

Voice Classification Based on Fast Independent Component Analysis to Support Nuclear Power Plant Security

R.F.S. Budi^{*} and Suparman

Center for Assessment of Nuclear Energy System, National Nuclear Energy Agency,
Jl. Kuningan Barat Mampang Prapatan, Jakarta Selatan 12710, Indonesia

ARTICLE INFO

Article history:

Received 15 January 2018

Received in revised form 27 March 2019

Accepted 1 April 2019

Keywords:

National vital objects

Nuclear power plant

Voice classification

Fast ICA

Euclidean distance

Reliability

ABSTRACT

National vital objects have important role in national development, so they require special protection. Nuclear power plant (NPP) is one of them. Access restriction is required to prevent the NPP from potential hazards. The restriction can be improved by using face, fingerprints, retina, iris, and voice password. The improvement will enhance the security of the NPP. This research has implemented pattern recognition and classification of voice passwords. The passwords were a, i, u, e, and o. The features vector was searched by using Fast ICA method while the pattern classification was performed by minimum Euclidean method. The purpose of this research is to recognize and classify those letter password, so people who have access to the nuclear area can be distinguished. The methodology of this research consists of input data, pre-processing data, feature extraction, and classification. Pre-processing was done by normalization, denoising, centering, and whitening. Feature extraction was performed by Fast ICA method, and classification was done by minimum Euclidean distance. The results show that Fast ICA and minimum Euclidean methods can 100 % distinguish between the employees who have access permit and those who have no access permit. When an employee with access permit says "aiueo", it will be recognized as password, whereas when an employee with no access permit says the password, it will be recognized not as the password.

© 2020 Atom Indonesia. All rights reserved

INTRODUCTION*

National vital objects require special protection because of their role in national development. Nuclear facilities are included in the national vital objects. One of the nuclear facilities areas in Indonesia is PUSPIPTK Serpong, where G.A. Siwabessy research reactor is located [1]. In addition, a nuclear power plant (NPP) as an experimental power reactor is planned to be constructed [2]. An NPP is a power plant that requires high level of security, reliability, and availability [3-5]. The security and reliability can be influenced by technical and non-technical aspects. The technical aspects embrace the technical aspects

of power plant equipments while non-technical factors are those non-equipment aspects such as natural disaster and illegal access. Illegal access can result in sabotage, errors in the power plant operation, and errors in maintenance.

Access restriction is required to prevent potential hazards. Based on previous research [6], some countries pay less attention to the NPP access restriction, where restriction implementation only uses identity check and written password. The restriction, meanwhile, can be improved by using biometrics security systems. The improvement will enhance the security of the national vital objects especially NPP.

A biometrics security system is a security system that uses biometric data. Biometric data can be distinguished as physical and behavioral. Physical data can be derived from face, fingerprints, iris, and retina, while behavioral data can be retrieved

* Corresponding author.

E-mail address: rizkifirmansyah@batan.go.id

DOI: <https://doi.org/10.17146/aij.2020.813>

from voice, handwriting, and signature. Voice, face, fingerprints, iris, and retina are always used for security systems [7-9].

Biometrics security systems by using face, fingerprints, iris, and retina are based on image data. They require more complicated pre-processing than voice to obtain good features vector. Voice data require simpler pre-processing because they are based on voice wave shape and have lower implementation costs [10]. Capturing image, meanwhile, requires more complicated and high specifications in order to retrieve good image details. The accuracy level is almost the same between each of biometric data. The accuracy depends on the input data quality [11,12]. This research used voice password in biometrics security system.

The processes involved in voice password authentication include pattern recognition and classification. The recognition and classification can be done through recognizing and classifying the password, either as a whole word or letter by letter.

Previous researches [13,14] have divided letters into two classes: vowels and consonants. Vowels are spoken by adjusting the vibrations of vocal fold without any airflow arrangement while consonants are spoken by adjusting the vocal fold and arranging the airflow inside a mouth. The airflow setting in pronouncing consonants will cause the waveform to be very different from person to person, while in vowels the waveforms are more similar. In addition, the sound produced by each person will differ depending on the type of the sound, mouth shape, tongue shape, and tooth shape. Based on these differences, voice classification of each particular person can be set as a password. This research implemented pattern recognition and classification of vowel letters (a, i, u, e, and o) to support the application of voice password in the experimental power reactor.

Vowel letters have been chosen as voice password in this research because vowel letters produce similar waveform among the pronouncers. This similarness makes vowel letters identification and classification harder than consonants. Similar waveform can give wrong result if the classification is not appropriate. If classification of vowel letters can be done without error, consonant letters will not be difficult to classify because they have specific waveforms that differ among individuals.

Some researches have performed voice recognition by using different methods. Paul *et al.* [15] performed voice recognition by using hard threshold based system and cohort based system using 30 speakers as a data sample for testing and validating. The best accuracy attained was 85.61 %.

Guanyu *et al.* [16] implemented voice recognition as an authentication of client/server system. To extract the features vector from the voice, Mel Frequency Cepstral Coefficient (MFCC) method was used. The features vector classification was performed by vector quantization (VQ) method using three sample size of data: 30 speakers, 60 speakers, and 90 speakers. The results showed that short-term variance in 30 speakers was 97 %, short-term variance in 60 speakers was 93 %, and short-term variance in 90 speakers was 88 % [16]. Nair and Salam [17] implemented voice recognition by using linear predictive cepstral coefficient (LPCC) and dynamic time wrapping (DTW). The best accuracy achieved by [17] was 97 %. Paul and George [18] used voice recognition as a secure authentication system in a laboratory. The system was able to identify which person to be authorized to enter the laboratory and which one not to be authorized. The research used fast fourier transform to recognize the voice.

Independent component analysis (ICA) is a stochastic method used to transform multi-dimensional random vectors into several components that are statistically independent of each other [19-21]. ICA has been widely used to find the features vector of a wave, and based on the features, recognition and classification can be done. The advantages of using ICA are saving the size of the features vector dimension without reducing the ability to recognize the patterns and also saving the iteration time [22,23].

Anishchenko [24] has used ICA to distinguish respiration and heartbeats signals. King and Dessaint [25] have used ICA to simplify the features vector of disturbance signals to reduce the estimated clearing time in the event of a transient disturbance. Shen *et al.* [26] have used ICA in the blind decoding of massive multiple-inputs multiple-outputs. Dharmapranjani *et al.* [27] have compared some ICA algorithms in the implementation of electroencephalogram (EEG) distinguisher from interference signals. The algorithms were joint approximate diagonalization of Eigenmatrices (JADE), Information Maximization (Infomax), and FastICA. The comparison results show that FastICA can differentiate EEG signals at a faster time than the other algorithms.

