BIOMETRIC VOTING SYSTEM

Abstract:

It has always been an arduous task for the election commission to conduct free and fair polls in our country, the largest democracy in the world. Crores of rupees have been spent on this to make sure that the elections are riot free. But, now- a -days it has become common for some forces to indulge in rigging which may eventually lead to a result contrary to the actual verdict given by the people.

This paper aims to present a new voting system employing biometrics in order to avoid rigging and to enhance the accuracy and speed of the process. The system uses thumb impression for voter identification as we know that the thumb impression of every human being has a unique pattern. Thus it would have an edge over the present day voting systems.

As a pre-poll procedure, a database consisting of the thumb impressions of all the eligible voters in a constituency is created. During elections, the thumb impression of a voter is entered as input to the system. This is then compared with the available records in the database. If the particular pattern matches with any one in the available record, access to cast a vote is granted. But in case the pattern doesn't match with the records of the database or in case of repetition, access to cast a vote is denied or the vote gets rejected. Also the police station nearby to the election poll booth is informed about the identity of the imposter. All the voting machines are connected in a network, through which data transfer takes place to the main host. The result is instantaneous and counting is done finally at the main host itself. The overall cost for conducting elections gets reduced and so does the maintenance cost of the systems.

Key Words: *election commission, biometrics, pre-poll procedure, database, voting machine, network.*

Conclusion: Thus the advent of this biometric thumb impression voting system would enable hosting of fair elections in India. This will preclude the illegal practices like rigging. The citizen can be sure that they alone can choose their leaders, exercising their right of democracy.

INTRODUCTION

Biometrics is the term given to the use of biological traits or behavioral characteristics to identify an individual. The traits may be fingerprints, hand geometry, facial geometry, retina patterns, voice recognition, and handwriting recognition.

In this paper we have used thumb impression for the purpose of voter identification or authentication. As the thumb impression of every individual is unique, it helps in maximizing the accuracy. A database is created containing the thumb impressions of all the voters in the constituency. Illegal votes and repetition of votes is checked for in this system. Hence if this system is employed the elections would be fair and free from rigging. Thanks to this system that conducting elections would no longer be a tedious and expensive job.

DESIGN

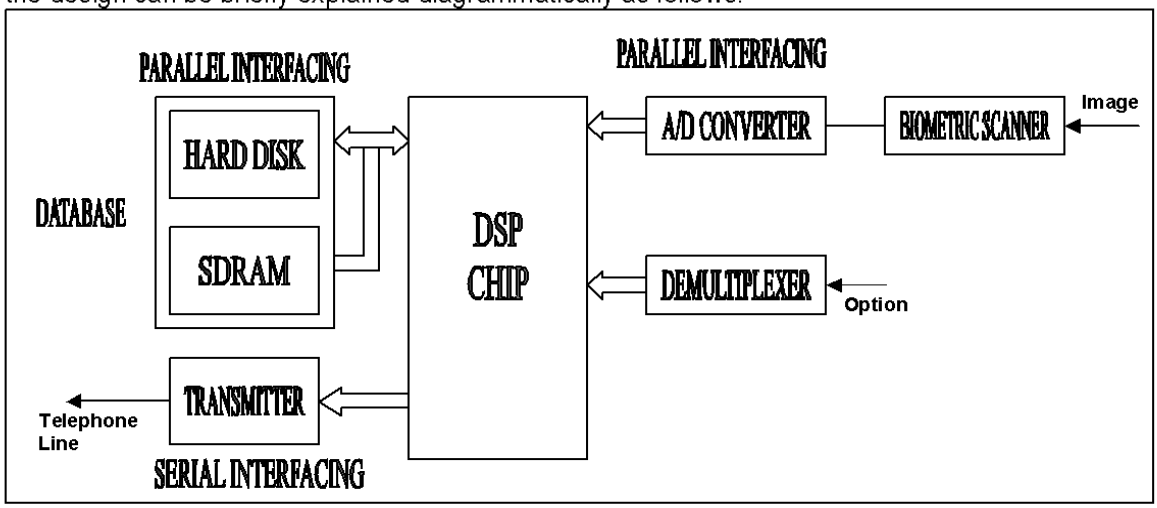
The design of the system consists of the following important parameters

1. Scanning- using DSP Processor
2. Searching- based on the principle of GOOGLE SEARCH
3. Networking- all the election booths are connected in a network
4. Data transfer– using telephone lines..

