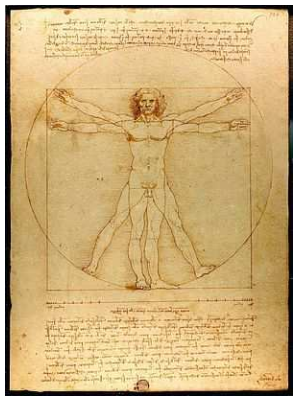
2: Zadania i metody biometrii



2.1: Biometria a rozpoznawanie tożsamości

Biometria: definicje

Biometria (biometrics): (gr. bios - życie, metron - pomiar)

biometria (ang. *biometrics*)

- wg *The American Heritage® Dictionary of the English Language, Fifth Edition ©Houghton Mifflin Harcourt Publishing Company*
  1. Analiza statystyczna zjawisk biologicznych
  2. **Pomiary charakterystyk fizycznych takich jak odciski palców, DNA lub wzory siatkówki do stosowania w weryfikacji tożsamości osób**
- wg. *Merriam-Webster Dictionary 2014*
  1. *biometry*; analiza statyczna obserwacji i zjawisk biologicznych
  2. **pomiar i analiza niepowtarzalnych charakterystyk fizycznych lub behawioralnych (jak odciski palców czy charakterystyka głosu), szczególnie jako środek weryfikacji tożsamości**
- wg *Dictionary.com Unabridged. Random House, Inc.*
  1. biostatystyka
  2. *biometry*; obliczenia prawdopodobnego czasu trwania ludzkiego życia
  3. **proces w którym niepowtarzalne cechy osób - fizyczne lub inne - są wykrywane i rejestrowane elektronicznie w celu potwierdzania tożsamości**

Biometria: nasza definicja

Biometria

Zautomatyzowane wykorzystanie pomiarów cech anatomicznych lub cech zachowania człowieka do rozpoznania jego tożsamości

Biometria: analiza definicji (1)

"cechy anatomiczne lub cechy zachowania"

Zautomatyzowane wykorzystanie pomiarów **cech anatomicznych lub cech zachowania** człowieka do rozpoznania jego tożsamości

Rozpoznawanie biometryczne wykorzystuje

- *cechy człowieka* (*"jacy jesteśmy"*)
  - *cechy anatomiczne* (cechy fizjologiczne, cechy statyczne)
  - *cechy zachowania* (cechy behawioralne, cechy dynamiczne)
- nie: wiedzę człowieka (ang. *knowledge-based*) ("coś, co wiemy": hasło, PIN)
- nie: posiadane tokeny (ang. *token-based*) ("coś, co mamy": klucz, karta ID)

Biometria: analiza definicji (2)

"rozpoznawanie tożsamości"

Zautomatyzowane wykorzystanie pomiarów cech anatomicznych lub cech zachowania człowieka do **rozpoznania jego tożsamości**

- tożsamość (ang. *identity*): bycie określoną osobą (nie chodzi o tożsamość w sensie psychologicznym)
- zagadnienia rozpoznawania tożsamości (ang. *identity recognition*)
  - *weryfikacja* (ang. *verification*), rozpoznawanie 1:1 – *potwierdzenie tożsamości*; sprawdzenie, czy osoba jest tą, za którą się podaje (obraz vs. wzorzec biometryczny)
  - *identyfikacja* (ang. *identification*), rozpoznawanie 1:N – *ustalenie tożsamości*, sprawdzenie, czy osoba została wcześniej zarejestrowana w bazie danych (obraz vs. baza wzorców biometrycznych)
  - *identyfikacja negatywna* – stwierdzenie, czy badana osoba *nie jest* zarejestrowana w bazie danych
  - *ślepa identyfikacja* (ang. *blind identification*) – sprawdzenie, czy podmiot jest w bazie danych bez ujawniania tożsamości (przykład: prawo do głosowania)

Biometria: analiza definicji (3)

"zautomatyzowane"

Zautomatyzowane wykorzystanie pomiarów cech anatomicznych lub cech zachowania człowieka do rozpoznania jego tożsamości

- stopień "automatyzacji"
  - wspomaganie eksperta

    system 'przesiewa' osoby, ekspert zajmuje się tylko wybranymi przypadkami (ochrona lotnisk; system AFIS)
  - systemy nadzorowane

    przeszkolony personel daje wskazówki i zapobiega nadużyciom
  - systemy autonomiczne / zdalne rozpoznawanie

    systemy bez nadzoru
- metodologia biometryczna może/powinna wykorzystywać doświadczenie eksperta
- możliwość braku nadzoru, szybkość przetwarzania

Biometria: analiza definicji (4)

"pomiary cech człowieka"

Zautomatyzowane wykorzystanie pomiarów cech anatomicznych lub cech zachowania człowieka do rozpoznania jego tożsamości

- potrzebna pewność, że badane i porównywane są cechy człowieka: detekcja żywotności

Człowiek jako beneficjent biometrii

Czy beneficjent ?

- akceptacja celów pomiaru - przykłady testów (A. Krupp, C. Rathgeb and C.Busch. Social Acceptance of Biometric Technologies in Germany: A Survey)
  - UK 2000 (175 osób): preferencja hasła nad biometrią
  - USA 2006 (300 osób): ok 1/2 z 300 uczestników akceptuje zastosowania biometrii do paszportów, 1/3 do kart kredytowych
  - UK 2006 (154 osób): 40% uczestników wątpi w zachowanie poufności danych
  - Kanada 2007 (24 osoby): prawie wszyscy lepiej oceniają użycie odcisków niż hasła; większość (60%) z powodu wygody, mniejszość ze względu na bezpieczeństwo
  - USA 2007 (uniwersytet w płd-wsch. USA, 115 osób) większość wątpi w bezpieczeństwo danych
  - Chiny 2012 (305 osób): preferowane odciski, tęczówka, twarz; zastosowania: lotniska, banki
  - Niemcy 2013 (140 osób): mniej niż 1/2 uczestników znających systemy biometryczne sądzi że są mniej wygodne od podejść opartych na wiedzy

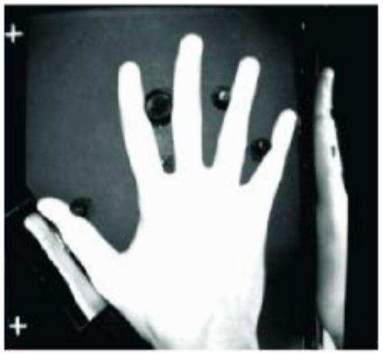
Człowiek jako beneficjent biometrii

Obawy przed stosowaniem biometrii

- obawa przed brakiem ochrony danych osobowych
  - dane biometryczne są danymi osobowymi (Polska: Ustawa o ochronie danych osobowych z 29 sierpnia 1997)
  - ale: "informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań"
  - biometria może być uważana za ingerencje w dane osobowe niewspółmierne do celów (np. rejestracja czasu pracy)
- możliwość gromadzenia informacji w centralnych bazach danych i kradzieży tożsamości
- obawy przed dostępem do informacji o chorobach (podpis, tęczówka ?, linie dłoni ??), podglądanie osobowości
- syndrom "wielkiego brata": możliwość gromadzenia danych bez zgody i wiedzy osoby obserwowanej,
- podejmowanie ważnych decyzji przez maszynę (ang. *ubiquitous computing*)
- metody biometryczne potęgują nierówności etniczne, rasowe, związane z płcią, wiekiem etc (http://www.timeshighereducation.co.uk/420116.article na podst. S.A. Magnet "When biometrics fail: Gender, race and the technology of identity", Duke Univ. Press 2012)

Modalności biometryczne

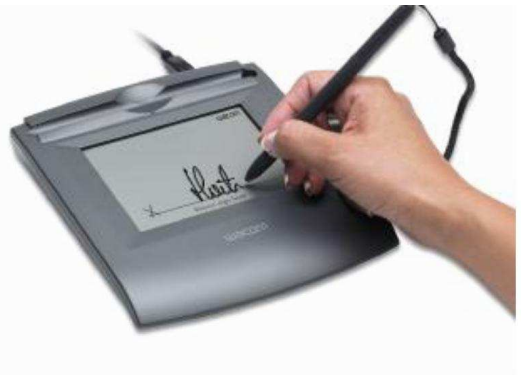
kształt dłoni



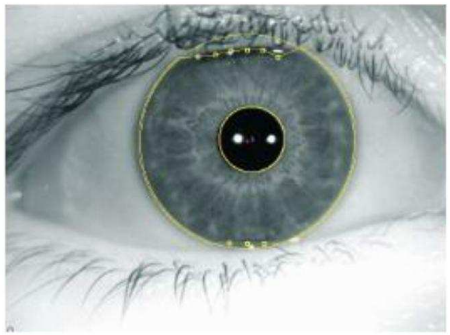
naczynia palca / dłoni

odcisk palca

podpis on-line



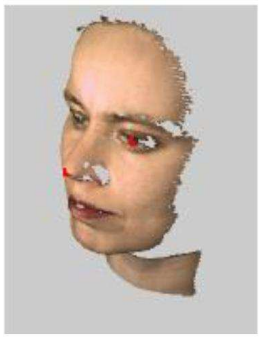
termogram



podpis off-line

wzór tęczówki

obraz twarzy



twarz 3D

EEG

chód – *mowa* – DNA – *rytm klawiatury* – kształt ucha – obraz siatkówki

Pożądane atrybuty modalności biometrycznych

Odpowiednio wysoki stopień różnicowania

- potrzebna jak najmniejsza zmienność "wewnątrzosobnicza"
- potrzebna jak największa zmienność "międzyosobnicza"
- *penetracja genetyczna*: wpływ genotypu na modalność
  - DNA, geometria dłoni, geometria twarzy ⋆ ⋆ ⋆
  - podpis odręczny, odcisk palca ⋆ ⋆
  - tęczówka ⋆
- problem modalności o wysokiej penetracji genetycznej: bliźnięta: 1 na 80 urodzin, bliźnięta jednojajowe: 1 na 240 urodzin - co najmniej 0.8% osób błędnie rozpoznanych
- DNA – z pominięciem problemu bliźniaków jednojajowych: bardzo wysoki stopień różnicowania, zalety znacznie górują nad wadami

Pożądane atrybuty modalności biometrycznych

Akceptacja społeczna / religijna

- akceptacja religijna pomiaru
  - obraz twarzy
  - *2006, sieć sklepów spożywczych Piggly Wiggly USA: zastosowanie RFID (radio-frequency identification) i biometrii odcisków palca: niektórzy klienci wyrazili obawę, że RFID i biometria są ucieleśnieniem biblijnego 'znaku bestii" z Księgi Objawień* (http://www.securitymanagement.com/article/biometric-devils-details-004961)
- higiena i bezpieczeństwo zdrowotne pomiaru
- akceptacja celów pomiaru

Pożądane atrybuty modalności biometrycznych

Niezmienność

- niezmienność w czasie: efekt upływu czasu od pobrania wzorca (podpis !)
  efekty starzenia (twarz !)
- niezależność od stanu zdrowia (twarz, podpis, tęczówka !)
- niezależność od ubioru, mimiki etc. (twarz !)
- niezależność od warunków zewnętrznych

- zagadnienia słabo zbadane (brak odpowiednich baz danych!)
- twarz: baza MORPH (odstęp < 30 lat), KFRiA odciski (1 rok), BIOBASE twarz, tęczówka, odcisk, podpis on-line, kształt dłoni (5 lat), NIST tęczówka (4lata)
- pobieranie wzorców częściej niż co roku słabo akceptowalne

Pożądane atrybuty modalności biometrycznych

Bezpieczeństwo zdrowotne pomiaru

- higiena pomiaru
  - preferencja czujników bezdotykowych, kamer
- inwazyjność pomiaru
  - światło laserowe, badanie siatkówki, badanie USG – odbierane jako inwazyjne
- bezpieczeństwo zdrowotne pomiaru
  - niezbędne ograniczenia natężenia oświetlenia, zmienności oświetlenia

Pożądane atrybuty modalności biometrycznych

Wygoda i niski koszt pomiaru

- możliwość pomiaru – dostępność mierzonej cechy u każdego człowieka
- komfort pomiaru
- niski czas trwania pomiaru
- niski koszt urządzeń pomiarowych i pomiaru

Pożądane atrybuty modalności biometrycznych

Problem fałszerstw

- trudność fałszowania (ang. *vulnerability*)
  - modyfikacja cech biometrycznych niemożliwa / trudna (podpis) / kosztowna (operacja opuszka palca)
- niedostępność wyników dla postronnego obserwatora
  - większość danych biometrycznych jest łatwo dostępna (podpis off-line, twarz !)
  - wzrost zainteresowaniami wzorem naczyń krwionośnych

Pożądane atrybuty modalności biometrycznych

Podsumowanie

- odpowiednio wysoki stopień różnicowania (ang. *distinctiveness*)
- powszechność (ang. *inclusiveness*)
- akceptacja społeczna / religijna
- niezmienność w czasie (ang. *stability*) akceptacja ¿ 1 rok
- niezależność od stanu zdrowia
- niezależność od ubioru, mimiki
- wygoda i niski koszt (ang. *usability*)
- niedostępność dla postronnego obserwatora
- niezależność od warunków zewnętrznych (ang. *insensitivity*)
- trudność fałszowania (ang. *vulnerability*)
- higiena, nieinwazyjność i bezpieczeństwo zdrowotne pomiaru

Modalności biometryczne

Atrybuty

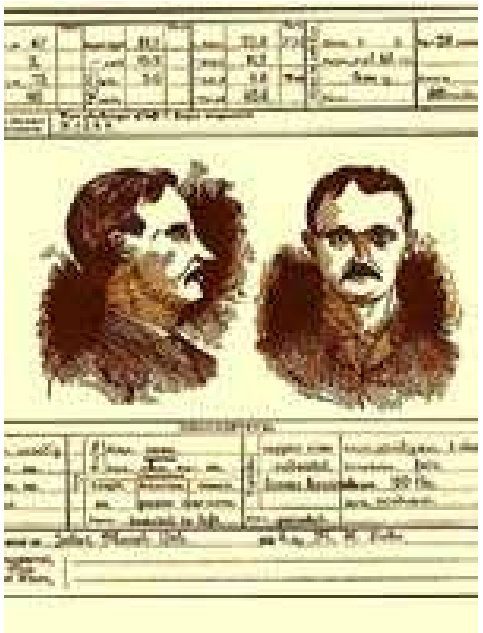
modalność	uniw.	akcept.	różnic.	starz.	pomiar	jakość	niedost.
twarz	⊕		⊙		⊕	⊙	
odcisk palca		⊙	⊕	⊕	⊙	⊕	
geometria dłoni		⊙	⊙	⊙	⊕	⊙	
naczynia	⊙	⊕	⊕	⊙	⊙	⊙	⊕
tęczówka	⊙	⊕	⊕	⊕	⊙	⊕	⊕
siatkówka	⊕		⊕	⊙		⊕	⊕
DNA	⊕		⊕	⊕		⊕	⊕
termogram	⊕	⊕	⊙		⊕	⊙	⊙
zapach	⊕	⊙	⊙				⊕
ucho	⊙	⊕	⊙	⊕	⊙	⊙	
podpis off-line	⊙	⊕			⊕		
podpis on-line	⊙	⊕	⊕		⊙	⊙	⊙
głos	⊙	⊕	⊙	⊙		⊕	⊙
rytm klawiszy		⊕			⊙		⊙
chód	⊙	⊕	⊙		⊕		

