Face Recognition as an Authentication Technique in Electronic Voting

Noha E. El-Sayad
Electrical Engineering Department
Faculty of Engineering, Port-Said University PortFouad42523,
Port-Said, Egypt

Rabab Farouk Abdel-Kader
Assistant Prof. Electrical Engineering Department
Faculty of Engineering, Port-Said University PortFouad 42523, Port-Said, Egypt

Mahmoud Ibraheem Marie
Assistant Prof. In Computer and System Engineering Department
Faculty Of Engineering, Al-Azhar University

Abstract—In this research a Face Detection and Recognition system (FDR) used as an Authentication technique in online voting, which one of electronic is voting types, is proposed. Web based voting allows the voter to vote from any place in state or out of state. The voter's image is captured and passed to a face detection algorithm (Eigenface 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 number is used to retrieve and return his saved photo from the database of the Supreme Council elections (SCE) which is passed to the same detection algorithm (Eigenface 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 wither 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. If he has right to vote then a voting form is presented to him.

The result shows that the proposed algorithm capable of finding over 90% of the faces in database and allows their voter to vote in approximately 58 seconds.

Keywords—Electronic Voting; Face Recognition; Gabor Filter; Eigenface.

I. INTRODUCTION

Online voting system is a voting system in which the election data is recorded, stored and processed primarily as digital information and it needs to address, obtain, mark, deliver, and count ballots via computer. Therefore voter identification and authentication techniques are essential for more secure platform mechanisms to overcome vulnerabilities of the client used by the voter to cast her vote.

Security can be achieved using some of techniques of electronic voting such as *Guidelines*, only need to develop a list of instructions and then send it via email or put it on the election web page; *Bootable CD*, approach to overcome the secure platform problem was proposed by Otten (2005). She recommended developing a special voting operating system based on Knoppix. It is an operating system based on Debian that is designed to be booted and run directly from a CD or DVD; *Smart Cards as Observers*, in which an observer is a manipulation resistant piece of hardware which is owned by the voter. The idea is that the observer is not allowed to directly communicate with the Internet. All the communication needs to be forwarded by the voter; *Code Sheets*, the idea of code sheets is that the voter gets a piece of paper together with the general election information via post where each candidate or each party is linked to a particular code. Now, in order to cast a voter the voter does not click on the candidate or party of her choice but enters the corresponding code; *Trusted Computing*, the idea is to use an appropriate security architecture based on a security kernel and on Trusted Computing elements. Such a solution is the only one that could efficiently overcome malicious software on the voting casting device as well as potential malicious voters installing malware on purpose on their device. However, currently, there are still open problems with Trusted computing itself and it is not wide-spread enough; *Individual Verifiability* [5], the idea is that you use one software to prepare a voter and a second one to verify that the vote has been properly prepared (encrypted). Plus, you can also do the verification with an offline tool

In this research, we proposed an authentication technique using a Face Detection and Recognition system in online voting to achieve the rules of Supreme Electoral Council as follow: Only eligible persons vote, No person gets to vote more than once, the vote is secret, and each (correctly cast) vote gets counted and to achieve the aims of online voting as follow: increase participation, lower the costs of running elections, and improve the accuracy of results.

In general, an FDR system starts by Interfacing with an image source for grabbing facial images, Automatic detection or manual selection of human face may be found within the scene, Manipulate (create, add, delete) a database of faces, Launching the recognition process by comparing the face previously detected with the database's faces.

The remainder of this paper is organized as follows: Section 2 is devoted to mention the previous related work. In Section 3, explain the proposed algorithms (Gabor filter and Eigenface). Experimental results and comparison between two algorithms in Section 4. Finally concluding remarks are drawn in Section 5.

II. RELATED WORK

In related research, several voter identification and authentication techniques were introduced to secure voting platforms and overcome fake voting. Some of these techniques are:

Highly Secure Online Voting System with Multi Security using Biometric and Steganography, the basic idea is 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 [9].

