International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 9611-9629

http://www.ripublication.com

Integrated Multi-Stage Biometric System Design

[1]Ravi Lakshmanan,[2] Dr Sathish Kumar Selvaperumal, [3] Chow Hin Mun

[1,2]Senior Lecturer, School of Engineering,
Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia.
[3] IT support Engineer, Fusionex Corp Sdn Bhd, Kuala Lumpur, Malaysia
E-mail: [2]skspresearch@gmail.com,[1]ravi@apu.edu.my,[3]chm1990@hotmail.my

Abstract

In this paper, an integrated multi stage biometric system design is proposed using speech, face and finger print along with Artificial Neural Network (ANN). The voice recognition subsystem utilises Mel-frequency Cepstrum Coefficient (MFCC) feature extraction algorithm to represents the voice signal of the user in the form of cepstrum of the voice derived from Discrete Cosine Transform (DCT) on the log power spectrum on a non-linear Mel-scale frequency. Face recognition subsystem utilises closing algorithm image morphology that extracts the features of the face based on the facial outline, via superimposing of the dilation and erosion of the facial image. Fingerprint recognition subsystem utilises minutiae extraction to extract the ridge termination and bifurcation points of the fingerprint. The integrated biometric recognition system consists of three neural networks configured consistently with 50 hidden neurons. The simulation result yielded an overall False Rejection Rate of 4% and False Acceptance Rate of 8%. Also, the calculated average time taken to train the neural network is 3.848 seconds only.

Keyword- Artificial Neural Network, Fast Fourier Transform, Direct Cosine Transform, Mel Frequency Cepstrum Coefficient.

INTRODUCTION

In the past two decades, electronic security systems have been extensively researched and developed, due to the increasing demands for high level security protection and encryption. With gradual advancement of technology, specifically in the field of Very Large Scale Integration (VLSI) technology applied in embedded system, security systems are applied widely in various areas, from software computer-based access control to hardware-based sophisticated vault lock, replacing the traditional mechanical key and lock system. Hence, a wide range of security systems has been developed and implemented to prevent unauthorised access, hacking and protection of intellectual property.

Traditional electronic security systems are implemented using user-password based approach, where users are required to key in their username and an assigned password for verification. This type of security systems are usually found in software computer-based application such as user profile access and online banking account management.

Radio frequency identification (RFID) and token-based security systems are applied on physical hardware security systems such as door lock access. Similar to key and lock system, users are required to use an object such as ID cards, tags, etc. to identify and verify themselves as the authorised user to gain access.

The next generation of security systems is based on verification of biometric signature. Biometric refers to the measure of biological characteristics of the human body. Biometric characteristics are unique among every human and remain permanent to the human, so as the means to identify the user is always available, cannot be lost unlike the previously mentioned security system (Gregory & Simon, 2008).

The main concern of all security systems is the integrity of the system towards protection of users' data and assets. Problems and limitations of traditional user-password based systems are generally associated with the lack of uniqueness of the password. To prevent this, users are encourage to set up complicated password, however this make the password hard to remember and easily forgotten. RFID-based security system eliminates the problem of remembering password, where access cards unique to each user are provided and used for identification. However, users are not able to gain access to the system if they lost their access card. This system is also vulnerable to unauthorised access if the access card has been stolen or reproduced by unauthorised user.

With the advent of biometric security system, problems and limitations in previous security systems can be solved. Biometric signatures act as a unique feature to identify users and remain part of the users' body. However, the problem in the current use of single biometric system can still be easily hacked using fake credentials. This is known as replay attack (Gregory & Simon, 2008), where an intruder is able to perform a correct authentication to access the system by capturing the biometric data of the authorised user. In the case of fingerprint recognition, fake rubber fingers can be easily imprinted with the authorised fingerprint of the user, which is used as a faked credential to gain access of the system.

Matching flaws have been a main research problem in biometric security system, where excessive False Acceptance Rate (FAR) and False Rejection Rate (FRR) will cause the system to incorrectly recognise users. FAR refers to the percentage of accepting unauthorised user, while FRR refers to the percentage of rejecting authorised user (Vasuhi et al., 2010). A lot of researches have been focus on developing robust and accurate biometric recognition system to improve on the FAR and FRR values. Various intelligent systems such as fuzzy logic and neural networks have been applied to improve biometric recognition rate.

In addition, the use of biometric recognition system is nearly universal to everyone. However, using only a type of biometric measure will limit the scope of usage of the system. Take an example of voice recognition system, if the person is mute, voice recognition cannot be perform on that person. In addition, certain cases

do not provide the proper environment to perform specific type of biometric measure, such as fingerprint system cannot be implemented in dirty environment or workplace. Therefore, there is a need to implement multiple biometric measures to provide usage and flexibility to those situations.

The identified research problems in existing biometric security system are vulnerability to replay attacks, matching flaws and constrained usage in single type biometric. Therefore, by integrating multiple biometric measures into a multi-stage system with the use of intelligent neural network pattern recognition approach, the proposed system is able to strengthen the level of security, improve on recognition rate and provide usage flexibility in biometric measures.

After the introduction in section I, the rest of the paper is organized as follows. The implementation of the proposed method is detailed in section II. The experimental results are discussed in section III and the simulated results are discussed in section IV. Finally, the conclusion is concluded in section V.

II. PROPOSED METHOD

Figure 2.1 shows the block diagram of the proposed design for the intelligent biometric security system. The approach in proposing a model for the intelligent biometric security system is based on segmenting the overall system into three recognition subsystems. The important design aspects of the recognition subsystem are the feature extraction algorithms and the configuration of the neural network. Each recognition subsystem has its own feature extraction algorithm; voice signals are extracted based on Mel-frequency Cestrum Coefficients (MFCC) algorithm, facial images undergo digital image processing based on closing algorithm image morphology and fingerprint features are extracted based on minutiae points.

