

Universiti Utara Malaysia



Information Technology for Managers STIM5013

BIOMETRICS

Prepared for;

Associate Prof Azizi Bin Zakaria

By;

Yosman Hussien (804020)
Syafira Bt Sarapol (803574)
Harcharanjit Singh (800785)
Ahmad Humaizi Bin Mat Noor (804239)

Table of Contents

	CONTENTS	PAGE
1	What Is Biometrics?	1
2	History Of Biometric	1
3	Biometric Characteristics	2
4	How Does A Biometric System Work?	6
5	Why Use Biometrics?	7
6	Advantages Of Biometrics	8
7	The Disadvantages Of Biometric System	9
8	Current Issue Of Biometric System	12
9	Application Of Biometric In Malaysia	16
10	Key Issues And Challenges Of Biometrics In Malaysia	21
11	The Need Of Biometrics	22
12	Border Control	23
13	E-Passports	24
14	Banking	25
15	Standards	25
16	In The Boardroom	26
17	Looking Forward	27
18	Future Direction Of Biometrics	28
19	Security In Numbers	30
20	Future Outlook And Standardization And Hybrid Technology	32
21	Conclusion	34
	Reference	36

1 WHAT IS BIOMETRICS?

- 1.1 The term "biometrics" is derived from the Greek words bio (life) and metric (to measure).
- 1.2 Biometric system is a system for the automated recognition of individuals based on their behavioral and biological characteristics. Biometrics is the development of statistical and mathematical methods applicable to data analysis problems in the biological sciences.
- 1.3 Biometrics can be used to secure transactions at automatic teller machines, no longer requiring the presentation of an ATM card (a biometric is hard to steal).
- 1.4 It could also be used for transactions at point of sale. Other markets include telephone banking and Internet Banking. Biometrics can be used in any network where the utmost security is needed. It doesn't just provide security because the physiological traits between people are unique (PIN numbers should also be unique), but also because these traits cannot be interchanged between people.

2 HISTORY OF BIOMETRIC

- 2.1 During the period of World War II, biometric technology was expensive and infrequently use. Initially it was used manually prior to the development of the computerized technology, After World War II American military found a biometric voice recognition as to identify the fighter pilot's voice.

- 2.2 In 1960 the Federal Bureau of Investigation (USA) found fingerprint recognition method (Automate Fingerprint Identification System - AFIS) to identify and analyze the fingerprint sensor. After discovery of biometric sensors in 1999, the biometric device become cheaper and allows people to use i.e. fingerprint attendance as a key fingerprint.
- 2.3 Traditional methods to secure such applications include magnetic and smart cards, tokens as well as passwords and PINs. However, when it comes to identity assurance, biometric technologies have an unsurpassed advantage: they are intrinsically linked to the person.

3 BIOMETRIC CHARACTERISTICS

- 3.1 Biometric characteristics comprise elements of both biology and behavior to detect and distinguish biometric features for the purpose of automated recognition of individuals.
- 3.2 Biological and behavioural characteristics of an individual are those that can be detected and from which distinguishing repeatable biometric features can be extracted for the purpose of automated recognition of individuals. Such characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these.
- 3.3 Fingerprints, face geometry, iris patterns and hand geometry are examples of biological characteristics, while dynamic signature recognition (the way in which a signature is written rather than the resulting graphic) is

an example of a behavioural characteristic. In reality, most biometric characteristics comprise elements of both biology and behaviour.

3.4 Biometrics refers to methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In information technology, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

3.5 Basically, biometric characteristics can be divided in two main classes:

- Physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, hand and palm geometry, iris recognition, which has largely replaced retina, and odor/scent.
- Behavioral are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics for this class of biometrics.

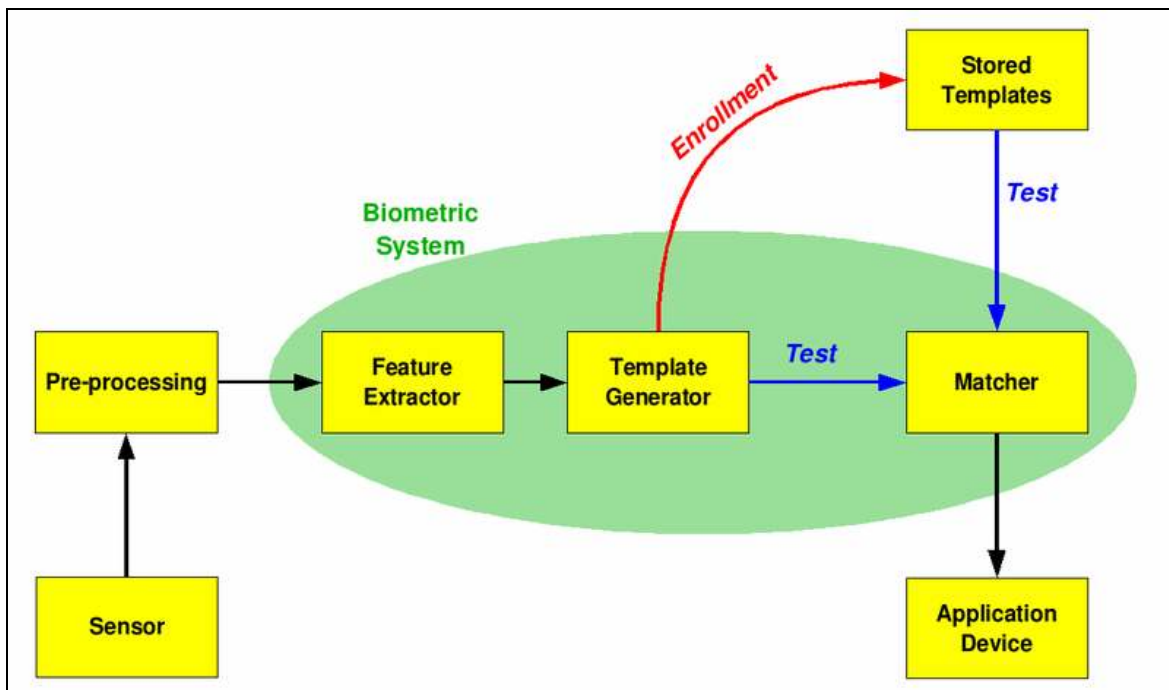
3.6 Strictly speaking, *voice* is also a physiological trait because every person has a different pitch, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioral.

3.7 It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters:

- Universality – each person should have the characteristic.

- Uniqueness – is how well the biometric separates individuals from another.
- Permanence – measures how well a biometric resists aging and other variance over time.
- Collectability – ease of acquisition for measurement.
- Performance – accuracy, speed, and robustness of technology used.
- Acceptability – degree of approval of a technology.
- Circumvention – ease of use of a substitute.

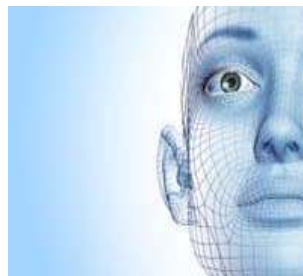
3.8 Simple diagram showing the main logical block of a biometric system



4 HOW DOES A BIOMETRIC SYSTEM WORK?

4.1 A biometric system can operate in the following two modes:

- Verification – A one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. Can be done in conjunction with a smart card, username or ID number.
- Identification – A one to many comparison of the captured biometric against a biometric database in attempt to identify an unknown individual. The identification only succeeds in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.



5 WHY USE BIOMETRICS?

5.1 One area where biometrics can provide substantial help is in guarding against attempts to establish fraudulent multiple identities or prevent identity fraud.

5.2 By searching through the stored references, individuals who appear to have previously enrolled using a different identity can be highlighted for further investigation. It is very difficult to perform this type of check without the use of biometrics.

5.3 Desirable factors include:

- Accurate discrimination between individuals
- Ease of use and speed of operation
- The ability to deal with present and future numbers of individuals
- Environmental robustness, secure and robust against potential attackers
- Capable of coping with as much individual variability as possible
- Social acceptability, i.e. people are happy to use it

6 ADVANTAGES OF BIOMETRICS

6.1 Each form of biometric authentication has its own strengths and weaknesses, some of the advantages are as follows:-

- a) Increase security - Provide a convenient and low-cost additional tier of security.
- b) Reduce fraud by employing hard-to-forge technologies and materials.
- c) Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. Prevent unauthorised use of lost, stolen or "borrowed" ID cards.
- d) Reduce password administration costs.
- e) Replace hard-to-remember passwords which may be shared or observed.
- f) Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access.
- g) Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!
- h) Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance.
- i) Unequivocally link an individual to a transaction or event.

7 THE DISADVANTAGES OF BIOMETRIC SYSTEM

(a) It can be easily manipulated

- 7.1 Biometric system can be easily manipulated by attacking the channel between the stored templates and the matcher: The stored templates are sent to the matcher through a communication channel. The data traveling through this channel could be intercepted and modified - There is a real danger if the biometric feature set is transmitted over the Internet.
- 7.2 Someone can present fake biometrics or a copy at the sensor, for instance a fake finger or a face mask. It is also possible to try and resubmitting previously stored digitized biometrics signals such as a copy of a fingerprint image or a voice recording.
- 7.3 For example, there was a case where a pensioner who had passed away but his pension was withdrawn by using his finger print. After thorough checking, it was found up that his son has asked him to put his finger print on the form before he passed away.

(b) It requires huge data

- 7.4 Almost all systems using biometrics require an initial enrolment stage and this enrolment stage will be supervised by an officer who has been trained in the utilization of biometric in a specific application.
- 7.5 Depending on the biometric system, a person may need to present biometric data several times in order to enroll. The distinctive features of biometric data are located, encoded, and stored as a reference template for future comparisons.

7.6 Biometric systems extract features, encode and store information in the template based on the system vendor's proprietary algorithms. Template size might vary, depending on the vendor and/or technology. Although templates can range from 9 to 20,000 bytes, most of the templates are smaller than 1,000 bytes.

(c) Reliability

7.7 Paradoxically, the greatest strength of biometrics is at the same time its greatest liability. It is the fact that an individual's biometric data does not change over time: the pattern in your iris, retina or palm vein remain the same throughout your life.

7.8 Unfortunately, this means that should a set of biometric data be compromised, it is compromised forever. The user only has a limited number of biometric features (one face, two hands, ten fingers, two eyes). For authentication systems based on physical tokens such as keys and badges, a compromised token can be easily canceled and the user can be assigned a new token.

7.9 Similarly, user IDs and passwords can be changed as often as required. But if the biometric data are compromised, the user may quickly run out of biometric features to be used for authentication.

(d) Privacy Issue

7.10 Biometric data contains information acquired from individuals, which can be used to identify them. This raises issues of privacy and data protection. If the biometric data is recorded in a central database, privacy concerns

may be higher than for systems where an individual's data is stored only on a card retained by the individual.

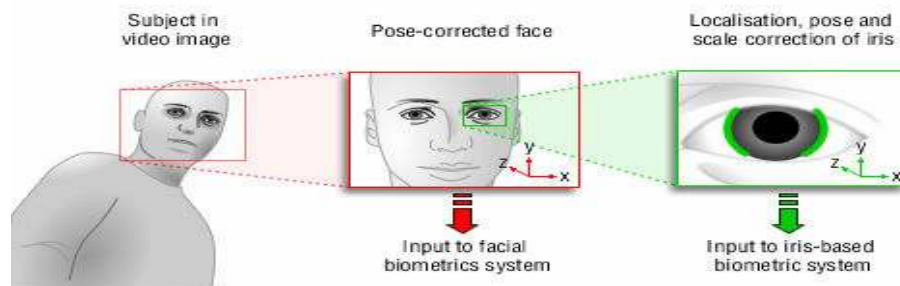
- 7.11 Note however, some biometric applications require a central database for their basic functionality e.g. to check for multiple enrolment attempts. Enrolees may be concerned that their biometric data could be used for other purposes than it was originally acquired; for example, face image data might be used for surveillance purposes and fingerprint data checked against forensic databases. These concerns are at the heart of many objections to the use of biometrics.

8 CURRENT ISSUE OF BIOMETRIC SYSTEM

(a) Reliability of Biometric System

- 8.1 Current security mechanism is based on either 'something you know', 'something that you have' or a combination of both. The most frequently used authentication technologies are passwords, PINs and tokens (e.g. keys and cards).
- 8.2 Single biometric technology/system may not always be able to meet market performance requirements. Currently, the development of systems that integrate two or more biometrics is emerging as a trend. These integrated systems are also able to meet the stringent performance requirements imposed by various applications.
- 8.3 Multimodal biometric systems can address the problem of non-universality, since multiple traits ensure sufficient population coverage.

Furthermore, multimodal biometric systems could provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. By asking the user to present a random subset of biometric traits (e.g., right index and right middle fingers in that order), the system ensures that a “live” user is indeed present at the point of data acquisition.



8.4 Multimodal biometrics could be two types of biometrics, such as combining facial with iris recognition. Multiple biometrics could also involve multiple instances of a single biometric, such as 1, 2, or 10 fingerprints, 2 hands, and 2 eyes. A commercially available system, BioID by Human Scan combines face, lip movement, and speaker recognition to control access to physical structures and small office computer networks. Depending on the applications, both systems can operate for either as verification or identification system.

i. Interoperability and difference standard of Biometric System

Leading corporations around the world have recognized that one of the deterrents to the adoption of biometric technologies was the lack of interoperability and standards between systems. Identifying, exchanging, and integrating information from different or unfamiliar

sources and functions are essential to an effective biometrics application. Without predefined standards, system developers may need to define in detail the precise steps for exchanging information; which is a complex, time-consuming and expensive process. Standards not only reduce the difference between the products but also decrease the risk of using automated biometrics.

ii. Denial to access due to incapable to verify identity

The effectiveness of a biometric system is characterized by two error statistics: False Rejection Rates (FRRs) and False Acceptance Rates (FARs). For each FRR, there is a corresponding FAR. A false reject occurs when a system rejects a valid identity; a false accept occurs when a system incorrectly accepts an identity. If biometric systems are perfect, both error rates would be zero. However, all biometric technologies suffer FRRs and FARs that vary according to the individual technology and its stage of development. As biometric access control systems are not capable of verifying identities with 100% accuracy, trade-offs must be considered during the final step of the risk management process when deciding on the appropriate level of security to establish.

8.5 These trade-offs have to balance acceptable risk levels with the disadvantages of user inconvenience. The tighter the security required, the lower the tolerable FAR.



The effectiveness of facial recognition technology is heavily influenced by environmental factors especially lighting factors

8.6 Vendors of biometric systems are currently claiming that false accepts occur once out of every 100,000 attempted entries and that the FRR is about 2% to 3%. However, due to the fact that system thresholds are adjusted to accommodate different FARs, it is often difficult to measure and compare their effectiveness. Vendors also describe the accuracy of their systems in terms of an equal error rate, or the point where the FAR equals with the FRR.

iii. Acquisition data Vs Enrolment verification

8.7 2% - 5% of finger prints cannot be captured due to build up dirt, dry or worn out as a result of aging, extensive manual labor or exposure to corrosive chemicals. Table 1.0 depicted sample of finger print acquisition, which are different between finger print data stored for verification purpose.

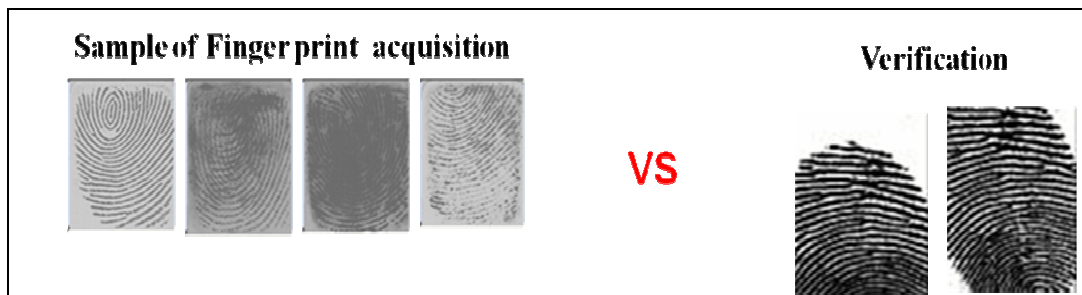


Table 1.0 – Sample of finger print acquisition Versus Verification

8.8 The fingerprints of those people working in Chemical industries are often affected. Therefore these companies should not use the finger print mode of authentication. It is found that with age, the voice of a person differs. Also when the person has flu or throat infection the voice changes or if there are too much noise in the environment this method may not authenticate correctly. Therefore this method of verification is not workable all the time. Even for those people affected with diabetes, the eye will get affected resulting in differences.

9 APPLICATION OF BIOMETRIC IN MALAYSIA

9.1 Biometrics industry has been tremendously growing in developed countries like US and Japan. There are many gadgets being introduced in those countries in order to facilitate the current lifestyle. In Malaysia, as we are moving towards a developed country by the year 2020, it is believed that biometrics could be a key driver of growth for Malaysia. As most of the companies are targeting globalization in its operation, biometrics markets will definitely boost its market in the global arena.

9.2 In pursuant to that, we believe that Malaysia can play a significant role to successfully contribute to the biometric industry and technology. From the perspective of significance of biometric technologies and global needs and national needs which are in alignment, Malaysia can contribute and even lead the biometric technologies as the government is supporting the

research and development done by the Malaysian in achieving this mission.

9.3 Biometrics is important in enhancing Malaysia's security, either physically or virtually, from any threats in the future. As our government always emphasize on security and privacy protection in financial, economical, political, it is undeniable that biometrics technology could contribute in achieving that. We could see and observe the importance and needs of biometric technologies in Malaysia being implemented in E-Commerce, Tele-health, E-Business, MyKad, Internet based business and other areas

9.4 In Malaysia, there are Five Industries utilizing the Biometric technologies i.e. Government Sector, Financial Sector, Health Sector, Travel Sector and Private Sector/ Consumer Market. From these five sectors, government sector represents the biggest end user of biometric technologies in Malaysia. Biometric technologies are implemented in government agencies such as state, federal and local government agencies and military sites.

9.5 Government sector

- Law and Military enforcement
- Criminal and civil investigations
- National ID and passport
- Border control
- Surveillance

- Voting
- Tax payment
- Physical access control

9.6 Financial sector

- Account management
- ATM
- E-commerce
- Physical access control
- Access to networks / Web applications
- Retail point of sale

9.7 Health sector

- Telemedicine
- Medical card
- Hospital services
- Physical access control
- Access to networks / Web applications
- Emergency procedures

9.8 Travel sector

- Passport
- Frequent travelers
- Baggage ID
- Surveillance
- Physical access control

- Access to networks / Web applications

9.9 Private sector and Consumer markets

- Call centers
- Surveillance
- Physical access control
- Access to networks / Web applications
- Keyless car
- Privileged services

Jabatan Pendaftaran Negara (JPN)

9.10 Our Government has introduced MyKad for identification and it is a standard credit-card-sized plastic token with an embedded microchip. It has been issued progressively since 2001, with the intention of being obligatorily used by the entire population of 18 years and over by the end of 2007. The card displays several items of data, carries several categories of data in the chip, including a biometric, is used by multiple government agencies, and has been designed for extensibility and 'function creep'.

9.11 The card bearing respectively a 32Kb and a 64Kb EEPROM (Electrically Erasable Programmable Read-Only Memory) chip, using the M-COS operating system. The larger version supports a digital signature key and digital signing. Malaysia is the first nation in the world to integrate the

biometrics technology in the smart card, namely MyKad. JPN is the largest user of biometrics in Malaysia. It is also claimed that Malaysia has the largest database of thumbprint.

Immigration Department

- 9.12 Malaysia is one of the first nation in the world to embed smart card containing biometric (thumbprint template) in the passport. We also have AutoGate system installed in KLIA, where Malaysian passengers could pass through the immigration checkpoint by scanning their thumbprint.

Jabatan Pengangkutan Jalan (JPJ)

- 9.13 The General Insurance Association of Malaysia reported that an average of 2.3 vehicles was stolen every hour in 2000. By 2004, car thefts had increased tenfold resulting in losses of more than RM750mil. In February 2006, JPJ has proposed to replace paper-based vehicle registration cards with biometric cards with the owners' thumbprint by the end of the 2006 (The Star, 28 Feb 2006).
- 9.14 This is to stop the increasing number of car thefts and forgeries. Once implemented, owners will get the chip-based biometric cards when they renew their road tax. The personal details will be linked to the National Registration Department to counter fraud cases. The biometric card would complement the e-registration and e-kiosk projects of JPJ. E-registration

involves the online registration of new vehicles by distributors, while e-kiosk allows the renewal of road taxes at selected locations.

Suruhanjaya Pilihanraya (SPR)

- 9.15 There was a proposal submitted to SPR to use biometrics in the last March 2008 election, but it could not be implemented due to high cost and time taken to develop the system. The implementation would also deny the rights of Malaysians who had yet to convert to MyKad system (The Star, 22 July 2007).

Polis Diraja Malaysia (PDRM)

- 9.16 PDRM has used fingerprint recognition more than 100 years. Further initiatives proposed by PDRM: (1) to scan each criminal's fingerprints and palmprint with the latest fingerprint and palm recognition technology, (2) to collect DNA sample collection of criminals and this is currently pending approval by the law and legislation. Government is also proposed to install more CCTVs at public areas, as a measure to fight crimes. Biometrics that suitable for surveillance such as facial and gait recognition could be integrated.

10 KEY ISSUES AND CHALLENGES OF BIOMETRICS IN MALAYSIA

- Lack of public awareness in biometric applications and advantages over existing conventional security systems.

- High costs as compared to traditional identification systems.
- Lack of interoperability and standardization between components provided by different products.
- Lack of coordination and collaboration among researchers.
- Lack of research funding to focus on research areas in Biometrics.

11 THE NEED OF BIOMETRICS

- 11.1 Imagine a world where interstate air travel is allowed automatically via a full body scan that not only verifies identity but simultaneously searches for insecure or illegal paraphernalia. Where access to the bank or credit accounts is granted only after identification via iris or retina scan. Where a shopping trip is made possible by a vehicle that operates only with biometric verification of ownership and payment is made via a fingerprint scan that links directly to ones credit account.
- 11.2 As such are growing concern for the future human identification moreover one of the highlights of the year was a US\$1 billion FBI contract won by Lockheed Martin, to develop and maintain its Next Generation Identification (NGI) multi-modal biometrics system for use by state, local and federal authorities in the US.
- 11.3 The system will expand the FBI's fingerprint capacity, doubling the size of its previous database. It will also include palm prints, iris and facial recognition capabilities, and be able to accommodate other biometric

forms that may mature and become important to law enforcement efforts in the future.

12 BORDER CONTROL

- 12.1 Biometrics at the border received a boost early in the year when the European Commission (EC) unveiled plans to strengthen Schengen zone border security, while facilitating travel for citizens, tourists and legal migrants.
- 12.2 The ideas include proposals for the introduction of a biometric based entry/exit system, the implementation of automated border crossing facilities for bona fide travelers, and the possible introduction of an electronic travel authorization system.
- 12.3 In the first half of the year, the UK Border Agency (UKBA) announced plans to trial automated border gates equipped with facial recognition technology where a comparison is made between the image in the ePassport chip and the live image. Manchester Airport was one of the locations that began trialing the technology, which can be used by adult biometric passport holders from the UK and European Economic Area using a system supplied and run in partnership by VisionBox and Fujitsu.
- 12.4 Across the Atlantic, US Customs and Border Protection (CBP) launched its Global Entry pilot aimed at expediting the screening and processing of low-risk frequent international trusted travelers entering the country. In just under five months, the Department of Homeland.

12.5 Security (DHS) had enrolled approximately 4000 in the scheme. The DHS says that during that time, more than 1700 Global Entry members used the kiosks at three pilot locations: JFK in New York, George Bush Intercontinental in Houston and Washington Dulles. The scheme has also been expanded to four additional airports: Los Angeles International, Atlanta Hartsfield-Jackson International, Chicago O'Hare International and Miami International. The UAE adopted advanced facial recognition to help protect critical infrastructure across the country. The system, provided by Crypto Metrics, was initially rolled out at Abu Dhabi International Airport, enabling critical ID checks to be performed from a distance without a person's active participation. This system will search against a number of data sources, from internal wanted persons lists to international databases such as Interpol's.

13.0 E-PASSPORTS

13.1 More countries took steps towards implementing ePassports, including India, which began a phased rollout during the year. Taiwan started issuing its ePassports at the end of December. Botswana became one of the first southern African countries to start issuing the documents, while South Africa awarded its ePassport tenders, confirming rollout would begin in 2009.

13.2 The UAE launched a tender process for its new ePassports. In the EU – already a couple of years into ePassport rollout – some countries started

introducing the second generation of documents ahead of June 2009's deadline for the incorporation of fingerprint data. The second generation framework is underpinned by Extended Access Control (EAC), a complex mechanism that involves establishing chains of trust between ePassports, the reader infrastructure and the issuing nations.

- 13.3 In December, Entrust confirmed it had won the contract to supply the CA software for Finland's migration to second generation ePassports. Gemalto was selected to personalise the new French ePassports.

14 BANKING

- 14.1 Although there was a lot of big-name action in the government sector, a number of private enterprises also took steps to implement the technology. For example, one of China's largest banks, China Merchants Bank (CMB), deployed PerSay's Free Speech voice biometrics system to make phone-based transactions more secure.

15 STANDARDS

- 15.1 Work progressed in the world of standards. Among numerous developments, ISO 19092:2008, financial services – Biometrics – Security framework, was announced, establishing the security requirements for the implementation and management of biometric identification technology within the financial industry. "Over the next five years the effort to create standards for biometric technologies will be rewarded with a significant

growth in biometric system adoption,” says Jonathan Collins, principal analyst, ABI Research.

- 15.2 Meanwhile, according to Detlef Houdeau of Infineon Technologies: “One of the problems holding back the deployment of biometrics in the private sector was the lack of standards for biometric verification in physical access control.”

16 IN THE BOARDROOM

- 16.1 Mergers and acquisitions continued. One of the biggest sagas of the year was the series of bids and counter bids for Digimarc by two of the world’s most powerful biometrics companies. Eventually, Digimarc rejected an unsolicited offer from Safran in favour of its original suitor, L-1 Identity Solutions.
- 16.2 Earlier in the year, L-1 added 3D face recognition to its portfolio following the acquisition of Bioscrypt, a provider of enterprise access control solutions based on fingerprint and 3D facial recognition. Although Safran failed in its bid for Digimarc, it did manage to acquire the Netherlands-based passport and secure ID document maker Sdu-Identification.
- 16.3 Elsewhere, Hitachi took a majority ownership interest in M-Tech Information Technology; bioMETRX acquired a controlling interest in engineering firm Biometric Solutions, and Logica Holdings bought Dolphin Digital Media. And in Germany, Bundesdruckerei returned to public

ownership after shareholders agreed the firm should be sold back to the German government.

17 LOOKING FORWARD

- 17.1 During 2009, government contracts look set to provide the lion's share of industry revenue. European countries will carry on the work they started in 2008 to achieve the June 2009 deadline for incorporating fingerprint data into second generation ePassports. "Border control based on ICAO standards in countries such as the US, Portugal and Thailand will be important," says Houdeau. "There will also be developments with registered traveller schemes in the US, Europe, Gulf Cooperation Council (GCC) countries and Asia Pacific.
- 17.2 There will also be further developments with national eID." Work will continue to move forward in the world of eID. For example, Israel is expected to start issuing its new eID documents before the end of 2009 following the signing of a contract between the Israeli Ministry of Interior and a consortium led by HP Israel.

18 FUTURE DIRECTION OF BIOMETRICS

- 18.1 Besides fingerprints, other physiological biometrics include face recognition, iris scan, retina scan, hand geometry, facial thermo gram, body odor, hand or finger veins, footprints and palm prints.
- 18.2 Of these, iris scanning is the most accurate -- with an average of approximately 250 distinctive characteristics in an iris, the odds of two people having the same pattern are 1 in 7 billion. And as it is relatively difficult to copy, it's also considered of one the most secure biometrics.
- 18.3 However given the complexity of the process, it's also the most costly, and its accuracy depends on the cooperation of the subject. (For example, criminals have been known to use eye drops to dilate their pupil, thus masking the majority of their iris).
- 18.4 Conversely, face recognition is technically the least intrusive, as faces can be scanned at a distance by surveillance cameras (although this also poses privacy issues), but its accuracy varies greatly according to light, exposure, etc.
- 18.5 Another biometric identification system currently under development by Hong Kong Polytechnic University's Biometrics Research Center is tongue scanning. "The tongue shapes of different people are different, and thus the tongue can be used to tell different subjects," says Lei Zhang, assistant professor at the university. "Our system uses laser scanning to construct the 3-D shape of the tongue.

- 18.6 The tongue shape information can be collected in about two-three seconds. Then after feature extraction and matching, the person's identity can be determined."
- 18.7 Other biometric identification systems, which require capturing the subject in action and similarly comparing it to a database of samples, are behavioral. These include voice print (the way a person talks), signature or handwriting dynamics (the way a person writes), keystroke dynamics (the way a person types, most often used as an extra layer of security over a password) and gait (the way a person walks).
- 18.8 Recent progress on most face recognition, voice recognition or speech recognition algorithms has been made and proved in laboratories," says Professor Hanseok Ko, director of the Intelligent Signal Processing Laboratory at Seoul's Korea University, "but the deployment of such products has been limited to criminal investigations, as opposed to individual personal identification. Commercial products are still primarily limited to fingerprint ID technologies applied to door locks and PC/laptops."
- 18.9 Taking it further one step at a time, electronics manufacturer Fujitsu is selling peripherals such as the PalmSecure PC Login Kit with functional mouse, which authenticates users' identity by analyzing the veins under their palm.
- 18.10 Meanwhile, Motorola, an active developer of Automatic Fingerprint Identification Systems (AFIS) for over 30 years, is now marketing its own

Mobile AFIS device, which captures both fingerprints and facial images, connects to wireless networks to upload data, runs on Windows Mobile, integrates bar code scanners, a smart card reader/writer, GPS, phone, and can be held in the palm of a hand.

19 SECURITY IN NUMBERS

- 19.1 So it is only natural that the protection of this highly personal data is taken very seriously. While biometrical identity theft is much more challenging than forging a credit card signature, illegally accessing and copying archived prints, which can then be used to produce artificial models, is still possible.
- 19.2 "In general, those systems where biometric data is readily obtained (stolen) are expected to be more vulnerable, since the availability of such data increases the number of ways in which a system may be attacked," says Moeller at the Biometrics Institute.
- 19.3 "We have tested face and fingerprint systems, which fall into this category. Speaker recognition, which we are testing at present, is also of this type. It is slightly more difficult to 'steal' biometric data from hand geometry, iris and DNA, and more difficult still for palm/finger vein and retinal scans, so we would expect decreasing vulnerability for this biometrics."
- 19.4 With the aim of applying research to real situations, the Biometrics Institute recently announced its proprietary Biometrics Vulnerability Assessment Service (BVAS). "The customer submits the system to us for

independent testing," explains Moeller. "The testing will be conducted in an independent laboratory where biometric devices can be sent to have their vulnerabilities investigated, assessed and reported. The laboratory will then collaborate with the contracting organization to work out how any vulnerability uncovered could be addressed through appropriate countermeasures."

- 19.5 One method of increasing security is to ensure that the data is transferred and stored with a strong encryption. Another technique is to use multimodal biometrics (using more than one biometric system simultaneously to confirm identification).
- 19.6 At the Biometrics Research Center, Zhang says they are working hard to make counterfeiting as difficult as possible: "We have already developed a 3-D palm-print system, which has a much higher anti-counterfeit capability than the 2-D palm-print system. We also have developed the near-infrared palm-print system, which can do liveness detection."
- 19.7 "Anti-hacking techniques are being introduced in the form of laboratory algorithms," adds Professor Ko at Korea University. "For example, impersonation by using fingerprint/palm molding in plastic form can be prevented by tying it to a heat sensor to confirm that an actual human specimen is being presented for verification."

(Source: cnn.com)

20 FUTURE OUTLOOK AND STANDARDIZATION AND HYBRID TECHNOLOGY

20.1 According to most experts, the future of biometrics is dependant upon two critical areas: standardization and the use of hybrid technologies.

Standardization

20.2 Currently, the biometrics industry is very fragmented, with more than 150 companies with their own proprietary systems and methodologies. Standards have only recently been established in order to provide direction for the development of a common interface that will allow for shared biometric templates.

20.3 The BioAPI created by the BioAPI group of more than 60 vendors and government agencies, defines a common structure for interfacing with biometrics. Yet, competitive forces remain as technology giants like Microsoft have abandoned the consortium and the BioAPI created by the BioAPI a group of more than 60 vendors and government agencies, defines a common structure for interfacing with biometrics.

20.4 Yet, competitive forces remain as technology giants like Microsoft have abandoned the consortium and the BioAPI standard to develop their own proprietary software standards. The development and acceptance of a primary standard is critical for the growth and applicability of the biometrics industry. Only after the technological standard is more established can systems integrate and interact efficiently.

Hybrid Technologies

20.5 One of the critical concerns with the use of biometric technologies is that of privacy and security of stored personal biometric data. To have personal data stored in a centralized database leaves the information potentially open to theft or compromise. The concept of combining smart card or public key infrastructures with biometric readers where the biometric template is stored on an individually controlled key has been suggested as a solution for the privacy concern and is considered by some critical to the advancement of biometric applications.

21 CONCLUSION

- 21.1 Biometrics is a powerful combination of science and technology that can be used to protect and secure our most valuable information and property. The future holds no limits for this industry as more applications are found. Further, the technology itself continues to improve in terms of application and accuracy.
- 21.2 In the future, we will live in a faster paced, more secure world where verification of one's identity is critical for daily activities. Technology is evolving at a very rapid speed. As technological advances in terms of biometrics advancement and security, there are other groups of people who are always trying to hinder its developments and exploit its weaknesses.
- 21.3 With the emergence of ambient intelligence technologies, policy-making increasingly will need to be more contextual. If they do not already appreciate the fact, policy-makers will need to recognize that privacy and trust are context dependent, that they do not mean the same thing to all people in all situations, nor do all people attach the same value to these concepts, however they define them.
- 21.4 Moreover, people's sense of privacy and trust again however one chooses to define them will continue to change over time. The biometrics industry has stood up to the challenges of the credit crunch throughout 2008. The question now is how well it will withstand the tough economic times predicted for 2009.

21.5 The measurement of government based projects aimed at beefing up security or complying with international obligations should continue to safeguard the interest of the nation. While some might argue that privacy and personal "freedom" are sacrificed with this level of control, but most people believe that it is the necessary price for a secure world environment.

References:

Biometrics – A Global Strategic Business Report, Global Industry Analysts Inc, May 2008.

European Biometrics Portal, Biometrics in Europe Trend Report, 2007.

Staire, R.M. & Reynolds, G.W. (2009). “Principles of Information Systems: A Managerial Approach”9th Edition, Course Technology, ITP.

Strategic ICT Roadmap for Malaysia. Ministry of Science, Technology and Innovation (MOSTI) Malaysia, 2007

The Star, ‘Biometric cards for vehicle owners’. 28 Feb 2006

The Star, ‘EC Unlikely to Go Biometric for Next Polls’, 22 July 2007

<http://bowojoey.wordpress.com/2007/10/01/biometric>

<http://edition.cnn.com/2008/TECH/12/12/digitalbiz.biometrics/index.html>

<http://en.wikipedia.org/wiki/Biometrics>

<http://ntrg.cs.tcd.ie/undergrad/4ba2.02/biometrics/index>