

Face-Scanning Failures Need to Be Publicized to Help Security

The results of tests with face scanning at Boston's airport have come to light only a year after the trial ended. Experiments will eventually identify the right conditions for success, but real progress requires sharing results openly.

Event: On 2 September 2003, USA Today reported that face-recognition systems from Identix and Viisage fared poorly in a pilot project at Boston's Logan Airport in 2002. The airport completed its report in July 2002 but did not make it public. The American Civil Liberties Union obtained a copy in August 2003 through a Freedom of Information Act request. In the test, the airport put photographs of 40 airport employees, who volunteered to play potential terrorists, into a database. The employees then attempted to pass through two security checkpoints with face-recognition cameras. The systems failed 96 times out of 249 to detect them as they passed through during a three-month test period: a 39 percent failure rate.

First Take: This report deals a further blow to the use of this biometric technology to uncover criminals, terrorists or others on watchlists. Facial recognition is the only such technology available today for this application. Recently, police in Tampa, Florida, stopped a two-year facial-recognition trial that resulted in no arrests. Watchlist applications encounter the following challenges:

- Data that comes from photographs of the subjects (not the subjects themselves)
- Uncooperative subjects
- A variety of environmental conditions (variable lighting, for instance)
- Surveillance camera images that seldom show the subject full face or profile

The Logan test shows that even at airport security checkpoints, where environmental conditions are typically more favorable than on a city street, many other factors can prevent success.

Experiments like this will help identify the conditions that result in success and failure. However, such experiments will advance security only if the results are widely published. Gartner believes that the parties involved in the Logan test should have made the full results public immediately (an article on the test in the Boston Globe in August 2002 doesn't count).

Face-scanning can still provide benefits in other applications beside watchlists. Face scanning has prevented multiple registrations and so reduced identity theft and benefits fraud. Face scanning also shows promise for identification and authentication in physical and logical access control systems, but more mature technologies, such as smart cards, remain more effective in enhancing enterprise security.

Recommendations

Gartner

The content herein is often based on late-breaking events whose sources are believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of the information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The conclusions, projections and recommendations represent Gartner's initial analysis. As a result, our positions are subject to refinements or major changes as Gartner analysts gather more information and perform further analysis. © 2003 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction of this publication in any form without prior written permission is forbidden.

- Experiments with clearly stated and measurable criteria for success should continue to test the strengths and limitations of face-scanning and other biometric technologies in watchlist applications.
- Ideally, experiments should be coordinated with — and the results published by — organizations such as the U.S. Biometric Consortium and the European Biometrics Forum.
- Before purchasing facial-recognition or other biometric products, enterprises should understand which applications suit each technology and what threats and vulnerabilities biometrics cannot address.

Analytical Source: Anthony Allan, Gartner Research

Recommended Reading and Related Research

- “Test Shows Challenges of Automated Facial-Recognition Surveillance” — Avoid widespread deployments of automated surveillance technologies until the conditions that result in success and failure have been identified via controlled experiments. **By Richard Hunter**
- “Biometric Authentication: Perspective” — Midsize and large enterprises should adopt authentication middleware that allows biometrics to be used in combination with other authentication methods. **By Anthony Allan**

(You may need to sign in or be a Gartner client to access all of this content.)