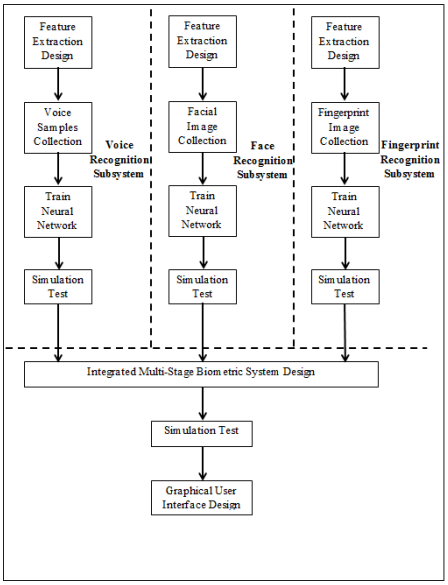

Figure 2.1: Operation Flowchart of the Proposed Design

These extracted features for each of the biometric measures for the subsystems are used as inputs to train the neural networks, which are configured consistently in all three subsystems based on feedforward network with back propagation training. These neural networks also act as a database to store the biometric templates of the users. The output decision of the neural network is sent to the GUI for validation.

Before the recognition system can be utilised, user enrolment process have to be done where the neural network is trained with multiple biometric samples of the users, for each of the recognition subsystem as shown in the flow chart Figure 2.2. Then, the overall recognition system can be tested.

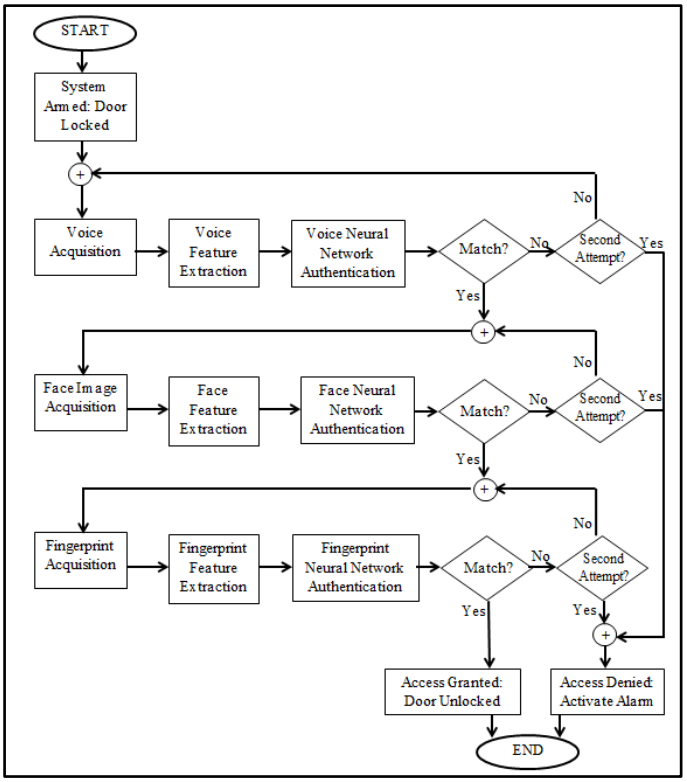

Figure 2.2: Operation Flowchart of the Proposed Design

The authentication process is same all three of the recognition subsystems, which begins with the acquisition of input biometric data, performing feature extraction and using the trained neural network to authenticate the input biometric data with the stored template. The authentication process is in a stage-by-stage basis, where a sequential successful authentication in the order of voice, face and fingerprint subsystems are required to unlock the door and granted access. For instance, if the users succeed in voice and face authentications, but failed in fingerprint authentication, the door will still remain locked and access is denied. Two attempts are given for authentication in each recognition subsystem, when the users fail to authenticate themselves on the second attempt, the door will remained locked and an alarm will sound, to indicate access denied.

The design and implementation of the feature extraction algorithm for voice recognition system is done by first writing the source code in MATLAB. Figure 2.3 shows the block diagram of the feature extraction processes for voice recognition system based on Mel-Frequency Cepstrum Coefficient (MFCC) algorithm.The novelty provided is that silence detection and hamming window technique used for pre-processing is integrated with the MFCC algorithm and neural network.

A. MFCC Feature Speech Recognition

1. Voice Acquisition via Sound Card

Based on Figure 2.3, the processing chain of the voice recognition system begins by first obtaining the voice sample of the user in the form of continuous voice signal, via the sound card of the computer.

The continuous voice signal will be converted into discrete voice signal, with sampling frequency set to 10 kHz with duration of the recording time set to 1 second. The sampling time is given by:

$$Sampling\ Time\ (nT) = Sampling\ Frequency \times Recording\ Time$$

$$Sampling\ Time\ (nT) = 10000\ Hz \times 1\ sec$$

$$Sampling\ Time\ (nT) = 10000\ samples$$

According to Nyquist limit, the sampling frequency is twice the amount of the maximum analogue frequency, such as:

$$Sampling\ Frequency = 2 \times Maximum\ Analogue\ Frequency$$

$$Maximum\ Analogue\ Frequency = \frac{Sampling\ Frequency}{2}$$

$$Maximum\ Analogue\ Frequency = \frac{10000}{2}$$

$$\therefore Maximum\ Analogue\ Frequency = 5000\ Hz$$

Hence, the maximum analogue frequency of the continuous voice signal that can be obtained is 5000 Hz, which is within sufficient range that covers the voice frequency produced by human.

