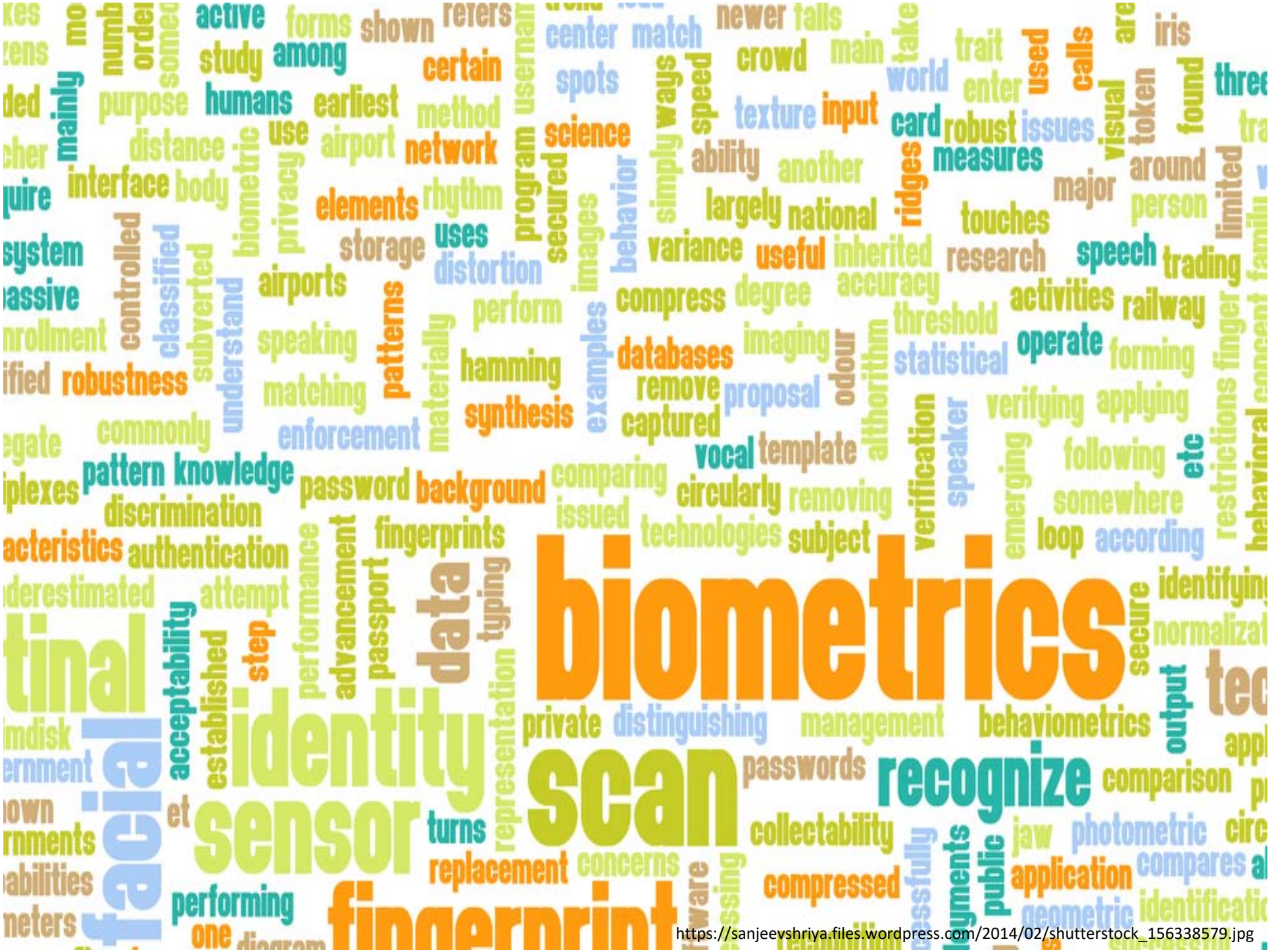
POLITECHNIKA GDAŃSKA

Przegląd technologii biometrycznych

Prof. Andrzej Czyżewski, mgr inż. Piotr Hoffmann
Katedra Systemów Multimedialnych,
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechnika Gdańska

Spis treści



https://sanjeevshriya.files.wordpress.com/2014/02/shutterstock_156338579.jpg

Nowoczesne technologie w bankowości

http://raconteur.net/public/img/articles/2015/04/Countering-cyber-criminals-with-Biometrics-760x428.jpg

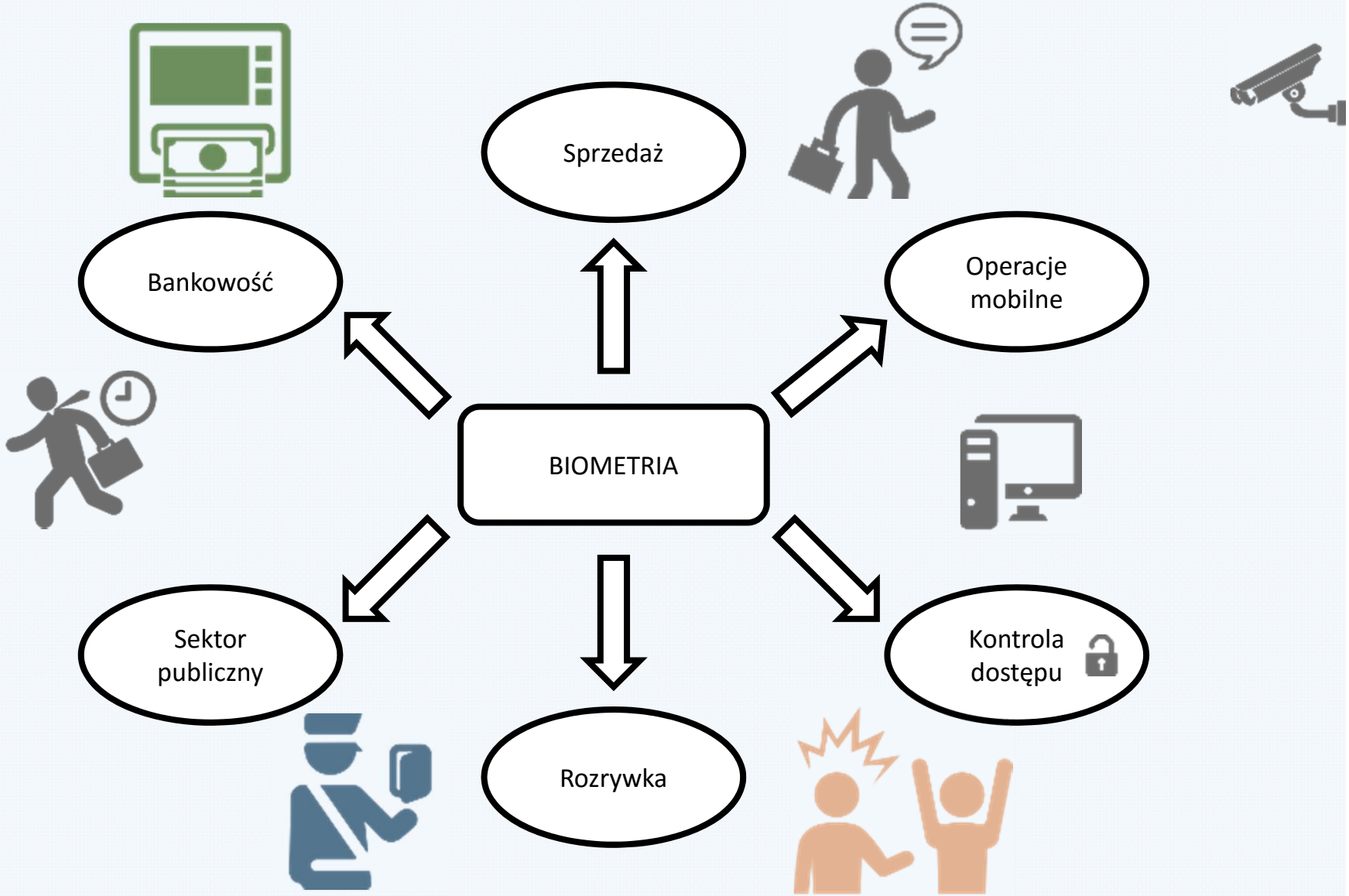
Początki biometrii

- Pierwsze, znane metody biometryczne wykorzystywały proces rozpoznawania twarzy oraz głosu.
- Identyfikacja osoby odbywała się z wykorzystaniem narządów wzroku i słuchu

