Biometryczne
wspomaganie interakcji człowiek-komputer
Wprowadzenie

Bartłomiej Stasiak

bartlomiej.stasiak@p.lodz.pl
basta@ics.p.lodz.pl

Instytut Informatyki
Politechnika Łódzka

2017

Plan wykładu

1. Literatura

2. Wprowadzenie
   - Czym jest biometria
   - System biometryczny
   - Miary efektywności systemów biometrycznych
   - Przegląd metod (modalności) biometrycznych

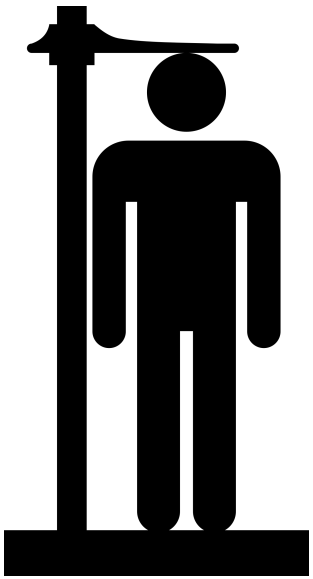
Literatura

- Anil K. Jain, Patrick Flynn, Arun Abraham Ross: *Handbook of Biometrics*, Springer (2007)
- Krzysztof Ślot: *Wybrane zagadnienia biometrii*, WKiŁ (2008)
- Krzysztof Ślot: *Rozpoznawanie biometryczne*, WKiŁ (2010)
- Homayoon Beigi: *Fundamentals of speaker recognition*, Springer (2011)
- Rafael C. Gonzalez and Richard E. Woods: *Digital Image Processing*, Prentice Hall (2007)
- Alexander Lerch: *An Introduction to Audio Content Analysis*, IEEE/Wiley (2012)
- Richard Lyons: *Wprowadzenie do Cyfrowego Przetwarzania Sygnałów*, WKiŁ (2010)

Czym jest biometria

Biometria – obszar nauki i techniki związany z dokonywaniem pomiarów cech fizycznych i behawioralnych użytkownika na potrzeby identyfikacji i weryfikacji tożsamości.
Metody biometryczne rozumiane szerzej w kontekście *badania zmienności populacji organizmów* znajdują także zastosowanie m.in. w:

- medycynie
- kryminalistyce
- antropologii
- fizjologii
- genetyce
- hodowli
- paleontologii
- ...



Czym jest biometria

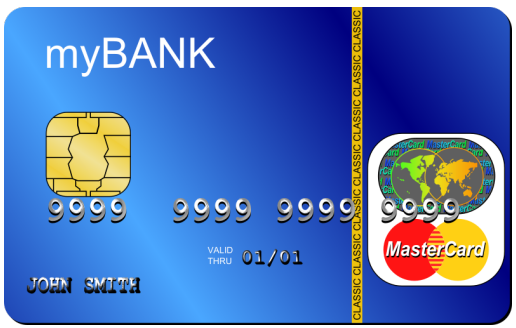
Jednym z nowszych zastosowań metod biometrycznych jest również wspomaganie interakcji człowiek-komputer (ang. *Human-Computer Interaction*, HCI)
Poza typowymi zastosowaniami (uwierzytelnianie, logowanie, etc.) metody biometryczne mogą być używane do rozszerzania możliwości interfejsu użytkownika i projektowania interakcji w zakresie m.in.:

- rozpoznawania płci użytkownika,
- rozpoznawania emocji w głosie,
- rozpoznawania nastroju na podstawie obrazu twarzy
- ...

Uwierzytelnianie (ang. *authentication*)

Podstawowy podział funkcjonalny metod uwierzytelniania

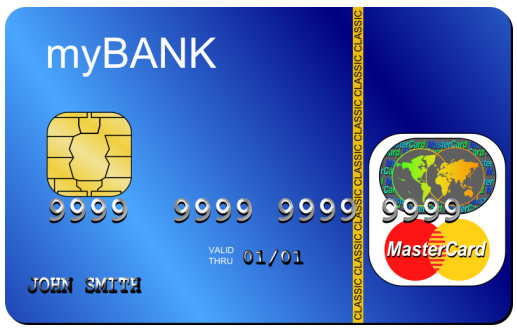
- Coś co masz
  (ang. *something you have*, SYH)



Uwierzytelnianie (ang. *authentication*)

Podstawowy podział funkcjonalny metod uwierzytelniania

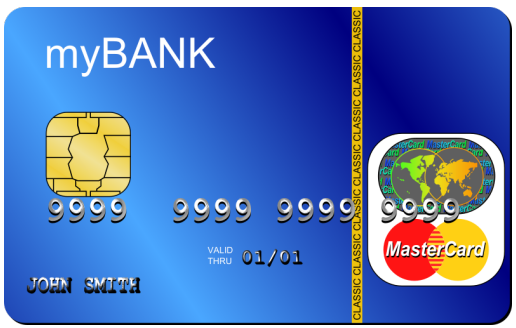
- Coś co masz
  (ang. *something you have*, SYH)
- Coś co wiesz
  (ang. *something you know*, SYK)



Uwierzytelnianie (ang. *authentication*)

Podstawowy podział funkcjonalny metod uwierzytelniania

- Coś co masz
  (ang. *something you have*, SYH)
- Coś co wiesz
  (ang. *something you know*, SYK)
- Coś czym jesteś
  (ang. *something you are*, SYA)



