Biometric Security based Intelligent E-Voting System

Sanjay Kumar
Computer Science & Engineering Department
Maharishi Markandeshwar University
Mullana, Ambala, Haryana, India

Manpreet Singh
Computer Science & Engineering Department,
Maharishi Markandeshwar University, Ambala,
Haryana-133203, India

ABSTRACT
Due to advancement in information and communication technology (ICT), E-voting can easily be implemented in electoral process by using available services from locations and at time that are convenient to public to cast their vote with no restriction on geographical location. Security is one of the most important parameter in E-voting system. This research work is an attempt to make the existing E-voting system intelligent enough to ensure security aspect of electoral process specially regarding voter authentication, vote casting authenticity and mobility to avoid fake voting and to maximize the percentage of vote cast despite of corrupted (partial) input presented on EVM (Electronic Voting Machine) during vote casting.

Keywords
EVM, ICT, AVM, Fault Tolerance, Authentication, Security, Fingerprint, Biometric.

1. INTRODUCTION
Electoral system is facing a number of problems in different phases of elections including the weakness in authenticating the voter's identity. In manual verification, voter is identified by his voter ID card which may be tempered also.

Biometric techniques are most popular for authentication of voters. Authors in [1] presented the applications of some of the popular biometrics such as facial recognition, signature dynamics and iris verification in many security systems. Authors in [2] well described the use of artificial neural networks to identify and validate the images in pattern matching applications. Authors in [3] have used principal component analysis on images for dimensionality reduction to improve the performance of pattern matching process. A face detection and recognition system used in on line voting, which one of the electronic is voting types, has been described in [4]. Error back propagation feed forward neural network has been used in [5] to solve matching problems for identification. Author proposed a design of an E-voting system by leveraging biometric key generation to enhance E-voting system in [6].

Authors in [7], observe some limitations in traditional methods of voting systems like fake voting, counting mistakes, high voting cost and long period of counting process and strongly supported the use of biometric finger print authentication in order to avoid these limitations.

2. UNIVERSALITY OF ELECTORAL PROCEDURE
E-voting improves the universality of electoral procedure as it provides some additional options to participate in election such as remote voting. A number of requirements can be identified in respect to the universality of any election such as:

i. Easily understandable and usable voter interface need to be designed.
ii. User interface should be designed after consulting voters during design and testing of vote casting and voter registration procedure.
iii. The needs of physically challenged voters should be considered during interface design.
iv. Voter should be given training to practice the use of vote-casting interface.
v. Guidance should be available to voters through communication channels also.
vi. E-voting system design should maximize the opportunities for the disable persons.
vii. E-voting system should be threat tolerant.
viii. Schedule for voting shall be designed to maximize the voter access and should be announced in public well in advance.

2.1 Major aspects of Electoral Process
a. Fairness of election: In respect to fairness of election it must be ensured that all ballots are accounted for equally. Some major requirements for fair elections are as under:

i. Participant equality (political parties and candidates).
ii. Voting right equality for each voter.
iii. Only authorized, authenticated and eligible voters should be permitted for vote casting.
iv. Voter should not be allowed to cast his/her vote more than once.

b. Security in E-voting: In electoral process only voter knows where he has cast the vote to ensure that votes are cast freely without any outside interface. In general, no voter should be in position to prove that he/she has casted the vote to a particular party in a particular way.

To design an E-voting system, following requirements should be considered in respect to the secrecy of electoral process:

i. Voter authentication or anything else leading to the disclosure of secrecy of voter should be considered as prime at any stage of voting procedure.
ii. E-voting system should guarantee that number of votes in electronic ballot box is same as counter of machine indicates.
iii. Information needed during election should not be used in any way to breach the secrecy of vote and voter.

c. Democracy in election process: Transparency, accountability, security and accuracy are the main parameters of democracy in election procedure.

d. Transparency: An E-voting system should exhibit enough transparency and should treat just like an open system and therefore

i. Necessary steps should be taken to ensure that voter have confidence and understand everything about the E-voting system in use.

ii. Functionality of E-voting system should be announced in public.

e. Accountability: E-voting system shall be discussed with electoral authorities for verification purposes.

f. Reliability: E-voting system is said to be reliable if it performs correctly as per specification for specified period of time and minimizes the chance of equipment breakdown, therefore

i. Authorities should ensure the reliability and security of E-voting system and all possibilities should be explored to avoid any kind of fraud or unauthorized intervention.

ii. Infrastructural access like election data and server should be given to the authorized officials only.

iii. E-voting system should not only maintain the integrity of votes but also the confidentiality of the votes and should keep them sealed until the final phase of election is over.

g. Mobility: E-voting system should be mobile in nature with no restriction on location to allow a voter to cast his/her vote from any location/station.

h. Robustness: E-voting system should be able to cope with errors during execution and should continue to operate despite of the abnormities in input etc.

i. Fault tolerant: E-voting system is said to be fault tolerant if it works properly despite of corrupted input.

j. Scalability: Scalability of a system is defined as the ability of system to handle rising demands without compromising at performance level.