After the features vector is obtained, the classification is done by using minimum Euclidean distance, which is the fastest and simplest way than other methods [28,29].

This research implemented pattern recognition and classification of vowels voice password of i.e. a, i, u, e, and o. The features vector searching was performed using FastICA while the pattern

classification was done using minimum Euclidean distance. The purpose of this research is to recognize and classify the letter password (a, i, u, e, and o), so people who have access to enter the national vital objects such as nuclear area can be distinguished.

The use of voice password is expected to enhance the reliability of the national vital objects, especially experimental power reactor in PUSPIPTEK area which is planned to be build in the near future. The reliability increment will increase the availability factor. This is in line with the contents of the IAEA document, which states that NPP must have high reliability and availability.

Pattern classification

The pattern classification can be done by several processes as follows: pre-processing, feature extraction, and classification. These processes will be discussed in this section.

Pre-processing

Pre-processing is performed to process input data to be used in the next process. Data processing is necessary because the quality of each input data is different and needs to be equated. The difference is caused by noise [30,31]. The quality of the data depends on the conditions during data collection [32]. The pre-processing method used in previous researches show that each problem will require different methods depending on the problems [30-33].

Pre-processing process on vocal signals can be done by normalization, denoising, centering, and whitening. Normalization is done to the data concerning data pattern, not data magnitude. Normalization can be done by using equation (1).

$$Norm\ x_i = \frac{x_i}{|max(x)|} \tag{1}$$

where :

- Norm x_i = Normalization of components i of vector x
- x_i = Component i of vector x
- $|max(x)|$ = The absolute of maximum value of vector x

Denoising is the process of noise removal in the input data. Denoising can be done by deleting data whose values are too small because they are considered as noise [34-36]. Denoising can be done using equations (2) and (3).

$$x_i = 0, \text{ for } x_i \leq 0.1 \tag{2}$$

$$x_i = x_i, \text{ for } x_i > 0.1 \tag{3}$$

where : x_i = Component i of vector x

Centering is the reduction of data x by the mean of data x , so the average value of x is 0. Centering can be done using equation (4).

$$x_i = x_i - \bar{x} \tag{4}$$

where : x_i = Component i of vector x

\bar{x} = Mean of data x

Whitening is the process of transforming data x linearly to obtain independent components, the variance value of which is 1 [37,38]. Equation (5) and (6) show whitening of the data x [25].

$$E\{xx^T\} = I \tag{5}$$

$$\tilde{x} = \mathbf{E} \cdot \mathbf{D}^{-1/2} \cdot \mathbf{E}^T \cdot x \tag{6}$$

where

x = Voice data

\tilde{x} = Whitened x

I = Identity matrix

\mathbf{E} = Ortopogonal matrix of eigenvectors $E\{xx^T\}$

\mathbf{D} = Diagonal matrix of eigenvalues $E\{xx^T\}$

Feature extraction using fast ICA

The process of voice data classification can be done after the features vector of each data has been obtained. The features vector can be searched by using ICA method. ICA is a computational method for analyzing data by treating the data as a combination of multiple data that are statistically independent of each other and have non-Gaussian distributions. If there is a random vector x with random variables n ($x = (x_1, x_2, \dots, x_n)^T$) obtained from the sum of independent components $s = (s_1, s_2, \dots, s_k)^T$ then ICA will perform a linear transformation of vector x into an independent component s using equation (7).

$$s = W \cdot x \tag{7}$$

where : s = Independent component of vector x

W = Matrix weight

x = Vector data

To obtain n independent components, n data of x are needed [27,39]. The vector s will be the features vector of the vector x and is used for the classification process. Matrix W is the inverse of matrix A . Matrix A is a linear representation of non-Gaussian data that are statistically independent of each other [25].

The most widely used and the fastest ICA algorithm is FastICA [25,27]. FastICA is a fixed point iteration scheme to find a maximum non-gaussianity value of $w^T x$. The FastICA algorithm to find the W matrix is as follows [37]:

1. Determine the random initial value of w
2. Calculate the value of w^+ , $w^+ = E \{xg(w^T x)\} - E\{g'(w^T x)\}w$
3. Make w^+ to be w , $w = w^+ / |w^+|$
4. If not convergent, go back to the step 2.

Classification using euclidean distance

The purpose of classification is to classify the input data into an existing class. The class determination is based on the proximity of the features vector between training data and input data. The proximity can be determined by using a minimum Euclidean distance shown by equation (8) [29].

$$d(s, y) = \sqrt{\sum_{i=1}^k (s_i - y_i)^2} \tag{8}$$

where :

- $d(s,y)$ = Euclidean distance from x to y
- s_i = Feature vector of input data
- y_i = Feature vector of training data

RESEARCH METHODS

The research was conducted using a methodology as shown in Fig. 1. The first step was finding the features vector of the training data. The data was voices data from employees having access right to the experimental power reactor.

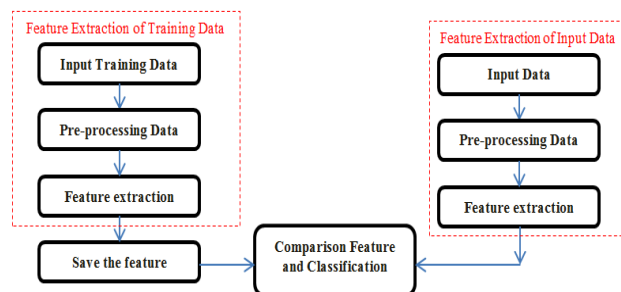


Fig. 1. Research Methodology.

The data voices were voices data of vowel letters spoken by employees having the access right. Vowel letters were chosen as a password because they have similar waveform but are more difficult to identify than other letters. This research used all vowel letters as a password (a, i, u, e, and o), not

only any one vowel letter, because of redundancy principle. By using all of the five vowel letters, the security of password will be enhanced because to access the area, all of the five passwords should be validated. The situation could be different if the password only uses one vowel letter, where the probability to break the password will be higher.

