ISSN (1681- 6870)

Secure E - Voting System using Voiceprint

Noor SH. Hameed nooruot1@gmail.com
Dr. Bashar M. Nema bashar_sh77@uomustansiriyah.edu.iq
Al Mustansiriyah University - College of Science - Dept. of Computer Science
Received 1/9/2019 **Accepted 28/9/2019**

Abstract: *Electronic voting systems are considered to be one of the modern systems that are widely used recently. The great challenge which is facing researchers in this field is how to verify the voter. This paper discussed and implemented online secure E- voting system depends on speech recognition. The proposed system represents a very important stage in identity of the voter personality. The researcher used voiceprint feature (Pitch Detection), where the system included the recognition of voiceprint through the use of (MFCC) method, which proved a great success for sample of society that has been used in the proposed system. The researcher has faced many problems in dealing with human voice as a means of proof. The work required a set of processors for the sound signal (Preprocessing), the addition that the researcher has done is no intensive circumstances or special requirements for the of recording voice but, the system works through very normal circumstances as it has been benefited from merging and propose recording machinery and processing the voice by using hybrid way that using (framing and windowing). The results of voiceprint recognition with a ratio that is more than 98%. These results had a great role in achieving privacy and data integration for the later stages of the proposed system.*

Keywords: Electronic voting, Authentication, Feature extraction, Mel-Frequency Cpestral Coefficient (MFCC), Fast Fourier Transform (FFT).

نظام تصويت الكتروني امن بأستخدام البصمة الصوتية

نور شاكر حميد nooruot1@gmail.com
أ.م.د. بشار مكي العيساوي bashar_sh77@uomustansiriyah.edu.iq
الجامعة المستنصرية – كلية العلوم – قسم علوم الحاسوب

المستخلص

تعتبر أنظمة التصويت الإلكترونية واحدة من النظم الحديثة التي تستخدم على نطاق واسع في الآونة الأخيرة. التحدي الكبير الذي يواجه الباحثين في هذا المجال هو كيفية التحقق من الناخب. في هذه الورقة ، تتم مناقشة وتنفيذ نظام التصويت الإلكتروني الآمن عبر الإنترنت بأستخدام التعرف على الكلام. يمثل النظام المقترح مرحلة مهمة للغاية في تحديد الهوية الشخصية الناخب. هنا قام الباحث باستخدام خاصية البصمة الصوتية (Pitch Detection)، حيث تم تضمين منظومة تمييز البصمة الصوتية من خلال استخدام طريقة (MFCC) والتي اثبتت نجاحا كبيرا لعينة المجتمع المستخدمة في النظام المقترح. واجهت الباحث العديد من المشاكل اثناء التعامل مع الصوت البشري كوسيلة اثبات مما تطلب العمل على اجراء مجموعة من المعالجات لأشاره الصوت (Preprocessing)، الإضافة التي قام بها الباحث هو عدم وجود ظروف مشددة او متطلبات خاصة لتسجيل الصوت، وانما تعمل المنظومة في ظروف طبيعية جدا

ISSN (1681- 6870)

حيث تم الاستفادة من دمج واقتراح الية تسجيل ومعالجة الصوت باستخدام طريقة هجينة تستخدم طرق (framing & windowing). كانت نتائج تمييز البصمة الصوتية بنسبة تزيد على 98%. هذه النتائج كان لها الدور الكبير في تحقيق الخصوصية وتكامل البيانات للمراحل اللاحقة في النظام المقترح.

الكلمات المفتاحية: التصويت الالكتروني، المصادقة، استخراج المميزات، تحويل فورير السريع، ميل التردد.

1. Introduction

In the past few years, electronic voting has become commonplace and the importance of electronic voting has emerged because of the benefits of reducing human resources and traditional work. It is less corrupt and fraudulent and also allows anyone to vote remotely. the Internet voting Advantages over the common "queue method" is that voters vote during their free time but within the specified voting period and there is no need to wait .The purpose of a secure vote is to assure the confidentiality of voters and the accuracy vote and to assure the person's authorization.

