Distributed, Integrated Biometric Authentication System (DIBAS)

Traditionally, access to high security work areas and warehouses is restricted to a well-defined population of trusted employees. Such building access control systems often employ key cards to identify those in the trusted group. Doors to such areas are only unlocked if a valid key card is presented. While this provides some degree of security, key cards can easily fall into the wrong hands. The Distributed, Integrated Biometric Authentication System (DIBAS) aims to combat this problem by authenticating the holder of each key card using his or her fingerprint or similar unique physical characteristic. This type of biometric verification is already appearing in commercial building access control systems, but current verification algorithms produce error rates that are unacceptably high for most secure buildings. To combat this problem, DIBAS enables biometric devices throughout a building to combine their verification results. As a person passes through several secure doors, he or she creates a path of previous verification information for combination. Using a custom simulation framework, we have shown that verification accuracy at each door can be improved significantly by combining the decisions along this path. Future work will seek to improve the algorithm by which decisions are combined and deploy a small access control testbed.