

AUTOMATED FINGERPRINT IDENTIFICATION SYSTEMS

2005 COMPUTERWORLD HONORS CASE STUDY

BUSINESS & RELATED SERVICES

THIS SYSTEM IS THE FIRST TO APPLY SUPERCOMPUTING PRINCIPLES TO ENABLE HIGHLY SCALABLE AND ACCURATE BIOMETRIC FINGERPRINT COMPARISONS, LEADING THE WAY TO PROVEN, COST-EFFECTIVE IDENTIFICATION SOLUTIONS WHICH ARE CRITICAL TO THE SAFETY AND INTEGRITY OF TRANSACTIONS, COMMUNICATIONS, TRAVEL AND LIFE IN TODAY'S SOCIETY. [20055293]

SUMMARY

First to apply supercomputing principles to enable highly scalable and accurate biometric fingerprint comparisons, leading the way to proven, cost-effective identification solutions which are critical to the safety and integrity of transactions, communications, travel and life in today's society.

APPLICATION

Cogent Systems is a leading provider of Automated Fingerprint Identification Systems, or AFIS, and other fingerprint biometric solutions to governments, law enforcement agencies and other organizations worldwide. Cogent's AFIS solutions enable its customers to capture fingerprint images electronically, encode fingerprints into searchable files and accurately compare a set of fingerprints to a database containing potentially millions of fingerprints in seconds. For over fourteen years, Cogent has researched, designed, developed and marketed fingerprint biometrics technologies that incorporate advanced concepts in fluid dynamics, neural networks, image enhancement, data mining and massively parallel processing. Its proprietary software algorithms, together with optimized hardware, enable customers to cost-effectively achieve industry-leading accuracy rates and performance. Cogent solutions support the latest standards in fingerprint biometrics and are based on cost-effective industry-standard hardware and software platforms.

Cogent is headquartered in Pasadena, California and was founded by Ming Hsieh fourteen years ago. Ming bootstrapped the Company with a \$120,000 loan and never raised any venture capital funding. Cogent currently has approximately 130 employees and recently completed an initial public offering on the NASDAQ stock exchange (COGT) in September 2004.

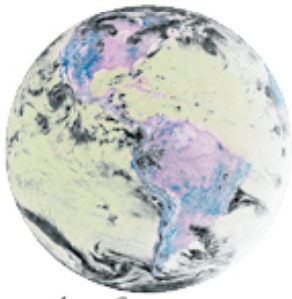
BENEFITS

Cogent has designed and developed a fully integrated AFIS solution comprised of proprietary fingerprint biometric software, together with optimized hardware and professional services. This end-to-end solution equips its customers with all of the elements necessary to deploy fingerprint biometric solutions, including:

- Search and Retrieval Software. At the core of Cogent's solutions are its proprietary search algorithms that accelerate the matching process while maintaining accuracy.
- Capture Devices. Cogent's live-scan devices run its proprietary Image Flow software, which employs advanced algorithms to improve feature extraction from the fingerprint images, thereby enhancing accuracy.
- Systems Integration Services. Cogent's service abilities enable them to deliver full end-to-end solutions regardless of the operating or network environment and to design custom interfaces to existing systems.

Cogent's proprietary search algorithm searches the entire database instead of using binning like most other AFIS, which enables its customers to search large databases with industry leading accuracy and performance. Moreover, Cogent solutions enable rapid response times while still maintaining a high degree of accuracy. Its Programmable Matching Accelerator, or PMA, servers accelerate the processing capability of standard server architectures and can compare over one million fingerprints per second per PMA server.

