iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 6 **Issue:** IV **Month of publication:** April 2018

**DOI:** http://doi.org/10.22214/ijraset.2018.4026

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue IV, April 2018- Available at www.ijraset.com*

# Authentication of Electronic Voting Machine (EVM)

Mihir Shah[1], Prof. Rajakumar K.[2]
[1, 2] *Vellore Institute of Technology, Vellore, Tamil Nadu*

***Abstract:*** ***Elections in India are conducted almost exclusively using electronic voting machines developed over the past two decades by a pair of government-owned companies. These devices, known in India as Electronic Voting Machine (EVMs), have been praised for their simple design, ease of use, and reliability, but recently they have also been criticized following widespread reports of election irregularities. This project is made with the intention to authenticate the voters wherein their unique ID will be matched with the already available data of the voters. Added to this, a face detection and recognition system will also be used to check if that particular person corresponds to the one with that ID. The two matching points are used by a matching algorithm to check whether they are identical or not. If the results of the matching algorithm are two point match then checks wither this person has the right to vote or not.***

***Keywords: Electronic Voting Machine (EVM), Radio Frequency Identification (RFID), Face Detection, Face Recognition.***

## I. INTRODUCTION

The focus of this project is on making the electronic voting machine as secure and as fraud proof as possible. To achieve this objective two matching points are considered – unique ID and face recognition.

Deployment in elections to cast cote and let only the correct person with right to vote be allowed to vote. Face detection and recognition provides an added security measure for authentication.

In this research a Face Detection and Recognition system (FDR) is used as an authentication technique in proposed type of electronic voting. The voter's image is captured and passed to a face detection algorithm (Eigen face or Gabor filter) which is used to detect his face from the image and save it as the first matching point. The voter's National identification card act as RFID which is used to retrieve and return the saved photo from the database of the concerned authority, which is then passed to the same detection algorithm (Eigen face or Gabor filter) to detect face from it and save it as second matching point. The two matching points are used by a matching algorithm to check whether they are identical or not. If the results of the matching algorithm are two point match then checks whether that particular person has the right to vote or not. If the has the right to vote then the next step for casting the vote is initiated.

## II. RELATED WORKS

In related research and works, several voting system, voter identification and authentication techniques were introduced to secure voting platforms and overcome fake voting.

Some of these techniques are really worth the time been given.

In paper [6], Highly Secure Online Voting System with Multi Security using Biometric and Steganography, the basic idea suggests to merge the secret key with the cover image on the basis of core image. The result of this process produces a stego image which looks quite similar to the cover image. The core image is a biometric measure, such as a fingerprint image. The stego image is extracted at the server side to perform the voter authentication function. It used secret message with 288 bit length. As the actual secret key is never embedded in the stego image, there will be no chance of predicting secret key from it.

In paper [9] and [10], Holistic Methods use entire face image as a raw input for further processing. A famous example of this method is PCA-based approach presented by Sirovich and Kirby, followed by Pentland and Turk.

In paper [11], for extracting local features which are nose, ears, eyes and lips, the Local Feature-based Methods are used. Their positions and local look are key to the recognition phase. This is done by using Elastic Bunch Graph Matching (EBGM).

## III. PROPOSED WORK

First of all, voter gets its RFID tag scanned by the RFID reader. The ID number obtained by RFID reader is checked with the database. If a match is found then face recognition is done else the voter is declared not eligible and sent away. Later if even face

recognition is also cleared successfully then the voter proceeds to the GUI voting interface, wherein the voter can cast the vote for desired candidate from the given choices.

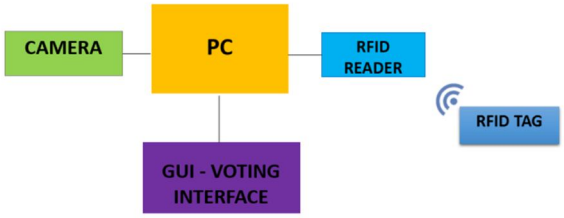



Fig 1. System Architecture

## IV. METHODOLOGY

In order to recognize the face, Principal Component Analysis (PCA) algorithm is utilized. PCA is a statistical approach used for reducing the number of variables in face recognition. In PCA, every image in the training set is represented as a linear combination of weighted eigen vectors called eigenfaces.

