will look at the technology's accuracy, implementation challenges, and possible consequences on voting integrity.

II. Literature Survey

B Singh, et.al.[5] proposed an International Direct Digital Election method using Android smartphones for voting and voter verification through face recognition proposed in previous research. They used techniques like face recognition, Aadhar number verification OTP verification with mobile numbers. Fatimah Dhaher, et.al.[6] proposed Face and fin-fingerprint identification through automated methods for voter authentication. They used DNN recognition for face mat-

978-8-3315-2935-2/24/$31.00 ©2024 IEEE

C. Research Papers Status

raisoni EDUCATION

HIMANSHU KATROJWAR <himanshu.katrojwar.ds@ghrce.raisoni.net>

Acceptance Notification ICETEMS 2024

4 messages

Microsoft CMT <email@msr-cmt.org> Tue, Sep 17, 2024 at 4:12 PM
Reply-To: Yogita Dubey <yogeetakdubey@yahoo.co.in>
To: Himanshu Ravindra Katrojwar <himanshu.katrojwar.ds@ghrce.raisoni.net>

Dear Himanshu Ravindra Katrojwar

Paper ID / Submission ID : 71

Title : Comprehensive Study of Face Verification in Voting System

Greeting from 2nd ICETEMS 2024.

We are pleased to inform you that your paper has been accepted for the Oral Presentation as a full paper for International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS 2024), Nagpur, India scheduled from 22 November 2024 to 23 November 2024.

All accepted and presented papers will be submitted to IEEE Xplore for the further publication.

Note:
All of Accepted and Presented Papers of 1st ICETEMS conference has been Published by IEEE Xplore and indexed by Scopus
https://ieeexplore.ieee.org/xpl/conhome/10093235/proceeding

Complete the Registration Process before 20 September 2024 for Early Bird Registration.

The registration details are available at
https://ycce.edu/icetems/registration.php
Fill the google form https://forms.gle/foK4mcT74LPDPoZMA after registration.
Further steps like IEEE PDF express and E copyright will be given later once registration is over.

Note :
1. Any changes with the Author name, Affiliation and content of paper except for review comments will not be allowed after acceptance.
2.This is Hybrid Conference, both online and physical presentation mode is available.

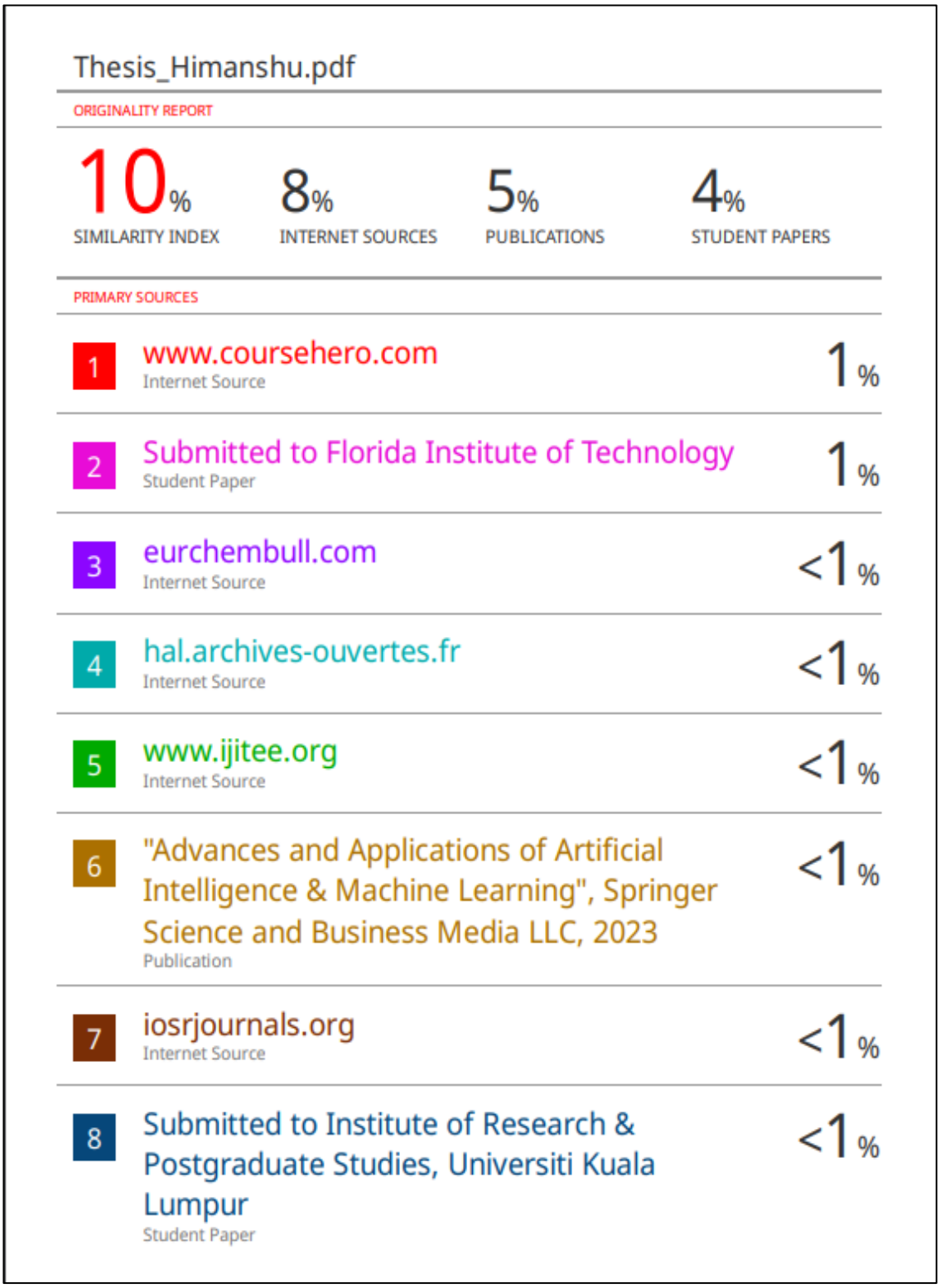
Chair, TPC
yogeetakdubey@yahoo.co.in
ICETEMS 2024

To stop receiving conference emails, you can check the 'Do not send me conference email' box from your User Profile.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

D. Plagiarism Report



Thesis_Himanshu.pdf

ORIGINALITY REPORT

10%	8%	5%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.coursehero.com Internet Source	1%
2	Submitted to Florida Institute of Technology Student Paper	1%
3	eurchembull.com Internet Source	<1%
4	hal.archives-ouvertes.fr Internet Source	<1%
5	www.ijitee.org Internet Source	<1%
6	"Advances and Applications of Artificial Intelligence & Machine Learning", Springer Science and Business Media LLC, 2023 Publication	<1%
7	iosrjournals.org Internet Source	<1%
8	Submitted to Institute of Research & Postgraduate Studies, Universiti Kuala Lumpur Student Paper	<1%