Karlof et al., combines the verifiability definition without distinguishing universal or individual as follows: "Verifiably cast-as-intended means each voter should be able to verify his ballot accurately represents the vote he cast. Verifiably counted-as-cast means everyone should be able to verify that the final tally is an accurate count of the ballots." [11]

Online Signature Verification Using Temporal Shift Estimated by the Phase of Gabor Filter, A new online signature-verification method using temporal shift estimation is presented. Local temporal shifts existing in signatures are estimated by the differences of the phase outputs of Gabor filter applied to signature signals. An input signature signal undergoes preprocessing procedures including smoothing, size normalization and skew correction, and then its feature profile is extracted from the signature signal. A Gabor filter with the predetermined center frequency is applied on a feature profile, and phase profile is computed from the phase output. The feature profile and the phase profile are length normalized and quantized so that a signature code of fixed size is generated. The temporal shifts existing between two signatures are computed by using the differences between the phase profiles. The information about the temporal shifts is used as offsets for comparing the two feature profiles. Therefore, two kinds of dissimilarities are proposed. Temporal dissimilarity is a measure reflecting the amount of total temporal disturbance between the two signatures. The difference between the two signature profiles is computed at each corresponding point pair and is accumulated into temporally arranged feature profile dissimilarity. The decision boundary is represented as a straight line in the dissimilarity space whose two axes are the two dissimilarity measures. The slope and the position of the decision boundary are computed using the distribution of the dissimilarities among the sample signatures involved in the enrollment procedure [9], [11].

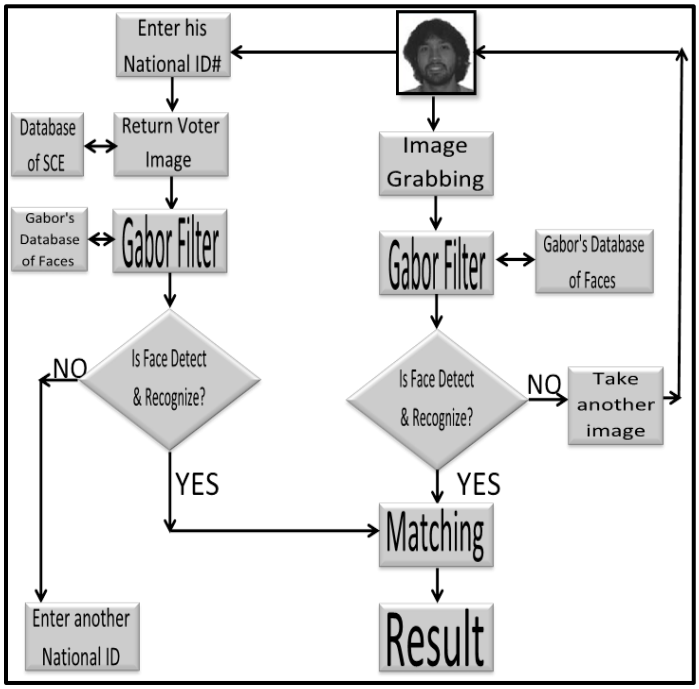
III. IMPLEMENTATION

Identity authentication applied for online voting system: The Online Voting System is an online application designed to be operated by two users, the election controller or administrator and the voter.

"Identity Authentication" generally involves two stages: the first is Face Detection and Recognition, where a photo is searched to find any face in it. Next, an image processing algorithm is applied to clean up the facial image for easier recognition. The second stage is Face Matching, where the detected face is compared to an image retrieved from the SCE database using a national ID#. A matching algorithm is applied to verify the person for both matching.

We compared between two Identity Authentication algorithms. The first algorithm is face recognition using Gabor filter and the second algorithm is Face Recognition with Eigenface.

A. ***First algorithm****, a schematic diagram for the Online Voting System Based on Face Recognition using Gabor Filters is show in Figure 1.*



Online Voting System Based on Face Recognition using Gabor Filters.

