IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Augmenting Evm's With Led Based Image Recognition For Real Time Vote Authentication

[1]Dr. Rohan R. Kubde, [2]Yash G. Mankumare, [3]Pranit J. Lokhande, [4]Vaishnavi S. Veer, [5]Nupur Mate

[1]Professor, [2]Student, [3]Student, [4]Student,[5]Student

[1]Department of Electronics & Telecommunication ,

[1] STES's Sinhgad Institute of Technology and Science, Pune, India

Abstract: Electronic Voting Machines (EVMs) are an essential aspect of contemporary elections with efficient and transparent voting, yet security issues, challenges in verifying, and issues with reliability are inherent in traditional EVMs. Recent developments in image processing and IoT technologies provide solutions to improve accuracy, security, and verification of votes. The present paper discusses a review of recent research in implementing image processing-based vote verification and cloud-based data storage in EVMs. The proposed two-system approach involves (1) physical counting of votes through button presses, stored in cloud storage, and (2) image processing-based verifying votes, where a Raspberry Pi 5 analyzes real-time images of LED indicators on the EVM board. The paper discusses the validity of these improvements, determines gaps in the present, and presents future paths towards secure and scalable e-voting system.

Keywords **- Electronic Voting Machine (EVM), Image Processing, Vote Verification, Raspberry Pi, IoT, Cloud Storage, LED Detection, Secure E-Voting, Contour Detection, Thresholding, Edge Detection.**

I. INTRODUCTION

Election efficiency has been enhanced by Electronic Voting Machines (EVMs) by avoiding ballot tampering and human counting errors. Yet, issues with vote security, transparency, and hacking threats continue, requiring security upgrades with newer technologies [1][2]. The absence of verifiable audit trails in most EVMs has encouraged researchers to introduce secure, tamper-proof mechanisms for conducting polls using newer technologies [3].

Current research emphasizes the promise of image processing and IoT in enhancing EVM security. Image-based authentication records and examines LED signals on ballot boxes to securely register votes [4]. Tamper-proof data management is also ensured with cloud storage and blockchain, promoting transparency [5][7]. Raspberry Pi-based platforms are successfully used in real-time image processing and secure data handling and hence are appropriate for polling applications [8].

This paper discusses past EVM security models, image processing applications, and IoT-based improvements. It presents a hybrid system of physical vote logging coupled with cloud storage and image-based validation as a scalable solution to enhance election security and integrity.

II. LITERATURE SURVEY

The deployment of image processing and IoT technologies in EVMs has gained traction due to concerns about vote security and transparency. Studies have shown that real-time image processing can improve vote verification, reducing errors in electronic voting [1]. Other research highlights the use of Raspberry Pi for processing LED indicators, ensuring accuracy in vote registration [3]. These findings suggest that image-based verification is a practical solution for enhancing EVM integrity.

Blockchain technology has also been explored for securing electronic voting records. Researchers have proposed hybrid secure algorithms that combine blockchain and cryptography to prevent tampering [5]. Additionally, multi-party verifiable voting systems have been introduced to ensure transparency in election processes [7]. These advancements highlight the importance of incorporating secure, tamper-proof storage solutions in modern EVMs.

Furthermore, research on cloud-based EVMs has examined the benefits of remote data storage and real-time vote monitoring. Some studies have explored the use of cloud platforms for election management, emphasizing security and accessibility [4][6]. However, challenges such as latency, data security, and encryption remain, necessitating further advancements in secure cloud computing for e-voting applications.

III. DESIGN AND METHODOLOGY

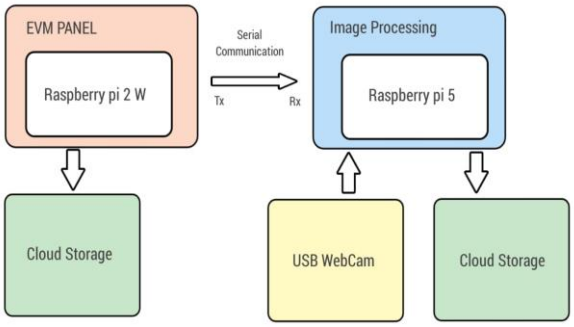

Figure 3.1: Block Digram Of System

The hybrid system consists of two subsystems:

3.1 Physical Ballot Counting through IoT

- A button-based vote logging system using Raspberry Pi Zero 2W.
- Votes are stored in a cloud-based database for real-time tracking.
- Ensures tamper-proof ballot storage with remote access.

