International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 5 (2013) pp. 373-382

Consolidation of Fingerprint Databases: Challenges and Solutions in the Malaysian context

Chiung Ching Ho[1], C. Eswaran[2]

[1] Faculty of Computing and Informatics, Multimedia University
Jalan Multimedia, Cyberjaya 63100, Selangor, Malaysia
ccho@mmu.edu.my

[2] Faculty of Computing and Informatics, Multimedia University
Jalan Multimedia, Cyberjaya 63100, Selangor, Malaysia
eswaran@mmu.edu.my

***Abstract*: This paper presents the challenges of consolidating fingerprint databases in Malaysia as well as approaches that can be taken to solve some of these challenges. Solutions leverages on opportunities presented by standard bodies, advances in cloud computing as well as a framework which leverages on classifiers and decision fusion in order to reduce the large search space expected of a consolidated fingerprint database. Empirical results are presented to demonstrate the viability of the feature search space reduction framework, as well as to demonstrate the robustness and scalability of the framework when additional biometric modalities are required to be considered.**

***Keywords*:** Finger print database, multimodal biometric framework ,AFIS, MAFIS, BIOFIS, NERS

I. Introduction

Fingerprint is a biometric modality that is often used in a security setting [1]. Fingerprint databases are in use worldwide for the purposes of personal identification, border control as well as to facilitate criminal forensic investigation. Many countries have multiple fingerprint databases, with each database serving a specific purpose. In Malaysia, there are at least 4 different fingerprint databases; namely PDRM-MAFIS (Polis Di Raja Malaysia- Malaysian Automated Fingerprint Identification System), PDRM-BIOFIS (Polis Di Raja Malaysia-Biometric Identification System), NRD-AFIS (National Registration Department- Automated Fingerprint Identification System), and NERS (National Foreigners Enforcement and Registration System). Two more fingerprint databases are in the planning, one for the registration of foreign maids and other foreign workers and another for the use of the EC (election commission) for the maintenance of the electoral roll.

The consolidation of fingerprint databases will enable cross-referencing to be done easily. For instance, the PDRM-BIOFIS fingerprint database contains the fingerprints of criminals. These criminals are often under travel restriction, and upon cross-referencing with the NERS fingerprint database will allow easy refusal of entry and exit at immigration points. Other uses-cases for integration of fingerprint databases will be highlighted in a latter section of this paper.

This paper will examine the current state of integration of fingerprint databases in Malaysia, the challenges of integration, and possible solutions for fingerprint database integration. Section I of this paper presents an overview on fingerprint databases in Malaysia. Section II contains an overview of the development of fingerprint databases, fingerprint recognition and the description of the individual fingerprint databases in Malaysia. Section III presents use cases for consolidating existing Malaysian fingerprint databases. Section IV describes the challenges of integrating different fingerprint databases while Section V presents possible solutions. Section VI continues the paper by summarizing key points as well as presenting a discussion on the way ahead in future.

II. Related Works

A. History of fingerprint and fingerprint databases

Fingerprints are the first biometric modality to be easily captured, stored and compared for recognition of an individual. A fingerprint is an efficient proof of a person's identity as it is unique, universal (except for rare cases whereby a person's fingerprint is not legible due to genetic mutation [2], illness or physical harm) and does not change much over time.

In 1858, Sir William James Herschel used fingerprints on contracts in India as proof of identity. Gilbert Thompson used his own set of fingerprints to prevent forgery of documents in 1892. This practice is still prevalent in modern society, as an acceptable alternative to signatures for contracts and other legal documents. Cole's work in [3] is a good summary of the history of fingerprints.

The works of Malpighi in the 17th century laid the groundwork for the usage of fingerprint in forensic science. Coulier established the technique for capturing fingerprints on paper via iodine fuming, to be examined later by a magnifying

glass. Dr. Henry Faulds furthered the field of fingerprinting by classifying fingerprints in the 1870s, and published his ideas on the potential of fingerprints for personal identification in a short letter to the journal Nature. Bertillon incorporated fingerprints as an extension to his anthropometry framework for person identification in the late 19th century. The first finger print database was created by Juan Vucetich [4] in 1891, and it was used to successfully solve a murder case in 1892. Azizul Haque and Hem Chandra Bose subsequently established the world's first Fingerprint Bureau and developed the Henry system of fingerprint classification as reported in [3]. The Henry system of fingerprint classification was then used extensively in the penal systems and armed forces of the United Kingdom and United States of America in the early 20th century. In 1924, the FBI (Federal Bureau of Investigation) was authorized by law to establish an Identification Division, which saw the consolidation of the National Bureau of Criminal Identification and the US Justice Department's Bureau of Criminal Identification fingerprint files. By 1971, the FBI's database of fingerprints has grown to 200 million records. This set of 200 million records was computerized in 1980 to become the fingerprint identification system known as FBI-IAFIS (Integrated Automated Fingerprint Identification System). Figure 1 shows the IAFIS system as shown on the FBI's homepage.

Figure 1. IAFIAS system

B. Discriminating features in fingerprint

Fingerprints are unique across individuals by virtue discriminate features. A fingerprint can be described as a combination of ridges and valleys on the skin. Ridges and valleys form patterns known as arches, loops and whirls as described by Kawagoe and Tojo in [5] and by Moayer and Fu in [6]. [4] and [5] both extend on Henry's system of fingerprint classification. Minutia points can be extracted from ridge endings (where the ridge ends) and ridge bifurcation (where the ridge splits into two). Minutia points can further be described as dots (tiny ridges), islands (ridges slightly longer than dots, occupying a middle point between two temporarily branching ridges), ponds or lakes (empty points between two temporarily radiating ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other). Individual minutia features also has local features, such as orientation, size and pores. Chen and Jain suggested a hierarchy of features starting from fingerprint patterns, to minutia and ridges ; and finally pores in their work reported in *[7]*. Fig. 2 shows the location of minutia points on a finger print.

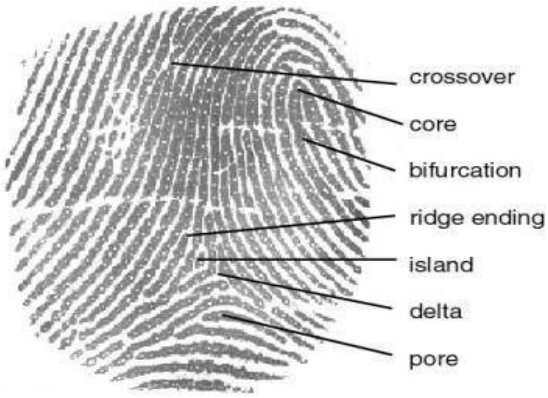

Figure 2. Minutia points on a fingerprint

C. Fingerprint recognition

Fingerprint recognition is a 1:M process that compares features extracted from fingerprints to an existing fingerprint database. The fingerprint recognition process is shown in Fig. 3.

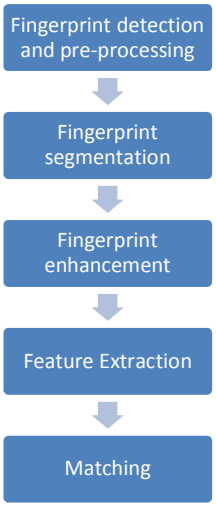

Figure 3. Fingerprint recognition process

The process of automatic fingerprint recognition begins by the detection of the fingerprint. Pre-processing such as orientation correction and scaling is done next. Fingerprint segmentation is the process whereby the fingerprint image is extracted from the background. Segmentation will save on processing time as the region of interest (ROI) is minimized. Subsequently the fingerprint image that has been segmented is then enhanced via image processing techniques, especially if the fingerprint image quality is low. Enhancement will aim at improving the quality of the ridge structure as well as increasing the consistency of the ridge orientation. Feature extraction is then done, on both a global and local feature level. Global features of a fingerprint includes orientation, and singularity . Minutia features are extracted via operations such as thinning and binarization after minutia detection. Features extracted from the fingerprint are then assessed either as coordinates , or assessed in terms of quantity and quality. Subsequently, classification algorithm are employed to classify each fingerprint. A probe (unknown fingerprint) is then submitted to the classifier for the recognition process to be completed. Karu's work in [8] reports on the effectiveness of rule-based algorithm for classification of fingerprints while Ratha demonstrates the viability of fingerprint recognition on a large fingerprint database with a real time constraint in [9]. Other usage of innovative classifiers included efforts such as Ben Ayed et al. [10] which utilized the DECOC classifier in an automatic fingerprint recognition system. Griaule Biometric has an e-book [11] which further describes the recognition process as well as discusses SDK(software development kit) available for use in fingerprint recognition.

D. Fingerprint databases

1) FBI IAFIS

The FBI-IAFIS [12] is perhaps the world's best known fingerprint database, given its exposure in the media as well as in the entertainment industry. FBI-IAFIS is available 24-hours year round. It contains the fingerprints of 69.8 million criminals, as well as 31 million civil subjects. For the criminal records, fingerprint are stored with additional information such as past criminal record, outstanding arrest warrants, mug shots and physical characteristics such as height, weight and tattoos. FBI-IAFIS started in July 28, 1999 and its records grow by 8,000-10,000 records per day.

Each record submitted consists of a 10 rolled fingerprint and their corresponding flat fingerprint. Palm prints are also beginning to be submitted which saw 109,707 palm prints submitted in the year 2011 up to the month of July. Average response time to an electronic submission for information is 10 minutes.

Information interchange is done via the EFTS (Electronic Fingerprint Transmission Specification) which specify the format for electronic interchange between the FBI and its partner agencies. EFTS is currently at version 7.1 which has been expanded to include other biometric modalities such as palm prints and iris scans. EFTS 7.1 is compliant to the American National Standards Institute/National Institute of Standards and Technology-Information Technology Laboratory 1-2007 (ANSI/NIST-ITL 1-2007) [13] standard includes new record types to facilitate data sharing for new biometric modalities.

The FBI-IAFIS sets the standard for fingerprint databases the world over due to its size and efficiency. The adoption of the ANSI/NIST-ITL 1-2007 standard for electronic record interchange will go a long way towards subsequent adoption of the same standard by other fingerprint databases.

2) PDRM-MAFIS

PDRM-MAFIS is the name of the fingerprint database maintained by the Royal Malaysian Police. It is a manual system with 1.5 million records stored and has been in used since 1996. PDRM-MAFIS , like other manual fingerprint database; has low effectiveness with 377 matches in 2008 and 356 in 2007 [14]. Fingerprints were recorded using ink and then manually submitted on a paper form to one of the 3 centres for processing. Average processing time was between 3-4 days. Fig. 4 shows a screenshot of the system.

Figure 4. PDRM-MAFIS screenshot

3) PDRM-BIOFIS

PDRM-BIOFIS is an upgrade of the PDRM-MAFIS fingerprint database [15]. The most significant update was that fingerprints are scanned into the PDRM-BIOFIS database at 50 police stations nation-wide and electronic data interchange allows instantaneous submission to the centralized database located in police headquarters in Bukit Aman, Kuala Lumpur. Processing time is reduced to 10 minutes compared to the 3-4 days required by PDRM-MAFIS. The increased efficiency saw 1015 successful fingerprint matches achieved in 2009 compared to just a few hundred successes in the previous two years. There are 1.3 million records stored in PDRM-BIOFIS and it is linked electronically to the NRD-AFIS. Fig. 5 shows a screenshot of PDRM-BIOFIS.

Figure 5. PDRM-BIOFIS screenshot

4) NERS

NERS is the latest finger database to be introduced in Malaysia. The purpose of NERS is to collect fingerprints of non-Malaysians who enter the country, as well as non-Malaysians already working in the country. NERS fingerprint capture will be done at 96 immigration entry-and-exit points in the country [16]. As of July 27th 2011, 390,404 non-Malaysian workers were registered via 37 Immigration Department offices, with each enrolment completed in 2 minutes on average. In the future, an additional 250,00 non- Malaysian maids are expected to be added to NERS upon the renewal of their work permit[17]. Currently, NERS is planned to connect electronically to PDRM-BIOFIS and there are also plans to connect NERS to the Advanced Passenger Screening System (APSS) to speed up the screening process [18]. Fig.6 shows an excerpt from a Immigration Department pamphlet describing the usage of NERS.

Figure 6. NERS recording of fingerprint

5) Immigration Biometric Control System(IBCS) fingerprint database

The ICBS fingerprint database is used as part of Malaysia's amnesty programme for foreign worker. This programme known as PATI[19] is meant to collect an accurate count of foreign workers currently in Malaysia, notwithstanding their legal status as foreign workers. Non-registered foreign workers who sign up for the PATI programme will be granted amnesty and will not be subjected to legal action. To date, 2,222,636 foreign workers has been enrolled in the PATI programme [20]. Fig.7 shows a screenshot of the ICBS.

Figure 7. Screenshot of ICBS

III. Consolidation of Fingerprint Databases in Malaysia

A. Use cases for consolidated fingerprint databases

The argument for consolidating separate fingerprint databases into a consolidated fingerprint database resource is many-fold. A consolidated fingerprint database will:

- Save storage space by removing redundant fingerprints
- Ease cross-referencing between previously disparate fingerprint databases
- Reduce network traffic overhead
- Save cost on equipment and software

The Biometric Identifiers and Border Security: 9/11 Commission reported in [21] the need for integration of biometric databases in the USA. In 2005, the USA had the FBI-IAFIS fingerprint database, the Automated Biometric Fingerprint Identification System (IDENT) for non-US citizens, the National Security Entry-Exit Registration System (NSEERS) for non-US citizens on watch lists, the US-VISIT fingerprint database for visitors to the USA, and the Consular Consolidated Database (CCD) which records fingerprints of visa applicants.

The same report described an issue with rising cost for maintaining so many different fingerprint databases (primarily the cost of equipment and software) and performance of these different fingerprint databases.

Table 1 describes use cases for consolidating fingerprint databases in Malaysia.

Table 1 : Use cases for consolidating fingerprint databases in Malaysia

Fingerprint Database 1	Fingerprint Database 2	Use case for consolidation
PDRM-BIOFIS	NERS	Visitors to Malaysia as well as non-citizen workers can be

		screened for criminal activities – corrective action such as denial of entry or tracking can be done
PDRM-BIOFIS	NRD-AFIS	NRD can update records of deceased Malaysian as the death certificate is issued by the Police Department
PDRM-BIOFIS	NERS	Non-Malaysian maids can be checked for criminal records prior to the renewal of their work permit
Electoral Roll	NRD-AFIS	Voters' list can be updated at all times to reflect change of address, change of citizenship as well as death of voters

IV. Challenges of Integrating Fingerprint Databases in Malaysia

A. Non-uniform format for fingerprint capture

Each of the fingerprint database used in Malaysia have their own format for capturing and recording fingerprints. NRD-AFIS, being a civil fingerprint database; only stores the left and right thumbprints. This is similar to the Immigration Department's fingerprint database for passports, which likewise stores the left and right thumb prints only. ICBS stores 8 fingerprints from the left and right hand, without storing the thumbprints. NERS stores the right and left index fingers. PDRM-BIOFIS, being a law enforcement fingerprint database, stores a tenprint roll, which consists of all ten digits of the left and right hand. The most glaring discrepancy is the lack of thumbprints in ICBS and NERS, which may make consolidation with NRD-AFIS and the passport related fingerprint database impossible. PDRM-BIOFIS on paper should be able to be consolidated with the other fingerprint databases easily.

Related data fields for each of the fingerprint such as the identifier, date and time of recording, purpose etc. and so forth are also highly differentiated across these fingerprint databases. This further complicates the consolidation process should information integrity and accuracy be of concern.

B. Number of records

Consolidation of fingerprint databases in Malaysia is also affected by the number of records stored in each database. Table 2 shows the known number of records in each database.

Table 2: Number of known records in Malaysian fingerprint databases

FINGERPRINT DATABASE	NUMBER OF RECORDS
PDRM-BIOFIS	1.3×10^6
NRD-AFIS	18×10^6
NERS	390,404
ICBS	2.2×10^6

If these records were to be consolidated using a SQL JOIN operation the resulting dataset could be 2×10^{25} records. Such a huge database would require considerable computational resources in order to give useable matching results.

Even if a more traditional 1:M combination of data set is done, it would mean consolidating the PDRM-BIOFIS (containing 1.3 million records) fingerprint database with any of the other fingerprint database. At this juncture, it is worth noting that each individual record in these fingerprint database contain at least 2 to 10 fingerprints, all of which need to be probed in a fingerprint recognition process.

C. Physical distance

At present, the PDRM-BIOFIS fingerprint database is situated at Bukit Aman, Kuala Lumpur. This fingerprint database will be cross-referenced by other fingerprint databases which are located far away. For instance, there are 33 Customs, Immigration and Quarantine (CIQ) centres located at major entry points to the country. The distance to th CIQ centre in Johor Bahru (which is the nearest checkpoint to Singapore) is 339 kilometres , while the distance to the CIQ in Padang Terap (which is the nearest checkpoint to Thailand) is 465 kilometres. The CIQ centres in Kuching and Kota Kinabalu are 997 kilometres and 1622 kilometres away from PDRM-BIOFIS respectively. Fig. 8 shows the relative position of PDRM-BIOFIS to the aforementioned CIQ centres.

Figure 8. Location of PDRM-BIOFIS relative to major CIQ centres

Physical distance will increase the processing time of fingerprint matching as the data needs to travel over a great distance due to signal attenuation and network related delays such as propagation, queuing, variation, retransmit, coarse timeout and domain name servers (DNS).

D. Scalability and integration with facial biometrics

Civil fingerprint databases are expected to grow in size so long as the national population increases. Law enforcement fingerprint databases will likewise grow naturally due to new cases brought for investigation. Any future consolidated databases will need to be inherently scalable to accommodate future growth.

At the same time, the need for near 100% recognition accuracy may necessitate the incorporation of additional biometric features in addition to fingerprints. The Indian Express [22] has reported that the UID Authority of India expects only 95% accuracy for its upcoming 600 million strong fingerprint database, and thus will be incorporating iris and facial biometrics in addition to fingerprints for increased accuracy.

In Malaysia, the increasing number of camera protected premises as well as camera equipped phones suggests that the usage of facial biometrics alongside fingerprints to be the next logical evolution for fingerprint databases. Civil documents such as the identity card, driving license and passports all currently have the photo identity of the owner of such documents.

V. Solutions

A. Non standardization of fingerprint databases

The problem of non-standardization of fingerprint databases in terms of the format used for the capture and storage of fingerprints has been discussed in Section IV of this paper.

This problem can be addressed in a few ways. The first would be to standardize the process of capturing and fingerprints. This could be done by adhering to international standards such ones developed by the ISO/IEC JTC 1/SC 37 – Biometrics. Table 3 describes some of the standards that could be adopted for standardizing Malaysian fingerprint databases[21].

Although the adaption of these standards may come at a cost, adoption would go a long way towards not only standardizing fingerprint capture and storage, but would also provide a common framework for developing the information technology infrastructure to support the usage of these databases. Furthermore, cost of acquiring these standards could be lowered by the adaptation of these standards as part of the Malaysian Standard for Biometrics. A further advantage of adopting the ISO standards is the ability to share information electronically with other providers and consumers of fingerprint data.

Table 3: ISO standards for fingerprints

STANDARD	PURPOSE
ISO/IEC 19794-4: 2005	Specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas
ISO/IEC 19794-1: 2006	Describes the general aspects and requirements for defining biometric data interchange formats
ISO/IEC 19784-1:2006	Provides a defined interface that allows a software application to communicate with (utilize the services of) one or more biometric technologies
ISO/IEC 19784-2:2007	Describes the interface between a biometric service provider (BSP) and a biometric archive function provider
ISO/IEC 19785-1: 2006	This part of the standard defines a basic structure for standardized biometric information records (BIRs) that consists of three parts, the standard biometric header (SBH), the biometric data block (BDB), and the security block (SB)

B. Feature database instead of fingerprint database

The size of a consolidated fingerprint database comprising of the fingerprint databases mentioned in Section II of this paper is substantial and needs to be addressed accordingly.

Instead of consolidating multiple fingerprint databases, there is another option of converting these fingerprint databases into feature databases. A fingerprint feature database will be substantially smaller in size compared to a conventional fingerprint database. This will speed up data transfer and processing time for fingerprint recognition. Adoption of standards such as ISO/IEC 19794-2: 2005 and ISO/IEC 19794-3: 2006 will further standardize the representation of extracted fingerprint features (the standards currently uses minutiae and spectral features) as well as the techniques used for extraction (quantized cosinusoidal triplets, Discrete Fourier Transformations or Gabor filters). One standard of particular interest is ISO/IEC 19794-8:2006. This standard describes all characteristics of a fingerprint in a small data record and allows for the extraction of both spectral information (orientation, frequency, phase, etc.) and features (minutiae, core, ridge count, etc.).

C. *Replication of databases*

The average time taken for a fingerprint recognition request submitted to PDRM-BIOFIS is reported to be 10 minutes. While this wait time is acceptable for crime scene processing, it becomes unacceptable should it be applied to counter services application such as CIQ or NRD checkpoints. The long wait time can be attributed to the fact that currently there is only one copy of the PDRM-BIOFIS fingerprint database. In Section IV, the challenges posed by distance between databases have been discussed. This problem is made worst considering the importance of PDRM-BIOFIS in any integration scenario – the ability to cross check for criminal history as well as PDRM-BIOFIS' extensive capture of fingerprints (all ten digits are recorded compared to other fingerprint databases which captures limited fingerprints) makes PDRM-BIOFIS a good base for integration, whereby other fingerprint databases would be compared to PDRM-BIOFIS.

One solution would be to replicate the PDRM-BIOFIS fingerprint database across the nation. Having a copy of the PDRM-BIOFIS fingerprint database in Kuala Lumpur (to serve the southern and central region of Malaysia) , Kedah (to serve the northern region of Malaysia) , Kuching (to serve Sarawak) and Kota Kinabalu (to serve Sabah) would go a long way towards reducing the time taken to process fingerprint recognition request. Replication of the PDRM-BIOFIS could be implemented on a private cloud infrastructure to further enhance security, whereby the content is encrypted while being accessible, as described by Curino et. al in [23]. Fig.9 shows the *CyrptDB* technique described by Curino which allows for replication of a relational database over a cloud infrastructure with provisioning for different levels of encryption.

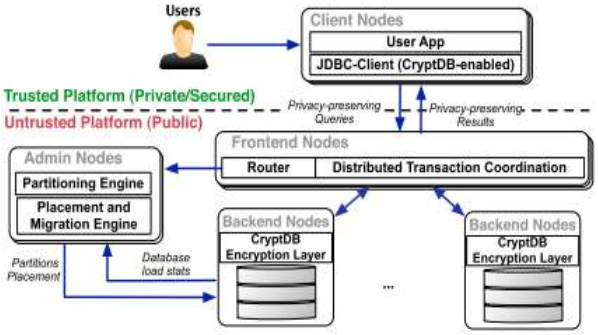

Figure 9. *CryotDB* as shown in [23]

D. *Two-stage verification and recognition framework for consolidating multiple fingerprint databases*

The use of multi-classifiers for solving pattern recognition problems has been reported extensively in literature. Frameworks that incorporates multi-classifiers and fusion have been used for multi biometric systems as reported by the authors in [24],[25],[26],[27],and [28]. These frameworks could be adapted towards consolidation of fingerprint databases. Fig.10 shows the framework in mind.

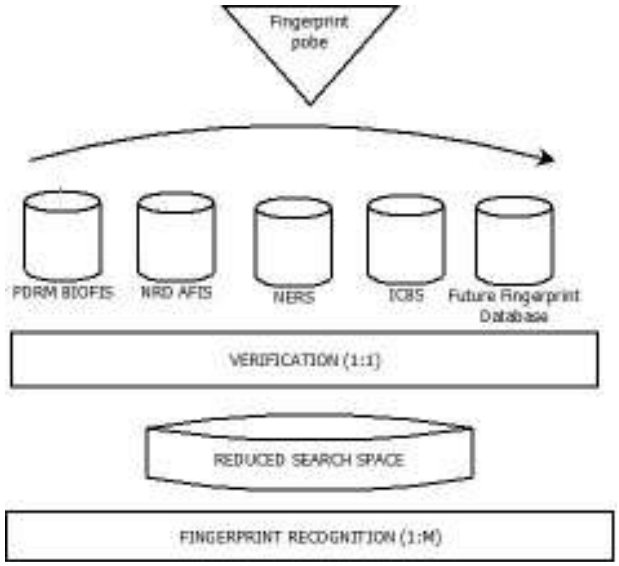

Figure 10. Two-stage verification and recognition framework for consolidating multiple fingerprint database

The main challenge of consolidating all the described fingerprint databases; especially if every possible combination of fingerprints are considered, would be the huge search space. A large search space will be take time to be processed, thus impacting the effectiveness of a consolidated fingerprint database in a real-time setting.

The search space can be reduced by subjecting every fingerprint probe to a 2 stage process. Stage 1 would involve a verification process whereby the fingerprint probe would be classified as either belonging to a particular fingerprint database or not. The result of verifying the fingerprint's database (class) membership can then be fused using fusion techniques such as score-based measures, expert voting, Borda ranking, etc. and so forth. Classifiers of a non-supervised nature would be preferable as the fingerprint databases keeps growing with time. Halici and Ongun used self-organizing maps (SOM) for this purpose in [29]. Stage 1 will result in a smaller search space for the probe.

Stage 2 will then see the probe undergoing a standard fingerprint recognition process. Recognition should be hastened due to the reduced search space.

VI. Experimental Results

A. *Fingerprint verification*

Experiments were conducted on fingerprint verification, on the viability of the two stage verification and recognition framework for consolidating multiple fingerprint databases shown in Fig.9, as reported first in the authors' work in [30].

A subset of the Biosecure database [31], as released under the The BioSecure Multimodal Biometric Feature Selection Challenge; was used for the fingerprint verification experiment. The dataset provided consisted of 300 feature files of minutiae features (ridge ending and bifurcation), their orientation and quality. 150 subjects contributed their fingerprints, with each subject contributing two sessions each; giving a total of 300 fingerprint feature files.

The fingerprint features were made up of 4 elements namely the X and Y coordinates of ridges and bifurcation, minutiae orientation angle and the quality of the minutiae.

These features were transformed into polar coordinates using the techniques described by Ravi et al. [32].

WEKA (Weikato Environment for Knowledge Analysis) [33] was used for classification, with the following set of results as shown in Table 4.

Table 4: Fingerprint verification experiment

CLASSIFIER	ACCURACY %	TRUE POSITIVE RATE	FALSE ACCEPT RATE	FALSE REJECT RATE
KNN(1NN)	91.47	0.909	0.078	0.091
NaiveBayesian	73.55	0.745	0.275	0.255
AdaBoostM1	76.0257	0.956	0.463	0.044
DecisionTable	100.0	1	0	0

B. *Face verification*

Another set of experiments were carried out for facial biometric verification, with the intention of investigating the usefulness of a fingerprint-facial biometric database.

A subset of the same Biosecure database was used for the facial verification experiment. This dataset consisted of 300 feature files, and each feature files contained 10 faces described by the first 164 eigenface coefficient. 150 subjects had their photos taken, in two sessions; resulting in a total of 300 facial feature files.

WEKA was also used to conduct the verification experiment, the result of which is shown in Table 5.

Table 5 : Face verification experiment

CLASSIFIER	ACCURACY %	TRUE POSITIVE RATE	FALSE ACCEPT RATE	FALSE REJECT RATE
KNN(1NN)	97.39	0.972	0.024	0.028
NaiveBayesian	59.49	0.654	0.466	0.364
AdaBoostM1	57.79	0.464	0.304	0.536
DecisionTable	59.26	0.560	0.374	0.440

Figure 10 shows the ROC (Receiver operating characteristic) curve for Face biometric classification using KNN(1NN).

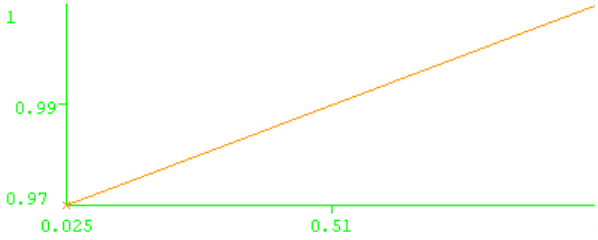

Figure 10. ROC for Face Biometric using KNN(1NN)

C. *Score level fusion for fingerprint and face biometrics*

A score level fusion experiment was then conducted for fusing fingerprint and face biometrics. Both the AND rule and the OR rule was used.

For the AND rule, fusing FAR(False Accept Rate) is given as follows:

$FAR_{1,2}=FAR_1*FAR_2$ while

FRR(False Reject Rate) is fused as follows:

$FRR_{1,2}=FRR_1+FRR_2-FRR_1*FRR_2$

For the OR rule, fusing FAR(False Accept Rate) is given as follows:

$FAR_{1,2}= FAR_1+FAR_2-FAR_1*FAR_2$ while

FRR is fused as follows:

$FRR_{1,2}= FRR_1*FRR_2$

Accuracy using the OR AND score fusion was calculated as follows:

P(A and B)= P (A).P(B)

while

P(A or B) = P(A)+P(B)-P(A and B)

At the same time, a simple weighted fusion strategy was also considered. The simple weighted fusion strategy can be described using the following formula:

Let S be the weighted fusion score while w is the weight attached to fp fingerprint score and f face score.

$$S=w_1fp_1+w_2f_2$$

The value of weights w_1 and w_2 adds up to 1, and several combination are tried in order to arrive at an optimal solution.

Table 6 shows the score level fusion for fingerprint and face biometrics using the AND, OR and simple weighted fusion strategy.

Table 6: Score level fusion for fingerprint and face

FUSION TECHNIQUE	ACCURACY %	FALSE ACCEPT RATE	FALSE REJECT RATE
AND	97.39	0	0.028
OR	100	0.024	0
Simple weighted	99.739	-	-

From the experiments done it can be concluded that the choice of fusion technique would be driven by the sensitivity of the verification process towards False Accept or False Rejects. In a secured and inclusive environment (for example at the polling stations, where the intention is to increase user participation while maintaining security), the OR fusion strategy would work well. In a secured and restrictive environment where impostors are not tolerated (for example a bank vault), the AND fusion strategy can be adopted with a cost in terms of reduced accuracy. The simple weighted score fusion strategy would appear to work in situations where one biometric modality significantly outperforms the other biometric modality.

The experiments conducted have further proven that:

1. It is very possible to classify fingerprints, with the intention of reducing the feature search space ; in line with the framework suggested in Fig. 9.
2. The viability of incorporating additional biometric modalities to fingerprint databases and still be able to utilize the aforementioned framework.

Future investigation in this work may be extended to palm based biometrics as reported in [34], as well as combination of fingerprint with more robust face recognition technology as shown in [35].

References

[1] V. Matyáš and Z. Říha. "Security of Biometric Authentication Systems," *IJCISIM*, vol. 3 (2011), pp. 174–184, 2011.

[2] J. Nousbeck, B. Burger, D. Fuchs-Telem, M. Pavlovsky, S. Fenig, O. Sarig, P. Itin, and E. Sprecher. "A Mutation in a Skin-Specific Isoform of SMARCAD1 Causes Autosomal-Dominant Adermatoglyphia," *The American Journal of Human Genetics*, vol. 89, no. 2, pp. 302–307, Aug. 2011.

[3] S. A. Cole. "History of Fingerprint Pattern Recognition," in *Automatic Fingerprint Recognition Systems*, N. Ratha and R. Bolle, Eds. New York: Springer-Verlag, 2004, pp. 1–25.

[4] "The History of Fingerprints." [Online]. Available: http://onin.com/fp/fphistory.html. [Accessed: 14-Aug-2011].

[5] M. Kawagoe and A. Tojo. "Fingerprint pattern classification," *Pattern Recognition*, vol. 17, no. 3, pp. 295–303, 1984.

[6] B. Moayer and K. S. Fu. "A syntactic approach to fingerprint pattern recognition ☆ ," *Pattern Recognition*, vol. 7, no. 1–2, pp. 1–23, Jun. 1975.

[7] "Biometric Publications," *To appear at the International Conf. on Biometrics (ICB) June 2009*, 15-Aug-2011. [Online]. Available: http://biometrics.cse.msu.edu/Publications/Fingerprint/ChenJainIndividuality_ICB09.pdf. [Accessed: 15-Aug-2011].

[8] K. Karu. "Fingerprint classification," *Pattern Recognition*, vol. 29, no. 3, pp. 389–404, Mar. 1996.

[9] N. K. Ratha, K. Karu, Shaoyun Chen, and A. K. Jain. "A real-time matching system for large fingerprint databases," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 18, no. 8, pp. 799–813, Aug. 1996.

[10] M. Ben Ayed, F. Bouchhima, and A. Mohamed. "Automated Fingerprint Recognition Using the DECOC Classifier," *IJCISIM*, vol. 4 (2012), pp. 546–553, 2012.

[11] "Understanding Biometrics | Griaule Biometrics." [Online]. Available: http://www.griaulebiometrics.com/en-us/book/understanding-biometrics. [Accessed: 15-Aug-2011].

[12] "FBI — IAFIS." [Online]. Available: http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis. [Accessed: 15-Aug-2011].

[13] "Biometrics Standards." [Online]. Available: http://www.itl.nist.gov/div893/biometrics/standards.html. [Accessed: 15-Aug-2011].

[14] "High tech fingerprint ID solution to fight crime | Malay Mail Online." [Online]. Available: http://www.mmail.com.my/content/31504-high-tech-fingerprint-id-solution-fight-crime. [Accessed: 15-Aug-2011].

[15] "Yasmin Technology Company Profile," *Yasmin Technology Company Profile*, 15-Aug-2011. [Online]. Available: http://www.yasmin.com.my/v2/company/profile.pdf. [Accessed: 15-Aug-2011].

[16] "Biometric registration of foreigners from June 1 | New Straits Times Newspaper | Find Articles at BNET." [Online]. Available: http://findarticles.com/p/news-articles/new-straits-times/mi_8016/is_20110318/biometric-registration-foreigners-june-1/ai_n57098795/. [Accessed: 15-Aug-2011].

[17] "Biometric registration when employers renew maid permit: Subramaniam." [Online]. Available: http://www.nst.com.my/nst/articles/Foreignmaidbiometricregistrationtobedonewhenemployersrenewtheirworkpermit_Subramaniam/Article/. [Accessed: 15-Aug-2011].

[18] "Biometric programme registers 390,404 foreign workers | BorneoPost Online | Borneo , Malaysia, Sarawak Daily News." [Online]. Available: http://www.theborneopost.com/2011/07/27/biometric-programme-registers-390404-foreign-workers/. [Accessed: 15-Aug-2011].

[19] "PATI | Program Penyelesaian Menyeluruh Pekerja/Pendatang Asing Tanpa Izin (PROGRAM 6P)." [Online]. Available: http://www.pati.com.my/. [Accessed: 07-Sep-2011].

[20] "Jumlah Statistik Pekerja Asing Sah Dan PATI Yang Telah Didaftarkan Menerusi Program 6P (sehingga 24 Ogos 2011)." [Online]. Available: http://www.imi.gov.my/index.php/en/component/content/article/1-berita-terkini/524-jumlah-statistik-pekerja-asing-sah-dan-pati-yang-telah-didaftarkan-menerusi-program-6p-sehingga-18-ogos-2011. [Accessed: 07-Sep-2011].

[21] Morgan, Daniel and Krouse, William. "Biometric Identifiers and Border Security: 9/11 Commission Recommendations and Related Issues." [Online]. Available: http://www.fas.org/sgp/crs/homesec/RS21916.pdf. [Accessed: 15-Aug-2011].

[22] "Face, fingerprints, iris details on unique ID." [Online]. Available: http://www.indianexpress.com/news/face-fingerprints-iris-details-on-unique-i/568033/. [Accessed: 26-Mar-2012].

[23] C. A. Curino, E. P. C. Jones, R. A. Popa, N. Malviya, E. Wu, S. R. Madden, H. Balakrishnan, and N. Zeldovich. "Relational Cloud: A Database-as-a-Service for the Cloud," in *5th Biennial Conference on Innovative Data Systems Research*, Asilomar, California.

[24] C. C. Ho, H. Ng, and C. Eswaran. "Survery of approaches and challenges in multimodal biometric authentication systems," in *The Proceedings of the 3rd International Conference on Artificial Intelligence in Engineering and Technology*, Sabah, 2006.

[25] C. C. Ho, H. Ng, and C. Eswaran. "A RESEARCH FRAMEWORK FOR A MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM.doc," in *The Proceedings of the 3rd International Conference on Artificial Intelligence in Engineering and Technology*, Sabah, 2006.

[26] C. C. Ho and C. Eswaran. "Do you see or hear first:The case for perception simultaneity as a quality measure for multimodal biometric fusion," in *Proceedings of the Annual International Conference on Information Technology Security (ITS 2010)*, Phuket, 2010.

[27] C. C. Ho and C. Eswaran. "Multimodal Biometric For Secured Role Based Access Control In E-Commerce System," in *The Proceedings of the 2009 International*

Conference on e-Commerce, e-Administration, e-Society, and e-Education., Singapore, 2009.

[28] H. C. Ching and C. Eswaran. "A Nature Based Fusion Scheme for Multimodal Biometric Person Identity Verification at a Distance," pp. 94–97, 2009.

[29] U. Halici and G. Ongun. "Fingerprint classification through self-organizing feature maps modified to treat uncertainties," *Proceedings of the IEEE*, vol. 84, pp. 1497–1512, Oct. 1996.

[30] C. C. Ho and C. Eswaran. "Consodilation of fingerprint databases: A Malaysian case study," pp. 455–462, 2011.

[31] J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez, J. Galbally, M. R. Freire, J. Gonzalez-Rodriguez, C. Garcia-Mateo, J.-L. Alba-Castro, E. Gonzalez-Agulla, E. Otero-Muras, S. Garcia-Salicetti, L. Allano, B. Ly-Van, B. Dorizzi, J. Kittler, T. Bourlai, N. Poh, F. Deravi, M. Ng, M. Fairhurst, J. Hennebert, A. Humm, M. Tistarelli, L. Brodo, J. Richiardi, A. Drygajlo, H. Ganster, F. M. Sukno, S.-K. Pavani, A. Frangi, L. Akarun, and A. Savran. "The Multiscenario Multienvironment BioSecure Multimodal Database (BMDB)," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 6, pp. 1097–1111, Jun. 2010.

[32] J. Ravi, R. K.B., and K. R. Venugopal. "FINGERPRINT RECOGNITION USING MINUTIA SCORE MATCHING," *IJEST*, vol. 1, no. 2, pp. 35–42, 2009.

[33] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten. "The WEKA data mining software," *ACM SIGKDD Explorations Newsletter*, vol. 11, no. 1, p. 10, Nov. 2009.

[34] K. Krishneswari and S. Arumugam, "A Review on Palm Print Verification System," *IJCISIM*, vol. 2 (2010), pp. 113–120, 2010.

[35] K. R.Singh, M. A.Zaveri, and M. M. Raghuwanshi, "Illumination and Pose Invariant Face Recognition: A Technical Review," *IJCISIM*, vol. 2 (2010), pp. 029–038, 2010.

Author Biographies

Chiung Ching Ho is a lecturer in the Faculty of Computing and Informatics Multimedia University, in Malaysia. He graduated from Universiti Putra Malaysia with a MSc Computer Science in the year 2001. Ho's research interests lies in the area of multimodal biometrics, classification and pattern recognition, and smart mobile computing.

C. Eswaran is a full professor in the Faculty of Computing and Informatics Multimedia University, in Malaysia. He graduated with B.Tech, M.Tech and Ph.D degrees in Electrical Engineering from the Indian Institute of Technology Madras, India He has also held fellowships and visiting positions in Germany, Canada and Singapore. He has held led numerous funded research projects and has supervised many Masters and PhD students. His current research interests lies in the areas of Multimedia Digital Signal Processing and Compression, Neural Networks, and Bio-medical Engineering,