



# Zaawansowane techniki ochrony systemów: biometria



## Wprowadzenie



### Sposoby autoryzacji i identyfikacji

- Na podstawie posiadania określonego zasobu (identyfikator, ...)
- Na podstawie znajomości ustalonej informacji (PIN,...)
- Kombinacja obydwu podejść



### Biometria

- Identyfikacja na podstawie cech osobniczych ('posiadanie' ustalonego zasobu)



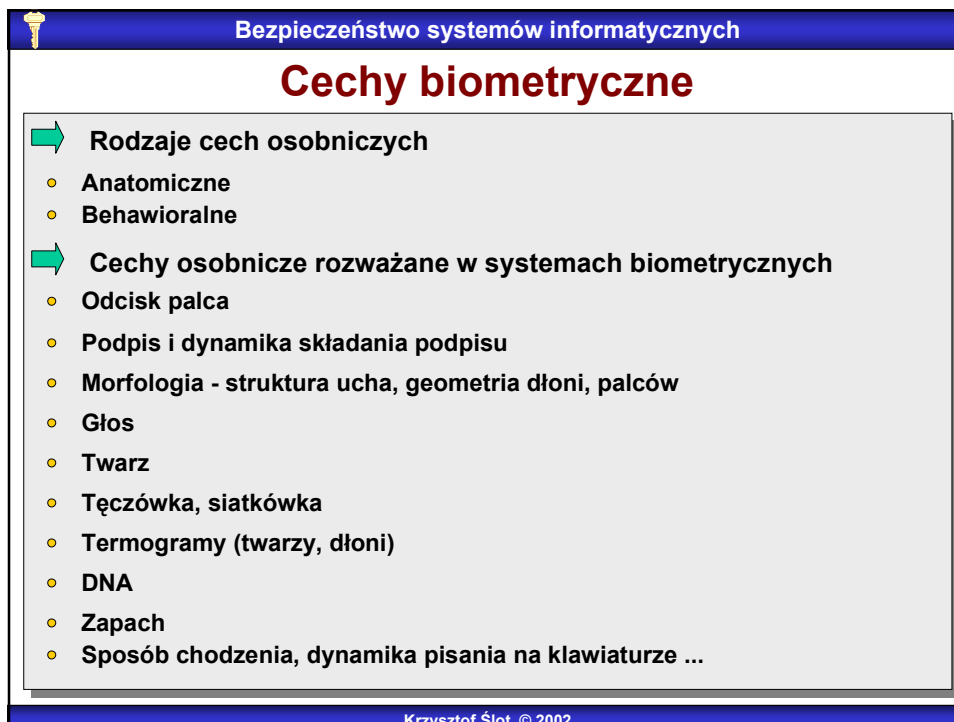
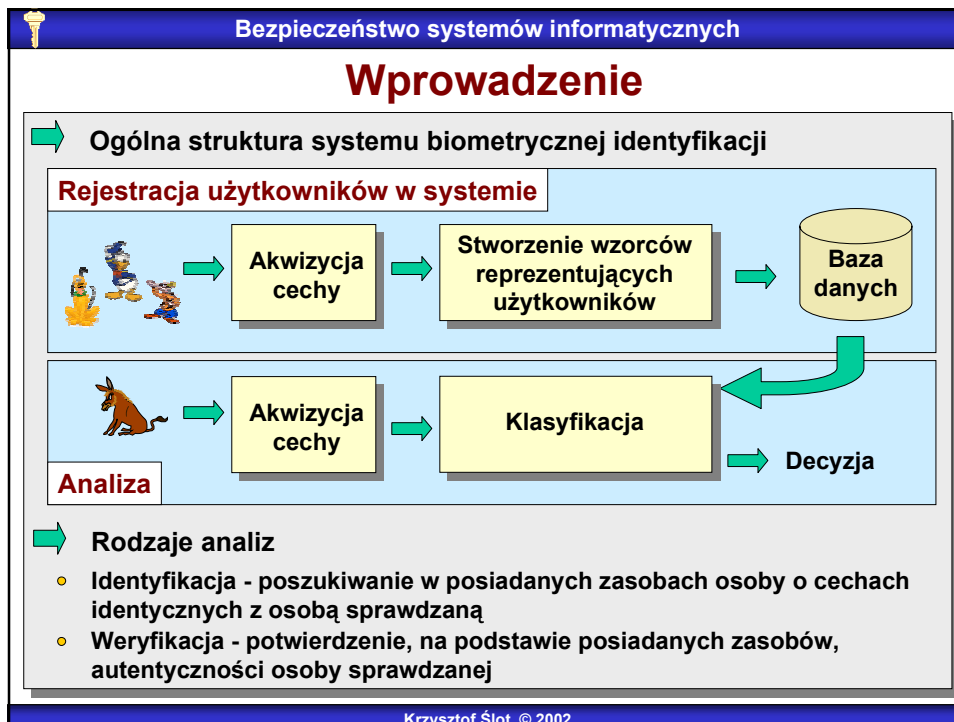
### Podstawowe wymagania na cechy służące do identyfikacji