The number of employees having the access right in this research was 32 persons. Each employee had 5 voices data (a, i, u, e, and o), so the total voices training data were 160. The voice data were recorded by an application-based recording tool on a smartphone. The application allowed the sampling rate to be adjusted from 8 kHz to 44.1 kHz. This research employed a sampling rate of 16 kHz using an android internal microphone. The gain of the microphone was adjusted by using the recording application. In other words, the recording process of this research was done by using a smartphone.

The features vector was searched within these 160 data. Input training data had a function to input the 160 voices data into a source code based on MATLAB program for use in the searching process of the features vector. The input function converted the voices data into two dimensional matrices, which were then used for the searching process.

The searching process was started with the training data pre-processing. The pre-processing processes used in this research were normalization, denoising, centering, and whitening. The process was done sequentially starting with normalization and ending with whitening as shown in Fig. 2.

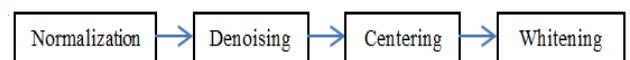


Fig. 2. Pre-processing Process.

Normalization was done because each vocal has different level of magnitude, while the vocal classification does not need the magnitude data but the wave pattern data. Normalization was done using equation (1). Denoising was done because each vocal data has different level of noise and different vocal starting point. Denoising was done using equations (2) and (3). Centering was done because each vocal data has different mean. It is necessary to make the mean to be zero without changing the wave pattern. Centering was done by using equation (4). Whitening was performed to find vectors, which are mutually independent, using equations (5) and (6).

Searching of the features vector was done by Fast ICA method after pre-processing. The searching process of the features vector has been described in the feature extraction using Fast ICA section. By using FastICA, the features that are not

significant to the classification process will be eliminated. Based on FastICA principle, the significant features are waveform data that are statistically independent of each other and have non-Gaussian distributions. The outputs of the method are features vectors, which are independent of each other.

The features vectors of the 160 vocal data were saved and used as references for the determination of the class of the input data. After saving the references, the next step was finding features vector of the input data.

The finding process of the features vector of the input data was done in a similar way with the process with training data. The input data used in this research were a, i, u, e, and o vocal data from each employee joining in this research. The employees were selected randomly. The total selected employees were 64 persons with a composition of 32 employees having access permission and 32 employees not having access permission. Previous researches [40,41] have shown that for an experimental research, a minimum of 15 samples are needed to make a representation of the total population.

Having obtained the features vector of each a, i, u, e, and o letter of each employee, the features vector was compared with the a, i, u, e, and o features vector that had been stored as reference. The comparison was performed using minimum Euclidean distance method as shown in equation (8). For example, when an employee says "A", the features vector of "A" will be compared with the features vector of a, i, u, e, and o that are used as reference. The Euclidean distance A to a is 10, A to i is 19, A to u is 11, A to e is 12, and A to o is 10.75. Therefore the letter A will be classed as "a" because it has the least Euclidean distance.

RESULTS AND DISCUSSION

The use of voice passwords as biometrics security systems has the advantages of simpler sensor tools and simpler pre-processing. The accuracy level is almost the same between each biometric data [10-12].

Sensor tools for face, iris, and retina require a camera with high specifications for obtaining a good image quality and details. Sensor tool for fingerprints is a scanner with high level of accuracy. As for the voice, the recorder based on a smartphone application can be used as it was applied in this research.

Pre-processing on the face, fingerprints, iris, and retina are more complicated than voice because the required input data are image data. The quality of the image data varies depending on the position, brightness, and image details. Therefore, to obtain

good image quality as a standard, more complicated pre-processing is required. Pre-processing for voice, on the other hand, is simpler, and it was implemented in this research. The pre-processing in this research were normalization, denoising, centering, and whitening.

The challenges of using voice passwords are basically the same as other biometric passwords, namely noise. Noise on voice can reduce the data quality. The noise can be overcome by normalization and denoising. In addition, the noise can be reduced by improving the quality of voice data retrieval, i.e. by making the soundproof room so that no noise from the surrounding is disturbing. This research did not use soundproof room, so the voice records still had noise. To handle the noise, this research used normalization and denoising.

It has been explained that the voice data have different qualities. The quality is affected by noise, voice magnitude, and voice start point. Therefore, pre-processing the data is necessary to obtain a good quality data. Figure 3 shows the input data and the pre-processing result data for letter "a" from 2 employees. The data from employee 1 and 2 have different qualities (the noise and the start point). The longer starting point of the sound, the more data will be recorded. The number of data will affect the iteration time of the classification. The noise will make different features vector and cause the classification accuracy to decrease.

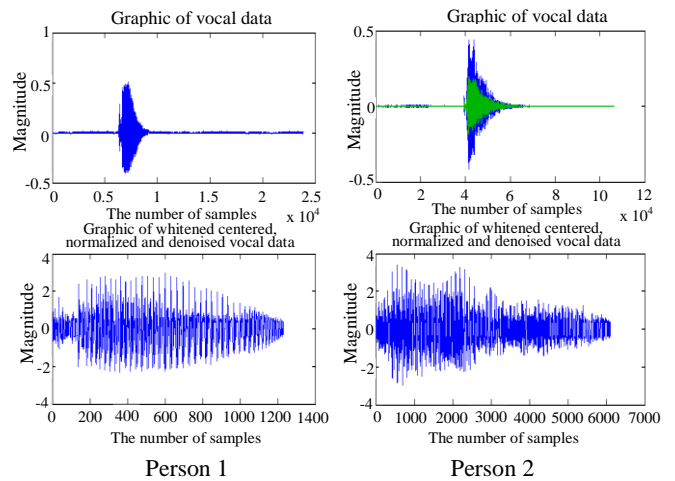


Fig. 3. Pre-processing results of letter A in 2 persons.

The input data undergone pre-processing indicate that the starting point is still the same but the noise has gone. That condition has made the number of the data decrease, and thus the features vector is easier to be found.

Figure 4 shows the features vector of the letter "A" from 2 employees. The number of vector elements in the features vector is much lower than that in the input data. This is in agreement with "a good feature has a little number of feature but can distinguish more" [10,42]. Based on the features

vector, comparison and classification of the letters can be done.