The only pre-requisite for the use of this finger print scanner is a personal identification card. We hope that this system proves to be efficient and enables the people to be smarter in choosing their leaders.

SUMMARY OF DESIGN

The main aim in designing this product is to provide the concept of the personal identity for each individual. This is extended to a special case of electronic voting machine concept. The summary of the design can be briefly explained diagrammatically as follows.

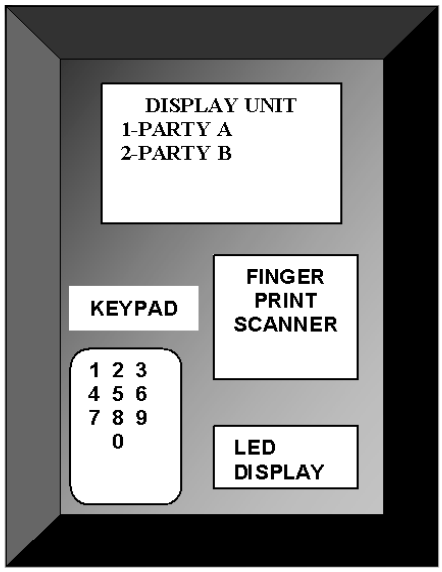


As a pre-poll procedure the finger prints of all the voters are collected and stored in a database initially at time of distributing voting cards. At the time of voting, the option of the voter is taken along with the finger print. The finger print taken by the scanner is sent to the DSP chip through an in-built A/D converter. The processed image is transferred to hard disk with biasing of SDRAM.

The option entered by the voter is transferred to chip through DEMUX and is stored in the memory. If the transferred image is matched with any of the records in the data base, then the interrupt is given by the HARD DISK to DSP chip. Then the option is considered in the count. After the acquisition of the count this is transmitted to the HOST computer or central server using telephone lines. As the count of each party is transmitted to the HOST from all the VOTING MACHINES present in the constituency, the HOST will add parallel count of particular party and

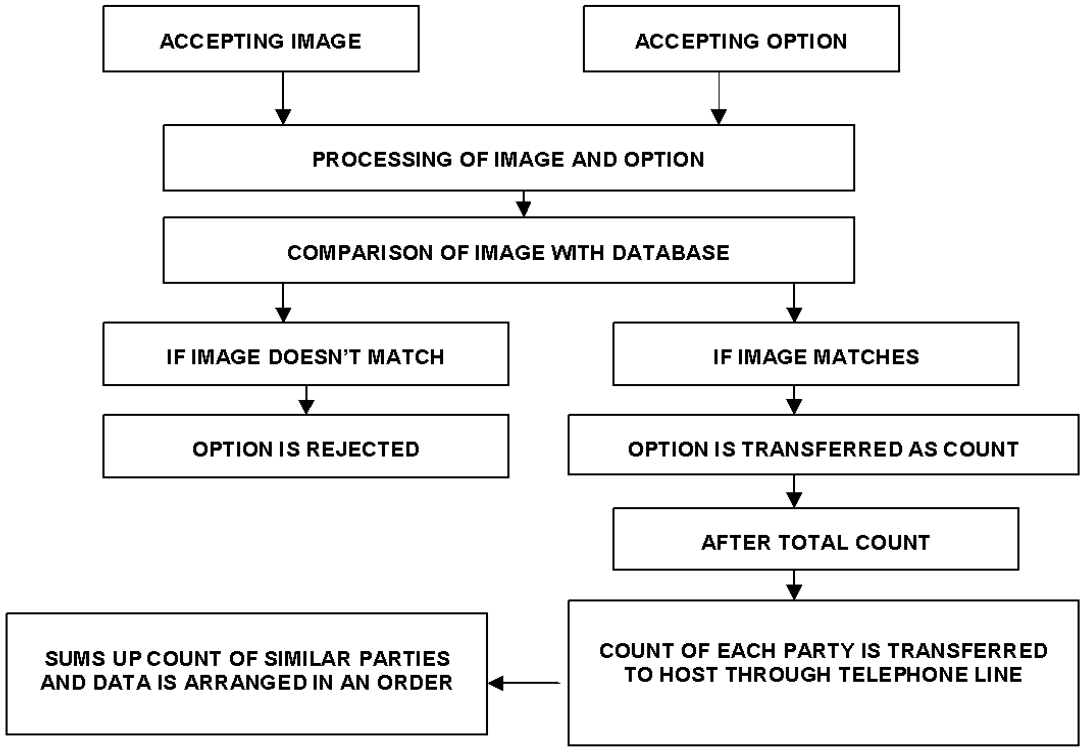
makes the final count of each party in ascending order. The final count is transferred to the main HOST (head quarters) using either telephone lines or radio waves.

