MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

Signal Processing for Biometric Systems (DSP Forum)

Anil K. Jain, Rama Chellappa, Stark C. Draper, Nasir Memon, P. Jonathan Phillips and Anthony Vetro

TR2007-071 November 2007

Abstract

This IEEE Signal Processing Magazine (SPM) forum discuses signal processing applications, technologies, requirements and standardization of biometric systems. The forum members bring their expert insights into issues such as biometric security, privacy, and multi biometric and fusion techniques. The invited forum members are Prof. Anil K. Jain (Michigan State University), Prof. Rama Chellappa (University of Maryland), Dr. Stark C. Draper (University of Wisconsin-Madison), Prof. Nasir Memon (Polytechnic University), and Dr. P. Jonathan Phillips (National Institute of Standards and Technology). The moderator of the forum is Dr. Anthony Vetro (Mitsubishi Electric Research Labs and associate editor of SPM).

IEEE Signal Processing Magazine

Anil K. Jain, Rama Chellappa,
Stark C. Draper, Nasir Memon,
P. Jonathon Phillips, and Anthony Vetro

Signal Processing for Biometric Systems

This *IEEE Signal Processing Magazine (SPM)* forum discusses signal processing applications, technologies, requirements, and standardization of biometric systems. The forum members bring their expert insights into issues such as biometric security, privacy, and multibiometric and fusion techniques. The invited forum members are Prof. Anil K. Jain (Michigan State University), Prof. Rama Chellappa (University of Maryland), Dr. Stark C. Draper (University of Wisconsin-Madison), Prof. Nasir Memon (Polytechnic University), and Dr. P. Jonathon Phillips (National Institute of Standards and Technology). The moderator of the forum is Dr. Anthony Vetro (Mitsubishi Electric Research Labs, and associate editor of *SPM*).

Our readers may agree or disagree with the ideas discussed next. In either case, we invite you to share your comments with us by e-mailing avetro@merl.com or SPM_columns_forums@yahoo.com.

Moderator: Biometric technology has seemed to mature in recent years. Are we getting close to the point where biometric applications will be an integral part of our everyday life (for instance, to access ATMs or conduct sensitive transactions online), or will the dominant applications continue to be in the area of access control (for instance, to obtain entry access in buildings and passport control)?

R. Chellappa: In the immediate future, I feel that biometric applications will be employed in workplace access control and airport access control. Overall, it is not clear if biometrics will have a big market outside the security, military, and law enforcement domains. This depends very much on whether the younger generation catches on to the idea of biometrics. I feel that we are in a phase where we have the technology but are looking for wider applications.

P.J. Phillips: Historically, one of the most well-known biometric technologies has been fingerprint recognition. For most of the last century, fingerprints were recorded and examined for law-enforcement applications and for common non-law-enforcement applications such as background checks. Since the events of September 11, 2001, fingerprints have been used in the US-VISIT system for incoming visitors to the United States.

Iris recognition technology has been deployed at border control points in the United Arab Emirates and has been proposed for maintaining identity integrity in the United Kingdom's national identity system.

While face recognition technologies in biometric applications have been less popular, human face recognition has long been used. For instance, to enter many government facilities a person must show a security guard an identification card or badge with a photo. Recent results show that face recognition algorithms are capable of outperforming humans on recognizing unfamiliar faces across illumination changes. Therefore, face recognition algorithms now have the potential to be incorporated into applications currently performed by humans. Results from the Face Recognition Vendor Test (FRVT) 2006 and Iris Challenge Evaluation (ICE) 2006 show that face recognition is capable of performance comparable to iris recognition for verification applications such as access control.

R. Chellappa: An interesting new application of face recognition that is related to what you just mentioned involves biometrics for passport renewal: facial images of an adult separated by ten years are compared for face matching and authentication purposes. I also recall that in the mid-1990s, face recognition algorithms were used in state offices for detecting potential abusers of welfare systems, but I do not know if these applications are still in effect.

S.C. Draper: To understand whether biometrics will diffuse into a wider range of applications, it is useful to decide how biometrics fit into broader technological categories. For instance, do biometrics complement or compete with public-key cryptography? Are biometrics good for low- or high-security applications? How appropriate are biometrics for centralized or peer-to-peer applications? Are biometric technologies more or less susceptible to important classes of attacks such as peer-to-peer worm attacks? All are important questions to be answered.