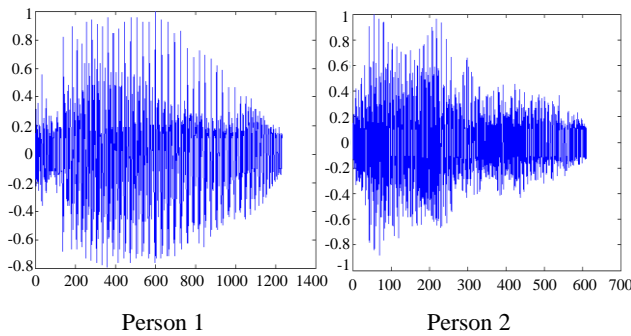


Fig. 4. Letter A feature vector of 2 persons.

The comparison was performed by comparing the features vector of the input data with the references. Based on the comparison, the Euclidean distance between the input data and the references could be obtained, and by using Euclidean distance, the classification could be done.

Based on the research results, whether the employees are allowed to enter the nuclear area or not can be identified. The comparison of Euclidean distance between the letters spoken by the employee and the references (password) is shown in Table 1.

LW (legal worker) designates employee having access permission. IW (illegal worker) designates employees having no access permission. The green color indicates that the letter spoken by employees is in agreement with the reference (password). The red color indicates that the letter spoken by employees is not in agreement with the reference. An employee with access permission was identified when all of the spoken letters (a, i, u, e, and o) were green. If any of the spoken letters was red, then the employee was identified as an employee with no access permission. The table shows that all LW have the green color for all of the spoken letters, whereas all IW have the red color. It means that the pattern recognition and classification using Fast ICA has been successfully implemented in this research.

In the LW 1-32, it is indicated that the spoken letters can be classified in accordance with the password (reference) letters, which is shown by a zero Euclidean distance. When an LW pronounces the letters, Fast ICA will seek its features vector and compare it with the reference features vector stored. Zero Euclidean distance is an indication that the features vector is similar or having no distance between the spoken data and the reference password. Euclidean distance appears if the features vector is not similar. For example, when LW 1-32 say "A",

Table 1. Euclidean distance comparison on letters spoken and the password letters.

Employees	Spoken Letters	Password Letters					
		A	I	U	E	O	
LW 1	A	0	16	15.6	14.5	13.1	
	I	26.7	0	27.8	26.8	25.7	
	U	22.7	27.6	0	23.3	24.6	
	E	15.4	16	15.5	0	13.3	
	O	18.5	19.8	19.9	18.3	0	
LW 2	A	0	17.4	16.8	16	14.5	
	I	24.3	0	24.2	24	22.7	
	U	22.1	26	0	21.7	22.7	
	E	17.1	18.2	17.7	0	15	
	O	19.3	19.7	19.5	18.6	0	
LW 3	A	0	15.8	15.5	14.4	13.2	
	I	21.6	0	22.4	21.6	20.2	
	U	20.2	24.2	0	20.2	20.6	
	E	14.5	15.5	15.1	0	12.8	
	O	19.2	20.7	20.4	18.2	0	
LW 4	A	0	22.8	27	17.9	21.3	
	I	15.8	0	25.2	15.5	20.4	
	U	16.2	24.5	0	16.1	21.2	
	E	15.7	23	26.3	0	20	
	O	15.6	23.2	25.9	15.6	0	
LW 5	A	0	24.7	27.5	19.2	22.9	
	I	17.3	0	28.6	17.2	22	
	U	23.4	29.4	0	23.3	27	
	E	21	27.6	31.1	0	25	
	O	21.6	29	32.6	21.5	0	
LW 6	A	0	24.9	26.3	17.9	22	
	I	24.3	0	31.9	24.2	28	
	U	18.4	25.7	0	18.2	23	
	E	17.3	24.3	23.2	0	19.7	
	O	18.5	26.5	30.3	18.2	0	
LW 7	A	0	22.9	24.5	16.3	19.9	
	I	16.7	0	28.9	16.4	21.2	
	U	20.9	28.3	0	20.8	25.8	
	E	16.7	24.8	29.5	0	20.9	
	O	13.1	20.2	20.6	12.8	0	
LW 8	A	0	22.8	25.3	16	20.3	
	I	15.8	0	24.2	15.6	19.7	
	U	16.3	23.4	0	16.2	20.2	
	IW 1	A	18.9	24.2	28.4	18.8	23
	IW 1	I	19.6	26.9	30.2	19.3	23.6
IW 1	U	22.6	29.5	34.3	22.7	27.4	
IW 1	E	17.2	24.4	25.9	16.9	21.2	
IW 1	O	17.3	24.7	27.7	16.6	21.4	
IW 2	A	15.4	22.9	24	15.1	19.7	
IW 2	I	18.1	25.4	28.2	18.2	22.4	
IW 2	U	18.3	25.2	29	18.2	22.3	
IW 2	E	16.3	23.6	26.5	16.1	20.6	
IW 2	O	17	23.5	26.3	16.7	21.1	
IW 3	A	12.4	19.5	20	12.1	15.9	
IW 3	I	17.6	24.8	27	17.4	21.7	
IW 3	U	15.6	23.2	27.3	15.5	20.3	
IW 3	E	15.5	22.4	24	15.2	19.4	
IW 3	O	15.8	23	25	15.5	19.9	
IW 4	A	19.2	21.3	21	19	17.5	
IW 4	I	17.4	19.8	20	17.3	16.1	
IW 4	U	25	31.1	32.3	24.8	28.4	
IW 4	E	18	21.6	21.6	18.1	17.7	
IW 4	O	21.6	25.6	25.8	21.2	22.3	
IW 5	A	20	23	23	20.2	19.7	
IW 5	I	18.2	23.9	24.8	18.4	20.3	
IW 5	U	20.4	23.8	24	19.7	20.4	
IW 5	E	18.4	24.5	25.4	18.3	20.4	
IW 5	O	19.6	24.3	24.6	19.3	20.5	
IW 6	A	18	18.9	18.3	17.4	16	
IW 6	I	17.2	19.6	19.5	16.7	16.1	
IW 6	U	21.9	25.9	26.4	22	22.9	
IW 6	E	19.3	25.1	25.5	19.7	21.5	
IW 6	O	22	24.5	24.4	21.9	21.2	
IW 7	A	21.3	26.2	27.1	21.2	23.1	
IW 7	I	20.5	25.8	26.9	20.3	22	
IW 7	U	20.3	24.8	25.2	20	21	
IW 7	E	18.6	20.3	20	17.2	16.9	
IW 7	O	20.4	24.5	24.8	20.6	21.6	
IW 8	A	17.1	23.7	24.6	16.9	20.4	
IW 8	I	19.8	26.3	28.6	19	23.2	
IW 8	U	18.2	25.5	28.6	18.1	22.5	

Table 1. Euclidean distance comparison on letters spoken and the password letters.