⊕- na ogół tak, ⊙- średnio, - na ogół nie

2.2: Historia, współczesność, prognozy

Pre-biometria

- 7 w. pne. - Chiny, Babilonia i Asyria
  - tabliczki gliniane z odciskami palców (transakcje)
- 1686 - Marcello Malpighi, Uniwersytet w Bolonii
  - charakterystyka odcisków palców
- 1823 - John Purkinje, Uniwersytet Wrocławski
  - charakterystyka dziewięciu typów odcisków palców
- 1856 - Sir William Herschel, Indie
  - odcisk dłoni w uwierzytelnianiu kontraktów
- 1880 - Henry Faulds, Tokio
  - identyfikacja odcisku pozostawionego na butelce
- 1880 - Alphonse Bertillon, Francja ►
  - pomiary długości kości
  - osoby o identycznych długościach kości (1903)
- 1888 - Sir Francis Galton
  - klasyfikacja punktów osobliwych, minucje, jakość weryfikacji (błąd 1:64 mld)

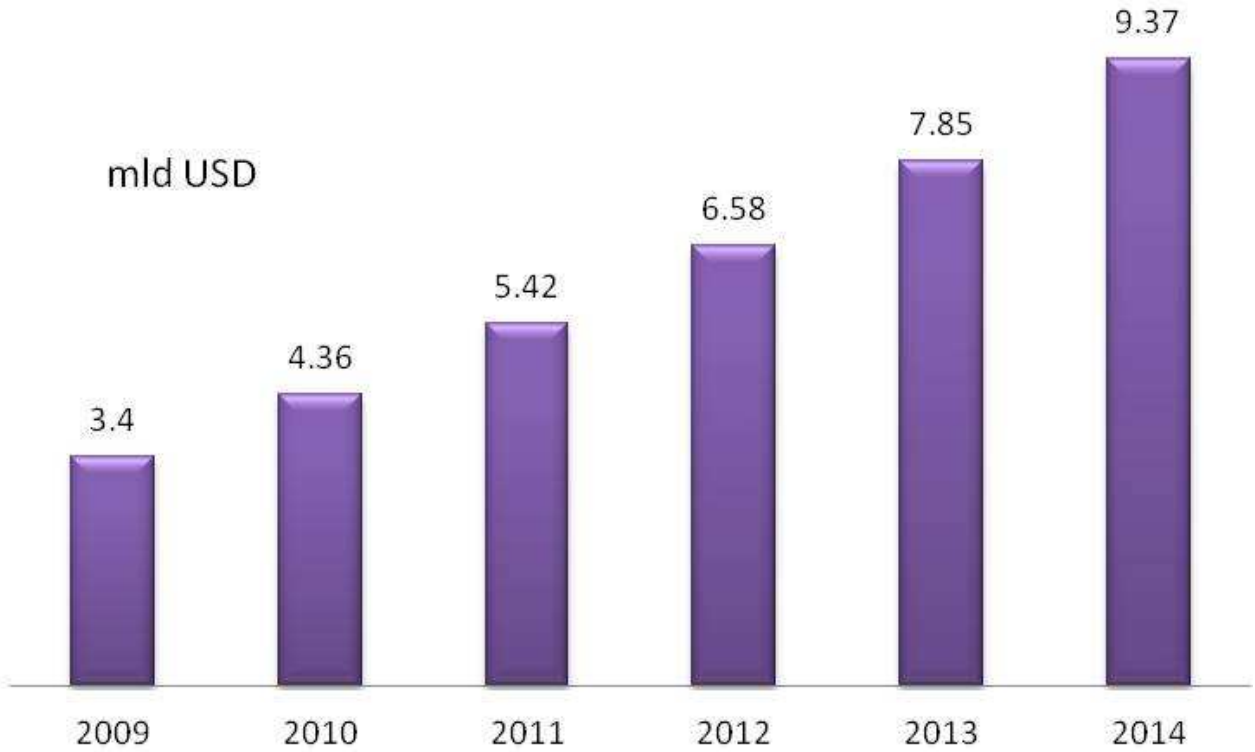


H.H. Heafner, “The Police Artist & Composite Drawings”, http://www.forensicartist.com/ history/index.htm

Historia

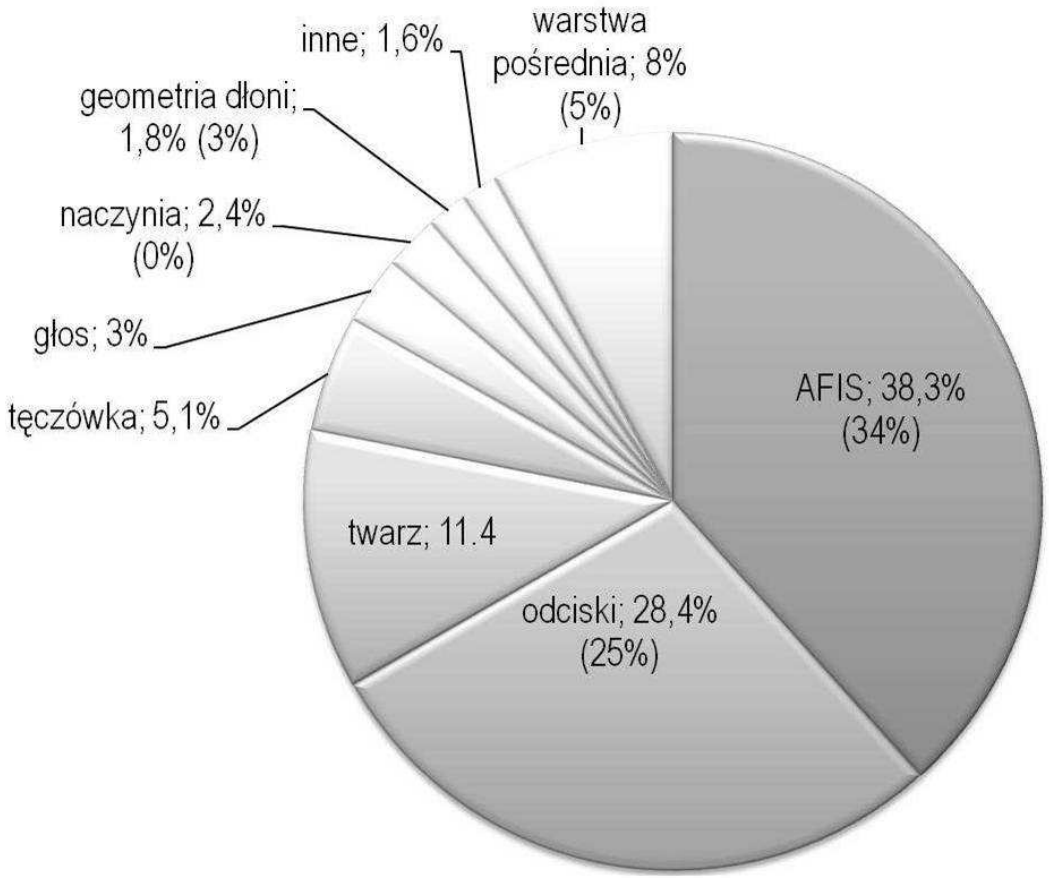
- lata 60. XX wieku
  automatyczna identyfikacja na podstawie odcisku palca, głosu
- lata 70. XX wieku
  geometria dłoni
- lata 80. XX wieku
  obraz siatkówki oka, podpis odręczny
- lata 90. XX wieku
  systemy biometrii tęczówki
- 1. dekada XXI wieku
  naczynia krwionośne

