FOR INTERNAL USE ONLY / DO NOT COPY. PAPER ACCEPTED AT
The 2003 International Conference on Artificial Intelligence / Las Vegas / June 23-26

BIOMETRICS FOR LARGE-SCALE CONSUMER PRODUCTS

Jean-François MAINGUET

Atmel-Grenoble, Avenue de Rochepleine, BP 123, 38521 Saint-Egrève, France

Abstract

Personal digital assistants are now multimedia devices, containing personal sensitive information. Built-in biometrics enhances the protection of these data, offering convenience and better security without hassles related to passwords. The FingerChip®, the sweep thermal fingerprint sensor from Atmel, has been successfully implemented in the iPAQ Pocket PC®, the Personal Digital Assistant (PDA) from HP, using the recognition software from Cogent Systems, as this system offers all the requirements a biometric device needs to fulfill for a PDA.

Keywords: biometrics, fingerprint

1. Introduction

Protecting information is important but is a hassle to the user. People hate to remember PINs (Personal Identification Number) or passwords, so they are generally not very secure as written somewhere else. Most of the time, people do not enable the password protection on PDA, just because they are always turning on/off the device, and it becomes annoying to enter each time the secret word with the feeling that surrounding persons are staring at you to catch your secret…

Biometrics, if properly implemented, remove these problems. In this paper, conditions to implement biometrics in a personal digital assistant (PDA) are discussed, and can be applied to any small portable electronic systems such as cellular phones.

2. Requirements

In the case of a portable device such as a PDA, a biometric system needs to fulfill the following requirements:

1. Low cost
2. Small form factor
3. Easy to use, fast
4. Reliable
5. Industrial device / mature technology
6. Acceptance (by users)

and some others considered as less important for this kind of applications.

3. Biometrics selection

Which biometrics can fulfill the requirements? Let's consider the main technologies available now.

- Hand geometry, vein recognition: obviously too large sensor.
- Iris/retina recognition: the autofocus camera to acquire the iris image is too expensive, and too large.
- Face recognition: not expensive if the camera is already build-in for other applications. Face recognition is not as reliable as other biometrics, but should be nice for authentication situation. A secondary problem is the acceptance of this technology, and people may think that a simple photo will fake the system (which is not true for good face recognition systems).

- Voice recognition: most of the time, PDA already integrates a microphone, so low cost is not an issue. Software are already available, it is just a matter to use it. We believe that's mainly because of reliability problems -voice is known to be inaccurate in noisy environment- that it is not used today. A secondary problem is the fact that you need to "talk to your PDA": you may feel stupid doing this, especially if random phrases are generated.

- Signature recognition: same as voice. Hardware and software are already available. Also, it seems that reliability and acceptance by users are the main reasons that voice and signature have not succeeded up to now. But this will certainly change in the future.

- Fingerprint: meets all requirements, the most difficult is probably the "ease of use", as most people are not used to fingerprinting.

It has to be noticed that fingerprint is very similar to typing a password from a "social" point of view: you don't need to speak to your PDA, or making an unusual movement to capture your face image. Coupled with the fact that police has proved the efficiency of fingerprints for identification, this is facilitating a lot the acceptance of fingerprinting.

4. Hardware selection

4.1. Built-in biometrics

Biometrics has already proposed for several PDAs, but it was always an add-on: the user was obliged to connect a separated biometric system to the device to protect. This is not a practical solution (ease of use criteria), because you need to carry this supplemental device, install the proper software to make it work. So a build-in device is better accepted and is more secure, because the design is adapted, and there are fewer possibilities to hack the system, as everything is integrated.

4.2. Fingerprint sensor selection

Several technologies exist to acquire fingerprints [1][2][3][4]. Optical devices cannot be used because of their large form factor, mainly because of the prism/lens apparatus. A flat device is required, and silicon sensing is the best solution at the moment: low cost, industrial and reliable.