2.2 Functionality Requirements for Different Phases of Election

E-voting requirements are described in Fig 1 to meet the challenges of electoral process. An election is normally divided into three phases; Initial setup phase, voting phase and counting phase.

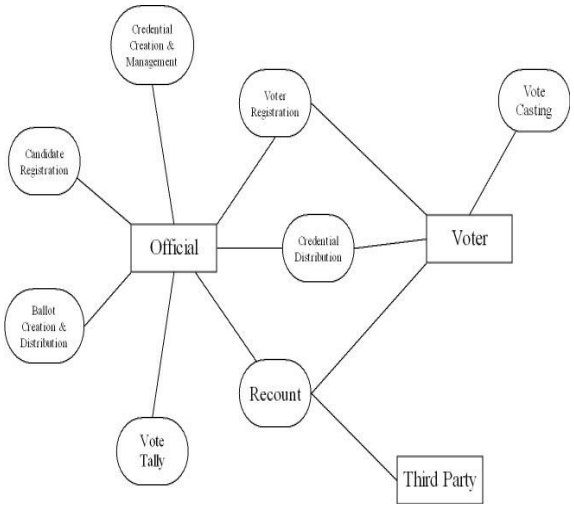

Fig 1: E-Voting Requirements

a. Initial Setup Phase: In this phase, all requirements to conduct the election shall be satisfied. Officers deputed to conduct the election are supposed to do the followings:

i. To ensure that ballot box is empty.

ii. To verify the list of candidates.

iii. To verify the list of voters.

iv. To verify whether the ballot box is properly sealed.

Candidate registration, ballot creation and distribution, voter registration along with credential creation and management are answered in the initial phase before the start of election.

b. Voting Phase: In this phase, authorities must check the identity of voters with registered and authorized list of voters to ensure that one is able to cast a vote before successful completion of the process as shown in Fig 2.

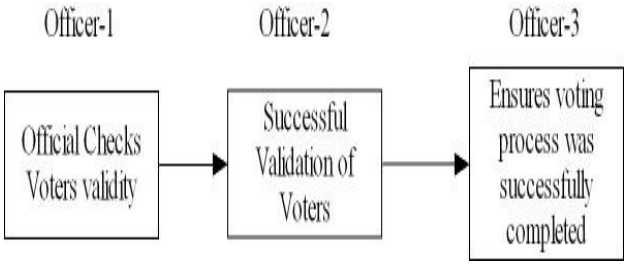

Fig 2: Voting Phase

c. Vote casting: the process of vote casting is performed after successful authentication of voter's identity. Voter cast his/her vote with full secrecy and record of individual voter is updated accordingly.

d. Counting Phase: Ballot counting phase starts after successful completion of voting stage. Station In-charge proceeds with opening of sealed ballot boxes and inform the count to the respective computing centre for publication of result after proper scrutiny of the casted votes.

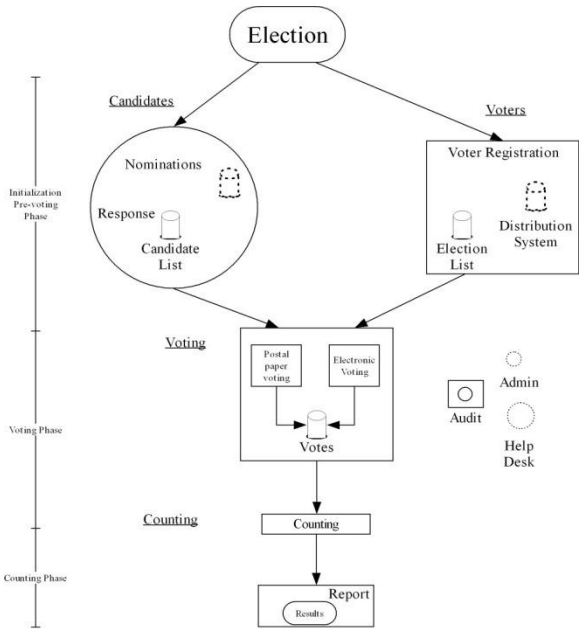

Fig 3: Election Phases

Tallying is done to validate the votes by counting the number of invalid votes.

Recounting is done on the request of a party. If any party is not satisfied with the result, E-voting system must be able to perform recounting.

From a conceptual perspective, E-voting can be described as shown in Fig 3.

3. TRUSTED E-VOTING SYSTEM

Developing a framework for generating and maintaining the necessary characteristics to establish the trust is a critical issue for an E-voting system. E-voting process is highly complex and an average voter does not easily trust. Voters trust on E-voting system is directly related with trust in technology used and persons involved directly or indirectly in the process.

A trusted E-voting system has the following features:

a. **Correctness:** system should work correctly and should do what is expected.

b. **Integrity:** invalid commands or any kind of outside interference/access by an unauthorized user should not have any effect on the correctness of data.

c. **Privilege level:** program has limited access for secure data but access rights or data can not be passed to other un-trusted end.

d. **Confidence level:** program should be tested to ensure the degree of trust level for the environment where to be used finally.

