Biometrics: A Grand Challenge

Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, and Arun Ross
Michigan State University, IBM T. J. Watson Research Center, DigitalPersona Inc., Siemens Corporate Research, West Virginia University
jain@cse.msu.edu, sharat@us.ibm.com,salilp@digitalpersona.com, lin.hong@scr.siemens.com, ross@csee.wvu.edu

Abstract

Reliable person identification is an important problem in diverse businesses. Biometrics, identification based on distinctive personal traits, has the potential to become an irreplaceable part of any identification system. While successful in some niche markets, the biometrics technology has not yet delivered its promise of foolproof automatic identification. With the availability of inexpensive biometric sensors and computing power, it is becoming increasingly clear that widespread usage of biometric person identification is being stymied by our lack of understanding of three fundamental problems: (i) How to accurately and efficiently represent and recognize biometric patterns? (ii) How to guarantee that the sensed measurements are not fraudulent? and (iii) How to make sure that the application is indeed exclusively using pattern recognition for the expressed purpose (function creep [16])? Solving these core problems will not only catapult biometrics into mainstream applications but will also stimulate adoption of other pattern recognition applications for providing effective automation of sensitive tasks without jeopardizing our individual freedoms. For these reasons, we view biometrics as a grand challenge - "a fundamental problem in science and engineering with broad economic and scientific impact[1]".

1. Introduction

Since the beginning of civilization, identifying fellow human beings has been crucial to the fabric of human society. Consequently, person identification is an integral part of the infrastructure needed for diverse business sectors such as finance, health care, transportation, entertainment, law enforcement, security, access control, border control, government, and communication.

As our society becomes electronically connected to form one big global community, it has become necessary to carry out reliable person identification often remotely and through automatic means. Surrogate representations of identity such as passwords (prevalent in electronic access control) and cards (prevalent in banking and government applications) no longer suffice. Further, passwords and cards can be shared and thus cannot provide non-repudiation. Biometrics, which refers to automatic identification of people based on their distinctive physiological (e.g., face, fingerprint, iris, retina, hand geometry) and behavioral (e.g., voice, gait) characteristics, should be an *essential* component of any effective person identification solution because biometric identifiers cannot be shared, misplaced, and they intrinsically represent the individual's identity. Consequently, biometrics is not only an important pattern recognition research problem but is also an enabling technology that will make our society safer, reduce fraud and lead to user convenience (user friendly man-machine interface) by broadly providing the following three functionalities:

(a) Positive Identification ("Is this person who he claims to be?"). A positive identification (also called authentication or verification) verifies the authenticity of a claimed enrolled identity based on the input biometric sample. For example, a person claims that he is John Doe to the authentication system and offers his fingerprint; the system then either accepts or rejects the claim based on **a single match** performed between the input pattern and the enrolled pattern associated with the claimed identity. Commercial applications such as computer network logins, electronic data security, e-commerce, Internet access, ATMs, credit card purchases, physical access control, cellular phones, PDAs, medical records management, and distance learning are sample authentication applications.

[1] Definition of *grand challenge* by the High Performance Computing and Communication (HPCC) program: http://www.hpcc.gov/

Authentication applications are typically cost sensitive with a strong incentive for being user-friendly.

(b) Large Scale Identification ("Is this person in the database?"). Given an input biometric sample, a large-scale identification (also referred to as recognition or negative identification) determines if the pattern is associated with any of a large number (e.g., millions) of enrolled identities. Typical large-scale identification applications include welfare-disbursement, national ID cards, border control, voter ID cards, driver's license, criminal investigation, corpse identification, parenthood determination, missing children identification, etc. These large-scale identification applications require a large sustainable throughput with as little human supervision as possible.

(c) Screening ("Is this a wanted person?"). Screening applications covertly and unobtrusively determine whether a person in a (public) space belongs to a watch-list of identities. Examples of screening applications include terrorist identification, airport security, security at public events, and other surveillance applications. The screening watch-list consists of a moderate (e.g., a few hundreds) number of identities. By their very nature, the screening applications (i) do not have a well-defined "user" enrollment phase; (ii) cannot expect any control over their subjects or imaging conditions; and (iii) require large sustainable throughput with as little human supervision as possible. Note that both large scale identification and screening cannot be accomplished without biometrics (e.g., by using token-based or knowledge-based identification).

