Technology Analysis & Strategic Management

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ctas20

Biometrics technology evaluating and selecting model building

Jen-Sheng Wang[a], Che-Hung Liu[b] & Joseph Z. Shyu[a]

[a] Institute of Technology Management, National Chiao Tung University, Hsinchu, Taiwan

[b] Department of Business & Management, National University of Tainan, Tainan, Taiwan

Published online: 25 Sep 2013.

To cite this article: Jen-Sheng Wang, Che-Hung Liu & Joseph Z. Shyu (2013) Biometrics technology evaluating and selecting model building, Technology Analysis & Strategic Management, 25:9, 1067-1083, DOI: 10.1080/09537325.2013.832747

To link to this article: http://dx.doi.org/10.1080/09537325.2013.832747

Technology Analysis & Strategic Management, 2013
Vol. 25, No. 9, 1067–1083, http://dx.doi.org/10.1080/09537325.2013.832747

Biometrics technology evaluating and selecting model building

Jen-Sheng Wang[a], Che-Hung Liu[b]* and Joseph Z. Shyu[a]

[a]*Institute of Technology Management, National Chiao Tung University, Hsinchu, Taiwan;* [b]*Department of Business & Management, National University of Tainan, Tainan, Taiwan*

Biometrics has been vigorously promoted around the world as a means to strengthen security and privacy in the IT world. Biometrics has been applied in specific areas for decades and proliferated in customer and resident electronic products to enhance security and privacy. This study evaluated biometrics through conventional technology assessment considerations combined with viewpoints from the particularity of biometric technologies and provides suggestions for selection. In order to achieve biometric technology assessment, we examined how different evaluating objects, technology assessment, biometric competence and key elements of biometric, lead to corresponding biometric technologies. The relative importance of each object was evaluated using the analytic hierarchy process. The weight of each object was adjusted separately to construct evaluating scenarios by sensitivity analysis. The results show that fingerprint recognition, iris recognition and palm print recognition are three biometric technologies that could meet the three objects requirements at the same time.

Keywords: biometric technology assessment; analytic hierarchy process; sensitivity analysis

1. Introduction

The security of privacy and confidentiality has become a major concern for people all over the information world in daily life. In general, the primary goal of biometrics is to provide more security through features of unique human bodies (Adeoye 2010). Biometric recognition systems should provide a reliable personal recognition scheme to either confirm or determine the identity of an individual (Jain, Nandakumar, and Nagar 2008). Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, and health and social services (Bhattacharyya, Ranjan et al. 2009). However, each technology has its specialty and expertise in verification (Jain and Ross 2004). Despite the number of evaluations of biometric technologies, the opinions are widely divided and the analysed viewpoints come mostly from technology aspects that give little thought to management or market sides (Riley and Kleist 2005).

Notwithstanding, several management studies have tried to examine generic assessed technology models to evaluate specific technologies (Ho and Chen 2009; Shen et al. 2010). This research

*Corresponding author. Email: chehung@gmail.com

assessed various biometric technologies – those ranked top six by the International Biometric Group (IBG) (International Biometric Group, 2009) – in order to meet two major viewpoints of assessment, including technology and management objects. In this way, this study investigated the purposes of technology assessment in biometrics.

There are many sophisticated analytical methods that look for optimal solutions to the multi-goal problem, which are also applied in technology assessment research (Tran and Daim 2008). The analytic hierarchy process (AHP) (Saaty 1980) is one of the most widely used techniques for assessing each alternative against a set of identified criteria. In this study, AHP was adopted to construct a biometrics assessment model in order to identify and weigh the criteria that are critical in the assessment of biometric technologies.

Moreover, AHP provides quantitative output that can be used with sensitivity analysis to explore how changes in criteria or weights affect strategic scenarios (Winebrake and Creswick 2003). Sensitivity analysis can improve the credibility of AHP by providing appropriate answers to 'what if' questions and is particularly valuable for multi-object decision-making problems (Erkut and Tarimcilar 1991). By performing sensitivity analysis, the value of AHP can be extended by including scenario building and analysis into the AHP process. Analysts can build scenarios to depict possible circumstances that affect the criteria weights or attributes for each alternative (Winebrake and Creswick 2003). In this study, sensitivity analysis was employed to change the weights of each object in order to draw possible biometric technology assessment scenarios. Using these technology assessment scenarios as a guideline, researchers can apply AHP to examine the impact of each biometric assessment object on the determination of biometric technology.

The next section briefly introduces six biometric technologies. In Section 3, a multi-object framework is constructed for assessing the biometric technologies according to technology assessment theories and related literature. Section 4 describes the AHP method and sensitivity analysis applied in this study. The empirical analysis conducted by AHP and sensitivity analysis is presented in Section 5. Finally, Section 6 presents the conclusions and management implications based on the results of Section 5.

2. Literature review

We will refer to the definitions of biometrics and introduce the top six biometric technologies ranked in the IBG 2009 market report, which are also the most often discussed in assessment of the technology.

2.1. *Biometrics definition*

For the purpose of this paper, the definition of biometrics offered by the US Department of Defense's Biometrics Identity Management Agency is more than sufficient to convey the two common meanings of the term:

> A general term used alternatively to describe a characteristic or a process. As a characteristic: The measure of a biological (anatomical and physiological) and/or behavioral biometric characteristic that can be used for automated recognition. As a process: Automated methods of recognizing an individual based on the measure of biological (anatomical and physiological) and/or behavioral biometric characteristics. (Biometrics Identity Management Agency 2010; Jain, Ross and Prabhakar 2004)

Biometric systems are generally composed of a series of components (Heyer 2008):

- A data collection component that collects the biometric data.
- A data storage component that stores the biometric data.
- A signal processing component that processes the biometric data.
- A decision component that makes decisions regarding matches between biometric data and whether to accept or reject.
- A transmission component that aids the data collection, data storage and signal processing components in compressing and expanding files required at different stages of the process.

A practical biometric system should meet the specified recognition accuracy, speed and resource requirements, be harmless to the users, be accepted by the intended population and be sufficiently robust to various fraudulent methods and attacks to the system (Jain, Ross, and Prabhakar 2004; National Biometric Security Project 2008).

