Integrating RBF-based Neural Network Face Expression Recognition in Access System

Ch'ng Yau Yau[1], A. F. Kadmin[1*], S. F. Abd Gani[1], K. A. A. Aziz[1], R. A. Hamzah[1], A. Z. Jidin[1]

[1]*Faculty of Electrical and Electronic Engineering Technology, Universiti Teknikal Malaysia Melaka, Malaysia*

fauzan@utem.edu.my

Abstract—**Biometric recognition system such as facial recognition system was widely developed over the past few years. Facial recognition system is commonly used in security system to allow user to protect their privilege. The normal security like key or password is no longer relevant as people prefer an easier and flexible way. Therefore, this paper presents a better and easier way of security system that can recognise the user successfully and give the matching percentage. By using Radial Basis Function Neural Network in MATLAB, a face recognition system can be created. The RBF system have been trained by data as reference, input image undergoes the same process and the data obtained is used to match with the data in the RBF to obtain the matching percentage. A suitable matching percentage reference was chosen from this analysis as the minimum require matching to access the security system where error rate is one of the main concerns where it is the unwanted result that might occur. Different threshold number, spread value, and sizes of dimension also tested, the differences on the output matching result were observed. By using the microcontroller to control a relay to control the magnetic door lock, the system was able to successfully control the door lock.**

Keywords—RBF, ANN, face recognition, matching percentage

I. INTRODUCTION

Biometrics is widely used for security purpose. Biometrics is extrapolating from the Greek words, bio and metrikos which has the meaning of life and relating to measure. Biometric become popular in security system when the society requirement of security in the field of information, business, military, e-commerce etc. [1]. The biometric system that existed in our daily life got hand geometry reader, fingerprint reader, iris scanner, retina scanner, voice recognition, signature recognition and facial recognition.

Gong et al. [2] described Artificial Neural Network (ANN) as a complex adaptive system where it learned and changed its internal structure based on information flowing through it. ANN can use supervised learning, unsupervised learning or reinforcement learning. Online face recognition using ANN is a system that recognise the user's face for multiples of time. The image of user used by converting to 2D matrix form and save as data for ANN to learn. A camera used to capture the picture of user for undergoing the ANN matching with MATLAB software. The image of use then been captured to be undergo matching of the data using ANN to provide the percentage of similarity.

Fig 1 shows how a neural network functions as a brain system where as it contains of three layer; input layer, hidden layer and output layer. Our brain system will remember what we have seen and memorized it and the brain was trained as the same time. ANN work similar as brain, it can be trained with several images so that it memorizes it [3]. Another process used to test whether the ANN system to recognise the system that trained.

Article history: Manuscript received 15 August 2019; received in revised form 18 September 2019; Accepted 23 September 2019.

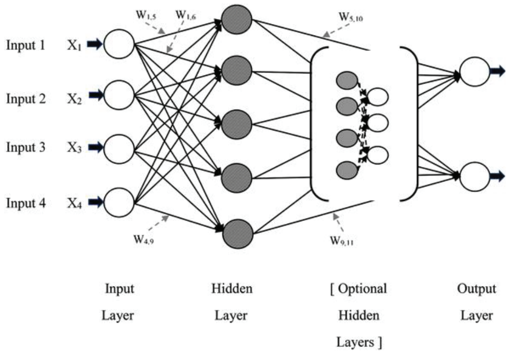

Fig 1. Basic Structure of an Artificial Neural Network (ANN) [4]

Facial recognition is one of the common biometric and widely used method, it may differ to many methods to recognise the facial of the user. A system of face recognition system was created by using radial basis function neural network [4-5]. The most common errors that might occur are False Accept Rate (FAR) and False Reject Rate (FRR). These two errors occur due to the system wrongly accept or reject the input from user when matching with the sample of database. The system gives the rejection when the system receiving the input from an authorized person known as False Reject; while the system accepted the input when the system receiving the input from non-authorized person known as False accept. Furthermore, there are other factors that cause biometric system to fail. The growth of human or situations or environments or their daily activities done all contributed to the affect the system to fail the recognition

Most of the users wanted their information and place to be secure with a trusted security system. The normal security like password is no longer relevant as people prefer an easier and flexible way [6]. Face recognition system is being research to make the system more advanced. By using the neural network is more suitable for the medium of face recognition system.