LW 9	E	14.8	22.1	24.3	0	19.3	IW 9	E	19.2	25.6	27.3	19	22.8
	O	16.6	23.9	26.9	16.6	0		O	20	26.5	29.6	19.8	24.1
	A	0	19.2	19.4	14.5	14		A	22.1	21.6	23.4	18.2	19.7
	I	16.1	0	25.5	15.8	20.3		I	23	24.5	23.2	23.7	21.8
	U	15.5	22.4	0	15.1	19.5		U	23.4	18.2	16.9	24.6	21.7
LW 10	E	14.4	21.6	23.6	0	18.6	IW 10	E	19.8	21.3	18.5	23.8	25.3
	O	15.9	22.9	25.3	15.7	0		O	22.3	25.1	25.9	21.8	28.3
	A	0	25.8	29	19.1	23.2		A	19.7	24.8	21.8	18.5	26.3
	I	16.3	0	24.5	16.1	19.8		I	22.4	24.8	25.6	20.2	23.7
	U	16.9	23.7	0	16.3	20.5		U	27	26.2	25.8	19.3	25.4
LW 11	E	18.3	25	28.1	0	22.6	IW 11	E	23.9	22.7	27.5	21.4	24.3
	O	17.4	24.4	26.7	17.4	0		O	24.5	25	25.9	20.8	22.3
	A	0	16.4	15.9	17.3	15.5		A	29.1	20.9	22.8	28.2	20.2
	I	23.2	0	25.7	21.4	20.8		I	20	21.2	26.4	18.6	23.1
	U	21.1	25	0	22.8	20.9		U	15.8	19.5	25	25.5	24
LW 12	E	18.3	19.1	18.8	0	16.2	IW 12	E	19.3	23.4	22.9	17.7	22.5
	O	19.8	21.2	20.4	17.9	0		O	25.7	22.1	23.7	20.1	23.4
	A	0	14.6	14.1	15.6	14.1		A	15.8	23.2	25.9	25.6	21.4
	I	20.5	0	21.3	20.5	21.3		I	20.4	27.3	25.7	19.5	22.3
	U	19.3	23.5	0	21.8	21.9		U	27.1	24.6	26.3	17.8	23.1
LW 13	E	13.5	14.2	14.4	0	11.9	IW 13	E	24.1	25.8	22.9	24.5	27.2
	O	18.1	19.6	19.3	17.1	0		O	23.5	22.8	27.4	19.3	25.3
	A	0	21.7	26.1	16.8	20.2		A	25.3	27.4	21.5	24.2	20.3
	I	16.9	0	26.3	16.6	21.5		I	20.4	23.6	27.4	18.9	23.2
	U	15.3	23.6	0	15.2	20.3		U	24.4	20	22.1	19.3	29.1
LW 14	E	16.8	24.2	25.4	0	21.1	IW 14	E	19.8	26.1	20.3	18.1	20.9
	O	14.5	22.2	24.8	14.6	0		O	28.1	22.4	21.2	20.6	24.1
	A	0	15.1	14.5	13.4	12		A	19.5	26.7	30.7	18.3	20.4
	I	24.5	0	25.7	27.7	24.6		I	20	20.8	23.2	18.6	17.8
	U	21.6	26.5	0	22.3	23.5		U	18.7	20.5	25.7	16.7	24.2
LW 15	E	14.3	15	16.4	0	13.2	IW 15	E	19.4	22.6	24.7	16.1	21.3
	O	19.5	19	19.6	18.9	0		O	24.1	25.8	20.1	27.4	20.8
	A	0	18.2	18.4	15.5	13.2		A	23.9	22.8	23.7	24	26.5
	I	17.1	0	22.4	14.8	21.3		I	20	29.7	35.1	24	22.3
	U	14.6	20.9	0	17.1	18.5		U	16.9	24.3	20.8	16	22
LW 16	E	13.3	22.7	21.6	0	16.6	IW 16	E	16.7	28.4	27.1	16.3	21.5
	O	14.8	21.8	22.3	15.7	0		O	16.5	22.3	23.7	15.2	23.1
	A	0	20.7	22.3	17.1	17.8		A	15.9	24.2	20.4	15.3	19.8
	I	15.5	0	26.7	15.3	19		I	18.5	20.3	20.5	17.2	19.4
	U	22.7	27.6	0	21.9	26.2		U	19.1	23.1	20.1	18.4	17.2
LW 17	E	17.5	25.9	28.7	0	22.8	IW 17	E	17.6	18.9	20.8	17.6	16.9
	O	14.2	21.3	21.7	13.9	0		O	20.5	21.1	23.2	24.3	24.8
	A	0	22.8	25.3	16	20.3		A	18.2	21.8	20.9	18.4	17.9
	I	15.8	0	24.2	15.6	19.7		I	26.1	25.8	28.5	22.1	23.2
	U	16.3	23.4	0	16.2	20.2		U	20.4	23.2	22.3	20.9	19.1
LW 18	E	14.8	22.1	24.3	0	19.3	IW 18	E	18.6	23.7	24.9	18.2	20
	O	16.6	23.9	26.9	16.6	0		O	24	28.3	20.4	19.3	24.1
	A	0	22.8	27	17.9	21.3		A	18.2	25.4	24.3	18.9	24
	I	15.8	0	25.2	15.5	20.4		I	20.4	27.1	23.2	19.4	18.1
	U	16.2	24.5	0	16.1	21.2		U	19.5	20.8	28.6	17.2	21.3
LW 19	E	15.7	23	26.3	0	20	IW 19	E	21.2	24.7	20	21.8	24.2
	O	15.6	23.2	25.9	15.6	0		O	16.5	23.5	24.8	20.4	27.2
	A	0	22.5	25.3	17	20.7		A	19.2	21.4	25.2	16.1	21.5
	I	15.1	0	27.4	16	21.8		I	20.3	22.1	24.7	17.8	20.9
	U	21.4	28.5	0	24.7	28		U	18.5	19.8	23.2	16.5	21.2
LW 20	E	23	28.2	32.7	0	26	IW 20	E	23.1	20.5	27.6	20.2	21.5
	O	20.5	27.9	31.5	20.4	0		O	21	24.9	23.1	22.6	24.6
	A	0	25.1	27.4	18.1	23		A	18.1	19.7	18.6	20.4	16.5
	I	24.4	0	32.1	25.3	29.1		I	19.7	21.1	20.2	17.8	20.9
	U	19.5	26.8	0	19.3	20.5		U	20.9	16.4	18.1	16.6	14.3
LW 21	E	18.2	23.2	22.1	0	21.4	IW 21	E	20.1	24	23.1	25.2	23.1
	O	19.6	27.6	31.2	19.6	0		O	19.1	25.3	21.4	28.1	26.9
	A	0	20.7	22.3	18.1	18.7		A	15.3	14.8	15.2	20	19.1
	I	18.5	0	27.5	17.6	22.4		I	24.3	29.8	22.6	21.5	28.3
	U	21.7	27.1	0	21.6	24.7		U	16.7	18.3	17.6	19.3	17.8
LW 22	E	17.6	25.9	29.4	0	21.4	IW 22	E	22	16.8	24.1	18.7	20.8
	O	18.3	22.1	15.9	15.7	0		O	20	29.9	28.4	26.2	22.1
	A	0	15	14.6	14.3	14.9		A	18.7	19.9	20.2	19.5	21.5
	I	24.5	0	28.7	25.9	24.6		I	21.3	17.3	18.6	16.4	15.4
	U	23.4	28.9	0	25.1	23.8		U	24.2	20	22.4	25.2	27.2
LW 23	E	17.6	18.1	16.7	0	17.2	IW 23	E	22	26.5	20.4	21.3	19.1
	O	20.2	18.6	21.4	19.2	0		O	17.4	18.5	18.1	20	22.4
	A	0	30.2	24.8	22.6	21.2		A	19.2	19.6	19.4	18.5	20
	I	29.5	0	30.2	15.8	20.3		I	20	15.7	15.4	14.3	13.1
	U	15.5	22.4	0	28.2	29.9		U	21.5	22.9	22.3	21.5	20.1
LW 24	E	12.2	14.9	18.4	0	17.9	IW 24	E	20.7	24.1	24.1	20.1	20.5
	O	22.4	24.8	26.4	14.9	0		O	14.4	15.4	15	22.8	18.2
	A	0	20.7	22.3	19.8	18.2		A	19.1	20.6	20.3	18.1	20
	I	15.9	0	27.8	17.3	23.1		I	20	22.7	26.9	17.8	21.2
	U	21	27.4	0	21.6	24.9		U	16.1	24.4	19.9	16	20.1
E	15.6	23.7	28.4	0	22.7	E	15.6	22.9	26.2	20.3	19.8		