One of the simplest and most effective PCA approaches that can be used in face recognition systems is known as eigenface approach. This approach transforms faces into a small set of essential characteristics, eigenfaces, which are the main components of the initial set of learning images (training set). Recognition is done by projecting a new image in the eigenface subspace, after which the person is classified by comparing its position in eigenface space with the position of known individuals. The advantage of this approach over other face recognition systems is in its simplicity, speed and insensitivity to small or gradual changes on the face. The problem is limited to files that can be used to recognize the face. Namely, the images must be vertical frontal views of human faces.

*A. The whole Recognition Process Involves Two Steps*

*1)* Initialization process

*2)* Recognition process

*B. The Initialization Process Includes the Accompanying Tasks*

*1)* Acquire the initial set of face images called training set.

*2)* Calculate the Eigenfaces from the training set. Only the highest eigenvalues are kept. These M images define the face space. As new faces are found, the eigenfaces can be restructured or recalculated.

*3)* Calculate distribution in this M-dimensional space for each known person by projecting his or her face images onto this face-space. These operations can be performed from time to time whenever there is a free excess operational capacity.

*C. Having initialized the system, the next process involves the steps:*

*1)* A set of weights is calculated based on the input image and the M eigenfaces by projecting the input image onto each of the eigenfaces.

*2)* The image is checked if it is a face at all (known or unknown).

*3)* If it is a face, then classify the weight pattern as either a known person or as unknown.

*4)* Update the eigenfaces as either a known or unknown.

The last step is not usually a requirement of every system and hence the steps are left optional and can be implemented as when the there is a requirement.

In order to calculate the eigenfaces assume a face image Γ(x, y) be a two dimensional M by N array of intensity values. An image of dimension M × N is considered as a vector.

Step 1: Prepare the training faces. Obtain face images (training faces). The face images must be centered and of the same size.

Step 2: Prepare the data set in the database by transforming them into a vector and place into a training set S.

Step 3: Compute the average face vector.

Step 4: Subtract the average face vector. The average face vector is subtracted from the original faces and the result stored in the variable.

Step 5: Calculate the covariance matrix.

Step 6: Calculate the eigen vectors and eigen values of the covariance matrix. Step 7: Keep only K eigen vectors (corresponding to the K largest eigenvalues)
Eigenfaces with low eigen values can be omitted, as they explain only a small part of characteristic features of the faces.

## V. RESULT

The two point security features of RFID matching and face recognition has given the desired result of high level security by authenticating the voters.

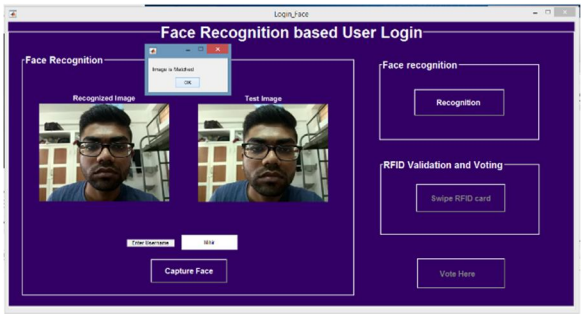



Fig 2. Face Recognition showing the matched faces

A fully functional electronic voting machine with GUI interface is made which is very secure and reduces the potential risks of frauds to minimal levels.