Algorithm steps are as follows:

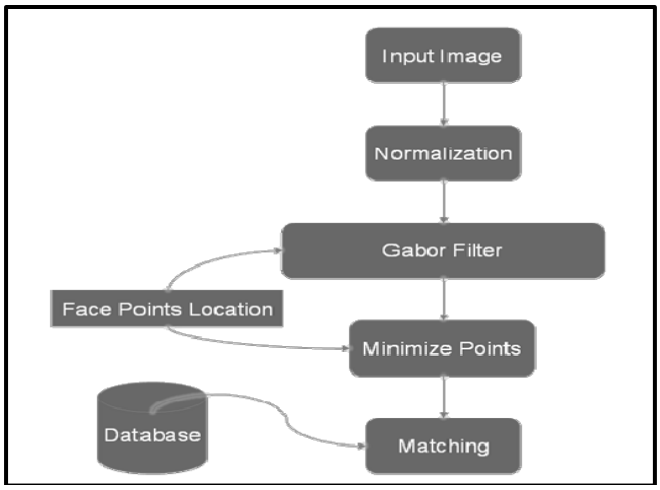
1) The voter's image which is captured using a webcam is used as the input to the face detection algorithm.

2) Before entering image to Gabor filters, it must be normalized by three steps as show in Figure 2.

a) Input image is resized to 128×128.

b) Pixel adjustment, in this step, Image Pixel intensities are used, such that the standard deviation of Image Pixel is one.

c) Borders are smoothed, across band 30 pixels wide and they are weighted by an aspect d= 30, where d is distance of image edge.



Normalize image

3) Gabor filter algorithm consists of 40 filter used to detect faces from the captured image; the proposed system applied different Gabor filters on the image to generate 40 images with different angles and orientation [1] [2] [8].

4) Next, maximum intensity points in each filtered image are calculated and marked as fiducial points. If the distance is minimum between these face points then system reduces the points. The next step is calculating the distances between the reduced points using distance formula. At last, the calculated distances are compared with Gabor database. If match occurs, it means that the image is recognized as a face.

5) Eq. (1) shows the major expression of Gabor wavelet as a Gaussian kernel function which is changed by sinusoid [1].

$$W(x,y) = \mathcal{F}e^{-\frac{x'^2+y'^2}{2x^2}}(\cos(2\pi\mathcal{F}x' + \theta) - DC) \quad (1)$$

Where,

$$DC = \cos\theta\, e^{-2\pi\frac{e^2}{\mathcal{F}^2}}$$

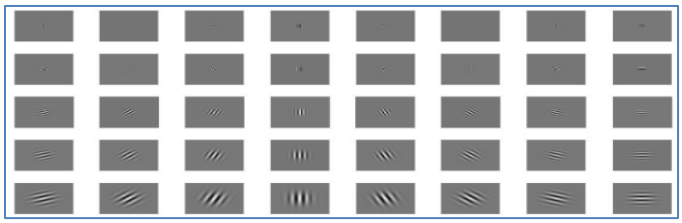
And,

$$x' = x\cos\theta + y\,sin\theta,$$
$$y' = -x\sin\theta + y\cos\theta$$

The factor $F=\sigma/K$ makes sure the filter spatial range of action is partial correspondingly to the central frequency f. In this equation σ is frequency of filter, θ are 8 different orientations in the filter. A discrete recognition of Eq. (1) using five dissimilar scales and eight angles are engaged and in result of it, 40 Gabor filters are acquired. In the end of Eq. (1), the term *DC* creates the filter *DC*-free.

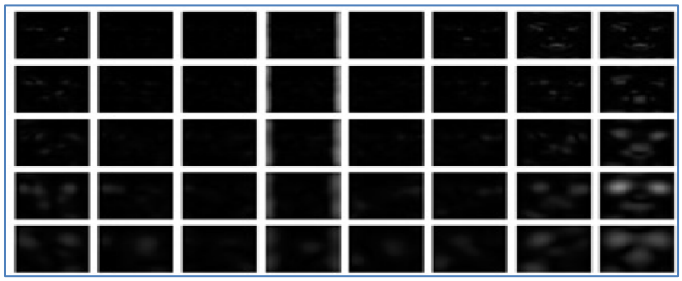
6) Then, Gabor filters are applied on the input images

a) Gabor Filters: an image of the 40 Gabor filters are shown below in figure 3.



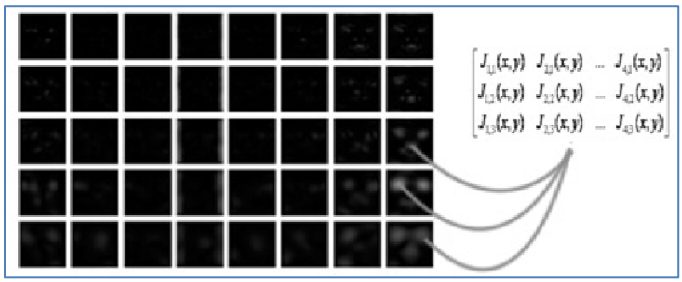
Gabor Filters

b) Results of applying Gabor Filter on image show in figure 4.