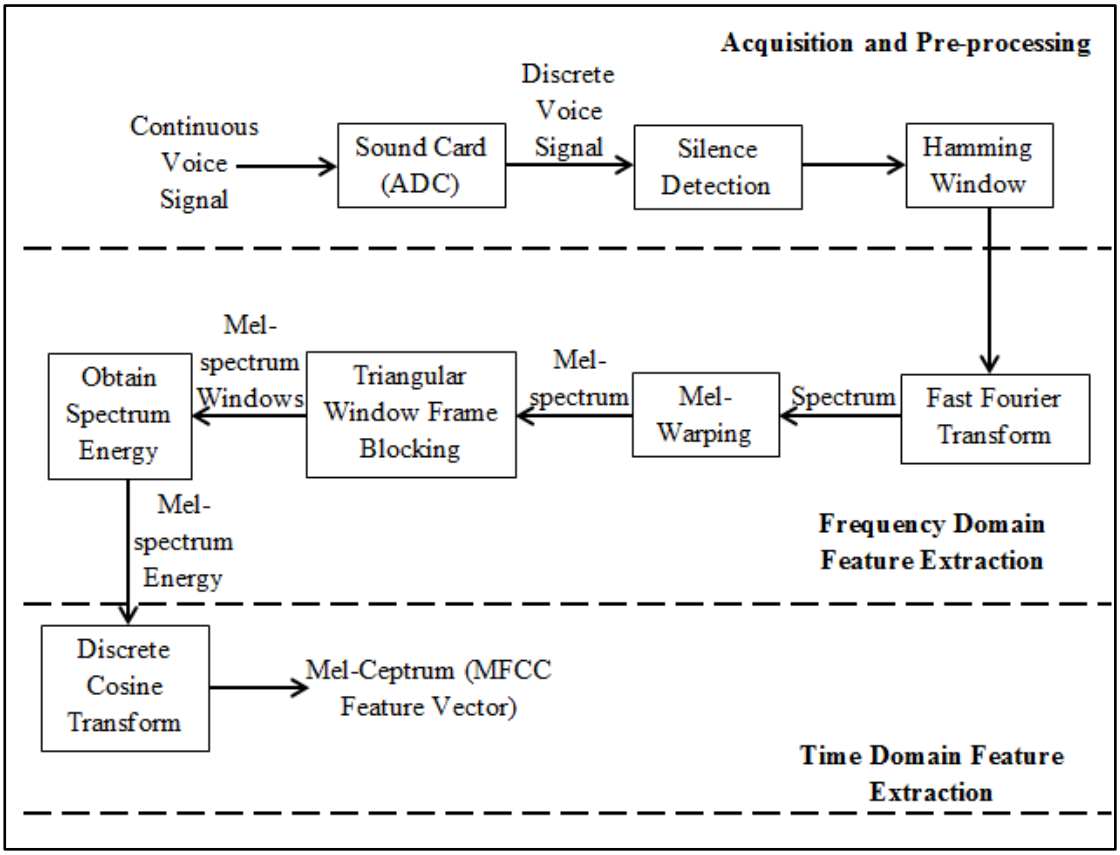

Figure 2.3: Proposed Automated Speech Recognition Method

2. Silence Detection

Next, the voice signal will undergo pre-processing to condition the signal into a suitable format for further processing during feature extraction. Silence detection is used to detect the silent portion of the voice signal, where the high amplitude portion of the voice signal will be time-shifted to the starting point, at n = 0. As a result, any silent portion of the voice signal at the beginning will be eliminated, which acts to normalize the voice signal. The absolute value of the voice signal amplitude must be above 0.05 to be considered as non-silent portion of the signal.

3. Hamming Window

The next pre-processing step is to apply Hamming windowing technique in time domain to the voice signal. A Hamming window with 4000 samples is defined, and then fit into 10000 samples of the voice signal. Hamming window is used to condition the voice signal to suit the condition of Mel-frequency warping at the later stage of the feature extraction process.

4. Fast Fourier Transform (FFT)

After all the pre-processing is done, the voice signal is transformed from time domain to frequency domain using Fast Fourier Transform (FFT). The FFT of the voice signal is symmetrical at the central frequency, 5000 Hz, which also corresponds to the defined maximum analogue frequency of the voice signal.

5. Mel-Warping

Mel-warping is done to transform the spectrum of the voice signal obtained after FFT, into Mel-spectrum of the voice signal. In order to perform Mel-warping, the Mel-frequency scale must be defined first. After defining the Mel-frequency scale, Mel-warping can be done by combining the spectrum of the voice signal in frequency domain with the Mel-frequency scale.The process of Mel-warping is crucial in the feature extraction stage, as the frequency of the voice signal is transformed into Mel-frequency scale, in the attempt to emulate the biological hearing sense in human that perceive the frequency contents of voice signal, in a non-linear scale similar to the Mel-frequency.

6. Triangular Window Frame Blocking

Frame blocking serves to truncate the Mel-spectrum of the voice signal into individual frame. To do this, a number of 20 overlapping triangular windows are defined. The 20 triangular windows overlap each other with a bandwidth of 50 Hz. For instance, the eleventh triangular window will occupy the range of 500 Hz to 600 Hz, overlapping 50 Hz with the tenth triangular window. This is done to prevent discontinuities of the resultant truncated Mel-spectrum voice signal. After all the 20 triangular windows have been defined, the voice signal in the form of Mel-spectrum can be truncated into 20 individual frames.

7. Obtain Spectrum Energy

The spectrum energy of the voice signal can be calculated by first summing the square of the Mel-spectrum within the frame. After that, a vector of spectrum energy can be obtained by summing the log of all the 20 spectrum energies obtained from the 20 frames.

8. Discrete Cosine Transform (DCT)

The final step of the feature extraction is to transform the log of the spectrum energy from frequency domain back to time domain, using Discrete Cosine Transform (DCT). Finally, the output of the MFCC feature extraction algorithm produces the Mel-cepstrum coefficient of the voice signal, which can be used to uniquely represent the voice of the user and train the neural network during the pattern recognition process.

B. Face Feature Recognition

Figure 2.4 shows the block diagram of the feature extraction process for face recognition subsystem based on closing algorithm image morphology. The novelty provided is that the histogram equalization technique is used for preprocessing integrated with the Closing algorithm image morphology and Neural network.