2.2. *Biometrics introduction*

2.2.1. *Face recognition*

Facial recognition is a well-known biometric and is the most natural means of biometric identification (Dabbah, Woo, and Dlay 2007). It can serve for stand-off or covert biometric systems and be combined with other biometrics for increased confidence in results (National Science and Technology Council 2006). Human performance, however, declines with fatigue and repetition (Biometrics Identity Management Agency 2010), and owing to changes in facial appearance over time, this biometric generally requires some periodic re-enrolment (Goudelis, Tefas, and Pitas 2008). It is the least intrusive of biometrics, but when combined with extensive surveillance camera systems it can raise issues of privacy (Hong, Yun, and Cho 2005). Facial recognition technologies have developed into two areas: facial metrics and eigenfaces, both of which are advantageous and integrative (Bhattacharyya, Ranjan et al. 2009; Dabbah, Woo, and Dlay 2007).

2.2.2. *Fingerprint recognition*

Fingerprint identification is the leading biometric in terms of market share and the oldest with a scientific record (Vielhauer 2006). Recognition accuracy can be increased by using prints from multiple fingers. It can be used easily in the field and for forensic purposes (Jain, Ross, and Pankanti 2006). Drawbacks generally include the need for contact with a sensor, degraded performance when in the presence of dirt or degraded fingerprints (by age, manual work, or injury) and the requirements for intensive computation when trying to match a sample to the templates in a large database. In the modern approach, live fingerprint readers are used and are based on optical, thermal, silicon, or ultrasonic principles to prevent counterfeiting (Ross, Dass and Jain 2005). Fingerprint matching techniques can be placed into two categories, minutiae based and correlation based. Minutiae-based techniques find the minutiae points first and then map their relation placement on the finger while correlation-based techniques compare the global patterns (Bhattacharyya, Ranjan et al. 2009).

2.2.3. *Iris recognition*

The iris recognition method uses the iris of the eye, which is the coloured area that surrounds the pupil. Iris patterns are unique and are obtained through video-based image acquisition systems

(Bhattacharyya, Ranjan et al. 2009), which rely on light to sense the unique features of a person's iris (Ross 2010). This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings (National Science and Technology Council 2006). Iris recognition requires cooperation, since enrolment and re-enrolment may be required over a lifetime. It has demonstrated low-error rates in tests and performance in fielded systems is improving (Goudelis, Tefas, and Pitas 2008). However, there are two influences that need to be computed. One is the overall darkness of the image influenced by the lighting condition and the other is the change in iris size as the size of the pupil changes (Ganorkar and Ghatol 2007).

2.2.4. *Speaker recognition*

Speaker recognition relies on the temporal and spectral characteristics of an individual's voice for identification (National Science and Technology Council 2006). Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy and learned behavioural patterns (Bhattacharyya, Ranjan et al. 2009). Low to medium error rates are obtained and are dependent on the quality of the communication link and ambient noise, and can be affected by the speaker's condition (Vielhauer 2006). Its strength is that it is currently the only biometrics applicable to voice communication systems. The technology needs additional hardware to allow for recognition over long distances via ordinary telephones (wire line or wishes) (Jain and Ross 2004).

2.2.5. *Vascular pattern recognition*

Vascular pattern recognition relies on the unique pattern of blood vessels of an individual, generally using the back of the hand (National Science and Technology Council 2006). Using near-infrared light, reflected or transmitted images of the blood vessels of a hand or finger are derived and used for personal recognition (Adeoye 2010). Different vendors use different parts of the hand, e.g. palms or fingers, but rely on a similar methodology. Researchers have determined that the vascular pattern of the human body is unique to a specific individual and does not change as people age (Bhattacharyya, Das et al. 2009). It also has many and varied uses. For example, this biometrics is quite popular in Japan for banking and ATM access (Goudelis, Tefas, and Pitas 2008).

2.2.6. *Palm print recognition*

The inner surface of the palm normally contains three flexion creases, secondary creases and ridges. The flexion creases are also called principal lines and the secondary creases are called wrinkles. Even identical twins have different palm prints (Kong, Zhang, and Kamel 2009), which makes it ideal for identification. Palm print recognition inherently implements many of the same matching characteristics that have allowed fingerprint recognition to be one of the most well-known and best publicised biometric. Because fingerprints and palms have both uniqueness and permanence, they have been used for over a century as a trusted form of identification. However, palm recognition has been slower in becoming automated owing to some restraints in computing capabilities and live-scan technologies (National Science and Technology Council 2006). With this, a large number of templates can be easily stored in a standalone device. The weaknesses of this biometric are lack of accuracy, size of the scanner, fairly expensive price compared with fingerprint systems and the fact that injuries to palms can prevent the system from working properly (Adeoye 2010). It has gained a niche market in the areas of access control and time/attendance monitoring. This may be due to the size of the sensor, making it more practical for fixed applications, and the

fact this biometric may not be very distinctive when applied to large populations (Hong, Yun, and Cho 2005).

3. The assessment framework

The technology assessment involves different perspectives of diverse stakeholders, including practitioners, decision makers, researchers and R&D personnel in private and public sectors (Tran and Daim 2008). In general, the concerns of technology assessment include technological, economic, technology development and risk aspects (Shen et al. 2010). Hence, the perspectives of these technology assessment methodologies should be taken into consideration as well.

This study constructs a tailor-made technology assessment framework for biometrics (Figure 1) with relative literature. Moreover, this research processed in-depth interviews with experts and enterprises within the biometrics field to ensure the validity of the proposed framework. The contents of the objects in the analysis model and corresponding criteria are illustrated as follows.