Moderator: What are the advantages of using biometric technologies and can/will they replace other technologies?

A.K. Jain: In some applications, biometrics can replace or supplement the existing technology. In others, it is the only viable approach (for instance, preventing multiple enrollments by an individual for obtaining government benefits, driver licenses, and passports). I think that ultimately the decision to add or replace existing personal recognition methods with biometrics-based

Digital Object Identifier 10.1109/MSP.2007.905886

solutions should be based on a cost-benefit analysis or return on investment. So far, this has been easier to justify in many mandated government applications in the United States and overseas (the already-mentioned US-VISIT program and the Hong Kong national ID card). But, it is being increasingly adopted in a number of commercial applications (e.g., access to Disney Parks in Orlando), albeit slower than anticipated.

The main advantages of a biometric system are as follows: 1) it offers greater security and convenience than traditional methods of personal recognition [credentials—ID cards, personal identification numbers (PINs), and passwords] and 2) it gives users greater convenience (no need to remember passwords) while maintaining sufficiently high accuracy and ensuring that the user is present at the point and time of recognition. However, widespread adoption of biometric technology will really depend on how secure biometric technologies are and the privacy implications of using biometrics.

N. Memon: I tend to believe that no matter how secure biometrics can be, they are more likely to complement existing security systems instead of replacing them. So I agree that it is important to find out where and how biometrics should be used.

To do that, we need to understand that biometrics have some intrinsic differences from other types of identification credentials. For example, biometrics cannot be forgotten. If we compare a system where everyone uses fingerprints (which can be left on car doors) and a system where everyone uses strong passwords (which can be written on a piece of paper beside the keyboard), it is hard to conclude which is better. If a company policy can be enforced such that no one should write down their passwords, a similar policy for fingerprints could be that everyone should wear gloves. Both appear to be quite ridiculous. But the point I am making is that the real question may be not whether they can be easily stolen, but how much we are willing to invest to protect them and whether they are worth the price, which in turn depends on the application scenario.

S.C. Draper: I believe that an application scenario that proves the unique capabilities of biometrics is needed. To allay widespread concerns about privacy and gain public support, the application must be one that is important to the individual and either is not possible with other methods or cannot be enforced with other methods. While government-mandated biometric requirements increase the market and need for biometric solutions, they do nothing to assuage the concerns of the public or increase the acceptability of biometrics.

Moderator: In addition to fingerprint and face recognition, what other technologies are available for biometric applications to date?

A.K. Jain: Human biometric traits can be classified into two main categories: anatomical (e.g., fingerprint, face, iris, hand geometry, ear, palmprint) and behavioral (e.g., signature, gait, keystroke dynamics). Voice or speech biometrics have both anatomical and behavioral components. Among the various biometric traits that have been proposed in the literature, I believe recognition systems based on fingerprint, face, iris, palm print, hand geometry, and speech have been most effective. New sensor technologies (e.g., multispectral and touchless for fingerprints, iris at a distance, iris on the move, whole hand imager that captures fingerprint, simultaneous palm print and hand shape) will improve the performance as well as usability of the biometric systems.

R. Chellappa: On the other hand, the only true remote biometric that is available is gait-based, working with which is still in its infancy. Gait analysis may be effective in surveillance applications, but further testing on larger data sets is needed to prove its effectiveness for person authentication.

Moderator: Effective protection of the biometric data and handling of privacy issues, high recognition accuracy, and usability are typically listed as requirements for biometric technologies and systems. Let us discuss each and outline the associated signal processing challenges. To begin with, why are we concerned with securing biometric systems and biometric data?

N. Memon: Although biometrics provide a simple and effective mechanism for authentication and/or identification, there is widespread concern about the dangers of using them in a ubiquitous and unchecked manner. These concerns mostly center on the security of biometric data and the privacy of individuals whose biometric data is captured. Security concerns stem from the fact that biometric data cannot be easily revoked or replaced. Once a biometric is compromised, it remains compromised forever. Privacy concerns arise from the fact that biometric data is so tightly bound to a person's identity. Hence, it can be used to track the activity and behavior of individuals and violate their privacy in ways that would be entirely unacceptable in most open societies. Despite that, there has been a lot of research done over the past few decades on developing techniques for capturing and matching biometric data, while security and privacy issues have received comparably less attention.

A.K. Jain: Like any security system, biometric systems are vulnerable to a variety of attacks. In fact, since biometrics are usually a component (embedded) in a security infrastructure (ID cards, alarms), even with the introduction of biometrics the existing security breaches are still possible.

Consider the iris recognition Teacher-Parent Authorization Security System (T-PASS) that was installed in New Egypt, New Jersey, a couple of years back to let parents and other authorized individuals into the school building, while keeping out unauthorized people without using up staff time to check identities. Although the iris biometric systems worked well and users were satisfied, a number of security issues came up that had to do with the personal behavior and habits of the users than any weakness in the biometric systems. Some users, after they were recognized based on their iris scans, held the door open for another person

entering the building behind them (scenario referred to as tailgating). Another problem involved some users who went outside the building during their breaks to take a walk or smoke and propped open a door behind them so they could get back into the building easily without using the iris system again.

Moderator: What are the main risks related to the security of biometric systems?

A.K. Jain: The risk of stolen biometrics and the risk of compromising a biometric template are some of the most publicized and frequently cited in relation to the security of biometric systems.

The former refers to the case when a hacker might use a very specific target and present the system with a copy of a known person's biometric sample. It has been reported that insiders commit about 80% of all cyber-crimes (an assessment based only on reported security breaches). In such cases, the individual breaching the system's security very likely knows an authorized user personally, can acquire a sample biometric (for example, a latent fingerprint), can make a duplicate [such as a three-dimensional (3-D) mold of the fingerprint], and present it to the biometric systems. But, this is not an easy process in practice. Although producing a gummy clone of an available real finger (from a consenting user) is relatively simple, reconstructing a fake finger from a latent fingerprint to perform a fake biometric attack remains quite complicated.

The latter refers to the case when a system deals with a compromised biometric template. If a biometric is compromised (e.g., stolen), it is compromised forever. Since a user has only a limited number of biometrics, they are not easy to replace, unlike ID cards and passwords. A number of solutions have been proposed to address this security issue. Biometric templates are never stored in their raw form; they are encrypted and sometimes doubly encrypted. Still, for matching purposes, the template must be decrypted and that's when, while very unlikely, a hacker may sniff it. Integrating cryptographic techniques along with biometric matchers can help address this problem. For example, instead of storing the original biometric signal in the database during enrollment, the system could store only its noninvertible transformed version (for example, a hash). The user himself/herself could provide the transform's parameters in terms of a password or PIN. If a hacker ever compromises such a (transformed) biometric template, the system can issue a new one using a different transform or different parameters. This requires a tradeoff between invertibility and discriminability of the transformed template. Published works show that the current approaches lead to some loss in the matching performance. This continues to be an active area of research in biometrics. It is not clear whether we will find the perfect noninvertible transform.

Moderator: How would you define the second requirement for biometric systems, which is related to the privacy of biometric data?

A.K. Jain: "Privacy is the ability to lead your life free of intrusions, to remain anonymous and to control access to your personal information" (from A.K. Jain, et al., "Biometric Recognition: Security & Privacy Concerns," *IEEE Security & Privacy Magazine*, vol. 1, no. 2, pp. 33–42, Mar.-Apr. 2003). As the incidence of identity fraud increases, biometrics will increasingly come to play for positively recognizing people. U.S. legislation already requires strong recognition schemes such as biometrics to limit access to sensitive medical records. Automated database access mechanisms through a secure biometric system would allow system administrators to track all accesses to privileged information; biometric-based accesses are less repudiable than other types of access control mechanisms.

However, biometrics does raise three systematic privacy concerns: unintended functional scope, unintended application scope, and covert recognition. These possible abuses or unacceptable use of biometrics can be addressed by government regulation, assurance of self-regulation, and enforcement by independent regulatory organizations. But, in the end, we must come to terms with security versus privacy tradeoff. In my opinion, security and privacy issues associated with biometric systems will not be the bottleneck in adopting this technology in the long run.

Moderator: What signal processing techniques are available to ensure security of biometric systems and privacy of biometric data?

A.K. Jain: In applications where fake biometric attacks remain a serious concern, vitality detection mechanisms based on hardware (multispectral finger imaging from Lumidigm, Inc.) and software (finger deformation) have been implemented. Multimodal biometric systems that incorporate several different traits (e.g., face, finger, and iris) have also been proposed to thwart these attacks. In my opinion, stolen biometric attacks are more severe from the point of user perception/acceptance than real threats to system security. A fake biometric attack presents a smaller risk than an attack on a password-based system.

N. Memon: There have been some very clever techniques proposed in the past few years for secure storage of biometric data. Examples include fuzzy hash, fuzzy vault, and secure sketch techniques. However, they suffer from one of two problems. First, many of the techniques proposed security in an information-theoretic sense, are designed for discrete data, and use simple similarity measures. However, real biometric data is continuous and requires complex similarity functions. Second, the techniques that are designed for real-world biometric data are either ad hoc and without formal proof of security, or do not provide a sufficiently rigorous security formulation that would provide the guarantees one needs before they can be safely used in real-world applications. In my opinion, there is a lot of work that still needs to be done towards the security and privacy of biometric data.

S.C. Draper: I agree. The types of solutions addressed by fuzzy hashes, fuzzy vaults, secure sketches, etc. are

very interesting variations on traditional biometric matching and have great potential. However, they have a long way to go before they mature and are ready for deployment.

Even if the signal processing challenges can be surmounted to produce a provably secure and operationally robust biometric system, this strengthens only one link in the chain. Many questions remain on how to integrate such a piece to provide a secure end-to-end solution. As an example, consider biometric authentication over a public network. Different protocols and technologies enhance security in different parts of the network: in a central repository where biometric information is stored, during the transmission of biometric-derived information over the network, etc. The weakest link would be the one attacked. Good solutions cannot strengthen one link to the detriment of another.

A problem posed by using biometrics in such remote authentication scenarios is that the data communicated over the network is just bits. Fuzzy hashes, fuzzy vaults, etc. aim to protect biometric information. But, the usefulness of that extra protection is based on the assumption that the raw biometric itself is a secret. It's important to understand how "leakable" different biometric modalities are. For instance, an attacker could conceivably collect enough people's iris scans (say, even in a localized area around an ATM machine) that the extra security afforded by the fuzzy hash would be obviated. That is, given a dictionary of collected iris information, an attacker will be able to break in regardless of how the biometric is stored. A natural pair of follow-on questions is what modalities present the highest barrier to collection and whether that barrier is high enough to prevent the development of an illegal repository of raw fingerprint data. The incentive to compile such databases will grow as biometrics become widespread.

Moderator: A third requirement for biometric systems is that they yield high recognition accuracy. What are the signal processing challenges to achieving this?

R. Chellappa: In face recognition, the variations due to pose and illumination changes are the most challenging. Over the last five years, variations due to pose have been effectively handled using 3-D morphable models. Variations due to illumination changes have not been addressed as effectively yet, but reasonable progress has been made.

In gait-based human recognition the variations due to pose create even more challenges. Existing methods are effective when the human is walking in a fronto-parallel direction. View-invariant signatures for gait-based identification have received some attention, but the problem is yet unsolved.

As far as resolution (or lack thereof), efforts are underway for superesolving face images in a video for improved face recognition. Again, the full impact of this approach has not been established.

N. Memon: In my view, the main difficulty is that biometric samples cannot be exactly reproduced, and traditional cryptographic primitives do not allow even a single bit of error. For example, two fingerprint scans of the same individual will not be identical due to sensor acquisition noise. So one cannot apply digital signatures or traditional cryptographic hash functions to them. Even the minutiae extracted will vary depending on the angle at which the finger was placed, how hard it is pressed, and the presence of dust, sweat, oil, scars, etc.

S.C. Draper: The algorithmic solutions required to deal robustly with the variability intrinsic to biometric measurements need more work. As noted by Nasir, such variations may result from changes in the underlying biometric or from the measurement process. The key components that underlie many signal processing techniques consist of a good understanding of the statistical structure of the source data (say the enrollment biometric) and the relationship between the source data and the decision data (the data presented at authentication). The first could be termed the "source model" and the latter the "noise model." These models would vary with biometric modality, as well as with the sensing system and environment. Refinements in either could lead to major improvements in system performance. Furthermore, for multimodal biometrics, better understanding of the source and noise models would allow us to fuse likelihood ratios in a more reasoned manner. Opportunities might come from exploiting recent modeling advances in machine learning or universal compression.

A.K. Jain: I would add that advances in sensor technology, and having cooperative and habituated users, will also improve the recognition accuracy. Take the example of fingerprints. Similar to work on 3-D face recognition, sensors that capture 3-D fingerprints have been developed that provide 3-D models of fingerprints during enrollment so that they can be effectively matched with partial prints during authentication. If a user wants to be recognized—for instance, to access a laptop—the user is more likely to ensure that his finger is clean and he places it on the plate center with the right amount of pressure.

Moderator: How would you summarize the main directions of R&D to improve the performance of biometric systems in terms of the requirements that have been discussed?

S.C. Draper: I believe that progress requires a two-pronged approach. First, effort needs be devoted to refining the statistical models of the underlying biometric and measurement processes. Without good models, recognition accuracy and security will be far from optimum.

Second, in the case of security techniques such as fuzzy hashes or fuzzy vaults, effort needs be devoted to developing codes matched to the particular source and channel under consideration. One may draw an analogy with storage and communication applications. Different classes of codes are used to protect information in different settings, e.g., on a CD, in a magnetic recording, over a wireless channel. In the same vein, we need codes matched to the "biometric channel" relating the biometric as measured at enrollment

to the biometric as measured at authentication.

One should note that both the statistical models and the corresponding matched codes will vary from one type of biometric to another, for instance, from iris to fingerprint to face. They will further vary between representations of a single type of biometric, for example, from a minutiae-based feature set of a finger to a Fourier-based feature set.

N. Memon: On the other hand, in addition to understanding data and noise models, more work is needed in the area of multifactor (multimodal) biometrics since single-modality biometrics schemes are limited.

S.C. Draper: I agree, the trouble with single-modality biometric systems is that many biometrics lack secrecy. Raw biometric data can be sniffed by a worm, fingerprints can be lifted off a car door, and iris data can be extracted from high-resolution photographs. Hence, one should not protect important government secrets with single-modal biometrics. Using multimodal biometrics is one method of increasing security.

P.J. Phillips: Multibiometrics and improved techniques for matching biometric samples are interesting avenues to pursue. Other areas of importance include sensor design and acquisition algorithms, human-computer interfaces, secure communications and encryption, and distributed and embedded computing.

Moderator: Among the solutions to improve the accuracy of biometric systems you have mentioned multibiometric (or multifactor) techniques. What are the detailed reasons for using a multibiometric system and what are the data sources of such a system?

A.K. Jain: There are three main reasons for using multibiometric systems: 1) to improve the matching accuracy, i.e., reduce false accept rates (FARs) and false reject rates (FRRs); 2) to increase the population coverage; for example, some individuals who may not be able to provide good-quality fingerprint images can be identified using their iris; and 3) to minimize incidence of spoof attacks; it would be difficult to present fake biometric for more than one trait.

Many sources of information can be considered in designing a multibiometric system. Each has its own advantage and disadvantage in terms of cost of the system, time to enroll and verify, and ease of use. These sources are:

- Multisensor: A single biometric trait is imaged using multiple sensors (e.g., visual and infrared face cameras).
- Multialgorithm: The same biometric data is processed using different (feature extraction and matching) algorithms.
- Multiinstance: This uses multiple instances or units of the same body trait (e.g., left and right irises).
- Multisample: This uses a single sensor to acquire multiple samples of the same biometric (e.g., two face views) to account for intra-user variations in the trait.
- Multimodal: Evidence provided by different body traits (e.g., face and finger) are used for establishing identity.

One can also design a hybrid multibiometric system by integrating a subset of the five scenarios mentioned above via fusion.

N. Memon: This is also a nice way to combine the strengths of biometrics and other security schemes while perhaps keeping the costs low by using multifactor applications. If each factor is sufficiently protected, the overall system can be quite secure, despite the possible increase in the inconvenience. The challenge here is how to combine different systems with minimum increase in inconvenience.

Moderator: Multibiometric methods in general, and fusion methods in particular, have proven to be useful for many application domains including communications, data mining, image processing, and semantic retrieval. What are the specific problems in the biometric domain?

A.K. Jain: Some of the major problems associated with fusion techniques for biometrics are as follows: 1) collection from multiple sources of information takes more time to enroll and to verify an individual (the verification time is particularly critical as it decreases the throughput of the system); 2) system cost for authentication in commercial applications of biometrics such as verification at point of sales and sensor cost, amount of storage (for templates), and processing time need to be considered; 3) while there are large public domain databases available for individual biometric traits (face, finger, and iris), the size of public domain multibiometric databases available is rather small—this limits the evaluation of various fusion algorithms; 4) which fusion technique is the best has yet to be decided. A large number of ad hoc techniques have been tried, and it is generally agreed that the simple score level fusion works well most of the time. A more principled approach using likelihood ratio is being recommended as the optimal approach that avoids the need for score normalization and evidence weighting.

P.J. Phillips: Anil did an excellent job of articulating the potential of multibiometric and fusion techniques, and I emphasize the word *potential*. Numerous fusion methods exist in the biometric literature. Unfortunately, there does not exist the experimental infrastructure for determining which fusion methods are appropriate for different applications. Comparisons of different biometrics in multibiometric challenges such FRVT and ICE aim to help answer this question using specific multibiometric datasets. The combination of FRVT 2006 and ICE 2006 measures performance of iris recognition, face recognition from still images, and face recognition from 3-D scans. A further challenge for the biometric research communities is to develop experimental and data collection protocols for further assessing fusion techniques.

R. Chellappa: Although biometric fusion techniques have been developed for fingerprint and faces, faces and gait, and audio and faces, I believe that fusion of multibiometrics is still a largely unexplored area. One of the problems that still needs to be addressed is accounting for the correlation among the different single biometric algorithm. Fusion of

correlated classifiers is a difficult problem. What we are seeing is that, when the data is good, both biometric methods perform well, and when challenging examples are presented, both methods fail. We can expect real progress in the recognition performance of real biometric systems when more sophisticated rules are used.

S.C. Draper: Average performance is not a good measure for biometric systems. This is not necessarily unique to biometrics, but it differentiates them somewhat from other applications. In communications, for example, if a packet transmission fails, one can always retransmit. If retransmissions are independent, the probability that all transmission attempts fail drops exponentially with the number of attempts. On the other hand, in a biometric system, a system that works well for the average user, but fails almost always for the most challenging users, will not be acceptable. Robust worst-case performance in biometric authentication is much more important than in many other signal processing contexts.

N. Memon: Correlations among biometric data are indeed a difficult issue to deal with. On one hand, I agree that the understanding of how the data is correlated would allow us to design systems with better performance and/or security. One the other hand, I tend to believe that correlations that are hard to understand can also work to our advantage.

Let us consider a simple example. When we choose a key for a cryptographic cipher, usually the best practice is to choose the bits uniformly, such that the entropy of the key is maximum with the same key length. However, we can also argue that, with the same entropy, we can actually create much longer keys, where the bits are correlated in some complex manner that is hard to exploit. In such cases, the burden to analyze the correlation of the bits would be on the attackers who try to guess the key, and a naive (brute-force) attacker would have to spend much more time compare with the uniform-key case, even if the entropy of the key is actually the same.

Moderator: There is ongoing work in the biometric standards community to ensure interoperability between systems by specifying common data exchange formats and application interfaces. What critical issues need to be addressed in this area for next-generation biometric standards?

P.J. Phillips: The biometric standardization activities range from the nuts and bolts of interoperability of large-scale biometric systems to areas that are active research topics. Multibiometric systems and biometric quality metrics are examples of topics that are active research areas.

S.C. Draper: The main domestic biometric standardization committee is INCITS-M1, founded in November 2001. The timing and activities of this committee, as well as its list of participants, demonstrate the growing importance of biometrics. INCITS-M1 members include governmental, commercial, and academic organizations.

A prime objective of the committee is to provide comprehensive and well-founded U.S. positions for international standards activities. INCITS-M1 serves as the U.S. Technical Advisory Group for the international organization ISO/IEC JTC-1/SC-37, which was established in June 2002. Its task groups include Technical Interfaces (M1.2), Data Interchange Formats (M1.3), Biometric Profiles (M1.4), Performance Testing and Reporting (M1.5) and Cross Jurisdictional and Societal Issues (M1.6).

The ad hoc groups within M1 give an indication of next-generation issues. Two current groups whose foci have been touched on in this forum are AHGEMS (multibiometric systems) and AHGBEA (Biometrics and E-Authentication). The latter has produced a report (available on the INCITS-M1 Web site) detailing many issues of security and privacy in networked contexts. A sampling of issues that are raised in the report on biometrics and E-authentication, and also engender much discussion at committee meetings, include: 1) methods to ensure the privacy of biometric data; 2) how to demonstrate to the cryptography-focused security community that there is a role for biometrics to play across a range of applications with differing security requirements; 3) quantifying the inherent entropy (and therefore security limits) of biometric data; 4) the additional requirements of remote authentication context were, e.g., liveliness testing may not be possible as the authenticator may not control the sensor and so the sensor can be fed synthetic data; and 5) whether secrecy can be ensured by keeping the (e.g., matching) algorithm secret rather than the biometric data.

Moderator: Usability is important for biometric systems to gain user acceptance, and there seem to exist promising design considerations. What efforts are needed to increase the user acceptance of biometric systems for a broader range of applications?

P.J. Phillips: Human interaction with biometric systems can be divided into two cases: acquisition and decision-making.

In the first case, a user provides a biometric sample, such a fingerprint or face image, to a system. The goal of a biometric acquisition system is to reliably acquire a high-quality biometric sample. The design of the sensor, configuration of the sensor, and user interface type are important. For instance, the sensor may use a single finger or four-finger slap. The height of the fingerprint sensor can affect performance. Also, experimental results show that video instructions are better than instructions on a poster.

In the second case, the result of biometric matching needs to be presented in a manner that helps facilitate a human operator's decision-making. For example, in face recognition, a system could present an operator with a list of candidate face images. Testing the efficacy of this method requires a comparison between operator and computer performance. Recent results have found that computers are capable of performing better than humans for recognition of frontal faces across illumination changes (humans are asked to recognize unfamiliar faces). Correctly, the human and machine recognition results yield performance superior to that of either machine or human.

S.C. Draper: In my view, usability is most affected by sensor design and can also be impacted by the selection of algorithms. For example, being able to segment and extract features of an iris at long range (one to a few meters) and in real time would improve the acceptability of iris biometrics. However, such developments would also raise privacy concerns.

Improved matching algorithms can lead to better overall matching accuracy and, often more significantly, can improve performance for users with more challenging biometrics (e.g., those whose finger prints do not register well on many devices). Faster algorithms and intelligent search techniques can yield massive speed-ups when searching large databases for a match with an unlabeled probe data (i.e., a probe without an associated user identification number). Such developments would increase the acceptability of a biometric system.

Moderator: If you were to summarize one last thought or outlook on what comes next for biometrics, what would that be?

P.J. Phillips: I would mention the development of personal biometric information systems (PBIS) for mobile Web-enabled cell phones. In a mobile Web PBIS, facial images or fingerprints acquired by a cell phone (using included sensors) could be sent via the mobile Web to a personal biometric information system's provider for matching against a personal biometric database. The results of the search could then be transmitted to the originating cell phone. This would provide a capability to identify people on an extensive business contact list.

R. Chellappa: My thought is that next, biometric systems may be employed for keyless access to office rooms, homes, cars, and other devices. They may also be used to personalize settings in a given space, e.g., to adjust car seats, temperature control, positions of mirrors, etc.

A.K. Jain: With a wider perspective in mind, any system for reliable person recognition must contain a biometric component. Because of the unique person recognition potential provided by biometrics, they have and will continue to provide useful societal value by deterring crime, identifying criminals, securing our borders, and eliminating fraud. At the same time, the success and acceptance of their deployment will depend on our ability to create systems that are cost effective, usable, and that do not threaten basic rights to privacy and anonymity.

PANELISTS

Anil K. Jain (jain@cse.msu.edu) is a University Distinguished Professor at Michigan State University with appointments in the Computer Science and Engineering, Electrical and Computer Engineering, and Statistics and Probability departments. He serves on the National Academies panel on biometrics and is a member of biometrics defense support team. He is the author of a number of books on biometrics, including *Handbook of Biometrics,* Springer, 2007. He is a Fellow of the IEEE.

Rama Chellappa (rama@cfar.umd.edu) is a Minta Martin Professor of Engineering, professor of electrical and computer engineering, and an affiliate professor of computer science at University of Maryland, College Park, Maryland. His research interests are face and gait recognition, activity modeling and recognition, markerless motion capture for analysis of movement disorders, multisensor fusion, anomaly detection in still and video images, 3-D modeling, and video indexing and retrieval. He is a Fellow of the IEEE.

Stark C. Draper (sdraper@ece.wisc.edu) is with the Department of Electrical and Computer Engineering at the University of Wisconsin in Madison. His research interests include signal processing, communications, biometric security, streaming media, estimation, information theory, queuing, and networking. He is a Member of the IEEE.

Nasir Memon (memon@poly.edu) is a professor in the Computer Science Department at Polytechnic University, Brooklyn, New York, where he is the director of the Information Systems and Internet Security (ISIS) Laboratory. His research interests include data compression, computer and network security, digital forensics, and multimedia data security. He is a Member of the IEEE.

P. Jonathon Phillips (jonathon@nist.gov) is an electronic engineer with NIST. His current research interests include computer vision, face recognition, biometrics, evaluation methodologies, and computational psychophysics. He is a Senior Member of the IEEE.

Anthony Vetro (avetro@merl.com) is with Mitsubishi Electric Research Labs, Cambridge, Massachusetts, where he is a group manager responsible for multimedia technology. His research interests include information coding, media streaming, and multidimensional signal processing. He is a Senior Member of the IEEE. SP

life SCIENCES continued from page 126

[8] H. Gray, *Anatomy of the Human Body*. Bartleby, 20th ed edition, 1918. Bartleby.com Great Books Online: http://bartleby.com/107/illus751.html.

[9] A. Brun, M. Björnemo, R. Kikinis, and C.-F. Westin, "White matter tractography using sequential importance sampling," in *Proc. ISMRM Annu. Meeting (ISMRM'02)*, Honolulu, Hawaii, May 2002.

[10] T. Behrens, M. Woolrich, M. Jenkinson, H. Johansen-Berg, R. Nunes, S. Clare, P. Matthews, J.M. Brady, and S. Smith, "Characterization and propagation of uncertainty in diffusion-weighted MR imaging," *Magnetic Resonance Med.*, vol. 50, pp. 1077–1088, 2003.

[11] M. Lazar and A. Alexander. "Bootstrap white matter tractography (boot-trac)," *NeuroImage*, vol. 24, no. 2, pp. 524–532, 2005.

[12] O. Friman, G. Farneback, and C.-F. Westin, "A Bayesian approach for stochastic white matter tractography," *IEEE Trans. Med. Imaging*, vol. 25, no. 8, pp. 965–978, 2006.

[13] A. Doucet, N. de Freitas, and N. Gordon, editors. *Sequential Monte Carlo Methods in Practice*. New York: Springer-Verlag, 2001.

[14] A. Brun, H. Knutsson, H.J. Park, M.E. Shenton, and C.-F. Westin, "Clustering fiber tracts using normalized cuts," in *Proc. 7th Int. Conf. Medical Image Computing and Computer-Assisted Intervention (MICCAI'04)*, Rennes–Saint Malo, France, Sept. 2004, pp. 368–375.

[15] L. O'Donnell and C.-F. Westin, "White matter tract clustering and correspondence in populations," in *Proc. 8th Int. Conf. Medical Image Computing and Computer-Assisted Intervention (MICCAI'05)*, Palm Springs, CA, Oct. 2005, pp. 140–147.

[16] L. O'Donnell, M. Kubicki, M.E. Shenton, M. Dreusicke, W.E.L. Grimson, and C.-F. Westin, "A method for clustering white matter fiber tracts," *Amer. J. Neuroradiology*, vol. 27, no. 5, pp. 1032–1036, 2006. SP