In addition to the high accuracy rates and performance of Cogent's solutions, the power, linear scalability and flexibility of its solutions can result in significant cost savings for its customers. The power of Cogent solutions reduces a customer's initial cost and related ongoing maintenance and administrative cost because one of its PMA servers running its software can typically accomplish the equivalent processing of multiple Windows, UNIX or Linux servers working with other existing AFIS solutions. Moreover, solutions enable customers to expand their systems smoothly and economically as their processing needs grow and as their



A Search for New Stories



Robert Carrigan,
Chairman of the Chairmen's Committee

Ron Milton,
Vice-Chairman of the Chairmen's
Committee

Dan Morrow,
Chief Historian

systems evolve because they can incrementally purchase additional PMA servers which can be easily connected to one another, or rack mounted, to linearly scale matching throughput and support system growth as their databases grow and the number of required searches increases. Additionally, all of Cogent's current solutions are flexible and work effectively in heterogeneous network environments that include multiple hardware systems and operating systems such as Windows, UNIX and Linux.

IMPORTANCE

Positive identification of individuals is an essential societal requirement. As more interactions take place electronically, it becomes even more important to have an electronic verification of a person's identity. Biometric solutions provide secure, effective and efficient identification of individuals in a wide array of applications and contexts. The deployment of biometric solutions will ultimately create a safer and more convenient society.

Law enforcement agencies use biometric AFIS solutions to help identify and process individuals—quickly and accurately. AFIS is becoming an increasingly important tool in identifying suspects and can help greatly accelerate the investigative process. Los Angeles law enforcement agencies rely heavily on AFIS technology. Representing approximately 88 law enforcement agencies in the greater Los Angeles area, the LASD and LAPD must process all fingerprint matches for their region. Cogent Systems implemented the Los Angeles AFIS (LAFIS), improving the accuracy and speed with which it identified criminals and solved crimes.

Post September 11th, border security has become one of our nation's top priorities. This increased demand for secure borders has manifested itself in more rigorous security measures at points of entry. Without Cogent's technological leadership, security solutions currently implemented by many federal, state and local, and international governments would not be possible. The US Department of Homeland Security, Cogent's largest customer, relies on Cogent as its sole provider of back-end biometric processing for the US VISIT program. US VISIT helps track all foreigners entering and leaving the US by capturing their fingerprints and searching for a match against terrorist and criminal databases, and then storing the prints for future reference. Cogent provides the US VISIT program with programmable matching accelerators (PMA servers), which allow for very fast processing of travelers through customs. PMAs are industry-standard servers, optimized in racks and loaded with Cogent's proprietary software algorithms that improve response time and accuracy.

In choosing vendors for US VISIT, DHS gave bidders an 8-second limit to capture two fingerprints from a traveler, check those against existing watch lists, and deliver a match if available and add the traveler to a separate database. Cogent executed in 4 seconds--half the time--and won the business. Without Cogent's proprietary software algorithms that are at the core of its biometric offering, US VISIT's airport security checks would take twice as long, potentially making the whole policy prohibitively time-consuming and infeasible. Cogent's AFIS solution enables safe and efficient implementation of our nation's increasingly demanding security requirements.

In addition to keeping criminals and terrorists in check, AFIS solutions can also be leveraged for specific civilian applications in which identity (and hence the forging of identity) holds significant value. By uniquely determining identity, biometric solutions enable voting and welfare systems to function both more securely and conveniently. National ID cards and passports, which if counterfeited or stolen can be used in an improper fashion, could be replaced with AFIS solutions, which can't be taken away or lost. Biometric solutions could even replace lock and key and other physical entry systems.

On the civilian front, Cogent successfully deployed AFIS in the Venezuelan national elections held in August 2004. Voters submitted fingerprints on a live-scan device, and the fingerprints were enrolled in a database and matched to authenticate the voters' identities and prevent duplicate registration. The Venezuelan National Electoral Council (NCE) used Cogent's solution to enable the real-time authentication of voters' identities.

Cogent has also implemented commercial biometric solutions. Hewlett Packard's iPAQh5550 Pocket PC, enabled by Cogent's proprietary fingerprint scanner and ASIC, enables users to implement access protection that far exceeds the conventional password methodology.

Commercial AFIS applications have the potential to make our society as a whole more convenient by making tasks that we undertake everyday more efficient. Point of sale biometric solutions could revolutionize the exchange of goods by getting rid of the need for a physical monetary system. With Cogent's AFIS technology, using paper currency to buy goods may some day be as archaic as bartering for goods is to us today.