E- Voting is a procedure by electronic device as computers and telecommunication technologies. Elections are so sensitive in expression of secure. [1] The application of E- voting will allow increased access to the voting process for millions of voters. In public, every electronic voting system consists of enrollment, authentication and authorization, voting, voting tallying and voting verification [2].

2. Theoretical background

In this section the explanation of Electronic voting, biometric, authentication, and classification, the discussion for voice recognition and stage preprocessing with the feature extraction and its classification.

2.1.Electronic voting

Electronic voting is a system wherein voting information is recorded and put away as a digital data. Voting just comprises of simple procedure or system which requires few workers for the process the E-voting may become the cheap, fast, and extreme efficient way to manage polling and count [3] . This system consists of two types of e-voting. The first type is offline using voting machine or an electronic polling booth. The second type is On-line voting which used via Internet [4]

2.2.Authentication methods

There are several issues facing electronic voting systems, which are the reason of system success or failure and the most important of these issues is security and privacy by making sure that the person who votes is the legitimate voter and not someone else and there are a number of security requirements of the electronic system must include the eligibility,, authentication, privacy, robustness. The eligibility means those who participate in the vote and cast their votes during the election period are eligible voters only .The authentication includes the person who votes is the same and not someone else Voter. Privacy is a very special way through protected personal information that no one can know. Robustness means the voting system is safe against any attacks or fraud. Finally, legibility, in announcing voting results only at the end of allowable voting period [5, 6, 7].

2.3.Biometric

Biometric measurements are used for identification and security authorization for more than two decades. This is because the biometric data of their qualities are unique and non-convertible. You cannot forget and own it with us. Recently, biometrics has been deployed in security applications that can be included under the topic of "biometric coding systems". Although the use of one type of

ISSN (1681- 6870)

biometric data is questionable in terms of safety, integration with other technologies such as digital signature and cryptographic systems produces security applications Biometrics [8].

2.3.1. Types of Biometrics [9]

There are more than one biometrics type already in use and there are also many other types will be used in the future as DNA, holograms [10], etc. . . ., Biometrics are classified into two categories as shown in Figure (1). The upper part consists of physiological biometrics such as face, finger prints and iris. The second part represents behavioral biometrics such as voice, signature, and keystroke [9]. The most common types:

- Finger print
- Iris recognition
- SR
- Face recognition

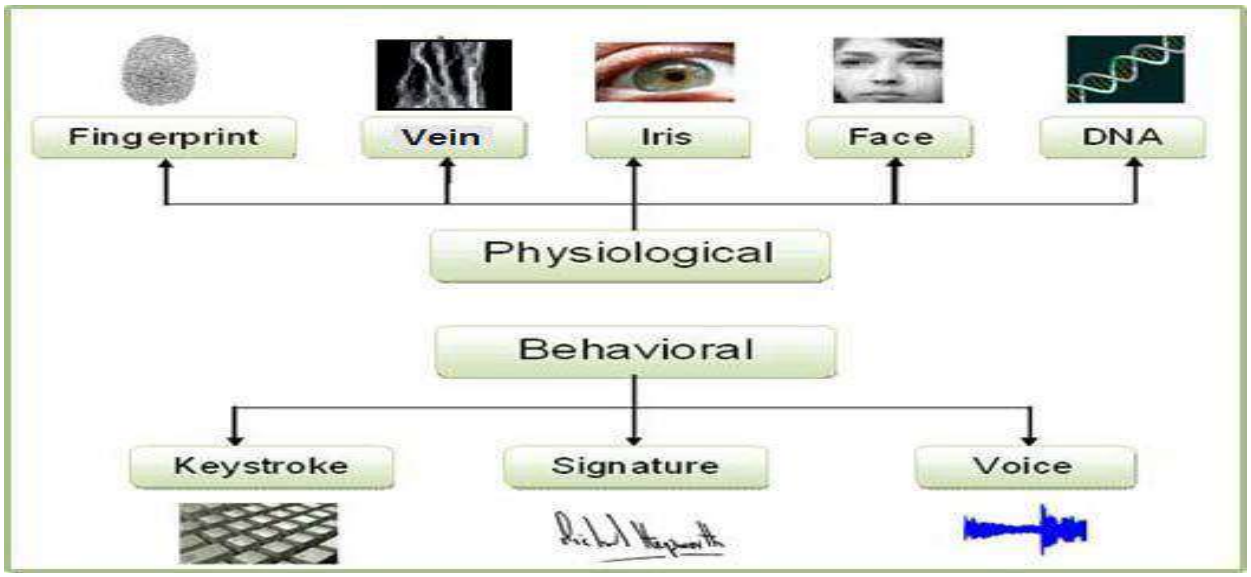

Figure (1): Different of biometrics [9]

3. Related work

Md.Mahiuddin (2019), in this paper, the researcher discusses the voting system of Bangladesh and developing a safe voting system using methods of the identification person through the iris recognition and smart cards identification [11].

Ch.Jaya Lakshmi and S.Kalpana (2018), in this research, the researcher developed a secure electronic voting using a valid Unique Identification (UID) and use fingerprints for authentication [12].

Paulo Realpe-Mu˜noza (2017), this paper gave a study on user behavior when utilizing e-voting applications, using eye tracking technique for behavior 865 qualitative and quantitative data analysis[13] .

ISSN (1681- 6870)

Adem Alpaslan ALTUN and Metin BĐLGĐN (2011), in this research, the researcher developed the system of electronic voting in the general elections and the use of fingerprints to authenticate the person and thus the system is improved by the use of biometric authentication system. As well as the researcher processes the disadvantages of traditional voting [14].

4. Proposed system

This paper focused on a series of steps used through planning in the proposed system. These steps involve: Data analysis, security level, E- voting parts, and determine the methods and techniques used in each part.

4.1.Data analysis

In the data analysis phase, we can visualize how to change the voice data during the use of voting system. For sound data, several operations are performed in audio signal, which converts them from large data into small unique data and is stored through a matrix. The dataset used a number of speeches: 20 voice samples: (14 females, 6 males). Speech properties as in table (1).

Table (1): Speech properties

Format	Bit Resolution	Duration
Wave files	16 bps	9 second

4.2.Security level:

In this paper the security is achieved by Biometrics. The proposed system using biometric online system used to identify a person. This is done by using a biometric voiceprint recording speech in a computer device. It takes analog signal about natural characteristics of individuals and then converts them into digital. This type of identification is quite successful compared to other methods, due to the unique feature of any person. . Biometric system consists of two Phases: User Registration, Login User

- **User Registration**

The user can register in this system by microphone speaker's speech in a computer device. After the user enters his voice he must clicks on " save" button to save voice and send his registration request to the system administrator and after the accept of the request the voice is saving in dataset .

- **Login User**

The user login in the system by using a voice that he creates in the previous step he send it to the server to verification from identifying a user.

Process verification and user identification by voice consist of three phases. As in figure (3).