- Unikatowość (u każdego wygląda inaczej)
- Trwałość (nie zmienia się w czasie, stanach chorobowych, emocjonalnych)
- Uniwersalność (każdy ma daną cechę)
- Możliwość pomiaru



### Dodatkowe wymagania na cechy służące do identyfikacji

- Akceptowalność pomiaru
- Łatwość analizy, dokładność, trudność dokonania oszustwa ...





## Odciski palca

### → Informacje ogólne

- Najstarsza cecha używana poświadczania autentyczności - pieczęcie na glinianych tabliczkach (Babilon (ok. 1700 p.n.e), Chiny, Rzym)
- 1901 - odciski palców zostały oficjalnie wprowadzone jako metoda kryminalistyki (Wielka Brytania)
- Unikatowość - do dnia dzisiejszego nie znaleziono dwóch osób o identycznych odciskach palców
- Trwałość - odcisk palca nie ulega zmianom na przestrzeni życia (wyjątek - niemowlęta)
- Możliwość pomiaru - szereg technik akwizycji

Fragment obrazu  
odciska palca



Krzysztof Ślot © 2002



## Odciski palca

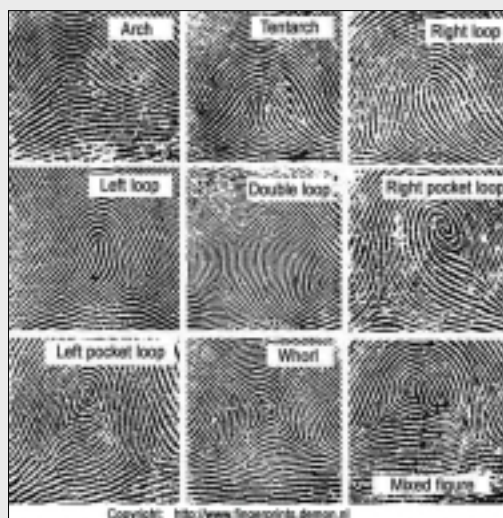
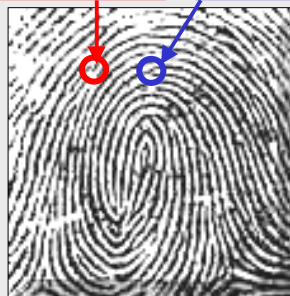
### → Klasyfikacja odcisków palców

- Kategorie wzorów →  
Służą do wstępnej klasyfikacji odcisków

- Cechy

Zakończenia

Rozdwojenia



Copyright: <http://www.fingerprints.demon.nl>

Krzysztof Ślot © 2002

Bezpieczeństwo systemów informatycznych

## Analiza odciska palca

Obraz badany







Obraz z wydzielonymi cechami

Przedmiot analizy - określenie i porównanie położenia punktów charakterystycznych

- Baza danych pamięta tylko 'minucje'
- Wystarczy 10-12 zgodności (na ok. 40) do poprawnej klasyfikacji

Krzysztof Ślot © 2002


Bezpieczeństwo systemów informatycznych

## Odcisk palca

➡ Rodzaje skanerów

- Optyczne (wady - zabrudzenie, łatwe do oszukania)
- Pojemnościowe (wady - wilgoć)
- Termiczne

➡ Tendencja do integracji skanerów z urządzeniami peryferyjnymi komputerów



Myszka z czytnikiem linii papilarnych produkcji SIEMENS-a

➡ Typowe parametry systemów identyfikacji

- Pewność działania - FAR < 1:100 000; FRR < 1:100
- Szybkość działania - rozpoznawanie (zależne od rozmiaru bazy), weryfikacja - <1 s, rejestracja w systemie - < 5s

Krzysztof Ślot © 2002



## Tęczówka

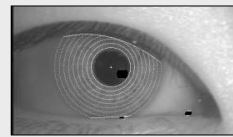
### ➡ Informacje ogólne



- Unikatowość - do dnia dzisiejszego nie znaleziono dwóch osób o identycznych wzorach tęczówki
- Trwałość - tęczówka nie ulega zmianom na przestrzeni życia
- Możliwość pomiaru - rejestracja stosunkowo prosta i akceptowalna

