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

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

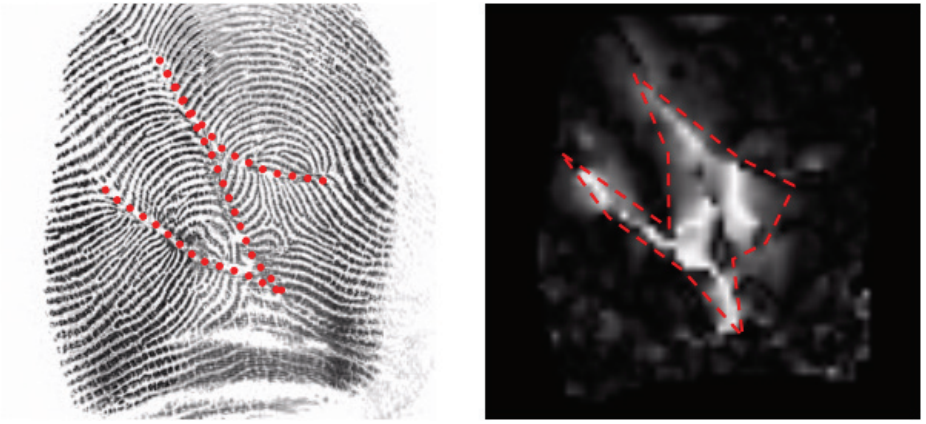
Automated Detection of Altered Fingerprints

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 wish 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 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).



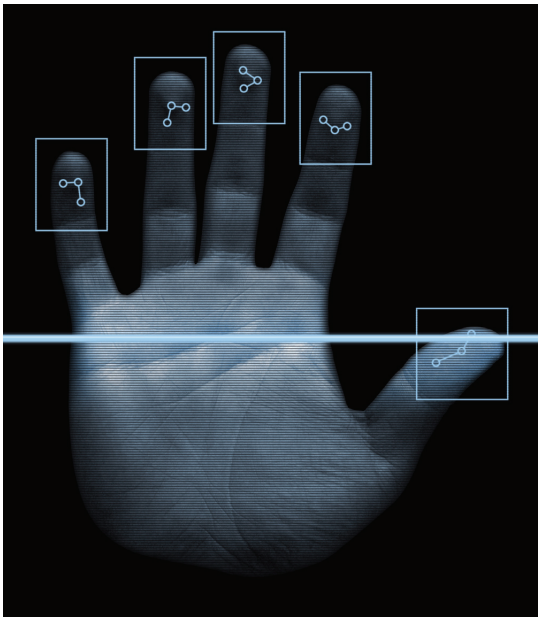
Detection of altered fingerprints. (Left) Altered fingerprints with 'Z'-shaped cut and (right) automatic detection of fingerprint alteration based on orientation field discontinuity. Brighter pixels in (right) represent discontinuity in orientation field and correspond to the scarred region in the altered 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. 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 combined that was bulky and inconvenient and possibility spoofable by a live (un-authorized) finger in combination with the spoof finger.

The advantage of the 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. These CITeR-developed algorithms are being considered by major biometric companies internationally. Researchers have developed and applied for patents that represent the next generation of these original liveness algorithms. The center universities have licensed the intellectual prop-

erty to a start-up company, called NexID Biometrics, LLC, incorporated and owned by the researchers. The company is now developing the technology for licensing to the biometric industry and system integrators for integration with their devices.

Economic Impact: Research performed in CITeR has been followed by thorough evaluation and commercialization through a small company. The algorithm has been customized to provide liveness detection for variety of fingerprint sensors. Its commercialization pathways included collaboration with CITeR affiliates on high-security applications as well as integration in mass market swipe fingerprint sensors integrated with laptops. At this time, well over 1,000,000 laptops sold worldwide include versions of fingerprint liveness detection approaches derived from CITeR research.

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

Multimodal Biometric (MUBI) Toolset

The design of multi-biometric systems has become significantly easier. Researchers at the Center for Identification Technology Research (CITeR) have developed the Multimodal Biometric (MUBI) Toolset. This toolset addresses the growing need in the prediction and evaluation of performance of systems that integrate multiple biometric devices and/or modalities. The toolset brings together more than a dozen algorithms from the research literature. It includes an embedded tutorial on multimodal biometric systems and fusion techniques. These algorithms represent all major types of biometric score normalization and fusion. The toolkit offers performance curves representing each biometric device. Then, it calculates ranges of performance characteristics (genuine accept vs. false accept rates) of different multi-biometric system configurations. It assists users with the selection of individual device performance characteristics such that they meet the desired application-specific performance goal. No such tool existed before the MUBI became publicly available as an open source software product, downloadable at no charge from CITeR's Web site. The toolset supports biometric systems designers, system evaluators, students and all others interested in performance analysis and integration of biometric systems. For the developers of multi-biometric systems, MUBI significantly reduces the time needed to analyze and define the most suitable combination of biometric devices/modalities. Center developers are receiving numerous inquires about specific tool features from companies and federal agencies. The development of MUBI continues by adding features, improving graphical user interface, and allowing tool users to integrate their own experimental fusion techniques into the tool.

Economic Impact: The toolset has been downloaded hundreds of times, mostly by students studying information fusion techniques in biometrics, software engineering and sensor networks. At the time that MUBI was being developed by CITeR researchers, major biometric systems in the US government (FBI's New Generation Identification system and the Department of Defense's Automated Biometric Identification System, etc.) moved towards adopting such multimodal identification techniques. Currently, MUBI is being used by CITeR members to investigate and develop optimal combinations of biometric modalities for clients. CITeR is committed to keeping MUBI available free of charge through an open source software license.

For more information, contact Bojan Cukic or Arun Ross, 304.293.9686, bojan.cukic@mail.wvu.edu, arun.ross@mail.wvu.edu.