SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2015; **8**:727–739
Published online 3 July 2014 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1020

RESEARCH ARTICLE

Evaluating and selecting the biometrics in network security

Che-Hung Liu[1]*, Jen-Sheng Wang[2], Chih-Chiang Peng[2] and Joseph Z. Shyu[2]

[1] Department of Business and Management, National University of Tainan, Tainan, Taiwan
[2] Institute of Technology Management, National Chiao Tung University, Hsinchu, Taiwan

ABSTRACT

Since Apple merged with AuthenTec, a leading fingerprint recognition company, in 2012, biometrics has widely been considered to strengthen security and privacy in the network security field. Although biometrics has been applied in specific areas for decades, it has gradually proliferated in customer and mobile electronic products to enhance security and privacy. This study aims to evaluate biometrics through conventional technology assessment considerations combined with viewpoints on the specifics of biometric technologies and then to provide suggestions for selection. To conduct the biometric technology assessment, the fuzzy analytic hierarchy process and non-fuzzy best performance approaches are used. Although the outcomes first indicate that technology assessment should be the key object in selecting biometric technologies, that object is followed by biometric competence and key elements of biometrics. The outcomes also indicate that features of the target technologies should be considered when evaluating them. Additionally, fingerprint recognition, iris recognition, and face recognition are the preferred biometrics in evaluation and selection. Copyright © 2014 John Wiley & Sons, Ltd.

KEYWORDS
biometrics; network security; fuzzy analytic hierarchy process; best non-fuzzy performance

***Correspondence**
Che-Hung Liu, Department of Business and Management, National University of Tainan, Tainan, Taiwan.
E-mail: chehung@mail.nutn.edu.tw

1. INTRODUCTION

Security and privacy have become major concerns in everyone's daily networking life. To face future challenges, many companies and institutions are devoting themselves to researching and developing biometric products, such as Apple's purchase of AuthenTec in 2012 and launch of the iPhone 5S with fingerprint authentication [1,2]. Generally, the main purpose of biometrics is to improve security through recognition of unique features of human bodies [3,4]. Biometrics should offer dependable and robust personal recognition for confirming or determining an individual identity [5]. Biometric applications are found across the network security field as part of such applications as secure electronic banking, computer systems security, mobile phones, secure access to buildings, credit cards, and social and health services [6,7].

However, a closer look reveals that the various areas that biometrics is anticipated to support all focus on its verification aspects [8]. In addition, despite the many evaluations of biometric technologies, opinions are widely divided, with analyses coming mostly from the technology side, lacking either management or marketing points of view [9]. In contrast, there are several technology management studies that have tried to address generic technology assessment models to evaluate certain technologies [10–12]. However, biometric technologies in network security are more distinctive and complicated. Hence, this research aimed to assess various biometric technologies applied in network security, a subject that ranked in the top six in the International Biometric Group's investigation [13]. To combine the two major assessment perspectives of technology specialization and management, this study built and tailored a specific evaluation and selection model to understand the purposes of biometric technologies applied in network security. On the basis of the research results, we provide suggestions for relevant persons to consider.

Usually, technology assessment studies apply many sophisticated analytical methods [10]. The analytic hierarchy process (AHP) built by Saaty is one of the most widely used [14]. It is worth noting that decision makers' judgments about the problems that they want to solve are often ambiguous and uncertain. Fuzzy AHP (FAHP), which is AHP integrated with fuzzy set theory, could measure the ambiguity and uncertainty that exist in the subjective opinions of decision makers. In the study, we adopted FAHP to form a biometrics evaluation model for identifying and weighing the criteria critical to the topic of this study.

The arrangement of this paper is as follows. Section 2 briefly introduces six biometric technologies. An evaluating framework is constructed in Section 3 based on technology assessment theories and the specific characteristics of biometric technologies. Section 4 introduces the applied FAHP method. The research analysis conducted using FAHP appears in Section 5. Section 6 draws conclusions from the research summary results in Section 5 and discusses management implications.

2. LITERATURE REVIEW

We introduce six top-ranked biometric technologies from the IBG 2009 market report [13]. The definitions most likely are not exhaustive but are representative of the target biometrics in terms of technological maturity, capability, and potential applicability.

2.1. Biometrics

On the basis of the goal of this study, 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 [15]: "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" [15,16]. Biometrics generally comprise a set of elements [17]:

- Biometric data-collecting components.
- Biometric data-storing components.
- Biometric data-processing components.
- Decision-making components regarding matches between biometric data and verification results.
- Transmission components for aiding the data collection, data storage, and signal-processing components to compress and expand necessary files in the different process stages.

Practical biometric systems should confirm the accuracy, speed, and resource requirements for the specified recognition. They must also be harmless to the users, be accepted by the intended population, and be sufficiently robust against various fraudulent methods and attacks to the systems [16,18].

2.2. Face recognition

Face recognition is well known to humans and is the most natural biometric identification [19]. Human performance, however, declines with fatigue and repetition (e.g., an operator verifying photo identification of passengers boarding an airplane) [15]. Face recognition can serve in standoff or covert biometric systems and can be combined with other biometrics to increase confidence in results [20]. With iris recognition, it is a strong contender for second place (in market share) among biometric systems. These biometrics can be the object of a variety of modalities, including 2D and 3D imaging, 2D/3D combination, thermograms, and various analytical methods for recognition [21]. Because of changes in facial appearance over time, this biometric generally requires periodic re-enrollment. It is the least intrusive of biometrics, but when combined with extensive surveillance camera systems, it can raise issues of privacy [22].

2.3. Fingerprint recognition

Fingerprint identification is the leading biometric in terms of market share and is the oldest with a scientific record [23]. It is characterized by relative ease of enrollment and low error rates [24]. Recognition accuracy can be increased by using prints from multiple fingers and can easily be used in the field for forensic purposes [20]. Drawbacks 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 requirements for intensive computation when trying to match a sample to templates in a large database. Modern approaches use live fingerprint readers based on ultrasonic, optical, silicon, or thermal principles [25,26].

2.4. Iris recognition

Automated iris recognition emerged in the 1990s. It samples the iris of the eye, which is the colored area surrounding the pupil. Iris patterns are unique and can be obtained with a video-based image acquisition system [7]. Iris recognition relies on light to sense the unique features of a person's iris [27]. These features could be a composition of specific traits comprehended as crypts, corona, freckles, filaments, furrows, pits, rings, and striations [20]. Iris recognition has demonstrated low error rates in tests, and performance in field systems is improving [21]. It requires cooperation for enrollment, and re-enrollment may be required over a lifetime. However, designers of an iris recognition system must take care to consider two influences: lighting conditions and the size of the iris change. Before computing the iris code, the system has to process a proper transformation [24,28].