ORIGINALITY

Cogent maintains two key areas of technological differentiation over its competition. First, Cogent's utilizes a unique methodology for comparing a set of fingerprints which generates an unparalleled degree of accuracy with far less information than is necessary for competitors' solutions to achieve similar levels of accuracy. The conventional methodology utilized by the competition is called "binning". When comparing two fingerprint images, if the unknown fingerprint can be classified into a number of standard categories, then the fingerprint is searched against only a subset of known fingerprints that are of the same classification (i.e. right loop, arch, whorl). This is done because conventional systems are limited in their ability to search large amounts of information. However, this methodology is quite error-prone, as fingerprints are natural and oftentimes cannot be conveniently classified into one specific category. Cogent utilizes advanced fluid dynamics principles to create a very accurate model of the unknown fingerprint, enabling its technology to search the entire fingerprint and not have to rely on binning. Second, Cogent's PMA servers enable the Company to utilize off-the-shelf hardware, combined with its proprietary software technology, to execute its search algorithms at very high rates, as much as 1 million comparisons per second. The combination of the unique search algorithm and the PMA approach enables the Company to achieve superior accuracy and performance to its competition.

SUCCESS

The Need: Effective Authentication and Identification of Individuals

Effectively authenticating and identifying individuals is critical to the safety and integrity of transactions, communications, travel and life in today's society. Security breaches and frauds resulting from failures in authentication and identification systems can cause economic harm and loss of life. As a result of growing public awareness of security and economic risks, people are becoming increasingly willing to submit to security checks and other identity verification procedures. Authentication of an individual's identity is necessary when governments, law enforcement agencies and other organizations need to confirm that an individual is who he claims to be. This necessity arises, for example, when a traveler enters a foreign country, a suspect is arrested, an individual withdraws money from an ATM, a consumer purchases an item on the Internet or an employee seeks access to a restricted area. To authenticate the individual's claimed identity in these types of scenarios, organizations traditionally implement processes to examine the individual's credentials, such as signatures, drivers' licenses, passports, access cards, PINs or passwords. If the authentication process indicates that the credentials are invalid or if there are no credentials to examine, such as when an unknown person leaves evidence fingerprints, known as latents, at the crime scene, organizations frequently initiate an identification process to determine the individual's identity.

Traditional processes for authenticating and identifying individuals have inherent weaknesses. Criminals and imposters can easily compromise these processes by falsifying credentials by forging a signature, altering a photograph on a driver's license or passport or stealing a physical access card. Imposters can use the compromised credentials to gain unauthorized access to physical locations, such as buildings and airplanes, and to confidential information, such as medical data and financial records, and cause significant harm. Traditional authentication and identification methodologies can also be cumbersome and inefficient to use. Individuals are required to remember several passwords and PINs for the multitude of access, credit and membership cards they carry. The costs incurred by organizations to administer these traditional processes can be significant.

The inadequacies of traditional authentication and identification processes, coupled with more stringent security requirements and an increasingly global economy and mobile population, have in recent years contributed to the increased focus on the development of biometrics. Biometrics is the automated use of unique physiological characteristics of individuals, such as fingerprints, palm prints, faces or irises, to determine or verify an individual's identity. The individual's biometric characteristic is captured and encoded and then compared against previously encoded biometric data stored in an electronic database to determine or verify the individual's identity. Because biometrics technology utilizes an unchanging, unique characteristic of a person that cannot be lost, stolen, shared or forgotten, it has the capability to be more accurate, convenient and cost-effective than traditional methodologies.

Fingerprints have been the most widely used biometric because they are relatively simple to capture, either voluntarily or from latents at crime scenes, are relatively non-intrusive and benefit from a substantial existing infrastructure that employs fingerprints for identification. The most pervasive, large-scale fingerprint biometrics technology implementations today are AFIS. AFIS have achieved widespread acceptance with national, state and local law enforcement agencies globally and is comprised of fingerprint input scanning devices and software and computers that encode, process and store electronic versions of fingerprints.