Based on the above features, a trusted E-voting system needs to take up the following issues:-

i. Provisions are made for a voter to cast his vote.

ii. Each voter is allowed for one vote only.

iii. Vote casting is confidential.

iv. Vote can not be altered.

v. Ensuring that vote once cast is not lost.

vi. Unauthorized voters do not cast their votes.

These concepts are the basis for enforcement of security in an E-voting system.

3.1 Security in E-voting:

Security is one of the most important aspect in electoral process to guarantee the integrity and public trust in E-voting system. In E-voting system, security is a way of protecting the data and information system from unauthorized users.

Security is closely related with integrity, availability and confidentiality, and hence are considered as basic building blocks of any secured system during design phase.

a. **Integrity:** aspect of integrity is considered to avoid undesired alteration of information and to ensure authenticity of information.

b. **Confidentiality:** this aspect is considered to maintain personal privacy and to preserve authorized restrictions on access.

c. **Availability:** availability ensures the reliable access and use of information at the right time.

3.2 Threats in E-voting system

Possibility of risk may be minimized if assets are non-vulnerable to threats. Following assets need to be safe guard in E-voting system:

i. Data for authentication and identification.

ii. Election data

iii. Ballots and votes

iv. Poll phase data

v. Results

Attacks on E-voting system can be for publicity, profit or for creating instability in existing government. Attacks may be categorized as under:

a. **Inside attacks:** Inside attackers may be private vendors, government officials, system administrator, system engineer or election officers.

b. **Outside attacks:** outside attackers may be opposition parties, foreign governments, criminals, terrorist or foreign agencies.

4. SYSTEM MODEL

Presented model is an attempt to make E-voting system intelligent enough to ensure that no voter cast his/her vote more than once by maintaining the confidentiality of vote. This model is based on artificial neural networks where finger prints of each voter have been associated with unique voter Id number. During the initial phase, before the start of election, finger prints of all voters of a constituency are captured. During the training phase of the network, each input pattern (feature of individual voter) is applied on the network and an association is encoded. Associated vector is the respective voter ID number of each voter. Voter is supplied an electronic voter ID card called Automatic Voting Machine card (AVM) to be used at the time of poll to activate E-voting machine. In voting phase, voter insert his/her AVM card into the card reader slot of E-voting machine, card reader reads the voter ID number to activate E-voting machine. Voter press any one option of his/her choice to activate button for finger print associated with respective AVM card ID number to finally confirm the vote cast. Once the voter cast his/her vote, intelligent E-voting machine sends a signal to card reader/writer to disable the unique ID number of the respective AVM card by breaking the associations between the voter ID number and finger impression of individuals to ensure that voter can't cast his/her vote more than once.

Neural network based classifier has been used in this model to identify the polling booth with respect to the individual voter. During the activation process of E-voting machine through AVM card, polling booth is also identified. Once the class (poling station) is identified, then it's the responsibility of that class (booth) to authenticate the voter identity by matching the finger impression of the voter from the knowledge base of respective polling station. As neural networks are fault tolerant, this inherent feature has been explored in this model for the authentication of voters despite of corrupted (partial) input applied through thumb impression.