Table 1. Euclidean distance comparison on letters spoken and the password letters.

	O	12.9	21.8	22.5	11.6	0		O	15.5	23.1	25.8	15.3	20
	A	0	24.1	27.4	17.5	20		A	19.8	24.5	27.3	19	22.7
	I	18.4	0	23.4	16.8	22.1		I	17.4	19.3	28.5	17.1	21.9
LW 25	U	21.4	27.5	0	21.8	26.9	IW 25	U	21.2	28.3	19.8	24.5	27.8
	E	19.2	21.5	22.3	0	21.5		E	21.4	27.2	20	24.4	26.8
	O	18.4	23.5	24.6	18.7	0		O	23.3	24.1	24.9	19	23.7
	A	0	22.4	24.3	13.4	17.8		A	20.9	24.2	23.6	19.8	21.5
	I	17.1	0	29.2	19.5	21.3	IW 26	I	20.4	21.7	22.6	21.2	23.9
LW 26	U	17.3	24.5	0	18.2	22.3		U	17.6	20.2	19.4	18.6	18
	E	15.3	22.6	29.5	0	26		E	21.7	28.8	19.8	28.2	24.6
	O	19	25.8	23.3	14.1	0		O	19.3	22.3	23.2	20	17.8
	A	0	21.5	22.4	15.3	18.3		A	26.1	26.4	24.4	22.8	19.9
	I	19.4	0	29.1	18.5	20.5	IW 27	I	20	20.1	22.4	21.2	17.6
LW 27	U	21.5	27.3	0	24.5	26.9		U	19.4	22.7	23.4	19	22.7
	E	23.4	24.2	25	0	23.8		E	24.2	23.6	20.2	20.8	21.5
	O	21	24.3	23.7	19.9	0		O	15.4	23	27.1	15.3	20.1
	A	0	21.3	22.3	20.7	23.5		A	15.3	22.2	23.8	15	19.2
	I	17.4	0	19.2	18.4	17.8	IW 28	I	15.6	22.8	24.9	15.4	19.8
LW 28	U	21.9	29	0	28.4	24.8		U	19	21.1	20.8	18.8	17.2
	E	19.4	22.4	23.4	0	17.9		E	17.3	19.7	19.9	17.2	16
	O	26.2	26.5	24.5	22.9	0		O	24.8	30.9	32.1	24.6	28.2
	A	0	20.2	22.5	21.3	17.9		A	18.1	21.7	21.7	18.2	17.8
	I	19.5	0	23.6	19.2	23	IW 29	I	21.8	25.8	26	21.4	22.5
LW 29	U	24	23.4	0	20.6	21.3		U	19.8	22.8	21.7	20	19.6
	E	19.5	23.7	24.5	0	20.1		E	19	20.5	20.2	18	19.8
	O	18.9	23.4	26.4	19.8	0		O	20	22.7	26.9	17.8	21.2
	A	0	19.8	18.7	18.3	17.5		A	15.6	20.1	25	15.3	20.2
	I	19.1	0	18.6	17.8	19.9	IW 30	I	16	24.3	20.1	15.9	21
LW 30	U	22.8	24.6	0	23.8	23.2		U	15.6	22.9	26.2	20.9	19.8
	E	18.4	24.2	26.4	0	20.4		E	15.4	23	25.7	15	30.9
	O	21.6	25.4	25.1	22.7	0		O	20	24.5	27.3	19	22.7
	A	0	24.9	26.7	22.4	24.2		A	17.5	19.8	28.4	17	21.8
	I	25.0	0	25.2	23	23.1	IW 31	I	23.3	29.3	20.2	23.1	26.8
LW 31	U	22.4	23.9	0	22.1	20.9		U	21.1	27.7	31.2	20.1	25.1
	E	19.3	21.7	20.2	0	19.6		E	21.4	28.8	32.4	21.3	20.1
	O	24	25.4	24.1	26	0		O	21.2	29.4	23.6	19.7	22.2
	A	0	22.4	26.4	19.8	24.3		A	24	19.7	31.4	22	28.1
	I	18.9	0	26.5	18.7	22.3	IW 32	I	19.5	21.6	21.3	19.1	17.8
LW 32	U	18.5	23.5	0	18.3	25.2		U	17.2	19.7	19.8	17.1	15.9
	E	19.8	25.6	23.4	0	23.4		E	25	31.1	32.2	24.8	28.2
	O	21.7	25.9	27.2	19.8	0		O	18.2	21.7	21.9	19.3	17.8