DESCRIPTION OF THE VOTING MACHINE



Front view of the voting machine

BLOCK DIAGRAM FOR THE WHOLE PROCESS IN BRIEF:



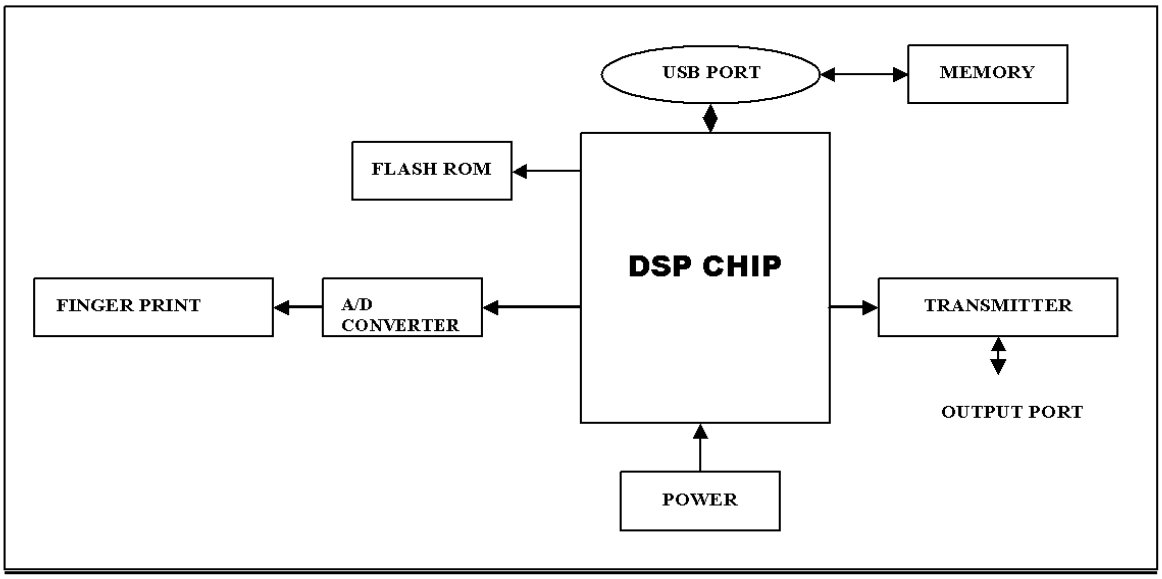
The detailed description of each and every internal unit in the VOTING SYSTEM is given below. It can be divided in to the following main categories.