This research used MATLAB as the main software to develop the neural network system. Graphical User Interface of MATLAB used in this system. A camera is operated to capture the image of user and converted the image into grayscale format. The analysis of the system using grayscale image as the input where it then converted into 2D matrix form by MATLAB for the training process of ANN. The hardware part is constructed by using microcontroller with serial connection to control the magnetic door lock.

In this paper, we focus on optimizing the RBFNN for percentage of acceptance. A suitable value of percentage is been set as the matching percentage. The objectives of this project are to develop a face recognition system by using Radial Basis Function Neural Network with MATLAB. A matching percentage would be produced through the input into trained RBF and a suitable value of matching percentage would be chosen. As the matching percentage is higher than 90%, the door lock would be unlocked. Through this system, the error rate such as False Acceptance Rate (FAR) and False Rejection Rate (FRR) can be identified to produce a better matching percentage.

II. METHODOLOGY

The methodology for this project can be categorized into 3 phases; 1. RBF training, 2. RBF testing and 3. GUI result. The experiment conducted in laboratory environment and the operation of the whole system can be explicated in this part. The block diagram as shown in Figure 1 described the flow of this system. A block diagram is provided a better understand of how the system work and function.

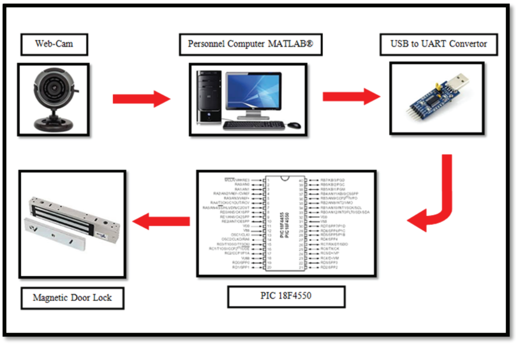

Fig 2. Block diagram for face recognition system.

The block diagram started from the webcam that captured the image and send to the MATLAB GUI interface. Then, the selection of training or testing the image can be made at the GUI interface. If training was requested, the image must first to be saved to the neural database. If test was requested, RBF is called to do the analysis and comparison of both matrix and send the output to microcontroller. Low output would be sent by the output of microcontroller and opened the magnetic door lock.

A. RBF Training

Image captured turned into grayscale and RBFNN distinguishing the face and non-face images. As the face image cropped and save into the size of 50*50 pixels and it converted into a double class in matrix form. The matrix is then converted into column of matrix 1*n. The new matrix has fed into the RBF network. Supervised training is used for training the rbf as training patterns are provided to the RBFNN together with a teaching signal or target.an. Figure 3 shows the flowchart in RBF training.

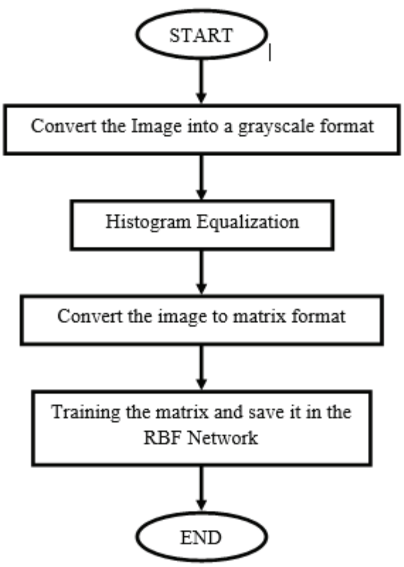

Fig 3. RBF training flowchart

B. RBF Testing

Figure 4 shows the flowchart for RBF testing. 200 inputs of users' face and 160 inputs of non-user's face was used in testing. Image captured undergo same process as training without creating RBF but comparing with the existing RBF. As for the result, it determined both the genuine and impostor acceptance and rejection by the condition of similarity percentage of 88%, 89% and 90%. Through these comparisons of three condition, a suitable similarity percentage can be chosen to set as the acceptance of authorize person.

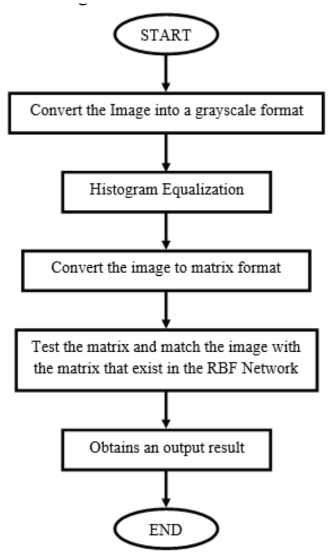

Fig 4. RBF testing flowchart

C. Graphical User Interface (GUI) Result

GUI displayed the picture captured and the colour coded image for the user to view. Other than this, user ID and value of similarity percentage and status also can be displayed. If the matching percentage reaches 90%, the magnetic door lock can be unlocked. There are 4 buttons that can be pressed to test on the system it is still functioning or not where it gives a matching percentage that over 90% and show the ID of user. For online testing, if impostor was tested on the system, all the matching percentage with all users show on the bottom part of the GUI as shown in Fig 5.

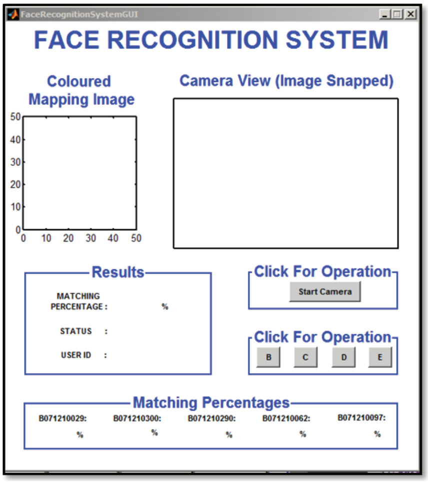

Fig 5. Graphical user interface

This system required a training process to create a RBF as the database as described in training RBF. Input are testing to obtain matching percentage. By using GUI to run the process of testing and give the execution instruction to microcontroller to control relay to control magnetic lock when matching percentage is over 90%. 360 inputs were used to determine a suitable matching percentage to be set as reference matching percentage.

III. RESULT AND DISCUSSION

Analyses were run to determine a suitable spread value, threshold value and the size of image of face for matching. In this face recognition system; there are 4 possible outcomes that produced through the two analyses comprised of the comparison by using genuine match and impostor match. The possible outcomes are:

(a) Genuine acceptance;
(b) Impostor rejection;
(c) Genuine rejection (False Reject);
(d) Impostor acceptance (False Accept).

Moreover, the verification of similarity value for verifying whether to unlock or not also can be obtained from these data obtained. A system was developed for 5 users where a Graphical User Interfaces (GUI) was developed as shown in Figure 6. The matching probability value, description and number of which user displayed on the 'Results' column. A picture taken and displayed on the screen display and another colour coded image displayed on the other small screen display. The picture shown was the data obtained from the intensity of grayscale picture. For the operation for buttons 'B' to 'E' were used to show the other 4 users able to recognise by the system. Since If-else condition was used in the system, the matching rate shows when the system unable to recognise the input face. Once the matching rate of user matched, it will not show the matching rate with the next user in the system as shown in Figure 6 where the fifth matching rate was not shown.

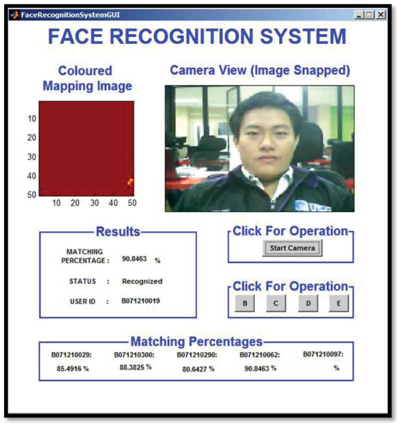

Fig 6. Graphical matching result display

A. *Genuine Testing*

A total of 400 inputs of user's images were used to undergo the genuine testing. The testing was undergoing in two conditions which is with sunlight and without sunlight condition, 200 inputs were obtained from each condition. Fig 7 and Fig 8 show that the matching percentage of the 400 inputs from user's image; while Table 1 and Table 2 show that the genuine acceptance rate and False Rejection Rate (FRR) was corresponding to each other.

From the data obtained from Table 1 and Table 2, the genuine acceptance for the condition without sunlight was higher than the condition with sunlight. A short conclusion that can make from this situation was light intensity affected the matching percentage of the system. For the condition without sunlight, it has a more stable light intensity whereas the light source was from fluorescent light. For the condition with sunlight, cloud affected the light intensity. Hence, another experiment should be conducted to test on the effect of light intensity toward the matching percentage.

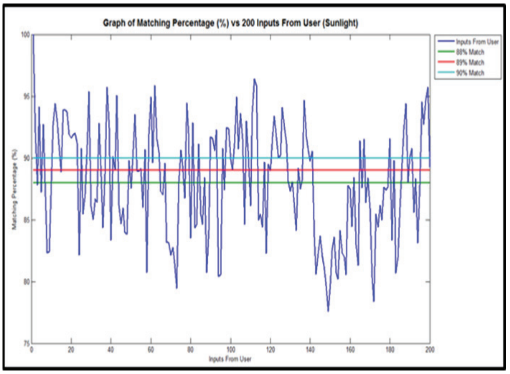

Fig 7. 200 Inputs from User with Sunlight.

TABLE 1GENUINE ACCEPTANCE AND REJECTION RATE WITH SUNLIGHT.

Genuine	Acceptance		Rejection (FRR)	
Condition	Accept	Percentage	Reject	Percentage
88% Similarity	108/200	54.0%	92/200	46.0%
89% Similarity	91/200	45.5%	109/200	54.5%
90% Similarity	75/200	37.5%	125/200	62.5%

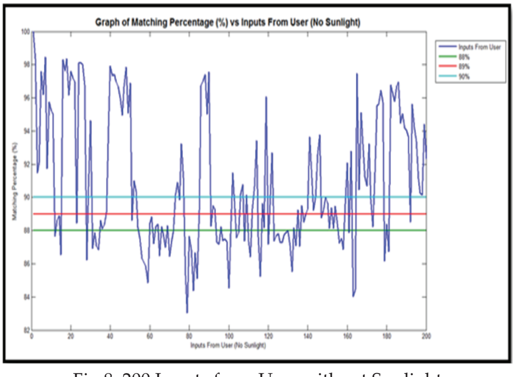

Fig 8. 200 Inputs from User without Sunlight

B. *Impostor Testing*

160 inputs non-users' image as shown in Fig 9 gave the result as shown in Table 3. Impostor rejection rate and False Acceptance Rate (FAR) were another important element in face recognition system. As the matching similarity percentage decreased, the FAR increased and this caused the system to be unsafe.

TABLE 2 GENUINE ACCEPTANCE AND REJECTION RATE WITHOUT SUNLIGHT

Genuine	Acceptance		Rejection (FRR)	
Condition	Accept	Percentage	Reject	Percentage
88% Similarity	139/200	69.50	61/200	30.50
89% Similarity	113/200	56.50	87/200	43.50
90% Similarity	93/200	46.50	107/200	53.50

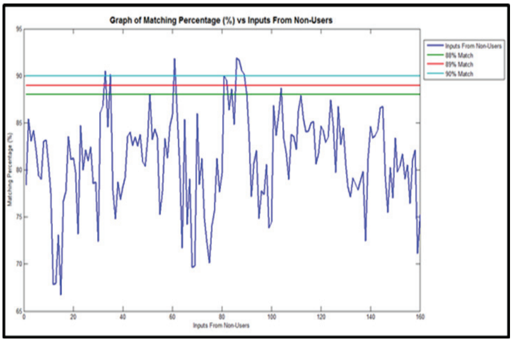

Fig 9. 160 Inputs from Non-Users.

All of 160 impostor inputs were obtain as same condition with 200 inputs from user with the condition without sunlight. Hence, a comparison of both genuine and impostor can be made to choose a better matching percentage for the system. In order to make the system security safer, the matching percentage is maintained the higher the better. Unfortunately, the range of the inputs by user obtained was around 0.77 to 0.96. If the matching percentage was increased for certain high value, vice versa the FRR also increased. As for a safe and secure security system, FRR increase is better than FAR increase; but this caused the system become inefficient as the user was not able to access the system easily. Hence, matching percentage was set to be 90% with genuine acceptance of 46.5% whereas the FAR was only 5%-page number should appear on the below right manuscript.

TABLE 3 IMPOSTOR ACCEPTANCE AND REJECTION RATE

Impostor	Acceptance (FAR)		Rejection	
Condition	Accept	Percentage	Reject	Percentage
88% Similarity	13/160	8.1%	147/160	91.9%
89% Similarity	9/160	5.6%	151/160	94.4%
90% Similarity	8/160	5.0%	152/160	95.0%

TABLE 4 MATCHING PERCENTAGE OF 5 USERS OF SYSTEM

Matching Percentage	Test Image				
Training Image	User 1	User 2	User 3	User 4	User 5
User 1 (ID:0029)	96.33%	84.34%	82.52%	88.38%	76.77%
User 2 (ID:0300)	84.03%	91.19%	78.58%	81.90%	75.61%
User 3 (ID:0290)	82.66%	79.53%	95.09%	80.19%	75.19%
User 4 (ID:0062)	88.72%	81.16%	82.00%	92.35%	78.20%
User 5 (ID:0097)	72.28%	72.22%	72.11%	73.29%	93.33%

A system of 5 users were developed, Table 4 shows that the recognised of user when the correct matched of input given and the incorrect matched done. The matching percentage shown in grey box was the succeed matching of user face recognised by the system. Other matching percentages were less than 90% which considered as matching failure.

IV. CONCLUSION

As conclusion, a face recognition system was developed where first a RBF was trained and the matching value was set to be 90%. The matching percentage of more than 90% only produced the positive recognise result where the positive result unlocked the magnetic door lock. The matching percentages and User ID also show in the Graphical User Interface that created in MATLAB. The value of FAR and FRR were also analysed to see the error rate given by the system. These error rates affected the output result of the security system created. FRR can be higher that only caused the system to be inefficient, but FAR must keep as low as possible whereas FAR caused the system to become an unsecure system. 90% was chosen as matching percentage was because the False Acceptance Rate can be maintaining as low as 5% to ensure the system is secure and safe system.

ACKNOWLEDGMENT

We are grateful to Kementerian Pengajian Tinggi Malaysia, Universiti Teknikal Malaysia Melaka (UTeM) and Centre for Research and Innovation Management (CRIM) for their kind and help for supporting financially and supplying the research components and giving their assistance to complete this project.

REFERENCES

[1] Ijaz, Sidra, Munam Ali Shah, Abid Khan, and Mansoor Ahmed, "Smart cities: A survey on security concerns," International Journal of Advanced Computer Science and Applications 7, no. 2: 612-625, 2016.

[2] Gong, Yicheng, Yongxiang Zhang, Shuangshuang Lan, and Huan Wang, "A comparative study of artificial neural networks, support vector machines and adaptive neuro fuzzy inference system for forecasting groundwater levels near Lake Okeechobee, Florida," Water resources management 30, no. 1: 375-391., 2016.

[3] Litjens, Geert, Thijs Kooi, Babak Ehteshami Bejnordi, Arnaud Arindra Adiyoso Setio, Francesco Ciompi, Mohsen Ghafoorian, Jeroen Awm Van Der Laak, Bram Van Ginneken, and Clara I. Sánchez, "A survey on deep learning in medical image analysis," Medical image analysis 42: 60-88, 2017.

[4] Yoo, Sung-Hoon, Sung-Kwun Oh, and Witold Pedrycz, "Optimized face recognition algorithm using radial basis function neural networks and its practical applications," Neural Networks 69: 111-125, 2015.

[5] Agarwal, Vandana, and Surekha Bhanot, "Radial basis function neural network-based face recognition using firefly algorithm," Neural Computing and Applications 30, no. 8: 2643-2660, 2018.

[6] Jose, Arun Cyril, and Reza Malekian, "Smart home automation security: a literature review," SmartCR 5, no. 4 : 269-285, 2015.

[7] Walczak, Steven, "Artificial neural networks," In Advanced Methodologies and Technologies in Artificial Intelligence, Computer Simulation, and Human-Computer Interaction, pp. 40-53. IGI Global, 2019.

[8] Halali, Mohamad A., Vahid Azari, Milad Arabloo, Amir H. Mohammadi, and Alireza Bahadori, "Application of a radial basis function neural network to estimate pressure gradient in water–oil pipelines," Journal of the Taiwan Institute of Chemical Engineers 58: 189-202, 2016.

[9] Aziz, K. A. A., M. H. Mustafa, N. M. Z. Hashim, N. R. M. Nuri, A. F. Kadmin, and A. Salleh, "Smart android wheelchair controller design," International Journal for Advance Research In Engineering and Technology (IJARET) 3, no. 3: 42-48, 2015.

[10] Majdisova, Zuzana, and Vaclav Skala, "Radial basis function approximations: comparison and applications," Applied Mathematical Modelling 51: 728-743, 2017

[11] Kadmin, A. F., A. Z. Jidin, Abu Bakar, KA A. Aziz, and WN Abd Rashid, "Wireless voice-based wheelchair controller system," Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 8, no. 7 : 117-122, 2016

[12] Montazer, Gholam Ali, and Davar Giveki, "An improved radial basis function neural network for object image retrieval," Neurocomputing 168 : 221-233, 2015.

[13] Akpan, Vincent A., Joshua B. Agbogun, Michael T. Babalola, and Bamidele A. Oluwade, "Radial basis function neuroscaling algorithms for efficient facial image recognition," Mach. Learn. Res. 2, no. 4 : 152-168, 2017.

[14] Hamzah, Rostam Affendi, M. Saad Hamid, A. F. Kadmin, and S. Fakhar Abd Ghani, "Improvement of stereo corresponding algorithm based on sum of absolute differences and edge preserving filter," In 2017 IEEE International Conference on Signal and Image Processing Applications (ICSIPA), pp. 222-225. IEEE, 2017.

[15] Santoro, Adam, David Raposo, David G. Barrett, Mateusz Malinowski, Razvan Pascanu, Peter Battaglia, and Timothy Lillicrap, "A simple neural network module for relational reasoning," In Advances in neural information processing systems, pp. 4967-4976. 2017.

[16] Schroff, Florian, Dmitry Kalenichenko, and James Philbin, "Facenet: A unified embedding for face recognition and clustering," In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 815-823. 2015.

[17] Kadmin, A. F., K. A. A. Aziz, A. R. Soufhwee, SS Abd Razak, M. Z. Salehan, NA Abdul Hadi, R. A. Hamzah, and WN Abd Rashid, "Performance analysis of neural network model for automated visual inspection with robotic arm controller system," Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 10, no. 2-2 : 19-22, 2018.