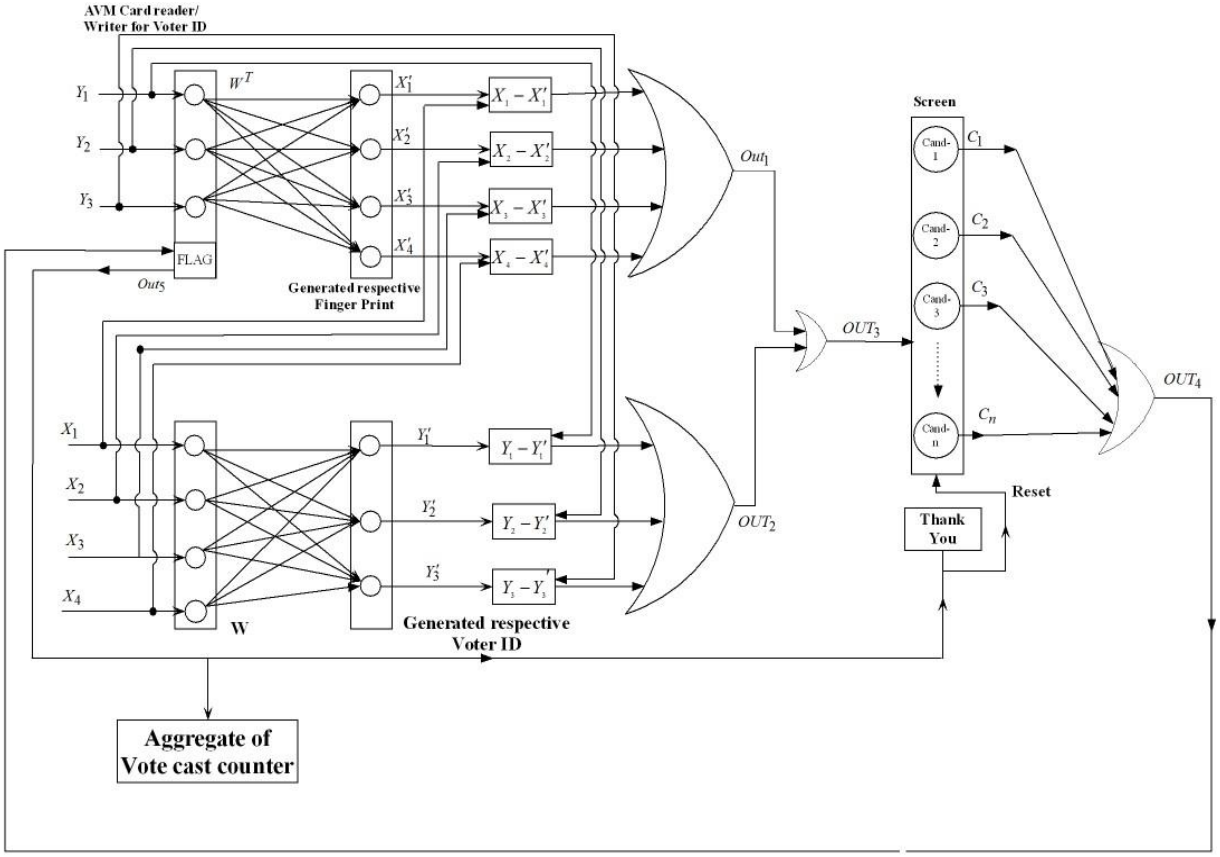

Fig 4: Biometric Security for Intelligent E-Voting

Summarized Functionality of E-Voting System

$Out_3 = 0; When\ Out_1 = 0\ and\ Out_2 = 0;$ Indicate Voter is authenticated Candidate display is activated
$1; Otherwise$; Invalid Voter

$C_i = 1; When\ Out_1 = 0\ and\ Out_2 = 0;$ If candidate i is selected
$0; Otherwise$

$Out_4 = 1; if \sum C_i = 1;$ Sends a signal to card reader to disable AVM card Flag
$0; Otherwise;$

$Out_1 = 1; if\ Flag\ is\ disable;$ Sends a signal on AVM to display Thank You Indicate successful cast of vote and to disable candidate list on screen and increase the count of "Aggregate of vote cast" and "count of selected candidate" by one
$0; Otherwise$;

Mobility aspect has also been taken into consideration to maximize the percentage of voting in election as it provides the flexibility to the voter to cast his/her vote from any nearest polling station of his/her constituency with no restriction to caste vote from home polling station.

Fig 4 represents the architecture of the system model for E-voting addressing the issues as under:

i. Each voter is provided with the means to cast his/her vote.

ii. One to many correspondence is prevented with respect to voter and vote cast.

iii. Two way voter authentication to avoid fake voting.

iv. Mobility provides the flexibility to voters to cast their vote from any polling station in his/her constituency.

v. Despite of corrupted (partial input) finger impression, system has the power of generalization to identify the desired pattern stored in knowledgebase due to inherent fault-tolerant feature of neural network.

4.1 Training procedure

a. Encoding the associations: Neural network embedded in the voting machine provides the means to authenticate the voter before vote cast. In this phase of training, captured finger impressions of voters are applied on the network one by one and an association is encoded between the finger impression and respective unique voter ID number. Input is applied in the form of bipolar version to have better fault tolerance during recognition once the network training is over. Encoding procedure is described as under:

Consider the training pairs given in the problem definition as shown in Table 1 and 2.

Table 1: Binary version

Input Pattern (Finger impression)	Output pattern (unique voter ID number)
$A_1 = (X_1, X_2, X_3, ...X_n)$	$B_1 = (Y_1, Y_2, Y_3, Y_4, ...Y_k)$
:	:
:	:
$A_i =$	$B_i =$

Table 2: Bipolar version

Input Pattern (Finger impression)	Output pattern (unique voter ID number)
$A_1' = (X_1', X_2', X_3', ...X_n')$	$B_1' = (Y_1', Y_2', Y_3', Y_4', ...Y_k')$
:	:
:	:
$A_i' =$	$B_i' =$

Where A_i and B_i are the vectors representing the finger impression and unique voter ID number. Knowledge base of the network captures the associations among the different training pairs in the form of weight matrix given by

$W = \sum_i (A_i')^T B_i'$; Where T represents the transpose of matrix.

b. Retrieval of associations:

i. Voter ID generation from Finger Impression

Once the knowledgebase is build up for the entire problem space and associations are captured in the memory as given in expression (i), application of vector A_i on weight matrix W recalls the respective associated vector B_i.