Among silicon sensors, two main solutions are proposed:

- Static sensing: the user has to put his/her finger on the sensor, without moving. The silicon area is necessarily more or less the size of the finger.
- Sweep sensing: the user needs to sweep his/her finger over a linear sensor, which just need to be the width of the finger (fig.1).

Sweep technology reduces the cost of the sensor compared to static sensing, as less silicon area is required. This is a major advantage for PDA manufacturers and final users.

Sweep sensing also has a smaller form factor: it takes less area on the front side area of the PDA mainly reserved to the screen.

The only concern is about the "ease of use". Is sweeping a finger more complicated than putting a finger? This is different, and none is more or less complicated. You have to sweep your finger, not too fast although fairly high speeds are possible, and make sure to touch the sensor. With a static sensor, you have to press, not too much, without rotating at the same time, the same area of your fingerprint each time. And you have to learn how much time you need to let your finger, when to remove before trying again if needed.

Fig.1 sweep silicon fingerprint sensor

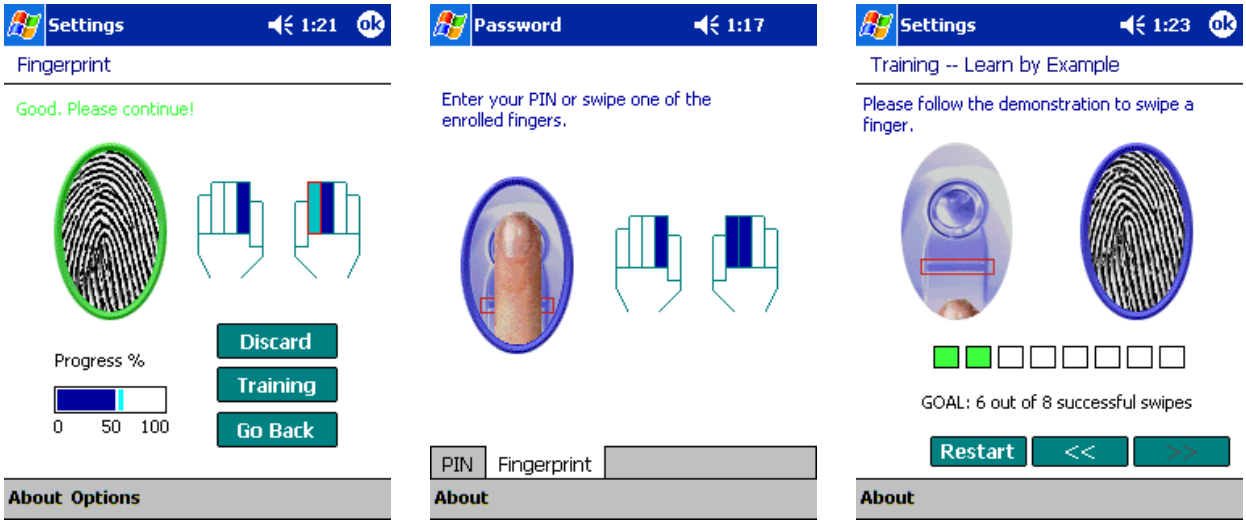

Fig.2: enrollment, logon and training. Note that the user interface is similar and very intuitive.

You can compare this to smart cards against magnetic stripe cards: you get quickly used to swipe your card, as well as insert your card in the reader in the right position. This is different, none is more difficult than the other is.

Physical sensing technique is a secondary parameter. Several physical effects such as capacitance [5] can be used. Atmel proposes the thermal sensing, which gives better images when the conditions are becoming difficult, especially with fingers qualified as "poor", with low depth between ridges and valley. And the thermal technology with sweep has been the very first mature sweep silicon fingerprint technology in high volume production.

5. Software implementation

Ease of use is also an important key for the software. If the software is not practical, complicated to adjust and difficult to understand, then people will reject the system. At best, good biometric software should be forgotten.

Biometrics are implemented exactly like the regular password application, there is nothing new on this side: you have to register several fingers (in case of), then give your finger each time the "password" is requested.

Only two new fundamental pieces of software are added to the regular password application:

1. The sensor driver, which will return a fingerprint image when requested.
2. The authentication software (often called the "bioengine") that will process the image, first at enrollment (signature storage), second at recognition (matching with the stored signature).

The driver has the particularity to have a very high priority, because the sensor must be available at logon, or the device will be locked.

User interface for biometrics appears in several places (fig.2):

- The password application, where the user enrolls, and also selects how to access the device. To enroll, several fingerprints (of the same finger) are acquired, processed, and a signature is extracted and stored in the non-volatile memory of the PDA.
- At logon: the user has to propose his/her finger that will be challenged against the enrolled fingers. To use the device, the user need to press the on/off button, then sweep his/her finger: nothing to click or select is required, to get a friendly and "forget it" interface. It must be fast: waiting one or two seconds is acceptable, but not 10.
- Training: prior the first enrollment, a simple training application is proposed to the user to teach the right movement to get good results.

Moreover, although some parameters can be adjusted, defaults are chosen so that the average user doesn't need to care. But it is possible to adjust some parameters to increase the security.

6. Convenience & security

Speaking of security is very often a difficult task if you don't refer to a system. It has to be understood that biometrics does not mean security. This is only when properly implemented in a system that it makes sense, and we can speak of *increased security* when comparing the same PDA using the regular password and the biometric system.

For instance, when you are speaking of security for a PDA, you are speaking of the personal data inside. Adding biometrics will not avoid the hardware to be stolen, but only the internal data.

We prefer to speak of *convenience* rather than security, in the way that the FingerChip is just replacing the password in the iPAQ Pocket PC. It's more practical to use his/her finger than remembering a password and you don't need to hide when typing your password: these are the benefit of biometrics, but there is nothing changed from a security point of view inside the device, compared to a password scheme.

It is always possible to increase the security level, but you need to add *security* features such as encryption, for instance to protect all communications between the sensor, the processor that runs the authentication software, the memory that stores the signature, etc…

7. Security related parameters

Only very few parameters are possible to adjust. It is not possible to propose a too complicated system to users, as most of the time, they don't want to read the documentation, and don't want to bother with difficult parameters.

For instance, it is possible to let the user choosing the number of matched minutiae to accept a fingerprint, but you will need to explain what is a minutiae, what is the probability to match and some other things the average user has never heard about.

So only simple and intuitive parameters are proposed:

- The number of trials before proposing a full reset. If you fail to enter for instance 6 times, then a full reset, erasing all the data, is proposed.
- Choice between 3 "security levels", which is not a so much good name, as this is only the probability a false match occurs that is adjusted.

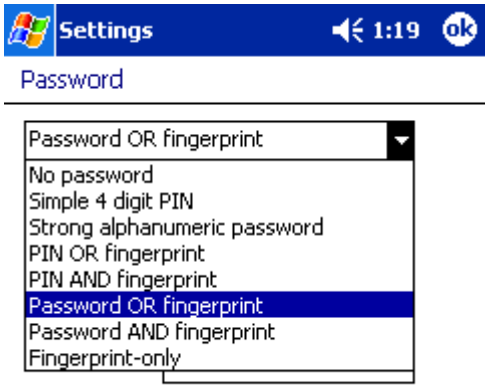

Fig.3 Selecting a protection method

The combination of the bioengine, the sensor and the ergonomics defines the false acceptance rate (FAR) and false rejection rate (FRR) (see [1] for more information). Remind that biometrics cannot be a 100% technology. We need to manage different fingerprint quality, and it always exists a possibility that a user cannot enroll (no fingerprint in the case of certain diseases).

Parameters have been chosen to fit the greater number of people, and take advantage that we are in a "1 to a few" situation. The probability that someone steal your device, and has fingerprints close enough to enter is extremely low, but not null.