Przychody i prognoza rozwoju



dane: Biometrics Market and Industry Report 2009-2014, International Biometric Group 2010

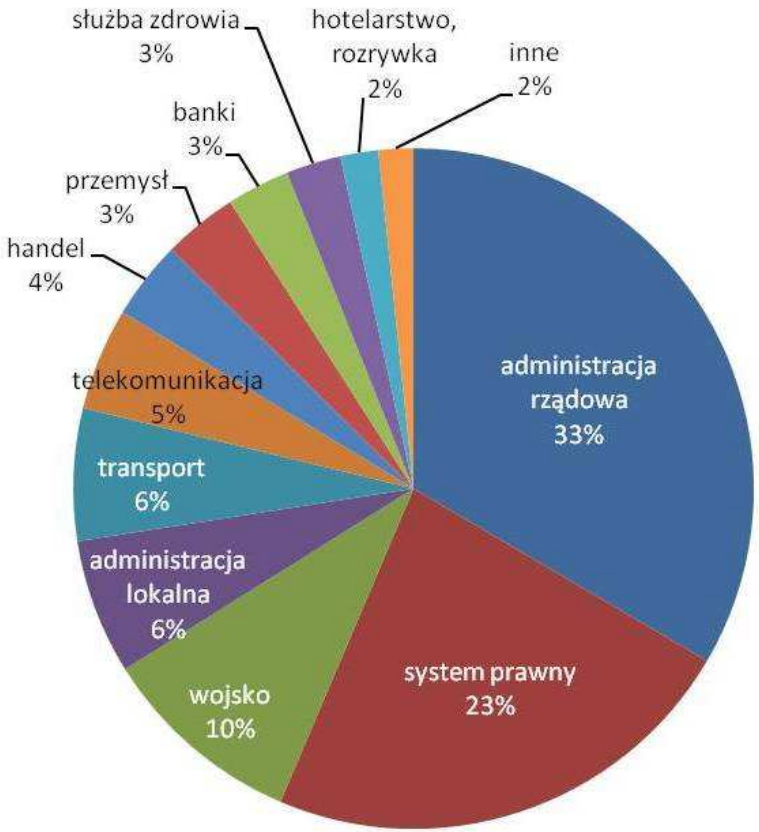
Modalności biometryczne na rynku



dane: Biometric Revenues by Technology, 2009-2014, 2008 International Biometric Group

Zastosowania 2009 - gałęzie rynku

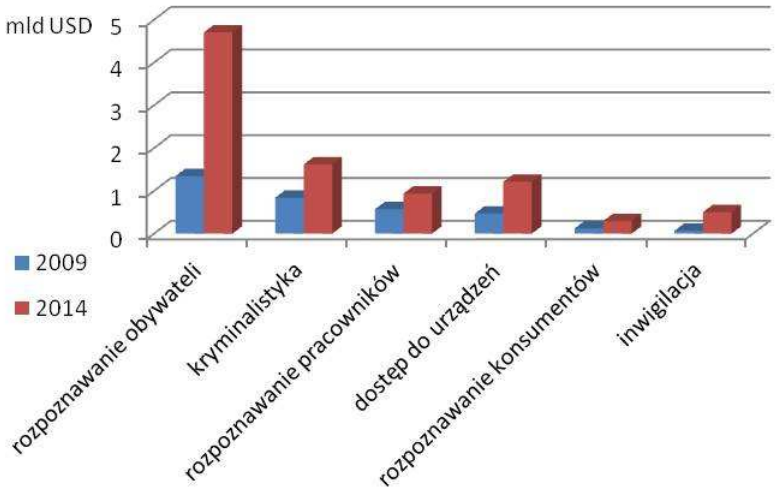
- państwowe 72.5%
- prywatne 27.5%



dane: Biometrics Market and Industry Report 2009-2014, International Biometric Group 2010

Kategorie zastosowań : 2009-2014

- rozpoznawanie obywateli
  identyfikacja obywateli, kontrola graniczna, wybory
- kryminalistyka
  tożsamość podejrzanych / uwięzionych, badanie przeszłości kryminalnej
- rozpoznawanie pracowników
  kontrola dostępu zatrudnionych, potwierdzenie obecności
- dostęp do urządzeń i systemów
  dostęp do systemów, dostęp zdalny
- zastosowania konsumenckie
  autoryzacja transakcji
- inwigilacja
  stwierdzenie tożsamości bez wiedzy osoby badanej



dane: Biometric Revenues by Technology, 2009-2014, 2008 International Biometric Group

2.3: Od pomiaru do decyzji

Pomiary biometryczne

Od człowieka do wzorca biometrycznego

modalność (właściwość) biometryczna (ang. *biometric modality, biometric characteristic*)

(np. tęczówka, twarz, linie papilarne)

⇓

pomiar

⇓

próbka biometryczna (ang. *biometric sample*)

(np. obraz oka, obraz twarzy, odcisk palca)

⇓

przetwarzanie pomiaru

⇓

cecha biometryczna (ang. *biometric feature*): reprezentacja próbki biometrycznej

(np. wartości filtrów Gabora dla tęczówki, cechy twarzy, lista minucji)

⇓

uzupełnianie o dodatkowe informacje

⇓

wzorzec biometryczny (ang. *biometric template*)

(np. kod tęczówki, kod twarzy, kod odcisku palca)

Pomiary biometryczne

Tryby pracy systemu biometrycznego

- *rejestracja* (ang. *enrolment (UK), enrollment (US)*)
  - zwykle wielokrotny pomiar; zaostrzona kontrola jakości, test autentyczności
  - sprawdzenie jakości pomiaru (ewent. kontynuacja transakcji)
  - zapis biometrycznego *wzorca referencyjnego*
    - zapis w bazie danych
    - zapis na indywidualnym nośniku (np. karcie chipowej)
  - powiązanie danych biometrycznych z innymi danymi osobowymi
  - zapis w bazie danych lub na nośniku indywidualnym
- *rozpoznawanie* (ang. *recognition*)
  - *pomiar*; przydatny test autentyczności
  - *porównanie*
    - z jednym wzorcem (weryfikacja)
    - z wieloma wzorcami (identyfikacja)
  - *decyzja* - zależna od *polityki decyzyjnej*
    - przykład: przy weryfikacji:
      zgodność z wzorcem - zaakceptować tożsamość
      niezgodność z wzorcem - powtórzyć pobranie próbki (jeden raz)
      zgodność w drugim podejściu - zaakceptować tożsamość
      ponowna niezgodność 0 odrzucić tożsamość

Pomiary biometryczne

Tworzenie obrazu biometrycznego

- *prezentacja* (ang. *presentation*) (jedna lub więcej)
- *podejście* (ang. *attempt*)) - ciąg (1 lub więcej) prezentacji
  - więcej niż jedna prezentacja np. w celu doboru najlepszej
- *transakcja* (operacja) - ciąg (1 lub więcej) podejść
  - polityka decyzyjna może dopuszczać np. 2 podejścia

2.4: Losowość pomiarów biometrycznych

Ocena zgodności próbek

Rodzaje próbek

- zagadnienie rozpoznawania dla danej modalności
  - dla danej modalności ta sama osoba może być charakteryzowana przez wiele klas (lewe/prawe oko, odciski poszczególnych palców etc.)
- rozpoznawanie biometryczne: badanie zgodności prezentowanej próbki z wzorcem określonej klasy (weryfikacja) lub wzorcami określonych klas (identyfikacja)
- najistotniejszym elementem rozpoznawania jest oszacowanie błędu pojedynczego porównania próbki i wzorca
- próbka może
  - pochodzić z rozpatrywanej klasy (*próbki własne*)
  - pochodzić z innej klasy (*próbki obce*, fałszerstwa bezwysiłkowe)
  - być specjalnie spreparowaną próbką mającą imitować próbki z badanej klasy (*fałszerstwa zaawansowane* o różnym stopniu zaawansowania)
- błędy porównania próbki z wzorcem: błąd fałszywej niezgodności i błąd fałszywej zgodności

