International Journal of Innovative
Computing, Information and Control
Volume **8**, Number **11**, November **2012**

 ISSN 1349-4198
pp. **7983–7999**

TECHNICAL ISSUES AND CHALLENGES OF BIOMETRIC APPLICATIONS AS ACCESS CONTROL TOOLS OF INFORMATION SECURITY

Sharifah Mumtazah Syed Ahmad, Borhanuddin Mohd Ali and Wan Azizun Wan Adnan

Faculty of Engineering
Universiti Putra Malaysia
43400, UPM, Serdang, Selangor, Malaysia
{ s_mumtazah; borhan; wawa }@eng.upm.edu.my

Received July 2011; revised December 2011

Abstract. *Recent advances in biometric technologies coupled with the increased threats in information security has proliferated the applications of biometric systems to safeguard information and its supporting processes, systems and infrastructures. This paper discusses the technical issues and challenges faced by biometric technologies within the physical and logical access control applications of information security. The discussion includes concerns on the system performances with regard to robustness to the actual operating environment and recognition capability of different biometric traits. It also addresses various security threats which include spoofing and replay attacks. In addition, this paper highlights the challenges in interoperability as well as needs for reliable testing and reporting. The overall discussions provide imperative insights for an effective trade-off and risk management analyses in information security policy and decision making.*
Keywords: Biometric, Access control, Biometric menagerie, 'Liveness' detection, Template protection scheme, Standards, Interoperability

1. **Introduction.** Information security basically ensures the confidentiality, integrity and availability of information. It essentially provides the necessary protection to information and the supporting processes, systems and infrastructures from various forms of possible threats and vulnerabilities. Both physical and logical access controls are amongst the imperative protection schemes in information security [1,2]. Physical access controls ensure that only authorized personnel are provided access to buildings or rooms containing IT infrastructures, documents filling, etc. On the other hand, logical access controls protect the computers, network facilities and information systems from threats of unauthorized access.

Physical and logical access controls are essentially based on user authentication whereby an individual's identity is verified through either one of the three following means [3-5]: 'by something he knows', 'by something he has' or 'by something he is' (or through combinations of any of the three means). Traditional approaches are basically based on the first two methods. The former implies password authentication that can be forgotten, guessed or cracked through dictionary or brute forced attacks [2,4], whereas the latter involves the use of tokens as identifiers such as keys or smartcards for authentication purposes. Unfortunately, the second method is also at risk of being shared, lost, duplicated, or stolen [4]. The emerging solution is based on biometric which is claimed to be more reliable and more fool-proof [2,4] that relies on 'something that you are', to make personal authentication.

Biometric authentication is synonymous with the way human identifies one another. In other words, biometric systems rely on measurable physiological or behavioural characteristics that can be utilised to identify or verify the identity of an individual [2-5]. Biometric systems establish a person's identity based on pattern analyses carried out on specific human traits [2,3]. Physiological-based biometric systems include fingerprints, retina, iris, hand geometry, hand vein, ear shape and facial recognition systems. These features are usually unalterable without causing trauma to individual. On the other hand, behavioural biometric characteristics are traits that are learned or acquired, which later stabilize over a period of time. Examples of behavioural-based biometric systems are voice recognition, keystroke dynamics, signature verification and gait analysis.

Biometric systems were initially made available in the 1970s for law enforcement agencies to identify criminals through fingerprint recognition [6]. However, recent advances in biometric technologies, coupled with the increased threats in information security, have proliferated the applications of biometric systems into the physical and logical access control domains [2-7]. Such applications have also been spurred due to cost reduction of biometric capture devices [3,7]. Biometric market is projected to experience a steady compound average growth rate (CAGR) of 22.3% reaching over USD9.36 billion in the year 2014, whereby over 30% of which is for physical and logical access control applications [7]. These applications can be applied at various levels which include national or corporate domain; besides, they can be incorporated within an individual customer's products. To illustrate, the Malaysian identity card known as 'MyKad' is a national initiative deployed by the government that incorporates fingerprint biometric to enhance its function and effectiveness [8]. Here, a person's identity and citizenship can be verified based on his fingerprint, which also prevents fraud and spoofing of national IDs. In addition, MyKad biometric authentication is also used at the automatic kiosk of Malaysia's Employees Provident Fund (EPF) and at the counter of other government agencies [8] providing an authentication scheme to individual account holders. In the United States, physical entrances into its nuclear power plants are only granted based on hand geometry recognition [3]. In addition, iris scanning has also been deployed at its Office of Legislative Counsel [3] to ensure the confidentiality of its files and documents. Examples of biometric authentication which are incorporated within individual consumer products include login into notebooks and smartphones that utilize low-cost sweep fingerprint sensors [6].

Different biometric systems basically differ in the underlying technologies, complexities and performances [2,3]. Each biometric technology has its strengths as well as limitations. It is often difficult to find a biometric technology that satisfies all technical requirements. Thus, a detailed study on the trade-off and risk management is imperative in information security policy and decision making prior to and during the deployment of a biometric system. The main objective of a trade-off analysis is to identify the requirements of the access control applications; hence, assisting in identifying the right biometric solution. On the other hand, the technical design and operational issues identified in the risk management analysis assist in defining additional or alternative security control for effective information security governance [9].

This paper provides a holistic view on the current technical issues and challenges regarding the use of biometric system. The prime aim of this paper is to assist in information security policy and decision making, particularly in providing insights for information security trade-off and risk management analyses. Most literature on information security [65-70] mainly focuses on the legal, ethical and social concerns over biometric system deployment. Discussions on its technical aspects have been less reported; in fact, the few that are available [6,26,29,30] are based on selected and focused issues which are not comprehensive. In this paper, a more structured state-of-the-art discussion is presented which

covers technical concerns that are specifically linked to biometric performances affected by different components that build up the system. One of the key findings includes the dilemma over the adverse effects of different types of biometric user population particularly the 'goats', 'wolves', and 'lambs' on the system accuracy. In addition, this paper reveals that both issues on the robustness of the system to variations in actual operating environment, as well as the security treats of spoofing and replay attacks remain the prime technical concerns over biometric system deployment. This paper also emphasizes on the need for reliable biometric system test reporting and assurance of product and device interoperability.

Though biometric systems are deployed in a wide range of applications which include surveillance, border control, criminal identification, forensic applications, etc. [3-7], this paper focuses only on physical and logical access control applications which are linked to information security measures. The organization of the rest of this paper is as follows. Sections 2 and 3 provide an introduction to biometric system components and performance measurements respectively. These chapters serve as backgrounds in understanding the technical issues and concerns on biometric security, accuracy, interoperability, testing and reporting which are deliberated in Sections 4-9. Discussions and conclusions are presented in Sections 10 and 11 respectively.

2. **Biometric Systems' Components.** A biometric system's operation mainly involves two phases, namely enrolment and recognition [3,5]. Both phases require the use of biometric sensors such as cameras, microphones, fingerprint scanners, and tablets. to capture the specific biometric human traits from individuals and convert the input samples into relevant digital format. Next, the salient features are extracted into biometric templates. An optional pre-processing module may exist in between the two processes, particularly to 'clean' the samples which may be subjected to various types of noise and interference, and to prepare the samples into appropriate format for feature extraction. The biometric templates are then stored in the databases as individuals' references.