8. Combined authentication systems

The use of the fingerprint is simply added to the existing security scheme, the PIN or the password, so that the user will choose his/her own logon management, from nothing up to fingerprint AND password.

Password already offers a good protection if properly implemented and used, so the combination of password and fingerprint should answer to most situations. Password is still necessary because you can *remotely* connect to the PDA through the infrared wire, Bluetooth, Wi-Fi or any other communication tools, so fingerprints cannot be used.

We do not believe that adding another biometrics such as voice recognition or signature will happen in the future, because it will be less practical to use.

Maybe an alternate biometrics will be proposed for people that cannot use fingerprints for some reasons (disabilities).

At the moment, with the actual device, we suggest paranoiac people to use a complicated password and fingerprints, but they are leaving the convenience / ease of use area. And forbid any contact through any communication tools.

This is a good example to show that security rely on the overall organization of the system, and not just on one feature. It is likely that in the future, some more security features such as SIM cards/ smart cards will be added.

9. Legal aspects

There is no legal problems as the fingerprints are not stored as images but as a signature, and moreover, there is no direct link with a username. This is rather "this machine is protected with this fingerprint". Note that you are even not obliged to enter your real name in the device! There is no database: only ten fingerprints can be stored.

10. More applications

The first use of the FingerChip in the iPAQ was to protect the access to the device. This will enable more applications than the basic logon:

- Electronic signature
- Encryption of data using fingerprint as a key
- Electronic commerce
- Personal access control device: the "door" asks your (wireless) iPAQ, properly registered (what you have), that you sweep your finger (what you are), and possibly write your password (what you know). You do not need to install a fingerprint reader at the door!

11. Conclusion

Biometrics has reached maturity: all the basic requirements are now available. The Atmel FingerChip sensor + the Cogent Systems Bioswipe bioengine in the HP iPAQ Pocket PC is the first built-in application in a large-scale consumer device, opening a new era.

Fig.4 iPAQ Pocket PC h5455 with the FingerChip

12. References

[1] J.F. Mainguet, M. Pegulu and J.B. Harris, “Fingerprint recognition based on silicon chips” *Future Generation of Computer Systems 16 (2000),* Elsevier, pp. 403-415.

[2] S. Shigematsu, H. Morimura, Y.Tanabe, T. Adachi, K.Machida1, “A Single-Chip Fingerprint Sensor and Identifier” in *IEEE Journal Of Solid-State Circuits*, Vol. 34, No. 12, pp. 1852-1859, December 1999

[3] C. Inglis, L. Manchanda, R. Comizzoll, A. Dickinson, E. Martin, S.Mandis, P. Silveman, G. Weber, B. Ackland, and L. O’Gorman, “A robust, 1.8 V 250 _W direct-contact 500 dpi fingerprint sensor,” in *ISSCC Dig. Tech. Papers*, Feb. 1998, pp. 284–285.

[4] M. Tartagni and R. Guerrieri, “A Fingerprint Sensor Based on the Feedback Capacitive Sensing Scheme,” in *IEEE Journal of Solid-State Circuits*, vol. 33, pp.133-142, Jan. 1998.

[5] J.-W. Lee, D.-J. Min, J. Kim, W. Kim, “A 600-dpi Capacitive Fingerprint Sensor Chip and Image-Synthesis Technique” *in IEEE Journal Of Solid-State Circuits*, Vol. 34, No. 4, pp. 469-475 April 1999

Jean-François Mainguet was born in Sarrebourg, France, on July 3, 1960. He became an engineer for Télécommunications de Bretagne in 1984.

Since joining Thomson-CSF Semiconducteurs Spécifiques, now Atmel, Grenoble in 1984, he has been engaged in the development of SOS and SOI rad-hard semiconductor devices, electrical simulation, layout & mask design tools, and analog to digital converter design.

He’s the inventor of the sweeping technique for direct silicon fingerprint scanning, and chief scientist of the FingerChip® project.