1. Feature extraction.
2. Normalization.
3. Classification.

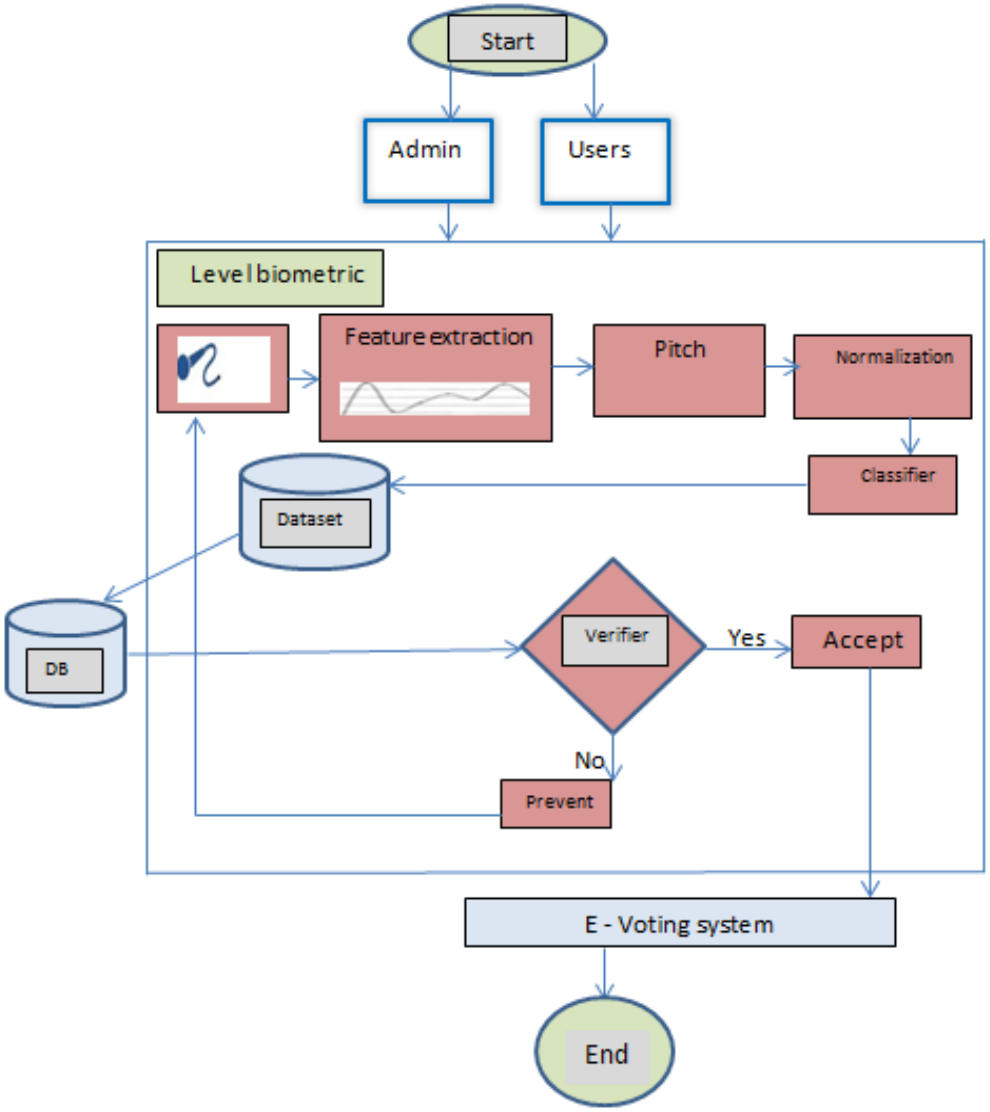

Figure (2): Propose system

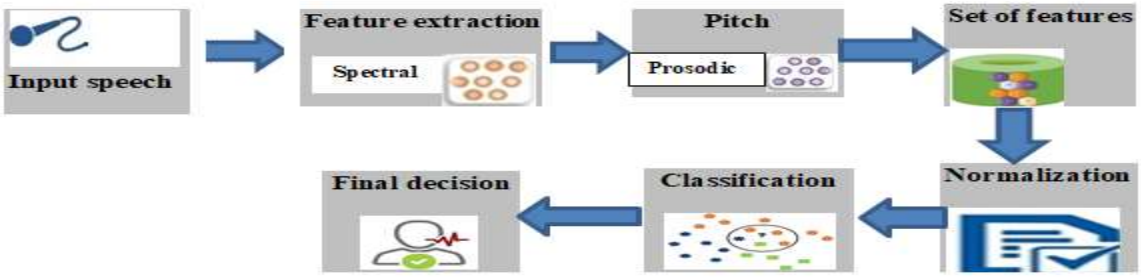

Figure (3): Proposed System of Speech in Real time

ISSN (1681- 6870)

1. Feature extraction stage

The feature extraction method is applied on input speech signal for extracting unique feature for each trained speech (voiceprint) and stores it in a vector. These vectors can be used then to build speaker model. The amount of captured speech data is quite large; on the other hand the essential features of the human speech change relatively slowly. Therefore, feature extraction is used to reduce data and retain speaker distinctive information. In this paper, Prosodic spectral and statistical features are extracted. The Prosodic, Spectral features and statistical parameters are proposed features extracted from the input speech sample for each speech person and save it as vectors in a model. There are two types in feature extraction.