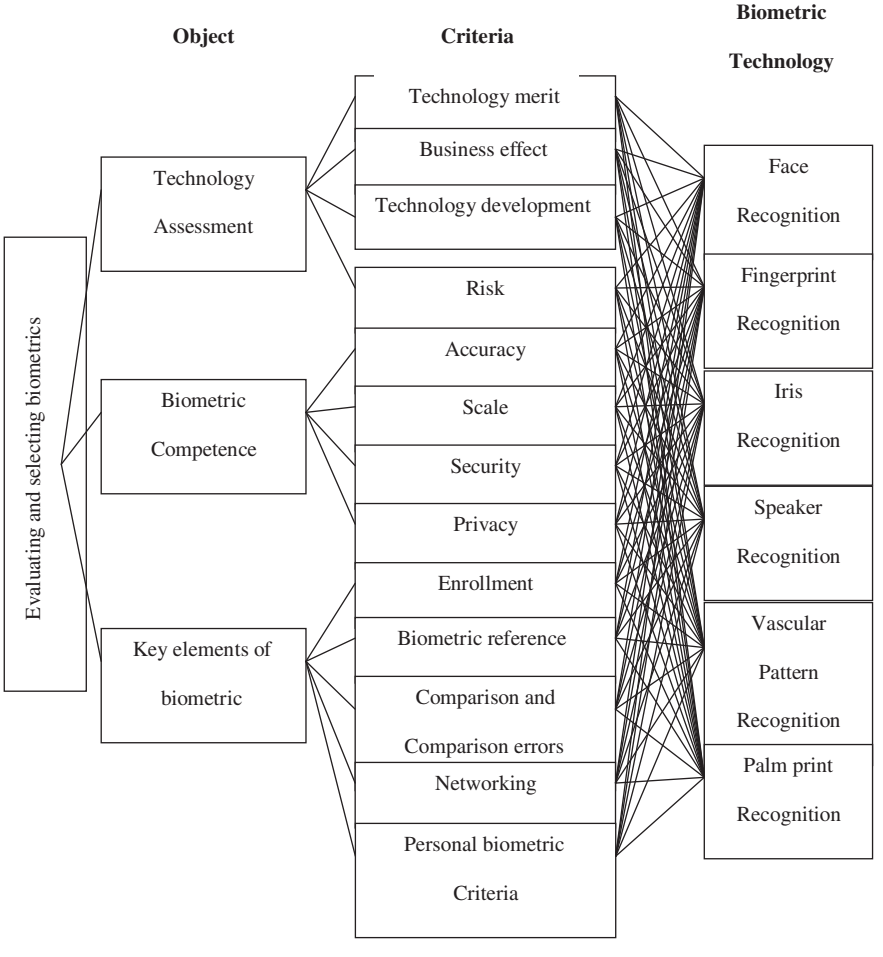

Figure 1. The evaluating and selecting model for biometrics.

3.1. *Technology assessment*

The considerations of technology assessment can be synthesised and categorised into several criteria, which should discriminate between positive prospects and negative problems existing in the technology development by interpreting related literature and secondary documents in order to deeply analyse the potential effects (Shen et al. 2010).

3.1.1. *Technological merit*

Research indicates that the technological aspect plays an important role in technology assessment (Hsu, Tzeng, and Shyu 2003). Technological merit can be viewed from the following aspects: (1) advancement of technology; (2) innovation of technology; (3) key of technology, (4) proprietary technology; (5) generics of technology; (6) technological connections; and (7) technological extendibility (Hsu, Tzeng and Shyu 2003; Shen et al. 2010).

3.1.2. *Business effect*

When evaluating technology, the effects that benefit corporations and economic/industrial developments are ones of considerable import. Hence, we should take business factors into account, including: (1) potential return on investment; (2) effect on existing market share; (3) new market potential; (4) potential size of the market; and (5) timing for technology (Ho, Liu, and Lee 2011; Hsu, Tzeng, and Shyu 2003; Huang et al. 2011; Shen et al. 2010).

3.1.3. *Technology development potential*

It is also necessary to consider the availability of related technological resources in technology assessment. The factors that affect the realisation of the technology development include: (1) technical resources availability; (2) equipment support; and (3) opportunity for technical success (Hsu, Tzeng, and Shyu 2003; Huang et al. 2011; Shen et al. 2010).

3.1.4. *Risk*

When assessing new technologies, decision makers are faced with the potential risks of the technology development. The criteria of the risk aspect include: (1) commercial risk; (2) technical risk; (3) technical difficulties; and (4) ethical risk (Hsu, Tzeng, and Shyu 2003; Kjølberg et al. 2008; Shen et al. 2010).

3.2. *Biometrics performance*

Jain, Ross and Prabhakar (2004) categorised the fundamental required performance in biometrics into four main categories: accuracy, scale, security and privacy.

3.2.1. *Accuracy*

The critical promise of ideal biometrics is that, when a biometric identifier sample is presented to the biometric system, it will offer the correct decision (Bolle et al. 2004). Even ignoring the requirements of complete automation and assuming the possibility of good biometric signal acquisition from a distance, it is easy to note that there is a need to bridge the gap between the current technology and performance requirements (Jain, Ross, and Prabhakar 2004).

3.2.2. *Scale*

In the case of verification systems, the size of the database does not really matter since it essentially involves a 1:1 match, comparing one set of submitted samples with one set of enrolment records (Bolle et al. 2004). There is a need to efficiently scale the system to control throughput and false-match error rates with an increase in the size of the database (Jain, Ross and Prabhakar2004).

3.2.3. *Security*

There are two very serious criticisms against biometric technology that have not been addressed satisfactorily: (1) biometrics are not secrets and (2) biometric patterns are not revocable (Kent and Millett 2003). The challenge is to design a secure biometric system that will accept only the legitimate presentation of the biometric identifiers without being fooled by the doctored or spoofed measurements injected into the system (Jain, Ross, and Prabhakar 2004).

3.2.4. *Privacy*

A reliable biometric system provides irrefutable proof of the identity of the person. Consequently, the users have multiple concerns, especially about privacy (Jain, Ross, and Prabhakar 2004). While one could stipulate some ingredients for a successful strategy, it requires many efforts to find satisfactory solutions for this fundamental privacy problem.

3.3. *Key elements of biometrics*

There are five common elements to all biometric systems: enrolment, biometric template, comparison and comparison errors, networking and personal biometric characteristics.

