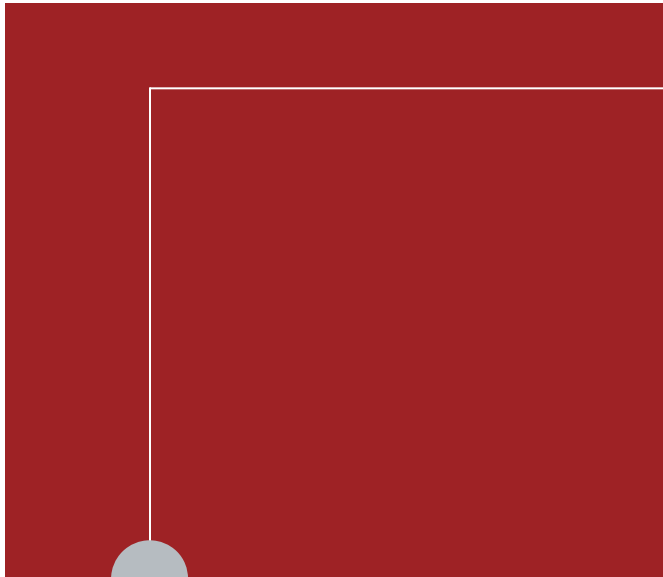


Phone: (888) 567-7347
www.motorola.com/publicsafety



MOTOROLA and the Stylized M Logo are registered in the U.S. Patent and Trademark Office. All other product or service names are the property of their respective owners.
© Motorola, Inc. 2004.



WHITE PAPER

*BIOMETRIC TECHNOLOGY:
OUR FIRST LINE OF DEFENSE
AGAINST TERRORISM*

SITUATION ANALYSIS

The theme song of the popular television dramas collectively titled CSI – Crime Scene Investigator – has a title that goes right to the heart of biometric technology: “Who Are You?”

Since the September 11th terrorist attacks against the United States, homeland security – including securing the nation's borders – has become a critical issue. At the time of those attacks, the U.S. followed century-old entry-exit policies and procedures that made it easy for individuals posing a national security threat to enter and leave the country undetected. U.S. government officials lacked the framework, the tools and the time to identify national security threats:

- The current system is designed to process events - not unique identities
- National security threats can use fraudulent identities and travel documents
- There is little knowledge of foreign nationals and their whereabouts once they are in the United States
- Watch list information (includes foreign nationals who may be national security threats) is incomplete and often delayed

Today, democratic nations are faced with a radically new strategic challenge: how to identify, out of the many millions of foreign nationals who seek entry each year, those few who may be threats to our national security? The key word is “identify.” We cannot stop the terrorists unless we know who they are – and can identify them in time to get the right information to the right people.

Accomplishing this goal will require overhauling the border security process, which entails built-in conflict. Perfect border security means letting no one in. But in his April 21, 2004 testimony before the House Judiciary Committee, Secretary of State Colin Powell pointed out that “keeping everyone out means that the terrorists won.” Blocking access to tourists and business visitors would have a devastating economic impact. (A screening procedure that is slow or inconvenient would have the same negative effect.) But a system that lets everyone in raises obvious security concerns.

Balancing these conflicting goals demands a screening process that nets the bad guys while letting legitimate visitors through with minimal delay and inconvenience. This is where biometric technology comes in. Only biometric solutions such as those offered by Motorola provide the thoroughness that homeland security demands with the speed and convenience to avoid alienating the vast majority of legitimate visitors we would welcome. The goal is to assure that, as Homeland Security Secretary Tom Ridge put it, “Our doors are open but our borders are secure.”

WHAT IS BIOMETRICS?

A basic definition is simple: Technology that automates use of physiological or behavioral characteristics to determine or verify identity. Right now companies such as Motorola offer highly effective biometric technologies that capture and compare physiological data derived from direct measurement of a part of the human body – a fingerprint or a face, for example.

Biometric technologies are essentially pattern recognition systems. Electronic or optical sensors such as cameras and scanning devices capture images, recordings or measurements of a person's characteristics. Then, computer hardware and software extract, encode, store and compare these characteristics. The result: biometric decision-making that is very rapid and in most cases occurs in real-time.