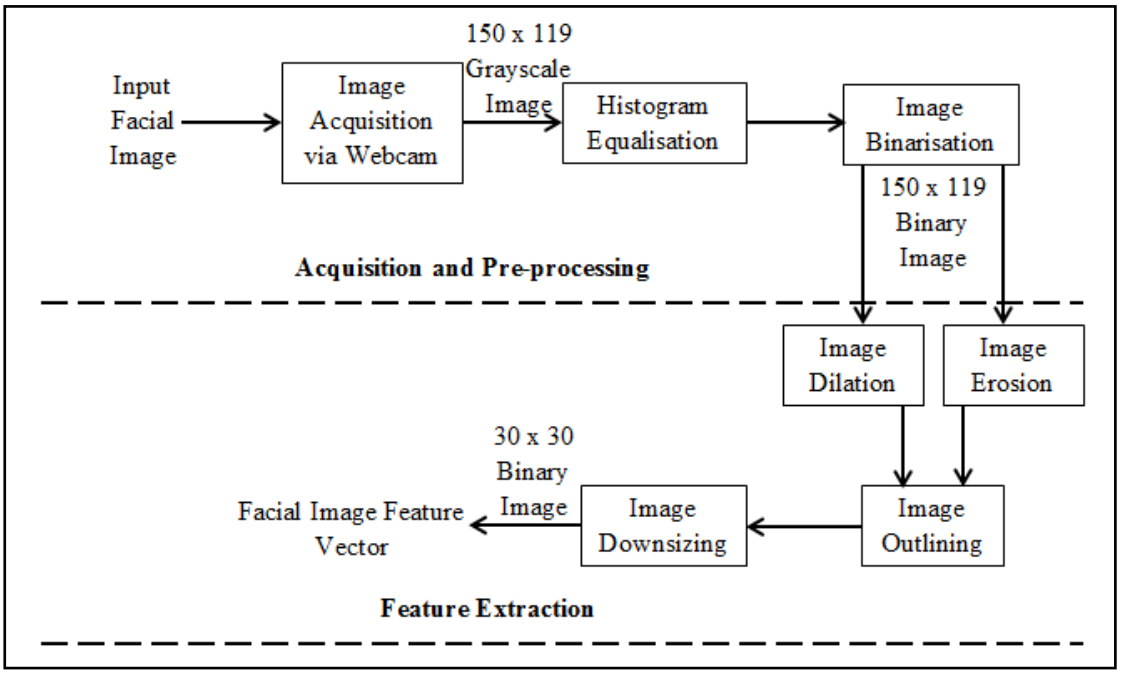

Figure 2.4: Block diagram of the Feature Extraction Process for Face Recognition System

The Closing algorithm image morphology algorithm is detailed as below:

Step 1: Image Acquisition via Webcam

Based on Figure 2.1, the processing chain of the face recognition subsystem begins by first obtaining the facial image of the user via the webcam of the computer and using the image acquisition toolbox in MATLAB to configure the acquisition parameters. The acquired facial image can then be saved as Tagged Image File Format (TIFF) and exported to the MATLAB workspace for pre-processing.

Step 2: Histogram Equalization

Image histogram equalization is done to enhance the contrast of the image by equally distributing the colour contrast of the image. After performing image histogram equalization, the resultant facial image shows a more distinctive outline of the face with respect to the background.

Step 3: Image Binarization

The next pre-processing is to perform image Binarization to convert the grayscale

image to binary image. The resultant facial image will be in the form of 150 x 119 represented by binary bits of 1 and 0.

Step 4: Image Dilation
Facial image feature extraction using closing algorithm begins with first creating a morphological structuring element. A flat, disk-shaped structuring element 'SE', with the value of radius, 3is created. This morphological structuring element is used with the binarized facial image to perform image dilation. The resultant facial image is the output of binary dilation through the decomposition of the defined structuring element 'SE'.

Step 5: Image Erosion
Similar to image dilation, the defined morphological structuring element 'SE' is used with the binarized facial image to perform image erosion. The resultant facial image is the output of binary erosion through the decomposition of the defined structuring element 'SE'. When performing binary dilation along with binary dilation, erosion is applied by automatically using the binary image packing to speed up the dilation.

Step 6: Image Outlining
After image dilation and erosion are done, the facial image outline. Closing algorithm image morphology involves obtaining the outline of the face shape and certain details of the face structure such as the eyes, nose and mouth. This is done by superimposing the dilation and erosion of the facial image. The resultant facial image illustrates the outline of the facial image, where the details of the eyes, nose, mouth and even the shape of the hair can be seen.

Step 7: Image Downsizing
Image downsizing serves to compress the extracted features from the facial outline, to a smaller dimension, in order to suit the process for training the neural network for facial recognition. The resultant downsized facial is a 30 x 30 image represented by binary bits of 1 and 0. Finally, the downsized facial image will be reshaped into a column vector with 900 feature points of binary number, to train the neural network.

C. Finger Print Feature Recognition

The design and implementation of the future extraction algorithm for fingerprint recognition system is done by first writing the source code in MATLAB. Figure 2.5 shows the block diagram of the feature extraction processes for fingerprint recognition system based on fingerprint minutiae points feature extraction algorithm:

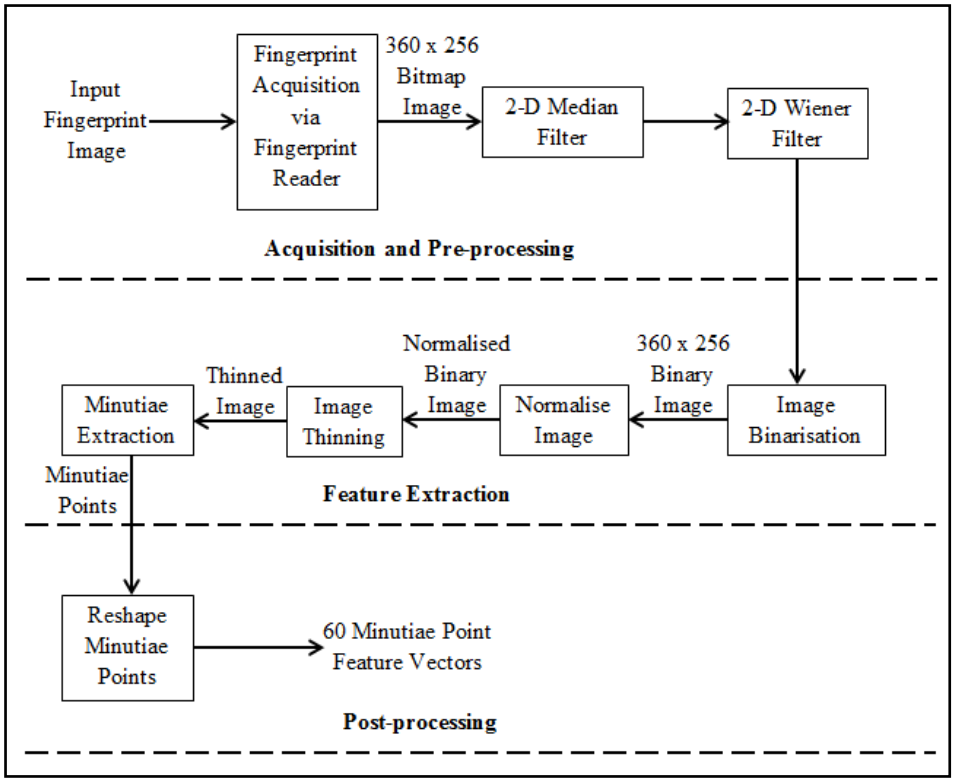

Figure 2.5: Block Diagram of Fingerprint Minutiae Points Feature Extraction Algorithm

Step 1: Fingerprint Acquisition via Fingerprint Reader
Based on Figure 2.5, the processing chain of the fingerprint recognition subsystem begins by first obtaining the fingerprint image of the user via a fingerprint reader and using a Security Development Kit (SDK) known as UniFinger, as a software interface to save the fingerprint image. Using the user interface, the captured fingerprint image can be saved in the computer as a bitmap image file, where subsequent processing can be done by loading the fingerprint image over to MATLAB.

Step 2: Image Enhancement via Filtering
The captured fingerprint image in the form of 360 x 256 bitmap file is exported to the workspace and pre-processing is done to enhance the quality of the image. The fingerprint image will undergo two types of noise removal filters which are 2-D Median filter and 2-D adaptive Wiener filter.The fingerprint image after applying Median filter contains less dotted points. While the fingerprint image after applying Wiener filter have a smoother edge and better image quality. As a result, the ridge pattern of the fingerprint can be clearly seen and the feature points can be properly extracted in the following processes.

Step 3: Image Binarization
Fingerprint feature extraction begins with first converting the pre-processed

fingerprint image into binary. The resultant image seen will be in the form of 360 x 256 represented by binary bits of 1 and 0.

Step 4: Image Normalization
The next step in feature extraction is to normalize the dimension of the fingerprint image, to focus on the Region of Interest (ROI). The resultant fingerprint image shown illustrates the ROI of the fingerprint, where the more distinctive ridge pattern of the fingerprint is focused, so that the feature points can be extracted easily and consistently.

Step 5: Image Thinning
Image thinning, also known as skeletonisation is done to thin down the ridge pattern into a single line. Thinning of the fingerprint image shows a single line skeletal view of the fingerprint ridge pattern.

Step 6: Minutiae Extraction
Minutiae extraction algorithm is based on finding the termination and bifurcation points in the ridge pattern of the fingerprint. The resultant extracted minutiae image consists of a combination of red and blue markings. The red markings represent the ridge termination points, while the blue markings represent the ridge bifurcation points.

Step 7: Reshape Minutiae Points
The position of the minutiae points is described by their coordinates in the form of x-axis and y-axis relative to the origin. Hence, these minutiae points will be reshaped into 60 feature vectors. Pythagoras' Theorem is used to determine the exact point of the ridge termination and bifurcation, based on their coordinates on the x-axis and y-axis. Finally, these points are combined into a column vector of 60 feature vectors, which will be used in training the neural network.

D. Neural Network:

After obtaining and compiling all the extracted biometric data from the users, the next procedure is to configure and train the neural network using the neural network toolbox utility in MATLAB. However, due to the limited number of biometric samples which are 25 samples, the number of samples is duplicated 4 times, which gives a total of 100 samples. This would be sufficient to properly train the neural network.

In supervised training of the neural network, the biometric feature vectors are the inputs to the neural network, where the neural network will be trained to map the corresponding targets of the inputs. The 100 input data containing the biometric feature vectors will be randomly divided into 70% for training data, 15% for validation data and 15% for testing data. Training data constitute the major samples, as they are presented to the network during training, where the value of the weight and bias are adjusted to reduce the error rate in recognising the pattern. Validation data are used to measure the generalisation of the neural network. The training of the

neural network will be stopped when generalisation stops improving, as the neural network starts to memorise the pattern, instead of learning to recognise. Testing data have no effect on the training, only to provide independent measure on the performance of the network during and after training.

The structure of the neural network is be configured as feedforward network. The number of hidden neurons in the hidden layer can be defined. For the purpose of simulation test and analysis, three different neural networks are configured with 10, 50 and 100 hidden neurons. Table 2.1 shows a summary on the number of neuron for each layer of the neural networks for each of the recognition subsystem:

Table 2.1: Number of Neuron in Each Layer

Recognition Subsystem	Input Neuron	Hidden Neuron	Output Neuron
Voice	20	10, 50, 100	5
Face	900	10, 50, 100	5
Fingerprint	60	10, 50, 100	5

The number of input neuron will correspond to the number of input biometric feature vector. For voice recognition subsystem, there are 20 MFCC feature vectors and hence there are 20 input neurons, same goes for the face and fingerprint recognition subsystem. The output layer consists of 5 output neurons which correspond to the number of users enrolled to the system. Hence, the output layer is acting as similar to the database that stores the template of the enrolled users. The transfer function used in these feedforward neural networks is tangent-sigmoid, which is commonly used for pattern recognition.When the neural network is properly configured, training can be commenced, with the use of a training algorithm known as scaled conjugate gradient back-propagation.