3.3.1. *Enrolment*

Proper enrolment instruction and training are essential to good biometric system performance (Heyer 2008). Enrolment is the first stage for biometric system set-up because it generates the template that will be used for all subsequent comparisons and user recognition (Biometrics Identity Management Agency 2010). During enrolment, a biometric system averages them or selects the best quality sample to produce an enrolment reference or template.

3.3.2. *Biometric template (or reference)*

The biometric system software will use a proprietary algorithm to extract features that are appropriate to that biometric as a template or reference. Templates are usually not actual images of the fingerprint, iris, hand, etc. (Heyer, 2008), but are generally only numerical representations of key data points (or minutia) read in a person's biometric feature.

3.3.3. *Comparison and comparison errors*

Comparison is the act of comparing one (or more) acquired biometric samples with one (or more) stored biometric templates for recognition (Biometrics Identity Management Agency 2010). No biometric decision is 100% perfect in either verification or identification mode. Therefore, biometric systems can be configured to create a threshold, which establishes the acceptable degree of similarity (Heyer 2008).

3.3.4. *Networking*

There are possible variations on a theme with regard to networks. Biometric systems/readers have integral networking functionality with a proprietary protocol (Heyer 2008). This may enable networking a number of readers together with little or no additional equipment involved, or a monitoring PC connected at one end of the network.

3.3.5. *Personal biometric characteristics*

Any human biological or behavioural characteristic can become a biometric identifier, provided the following properties are met (Jain, Ross, and Prabhakar 2004): (1) universality: almost every person should have the characteristic; (2) distinctiveness: no two people should have identical biometric characteristics; (3) permanence: the characteristics should not vary or change with time; and (4) collectability: obtaining and measuring the biometric feature(s) should be easy, non-intrusive, reliable and robust.

4. Research methods

The major purpose of this study was to explore the corresponding biometric technology alternatives under different technology assessment perspectives. This research primarily uses the AHP to determine the feasibility of biometrics to meet the evaluating objects and criteria. For assessment purposes, it is important that assessment succeeds not only in evaluating the priority of different objects, but also in estimating whether the alternatives meet the objects. Biometric technologies assessment should be better planned to allow the resources and efforts to be allocated to evaluate the importance of the objects. In such a context, the AHP proposed by Saaty (1980) appears to be an extremely useful mechanism that allows decision makers to express their qualitative and subjective judgments. Furthermore, the results derived by AHP can test the priority of alternatives under different presumed scenarios with sensitivity analysis. In this section, the AHP and the sensitivity analysis are illustrated.

4.1. *AHP*

The AHP method is a popular multi-object decision-making and planning tool that is analysis based on an additive weighting process, in which several relevant attributes are represented according to their relative importance (Erkut and Tarimcilar 1991). AHP has been extensively applied by academics and professionals in the field of technology assessment (Balestra et al. 2007; Vaidya and Kumar 2006). In the specific case of analysis of biometric technologies, the AHP allows the 'hierarchisation' of different evaluation objects and their affiliated criteria, making quantitative treatment that leads to a numerical estimate of the relative importance of each criterion and alternative possible.

Literature review, brainstorming and the Delphi method can be used to search for criteria when establishing a hierarchical structure. After that, the criteria are mutually compared for $n \times (n-1)/2$ times if there are n criteria. A nine-point scale recommended by Saaty (1980) was adopted to obtain experts' opinions, with preferences between options given as equally, moderately, strongly, very strongly, or extremely preferred (with pairwise weights of 1, 3, 5, 7 and 9, respectively), and values of 2, 4, 6 and 8, respectively, as the intermediate values for the preference scale. To estimate the relative weights of the criteria in this matrix, the priority of the criteria is compared by computing the eigenvalues and eigenvectors.

4.2. *Sensitivity analysis*

Sensitivity analysis generally involves the manipulation of model criteria in an attempt to determine the degree of influence the criterion has on the overall model output (Ho and Chen 2009). This type of analysis is useful in that it allows for an understanding of the different outcomes that could arise given a certain amount of variation in the model assumptions (Winebrake and Creswick 2003). In the AHP process, the results are dependent on the decision makers' subjective perceptions of the relative importance of those elements (Erkut and Tarimcilar 1991). By using sensitivity analysis, AHP can build assumed scenarios that provide more information for decision makers to determine how different circumstances affect their decision making without forcing them to change their original considerations. Many studies regarding related technology assessment issues have applied sensitivity analysis to consider the output effect that changes in criteria weight lead to (Ayağ 2007; Banuls and Salmeron 2007). This research employed sensitivity analysis to explore how a specific biometric technology assessment object affects the determination of corresponding biometric technology.

5. Empirical analysis

In this section, the constructed evaluating and selecting model was used to assess the top six biometric technologies that have emerged in the market (International Biometric Group 2009) to recommend the potential biometric technology under different considerations. The weights of each criterion were obtained using AHP and are presented below. Moreover, a potential biometric technology was evaluated by applying sensitivity analysis to achieve a set of assessment objects. The four assessment object scenarios built by sensitivity analysis include the general condition, the technology assessment dominate scenario, the biometric dominate scenario and the key elements of biometric dominate scenario. The results are described below.

5.1. *Analysis of AHP*

Before engaging in discussing this result, it is instructive to take a closer look at Table 1. To accomplish the research purpose, this study surveyed experts in the biometrics field, who are familiar with the status quo development of biometric technologies and the market conditions, to assess the top six major biometrics ranked in the Biometrics Market and Industry Report 2009–2014 (International Biometric Group 2009). The consistency of 17 expert questionnaires was verified using CI and CR, as suggested by Saaty (1980). As a result, 15 valid questionnaires with values of CI and CR smaller than 0.1 were used to obtain the final criteria weights of the assessment framework by adopting the AHP illustrated in the previous section.

As presented in Table 1, the technology assessment object (0.418) was the most emphasised object when evaluating biometric technologies, with the biometric competence (0.349) and the key elements of biometric (0.233) objects ranked second and third, respectively. Nevertheless, biometric competence and the key elements of biometric were over 0.5, but technology assessment was not. This indicates that when evaluating biometric technologies, evaluators should still take the particularities of target technology into account.

