Center for Identification Technology Research (CITeR)

A CISE-funded Center

Clarkson University, Stephanie Shuckers, Director, 315.268.6536, sschucke@clarkson.edu
West Virginia University, Bojan Cukic, 304.293.9686, bojan.cukic@mail.wvu.edu
University of Arizona, Judee Burgoon, 520.621.5818, jburgoon@cmi.arizona.edu
University at Buffalo, State University of New York, Venu Govindaraju, 716.645.1558, govind@buffalo.edu

Center website: http://www.clarkson.edu/citer/

Automated Virtual Agent for Truth Assessments in Real Time (AVATAR)

An AVATAR kiosk conducts natural credibility assessment interviews automatically. AVATAR avoids bias, favoritism, or fatigue by using non-contact sensors to determine credibility risk.

Researchers at CITeR have developed AVATAR, a kiosk-based automated screening system for credibility assessment. AVATAR automatically conducts natural, brief interviews for trusted traveler application programs, personnel reinvestigations, visa application reviews, or similar scenarios where truth assessment is a key concern. AVATAR uses non-invasive sensors to identify suspicious or irregular behavior that deserves further investigation. Unlike human interviewers, AVATAR's credibility assessment is free of biases, profiling and distractions. They may be capable of delivering more valid risk score than interviewer's "gut instincts." AVATAR also incorporates identity confirmation, biometric identification, document authentication, and payment processing. Using AVATAR technology, customers can automate organizational and security processes that normally require costly, labor-intensive interactions. This technology emerges at a critical juncture when organizations, particularly in government, have increasing workloads, but few additional manpower resources. Finally, kiosks never have bad days, unless they freeze or become non-operations; nor do they get fatigued at the end of 12 hour shifts.

Whereas current state-of-the-art products take extensive human skill and uses contact sensors like electrodes or blood pressure cuffs, the AVATAR uses a suite of non-contact sensors to monitor patterns in an interviewee's physiology and behavior. It then analyzes those patterns to guide the interview conducted by the system. In addition, the AVATAR includes biometrics (like iris scans) and document scanning to facilitate full self-service interviewing and screening. For example, an airport traveler can scan their passport, complete a screening interview, be identified biometrically (fingerprint or facial recognition), pay for additional services with a credit card, and receive a print out of their transaction.

While AVATAR researchers have spent many years conducting basic research and prototyping systems, they have also acquired a deep understanding of the most likely operational environments. All AVATAR kiosks

are networked wirelessly and securely to an administration tablet that can be monitored by a human screener. The system can be used to complement a human interviewer by presenting enhanced analysis of behavior and physiology, or it can serve as a stand-alone, completely automated solution.

A personalized interviewer may be desirable because all interviewees are not the same and would be expected to respond differently to diverse situations. AVATAR systems can be customized to speak and understand any language using advanced speech recognition. They can draw upon information from existing organizational databases to inform the interview (e.g., refer to the interviewee by name, ask personally relevant questions) and can store collected data such as spoken interview responses and interaction statistics.

In many setting where large-scale processing of people and data are required, AVATAR kiosks could relieve people from the most mundane, repetitive tasks so that their skills and training are put to better use, but can also detect subtle indicators of threat, risk, or misrepresentation that might be missed by all but the most experienced and skilled humans. The AVATAR kiosk is not limited to security screening. Other commercial applications are numerous. For example, businesses with a large employee base could use AVATAR to streamline employment applications by collecting preliminary demographic data, searching out prior employment history and gauging a person's truthfulness and suitability for a given workplace. In financial fields, AVATAR's sensors have already been tested for their ability to detect fraud in written statements and during interviews. In the medical environment, AVATAR systems could be equipped to do routine medical exams (e.g., collect heart rate), triage patients, dispense health information and encourage more candid disclosure of compliance or noncompliance with medical regimens. In the educational context, AVATAR systems might administer skill tests while detecting levels of stress or loss of attention. For written exams, AVATAR might reduce opportunities for cheating.