Błędy porównań

Fałszywa niezgodność (FNM)

- *fałszywa niezgodność* (fałszywe niedopasowanie) FNM (ang. *false non-match*): błędne uznanie próbki za niezgodną z odpowiednim wzorcem klasy przy prezentacji próbek własnych (ang. *genuine*)
- FNM odpowiada błędowi 1 rodzaju w testowaniu hipotez statystycznych (odrzucenie hipotezy prawdziwej)
- miarą empiryczną FNM jest *częstość fałszywej niezgodności* *FNMR* (ang. *FNM rate*) obliczana przy uwzględnianiu tylko prezentacji próbek własnych, tzn.

$$FNMR = \frac{\text{liczba podejść uznanych za niezgodne z wzorcami}}{\text{liczba wszystkich podejść}}$$

- *FNMR* jest funkcją progu zgodności/niezgodności

Błędy porównań

Fałszywa zgodność (FM)

- *fałszywa zgodność* (fałszywe dopasowanie) FM (ang. *false match*): błędne uznanie próbki obcej lub fałszywej za zgodną z odpowiednim wzorcem
- FNM odpowiada błędowi 2. rodzaju w testowaniu hipotez statystycznych (nieodrzucenie hipotezy fałszywej)
- miarą empiryczną FM jest *częstość fałszywej zgodności FMR* (ang. *FM rate*) obliczana dla ustalonego progu tylko dla próbek fałszywych lub obcych, jako

$$FMR = \frac{\text{liczba podejść uznanych za zgodne z wzorcami}}{\text{liczba wszystkich podejść}}$$

- *FNMR* jest inny (zwykle niższy) dla próbek obcych (bezwysiłkowe fałszerstwa) niż dla próbek fałszywych

⊛ Ocena zgodności próbek

⊛ Dopasowanie próbek

- *stopień dopasowania* (ang. *matching score*) lub *stopień podobieństwa* (ang. *similarity score*) $s(i,j)$: ocena podobieństwa cech próbki i do cech wzorca j
- macierz podobieństwa $S = \{s(i,j)\}$

	wzorzec 1	wzorzec 2	…	wzorzec n
próbka 1	$s(1,1)$	$s(1,2)$	$\cdots$	$s(1,n)$
próbka 2	$s(2,1)$	$s(2,2)$	$\cdots$	$s(2,n)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
próbka n	$s(n,1)$	$s(n,2)$	$\cdots$	$s(n,n)$

- problemy
  - $s(i,j) = 0$ - próbki całkowicie niedopasowane (??)
  - próbki identyczne: $s(i,j) =$??

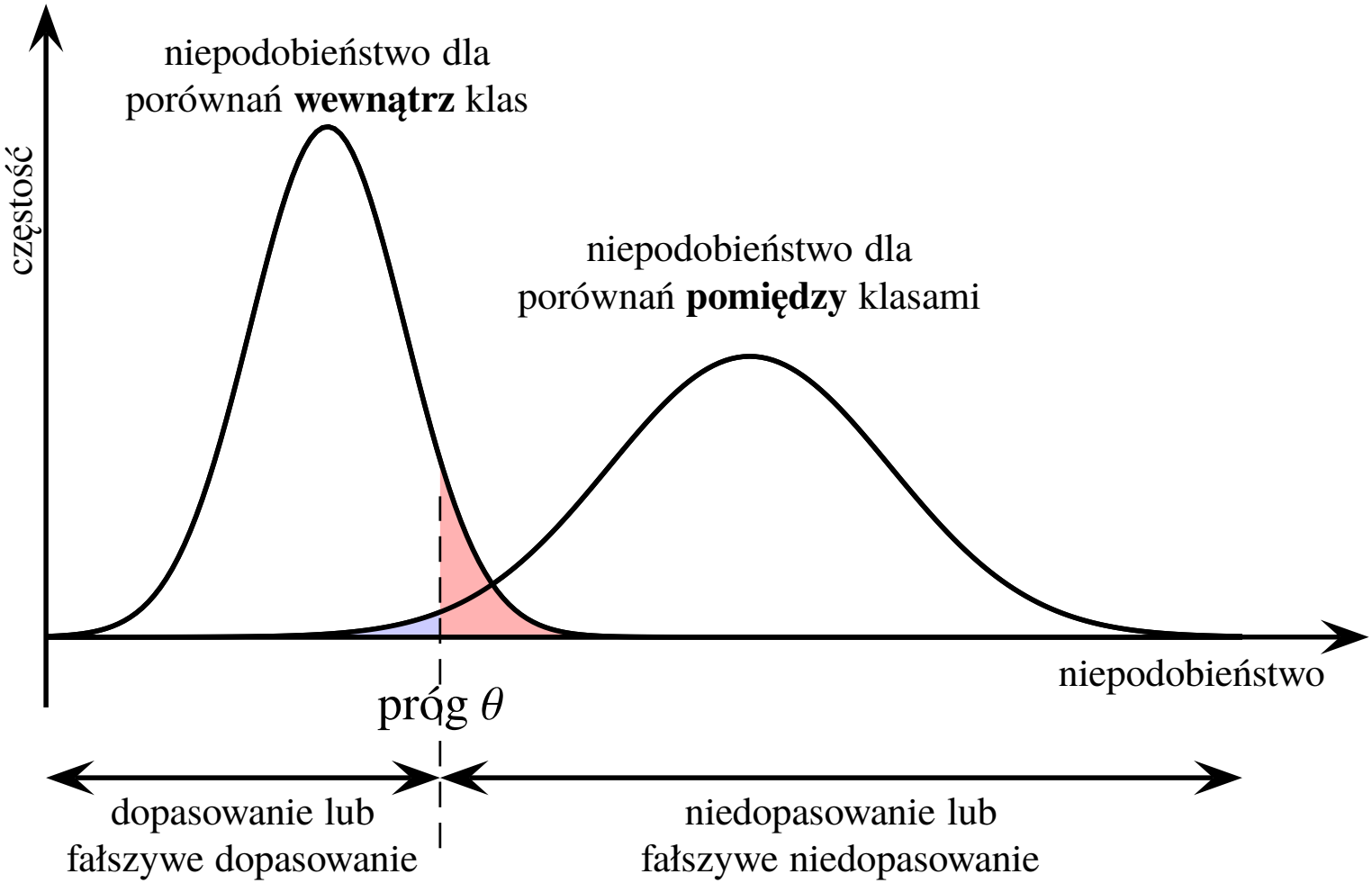
⊛ Ocena zgodności próbek

⊛ Niedopasowanie próbek

- *stopień niedopasowania*, *stopień niepodobieństwa* (ang. *dissimilarity score*) $d(i,j)$: ocena niepodobieństwa cech próbki i i cech wzorca j, macierz niedopasowania $D = \{d(i,j)\}$
  - $d(i,j) = 0$ - próbki identyczne
  - odległość ma własności niepodobieństwa
- nie ma prostego przejścia pomiędzy stopniem dopasowania a stopniem niedopasowania
- decyzja: *dopasowanie / niedopasowanie* (ang. *match/non-match*) jest podejmowana przez porównanie stopnia dopasowania (lub niedopasowania) z *progiem decyzyjnym* (ang. *decision threshold*)
- zwykle urządzenie biometryczne może być badane przez użytkownika tylko dla ustalonej przez producenta wartości progu decyzyjnego, czasem – dla różnych wartości progu