Motorola biometric technologies have been used in a wide array of applications that include passports, national ID cards, refugee and asylum programs and welfare fraud prevention. And now biometrics are being called upon to work on a larger stage – the ongoing struggle against terrorism. The U.S. Department of Homeland Security (DHS) has mandated a biometric solution to border screening.

HOW BIOMETRICS WORK IN PROTECTING HOMELAND SECURITY

Most border security processes identify travelers by what they have (travel documents such as passports and visas) and what they know (asking travelers questions). The travel document also establishes a traveler's eligibility to enter the country. Biometrics on the other hand, focuses more on who the person is – characteristics that can more securely bind a person's identity to a travel document. Such documents are more reliable, cannot be forgotten and are less easily lost, stolen or guessed.

Two processes are keys to achieving this binding. The first is enrollment, the process of establishing document ownership by using unique individual characteristics to create a secure credential. This ties the person's identity to the travel documents. The identity claimed by the traveler is based on documents such as a birth certificate, passport or other government-issued documents. This enrollment process is required to capture a biometric sample, extract and encode the sample as a biometric template and store the data in a database to facilitate the second process – identification and verification:

Identification

– or one-to-many (1:N) recognition – determines a person's identity by performing matches against multiple biometric templates. Positive biometric identification answers the "Who is this person?" – although the response is not necessarily a name. It could be anything from an employee ID number to a terrorist's alias.

Verification

– 1:1 matching or authentication – is the process of establishing the validity of a claimed identity by comparing a verification template to an enrollment template. Verification answers the question, "Am I who I claim to be?"

TYPES OF BIOMETRICS

Motorola's more than 25 years' experience in providing the latest identification technology to the law enforcement community – and more than 65 years of delivering public safety technology solutions - gives us the broader perspective needed to analyze the biometric options available today. Our conclusion is that all biometric technologies offer promise – some today and some in the future. A matrix of factors – accuracy, ease of use, stability, vendor and technology experience in the field, track record and acceptance – combine to make some specific biometric applications more widely deployed. The pressing needs of homeland security demand biometrics that can be put to work today. Thus the three leading biometric technologies for homeland security applications are:

- Fingerprint scan
- Facial scan
- Iris scan

Let's take a look at each of these biometrics systems as well as some other technologies that right now do not meet the expanding needs of Homeland Security.

FINGERPRINTS

Fingerprint identification has two basic premises: The basic characteristics of fingerprints do not change over time and each person's fingerprints are unique. It has been estimated that the number of possible fingerprint patterns is 10 to the 48th power. This makes duplicates nearly impossible.

Fingerprint identification has been used in law enforcement for more than a century and has become the de facto international standard for positively identifying individuals. The FBI has been using fingerprint identification since 1928.

Today fingerprint recognition is one of the best known and most widely used biometric technologies. This is why the DHS has designated fingerprint identification the primary technology for its US-VISIT program. Consider its application to the three stages involving machine readable passports that incorporate biometric identifiers to comply with standards established by the International Civil Aviation Organization (ICAO):

Enrollment. When a would-be visitor applies for a passport in his home country, his fingerprint must be scanned and its biometric template embedded in the passport. The Motorola LiveScan Station, using our proven Printrak technology, provides complete fingerprinting capabilities in an inkless environment – ideal for machine readable passports. Advances in optical scanning – exemplified by Printrak and now Motorola who acquired Printrak – have given fingerprint technology the speed and performance necessary for such a massive application.

Printrak/Motorola fingerprint recognition is a proven identification tool developed for law enforcement agencies more than 25 years ago. This technology extracts features from impressions made by the distinct ridges on the fingertips. The fingerprint image is then scanned, enhanced and converted into a template. Enhancement reduces "noise" – caused by dirt, cuts, scars, creases or dry, wet or worn fingerprints – and enhances ridge definition. Motorola's proprietary algorithms extract minutiae, points relating to breaks in the ridges of the fingertips. Other algorithms extract ridge patterns.