III. EXPERIMENTAL RESULTS

Database

For the proposed voice recognition system, testing is done on two different scenarios which are word independent recognition and word dependent recognition. 5 voice samples of 5 users have been obtained, which provide a total of 25 voice samples, where these voice samples act as the voice biometric data that will undergo MFCC feature extraction. The extracted MFCC feature vectors of these voice samples are used to train the neural network.

For the first case scenario for simulating word independent recognition, the voice recognition system is tested in recognizing the users when all the uttered passwords are same; hence it is a word independent recognition basis. Table 3.1 shows the name of the users, user ID and the uttered password ‘Activate’, which is same for all users.

Table 3.1: Users Details for Word Independent Simulation

User ID	Username	Uttered Password
1	Ivan	Activate
2	Paul	Activate
3	Ian	Activate
4	Esther	Activate
5	Steven	Activate

For the second case scenario for simulating word dependent recognition, the voice recognition system is tested in recognizing the users when the uttered passwords are different; hence it is a word dependent recognition basis. Table 3.2 shows the name of the users, user ID and the different uttered password assigned to each user.

Table 3.2: Users Details for Word Dependent Simulation

User ID	Username	Uttered Password
1	Ivan	Omega
2	Paul	Alpha
3	Ian	Beta
4	Esther	Delta
5	Steven	Hello

For face recognition subsystem, 5 facial image samples are collected from 5 users, summing up to a total of 25 facial image samples, where these facial image samples acting as the face biometric data will undergo closing algorithm image morphology feature extraction. The extracted facial feature vectors will be used to train the neural network. The facial images are taken with a slight variation from each other, in terms of the capture angles, facial expressions and lightings. This is done so that the neural network can be trained to recognise the face of the users at different conditions.

For fingerprint recognition subsystem, 5 fingerprint samples taken are collected from 5 users, summing up to a total of 25 fingerprint samples, where these fingerprint samples acting as the fingerprint biometric data will undergo minutiae points feature extraction. The extracted minutiae point feature vectors of these fingerprint samples will be used to train the neural network.

Graphical User Interface

Graphical User Interface (GUI) is designed to replace the MATLAB command line interaction when operating the system. The GUI maintains the same function and processing flow, but it is design to provide user-friendly interaction when using the system. The layout of the GUI is design using GUI Development Environment (GUIDE) in MATLAB and a script file is generated containing the source code to implement all the recognition function into the GUI. Four GUIs have been design, one

main GUI and three GUIs for the individual recognition subsystem.Figure 3.1 shows the design of the Main GUI:

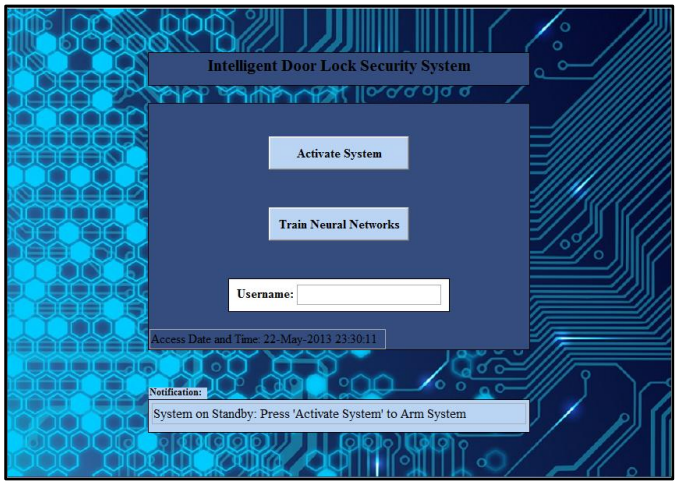

Figure 3.1: Main GUI

The Main GUI represents the input stage of the overall system, where it functions to activate the peripheral door lock system through serial port communication, user enrolment by training the neural networks and username input. In addition, the date and time of access is displayed for reference. A notification bar is also included at the bottom of the GUI, which display a text that instructs and provides guidance to user in using the system. The notification bar remains present in the all the GUIs.Besides that, message box will pop up to provide additional options for user to select, such the option to retrain neural networks as or as an error message when invalid action is done, such as an invalid username is entered. Figure 3.2illustrates then mentioned two types of message boxes:

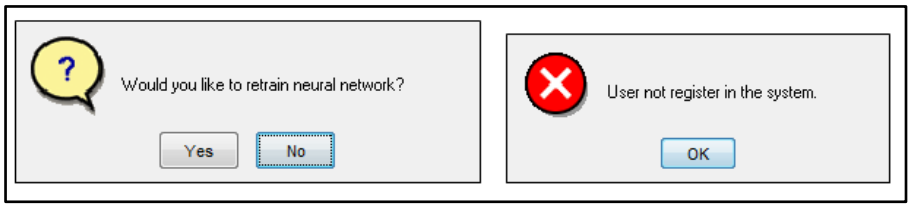

Figure 3.2: Option and Error Boxes

When the system is activated, all neural networks have been trained and a valid username is entered, the system will prompt the user to proceed to the next GUI, where the authentication stage begins. The authentication flow is the same as designed using the command line interface, which starts with voice authentication, followed by face and fingerprint authentication.