Biometric recognition often makes use of a comparator module which can be carried out in two different modes, namely user verification and user identification [3-5]. The former performs authentication based on 'are you who you claimed to be' mode. This mainly involves a straight forward '1 to 1' comparison, whereby the final verdict is a binary 'accept' or 'reject' decision. The identifiers are usually in the form of user IDs or smartcards. On the other hand, the latter performs an exhaustive '1 to many' searches on the entire user database to solve the 'who are you' question. The main aim of user identification is to find the closest matching identity, if any exists. Biometric identification is often carried out in surveillance and forensics applications [3,4]. Both logical and physical access control applications usually involve biometric verification mainly to provide for a positive recognition that prevents multiple users using the same identity [5] and to avoid lengthy searches time [2]. However, in the case of a small number of user population such as logical access control to notebooks and smartphones, an identification mode can be applied without much degradation to the overall duration taken for system authentication and performance measurements. Figure 1 illustrates the different components of a biometric system.

3. **Biometric Performance Measurements.** The performance measurements of a biometric system can be tied closely to its main phases and processes as defined in the previous section. Jain et al. [4] has enlisted recognition accuracy under performance measurement of a biometric system which includes False Reject Rate (FRR) and False Accept Rate (FAR) [6,10]. FRR is also known as Type I error or False Non Match Rate

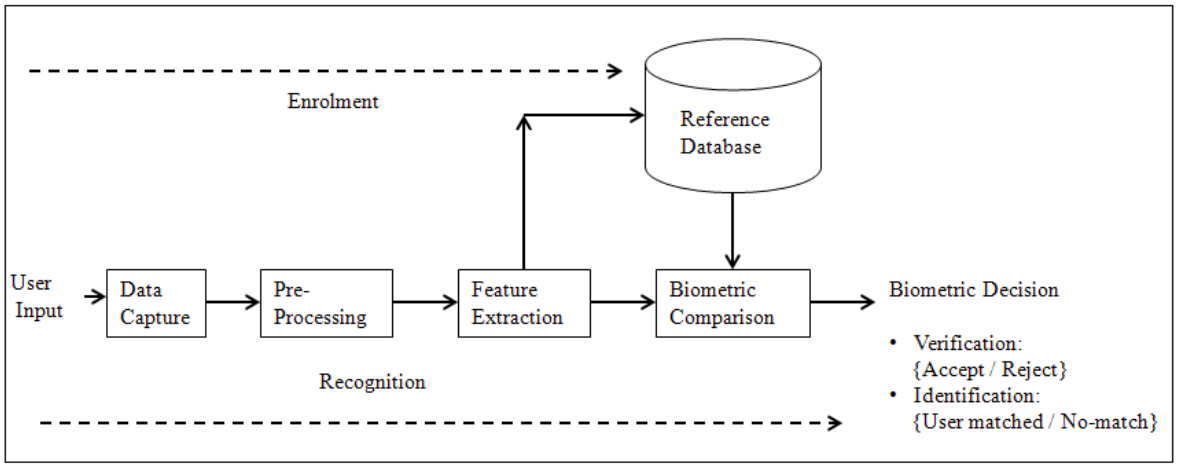

FIGURE 1. The components of a biometric system

(FNMR) [2-5] which describes the likelihood that a legitimate user is rejected by the system. On the other hand, FAR measures the probability that an impostor is accepted by the system as a genuine user. FAR is sometimes referred in the literatures as Type II error or False Match Rate (FMR) [2-5]. Both measurements of False Accept Rate (FAR) and False Reject Rate (FRR) vary with the corresponding system recognition threshold at the comparison module [4,5]. They are also related to each other where in general, if one figure is improved, then the other deteriorates. Ideally, a biometric system should produce zero values for both FAR and FRR, that is, it should be able to accept all genuine users and reject all false claims of identity. However, the performance of current biometrics technologies is still far from the ideal; hence, a trade-off is often necessary depending on the access control requirements. The need and type of biometric solution can be determined through a thorough risk management analysis [3]. Different applications require different levels of accuracy and tolerate different types of errors [4]. For instance, a very demanding authentication system such as a high security application, does not tolerate any intruders, thus requiring low FAR. On the other hand, a biometric authentication system embedded within a customer's notebook may require low FRR which is more convenient to its user. National civilian applications would demand low FRR and low FAR [4] in order to instil public trust and confidence with the deployed system.

In addition, 'collectability' has also been identified [4] as one of the important characteristics of a good biometric system. Since all biometric systems, regardless of the underlying technologies, heavily depend on input devices which are subjected to operational constraints, there are occasions whereby the devices themselves may fail to capture the necessary input samples of sufficient qualities. In such a situation, they may fall short of the 'collectability' requirement which in turn hinder recognition. Hence, it is desirable to measure the Failure to Acquire (FTA) Rate [10] which is also known in several biometric literatures [3-5] as Failure to Capture (FTC) Rate. FTA also reflects the convenience aspect in using the biometric system which is an important consideration factor in product selection for information security planning. For example, a civilian application which requires a high throughput often necessitates for a low value of FTA in order to avoid unnecessary delay in authenticating an individual.

Apart from these, an ideal biometric system should satisfy the 'universality' requirement [4], which essentially implies that it is usable to all or at least the majority of the users in the population. Universality aspect of a biometric system is measured though the Failure to Enrol (FTE) Rate. This figure indicates the cost effectiveness of a biometric investment.

A high value of FTE also highlights the need for alternative measures for access control to cater for those users whom cannot be authenticated through the biometric system.

4. **The Effect of Biometric Menagerie on System Performance.** Biometric menagerie was introduced in the late 1990s which recognize the division of user population into several possible categories namely 'goats', 'sheep', 'lambs' and 'wolves' [11,12]. 'Goats' are basically a subset of users with high level of intra user variability within their genuine samples; conversely, 'sheep' encompass users with characteristics opposite to 'goats'. 'Lambs' are users who are particularly vulnerable to impersonation and 'wolves' are individuals that are good at impersonating others. 'Goats' and 'lambs' are not the ideal group of users since they result in a high level of False Reject Rate (FRR) and False Accept Rate (FAR) respectively. Though a 'wolf' is not necessarily an enrolled user, the fact that a biometric system is susceptible to spoofing indicates the possible negative implications on the False Accept Rate (FAR).

It is somewhat imperative to understand such concepts of biometric menagerie particularly on their effects on system performance of different biometric technologies. For example, recognition systems which are based on biometric data with a high level of 'distinctiveness' and 'permanence' [4] such as the iris and fingerprint patterns are unlikely to be badly affected by 'goats', 'lambs' and 'wolves'. These physical traits are known for their high level of uniqueness and stability whereby the iris patterns of both left and right eyes and fingerprints of twins are not the same. Most importantly, they usually remain consistent throughout the life time of the individuals [2,3].

However, the performance of a signature verification system may be adversely affected by 'goats', 'lambs' and 'wolves'. Such a biometric system may not be feasible for writers with highly inconsistent signatures [13]. Besides, there often exist a subset of writers whose signatures are very simple and easy to be forged. This type of user population may significantly degrade the performance of the system. Similarly, the facial recognition system may be ineffective in differentiating identical twins.