Result of applying Gabor Filter

c) Face point extraction, When the original image I(x, y) multiplied with Gabor filter g(x, y), a new image is acquired which is equal to J(x, y). Where x is height and y is width of image show in figure 5.



Face point extraction

d) Find the maximum intensity face points using the formula in Eq. (2).

$$\sum_{i=1}^{N1}\sum_{j=1}^{N2}(\max(x_{ij})) \quad (2)$$

Where:

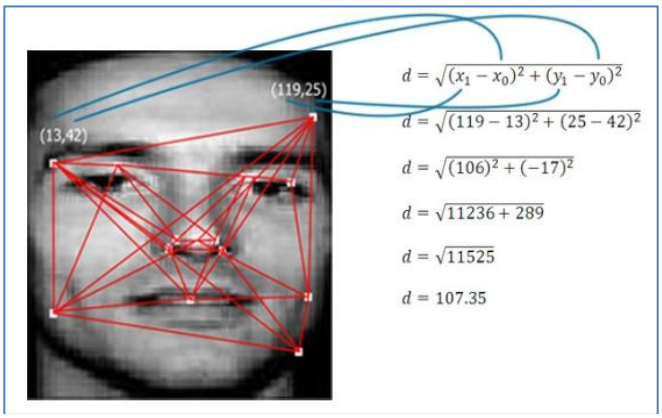
$$X = I_{ij}$$

$$I = Intensity\ at\ coordinate\ i,j$$

Where *N1, N2* are the width and height of image.

e) Calculate the distance d to minimize the points as in Eq. (3).

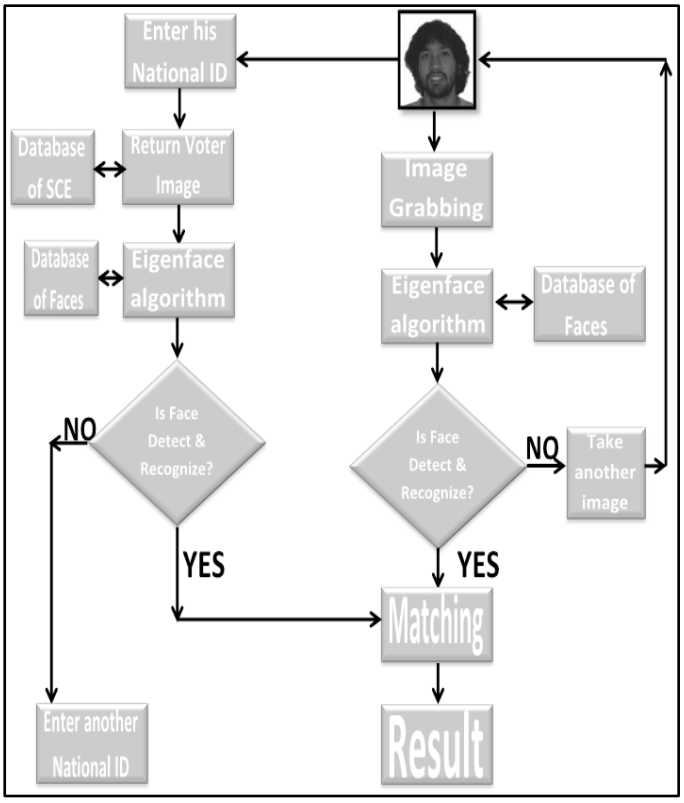
$$d = \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2} \quad (3)$$