Metoda wykorzystywana z powodzeniem do dziś

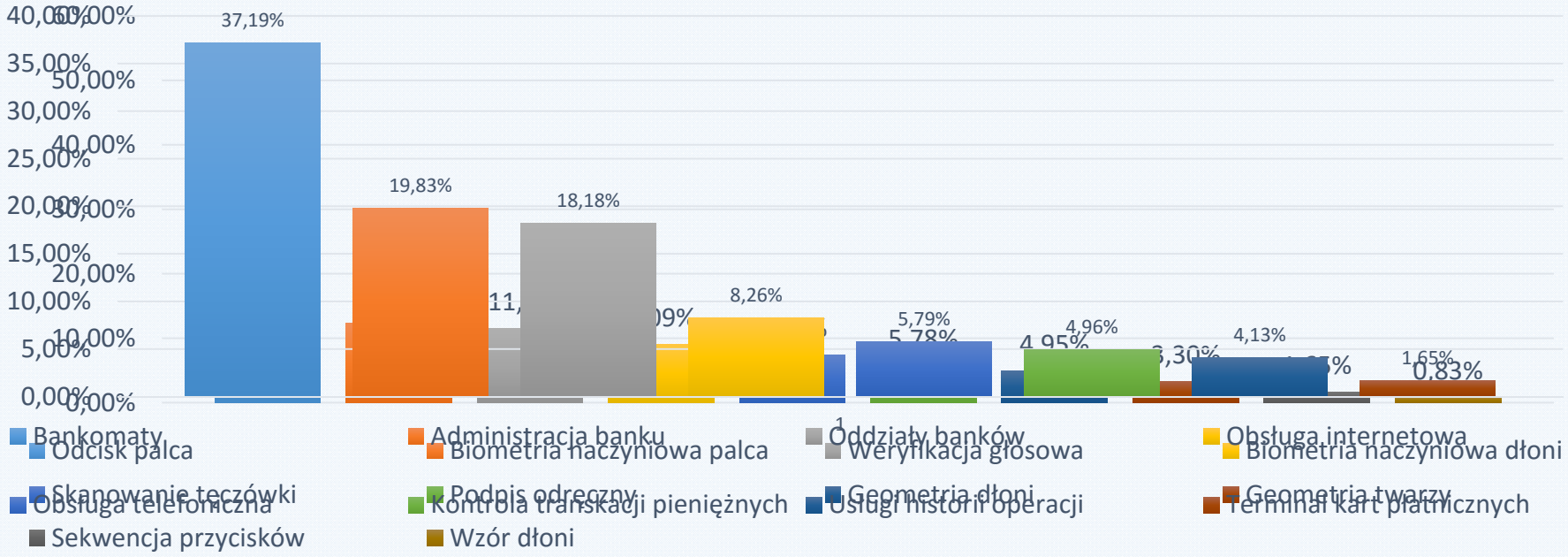
Rozwój metod biometrycznych rozpoczął się połowie XX wieku razem z zaawansowanymi, wojskowymi systemami informatycznymi

Obszary zastosowań biometrii



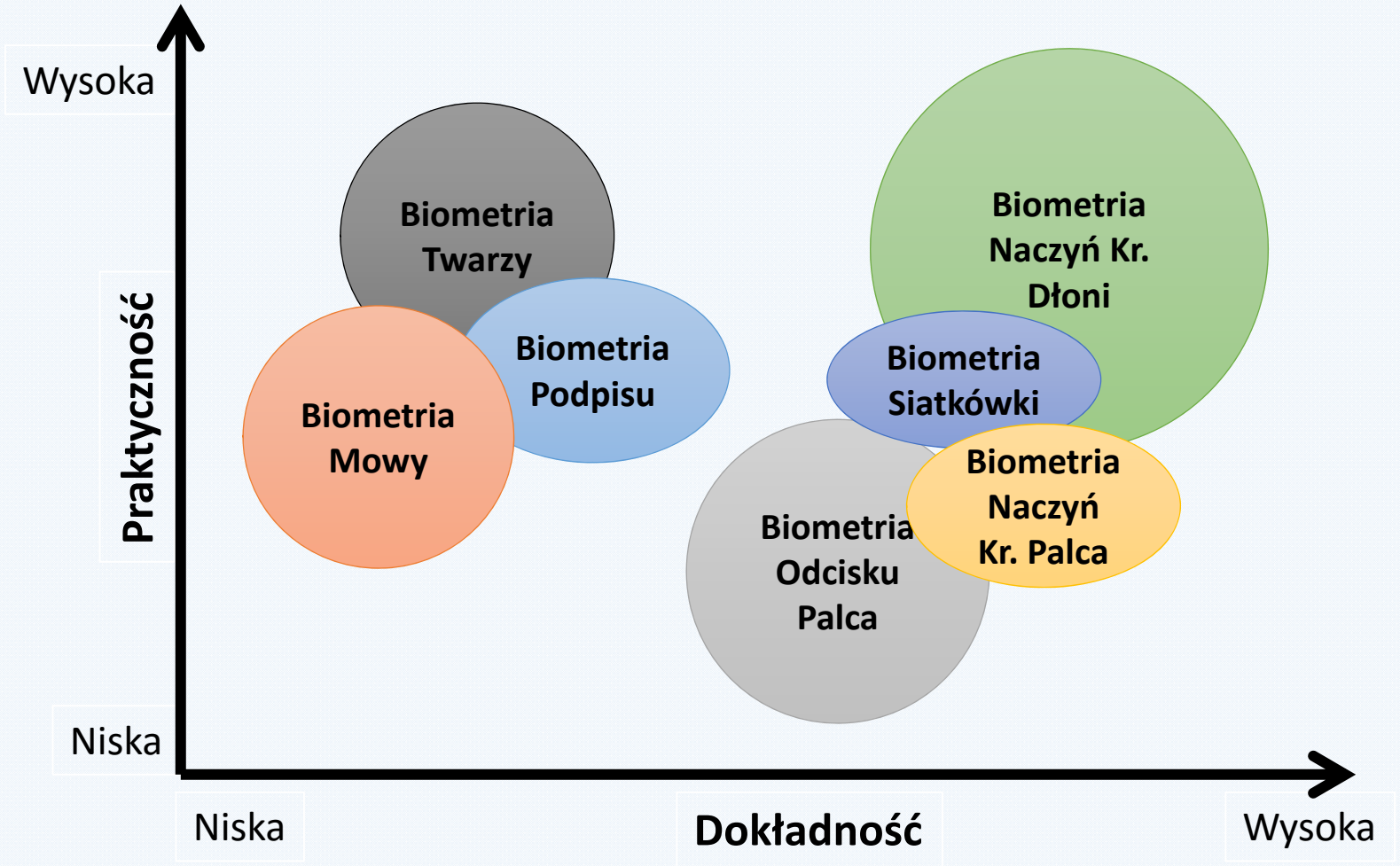
Statystyki biometryczne

Przeprowadzone w 2014 roku badania TNS potwierdzają, że blisko połowa respondentów (49%) chętnie wykorzysta metody biometryczne zamiast haseł i kodów PIN.