2.5. Speaker recognition

This recognition identifies subjects using the temporal and spectral characteristic of an individual's voice [20]. It uses the acoustic characteristics of speech that differ from one individual to another. These acoustic patterns cover both learned behavioral patterns (e.g., speaking style, voice pitch) and anatomy (e.g., shape and size of the mouth and throat) [7,29]. Low to medium error rates are obtained, depending on the quality of the communication link and ambient noise, and can be affected by the speaker's condition (e.g., emotional state, health) [23]. The strength of speaker recognition is that it is, with qualified hardware, currently the only biometrics applicable to voice communication systems over long distances [16].

2.6. Vascular pattern recognition

Vascular pattern recognition, also generally known as vein pattern authentication, is an emerging biometric compared with existing systems. This biometric relies on the unique pattern of blood vessels of an individual, generally using the back of the hand [20]. Using near-infrared light, it detects the transmitted or reflected images of the blood vessels of a finger, palm, or hand for personal recognition. This requires proximity to, but no contact with, a sensor (in contrast to fingerprints) [4]. Different vendors employ different parts of the fingers, palms, or hands but use a similar methodology. Researchers have confirmed that the vascular pattern of the human body is unique to a certain person and does not change with age [30]. Vascular pattern recognition has been applied in various cases; it is quite popular in Japan for ATM and banking access [21].

2.7. Palm print recognition

The inner surface of the palm commonly has three flexion creases, secondary creases, and ridges. The flexion creases are also named principal lines, and the secondary creases are named wrinkles. Even identical twins have different palm prints [31]. Palm print recognition inherently employs many of the same matching traits that allowed fingerprint recognition to be one of the most famous and publicized biometrics. However, automation of palm recognition has lagged because of some constraints in live-scan technologies and computing capabilities [20]. The weaknesses of this biometric are lack of accuracy, size of the scanner, cost (the scanners are fairly expensive), and the fact that injuries to palms can hinder the system's function [4]. It has gained a niche market in the areas of access control and time/attendance monitoring, possibly because of the size of the sensor making it more practical for fixed applications [22].

3. THE EVALUATION FRAMEWORK

Technology assessment involves different perspectives of diverse stakeholders, including practitioners, decision makers, researchers, and R&D personnel in private and public sectors [10]. In general, concerns in technology assessment comprise technological, economic, technology development, and risk aspects [11]. 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) following related literature and includes in-depth discussions with enterprises and experts in the biometrics field to ensure the validity of the proposed framework. The content of the objects in the analysis model and corresponding criteria are illustrated as follows.

3.1. Technology assessment

The considerations of technology assessment can be synthesized and distinguished into several criteria, which should be grouped into positive prospects and negative

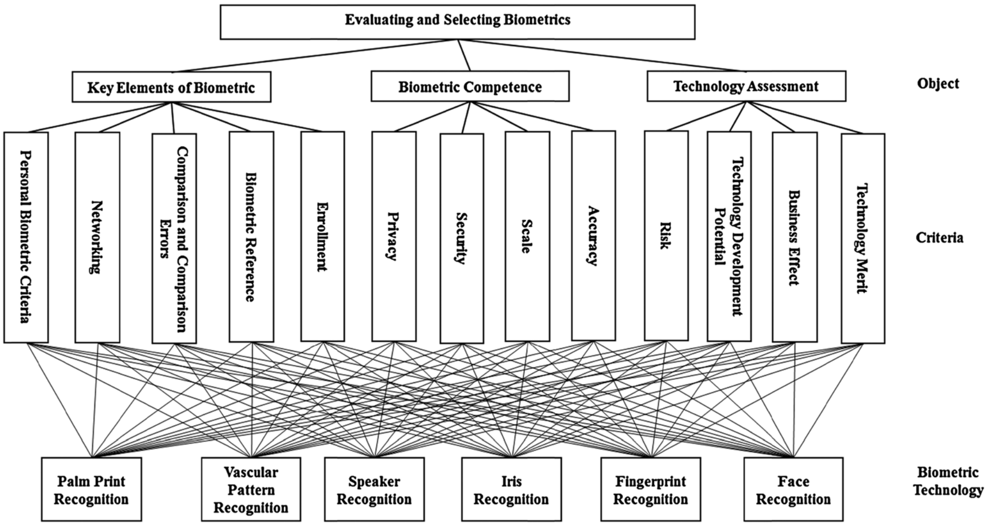

Figure 1. Evaluation and selection model for biometrics.

problems existing in technology development by interpreting related literature and secondary documents to deeply analyze potential effects [11].

3.1.1. Technological merit.

Studies indicate that the technological aspect plays an important role in technology assessment [32,33]. Technological merit can be viewed from the following aspects [11,32–34]: (1) advancement; (2) innovation; (3) key technology; (4) proprietary aspects; (5) generic aspects; (6) technological connections; and (7) technological extendibility.

3.1.2. Business effects.

Effects benefitting corporations and economic/industrial development are of considerable weight in the evaluation of technology. Hence, we should consider business factors. These include the following: (1) possible investment returns; (2) existing market share variation; (3) new market growth; (4) possible scale of the market; and (5) product life cycle [11,32,34–36].

3.1.3. Technology development potential.

It is necessary to consider the availability of related technological resources upon technology assessment. Factors affecting the realization of technology development are as follows: (1) technical resource availability; (2) equipment support; and (3) opportunity for technical success [11,32,34,37].

3.1.4. Risk.

When assessing new technologies, decision makers are faced with potential risks associated with the technology development. The criteria of risk aspects are as follows: (1) commercial risk; (2) technical risk; (3) technical difficulties; and (4) ethical risk [11,34,35,38].

3.2. Biometrics performance

Jain *et al.* grouped fundamental required performance in biometrics into four categories: (1) accuracy; (2) scale; (3) security; and (4) privacy [16].

3.2.1. Accuracy.

An ideal biometrics system should promise to offer the correct decision when presented with a biometric identifier sample hand [39]. Even ignoring the requirements of complete automation and assuming the possibility of good biometric signal acquisition from a distance, this need should clearly be noted when attempting to bridge the gap between performance requirements and current technology [16].

3.2.2. Scale.

Because verification systems essentially involve a 1:1 match, the size of the database is not so critical, requiring only comparing one set of enrolled samples to one set of enrollment templates [39]. Efficient scaling is required for system control throughput and false-match error rates as the size of the database increases [16].

3.2.3. Security.

In the past, two serious criticisms of biometrics have been that they are not secret and that biometric patterns have not been appropriately assessed [40]. However, biometric template protection is a rapidly developing area; extensive research in this area has been conducted in the last several years to enhance security [41]. For example, cancellable templates are perfect examples to address the issue of biometric non-revocability [42]. A secure biometric system is a design challenge requiring the ability to not be fooled by doctored or spoofed measurements injected into the system while accepting only the legitimate presentation of biometric identifiers [16].

3.2.4. Privacy.

A biometric system should provide irrefutable proof of the identity of the person with extreme reliability. In consequence, privacy is one of the most significant user concerns [16]. Much hard work is required to provide satisfactory solutions for this fundamental privacy problem. There are several ingredients needed for a successful strategy [43].

