# A Hash Algorithm based Approach for Verifiability and Detection of EVM Tampering

Bhople Yogesh Jagannath
Department of Information Technology,
Government Polytechnic Washim, India

## ABSTRACT
A comprehensive and efficient hash algorithm-based approach is proposed to detectthe tampering of Electronic Voting machines (EVM). There are two cases where a particular EVM machine can be tampered. Either embedded program stored in ROM whichis used during the overall voting process can be tampered with to behave maliciously before the start of the casting of votes or Memory Unit (MU) which stores the casted votes can be tampered after the voting ends and before counting .Hash algorithm based solution is provided for both the above-mentioned cases to detect the tampering.

## Keywords
Hash Value, Electronic Voting Machine (EVM),Memory Unit (MU), Control Unit (CU),VoterVerifiablePaperAuditTrail(VVPAT),Tampering,SecureHashAlgorithm(SHA)

## 1. INTRODUCTION
With Independence, most of the countries have adopted a Democratic form of Government (political system). The election is the backbone of Democracy. So free, fair, and verifiable elections are crucial to maintaining the sanctity of Democracy [4]. Earlier, the Election Commission of India (ECI) was used to hold a paper ballot- based election where the voter was supposed to cross mark voting response on the ballot paper where different contesting candidate's election symbols were used to be printed. This system had some flaws such as wastage of votes (Invalid votes), booth capturing and also was not eco- friendly. So ECI introduced a more efficient and eco-friendly electronic-based voting system (EVM). Even though elections are being held using EVM are free and fair, there is no concept of verifiability where voters, as well as contester, can ensure the genuineness of EVM. After every election, media is flooded with news of EVM tampering as well as malfunctioning of EVM where even though voters press any button on ballot unit, votes go to some other candidate. Even some bureaucrats (Those who are in charge of executing the election process) also agree with above mentioned claim. So, it's high time to provide verifiability to the EVM. That's why ECI came up with VVPAT (Voter Verifiable Paper Audit Trail) where after pressing the ballot button, the voter can see the print of his response which is dropped in nearby voting box automatically. Even after the election, if any contester doubts EVM is being tampered with, it can be verified using VVPAT. But, with the introduction of VVPAT, is election commission not moving to an earlier manual process that is not eco-friendly? So, now, as the world is witnessing Industrial Revolution 4.0, technically more vibrant solutions should be provided to ensure the verifiability of EVM.

## 2. EXISTINGISSUESOFEVM
So, here, a hash algorithm-based approach is proposed to provide verifiability to EVM. First, two possible cases of EVM tampering are emphasized here.

### Case1.
Tampering of an embedded program stored in ROM (or replacing existing ROM with ROM loaded with a new program is the core of EVM election process. This can be done possibly after EVM has been issued from ECI.

### Case2.
Tampering of memory unit (or replacing existing memory unit with new data loaded memory unit) present in Control Unit (CU) where all the voting data is saved. This can be possibly done after the election process is over and before the counting.

## 3. HASHALGORITHM BASEDSOLUTIONFORABOVEMENTIONEDSCENARIO

### 3.1 Case 1
The content of the ROM (loaded embedded program) should be read and fed to hash algorithms (program) such as SHA, MD5, etc. The hash value thus obtained as an output from the hash algorithm is written on some external ROM-based device. The hash algorithm (program) is stored on a separate ROM in the control unit. As all the EVM issued by ECI are loaded with the same embedded program in their respective ROM, the hash value of all the ROM (embedded program) is the same. So, ECI can create several replicas of above mentioned external ROM-based device containing the hash value. Whenever there is doubt/complaints of Tampering of EVM (ROM containing embedded election ROM), a new hash value is calculated using the embedded ROM program as an input to hash algorithm. The newly calculated hash value is compared with the hash value stored in an external ROM-based device (which is in the custody of ECI). If both the hash values are bit by bit equal, then this means the embedded program in ROM is intact (or ROM is not changed) and tampering has not occurred. If both hash values are not the same, then this means an embedded program in ROM is changed (or ROM is replaced with a new embedded program loaded ROM).

