

Eye-catching mobile security on its way

The mobile phone may soon be equipped with a higher level of security thanks to Leeds, United Kingdom-based technical solutions company xVista and its iris-scanning technology.

The company says it has developed what it considers to be United Kingdom's first iris-scanning system that can be housed within compact low-power computing systems such as a camera mobile phone. And with this technology developed in collaboration with the University of Sussex under a \$3.4 million six-year partnership, xVista is hoping to capitalize on the rapid growth of the \$1.5 billion global biometrics market, it says.

"The xVista technology performs a similar task to the traditional signature, photograph or pin number in confirming an individual's identity, but is far more reliable," remarked xVista Managing Director Karlis Obrams, who formed the company back in 2000. "The fact that the system can run from portable devices like the mobile phone and SIM card opens up fantastic potential for its use, making it far more effective than other scanning systems that are usually bulky and limited to fixed points."

According to xVista, the technology that scans and maps the iris for individual characteristics uses a unique algorithm designed specifically to be operated on low-power computing devices such as a phone with a standard 256 MB mobile-phone memory card -- which is able to hold over 250,000 separate iris templates and from a database of 1,000,000 irises could take less than one second to verify an individual iris.

And with the iris data scanned onto a central database, a template is created to be checked against all further scans to verify the user's identity, the company said.

"Using an airport as an example, the xVista system can be deployed across all members of a security team in a discreet handheld device, enabling staff to know within seconds whether a pilot, crew member or baggage handler is who they say they are, offering peace of mind against threats such as identity theft and terrorism," Obrams added.

But that's not all xVista's iris scanning and verification technology can be used for, as the company said it could be applied to other markets including consumer electronics security, financial transactions, mobile telecom and banking.

In a further interview with United Press International, Obrams explained that even though the mobile phone isn't as efficient as a PC, the scanning technology's ability to be operated by low-power computing system opens up a range of applications especially as the chances of two irises matching is about one in 7 billion, protecting against fraud.

"The system is so efficient that it doesn't even interfere with the use of a mobile phone," Obrams said.

As an example, Obrams suggests that if an individual's mobile phone is stolen, with their iris scanning technology, it acts both as a theft prevention mechanism by identifying and verifying the owner and scanning the iris of the thief storing it on the database.

He also proposes that their technology be used as an element of security for financial transactions in terms of micro-payments, useful as the mobile eventually may soon carry small deposits of cash, electronic cash, or used for Internet shopping.

Moreover, he also recommends that xVista's technology be used for other security issues such as authenticating individuals in medical/aid distribution as well as for voter registration in other countries other than using blue/black ink.

But as the company is currently in discussion with the U.K. Defense Diversification Agency -- responsible for identifying new civil technology for defense and homeland security application -- it is also seeking opportunities from financial institutions and their customers from the micro-payment and security arenas interested in implementing additional security in such devices as the mobile phones, according to Obrams.

"Our technology gives the public the control over their biometrics and the mobile phone is something you don't leave behind," he said.

Copyright 2006 by United Press International

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.