In view of the above threats, a thorough risk management analysis must be carried out prior to finalizing on the choice of biometric technology to be deployed particularly with regard to the effect of the biometric menagerie on the system performance. There are scenarios whereby limited choices of biometric technologies are suitable for an application such as access control through telephony services that only allow for a speaker verification system in addition to password authentication [3,6]. In such cases, proper information security policy and procedures should be defined in addressing the technical performance limitations [3].

One of the extreme counter measures include identification and exclusion of 'goats' from the overall user population, and to provide them with an alternative access control mechanism which is synonymous to the 'sorting the sheep from the goats' idiom [12]. 'Goats' can be identified by analysing individual's False Rejection Rate [13]. However, since 'universality' is one of the key characteristic of a good biometric system, others have proposed the use of multimodal biometrics with the aim of compensating each other's performance limitations with regard to the 'goats', 'lambs' and 'wolves' issue [4,12,14].

A multimodal biometrics that combines several biometric technologies is essentially more resilient to spoofing as impersonation; however, it would require more efforts and more resources [4]. Biometric security concerns with regard to 'wolves' are further discussed in Section 6 on 'liveness' detection. There is also a hybrid approach that seeks a trade-off between 'goats' exclusion and multimodal biometrics deployment [12].

In addition, to cater for biometric data with a low level of stability, accurate recognition often necessitates a request for multiple input samples during enrolment [15] which may

reduce the convenience aspects of the system. Thus, it would be ideal if the user's reference model are updated regularly [3] considering changes of biometrics data to due aging, health issues, etc. It is most likely for these counter measures to incur extra costs that may not reflect well in the cost-benefit analysis. Nevertheless, such investments are expected and necessary, particularly when almost all information security technologies are subjected to an escalating chain of cause and effect issues.

5. **Robustness of a Biometric System to Actual Operating Environment.** Early deployment of biometric access control applications fall short of the 'robustness' characteristic with regard to the actual performance in the target operating environment [6]. The high system performances claimed by biometric manufacturers were often difficult to be realized in actual operating environments [53]. One of the possible reasons for this is that most test beds were conducted in controlled laboratory environments whereby subjects were supervised to interact well with the recognition systems that were sited in ideal environmental setups. Examples include a voice recognition system which worked well with a quiet background, a facial recognition system that necessitated for a controlled ambient lighting conditions, and subjects who were trained to clean and place their fingers properly on the fingerprint scanners. However, such ideal conditions may not be available in actual target operating environments because of several reasons [6].

First, it is often difficult to enforce ideal human-machine interactions. Continuous close supervision is costly and defeats the purpose of automatic authentication, whereas instruction manuals are often neglected by users. Poor human-machine interactions may unnecessarily affect both Failure to Enrol (FTE) as well as Failure to Acquire (FTA) rates. The system performance is further degraded when FTA is mistakenly identified as False Reject Rate (FRR) [9]. New deployment of a biometric technology is similar to the introduction of any other systems [16] whereby it will often take a while for the general users to get accustomed to it. Thus, it is highly recommended that proper information security policies and procedures are in place to ensure that biometric users are closely guided in interacting with the system, particularly throughout enrolment and the initial stage of recognition. This in turn may inculcate the ideal user conducts which are desirable in maintaining the accuracy and convenience aspect of using biometric systems. However, such a scenario may only be effective for biometric systems which are used frequently by the users such as physical access control to work places which results in 'habituated' user population [16]. On the other hand, systems which are not frequently used may necessitate regular user supervision and training. For example, automatic kiosks at Malaysian Employee Provident Fund are incorporated with user-friendly GUI that guides users step-by-step in using the biometric authentication system. Though the system takes several minutes to process an individual user's request, it saves cost by reducing expensive human labour. Furthermore, it is still a faster information retrieval mechanism compared to traditional manual verification carried out at the counter.

Apart from the issue of variability in user conducts, actual operational setups may also contain a wide spectrum of possible 'noises' and interferences which makes extraction of a salient set of features a difficult task [2-4,6]. Such a condition may produce ambiguities in biometric template that hinder accurate recognition. For example, dusts dropped on optical fingerprint scanners may degrade the quality of the images resulting in a higher Failure to Acquire (FTA) rate. Also, facial recognition systems that are based on conventional cameras are also badly affected by problem of illumination. The communication networks which are used in telephony services often introduce undesirable noises that affect the accuracy of voice verification systems.

Early biometric system deployments were engineered with the focus of getting the system 'workable'. However, the increased concerns over robustness of biometric systems particularly with regard to the adverse actual operating environments has somewhat led to the improvement in the system design through various research efforts. These improvements are targeted at different levels of biometric processes ranging from the capture device, pre-processing, feature extraction and matching algorithm. For example, infra-red cameras are introduced in facial recognition in which images are not affected by ambient or incident lights [17]. In addition, a pre-processing module that performs illumination normalization is proposed in similar applications which are more backward compatible with the existing cameras [18]. Optimization efforts on the feature extraction and modelling modules have produced high level of recognition accuracy on the legacy system which is capable of handling a wide variation in pose, illumination and expression. A recent work on facial recognition system has addressed the possibility of occlusions such as those that wear sunglasses, and scarves by iteratively recovering the facial features.

In other domains such as in palm-print recognition, robust features have been introduced that are claimed to be invariant to different hand translations and scanner rotations [19]. Recent research work in hand geometry recognition has also demonstrated good performance despite using low quality images by optimizing both the image segmentation and feature extraction modules [20]. In speaker recognition, a more robust feature estimation mechanism has been proposed to maintain the accuracy rate under noisy environment which can withstand up to 15dB of the signal to noise ratio [21]. Also, a multimodal biometric approach is proposed recently in literature which compensates the limitation of both face and finger veins recognition systems in discriminating images of low resolution.

Regardless of these improvements, the question remains as to what extent have the proposed techniques been integrated in commercial access control applications and whether the improved systems have been tested using reliable data that reflects the actual target operating environment. The first argument essentially refers to the technology transfer rate taken to materialize the research design which may be affected by other issues such as feasibility, complexity, backward compatibility and additional costs incurred. The latter is imperative since any test conducted in laboratories would usually inherit some level of 'controlled' properties, especially if the test is not conducted by a certified independent third party. Issues on reliable biometric system testing and reporting are deliberated further in Section 8. Recent report by A. K. Jain et al. [6] highlighted that robustness to various operating environment still remains one of the prime technical challenge for the next biometric generation.

6. **The Need for 'Liveness' Detection in Capture Devices.** The elements of adversarial testing in biometric were initially neglected in the first biometric generation, except for certain technologies such as in signature verification. To better understand this scenario, it is necessary to recapture the history of biometric systems themselves. The role of human signatures in authentication has long been established even before the introduction of biometric systems [22,23]. Since then, signature forgery is a vulnerability that remains a forensic challenge particularly in establishing the authenticity of questioned documents in courts [22,23]. Hence, when automatic signature verification system was introduced to the market, it was only natural to test the system with forged signature samples of closed resemblance in order to investigate its accuracy with regard to False Accept Rate (FAR). Several signature databases are available for testing and reporting of skilled forgery detection, amongst which include Sigma [13] and GPDS [21]. In addition, there are also research efforts to automatically synthesize forged handwritten specimens [26] mainly to overcome the limitation of naive forgers in producing reliable forgery samples.

Similar adversaries-based test databases were hardly presented in evaluating the performance of other first generation biometric technologies such as those which are based on fingerprint, hand geometry, face and iris scanning [6]. A possible explanation for this is that unlike signature forgery which has long existed, spoofing methods to other types of biometric technologies have just been recently introduced, hence the issue was overlooked. The adversarial issue was probably compounded due to the assumptions those biometric traits are highly unique and consistent across the user population, thus are supposed to be fool-proof. This implies that spoofing efforts are supposed to be difficult, unlike human signature counterparts which can be easily forged.

For other types of biometrics, most initial test procedures on the investigation of the system's False Accept Rate (FAR) were carried out based on 'zero effort' attacks [2], i.e., those that tend to compare the biometric samples of other legitimate users with the claimed reference model. It was only after the initial deployment of the biometric systems that the counter attacks using fake or dummy artefacts appeared. For example, Matsumoto et al. [27] successfully fooled several commercial fingerprints optical and capacitive scanners by using moulded artificial fingers made from inexpensive gelatine. In addition, Thalheim et al. [28] were able to outwit capacitive fingerprint scanner by using simple breathing technique upon the fingerprint traces left on the sensor's surface. They also reported an almost 100% False Accept Rate (FAR) by dusting graphite over platen residues and stretching an adhesive strip over latent prints with applied pressure, a technique which was devised from the existing fingerprint forensic investigation. Their efforts to fool both face and iris recognition systems were also successful, just by using static copies of iris and face captured images. Indeed early biometric systems were not as secure as they were assumed to be, and worse still, they could be deceived easily through simple spoofing techniques.

The cause of biometrics were further harmed with the adverse news in 2005 in Malaysia when a man's index finger was severed by carjackers in their attempt to disable the car's immobilizer which uses fingerprint verification [29]. This gives credence to the users' anxiety over their safety with biometric systems. Since biometric market is projected to experience a steady growth rate [7], it is of paramount importance to ensure the safety of biometric users as well as to further secure the system from spoofing. In information security access control applications, a successful spoofing attempt may result in an impostor gaining access to IT infrastructures, filing documents, user's accounts, etc. that risk confidentiality, integrity and availability of information.

There are now increased research efforts in 'liveness' detection which aims at identifying fake or 'dead' copies of biometric samples. Such detection can be incorporated either at the data acquisition stage or at the pre-processing stage [30]. For example, Tan et al. [31] explored the various imaging variability between a webcam's captured facial images of live human samples and photographs in order to improve static facial recognition system against photo spoofing attempts. The proposed mechanism has the advantage of backward compatibility with existing webcam-based capture devices and static facial recognition; however, it may still be vulnerable under improved adversary photography techniques. Others have opted for a dynamic approach instead in which authentication is based on a sequence of captured images or video [32,33]. Here, the proposed 'liveness' detection techniques include analysing the small involuntary movements of the face [32] as well as the eye-blinking properties [33]. Recent advances in audio-video biometric include checking the video lip movements in addition to the correlated audio-lip features in establishing the identity of an individual [34].

Similarly, in the fingerprint recognition domain, there has been research in incorporating the 'liveness' detection by analysing and exploiting different characteristics inherent within

live and fake fingerprint images [35,36]. For example, Jin et al. [35] proposed spectral features of the ridges which are distinct between the two groups of samples. On the other hand, Choi et al. [36] utilised pore spacing and residual noise features for dummy detection. Both techniques are more compatible with existing systems in which authentication is largely based on static images. In addition, there has also been a move towards dynamic fingerprint recognition which is capable of extracting the skin elasticity information that is not inherent in fake artefacts [37].

A different approach at data acquisition level involves detection and analysis of the blood flow which provides for live finger detection [38]. Such a technique necessitates additional or different input capture devices which can be costly for system migration. However, for hand vein recognition system, it is easier and cheaper to incorporate similar detection by further analysing the captured vein images for vital signs of 'liveness' such as oxygen saturation and heart beat [39]. Recent advances in the research domain of iris recognition have also resulted in passive and active anti-spoofing methods. The former analysed the wavelength illumination reflection on the iris [40-42] whilst the latter studied the dynamics of the pupil reacting to changes in the ambient lighting [41,42]. Many researchers have opted for a hybrid approach that combines both methods for increased security against impersonation [41,42].

Jain et al. [6] highlighted that 'liveness' detection remains a technical challenge for the second generation of biometric systems many of which are still in the research domain [6,30], while several early products with liveness detection have been defeated by advanced spoofing attempts [28,43]. Toth [30] argued that amongst the trade-offs include cost and user's convenience which may negate its actual implementation. Since security controls often have limited life time [30] particularly with the rapid advancements in spoofing methods, it is imperative that the research and development in this domain is proactive and always be at the forefront of the technologies. Manufacturers should view spoofing as a serious threat and make dedicated efforts to incorporate suitable counter measures in their products.

7. **Security of Biometric Data within the System.** A biometric system is basically a digital system made up of vulnerable components such as capture devices, communication channels and databases which are subjected to a wide spectrum of replay attempts and other forms of adversary attacks. Once the biometric sample is captured in the access control application, the digital biometric representation can be intercepted and misused to provide for illegitimate authentication. Since biometric information describes a person, it is unlikely to be reset or reproduced should it be compromised unlike passwords or smartcards. Hence, the protection of the biometric data itself is of utmost importance, in order to allay anxiety among users over the privacy of their biometrics data. Acceptance of the system is also influenced by the security measures implemented on the biometric data [5,6,44,47,48].

There are different types of adversary attacks depending on the localization of the occurrences, one of which includes attacks at the internal interfaces of a biometric system's modules which can be carried out via a jammer on the communication media [44] or via eavesdropping snooping tools attached to the USB ports that connect capture devices with the system [28]. An effective counter measure to this vulnerability is to provide for secure communications through encryptions. However, encryptions alone do not guarantee protection against replay attacks; hence, it must be coupled together with other validation methods such as time stamps [44] or challenge-response interactions [28,44].

Another biometric system vulnerability is related to possible attacks on the template databases. There have been reports on the reconstruction of the original biometric data

from the unprotected biometric template [45,46]. Nevertheless, research efforts in developing robust and effective biometric template protection schemes synonym to the passwords' identity management counterparts have also increased [47-51]. On this note, the ISO JTC1 subcommittee 27 has also issued a working draft on biometric template protecting scheme [52] which highlights several important aspects in its framework that includes 'irreversible', 'unlinkable' and 'renewable'.

Securing a biometric template essentially involves encryption with irreversibility properties [44,47-52], making it difficult for hackers to compute or deduce the original biometric information from secure template. Another essential criterion for each generated biometric template is called 'unlinkable' which emphasizes on its uniqueness [44-48]. This is important in order to increase security aspects particularly because the same biometric characteristics may be used to identify an individual in different applications. For example, assuming that the same scheme is applied for two different fingerprint biometric applications, one which grants physical access to a secure building where the biometric template is stored on a smartcard, while another performs authentication with a centralized database that provides administrative privileges to an account. Should a hacker manage to retrieve a legitimate biometric template from a stolen smartcard, he will not be able to use this template to gain access to the user's account, though both verifications may be based on the same biometric index finger of the user.

The third criterion refers to the 'renewable' aspect, emphasizing on the ability to reproduce another template should the existing one be compromised [44,47,48-52]. 'Renewable' essentially requires for revocability property that would allow a biometric template to be reissued in a similar manner that a lost or stolen smartcard is reproduced. This characteristic is also closely linked to the cancellable property which assists in the deactivation of the compromised template without affecting its new replacement [49-51].

Both 'renewable' and 'unlinkable' characteristics can be achieved through 'salting' techniques [44]. This is synonymous to the password protection approach that seeks to differentiate stored passwords belonging to different users even if they coincidently tend to choose the same combination of letters. 'Salting' basically adds random unique generated data known as 'salt' to the original information making it distinct from the others, where such a process often takes place prior to encryption. In addition, 'hashing' method is equally effective [44,47,48] provided that a different permutation is applied with each template generation. Hashing is essentially an encryption technique that scrambles the data based on permutation algorithm. Different permutations ensure the uniqueness of templates despite using the same input biometric data.

Others [44,51] have added the 'performance' criterion for a good protection scheme, which basically describes the accuracy of the system with regard to both False Accept Rate (FAR) and False Reject Rate (FRR). It is a technical challenge to design a protection scheme which meets all the previously mentioned characteristics whilst maintaining the same error rate. This is mainly due to the random attributes of encryption algorithms that make accurate matching of protected template a difficult task. This problem is more prevalent in biometrics compared to the password counterparts [44,47-49]. Unlike passwords which are of absolute nature, all biometrics suffer from some level of variability [2,4] either due to the attributes of the biometric data itself, or due the variations which occur during the capturing process of the biometric samples. Hence, care must be taken in selecting the suitable encryption algorithm since some may amplify the small variations inherent in an individual's biometric data leading to a higher value of False Reject Rate (FRR).

On the other hand, a loose protection scheme with a high level of tolerance to the intra user variability may not possess the ideal 'unlinkable' property possibly resulting

in an increased False Accept Rate (FAR). In addition, wide-scale applications may pose greater challenges in the designs of encryption algorithms with distinct capabilities whilst satisfying the performance requirements [44]. Matching using the original biometric templates that have been decrypted is more accurate; however, it is somewhat impractical. It defeats the security purpose by leaving the original biometric template vulnerable within the matching module [44].

8. **Concerns over Biometric System Testing and Reporting.** The test results on biometric systems' performance as reported by the manufacturers can be rather controversial. The results on the accuracy of the first generation biometrics are usually overoptimistic which may not be realised in practice [53,54]. Early tests were often carried out by vendors and manufacturers themselves on a limited number of subjects under controlled laboratory conditions. Most subjects were selected and trained to interact in an ideal way with the devices; therefore, many errors such as unreadable, dirty thumbs or thumbs which were placed wrongly on the scanners were not reflected in the test figures. Several reports [53,54] have highlighted the concerns over a high level of Failure to Enrol (FTE) exhibited in the early tested products. However, both FTE and Failure to Acquire (FTA) rates which are amongst the two crucial parameters in information security policy and decision making have been rarely reported by the manufacturers. Failure to do so gives wrong impressions on the universality and convenience aspects of using the biometric systems that would cost organisations substantial financial loss due to ineffective solutions.

There is also no validation on the results over tampering attempts which occur because there is no proper control over the testing procedures. This leaves the results exposed to manipulation by overzealous parties in marketing the products. Toth [30] highlighted the importance of using a reliable independent testing mechanism in investigating the effectiveness of 'liveness' detections as claimed by the manufacturers. The testing results run by independent third party must also be repeatable and accessible which should focus not just on the system accuracy, but also on other performance characteristics such as on operating speed and level of interoperability [55].

In order to provide independent views, government agencies of certain countries have taken the necessary initiatives to launch national programmes on biometric product validation and verification. For example, the US National Institute of Standards and Technology (NIST) though the US Biometric Consortium has conducted a series of independent test and evaluation on application of biometric-based personal identification technology whereby the results were mostly made available to the general public [56]. NIST testing results are often used as references particularly for wide scale applications since the systems are tested on large databases comprising up to millions of subjects.

Similar efforts have been carried out in Europe with the foundation of BioTesting Europe [55], an initiative funded by the European Commission to provide objective performance characteristics of biometrics products. In the UK itself, there are efforts to establish common ground rules on biometrics testing. In February 2000, the UK Government's Biometric Working Group has published a document to guide best practices in the testing of biometric devices. This is followed by a revised version released in 2002 [57]. According to this guide, there are three basic types of evaluation of biometrics systems namely:

- **technology evaluation**

  The goal of technology evaluation is to compare competing algorithms from a single technology, where all tests will be carried out using an offline-processing mode on a standardised database collected by a universal sensor.

- **scenario evaluation**
  The goal of scenario evaluation is to determine the overall system performance in a prototype or simulated application, where all tests will be carried out in an environment that models a real world target application of interest.
- **operational evaluation**
  The goal of operational evaluation is to determine the performance of a complete biometric system in a specific application environment with a specific target population using online processing mode.

The Biometric Working Group itself has conducted a series of tests on a range of commercial devices using its proposed standardised procedure. The results of the first test were released in March 2001 [54]. The system performances are characterised in terms of False Acceptance Rate (FAR), False Rejection Rate (FRR), Failure to Enrol (FTE) Rate and Failure to Acquire (FTA) Rate. There is also independent testing of biometric solutions run by biometric consultants such as the International Biometric Group [53] which is based in the United States. Government agencies of other countries such as Japan, Korea and China have also established similar testing programmes particularly on their biometric products.

Due to the globalization of biometric market, there has been an increased need for international standards on biometric. As a result, SC 37 subcommittee on Biometric was formed in 2002 as part of the ISO/IEC joint technical committee. The subcommittee is currently drafting the guidelines for testing methodologies on operational evaluation. A standard [10] has also been published on grading and testing of biometric access control applications which emphasizes on the importance of publishing the details of testing procedures, physical layout of test environment, demographic of test crew, performance results and representative examples of the data set. Among other recommendations include that the minimum crew size should be set to 200, crew members should be sufficiently trained during enrolment whilst the demographics of the crew shall be controlled in terms of gender and age.

In the product selection process, it is of paramount importance to consider solutions which meet the operational requirements that include system performance with regard to FTE, FTA, FAR and FRR as well as other characteristics such as throughput, and database capacity. It is also imperative to validate the testing results claimed by the manufacturers and vendors. A simpler means to this effect is to test results verification against those that have been carried out by independent third parties, or based on the testing conformance to established standards. However, the former is currently limited to well-known products available mostly in the west, whilst the ISO standards have just been released and may not have been applied in the early product testing.

9. **Assurance of Interoperability.** An ideal biometric-based authentication system must also ensure interoperability across different platforms and devices which can be achieved through conformance to biometric standards [6]. Early deployment of biometrics systems with mainstream PC technology was problematic due to lack of standards. However, nowadays standards have become business strategies. Conformance to standards creates new markets and increases competitiveness of biometric products. Currently, there is an increased activity of biometrics industry standards and related activities to support the expansion of the marketplace for biometric. Standards assure the availability of multiple sources for comparable products which prevent the sole source lock-in by vendors. Standards also reflect the maturity of biometrics technologies which have advanced rapidly since the early 1990s.

The purpose of a standard is to allow for interchange capability and interoperability; thus, reducing risk to the clients for future upgrades and expansions [6,58]. The proposal of standards through creation of common Application Program Interfaces (APIs) allows for software interactions independent of products from different vendors. This in turn provides modularity which assists in easy substitution of biometrics technologies, simple integration of multiple biometrics using the same interface and rapid extension of biometrics across multiple extensions. In addition, APIs also allow biometrics software developers to write programs without even selecting the particular biometrics devices that they are going to use.

Early biometric standards include Human Authentication API (HA-API) [59] which provides a generalized interface between biometrics applications and the technologies. HA-API was initially developed for the guidelines of US Department of Defence (DoD); nevertheless, it has now been made available to the public. Another API is Biometric Authentication API (BAAPI) developed by True Touch Technologies [60]. In principle, both BAAPI and HA-API serve the same objectives; however, BAAPI provides for additional Biometric Hardware Abstraction Layer. A new set of Data Link Layers (DLLs) is proposed in BAAPI that hides the actual device dependent calls. This in turn, assists in the software development process by eliminating the needs to specify the device during the design of the application. In addition to generic biometric API, there is also Speaker Verification API (SVAPI) developed under the sponsorship of Novell Corporation which is more biometrics type-specific [57].

The wide variety of biometrics methods, devices, algorithms and applications has led to different views on the best standard architecture. In 1998, a number of separate application level initiatives were brought together in the US BioAPI Consortium. This organization includes different biometrics companies, integrators and user communities. It has released two versions of the BioAPI which include 'best of breed' features from HA-API, and BAPI. The former version which is BioAPI 1.1 is developed for the US National Institute of Standards and Technology (NIST). The latter version (i.e., BioAPI 2.0) is developed for the International Organization for Standardization (ISO).

In January 2001, the collaboration between US National Institute of Standards and Technology (NIST) and US Biometric Consortium published a standardised format for exchange of biometrics data [64] called Common Biometric Exchange File Format (CBEFF). It describes a set of data elements necessary to support biometrics technologies which is independent of application.

With the establishment of ISO/IEC subcommittee 37 (i.e., SC37) on Biometrics under Joint Technical Committee 1 (i.e., JTC1) in 2002, new standards are under development, several have been published whereby a couple are based on BioAPI and CBEFF [58]. The SC37 is divided into six working groups (WG) addressing different aspects as follows:

- biometric vocabulary (WG1)
- data exchange infrastructure and application programming interface (WG2)
- data interchange formats (WG3)
- related applications profiles (WG4)
- performance evaluation (WG5)
- cross-jurisdictional and societal aspects (WG6).

The combination of work by all the working groups provides a holistic standardization approach to biometric systems.

10. **Discussions.** Physical and logical access controls are amongst the most important protection schemes in information security. Traditional approaches to access controls include smartcard and password authentication. However, with the increased threats

on information security, there has been increased need for biometric-based authentication systems. Such applications have also been spurred by the advances in biometric technology coupled with the cost reduction of biometric capture devices.

Despite various claims on increased security provided by the biometric based authentication system, current technologies are still beset with limitations particularly in terms of robustness with regard to the variations in the actual operating environment. Like any other control measures, biometric systems are also subjected to an escalating chain of cause and effect issues. The deployment of biometric system has led to the proliferation of new spoofing techniques using fake or dead artefacts, which calls for incorporation of 'liveness' detection in biometric system. New techniques and algorithms have been proposed to overcome both limitations; however, they are largely in research domain and are mostly not available commercially. The proposed spoofing countermeasures and robust optimization approaches often incur additional costs whereby some may even affect user convenience which hinder their implementations.

Security of biometric data within the system is also a big concern. Like any other digital systems, biometric information of an individual can be intercepted and reused in illegitimate authentication attempts. Hence, it is necessary to ensure that both the communication channels and biometric templates are secure, which can be achieved through encryption techniques. Proper design of biometric template protection scheme also enables a compromised template to be revoked and replaced, which will increase public confidence and acceptance of the system.

Different biometric systems differ in the underlying technologies, complexities and performances. Each biometric technology has its own strengths and limitations. Several technologies may be adversely affected by the user group of 'goats', 'lambs' and 'wolves' of biometric menagerie. This in turn may affect the system's False Reject Rate (FRR) and False Accept Rate (FAR) respectively resulting in ineffective access control solutions. There is also no ideal biometric system which meets all the performance criteria; thus, a trade-off between FRR and FAR is often sought based on the security needs. A detailed study on the risk management, which takes into consideration the effect of biometric menagerie on different technologies, is imperative in specifying the requirements of the access control application and identifying the right biometric solution.

Apart from FAR and FRR, it is important to clarify the Failure to Enrol (FTE) and Failure to Acquire (FTA) rates as it reflects the universality and the convenience aspects of using the system respectively. A high value of FTE also highlights the need for alternative measures for access control to cater for those users who cannot be authenticated through the biometric system.

In biometric product selection process, it is important to validate the performance claimed by the manufacturers and vendors. A recommended step to this effect is to validate the claimed testing results against those that have been carried out by independent third parties. An organization should also prioritise products that conform to established standards such as those produced by the ISO/IEC JTC1 SC37 as they ensure interoperability across different devices and platforms. This consideration is important to facilitate the upgrading process and mitigate the risk of obsolescent.

11. **Conclusions.** This paper presents a holistic view on current technical issues and challenges of biometric systems as physical and logical access control tools in information security. Each topic is discussed in terms of the effects on various biometric system performances which are deliberated across individual sub-components of biometric system architecture. Amongst the identified issues include (1) the effects of biometric menagerie (2) robustness of the system to actual operating environment (3) the need for 'liveness'

detection (4) security of biometric data within the system (5) concerns over biometric system testing and reporting and (6) assurance of interoperability. These issues can be used as guidelines by the industries with regard to information security policy and decision making. In the future, as the target access control user population increases, we foresee the need for scalable biometric authentication. In addition, biometric-based access control applications may necessitate for ambient intelligence whereby authentication can be carried out on the fly without the need for active user participation. In short, both aspects remain as two technical issues to be studied and addressed in our future work.

REFERENCES

[1] *ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management*, International Organization for Standardization, 2005.

[2] A. K. Jain, A. Ross and S. Pankanti, Biometrics: A tool for information security, *IEEE Transactions on Information Forensics and Security*, vol.1, no.2, pp.125-143, 2006.

[3] K. A. Rhodes, *Information Security: Challenges in Using Biometrics*, United States General Accounting Office, 2003.

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

[5] S. Prabhakar, S. Pankanti and A. K. Jain, Biometric recognition: Security and privacy concerns, *IEEE Security and Privacy*, vol.1, no.2, pp.33-42, 2003.

[6] A. K. Jain and A. Kumar, Biometrics of next generation: An overview, *The 2nd Generation Biometrics*, 2010.

[7] *Biometric Market and Industry Report 2009-2014*, International Biometric Group, 2008.

[8] M. Thomas, Is Malaysia's MyKad the 'one card to rule them all'? *Melbourne University Law Review*, vol.28, no.2, 2004.

[9] S. Kim, Governance of information security: New paradigm of security management, *Computational Intelligence in Information Assurance and Security, Studies in Computational Intelligence*, vol.57, pp.235-254, 2007.

[10] *ISO/IEC 19795-5:2011, Information Technology – Biometric Performance Testing & Reporting – Part 5: Access Control Scenario and Grading Scheme*, International Organization for Standardization, 2011.

[11] N. Yager and T. Dunstone, The biometric menagerie, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.32, no.2, pp.220-230, 2010.

[12] N. Poh and J. Kittler, A methodology for separating sheep from goats for controlled enrolment and multimodal fusion, *Proc. of the Biometric Symposium*, Tampa, FL, USA, pp.17-22, 2008.

[13] S. M. S. Ahmad, A. Shakil, M. A. Faudzi and R. M. Anwar, Analysis of 'goat' within user population of an offline signature biometrics, *Proc. of the 10th International Conference on Information Science, Signal Processing and Applications*, Kuala Lumpur, Malaysia, pp.765-769, 2010.

[14] A. Kumar, V. Kanhangad and D. Zhang, A new framework for adaptive multimodal biometrics management, *IEEE Transactions on Information Forensics and Security*, vol.5, no.1, pp.92-102, 2010.

[15] S. M. S. Ahmad, A. Shakil and M. A. M. Balbed, Study on the effects on the number of training samples on HMM based online and offline signature verification system, *Proc. of the International Symposium on Information Technology*, Kuala Lumpur, Malaysia, 2008.

[16] J. Wayman, A. K. Jain, D. Maltoni and D. Maio, An introduction to biometric authentication systems, *Biometric Systems*, pp.1-20, 2005.

[17] P. Buddharaju, I. Pavlidis and C. Manohar, Face recognition beyond the visible spectrum, *Advances in Biometrics*, pp.157-180, 2008.

[18] S. Aly, A. Sagheer, N. Tsuruta and R. Taniguchi, Face recognition across illumination, *Artificial Life and Robotics*, vol.12, no.1, pp.33-37, 2008.

[19] G. S. Badrinath and P. Gupta, Robust biometric system using palmprint for personal verification, *Lecture Notes in Computer Science*, vol.5558, pp.554-565, 2009.

[20] J. Montalvão, L. Molina and J. Canuto, Robust hand image processing for biometric application, *Pattern Analysis & Applications*, vol.13, no.4, pp.397-407, 2010.

[21] N. Wang, P. C. Ching, N. Zheng and T. Li, Robust speaker recognition using denoised vocal source and vocal tract features, *IEEE Transactions on Audio, Speech, and Language Processing*, vol.9, no.1, pp.196-205, 2011.
[22] R. C. Park, Signature identification in the light of science and experience, *Hasting Law Journal*, vol.59, pp.1101-1158, 2008.
[23] K. M. Koppenhaver, *Forensic Document Examination, Principles and Practice*, Humana Press, Totowa, New Jersey, 2007.
[24] J. Ruiz-del-Solar, C. Devia, P. Loncomilla and F. Concha, Offline signature verification using local interest points and descriptors, *Progress in Pattern Recognition, Image Analysis and Applications, Lecture Notes in Computer Sciences*, vol.5197, pp.22-29, 2008.
[25] M. Freire, J. Fierrez, M. Martinez-Diaz and J. Ortega-Garcia, On the applicability of off-line signatures to the fuzzy vault construction, *Proc. of the 9th International Conference on Document Analysis and Recognition*, Paraná, Brazil, pp.1173-1177, 2007.
[26] L. Ballard, F. Monrose and D. Lopresti, Biometric authentication revisited: Understanding the impact of wolves in sheep's clothing, *Proc. of the 15th USENIX Security Symposium*, Vancouver, Canada, pp.29-41, 2006.
[27] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, Impact of artificial 'gummy' fingers on fingerprint systems, *Proc. of SPIE Optical and Counterfeit Deterrence Techniques*, San Jose, CA, USA, pp.275-289, 2002.
[28] L. Thalheim, J. Krissler and P.-M. Ziegler, Body check: Biometric access protection devices and their programs put to the test, *c't Magazine*, 2002.
[29] S. A. Shaikh and C. K. Dimitriadis, My fingers are all mine: Five reasons why using biometrics may not be a good idea, *Proc. of the International Symposium on Biometrics & Security Technologies*, Islamabad, Pakistan, 2008.
[30] B. Toth, Biometric liveness detection, *Information Security Bulletin*, vol.10, pp.291-297, 2005.
[31] X. Tan, Y. Li, J. Liu and L. Jiang, Face liveness detection from a single image with sparse low rank bilinear discriminative model, *Lecture Notes in Computer Science*, vol.6316, pp.504-517, 2010.
[32] K. Kollreider, H. Fronthaler and J. Bigun, Non-intrusive liveness detection by face images, *Image and Vision Computing*, vol.27, no.3, pp.233-244, 2009.
[33] L. Sun, G. Pan, Z. Wu and S. Lao, Blinking-based live face detection using conditional random fields, *Lecture Notes of Computer Science*, vol.4642, pp.252-260, 2007.
[34] G. Chetty and M. Wagner, Biometric person authentication with liveness detection based on audio-visual fusion, *International Journal of Biometrics*, vol.1, no.4, pp.463-478, 2009.
[35] C. Jin, H. Kim and S. Elliott, Liveness detection of fingerprint based on band-selective fourier spectrum, *Lecture Notes of Computer Science*, vol.4817, pp.168-179, 2007.
[36] H. Choi, R. Kang, K. Choi and J. Kim, Aliveness detection of fingerprints using multiple static features, *International Journal of Biological and Medical Sciences*, vol.2, no.3, pp.200-205, 2007.
[37] J. Jia, L. Cai, K. Zhang and D. Chen, A new approach to fake finger detection based on skin elasticity analysis, *Lecture Notes in Computer Science*, vol.4642, pp.309-318, 2007.
[38] A. Kumar, Fingerprint spoof detection using blood flow analysis, *SPIE Newsroom*, 2009.
[39] B. Qin, J.-F. Pan, G.-Z. Cao and G.-G. Du, The anti-spoofing study of vein identification system, *Proc. of the International Conference on Computational Intelligence and Security*, Beijing, China, pp.357-360, 2009.
[40] S. J. Lee, K. R. Park and J. Kim, Robust fake iris detection based on variation of the reflectance ratio between the iris and the sclera, *Proc. of the Biometrics Symposium*, Baltimore, Maryland, 2006.
[41] A. Pacut and A. Czajka, Aliveness detection for iris biometrics, *Proc. of the 40th IEEE International Carnahan Conference on Security Technology*, Lexington, Kentucky, pp.122-129, 2006.
[42] R. Bodade and S. Talbar, Fake iris detection: A holistic approach, *International Journal of Computer Applications*, vol.19, no.2, 2011.
[43] D. J. Brooks, Assessing vulnerabilities of biometric readers using an applied defeat evaluation methodology, *Proc. of the 3rd Australian Security and Intelligence Conference*, Perth, Australia, pp.23-34, 2010.
[44] A. K. Jain, K. Nandakumar and A. Nagar, Biometric template security, *EURASIP Journal on Advances in Signal Processing*, 2008.
[45] R. Cappelli, A. Lumini, D. Maio and D. Maltoni, Fingerprint image reconstruction from standard templates, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.29, no.9, pp.1489-1503, 2007.

[46] A. Ross, J. Shah and A. K. Jain, From template to image: Reconstructing fingerprints from minutiae points, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.29, no.4, pp.544-560, 2007.
[47] B. Chen and V. Chandran, Biometric template security using higher order spectra, *Proc. of the IEEE International Conference on Acoustic Speech and Signal Processing*, Dallas, TX, USA, pp.1730-1733, 2010.
[48] X. Zhou, A. Kuijper and C. Busch, Template protection for 3D face recognition, *Face Recognition, InTech*, pp.315-328, 2010.
[49] A. B. J. Teoh, Y. W. Kuan and S. Lee, Cancellable biometrics and annotations on BioHash, *Pattern Recognition*, vol.41, no.6, pp.2034-2044, 2008.
[50] L. Leng, J. Zhang, M. K. Khan, X. Chen, M. Ji and K. Alghathbar, Cancellable PalmCode generated from randomized Gabor filters for palmprint template protection, *Scientific Research and Essays*, vol.6, no.4, pp.784-792, 2011.
[51] E. Maiorana, P. Campisi, J. Ortega-Garcia and A. Neri, Cancellable biometrics for HMM-based signature recognition, *Proc. of the 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems*, Arlington, VA, USA, 2008.
[52] J. Breebaart, B. Yang, I. Buhan-Dulman and C. Busch, Biometric template protection – The need for open standards, *Datenschutz und Datensicherheit*, pp.299-304, 2009.
[53] *Lessons Learned from Comparative Biometric Testing*, International Biometric Group, 2003.
[54] T. Mansfield, G. Kelly, D. Chandler and J. Kane, Biometric product testing final report, *Communications Electronics Security Group*, 2001.
[55] Towards European testing and certification of biometric components and systems, *BioTesting Europe*, 2008.
[56] NIST verification test shows security trade-off, *ID Newswire*, vol.2, no.15, 2003.
[57] A. J. Mansfield and J. L. Wayman, Best practices in testing and reporting performance of biometric devices, *UK Biometrics Working Group*, 2002.
[58] P. Grother, Biometrics standards, *Handbook of Biometrics*, pp.509-527, 2008.
[59] Interface specification human authentication – Application program interface, *US Biometric Consortium*, 1998.
[60] *TrueTouch Demonstrates Its Biometric Authentication Application Programmers Interface – BAAPI – At CardTech/Secur Tech.98*, http://www.thefreelibrary.com/TrueTouch+Demonstrates+its+Biometric+Authentication+Application...-a020547012, BusinessWire, 1998.
[61] S. H. Maes and H. S. M. Beigi, Open sesame! Speech, password or key to secure your door? *Lecture Notes of Computer Science*, vol.1351, pp.531-541, 1997.
[62] ANSI INCITS 358-2002, version 1.1 of the BioAPI specification, *US BioAPI Consortium*, 2002.
[63] ISO/IEC 19784-1: 2006, version 2.0 of the BioAPI specification, *US BioAPI Consortium*, 2002.
[64] F. L. Podio, J. S. Dunn, L. Reinert, C. J. Tilton, L. O'Gorman, M. P. Collier, M. Jerde and B. Wirtz, NISTIR 6529, *CBEFF – Common Biometric Exchange File Format*, 2001.
[65] Y. Li, Identifying legal concerns in the biometric context, *Journal of International Commercial Law and Technology*, vol.3, no.1, pp.45-54, 2008.
[66] M. Sutrop, Ethical issues in governing biometrics technologies, *Ethics and Policy of Biometrics Lecture Notes in Computer Science*, vol.6005, pp.102-114, 2010.
[67] A. Sprokkereef and P. De Hert, Ethical practice in the use of Biometric identifiers within the EU, *Law Science and Policy*, vol.3, pp.177-201, 2007.
[68] C. Prins, Making our bodies work for us: Legal implications of biometric technologies, *Computer Law & Security Report*, vol.14, no.3, pp.159-165, 1998.
[69] E. Mordini and C. Pertrini, Ethical and social implications of biometric identification technology, *Ann 1st Super Sanita*, vol.43, no.1, pp.15-11, 2007.
[70] K. Michael and M. G. Michael, The social, cultural, religious and ethical implications of automatic identification, *Proc. of the 7th International Conference in Electronic Commerce Research*, Dallas, TX, USA, pp.433-450, 2004.

This paper discusses the technical issues and challenges faced by biometric technologies within the physical and logical access control applications of information security. The discussion includes concerns on the system performances with regard to robustness to the actual operating environment and recognition capability of different biometric traits. It also addresses various security threats which include spoofing and replay attacks. In addition, this paper highlights the challenges in interoperability as well as needs for reliable testing and reporting. The overall discussions provide imper Applications as access control tools of information security. Sharifah Mumtazah Syed Ahmad, Borhanuddin Mohd Ali. and Wan Azizun Wan Adnan Faculty of Engineering Universiti Putra Malaysia 43400, UPM, Serdang, Selangor, Malaysia { s mumtazah; borhan; wawa }@eng.upm.edu.my. Received July 2011; revised December 2011. Abstract.Â This paper discusses the technical issues and challenges faced by biometric technologies within the physical and logical access control applications of information security. The discussion includes concerns on the system performances with regard to robustness to the actual operating environment and recognition capability of diï¬€erent biometric traits. The security of biometric authentication data is of vital importance, even more than the security of passwords, as passwords can be easily changed if exposed. A fingerprint or retinal scan, however, is immutable. Disclosure of this or other biometric information can put users at permanent risk and create significant legal exposure for the company that loses the data.Â In the event of a breach, it creates an enormous challenge because physical assignments, such as fingerprints, cannot be replaced. Biometric data in the hands of a corrupt entity also has very frightening but real implications. Ultimately, every company is responsible for its own security decisions. Law enforcement biometrics are referring to applications of biometric systems that support law enforcement agencies. This category can include criminal ID solutions such as Automated Fingerprint (and palm print) Identification Systems (AFIS).Â They are challenged and sometimes put on hold. Read California bans law enforcement from using facial recognition. #2 Military - Know your enemy.Â In IT, biometric access control can be a complementary userâ€™s authentication factor and supports organizationsâ€™Identity and Access Management (IAM) policies. Unlike codes, static passwords, one-time passwords, or access cards that rely on data that can be forgotten or lost, biometric authentication is based on who people are (and not what they have). Biometrics are body measurements and calculations related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological characteristics, which are related to