Results

After the multi-stage biometric recognition system has been designed and implemented, simulation testing is done to evaluate the overall performance of the system. The simulation setup will be the same as the setup for the recognition subsystem, where the overall FRR and FAR is used to evaluate the overall recognition rate of system with respect to raw biometric test samples. Mean Squared Error (MSE), number of epoch and percentage error (%E) are used to evaluate the training performance of the neural networks. Table 3.3 shows the training performance of neural networks configured with 50 hidden neurons for the individual recognition subsystem:

Table 3.3: Neural Networks Performance for Multi-Stage Biometric Recognition system

Recognition Subsystem	MSE	Epoch	Percentage Error
Voice	1.9765×10^{-7}	40	0%
Face	1.3901×10^{-7}	31	0%
Fingerprint	1.3906×10^{-7}	49	0%

Table 3.4shows the result tabulation of FRR test on the overall system when tested with 25 raw biometric samples from 5 users:

Table 3.4(a): Result Tabulation of FRR Test

	Raw Test Biometric Samples									
Users	Ivan1	Ivan2	Ivan3	Ivan4	Ivan5	Paul1	Paul2	Paul3	Paul4	Paul5
Ivan	1	1	1	1	1	0	0	0	0	0
Paul	0	0	0	0	0	1	0	1	1	1
Ian	0	0	0	0	0	0	0	0	0	0
Esther	0	0	0	0	0	0	0	0	0	0
Steven	0	0	0	0	0	0	1	0	0	0
False Rejection	No	No	No	No	No	No	**Yes (Voice)**	No	No	No

Table 3.4(b): Result Tabulation of FRR Test

	Raw Test Biometric Samples									
Users	Ian1	Ian2	Ian3	Ian4	Ian5	Esther1	Esther2	Esther3	Esther4	Esther5
Ivan	0	0	0	0	0	0	0	0	0	0
Paul	0	0	0	0	0	0	0	0	0	0
Ian	1	1	1	1	1	0	0	0	0	0
Esther	0	0	0	0	0	1	1	1	1	1
Steven	0	0	0	0	0	0	0	0	0	0
False Rejection	No	No	No	No	No	No	No	No	No	No

Table 3.4(c): Result Tabulation of FRR Test

	Raw Test Biometric Samples				
Users	Steven1	Steven 2	Steven 3	Steven 4	Steven 5
Ivan	0	0	0	0	0
Paul	0	0	0	0	0
Ian	0	0	0	0	0
Esther	0	0	0	0	0
Steven	1	1	1	1	1
False Rejection	No	No	No	No	No

Based on the tabulation of the simulation results shown in Table 3.4, the FFR is calculated as shown in the following:

$$False\ Rejection\ Rate\ (FRR) = \frac{Number\ of\ False\ Rejection}{Total\ Number\ of\ Test} \times 100\%$$

$$False\ Rejection\ Rate\ (FRR) = \frac{1}{5\ users \times 5\ tests} \times 100\%$$

$$False\ Rejection\ Rate\ (FRR) = 4\%$$

Table 3.5 shows the result tabulation of FAR test on the overall system when each user is asked to access the system as the other users, but using their own biometric data:

Table 3.5(a): Result Tabulation of FAR Test

		Raw Test Biometric Samples									
	Users	Ivan1	Ivan2	Ivan3	Ivan4	Ivan5	Paul1	Paul2	Paul3	Paul4	Paul5
Users Access as:	Ivan	NA	NA	NA	NA	NA	0	0	0	0	0
	Paul	0	0	1	0	0	NA	NA	NA	NA	NA
	Ian	0	0	0	0	0	0	0	0	0	0
	Esther	0	0	0	0	0	0	0	0	0	0
	Steven	0	0	0	0	0	0	0	0	0	0
False Acceptance		No	No	**Yes (Face)**	No	No	No	No	No	No	No

Table 3.5(b): Result Tabulation of FAR Test

		Raw Test Biometric Samples									
	Users	Ian1	Ian2	Ian3	Ian4	Ian5	Esther 1	Esther 2	Esther 3	Esther 4	Esther 5
Users Access as:	Ivan	0	0	0	0	1	0	0	0	0	0
	Paul	0	0	0	0	0	0	0	0	0	0
	Ian	NA	NA	NA	NA	NA	0	0	0	0	0
	Esther	0	0	0	0	0	NA	NA	NA	NA	NA
	Steven	0	0	0	0	0	0	0	0	0	0
False Acceptance		No	No	No	No	**Yes (Voice)**	No	No	No	No	No

Table 3.5(c): Result Tabulation of FAR Test

		Raw Test Biometric Samples				
	Users	Steven1	Steven 2	Steven 3	Steven 4	Steven 5
Users Access as:	Ivan	0	0	0	0	0
	Paul	0	0	0	0	0
	Ian	0	0	0	0	0
	Esther	0	0	0	0	0
	Steven	NA	NA	NA	NA	NA
False Acceptance		No	No	No	No	No

Based on the simulation results shown in Table 3.5, the FAR is calculated as shown in the following:

$$False\ Acceptance\ Rate\ (FAR) = \frac{Number\ of\ False\ Acceptance}{Total\ Number\ of\ Test} \times 100\%$$

$$False\ Acceptance\ Rate\ (FAR) = \frac{2}{5\ users \times 5\ tests} \times 100\%$$

$$False\ Acceptance\ Rate\ (FAR) = 8\%$$

The simulation results have shown that the overall multi-stage biometric recognition system is able to achieved FRR of 4% and FAR of 8%. Thus, the system has been design, implemented and tested to fulfill the research objective of achieving overall FRR and FAR of less than 10%.