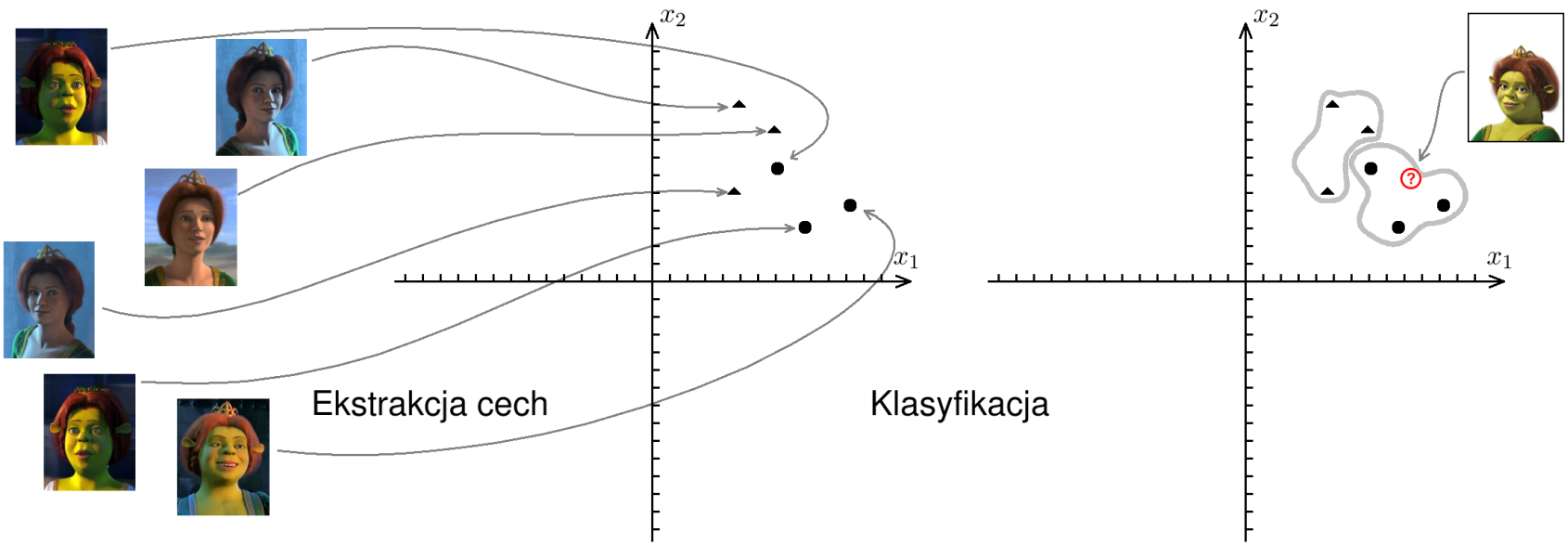
Uwierzytelnianie (ang. *authentication*)

Uwierzytelnianie biometryczne – właściwości:

- Brak konieczności użycia klucza/karty, etc. które mogłyby zostać zgubione/skradzione oraz hasła, które mogłoby zostać zapomniane/podsłuchane
- Możliwość jednoznacznego potwierdzenia, że użytkownik jest zapisany w systemie, nawet jeśli on sam temu zaprzecza (ang. *negative recognition*)
- Możliwość jednoznacznego potwierdzenia, że użytkownik korzystał z systemu (niezaprzeczalność, ang. *non-repudiation*)
- Brak możliwości łatwej zmiany cech biometrycznych (tak jak się zmienia hasło, czy wymienia zamki)
- Możliwość wystąpienia zmian cech biometrycznych na skutek czynników biologicznych (choroby, urazy, starzenie)

System biometryczny

- System biometryczny jest przykładem specjalizowanego systemu rozpoznawania wzorców (ang. *pattern recognition*)
- Podstawowe zadania systemu biometrycznego, to:
  - Ekstrakcja cech z danych biometrycznych użytkowników
  - Klasyfikacja nowych danych i podejmowanie decyzji



Funkcje decyzyjne

Niech K oznacza liczbę klas $(c_1, c_2, ..., c_K)$ w pewnym problemie, w którym klasyfikacji poddawane są wzorce (wektory) d-wymiarowe. Zadanie klasyfikacji sprowadza się do znalezienia K *funkcji decyzyjnych* $d_1(\mathbf{x}), d_2(\mathbf{x}), ..., d_K(\mathbf{x})$ takich, że dla dowolnego wektora $\mathbf{x} = (x_1, x_2, ..., x_d)$ należącego do klasy c_i zachodzi:

$$d_i(\mathbf{x}) > d_j(\mathbf{x}); \text{dla } j \neq i$$

Granica decyzyjna separująca klasy c_i i c_j to zbiór wszystkich punktów $\mathbf{x}$, dla których $d_i(\mathbf{x}) = d_j(\mathbf{x})$, czyli równoważnie:

$$d_i(\mathbf{x}) - d_j(\mathbf{x}) = 0$$

Klasyfikator minimalnoodległościowy

Załóżmy, że każda klasa reprezentowana jest przez pojedynczy wektor (prototyp, modę), będący np. średnią wszystkich wektorów z tej klasy:

$$\mathbf{m}_j = \frac{1}{N_j} \sum_{\mathbf{x} \in c_j} \mathbf{x}_j \ ; \ \text{dla } j = 1, 2, ..., K$$

gdzie N_j jest liczbą obiektów w klasie c_j. Przynależność nieznanego wektora $\mathbf{x}$ do klasy c_j określamy licząc odległość (np. euklidesową):

$$\rho_j(\mathbf{x}) = ||\mathbf{x} - \mathbf{m}_j|| \ ; \ \text{dla } j = 1, 2, ..., K$$

i wybierając klasę, dla której wartość ρ_j jest najmniejsza.