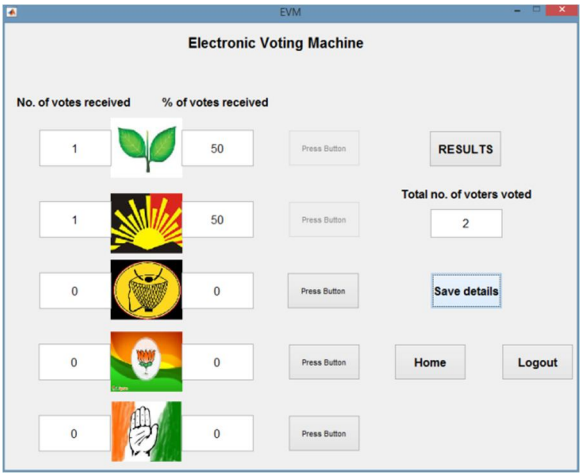



Fig 3. EVM GUI voting interface

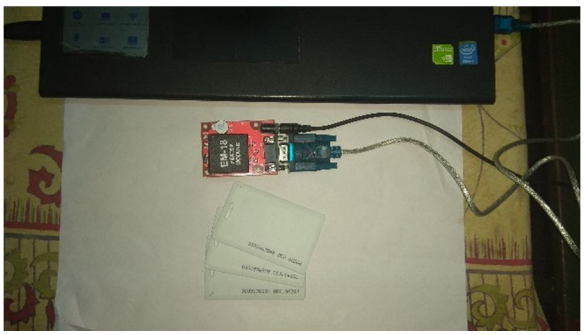


Fig 4. Proposed work hardware and circuitry

## VI. CONCLUSION

RFID which stands for Radiofrequency Identification has enormous uses compared to old bar-code systems like there read and write data without any contact, different ranges to read, more data capacity are the advantages using radio frequency identification technology compare to old bar code system. Like every system have advantages and disadvantages, RFID too has the problems in

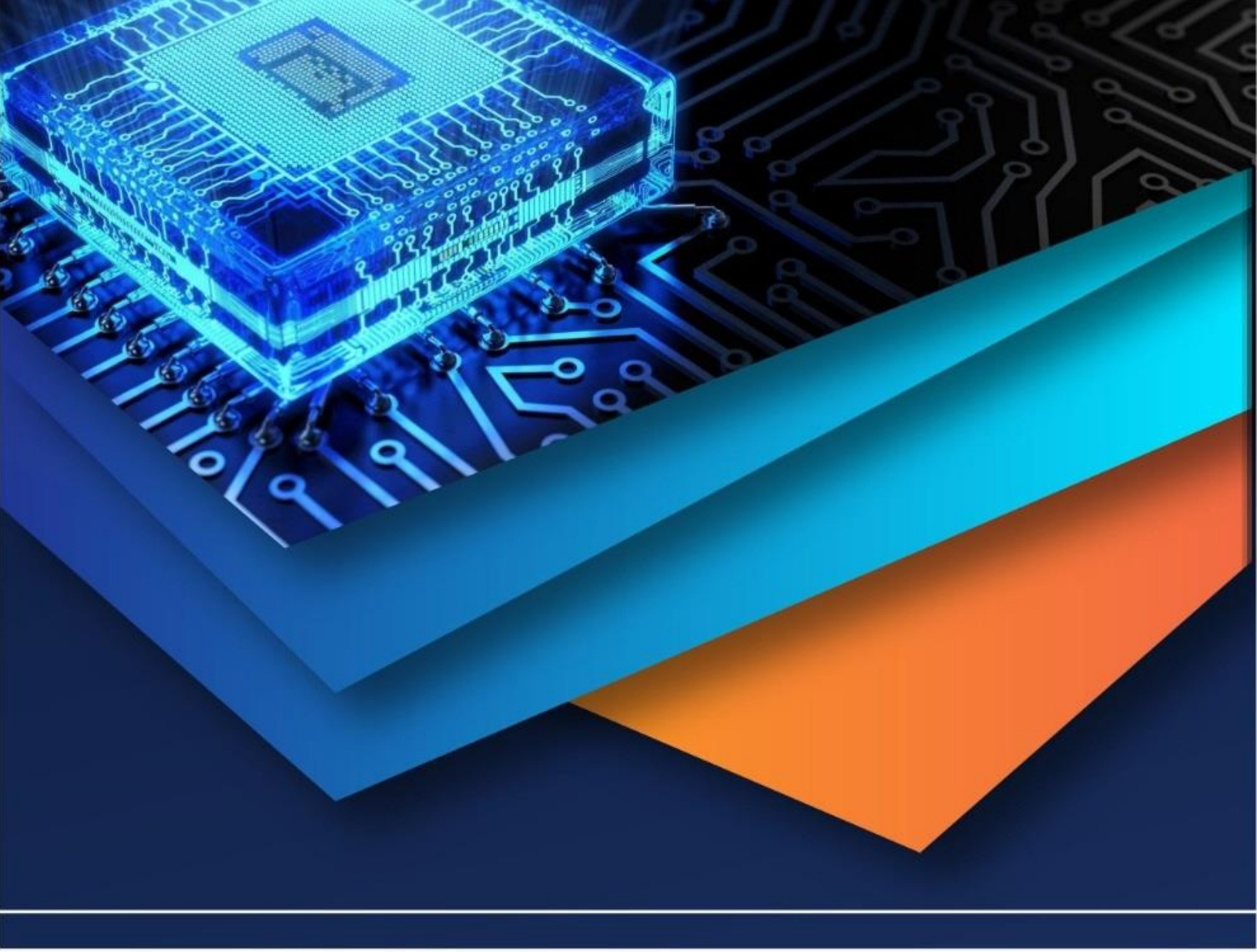
terms of performance, cost, hardware, interferences etc. There are some competing standards that have been more difficult problems for RFID. The readability of the tags through different materials is very tedious to achieve. There still have been an issue for end users privacy especially in case of health care which is concerned with transmission frequency and access to unauthorized people. To tackle this issue, face detection have been employed so that unauthorized people can be prevented from misusing it.

