

Tuesday, July 17, 2007

Looking for Signs of Life

New facial-recognition software features a test that can root out fraudsters trying to pass off a photograph as a real person.

By Duncan Graham-Rowe

Scientists in Sweden have developed a liveness-detection system that they say should help reduce the chances of face-biometrics systems being fooled by photographs.

"Liveness is going to be a major issue for biometrics," says [Josef Bigun](http://www2.hh.se/staff/josef/) (<http://www2.hh.se/staff/josef/>), a professor of signal analysis who led the research at Halmstad University, in Sweden. This is particularly the case with face recognition. "[Today's systems] cannot tell the difference between a picture and a face," he says.

While some systems have rudimentary defences designed to spot photographs, a crook can easily foil them just by bending the picture, says Bigun. Detection systems need to be "a little bit more sophisticated," he says.

Most face-recognition systems assume that the users will always be accompanied by an official to monitor the process.

But as face biometrics becomes more ubiquitous, this will not always be an option. Some companies, such as the Japanese firm [Fujitsu](http://www.fujitsu.com/) (<http://www.fujitsu.com/>), are already using unattended hand geometry readers to enable people to withdraw cash at ATMs. Face biometrics is likely to follow a similar path, says Bigun.

[Michael Jones](http://www.merl.com/people/mjones/) (<http://www.merl.com/people/mjones/>), a face-recognition researcher at the Mitsubishi Electric Research Laboratories, in Cambridge, MA, believes that face recognition will be more prone to fraud: "It's so easy to get a photo of a face. You can't get someone's irises or fingerprints off the Internet."

Bigun is trying to combat the problem by using an algorithm that measures the optical flow--a measurement of the 3-D movement of two-dimensional information--to detect how parts of a real face should move in 3-D relative to each other.

Face biometrics currently use two much simpler processes to try to detect liveness. One is to measure how similar the face being presented is to the stored face template of a particular person. Since no two presentations of the same face will look exactly the same, biometrics systems are, somewhat ironically, designed to reject faces that too closely match the original template. So in theory, it may detect a picture if it looks too similar to the original template. But there's an easy way to get around this, says Bigun: "You simply add statistical noise to an image." This could be done using a digital copy of the image and basic photo-manipulation software: a user could randomly add dots to the image to introduce small errors.

The second approach uses optical flow to measure the movement of key parts of the

face--such as the nose, eyes, and ears--relative to each other. The aim here is to detect slight movements of a photo as the fraudster holds it in front of the camera. If all regions of the image move in a perfectly linear fashion--that is, the nose, eyes, and ears all move in precisely the same way--then the system recognizes that a photo is likely being used.

However, this approach runs the small risk of rejecting a legitimate person if he or she happens to be holding his or her facial expression very still. Also, as mentioned, simply bending a photo can fool these algorithms because it will cause different points of the photo to move at slightly different trajectories from the point of view of the camera, since they are not on the same two-dimensional plane.

According to [Michael Bronstein \(http://www.cs.technion.ac.il/~mbron/\)](http://www.cs.technion.ac.il/~mbron/), a computer scientist who works on 3-D face recognition at the [Technion Institute of Technology \(http://www.technion.ac.il/\)](http://www.technion.ac.il/), in Israel, another method used by commercial face-biometrics systems is to try to detect natural movements, such as blinking. However, these systems could be fooled by a video recording, Bronstein says.

Bigun's approach takes the optical-flow concept a step further. "We looked at how a 3-D face moves," he says. By comparing how bent photos of faces and real faces move, the researchers were able to identify differences in the trajectories of key facial points. For example, the movement of an ear and nose as a head turns slightly will be different from those appearing on a bent photo. This is because the parts of the face in the photo are still on a single plane, even if the photo is bent; conversely, the trajectories of 3-D facial features are more complex and follow a particular pattern relative to each other. Using this information, the researchers created a system to detect such discrepancies.

In experiments using 400 high-quality photographs and 400 video recordings of real people, the system was able to achieve an equal error rate--a common standard in biometrics in which the number of false matches is equal to the number of false rejections--of 0.5 percent. The results will be published in a forthcoming issue of the journal *Image and Vision Computing* (http://www.elsevier.com/wps/find/journaldescription.cws_home/525443/description#description).

"It makes sense to do this," says [Mark Nixon \(http://www.ecs.soton.ac.uk/people/msn\)](http://www.ecs.soton.ac.uk/people/msn), a professor of computer vision at the University of Southampton, in the UK. "Liveness is quite an issue." Some other kinds of biometrics already have ways of dealing with it, such as fingerprint biometrics. "You can use infrared and sweat to give a liveness measure," Nixon says.

According to Bigun, the only way of beating the system he helped develop would be to make an accurate 3-D mask of someone's face. While it's feasible that someone with connections to Hollywood makeup artists could do this, it's pretty unlikely, says Mitsubishi's Jones. "It's just not practical for the random criminal."

Copyright Technology Review 2007.

Upcoming Events

[AVS 55th International Symposium and Exhibition \(http://www2.avs.org/symposium\)](http://www2.avs.org/symposium)

Boston, MA

Monday, September 01, 2008 - Friday, October 31, 2008

<http://www2.avs.org/symposium> (<http://www2.avs.org/symposium>)

[EmTech08 \(http://www.technologyreview.com/emtech/08/\)](http://www.technologyreview.com/emtech/08/)

MIT Campus, Cambridge, MA

Tuesday, September 23, 2008 - Thursday, September 25, 2008

<http://www.technologyreview.com/emtech/08/> (<http://www.technologyreview.com/emtech/08/>)

[Nano-Net 2008 \(http://www.nanonets.org\)](http://www.nanonets.org)

Boston, MA

Monday, September 15, 2008 - Thursday, September 18, 2008

<http://www.nanonets.org> (<http://www.nanonets.org>)

[NanoMedicine Summit \(http://www.nanomedicinesummit.org\)](http://www.nanomedicinesummit.org)

Cleveland, OH

Thursday, September 25, 2008 - Friday, September 26, 2008

<http://www.nanomedicinesummit.org> (<http://www.nanomedicinesummit.org>)

[WHIT 4.0 \(http://www.whitcongress.com\)](http://www.whitcongress.com)

Washington, DC

Monday, December 08, 2008 - Wednesday, December 10, 2008

<http://www.whitcongress.com> (<http://www.whitcongress.com>)