http://www.bankinfosecurity.com/users-want-new-forms-authentication-a-5692

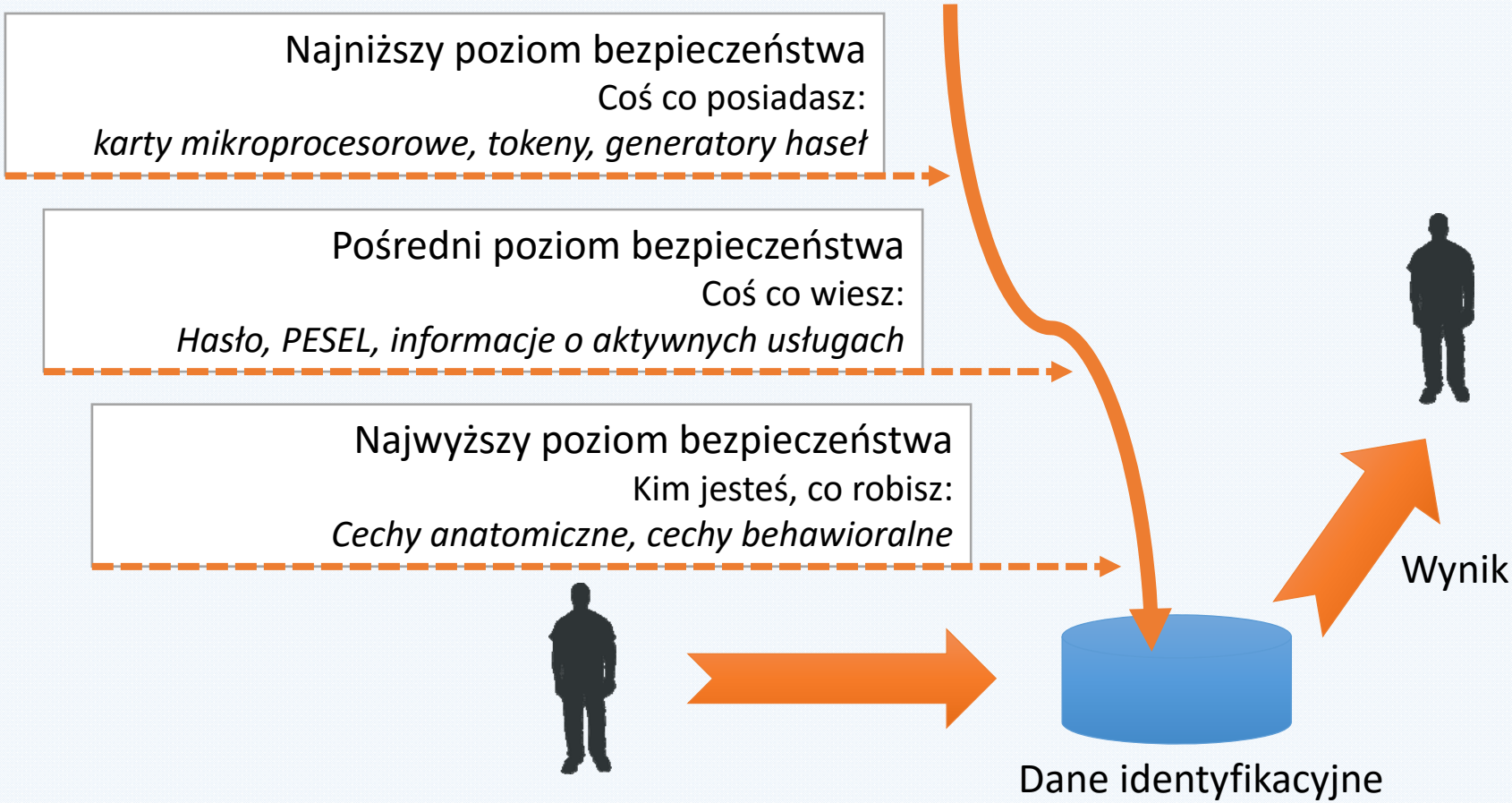
Klasyfikacja cech biometrycznych



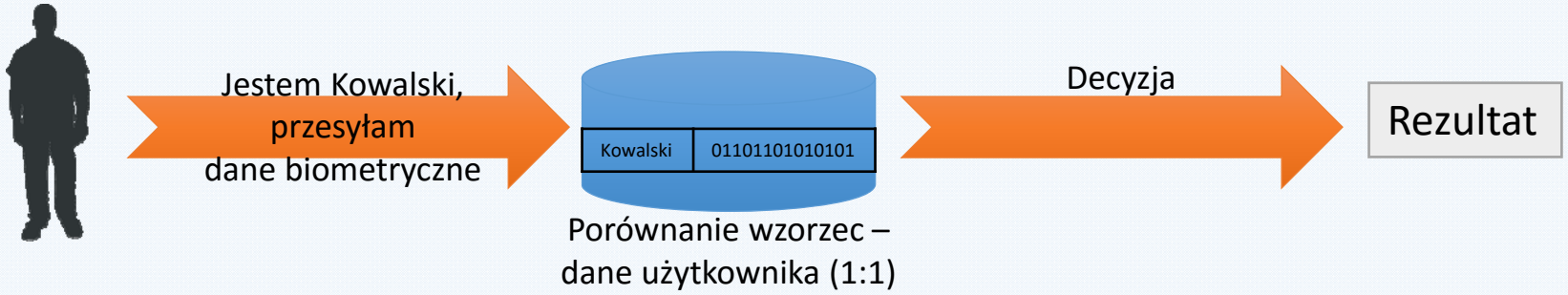
Biometria – szanse i ograniczenia

	Bezpieczeństwo		Praktyczność				
	Odporność na fałszerstwo	Dokładność	Szybkość	Rejestracja	Wygoda	Koszt	Rozmiar
Odcisk palca							
Tęczówka							
Geometria twarzy							
Weryfikacja głosowa							
Biometria naczyniowa palca							

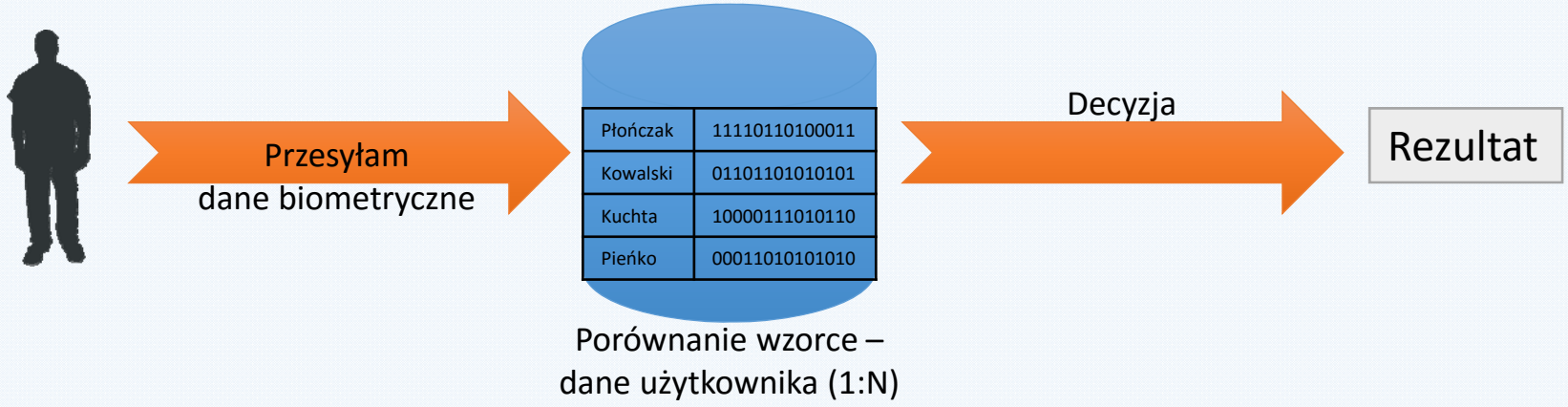
Uwierzytelnienie - jest to proces weryfikacji tożsamości użytkownika, sprawdzenie, kontrola zgodności z prawdą, określenie autentyczności, stwierdzenie, poświadczenie prawdziwości również z uwzględnieniem określonego prawdopodobieństwa



Weryfikacja – polega na przedstawieniu się użytkownika, a następnie porównaniu wskazanego identyfikatora ze wzorcem zapisanym w bazie (porównanie 1:1)

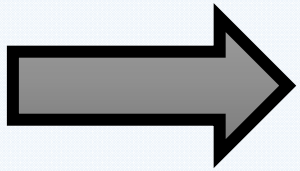


Identyfikacja – polega na analizie cech użytkownika, a następnie porównaniu ich ze wszystkim dostępnymi wzorcami w bazie (porównanie 1:N)



Autentykacja biometryczna

- Unikatowa
- Trwała
- Uniwersalna
- Bezpieczna



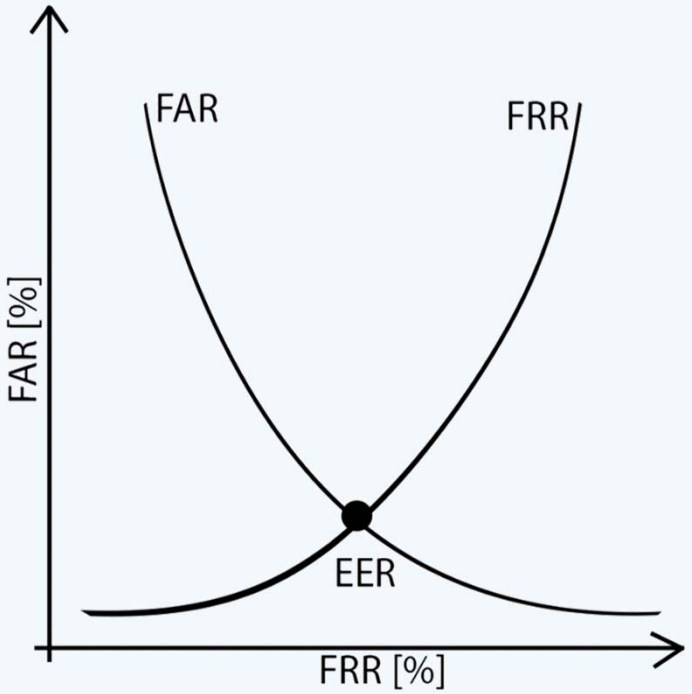
Skuteczna

- Wygodna
- Powszechna
- Akceptowalna
- Łatwa w przetwarzaniu

Ocena skuteczności metod biometrycznych

Do oceny skuteczności metod biometrycznych najczęściej stosuję się dwie miary:

- FAR (ang. *false acceptance ratio*) określa prawdopodobieństwo, że system biometryczny pozytywnie zweryfikuje sytuację (udzieli dostępu), w której nie powinien udzielić dostępu.
- FRR (ang. *false rejection ratio*) określa prawdopodobieństwo, że system biometryczny odrzuci próbę dostępu osobie, która jest do niego uprawniona. Obie te miary powinny być możliwie jak najniższe dla bardzo dużych prób ilościowych.