### ➡ Metoda rozpoznawania - tzw. IrisCode

- Podział obrazu tęczówki na zbiór koncentrycznych pierścieni
- Binaryzacja obrazu: efekt - 512 bitowy kod



Praktycznie niemożliwe powtórzenie identycznego kodu, statystyczny charakter rozpoznawania



## Siatkówka

### ➡ Cecha szczególna

- Geometria naczyń krwionośnych

### ➡ Informacje ogólne

- Unikatowość



- Trwałość - siatkówka ulega zmianom jedynie w wyniku wylewów i stanów chorobowych
- Możliwość pomiaru - rejestracja wymaga specjalizowanego sprzętu, **nie jest łatwo akceptowalna**

### ➡ Deklarowane parametry systemów

- FAR: < 1 : 1 000 000



## Twarz

### ➡ Informacje ogólne

- Unikatowość - może być trudna do rozstrzygnięcia: charakteryzacja, maski
- Zmienność (mimika, starzenie, oświetlenie, kąt widzenia, elementy kontekstowe - różne fryzury, okulary, szminka itp....)



- Możliwość pomiaru - prosta rejestracja

Krzysztof Ślot © 2002



## Twarze

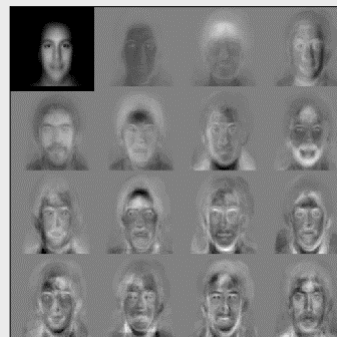
### ➡ Metody automatycznego rozpoznawania

- Metody statystyczne ('eigenfaces')

Dla zbioru twarzy, metodą analizy PCA wyznaczane są wektory bazowe nowej przestrzeni - o maksymalnych wariancjach. Wektory te stanowią tzw. twarze własne

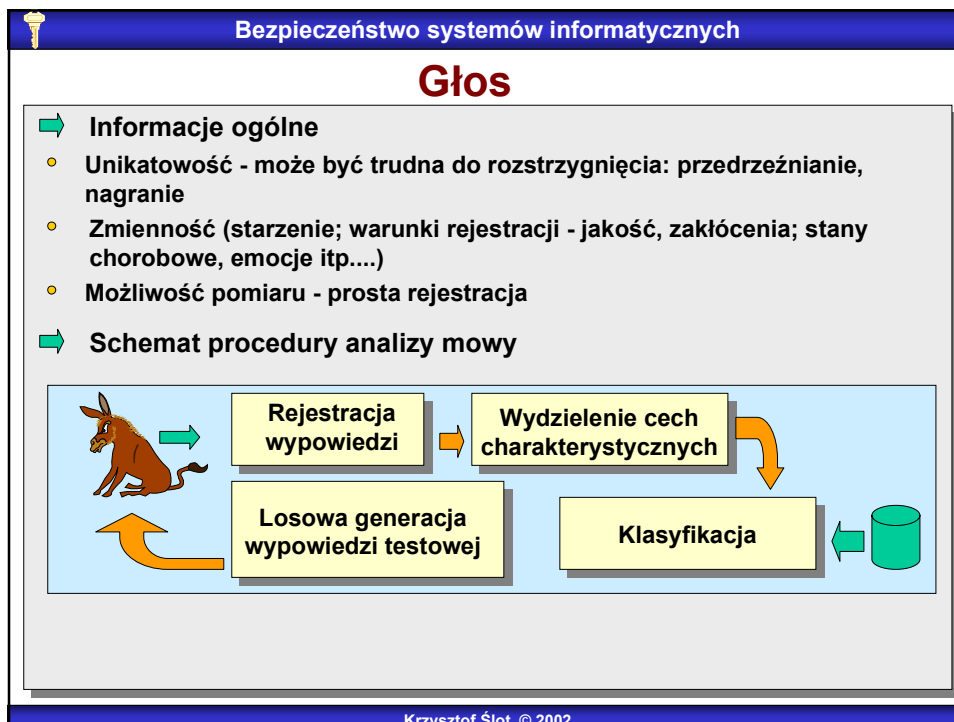
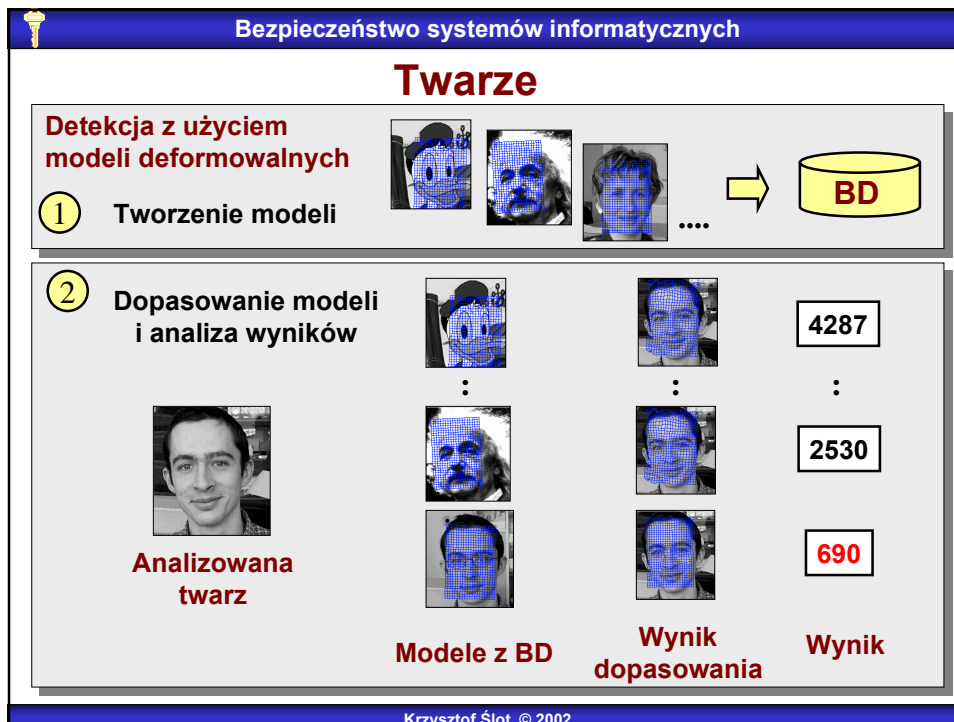
Twarze własne ➡