> **Economic Impact**: In today's security conscious environments, border screening is a time and labor intensive process. It requires a vast work force to provide efficient and effective screening for the millions of crossers entering the US daily. Border security organizations have been early testers of prototype versions of AVATAR. The Department of Homeland Security (DHS) has tested it with its Trusted Traveler program. The European Union border control agency has tested it for imposter detection, deception detection and risk assessment. Automating the screening process and providing customs and border agents enhanced information on individuals seeking entry can significantly reduce labor costs by having one officer oversee a bank of kiosks. For DHS, AVATAR could serve as a force multiplier that frees personnel to focus on other mission-critical tasks while at the same time improve outcomes by providing more accurate decision support and risk assessments. This could be accomplished by automating interviews and document/biometric collection and by delivering real-time multi-sensor credibility assessments. Successful large-scale implementations could lead to multibillion dollar operational savings and perhaps even real improvements in security. A new company has been established to work on customizing AVATAR for specific contexts and uses, such as border screening, border adjudication, personnel investigations and re-investigations, and asylum and refugee applications. The potential economic benefits are therefore only limited by one's imagination.

For more information, contact Judee Burgoon at the University of Arizona, 520.621.5818, jburgoon@cmi.arizona.edu.

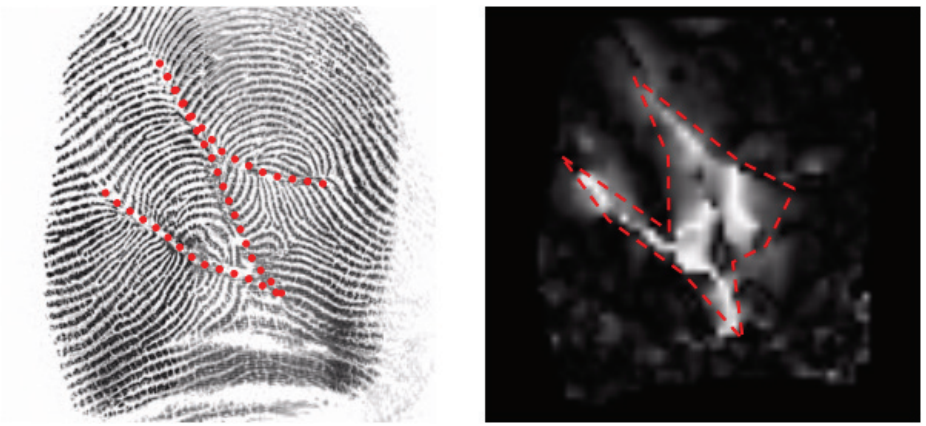
Automated Detection of Altered Fingerprints

For over 100 years, fingerprint identification has been successfully used to identify suspects and victims, primarily in law enforcement and forensics. Now it has become the backbone for broad security applications at border crossings, civil registration, and access control to secure buildings, or computer login. With the widespread deployment of Automated Fingerprint Identification Systems (AFIS), there have been growing instances worldwide where individuals, particularly criminals wish to conceal their true identity and illegal aliens wishing to enter another country. Such individuals have altered (mutilated or destroyed) their fingerprint patterns by means of abrading, cutting, burning, or performing a plastic surgery on fingertips in order to evade AFIS.

Images of altered fingerprints. (Left) Fingerprint pattern destroyed by biting the finger skin. (Right) Transplanted friction ridge skin from sole.

Fingerprints of Gus Winkler before and after alteration.

One of the urgent tasks faced by law enforcement and border control agencies worldwide is to detect the altered fingerprints automatically so that individuals with altered fingerprints go through a secondary inspection to establish true identity. Because law enforcement officers handle millions of fingerprints every day, this detection needs to be extremely fast and reliable; meaning very few false alarms (as is the Department of Homeland Security's US-VISIT system and the FBI's IAFIS system). Research supported by the Center for Identification Technology Research (CITeR) has led to the development of an innovative approach for automatically detecting altered fingerprints based on pattern analysis techniques and mathematical modeling of fingerprints. Altered fingerprints are detected by observing abnormality in two fundamental fingerprint features – orientation field (fingerprint ridge flow) and minutiae (ridge bifurcation and ending points).



Detection of altered fingerprints. (Left) Altered fingerprints with 'Z'-shaped cut and (right) automatic detection of fingerprint alteration based on orientation field discontinuity. Brighter pixels in (right) represent discontinuity in orientation field and correspond to the scarred region in the altered fingerprint in (left).

With CITeR funding, Anil Jain and his students at Michigan State University (MSU) have developed algorithms for automatic detection of altered fingerprints. The resulting software for detecting altered fingerprints has been licensed to Morpho (Safran Group), one of the world's leading suppliers of identification, detection, and e-document solutions. Morpho customers include the Federal Bureau of Investigation (FBI) and more than 450 government agencies in over 100 different countries. The technology for automatic detection of altered fingerprints, developed by the MSU team through CITeR funding, will be integrated in Morpho products to prevent criminals and asylum seekers worldwide to evade identification through AFIS. This is an example of a successful transition from university research to a proof-of-concept to a commercial product.