Within the technology assessment object, business effect (0.371) was identified as the most critical criteria to evaluate biometric technologies. According to the 2009 IBG report, the major expectation of biometrics development and popularisation is to enhance commercialisation which is also found out by some researches in new technology developing stage (Ho, Liu, and Lee 2011;

Table 1. Results of general condition.

Criteria	AHP weights	Final weights	Face recognition	Fingerprint recognition	Iris recognition	Speaker recognition	Vascular pattern recognition	Palm print recognition
Technology assessment	0.418		0.167	0.193	0.158	0.147	0.163	0.172
Technology Merit	0.183	0.076	0.171	0.165	0.224	0.077	0.177	0.185
Business Effect	0.371	0.155	0.176	0.230	0.117	0.177	0.144	0.156
Technology Development Potential	0.247	0.103	0.148	0.162	0.217	0.099	0.207	0.166
Risk	0.199	0.083	0.168	0.188	0.100	0.217	0.131	0.196
Biometric competence	0.349		0.159	0.177	0.187	0.156	0.159	0.162
Accuracy	0.236	0.083	0.143	0.171	0.218	0.139	0.166	0.163
Scale	0.161	0.056	0.192	0.182	0.119	0.191	0.150	0.166
Security	0.334	0.116	0.149	0.174	0.222	0.142	0.157	0.156
Privacy	0.269	0.094	0.166	0.184	0.159	0.166	0.160	0.166
Key elements of biometric	0.233		0.173	0.177	0.173	0.162	0.148	0.167
Enrollment	0.199	0.046	0.168	0.174	0.140	0.162	0.145	0.210
Biometric Reference	0.177	0.041	0.175	0.174	0.186	0.156	0.152	0.158
Comparison and Comparison Errors	0.258	0.060	0.182	0.177	0.188	0.159	0.159	0.135
Networking	0.174	0.040	0.176	0.179	0.135	0.192	0.142	0.176
Personal Biometric Criteria	0.192	0.045	0.161	0.182	0.209	0.144	0.139	0.165
Final scores			0.165	0.184	0.172	0.154	0.158	0.167
Rank			4	1	2	6	5	3

Huang et al. 2011). By complying with the first item of the report, business ranks first within the technology assessment to further accentuate the challenge of realising and promoting biometrics.

Security (0.334) was identified as the first priority factor within the biometric competence object. The need for reliable user authentication techniques has increased in the wake of heightened concerns about security; therefore, biometric technology is regarded as an effective tool for providing information security (Jain, Ross, and Prabhakar 2006). In some instances, biometrics can be used in conjunction with passwords (or tokens) to enhance the security offered by the authentication system. Thus, biometric systems can be used to enhance user convenience while also improving security. It is implied that security is helpful to facilitate the popularisation of new technologies (Kjølberg et al. 2008), so do the biometrics.

The comparison and comparison errors factor (0.393) was the dominant factor within the key elements of biometric object to evaluate biometric technology. It is necessary to evaluate the setting of the threshold in identification systems for better matching, since both failure to enrol and failure to acquire (during the comparison process) mean that the system is unable to 'extract' and distinguish the appropriate features of the user's biometric. Failure to enrol and/or failure to acquire indicate that this person's biometric characteristics may not be of sufficient quality to be used for recognition. Alternatively, a convenience-focused application, software, or mechanism could be adjusted to offer little or no denial of legitimate matches, while allowing some minimal acceptance of impostors. Hence, customers would be more likely to accept the biometric (Kjølberg et al. 2008).

5.2. *Scenario 1: General condition*

This scenario represents experts' perspectives regarding evaluating objects associated with the corresponding biometric technologies. The synthesised result in this scenario indicates how to achieve all three evaluating objects at the same time. After completing the biometrics evaluating and selecting model, the six biometric technologies were evaluated by our chosen experts to determine the most potential and recommendable biometric technologies. The performance of each biometric technology was compared pairwise by our experts. As presented in Table 1, fingerprint recognition (0.184) was the most suggested biometric technology among all six technologies, followed by iris recognition (0.172), palm print recognition (0.167), face recognition (0.165), vascular pattern recognition (0.158) and speaker recognition (0.154).

Furthermore, each cell in Table 1 identifies scores for each alternative by criterion. These scores represent the performance distribution of a specific criterion across the alternatives. Several important explanations can be made regarding the results of the general condition based on Table 1. Fingerprint recognition performed the best overall among the six biometric technologies owing to its potential of meeting the requirements of the technology assessment and key elements of biometric objects. Iris recognition and palm print recognition also performed well (Figure 2). In addition to meeting the requirement of technology assessment, fingerprint recognition, iris recognition and palm print recognition also work well in the other two objects originated from the characteristics of biometrics, which is why they scored high in the AHP. However, only the fingerprint recognition ranking was similar to the IBG report. The results suggest that iris recognition and palm print recognition may still have room to grow.

5.3. *Scenario 2: Technology assessment dominate scenario*

By adjusting the weights given to the three analytic objects, one can test the preference of alternatives corresponding to a specific condition. In this scenario, the technology assessment object

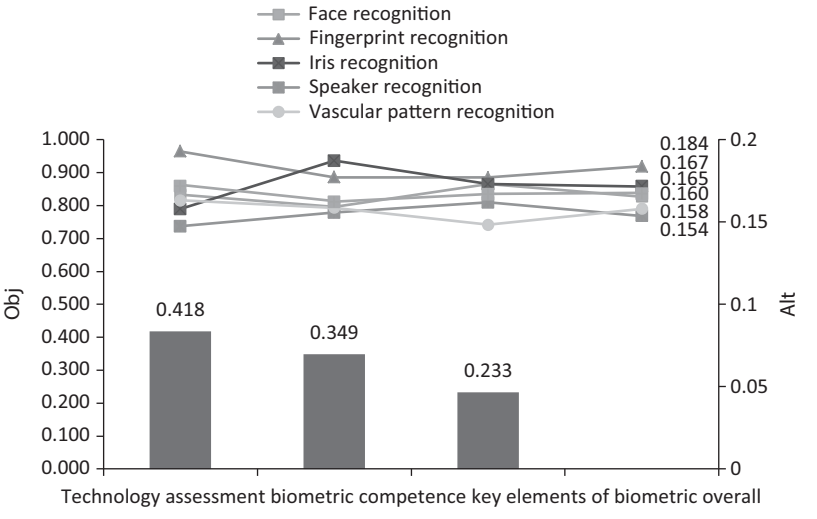

Figure 2. General condition.