Rozpoznawanie to rzutowanie analizowanych obrazów na wyznaczone kierunki i procedura klasyfikacji



Źródło - MIT Media Lab

Krzysztof Ślot © 2002



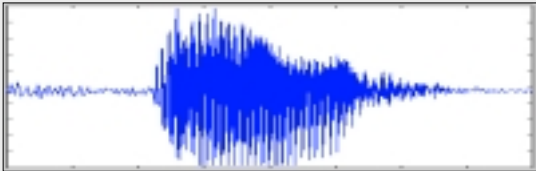



Bezpieczeństwo systemów informatycznych


## Głos

➔ Cechy wydobywane z sygnału mowy

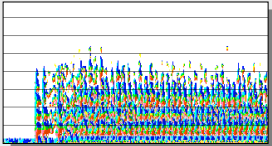
“Bat”



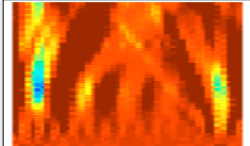




Współczynniki widmowe  
(spektrogramy)



Współczynniki DWT  
(skalogramy)



...

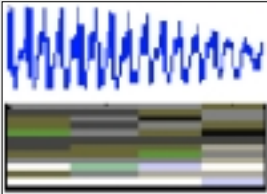
Krzysztof Ślot © 2002

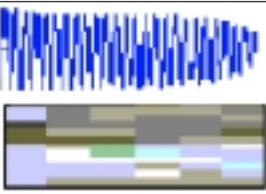
Bezpieczeństwo systemów informatycznych

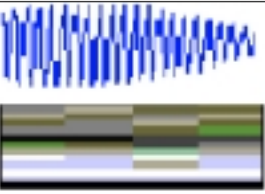
## Głos

➔ Zmienność charakteru wypowiedzianych głosek może być duża

Fragment głoski ‘a’ ze słowa ‘bat’ wypowiedziany przez różnych mówców i odpowiadające wartości współczynników LPC







Krzysztof Ślot © 2002



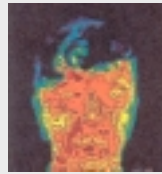
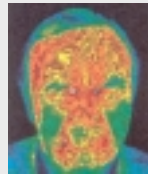
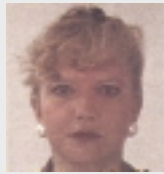


## Inne techniki biometryczne



### Detekcja obrazów termograficznych

- Podejście nowatorskie, o trudnym do określenia stopniu przydatności
- Prawdopodobnie unikatowe
- Silnie zmienne i zależne silnie od warunków rejestracji
- Dość kosztowna akwizycja (ale łatwo akceptowalna)



### DNA

- DNA osoby nie jest unikatowe (bliźniaki)
- Łatwe do 'wykradzenia' i podrzucenia
- Trudne do zaakceptowania (mnóstwo informacji dodatkowych)