1.生物辨識概論

陳慶瀚
機器智慧與自動化技術(MIAT)實驗室
義守大學電機系
pierre@isu.edu.tw
2005年9月20日

大綱

什麼是生物辨識？

各種生物辨識的方法

生物辨識的應用

生物辨識的未來趨勢

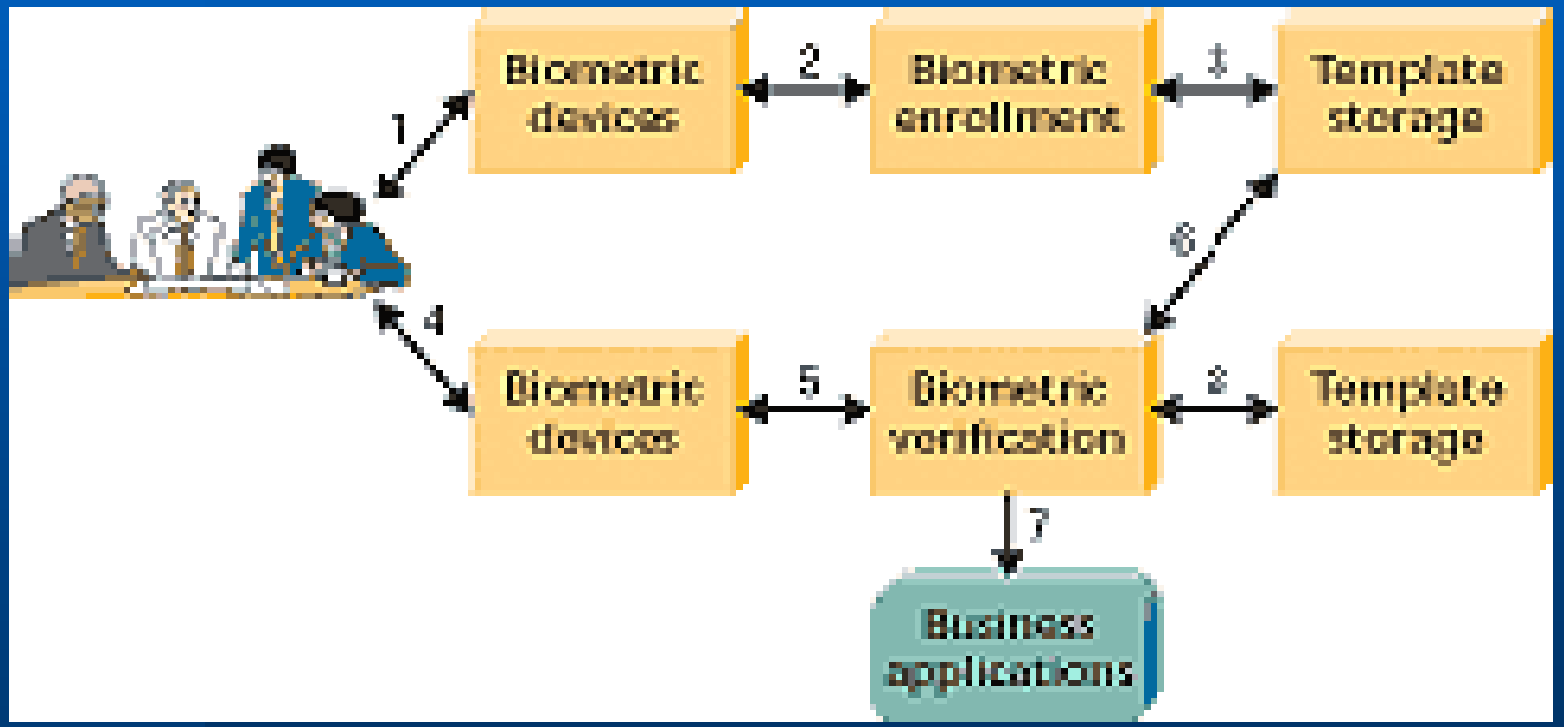
何謂生物辨識(BIOMETRICS)?

