# A Secure and Authenticating E-Voting System Using Multiple Biometrics

## Kadhim Hasen Kuban[1], Fatimah Ajeel Dhaher[2]

Computer Department. College of Education for pure science University of Thi - Qar, Thi - Qar. Iraq

**Abstract:**

This study suggested design and implementation biometric-based electoral system for Iraqi state institutions and its political system. The proposed system employs automated methods of identifying and authenticating the identity of a voter based on his/her face image and fingerprints. Using face and fingerprint, ease of acquisition and high matching accuracy made them suitable for biometric application. The system consists of two phases: the voter registration phase and the verification phase that is activated on the Election Day. Voters interacting with the system through graphical user interface, which gathers their data in different databases to reflect their functions. Flexible and user-centric design methodologies have been adopted. The system was designed using Python programming language, MySQL database server and Apache web server in addition to some other descriptive languages as PHP. The implementation of this system shows that the integrity of the Iraqi Electoral Process can be greatly enhanced in the state instead of the previous election system.

Keywords: php(mysql), Dlib library, Python Fingerprint Recognition, DNN, SIFT.

## 1-Introduction:

"The electoral process has emerged since the eighteenth century. The electoral process is a process adopted by countries that follow democratic systems. A group of people aged 18 years or older who are eligible to participate in the electoral process selects persons holding key positions in the state, such as the president, prime minister and members. Parliament and others. Elections can be used by informal institution at the local level [1].

"The electoral process allows people to choose their representative and express their desire for their own governance. Of course, the integrity of elections is essential to the integrity of democracy itself [2].

In the context of Western countries, the process of electronic election has become a common theme in academic and technical circles. Voting is the way voters are helped to make decisions or to choose a person who represents them. This is often done after debates, debates or election campaigns. The term electronic voting includes several different types of voting, including electronic means of voting and electronic means of counting votes [3]. Voters express their will through means of electronic registration systems by placing a mark directly into the electronic device through a touch screen or pressure buttons or a keyboard that allows the voter to cast his vote. Biometric techniques use automatic methods to identify or document a person's identity based on physiological and behavioral characteristics [4].

The electoral system or the voting system must be sufficiently secure to be robust to resist a different set of fraudulent behaviors and must be transparent and inclusive so that both voters 2
and candidates are confident of the integrity of the election results [5]. Automatic fingerprint recognition is one of the most reliable biometric techniques [6].

The biometric voting system for voter identification and documentation uses an excellent impression. Therefore, the app will not accept all hacking, illegal and duplicate votes, and the election results will be highly credible [1].

Biometrics has become an essential element in the identification solution, where identifiers cannot be misplaced and represent any individual identity. Identification refers to the use of the iris, fingerprints, face and speech properties called biometric identifiers

In recent years, face recognition plays an important role in intensive research with the current global security situation is distinctive, Requiring Governments as well as the private sector reliable methods to identify individuals accurately without overlapping or conflict with privacy rights or require significant compliance by the individual is being recognized.

In this paper we will propose a safe and sound voting system using powerful biometric methods such as face recognition and fingerprinting. Voting is a public voting system deployment to make the electoral process system safe, fast and the results will be crystal clear and concise for all questions such as time delay, counting, security, high reliability and the absence of any false retrial. The main concept behind this paper is to provide additional security power using various biometric techniques such as facial recognition technique to scan the face, then the system to detect the stored face of the voter in the database. Then fingerprint this voter to achieve matching in order to give more security, after recognizing the faces, the fingerprint is checked. And whether the voter is allowed to vote if they are identical or repeal. After voting, the number of votes is updated automatically"[7].

## 2-Related Work:

" There is a set of studies in the establishment of a biometric voting system, Zinah J Mohammed Ameen (2018) [8] proposed a secure E_Voting application based on face recognition and ciphering. The RSA public key algorithm proposes to encrypt the voter's choice, and then relies on a secret key assigned to each voter with the image of the instantaneous voter entered. Encrypted data is encrypted using the RSA algorithm again before being sent to the server using propagation spectrum information dissemination technology."

"A. piratheepan et al, (2017) [9] fingerprint voting system using Arduino technology. In this system, all voter information is stored. The voter must complete the registration form with the help of user ID and password. This information will be checked by the database server. Because all information about the voter will already exist and all using Arduino technology".

" Syed Shahram Najam et. al. (2018) [10] the facial recognition system uses the Fiola Jones algorithm along with the method of choosing Haar's rectangular feature to detect and extract features to develop a biometric template and extract the feature during the voting process. v

## 3-Proposed System Architecture:

As mentioned earlier that the establishment of an integrated electoral system goes through several stages. The Figure.3 outline shows the important steps in the implementation of the system. The proposed system consists of two main stages: -

**Journal of Education for Pure Science- University of Thi-Qar**
**Vol.10, No.1 (March., 2020)**
*Website: jceps.utq.edu.iq*                                    *Email: jceps@eps.utq.edu.iq*

## A-Registration stage: -3

Every person who has attained the age of 18 years is entitled to participate in the elections, Therefore, the Independent High Electoral Commission is updating the electoral register and this process requires the obtaining of face and fingerprints image for each voter Then the voter card is issued, Each card has a unique number and through this card you can know the constituency of the voter in addition to all personal information. This stage is shown in Figure.1.

The registration stage is one of the most important stages in the proposed electoral system because the voting stage depends on it mainly

Four basic information is provided for each voter in the registration phase, as follows:

**1- ID-Voter: -** Which is the primary key to the voter table, where it is unique for each voter and through which access to other voter data with ease so that it helps in the process of checking the voter data in both stages of registration and election and here the matching through one to one, which in turn helped to speed the performance of the system and give results high precision and speed in matching.

**2- Finger print: -** Take the fingerprint of each voter, train it and store the trained fingerprint in the database.

**3- Face image: -** Take a picture of the voter's face and store it in special templates in the database.
The recording stage is illustrated in the figure.1
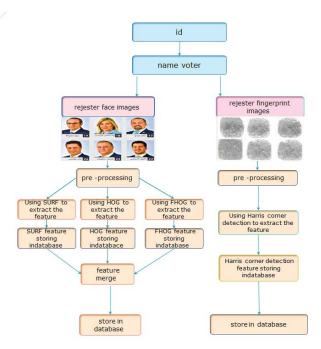Figure (1) represent the first stage Registration stage)



**Figure (1) represent the first stage Registration**

## B- Voting stage: -

The verification phase or the voting stage is activated on election day, the stage requires the election number (ID) If it is true, the image of the face and the fingerprint of one of the voters are requested, if both metrics are correct, the voting process is available to this voter and not excluded from the process. This stage is shown in Figure.2
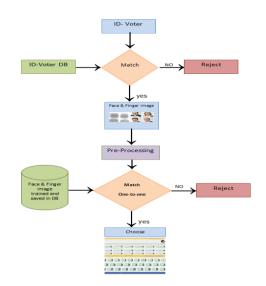
**Figure (2) represent the second stage (Voter stage)**

We note in the Figure.2 that the header of the input is the voter ID because the voting process will depend on it in the validity of the voter to enter the electoral page and access to the voter's data and audited. Here are many statistical processes to collect the votes of the lists and candidates that are linked to the tables of databases(Mysql).
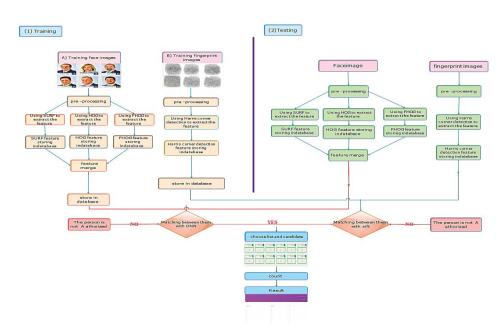


**Figure (3) the block diagram of proposed system**

**4- Face and fingerprint image processor:**

Facial and fingerprint image processing and database building are done using:

**4.1 Dlib C++ Library [11]**

" "Dlib may be a trendy(C++) toolkit containing machine learning algorithms and tools for making advanced software system in(C++) to resolve planet issues. it's employed in each business and domain during a wide selection of domains as well as artificial intelligence, embedded devices, mobile phones,

and huge high performance computing environments. Dlib's open supply licensing permits you to use it in any application, freed from charge, to process images in(Dlib) library, follow the steps below:"

1-Routines for Reading and Writing common image formats.

2-Automatic Color space conversion between Various pixel types.

3-Common Image Operations such as edge finding and Morphological operations

4-Implementations of the SURF, HOG, and FHOG Feature extraction Algorithms.

5-Tools for detecting Objects in images including frontal Face detection and object pose Estimation

6-High quality face recognition".

Figure (3) the block diagram of proposed system 6

## 4.2 Face Image recognition using DNN:

To recognize the faces, we adopted **DNN** a very high way of recognition, which is one of the fastest ways to recognize the faces. Face features are extracted using **SURF, HOG** and **FHOG** (face template)

| Algorithm(1): DNN Recognition |
|---|
| Input: Face template |
| Output: 1: match OR 0 : not match |
| Begin<br>" Step One: - input: f=x= (x1, x2, xn) denotes data matrix of n samples Y= (Y1, Y2, Yn) T as their corresponding output labels, the maximum number of selected attributes K.<br>Step Two: Initialize: S={bias}, C=F and WC= 0<br>Step Three: -While /S/ <= k+1 do<br>Step Four: - Assign Wc (candidate weights) = 0.<br>Step Five: - Update weight of hidden layers as well as input weight WC.<br>Step Six: - Multiple Time Drop out to be used and then obtain average GFC<br>Step Seven: - calculate j=arg ma ‖ GFC ‖g<br>Step Eight: - update learning rates using AdaDelta.<br>Step Nine: - Initialize WFj with Xavier initialization<br>Step Ten: - perform S=SUF and C=C\ F"<br>End Algorithm |

## 4.3 Python Fingerprint Recognition [12]

"Fingerprint recognition with (SKimage) and (OpenCV) Requirements:

. NumPy

. SKimage

. OpenCV

_Works by extracting mminutiae points Using (Harris corner detection).