Calculate of distance d

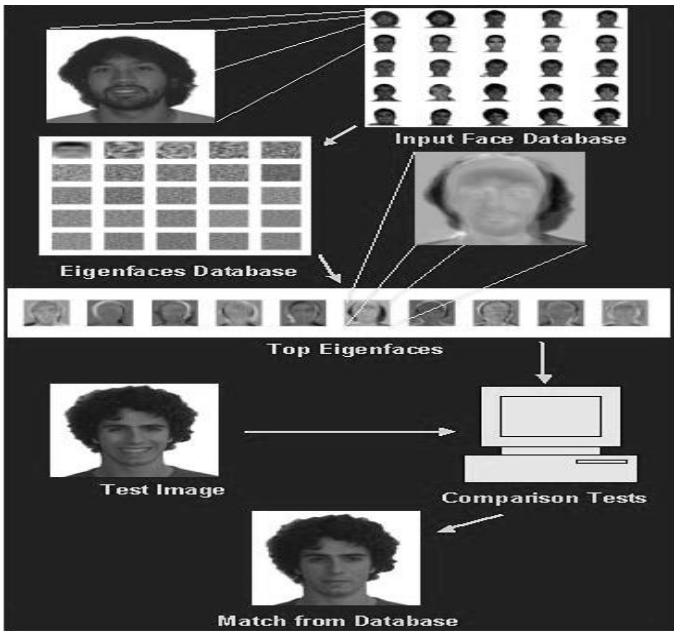
f)The distances of the selected points which show in figure 6 are compared with the database; if the distances get matched with database the face is recognized.

B. ***Second algorithm***, *Online Voting System Based on Face Recognition using Eigenface Filters. The suggested system is illustrated in figure 7.*



Online Voting System Based on Face Recognition using Eigenface system.

We used Eigenface system to detect and recognize face from image; this system can be divided into two main segments: creation of the Eigenface basis and recognition of a new face [3] [10]. The system follows the following general flow as show in figure 8.

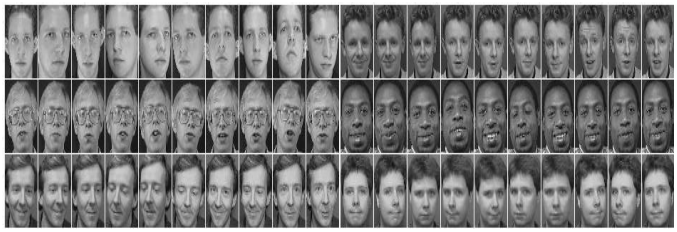


The Eigenface face recognition system segments.

The Eigenface technique uses much more information by classifying faces based on general facial patterns. These patterns include, but are not limited to, the specific features of the face [7]. Eigenface can be related directly to one of the most fundamental concepts in electrical engineering: Fourier analysis.

Eigenface system needs a database of known faces in which all images are the same size (in pixels), and grayscale, with values ranging from *0* to *255*. Each face image is converted into a vector of length *N* (where, *N=image width*image height*).

We will use The ORL Database of Faces (AT&T database) [6]. This database contains 400 pictures of 40 subjects. A preview image of the database of faces is shown in figure 9.



A preview image of the Database of Faces.

Eigenface system use of Fourier analysis reveals that a sum of weighted sinusoids at differing frequencies can recompose a signal perfectly. In the same way, a sum of weighted Eigenfaces can seamlessly reconstruct a specific person's face. The algorithm calculates the average face in face space and returns the top Eigenface vectors then it uses these differences to compute a covariance matrix *C* for our dataset. The covariance between two sets of data reveals how much the sets correlate [4], [7] as in Eq. (4).

$$C = \frac{1}{M}\sum_{n=1}^{M}\Phi_n\Phi_n^T = \frac{1}{M}\sum_{n=1}^{M}\begin{pmatrix} var(p1) & \dots & cov(P1,PN) \\ \vdots & \dots & \vdots \\ cov(PN,P1) & \dots & var(PN) \end{pmatrix}_n = AA^T \quad (4)$$

In Equation 4,

$A = [\Phi_1\ \Phi_2 \dots \Phi_M]$,

pi = pixel i of face n,

M= the number of faces in our set.

The Eigenfaces that we are looking for are simply the eigenvectors of C. However, since C is of dimension N (the number of pixels in our images), solving for the Eigenfaces gets ugly very quickly. Eigenface face recognition would not be possible if we had to do this. This is where the magic behind the Eigenface system happens.

The output of the Eigenfaces system is the first point extraction of the person's face which we will be used to verify the voter's identity. The voter will enter his ID number which is used to fetch his image from SCE data base this image will be considered as the first point. The voter's image captured using a webcam is the input to the Eigenface system to detect the face from image and this will be the second point. The two points are checked for matching using pattern matching algorithm.