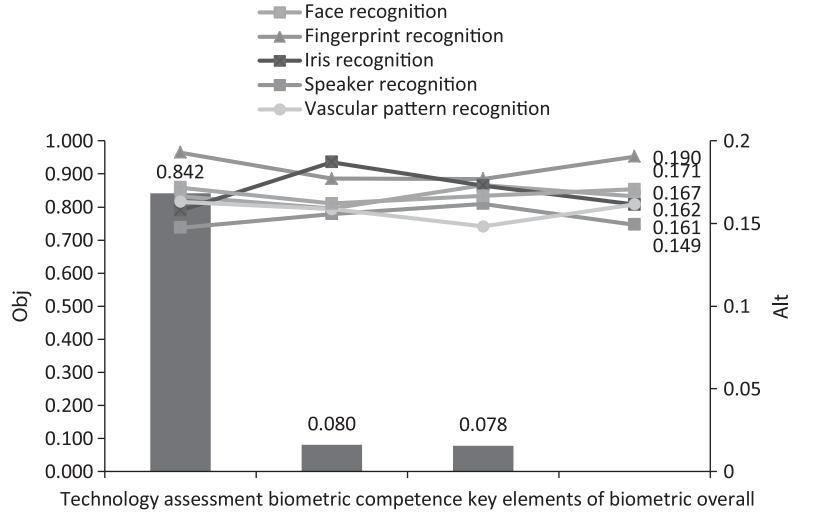

Figure 3. Technology evaluation dominate scenario.

is assumed to be dominant. As shown in Figure 3, the weight of technology assessment was increased to 0.842, while the weights of other two objects were decreased proportionately.

Figure 3 also shows that fingerprint recognition had the highest score (0.190), followed by palm print recognition (0.171), face recognition (0.167), vascular pattern recognition (0.162), iris recognition (0.161) and vascular recognition (0.149). We found that, although the top two remained the same, the priority of face recognition was ranked higher. In the present market, face recognition is the second most popular biometric technology (International Biometric Group 2009). Originally, face recognition had higher scores in the criteria technology merit, business

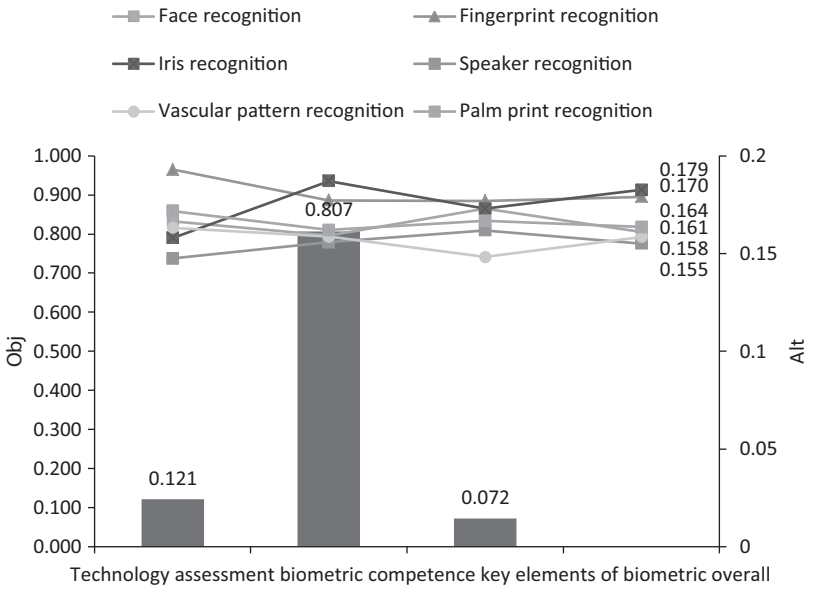

Figure 4. Biometric competence dominate scenario.

effect and risk, but was weaker on the other two criteria. Therefore, when the weight of technology increased, face recognition ranked higher. This leads to the obvious conclusion that biometric technologies evaluated under different scenarios will have different results. Under the technology assessment dominate scenario, fingerprint recognition was undoubtedly the most preferred biometric technology to fulfil the technology assessment object requirement. In the real world, fingerprint recognition is also the most preferred, accounting for 45.9% of the non-AFIS biometrics market in 2009, followed by face recognition at 18.5% and iris recognition at 8.3% (International Biometric Group 2009).

5.4. *Scenario 3: Biometric competence dominate scenario*

In the biometric competence dominate scenario, the weight of biometric competence was increased to 0.807 to be the dominant evaluating object. As presented in Figure 4, iris recognition (0.183) and fingerprint recognition (0.179) were more advantageous biometric technologies in this scenario. This result reveals the fact that when talking of the advantage of utilising biometric competence, iris recognition and fingerprint recognition would play well compared with the others owing to their high performance on 'accuracy' and 'security', as presented in Table 1. According to this result, the development of iris recognition may have a chance to catch up given its excellent biometric competence. Not surprisingly, iris recognition occupied the third rank in market revenue overall in 2009 (International Biometric Group 2009). As long as one biometric technology can facilitate its biometric competence, it creates the chance to enlarge market share and population.