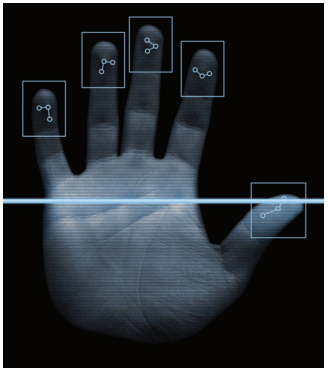
Economic Impact: The expected economic benefits of this breakthrough technology will come from the fact that it will foil most attempts by criminals and terrorists to alter fingerprints. This innovative advancement is expected to have many major, albeit hard to quantify positive economic impacts, mostly in avoided security breaches and the of the associated, oft incalculable costs. They will also result in economic benefits resulting from: 1) welfare programs secured by

fingerprint recognition, effectively preventing fraud through fingerprint alteration; 2) prevention of criminals and other undesirable individuals from crossing national borders; and, 3) forestalling asylum seekers with prior history of criminal conviction from gaining entry where they are not wanted.

For more information, contact Anil Jain, 517.355.9282, jain@msu.edu.

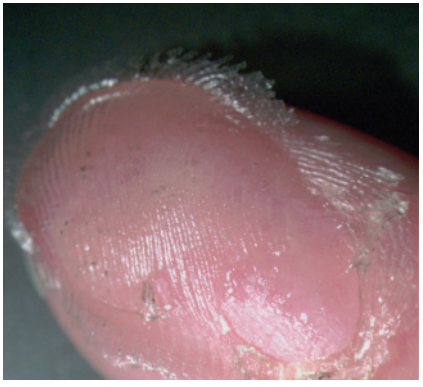
Fingerprint Liveness Detection

Researchers at CITeR have shown that fingerprint biometric scanners, used for secure authentication, can be deceived easily, using simple, inexpensive techniques with fake or dismembered fingers, called spoofing. In this CITeR breakthrough, it has been demonstrated that perspiration can be used as a measure of liveness detection for fingerprint biometric systems. As a result, the potential for spoofing biometric fingerprint devices, one major vulnerability in the industry, in being minimized. Unlike cadaver or spoof fingers, live fingers demonstrate a distinctive spatial moisture pattern when in physical contact with the capturing surface of the fingerprint scanner. The work has considerate applications for homeland security.



Fingerprints are useful as a convenient form of authentication, used alone or in combination with other forms such as passwords.

The pattern in the fingerprint images begins as 'patchy' areas of moisture around the pores spreading across the ridges over time. Image processing and pattern recognition algorithms have been developed to quantify this phenomenon using wavelet and statistical approaches. Previously, commercial biometric devices did not have a mechanism to prevent spoofing. Prior to the Fingerprint Liveness Detection (FLD) research, the main approach to spoofing prevention was to combine the biometric with additional hardware to measure liveness signals such as the electrocardiogram, pulse oximetry, or temperature. Disadvantages included the need for additional hardware that was bulky and inconvenient and possibility spoofable by a live (un-authorized) finger in combination with the spoof finger.



The CITeR breakthrough is a software method for fake fingerprint detection. The left image is an example fake finger and on right is a fake finger masking a real.

The work has considerable application for homeland security and mobile applications. The advantage of this new CITeR approach is that the biometric itself is naturally integrated with the liveness measure, requiring only an additional software algorithm to protect from spoofing. This research has raised the visibility of these major security issues through presentations, publications, and mainstream media (Discovery Channel, New York Times, National Public Radio) featuring FLD. As a result, industry has moved towards developing biometric devices that incorporate liveness, as well as other anti-spoofing measures. With three awarded patents, the CITeR-developed algorithms are being used by major biometric companies around the world.

Economic Impact: The center's universities have licensed the intellectual property to a start-up company, called NexID Biometrics, LLC, incorporated, owned by the researchers. Further development and commercialization was performed by NexID Biometrics, LLC, which now has three permanent employees. The algorithm has been customized to provide liveness detection for variety of fingerprint sensors. The company has licensed the software to biometric industry and to system integrators for integration with their biometric systems. Its commercialization pathways have included integration with single print fingerprint scanners and four print scanners, as well as integration in mass market swipe fingerprint sensors integrated with laptops. At this time, well over 1,000,000 laptops worldwide include versions of fingerprint liveness detection approaches derived from CITeR research.

For more information, contact Stephanie Schuckers, 315.268.6536, sschucke@clarkson.edu.