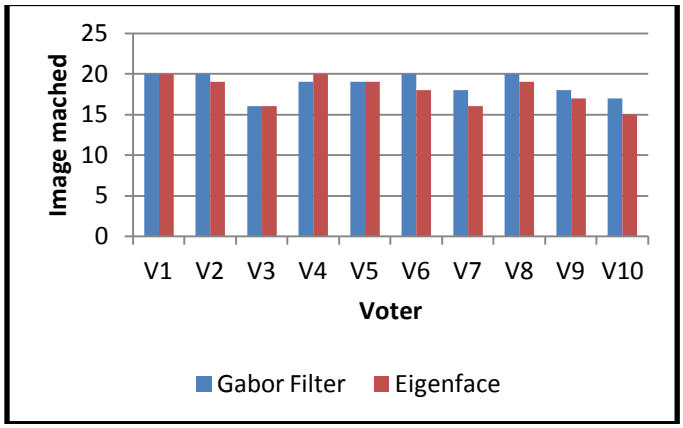
IV. Analysis

To measure the performance of the two proposed systems (Gabor filter and Eigenface algorithm) the standard database and SCE data base were used. The number of matched images and the execution time were calculated and used to compare between the two proposed systems.

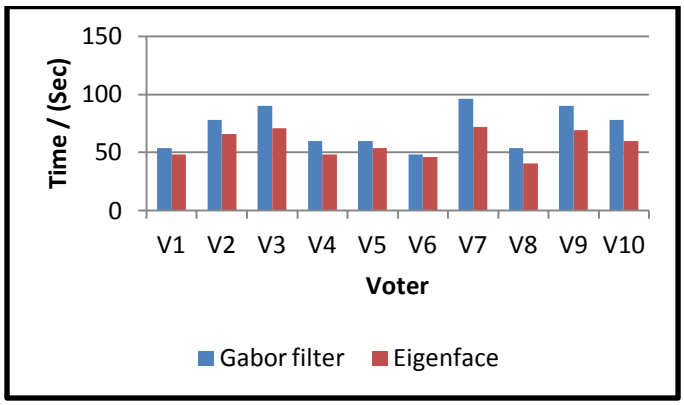
Images for ten different persons were used. For each person 20 images in different positions and different facial expressions were saved in the database. The proposed Gabor filter system was tested using 200 images. For each person 20 different images were tested. Figure 10, 11 represent the number of matched images and the average execution time respectively for both Gabor filter system and Eigenface system.

It has been observed that in the absence of face-facing webcam or in the case the of a rotated face captured image the efficiency of the Gabor filter algorithm is 80% as in the cases of voters 3, 7, 9 and 10.

While, in a face- facing webcam or a no rotated face the efficiency raises up to 100% as in the cases of voters 1, 2, 6, 8. And the efficiency of the Eigenface algorithm is 75% as in the cases of voters 10. While, in a face- facing webcam or a no rotated face the efficiency raises up to 100% as in the cases of voters 1.



Number of images matched for every voter.



Execution time for every voter.

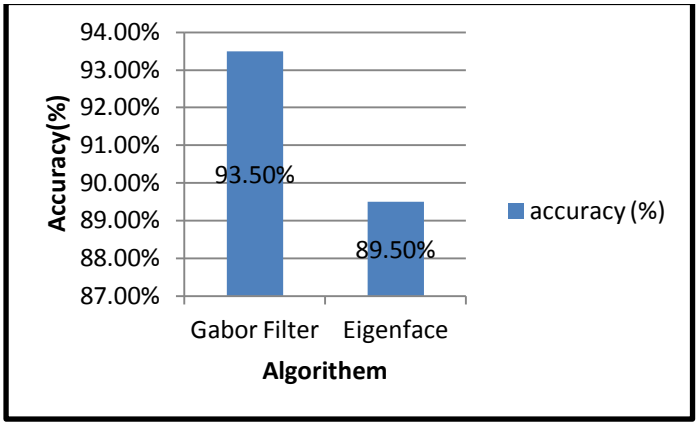
The results showed a 93.5% match in an average 70.8 Second for Gabor system. The same test set of images was used by the Eigenface system and resulted in 179 images were matched and 21 were not matched in an average of 57.48 Second. Total results are shown in figure 11, 12.