Compilation. The same fingerprint imbedded in the passport is also entered into the fingerprint databases of every participating country.

Search/match: During the application process, the Motorola Biometrics Automated Fingerprint Identification System (AFIS) compares the applicant's fingerprint against all fingerprints in the database. AFIS systems' most common use is in forensic applications, identifying suspects out of local, state or federal databases. But it can also be used to screen for potential terrorists. If AFIS scores a hit that shows the applicant is on a watch list, the application is denied.

The same scanning procedure is followed when a passport holder reaches the United States. His fingerprint is scanned again and a Motorola LiveScan station first makes sure that this fingerprint matches the one imbedded in the passport. If not, he is stopped. At the same time, Motorola compares that fingerprint to its AFIS database. Thanks to innovations such as faster match processors, enhanced matching algorithms and the significantly expanded capability to store, search and retrieve the right information from right database at the right time, this entire process takes just moments.

Motorola's comprehensive family of core technologies – the Digital Justice Solution™ - does more than meet the entire range of public safety and criminal justice information management needs. Many of these Motorola solutions are ideal for border security needs.

FACIAL RECOGNITION

Another biometric approach that can be particularly useful in spotting known terrorist threats is facial recognition. This technology identifies people by the sections of the face that are less susceptible to alteration – the upper outlines of the eye sockets, the areas around the cheekbones and the sides of the mouth.

The face is the only biometric used in a viable recognition technology that is able to operate without the subject's cooperation. Because facial images can be captured from video cameras, facial recognition is the only biometric that – in conjunction with closed-circuit television (CCTV) – can be used for surveillance to spot suspected criminals or terrorists whose facial characteristics have been captured and stored in a database on a template. Facial recognition technology can also be used to compare static images, such as digitized passport photographs, which makes it an ideal biometric for homeland security.

However, it should be noted that there four types facial recognition:

- Type 1: Photo ID recognition.

The computer will compare (match or deny) a stored original image to the picture image identification document.

- Type 2: High restriction live image.

The person places his chin on a certain spot while his picture is taken. This picture is then compared to the stored image.

- Type 3: Low restriction live image.

The person is asked to stand in a marked area and look forward.

- Type 4: No restriction.

The person walks through a security area and his image is captured and compared to the original image.

The accuracy of facial imaging ranges from type 1 which is the most accurate to type 4 which is the least accurate. Nevertheless, while the accuracy of facial recognition is not as reliable as fingerprints, they are ubiquitous in the world of identity documents. A facial image is usually a mandatory field on these types of documents and can be particularly useful when used with another biometric – for example, a passport that combines a facial image with a fingerprint.

Upon applying for a passport, Motorola's Imagetrak – a powerful photo imaging application – simplifies taking and processing the applicant's image. No film is involved, which eliminates the costs associated with the purchase and processing of film. Imagetrak imbeds this digital image in the passport and then allows the image and descriptor data to be stored and shared through seamless interfaces. Imagetrak easily integrates with Motorola's other Digital Justice Solution™ technology.

IRIS RECOGNITION

Developed in 1992, iris recognition is based on the distinctly visible characteristics of the eye's iris, the colored ring surrounding the pupil – a very rich source of biometric data, with approximately 266 distinctive characteristics. Iris recognition technology uses about 173 of these distinctive characteristics. The odds of two people having the same iris pattern are 1 in 7 billion.

Iris recognition systems use a small, high-quality camera to capture a black-and-white, high-resolution image of the iris. The technology then defines the boundaries of the iris, establishes a coordinate system over the iris and defines the zones for analysis within the coordinate system.

Some people resist technologies that scan the eye. But iris recognition requires no body contact and is more user friendly than retina recognition systems in that no light source is shone into the eye and close proximity to the scanner is not required. Images of the iris acquired for iris recognition reveal no information about a person's health.

AN INTEGRATED SOLUTION

These three technologies – fingerprint, facial and iris recognition – offer the most promise for defending homeland security. When iris scan becomes accepted for mass application, this biometric could add another layer of protection to our border security. But right now the International Civil Aviation Organization (ICAO) has defined the need with a published standard that requires nations to certify that they have programs to issue their nationals machine readable passports that incorporate two biometric identifiers – digital fingerprints and photos.