Firing mechanism of different neurons of the network is governed by the activation function described as under:

$$\left.\begin{aligned} Out_j = f(Net_j) &= 1; if\ Net_j\ is\ positive \\ &= 0; if\ Net_j\ is\ negetive \\ &= previous\ output; if\ Net_j = 0 \end{aligned}\right\}$$

Where

$Net_j = A_i'.W$

Net_j is known as weighted sum of inputs at j^{th} neuron and out_j is called output of j^{th} neuron.

ii. Finger impression generation Voter ID

Finger impression of i^{th} voter represented by vector B_i is generated when voter ID represented by vector B_i is presented on the transpose of the weight matrix W as described below:

$$\left.\begin{aligned} Out_j = f(Net_j) &= 1; if\ Net_j\ is\ positive \\ &= 0; if\ Net_j\ is\ negetive \\ &= previous\ output; if\ Net_j = 0 \end{aligned}\right\}$$

Where $Net_j = B_i' W^T$

4.2 Voter Authentication

At the time of voting, voter punch his/her AVM card in the slot available for card reader and subsequently apply thumb on the thumb button in E-voting machine for his/her authentication. Presented model authenticates voter through 2-way authentication mechanism to avoid fake voting.

a. Authentication through AVM card: Each voter has been provided an AVM card with unique ID number. Voter inserts his/her card in card reader slot of EVM to recall the associated pattern of voters thumb impression. Recalled pattern of thumb impression is compared bit by bit with the stored pattern in the knowledgebase and voter ID is authenticated if either there is no deviation or the deviation is within the tolerance specified for system. Voter ID authentication has been described as:

Voter ID is authenticated if deviation

$\sum_i (X_i - X_i')^2 = 0$, i.e. either zero or within specified tolerance

=1; otherwise to indicate invalid ID.

Flowchart shown in Fig 5 describes voter ID authentication process before vote casting.

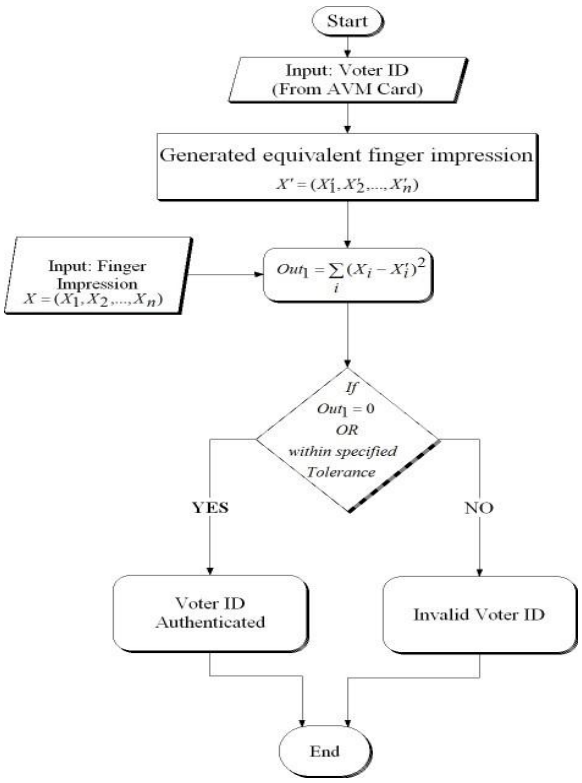

Fig 5: Voter ID authentication process

b. Authentication through thumb impression: At the time of voting, voter apply his/her thumb impression on the thumb button after punching his/her card in AVM card reader available on EVM. Input pattern (thumb impression) is applied on the weight matrix W to recall the associated user ID number.

Recalled associated user ID is compared bit by bit with the stored pattern in knowledgebase; and voter thumb impression is authenticated if either there is no deviation or the deviation is within the specified tolerance. Voter authentication through thumb impression is described as:

Out_2 =0; If either deviation $\sum_i (Y_i - Y_i')^2 = 0$, i.e. either zero or within specified tolerance; indicate successful authentication

=1; otherwise

Fig 6 illustrate the steps involved in authentication process of each voter through thumb impression applied on EVM at the time of voting.

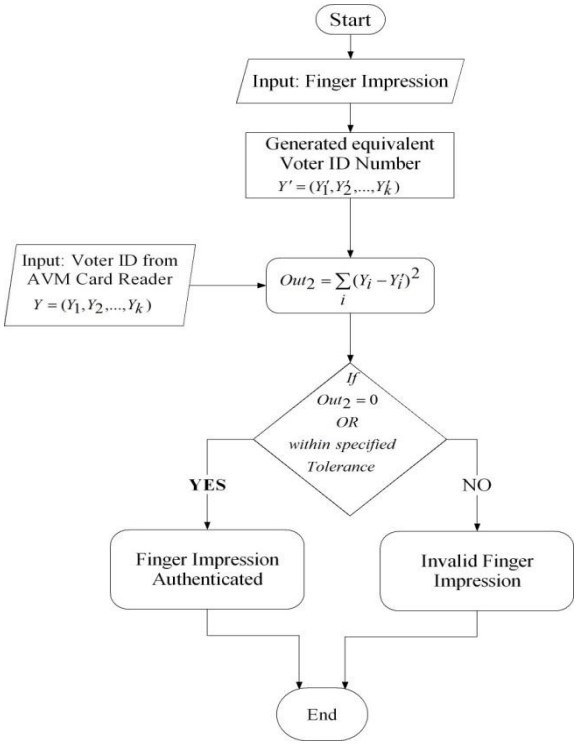

Fig 6: Finger Authentication process

4.3 Polling Station Selection

Mobility provides the means for vote casting irrespective of geographical location. Aspect of mobility has been implemented in this model by using the concept of classification through neural network to identify the polling station for a voter before vote cast. Polling station is identified through the AVM card when inserted in the card reader slot available in the EVM. Architecture based on neural approach is described as in Fig 5 for the identification of polling station for each voter.

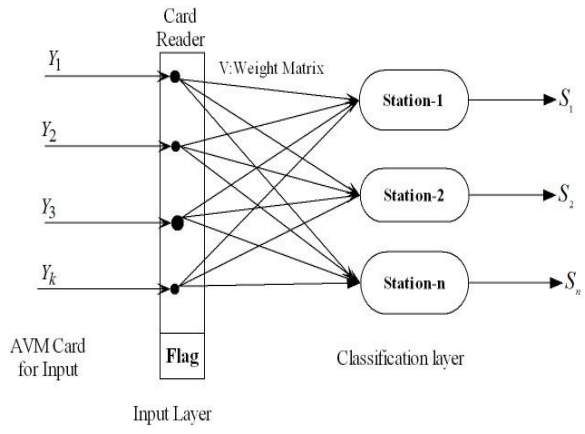

Fig 7: Neural network architecture for polling station selection

Activation function to identify respective polling station is as given below:

$$Output = s_i = 1; \text{ If } L_i \le Net_i \le H_i : \text{To indicate that } i^{th} \text{ polling station is winning neuron.}$$

$$= 0; \text{ Otherwise}$$

$$s_i = f(Net_i, Neuron_i)$$

Where Net_i=decimal value (y_1, y_2, …, y_k) and $Neuron_i$ is the feature of the i^{th} class represented by (L_i, H_i) where L_i is lowest ID in the i^{th} class and H_i is the highest ID assigned to any voter in the class.

Once polling station is identified then it's the responsibility of that class (polling station) to validate the voter through thumb impression by focusing on target class only rather matching thumb impression from knowledgebase of entire constituency. Fig 8 described the procedure for selection of associated polling Station for respective voter to increase the efficiency of the process followed to match the finger impression of individuals from stored patterns in the database.

Computation of Net_i :

Net_i represents the net input value at the i^{th} neuron at the classification layer which is nothing but the weighted sum of inputs to be compared with the feature (Li, Hi) of the ith class.

Net_i =YV;

Where Y is a vector representing voter ID in binary form and V is the weight matrix between input and classification layers.

Weight matrix V_{kn} is initialized as under to enable the network to convert binary number into equivalent decimal number:

$V_{kn} = [v_{ij}] = 2^{k-i}$ for all n

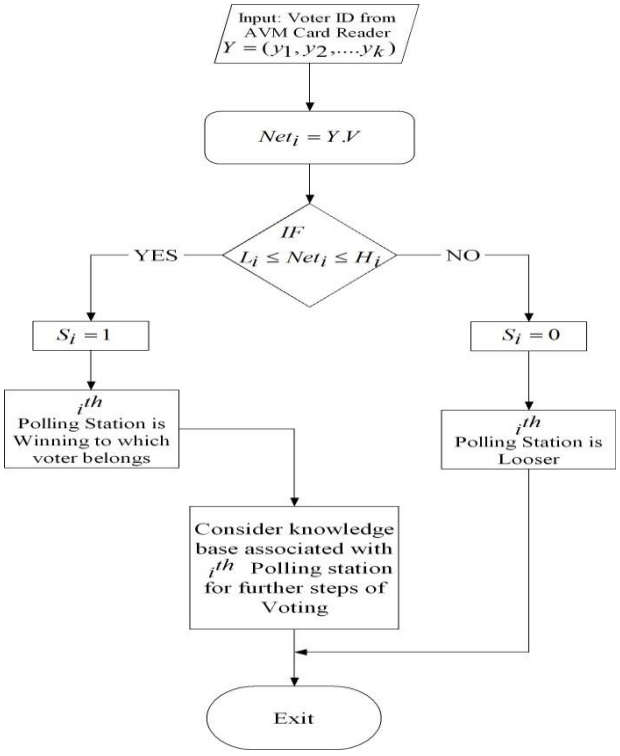

Fig 8: Polling Station Selection

4.4 EVM Activation

EVM is activated to display the list of candidates after the successful 2-way authentication of voter. Display of candidates list on EVM is controlled by the given activation function:

$$Out_3 = f(Out_1, Out_2)$$
$$= Out_1 \vee Out_2$$

$Out_3 = 0$; *Voter is identified as an authorized voter after sucessful* $2-$*Way authentication and a signal is sent to activate the list of candidates on screen.*
$= 1$; *Otherwise*

4.5 Vote Casting

After successful authentication and activation of "Display of candidates list", voter press any one button for the candidate of his/her choice to cast his/her vote. Activation, i.e. output of selected candidate becomes one and zero for losers at the instant. Activations of all candidates are summed together for final decision of that vote cast is described as under:

$$Out_4 = 1; if \sum_i C_i = 1; To\ indicate\ sucessful\ vote\ cast$$
$$= 0; Otherwise$$

Once $Out_4 = 1$; a signal is sent to AVM card reader to disable the flag of AVM card to prevent the voter to exercise his/her vote more than once.