To satisfy the evolving needs of the AFIS market and the emerging market for other fingerprint biometrics solutions, vendors must deliver systems that achieve increasingly high levels of both accuracy and performance in a cost-effective and scalable manner. Many existing solutions are challenged in their ability to meet these

needs because they are limited by inaccuracy, performance constraints, high costs and lack of linear scalability and flexibility.

The Solution: Fully Integrated AFIS Solutions

For over fourteen years, Cogent has researched, designed, developed and marketed advanced fingerprint biometric technologies and integrated solutions. It now offers a variety of products and services to the government sector, which consists of federal, state, local and foreign governments and agencies, including immigration/border control agencies and law enforcement agencies and the market for other fingerprint biometric solutions, which are emerging applications primarily for the commercial sector.

Cogent offers two primary AFIS solutions, each of which incorporates its PMAs and live-scan devices:

Cogent Automated Fingerprint Identification System (CAFIS). CAFIS is a full-function, networked AFIS solution for local, regional and national systems. While each CAFIS deployment is unique to the customer due to its specific design and integration requirements, all such deployments employ Cogent's proprietary software, and the larger deployments rely significantly on its PMA servers. CAFIS is largely used for twoprint, tenprint, latent and palm print searches.

Cogent Live-ID. Cogent's Live-ID AFIS solution enables its customers to rapidly identify individuals who submit their fingerprints for border crossings, background checks, fraud protection, criminal investigation, document identification and other activities where security is a concern. Live-ID has been deployed in many demanding environments, including the US-VISIT program.

Cogent also offers AFIS services including: design, integration and training and outsourced Live-ID biometric processing services.

The Results:

Examples of ongoing and successfully completed implementations of Cogent's AFIS solutions and other fingerprint biometric solutions include:

United States Visitor and Immigrant Status Indicator Technology (US-VISIT): The US-VISIT program, launched in January 2004, requires visitors traveling on a visa to submit two scanned fingerprints and have a digital photograph taken upon both entry to and exit from the United States. Under US VISIT, up to 70,000 travelers a day are fingerprinted, and then those fingerprints are checked against Cogent's database, which represents the nation's second largest fingerprint database after the FBI's. The program received \$330 million in funding for fiscal year ended September 2004. Upon completion, US-VISIT will employ Cogent's AFIS solution at numerous locations to enable real-time authentication of individuals' identities at high traffic areas of U.S. airports, seaports and land ports and U.S. consulates overseas.

National Electoral Council in the Republic of Venezuela (NCE): The NCE used Cogent's AFIS solution including software and hardware, as well as installation and maintenance services, for its national elections in August 2004. Voters submitted fingerprints on a live-scan device, and the fingerprints were enrolled in a database and matched to authenticate the voters' identities and prevent duplicate registration. The NCE used Cogent's solution to enable the real-time authentication of voters' identities. As a result of its successful implementation of AFIS in the national elections in August, Cogent was awarded a follow-on contract by the NCE in October 2004.

U.K. National Automated Fingerprint Identification System (NAFIS): The U.K.'s NAFIS supports the 43 police forces of England and Wales including the New Scotland Yard. NAFIS employs Cogent's Image Flow and Data Flow technology, enabling nearly 100% database penetration of a 5 million record database for every search. In its first year of operation, NAFIS identified more than 30,000 latent prints left at crime scenes.

Ohio Bureau of Criminal Investigation and Identification (OBCII): The OBCII provides scientific and investigative assistance to local law enforcement agencies throughout Ohio. We developed OBCII's AFIS system, which supports 1,300 civil and commercial agencies with a secure web-based system for civil fingerprint background checks that now take minutes instead of weeks. The OBCII AFIS also interfaces with all 650 law enforcement agencies and provides electronic filing of dispositions by courts.

