

Altered Fingerprints: Analysis and Detection

Soweon Yoon and Anil K. Jain

Michigan State University

The widespread deployment of Automated Fingerprint Identification Systems (AFIS) in law enforcement and border control applications has heightened the need for ensuring that these systems are not compromised. While several issues related to fingerprint system security have been investigated, including the use of fake fingerprints for masquerading identity, the problem of fingerprint alteration has received very little attention. Fingerprint alteration refers to the deliberate obfuscation of the fingerprint pattern by an individual for the purpose of masking his identity by means of abrading, cutting, applying acid, or performing plastic surgery on fingertips. Since the fingerprint alteration is a serious threat to the AFIS, detection and matching of the altered fingerprints are on the desired list of most law enforcement and border control agencies. In this talk, the followings will be presented:

- high profile fingerprint alteration cases reported in the press;
- impact of fingerprint alteration on the accuracy of state-of-the-art commercial fingerprint matchers;
- classification of altered fingerprints into three major categories;
- a technique to automatically detect altered fingerprints based on analyzing orientation field and minutiae distribution;
- performance evaluation of the proposed algorithm and a standard fingerprint quality assessment software, NFIQ algorithm, on a large database of altered fingerprints provided by a law enforcement agency.