Funkcja decyzyjna

Funkcja decyzyjna będzie w tym wypadku miała postać:

$$d_j(\mathbf{x}) = \mathbf{x}^T \mathbf{m}_j - \frac{1}{2}\mathbf{m}_j^T \mathbf{m}_j$$

a granica decyzyjna:

$$d_i(\mathbf{x}) - d_j(\mathbf{x}) = \mathbf{x}^T(\mathbf{m}_i - \mathbf{m}_j) - \frac{1}{2}(\mathbf{m}_i - \mathbf{m}_j)^T(\mathbf{m}_i + \mathbf{m}_j) = 0$$

stanowi hiperpłaszczyznę prostopadłą do odcinka łączącego $\mathbf{m}_i$ z $\mathbf{m}_j$, przechodzącą przez jego środek.

Określanie odległości

- W metodach minimalnoodległościowych określenie przynależności wektora do danej klasy związane jest z pojęciem *odległości* w przestrzeni cech X
- Do mierzenia odległości pomiędzy elementami $\boldsymbol{u}$ i $\boldsymbol{v}$ (punktami, wektorami) przestrzeni X definiuje się funkcję dwuargumentową ρ o wartościach nieujemnych, zwaną *metryką*, spełniającą warunki:
  - $\rho(u, v) = 0 \iff u = v$
  - $\rho(u, v) = \rho(v, u)$
  - $\rho(u, v) \leqslant \rho(u, z) + \rho(z, v)$
- Przestrzeń X z określoną metryką nazywamy *przestrzenią metryczną*

Określanie odległości

- Przykłady metryk
  - Metryka euklidesowa

$$\rho(\boldsymbol{u}, \boldsymbol{v}) = ||\boldsymbol{u} - \boldsymbol{v}|| = \sqrt{\sum_{n=1}^{N} (u_n - v_n)^2}$$

  - Metryka uliczna (taksówkowa)

$$\rho(\boldsymbol{u}, \boldsymbol{v}) = \sum_{n=1}^{N} |u_n - v_n|$$

  - Metryka Czebyszewa

$$\rho(\boldsymbol{u}, \boldsymbol{v}) = \max_{n} |u_n - v_n|$$

  - Metryka Minkowskiego

$$\rho(\boldsymbol{u}, \boldsymbol{v}) = L_m(\boldsymbol{u}, \boldsymbol{v}) = \left(\sum_{n=1}^{N} |u_n - v_n|^m \right)^{\frac{1}{m}}$$

System biometryczny

Budowa

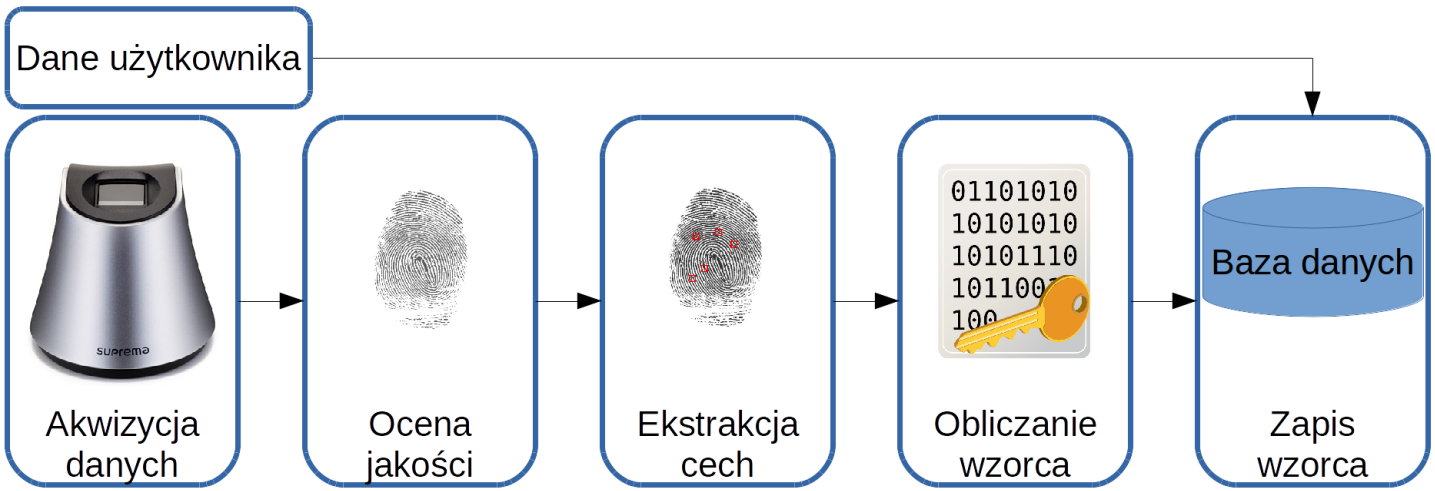
- Moduł akwizycji (czujnik, skaner)
- Moduł oceny jakości i ekstrakcji cech
- Moduł porównujący wzorce i blok decyzyjny
- Moduł bazodanowy

Funkcjonalność

- Zapisywanie nowych użytkowników (ang. *enrollment*)
- Uwierzytelnianie (autentykacja)
  - Weryfikacja
  - Identyfikacja
- Autoryzacja

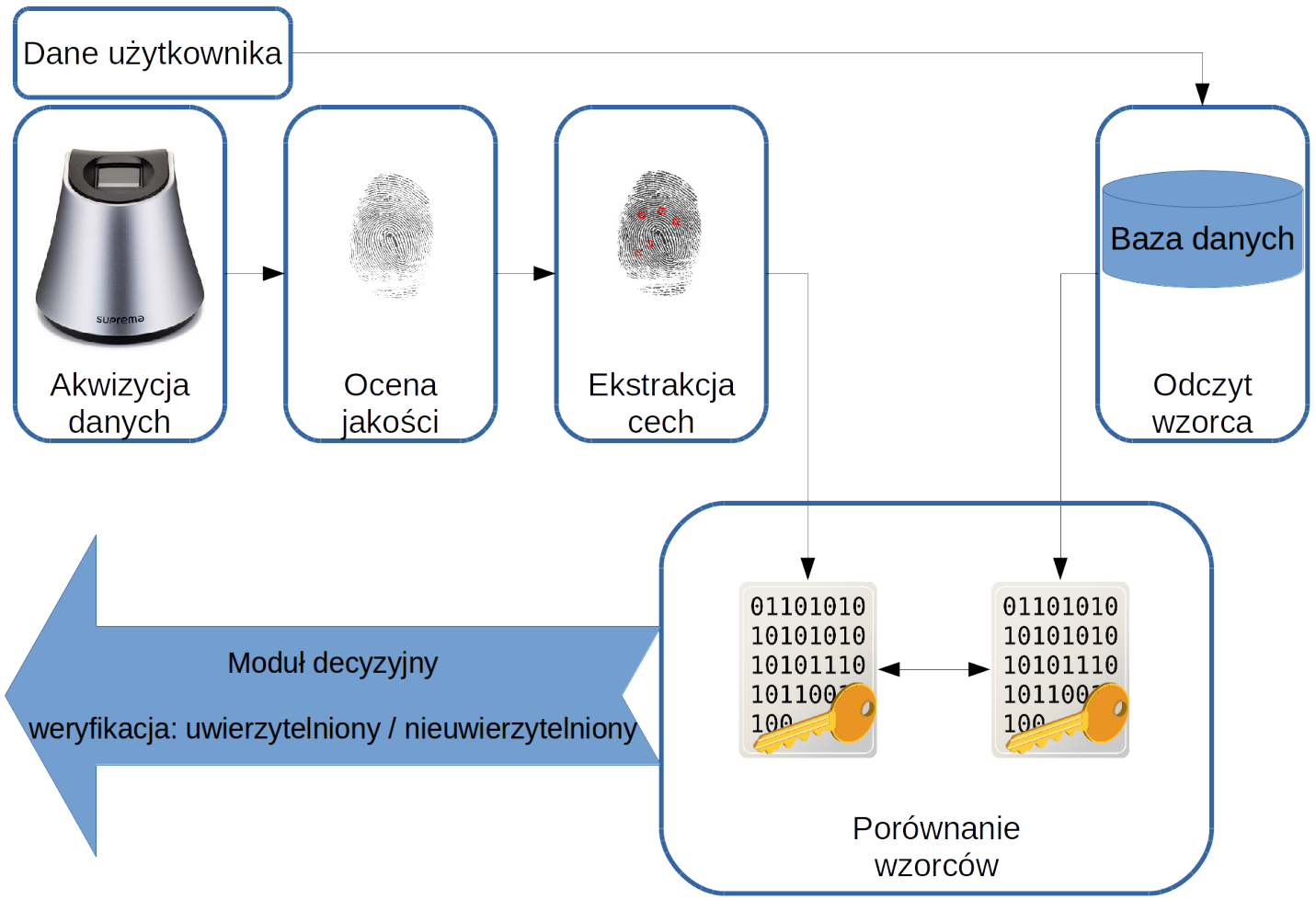
System biometryczny – funkcjonalność

Zapisywanie nowego użytkownika (ang. *enrollment*)