3.3. Key elements of biometrics

There are five common elements to all biometric systems.

3.3.1. Enrollment.

Proper enrollment instruction and training are essential to good biometric system performance [17]. Enrollment is the first stage for biometric system setup because it generates the template that will be used for all subsequent comparisons and user recognition [15]. During enrollment, a biometric system averages readings or selects the best quality sample to produce an enrollment reference or template [18].

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 [15,44]. Templates are usually not actual images of the fingerprint, iris, hand, and so on [17] but are instead generally only numerical representations of key data points (or minutia) read from a person's biometric feature [18].

3.3.3. Comparison and comparison errors.

Comparison is the act of comparing one (or more) acquired biometric samples to one (or more) stored biometric templates for the purpose of recognition [15]. No biometric decision is 100% perfect in either verification or identification mode [18]. Therefore, biometric systems can be configured to create a threshold establishing the acceptable degree of similarity [17].

3.3.4. Networking.

Regarding networks, there are potential variation issues. Biometric systems/readers require integral networking functionality with a proprietary protocol [17]. This allows networking a number of readers together with little or no additional equipment. A monitoring PC typically connects at an endpoint of the network [15,18].

3.3.5. Personal biometric characteristics.

Any human biological or behavioral feature can become a biometric identifier, provided the following properties are met [16,18]: (1) universality: almost every person should have the characteristics; (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

This study mainly applied the FAHP to assess the feasibility of using biometrics to achieve the evaluation objects and criteria. For determinations, it is critical not only to evaluate the priority of different objects but also to determine whether the biometrics fulfills the implementation objectives. Biometric technology evaluations should be well defined to allow resources and elements to be allocated to achieve the objectives. In this case, AHP is often a quite-useful approach that encourages decision makers to clearly describe their subjective and qualitative judgments [14]. However, to enhance AHP result reliability, we adopt FAHP rather than conventional AHP. Furthermore, the outcomes generated by FAHP complement the biometric technology preference recommendations produced by best non-fuzzy performance (BNP) analysis. We illustrated the FAHP steps in this section.

The AHP can support the process of assessing the fitness rank of a group of factors and the relative priority of a multi-criteria decision-making issue between them [14,45,46]. At the same time, academics and professionals have extensively applied AHP in the field of technology assessment [47–51]. In this biometric technology analysis, AHP permits the “hierarchization” of distinctive evaluation objects and their allied or related criteria, generating possible quantitative results that deliver a numerical estimate of the relevant consequences of each criterion and alternative.

Regardless, some researchers criticize AHP, claiming that it cannot accurately reflect human cognition because of the uncertainty and ambiguity of decision makers’ judgments [52–55]. It is difficult to understand the partiality of decision makers for certain numbers. The fuzzy method is proposed to improve the AHP [54,56,57]. Fuzzy set theory was introduced to solve puzzles with less-clearly defined criteria [58]. FAHP was developed to solve hierarchical problems. Decision makers are usually more confident giving interval judgments than fixed value judgments because they are usually unable to be explicit about their preferences concerning the fuzzy nature of the comparison process [59]. Linguistic variables are variables whose values are words or sentences in a natural or artificial language. In other words, they are variables with lingual expression as their values [54,57]. Hence, we use this type of expression to compare two approaches to creating the best plan evaluation criteria, applying five basic linguistic principles to a fuzzy level scale [60,61]. A similar structure concept combining FAHP with BNP has been adopted in many studies [62–64]. We feel that the scheme could be useful in this biometrics assessment study. The steps are as follows.

Step 1: Developing the assessment matrix structure

Construct pairwise comparison matrices among all the elements/criteria in the dimensions of the hierarchy system. Assign linguistic terms to the pairwise comparisons by asking which is more important for each two criteria for each of the K decision makers based on a nine-point scale [14].

Step 2: Checking for consistency

The AHP is applied to obtain the weights of the criteria, w1, …, wn, based on the hierarchy built in step 1. The reciprocal matrix A is a pairwise comparison, in which a_{ij} is the geometric mean of the criteria i and j comparison.

$$\mathbf{A} = [a_{ij}] = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a_{21} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 1/a_{12} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1/a_{1n} & 1/a_{2n} & \cdots & 1 \end{bmatrix} \tag{1}$$

The priority of the elements was compared by the computation of eigenvalues and eigenvectors in Equation (2), in which the eigenvector of the matrix A is w, which could be calculated per Equation (3). The largest eigenvalue of the matrix $\boldsymbol{A}$ is $\lambda_{\max}$, which could be the means that could be estimated per Equation (4), and n is the criterion number.

$$\boldsymbol{A} \cdot w = \lambda_{\max} \cdot w \tag{2}$$

$$\mathbf{w} = \left(\prod_{j=1}^{n} a_{ij} \right)^{1/n} \Bigg/ \sum_{i=1}^{n} \left(\prod_{j=1}^{n} a_{ij} \right)^{1/n} \tag{3}$$

$$\lambda_{\max} = \frac{1}{n} \sum_{i=1}^{n} \frac{(\mathbf{Aw})_i}{w_i} \tag{4}$$

The consistency property of the matrix is then checked to ensure the consistency of the judgments in the pairwise comparison. The consistency index (CI) and consistency ratio (CR) are defined as follows [14]. Random index (RI) in Equation (6) can be referred to in Table I according to criterion n.

Table I. Random index (RI).

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.51	1.48	1.56	1.57	1.59

$$CI = \frac{\lambda_{\max} - n}{n-1} \tag{5}$$

$$CR = \frac{CI}{RI} \tag{6}$$

Step 3: Constructing fuzzy positive matrices

To calculate criteria and sub-criteria weights to compare with each other, the Buckley method is used [65]. With the triangular fuzzy numbers in Table II, for calculating weights in each pairwise comparison matrix, the geometrical mean of each criterion was used in Equation (7), in which $\widetilde{A}^k$ is decision maker k's fuzzy positive reciprocal matrix and $\widetilde{a}_{ij}^k$ represents the relative importance of decision criteria i and j.

$$\widetilde{A}^k = \left[\widetilde{a}_{ij}^k\right] \tag{7}$$

Step 4: Calculating the fuzzy weights

On the basis of the Lambda–Max method [64], we calculate the fuzzy weights after step 3. The Lambda–Max method is introduced as follows.

(a) When $\alpha = 1$, we obtain $\widetilde{A}_m^k = \left[a_{ijm}\right]_{n \times n}$, and when $\alpha = 0$, we obtain the lower bound $\widetilde{A}_l^k = \left[a_{ijl}\right]_{n \times n}$ and the upper bound $\widetilde{A}_u^k = \left[a_{iju}\right]_{n \times n}$. The weight vector in the AHP process can be derived as $W_m^k = \left[W_{im}^k\right]$, $W_l^k = \left[W_{il}^k\right]$, and $W_u^k = \left[W_{iu}^k\right]$, $i = 1, 2 \ldots.. n$.

