International Journal of Computational Science and Engineering Research
ISSN: 3107 -8605 (Online) , http://www.ijcser.com/
Regular Issue , Vol.1, Issue. 3 (July – September) , 2024 , Pages: 57 - 62
Received **:** 30 April 2024 ; *Accepted* **:** 10 June 2024 ; *Published* **:** 17 September 2024
https://doi.org/10.63328/IJCSER-V1RI3P12
Original Paper : Applied Research – Compare and Contrast Research Paper

Design and verification of voting machine with Cross voter detection User Verilog

K Sai Venu Prathap [1]*, **R Prashanth** [2] , **M Prudvi Teja Reddy** [3] ,
P Narasimha [4] , **V. Naveen** [5]

[1-5] Department of Electronics and Communication Engineering , Aditya College of Engineering , Madanapalle ,India

* *Corresponding Author : K Sai Venu Prathap ; venuprathap9459@gmail.com*

Abstract: This article presents an efficient Verilog-based secure voting machine with cross-voter detection, ensuring election integrity. Designed for multiple candidates and voters, it prevents unauthorized votes through voter ID system. The Verilog module, using flip-flop, stores candidate votes and IDs, implementing cross-voter detection to maintain fairness. Parameterized for scalability, the module supports a configurable number of candidates and voters, featuring a reset option. Optimizing hardware resources, the design prioritizes efficiency and minimizes voting process latency. The Verilog code forms a foundation for a secure, scalable system adaptable to specify requirements, allowing for additional security measures. Rigorous simulation and testing validate its robustness before real-world deployment, advancing digital voting systems in efficiency, and adaptability. Simultaneously the module unit is used to check the cross voter and if it finds any cross-voter face those will be removed and respective votes will treat as invalid votes. Those invalid votes will remove from genuine votes. One critical aspect is the detection of cross-voter interface, where votes are unintentionally or maliciously attributed to the wrong candidate. Verilog, a hardware description language, offers a robust platform for designing and verifying digital circuits. This abstract presents a verification methodology for detecting cross-voter interference in electronic voting systems using verilog.

Keywords: Mobilities , Voting , Design of Voting Machine**.**

1. Introduction

A voting System is a critical component in democratic processes, ensuring fair and accurate elections. It allows citizensto cast their vote for their preferred candidates or issues. No one can deny that the integrity of our electoral system is essential to the integrity of our democracy. Previously, decisions were made using ballot frames, and people voted for their favorite challenger by simply stamping their name. To avoid this absurd outcome, we use a voting method. Voting systems are now being migrated to Electronic Voting Machines (EVMs) as they are reusable. This reduces election-related costs and facilitates large-scale election operations. Planning to use EVM with removable memory cards was tight. Accessing the memory card, even for a fraction of a second, turns the votes into completely different malicious code. In this project we gone the working of the voting machine and its basic functionalities, initially use FSM to designed the system which is used for fast response to the input provided and also easy to design project.

The primarily utilizes Verilog, a hardware description language (HDL), for designing and implementing the digital voting machine. Once designed we use the simulation tools like vivado software to design the system and also to verify functionalities on the other hand, it has a number of security weaknesses and is more vulnerable than the old approach. More authentication, confidentiality, and voter privacy, among other things, which are required by the security system. So, we need a framework that might be a better method for executing electronic voting machine.

Verilog, a hardware description language, offers a potent toolset for verifying the functionality and security of voting machines. By leveraging Verilog, we can meticulously design and test intricate algorithms aims at fortifying the verilog process against unauthorized manipulation. One critical aspect of ensuring the sancity of elections is the detected of cross-voter interference, where an individual attempts to cast multiple votes or tamper within the votes others. This article aims to develop a Design of a Cross Voting Proof System Based on Python and Verilog Implemented on FPGA along with IP cameras. This proposed work emphasizes the development voting system. This voting system is integrated with an IP camera to capture the real- time visualization of the voters and compares the voter images with could and find out whether any person again appeared for voting one more time. Moreover, the voting machine module provides a better voting mechanism such that no one can do cross voting for a short duration in addition to that whenever a vote cast a series of Led will glow along with a beep sound.

The rest of this article is organized as follows: Section II presents the literature review, Section III presents the system architecture of the proposed system, Section IV discusses the results, and Section V and VI present the conclusion and. future directions, respectively.

2. Materials and Methods

Several existing works have been studied to identify the gaps in the respective approaches. Some of the most relevant state-of-the-art voting machine approaches are discussed here.