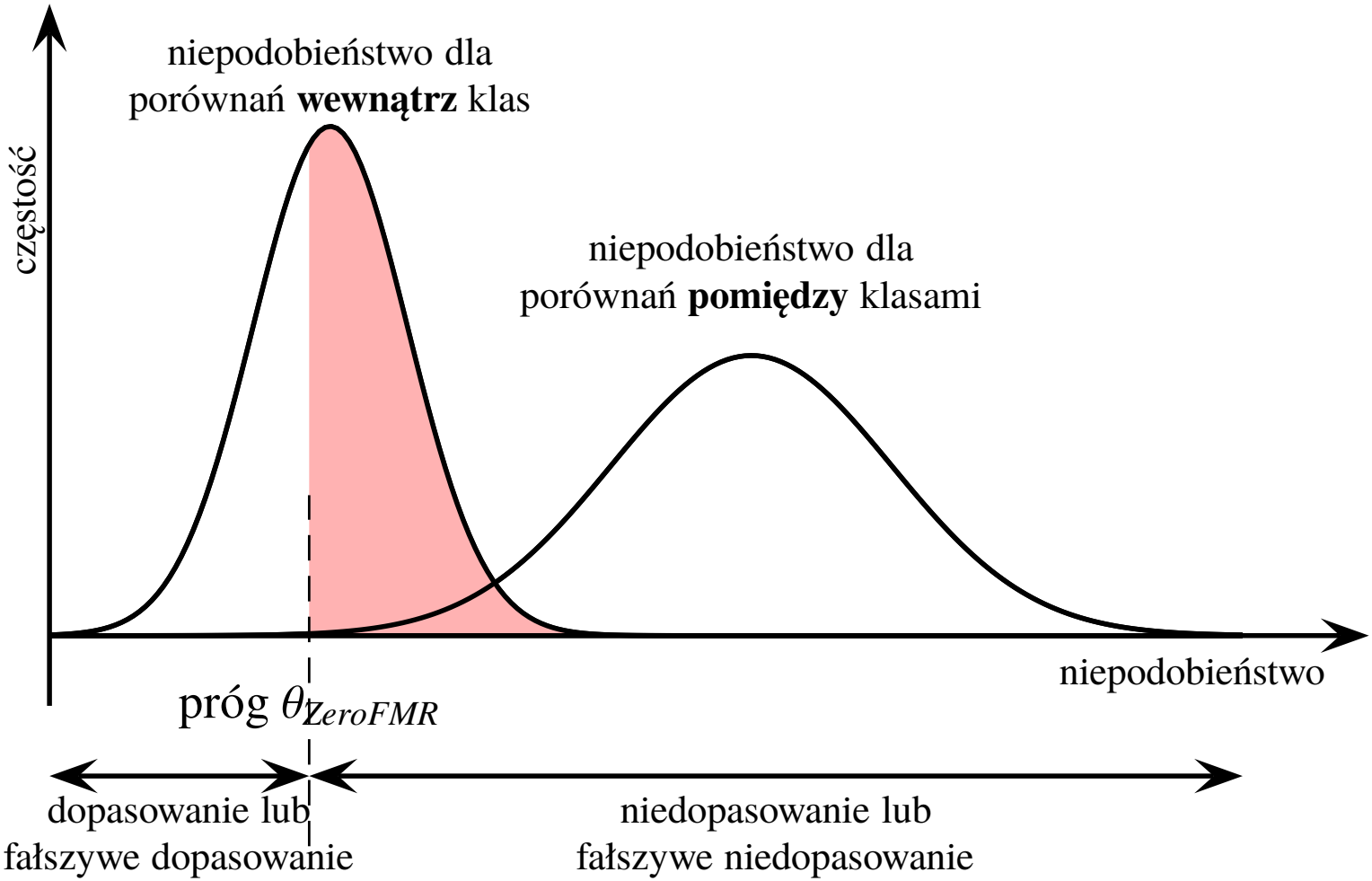
Ocena zgodności próbek

Losowość wyników



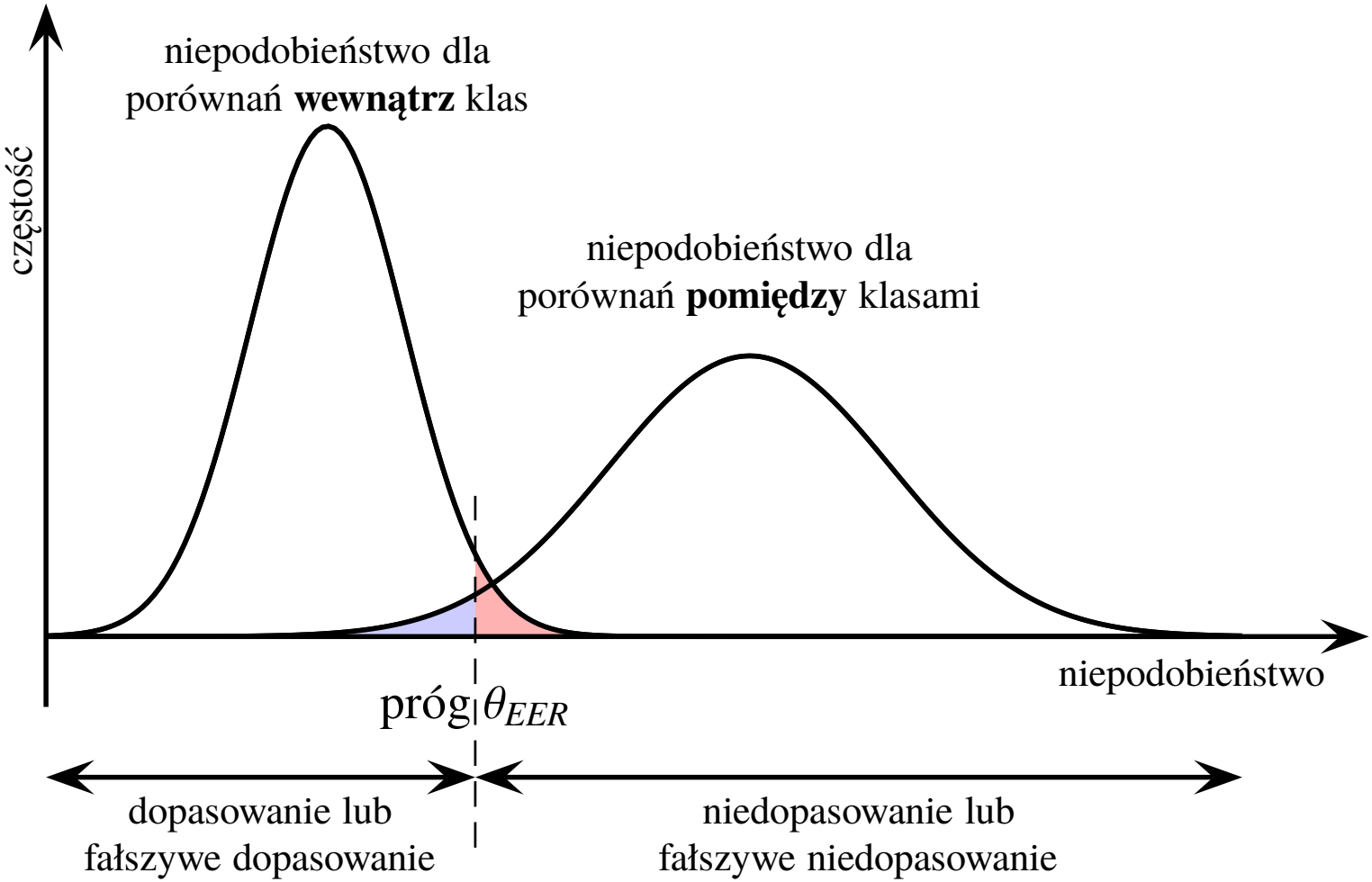
Ocena zgodności próbek

Losowość wyników: Zerowy błąd dopasowania



Ocena zgodności próbek

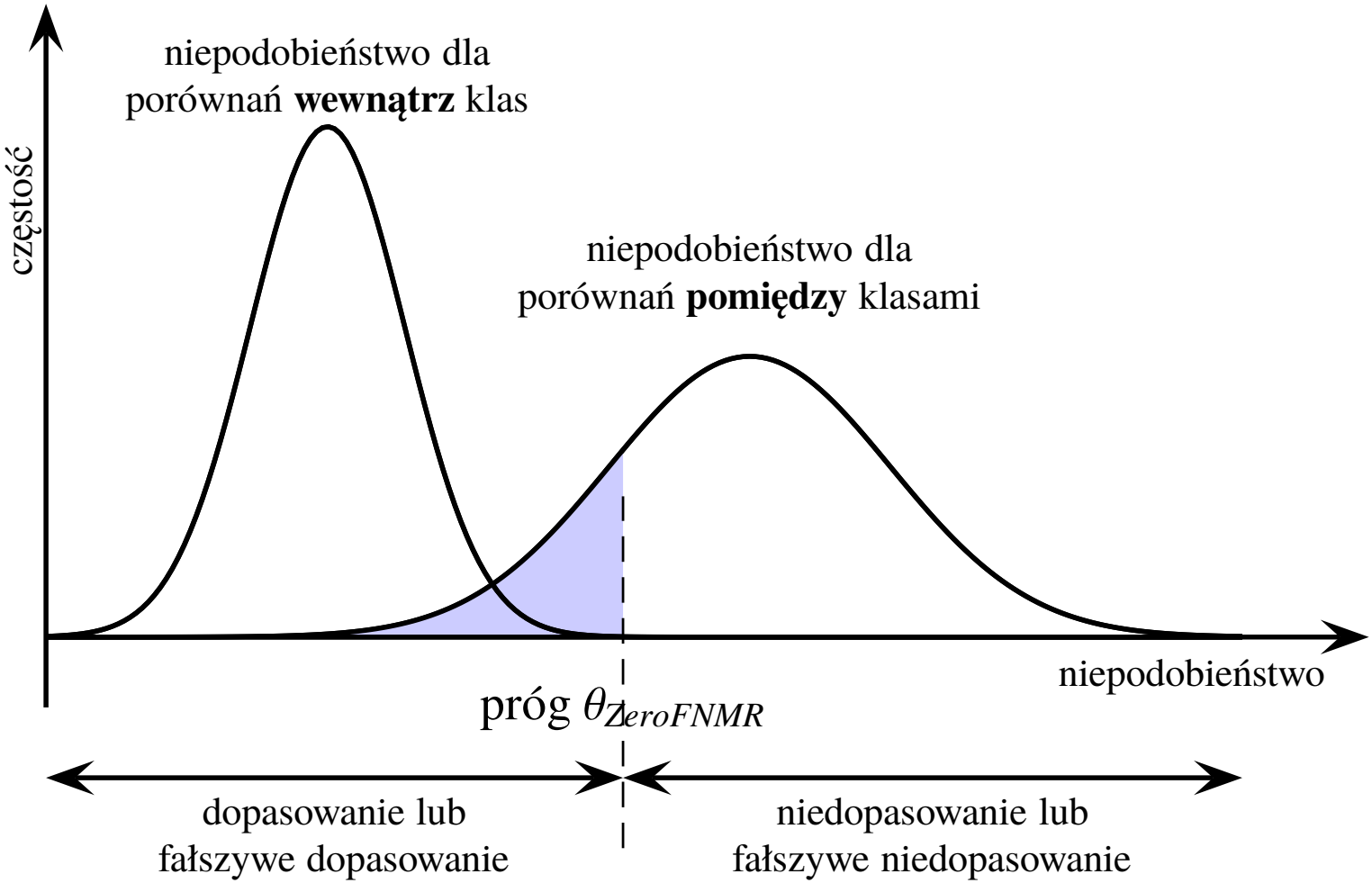
Losowość wyników: Błąd zrównoważony



równe pola (nie wartości !)

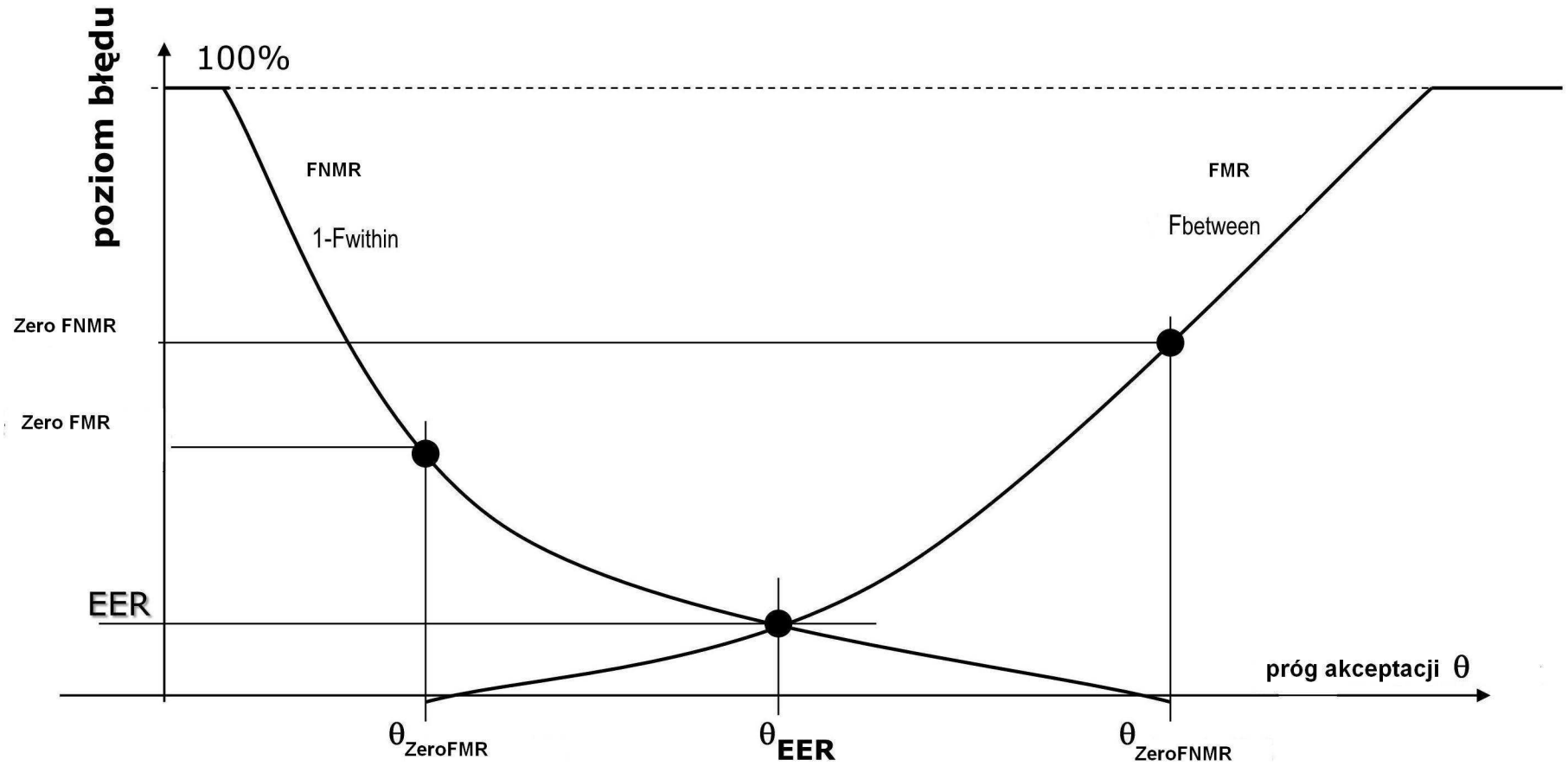
Ocena zgodności próbek

Losowość wyników: Zerowy błąd niedopasowania



Ocena zgodności próbek

FMR, FNMR, EER



® Błędy wyników testowania w statystyce

$\mathcal{H}$ = { próbka zgodna z wzorcem}

		decyzja	
		brak podstaw do odrzucenia $\mathcal{H}$	odrzucić $\mathcal{H}$
hipoteza	prawdziwa	✓	błąd 1. rodzaju
	fałszywa	błąd 2. rodzaju	✓