The Mel-Frequency Cpestral Coefficient (MFCC) feature extraction is used to extract features from trained speakers' speech for both training and testing phases. MFCC simulate human ears behavior. The input of MFCC is entering speech signal. The output of MFCC is set of MFCC's coefficients. The set of features that will be extracted using MFCC is number thirteen features. Figure (4) presents MFCC block diagram. The steps in the computation of the MFCC features are as following:.

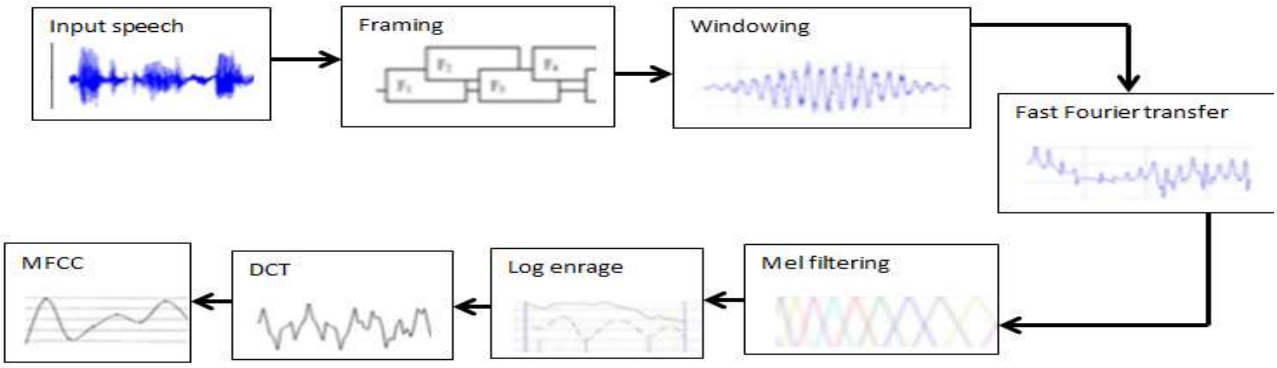

Figure (4): Feature extraction (MFCC)

a) Framing:

The person audio signal is tardily vary and can be handle when considered as short time frame. Therefore, the audio signal is usually divided into short period blocks called frames, and the spectral analyses is performed on these frames. Framing is a process that is used to convert the stream of signal into a set of frames has equal length (30 ms) and analyzed each frame independently. The original signal will be framed in overlapping blocks into N samples frame. Each frame is overlapping with M ms of time. Smaller overlapping means larger time shift in the signal whereas larger overlapping can result in a smoother change of the parameter values of the frames. In this paper data will be divided into frames of 30 ms with 75% overlap

b) Windowing:

The hamming windowing is used after dividing it into frames; each frame is multiplied by a window function before the spectral analysis to reduce the effect of discontinuity of (start and end) for each frame.

$$w(n) = 0.54 - 0.46\cos\left(\frac{2\pi n}{N-1}\right) \quad , 0 \le n \le N-1 \qquad \dots (1) \quad [15]$$

c) Fast Fourier Transform (FFT):

The FFT is used to convert each frame of N samples form time domain to Frequency domain. Implemented as in Equation (2).

$$X(K) = \sum_{X=0}^{N-1} x(n) W_N^{KN} \qquad \text{Where k =0, 1, 2…N-1} \qquad \dots (2) \quad [16]$$

d) Mel Filter Bank:

The magnitude of filter frequency response is used to obtain the log energy from this filter. The Mel filter bank is calculated by Equation (3). The triangular band-pass filters are used. The frequency response for every filter's size is triangular in format and equal to unity in the central frequency. The linear reduced to 0 at the central frequency of the neighboring filters.