More than a century has passed since Alphonse Bertillon first conceived and then industriously practiced the idea of using body measurements for identifying criminals [18]. In 1893, the Home Ministry Office, UK, accepted that no two individuals have the same fingerprints and set in motion a chain of events that led to the first Automatic[2] Fingerprint Identification System (AFIS) in the 1960s. The use of AFIS as an effective tool for criminal investigation and background checks is prevalent worldwide (The AFIS system at FBI consists of a large database of approximately 46 million "ten prints" and conducts, on an average, an impressive number of approximately 50,000 searches per day). Over the last couple of decades, a number of other biometric traits have been studied, tested, and have been successfully deployed in niche markets [25,26]. Thanks to the imaginative and flattering depiction of fancy biometric systems in Hollywood Sci-Fi flicks, the popularity of AFIS, and the intuitive appeal of biometrics as a crime deterring security tool, the success and widespread use of completely automatic biometric systems appeared to be very obvious. Not surprisingly, there is an overall (mis)perception in the pattern recognition community that this important research problem has been largely solved but for the clever bells and whistles needed for making this technology work in the real world.

And yet, this proverbial last mile of deployment has doggedly resisted our persistent attempts to broaden the scope of niche biometric systems to shrink-wrapped solutions. Humbled biometric road warriors everywhere seem to agree that it is not a mere matter of a superficial system tuning or clever system improvisation. These tricks have already been tried.

For example, almost a century after the fingerprints were observed to be unique, a 2004 fingerprint contest revealed that fingerprint matching has an equal error rate of 2% [19]![3] If this system were to be deployed in New York City Airports (~200,000 passengers/day [14]), it would result in 4,000 false alarms and 4,000 false rejects every day! While the error rate of the fingerprint system can be significantly reduced by using multiple fingers, the point we want to emphasize is that the error rate is non-zero. Similarly, even though the first paper on automatic face recognition appeared in the early 1970's [10], the state of the art face recognition systems have been known to be fragile in recent operational tests [12,13]. Speaker recognition field awaits good solutions to many of the critical problems [6,24]. More recent biometric identifiers such as iris have extremely low error rates, but it also displays signs of fragility in recent pilot studies (relatively high failure to enroll rates) [4]. The biometrics recognition problem appears to be more difficult than perceived by the pattern recognition research community. Why is biometrics so difficult?

The complexity of designing a biometric system based on three main factors (accuracy, scale or size of the database, and usability) is illustrated in Figure 1. Many application domains require a biometric system to operate on the extreme of only one of the three axes

[2] Many AFIS operations are actually supervised by human experts. FBI can process ~16% of the test images in the "lights out" mode - accept AFIS decisions without any manual inspection.

[3] The technology test [17] data may not be representative of a target application population but the performance is certainly representative of the order-of-magnitude estimate of the best-of-the-breed matcher capability. Operational test [17] performance is expected to be significantly lower than the technology test performance.

in Figure 1 and such systems have been successfully deployed. The grand challenge is to design a system that would operate on the extremes of all these three axes. This will entail overcoming fundamental barriers that have been somehow cleverly avoided in designing successful niche biometric solutions. Addressing these core research problems, in the opinion of the authors, will significantly advance the state of the art and make biometric systems more secure, robust, and cost-effective. This, we believe, will result in a widespread adoption of biometric systems, resulting in broad economical and social impact.

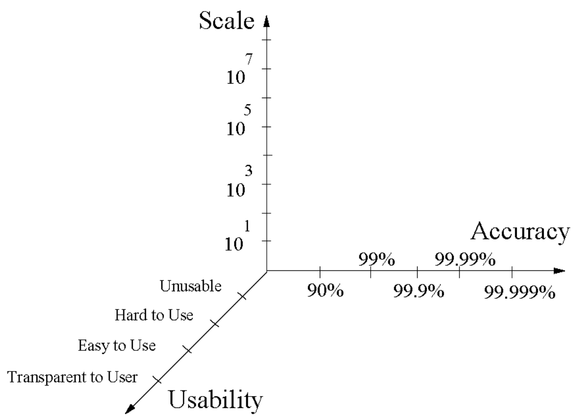

Figure 1: Biometric system characterization. Accuracy axis represents the intrinsic 1:1 accuracy of the matcher.