In cases of Eigenface, the recognition rates for a given number of Eigenfaces are reached relatively quickly. This indicates that in any implementation of such a recognition system there does not exist a meaningful advantage to using more Eigenfaces than first provide the desired level of accuracy and speed.

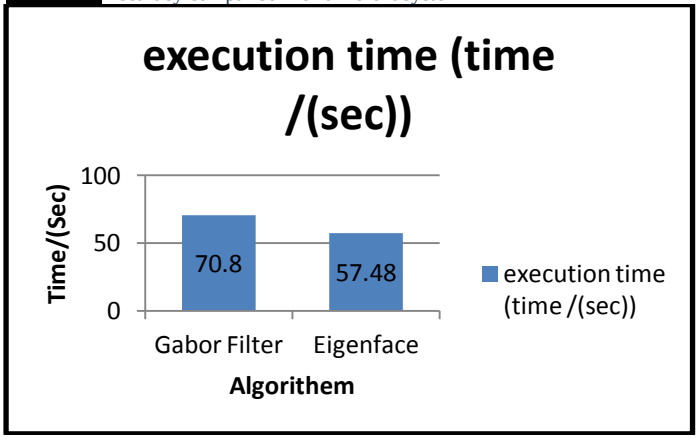
V. Conclusion

On line voting allow voter to vote 24 hour per day and 7 day per week also allow him to vote from anywhere in his state or out of state.

In this research, we proposed two FRD systems based on Gabor and Eigenface as authentication techniques in online voting. Both systems detect the face from an image captured using a webcam and recognize face from SCE database and check if the two images match. If a match accrues, then verify that the law and roles of voting are not violated then allow him to vote.



Accuracy comparison for different system



Execution time comparison for different system

Analysis of the Eigenface recognition technique using both averaging and removal methods gives evidence that the methods prove 89.5% accurate. But we achieve 93.5% accurate when we applied Gabor filter, but it take more time to recognize face from image.

In future work, we plan more extensive experimentation with a larger images database. We also plane on trying other good performance face detection and matching algorithms in aim to increase algorithm efficiency and improve execution time.

References

[1] Face Recognition using Gabor Filters, Muhammad SHARIF, Adeel KHALID, Mudassar RAZA, Sajjad MOHSIN, Department of Computer Sciences, COMSATS Institute of Information Technology, Wah Cantt-Pakistan J.

[2] Face Detection using Neural Network & Gabor Wavelet Transform, Avinash Kaushal1, J P S Raina2, 1GCET, Greater Noida, U.P., India; 2BBSBEC, Fatehgarh Sahib, Punjab, India.

[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] Oppliger, R., & Schwenk J., & Helbach, J. (2008). Protecting Code Voting Against Vote Selling. In A. Alkassar & J. H. Siekmann (Eds.), Sicherheit 2008; 128, 193–204.

[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, from http://fee.iavoss.org/2006/papers/fee-2006-avossEnabling_the_application_of_open_systems_like-PCs_for_Online_Voting.

[6] http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html.

[7] http://www.clear.rice.edu/elec301/Projects99/faces/index.html.

[8] Novel Face Detection Method Based on Gabor Features, ie Chen1, Shiguang Shan2 1 2, Peng Yang2, Shengye Yan2, Xilin ChenSchool of omputer Science and Technology, Harbin Institute of Technology, 50001, China ICT-ISVISION JDL for AFR, Institute of Computing echnology, CAS, Beijing, 100080, China 1 and, Wen Gao1,2

[9] Highly Secure Online Voting System with Multi Security using Biometric and Steganography J. Cross Datson Dinesh Assoc. Prof. Dept of Computer Science and Engineering Rajalakshmi ngineering College #2 Chennai, India

[10] http://aicat.inf.ed.ac.uk/category.php?id=12

[11] Verfication And Validation Issue In Electronic Voting. Orhan cetinkaya[1], and deniz cetinkaya[2]. [1]institute of applied mathematics, METU, Ankara, turkey. [2] computer engineering , METU , ankara , turk