FINGER PRINT SCANNER:

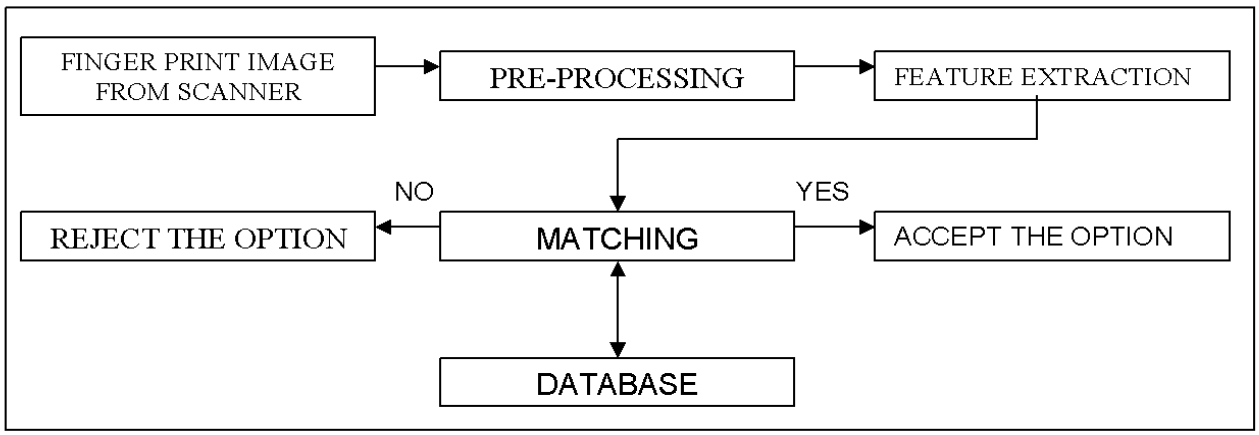
The finger print scanner consists of the following parts:

1. *FINGER PRINT SENSOR:* This is used to scan the thumb impression. The data obtained from this is analog in nature. This is transferred to the A/D converter for further processing.
2. *A/D CONVERTER:* This is used to convert the analog data from the SENSOR into the digital data and transfer it to the processor.
3. *FLASH ROM:* This is for the storage of the data temporarily in the DSP processor. This will work until the data is transferred to the main memory of the HOST.
4. *DSP CHIP:* This is used to receive the data and process it. This is connected to the USB port for further transfer of the data.
5. *USB PORT:* The sole purpose of the USB port is to establish a communication link between the DSP processor and the MEMORY (DATABASE).

EXTRACTION OF THUMB IMPRESSION:-



The next step in the process is the extraction of the thumb impression from the memory. The features of the finger print are stored in the form of pixels. This is further sent for pattern matching where the finger print is then compared with the records in the database. If the pattern matches with any one of he records then the vote is accepted. If the feature doesn't match with any one of the finger prints stored in the data base then the vote is rejected.



FEATURE EXTRACTION AND COMPARISON

SCANNING AND PROCESSING:

The biometric sensor scans the image. This so scanned data is in the analog form. This is converted into digital form by using an A/D converter. Since the image is to be transferred quickly to the converter, it is interfaced in parallel with the DSP chip. The data received from the parallel in ports is further processed in the chip. Parallel interfacing is done to have a quick performance.

