RC22203 (W0110-041) October 12, 2001
Mathematics

IBM Research Report

Biometric Technologies ... Emerging Into the Mainstream

Rudolf M. Bolle, Jonathan Connell, Arun Hampapur, Ehud Karnin, Ralph Linsker, Ganesh N. Ramaswamy, Nalini K. Ratha, Andrew W. Senior, Jane L. Snowdon, Thomas G. Zimmerman
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

Research Division
Almaden - Austin - Beijing - Delhi - Haifa - India - T. J. Watson - Tokyo - Zurich

Biometric Technologies ... Emerging into the Mainstream" was the theme for the Biometric Consortium 2000 Conference held September 13-14, 2000 in Gaithersburg, Maryland. In light of governments and airlines seeking to reduce the threat of hijackings by terrorists, biometrics has come into the spotlight and will likely enter the mainstream more quickly than previously anticipated.

Enhancing security at airports and other public and private buildings requires the solution of two key problems: 1) knowing the identity of people within a space and 2) knowing the activities of people and being able to provide timely warnings. Biometrics addresses the first question and visual surveillance and monitoring addresses the second.

Biometric systems are concerned with verifying (or authenticating) and identifying a person based on his or her physiological or behavioral characteristics. Examples include fingerprint, hand geometry, iris, voiceprint recognition, and face recognition; these five biometrics account for 95% of the market. These five biometrics together with online signature verification will be discussed in this paper. Verification answers the question "Are you the person you claim to be?" and assumes a good reference for the authentic person exists. Authentication is a one-to-one test. Existing user authentication techniques are described in Table 1. Identification answers the question "Who is this person?" or more precisely "Is this person a member of this group?" It is a much more difficult question because it requires a one-to-N matching. Using biometrics in combination enhances the automatic identity and verification of a person. The interested reader is referred to Liu and Silverman (2001) and Ratha, Senior, and Bolle (2001) for tutorial articles on biometrics.

Table1. Existing User Authentication Techniques (Source: Ratha, N. K., J. H. Connell, and R. M. Bolle, "Enhancing Security and Privace in Biometrics-based Authentication Systems," IBM Systems Journal, Vol. 40, No. 3, 2001, 614 - 634.)

METHOD	EXAMPLES	PROPERTIES
What you know	User ID Password PIN	Shared Many passwords easy to guess Forgotten
What you have	Cards Badges Keys	Shared Can be duplicated Lost or stolen
What you know and what you have	ATM Card + PIN	Shared PIN a weak link (writing a PIN on the card)
Something unique about the user	Fingerprint, Hand Face Iris Voice print	Not possible to share Repudiation unlikely Forging difficult Cannot be lost or stolen

Privacy concerns and the possible sharing of biometric data among law enforcement agencies or commercial enterprises have slowed the development and deployment of these technologies. Enhancing airport and aircraft security must be a collective responsibility by all the stakeholders: passengers, airlines, airports, and governments around the world. Continuity of identity throughout the entire journey is the key to improved security. Passengers, airport visitors, crew and all support personnel must be identified in a secure way and validated at various points throughout the journey or shift. Futhermore, collected data must be accessible universally and maintain privacy. Currently, information about undesirable individuals is stored on a "watch list" in different databases from the CIA, FBI, National Security Agency, Immigration and Naturalization Service, and local and state agencies. The problem is getting at the data and being able to analyze it, which requires both business intelligence software and application integration. Neither a single database nor an enterprise application integration technology is in place that would alert the airlines, for example, of a potentially undesirable passenger checking in at an airport. Local, state, and federal law enforcement systems must hook their systems into both international law enforcement and airport database systems worldwide.

The International Air Transport Association (IATA) formed an initiative in 2000 called Simplify Passenger Travel (SPT). The SPT initiative calls for biometrics to solve the following problems:

- Current process is not-customer friendly
- Air traffic will double again this decade
  - 453 million international passengers in 1998
  - 906 million international passengers predicted by 2010 (or 2012 conservatively).
- Safety and security concerns will not go away
- Facilities expansion / reconfiguration is costly.

The precedents to SPT include:

- Schiphol Travel Pass - Amsterdam, 1990.
- U. S. Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) - 1993 to present.
  - INSPASS is an automated immigration inspection system that utilizes hand geometry biometric imaging to identify and process pre-enrolled, low-risk frequent flyers. Arriving at a port-of-entry, the INSPASS traveler proceeds directly to an INSPASS automated inspection kiosk, inserts a card issued or registered at enrollment, and responds to kiosk touch-screen display messages to enter their flight number (non-APIS flights only) and place their hand in a hand geometry reader. The kiosk validation system uses display screen animation to achieve correct alignment of the hand with the hand reader, compares the scan of the traveler's hand geometry to the image captured at enrollment (stored in the secure Global Enrollment System database), prints a departure receipt for the traveler and directs the traveler to proceed to U.S. Customs. A traveler who is unsuccessful in completing the process is referred to an Immigration Inspector in a nearby inspection booth. INSPASS is operational in 9 airports: Los Angeles, Miami, Newark, New York (JFK), San Francisco, Toronto, Vancouver, Detroit, and Washington-Dulles. INSPASS eligible travelers are citizens of the United States, Canada, Bermuda, and Visa Waiver Pilot Program (VWPP) countries who travel to the U.S. on business 3 or more times a year, are diplomats or international organization representatives, or are airline crew from VWPP nations.

Persons ineligible to enroll in INSPASS are those who need a waiver to enter the U.S. or those with a criminal record. INSPASS uses the HandKey hand geometry verifier from Recognition Systems, Inc., Campbell, Calif.