(b) We compute the two constants M_l^k and M_u^k to minimize the fuzziness of the weight by using Equations (8) and (9). We define the lower and upper bounds of the weight separately as Equations (10) and (11) and acquire the fuzzy weight matrix for decision maker k, $\widetilde{W}_i^k = \left(W_{il}^{*k}, W_{im}^k, W_{iu}^{*k}\right)$, $i = 1, 2 \ldots.. n$.

Table II. Triangular fuzzy numbers.

Linguistic variables	Positive triangular fuzzy numbers	Positive reciprocal triangular fuzzy numbers
Extremely strong	(9, 9, 9)	(1/9, 1/9, 1/9)
Intermediate	(7, 8, 9)	(1/9, 1/8, 1/7)
Very strong	(6, 7, 8)	(1/8, 1/7, 1/6)
Intermediate	(5, 6, 7)	(1/7, 1/6, 1/5)
Strong	(4, 5, 6)	(1/6, 1/5, 1/4)
Intermediate	(3, 4, 5)	(1/5, 1/4, 1/3)
Moderately strong	(2, 3, 4)	(1/4, 1/3, 1/2)
Intermediate	(1, 2, 3)	(1/3, 1/2, 1)
Equally strong	(1, 1, 1)	(1, 1, 1)

$$M_l^k = \min\left\{\frac{W_{im}^k}{W_{il}^k} | 1 \le i \le n\right\} \tag{8}$$

$$M_u^k = \max\left\{\frac{W_{im}^k}{W_{iu}^k} | 1 \le i \le n\right\} \tag{9}$$

$$W_l^{*k} = \left[W_{il}^{*k}\right], W_{il}^{*k} = M_l^k W_{il}^k, i = 1, 2, \ldots, n \tag{10}$$

$$W_u^{*k} = \left[W_{iu}^{*k}\right], W_{iu}^{*k} = M_u^k W_{iu}^k, i = 1, 2, \ldots, n \tag{11}$$

Step 5: Integrating the fuzzy weights of decision makers

We apply the geometric average to obtain the aggregate of the fuzzy weights of decision makers per Table III and Equation (12) [66], in which $\overline{\widetilde{W}}_i$ is the aggregated fuzzy weight of criterion i and $\widetilde{W}_i^k$ is the fuzzy weight of criterion i.

$$\overline{\widetilde{W}}_i = \left(\prod_{k=1}^{K} \widetilde{W}_i^k\right)^{1/K}, \forall k = 1, 2, \ldots, K \tag{12}$$

Step 6: Ranking of criteria

A proximity coefficient was defined to obtain the ranking order of the decision elements. The proximity coefficient is defined as Equation (13), in which CC_i is the weight for criterion i. Additionally, $d^-\left(\widetilde{W}_i, 0\right)$ and $d^+\left(\widetilde{W}_i, 0\right)$ are the distance measurements between two fuzzy numbers that could be calculated per Equations (14) and (15).

$$CC_i = \frac{d^-\left(\widetilde{W}_i, 0\right)}{d^+\left(\widetilde{W}_i, 1\right) + d^-\left(\widetilde{W}_i, 0\right)}, \quad i = 1, 2, \ldots, n, 0 \le CC_i \le 1 \tag{13}$$

Table III. Linguistic scales.

Linguistic variables	Corresponding triangular fuzzy number
Very poor	(1, 1, 1)
Poor	(1, 3, 5)
Fair	(3, 5, 7)
Good	(5, 7, 9)
Very good	(7, 9, 9)

DOI: 10.1002/sec

$$d^{-}\left(\widetilde{W}_i, 0\right) = \sqrt{\frac{1}{3}\left[\left(\overline{W}^{*}_{il} - 0\right)^2 + \left(\overline{W}_{im} - 0\right)^2 + \left(\overline{W}^{*}_{iu} - 0\right)^2\right]} \tag{14}$$

$$d^{+}\left(\widetilde{W}_i, 1\right) = \sqrt{\frac{1}{3}\left[\left(\overline{W}^{*}_{il} - 1\right)^2 + \left(\overline{W}_{im} - 1\right)^2 + \left(\overline{W}^{*}_{iu} - 1\right)^2\right]} \tag{15}$$

Step 7: Evaluating the biometric technologies

With the results of a series of simple rankings, the weights of all criteria in each object of the hierarchy relative to the entire level directly above were obtained. These in turn were all ranked and were carried from the upper layer to the lower layer. After the aforementioned analytic process, the weight of each assessment criterion was determined for integrated assessment of the biometric technologies.

5. RESEARCH ANALYSIS

The study applied the assessment research model to evaluate the top six emergent biometric technologies discussed in the IBG market report [13] and considered the potential biometric technologies under different objects by using BNP analysis based on the weights of each criterion obtained per FAHP. Furthermore, according to the data analysis, we discussed management implications.

5.1. Data analysis

This study queried experts in the biometrics field who are familiar with biometric technology market conditions to assess the top six major biometric technologies to accomplish the research purpose. We used step 1 in the previous section to verify the consistency of the 18 expert questionnaires. There were 15 valid questionnaires whose values of CI and CR were less than 0.1. We employed the data to obtain the final criteria weights of the assessment structure, per steps 3–6. The analysis results are presented in Table IV.

Technology assessment (0.407) is the most-emphasized object when evaluating biometric technologies, with biometric competence (0.351) and the key elements of biometrics (0.242) ranking second and third, respectively. Nevertheless, biometric competence and the key elements of biometrics are greater than 0.5, but the technology assessment is not. This indicates that when evaluating biometric technologies, evaluators should still take the details of the target technology into account.

On the basis of the weights, the evaluation of biometric technologies relied on linguistic variables in Table III to express subjective judgments of the experts to reflect natural human considerations. The experts were asked to identify biometric technologies corresponding to each criterion; their opinions were later aggregated through the geometric average technique suggested by Buckley [61]. The fuzzy assessments of biometric technologies based on the evaluation criteria are presented in Table V. Next, the procedure of defuzzification locates the BNP value [66]. Therefore, it is used in this study. The BNP value of the fuzzy number R_i can be found by Equation (16). LR_i, MR_i, and UR_i are the lower, middle, and upper synthetic performance values of alternative i, respectively, and the calculations of each are as illustrated.

$$BNP_i = {}^{[(UR_i - LR_i) + (MR_i - LR_i)]}\Big/_{3} + LR_i, \forall i \tag{16}$$

The BNP values of the six biometric technologies on each criterion are shown in Table VI. The ranking of the biometric technologies then proceeds on the basis of the value of the derived BNP for each of the biometric technologies.

By applying the simple additive weighting method to calculate the final score of each biometric technology, we calculated the BNP values multiplied by the weights in Table VI to produce the final evaluation of the six

Table IV. Weights used in the evaluation of biometric technologies.

