Indonesian Journal of Electrical Engineering and Computer Science
Vol. 6, No. 3, June 2017, pp. 638 ~ 645
DOI: 10.11591/ijeecs.v6.i3.pp638-645

Facial Recognition in Multimodal Biometrics System for Finger Disabled Applicants

Faddly Mazlan, Afdallyna Harun*, Saifullzwan Suliman
Faculty of Computer and Mathematical Sciences, UniversitiTeknologi MARA, Shah Alam, Selangor
*Corresponding author, e-mail: afdallyna@tmsk.uitm.edu.my

Abstract

Citizen identification in Malaysia is managed by JabatanPendaftaran Negara (JPN); a Malaysian Government Agency responsible in producing a national identification card called MyKad which contains textual information of the MyKad holder as well as fingerprint data. The current business modal solely relies on fingerprint identification as recognition process which presents limitations to Malaysian citizens who have finger disabilities. Currently, this matter is addressed by having applicants provide proof of identification which is then verified by the agency within three months. To improve efficiency of this process as well as making it friendlier for applicants to apply their MyKad, the use of facial recognition is proposed as a potential solution. A series of study was conducted with JPN, which intends to measure the reliability of a multimodal biometrics system in JPN environment for finger-disabled applicants. Findings demonstrate that Multimodal Biometrics System using Facial Recognition is reliable for individual identification.

Keywords*: biometrics system; multimodal; facial recognition; system reliability*

1. Introduction

Many government agencies worldwide utilize the use of biometrics systems to govern, monitor, control and manage citizens' data [1]. Malaysia has moved to the use of biometrics system in managing citizens' data since 2001, through its government agency, Jabatan Pendaftaran Negara (JPN) or National Registration Department. JPN is responsible in keeping records of all Malaysian citizens as well as issuing Malaysian national identification card called MyKad to Malaysian citizens. MyKad is a mandatory document for citizens aged 12 and above to have. To manage such process, JPN currently employs the use of Automatic Fingerprint Identification System (JPN AFIS). For first time applicant, they need to provide birth certificate, have their fingerprints recorded as well as picture taken to be recorded into JPN AFIS. This information is then represented with the use of MyKad (see Figure 1) of which when read at a SmartCard reader, the afore-mentioned details will be shown. Of course it is important to note that in respect to data privacy, the use of SmartCard readers for MyKad data extraction is regulated by the government and only allowed to specific government agencies.

The simple process of MyKad application would allow MyKad approval and collection to be ready within two hours. However, the same cannot be applied for citizens with problematic fingerprint or finger disabilities. Citizens with unreadable prints, or is a finger/hand amputee are required to provide police reports, medical reports, and documents from commissioner of oath to proof their identity. These documents would then need to be reviewed, certified and approved by JPN which could take up to three months to complete. This long waiting time leaves a lot to be desired and appears unfriendly to handicapped users.

Multimodal biometrics system uses multiple biometrics characteristics such as facial data, fingerprint, iris and many more where these information are integrated for identification [2]. Seeing that JPN AFIS has facial data which is useful but under-utilized, we wanted to demonstrate the viability of applying multimodal system in the context of facial recognition in verifying an individual. This is because, multimodal biometrics system has better accuracy rate, can address interclass similarities and non-universality as well as reduces spoofing and noisy data [3] [4]. A study [5] similar to our concern was conducted in the context of Myanmar region which shows promising outcome of reliability. However, it is important to understand if facial biometrics is indeed feasible within JPN business environment. With that we were driven with

Received January 25, 2017; Revised April 2, 2017; Accepted April 16, 2017

the following research question “How reliable and efficient is the use of Multimodal Biometrics System for facial recognition in a JPN environment?”.

With that motivation, a series of studies that looks into assessing the reliability of facial recognition feature in multimodal biometrics system was conducted. The studies offer an insight to not only performance of the system but its applicability within an enforcement agency environment such as JPN.

Figure1. MyKad Sample

2. Research Method

Morpho’s Facial Biometrics System (FBS), which is a vendor recognition system was used for this study. According to the Face Recognition Vendor Test (FRVT) conducted by the National Institute of Standards and Technology, Morpho Biometrics System technology performs particularly well at the lowest false alarm levels, which corresponds to the operational setting with a multimillion gallery and limited resources for visual inspection [6].

Generally, every biometrics system includes the following processes:

a. Enrollment – presentation of facial image sample for database recording. However, in the context of this study, existing data is derived from JPN AFIS for FBS
b. Live Presentation – applicant present/provide a new live image sample where the biometrics system will extract facial features for the next process
c. Matching – stored image and live image are compared to one another resulting into biometrics matching score.

Five virtual machines were set up for JPN officers from the Government Query Department to use. The virtualization environment was set up using one unit of IBM x3650 server which had UNIX (CentOS 6.4) and VMWare version 11 installed. Each of the virtual machines was installed with Windows and Linux Operating System which also included Lightweight Directory Access Protocol (LDAP), Database, Matcher, Workflow and Client. The purpose of virtualization is to enable multiple operating systems and applications to run on one physical computer by multiplexing hardware resources [7]. Table 1 describes the purpose of each components installed in the virtual machines.

Table 1. Components of virtual machines

Components	Operating System	Purpose
LDAP	Win Server 2008	Manage and access the distributed directory information service for FBS
Database	Win Server 2008	Store 50,000 facial records which were selected randomly and acquired with permission from JPN AFIS
Matcher	CentOS 6	Run verification using facial algorithm
Workflow	Win Server 2008	Interact with database, matcher, client application and LDAP service
Client	Win 7	Allowing the display and interaction with FBS User Interface

As afore-mentioned, the Government Query Department was selected to use the FBS as this is the department responsible in handling MyKad finger-disabled applicants. The data collection period was set for two months. In using FBS, the officers need to upload photos of the applicants into the system by taking their live picture. The data is then compared with the data in the database and verified using Matcher. *Hit* transactions will proceed with MyKad approval while *No Hit* data would result into suspended application and applicants would have to proceed with the three-month manual verification process.

Each of the transaction results was then compiled to compute the overall FBS performance. This is an important process to assess if the resulting decision from FBS is a "genuine individual" type of decision or an "impostor" type of decision [8]. As the verification in the matching process are largely quantifiable, statistical calculation of various performance metrics were used which include False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER) as the results would demonstrate reliability and efficiency of the FBS [9]. The description of each statistical calculation together with its findings will be discussed in the following sections.

3. Results and Analysis

This section shall explain the results of the studies conducted.

3.1. Transactions with Hit and No Hit Results

To assess picture matching validity, every biometrics system measures and calculates its own matching score where the score represents similarity values between live sample and stored data from the system [10]. Figure 2 visualizes a *Hit Transaction* result. For the purpose of this study, a transaction is considered a *Hit* if it has a green checked mark and the matching result is number 1 in value ranking.

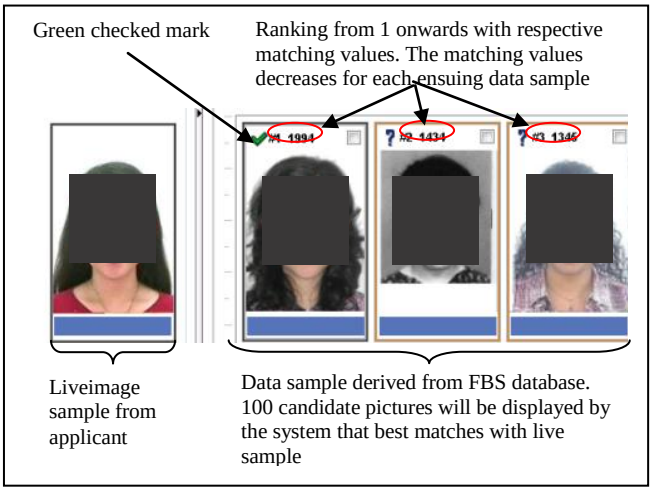

Figure 2. Example of a Hit Transaction result from FBS (images have been darken for privacy purposes)

During the course of data collection, there were 222 transactions for finger-disabled applicants. 196 of them were *Hits* and 26 of them resulted into *No Hit* when using the FBS. The latter was due to the live sample not matching with any sample in the database or rejected by the system. Table 2 summarizes the results for *Hit* and *No Hit* transaction.

Table 2. Transaction results

Total Transaction	Hit	No Hit
222	196	26

3.2. False Acceptance Rate and False Rejection Rate

False Acceptance Rate (FAR) is the percentage of imposters that are incorrectly granted access to a biometrics system [11] rendering them as supposed genuine individual [12].

This happens because the criteria of reference threshold are fulfilled [9]. FAR is calculated as, FAR = [Wrongly Accepted Individuals/Total Number of Identification Attempts].

As shown in Table 2, there were 196 *Hits*, however, within those numbers, 25 of them were decided as valid even though they do not match. Following the formula; FAR is 0.13% which is considered adequate for many authentication scenarios [13]. Moreover, as finger-disabled applicants are a small minority in Malaysia, the value is not worrying and shows a degree of reliability.

False Rejection Rate (FRR) is the probability that the system incorrectly rejects access to an authorized person as the criteria of reference threshold is not fulfilled [9]. This may be due to the failure in finding a match between live image samples to the data derived from the FBS as part of 100-candidate matching samples (see Figure 2). FRR is calculated as, FRR = [Wrongly Rejected Individuals/Total Number of Identification Attempts].

From the 26 *No Hit* value (see Table 2), one image actually matched. Following the formula, FRR is 0.005% which is within the acceptable value [13]. It needs to be noted though; the number of data from the database for matching purposes is limited to 100-candidate matching samples (see Figure 2). Which means, in terms of False Rejection Rate, the rejection may be due to the sample not available within the 100 candidates but there is a probability that a matching sample may exists in or outside the database (there were 50,000 data in the database).

3.3. Equal Error Rate

Equal Error Rate (EER) indicates a system's accuracy, where the lower the EER, the better is the system's performance [14]. The purpose of EER is to give a threshold independent performance measure. The False Acceptance Rate and False Rejection Rate intersect at a certain point which can be determined using the Receiver Operating Characteristics (ROC) curves. ROC is based on aggregated statistics of match scores corresponding to all biometrics samples to measure verification performance [15]. The intersection plots the Equal Error Rate (the point in which the FAR and FRR have the same value) [16], where in this study it was found to intersect at 10% (see Figure 3). This is within the accepted value 5% to 15% [13].

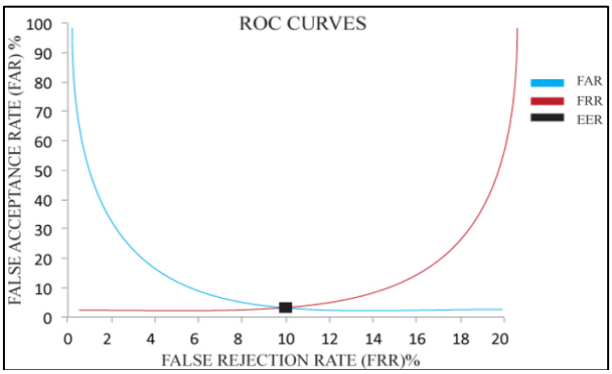

Figure 3. Equal Error Rate and ROC Curve

3.4. Verification Process Time

Verification Process Time is the average time taken (measured with time frequency) for the actual matching process to provide matching results. Figure 4 illustrates that the Verification Process Time for all 222 transactions varies from ten (fastest time) to twenty-four seconds (longest time). Average Verification Processing Time was 15.31 seconds (based on mean value calculation).

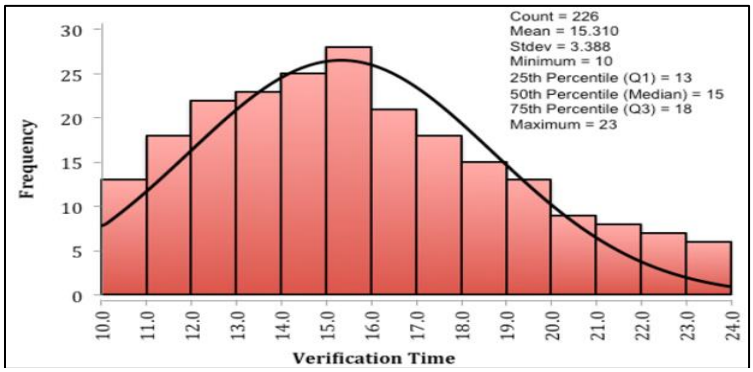

Figure 4. Verification Process Time

Further analysis conducted indicated that the varying processing time was due to (i) resources access, (ii) connectivity and (iii) complexity of matching process.

The FBS was running on virtual machine environments, where resources (i.e. processor cores and input output devices) are shared among virtual machines using time slicing method [17]. FBS is also dependent on network connectivity in enabling matching processes to take place. During the study period, connectivity from user workstation to FBS was running on JPN network environment where there is a high bandwidth usage due to the running of other system within the same environment.

Matching process in a biometrics system basically involves data transmission and compression [18] but it also involves data comparison where live image sample is compared with derived sample from FBS database using complex algorithm in the matcher server. Due to individual's unique image and features, it derives into a rather complex process affecting Verification Processing Time.

Long Verification Process Time could affect user perception on FBS performance even though this is largely due to consequence of poor network connectivity [18].

3.5. Match Score Analysis

Facial recognition technology works by using algorithms to perform face matching. This involves identifying extremities part of the image and marking center points of the eye socket providing a fixed reference point. This serve as facial landmark where it refers to the fiducial points on facial images, human facial shape, and even minute details of skin texture [19] [20].

Match Score Analysis was conducted to determine the threshold value of the FBS as the value has not been determined by JPN who is the potential stakeholder for this system.

During the proof of concept, four identical images were uploaded into the FBS. This was conducted in order to determine the optimum match score value for an identical facial image. Verification was done for these four identical images, and the system provides same match score for all four, which were 50000. This indicates that 50000 are the maximum match score for the FBS.

The study further followed with 196 transactions with varied match score (taken from hit transactions). Figure 5 shows the distribution of Match Score Results for 196 Hit transactions, where *x*-axis indicates match score results and *y*-axis indicates frequency of transactions.

From Figure 5, it can be seen that the minimum Match Score was 479, maximum Match Score was 9956 while the average Match Score was 2293 (mean value calculation). From this range, JPN can choose within the value of 479 to 9956 as threshold value. However, we would suggest 2293 as the threshold value as it can be seen that high Match Score results falls within 2293 value.

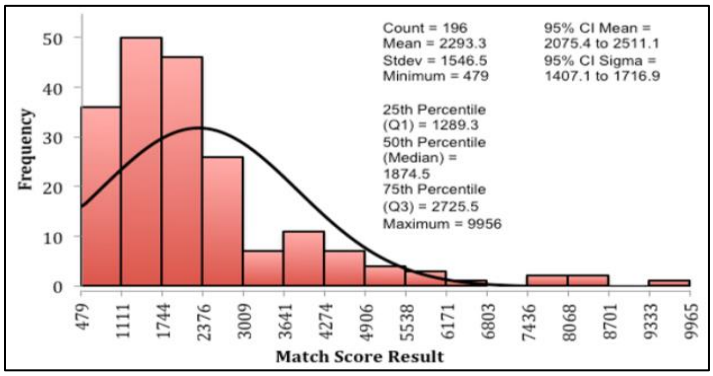

Figure 5. Distribution of Match Score Results

Further analysis conducted found that the varying Match Score was due to (i) quality of facial images in database, (ii) applicant's aging factors, and (iii) facial occlusion.

For good image analysis, the biometrics system should be presented with a live image sample that is high in resolution and taken under similar lighting conditions to the existing ones in the database as this would minimize differences in the appearance of skin tone, texture and facial features [19]. However, image data derived from JPN AFIS for the FBS database were found to have different image quality. This is because JPN has used different cameras since 2001, from ET Camera to Digital Camera and now IP Camera. Resulting images from each camera type are generally different in terms of quality and resolutions. Furthermore, each JPN branches have different lighting conditions further affecting image quality.

Aging is a natural process-however it would modify our facial features such as sagging, pigmentation, wrinkling and many more. This is a form of biometrics features modification that could affect the matching process between stored data and live image sample [21]. During the study period, it was found that some of the live image samples were compared with images taken decades ago–where facial features have changed rather significantly.

Facial occlusion is the use of accessories (i.e. eyeglasses) that partially occlude the camera view resulting into missing discriminative information [22]. It was found that if eyeglasses were present in the applicant's image sample, the FBS database would extract candidate images with similar eyeglasses rather than focusing on facial features alone. This is because eyeglasses can become a significant facial landmark [22].

4. Conclusion

The analysis conducted and the findings reported in the previous section gives light to the capability of FBS as a biometrics system for finger-disabled applicants. Despite its flaws, these are generally minor and within the acceptable rate for a biometrics system [13].

In stark reality, the system has demonstrated high capabilities of reliability even though only used in two months, as shown by the Equal Error Rate of 10% and high matching score within threshold value of 2293. It is also desirable to use considering that the verification process is at most 24 seconds, far more tempting than the three-month manual process finger-disabled applicants are usually subjected to. This shows that Multimodal Biometrics System using facial recognition such as FBS can work within JPN environment.

Of course, there is room for improvement to better improve the system's reliability which is largely technical in nature. If FBS is to be employed, there is a need for reliable network connectivity so the matching process can run smoothly particularly when deriving data for comparison. The image quality for data preservation needs to be maintained and this calls for standardization of camera use as well as lighting environment. It would also be useful if applicants could have their picture taken for data maintenance on a more frequent basis so the biometrics features modification can be registered into the system. All of this would further improve the matching algorithm calculation resulting into superior system performance.

For future work, additional features of soft biometrics traits such as gender, ethnicity, and facial markers can be introduced into the system. This is because Malaysia is a diverse country with many ethnicities each with its unique facial features. The introduction of soft biometrics traits could extract further features useful for identity matching and adding scenario flexibilities for JPN.

In depth studies such as regression analysis could be carried out to predict and forecast the FBS use on more transaction or longer usage period. Also, the system could be introduced to other group of users and not restricted to only finger-disabled applicants. Moreover, FBS can potentially work as multimodal system which can receive both fingerprint and image input. All that is required is the integration of fingerprint scanning hardware into the system. This would help JPN maintain one type of system when managing citizens data and issuing MyKad for Malaysia. Lastly, a comparative study with current study as well as other techniques could be considered to further establish the feasibility of this system.

Acknowledgment

The authors would like to express the gratitude to the Ministry of Higher Education, Malaysia and Universiti Teknologi MARA, Selangor, Malaysia for the financial support given for this project (Fundamental Research Grant Scheme–FRGS) [File No: 600-RMI/FRGS 5/3 (0007/2016)].

References

[1] Komarinski P. Automated Fingerprint Identification Systems. *Elsevier Academic Press*. 2005.
[2] Kataria AN, Adhyaru DM, Sharma AK, Zaveri TH. *A survey of automated biometric authentication techniques*. Nirma University International Conference on Engineering. 2013.
[3] Raju AS, Udayashankara V. *Biometric person authentication: A review.* In Proceedings of 2014 International Conference on Contemporary Computing and Informatics. 2014: 575–580.
[4] Khandait SP, Thool RC, Khandait PD. Hybrid Facial Geometry Algorithm for facial feature Extraction and Expression Recognition using ANFIS and BPNN. *Bulletin of Electrical Engineering and Informatics.* 2013; 2(1): 11-22.
[5] Sein MM, Win ZM, Wai EP. Authentications of Myanmar National Registration Card. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI).* 2013; 1(2): 53-58.
[6] Grother P, Ngan M. *Face recognition vendor test. Performance of face identification algorithms*. NIST Interagency Report 8009. 2014.
[7] Somani G, Chaudhary S. *Application performance isolation in virtualization*. IEEE International Conference on Cloud Computing. 2009: 41–48.
[8] Ross AA, Nandakumar K, Jain AK. Handbook of Multibiometrics. Springer. 2006; 6.
[9] Malik J, Girdhar D, Dahiya R, Sainarayanan G. Reference threshold calculation for biometric authentication. *International Journal of Image, Graphics and Signal Processing*. 2014; 6(2): 46
[10] Youmaran R, Adler A. Measuring biometric sample quality in terms of biometric feature information in iris images. *Journal of Electrical and Computer Engineering*. 2012: 22.
[11] Niinuma K, Park U, Jain AK. Soft biometric traits for continuous user authentication. *IEEE Transactions of Information Forensics Security*. 2010; 5(4): 771–780.
[12] Luque-Baena RM, Elizondo D, Lopez-Rubio E, Palomo EJ, Watson T. Assessment of geometric features for individual identification and verification in biometric hand systems. *Expert Systems with Application*s. 2013; 40(9): 3580–3594.
[13] International Biometric Group, "Comparative Biometric Testing", from http://www.biometricgroup.com/reports/public/comparative_biometric_testing.html
[14] Toh KA, Kim J, Lee S. Biometric scores fusion based on total error rate minimization. *Pattern Recognition*. 2008; 41(3): 1066–1082.
[15] DeCann B, Ross A. *Can a "poor" verification system be a "good" identification system? A preliminary study*. Proceedings of the 2012 IEEE Internmational Workshop on Information Forensics and Security. 2012: 31–36.
[16] Bansal A, Agarwal R, Sharma RK. *FAR and FRR based analysis of iris recognition system*. 2012 IEEE International Conference on Signal Processing, Computing and Control. 2012.
[17] Abadie A, Imbens GW. Matching on the estimated propensity score. *Econometrica.* 2016; 84(2): 781-807.
[18] Jain AK. *Biometric recognition: How do I know who you are?* Signal Processing and Communications Applications Conference. 2004: 3-5.
[19] Tan X, Triggs B. Enhanced local texture feature sets for face recognition under difficult lighting conditions. *IEEE Transactions on Image Processing*, 2010; 19(6): 1635–1650.

[20] Wu Y, Wang Z, Ji Q. *Facial feature tracking under varying facial expressions and face poses based on restricted boltzmann machines*. Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition. 2013: 3452–3459.
[21] Lanitis A, Tsapatsoulis N. Quantitative evaluation of the effects of aging on biometric templates. *IET Computer Vision*. 2011; 5(6): 338.
[22] Min R, Hadid A, Dugelay JL. *Improving the recognition of faces occluded by facial accessories*. IEEE International Conference on Automatic Face and Gesture Recognition and Workshops. 2011: 442–447.