_Uses (SIFT) go get formal descriptors around the Keypoints with brute-force Hamming distance and then analyzes the returned Matches using thresholds.

usage:

1-Place two fingerprint Images that you want to compare inside the Database folder

2-Pass the names of the Images as arguments in the console"

### 4.5 Fingerprint Image recognition using SIFT [13]:

After extracting Harris features we will distinguish the fingerprint using SIFT by as shown in Algorithm.

| Algorithm(2): SIFT Recognition |
|---|
| Input: Harris corner detection feature |
| Output: 1: match OR 0 : not match |
| Begin<br>" Step One: - Scale-space extreme detection<br>Step Two: -Keypoint Iocalization:<br>-Interpolation of nearby data for accurate position.<br>-Discarding low-contrast keypoints<br>- Eliminating edge responses.<br>Step Three:-Orientation assignment.<br>Step four: - Keypoint descriptor"<br>End Algorithm |

### 5- Software Used:

Database Programming in Python from a construction firm to exchange, each organization depends on massive databases. These are basically collections of tables, and' connected with one another through columns."These database systems support (SQL), the Structured query language, that is employed to make, access and manipulate the data. (SQL) is employed to access data, and additionally to make and exploit the relationships between the keep data. additionally, these databases support database standardization rules for avoiding redundancy of data. The Python programing language has powerful options for database programming. Python supports varied databases like (MySQL), Oracle, Sybase, PostgreSQL, etc. Python additionally supports data Definition Language DDL, data Manipulation Language (DML) and data question Statements. For database programming, the Python dB (API) could be a wide used module that has a database application programming interface [14]"., Technique is adopted client-server architecture It includes the following:

1-Databases Server(php), (mysql) is popular database system used with(PHP).

2-Languages for image processing(python).

3-Web server(apache).

4- Implement the system using Dell laptop platform with processor Intel(R) Core(TM) i5-7200U CPU@ 2.50 GHz 2.60 GHz, and RAM 8.00 GB.

5- User Interface React.

6- Analytical and experimental results of the system used in the recognition and verification of faces and fingers

Threshold = 0.6 (face image)

Threshold = 0.4 (fingerprint)

K = represent loop of set images one person. Take the first image (1) and match it

with the rest of the images for the same person (each person has 8 images).

No1. of Coff. = Number of people and here we have 200 people, (each person has 8 images).

No2. of Coff. = Number of people and here we have 50 people, (each person has 10images).

Match = The number of times he got a match.

Accuracy = Represents the percentage of face recognition accuracy which is the number of matches divided by the number of people.

$$\text{Accuracy} = \frac{\text{The number of matches}}{\text{The number of people}} \times 100$$

| K | No1. of Coff. | FRR% | Match Rat |
|---|---|---|---|
| 1 | 2 | 0 | 100 |
| 1 | 4 | 25 | 75 |
| 1 | 25 | 4 | 96 |
| 1 | 125 | 508 | 99 |
| 1 | 158 | 102 | 98.7 |
| 1 | 164 | 102 | 98.7 |
| 1 | 167 | 107 | 98.2 |
| 1 | 180 | 106 | 98.3 |
| 1 | 200 | 105 | 98.5 |

**Table.1 shows that when K was taking only the first image and matching it with**

the rest of the images 8 accuracy=98.5%.
But if we make K=8 take the first if it does not match take the second and so it will be accuracy =100%. As shown in Table.2

| K | No1. of Coff. | FRR% | Match Rat |
|---|---|---|---|
| 1 | 2 | 0 | 100 |
| 2 | 4 | 0 | 100 |
| 1 | 25 | 0 | 100 |
| 1 | 125 | 0 | 100 |
| 2 | 158 | 0 | 100 |
| 1 | 164 | 0 | 100 |
| 2 | 167 | 0 | 100 |
| 1 | 180 | 0 | 100 |
| 1 | 200 | 0 | 100 |

**B-Fingerprint:**

**The table (3) represents the results obtained from matching 50 people all person has 10 fingerprint**

| No2. of Coff. | FRR% | Match Rat |
|---|---|---|
| 4 | **0** | **100** |
| 14 | **1.7** | **92.8** |
| 24 | **4.1** | **95.8** |
| 34 | **5.8** | **94.1** |
| 39 | **5.1** | **94.8** |
| 44 | **6.8** | **93.1** |
| 45 | **6.6** | **93.3** |
| 49 | **6.1** | **93.8** |
| 50 | **6** | **94** |

Accuracy=94.0% &Total time =5.819349 seconds

**6- CONCLUSIONS AND FUTURE WORKS:**

1- Our proposed electronic electoral system will contribute to the participation of as many voters as possible in the electoral process so as to facilitate access to the electoral system, whether in the registration of their data or cast their votes with ease.