生物辨識是一種量測人體個體具有獨一鑑別性的生理或行為特徵，並以此作為身分認證(identity authentication)，常用的生理特徵有指紋、手形、掌紋、臉孔、虹膜、視網膜等生物特徵；行為特徵則有聲音、姿勢(gait)、敲鍵(Keystroke) 、簽名(signature)。

生物辨識的特色

1. ***Universality:***每個人均有擁有這些生物特徵;
2. ***Distinctiveness:*** 任意兩人的生物特徵都會呈現相當程度的差異性;
3. ***Permanence:***每個人的生物特徵在足夠長的時間中不會發生變化。
4. ***Collectability:***可以定量方式去測量這些生物特徵。

生物辨識系統的架構


Biometric devices
2
Biometric enrollment
3
Template storage
1
6
4
Biometric devices
5
Biometric verification
8
Template storage
7
Business applications

生物辨識流程

(1) Capture the chosen biometric;
(2) process the biometric and extract and enroll the biometric template;
(3) store the template in a local repository, a central repository, or a portable token such as a smart card;
(4) live-scan the chosen biometric;
(5) process the biometric and extract the biometric template;
(6) match the scanned biometric against stored templates;
(7) provide a matching score to business applications;
(8) record a secure audit trail with respect to system use.

生物辨識系統的兩種工作模式

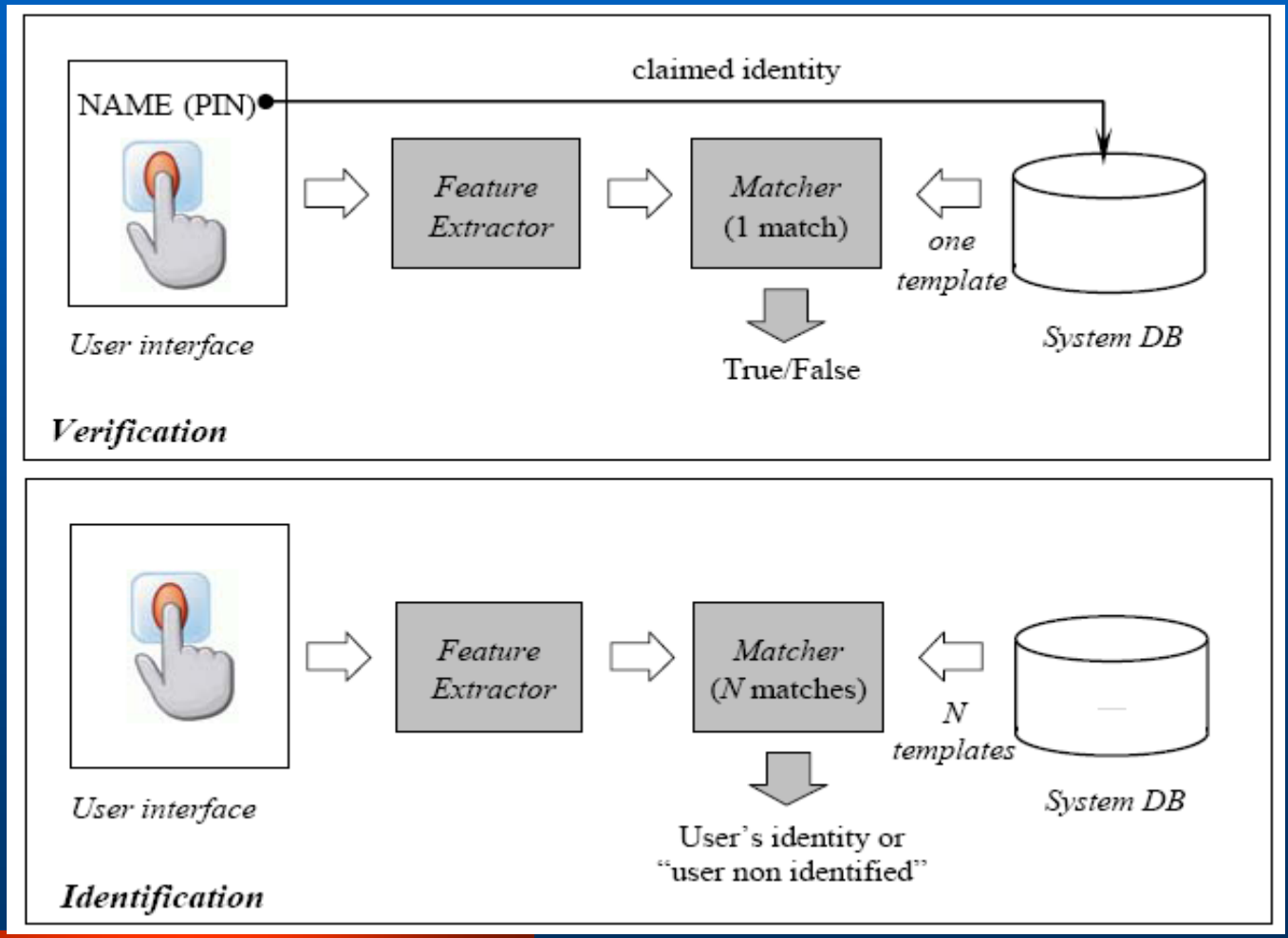
- ***verification* mode**

the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database.