5.5. *Scenario 4: Key elements of biometric scenario*

The relative importance of the key elements of biometric object was emphasised in this scenario as the dominant evaluating object (0.818). As shown in Figure 5, fingerprint recognition was the

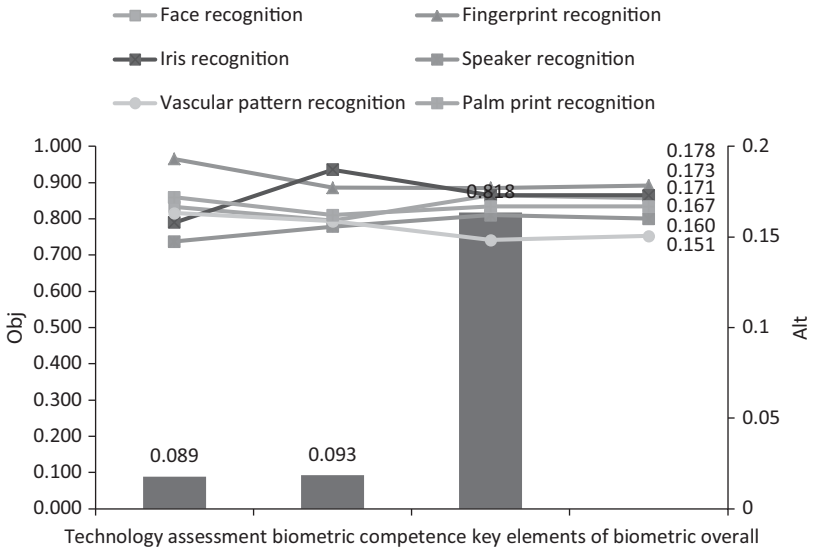

Figure 5. Key elements of biometric dominate scenario.

most preferred alternative with the highest score (0.178), followed by iris recognition (0.173), face recognition (0.171), palm print recognition (0.167), speaker recognition (0.160) and vascular pattern recognition (0.151). Since each biometric technology has its own supporting principles and mechanisms, it is difficult to tell which biometric technology is more outstanding in each criterion within this object. Hence the small difference in the scores. However, fingerprint recognition still ranked first and fully shows its leadership in biometric technology competition. As a result, fingerprint recognition is regarded as the most complete biometric technology, which has certain strengths in all key elements. In other words, the completeness of one biometric technology in the key elements of biometric object leads to its prosperity.

6. Concluding remarks

In recent years, biometrics has been vigorously promoted around the world as a means to strengthen the security and privacy in the IT world (Adeoye 2010), as well as in the facilitation of a new industry. Although biometrics has been applied in specific areas for decades, it has gradually proliferated in customer and resident electronic products to enhance security and privacy (Bhattacharyya, Ranjan et al. 2009). To meet various technology assessment aspects, every biometric technology should be carefully reviewed, since each has distinct features (Kim, Daim, and Anderson 2010). This study aimed to clarify how different evaluating objects determine the corresponding biometric technologies. In this research, AHP was used to evaluate the relative importance of each evaluating object. Moreover, the results of the AHP were applied to gather the corresponding biometric technologies under four different evaluating object scenarios with sensitivity analysis. The four scenarios were derived by changing the weights of the three evaluating objects separately. The results of this study have management implications, which are discussed below.

(1) The results indicate that in the general scenario, fingerprint recognition scored the highest, followed by iris and palm print recognition. In the technology assessment dominate

scenario, fingerprint recognition performed the best. Fingerprint recognition was the most recommendable biometric technology in the key elements of biometric dominant scenario as well, closely followed by iris recognition. In the biometric competence dominant scenario, iris recognition was regarded as the best technology to exhibit biometric competence. Based on these scenarios, a biometric technology suggestive list, from best to worst, is comprised of fingerprint recognition, iris recognition, palm print recognition and face recognition.

(2) In all scenarios, fingerprint recognition performed well and has more market share (International Biometric Group 2009). This result indicates that most people consider fingerprint recognition to have the most advantages in the visible future. Given this, people should think more about the strategies and measures to increase the number of fingerprint recognition applications and increase penetration.

(3) Our results show that iris recognition had the second highest score behind fingerprint recognition in the technology assessment scenario. This is in agreement with other reports showing that iris recognition always comes in second in multi-biometric systems (Ganorkar and Ghatol, 2007). Since the 9/11 terrorism attack, iris recognition has become the major recognition technology because it is the most reliable form of biometrics. The future of the iris recognition system is better in fields that demand rapid identification of individuals in a dynamic environment (Ross 2010). However, some considerations should be taken into account, such as the low performance of 'business effect' (0.117) and 'risk' (0.100) within the technology assessment object, as shown in Table 1. As long as iris recognition has more working credits, these considerations might be decreased.

(4) Finally, management researchers focus on the criteria for assessing which foresight technology could be used to evaluate them. However, what they think might be different from biometric ones could actually be closer to commerce and market stands. The research not only builds a technology-evaluating model, but also provides strategic suggestions for biometric system developing. Biometric systems could take the pros and cons outlined in Table 1 into future development consideration to either strengthen and improve or even eliminate components of the system. For example, face recognition could improve its score on the 'accuracy' criterion based on 3D imaging and thermogram (Goudelis, Tefas and Pitas 2008).

Taking together, our results show that fingerprint recognition, iris recognition and palm print recognition can meet all three objects requirements at the same time. In addition, while fingerprint recognition is considered the best biometric to date, iris recognition is becoming a viable alternative.

Notes on contributors

Jen-Sheng Wang is a PhD candidate at the Institute of Management of Technology, National Chiao-Tung University. His recent research interests include policy and industry analysis, open innovation and high-tech services, technology assessment and national innovation system.

Che-Hung Liu is an assistant professor in National University of Tainan, Taiwan. His research interests include knowledge management, e-commerce, cloud computing and energy resource management.

Joseph Z. Shyu holds a position of professor in the Institute of Technology of Management in National Chiao-Tung University. His recent research interests include national innovation system, high-tech industry analysis, strategic planning, management of high-tech services and global marketing strategy.

References

Adeoye, S.O. 2010. A survey of emerging biometric technologies. *International Journal of Computer Applications* 9, no. 10: 1–5.

Ayağ, Z. 2007. A hybrid approach to machine-tool selection through AHP and simulation. *International Journal of Production Research* 45: 2029–50.

Balestra, G., M. Knaflitz, R. Massa, and M. Sicuro. 2007. AHP for the acquisition of biomedical instrumentation. Paper presented at the IEEE Engineering in Medicine and Biology Society (EMBS 2007), August 22–26 in Lyon, France.