Fig 9 describes the vote casting phase after successful authentication of individual voter.

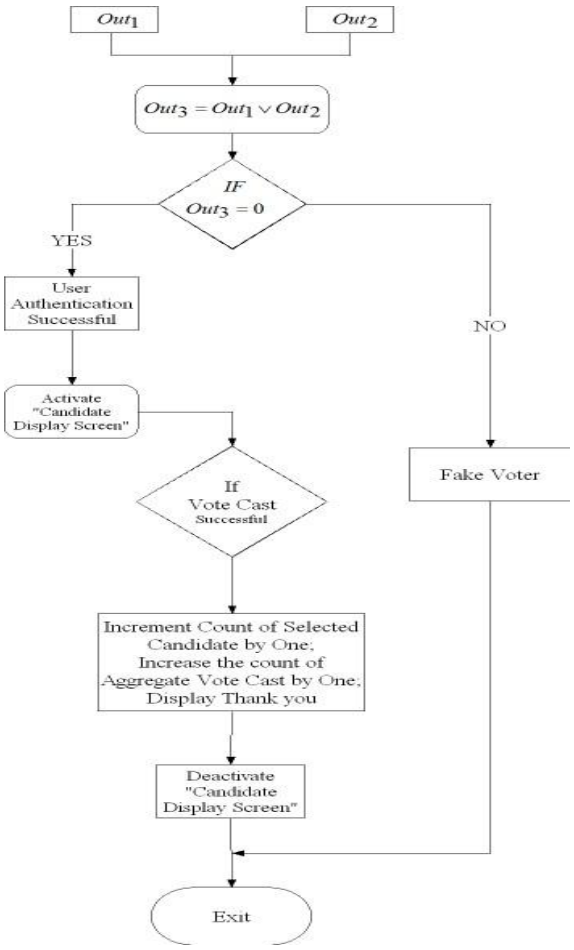

Fig 9: Vote Casting

4.6 Indication for Successful Vote Cast

Once the flag bit of AVM card is reset after authentication and subsequent step of candidate selection, AVM card reader sends a signal to "Display list of candidates" on EVM screen to reset the list of candidates on display screen and signals "Thank you" to indicate successful vote cast by the user.

$Out_5 = f(flag)$
$= 1$; *If* $flag = 0$: *sends a signal to reset the candidates list and display Thank you to indicate the sucessful vote cast and turn for next voter.*
$= 0$; *Otherwise*

4.7 Correctness Validation

After successful completion of each vote cast, AVM card reader sends a signal "Out_5" to "Aggregate vote cast counter" and selected "candidate counter" to increase the count value by one before disabling the candidate list on display screen of EVM. At the end of election at each polling station, the correctness of election process is validated as under:

Correctness=1; If "Aggregate vote counter" value= $\sum_i (Candidate\ count)_i$: which indicate correctness validation process in successful.
=0; Otherwise

4.8 System Analysis

Working procedure of this model has been illustrated with the help of an example to analyze the performance of the presented E-voting system.

Binary Version:

A_i (Finger impression)	B_i : Voter ID (Binary value)
1 0 1 1 1 1 0 1 1 0	1 0 1 1
1 1 0 0 1 0 1 0 1 0	0 1 0 1

Bipolar version:

A_i'	B_i'
1 -1 1 1 1 1 -1 1 1 -1	1 -1 1 1
1 1 -1 -1 1 -1 1 -1 1 -1	-1 1 -1 1

Encoding the associations:

$$W = \sum_i (A_i')^T B_i'$$

$$= \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \\ 1 \\ 1 \\ -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} \begin{bmatrix} 1 & -1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} \begin{bmatrix} -1 & 1 & -1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 & 1 & 1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & -1 & -1 \end{bmatrix} + \begin{bmatrix} -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 2 \\ -2 & 2 & -2 & 0 \\ 2 & -2 & 2 & 0 \\ 2 & -2 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 2 & -2 & 2 & 0 \\ -2 & 2 & -2 & 0 \\ 2 & -2 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & -2 \end{bmatrix}$$

i. **Retrieval of associated vector:**

a. ID generation from finger impression

- Case 1: input pattern is correct

Vector $A_1' = [1 \quad -1 \quad 1 \quad 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad 1 \quad -1]$ is applied on W

$$Net_j = A_i'.W = \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \\ 1 \\ 1 \\ -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} . \begin{bmatrix} 0 & 0 & 0 & 2 \\ -2 & 2 & -2 & 0 \\ 2 & -2 & 2 & 0 \\ 2 & -2 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 2 & -2 & 2 & 0 \\ -2 & 2 & -2 & 0 \\ 2 & -2 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & -2 \end{bmatrix}$$

=[12, -12, 12, 8]=[+ve,-ve,+ve,+ve]

$$\therefore Out_j = f(Net_j) = 1; If \ \ Net_j \ \ is + ve$$
$$= 0; If \ \ Net_j \ \ is - ve$$

=Previous Output; if Netj=0

Therefore B_1 =Out=[1 0 1 1]; recall the respective voter ID of first voter from his/her finger impression

- Case 2: corrupted Input pattern is applied on the network

1. One bit fault : suppose bit number 2 is missing

i.e., $A_1' = [1\,0\,1\,1\,1\,1\,-1\,1\,-1]$

$Net = A'.W_1 = [+ve, -ve, +ve, +ve] = [1\,0\,1\,1] = B_i$;
Recalled the associated voter ID.

2. Two bit fault: Say

$A_1' = [1\,0\,0\,1\,1\,1\,-1\,1\,-1]$

$Net = [+ve, -ve, +ve, +ve] = [1\,0\,1\,1] = B_i$;

Recalled the associated pattern.

3. Six bit fault: Say

$A_1' = [1\,0\,0\,0\,0\,0\,-1\,1\,0\,-1]$

$Net = [+ve, -ve, +ve, +ve] = [1\,0\,1\,1] = B_i$;

Recalled the associated voter ID.

b. Finger impression generation from voter ID

- Case 1: Input pattern (voter ID) B_i read by the card reader of EVM is correct:

B_1=[1 -1 1 1] is applied on W^T.

$$Net = B_i.W^T$$
$$= \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & -2 & 2 & 2 & 0 & 2 & -2 & 2 & 0 & 0 \\ 0 & 2 & -2 & -2 & 0 & -2 & 2 & -2 & 0 & 0 \\ 0 & -2 & 2 & 2 & 0 & 2 & -2 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & -2 \end{bmatrix}$$

=[2, -6, 6, 2, 2, 6, -6, 6, 2, -2]

=[+ve, -ve, +ve, +ve, +ve, +ve, -ve, +ve, +ve, -ve]

Out=[1 0 1 1 1 1 0 1 1 0] =A_i; recalled successfully finger impression of voter from voter ID .

- Case 2: input pattern (voter ID) B_i read by the card reader of EVM is partially corrupted:

Say bit-2 is missing, i.e. B_1=[1 0 1 1]:

When B_1 is applied on WT, then

Net=[+ve, -ve, +ve, +ve, +ve, +ve, -ve, +ve, +ve, -ve]

Therefore out=[1 0 1 1 1 1 0 1 1 0]=A_i; recall the associated pattern successfully despite of one bit corruption due to mal-functionality of card reader of EVM.

5. RESULTS AND DISCUSSION

Analysis shows that presented model has the power of generalization in the sense that it is capable to authenticate the voter in presence of faults. Fault tolerance feature of artificial neural network has been explored in this model to enable each authorized and eligible voter to cast his/her vote despite of the fact that at the time of voting thumb impression may deviate with the impression taken at the time of voters registration subject to the condition that deviation is not beyond the specified tolerance. In summary, presented model is intelligent enough to authenticate the authorized voter for vote casting despite of corrupted inputs (voter ID and thumb impression) received at EVM at the time of voting. 2-way authentication mechanism strongly supports the implementation of this model for electoral process to avoid fake voting.

It has also been analyzed that, in no case, any voter can cast his/her vote more than once as flag of AVM card is disabled immediately after the successful completion of first time vote cast and there after this card is not capable to activate the candidate list on the screen of EVM.

Mobility aspect has also been given fair attention in this work. Artificial neural network based model has been used to classify the constituency into polling booths which provides the flexibility to voters to cast their vote from their nearest available EVM.

Presented model guarantees to validate the correctness of election results ensuring total number of vote cast and sum of counts of votes of all candidates.

6. REFERENCES

[1] Sahoolizadeh, H.;Ghassabeh, Y.A. "Face recognition using eigen-faces, fisher-faces and neural network", Proc. 7th IEEE International Conference on Cybernetic Intelligent Systems, pp 1-6, London, 2008.

[2] A. Jain, R. Bolle, S. Pankanti Eds, "BIOMETRIC - Personal Identification in Networked Society", Kluwer Academic Publishers, Boston/ Dordrecht/ London, 1999.

[3] Smith, Lindsay." A tutorial on Principal Components Analysis". (www.cs.otago.ac.nz/cosc453/student_tutorials/principal_components.pdf)

[4] Noha E. El-Sayed etc, "Face recognition as an authentication technique in electronic voting", in IJCSA, Vol. 4, No. 6, 2013.

[5] Chesnut, C.2004, " Chesnut tablet pc ocr with neural network AI". Retrived April 13, 2010, from http://www.generation5.org/content/2004/aiTabletocr.asp .

[6] V. C. Ossai, et. Al., "Enhancing E-voting systems by Leveraging Biometric Key Generation (Bkg)" in American journal of Engineering research (AJER), Vol. 2, Issue-10, pp. 180-190, 2013.

[7] Available online at http://www.academicjournals.org/SRE.