$$m = 2595\log_{10}\left(1 + \frac{F}{700}\right) \qquad \dots (3) \quad [16]$$

$$S(m) = \sum_{K=0}^{N-1} \left| \, |X(K)|^2 \, Hm(K) \right| \qquad \dots (4) \quad [16]$$

e) DCT:

DCT is use to convert the log Mel spectrum into time domain. The outcome of transform is called MFCC. Output of feature extraction is 13 MFCC's coefficient. DCT is calculated by Equation (5).

$$c(n) = \sum_{m=0}^{m-1} log10(s(m)) \cos\left(\frac{\pi n(m-0.5)}{M}\right); \quad \text{n= 0, 1, 2 ….c-1} \qquad \dots (5) \quad [16]$$

Algorithm (MFCC)

Input:
WaveSample Frequency
Input wave
Sampling Frequency of Input wave

Output: MFCC

Begin
Step 1: Framing and Overlapping
Leng ⟵ Length (Wave Signal)
Overlap ⟵ 0.01 * Frequency
For i = 1 ⟶ No Frame -1
Frame1 ⟵ partition (Wave Signal, i)
Frame2 ⟵ partition (Wave Signal, i+1)
Segment Overlap ⟵ Overlapping (Frame1, Frame2)
WaveSignalOverlap ⟵ Merg (WaveSignalOverlap,SegmentOverlap)
End For
Step 2: Windowing
For i = 1 ➡ No Frame
Frame ⟵ Partition (WaveSignalOverlap, i)

ISSN (1681- 6870)

```
FrameWindowing ⟵ Windowing (Frame)  // using Equations (1).
WaveWindowing ⟶ Merg (WaveWindowing,FrameWindowing)
End For
  Matrix of windowed ⟵ WaveWindowing
Step 3: Appling FFT  on  matrix of windowing to get power spectrum
Spectrum ⟵FFT (matrix of windowed ) // using Equation (2)
Step 4:  triangular filter band
Mel⟵ H ToMel  (Spectrum ) // using Equation (3)
InvMel ⟵ InversWarping (Mel ) // using Equation (4)
MelLog ⟵LogInvMel(InvMel)
Step 5: Appling DCT
 CpestralDCT⟵DCT(MelLoge ) // using Equation (5)
MFCC⟵ CpestralDCT
End
```

f) Pitch:

Pitch is one of the useful features for prosody analysis of the speech signal and is considered as an important cue for recognizing the speaker's voice one of the important perceptual features, as it conveys much information about the sound. The Pitch is computed over all speech signals like ZCR. We estimate the pitch of the speech signal using the autocorrelation.

2. Normalization:

Normalization is an approach to Z-score (or standardization) is a scale data to fixed range - typically 0 to 1. The cost of this specified range - in contrast to standardization - is that we will end with smaller standard deviations, which can prevent the effect of extreme value.

3. Classification:

The classification is using one of the most simple and popular classification (KNN). The classification consists of two phases; training and testing.

➢ Training phase

In Training process, the classification of intelligent system is learned by using the features of the training dataset after normalizing these features. The training phase is responsible for building speech model. In this paper, the training phase is implemented in the following order:

- Input speech to dataset in server
- Perform MFCC feature extraction on input speech
- Perform normalization on MFCC's feature for each speaker.
- Perform classification by use KNN algorithm using Euclidean distance

➢ Testing phase

The testing phase is responsible of discovering the identity of unknown input speech. If the input speech belongs to a speaker model that has been trained and stored in the system, the system will find

ISSN (1681- 6870)

best match for this input speech. Otherwise, there will be ' No match speaker'. In this paper the testing phase is implemented in the following order:

- Input speech to dataset in server
- Perform MFCC feature extraction on input speech
- Perform normalization on MFCC's feature for each speaker.
- Perform classification by use KNN algorithem using Euclidean distance.