In [1] Authors stated that Biometric Electronic Voting Machine Using Fingerprint Sensor and Arduino in which consists 3 stages in the first stage number of voters and candidates will be decided, in the second stage voting process will begin and the voter can cast his/her vote for their respective candidate in the respective register whereas in the last stage votes will be compared and decide the winner of that election and they described that it can be implemented on FPGA.

In [2] Authors described a voting machine based on the Electronic Voting Mechanism using Microcontroller Atmega328P with face recognition in which a voter needs to enroll his/her fingerprint in the main system when the voter needs to cast the vote fingerprint must be enrolled. Enrolled members only are allowed to cast their vote via IR Sensor Button which represents the candidate.

In [3] Authors described the Radiofrequency based electronic voting machine such that they are using RFID tags to cast their votes and they are using facial recognition before casting his/her vote.

In [4] Authors proposed a voting system FPGA Based Real-Time Face Authorization System for Electronic Voting System that before casting a vote voter need to verify his/her identity if the identity is valid then the allowed for casting the vote and the voting system consists of Arduino a microcontroller and push buttons for representing the candidates with help of the ESP Wi-Fi module data sent to be things peak server and as well as votes will be displayed at LCD screen.

In [5] authors described a voting system with the integration of fingerprint ID and Facial recognition. If the voter's fingerprint id and facial id match then he is allowed for casting the vote. In this model raspberry pi is used as the main controller along with push buttons which represent the candidates and an LCD screen is used for displaying the vote’s purpose.

The system employs parallel processing techniques and modules like NI MyRIO FPGA demonstrating a combination of hardware and software for enhances performance while the system aims to address delays, real-time address performance may still be influenced by factors such as the complexity of face recognition algorithms. The potential for tampering and the need for continuous evolving cybersecurity threats. The techniques demonstrates high-speed processing and low computational.

In [6] Authors illustrated a voting system based on A MATLAB based face recognition system using image processing and neutral network. Authors designed a system in such a way that camera captures voter image it checks in its could whether it is matched then FPGA authorized those votes if face id doesn’t match security door won’t open.

In [8] Authors describe a voting system using Verilog and FPGA which works in two major units: Control Unit and Ballot Unit. The control unit counts the individual party results as well as the total vote counts. The ballot unit makes a beep sound and gives a green signal when a cast vote is accepted. It will also give out a punched paper for the appropriate party. If any error occurs, the ballot unit will give a red signal indication.

In [9] Authors described the same voting system which are represented in [5] but they enabled online voting option to the voters.

In [11] Authors discussed a finger print-based authentication and face recognition-based data exchange are used to address security concerns in electronic voting machines.

3. System Architecture

The architecture of the proposed system represents in Figure 1. The system architecture typically consists of input interfaces, processing logic, and output mechanisms. Input interfaces are responsible for receiving votes from voters through various channels, such as physical buttons, touchscreens, or electronic voting machines. These interfaces translate voter inputs into digital signals that can be processed by the system. The processing logic encompasses the core functionality of the voting system, including vote tallying, conflict resolution, and result generation. This logic is implemented in Verilog and defines how votes are processed, aggregated, and interpreted to determine the final outcome of the election. Additionally, the system architecture may incorporate security mechanisms, such as encryption, authentication, and tamper detection, to safeguard the integrity and confidentiality of the voting process. Output mechanisms are responsible for presenting voting results to stakeholders, including election officials, political parties, and the general public. These mechanisms may include display interfaces, printouts, or digital reports generated by the system. Overall, a well-designed system architecture forms the foundation for developing a Verilog-based voting system that is secure, reliable, and compliant with regulatory requirements. Through rigorous verification and testing, the integrity and accuracy of the system can be ensured, fostering trust and confidence in democratic processes. In addition to the core components of the system architecture, the Verilog-based voting system may incorporate additional features and functionalities to enhance its performance, usability, and security. These features could include voter authentication mechanisms to verify the identity of voters before allowing them to cast their votes, thereby preventing unauthorized access and ensuring the integrity of the electoral process.