Biometria odcisku palca

Jedna z najstarszych metod identyfikacji

- już około 500 roku p.n.e. babilońscy biznesmeni swoje transakcje protokołowali na glinianych tabliczkach zawierających odciski palca;
- Joao de Bartos, hiszpański podróżnik, odkrywca i pisarz, pisał, że w XIV wieku chińscy kupcy używali odcisków palca dla potwierdzania transakcji biznesowych;
- argentyński oficer policji Juan Vucetich w 1888 roku jako pierwszy użył daktyloskopii ;
- pod koniec XIX wieku stworzono w Indiach pierwszy kompleksowy system biometryczny (bazę danych odcisków palców). Dokonał tego główny inspektor policji Edward Henry.

Odcisk palca jest cechą niepowtarzalną dla każdego człowieka

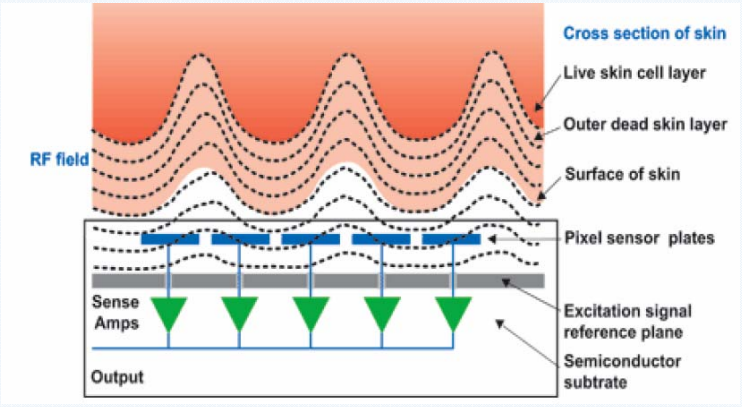
Linie są skanowane przez specjalistyczny czujnik eksportujący matematyczny odpowiednik obrazu

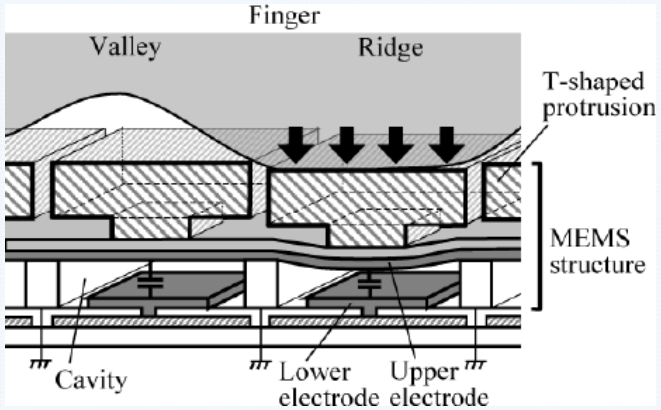
Autentykacja osób na podstawie odcisku palca odbywa się poprzez dopasowanie punktów charakterystycznych wzoru minucji

Biometria odcisku palca

Obecnie stosowane trzy typy czujników

- optyczne;
- półprzewodnikowe;
  - pojemnościowe,
  - RF,
  - termiczne,
  - piezorezystancyjne,
  - piezoelektryczne,
  - MEMS,
- ultradźwiękowe.



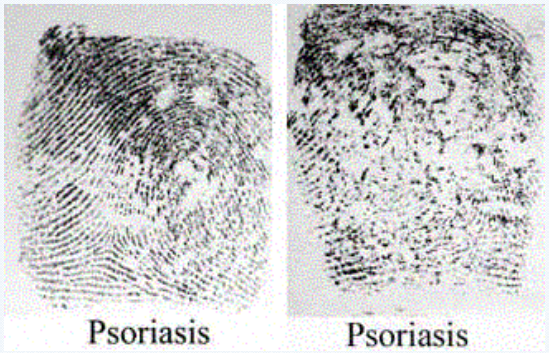


http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint.htm

Biometria odcisku palca

Możliwe problemy:

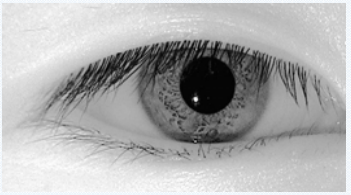
- Brak możliwości odczytu odcisku palca ze względu na:
  - Niedokładność kontaktu palca z czujnikiem
  - Zniszczone odciski palca
  - Zbyt dużą lub zbyt małą wilgotność skóry palca
- Próby oszustwa
  - Pierwsze próby już w latach 20-tych ub. wieku
  - W zależności od rodzaju czujnika istnieją różne metody obejścia systemu, np. zastosowanie sztucznego palca wykonanego z materiału o własnościach zbliżonych do prawdziwego



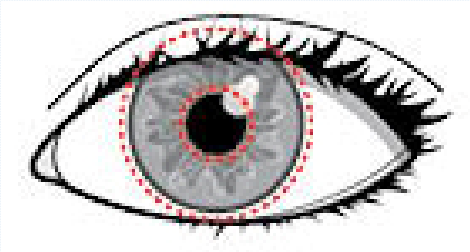
Nixon K.A., Aimale V., Rowe R.K., Spoof Detection Schemes, Handbook of Biometrics, Springer, 2007.

Biometria tęczówki

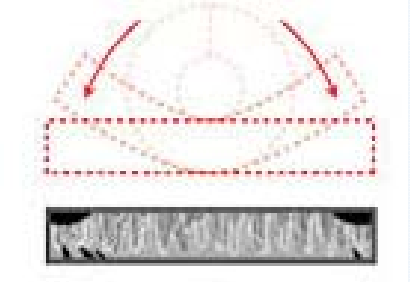
- Odczytywanie stanu zdrowia z tęczówki (irydologia) było znane już w starożytności
- Od lat 50 XX w. proponowano wykorzystanie wzorów tęczówki do identyfikacji
- Prototyp algorytmu rozpoznawania w 1991 r.
- Metoda oparta na analizie zdjęcia tęczówki oświetlonego światłem podczerwonym
- Z obrazu ekstrahowane są punkty charakterystyczne i zapisywane w skróconej postaci



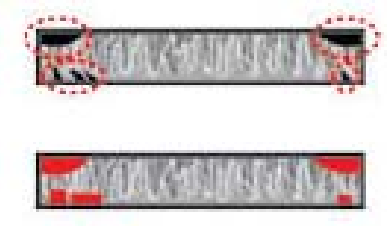
Biometria tęczówki



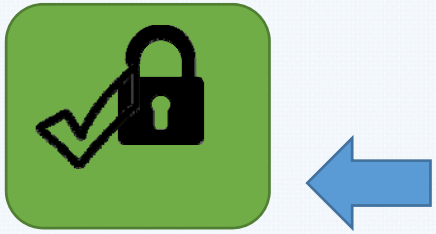
Obraz tęczówki przedstawiany jest w formie prostokątnej



Z obrazu usuwana jest źrenica i rzęsy



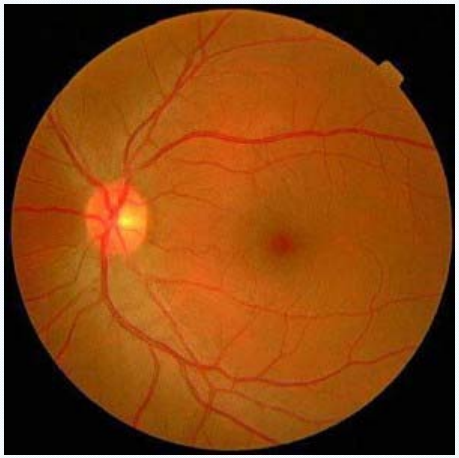
Obraz jest binaryzowany i porównywany z wzorcami w bazie



Znalezienie wzorca w bazie potwierdzeniem tożsamości użytkownika

Biometria siatkówki

- Jedna z najstarszych metod biometrycznych (unikalność ludzkiej siatkówki stwierdzono w 1935 r., komercyjny skaner w 1981 r.)
- Oparta na analizie obrazu naczyń krwionośnych siatkówki
- Obraz otrzymywany w wyniku odbicia promieniowania podczerwonego wysyłanego przez skaner od siatkówki
- Naczynia krwionośne pochłaniają więcej promieniowania, stając się wyraźnie widoczne



Biometria siatkówki

- Wysoce niezawodna metoda (niski poziom fałszywych akceptacji, praktycznie zerowy współczynnik fałszywych odrzuceń – przy poprawnie przeprowadzonym skanie)
- Choroby oczu wpływają na skuteczność metody (zaćma, jaskra, zakrzepy)
- Metoda stacjonarna – skanery siatkówek są drogie i nieporęczne
- Pomiar wymaga kooperacji użytkownika

Biometria podpisu

http://netdna.walyou.netdna-cdn.com/wp-content/uploads/2010/03/Multi-Pen-01.jpg

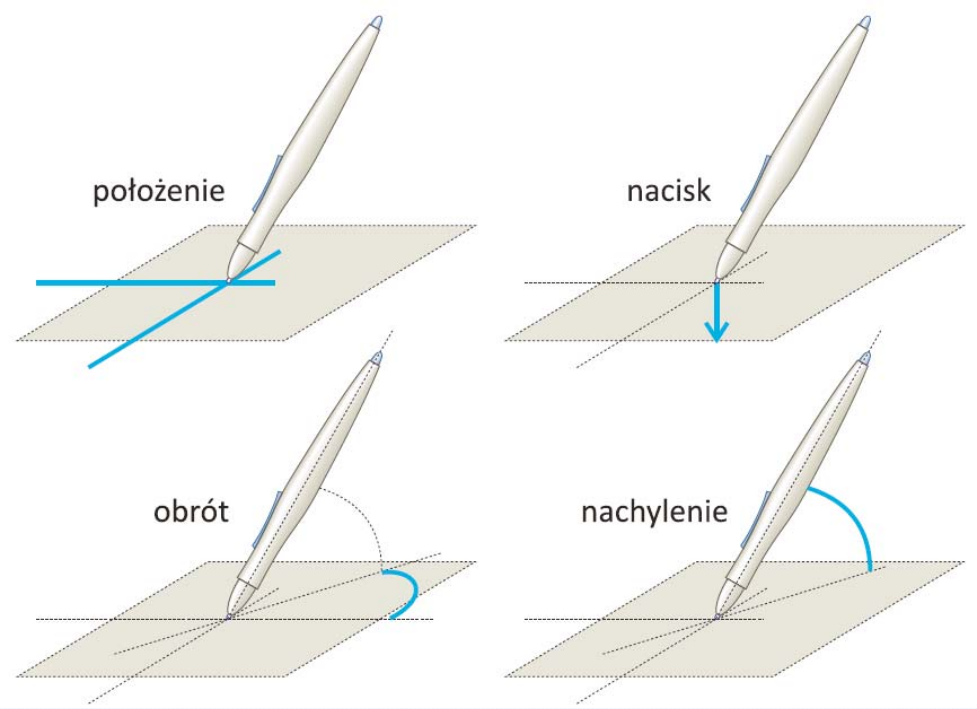
Cechy biometrii podpisu

- Charakterystyka wizualna podpisu
- Sposób w jaki został złożony
- Ogólnie akceptowalna metoda weryfikacji tożsamości, wygodna dla użytkownika

http://tech.batanga.com/files/Como-firmar-documentos-desde-Vista-Previa-en-Mac-OS-X-3.jpg

Pozyskiwanie danych

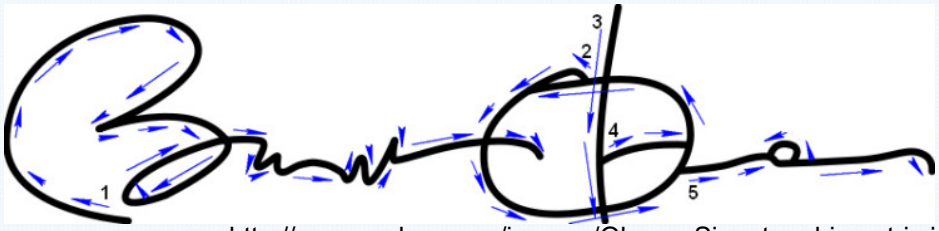
- Skanowanie obrazu (metody statyczne)
- Wykorzystanie tabletów graficznych
  - Próbki podpisu uporządkowane w czasie
  - Pomiar dodatkowych parametrów, np. nacisku na tablet
- Możliwość wykorzystania dowolnego ekranu dotykowego



Metody analizy podpisu

- Metody statyczne
  - Obraz statyczny podpisu
  - Brak informacji o kolejności występowania elementów podpisu

- Metody dynamiczne
  - Pozyskiwanie podpisu metodą elektroniczną
    - Rejestracja procesu podpisywania się
  - Zachowane informacje o kolejności występowania elementów podpisu



http://www.andxor.com/images/Obama Signature biometric.jpg

Biometria głosowa

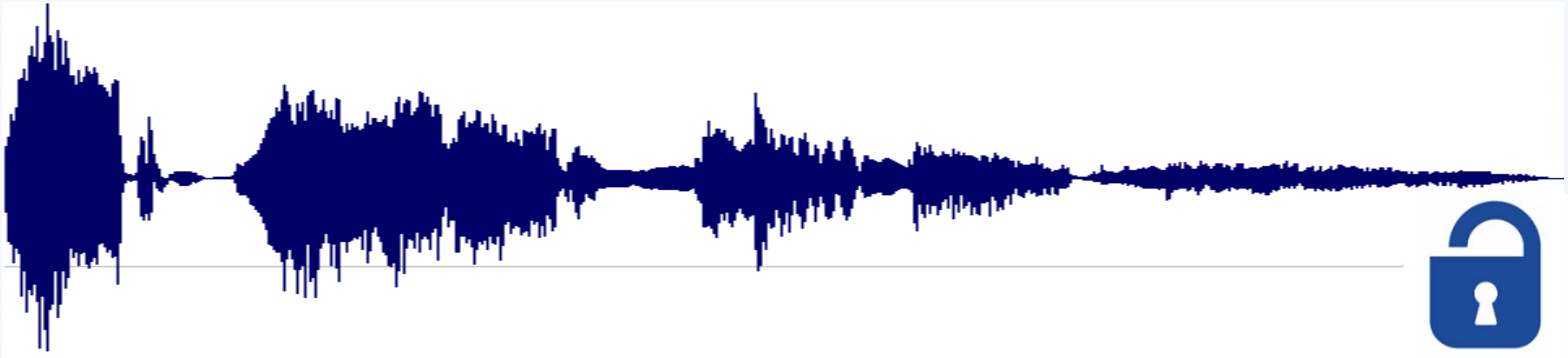
Każdy człowiek posiada unikatową barwę głosu, jest to cecha osobnicza wynikające z budowy anatomicznej traktu głosowego

Na barwę ludzkiego głosu mają wpływ:

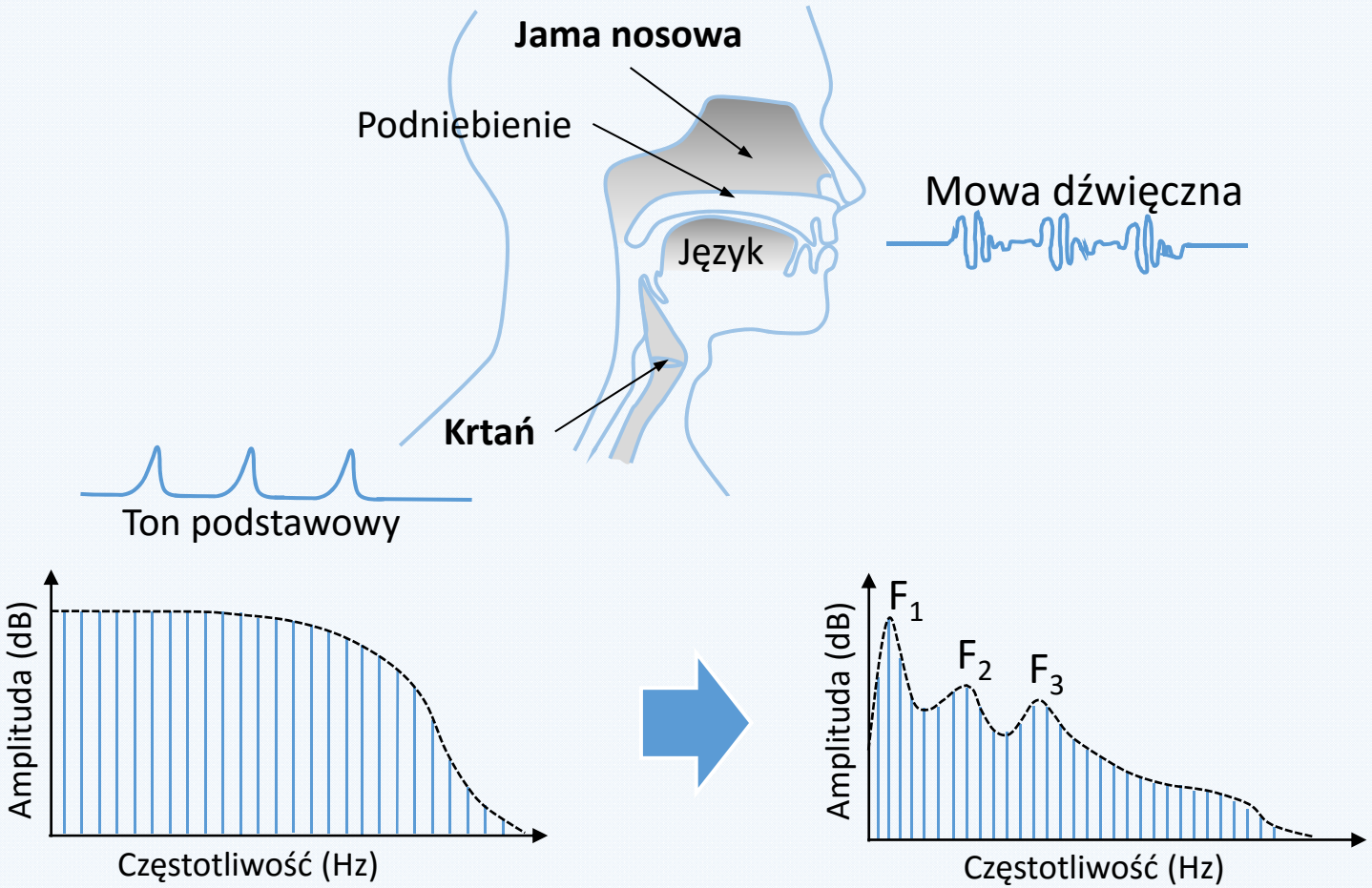
Budowa fizyczna kanału głosowego:

- wpływająca na pozycję, energię oraz kształt formantów głosowych
- kształt jamy nosowej wpływa na brzmienie głosek nosowych

Cechy behawioralne: idiolekt, dialekt, prozodia, nawyki mówcy



- **Krtań** – ton krtaniowy, fonacja, energia dźwięku
- **Jama ustna** – artykulacja, seria rezonansów związanych z kształtem jamy ustnej, pozycją artykulatorów (język, języczek, podniebienie, zęby, usta, jama nosowa)
- **Jama nosowa** – rezonans nosowy

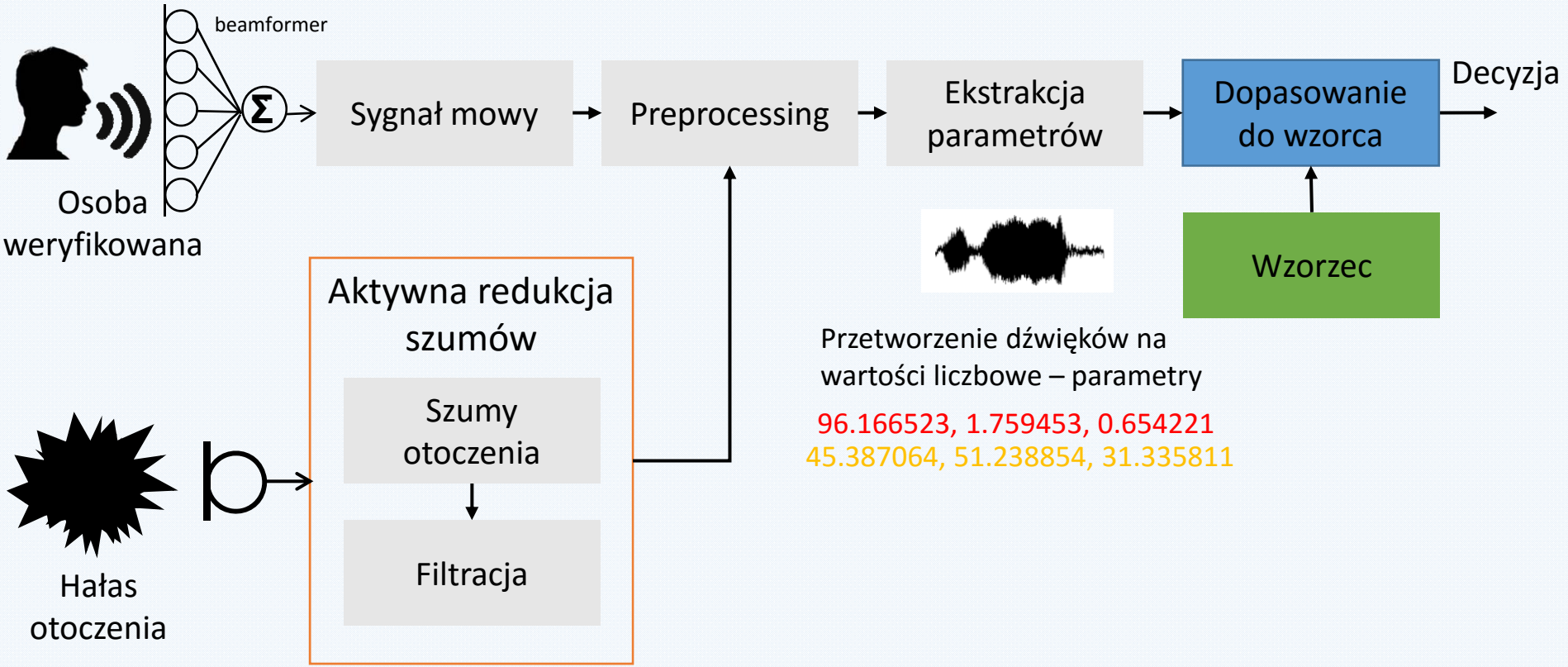


Systemy rozpoznawanie mówcy

- Zależne od treści (ang. *text dependent*)
  - Mówca w trakcie weryfikacji wypowiada znany zbiór lub podzbiór wyrazów (użytych w trakcie rejestracji w systemie)
  - Mówca jest świadomy, w którym momencie pobierana jest próbka głosu

- Niezależne od treści (ang. *text independent*)
  - Mówca w trakcie weryfikacji wypowiada dowolny ciąg wyrazów
  - Możliwa weryfikacja bez wiedzy osoby weryfikowanej

System rozpoznawania mówcy



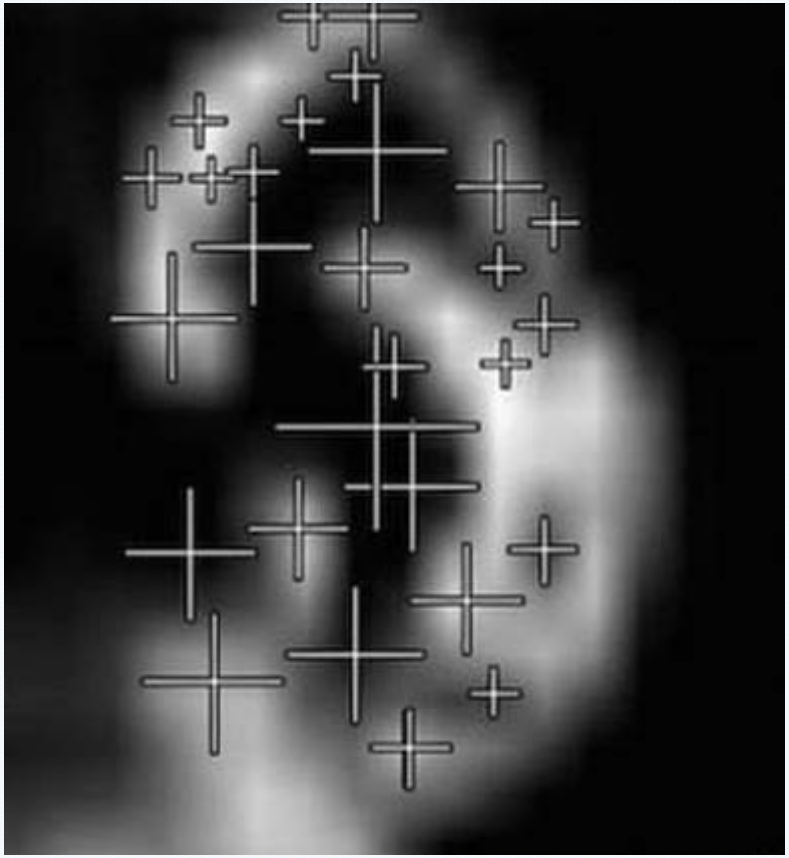
Biometria kształtu ucha

Własności ucha z punktu widzenia biometrii

- Unikalny kształt dla każdego człowieka
- Kształt nie ulega zmianie z wiekiem
- Indywidualny rozkład naczyń krwionośnych