The general block diagram of training and testing phases can be illustrated in Figure (5)

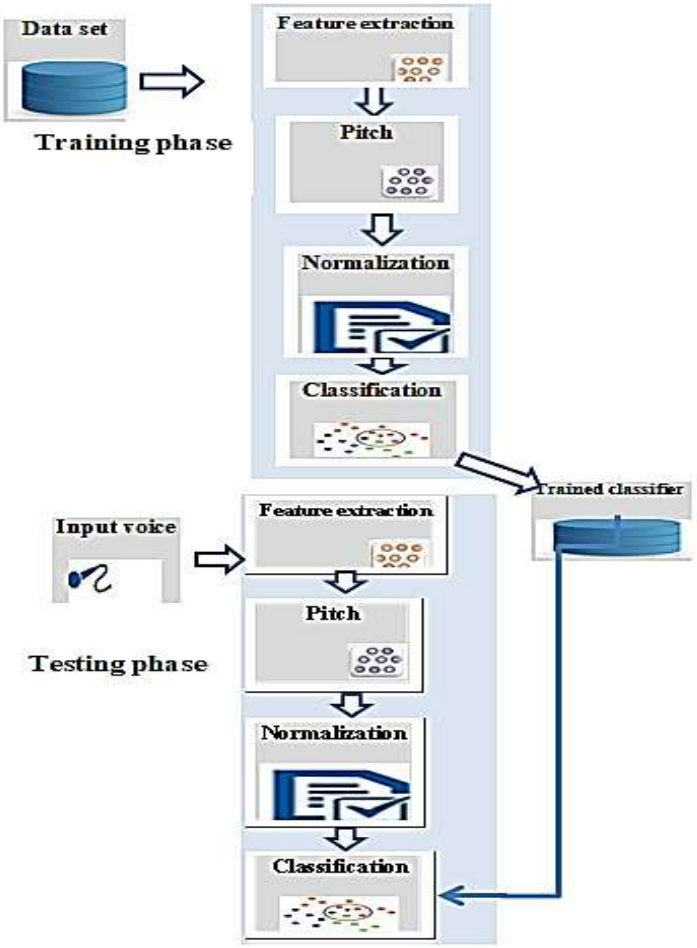

Figure (5): Training and Testing to voice Recognition

4.3.E- voting system

The system is available to the user, when that person is authorized to access the system by voice. The system consists of seven pages: Add user page, add a session page, edit a session page, and manage a session voting page, with a page to view reports and a system setting page with the system exit button.

5. Result of voice print using KNN algorithm

The voiceprint of the person was tested by taking a number of samples and training the system on them and then taking the votes of people for the purpose of testing and the result are as shown in table (2).

ISSN (1681- 6870)

Table (2) displays result and relationship between value test voice and detection rate.

person	Voice1	Voice2	Voice3	Voice4	Voice5	Voice6	Misclassified rate	Classification rate
A	T	T	T	T	T	T	0%	100%
B	T	T	T	T	T	T	0%	100%
C	T	T	T	T	T	T	0	100%
D	T	T	F	F	T	T	33.33%	66.67%
E	F	T	T	T	T	T	16.67%	83.33%
F	T	T	T	T	T	T	0%	100%
G	T	T	T	T	T	T	0%	100%
H	T	T	T	T	T	T	0%	100%
I	T	T	T	T	T	T	0%	100%
J	T	T	T	T	T	T	0%	100%
K	T	T	T	T	T	T	0%	100%
L	T	T	T	T	T	T	0%	100%
M	T	T	T	T	T	T	0%	100%
N	T	T	T	T	T	T	0%	100%
O	T	T	T	T	T	T	0%	100%
P	T	T	T	T	T	T	0%	100%
Q	T	T	T	T	T	T	0%	100%
R	T	T	T	T	T	T	0%	100%
S	T	T	T	T	T	T	0%	100%
T	T	T	T	T	T	T	0%	100%

Where (A, B, C, D, E, F …..T) are labels of person.