## VII. FUTURE SCOPE

A timer could be introduced, which could automatically end the voting after a specified duration of time. Biometric verification of voters can be introduced, this could include fingerprints, retina and iris patterns. This would automatically help us ensure that one person votes only one time. It can be made a little more interactive by adding sound speech to it. EEPROM can be used to store the data permanently. Moreover touch can also be implemented in place of switches. We can also add up acknowledgement process with the help RFID. An acknowledgement number can be generated so that the voter can get the SMS alert to their mobile number and also we can restrict and monitor the persons who are not allowed to vote.

## REFERENCES

[1] Shaik Mazhar Hussain, Chandrashekar Ramaiah, Rolito Asuncion, Shaikh Azeemuddin Nizamuddin, Rakesh Veerabhadrappa ;An RFID based Smart EVM System for Reducing Electoral Frauds. 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)
[2] D. Ashok Kumar, T. Ummal Sariba Begum; Electronic Voting Machine – A Review. Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering, March 21-23, 2012
[3] Heseltine T., Pears N., Austin J.; Evaluation of image pre-processing techniques for eigenface based face recognition. In Proc. of the Second International Conference on Image and Graphics, SPIE vol. 4875, (2002) 677-685
[4] Muhammad Sharif, Adeel Khalid, Mudassar Raza, Sajjad Mohsin; Face Recognition using Gabor Filters. Department of Computer Sciences, COMSATS Institute of Information Technology, Wah Cantt-Pakistan J
[5] Volkamer M., Alkassar A., Sadeghi A., Schultz, S.; (2006). Enabling the Application of Open Systems like PCs for Online Voting. Proceedings of the Frontiers in Electronic Elections – FEE ’06. Retrieved January 14, 2011
[6] B. Swaminathan, J. Cross Datson Dinesh; Highly Secure Online Voting System with Multi Security using Biometric and Steganography. Dept of Computer Science and Engineering, Rajalakshmi Engineering College #2 Chennai, India
[7] Avinash Kaushal, J P S Raina; Face Detection using Neural Network & Gabor Wavelet Transform. GCET, Greater Noida, U.P., India; 2BBSBEC, Fatehgarh Sahib, Punjab, India.
[8] Orhan Cetinkaya, Deniz Cetinkaya; (2007). Validation and verification issues in e-Voting. 7th European Conference on e-Government (ECEG'07)
[9] M. Kirby and L. Sirovich; Application of the Karhunen- Lo`eve procedure for the characterization of human faces. IEEE Transactions on Pattern Analysis and Machine Intelligence,12(1): pages 103–108, 1990
[10] M. Turk, A. P. Pentland; Eigenfaces for recognition. Journal of Cognitive Neuroscience, 3(1): pages 71–86, 1991.
[11] Al-Amin Bhuiyan, Chang Hong Liu; On Face Recognition using Gabor Filters. Proceedings of world academy of science, engineering and technology volume 22 July 2007 ISSN 1307-6884.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY