

Fusion of Face and Fingerprint for Robust Personal Verification System

Norsalina Hassan, Dzati Athiar Ramli, and Shahrel Azmin Suandi, *Senior Member, IACSIT*

Abstract—Personal verification system that uses a single biometric trait often faces numerous limitations such as noisy sensor data, non-universality, non-distinctiveness and spoof attack. These limitations can be overcome by multimodal biometric systems that consolidate the evidence presented by multiple biometric sources and typically has better recognition performance compared to systems based on a single biometric modality. This study proposes fusion of face and fingerprint for robust recognition system. The integration is performed at the matching score level. The matching tasks for both modalities are carried out by using support vector machines (SVM) as the classifier. Experiments on face expression and fingerprint database show that the performances of multimodal biometric system provide better recognition compared to single biometric modality. Based on the fusion techniques evaluated, trait-specific weight was found to be highly effective than the sum rule-based fusion. Equal error rate (EER) percentage for face- only and fingerprint- only systems are 2.50% and 5.56%, respectively, while the EER for system using sum rule- based fusion and system using trait-specific weights are 0.833% and 0.340%, respectively.

Index Terms—Multi-modal, sum-rule and trait-specific, face and fingerprint biometrics.

I. INTRODUCTION

Biometric recognition is a new technology that has become the foundation of an extensive array of highly secure identification and personal verification solutions. Biometric-based solutions are able to provide confidential financial transactions and personal data privacy. The aim of biometrics is to distinguish automatically between subjects based on one or more biometric factor derived from individual's physical or behavioral characteristics, such as fingerprints, face, irises, voice patterns, gait or written signature. Authentication system built based on single biometric feature sometimes fail to be exact enough for verifying the identity of a person because it only relies on a single evidence of information (e.g., single fingerprint or face). The desired performance in real application may not be achieved by the systems due to several limitations such as

Manuscript received April 8, 2014; revised May 24, 2014. This work is partially supported by Universiti Sains Malaysia Research University Individual (RUI) Grant No. 1001/PELECT/814208.

Norsalina Hassan was with Intelligent Biometric Group, School of Electrical & Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, 14300, Nibong Tebal, Pulau Pinang, Malaysia. She is currently with the Mathematic, Science & Computer Department, Politeknik Seberang Perai, Jalan Permatang Pauh, 13500 Permatang Pauh, Pulau Pinang, Malaysia (e-mail: nuanafeesa@yahoo.com).

Dzati Athiar Ramli and Shahrel Azmin Suandi are with the Intelligent Biometric Group, School of Electrical & Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, 14300, Nibong Tebal, Pulau Pinang, Malaysia (e-mail: dzati@usm.my, shahrel@usm.my).

noisy data, non-universality or lack of distinctiveness of the biometric traits, unacceptable error rates and spoof attacks [1]. By combining multiple modalities, enhanced performance reliability could be achieved. Multimodal biometric is essentially using more than one biometric factor or modality in establishing and verifying the identity of a given person. Thus, instead of only a fingerprint, the fingerprint is combined with a face image. Recently, multi-modal biometric fusion techniques have attracted increasing attention and interest among researchers in the hope that supplementary information between different biometrics might improve the recognition performance in some difficult biometric problems.

This paper focuses on recognition of a person using multimodal biometric traits namely face and fingerprint. The evidence presented by this multiple sources will be integrated in order to reduce the limitations that have been addressed by deploying single biometric systems. According to Ross and Jain [2], biometric system has four important components, which are sensor module, feature extraction module, matching module and decision-making module. A biometric data acquired from a user by a biometric sensor (e.g., a fingerprint image) is fed into the feature extraction module. Using signal processing methods, the feature extraction module converts a sample into feature set (e.g., fingerprint minutiae), which forms a representation for matching. Usually, multiple features are collected into a feature vector. The matching module takes the extracted feature vector as input and compares it to a stored templates using a classifier or matching algorithm in order to generate matching score. The result is a match score, which is used by the decision module to decide (e.g., by applying a threshold) whether the presented sample matches with the stored template. The outcome of this decision is a binary match or mismatch.

Biometric systems that applied single biometric trait, e.g. fingerprint for user authentication, suffer from several limitations such as noisy sensor data, non-universality or lack of distinctiveness of the biometric traits, unacceptable error rates and spoof attacks [1]. Due to these problems, the desired performance in the real application may not be achieved by the systems. This has motivated researchers in multi-biometric systems [3] to consolidate the evidence obtained from different sources. By using multi-biometric approaches, better performance requirement can be achieved as reported by several researches, for instances in [3]-[8].

When designing a multi-biometric system, one of the fundamental issues to be determined is the type of information that should be fused. The information can be consolidated at the sensor level, feature level, and score level or decision level fusion depending upon the type available in any of these levels. According to Sanderson and Paliwal [9],

information fusion in biometric systems can be classified into two broad categories: fusion before matching and fusion after matching. In order to determine the accuracy, performance of biometric system can be performed by measuring the error rates. There are two key error rates in biometrics, which are false acceptance rate (FAR) and false rejection rate (FRR) at various thresholds. False acceptance rate (FAR) is when the probability of an impostor is accepted as being a genuine individual (client), while false rejection rate (FRR) is when the probability of genuine individual (client) is rejected as being an impostor. An overall accuracy measurement of a biometric system is called Genuine Acceptance Rate (GAR), which equals to $1 - FRR$.

This work proposes multimodal biometric system to overcome the limitation of individual biometric system. The biometric modalities are processed sequentially until an acceptable match is obtained. The matching module for both modalities utilizes Support Vector Machine (SVM) classifier to generate the matching scores. The feature extraction for fingerprint images uses the existing minutiae extraction algorithm [10]. The integration of face and fingerprint traits is proposed to enhance recognition performance and accomplish better results compared with face-only or fingerprint-only system. The matched scores generated by each biometric source are directly combined into a total score by sum-rule. The performance achieved is then compared with the user-specific weight fusion technique.

The remaining of this paper is organized as follows: Section II describes the proposed multimodal biometric system. Section III discusses the result and discussion for this project. The performance of two fusion approaches is analyzed and compared. The final section, Section IV presents the conclusion and recommendation for future work.

II. PROPOSED MULTIMODAL BIOMETRIC SYSTEM

Fingerprint recognition system using minutiae extraction technique is adopted in this work. This method is taken from Ref. [10] who has utilized FVC2002 in his study. The same methods are tested on FVC2004 DB_1B. The available face database has also been prepared in which the background has been excluded, and the intensity is used as the feature vector. Fig. 1 shows the entire structure of the proposed system.

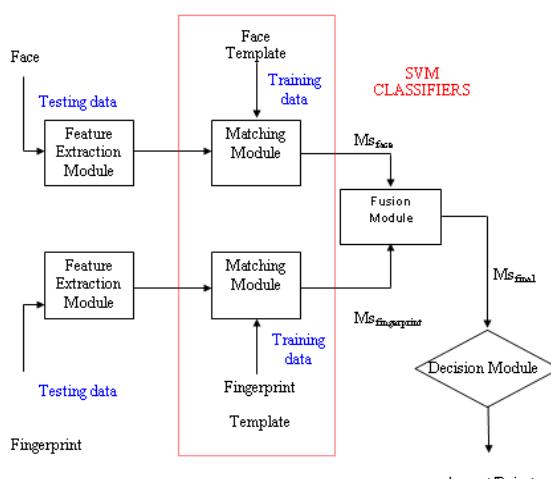


Fig. 1. Architecture of face and fingerprint multimodal biometric system.

Support Vector Machine (SVM) [11] is used as the classifier to execute the pattern matching phase. SVM is a useful technique for data classification within two-classes. But in this work, classification problems involve more than two classes. In order to modify from two classes to q -class problems with SVM, q training classes have to be involved. This can be done by using one-vs-all approach, which separates a single class from the remaining classes. For this one-vs-all, a test point is classified into the respective class which associated classifier has the highest score among all classifiers. In this study, there were 10 individuals in the database so there will be 10-class classification. That means 10 binary SVM models are being created. Each model is trained to discriminate one class from the remaining classes. Client samples are labeled as type +1 and imposter as type -1. Fig. 2 shows the testing protocol for both databases where shot 1 of P1 in training set is tested with all testing samples. For the purpose of this study, four images per subject are used as training samples. The remaining four images per subject are used as testing samples. The first shot of P1 corresponds to four genuine tests and 36 impostor tests. The whole recognition involves all training samples. Each of the training samples is able to give four genuine scores and 36 impostor scores.

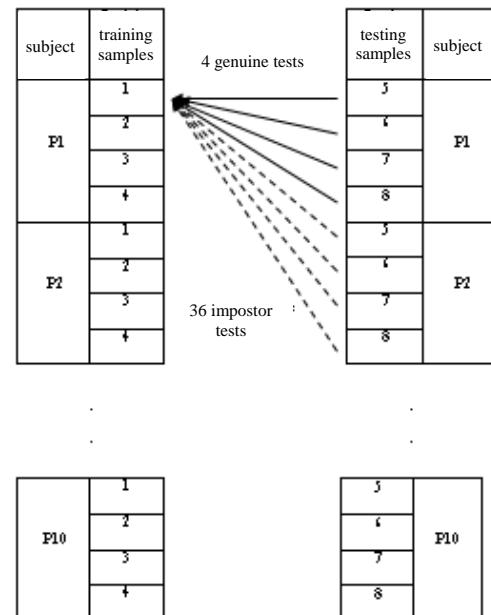


Fig. 2. Testing protocol for fingerprint and face database.

In our work, two fusion schemes are used to combine the scores of each sub-system, which are sum-rule and trait-specific weights. The method of sum-rule based fusion is stated in Equation (1). This procedure can be found in [2]. M_{fc} and M_{fp} are the matching scores produced by the face and fingerprint recognition, respectively. The fused score M_s is calculated using the Equation (1) below,

$$M_s = \omega_1 * M_{fc} + \omega_2 * M_{fp} \quad (1)$$

where ω_1 and ω_2 are the weights assigned to the two biometric traits, M_{fc} and M_{fp} , respectively. The bias of each classifier was not computed so the equal weights were assigned to both modalities. The value assigned in this work

is 0.5 for both ω_1 and ω_2 . These final matching scores are then passed to the decision module and being compared with a certain threshold to recognize the person as genuine or an impostor.

Trait-specific weight is actually the simplified version of user-specific weight [12]. Instead of computing the weighted sum of scores from different modalities for each user, this trait-specific weight computes merely the weights for different traits. Thus, making the similarity computation becomes simpler and more generalized among users. Let ω_1 and ω_2 be the weights assigned to the face and fingerprint, respectively. The weights trait are varied over the range of [0, 1] in step of 0.01, such that the limit $\omega_1 + \omega_2 = 1$ is fulfilled. Equation (2) is used to compute the weighted sum of scores, S_w .

$$S_w = \omega_1 * M_{fc} + \omega_2 * M_{fp} \quad (2)$$

III. RESULTS AND DISCUSSIONS

In this study, the face database is taken from Electrical and Computer Engineering Department of CMU (Advanced Multimedia Processing Lab) [13]. The database contains 13 subjects where the 75 facial images were taken with varying expressions for each subject. These face images are collected in the same lighting condition using CCD camera. Face images have been well-registered by the eyes location. For the purpose of this study, only 10 subjects with 8 images each were selected. The fingerprint images are taken from FVC2004 DB1_B database [14]. The database contains 10 fingers with 80 images. Four images per subject are used as training samples. The remaining four images per subject are used as testing samples. Consequently, the fusion experiment consists of $4 \times 10 = 40$ genuine scores and $36 \times 10 = 360$ impostor scores.

The performance is evaluated using Equal Error Rate (EER), a specific point attained when FAR (False Acceptance Rate) and FRR (False Rejection Rate) coincide. A graphical representation of the capabilities of the individual matchers is shown in the ROC (Receiver Operating Characteristic) plot. In these ROC curves, Genuine Acceptance Rate (GAR) are plotted versus FAR with the threshold varies in the step of 0.01. Performances of the proposed fusion schemes using sum-rule and trait-specific weight were evaluated and represented by ROC curves.

Fig. 3 shows the performance of face recognition system. At the false acceptance rate of 2%, the GAR performance is 97.5%. The system performance based on EER achieves the value of 2.5%. Fig. 4 shows the face distributed from genuine and impostor match similarity. Here, the two populations can be seen, i.e., one is genuine and the other is impostor. It is noticeable that there is a small overlap between the genuine and impostor, where they overlapped each other for the face score because it is nearly impossible to achieve a 100% accurate biometric system. FAR and FRR curves of face recognition system are presented in Fig. 5.

Fig. 6 presents the ROC curve for fingerprint recognition. At FAR equals 2%, the system reaches 77.5% GAR. The EER value is equivalent to 5.56%. The EER is greater compared to the face authentication due to relatively poor

quality of fingerprint images. Fig. 7 shows fingerprint distributed from genuine and impostor match similarity. FAR and FRR curves of fingerprint recognition systems are presented in Fig. 8.

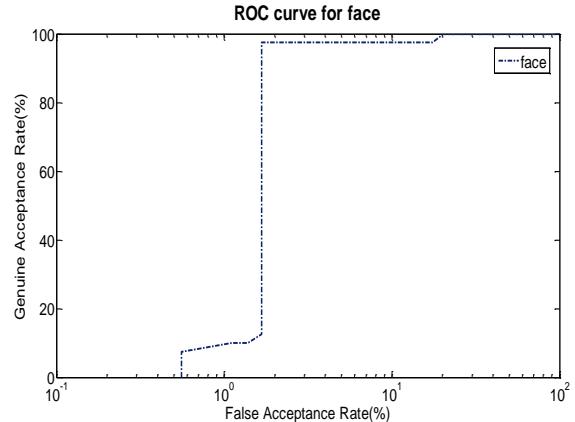


Fig. 3. ROC curve for face recognition performance.

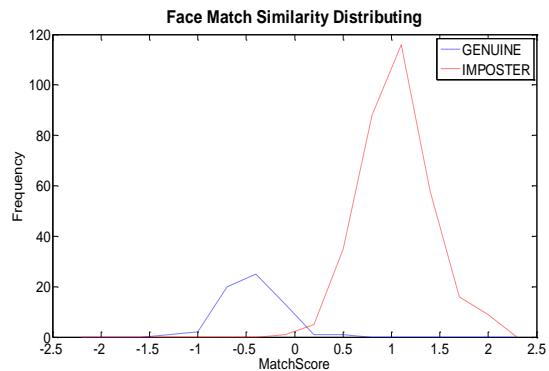


Fig. 4. Face Matching similarity distribution.

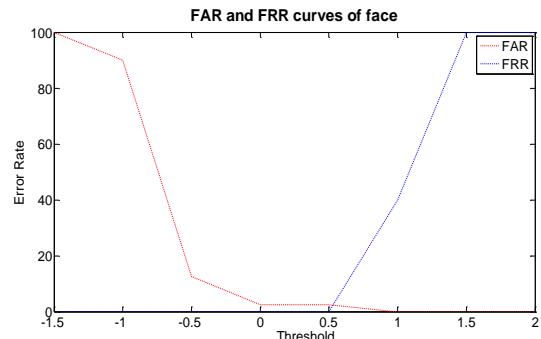


Fig. 5. FAR and FRR curves of face recognition systems.

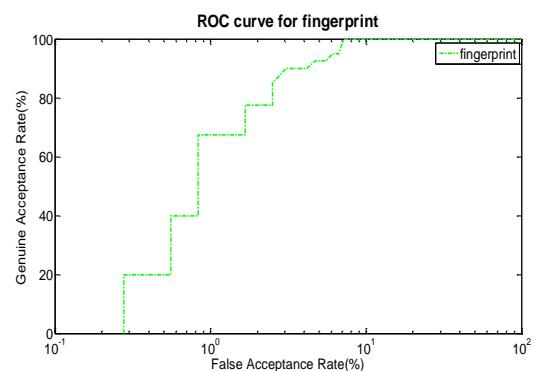


Fig. 6. ROC curve for fingerprint recognition performance.

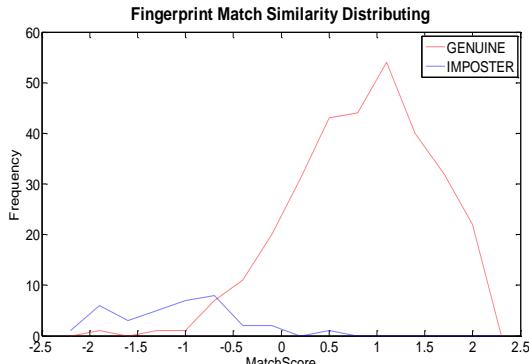


Fig. 7. Fingerprint Matching Similarity Distribution.

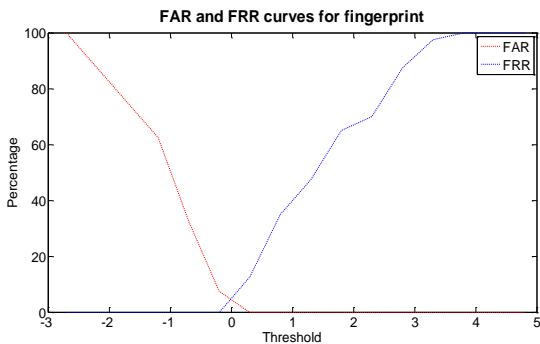


Fig. 8. FAR and FRR curves of fingerprint recognition systems.

The multimodal biometric system is constructed by integrating the fingerprint-only and face-only system. Figure 9 compares the performances of multimodal biometric using the sum-rule fusion technique and trait-specific weights. The sum-rule fusion technique reaches up to 100% GAR at FAR of 2% and the EER is equal to 0.833%. In order to further improve the system performance, traits-specific weights is incorporated in this study. The weights are approximated by finding the best set of weights, which can minimize the total error rate. These scores are weighted according to the biometric traits used in order to increase the influence of more reliable traits (face) and reduce the importance of less reliable traits (fingerprint). The weights ω_1 and ω_2 are varied over the range [0, 1] in steps of 0.01, such that the limit $\omega_1 + \omega_2 = 1$ is fulfilled. The best assigned weights of [0.3, 0.7] outperform the sum-rule fusion technique. The system performance is nearly 100% GAR at FAR equal 0.568% and the EER is equal to 0.34%. Table I shows the EER performances of face only system, fingerprint only system, sum-rule and trait-specific weights with different assigning weights.

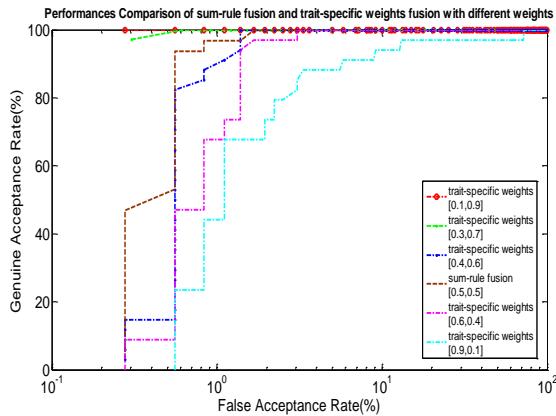


Fig. 9. Performances of sum-rule fusion and trait-specific weights fusion with different assigning weights for face and fingerprint trait.

TABLE I: EER PERFORMANCES OF SINGLE MODAL SYSTEM, SUM-RULE FUSION AND TRAIT- SPECIFIC WEIGHTS FUSION WITH DIFFERENT ASSIGNING WEIGHTS FOR FINGERPRINT AND FACE TRAIT

System	EER (%)
Face Only	2.50
Fingerprint Only	5.56
Sum-rule	0.83
$\omega_1 = 0.9,$ $\omega_2 = 0.1.$	0.00
$\omega_1 = 0.7,$ $\omega_2 = 0.3.$	0.34
Trait Specific Weights	0.69
$\omega_1 = 0.6,$ $\omega_2 = 0.4.$	0.69
$\omega_1 = 0.4,$ $\omega_2 = 0.6.$	2.98
$\omega_1 = 0.1,$ $\omega_2 = 0.9.$	8.85

IV. CONCLUSIONS

The performance of face-only systems and fingerprint-only systems are evaluated in this paper. Comparison between the two systems is conducted, in which the performances of face-only systems is better compared to the fingerprint-only system. Then the best matcher of individual modality is compared to the two fusion techniques proposed. The results using the sum rule-based fusion and trait-specific weights showed improved performance. The experimental results also demonstrated that the trait-specific weights outperformed the sum rule-based fusion in term of EER. The EER for fingerprint recognition is relatively high due to poor quality of fingerprint images in the database caused by skin and impression conditions. The feature extraction using minutiae-based should be improved in order to get clearer ridge details and minutiae localization. To obtain the best classification using SVM, the supplement of minutiae information for poor quality fingerprint images is needed.

REFERENCES

- [1] A. Ross and R. Govindarajan, "Feature Level Fusion Using Hand and Face Biometrics," in Proc. SPIE Conference on Biometric Technology for Human Identification II, vol. 5779, pp. 196-204.
- [2] A. Ross and A. K. Jain, "Information Fusion in biometrics," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2115-2125, 2003.
- [3] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEE Transactions on Circuits and Systems for video technology*, vol. 14, no. 1, 2004.
- [4] R. Brunelli and D. Falavigna, "Personal identification using multiple cues," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 1710, pp. 955-966, 1995.
- [5] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, "On combining classifiers," *IEEE transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 3, pp. 226-239, 1998.
- [6] L. Hong and A. K. Jain, "Integrating faces and fingerprint for personal identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 16, no. 1, pp. 66-75, 1998.
- [7] K. Nandakumar, *Multibiometric Systems: Fusion Strategies and Template Security*, Phd Thesis, Michigan State University, 2008.
- [8] M. He, S.-J. Horng, P. Fan, R.-S. Run, R.-J. Chen, J.-L. Lai, M. K. Khan, and K. O. Sentosa, "Performance evaluation of score level fusion in multimodal biometric systems," *Pattern Recognition*, vol. 43, issue 5, pp. 1790-1800, May 2010.

- [9] C. Sanderson and K. K. Paliwal, "Information fusion and person verification using speech and face Information," Research paper IDIAP-RR 02-33, 2002.
- [10] W. Vincent, "Fingerprint recognition," Thesis degree, Hong Kong Baptist University, 2002
- [11] V. Wan and W. M. Campbell, "Support vector machines for speaker verification and identification," in *Proc. the 2000 IEEE Signal Processing Society Workshop*, pp. 775-784, 2000.
- [12] A. K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric system," *Pattern Recognition*, vol. 43, pp. 2270-2285, 2005.
- [13] Face Authentication. (August 10, 2010). [Online]. Available: <http://chenlab.ece.cornell.edu/projects/>
- [14] FVC2004. (August 10, 2010). [Online]. Available: <http://bias.CSI.unibo.it/fvc2004/download.asp>



Norsalina binti Hassan was born in Penang, Malaysia in 1974. She received her M.Sc in electronic systems design from Universiti Sains Malaysia, Penang. B.Eng in electrical engineering from Universiti Teknologi Malaysia, Johor, Dipl. Eng in electronic engineering from Politeknik Ungku Omar, Ipoh in 2011, 2001 and 1996, respectively.

In 2002, she joined Electrical Department at Politeknik Seberang Perai as a lecturer and in 2011 became the Head of Course (Science) of Mathematics, Science & Computer Department at the same Polytechnic. She is one of the team writers of Engineering Science for Polytechnics Students Book published in 2012.



Dzati A. Ramli is a senior lecturer at Universiti Sains Malaysia. She received her B. App Sc. and MS degrees in mathematics from Universiti Sains Malaysia in 1995 and 1999, respectively, and her PhD degree in electrical, electronics & systems engineering from Universiti Kebangsaan Malaysia in 2010. Her current research interests include machine learning, artificial intelligence and biometric systems. She is a member of IEEE society.



Shahrel A. Suandi received his B.Eng. in electronic engineering, M.Eng. and D.Eng. degrees in information science from Kyushu Institute of Technology, Fukuoka, Japan, in 1995, 2003 and 2006, respectively.

He is currently an associate professor at Universiti Sains Malaysia, Engineering Campus, Penang, Malaysia and the coordinator of Intelligent Biometric Group (IBG). Prior to joining the university, he worked as an engineer at Sony Video (M) Sdn. Bhd. and Technology Park Malaysia Corporation Sdn. Bhd. for almost six years. His current research interests are face based biometrics, real-time object detection and tracking, and pattern classification. He has published more than 70 technical papers in book chapters, journals and proceedings. Recently, he and his team has commercialized a research product known as FaceBARS®.

Dr. Suandi is currently a member of IEEE, ACM, IET, IEICE and senior member of IACSIT. He has served as a reviewer to a few international conferences and journals including IET Computer Vision, IET Biometrics, Sensors, Journal of Visual Communication and Image Representation, Journal of Electronics Imaging, Journal of Computer Science and Technology (JCST), World Applied Science Journal (WASJ), International Journal of Computer Systems Science and Engineering (IJCSE), IEEE Workshop on Applied Computer Visions (WACV), IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS).