password

Philips Research technology magazine - issue **30** - September 2007

"Biometrics is entering our daily life."

Personal biometrics, private data

"New audiovisual techniques that greatly enhance the video phone call experience."

A natural feel for video telephony

"Non-experts should be able to carry out in-vitro diagnostic tests at a patient's hospital bedside or in a doctor's office waiting only a matter of minutes before the results are available."

From central laboratory to bedside – sense and simplicity in the diagnosis of disease

"The Compact Disc has played a pivotal role in the shift from analogue music to digital."

25 Years Compact Disc

PHILIPS


Biometric ePassport Authentication Kiosk
PHILIPS

Personal biometrics, private data

Place your hand on the door and it opens just for you. The entertainment system recognizes your face and plays your favorite music. Your computer reads your fingerprint and immediately lets you access your personal files and emails.

By Stuart Cherry
Photography/graphics: Michel Klop, Media Partners

Fast, convenient and secure, biometric identification is no longer just for passports and science fiction. It's now appearing in a growing variety of 'everyday' applications. Within this proliferation of biometric systems, a new technology from Philips Research could ensure private data stays just that – private.

Many people see biometrics as the ultimate form of identification. By using physical characteristics like fingerprints, facial image or hand geometry (rather than passwords or 'badges') to identify people, it enhances both convenience and security. After all, you can't forget your fingers and it would be difficult for someone to steal your retina!

Moreover, for the user, biometric identification is fast and simple. You just scan the appropriate characteristic and, in a fraction of a second, the system compares the scan to a stored biometric template.

Crime to consumer

Biometric identification dates back to the 1890s, when police began using fingerprint evidence to solve crimes. More recently, governments have started adding biometric data to passports and ID cards. However, convenience and security appeal as much to individuals as to governments. So it should be no surprise that manufacturers are looking to include biometrics in all kinds of more personal applications.

"Biometrics is entering our daily life. It started with biometric passports, visas and fast track border control at airports, but a large variety of commercial services that increase convenience by using biometrics are now under development," says Max Snijder, CEO of the European Biometric Forum.

The business world saw the first non-governmental biometric applications, with companies using biometric identification to control access to their buildings and computer systems. From the office, biometrics is now moving into the home. A few minutes on the Internet reveals numerous items like wall safes and jewelry boxes with 'fingerprint locks' for sale today. These applications are just the start and biometrics could soon be appearing in all kinds of lifestyle products as Michiel van der Veen, Cluster Leader Secure Identification Technologies at Philips Research, explains. "Products such as televisions could use biometrics to match people to their pre-

Keeping the noise down

privID™ uses cryptographic hash functions to encrypt data in a way that can never be decrypted. Applying the same hash function to the same template always gives the same result, but small differences between templates will lead to two completely different hash values.

This second property is great for security purposes as it makes it very difficult for a potential identity thief to link the hashed template back to the individual. However, it presents a real implementation challenge when applied to biometrics because biometric measurements are noisy: i.e. different scans of the same biometric will have small differences due to, for example, different lighting conditions or variations in the scanner.

To overcome this, privID™ combines techniques such as noise estimation and adaptive analog-to-digital conversion to reduce both the noise in and size of the template. It then employs error-correction codes similar to those used in scratch-tolerant CDs to give a noise-free representation of the biometric template – perfect for hashing.

stored personal settings. Voice recognition could be very useful for enhancing user interfaces, for example controlling hands-free access to computer systems. And then there's keyless entry – no more searching for keys, a biometric scanner in the handle could automatically open the door for you."

The privacy challenge

The proliferation of biometrics could greatly simplify life for us all, but it is not without its issues.

According to Ontario Information and Privacy Commissioner Ann Cavoukian, a world expert on biometric identification, "the fundamental fear from a privacy perspective is the possibility of rampant tracking of one's activities." She adds that biometric applications are a tempting target for identity thieves. Gaining access to your stored biometric template would allow unauthorized parties to "impersonate you ad nauseam."

For biometrics, this so-called 'privacy challenge' has a number of aspects. Firstly, a conventional biometric template can't be revoked. If a password is compromised (e.g. lost or stolen), it's a simple matter to cancel it and issue a new one. But you can't cancel a hand or face! Instead, if a biometric template is compromised (e.g. the device storing it is lost, hacked or stolen), you have to create a new template from a different biometric. And we only have a limited number of biometrics: one face, two eyes, ten fingers, etc.

Furthermore, a limited number of biometrics and a growing number of biometric applications would mean using the same template for more than one application. This opens up the risk of data mining. If an identity thief were to get hold of your template from one application, they could use it to access your information from any other system. For instance, by stealing your biometric TV, someone could get into your bank or medical records.

"Delivering both privacy and security through the use of privacy-enhancing biometrics is the best way to take advantage of the benefits of biometrics, while minimizing the drawbacks."
Ann Cavoukian, Ontario Information and Privacy Commissioner

Traditional biometric systems protect templates by storing them in encrypted form. However, to check someone's identity,

the template must be decrypted using a key before it can be compared with a live scan. This gives potential identity thieves two opportunities to access the template: intercepting the unencrypted template or stealing the encrypted template and key.

The privacy challenge becomes even more pressing as consumer biometric applications become more commonplace. More biometric systems means more opportunities for the theft and use of biometric information. In addition, consumer equipment tends to be less securely protected than government systems, so it is potentially easier to access biometric data without authorization.

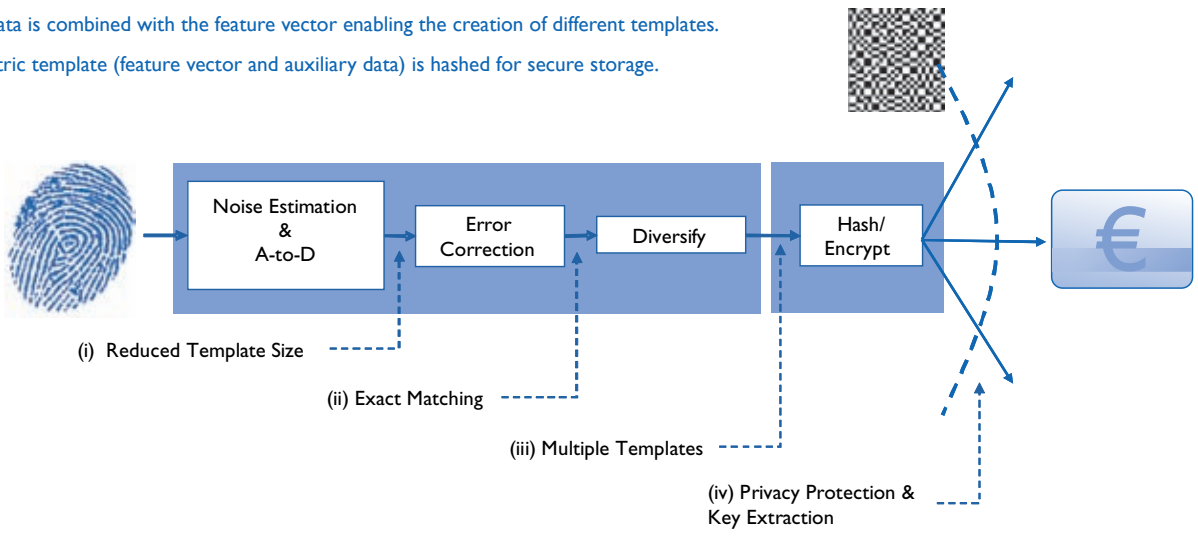
Secure biometric templates

To combat the privacy challenge, Philips Research has developed a new biometric storage approach that is inherently secure and enables the creation of multiple, easily revocable templates from a single biometric. Known as privID™, it has the potential to reduce both the chances of a template being compromised and the possible damage if it does occur.

privID™ protects biometric data through a technique known as one-way encryption or hashing. Once the template has been or hashed, it can never be decrypted. To check a person's identity, you scan the appropriate biometric, hash it and then compare the result with the stored hash value – the unencrypted template is never available to identity thieves.

Secure template creation

1. The biometric is scanned and transformed into a regular biometric feature vector. The signal-to-noise ratio is estimated and used to reduce the noise levels and data size without losing useful information.
2. Error-correction codes eliminate any remaining noise effects.
3. Auxiliary data is combined with the feature vector enabling the creation of different templates.
4. The biometric template (feature vector and auxiliary data) is hashed for secure storage.



Hashing is already widely used in password encryption systems. However, applying it to biometric templates was not straightforward. According to Michiel: "Our biggest challenge and breakthrough with privID™ was finding a way to hash data that isn't sensitive to the noise you always have with biometric measurements." (See 'Keeping the noise down'.)

Closing the data mine

While hashing ensures secure storage, it still only allows for one template per biometric. So privID™ incorporates auxiliary information into the template before it is hashed. The auxiliary information is essentially a random number but, crucially, that number can be different for each person and application.

"Biometrics is entering our daily life."
Max Snijder, CEO of the European Biometric Forum

With auxiliary information, each biometric can give rise to many different templates. So any compromised template can simply be revoked and replaced with a new one using the same biometric but different auxiliary information. Furthermore, as each template is radically different, an identity thief who gains access to one template can no longer use it to access other applications. The data mine is closed.

Driving market acceptance

Thus, privID™ helps solve the privacy challenge by ensuring unencrypted biometric templates are never available, by enabling renewable templates and by preventing data mining.
For Jean-Paul Jainsky, CEO of Sagem Securite (the market leader in biometric systems), such secure technologies are vital for public acceptance of biometric applications. "Sagem Sécurité has been involved in the implementation of biometric solutions for many years. Developing secure technologies to protect biometric templates is the key for the evolution of our business. Through the European research project 3D Face, we have teamed with Philips to explore this domain, and we intend to continue such cooperation in the future."

Besides its inherent security, privID™ leads to biometric templates that are relatively small and can be stored in binary form. Consequently, biometric applications can use low-cost storage media such as paper barcodes or simple RFID tags.
Not only is this a vital consideration for use in emerging markets, it opens the door to disposable biometric applications like event ticketing or boarding passes for air travel. It also means the templates can be quickly transmitted and compared. For the user, the whole process from scanning the biometric to having your identity confirmed takes a fraction of a second.

Although only in the very earliest stages of commercialization, privID™ has been warmly welcomed by the experts. "Legally, biometric information is considered personal data so its privacy and security are essential factors for the acceptance of biometric-enabled applications," says Max Snijder. "The privacy-enhancing technology Philips has developed is pivotal for a wide variety of large-scale applications where biometrics is being used for authentication and identification."

Ann Cavoukian agrees. She believes that "Delivering both privacy and security through the use of privacy-enhancing biometrics is the best way to take advantage of the benefits of biometrics, while minimizing the drawbacks. This is a very positive technology," she says. "It's new, but it's real and it's working now." PW

Extra info **www.research.philips.com/password**
biometrics • privID™