6. Conclusion

The security process is important in many systems especially in the electronic voting system in order to ensure true results and avoid manipulation of voting as it is not allowed. The main objective in this paper is to design a secure system for e – voting by using biometric features. We choose sound as biometric in order to achieve a secure system. The system also provides ease of use for anyone, as well as flexibility and simplicity of the web site usage. Regardless the types of hardware and software, there result of the voice recognition was through a number of procedures reached to obtain accurate identification the process of extracting the features used was more than the algorithm, this method gave good results to extract a powerful set of features. In the training phase, the accuracy of the system increased while using a large number of samples selected. The presentation proved that the sound recording and the selected feature are the best way to achieve stability, performance in the real – time environment, as well as ensuring a secure voting process while using the system.

Reference

[1] I. Jabbar and S. N. Alsaad," Design and Implementation of Secure Remote e-Voting System Using Homomorphic Encryption", International Journal of Network Security, Vol.19, No.5, PP.694-703, Sept. 2017.

[2] P. S. Naidu, R. Kharat, R. Tekade, P. Mendhe and V. Magade, "E-voting system using visual cryptography & secure multi-party computation", Proc. of International

ISSN (1681- 6870)

Conference on Computing Communication Control and automation (ICCUBEA), Pune, India, 2016.

[3] A. Al-Ameen and S. Talab, "The technical feasibility and security of E-Voting," Int. Arab J. Inf. Technol., vol. 10, no. 4, pp. 397–404, 2013.

[4] R. Alaguvel and G. Gnanavel, "Offline and Online E-Voting System with Embedded Security for Real Time Application", International Journal of Engineering Research, vol 2, no. 2, pp. 76–82, 2013.

[5] V. M. Patil, "Secure EVS by Using Blind Signature and Cryptography for Voter's Privacy & Authentication" Journal of Signal and Image Processing, Vol. 1, No. 1, pp. 01-06, 2010.

[6] S. Jafari, "A new secure and practical electronic voting protocol without revealing voters identity", International Journal on Computer Science and Engineering, vol. 3, no. 6, pp. 2191–2199, 2011.

[7] Y. Feng, L. Tian, F. Liu, and C. Gan,"Electronic Voting: A Review and Taxonomy" , International Conference on Industrial Control and Electronics Engineering Electronic, IEEE, 11 (9), 1937-1946. 2012.

[8] N. D. Sarıer, "Biometric Cryptosystems : Authentication , Encryption and Signature for Biometric Identities", Dissertation Mathematisch-Naturwissenschaftlichen Fakultät Rheinischen Friedrich-Wilhelms-Universität Bonn Neyire Deniz Sarıer aus, 2011.

[9] A. Shrestha, "Multi-biometric systems – Templates, Template Protection and Remote Authentication", B. Sc. thesis, Turku University of Applied Sciences, pp. 1–61, 2014.

[10] F.L.Podio and J.S.Dunn, "Biometric Authentication Technology: From the Movies to Your Desktop", ITL Bull. May 1–8 , 2001.

[11] Md. Mahiuddin, "Design a Secure Voting System Using Smart Card and Iris Recognition", International Conference on Electrical, Computer and Communication Engineering (ECCE) 2019.

[12] C. J. Lakshmi and S. Kalpana, "Secured and Transparent Voting", 2nd Int. Conf. Inven. Syst. Control, no. Icisc, pp. 343–350, 2018.

[13] P. Realpe-Muñoz, C. A. Collazos, J. Hurtado, T. Granollers, J. Muñoz-Arteaga, and J. Velasco-Medina, "Eye tracking-based behavioral study of users using e-voting systems", Comput. Stand. Interfaces, vol. 55, pp. 182–195, 2018.

[14] A. Altun and M. Bilgin, "Web based secure e-voting system with fingerprint authentication", Sci. Res. Essays, vol. 6, no. 12, pp. 2494–2500, 2011

[15] A. Amer, "Real-Time System for Arabic Speech Emotion Recognition", Thesis, Al Mustansiriyah University, 2018.

[16] Y. A. Mohammed, "Speaker Identification Using MFCC and VQ ", Thesis, Al Mustansiriyah University, 2016.