		decyzja	
		brak podstaw do odrzucenia $\mathcal{H}$	odrzucić $\mathcal{H}$
hipoteza	prawdziwa	$1-\alpha$	α
	fałszywa	β	$1-\beta$

$1-\alpha$ — poziom istotności
$1-\beta$ — moc testu

Błędy wyniku porównania

		wynik porównania	
		zgodność	niezgodność
próbka	własna	✓	FNM
	obca albo fałszywa	FM	✓

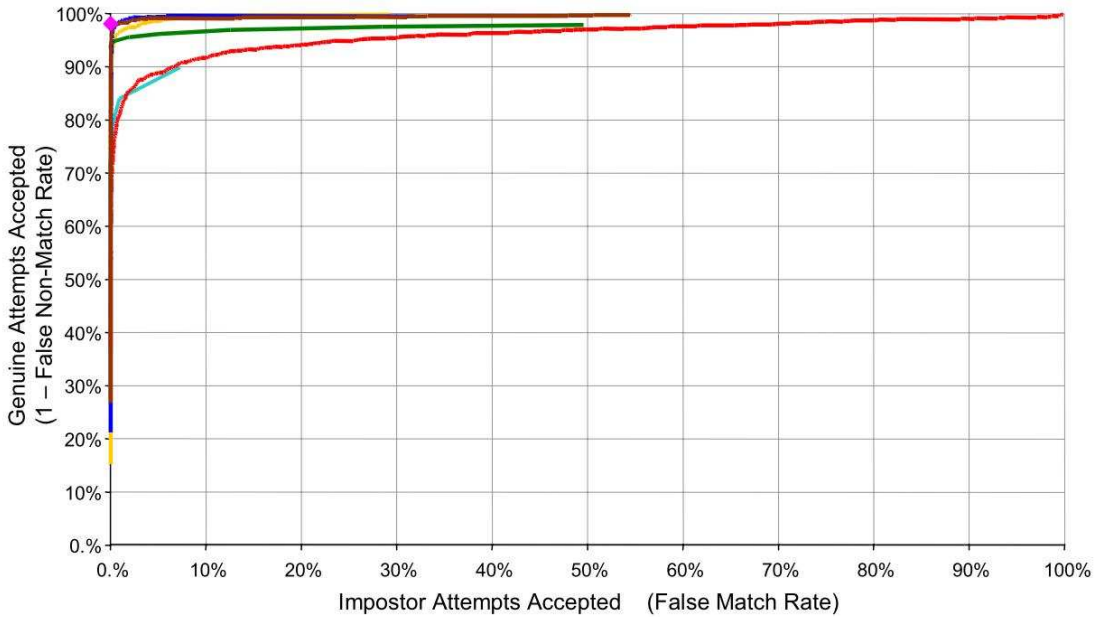
		wartość błędu	
		zgodność	niezgodność
próbka	własna	$1 - FNMR$	$FNMR$
	obca albo fałszywa	FMR	$1 - FMR$

- na podstawie wyników porównania/porównań podejmowane są decyzje dotyczące tożsamości zgodnie z polityką decyzyjną
- błędy wyniku rozpoznania to co innego niż błędy decyzji dotyczących tożsamości (błąd fałszywej akceptacji, błąd fałszywego odrzucenia) omawianych w dalszej części wykładu

Ocena zgodności próbek

Krzywa ROC

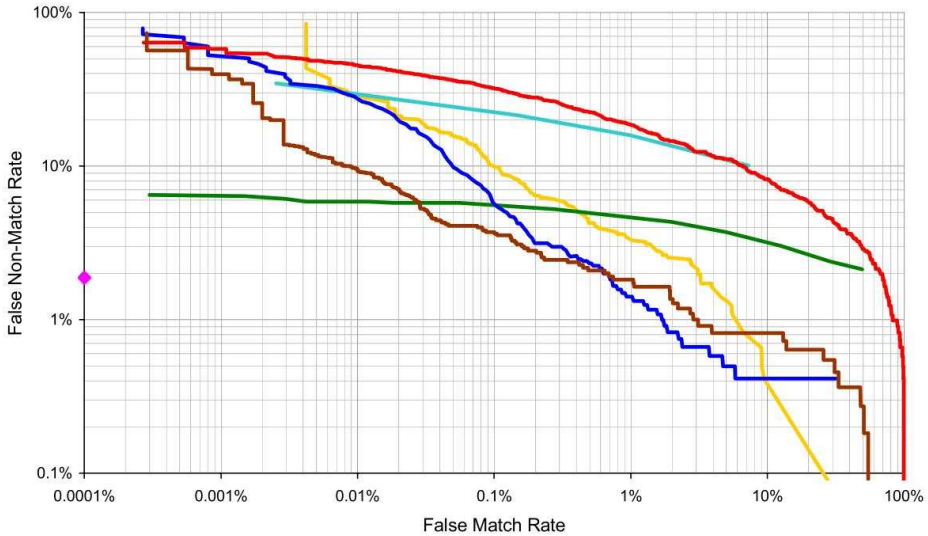
- charakterystyka operacyjna odbiorcy ROC (ang. *receiver operating characteristic*): częstość poprawnych zgodności 1 – *FNMR* w funkcji częstości błędnych zgodności *FMR* (z progiem jako parametrem)



Źródło: A.J. Mansfield, J.L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices", v. 2.01, *NPL Report CMSC 14/02*, National Physical Lab, 2002

Ocena zgodności próbek

Krzywa DET



Źródło: A.J. Mansfield, J.L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices", v. 2.01, *NPL Report CMSC 14/02*, National Physical Lab, 2002

krzywa DET ("kompromisu błędów detekcji" (ang. *detection error trade-off*)): *FNMR* w funkcji *FMR*

- modyfikacja: użycie skali logarytmicznych $x' = \log_{10} x$
- modyfikacja: użycie skali odchyłek normalnych (ang. *normal deviate scale*) $x' = \Phi^{-1}(x)$, gdzie Φ to dystrybuanta rozkładu normalnego standaryzowanego

Zagadnienia, pytania, zadania

Z2.1. Definicja biometrii i znaczenie poszczególnych jej elementów
Z2.2. Obawy zawiązane ze stosowaniem biometrii
Z2.3. Weryfikacja a identyfikacja
Z2.4. Typy i przykłady modalności biometrycznych
Z2.5. Pożądane własności modalności biometrycznych
Z2.6. Tryby pracy systemów biometrycznych
Z2.7. Próbki własne, obce, fałszerstwa
Z2.8. Błędy fałszywej zgodności, fałszywej niezgodności, błąd zrównoważony
Z2.9. Efekty losowości pomiarów biometrycznych
Z2.10. Krzywe ROC, DET