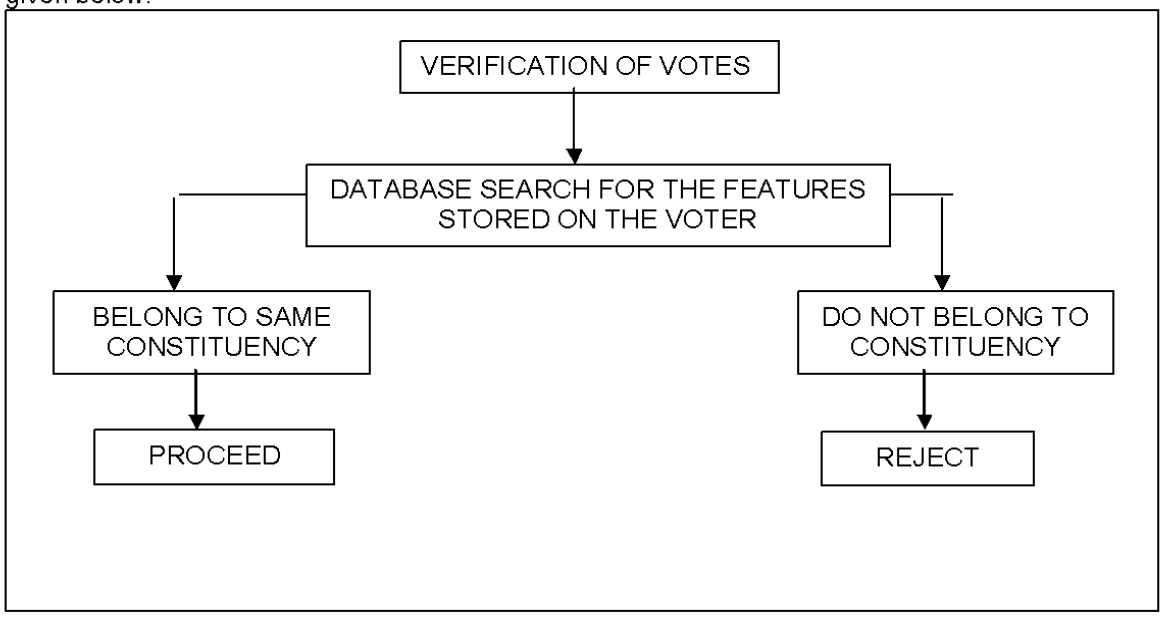
TRANSFER OF PROCESSED DATA TO THE HARD DISK:

The data which is processed in the DSP chip (finger print) is transferred in parallel to the HARD DISK for searching process. The BIOS language of the HARD DISK is stored in SDRAM which is also interfaced in parallel with the chip. This helps the chip to transfer the image to the HARD DISK for further process. The image transferred to the HARD DISK is compared with that of the DATA BASE..

BLOCK DIAGRAMS FOR VARIOUS PROCESSES

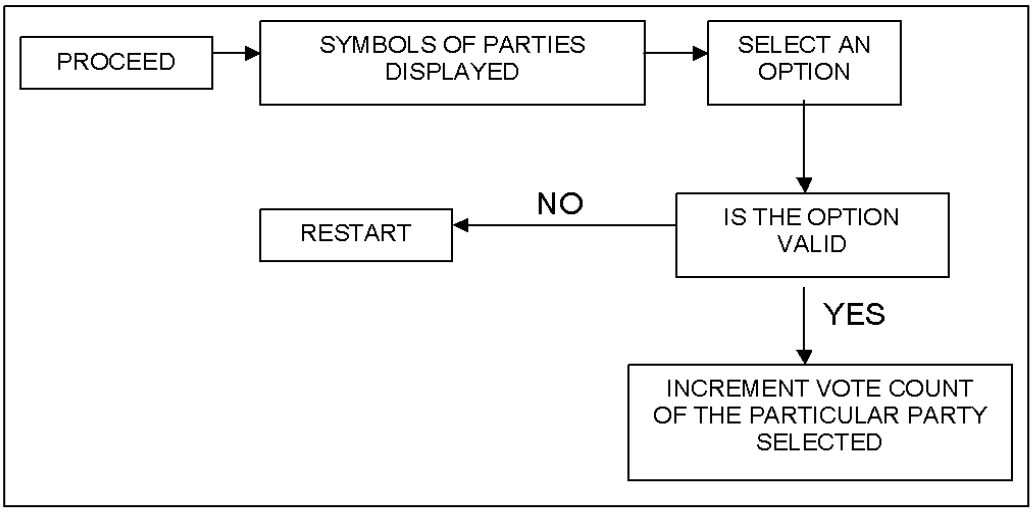
VERIFICATION OF VOTERS

Here the identity of a person is checked whether he\she belongs to the particular constituency or not. The machine which takes the finger print of the person checks it with the data base already stored in it. If the finger print matches it will give access to the person to cast his vote and if it doesn't match any of the finger prints stored in the data base then it will reject the voter. Thus his method will enable the members of that particular constituency only to vote. This can be taken as the first step to avoid rigging. To have a faster performance the searching technique is implemented on the basis of GOOGLE SEARCH. The process in the form of a flow chart is as given below.