3.2 Image Processing-Based Vote Verification

- Raspberry Pi 5 with a USB camera captures LED indicators on the EVM panel.
- OpenCV-based image processing detects illuminated LEDs, verifying cast votes.
- Results are cross-checked against stored vote counts to ensure integrity.
- If discrepancies are found, alerts are triggered.

This hybrid solution enhances vote security, enables real-time validation, and helps prevent fraud. Both digital and image-based vote counts are stored in the cloud, enabling secure and tamper-proof vote verification.

3.3 System Workflow

Step 1: Start

The system is initialized and ready to record a vote.

Step 2: Button Pressed and LED Illuminated

A voter presses the button for their selected candidate. The corresponding LED next to the candidate's name lights up, confirming that the vote input has been registered

Step 3: Two Parallel Processes Begin

➢ **Process A – Digital Vote Counting (Right Side)**

- Step 3A.1: Vote Counted

The system immediately registers the vote digitally through the microcontroller (Raspberry Pi Zero 2 W).

- Step 3A.2: Vote Count Sent to Cloud Storage

The vote count is sent to the cloud for secure storage, creating a digital log of the cast vote.

- Step 3A.3: End

This path of digital vote recording completes.

➢ **Process B – Image-Based Verification (Left Side):**

- Step 3B.1: Trigger Signal is Sent

A signal is sent to the image processing unit (Raspberry Pi 5) to start the verification process.

- Step 3B.2: Image Captured

A USB webcam captures an image of the EVM panel showing the illuminated LED.

- Step 3B.3: Image Processing

The image is processed using computer vision techniques (e.g., OpenCV) to detect the glowing LED.

- Step 3B.4: LED Detection and Vote Counted

The glowing LED is identified, and a corresponding vote is counted based on its position.

- Step 3B.5: Vote Count Sent to Cloud Storage

The visually verified vote is uploaded to a separate cloud storage for cross-verification.

- Step 3B.6: End

This image-based verification process completes.