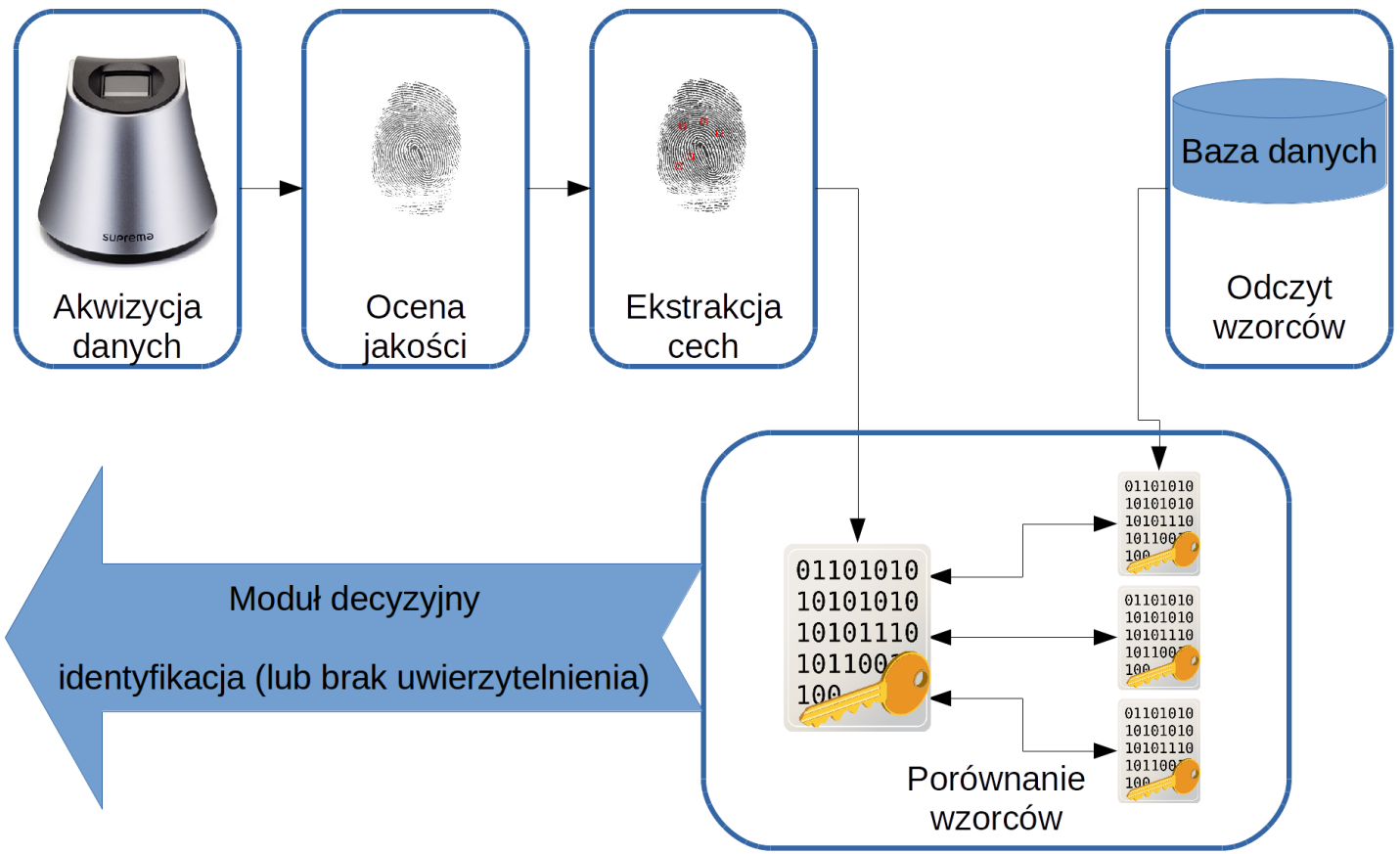
System biometryczny – funkcjonalność

Weryfikacja użytkownika (jeden-do-jednego)



System biometryczny – funkcjonalność

Identyfikacja użytkownika (jeden-do-wielu)



Miary efektywności systemów biometrycznych

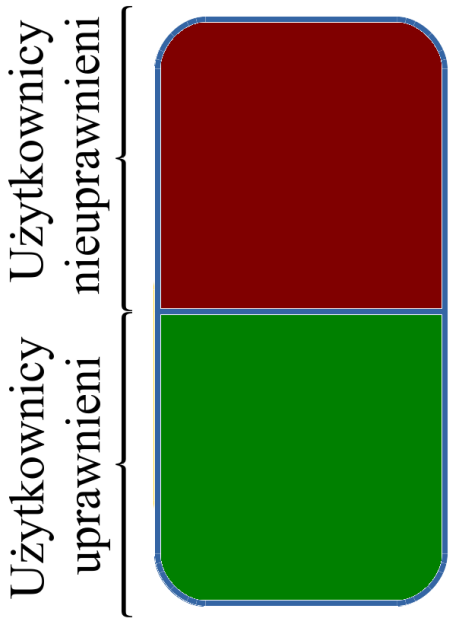
- W przeciwieństwie do haseł alfanumerycznych, które łatwo jednoznacznie zweryfikować, porównanie cech biometrycznych z wzorcem z bazy danych jest zawsze obarczone pewną niepewnością
- Cechy tej samej osoby zmieniają się w każdej kolejnej akwizycji (zmienność wewnątrzklasowa, ang. *intra-class variation*), m.in. z uwagi na:
  - Zmienne warunki akwizycji: oświetlenie, pozycja względem czytnika (odległość i orientacja), okluzje, zakłócenia zewnętrzne, etc.
  - Zmienny stan psychofizyczny i emocjonalny użytkownika
- Uzyskanie identycznego zestawu cech w kolejnej akwizycji jest tak wysoce nieprawdopodobne, że często sugeruje próbę oszustwa (ang. *replay attack*)

Miary efektywności systemów biometrycznych

- Użyteczny zestaw cech biometrycznych charakteryzuje się niską zmiennością wewnątrzklasową, ang. *intra-class variation* i wysoką zmiennością pomiędzy różnymi użytkownikami (ang. *inter-class variation*).
- Istotnym parametrem systemu biometrycznego jest próg określający jak bardzo podobne muszą być dwa wzorce, aby uznać je za pochodzące od tej samej osoby
- Wartość progu bezpośrednio wpływa na podstawowe współczynniki określające efektywność systemu:
  - FAR (ang. *False Acceptance Rate*) – procent udanych prób uwierzytelnienia użytkowników nieuprawnionych
  - FRR (ang. *False Reject Rate*) – procent nieudanych prób uwierzytelnienia użytkowników uprawnionych

Miary efektywności systemów biometrycznych

Współczynniki FAR i FRR – ilustracja:



Miary efektywności systemów biometrycznych

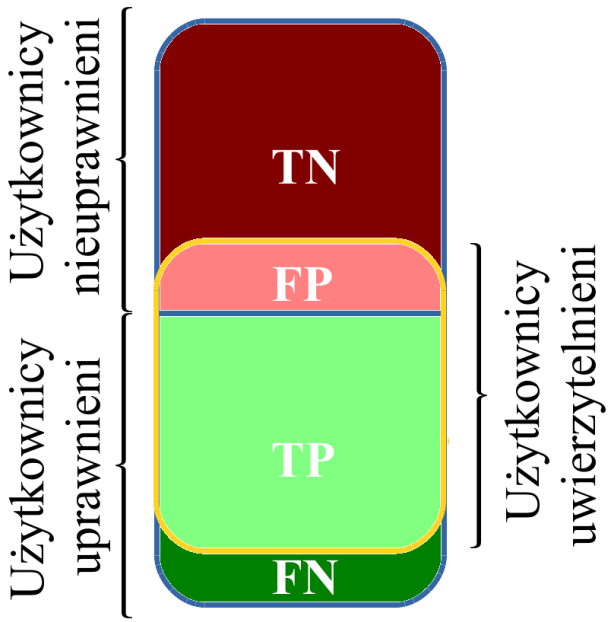
Współczynniki FAR i FRR – ilustracja:

- FAR (inaczej: FPR, ang. *False Positive Rate*, albo *fall-out*):

$$FAR = \frac{FP}{FP + TN} = \frac{FP}{N}$$

- FRR (inaczej: FNR, ang. *False Negative Rate*, albo *miss rate*):

$$FRR = \frac{FN}{FN + TP} = \frac{FN}{P}$$

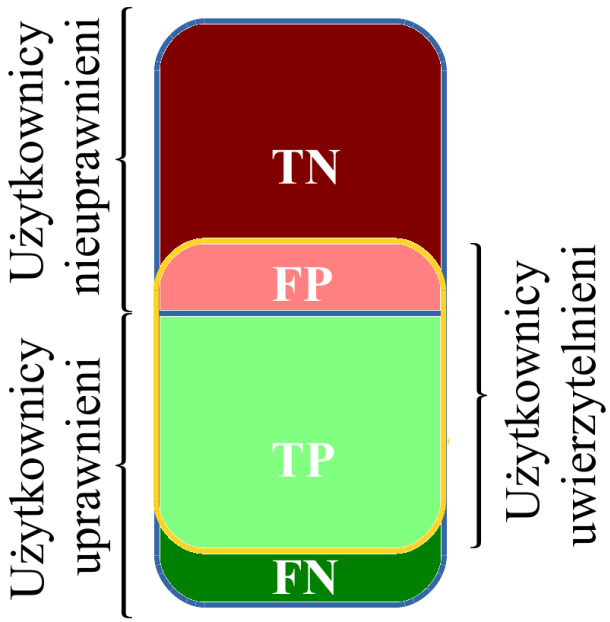


Miary efektywności systemów biometrycznych

Współczynniki FAR i FRR – ilustracja:

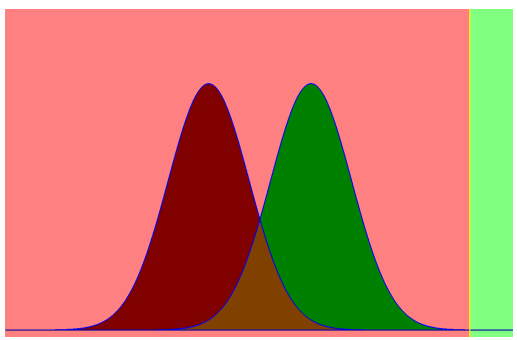
- GAR (ang. *Genuine Accept Rate*, inaczej: czułość, TPR, ang. *True Positive Rate*, albo *recall*):

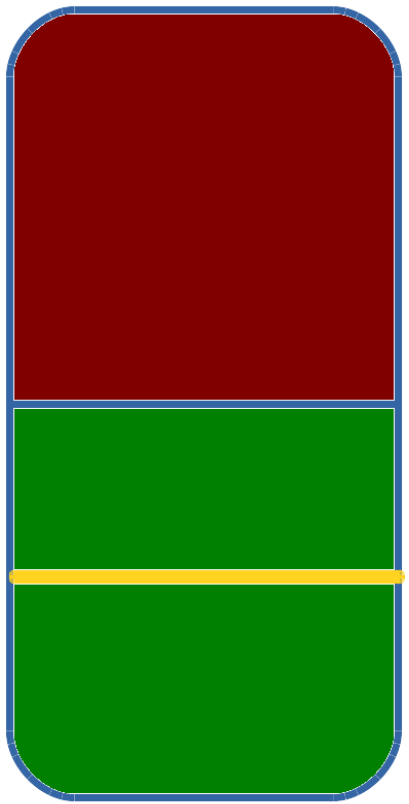
$$GAR = \frac{TP}{TP + FN} = \frac{TP}{P}$$



Miary efektywności systemów biometrycznych

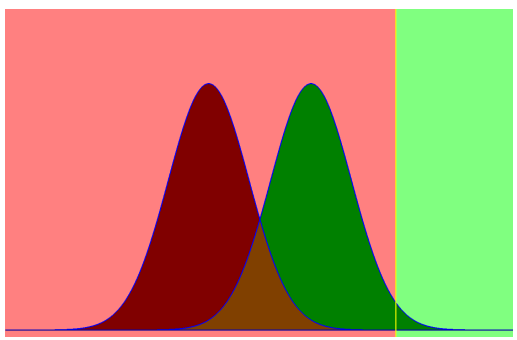
- Do oceny efektywności systemu można posłużyć się krzywą ROC (ang. *Receiver Operating Characteristic*), obrazującej zależność współczynnika GAR od FAR dla wszystkich możliwych wartości progu

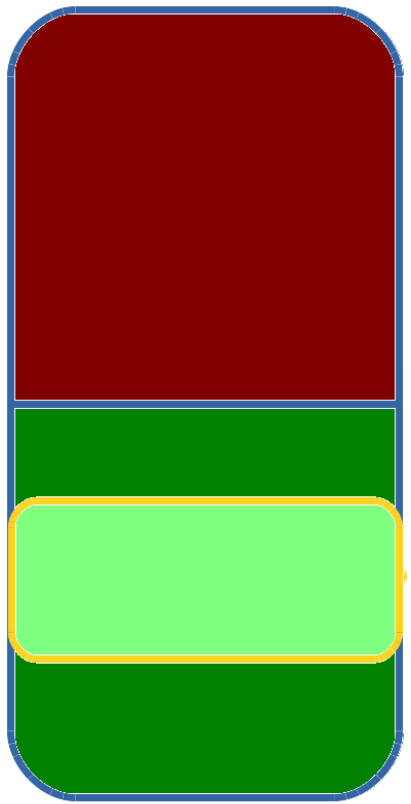




Miary efektywności systemów biometrycznych

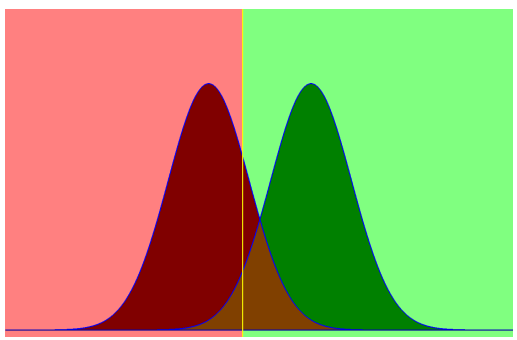
- Do oceny efektywności systemu można posłużyć się krzywą ROC (ang. *Receiver Operating Characteristic*), obrazującej zależność współczynnika GAR od FAR dla wszystkich możliwych wartości progu

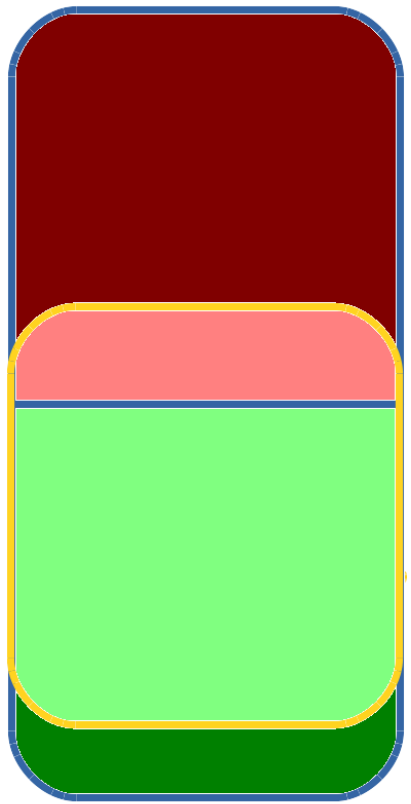




Miary efektywności systemów biometrycznych

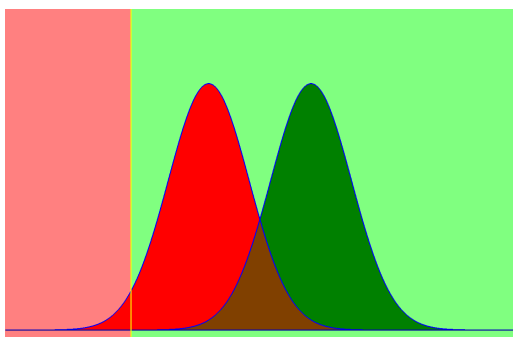
- Do oceny efektywności systemu można posłużyć się krzywą ROC (ang. *Receiver Operating Characteristic*), obrazującej zależność współczynnika GAR od FAR dla wszystkich możliwych wartości progu

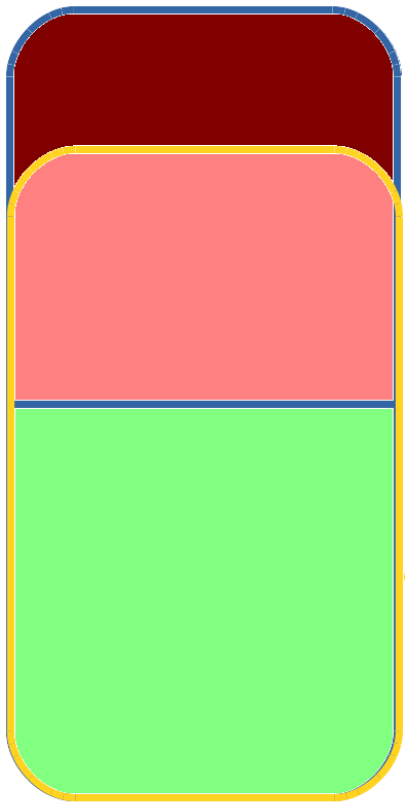




Miary efektywności systemów biometrycznych

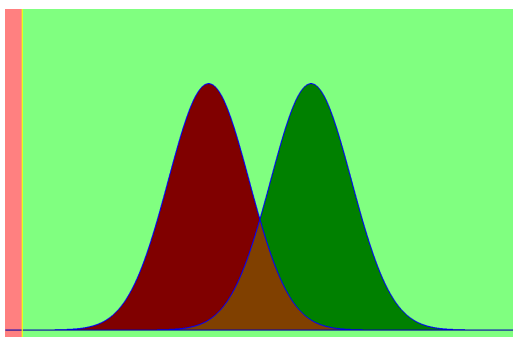
- Do oceny efektywności systemu można posłużyć się krzywą ROC (ang. *Receiver Operating Characteristic*), obrazującej zależność współczynnika GAR od FAR dla wszystkich możliwych wartości progu

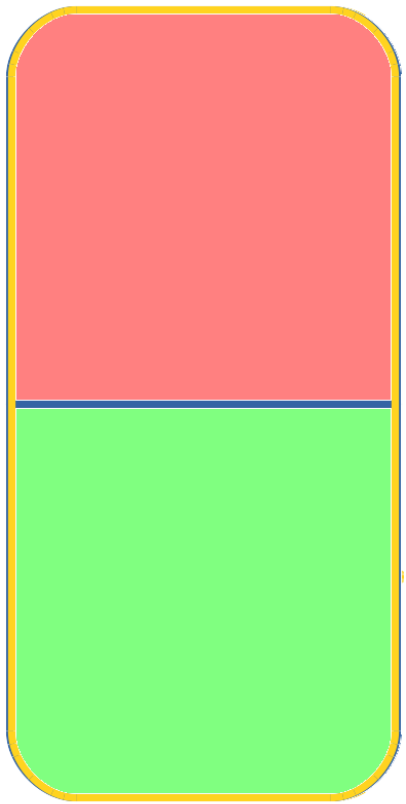




Miary efektywności systemów biometrycznych

- Do oceny efektywności systemu można posłużyć się krzywą ROC (ang. *Receiver Operating Characteristic*), obrazującej zależność współczynnika GAR od FAR dla wszystkich możliwych wartości progu





Przegląd metod (modalności) biometrycznych

Podstawowe własności cech biometrycznych

- Uniwersalność
- Unikalność
- Trwałość
- Mierzalność, łatwość akwizycji
- Akceptowalność społeczna
- Odporność na fałszerstwa
- Efektywność i wydajność przetwarzania

Przegląd metod (modalności) biometrycznych

- Twarz
  - Cechy ekstrahowane na podstawie:
    - punktów charakterystycznych (oczy, brwi, nos, usta, podbródek), ich przestrzennych relacji i kształtu
    - rozkładu obrazu twarzy na składowe główne (*eigenfaces*) z wykorzystaniem metody PCA (ang. *Principal Component Analysis*)
  - Wysoka akceptowalność i uniwersalność
  - Łatwość akwizycji, również bez wiedzy użytkownika
  - Problem z unikalnością i trwałością (różne warunki akwizycji, oświetlenie, pozycja względem kamery, niejednorodne tło, zmienny wyraz twarzy, fryzura, zarost, okulary, i in.)

Przegląd metod (modalności) biometrycznych

- Odcisk palca
  - Analiza wzoru linii papilarnych i minucji (ang. *minutiae*)
  - Wysoka unikalność
  - Akceptowalność mniejsza niż w przypadku twarzy
  - Konieczność użycia specjalnego skanera i bezpośredniego kontaktu z użytkownikiem
  - Uniwersalność wysoka, choć w pewnej części populacji mogą wystąpić problemy związane m.in. z:
    - wykonywaną pracą fizyczną
    - czynnikami genetycznymi
    - urazami

Przegląd metod (modalności) biometrycznych

- Tęczówka
  - Bardzo wysoka unikalność, trwałość i uniwersalność
  - Łatwość akwizycji, również bez wiedzy użytkownika (choć nie tak łatwa jak w przypadku twarzy)

Przegląd metod (modalności) biometrycznych

- Głos
  - Połączenie charakterystyk anatomicznych i behawioralnych
  - Łatwość akwizycji, również bez wiedzy użytkownika
  - Możliwość akwizycji zdalnej (np. przez linię telefoniczną)
  - Wysoka akceptowalność
  - Umiarkowana unikalność i trwałość
  - Możliwość użycia w schemacie rozpoznawania:
    - zależnego od tekstu
    - niezależnego od tekstu

Przegląd metod (modalności) biometrycznych

- Podpis odręczny
  - Cecha behawioralna
  - Bardzo wysoka akceptowalność
  - Niewielka unikalność i odporność na fałszerstwa
  - Możliwość poprawy unikalności poprzez zastosowanie specjalnego urządzenia wejściowego (tablet)

Przegląd metod (modalności) biometrycznych

- Analiza chodu (ang. *gait recognition*)
  - Cecha behawioralna
  - Wymaga opracowania odpowiedniego modelu (sylwetka/kontur, model 3-D)
  - Możliwość analizy z dużej odległości
  - Niewielka unikalność
  - Zależność od rodzaju ubrania, butów, wrażliwość na schorzenia narządu ruchu

Przegląd metod (modalności) biometrycznych

- Inne modalności biometryczne
  - Siatkówka
  - Geometria dłoni
  - Odcisk dłoni
  - Kształt ucha
  - Układ naczyń krwionośnych dłoni
  - Układ naczyń krwionośnych palca
  - Sposób pisania na klawiaturze
  - Analiza potencjałów wywołanych (ERP, ang. *event-related potentials*, fala P300)
  - Analiza termograficzna (np. twarzy)
  - Zapach
  - Analiza DNA

Dziękuję za uwagę