Zalety biometrii kształtu ucha

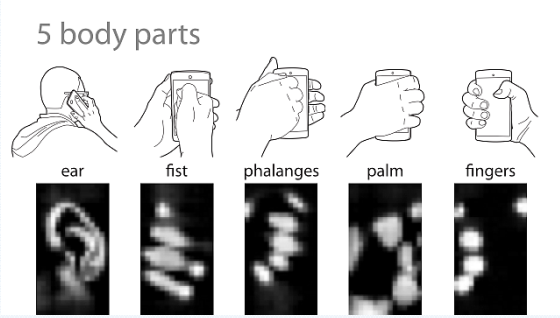
- Większa ochrona danych osobowych niż w przypadku weryfikacji na podstawie rozpoznawania twarzy
- Koszty elementów dokonujących akwizycji próbki biometrycznej niższe niż koszty czytników linii papilarnych
- Niewrażliwość na mimikę
- Duża precyja
- Bogactwo cech biometrycznych w przestrzeni 3D

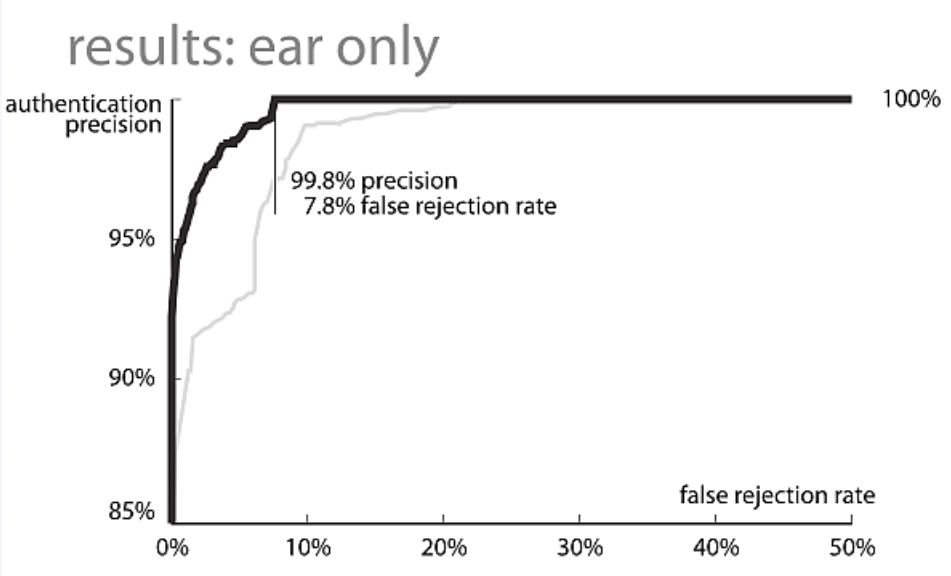


http://www.christianholz.net/bodyprint.html

Biometria kształtu ucha

- System Yahoo Labs Bodyprint
  - Uwierzytelnianie użytkownika telefonu poprzez przyłożenie ucha do powierzchni ekranu pojemnościowego
  - Rozdzielczość ekranu ~6 dpi
  - Testy z udziałem 12 uczestników
    - Dokładność identyfikacji = 99.8%
    - Poziom fałszywych odrzuceń = 7.8%

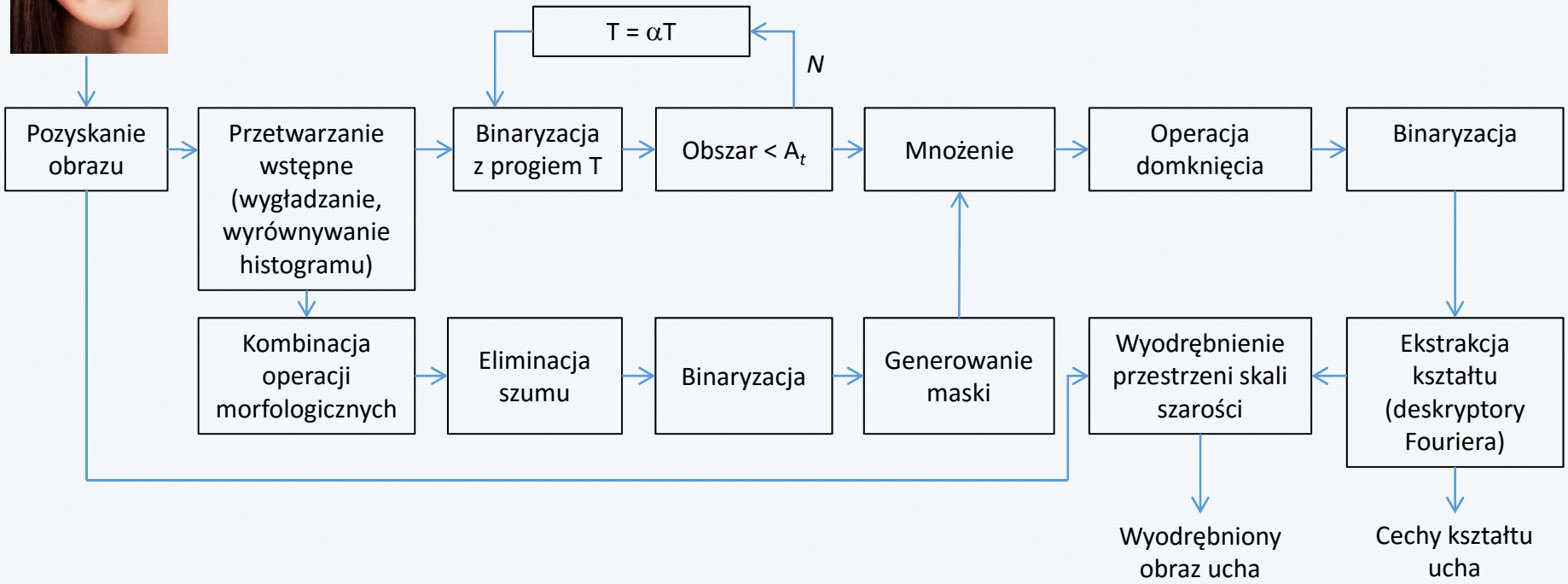




Biometria kształtu ucha

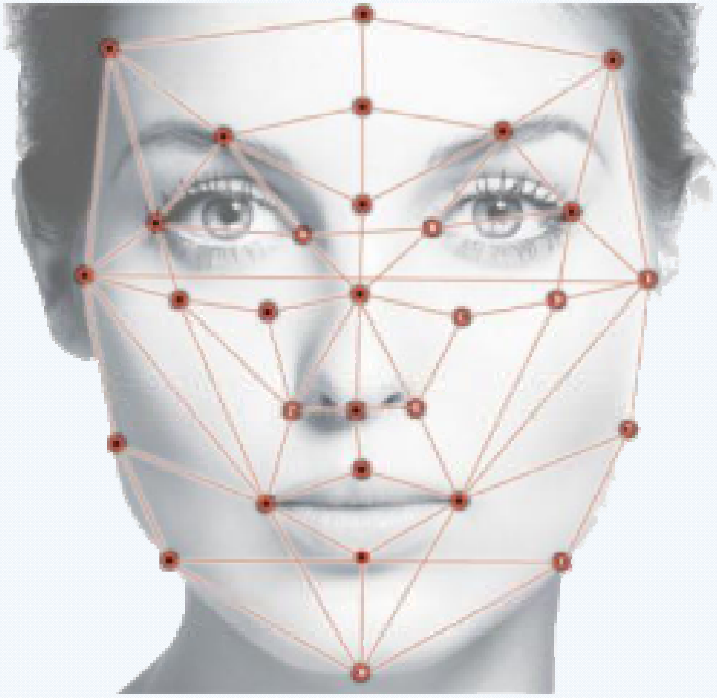
Wykorzystanie wizji komputerowej do pozyskiwania próbki biometrycznej kształtu ucha