The time taken to train three neural networks has been taken into consideration. Therefore, an additional test is conducted to record the average time taken to train the neural networks. Table 3.6 shows results of 10 simulation tests to; calculate the time taken to train three neural networks:

Table 3.6: Neural Networks Training Time

No. of Test	Training Time for Voice Neural Network (sec)	Training Time for Face Neural Network (sec)	Training Time for Fingerprint Neural Network (sec)	Total Training Time (sec)
1	1.09	1.21	1.33	3.63
2	2.03	1.33	1.01	4.37
3	1.01	2.10	1.06	4.17
4	1.23	1.16	1.17	3.56
5	1.67	1.32	1.05	4.04
6	1.17	1.43	1.00	3.60
7	1.03	1.11	1.22	3.36
8	1.02	1.35	1.62	3.99
9	1.35	1.08	1.12	3.55
10	1.04	1.61	1.56	4.21
Total	12.64	13.70	12.14	38.48

The average time taken for neural networks training is calculated as follows:

$$Average\ Training\ Time = \frac{Total\ Training\ Time}{No.\ of\ Test}$$

$$Average\ Training\ Time = \frac{38.48}{10}$$

$$\therefore Average\ Training\ Time = 3.848\ sec$$

IV. CONCLUSION

Thus an appropriate feature extraction algorithm for voice, face and fingerprint recognition were integrated into a multi-stage biometric recognition system with artificial neural network, in which the voice recognition system utilises Mel-frequency Cepstrum Coefficient (MFCC) feature extraction algorithm to represents the voice signal of the user in the form of cepstrum of the voice derived from Discrete Cosine Transform (DCT) on the log power spectrum on a non-linear Mel-scale frequency. Face recognition subsystem utilises closing algorithm image morphology that extracts the features of the face based on the facial outline, via superimposing of the dilation and erosion of the facial image. Fingerprint recognition subsystem utilises minutiae extraction to extract the ridge termination and bifurcation points of the fingerprint. Results show that 50 hidden neurons are sufficient to provide optimum performance for the neural networks to recognise voice, face and fingerprint biometric patterns. Therefore, the integrated biometric recognition system consists of three neural networks for configured consistently with 50 hidden neurons. An overall FRR and FAR below 10% is achieved, the outcomes for the simulation test on the integrated biometric recognition system have shown that, the calculated FRR value is 4% and FAR value is 8%.Also, the calculated average time taken to train the neural network is 3.848 seconds only.

REFERENCES

[1] Anusuya.M.A., &Katti.S.K., "Speech Recognition by Machine", International Journal of Computer Science and Information Security, Vol.6 (3), 2009, pp. 181-205.

[2] Azam,S.M., Mansoor,Z.A., Mughal,M.S., & Mohsin,S, "Urdu Spoken Digits Recognition Using Classified MFCC and Backpropagation Neural Network. Computer Graphics, Imaging and Visualisation", Bangkok. 14th to 17th August 2007. Bangkok: CGIV. pp. 414 – 418.

[3] ChadawanIttichaichareon, SiwatSuksri& Thaweesak Yingthawornsuk,"Speech Recognition using MFCC", in the International Conference on computer Graphics, Simulation and Modeling, July 28-29, 2012, pp.135-138.

[4] Chen, X.et al., "Incremental Feedback Learning Methods For Voice Recognition Based On DTW. 2012 Proceedings of International Conference on Modeling, Identification & Control", Wuhan, 24th to 26th June 2012. Wuhan: ICMIC. pp.1011 – 1016.

[5] DavoodZabihzadeh, & Mohammad Moattar, "Manifold learning based speaker dependent dimension reduction for robust text independent speaker verification", Inetrnational Journal of Speech technology, springer, 2014, pp.1-10.

[6] DebmalyaChaakrabarty, MahadevaPrasana& Rohan Kumar Das, "Development and evaluation of online text-independent speaker verification system for remote person authentication", International Journal of Speech Technology, Springer, 2013,pp. 75 – 88.

[7] DimitriosVerveridis, & Constantine Kotropoulos, "Emotional speech recognition: resources, features and methods", Aritificial Intelligence and Information Analysis Laboratory, Aristotle university pf Thessaloniki, Greece, pp. 1 – 22.

[8] Gandhiraj,R&Sathidevi,P.S., "Auditory-based Wavelet Packet Filterbank for Speech Recognition using Neural Network", International Conference on Advanced Computing and Communications. Guwahati, 18th to 21st December 2007. Guwahati: ADCOM. pp. 666 – 673.

[9] Gregory , P. & Simon, M. A.,"Biometric For Dummies. Indianapolis:" Wiley Publishing, Inc.,2008.

[10] Ibrahim Patel, &Dr.Srinivas Rao, " Speech Recognition using HMM with MFCC-An analysis using frequency spectral decomposition technique", International Journal of Signal & Image Processing, Vol.1(2), December 2010, pp. 101- 110.

[11] Muzaffar, F., Mohsin, B. & Naz, F, " DSP Implementation of Voice Recognition Using Dynamic Time Warping Algorithm", Student Conference on Engineering Sciences and Technology. Karachi, 27th August 2005. Karachi: SCONEST. pp. 1 – 7.

[12] SanjivaniS.Bhabad, &Gajanan K.Kharate, "An overview of Technical Progress in Speech recognition", International Journal of Advanced research in computer science and software engineering, Vol.3,Issue. 3, March 2013, pp. 488 – 497.

[13] Suzuki, H., Zen,H., Nankaku,Y., & Miyajima,C., "Speech recognition using voice characteristic dependent acoustic models", in the IEEE International conference on Acoustics, Speech, and Signal Processing, 6-10 April 2—3, pp. 740-743.

[14] Tsenov,G.T&Mladenov,V.M., " Speech recognition using neural netwroks", in 10th Symposium on Neural Network Applications in Electrical Engineeirng, 23-25 Sept.2010,pp. 181-186.

[15] Vasuthi, S, Vaidehi, V, Babu, N.T.N, and Treesa, T.M. , "An Efficient Multi-Modal Biometric Person Authentication System Using Fuzzy Logic",2010 Second International Conference on Advanced Computing. Chennai, 14th to 16th December 2010. Chennai: ICoAC., 2010, pp. 74–81.

[16] Yang Liu, Elizabeth Shriberg, & Andreas Stolcke, "Enriching Speech recognition with automatic detection of sentence boundaries and disfluencies", IEEE transactions on speech & audio processing, 2013, pp. 1- 15.