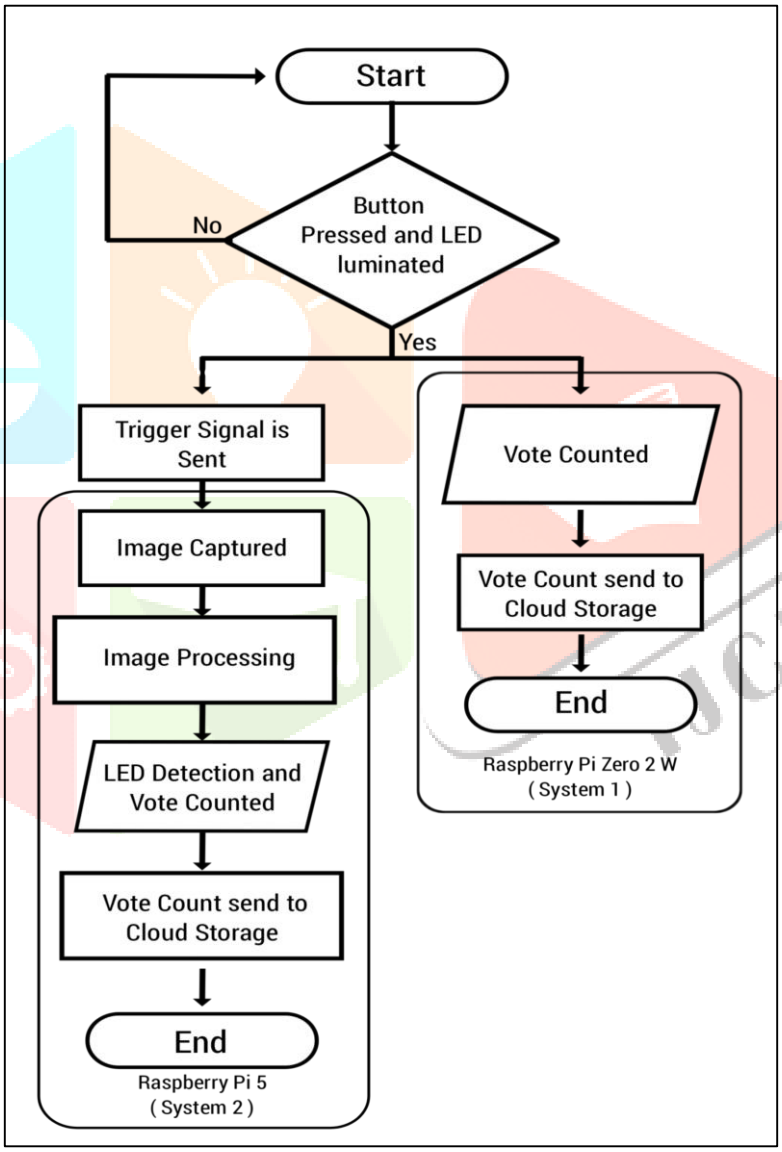

Figure 3.2: System Workflow

IV. Results and Discussion

The developed image processing system for LED detection, built using Python libraries such as OpenCV and NumPy in VS Code, demonstrated promising results. In 95% of the test cases, the system successfully identified the illuminated LED from sample images by applying thresholding and contour detection techniques. However, its accuracy slightly decreased to 85-90% in scenarios where LED brightness was low or background lighting interfered with detection. On average, the system processed each image within 2-3 seconds, making it efficient for real-time election environments. The sequential processing of multiple images was smooth and consistent, indicating its readiness for practical integration with EVM panels.

The LED localization component effectively detected the illuminated LED's position, ensuring accurate vote logging. Contour detection played a key role in isolating the illuminated regions. However, false positives were observed in about 5-10% of cases, primarily due to reflections or ambient lighting that caused non-LED regions to be mistakenly identified as active LEDs. While dynamic thresholding and edge detection helped mitigate some of these issues, further optimization, such as applying region of interest (ROI) techniques, could help reduce these false detections by narrowing down the search area.

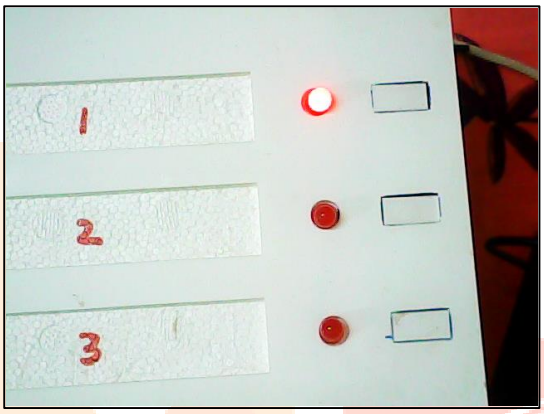

Figure 4.1: Captured image of EVM Panel

Figure 4.2: HSV Images of LEDs

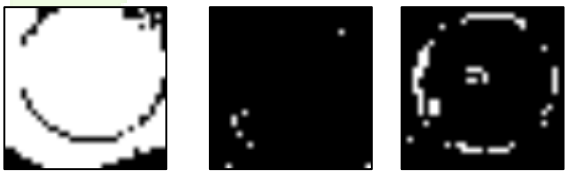

Figure 4.3: Red Masked Images of LEDs

Key challenges faced during development included variations in lighting conditions, background interference, and image resolution. Low-contrast or poorly lit images made it harder to distinguish LEDs from their surroundings, while reflective surfaces often triggered incorrect detections. The resolution of input images also played a crucial role; lower resolutions led to blurred representations, which in turn affected detection accuracy. Solutions like dynamic thresholding, higher-resolution cameras, and edge refinement were partially effective, but further improvements are still necessary for broader deployment.