Whatever the need – whether for one biometric measure or for technology that creates biometric fusion of more than one measurement – Motorola stands ready to apply our vast experience and expertise to create an integrated biometric solution for border security.

OTHER BIOMETRICS TECHNOLOGIES

There are other biometric technologies using diverse physiological and behavioral characteristics. Some of them are not yet viable. Others are commercially available but not appropriate for Homeland Security needs.

Among them:

Hand geometry

Systems take 96 measurements involving the width, height and length of the fingers, distances between joints and shapes of the knuckles. However, the shape and size of our hands, while reasonably diverse, are not necessarily unique. In larger populations it is almost certain that various people have very similar hand dimensions.

Speaker recognition

Focuses on voices differences resulting from the shape of vocal tracts and learned speaking habits. Because voice recognition operates best when there's no background noise, it still has an error rate of five percent.

Signature recognition

Treats one's handwritten signature as a series of movements that contain unique biometric data such as personal rhythm, acceleration and pressure flow. The real hurdle with this technology is differentiating between the consistent parts of the signature and the behavioral parts of the signature that vary with each signing. An individual's signature is never entirely the same every time it is signed and can vary substantially over an individual's lifetime. There are also the problems of dealing with foreign languages and people with writing difficulties.

Keystroke recognition

Assesses the user's typing style, determining dwell time (how long each key is depressed), flight time (how long to move between keys) and such other characteristics as typical typing errors. However, keystroke recognition is an internal security technology – say, for providing computer access within an organization – and is not applicable to border security.

Gait recognition

Analyzes how an individual walks by capturing a sequence of images to derive and analyze motion characteristics. Still in the early developmental stage, right now this technology is plagued by accuracy problems.

WHY BIOMETRICS ARE IMPORTANT

Because they are an effective weapon in protecting a nation from terrorists and those who support them.

In the wake of September 11, for example, it was discovered that information on the hijackers' activities was available through a variety of databases at the federal, state and local government levels as well as within the private sector. As a result, governments are now looking for ways to improve the way that agencies work together to serve citizens by maximizing the benefits of the government's overall investment in information technology.

This translates into three key goals:

1. Tear down unwarranted information "stovepipes" at every level of government. This means designing an information architecture that will support efforts to find, track and respond to terrorist threats within the nation and around the world in a way that improves both the time of response and the quality of decisions. To be effective, such an architecture must be horizontal to effectively promote interagency information at the national level.
2. Make this information architecture vertical, moving information as needed up and down the national, state/province, local government levels as well as the private sector.
3. Make this information architecture global, reaching out to other governments battling terrorism.

Having the right system of communication – content, process and infrastructure – is critical to bridging the existing gaps in our defenses. These new systems will greatly assist government officials at all levels to protect and defend against future terrorist attacks – and to effectively manage incidents whenever they should occur.

Biometrics can play a crucial role in the development and implementation of secure information systems to streamline the dissemination of critical homeland security information. Motorola's experience indicates that applying proven biometrics to any border security program offers a realistic approach to making this happen.

The U.S.-VISIT biometric program would interface and integrate with more than twenty existing systems. For the first time every agency working on behalf of securing our borders would be on the same page, with access to the same information. Suddenly it's much harder for anyone to slip between the cracks.

Biometrics solutions are designed to save time and increase accuracy in the identification, processing and management of individuals by border control and national security agencies as well as law enforcement agencies including police, criminal identification, jails and prisons, booking centers and civil identification bureaus/agencies.

Automating time-consuming processes provides for immediate and long-term cost savings, enhanced organizational capabilities, streamlined data processing, efficient and informed decision-making and the potential for greater ROI derived by integrating systems with other agencies. The bottom line: Biometrics give governments more tools to track terrorists, their supporters and their funding while protecting their citizens and foreign visitors as well.

THE ISSUES INVOLVED IN BIOMETRICS

Not everyone sees biometrics as a helpful tool. Their objections may focus on cost, effectiveness or inconvenience. These are practical questions that deserve practical answers.

Other people are – for a variety of reasons – personally uncomfortable with the idea of biometrics, which they consider intrusive, inherently offensive or just uncomfortable to use. They consider it to be physically intrusive to have to pause and position themselves in relation to a capture device while presenting their biometric. Or they consider being required to verify their identity through a hardware device rather than a human interaction to be too impersonal. Fingerprint systems, in particular, face opposition because of their association with criminal applications.

Some biometric devices also carry concerns about hygiene. For example, some people object to hand geometry scanners because they do not like to put their palms on the same surfaces where many other people have placed theirs. Other people fear that devices that scan particularly sensitive areas of the body, such as the eyes, will damage them.

These concerns are more of an emotional response to biometrics. But that doesn't mean such responses can be ignored. Motorola has found that the less intrusive people perceive a biometric to be, the more readily they accept it.

THE PRIVACY ISSUE

The highest hurdle to the widespread adoption of biometric technologies comes from public concern that the technology can be misused to invade or violate personal privacy. This fear – that biometrics will be used to track not just the “bad guys” but also law-abiding citizens – is the government as “Big Brother” scenario.

Among these fears are that biometric information will be gathered without permission or knowledge or without explicitly defined purposes, used for a variety of purposes other than homeland security (sometimes called “function creep”), shared without explicit permission or used to track people across multiple databases to amalgamate information for the purpose of surveillance or social control.

Of equal concern is a tendency for large organizations to develop secondary uses of information. Information collected for one purpose tends over time to be used for other purposes as well. The history of the U.S. Social Security number, for example, gives ample evidence of how an identifier developed for one specific use has become a mainstay of identification for many other purposes, governmental and nongovernmental.

Some people are concerned that biometric information can potentially be linked to multiple databases or to a vast national database. The concept of a repository storing biometric data used to “vet” a visitor or other traveler using a system of interoperable databases will likely generate significant discussion and debate.

Questions being raised include:

- What data would be included or linked to a biometric identification card?
- Who would have access to such information, legitimately or otherwise?
- How people who can access such data could use them?

Still others mention major concerns under the three headings of tracking, profiling and loss of anonymity.

Biometric data collected during enrollment will be stored in interoperable databases – and potentially on a travel document. A comprehensive set of effective access controls must be in place to ensure the security and privacy of the various interoperable databases. In this case, the strong desire for secure databases also builds strong privacy practices.

Getting a workable privacy framework in place is going to require leadership at all levels, including government.

It will require thoughtful examination of what kind of public policies – including legislation – should be implemented.

Policies concerning what the databases will be used for also need to be developed. And selecting from among the alternative methods for ensuring these protections within a system of interoperable databases will require careful study. That is why it is important to stress that the appropriate use of biometrics technology will help citizens and visitors by targeting only those that threaten them.

Motorola has a century-long tradition of developing technology that strengthens public safety, law enforcement and criminal management operations. We recognize that the same biometric innovations that can take a petty thief off the streets can also be aimed – effectively – at international terrorists. We would not offer biometrics unless we were first convinced that it will be used solely to identify and stop those who would threaten our homeland security.

Risk management is the foundation of effective security. In today's world, terrorism is a significant risk.

That risk can be mitigated by knowing who you are dealing with. And when the dust settles, we believe that Motorola biometrics will prove to be an effective risk management tool. It is the proven technology that asks, "Who are you? – and delivers the answer.

OVER 65 YEARS OF UNDERSTANDING THE NEEDS OF PUBLIC SAFETY

In today's world you need a partner who understands what mission critical is all about: the lives and well-being of your employees and the citizens they protect. That's why Motorola is a leading provider of interoperable communications systems for public safety and first responders. Our experience in the public sector, along with our skills, people, partnerships and alliances, allow us to build innovative, fully integrated technologies that help organizations like yours share vital information with ease and confidence. We've been doing it for 65 years, and we'll be standing by our customers for years to come. We are committed to bringing all of our knowledge and technical expertise together so you can focus on what you do best... to serve and protect the public.