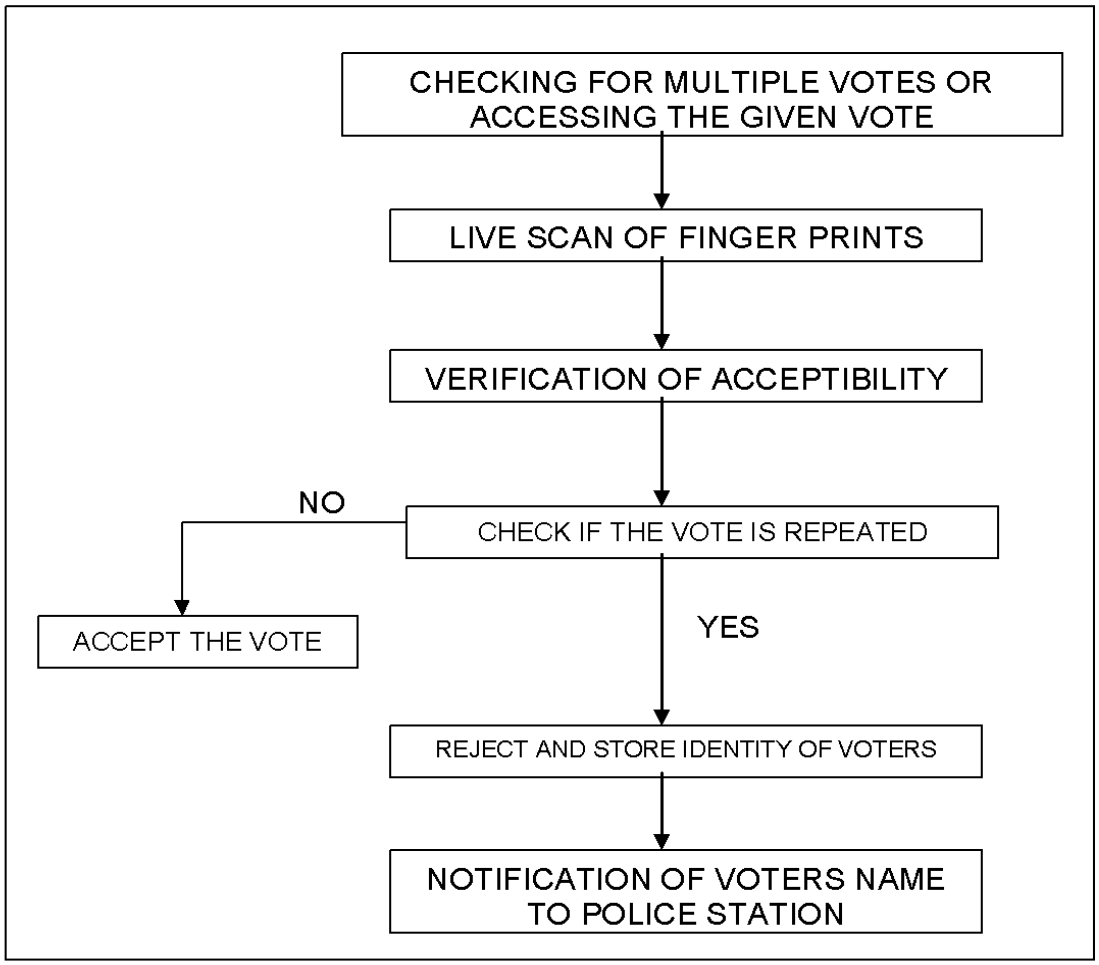
PROCESSING AND COUNTING:

After the person gets the PROCEED symbol from the voting machine, there appears a screen on which all the parties names along with the symbols are present. The person should select any one of the party by giving the number allotted to that particular party as input through the keypad. After the option is selected the voter is prompted for a confirmation. In case the voter enters an invalid number, the screen reappears and he\she is prompted to cast the vote again. Then according to the option selected, the vote count of the particular party gets incremented by one. Finally, at the end of the day, the position of the parties in terms of the total votes cast can be known. A very simple flow chart for the above process is as shown below:



REJECTION OF VOTER REPETITION

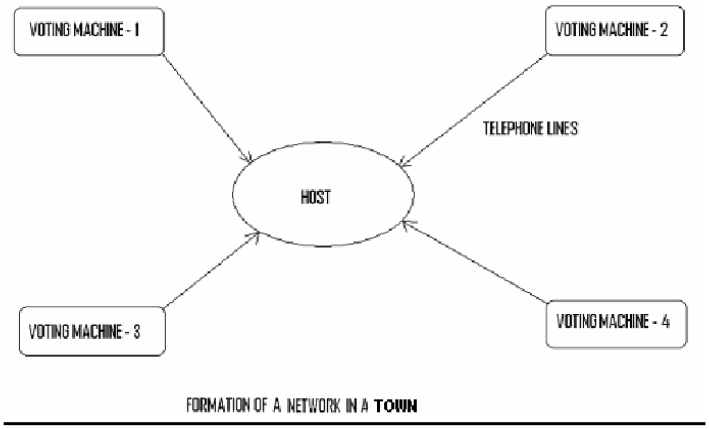
After we have emerged out with a solution to check voter's identity in a constituency, our next task is to see that a particular person cannot vote more than once i.e. to avoid multiple votes. This task can be accomplished by simple software technique employed. It consists of two folders namely searched and unsearched. Initially the searched folder consists of no images. The thumb impression images of all the voters of a constituency will be present in the unsearched folder. As and when a vote is cast, the image of the particular voter gets transferred to the searched folder. The searched folder is programmed such that an image cannot be present more than once in this folder. So when a voter casts multiple votes the exception is generated and an alarm is raised and even the police can be informed about the identity of the intruder indulging in this illegal activity. This is shown in the block diagram given below



The scanned vote is first checked with the acceptability of the voter as explained in the first flow chart. If the finger print is accessible then the data of the specified person is taken into account. The voter's thumb impression is verified with the previously cast votes. If there is no match then the vote is accepted and the count is increased by one. If the vote matches with any of the previous votes then the vote is rejected and the person's identity is stored and it is given to the police for further enquiry. There is a flash ROM in which these details can be stored.

FORMATION OF THE NETWORK

The voting machines present in a town are interlinked in the form of a highly secure LAN. This network is formed with the help of the telephone lines. All the data collected in the voting system is first stored in the voting machine itself. Then it is sent to the HOST which will be located at headquarters of the town. All the data is collected there and it is transferred to the main HOST. The purpose of saving the data in the voting machine at first is that even if there is loss of data by some means then it can be easily retrieved from the machine again. In this way all the things are bought into a network.



FORMATION OF A NETWORK IN A **TOWN**

These hosts are again grouped into network through radio waves or again telephone lines. Host is a device which consists of a PROCESSOR and a RAM. It will accept the data from all the voting machines through telephone lines and it will store the data in RAM (count of all parties). Then it will add the count of similar parties and store the count in ascending or descending order and display the result whenever it is necessary.

Thus all the voting machines in the state can be formed into a network. The network can make use of RADIO waves or TELEPHONE lines for the data transfer.

ADVANTAGES:

1. The system is highly reliable and secure.
2. In the long run the maintenance cost is very less when compared to the present systems.
3. Illegal practices like rigging in elections can be checked for.
4. It is possible to get instantaneous results and with high accuracy.