Fingerprint Advances Will Fight Cybercrime

February 24 2006

UB software is able to identify computer users even on the basis of partial prints of the same finger, like those pictured here.

Forgot your password? No problem. Biometrics researchers at the University at Buffalo have made important advances that bring closer the day when we can access devices and Web sites with nothing more than the touch of a fingertip.

"This research paves the way toward efficient methods of preventing unauthorized access to handheld devices, such as cell phones, wireless handheld devices and electronic audio players, as well as to secure Web sites," explained Venu Govindaraju, Ph.D., principal investigator, UB professor of computer science and engineering, and director of the university's Center for Unified Biometrics and Sensors (CUBS). "It also will help make fingerprint matching for forensic applications more effective."

Fingerprint access potentially can eliminate the need for consumers to remember all those annoying passwords, he added.

The UB research addresses a key problem that has emerged in the quest for fingerprint access to electronic devices and Web sites: quantifying how much security is possible with fingerprinting, given that most commercial sensors tend to capture only partial fingerprints.

"This problem needs to be overcome before it will be possible to routinely replace passwords with fingerprints," Govindaraju said.

The UB research specifies the physical dimensions of the keypad sensor in order to achieve specified levels of security, an issue that is of growing importance as devices become ever smaller.

Govindaraju explained that any company considering using fingerprint matching for access will want to be able to quantify what level of security is possible.

"With passwords, this is an easy task," he said, "obviously a six-letter password will be much more difficult to break than a three-letter password because there are so many more possible combinations."

Similarly, Govindaraju and his colleagues decided to try to quantify how big a fingerprint image has to be in order to achieve an acceptable level of security.

"For the first time, we have determined the minimum surface area required for fingerprint scanning in order to achieve a level of security that is roughly comparable to the security achieved with a six-letter password," he explained.

Called the Automated Partial Fingerprint Identification system, the algorithm developed by the UB scientists enables computer systems of, say, banks or online retailers, to determine whether or not to grant access, by securely matching two fingerprint images (the stored one and the "new" one) even when only part of the print is captured.

That's important, Govindaraju explained, because whether they are fingerprints, facial images or voice inputs, biometrics often are captured under less than ideal conditions.

"Since our matching method assumes that the fingerprint image is not complete, it allows for more robust feature matching," he said.

The work was published in Pattern Recognition, the Journal of the Pattern Recognition Society.

In a similar vein, the UB researchers solved another problem that stems from the fact that unlike a password, even the right fingerprint comes out slightly differently each time it's imaged.

"With passwords, it's always the same characters and the user hits the right keys," he said. "But with fingerprints, every time you touch the sensor, the image will be slightly different, just as no two photographs are ever exactly the same."

In order to protect a user's identity and access data, databases such as those of credit card companies don't store the exact password that you type into the computer each time. Rather, they store an "irreversible" transformation (called a "transform") of that password and when the entered password matches with the stored transform, access is granted.

To securely match fingerprint images with their "transforms," he explained, a robust system will have to ensure that it can compensate for the fact that from time to time, even the right fingerprint will vary in the amount of pressure that was used to create it, the amount of moisture on the finger or the part of the print that is captured.

"The algorithm we developed allows the system to make a transformation of the fingerprint image by encoding certain features of the fingerprint and then transforming them in a way that is unique to that fingerprint," said Govindaraju.

"This is one of the first implementations of what is known as a cancelable biometric, using standard feature representations, because what is being stored is not the fingerprint image itself, but a transformation of that image," he said. "It is nearly mathematically impossible to reverse engineer it."

A patent has been filed on this technology.

The research was funded by the University at Buffalo, a premier research-intensive public university, the largest and most comprehensive campus in the State University of New York.

Source: University at Buffalo

Citation: Fingerprint Advances Will Fight Cybercrime (2006, February 24) retrieved 26 April 2024 from https://phys.org/news/2006-02-fingerprint-advances-cybercrime.html