Biometric Authentication: System Security and User Privacy

Anil K. Jain
Michigan State University

Karthik Nandakumar
Institute for Infocomm Research, Singapore

While biometric systems aren't foolproof, the research community has made significant strides to identify vulnerabilities and develop measures to counter them.

Identity theft is a growing concern in our digital society. The US Federal Trade Commission reports that ID theft affects millions of innocent victims each year and is the most common consumer complaint (www.ftc.gov/opa/reporter/idtheft/index.shtml).

Traditional authentication methods such as passwords and identity documents aren't sufficient to combat ID theft or ensure security. Such surrogate representations of identity can be easily forgotten, lost, guessed, stolen, or shared.

Biometric systems recognize individuals based on their anatomical traits (fingerprint, face, palmprint, iris, voice) or behavioral traits (signature, gait). Because such traits are physically linked to the user, biometric recognition is a natural and more reliable mechanism for ensuring that only legitimate or authorized users are able to enter a facility, access a computer system, or cross international borders. Biometric systems also offer unique advantages such as deterrence against repudiation and the ability to detect whether an individual has multiple identity cards (for example, passports) under different names. Thus, biometric systems impart higher levels of security when appropriately integrated into applications requiring user authentication.

While law enforcement agencies have used fingerprint-based biometric authentication for more than a century in forensic investigations, the last two decades have seen a rapid proliferation of biometric recognition systems in a wide variety of government and commercial applications around the world. Figure 1 shows some examples.

Although many of these deployments are extremely successful, there are lingering concerns about the security of biometric systems and potential breaches of privacy resulting from the unauthorized release of users' stored biometric data. Like any other user authentication mechanism, a biometric system can be circumvented by a skillful impostor given the right circumstances and plenty of time and resources. Mitigating such concerns is essential to gaining public confidence and acceptance of biometric technology.

BIOMETRIC SYSTEM OPERATION

A biometric system first records a sample of a user's biometric trait using an appropriate sensor—for example, a camera for the face—during *enrollment*. It then extracts salient characteristics, such as fingerprint minutiae, from the biometric sample using a software algorithm called a *feature extractor*. The system stores these extracted features as a *template* in a database along with other identifiers such as a name or an identification number.

To be authenticated, the user presents another biometric sample to the sensor. Features extracted from this sample constitute the *query*, which the system then compares to the template of the claimed identity via a biometric *matcher*. The matcher returns a match score representing the degree of similarity between the template and the query. The system accepts the identity claim only if the match score is above a predefined threshold.

0018-9162/12/$31.00 © 2012 IEEE

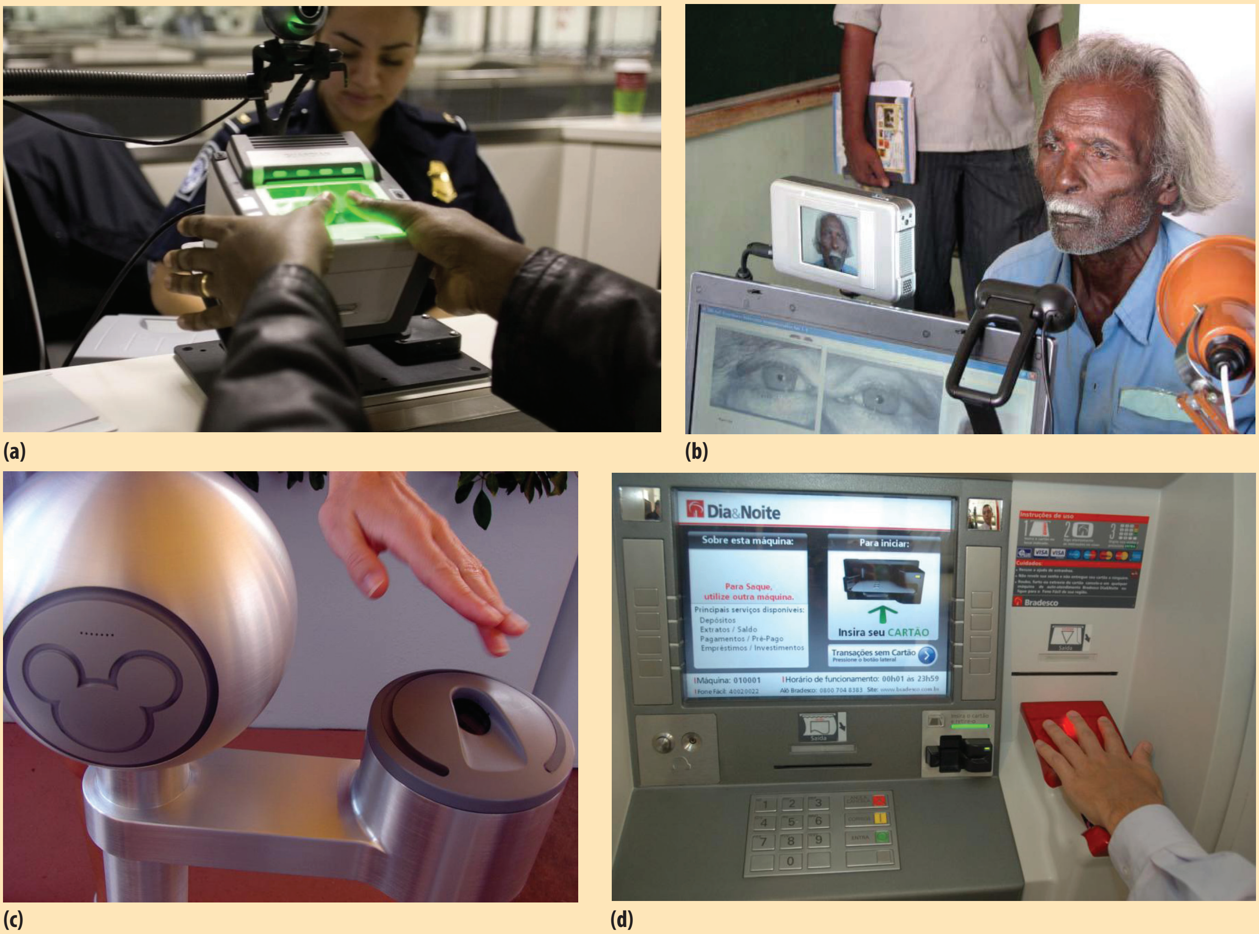

Figure 1. Examples of biometric authentication systems deployed in government and commercial applications. (a) The US-VISIT program to regulate international border crossings (www.dhs.gov/files/programs/usv.shtm) records all 10 fingerprints of a visa applicant. (b) India's Aadhaar civil registry system (www.uidai.gov.in) captures the iris and face images in addition to 10 fingerprints. (c) Walt Disney World Resort in Orlando, Florida, uses a fingerprint-based access system to prevent ticket fraud (www.boston.com/news/nation/articles/2006/09/03/disney_world_scans_fingerprint_details_of_park_visitors). (Photo by Mark Goldhaber; www.mouseplanet.com/9797/Walt_Disney_World_Resort_Update#rfid.) (d) Many banks in countries including Japan (www.theregister.co.uk/2012/04/12/ogaki_palm_scanning_cash) and Brazil (www.bradescori.com.br/site/conteudo/interna/default.aspx?secaoId=680&idiomaId=2) use palm-vein-based automated teller machines. (Photo courtesy of Bradesco; http://infosurhoy.com/cocoon/saii/xhtml/en_GB/features/saii/features/economy/2010/03/01/feature-04.)

BIOMETRIC SYSTEM VULNERABILITIES

A biometric system is vulnerable to two types of failures, as Figure 2 shows. A *denial of service* occurs when the system doesn't recognize a legitimate user, while an *intrusion* refers to the scenario in which the system incorrectly identifies an impostor as an authorized user. While there are many possible reasons for these failures, they can be broadly categorized as *intrinsic limitations* and *adversary attacks* (A.K. Jain, A.A. Ross and K. Nandakumar, "Security of Biometric Systems," *Introduction to Biometrics*, Springer, 2011, pp. 259-306).

Intrinsic limitations

Unlike a password-based authentication system, which requires a perfect match between two alphanumeric strings, a biometric-based authentication system relies on the similarity between two biometric samples.

Because an individual's biometric samples acquired during enrollment and authentication are seldom identical, as Figure 3 shows, a biometric system can make two types of authentication errors. A *false nonmatch* occurs when two samples from the same individual have low similarity and the system can't correctly match them. A *false match* occurs when two samples from different individuals have high similarity and the system incorrectly declares them as a match.

A false nonmatch leads to a denial of service to a legitimate user, while a false match can result in intrusion by an impostor. Because the impostor need not exert any special effort to fool the system, such an intrusion is known as a *zero-effort attack*. Most of the research effort in the biometrics community over the past five decades has focused on improving authentication accuracy—that is, on minimizing false nonmatches and false matches.

Adversary attacks

A biometric system may also fail to operate as intended due to manipulation by adversaries. Such manipulations can be carried out via insiders, such as system administrators, or by directly attacking the system infrastructure. An adversary can circumvent a biometric system by coercing or colluding with insiders, exploiting their negligence (for example, failure to properly log out of a system after completing a transaction), or fraudulently manipulating the procedures of enrollment and exception processing, originally designed to help authorized users.

External adversaries can also cause a biometric system to fail through direct attacks on the user interface (sensor), the feature extractor and matcher modules, the interconnections between the modules, and the template database.

Examples of attacks targeting the system modules and their interconnections include Trojan horse, man-in-the-middle, and replay attacks. As most of these attacks are also applicable to password-based authentication systems, several countermeasures like cryptography, time stamps, and mutual authentication are available to prevent them or minimize their impact.

Two major vulnerabilities that specifically deserve attention in the context of biometric authentication

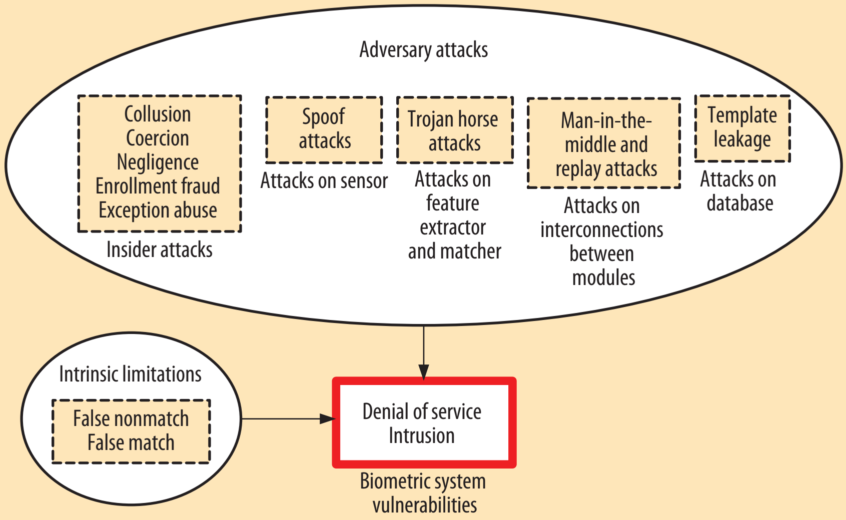

Figure 2. A biometric system is vulnerable to denials of service and intrusions, which can be caused by both intrinsic limitations and adversary attacks.

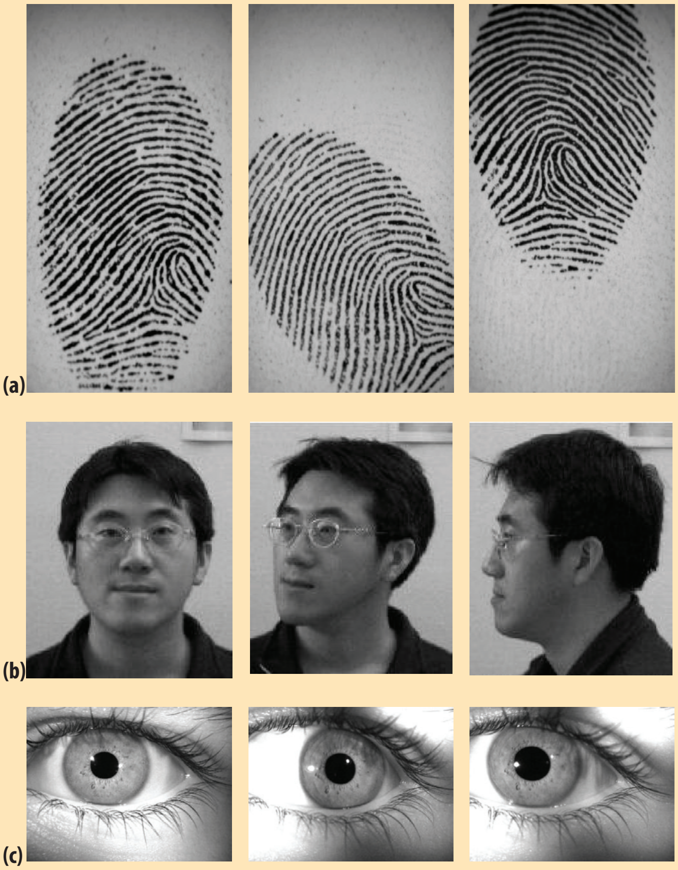

Figure 3. Inherent variability between biometric samples of the same individual. (a) Variations in fingerprint patterns of the same finger due to differences in finger placement on the sensor. (b) Variations in face images of the same person due to changes in pose. (c) Variations in iris images of the same eye due to differences in pupil dilation and gaze direction.

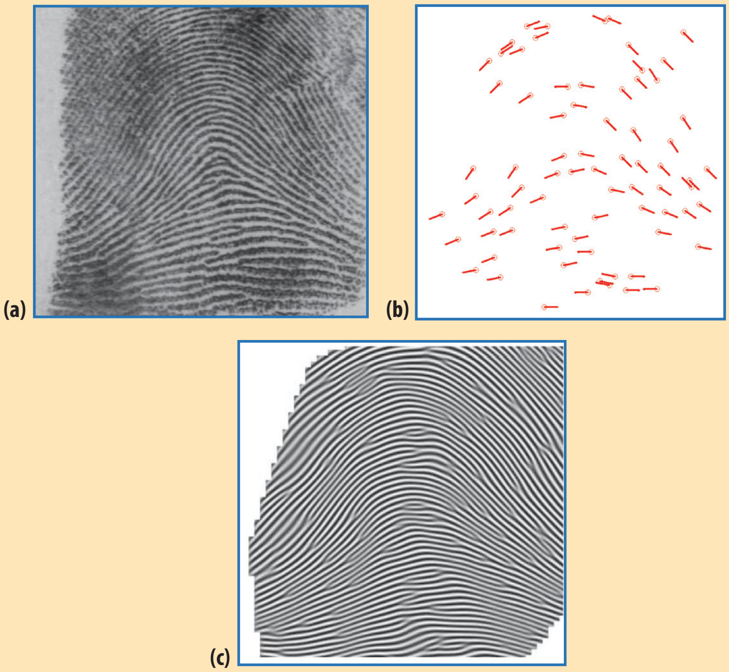

Figure 4. Example of obtaining a biometric trait by reverse engineering the corresponding biometric template: (a) original fingerprint image, (b) minutiae template information extracted from the fingerprint image, and (c) fingerprint image reconstructed using only the minutiae information. (Adapted from J. Feng and A.K. Jain, "Fingerprint Reconstruction: From Minutiae to Phase," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Feb. 2011, pp. 209-223.)

are *spoof attacks* at the user interface and *template database leakage*. These two attacks have serious adverse effects on biometric system security.

A spoof attack involves presenting a counterfeit biometric trait not obtained from a live person. Examples of spoofed biometric traits include a gummy finger, photograph or mask of a face, or dismembered finger from a legitimate user.

A fundamental tenet of biometric authentication is that even though biometric traits aren't secrets—it may not be very difficult to covertly obtain a photo of a person's face or the fingerprint pattern from an object or surface touched by a person—the system is still secure because the trait is physically linked to a live user. A spoof attack, if successful, violates this basic assumption and thereby greatly undermines the system's security.

Researchers have developed numerous liveness detection techniques—for example, verifying the physiological properties of human fingers or observing involuntary human actions such as blinking of the eye—to ensure that the biometric trait captured by a sensor indeed comes from a live person (K.A. Nixon, V. Aimale, and R.K. Rowe, "Spoof Detection Schemes," *Handbook of Biometrics*, A.K. Jain, P. Flynn, and A.A. Ross, eds., Springer, 2007, pp. 403-424).

Template database leakage refers to a scenario where a legitimate user's biometric template information becomes available to an adversary. This aggravates the problem of spoofing because it makes it easier for the adversary to recover the biometric pattern by simply reverse engineering the template, as Figure 4 shows. Moreover, unlike passwords and ID cards, it isn't possible to replace stolen templates with new ones because biometric traits are irrevocable. Finally, the stolen biometric templates can be used for unintended purposes—for example, to covertly track a person across multiple systems or obtain private health information.

BIOMETRIC TEMPLATE SECURITY

A critical step in minimizing the security and privacy risks associated with biometric systems is to protect the biometric templates stored in the system database. While the risks can be mitigated to some extent by storing the templates in a decentralized fashion—for example, in a smart card carried by the user—such solutions aren't feasible in applications requiring deduplication capability such as the US-VISIT or India's Aadhaar system.

Although many techniques exist for securing passwords including encryption/hashing and key generation, they're predicated on the assumption that passwords provided by the user during enrollment and authentication are identical.

Template security requirements

The main challenge in developing a biometric template protection scheme is to achieve an acceptable tradeoff among three requirements.

Noninvertibility. It must be computationally hard to recover the biometric features from the stored template. This prevents the adversary from replaying the biometric features gleaned from the template or creating physical spoofs of the biometric trait.

Discriminability. The template protection scheme shouldn't degrade the biometric system's authentication accuracy.

Revocability. It should be possible to create multiple secure templates from the same biometric data that aren't linkable to that data. This property not only enables the biometric system to revoke and reissue new biometric templates if the database is compromised, but it also prevents cross-matching across databases, thereby preserving the user's privacy.

Template security approaches

There are two generic approaches for securing biometric templates: *biometric feature transformation* and *biometric cryptosystems*.

In the case of biometric feature transformation, as Figure 5a shows, the secure template is derived by applying a noninvertible or one-way transformation function to the original template; this transformation is typically based on user-specific parameters. During authentication, the system applies the same transformation function to the query and matching occurs in the transformed domain.

Biometric cryptosystems, as Figure 5b shows, store only a fraction of the information derived from the biometric template known as the *secure sketch*. While the secure sketch in itself is insufficient to reconstruct the original template, it does contain sufficient data to recover the template in the presence of another biometric sample that closely matches the enrollment sample.

The secure sketch is typically obtained by binding the biometric template with a cryptographic key. However, a secure sketch isn't the same as a biometric template encrypted using standard cryptographic techniques.

In standard encryption, the encrypted template and decryption key are two separate entities and the template is secure only as long as the decryption key is secure. A secure sketch encapsulates both the biometric template and the cryptographic key as a single entity. Neither the key nor the template can be recovered using only the secure sketch. When the system is presented with a biometric query that closely matches the template, it can recover both the original template and the cryptographic key using common error detection techniques.

Researchers have proposed two main approaches for generating a secure sketch: *fuzzy commitment* and *fuzzy vault*. Fuzzy commitment can be used to protect biometric templates that are represented as fixed-length binary strings (A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," *Proc. 6th ACM Conf. Computer and Comm. Security* [CCS 99], ACM, 1999, pp. 28-36). The fuzzy vault is useful for protecting templates that are represented as a set of points (K. Nandakumar, A.K. Jain, and S. Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation & Performance," *IEEE Trans. Information Forensics and Security*, Dec. 2007, pp. 744-757).

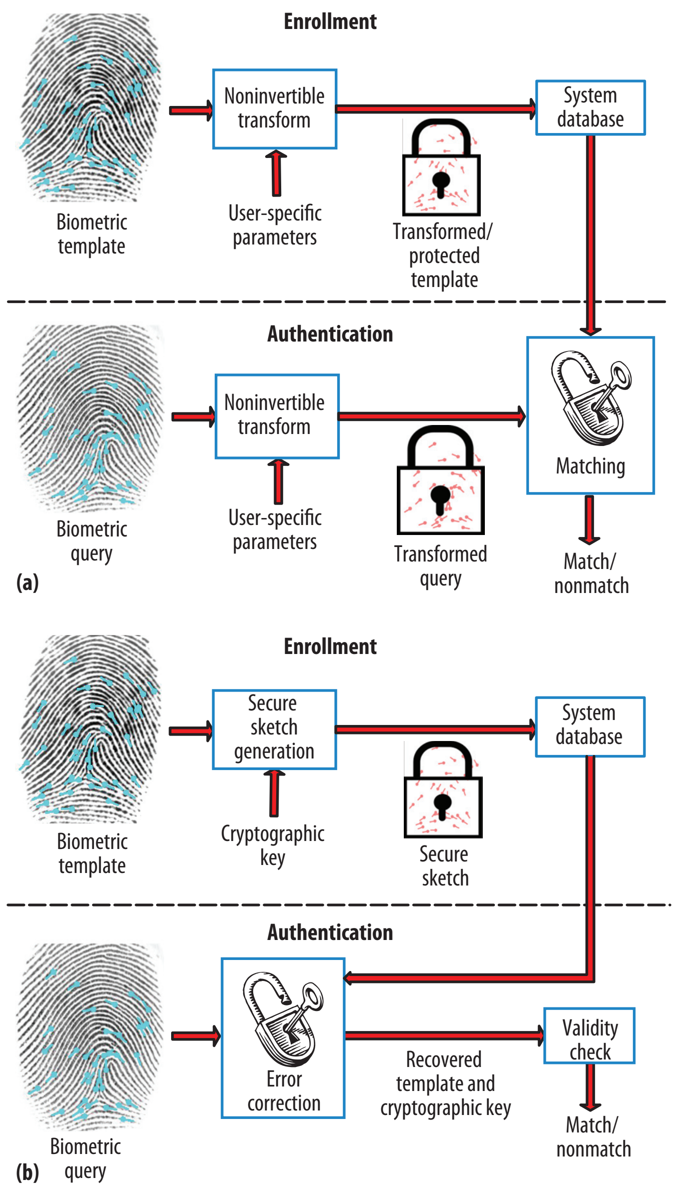

Figure 5. Securing biometric templates using (a) biometric feature transformation and (b) biometric cryptosystems.

Pros and cons

Biometric feature transformation and biometric cryptosystems have their own pros and cons.

Matching is often straightforward in a feature transformation scheme, and it may even be possible to design transformation functions that don't alter the original feature space's characteristics. However, finding an appropriate transformation function that is noninvertible but at the same time tolerant to inherent intra-user biometric variations can be difficult.

While secure sketch generation techniques based on sound information-theoretic principles are available for biometric cryptosystems, the challenge is to represent the biometric features in standardized data formats like binary strings and point sets. Therefore, an active research topic is designing algorithms that convert the original biometric template into standardized data formats like fixed-length binary strings or point sets without any loss of discriminative information (A. Nagar, K. Nandakumar, and A.K. Jain, "Multibiometric Cryptosystems Based on Feature-Level Fusion," *IEEE Trans. Information Forensics and Security*, Feb. 2012, pp. 255-268).

Fuzzy commitment and fuzzy vault have other limitations, including the inability to generate multiple nonlinkable templates from the same biometric data. One possible way to overcome this problem is to apply a feature transformation function to the biometric template before it is protected using a biometric cryptosystem. Such systems, which combine feature transformation with secure sketch generation, are known as *hybrid biometric cryptosystems*.

THE PRIVACY CONUNDRUM

The irrefutable link between users and their biometric traits has triggered valid concerns about user privacy. In particular, knowledge of the biometric template information stored in the database can be exploited to compromise user privacy in many ways.

Template protection schemes can mitigate this threat to some extent, but many thorny privacy issues remain beyond the scope of biometric technology:

- Who owns the biometric data, the individual or the service providers?
- Will the use of biometrics be proportional to the need for security in a given application? For example, should a fingerprint be required to purchase a hamburger at a fast food restaurant or access a commercial website?
- What is the optimal tradeoff between application security and user privacy? For example, should governments, businesses, and other entities be able to use surveillance cameras at public spaces to covertly track benign activities of users?

There are currently no satisfactory practical solutions on the horizon to address such questions.

Biometric recognition provides more reliable user authentication than passwords and identity documents, and is the only way to detect duplicate identities. While biometric systems aren't foolproof, the research community has made significant strides to identify vulnerabilities and develop measures to counter them. New algorithms for protecting biometric template data alleviate some of the concerns about system security and user privacy, but additional improvements will be required before such techniques find their way into real-world systems. C

Anil K. Jain *is a University Distinguished Professor in the Department of Computer Science and Engineering at Michigan State University. Contact him at jain@cse.msu.edu.*

Karthik Nandakumar *is a research scientist in the Institute for Infocomm Research, Singapore. Contact him at knandakumar@i2r.a-star.edu.sg.*

Editor: Karl Ricanek Jr., director of the Face Aging Group at the University of North Carolina Wilmington; ricanekk@uncw.edu