2- Designad a smooth electoral system which enables all different cultural classes to use the electoral system with ease.

3- In all countries of the world and in all institutions and in all elections in general, which uses paper elections in particular there is fraud and manipulation of votes, in our electronic electoral system here and provided an integrated electoral system up to high security as thereliance on electronic measurements and the use of methods of discrimination in Identification of face and fingerprint ( DNN ,SIFT), which are of the most important and most accurate methods of discrimination in the present time contributed to the strengthening of the electoral system significantly.

4- The fact that the election results are announced immediately after the electoral process will strengthen the confidence of the voter and encourage him to cast his vote.

5- Verifying the possibility of using the proposed electronic electoral system on the ground and benefited from the state, institution and organizations.

**References:**

 [1] McGrath, K., & Maiye, A. (2010). The role of institutions in ICT innovation: learning from interventions in a Nigerian e-government initiative. Information Technology for Development, 16(4), 260-278.

[2] Aishwarya A. S., Prashant P. (2015). Biometric Voting System with Centralized Database. [Online]. Available: http://www.iosrjournals.org/iosr-jeee/Papers/Vol10-issue4/Version-3/N010438890.pdf. (Accessed on 17th June, 2018). [3] Nwangwu, C. (2015). Biometric voting technology and the 2015 general elections in Nigeria. Department of Political Science, University of Nigeria, Nsukka.

[4] Oluwatosin A. (2015). Online Voting System with Biometric Authentication for UiElections. [Online]. AvailableHttps://Www.Researchgate.Net/Publication/310597883_Online_Voting_System_with_BiOmetric_Authentication_for_UI_Elections. (Accessed on 2nd December, 2017).

[5] Eduardo I., Nicolás G., Cesar E., Ariel P., Franco C., Ismael R., Patricia P. (2010). Biometric identification in electronic voting systems. [Online]. Available: https://pdfs.semanticscholar.org/276f/3e0a884635e85da647f70f3353d3ba5bfa74.pdf. (Accessed on 6th April, 2018).

[6] Thang K. F. (2008). Biometric-Secure E-voting System for Election Processes. [Online]. Avalaible: file:///C:/Users/Longe/Downloads/A_biometricsecure_evoting_system_for_election_pr.pdf.   (Accessed on 26th January, 2016).

[7] Patil Rahul H., TarteBabita B., Wadekar Sapana S., Zurunge Bhakti S.and Prof. Phursule Rajesh (2017)." A Secure E-Voting System Using Face Recognition and Dactylogram". Student at JSPM's ICOER, Wagholi, Pune - 412207, India. (IERJ). VOLUME 2, ISSN 2395-1621. (2017).

[8] Zinah J Mohammed Ameen. (2018)." Secure Electronic Voting Application Based on Face Recognition and Ciphering". Computer Engineering Department, University of Technology, Baghdad, Iraq. ISSN Online: 2474-9257.11

[9] A. Piratheepan, S. Sasikaran, P. Thanushkanth, S. Tharsika, M. Nathiya, C. Sivakaran, N. Thiruchchelvan and K. Thiruthanigesan. (2017)." Fingerprint Voting System Using Arduino". College of Technology Jaffna, Sri Lanka. Middle-East Journal. ISSN 1990-9233.

[10] Syed Shahram Najam, Aamir Zeb Shaikh, and Shabbar Naqvi. **"A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition".** Department of Electronic Engineering, NED University of Engineering & Technology, Karachi, Department of Computer Systems Engineering, Baluchistan University of Engineering & Technology, Khuzdar. Mehran University Research Journal of Engineering & Technology. Volume 37, [p-ISSN: 0254-7821, e-ISSN: 2413-7219]. (2018).

[11] " Dlib C++ Library " . http://dlib.net/

[12] "Kjanko/ Python Fingerprint Recognition", https://github.com/kjanko/python-fingerprint-recognition

[13] Unsang Park, Sharath Pankanti, and A. K. Jain(2008)." Fingerprint Verification Using SIFT Features" . IBM T. J. Watson Research Center, Hawthorne, NY, USA 10532; Dept. of Computer Science & Engineering, Michigan State Univ., East Lansing, MI, USA 48824. Orlando, Florida.

[14] " Database Programming in Python", https://opensourceforu.com/2019/04/database-programming-python/