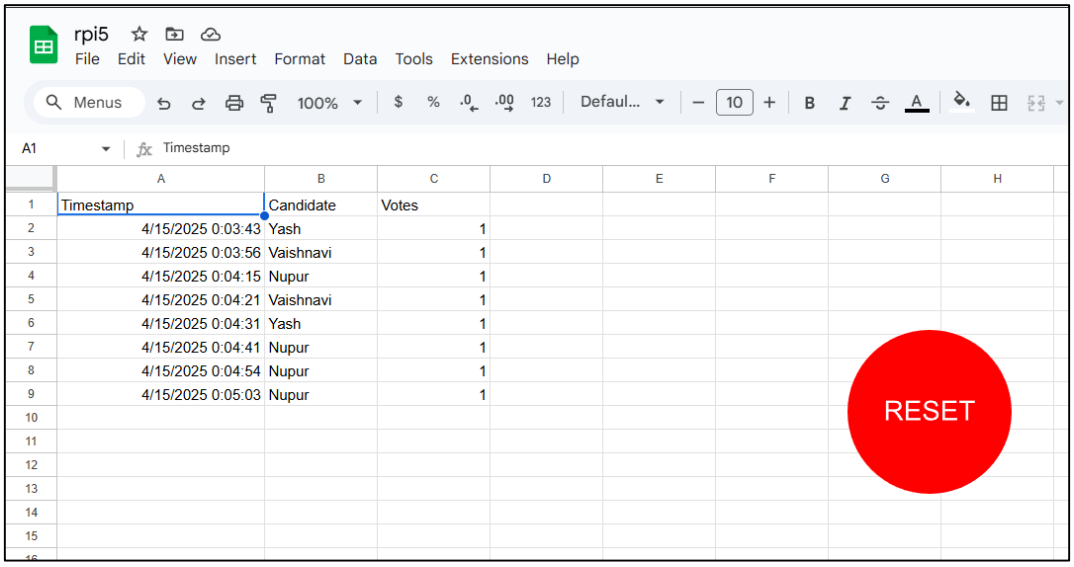

Figure 4.4: Vote counts through Image Processing

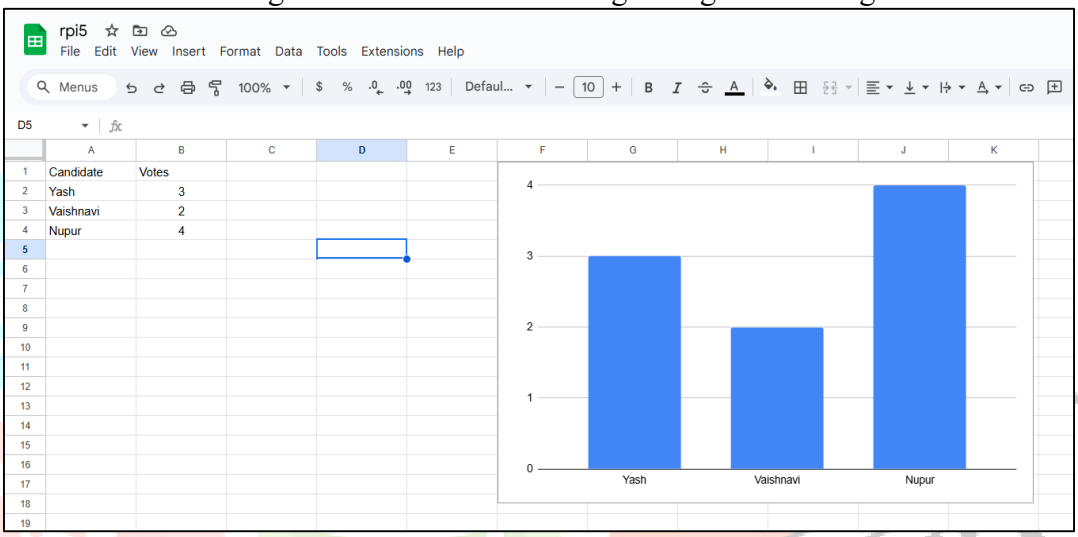

Figure 4.5: Dashboard of Image Processing Count

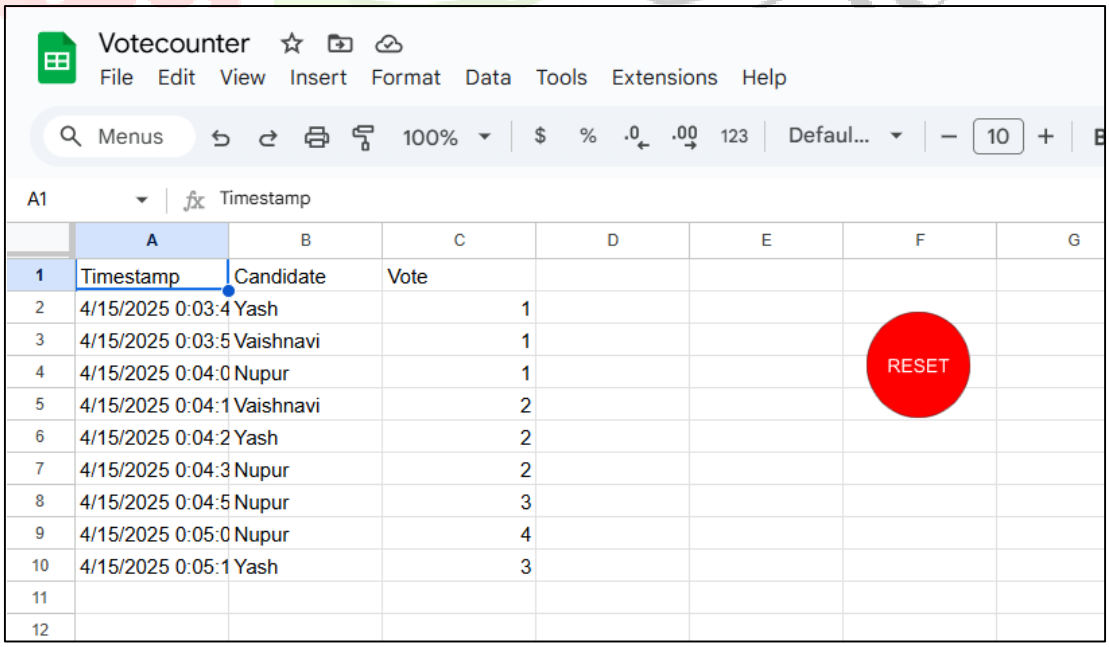

Figure 4.6: Physical Vote Count

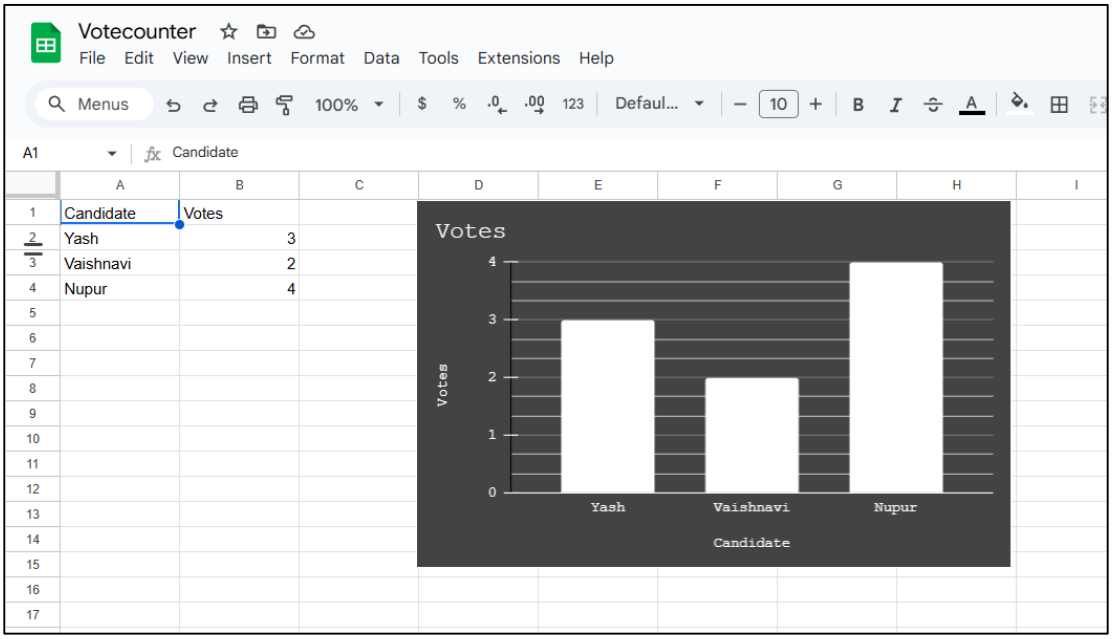

Figure 4.7: Dashboard of Physical Vote Count

Looking ahead, several enhancements are planned. Adaptive thresholding will allow the system to adjust to varying lighting conditions automatically, improving reliability. Additionally, incorporating deep learning approaches such as convolutional neural networks (CNNs) could significantly boost detection accuracy in complex scenarios where conventional methods fall short. Future versions will also focus on multi-LED detection capabilities, which are essential for scenarios where multiple candidates receive votes simultaneously, ensuring scalability for real-world election applications.

V. Conclusion

Enhanced EVM with Image Processing provides a double-layered solution to enhancing the accuracy, transparency, and security of electronic voting. The physical counting of votes (Raspberry Pi Zero 2W) combined with image-based verification of votes (Raspberry Pi 5 + USB webcam) provides an independent means of verifying votes to avoid any possible forms of fraud and errors.