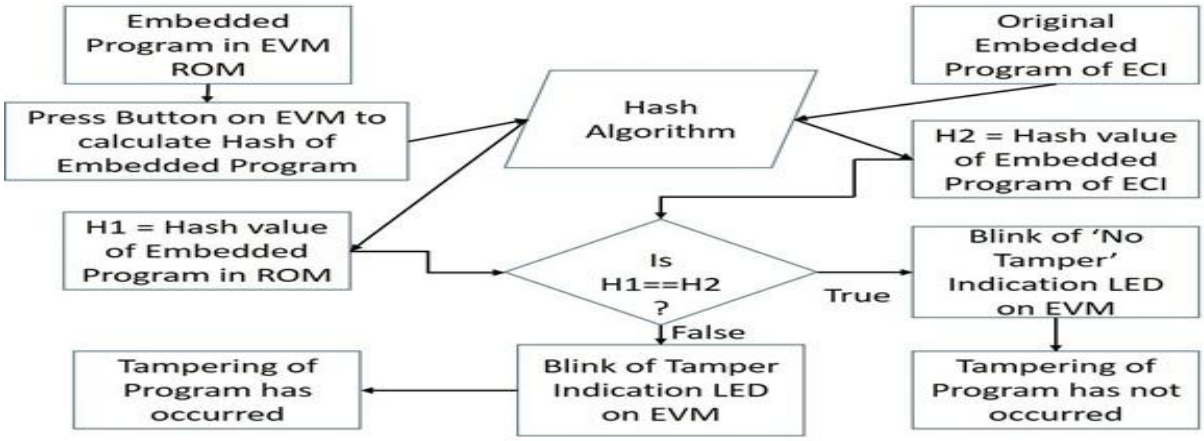


**Fig1: Block Diagram to detect Embedded Program in ROM Tampering**

This can be indicated by glowing a red signal and displaying an appropriate message on the display of CU. Possibly, a hash value comparison program and program to display an appropriate message on display and/or glowing signal are stored on the same ROM where the Hash algorithm is stored in CU. Cryptographic hash function verifies data integrity and sender identity or source of information[7]. Appropriate buttons can be provided on CU to calculate and compare hash values. A slot can be provided on CU to attach an earlier calculated hash value containing an external ROM-based device. This way whether EVM ROM is tampered with or not can be verified using the simple software-based solution. This can be depicted in the flowchart of Fig. 1.

## 3.2 Case2

A presiding officer should be provided with a blank ROM-based external writable device (ROM Pen drive). After the election process is over, before sealing the EVM, he should attach the provided ROM based external device to CU through provided port, press a button (Provided on CU) to calculate the hash value of data stored on the memory unit (MU) and write to the attached device using the same hash algorithm stored in separate ROM in CU mentioned in the above solution. The program to read content from the memory unit and to write a calculated hash value to the externally attached device can be provided in the same ROM in which the hash algorithm is stored. Indication of completion of the process of hash writing can be displayed on CU display.

On the day of Vote Counting, before proceeding to count, a new hash value is calculated using data present in the memory unit as input to the hash algorithm. The Newly calculated hash value is compared with the hash value stored in external ROM based device (calculated after election is over). The comparison program would be already present in same ROM where hash algorithm is stored in CU. Hash Value compare button can be provided on CU. If both the hash values are bit by bit are equal, then this means the memory unit in CU is intact and there is tampering of memory unit (or not replaced with new data loaded memory unit). If both the hash values are not equal, then this means memory unit is not intact and it is tampered (replaced with new data loaded memory unit)[6]. This can be indicated using glowing red signal and displaying on CU display. Hash value comparison program can be provided in external device which will be in custody of ECI. This way whether EVM memory unit is tampered or not can be verified using simple software-based solution. This can be depicted in flowchart of Fig. 2.

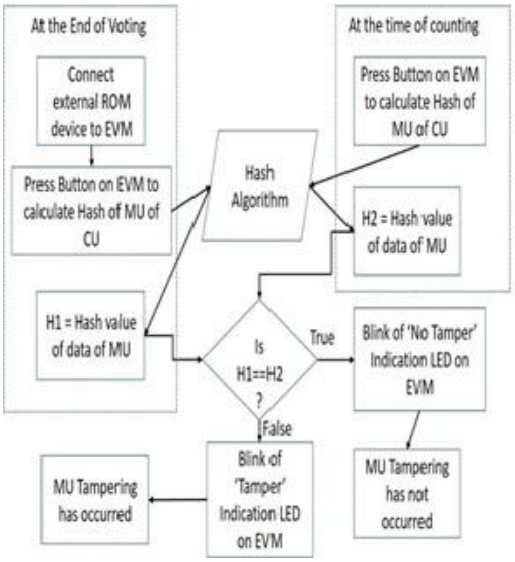


**Fig 2: Block Diagram to detect MU Tampering**

# 4. IMPORTANCE OFHASHALGORITHMINPROPOSEDSOLUTION

The above mentioned solutions are trustworthy and cannot be breached by any third party because of the properties of hash algorithm mentioned below.

i. It is one way (irreversible) function. It means one cannot find original input data given to hash function using hash value[3].

ii. Even if there is one bit change in input, there will be drastic change in output hash value[3].

iii. It is hard to find collision.(Different two data set with same hash value) [3].

# 5. CONCLUSION

This paper presented an innovative idea to provide verifiability and to detect tampering of EVM. Cryptographic hash algorithm is used for this purpose which verifies data integrity. As most of hash algorithm program are open source and storage of hash value require memory in the range of some bytes (hash value of SHA-1 is 160 bits, the above-mentioned solution is economically feasible. Alike VVPAT, it doesn't involve any paper usage, it is environmentally viable. And by making the citizens technologically aware, it can be made socially accepted and trustworthy.

## 6. REFERENCES

[1] NISTstd.FIPS180-2, Secure Hash Standard (SHS), National Institute of Standard and Technology (NIST),Oct. 2001

[2] Florent Chabaud, Antoine Joux, "Differential collisions in SHA-0," Advances in Cryptology-CRYPTO'98, LNCS 1462, SpringerVerlag,1998.

[3] William Stallings, "Cryptography and Network Security: Principles and Practice. Third edition, Prentice Hall.2003

[4] Website of Election commission of India , https://eci.gov.in/ accessed on 12 Dec 2021

[5] Website of Maharashtra State Election Commission,https://mahasec.maharashtra.gov.in /accessed on 12 Dec 2021.

[6] Abdulaziz Ali, Alkandari, ImadFakhri Al- Shaikhli, Mohammad A. Alahmad, "Cryptographic Hash Function: A High Level View",International Conference on Informatics and Creative Multimedia,IEEE,2013.

[7] Liu Jian-dong, Tian Ye, Wang Shu-hong, Yang Ka , "A fast new one-way cryptographic hash function" , IEEE International Conference on Wireless Communications, Networking and Information Security, 2010.