Banuls, V.A., and J.L. Salmeron. 2007. A scenario-based assessment model – SBAM. *Technological Forecasting and Social Change* 74: 750–62.

Bhattacharyya, D., P. Das, T.H. Kim, and K.S. Bandyopadhyay. 2009. Vascular pattern analysis towards pervasive palm vein authentication. *Journal of Universal Computer Science* 15: 1081–89.

Bhattacharyya, D., R. Ranjan, A.F. Alisherov, and M.K. Choi. 2009. Biometric authentication: A review. *International Journal of u- and e- Service. Science and Technology* 2: 13–28.

Biometrics Identity Management Agency. 2010. Biometrics glossary, version 4.0. http://www.biometrics.dod.mil/Files/Documents/Standards/BioGlossary.pdf

Bolle, R.M., J.H. Connell, S. Pankanti, N.K. Ratha, and A.W. Senior. 2004. *Guide to biometrics*. New York: Springer.

Dabbah, M.A., W.L. Woo, and S.S. Dlay. 2007. Secure authentication for face recognition. Paper presented at the Proceedings of IEEE Symposium on Computational Intelligence in Image and Signal Processing (CIISP 2007), April 15, in Honolulu, Hawaii, USA.

Erkut, E., and M. Tarimcilar. 1991. On sensitivity analysis in the analytic hierarchy process. *IMA Journal of Mathematics Applied in Business & Industry* 3, no. 1: 61–83.

Ganorkar, R.S., and A.A. Ghatol. 2007. Iris recognition: An emerging biometric technology, ISPRA'07 Proceedings of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation, February 16–19, in Corfu Island, Greece.

Goudelis, G., A. Tefas, and I. Pitas. 2008. Emerging biometric modalities: A survey. *Journal on Multimodal User Interfaces* 2: 217–35.

Heyer, R. 2008. *Biometrics technology review 2008*: Edinburgh, South Australia: Defence, Science and Technology Organisation.

Ho, C.J., and J.S. Chen. 2009. Forecasting VoWLAN technology for the Taiwan mobile telecommunication industry. *Technology Analysis & Strategic Management* 21: 213–32.

Ho, C.J., H.Y. Liu, and C.S. Lee. 2011. Technology evaluation process and its influential strategic factors: Cases in Taiwan's semiconductor sector. *Technology Analysis & Strategic Management* 23: 931–46.

Hong, J.H., E.K. Yun, and S.B. Cho. 2005. A review of performance evaluation for biometrics systems. *Biometrics Systems. International Journal of Image & Graphics* 5: 501–36.

Hsu, Y.G., G.H. Tzeng, and J.Z. Shyu. 2003. Fuzzy multiple criteria selection of government-sponsored frontier technology R&D projects. *R&D Management* 33: 539–51.

Huang, L., Y. Guo, Z.C. Peng, and L.A. Porter. 2011. Characterising a technology development at the stage of early emerging applications: Nanomaterial-enhanced biosensors. *Technology Analysis & Strategic Management* 23: 527–44.

International Biometric Group. 2009. *Biometrics market and industry report 2009–2014*. New York: International Biometric Group.

Jain, A.K., K. Nandakumar, and A. Nagar. 2008. Biometric template security. *EURASIP Journal on Advances in Signal Processing* Article no. 579416. doi:10.1155/2008/579416.

Jain, A.K., and A. Ross. 2004. Multibiometric systems. *Communication of the ACM* 47: 34–40.

Jain, A.K., A. Ross, and S. Pankanti. 2006. Biometric: A tool for information security. *IEEE Transactions on Information Forensics and Security* 1: 125–44.

Jain, A.K., A. Ross, and S. Prabhakar. 2004. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology* 14, no. 1: 4–20.

Kent, S., and L. Millett. 2003. *Who goes there? Authentication technologies through the lens of privacy.* Washington, DC: National Academies Press.

Kim, J., T. Daim, and T. Anderson. 2010. A look into the future of wireless mobile communication technologies. *Technology Analysis & Strategic Management* 22: 925–43.

Kjølberg, K., G.C. Delgado-Ramos, F. Wickson, and R. Strand. 2008. Models of governance for converging technologies. *Technology Analysis & Strategic Management* 20: 83–97.

Kong, A., D. Zhang, and M. Kamel. 2009. A survey of palm print recognition. *Pattern Recognition* 42: 1408–18.

National Biometric Security Project. 2008. *Biometric technology application manual*. Vol. 1. http://www.nationalbiometric.org/BTAM/btamvol1update.pdf

National Science and Technology Council. 2006. Biometrics foundation documents. Available at www.biometrics.gov/documents/biofoundationdocs.pdf

Riley, R.A., and V.F. Kleist. 2005. The biometric technologies business case: A systematic approach. *Information Management & Computer Security* 13: 89–105.

Ross, A. 2010. Iris recognition: The path forward. *IEEE Computer* 43, no. 2: 30–35.

Ross, A., S. Dass, and A.K. Jain. 2005. A deformable model for fingerprint matching. *Journal of Pattern Recognition* 38: 95–103.

Saaty, T.L. 1980. *The analytic hierarchy process*. New York: McGraw-Hill.

Shen, Y.C., Chang, S.H., Lin, T.R.G., and H.C. Yu. 2010. Hybrid selection model for emerging technology. *Technological Forecasting and Social Change* 77: 151–66.

Tran, T.A., and T. Daim. 2008. A taxonomic review of methods and tools applied in technology assessment. *Technological Forecasting and Social Change* 75: 1396–405.

Vaidya, O.S., and S. Kumar. 2006. Analytic hierarchy process: An overview of applications. *European Journal of Operational Research* 169: 1–29.

Vielhauer, C. (2006). Biometric modalities. Different traits for authenticating subjects: biometric user authentication for IT security. *Advances in Information Security* 18, no. 1: 33–75.

Winebrake, J.J., and B.P. Creswick. 2003. The future of hydrogen fueling systems for transportation: An application of perspective-based scenario analysis using the analytic hierarchy process. *Technological Forecasting and Social Change* 70: 359–84.