the Euclidean distance with reference (password) "A" is equal to zero and has a larger number if compared to other reference letters (I, U, E, and O). Therefore, the letter A spoken by LW 1-32 is identified as A and fits with the password. That situation will also occur when that particular LW speaks the other letters (I, U, E, and O). Therefore, when an LW says A, I, U, E, and O, the spoken voice will be recognized as A, I, U, E, and O and then the access permit is granted.

When IW 1-32 say the password letters, the spoken voice will not be recognized appropriately. In the IW table, it can be noticed that the spoken letters are identified as different letters, so the password letters spoken by the IW are identified as other letters. This condition makes the IW access permit not be granted. For example, when the IW say "aiueo", the spoken voice will be identified as "eeuee". This disagreement is caused by the fact that everyone has unique voice characters. The characters are influenced by the type of voice (alto, soprano, etc.), the shape of the teeth, and the shape of the mouth. Based on the different character of each person, it can be identified whether the voice has an access permit or not.

Based on the above discussion, it can be understood that all password letters spoken by the LW will be recognized appropriately, and all

password letters spoken by the IW will be recognized as different letters. Table 2 shows the result of the letters classification. All LW will have access permit, and all IW will not have access permission.

Table 2. Letters Classification of Each Employees.

Kind of Employees	A	I	U	E	O	Keterangan	Kind of Employees	A	I	U	E	O	Keterangan
LW 1	A	I	U	E	O	Has access permit	IW 1	E	E	U	E	E	Has no access permit
LW 2	A	I	U	E	O	Has access permit	IW 2	E	A	E	E	E	Has no access permit
LW 3	A	I	U	E	O	Has access permit	IW 3	E	E	E	E	E	Has no access permit
LW 4	A	I	U	E	O	Has access permit	IW 4	E	O	E	E	E	Has no access permit
LW 5	A	I	U	E	O	Has access permit	IW 5	O	A	O	E	E	Has no access permit
LW 6	A	I	U	E	O	Has access permit	IW 6	O	O	A	A	O	Has no access permit
LW 7	A	I	U	E	O	Has access permit	IW 7	E	E	E	O	A	Has no access permit
LW 8	A	I	U	E	O	Has access permit	IW 8	E	E	E	E	E	Has no access permit
LW 9	A	I	U	E	O	Has access permit	IW 9	E	O	U	E	E	Has no access permit
LW 10	A	I	U	E	O	Has access permit	IW 10	E	E	E	E	E	Has no access permit
LW 11	A	I	U	E	O	Has access permit	IW 11	O	E	A	E	E	Has no access permit
LW 12	A	I	U	E	O	Has access permit	IW 12	A	E	E	O	E	Has no access permit
LW 13	A	I	U	E	O	Has access permit	IW 13	O	E	E	E	E	Has no access permit
LW 14	A	I	U	E	O	Has access permit	IW 14	E	O	E	E	U	Has no access permit
LW 15	A	I	U	E	O	Has access permit	IW 15	I	A	E	E	E	Has no access permit
LW 16	A	I	U	E	O	Has access permit	IW 16	E	O	O	O	A	Has no access permit
LW 17	A	I	U	E	O	Has access permit	IW 17	O	E	O	E	E	Has no access permit
LW 18	A	I	U	E	O	Has access permit	IW 18	A	O	E	U	A	Has no access permit
LW 19	A	I	U	E	O	Has access permit	IW 19	E	E	E	E	A	Has no access permit
LW 20	A	I	U	E	O	Has access permit	IW 20	O	E	O	A	A	Has no access permit
LW 21	A	I	U	E	O	Has access permit	IW 21	I	E	A	I	A	Has no access permit
LW 22	A	I	U	E	O	Has access permit	IW 22	A	O	I	O	A	Has no access permit
LW 23	A	I	U	E	O	Has access permit	IW 23	E	O	O	E	A	Has no access permit
LW 24	A	I	U	E	O	Has access permit	IW 24	E	E	E	A	E	Has no access permit
LW 25	A	I	U	E	O	Has access permit	IW 25	E	E	U	U	E	Has no access permit
LW 26	A	I	U	E	O	Has access permit	IW 26	E	A	A	U	O	Has no access permit
LW 27	A	I	U	E	O	Has access permit	IW 27	O	O	E	U	E	Has no access permit
LW 28	A	I	U	E	O	Has access permit	IW 28	O	E	O	O	E	Has no access permit
LW 29	A	I	U	E	O	Has access permit	IW 29	E	O	O	E	E	Has no access permit
LW 30	A	I	U	E	O	Has access permit	IW 30	E	E	A	E	E	Has no access permit
LW 31	A	I	U	E	O	Has access permit	IW 31	E	U	E	O	E	Has no access permit
LW 32	A	I	U	E	O	Has access permit	IW 32	I	O	O	E	O	Has no access permit

The research results show that the model proposed in this research can be used as a biometrics security system and can enhance the security of NPP by using access restriction. Simpler pre-processing and simpler tool can be used to recognize and classify the voice data. Simpler tool and simpler pre-processing equal to lower cost for the implementation. However, there is still a possibility of classification and voice recognition error. The error may occur if an IW knows the password and can mimic the LW voice. This possible error can be overcome by combining voice password with other biometric passwords such as fingerprints [43,44], retina [45], iris [46], and face [47]. Further research is required to combine these passwords.

CONCLUSION

The Fast ICA method and the proposed model can be used to classify voices for deciding whether an employee has the access permit or not. The method seeks the features vector of the voices by searching the components that are statistically independent. The minimum Euclidean distance was used to identify the spoken letters based on the comparison of the features vector. The research used 32 data training and 64 data testing. The data training was used to determine the features vector of the voices that have access permit. The data testing was used to test the accuracy of the proposed model. The research's results show that Fast ICA and minimum Euclidean distance can 100 % distinguish between the employees who have access permit and the employees with no access permit. Based on the result accuracy, the model proposed in this research can be used as a biometrics security system.