Object	Weight	Criteria	Weight within object	Aggregated weight	Rank
Technology assessment	0.407	Technology merit	0.188	0.077	7
		Business effect	0.367	0.149	1
		Technology development potential	0.239	0.097	3
		Risk	0.206	0.084	6
Biometric competence	0.351	Accuracy	0.241	0.085	5
		Scale	0.158	0.055	9
		Security	0.329	0.115	2
		Privacy	0.272	0.095	4
Key elements of biometric	0.242	Enrollment	0.191	0.046	11
		Biometric reference	0.174	0.042	13
		Comparison and comparison errors	0.261	0.063	8
		Networking	0.178	0.043	12
		Personal biometric criteria	0.196	0.047	10

Table V. Fuzzy evaluation of six biometric technologies on criteria.

Criteria	Face recognition	Fingerprint recognition	Iris recognition	Speaker recognition	Vascular pattern recognition	Palm print recognition
Technology merit	(1.67, 2.35, 2.84)	(3.02, 4.31, 5.69)	(1.51, 2.26, 2.91)	(4.12, 5.88, 7.75)	(2.00, 2.90, 3.65)	(2.36, 3.05, 3.94)
Business effect	(3.75, 5.73, 7.27)	(2.98, 4.35, 5.42)	(2.60, 3.69, 4.56)	(2.53, 3.35, 4.03)	(1.99, 2.74, 3.70)	(2.98, 3.83, 4.87)
Technology development potential	(2.65, 3.62, 4.85)	(2.37, 3.41, 4.24)	(1.56, 2.22, 2.76)	(4.66, 5.83, 7.67)	(2.84, 4.30, 5.74)	(4.34, 5.90, 7.09)
Risk	(2.91, 3.75, 4.91)	(3.98, 5.38, 6.67)	(3.54, 5.25, 6.34)	(2.47, 3.14, 3.87)	(1.50, 2.20, 2.68)	(3.39, 4.66, 6.20)
Accuracy	(2.13, 3.06, 3.72)	(2.54, 3.26, 4.16)	(3.97, 5.06, 6.33)	(1.72, 2.55, 3.15)	(3.05, 4.36, 5.37)	(1.76, 2.22, 2.69)
Scale	(3.02, 4.39, 5.35)	(3.23, 4.57, 5.70)	(4.43, 5.73, 6.95)	(1.90, 2.85, 3.63)	(1.51, 2.19, 2.74)	(1.58, 2.26, 2.73)
Security	(4.19, 5.65, 6.96)	(4.15, 5.86, 7.27)	(2.13, 3.28, 4.06)	(2.72, 3.70, 4.53)	(2.67, 3.75, 4.79)	(2.30, 3.33, 4.17)
Privacy	(2.33, 3.51, 4.57)	(4.50, 5.77, 7.45)	(4.02, 5.57, 7.12)	(2.26, 3.10, 4.12)	(2.47, 3.67, 4.47)	(2.58, 3.87, 4.69)
Enrollment	(2.32, 3.31, 4.02)	(3.55, 5.45, 7.30)	(3.66, 5.08, 6.39)	(1.59, 2.30, 2.87)	(2.27, 2.86, 3.64)	(4.74, 5.98, 7.25)
Biometric reference	(1.65, 2.43, 3.16)	(2.77, 3.56, 4.31)	(1.98, 3.07, 4.01)	(2.01, 2.67, 3.21)	(2.65, 3.49, 4.49)	(3.75, 5.47, 7.31)
Comparison and comparison errors	(1.37, 1.99, 2.65)	(2.79, 3.62, 4.42)	(2.49, 3.42, 4.19)	(1.93, 2.90, 3.56)	(3.90, 5.67, 7.09)	(1.35, 2.01, 2.45)
Networking	(3.00, 3.75, 4.81)	(3.51, 4.86, 6.38)	(3.21, 4.35, 5.85)	(1.63, 2.09, 2.59)	(2.70, 3.82, 4.59)	(2.62, 3.55, 4.55)
Personal biometric criteria	(1.95, 2.80, 3.53)	(1.83, 2.31, 3.05)	(3.13, 4.56, 6.05)	(1.60, 2.00, 2.47)	(4.35, 5.76, 6.93)	(2.66, 3.82, 4.64)

Note: The fuzzy value of the six biometric technologies on each criterion is presented in the brackets.

biometric technologies. For example, the score of face recognition is as follows:

$$2.28 \times 0.077 + 5.58 \times 0.149 + 3.71 \times 0.097 + 3.86 \times 0.084 + 2.97 \times 0.085 + 4.25 \times 0.055 + 5.60 \times 0.115 + 3.47 \times 0.095 + 3.21 \times 0.046 + 2.41 \times 0.042 + 2.00 \times 0.063 + 3.85 \times 0.043 + 2.76 \times 0.047 = 3.831$$

As Table VII indicates, among all six biometric technologies, fingerprint recognition is the most preferred, followed by iris recognition and face recognition.

5.2. Management implications

The first FAHP result indicates that within the technology assessment object, "business effect" (0.367) is the most critical criterion in biometric technology evaluations. According to the IBG report in 2009 [13], the major expectation of biometrics popularization and development is the progress of commercialization. As the first criterion overall, "business effect" also ranks first within the technology assessment to further stress the necessity of the realization and promotion of biometrics.

The results identified "Security" (0.329) as the first priority criterion of biometric competence. The demand for reliable authentication techniques increased in the wake of heightened concerns about security; therefore, biometric technology is regarded as an effective approach for enhancing network security [24]. In some instances, biometrics could be integrated with passwords or tokens to strengthen the security offered by an authentication system. Thus, we can use biometrics to improve user convenience while enhancing security. This implies that security is beneficial in facilitating the popularization of biometric technologies.

"Comparison and comparison errors" (0.261) is the predominant ingredient within the key elements of biometrics used to evaluate biometric technology. It is necessary to evaluate the setting of the threshold in identification systems for better matching because both failure to acquire and failure to enroll in the comparison process mean that the system can distinguish and extract the qualified characteristics of the user's biometric. Failure to acquire and/or failure to enroll indicate that this person's detected biometric features may not have sufficient quality to verify and recognize. Alternatively, a convenience-focused application could adjust software or the mechanism to provide little or no denial of legitimate matches to allow a certain acceptable degree of impostors. Hence, customers would be more likely to accept biometrics [67].

Overall, "business effect" accounts for a 14.9% aggregated weight to further accentuate the challenge of the commercialization of biometric technologies, which is also the most critical part of evaluating the feasibility of biometrics. Additionally, "security" accounts for 11.5% and

Table VI. Best non-fuzzy performance values of six biometric technologies on criteria.

