

Center for Identification Technology Research (CITeR)

West Virginia University, Lawrence Hornak, Co-Director, 304.216.4539,
Lawrence.Hornak@mail.wvu.edu

West Virginia University, Bojan Cukic, Co-Director, 304.216.4540, Bojan.Cukic@mail.wvu.edu

West Virginia University, LaRue Williams, Assoc. Director of BKnC for CITeR, 304.293.8274,
Larue.Williams@mail.wvu.edu

University of Arizona, Judee Burgoon, Director of UA Site, 520.621.5818,
jburgoon@cmi.arizona.edu

Marshall University, Terry Fenger, 304.690.4363, fenger@marshall.edu

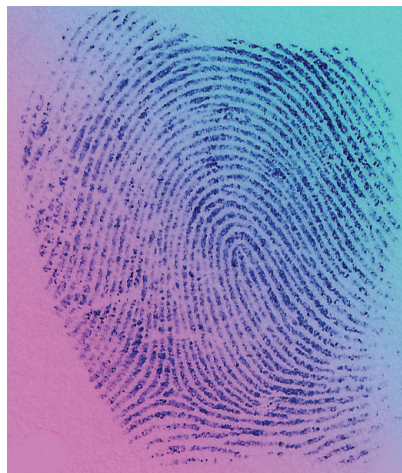
Michigan State University, Anil Jian, 517.355.9282, jian@cse.msu.edu

San Jose State University, James Wayman, 408.924.4037, biomet@email.sjsu.edu

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

Fingerprint Liveness Detection

It has been shown that fingerprint biometric scanners, used for secure authentication, can be deceived very 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, is 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 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 main stream 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



Center for Identification Technology Research (CITeR)

major biometric companies. Researchers have submitted and is continuing to develop patents for the liveness algorithms. The center universities are in the process of licensing the patents to a start-up company, called NexID Biometrics, LLC, incorporated and owned by the researchers. The company will develop and license the technology to the biometric device industry and system integrators for integration with their devices. For more information, contact Stephanie Schuckers at Clarkson University, 315.268.6536, sschucke@clarkson.edu or Lawrence Hornak at West Virginia University, 304.293.0405, lawrence.hornak@mail.wvu.edu.

Multimodal Biometric Toolset

The design of multi-biometric systems has become significantly easier. Researchers at the Center for Identification Technology Research (CITeR) have developed the MUBI Toolset which addresses the growing interest 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 techniques. The toolkit presents performance curves from multiple biometric devices. 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. 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, DoD's Automated Biometric Identification System, etc.) moved towards adopting such multimodal identification techniques. It is being used by CITeR members to investigate and develop optimal combinations of biometric modalities for clients. Center developers are receiving numerous inquiries about specific tool features from companies and federal agencies. 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 at West Virginia University, 304.293.0405, bojan.cukic@mail.wvu.edu, arun.ross@mail.wvu.edu.