ACKNOWLEDGMENT

The authors would like to thank Dr. Risanuri Hidayat for the support and the knowledge that has been shared.

REFERENCES

1. Anonymous, Masterplan Revitalisasi PUSPIPTEK dan Pengembangan I-STP, Kemenristek (2013). (in Indonesian)
2. Anonymous, Cetak Biru Pembangunan Reaktor Daya Eksperimental (RDE) 2014-2020, BATAN (2014). (in Indonesian)
3. J.R. Lovering, A. Abdulla and G. Morgan, Energy Policy **139** (2020) 1.
4. P. Kumar, L.K. Singh and C. Kumar, Nucl. Eng. Technol. **52** (2020) 560.
5. D.K, Gattie, Electr. J. **31** (2018) 23.
6. M. Bunn and E. Harrell, *Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey*, in: The Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School (2014).
7. A. Gumaei, R. Sammouda, A.M.S. Al-Salman *et al.*, J. Parallel Distrib. Comput. **124** (2019) 27.
8. A.K. Singh and C. Bhatnagar, Procedia Computer Science **46** (2015) 596.
9. M. Adamek, M. Matysek and P. Neumann, Procedia Engineering **100** (2015) 169.
10. K.K. Kumbhare and K.V. Warkar, Procedia Comput. Sci. **78** (2016) 382
11. Z.M. Hira and D.F. Gillies, Adv. Bioinformatics **2015** (2015) 1.
12. Z. Yao, J.L. Bars, C. Charrier *et al.*, IET Biometrics Journal **5** (2016) 243.
13. T. Sakai and S. Doshita, IEEE Trans. Electron. Comput. (1963) 835.
14. S. Kamalinia, M. Shahidehpour and L. Wu, Appl. Energy **133** (2014) 112.
15. S. Paul, T.K. Das, P. Saha *et al.*, *Comparative Analysis of Two Different System's Framework for Text Dependent Speaker Verification*, Proceedings of The 2015 International Conference on Circuit, Power, and Computing Technologies (ICCPCT) (2015) 1.
16. G. Guanyu, K. Kai and G. Shengxiao, *Design and Implementation of a High-Performance Client / Server Voiceprint Recognition System*, Proceedings of IEEE International Conference on Information and Automation (2012) 704.
17. R. Nair and N. Salam, *A Reliable Speaker Verification System Based on LPCC and DTW*, Proceedings of The 2014 IEEE International Conference on Computational Intelligence and Computing Research (2014) 1.
18. T. Paul and S. George, Int. J. Eng. Sci. Emerg. Technol. **6** (2013) 344.
19. Y.B. Monakhova and D.N. Rutledge, Talanta **208** (2020) 1.
20. S. Zhang and C. Zhao, Chemo. and Intel. Lab.

- Systems **185** (2019) 47.
21. S. Michelmann, M.S. Treder, B. Griffiths *et al.*, Journal of Neuro. Method **307** (2018) 125.
 22. X. Song, S. Bhinge, R.L. Quiton *et al.*, Journal of Neuro. Method **326** (2019) 1.
 23. A. Jimenez-Gonzalez and N. Castaneda-Villa, Biomed. Signal Proc. and Control **58** (2020) 1.
 24. L.N. Anishchenko, *Independent Component Analysis in Bioradar Data Processing*, Progress In Electromagnetic Research Symposium (PIERS) (2016) 8.
 25. R.T.F.A. King, X. Tu and L. Dessaint, *Independent Component Analysis for Feature Reduction in Critical Clearing Time Estimation*, Proceedings of The 2016 IEEE Can. Conf. Electr. Comput. Eng. Indep. (2016) 1.
 26. L. Shen, Y. Yao, H. Wang *et al.*, IEEE Trans. Veh. Technol. **65** (2016) 8322.
 27. D. Dharmaprani, H.K. Nguyen, T.W. Lewis *et al.*, *A Comparison of Independent Component Analysis Algorithms and Measures to Discriminate between EEG and Artifact Components*, Proceedings of The 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) (2016) 825.
 28. M.S. Srivastava and J. Multivar. Anal. **97** (2006) 2057.
 29. K.S. Sodhi and M. Lal, Int. J. Appl. or Innov. Engeering Manag. **2** (2013) 341.
 30. B. Vinzamuri, Y. Li and C.K. Reddy, IEEE Trans. Knowl. Data Eng. **29** (2017) 2111.
 31. D. Tomar and S. Agarwal, Int. J. Database Theory Appl. **7** (2014) 99.
 32. H.J. Jo, S.J. Gotts, R.C. Reynolds *et al.*, J. Appl. Math. **2013** (2013) 1.
 33. M. Abdel-nasser, J. Melendez, A. Moreno *et al.*, Int. Journal of Optics **2016** (2016) 1.
 34. T. Li, W. Liu, H. Liu *et al.*, Graphical Models **101** (2019) 17.
 35. G. Li and Y. Hu, Energy & Buildings **183** (2019) 311.
 36. H.R. Schubert, A.C. Jalba and A.C. Telea, Computers & Graphics **87** (2020) 30.
 37. A. Hyvärinen and E. Oja, Neural networks **13** (2000) 411.
 38. E. Ollila and V. Koivunen, Signal Processing **89** (2009) 365.
 39. R. Oostenveld and P. Praamstra, Clin. Neurophysiol. **112** (2001) 713.
 40. Halim and Ishak, Aust. J. Basic Appl. Sci., **8** (2014) 67.
 41. R. Hill, IPCT Journal **6** (1998) 1.
 42. M. Hassaballah, A.A. Abdelmgeid and H.A. Alshazly, Studies in Computational Intelligence **630** (2016) 11.
 43. L.H. Thai and H.N. Tam, International Journal Comput. Sci. **7** (2010) 11.
 44. M. Redhu and Balkishan, Int. J. Eng. Res. Appl. **3** (2013) 2488.
 45. F. Sadikoglu and S. Uzelaltinbulat, Procedia Comput. Sci. J. **102** (2016) 26.
 46. L. Hanfei and C. Jiang, Adv. Sci. Technol. Lett. J. **81** (2015) 85.
 47. F. Ahmad, A. Najam and Z. Ahmed, Int. J. Comput. Sci. **9** (2012) 169.