LEAVING A PRINT ON SAFETY

ORIGINATING TECHNOLOGY/ NASA CONTRIBUTION

Pattern-recognition technologies developed by NASA to identify spacecraft and other objects in space have helped in the development of new, biometrics-based security solutions on Earth that recognize individuals to grant access to protected facilities, equipment, or information.

PARTNERSHIP

The general principles of the pattern-recognition methods used at NASA's Johnson Space Center for spacecraft and object tracking have helped to direct the technology of Bioscrypt, Inc., a leading provider of identity-verification products. Dr. Colin Soutar, chief technology officer of Bioscrypt, worked at Johnson Space Center between 1992 and 1994 as a National Research Council Research Fellow. He worked in the Tracking and Communications Division with Johnson's Robotic Vision Manager, Dr. Richard Juday, on optical correlation systems and advanced research concepts based on pattern recognition, including autonomous rendezvous and capture of spacecraft, and autonomous, unmanned landings on Mars. The pattern-recognition skills that Soutar developed for optical correlation and space-related conceptual projects are applicable to his current position with Bioscrypt, as the company uses pattern-based processing to accomplish the task of fingerprint verification.

PRODUCT OUTCOME

Headquartered in Ontario, Canada, with a U.S. office in Van Nuys, California, Bioscrypt has installed over 70,000 fingerprint readers worldwide. The pattern-based templates behind Bioscrypt's fingerprint products have been carefully designed to produce one of the most robust fingerprint-verification algorithms in the world, as evidenced by the company's first-place performances at the 2002 and 2004 International Fingerprint Verification Competitions (held every other year). Bioscrypt's pattern-based approach filters, smoothes, and conditions an image to produce a high-quality representation, or template, of a fingerprint's "ridge pattern." Features such as creases, cuts, abrasions, and pores that appear inconsistently are removed. This way, the data that Bioscrypt use for comparison are the entire ridge pattern, which remains unchanged throughout a person's lifetime.

The Bioscrypt technique estimates and removes the relative distortion between the candidate fingerprint and the prevously enrolled fingerprint template. Every ridge of the candidate is then aligned with every ridge of the template image to provide maximum use of the entire fingerprint

The V-Smart™ two-in-one reader combines the high security of Bioscrypt, Inc.'s proven fingerprint-matching technology with a contact-less "smart" card that hosts an encrypted template of a user's fingerprint. The reader instantaneously matches the fingerprint to the template stored on the card, allowing for fast throughput.

image. Subsequent to the removal of the distortion, the ridge patterns are correlated, emphasizing areas in which the images are clean and highly complex and downplaying areas where the images are "noisy" and "bland." For example, noisy parts of the fingerprint would be where the ridges of the print are "broken up" due to poor imaging, and bland portions are typically where the information content of the print is low, such as at the tip of the finger where the ridges are generally straight lines.

This sophisticated methodology for enrolling and validating fingerprint images is at the heart of all Bioscrypt product offerings. Known as Bioscrypt Core,™ the methodology is available for licensing and has been selected by various fingerprint sensor manufacturers, including Atmel Corporation and AuthenTec, Inc., and application developers such as Sense Technologies, Inc.

One of the company's most successful products is a practical two-in-one reader known as V-Smart.™ V-Smart combines the high security of Bioscrypt's proven fingerprint-matching technology with a contactless "smart" card that hosts the mathematical template of a user's fingerprint. Personal information remains perfectly secure with V-Smart, since fingerprints are embedded within encrypted chips on the smart cards, and not on the reader or in a company database. The smart card allows a user to retain control of his or her template fingerprint. To access a facility protected by V-Smart, a user must place on the reader the pad of the finger that matches the previously created fingerprint template, while waving the smart card in front of the reader. The reader will instantaneously match the fingerprint to the template stored on the card, allowing for fast throughput.

The V-Smart two-in-one method provides safety and security for both the user and the establishment being protected. For example, if an employee of a company safeguarded by V-Smart loses his or her smart card, no one else could gain access to the workplace should they happen to find it, since the fingerprint would not match up. In addition to employee identity theft, companies can snuff out security-threatening situations such as equipment theft, vandalism, unauthorized access to restricted areas, and "buddy punching," when an employee clocks in or out another employee who is not present at the time. Employers also rack up significant costs attributed to replacing lost or stolen building keys or access cards, and correcting time and attendance issues—all of which can be eliminated with the V-Smart access system.

Bioscrypt's largest deployments of V-Smart readers include sensitive entry points at American Express worldwide headquarters in New York, New York, and the New York Police Department headquarters. At the police department, thousands of officers and government workers have been issued new badges containing digital copies of their fingerprints. According to one Bioscrypt official, the high-tech security system may soon be embraced by more than 200,000 New York City and State government employees.

Airports around the world are experiencing the benefits of Bioscrypt's advanced fingerprint technology as they implement new security systems to combat international terrorism. In 2004, Indiana's Fort Wayne International Airport selected V-Smart to verify individual access to sensitive areas. Little Rock National Airport in Arkansas has deployed over 100 V-Smart readers for approximately 5,000 users. In the Eastern Hemisphere, Russia's largest and foremost airport, Domodedovo International Airport, has installed V-Smart to control access to "staff-only" areas of the facility.

The technology had officially come full-circle when NASA implemented it to protect the Triana Science and Operations Center at the University of California in San Diego. The NASA-funded facility, a part of Scripps Institution of Oceanography, installed eight Bioscrypt units, one for every entry point and office. The facility uses Bioscrypt readers in conjunction with door controllers to protect the offices and work areas of employees engaged in developing a leading-edge Earth-imaging spacecraft. The Triana spacecraft has been completed and stored until a viable flight opportunity has been identified. NASA's intentions for the spacecraft are to transmit data back to the Triana center, where the information will be processed to provide scientists throughout the world with new insights into how our planet's climate works as an integrated system.

Bioscrypt's goal is to replace traditional access methods such as passwords, personal identification numbers, keys, and entry cards with its fingerprint-verification technology to enhance user convenience and security. As one assured customer puts it, "You can loan someone your card and personal identification number, but not your finger."

Bioscrypt Core™ and V-Smart™ are trademarks of Bioscrypt, Inc.

The airport industry continues to demonstrate that it is a first mover in the adoption of commercial biometric technology, having secured many critical access points with Bioscrypt products. The urgency to increase security within these facilities is perhaps greater than in any other environment.