Ref	Title	Main Components	Hardware implementation	Security	Language	Limitations
1	Biometric Electronic Voting Machine UsingFingerprint Sensor and Arduino	Arduino Fingerprint sensor IR sensor	Yes	Low	C	Malfunction can be done easily while using IR sensors
2	Electronic Voting Mechanism using Microcontroller Atmega328P with face Recognition	Microcontroller Atmega328P Camera	Yes	High	C	Malfunction can be done easily while using IR sensors
3	FPGA Based Real-time Face Authorization System for Electronic voting system	LabView	-	Medium	Not discussed	Require huge database for facial recognition
4	Xilinx Based Electronic Voting Machine	Arduino	Yes	Low	C, Python	Malfunction can be done easily Through separate push buttons
5	Implementation of authenticated and secure online voting system	Raspberry pi,Pi camera	Yes	High	Python	The system emphasizes non-traceability, ensuring the complete anonymity of votes
6	A MATLAB based face recognition system using image processing and neural networks	LabVIEW	-	Medium	Not discussed	Require huge database for facial recognition
8	Proficient FPGA Execution of Secured and Apparent Electronic Voting Machine Using Verilog HDL	Altera DE1	Yes	Medium	HDL	More Complex
9	Interfacing of Online and Offline Voting Systemwith an E-Voting Website	Raspberry pi,Pi camera	Yes	Medium	Python	Malfunction can be done easily Through separate push buttons
10	Design and verification of voting machine with cross voter detection using verilog	Xilinx Vivado	Yes	High	Verilog	Only 3 on board push buttons

4. Proposed Work

4.1. Design and Architecture

The voting machine's design prioritizes modularity, scalability, and efficiency. A modular design facilitates easy updates without disrupting the system. Scalability ensures it can handle various election sizes.

Input Processing: Input modules validate and sanitize voter data, ensuring its accuracy. Error checks and voter eligibility verifications are also crucial.

Vote counting and winner Determination: Vote counting modules update in real-time and employ efficient algorithms. winner determination logic ensures fairness.

Output generation and reporting: The system compiles results into understandable formats for stakeholders. Visualizations may enhance data presentation.

Testing and Validating: Various tests assess the system's correctness, robustness, and security. These include unit, integration, and security testing.

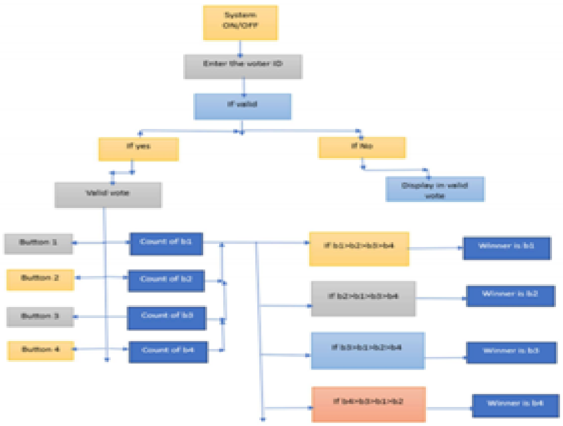


Figure.1 Block Diagram

4.2. Future Enhancement and Consideration

The design anticipates future technologies like biometric Authentication, blockchain based voting and verifiable voting protocols. The aim is to state at the art of electronic voting system which has the highest standards of reliability, security, transparency. this project is based on the reliability, security, and integrity of EVMs in design and verification methodologies. Testbenches and test cases are developed to validate the behaviour of Verilog module under various scenarios, including normal operation, edge cases and potential attack vectors. This project is based on the advancement of electronic voting machine technology by demonstrating a systematic approach design and verification using Verilog. The aim is to enhancement the trust, transparency, and confidence in electoral process. Accessibility, usability, and compliance are also prioritized.

4.3. New Proposed Method:

The systematic approach aimed at ensuring functionality, security and reliability of the system. The methodology includes Requirement analysis, Design specification, Verilog implementation, Verification planning, Testbench development, and Simulation and Testing.

4.4. Advantages

The Verilog for a voting machine, there are some advantages using this system.

Efficiency and Accuracy: Faster vote processing and reduced human errors. Each vote is recorded electronically, eliminating the risk of interruption with manual tabulation.

Security: Protection against tampering and fraud, with features for accessibility.

Scalability: Adaptable to elections of various sizes.

Data Analysis: Offers insights into voter behavior and trends.

Cost Savings: Reduces manual labour and paper usage.

4.5. Applications

Elections: For local to international government elections.

Corporate Governance: Shareholder voting and board elections.

Nonprofit Organisations: Student elections and organizational votes.

Community and Civic Organisations: Union elections and collective bargaining votes.

This comprehensive approach aims to develop a reliable electronic voting system, enhancing trust and transparency in democracy.