Criteria	Face recognition	Fingerprint recognition	Iris recognition	Speaker recognition	Vascular pattern recognition	Palm print recognition
Technology merit	2.28	4.34	2.23	5.92	2.85	3.12
Business effect	5.58	4.25	3.62	3.30	2.81	3.89
Technology development potential	3.71	3.34	2.18	6.06	4.29	5.78
Risk	3.86	5.34	5.04	3.16	2.13	4.75
Accuracy	2.97	3.32	5.12	2.48	4.26	2.22
Scale	4.25	4.50	5.70	2.79	2.15	2.19
Security	5.60	5.76	3.16	3.65	3.74	3.27
Privacy	3.47	5.91	5.57	3.16	3.53	3.71
Enrollment	3.21	5.44	5.04	2.25	2.92	5.99
Biometric reference	2.41	3.55	3.00	2.63	3.54	5.51
Comparison and comparison errors	2.00	3.61	3.37	2.80	5.55	1.94
Networking	3.85	4.92	4.47	2.11	3.70	3.57
Personal biometric criteria	2.76	2.40	4.58	2.02	5.68	3.71

Table VII. Ranking of biometric technologies.

Biometric technologies	Score	Rank
Face recognition	3.831	3
Fingerprint recognition	4.453	1
Iris recognition	3.973	2
Speaker recognition	3.294	6
Vascular pattern recognition	3.717	5
Palm print recognition	3.782	4

ranks second; it reflects that how to guarantee security will be a key task in biometrics. The development of biometric technologies should therefore focus on capabilities in the security area as well as on customer expectations for biometrics. There is a special criterion in biometrics, “privacy,” which accounts for 9.5% and ranks as fourth, playing a very important role in the biometrics growth path. Finally, according to the data analysis, we performed evaluations to determine which criteria of biometrics could facilitate its future development. These analyses could indicate chances to stimulate the growth of biometric technologies.

After completion of the biometrics evaluation and selection model using BNP analysis, the six biometric technologies were evaluated to determine those with the most potential and therefore most recommendable. The performance of each biometric technology is pairwise compared by our experts. In Table VII, fingerprint recognition (4.453) is the most likely biometric technology among all six, followed by iris recognition (3.973), face recognition (3.831), palm print recognition (3.782), vascular pattern recognition (3.717), and speaker recognition (3.294).

Furthermore, scores for each biometric are gathered by cell and by criteria in Table VI. These scores illustrate the achievement distribution of a specific criterion through biometrics. Some significant explanations can be inferred on the basis of the results of the BNP analysis in Table VI. Fingerprint recognition performs best overall among the six biometric technologies because of its potential to meet the criteria in the objects, technology assessment and biometric competence. Iris recognition and face recognition also separately perform well on certain criteria according to Table VI, which is why they could score high in the FAHP. However, only the ranking of fingerprint recognition is the same as in the IBG report.

In reality, fingerprint recognition is also the top one, accounting for 45.9% of the non automated fingerprint identification system (non-AFIS) biometrics market, followed by face recognition at 18.5% and iris recognition at 8.3% [13]. Face recognition may be less competitive in the future because, in the present market, face recognition is the second most popular biometric technology [13]. We can see that it originally receives higher scores on two criteria, business effects and security, but is weaker on the others. Therefore, it is obvious that biometric technologies evaluated under different viewpoints will have different results. Because each biometric technology has its own supporting principles and mechanisms, it is hard to tell which biometric technology is superior on each criterion within this object. Hence, the difference in the scores is also close. This indicates that when discussing the advantages of utilizing biometric competence, iris recognition and fingerprint recognition play well compared with the others because of their high scores on criteria in this object, as presented in Table VI. This result shows that iris recognition development may have a chance to catch up from behind with its excellent biometric competences. Not surprisingly, iris recognition occupied third place in market revenue overall in 2009 [13]. As long as one biometric technology can achieve its biometric competences, it should create chances to enlarge market share and penetration

6. CONCLUSION

Today, biometrics has been vigorously promoted around the world as a means to strengthen network security and privacy [3] as well as to facilitate a new industry. Although biometrics has been applied in specific areas for decades, biometrics has gradually proliferated in customer and embedded electronic products to enhance security and privacy [7]. To meet various technology assessment aspects, biometric technologies should be carefully assessed with regard to distinct features.

This study focuses on clarifying how differing evaluation objects determine relevant biometric technologies. We employ FAHP that clearly ranks the criteria of the objects built on the basis of a literature review. Using the analysis results, we assess biometric technologies with the perspectives in previous studies about factors affecting biometric evaluation and selection and conduct a systematic ranking of the factors. We also organize and interpret these outcomes to form suggestions. The FAHP research method employed by this study is capable of revealing the relevance of the criteria and aids in the comprehension of them. The deployment of FAHP also allows relevant authorities to understand the importance of considering objects to determine development strategies. The derived results disclose a synthetic conclusion for different dimensions. In sum, this research suggests that biometrics should enhance and support the ranked criteria to increase competitiveness. With the aforementioned, we have drawn several conclusions.

First, fingerprint recognition received the highest score, followed by iris and face recognition. In the technology assessment and biometric competence objects, fingerprint recognition was the most recommendable biometric technology, so fingerprint recognition was determined to be the first priority. As shown in Table VI, fingerprint recognition did not stand out in each object, but on average, it performed the best overall. Therefore, fingerprint recognition ranked first and fully shows its leadership in the biometric technology competition. As a result, fingerprint recognition is regarded as the most complete biometric technology, which has certain advantages in the market. This result also indicates that fingerprint recognition still has room to improve and keep up on the criteria on which it was not the best. Producers should think more about strategies and measures to solidify fingerprint recognition technology in the near future.

Furthermore, each cell in Table VI identifies scores for each alternative by criterion. These scores represent the performance distribution of a specific criterion across the biometric technologies. Several important explanations can be made regarding the results in Table VI. Iris recognition actually performed the best in the biometric competence object, and vascular pattern recognition especially met the requirements of the key elements of biometric objects. In other words, this indicates that relevant people could review each of the six biometrics from each viewpoint and obtain different explanations for specific purposes or certain applications. With this deduction, for example after the 9/11 terrorism attack, iris recognition became the primary recognition technology because it is the most reliable type of biometric and has advantages in the biometric competence object. Moreover, iris recognition always plays the second level in multi-biometric systems [28]. The future of the iris recognition system is better in fields that demand rapid identification of individuals in a dynamic environment [27]. However, some considerations may be argued because of its low performance on some criteria, as shown in Table VI. As iris recognition improves on these criteria, it could increase its penetration. Finally, we found that the priority of face recognition was ranked third. In the present market, face recognition is the second-most-popular biometric technology [13]. Originally, face recognition had higher scores on the business effect, security, and scale criteria but was weaker on the other criteria. Therefore, when only evaluating and selecting based on the technology assessment object, face recognition is preferable. This leads to the obvious conclusion that biometric technologies evaluated under different scenarios will have different results. Relevant persons could use these results as a lens to speculate how they could develop biometrics for commercialization. As long as one biometric technology can improve its advantage on criteria in this model, it creates the chance to enlarge the market share and penetration.