U.S. Citizenship and Immigration Services (USCIS): The USCIS (formerly known as the Immigration and Naturalization Service), which is part of DHS, is a government organization whose mission is to promote national security, continue to eliminate immigration adjudications backlogs, and implement solutions for

improving immigration customer services. We provided the technology for the USCIS IDENT system. The system uses high-speed digital communications to link over 500 workstations at border control points and USCIS locations throughout the United States. Using Cogent's Data Flow technology for nearly 100% database penetration, and handling 25,000 transactions per day, IDENT provides identification search responses in seconds for a database of over 9 million records.

Hong Kong Smart Identity Card Program (SMARTICS): SMARTICS is an identity card replacement program initiated by the Hong Kong Immigration Department in August 2003 for the residents of Hong Kong. Each new identity card being issued has Cogent's proprietary ASIC embedded in it. The ASIC has a digital template of the individual's fingerprints encrypted in it. The templates can be read and matched against a scan of the individual's thumb at any automated entry station to confirm the identity of the individual. The SMARTIC program enables real-time authentication of individuals' identities at Hong Kong's borders.

Los Angeles County Regional Identification System (LACRIS): The LACRIS program supports all 47 law enforcement agencies in Los Angeles County and is fully integrated with county, state and national justice information systems. We developed LACRIS solution which can search a subject database of both rolled and flat prints and achieve what we believe to be industry leading accuracy. The legacy system used in Los Angeles County had taken 1-2 days to process prints. This real-time response enables law enforcement officials to quickly identify individuals when they are arrested and to solve crimes based on fingerprints that are left at crime scenes.

Hewlett Packard (iPAQ h5550): Hewlett-Packard has integrated Cogent technology with its iPAQ h5550 Pocket PC to enhance security and improve ease of use. The iPAQ h5550 incorporates a fingerprint scanner and Cogent's proprietary ASIC to enable users to implement access protection that far exceeds the conventional password methodology.

DIFFICULTY

In order to offer a competitive solution in the AFIS market, vendors must offer three characteristics: 1) accuracy, 2) performance and 3) cost effectiveness. There are two typical real-world scenarios that AFIS systems are used. First, in law enforcement, AFIS systems are used to try and find a match for fingerprints that are recovered from crime scenes. In this scenario, often times the fingerprints that are recovered are very poor resolution and could only be partial fingerprints. Second, at border control facilities, like the US VISIT program, travelers are diverted to a line when they enter a U.S. airport. Currently any foreign traveler, regardless of visa status, must enter this line. At the US VISIT counter, the traveler's picture is taken and he/she is asked to submit two index fingers only, to be scanned and compared against the terrorist watch list. All of this must happen VERY fast, otherwise it would be incredibly inefficient and result in unmanageable lines and wait times at airports. These scenarios illustrate the importance of the three characteristics in the following manner:

- 1) Accuracy: the AFIS system has to have technology advanced enough to be able to compare a database of known fingerprints against an incredibly poor image of an unknown fingerprint, in the law enforcement example. In the US VISIT example, because only two index finger prints are taken from the traveler, instead of the typical "ten-prints" taken in law enforcement, the system must achieve very accurate results with far less information than typical ten-print systems. Mistakes in both cases would lead to unsolved crimes, mis-identification of criminals or terrorists and the unauthorized entrance of a terrorist into the country.
- 2) Performance: AFIS systems must utilize a tremendous amount of computing power to accomplish the mathematical computations that underlie the fingerprint comparison. Without an efficient algorithm and significant processing power to execute the algorithm, it would be impossible to achieve the kind of response times that are currently running live within the US VISIT program.
- 3) Cost-effectiveness: Governments and law enforcement agencies have limited financial resources. It is theoretically possible to achieve both significant accuracy and performance by using a standard algorithm and stringing together thousands of off-the-shelf servers to achieve the response times necessary for programs like the US VISIT. However, practically speaking this is not possible, and as such it is important for vendors to design AFIS systems that leverage highly efficient search algorithms and a minimal use of servers, thereby accomplishing a high degree of accuracy and performance in a cost-effective fashion.