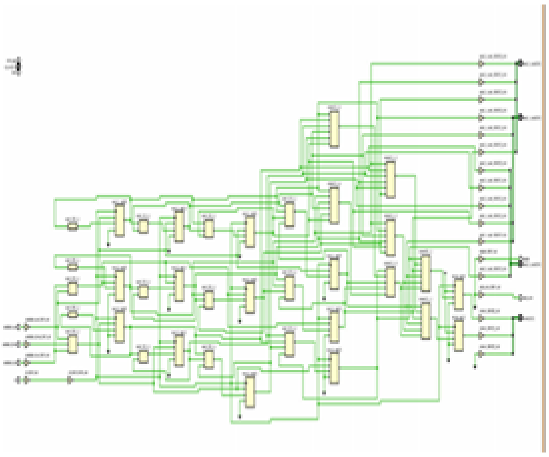


Figure. 2 Internal block level representation

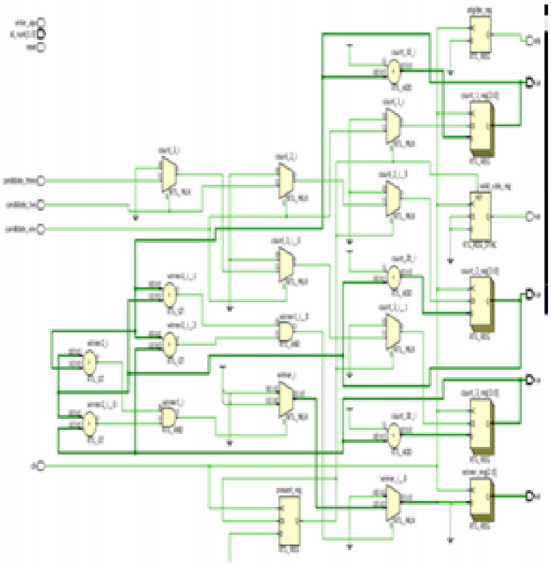


Figure. 3 Block level of synthesis design

5. Result and Discussion

Functional Prototype Development

The project successfully developed a functional prototype of the Verilog based voting system. This prototype validates the feasibility of using hardware solutions to facilitate voting processes.

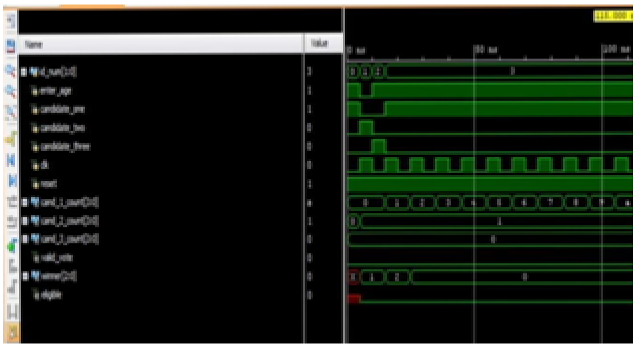


Figure. 4 Simulation Waveform Analysis

The circuit described has several inputs and outputs: id num, enter age, candidate one, candidate two, candidate three, clk, and reset, alongside outputs cand_1_count, cand_2_count, cand_3_count, valid vote, winner, and eligible.

For candidate Zero: In this scenario, a voter with an ID of 00 votes for candidate one and their age is 21. After 5time units, the vote is successfully registered, resulting in cand_1_count being incremented to 1, indicating one vote for candidate one. Meanwhile, cand_2_count and cand_3_count remain at 0. The valid vote output stays 0 as the vote is deemed valid. The winner output is expected to be candidate_1, based on the incremented vote count. Lastly, eligible is set to 1 since the voter's age exceeds 20.

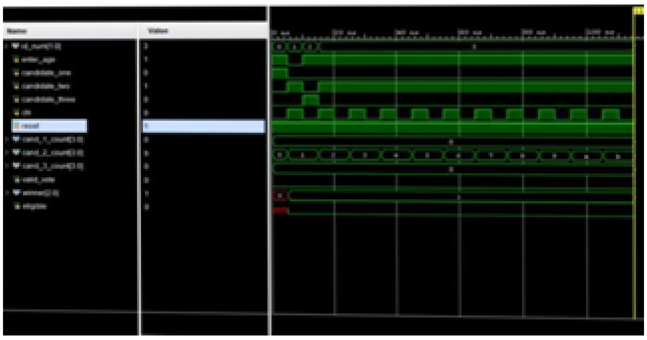
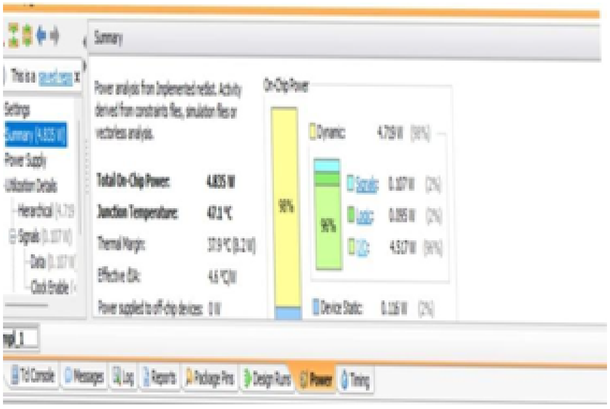


