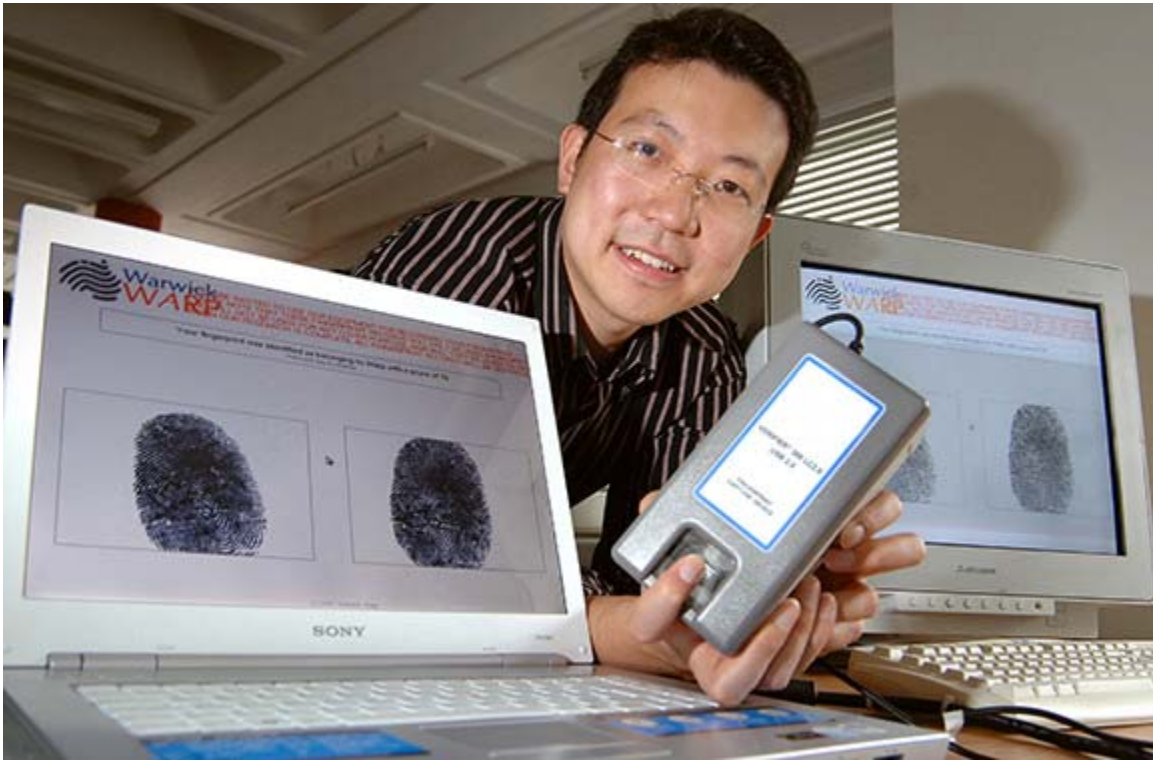


WIRED

[<< Back to Article](#)

New Fingerprint Tech Could Mean Never Losing Your Keys Again

By Alexis Madrigal 10.02.07 | 12:00 AM



Dr. Li Wang of Britain's University of Warwick shows a prototype of Warwick Warp, a biometric system that enables identification of distorted and partial fingerprints.

Photo: Courtesy of Alexis Madrigal

Scientists in Great Britain hope you may never have to worry about losing your keys or forgetting your password a

University of Warwick researchers have unveiled a new fingerprint recognition technology, which allows them to identify distorted prints. The technology could prove especially important in mass-market biometric access systems, which remained elusive because of small but significant rates of false positives and negatives.

Fingerprint recognition came into wide use in forensic investigations in the early 20th century. Ever since, sci-fi writers and scientists have dreamed of using the unique skin contours on our fingertips to tell our machines we really are who we are. The problem is that the number of errors has just been too high.

"In real settings, the best algorithms I've seen are still talking about an equal error rate of 3 to 4 percent," said [Dr. V Govindaraju](#), director of the Center for Unified Biometrics and Sensors at SUNY-Buffalo. "In good settings, we're at 0.2 to 0.3 percent." (The equal error rate is when the sensitivity of a test is adjusted to the point where the proportion of false-positive results equals the proportion of false-negative results.)

Three percent may be good enough for a low-security location like a public library, but nowhere near good enough for military-grade installations or even airport security.

Most current technologies focus on what the experts call Level 1 and Level 2 features. Level 1 is the general pattern fingerprint (you remember: arch, loop, whorl). Level 2 includes the specifics of the way the contours end and split. The problem is that a host of environmental factors can throw noise into the data. One major noise source is that people press their fingers onto sensors with varying amounts of pressure, generating non-linear stretching.

"The skin stretches differently depending on how hard you press, which moves the Level 2 features around," explains Govindaraju.

It's the same idea that web forms use to defeat spammers: Distort letters a certain amount and a person -- like a CS professor -- can recognize the pattern, while most electronic systems are defeated. Good for the cleanliness of [WiSci's](#) comment section, but bad for biometric researchers.

Enter [Warwick Warp](#), the brainchild of three British computer scientists. The company has received seed capital from [Early Investments](#), and it's on the prowl for another million dollars of equity financing. The scientists have come up with a system that recognizes the distortions introduced by those disobedient individuals who don't treat the sensor like an instrument.

"We're trying to model the variations and therefore minimize them," said Dr. Li Wang, chief technological officer at Warwick Warp. The company's algorithm filters out the environmental distortion and then unwraps the contours. Drawing on our distorted-letter analogy, it helps reflatten the letter into a shape recognizable by any spambot.

It's a promising technology, but one that is still unproven. "There's some merit to that idea," said Govindaraju. "But I've never seen real numbers."

We might see some real numbers very soon: The company plans a commercial release within six months.

Though it's not the company's focus, the Warp technology could have applications in forensics. After all, the system is designed to work with the kinds of non-ideal prints that unintentional situations tend to generate. The ability of the system to work with partial or smudged prints could increase the number of latent prints that investigators can use among those they find in the field. All those smudged prints that Horatio from *CSI: Miami* now tosses aside could now become evidence for his [famous one-liners](#).

Other companies, meanwhile, are looking at other ways of dealing with the mashable-finger problem. Some suggest that fingers shouldn't make any contact with the scanner. Mitsubishi [introduced the first such model](#) back in 2005, but with a hefty price tag of about \$4,500.

When it comes to the mass-market rollout of biometrics in access systems, fingerprinting technology is probably one piece of the puzzle. Face-recognition and iris-scanning products offer some advantages over fingerprinting but are more expensive. They could end up serving the high-end security markets, while simpler technologies with higher tolerance just keep us from getting locked out of our cars. The ultimate solution, though, might be a biometric mask using a fingerprint scan and facial recognition.

"The way biometrics is going is combining biometrics," said Govindaraju. "Why use just one?"

No story about biometrics is complete without mentioning privacy concerns. As they say in business, if you can manage it, you can manage it. And not everyone wants to be managed, especially if the government or a big corporation has the calipers. As the [Electronic Frontier Foundation](#) summed it up, "Biometric technology is inherently individuating at interfaces easily to database technology, making privacy violations easier and more damaging."

The privacy impact, however, will remain small until the technology becomes widespread. And because [companies actually prefer that you carry around their branded plastic](#), there's no guarantee that it will go mass-market, even in the long term.