In conclusion, management researchers are faced with the issue of assessing advanced technology to predict which will be utilized. This study applies FAHP and BNP analysis in evaluating biometric technologies to simulate how different evaluation objects affect biometric technology selection. With the weights of evaluation objects, we found that management aspects alone cannot determine the evaluation viewpoints. For example, the technology assessment object only accounted for 0.407. This enables researchers to recognize that technology assessment should focus more on the specifics of target technologies. Doing so could help them more comprehensively evaluate and select biometrics for network security.

REFERENCES

1. Gupta P, Carew S. Apple buys mobile security firm AuthenTec for $356 million. Retrieved from http://www.reuters.com/article/2012/07/27/us-authentec-acquisition-apple-idUSBRE86Q0KD20120727, Jul 27, 2012.
2. Apple Press Info. Retrieved from http://www.apple.com/pr/library/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World.html, Sep 10, 2013.
3. Yu FR, Tang H, Leung CMV, Liu J, Lung CH. Biometric-based user authentication in mobile ad hoc networks. *Security and Communication Networks* 2008; **1**(1):5–16.
4. Adeoye SO. A survey of emerging biometric technologies. *International Journal of Computer Applications* 2010; **9**(10):1–5.
5. Jain AK, Nandakumar K, Nagar A. Biometric template security. *EURASIP Journal on Advances in Signal Processing* 2008; Article ID 579416 2008: 17.
6. Delac K, Grgic M. A survey of biometric recognition methods. 46th International Symposium Electronics in Marine, ELMAR-2004, Zadar, Croatia, 16–18 June 2004.

7. Bhattacharyya D, Ranjan R, Alisherov AF, Choi MK. Biometric authentication: a review. *International Journal of u- and e- Service Science and Technology* 2009; **2**(3):13–28.
8. Jain AK, Ross A. Multibiometric systems, appeared in communication of the ACM. *Special Issue on Multimodal Interfaces* 2004; **47**(1):34–40.
9. Riley RA, Kleist VF. The biometric technologies business case: a systematic approach. *Information Management & Computer Security* 2005; **13**(2): 89–105.
10. Tran TA, Daim T. A taxonomic review of methods and tools applied in technology assessment. *Technological Forecasting and Social Change* 2008; **75**(9):1396–1405.
11. Shen YC, Chang SH, Lin GTR, Yu HC. A hybrid selection model for emerging technology. *Technological Forecasting and Social Change* 2010; **77**:151–166.
12. Fleischer T, Decker M, Fiedeler U. Assessing emerging technologies—methodological challenges and the case of nanotechnologies. *Technological Forecasting and Social Change* 2005; **72**(9):1112–1121.
13. International Biometric Group. *Biometrics Market and Industry Report 2009–2014*. International Biometric Group: New York, 2009.
14. Saaty TL. *The Analytic Hierarchy Process*. McGraw-Hill: New York, 1980.
15. Biometrics Identity Management Agency. Biometrics Glossary version 4.0. Software Engineering Center CECOM Life Cycle Management Command, 2010. Retrieved from http://www.biometrics.dod.mil/Files/Documents/Standards/BioGlossary.pdf [accessed 20 April 2013].
16. Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics* 2004; **14**(1):4–20.
17. Heyer R. *Biometrics Technology Review 2008*. Defence Science and Technology Organisation: Edinburgh, South Australia, publication DSTO-GD-0538, 2008.
18. NBSP. Biometric Technology Application Manual Volume One, Biometric Basics Compiled and Published by: National Biometric Security Project 2008. Retrieved from http://www.planetbiometrics.com/creo_files/upload/article-files/btamvol1update.pdf [accessed 25 April 2013].
19. Dabbah MA, Woo WL, Dlay SS. Secure authentication for face recognition. In *Proc. of IEEE Symposium on Computational Intelligence in Image and Signal Processing*, Honolulu, HI, Apr. 2007; 121–126.
20. National Science and Technology Council. Biometrics “Foundation Documents”. 2006. Retrieved from www.biometrics.gov/documents/biofoundationdocs.pdf [accessed 20 March 2013].
21. Goudelis G, Tefas A, Pitas I. Emerging biometric modalities: a survey. *Journal on Multimodal User Interfaces* 2008; **2**(3–4):217–235.
22. Hong JH, Yun EK, Cho SB. A review of performance evaluation for biometrics systems. *International Journal of Image & Graphics* 2005; **5**(3):501–536.
23. Vielhauer C. Biometric modalities. Different traits for authenticating subjects: chapter 3 in biometric user authentication for IT security. *Advances in Information Security* 2006; **18**(I):33–75.
24. Jain AK, Ross A, Pankanti S. Biometric: a tool for information security. *IEEE Transactions on Information Forensics and Security* 2006; **1**(2):125–144.
25. Xi K, Ahmad T, Han F, Hu J. A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment. *Scurity and Communication Networks* 2011; **4**(5):487–499.
26. Ross A, Dass S, Jain AK. A deformable model for fingerprint matching. *Journal of Pattern Recognition* 2005; **38**(1):95–103.
27. Ross A. Iris recognition: the path forward. *IEEE Computer* 2010; **43**(2):30–35.
28. Ganorkar RS, Ghatol AA. Iris recognition: an emerging biometric technology. in *Proc. of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation*, Greece, 2007; 91–96.
29. Kar B, Kartik B, Dutta PK. Speech and face biometric for person authentication. In *Proc. of IEEE International Conference on Industrial Technology*, India, 2006; 391–396.
30. Bhattacharyya D, Das P, Kim TH, Bandyopadhyay KS. Vascular pattern analysis towards pervasive palm vein authentication. *Journal of Universal Computer Science* 2009; **15**(5):1081–1089.
31. Kong A, Zhang D, Kamel M. A survey of palm print recognition. *Pattern Recognition* 2009; **42**(7):1408–1418.
32. Hsu YG, Tzeng GH, Shyu JZ. Fuzzy multiple criteria selection of government-sponsored frontier technology R&D projects. *R&D Management* 2003; **33**(5):539–551.
33. Lee YG, Song YI. Selecting the key research areas in nano-technology field using technology cluster analysis: a case study based on national R&D programs in South Korea. *Technovation* 2007; **27**(1–2):57–64.
34. Huang CC, Chu PY, Chiang YH. A fuzzy AHP application in government-sponsored R&D project selection. *Omega-International Journal of Management Science* 2008; **36**(6):1038–1052.
35. Coldrick S, Longhurst P, Ivey P, Hannis J. A R&D options selection model for investment decisions. *Technovation* 2005; **25**(3):185–193.
36. Shehabuddeen N, Probert D, Phaal R. From theory to practice: challenges in operationalising a technology selection framework. *Technovation* 2006; **26**(3):324–407.

37. The Advanced Technology Program. *How ATP Works*. 2010. Retrieved from http://www.atp.nist.gov/atp/overview.htm [accessed 25 March 2013].
38. Yu OS, Hsu GYJ, Chen TY. *Introduction to Technological Management: Technological Forecast and Planning*. Wu Nan Publishing Company: Taipei, 1998 (In Chinese).
39. Bolle RM, Connell JH, Pankanti S, Ratha NK, Senior AW. *Guide to Biometrics*. Springer: New York, 2004.
40. Kent S, Millett L. *Who Goes There?: Authentication Technologies Through the* Lens of Privacy. National Academies Press: Washington D.C., 2003.
41. Yang W, Hu J, Wang S. A finger–vein based cancellable biocryptosystem. *Network and System Security, Lecture Notes in Computer Science* 2013; **7873**:784–790.
42. Ahmad T, Hu J, Wang S. String-based cancelable fingerprint templates. In *Proc. of the 6th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, Beijing, 2011; 1028–1033.
43. Uludag U, Pankanti S, Prabhakar S, Jain AK. Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management* 2004; **92**(6):948–960.
44. Wang S, Hu J. Alignment-free cancellable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach. *Pattern Recognition* 2012; **45**(12): 4129–4137.
45. Wei CC, Chien CF, Wang MJ. An AHP-based approach to ERP system selection. *International Journal of Production Economics* 2005; **96**:47–62.
46. Hu AH, Hsu CW, Kuo TC, Wu WC. Risk evaluation of green components to hazardous substance using FMEA and FAHP. *Expert Systems with Applications* 2009; **36**(3):7142–7147.
47. Sloane EB, Liberatore MJ, Nydick RL, Luo W, Chung QB. Using the analytic hierarchy process as a clinical engineering tool to facilitate an iterative, multidisciplinary, microeconomic health technology assessment. *Computers & Operations Research* 2003; **30**(10):1447–1465.
48. Vaidya OS, Kumar S. Analytic hierarchy process: An overview of applications. *European Journal of Operational Research* 2006; **169**(1):1–29.
49. Balestra G, Knaflitz M, Massa R, Sicuro M. AHP for the acquisition of biomedical instrumentation. In *Conf. Proc. IEEE Eng. Med. Biol. Soc.*, Lyon, 2007; 3581–3584.
50. Gerdsri N, Kocaoglu DF. Applying the analytic hierarchy process (AHP) to build a strategic framework for technology road mapping. *Mathematical and Computer Modelling* 2007; **46**(7/8):1071–1080.
51. Kim WK, Han SK, Oh KJ, Kim TY, Ahn HC, Song CW. The dual analytic hierarchy process to prioritize emerging technologies. *Technological Forecasting and Social Change* 2010; **77**(4):566–577.
52. Kwong CK, Bai H. Determining the important weights for the customer requirement in QFD using a fuzzy AHP with an extent analysis approach. *IIE Transaction* 2003; **35**:619–626.
53. Chan FTS, Kumar N. Global supplier development considering risk factors using fuzzy extended AHP-based approach. *Omega* 2007; **35**(4):417–431.
54. Lee HI, Chen WC, Chang CJ. A fuzzy AHP and BSC approach for evaluating performance of IT development in the manufacturing industry in Taiwan. *Expert Systems with Applications* 2008; **34**(1):96–107.
55. Fu HP, Chao P, Chang TH, Chang YS. The impact of market freedom on the adoption of third-party electronic marketplaces: a fuzzy AHP analysis. *Industrial Marketing Management* 2008; **37**:698–712.
56. Gupta MM, Saridis GN, Gaines BR. *Fuzzy Automata and Decision Processes*. Elsevier North-Holland: New York, 1997.
57. Tsaur SH, Tzeng GH, Wang KC. Evaluating tourist risks from fuzzy perspectives. *Annual of Tourism Research* 1997; **24**(4):796–812.
58. Zadeh LA. Fuzzy sets. *Information and Control* 1965; **8**(3):338–353.
59. Deng H. Multicriteria analysis with fuzzy pairwise comparison. *International Journal of Approximate Reasoning* 1999; **21**(3):215–231.
60. Laarhoven PJM, Pedrycz W. A fuzzy extension of Saaty’s priority theory. *Fuzzy Sets and Systems* 1983; **11**(1–3):229–241.
61. Buckley JJ. Fuzzy hierarchical analysis. *Fuzzy Sets and Systems* 1985; **17**(3):233–247.
62. Shen YC, Lin GTR, Li KP, Yuan BJC. An evaluation of exploiting renewable energy sources with concerns of policy and technology. *Energy Policy* 2010; **38**:4604–4616.
63. Hsieh TY, Lu ST, Tzeng GH. Fuzzy MCDM approach for planning and design tenders selection in public office buildings. *International Journal of Project Management* 2004; **22**(7):573–584.
64. Csutora R, Buckley JJ. Fuzzy hierarchical analysis: the Lambda–Max method. *Fuzzy Sets and Systems* 2001; **120**(2):181–195.
65. Lee SK, Yoon YJ, Kim JW. A study on making a long-term improvement in the national energy efficiency and GHG control plans by the AHP approach. *Energy Policy* 2007; **35**(5):2862–2868.
66. Opricovic S, Tzeng GH. Defuzzification within a multi criteria decision model. *International Journal of Uncertainty Fuzziness and Knowledge-based Systems* 2003; **11**(5):635–652.
67. Grijpink JHAM. Trend report on biometrics: Some new insights, experiences and developments. *Computer Law & Security Report* 2008; **24**:261–264.

APPENDIX

Questionnaire Information Table

No.	Position	Affiliation
1	Vice President	Egis Technology Inc. (fingerprint authentication solution provider)
2	Sales	Hitachi, Ltd. Taiwan Branch (finger–vein authentication solution provider)
3	RD Director	Face-Tek Technology Inc. (face recognition access control system provider)
4	Asia Region Manager	Fingerprint Cards AB (FPC) Company
5	Algorithm R&D Senior Management	iFLYTEK Co., Ltd. (speech and language information processing provider)
6	Assistant Professor	Department of Electrical Engineering, Chang Gung University
7	Professor	Department of Electrical Engineering, National Tsing Hua University
8	Smartphone FW Integration R&D Division Manager	MediaTek Inc.
9	Professor	Department of Computer Science, National Tsing Hua University
10	Honorary Professor	Institute of Electro-Optical Engineering, National Chiao Tung University
11	RD Director	D-Link Corporation
12	System Customer Service Assistant Management	SYSTEM Corporation
13	Product Manager, Mobile Product Division	Asus Corporation
14	Manager of Human Interface System Development, RD Division	Acer Inc.
15	RD Hardware Manager	HTC Corporation
16	Software Project Manager	HTC Corporation
17	Associate Professor	Department of Electrical Engineering, National Sun Yat-Sen University
18	Senior Engineer	LG Electronics Inc., Iris Technology Division (iris authentication solution provider)