- ***identification* mode**

the system recognizes an individual by searching the templates of all the users in the database for a match.

生物辨識系統的兩種工作模式



生物辨識系統的組成

- 感測器模組
- 特徵擷取模組
- 分類器模組
- 資料庫模組

指紋(Fingerprint)

A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Most emulate the traditional police method of matching minutiae; others use straight pattern-matching devices; and still others are a bit more unique, including things like moiréfringe patterns and ultrasonics. Some verification approaches can detect when a live finger is presented; some cannot.

Fingerprint verification may be a good choice for in-house systems, where you can give users adequate explanation and training, and where the system operates in a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices.

手形(Hand Geometry)

Hand geometry involves analyzing and measuring the shape of the hand. This biometric offers a good balance of performance characteristics and is relatively easy to use. It might be suitable where there are more users or where users access the system infrequently and are perhaps less disciplined in their approach to the system. Accuracy can be very high if desired, and flexible performance tuning and configuration can accommodate a wide range of applications. Organizations are using hand geometry readers in various scenarios, including time and attendance recording, where they have proved extremely popular. Ease of integration into other systems and processes, coupled with ease of use, makes hand geometry an obvious first step for many biometric projects.

掌紋(Palmprint)

The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and as a result, palmprints are expected to be even more distinctive than the fingerprints. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper. Finally, when using a high resolution palmprint scanner, all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system.

視網膜(Retina)

A retina-based biometric involves analyzing the layer of blood vessels situated at the back of the eye. An established technology, this technique involves using a low-intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if you wear glasses or are concerned about having close contact with the reading device. For these reasons, retinal scanning is not warmly accepted by all users, even though the technology itself can work well.

虹膜(Iris)

An iris-based biometric, on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil. Iris scanning, undoubtedly the less intrusive of the eye-related biometrics, uses a fairly conventional camera element and requires no close contact between the user and the reader. In addition, it has the potential for higher than average template-matching performance. Iris biometrics work with glasses in place and is one of the few devices that can work well in identification mode. Ease of use and system integration have not traditionally been strong points with iris scanning devices, but you can expect improvements in these areas as new products emerge.

臉孔(Face)

Face recognition analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. This technique has attracted considerable interest, although many people don't completely understand its capabilities. Some vendors have made extravagant claims-which are very difficult, if not impossible, to substantiate in practice-for facial recognition devices. Because facial scanning needs an extra peripheral not customarily included with basic PCs, it is more of a niche market for network authentication. However, the casino industry has capitalized on this technology to create a facial database of scam artists for quick detection by security personnel.

簽名(Signature)

Signature verification analyzes the way a user signs her name. Signing features speed, velocity, and pressure are as important as the finished signature's static shape. Signature verification enjoys a synergy with existing processes that other biometrics People are used to signatures as a means of transaction-related identity verification, most would see nothing unusual in extending this to encompass biometrics. Signature verification devices are reasonably accurate in operation and obviously lend themselves applications where a signature is an accepted identifier. Surprisingly, relatively few significant signature applications have emerged compared with other biometric methodologies. But if your application fits, it is a technology worth considering.

聲音(Voice)

Voice authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics has the most potential for growth, because it requires no new hardware-most PCs already contain a microphone. However, poor quality and ambient noise can affect verification. In addition, the enrollment procedure has often been more complicated than with other biometrics, leading to the perception that voice verification is not user friendly. Therefore, voice authentication software needs improvement. One day, voice may become an additive technology to fingerscan technology. Because many people see finger scanning as a higher authentication form, voice biometrics will most likely be relegated to replacing or enhancing PINs, passwords, or account names.

敲鍵(Keystroke)

It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometric is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe large variations in typical typing patterns. Further, the keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information.

各種生物辨識技術的比較

Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very High	Very High	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Medium	High
Required security level	High	Medium	High	Very High	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

各種生物辨識技術的比較

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H