Figure. 5 Similar Outputs

In the second scenario, a voter with the ID 01 casts their vote in favor of candidate two, while their age is confirmed to be 22, meeting the age requirement of being above 20. Five time units later, the system successfully records the vote, leading to an increment in the vote count for candidate two. Consequently, cand_2_count will display 1, reflecting one vote received by candidate two.

In this third scenario, a voter with the ID 10 selects candidate three as their preferred choice, with their age being 25, satisfying the age requirement of being above 20. Five time units later, the system successfully records the vote, resulting in an increase in the vote count for candidate three. Consequently, cand_3_count will display 1, indicating one vote in favor of candidate three.



Power analysis from Implemented netlist. Activity derived from constraints files, simulation files or vectorless analysis.

Total On-Chip Power: 4.835 W
Junction Temperature: 47.1 °C
Thermal Margin: 37.9 °C (8.2 W)
Effective ϑJA: 4.6 °C/W
Power supplied to off-chip devices: 0 W

Dynamic: 4.709 W (98%)
Signals: 0.107 W (2%)
Logic: 0.095 W (2%)
I/O: 4.507 W (96%)
Device Static: 0.126 W (2%)

The waveform illustrates transitions over time, capturing the system's behaviour as it processes votes. Cross-voter detection might trigger an output change upon detecting multiple votes from one voter.

Table.1 Theoretical output comparison

Parameters	Original EVS	EVS using in Verilog
System clock speed	50MHz	100MHz
Efficiency	148.6%	206.48%
Power consumption	6.583%	4.583w

Table.2 Calculation

Max Theoretical Throughput	Actual Throughput	Efficiency
28,350,000 votes/sec	100,000,000 votes/sec	206.48%

6. Conclusion

The paper aims to create a digital voting machine using a programming language called Verilog. The expected outcomes include a clear and functional code that makes the voting machine work properly. We want to see the voting process, count the votes for each candidate, and make sure that no one can vote more than once. To check if our voting machine works correctly, we will run tests on a computer using simulated data. If we decide to use an vivado, we want the voting machine to work on a real physical device too. We also want the voting machine to be flexible, allowing us to easily change the number of candidates and voters. The goal is to make the voting machine efficient, using computer resources wisely and responding quickly.

References

[1] Smith, T.F., Waterman, M.S.: Identification of Common Molecular Subsequences. J. Mol. Biol. 147, 195–197 (1981) .

[2] Ehrlich, H.C., Steinke, T.: ZIB Structure Prediction Pipeline: Composing a Complex Biological Workflow through Web Services. In: Nagel, W.E., Walter, W.V., Lehner, W. (eds.) Euro-Par 2006. LNCS, vol. 4128, pp. 1148–1158. Springer, Heidelberg.

[3] Czajkowski, K., Fitzgerald, S., Foster, I., Kesselman, C.: Grid Information Services for Distributed Resource Sharing. In: 10th IEEE International Symposium on High Performance Distributed Computing, pp. 181–184. IEEE Press, New York.

[4] A.D.Rubin. Security considerations for remote electronic voting. Communications of the ACM, 45(12): 39-44, Dec.

[5] Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, and Tadayoshi kohno Analysis of an Electronic Voting System, in IEEE.

[6] Voting: What Is; What Could Be, July 2001. Available: http: //www. vote. Caltech. edu/Reports/.

[7] Voting, "Gujarat online voting model system". Available: http: //sec. Gujarat. gov. in/e-voting-system. Htm

[8] S. Tikoo and N. Malik, "Detection of face using Viola Jones and recognition using back propagation neural network", 2017.

[9] K.S. Kumar, V.B. Semwal and R.C. Tripathi, “Real time face recognition using AdaBoost improved fast PCA algorithm”.