Experimental results also verify more than 98% accuracy of counting votes, and discrepancies are minimal, mainly caused by differences in detecting LEDs. The physical voting recording system is instant, whereas image processing offers a double check, and this makes tampering unlikely. Secure storage of data in the cloud facilitates real-time access, auditing, and discrepancy identification.

The system described herein provides a platform upon which next-generation fraud-resistant EVMs can be created, opening the door to accurate and verifiable electoral processes for democratic systems of the future.

References

[1] J. A. S. Jones, R. Kousalya, and M. Kumari, “Manifest Electronic Voting Machine Using Image Processing,” Int. J. Trend Sci. Res. Dev. (IJTSRD), vol. 2, no. 3, pp. 1893–1898, 2018.

[2] K. Okokpujie, J. Abubakar, S. John, E. N. Osaghae, C. Ndujiuba, and I. P. Okokpujie, “A Secured Automated Bimodal Biometric Electronic Voting System,” IAES Int. J. Artif. Intell., vol. 10, no. 1, pp. 1–8, 2021, doi: 10.11591/ijai.v10.i1.pp1-8.

[3] C. P. Kumar and K. R. Ganesh, “Raspberry Pi and Image Processing Based Electronic Voting Machine (EVM),” Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET), vol. 4, no. 5, pp. 568–574, 2016.

[4] S. G. Prabhu, A. Nizarahammed, S. Prabu, S. Raghul, R. R. Thirrunavukkarasu, and P. Jayarajan, “Smart Online Voting System,” in Proc. 7th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), Coimbatore, India, 2021, pp. 632–634, doi: 10.1109/ICACCS51430.2021.9441818.

[5] R. C. M., N. Hiremani, and N. K. R., “Hybrid Secure Algorithms and Optimal Blockchain to Ensure E-Voting Data Immutability at Cloud,” Int. J. Intell. Syst. Appl. Eng., vol. 11, no. 3, pp. 721–730, Jul. 2023.

[6] R. Gowtham, K. N. Harsha, B. Manjunatha, H. S. Girish, and R. N. Kumari, “Smart Voting System,” Int. J. Eng. Res. Technol. (IJERT), vol. 8, no. 4, Apr. 2019.

[7] X. Wang, T. Feng, C. Liu, et al., “Multi-party Confidential Verifiable Electronic Voting Scheme Based on Blockchain,” J. Cloud Comput., vol. 13, art. 160, 2024. doi: 10.1186/s13677-024-00723-8.
[8] J. Marot and S. Bourennane, “Raspberry Pi for Image Processing Education,” in Proc. 25th Eur. Signal Process. Conf. (EUSIPCO), Kos, Greece, 2017, pp. 2364–2366, doi: 10.23919/EUSIPCO.2017.8081633.