2. Challenges

Here we categorize the fundamental barriers in biometrics into four main categories: (i) accuracy, (ii) scale, (iii) security, and (iv) privacy.

2.1 Accuracy

The critical promise of the ideal biometrics is that when a biometric identifier sample is presented to the biometric system, it will offer the correct decision. Unlike password or token-based system, a practical biometric system does not make perfect match decisions and can make two basic types of errors: (i) *False Match:* the biometric system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database (in the case of identification/screening) or the pattern associated with an incorrectly claimed identity (in the case of verification). (ii) *False Non-match:* the biometric system incorrectly declares failure of match between the input pattern and a matching pattern in the database (identification/screening) or the pattern associated with the correctly claimed identity (verification). It is more informative to report the system accuracy in terms of a Receiver Operating Characteristic (ROC) curve. Table 1 shows typical error rates of various biometric identifiers and Table 2 shows typical accuracy performance requirements. Even ignoring the requirements of complete automation and assuming viability of good biometric signal acquisition from a distance, it is easy to note that there is a need to bridge the gap between the current technology and performance requirements.

Biome-tric	FTE %	FNMR %	FMR1 %	FMR2 %	FMR3 %
Face	n/a	*4*	*10*	*40*	12
Finger	*4*	*2*	*2*	*0.001*	<1
Hand	2	1.5	1.5	n/a	n/a
Iris	7	6	<0.001	n/a	n/a
Voice	1	*15*	*3*	n/a	n/a

Table 1. Typical biometric accuracy performance numbers reported in large third party tests. FMR1 denotes verification match error rate, FMR2 and FMR3 denote (projected) large-scale identification and screening match error rates for database sizes of 1 million and 500 identities, respectively. n/a denotes data non-availability. The face recognition results are based on FRVT 2002 [12] and its extrapolation using Eyematic data. Fingerprint authentication errors are from [19]. The fingerprint screening assumes use of 2 fingers and fingerprint identification performance reflects state of the art AFIS performance based on 10 fingers. The hand geometry FTE is stipulated from the incidence of severe arthritic condition in the US [28], the voice FTE from the speech disability statistics in the 1997 US census, and iris and fingerprint FTEs from [4] and [29] respectively. Hand, iris, and voice error rates are from ([17], p. 121). These numbers are based on what the authors believe to be order of magnitude estimates of the performance of the state of the art systems. Note that the test results do not use similar test methodology or datasets of similar scale. The technologies may not be directly comparable in the extent of automation possible or sensing-at-a-distance capability.

It is important to realize that unlike other pattern recognition systems, the *reject* option is not a viable option in biometric systems since one will then have to resort to manual identification which many times is neither effective (authentication) nor feasible (e.g., large scale identification). Practical biometric systems also have significant failures both in terms of failure to acquire (FTA) and failure to enroll (FTE).

Application	FNMR%	FMR%
Authentication	0.1	0.1
Large Scale Identification	0.001	0.0001
Screening	1.0	0.0001

Table 2. Typical intrinsic matcher (1:1) performance requirements. It is assumed that large-scale identification consists of 1 million identities and screening involves 500 identities. FTA and FTE are assumed to be zero. These numbers are based on what the authors believe to be order of magnitude estimate of the performance needed for viability of a typical application.

There are three primary reasons underlying imperfect accuracy performance of a biometric system [32]. (i) *Information limitation*: The discriminatory/invariance information content in the pattern samples may be inherently limited due to the intrinsic signal capacity (e.g., individuality information [10]) limitations in the biometric identifier. For instance, the magnitude of discriminatory information in hand geometry is less than that in fingerprints. Consequently, hand geometry measurements can distinguish fewer identities than the fingerprint signal even under ideal conditions. Information limitation may also result due to inconsistent methods of signal acquisition (see Figure 2): differently acquired measurements of a biometric identifier limit the magnitude of invariance across different samples of the pattern. Another example of information limitation is when there is very little overlap between the enrolled and query fingerprints (e.g., left and right half of the finger). In such situation, even a perfect matcher cannot offer correct matching decision. An extreme example of information limitation is when the person does not possess the particular biometric needed by the identification system. (ii) *Representation limitation*: The ideal representation scheme should be designed to retain all invariance and discriminatory information in the sensed measurements. Practical feature extraction systems, typically based on simplistic models of biometric signal, fail to capture the richness of information in a realistic biometric signal resulting in the inclusion of erroneous features and exclusion of true features. Consequently, a significant fraction of legitimate pattern space cannot be handled by the biometric system resulting in high FTA, FTE, FMR, and FNMR. For example, the individuality information contained in minutia-based representation of fingerprints is shown in [10]. Figure 3 illustrates typical "poor quality" prints that cannot be processed by traditional minutiae-based fingerprint identification systems, although the fingerprint experts routinely use such smudged prints to make a reliable match decision. So, conventional representations and feature extraction methods are limiting the effective discrimination among the prints. (iii) *Invariance limitation:* Finally, given a representation scheme, the design of an ideal matcher should perfectly model the invariance relationship in different patterns from the same class. Again, in practice (e.g., due to non-availability of sufficient number of training samples) a matcher may not correctly model the invariance relationship resulting in poor matcher accuracy. Figure 4 illustrates mated fingerprint samples with significant distortion that will fail to match when the matcher assumes a rigid transformation invariance model [23].

Figure 2: Due to change in pose, an appearance-based face recognition system will not be able to match these 3 images successfully, even though they belong to the same individual.

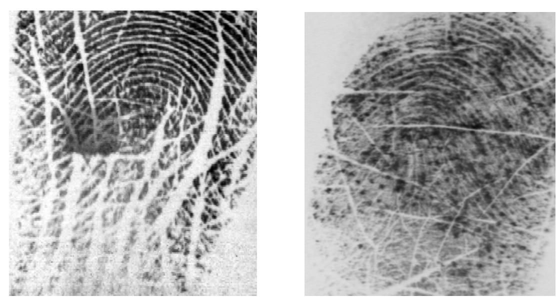

Figure 3: Poor quality fingerprint impressions. Minutiae extraction algorithms detect many false minutiae and miss many true minutiae.

Given a few samples of a biometric identifier, the design challenge is to be able to arrive at a realistic representational/invariance model of the identifier and, then, formally estimate the discriminatory information in the signal from the samples. This is especially difficult in a large-scale identification system where the number of classes/identities is huge (e.g., in the millions). One would also like to understand how to seamlessly integrate multiple biometric cues [20] to

0-7695-2128-2/04 $20.00 (C) 2004 IEEE

provide effective identification across the entire population.

Figure 4: Two (good quality) fingerprint impressions of the same finger exhibiting non-linear elastic deformation. A fingerprint matching algorithm that assumes a rigid transformation between the two fingerprint representations can not successfully match these two prints.

Screening systems are severely information limited. First, the conventional biometric traits that are available for unobtrusive covert capture from a distance (e.g., face and gait) offer limited discriminability. Secondly, the lack of user cooperation as well as lack of environmental control typically results in inconsistent presentation. Consequently, a two-pronged approach is necessary to offer an effective identification in screening systems: (i) exploring effective methods of spatio-temporally utilizing weak biometric cues (also called soft biometrics [21]) such as height, gait, hair color, coarse facial features, etc. to reliably identify people against the watch-list; and (ii) engineered approach to signal acquisition: significant innovation in designing active/purposive vision techniques to foveate on the object of interest to obtain higher resolution imaging which is prerequisite for better discrimination (e.g., [15]). Both these approaches have not received much research attention and are fundamental barriers for the success of screening systems.

2.2 Scale

How does the number of identities in the enrolled database affect the speed performance of the system? In the case of verification systems, the size of the database does not really matter since it essentially involves a 1:1 match. In the case of large scale identification and screening systems containing a total of N identities, sequentially performing N 1:1 matches is not effective (see Table 3); there is a need for efficiently scaling the speed of the system with an increase in the size of the database.

	Authentication	Large Scale ID throughput	Screening throughput
Finger	10 msec	1/min	>1/sec
Face	90 μsec	0.66/min	22/sec
Iris	< 1 μsec	> 1/sec	>2000/sec

Table 3. Achievable scaling performance for commonly used biometric technologies. The fingerprint screening assumes use of 2 fingers and fingerprint identification performance reflects state of the art AFIS performance based on 10 fingers. Face 1:1 matching speed is reported from [12,31]. Iris 1:1 matching speed is taken from [30]. These numbers do not include biometric presentation/feature extraction time and are based on what the authors believe to be order of magnitude estimate of the performance of the state of the art systems. The technologies may not be directly comparable in the extent of automation possible, the customized hardware CPU power, or sensing-at-a-distance capability.

Typical approaches to scaling include using multiple hardware units and coarse pattern classification (e.g., first classifying a fingerprint into major classes such as Arch, Tented Arch, Whorl, Left loop and Right loop). Both these approaches do not perform well in practice. Using hardware linearly proportional to the database size is not feasible. The conventional classification offers only a limited scaling advantage at best (e.g., a factor of two in case of fingerprints) due to non-uniform distribution of patterns among classes, fixed number of classes, and finite classification error rates.

Ideally, one would like to index the patterns similar to the conventional database records. However, due to large intra class variations, it is not obvious how to ensure the samples from the same pattern fall into the same index bin. There have been very few efforts in reliably indexing biometric patterns [9]. Offering a generic efficient indexing technology for biometric patterns would imply effective scalability of large-scale identification applications. Although the size of the watch-list database in a screening system is significantly smaller than that in a large-scale identification, the number of times an identification is conducted may be huge since it is “continuous/active”. Therefore, as in large scale applications, the throughput issues are also critical in screening applications.

Note that the computational requirements for almost real-time scaling of large scale application involving 1 million identities or screening the traffic for 500 wanted identities is beginning to become feasible (Table 3). However, building a real-time identification involving 100 million identities is outside the reach of the existing technology.

2.3 Security

The integrity of biometric systems, i.e., assuring that the input biometric sample was indeed presented by its legitimate owner, and the system indeed matched the input pattern with genuinely enrolled pattern samples, is crucial. While there are a number of ways a perpetrator may attack a biometric system [1], there are usually two very serious criticisms against biometric technology that have not been addressed satisfactorily: (i) biometrics are not secrets and (ii) enrolled biometric templates are not revocable. The first fact implies that the attacker has a ready knowledge of the information in the legitimate biometric identifier and, therefore, could fraudulently inject it into the biometric system to gain access. The second fact implies that when biometric identifiers have been "compromised", the legitimate user has no recourse to revoking the identifiers to switch to another set of uncompromised identifiers. We believe that the knowledge of biometric identifier(s) does not necessarily imply the ability of the attacker to inject the identifier measurements into the system. The challenge then is to design a secure biometric system that will accept only the legitimate presentation of the biometric identifiers without being fooled by the doctored or spoofed measurements injected into the system. Note that such a system obviates the need for revoking the "compromised" identifiers.

One could attempt various strategies to thwart fraudulent insertion of spoofed measurements into the system. For example, one could use liveness detection [7] to make sure the input measurements are not originating from an inanimate object. The other strategy to consider is multi-biometrics [22] - data from multiple and independent biometric identifiers are fused; reinforcing the identity of a subject offers increasingly irrefutable proof that the biometric data is being presented by its legitimate owner and not being fraudulently presented by an impostor. While we can stipulate these different strategies, it remains a formidable challenge to concretely combine these component blocks to arrive at a foolproof biometric system that does not accept fraudulent data.

2.4 Privacy

A reliable biometric system provides an irrefutable proof of identity of the person. Consequently, the users have two concerns: Will the undeniable proof of biometrics-based access be used to track the individuals that may infringe upon an individual's right to privacy? Will the biometric data be abused for an unintended purpose, e.g., will the fingerprints provided for access control be matched against the fingerprints in a criminal database? How would one ensure and assure the users that the biometric system is being used only for the intended purpose and none other? The problem of designing information systems whose functionality is verifiable at their deployed instantiation is very difficult. Perhaps, one needs to devise a system that meticulously records authentication decisions and the people who accessed the logged decisions using a biometric-based access control system. Such a system can automatically generate alarms to the users upon observing a suspicious pattern in the system administrator's access of users' logs. One promising research direction may be biometric cryptosystems [8] - generation of cryptographic keys based on biometric samples. There are also radical approaches such as total transparency [5] that attempt to solve the privacy issues in a very novel way. While one could stipulate some ingredients of the successful strategy, there are no satisfactory solutions on the horizon for this fundamental privacy problem.

3. Discussion and Conclusions

Any system assuring reliable person identification must necessarily involve a biometric component. Because of the unique person identification potential provided by biometrics, they have and will continue to provide useful value by deterring crime, identifying criminals, and eliminating fraud. Biometrics is one of the important and more interesting pattern recognition application with its associated unique challenges.

While this work emphasizes the open fundamental problems in biometrics, this should not be construed to imply that the existing biometric technology is not useful. In fact, there are a large number of biometric solutions that have been successfully deployed to provide useful value in practical applications. For example, the hand geometry system has served as good access control solution in many deployments such a university dorms, building entrance, time/place applications [16]. AFIS systems have been providing terrific value to the society by using a good integration of automatic and manual processes. The scope of this paper is intended to expand the frontiers of the state of the art biometric technology performance for their effective widespread deployment.

It needs to be emphasized that an emerging technology such a biometrics, is typically confronted with unrealistic performance expectations and not fairly compared with existing alternatives (e.g., passwords) that we have resigned to tolerate. A successful biometric solution does not have to be 100% accurate or secure. A particular application demands a *satisfactory* performance justifying the additional investments needed for the biometric system; the system designer can exploit the application context to engineer the system to achieve the target performance levels.

In this work, we have explored the fundamental roadblocks for widespread adoption of biometrics as a means of automatic person identification: effective and efficient pattern recognition; ensuring system integrity and system application integrity. From pure pattern recognition perspective, the large scale identification and screening applications are the two most challenging problems – today we cannot solve them no matter how many resources we throw at them. We really need to understand the effective representation space and the invariance properties much more clearly. From system perspective, both security and privacy are open problems with no clear satisfactory solutions on the horizon. It appears that surmounting these roadblocks will pave the way not only for inclusion of biometrics into mainstream applications but also for other pattern recognition applications.

The recognition problems have historically been very elusive and have been underestimated in terms of the effort needed to arrive at a satisfactory solution. Additionally, since humans seem to identify people with high accuracy, biometrics has incorrectly been perceived to be an easy problem. There is no substitute to realistic performance evaluations [27] and sustained R&D investment for achieving sustained improvements in pattern recognition solutions. Standardization efforts [2] will facilitate the cycle of build-test-share for transforming the technology into business solutions.

Considering the recent mandates of several governments for the nationwide use of biometrics in delivering crucial societal functions, there is a need to act with a sense of urgency. Pattern recognition systems have never been tried at such large scales nor have they dealt with such a wide use of sensitive personal information. As pattern recognition researchers, it is a great opportunity and challenge for us to make a difference in our society while engaged in the work that we love to do.

Acknowledgements

The authors would like to thank Anoop Namboodiri and Karthik Nandakumar of Michigan State University for their helpful suggestions.

4. References

1. L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication", *Proceedings of* the *IEEE*, Vol. 91, No. 12, Dec. 2003, pp. 2019-40.
2. R. McCabe et al., "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability", NIST Report to Congress, Appendix A, 2002.
3. S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security & Privacy Concerns", *IEEE Security and Privacy Magazine*, Vol. 1, No. 2, pp. 33-42, March-April 2003.
4. BBC News, "Long lashes thwart ID scan trial", 7 May 2004, news.bbc.co.uk/2/hi/uk_news/politics/3693375.stm
5. D. Brin, *Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Addison-Wesley, April 1998.
6. S. Furui, "Recent Advances in Speaker Recognition", *Pattern Recognition Letters*, Vol. 18, No. 9, 1997, pp. 859-872.
7. R. Derakhshani R, S.A.C. Schuckers, L. Hornak, L. O'Gorman, "Determination of Vitality From A Non-Invasive Biomedical Measurement for Use in Fingerprint Scanners", *Pattern Recognition*, No.2, pp. 383-396, 2003.
8. U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", *Proceedings of the IEEE*, *Special Issue on Enabling Security Technologies for Digital Rights Management*, Vol. 92, No. 6, June 2004.
9. R. Germain, A Califano, and S. Colville, "Fingerprint matching using transformation parameter clustering", *IEEE Computational Science and Engineering*, Vol. 4, No. 4, pp. 42--49, 1997.
10. S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 24, No. 8, pp. 1010-1025, August 2002.
11. T. Kanade, *Computer Recognition of Human Faces*. Birkhuser Verlag, Stuttgart, 1977.
12. P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J.M. Bone, "FRVT 2002: Evaluation Report", http://www.frvt.org/DLs/FRVT_2002_Evaluation_Report.pdf, March 2003.

13. Lee Gomes, "Can Facial Recognition Help Snag Terrorists?", *The Wall Street Journal*, September 27, 2001.
14. NYC Visit homepage, http://www.nycvisit.com/content/index.cfm?pagePkey=57.
15. A. Hampapur, S. Pankanti, A.W. Senior, Y-L Tian, L. Brown, and R. Bolle, "Face Cataloger: Multi-Scale Imaging for Relating Identity to Location", *IEEE conference on Advanced Video and Signal Based Surveillance*, Miami, FL, July 21-22, 2003.
16. A. K. Jain, R. Bolle, S. Pankanti (eds), *Biometrics: Personal Identification in Networked Society.* Kluwer Academic, December 1998.
17. R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, *Guide to Biometrics.* Springer, 2003.
18. H. T. F. Rhodes, *Alphonse Bertillon: Father of Scientific Detection*. Abelard-Schuman, New York, 1956.
19. FVC2004: Fingerprint Verification Competition, http://bias.csr.unibo.it/fvc2004.
20. A. Ross and A. K. Jain, "Information Fusion in Biometrics", *Pattern Recognition Letters*, Vol. 24, Issue 13, pp. 2115-2125, September, 2003.
21. A. K. Jain, S. C. Dass and K. Nandakumar, "Soft Biometric Traits for Personal Recognition Systems", To appear in *Proceedings of International Conference on Biometric Authentication*, Hong Kong, July 2004.
22. A. K. Jain and A. Ross, "Multibiometric Systems", *Communications of the ACM*, *Special Issue on Multimodal Interfaces*, Vol. 47, No. 1, pp. 34-40, January 2004.
23. A. Ross, S. Dass and A. K. Jain, "A Deformable Model for Fingerprint Matching", To appear in *Pattern Recognition*, 2004.
24. U.V. Chaudhari, J. Navratil, G.N. Ramaswamy, R.D. Zilca, "Future speaker recognition systems: Challenges and solutions" *Proceedings of AUTOID-2002*, Tarrytown, NY, March 2002.
25. "Streamlined airport services take flight – Case study", http://www.eds.com/case_studies/bgaa.pdf.
26. "Airport tests passenger eye IDs", http://news.bbc.co.uk/2/hi/uk_news/1808187.stm.
27. J. L. Wayman, "Technical Testing and Evaluation of Biometric Identification Devices", in *Biometrics: Personal Identification in Networked Society.* Kluwer Academic, December 1998.
28. National Center for Chronic Disease Prevention and Health Promotion http://www.cdc.gov/nccdphp/burdenbook2002/05_arthritis.htm.
29. NIST report to the United States Congress, "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability." Available at ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf, November 2002.
30. J. G. Daugman, "High Confidence Visual Recognition of Statistical Independence", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vo1. 5, No. 11, pp. 1148-1161, 1993.
31. Eyematic homepage, http://www.eyematic.com.
32. A. K. Jain and S. Pankanti, "Biometrics Systems: Anatomy of Performance", *IEICE Transactions Fundamentals*, Vol. E84-D, No. 7, pp. 788-799, 2001.