- Fastgate - Bermuda International Airport, 1997
  - Fastgate, developed by IBM's Hursley Laboratory in the U.K., is an automated passenger clearance system using hand geometry biometrics, analagous to INSPASS, to verify a traveller's identity. Fastgate was piloted at Bermuda International Airport beginning in 1997 and is still installed today. Information, such as name, address, date of birth, and passport number is recorded on a standard credit, frequent traveller or other commercial card, while the traveller's biometric is digitally recorded at any airport offering the Fastgate service. Once enrolled, the traveller simply inserts the card into a kiosk reader at the airport. Fastgate retrieves the traveller's information from the database and compares the biometric information to verify identity. Travellers use a touch screen to answer a few simple questions. The computer checks the data against information held on computers and also makes sure there are no arrest warrants out or requests to intercept the traveller. In general, the process takes less than 15 seconds to 'clear' the traveller through an immigration checkpoint. Fastgate uses the HandKey hand geometry verifier from Recognition Systems, Inc., Campbell, California and compares the biometric data with an IBM-run database (DB2, message and transaction processing via MQSeries and CICS, system and network management capabilities via TME10, and a secure worldwide private network via IBM Global Network).
- Expedited Passenger Processing System (EPPS) - Canada, 2001.
  - EPPS is an automated customs system that uses hand geometry biometrics to authenticate pre-approved air travellers and automated kiosks for declaring and paying duties and taxes. These travellers will be able to go through customs without having to talk to a customs officer, unless they are stopped for a spot check. Under the proposed joint Canada/U.S. Intransit Preclearance initiative, travellers who are in transit through major Canadian airports on their way to the United States will not have to clear Canadian customs, but instead will be able to proceed directly to U.S. Pre-clearance.

IATA proposed the following SPT vision for passenger processing with three biometric identity checkpoints as depicted in Figure 1. The key message here is that passenger identity must be established in a secure way and must be validated at various points throughout the journey from the method used to make a reservation (telephone, corporate travel company, IP address from a personal computer), to ensuring that the person who checked-in is the same person who passes the security and customs and immigration checkpoints, the same person who boards the aircraft, and the same person who collects his or her baggage at the destination. This concept must be expanded to also include non-traveling airport visitors, airline and airport employees as described in a later section of this report.

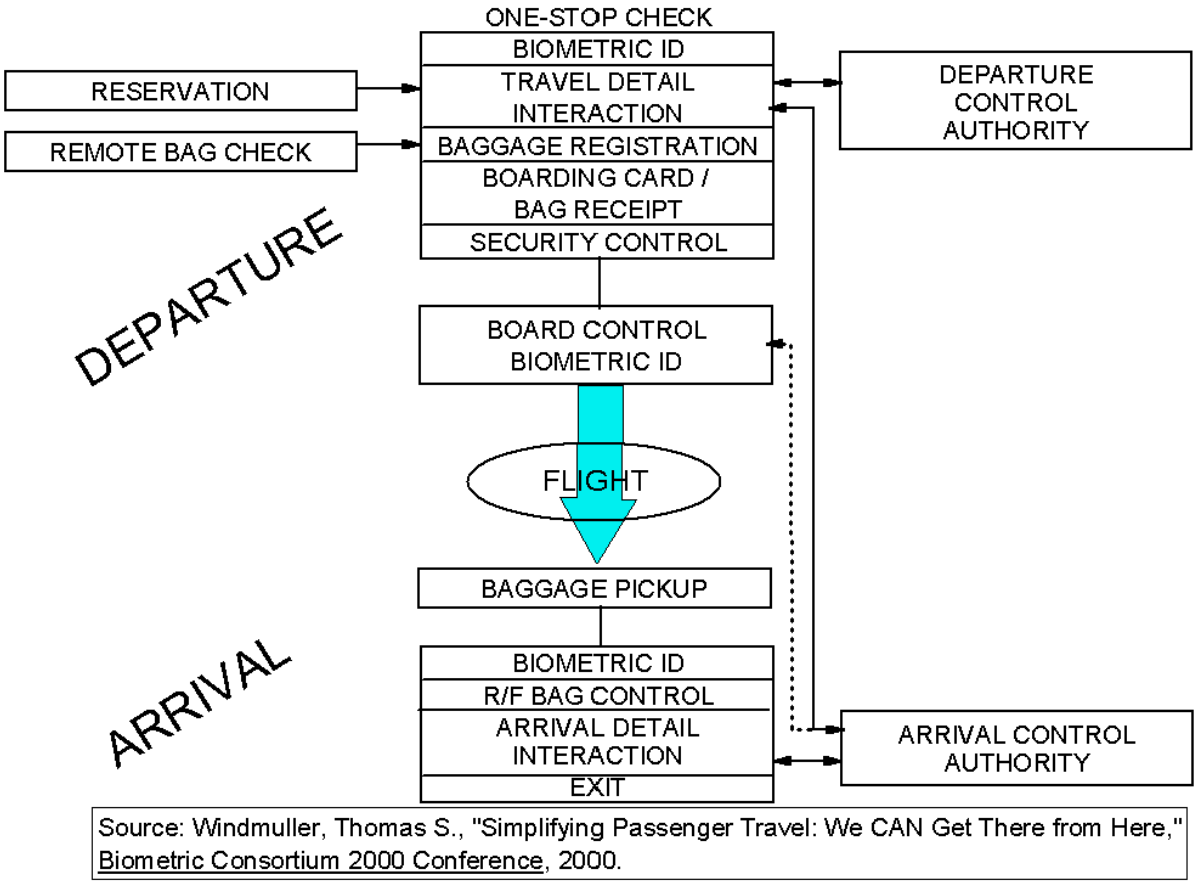

Figure 1. IATA SPT Vision

Hand Geometry

One way to identify a person is to measure the unique geometry of their hand. Feature extraction involves computing the widths and lengths of the fingers at various locations using the captured image. These metrics define the feature vector of the user's hand.

Hand geometry has been used for physical access and time & attendance at a wide variety of locations, including Citibank data centers, the 1996 Atlanta Olympics and New York University dorms. The University of Georgia uses hand geometry to verify students when they use their meal card. At Walt Disney World, season pass holders place two fingers in a hand geometry reader to gain physical access to the park. As mentioned above, the U. S. Department of Immigration and Naturalization Services has implemented INSPASS and IBM piloted and installed Fastgate in production at Bermuda International Airport.

The hand-scan market is dominated by Recognition Systems Inc. (RSI), a division of equipment manufacturing giant Ingersoll-Rand. Founded in 1986, RSI has focused on applying its patented hand-scan technology in areas such as access control and time and attendance.

Pros:

- Public acceptance. Used at Disney World, INSPASS, University of Georgia
- Good for verification, not for identification
- Easy to self-administer

Cons:

- Poor for identification
- No international database, but is the INSPASS database growing?
- Contact based sensing

IBM Experience:

- Fastgate pilot and implementation at Bermuda International Airport
- 1996 Atlanta Olympics
- Walt Disney World

Fingerprints

Fingerprints are a distinctive feature and remain invariant over a person's lifetime, except for cuts and bruises. Fingerprint authentication requires acquiring and digitizing a fingerprint impression. The digital image of the fingerprint includes several unique features in terms of ridge bifurcations and ridge endings, collectively referred to as minutiae. The next step is to locate the minutiae in the fingerprint image using an automatic feature extraction algorithm, which analyzes spatial relationships. Finally, a matching system attempts to arrive at a degree of similarity between the stored image and the fingerprint sample.

IBM Research has a unique differentiator called FLASH (Fast Lookup Algorithm for Structural Homology). FLASH is a large-scale fuzzy search engine, which contains sophisticated combinatorial pattern matching algorithms to deliver technology and applications in the most

diverse domains from computational biology and genetics to rational drug design and discovery, to fingerprint matching. FLASH technology (a search algorithm for images) is fast and accurate. It can search a database of tens of millions of records in a few seconds to determine whether there is a match. FLASH technology was used for a fingerprint-based voter registration verification system in Peru to prevent voter fraud. FLASH is fast because an elaborate representation of the fingerprint database, or indexing structure, is constructed during enrollment of the population. This indexing structure was developed in tandem with IBM's fingerprint image analysis software that extracts minutiae. More details on the availability of fingerprint authentication software from IBM Research can be found at: http://w3.research.ibm.com/ecvg/biom/fp-sdk.html.

The top fingerprint scanner vendors are: Identix, DBI, and Crossmatch, all of whom are FBI certified. They also offer low-resolution non-FBI compliant fingerprint scanners. The top non-optical scanner vendors are Veridicom, Infineon, and Authentec.

Identix Inc. (Sunnyvale, Calif.; www.identix.com), a provider of live-scan identification and biometric imaging systems, is providing the U.S. Immigration & Naturalization Service (INS) with TouchPrint 600 live-scan fingerprint image systems. Identix's devices combine optical scanning technology, image processing software and pattern-matching algorithms. The TouchPrint systems will be employed by the INS at centers nationwide to screen individuals from other countries applying for various benefits and entitlements ranging from work cards to citizenship. While this is the first use of Identix technology by the INS for benefits verification, the enforcement arm of the agency has used the TP-600 for some time, primarily at deportation centers. The deployment by the INS of Identix single-digit scanners is a part of Ident, a security network extending along the U.S./Mexico border from California to Texas, as well as the use of Identix equipment for identification and verification at other major ports of entry throughout the U.S. In an experiment conducted by IBM Hursley lab, IBM's fingerprint authentication software performed very well against Indentix for the FBI compliant sensors. IBM has not compared against their other scanners, which may not be relevant in the present application.

NEC Technologies is a big player in the AFIS for law enforcement agencies and holds about 60 percent of the U. S. market. Back in 1970's NEC made a big impact in California when they solved a major crime matching a scene-of-crime latent print. NEC's biggest client is probably the California Department of Justice, which, along with various other agencies that operate through its database, uses the company's file log of 40 million prints to match over 12,000 prints a day. The other players are Prinrak and Sagem-Morpho. These big AFIS vendors do not operate in the fingerprint authentication area directly. They buy technology from small vendors. For example, NEC used to sell ABC's software and hardware for online authentication. The criminal ID systems are different in the sense that they ask for all 10 fingers and the associated latent fingerprint matchers do not match against large databases.

Pros:

- Long tradition of use as immutable identification in law enforcement
- Large existing database. California, Colorado, Florida, and Texas Department of Motor Vehicles are working to establish a fingerprint biometric system for drivers licenses and record data.
- Good for forensic investigation. Criminal often leaves a trail of fingerprints (e.g. hotel, car, door knob, glass, weapon).
- Can be collected using low-tech means and converted into digital form.
- Low cost readers (under $100)

Cons:

- Public acceptance in some countries due to association with criminal activity.
- Contact based sensing
- Can be hard to get a good read with old, cold, greasy, cut or bruised fingers

IBM Experience:

- IBM Research participated in the NCITS/ANSI B10.8 Minutia Standardization effort. Participants included U.S. state and Canadian province government representatives, FBI, NIST, standards representatives from financial/banking (X9), and biometric vendors from the U. S. and abroad. The objective was to propose a format for fingerprint minutia data that would be readable across state and province boundaries for driver's licenses. The broader objective was to propose a format that could be used beyond motor vehicle application, a standard for fingerprint data. The result is the AAMVA national standard for the driver license/identification card (http://www.aamva.org). Two vendors, IBM and Veridicom, were asked to implement the common fingerprint minutia exchange format to demonstrate that it is possible for some fingerprint minutia matchers to inter-operate.
- FLASH search algorithm and fingerprint authentication software from IBM Research
- Voter registration verification system for Peru
- IBM's Personal Computer Division works with Digital Persona for fingerprint solutions (contact John Nicholson)

IBM Capability:

1) Finger biometric technologies we can provide that are truly unique:
- FLASH for fingerprint Identification
- Cancellable biometrics (research level)

2) Fingerprint biometric technologies where others can do it (have done it) but IBM should be listened to because IBM can do it better/faster/cheaper/broader:
- IBM Fingeprint Authentication SDK
- Integrating biometrics with smartcards

3) Fingerprint biometric technologies where IBM cannot claim to do it better etc but can claim unrivaled ability to integrate better than anyone else:
- Evaluating proper biometrics technology applicable to a problem (e.g., evaluate if a particular fingerprint solution is as accurate as claimed)

Face Recognition

There are a number of applications of face recognition including surveillance, database lookup, video indexing, secure computer logon, and airport and banking security. Face recognition (and face understanding) requires acquiring face images (color or black and white) from video tape, MPEG, live camera, photograph (passport or driver's license), or a database of undesirable individuals. IBM Research's face recognition system automatically finds all faces in the input image, using a combination of features such as motion, skin-tone (robust to different skin colors) and face-like appearance, and then finds eyes, nose and mouth within the face. Faces are identified by comparing local features with those for faces stored in a database. Partial matches allow recognition even though glasses or beards have changed, for instance, or if sunglasses are being worn. Face recognition can be used in two modes: identification (picking one person out in a database of many) and verification (confirming a claimed identity, such as with a computer logon or an ATM). This system can store the facial features on a smartcard. The system derives information useful for other applications particularly in Human-Computer Interaction, such as detecting user presence and gaze direction, lip-reading, and facial expressions.

Face recognition requires that the face image be above a minimum resolution and performs poorly when the face pose and expression are not neutral. Current face recognition systems need user compliance to ensure the quality of the face image. Dynamic face recognition is an emerging technology where high quality face images are acquired without requiring user compliance. Further discussions of dynamic face recognition are presented in the section of Visual Surveillance and Multiscale Tracking.

The top suppliers of facial recogntion systems are Viisage Technology and Visionics. Viisage Technology supplies facial recognition and fingerprint imaging identification systems to customers in 13 U.S. States, which use Viisage products in their motor vehicle departments and other agencies, and to the US Immigration and Naturalization Service. Visionics is a biometrics firm specializing in face and also fingerprint recognition. Visionics' whitepaper on biometrics & counterterrorism is a well-reasoned discussion of the general air security issue, with special reference to biometrics. See
http://www.visionics.com/newsroom/downloads/whitepapers/counterterrorism.pdf
Visionics has outperformed competitors in Department of Defense face recognition tests (please refer to http://www.dodcounterdrug.com/facialrecognition/DLs/FRVT_2000.pdf).

A pilot project conducted by IBM at an airport allows passengers to self check-in and board using a personal digital assistant (PDA). The PDA runs a microbrowser wirelessly networked to a server. Software connects PDA, gate readers, and displays to the legacy departure control system. Gate readers cause digital photographs of passengers to appear during boarding for security check. Flight attendants and reception desks receive digital photographs, that have been retrieved from the airline's secure server, and flight records of passengers as they approach to allow personalized greetings and to perform face recognition manually.

Pros:

- Public acceptance. No criminal association. Photos are widely used in passports and drivers licenses.
- Non intrusive and contactless. Can function in a crowd, real-time
- Works with photographs, videotape, or other image sources
- Good for verification.

Cons:

- Need good lighting
- Poor for identification, better for verification.
- Individuals have option of disguising the face

IBM Experience:

- Airport self check-in (manual face recognition)
- IBM's Personal Computer Division works with Visionics for face recognition (contact John Nicholson).

IBM Capability:

1) Face recognition biometric technologies we can provide that are truly unique:
- Work on fusion with speaker ID for video indexing (research level)
2) Face recognition biometric technologies where others can do it (have done it) but IBM should be listened to because IBM can do it better/faster/cheaper/broader:
- None
3) Face biometric technologies where IBM cannot claim to do it better etc but can claim unrivaled ability to integrate better than anyone else:
- None

Voice-Print Recognition and Conversational Biometrics:

Voice biometrics has a unique advantage over other biometrics because is relies on human speech, which is the primary modality in human-to-human communication, and provides a non-intrusive method for authentication. By extracting appropriate features from a person's voice and modeling the *voiceprint*, the uniqueness of the physiology of the vocal tract and the articulatory properties can be captured to high degree and used very effectively for recognizing the identity of the person. Recognizing a user based on voiceprints is commonly known as *speaker recognition* in the academic community, encompassing speaker verification, speaker identification, speaker classification, speaker segmentation and speaker clustering. Speaker recognition accuracy has improved significantly over the last few years, and a recent independent study compares speaker recognition very favorably with respect to fingerprint recognition and other biometrics [Mansfield, et.al. (2001)].

International Data Corporation (IDC) expects voice biometrics to have the highest growth rate (excluding hardware) among all biometrics. The analysis is supported by straightforward observations regarding the convenience aspect of using voice as the biometrics for authentication because it is non-intrusive compared to other forms of biometrics, and does not need any

additional hardware, since PC microphones and telephones (including mobile phones) are everywhere. And when used in a *text-independent* mode (i.e. no constraints on the words to be spoken), voiceprint recognition offers many other advantages. Users do not have to remember passwords or passphrases. Users do not have to go through a separate process for verification, since anything they say as part of the transaction dialog can be used to verify their identities, resulting in a truly integrated and non-intrusive verification process. Verification can take place continuously or periodically in the background as needed (when fraud is suspected in the middle of the dialog, for instance), or at anytime after the transaction is completed by recording the spoken command and analyzing it later for voiceprint match. Verification can also take place in an incremental manner, and the user may be granted higher privileges if higher verification scores are obtained with more speech data collected as the dialog progresses. The verification data can also be used to update the speaker models online, thereby capturing any additional acoustic evidence or changes in acoustic characteristics of the user's voiceprints. Text independent verification is usually also language independent, and the user can speak in multiple languages or different languages for enrollment and verification.

Speaker recognition based on voiceprints, or *acoustic* speaker recognition, may be sufficient for a wide variety of applications. However, when higher accuracy or greater flexibility is desired, multiple biometrics sources may be combined. Unlike other biometrics, voice contains two information sources for user recognition, namely acoustic voiceprints and knowledge, and hence the user does not have to go through two different processes (which would be the case if we were to combine face detection and fingerprint recognition, for example). By analyzing the *same* spoken input for acoustic voiceprint match and knowledge match, we can provide higher accuracy or greater flexibility, or both, without any added inconvenience to the user. Voiceprint match scores are generated using a text-independent speaker recognition engine, and knowledge match scores are generated using a conversational interface consisting of speech recognition, natural language understanding, and dialog management components. Combining voiceprint recognition with knowledge-based recognition is called *conversational biometrics*, since we are examining multiple biometrics evidence present in a conversation.

A conversational biometric systems engages in a natural language dialog with the user, presents randomly generated questions, and collects the user's responses. When appropriate, the conversation may be embedded into the natural transaction dialog. The questions to be asked can be randomly generated from a large collection of questions and answers that the user provides during an explicit knowledge enrollment stage (e.g. "what is your favorite color?") , or may be generated from user-specific information available from the application (e.g. "what is the balance in your last statement?"). A policy management module generates a policy dynamically for each transaction, based on the application requirements. The policy specifies the maximum number of questions to be asked, and the minimum number of correct answers, or alternatively, the policy may specify the minimum score needed for the knowledge match. The policy also specifies the minimum score required for the acoustic voice-print match, and may adaptively modify the maximum number of questions to be asked, based on the voice-print match scores. By generating appropriate policies, we can provide higher accuracy or greater flexibility, or both. False acceptance rates below 10e-12 % are possible, making conversational biometrics very attractive for high security applications [Maes, et.al (2001), Ramaswamy(2001)].

According to International Data Corporation (IDC), the major vendors of voice authentication products are T-Netix, ITT, Nuance, and Veritel. The offerings from all of these vendors are still based on text-dependent acoustic-only speaker verification. Among these vendors, Nuance seems to have the most promising offering. Nuance conducted a pilot study with Home Shopping Network (HSN), where voice biometrics was used for both speaker verification and for speaker identification, based on home phone number. Voice is used for providing secure access to customer record and credit card information, and also to enable HSN operators to provide a more personalized shopping experience to the customers.

IBM's strength lies in a number of different areas. First, a variety of compensation techniques, including handset normalization, target normalization, feature warping, short-time Gaussianization, and speaker model synthesis techniques have been developed and enhanced to ensure robust speaker recognition under noisy and mismatched conditions [Navratil, et.al. (2001)]. As a result, speakers enrolled using one connection environment (e.g. analog landline telephone) can be verified using a different connection environment (e.g. GSM cellphone), even under moderately noisy conditions. To further strengthen the recognition process, IBM has developed conversational biometrics which combines acoustic voiceprint recognition with knowledge-based recognition, and more than 60 invention disclosures have been filed, covering various aspects of robust acoustic voiceprint recognition, knowledge-based recognition, and multi-biometrics combination [Ramaswamy (2001)].

Pros:

- Very high accuracy and flexibility when combined with knowledge verification
- Non-intrusive authentication.
- Incremental authentication (e.g. wait for more voice/knowledge data when higher degree of recognition confidence is needed)
- Continuos authentication, maybe embedded in natural dialog
- Background authentication
- Public acceptance. No criminal association.
- Inexpensive hardware, suitable for pervasive security management

Cons:

- Performance degrades under severe environmental noise
- Lack of public awareness of recent innovations makes market penetration and deployment more challenging

IBM Experience:

- Conversational biometrics technology from IBM Research, including 60+ invention disclosures. VIVA (Verbal Identification & Verification Agent) prototype for the telephony environment. For a demostration of the prototype, see: http://voiceprint.watson.ibm.com/VIVA/VIVA_html/viva.html
- NIST-2001 Speaker Recognition Evaluations: IBM was placed in the top cluster.

- Speaker recognition engine incorporated into a restricted product for a customer engagement (with Virage), as part of the ViaVoice Broadcast News solution, which is still in use by the customer.
- Adventurous Systems and Software Research (ASSR) project on large population speaker recognition, completed in 2000. This is the only known published work in speaker recognition addressing population size of 10000+ speakers [Chaudhari, et.al. (2001)].

IBM Capability:

- Biometric technologies we can provide that are truly unique:
  Conversational biometrics, to combine voiceprint recognition with knowledge-based recognition using an integrated conversational interface
- Biometric technologies where others can do it (have done it) but IBM should be listened to because IBM can do it better/faster/cheaper/broader:
  Text-independent acoustic voiceprint recognition, with techniques to handle mismatch conditions
- Biometric technologies where IBM cannot claim to do it better, etc., but can claim unrivaled ability to integrate better than anyone else:
  Combining conversational biometrics with other biometrics where IBM lacks experience (e.g. iris recognition)

Iris:

The origins of iris recognition technology date back to the late 19th century, about the same time fingerprints were gaining acceptance as a forensic tool. At this time, French criminologist Berthillon did exploratory work linking iris patterns to prisoner identity. It took over a century to make the leap to high tech, when, in the 1980s, opthamologists Leonard Flom and Aran Safir posited that no two irises were alike and could be the basis of a human authentication technology. Their 1987 concept patent was followed seven years later by Dr. John Daugman's (Cambridge) patent on the algorithms in 1994 and IrisCode® generation (the IrisCode is a 512-byte digitized record that is created from the video image produced after an individual glances into the camera) and one-to-many matching that gives this technology its unmatched robustness as an authentication tool. Iridian Technologies is the holder of exclusive U.S. and international patents (including John Daugman's) on the core concepts and technologies behind iris recognition technology. IBM Research has limited experience in iris scanning biometrics. While Iridian holds the algorithmic patents, of course this doesn't preclude IBM partnering with them (or their partners) for system integration.

According to the Washington Times on July 27, 2001, EyeTicket, a small, privately held company, will install iris-recognition cameras at its immigration checkpoints in terminals three and four in Heathrow, probably by October, for a six-month trial. Only North American passengers traveling to Heathrow on British Airways or Virgin Atlantic flights from Washington Dulles International Airport and from airports in Chicago, New York, Boston, Miami, Los Angeles, Detroit, Seattle, Philadelphia and San Francisco are eligible to enroll and participate in the limited trial. Once passengers enroll, they won't have to stop at British Immigration Service checkpoints. Instead, they will have their identity verified when they have their iris matched

against a photograph in a database, a process that takes about 2 seconds. EyeTicket, British Airways, Virgin Atlantic, the British Immigration Service, and the Customs and Excise Department will share the cost of the Heathrow program. US Airways pilots at Charlotte/ Douglas International Airport in North Carolina have used equipment developed by EyeTicket since May 2000 to gain entry to restricted areas. The patent on iris-scanning technology is held by Iridian Technologies, in Marlton, N.J. EyeTicket received a patent last year that covers its method of ticketing and checking in airport passengers.

In June, 2001 EyeTicket Corporation and Unisys Corporation jointly announced a new strategic marketing alliance under which Unisys will offer the EyeTicket passenger processing system to its customers. The two companies signed a Memorandum of Understanding defining the principal business terms of the alliance, which has an initial term of two years. The agreement provides that Unisys will offer EyeTicket systems to Unisys customers seeking iris recognition-based systems for ticketing, check-in, baggage check, baggage identification and boarding in all airport and airline applications for commercial aircraft passengers. The alliance will provide further optional marketing opportunities for each company. Unisys is authorized to offer EyeTicket products for other applications as desired, and EyeTicket can take advantage of Unisys installation and support services as desired for its worldwide projects.

Pros:

- Believed to be most accurate.
- No contact with subject
- Does not need much operator training
- Public acceptance. No criminal association.

Cons:

- No database of iris scans. More useful for verification than identification.
- Readers are expensive
- Small field of view, made need to be tilted for short or tall subjects.
- Performance may be impaired with tinted glasses or sunglasses
- Biometric not left as evidence (can only be read on-line)

IBM Experience:

- Very limited.

Online Signature Verification

The need for a reliable means of personal identification presents a challenge to almost any large modern organization. This system provides multimedia application developers with an engine for online signature verification. Unlike offline verification, online verification uses not only the shape of an individual's signature, but actually logs the pen timing throughout the duration of the signing process.

The system learns user's signature from examples (say 6 signatures samples), and after that it can verify the signatures with high precision. Some additional features, like image compression, are

also available. Verification of signatures can be captured on tablets (e.g., PalmPilot). A prototype is available; examples can be found at: http://w3.haifa.ibm.com/Projects/Image/sigver/sigver.html.

Online signature verification could be used as one possible means of biometrics to verify passenger identity once the integrity of the passport has been verified.

Pros:

- Forgery is detected even when forger managed to get a copy of the authentic signature.
- Possibility to detect inconsistent user on the stage of enrollment
- Fast and simple training
- Cheap hardware (no pressure information is required, so almost any tablet device is allowable)
- Little storage requirements
- Fast response (about 1 sec per signature on the "old" 486DX-33 computer)
- The results do not depend on the native language of the user
- You can use any kind of information as your signature: name, second name, or even nice curves
- Very high compression rate (100-150 bytes are needed to keep the shape of the signature)

Cons:

- New procedure, may not be accepted by passengers.

Integrating Biometrics

There comes a stage in the development of any biometric authentication system where it becomes increasingly difficult to achieve significantly better accuracy from a biometrics and the need to explore other sources for improvement becomes a practical necessity.

Multiple biometrics can alleviate several practical problems in the biometrics-based personal identification. Although a biometrics is supposed to be *universal* (each person in the target population should possess it), in practice, no biometrics truly is. For instance, a small fraction of the population possesses fingerprints which are not easily captured by the representations (features) adopted by a given system. Further one single biometrics may not be acceptable to different sections of the target population and one could give users a choice of biometrics. In addition, and probably most important, reinforcement of evidence from multiple independent biometrics offers increasingly irrefutable proof of the identity of the authorized person.

IBM has experience in the following areas of combining biometrics: knowledge and voice (conversational biometrics), face and voice, multiple fingers, voice and fingerprint, face and fingerprint, hand geometry and fingerprint. As noted earlier, an area where IBM could be an immediate credible player is in conversational biometrics, which could be further strengthened by including face recognition or fingerprint recognition for handling noisy acoustic conditions.

Table 2 below compares features of various biometric technologies. There are two types of recognition errors in biometrics, namely the false accept rate (FAR) and the false reject rate (FRR). FAR indicates the likelihood that someone may be falsely accepted by the system. FRR indicates the likelihood that a genuine user may be rejected by the system. These measures are expressed in percentage (of error transactions) terms, with an equal error rate of somewhere around 0.1% being a typical figure. The smaller the number, the better the performance. Besides accuracy, there are many factors to consider, such as ease of use and user acceptance, and implementation cost in selecting a biometric technology. For additional comparison of biometric technologies, see Mansfield, et.al. (2001). It should be noted that the voice column is for acoustic-only voiceprint recognition, and does not include conversational biometrics, which is unique to IBM.

Table 2: Comparison of Biometrics

Characteristics	Finger-prints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of use	High	High	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand Injury, age	Glasses	Poor lighting	Lighting, hair, glasses, age	Changing signatures	Microphone, noise, colds
Accuracy	High	High	Very High	Very HIgh	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	Medium	High
Long-Term Stability	High	Medium	HIgh	HIgh	Medium	Medium	Medium

Source: "A practical guide to biometric security technology", IEEE Computer Society IT Pro - Security, Jan-Feb 2001, Simon Liu and Mark Silverman

Automatic Visual Surveillance and Multiscale Tracking (AVSMT):

While biometric technologies provide the capability to identify people, visual surveillance technologies provide the capability to monitor activities and provide timely alerts in case of suspicious activities. In addition, emerging multiscale visual tracking technologies extend the applicability of visual biometrics like face recognition and iris recognition to situations where the user is moving around the space.

Camera based surveillance systems are already very widely used in public spaces, ranging from airports to department stores and from ATM kiosks to hospitals. At the present time the vast majority of such surveillance systems fall into two categories: 1) passive logging systems and 2) human monitored systems. Passive logging systems provide some deterrence and serve investigative purposes: they are used to determine the perpetrators and circumstances of an incident after it has occurred. Human monitoring of surveillance cameras is used in situations requiring active deterrence. For example, department stores use security professionals to actively monitor surveillance video from multiple steerable cameras in various areas in the store. Their goal is to locate potential shoplifters and arrest them upon attempting to exit the store with unpurchased merchandise.

Human monitoring of surveillance video is very labor intensive. Especially in large public spaces like airports with heavy pedestrian traffic, the number of monitoring professionals required can become prohibitively large. Human monitoring of surveillance camera video is a very tedious task. Effective visual attention and errors due to visual inattentiveness has been studied extensively (e.g., surgeons, drivers, and coast guard watchers, life guards). Among all tasks requiring visual attention, it is generally agreed that the most difficult task is vigilance, the ability to hold sustained attention and to react to rarely occuring critical events (e.g., surveillance, inspection) (Miller et al). Since visual attention is sensitive to many uncontrollable factors, any meaningful aid provided by automation will relieve human tedium, stress, and amount of attentional effort.

Automatic Visual Surveillance is an active area of research both in academia and industry (PAMI Special Issue, PETS 2000). Automatic people detection and location tracking based on camera inputs is a maturing technology. The critical advantage provided by automatic surveillance technology is to extend the deterrence capability of human monitoring to large spaces. Automatic tracking algorithms can be used to select only those areas of the space which require a human monitor's attention. In addition, automatic visual surveillance can be used to gather long term statistics on the usage of public spaces. This information can be used to redesign the public space to eliminate potential security holes in the building.

Multiscale Tracking is an emerging research area, which aims to track people at multiple scales, i.e., tracking the position of a person within a space while simultaneously tracking the person's head orientation. Multiscale tracking can potentially deliver much finer grained information on activities that can be effectively used to enhance the deterrence capabilities of surveillance systems. One of the immediate benefits of multiscale tracking is to enable dynamic face capture and recognition, as outlined below.

Person ‘A’ walks into a passenger terminal at JFK. His presence is automatically detected by the wide angle static cameras of the AVSMT system. The system obtains a fix on his 3D location and steers a Pan-Tilt-Zoom (PTZ) camera to capture the person’s face. The images from the PTZ camera are used to measure the head pose and facial expression to determine suitability for face recognition. This high quality image is passed on to a face recognition system for further processing, and could be archived for later use.

Suggestions for Implementation of Biometrics for Airport Visitors and Personnel for an End-to-End Secure Environment

People at airports can be categorized into different groups:

1. Passengers
2. Visitors
   - accompanying passengers to a gate
   - meeting passengers at a gate or at other locations
3. Pilots and Crew
   - in the airport
   - in the aircraft
4. Airline staff
5. Security staff
6. Janitorial staff
7. Baggage operators
8. Other staff on the tarmac
9. Other staff

These groups require different authentication procedures

1. Passengers:

At reservation time:
- collect voiceprint during reservation
- frequent travellers can utilize existing voiceprint and knowledge enrollment

At check-in time:
- provide a on-line verifiable ID card containing biometrics template
- biometrics is verified automatically against the template
- face image and voiceprint collected and added to the flight manifest

At boarding:
- re-authentication using the same template
- a face image and voiceprint also acquired to match against the data collected at reservation time (for voiceprint only) and check-in (for both voiceprint and face image)

At destination gate:
- a face image and voiceprint collected to match against the flight manifest

When leaving the destination airport, the passenger needs to be authenticated again.

2. Visitors:

Accompanying the passenger: Passenger asks for visitor passes and the visitors produce ID cards. Voiceprint and image are recorded in the database. After they have been authenticated, their exit from the airport is recorded.

Receiving a passenger: Passenger declares at check-in. At destination, the visitor produces ID for verification. Face images and voiceprints are acquired, and are used to provide visitor passes. Along with the arriving passenger, they have to be authenticated at the airport exit.

If there are corporate receivers (cabs, limos etc.) how should they be handled as the passenger will not know them in advance?

3. Pilots and Crew:

Pilot and crew ID card with stored biometrics verified at airport entry. Pilot and crew photographs imaged at the departure gate and final destination gate (when leaving the aircraft), along with voiceprints.

In the air, every *x* hours, the pilot and crew need to authenticate to an onboard system that sends images to the airline, controller. Of special importance are the pilot and copilot. Should their identity be verified more often? Once the aircraft is in air, the pilot(s) cannot be changed without authorization from ground control.

Pilot and crew must authenticate the system when exiting the destination airport, or in the case of sick crew for example, at the originating airport.

Whenever there is a flight engineer in the aircraft, they would be treated just like the pilots.

4. Airline staff:

Entering the airport is based on ID card and biometrics. Check-in operations: each transaction is approved only after authentication with biometrics for the operator. They have to authenticate to exit the airport.

5. Security staff:

The security staff authenticate to the system at the start of their day and for every exception transaction. At exiting the airport, they have to authenticate with their biometrics and ID card.

6. Janitorial staff:

Their entry into the airport is controlled with the help of an ID card and their biometrics. In addition, their carts could have a microphone to record unusual activities. At airport exit points, they have to be authenticated.

7. Baggage operators:

The baggage operators enter the airport with help of their ID card and their biometrics. In the baggage handling area, there should be additional microphones and cameras to report unusual activities. Access should be matched with the work shift schedule. They authenticate at the time of exit.

8. Other staff on the tarmac:

For every arriving airplane at the gate, the staff has to authenticate with their ID card and biometrics. In addition there should be a microphone and camera watching over for unusual activities. When they exit the airport, they authenticate to the airport security computer.

9. Other staff:

The retail store staff and other categories not covered above enter the airport through their ID cards and biometrics. At their exit from the airport, they authenticate to the system.

Issues / discussion points:

At any point of time, the number of people inside the airport and who they are should be known.

Do we also need to know their activities?

How does one issue a unique identifier card?

A consortium of airlines may provide the air-travel ID card with biometrics that can be used by the participating airlines. During the enrollment, extreme care must be taken to ensure that duplicates do not exist in the database and also verify the prerequisite documents for the enroll procedure. Background check and approval from the law-enforcement may be sought in special cases.

Should there be several such consortium or a Govt.-controlled ID program?

There are privacy issues that need to be addressed.

Should law enforcement agencies be involved in this exercise to decide who should be enrolled?

References:

Bernie Ashe, President and CEO, AiT Corporation, "SPT and The Secure Internet," Biometric Consortium 2000 Conference, September 13-14, 2000, Gaithersburg, MD.

Jeff Betts, "Fastgate, Why Wait? Automated Passenger Clearance," IBM Canada, Freelance presentation.

U.V. Chaudhari, J. Navratil, G. N. Ramaswamy, S.H. Maes, ``A very large population text-independent speaker identification using transformation enhanced multi-grained models," ICASSP 2001, Salt Lake City, Utah, May 2001.

Michael Cronin, Assistant Commissioner, Inspections, U. S. Immigration & Naturalization Service, "U. S. Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS)," Biometric Consortium 2000 Conference, September 13-14, 2000, Gaithersburg, MD.

R. Germain, A. Califano, and S. Colville, "Fingerprint Matching Using Transformation Parameter Clustering," IEEE Computational Science and Engineering, Vol. 4, No. 4, 1997, 42 - 49.

S. Liu and M. Silverman, "A practical guide to biometric security technology," IEEE Computer Society IT Pro - Security, January, 2001, 27 - 32.

S.H. Maes, J. Navratil, and U.V. Chaudhari, ``Conversational Speech Biometrics," Chapter in "E-Commerce Agents. Marketplace Solutions, Security Issues, and Supply Demand," Springer Verlag, 2001.

T. Mansfield, G. Kelly, D. Chandler, and J. Kane, "Biometric Product Testing Final Report," CESG Contract X92A/4009309, National Physical Laboratory, Middlesex, UK, March 2001.
.
James C. Miller, Matthew L. Smith, and Michael E. McCauley, Crew Fatigue and Performance on U.S. Coast Guard Cutters , Report No. CG-D-10-99/ADA366708, October 1998, U.S. Department of Transportation United States Coast Guard , Human Resources (G-W), Washington, DC. Http://www.rdc.uscg.mil/Reports/CGD1099DPExS.pdf.

J. Navratil, U.V. Chaudhari, and G.N. Ramaswamy, ``Speaker verification using target and background dependent linear transforms and multi-system fusion," EUROSPEECH 2001, Aalborg, September 2001.

PAMI Special Issue: IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 22 Number 8, August 2000.

PETS 2000: IEEE Workshop on Performace Evaluation of Tracking and Surveillance, March 2000, Grenoble, France.

Richard E. Norton, Executive Director, International Biometric Industry Association, "Simplifying Passenger Travel," Biometric Consortium 2000 Conference, September 13-14, 2000, Gaithersburg, MD.

Ganesh N. Ramaswamy, "Conversational Biometrics: The Future of Personal Identification," IBM Research White Paper, IBM T. J. Watson Research Center, September 2001.

N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems," IBM Systems Journal, Vol. 40, No. 3, 2001, 614 - 634.

N. K. Ratha, A. W. Senior and R. M. Bolle, "Automated Biometrics", Proceedings of IACPR, March 2001.

Ephraim Schwartz and Tom Sullivan, "Data Systems Offer Answer," InfoWorld, Issue 38, September 17, 2001, 22.

Evan Smith, Senior Vice President, EyeTicket Corporation, "Simplifying Passenger Travel: Biometrics for Airline Ticketing and Boarding," Biometric Consortium 2000 Conference, September 13-14, 2000, Gaithersburg, MD.

Thomas S. Windmuller, Director, STP Interest Group, International Air Transport Association, "Simplifying Passenger Travel: We CAN Get There From Here," Biometric Consortium 2000 Conference, September 13-14, 2000, Gaithersburg, MD.

Tom Zimmerman, "Air Travel Security and Safety: Technology for the 21st Century," IBM Almaden Research Center working paper, September, 2001.