Automatyczna segmentacja kształtu ucha



Biometria kształtu twarzy

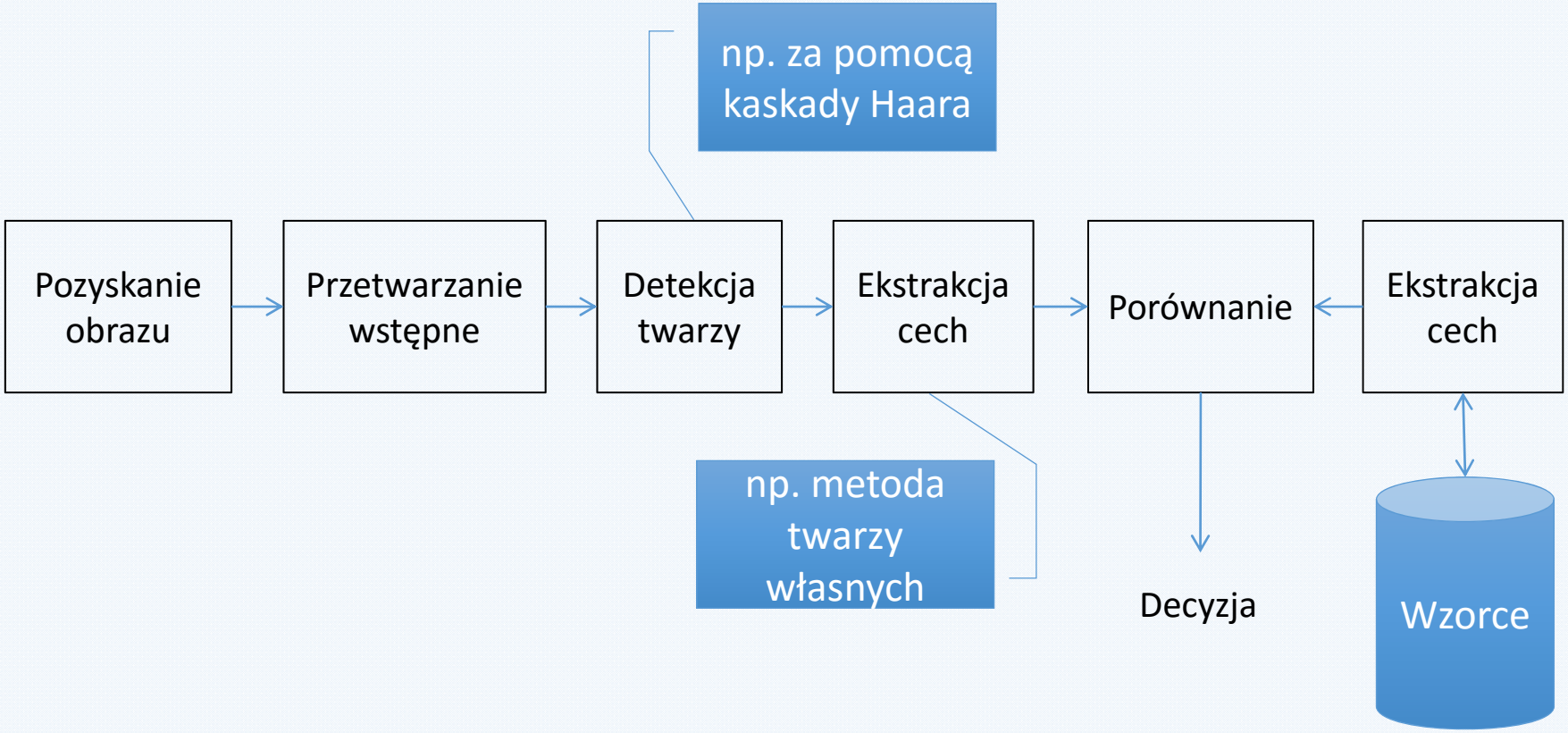
- Własności twarzy z punktu widzenia biometrii
  - Zależności pomiędzy poszczególnymi częściami twarzy nie ulegają znaczącym zmianom z wiekiem
  - Duża liczba cech biometrycznych
    - Cechy geometryczne: np. kształt brwi, kształt nosa, kształt ust, kształt podbródka
    - Cechy antropometryczne: np. odległość między środkami oczu, odległości pomiędzy oczami i nosem, odległość pomiędzy linią oczu i linią ust



http://functionspace.com/quartertopic/957/Face-Recognition

Biometria kształtu twarzy

Wykorzystanie wizji komputerowej w biometrii kształtu twarzy



Biometria chodu

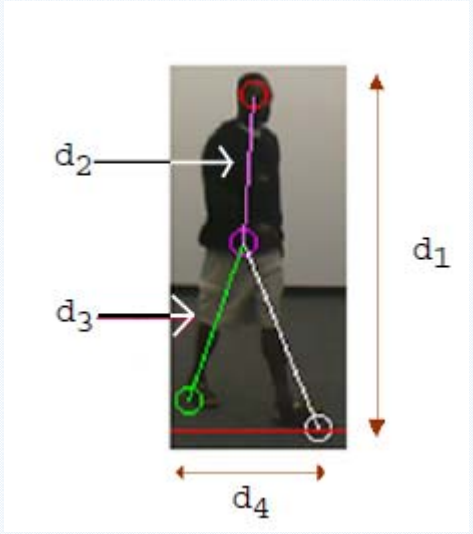
Polega na identyfikowaniu osobnika na podstawie sposobu poruszania się

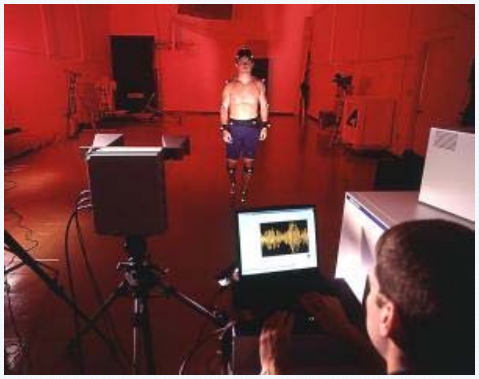
- zalety:
  - możliwość identyfikacji na odległość
  - osobnik nie musi wiedzieć o tym, że jest identyfikowany, co zmniejsza prawdopodobieństwo zmian zachowania wymuszonych pomiarem
  - trudno zamaskować maniery poruszania się (w porównaniu np. z pokazywaniem twarzy)
  - trudno naśladować czyjś chód
- wady
  - chód nie identyfikuje człowieka tak jednoznacznie jak np. odcisk palca

Biometria chodu

Dwie metody rozpoznawania chodu:

- w oparciu o analizę obrazu z kamer (np. monitoringu)
  - najczęściej obliczany jest model ruchu obiektu
- z użyciem radaru (analogicznego jak do pomiaru prędkości samochodów)
  - rejestrowany jest sposób poruszania się poszczególnych części ciała
  - rzadziej używany





Gait Recognition: Screening From a Distance May Offer Earlier Detection and Quicker Response

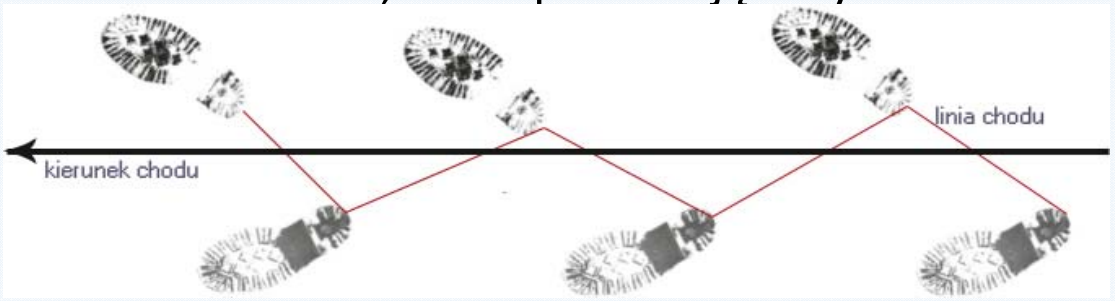
Metody analizy chodu

Wykrywanie ruchomego obiektu (np. z użyciem *Gaussion Mixture Models*)

- lokalizacja części ciała (np. głowa, biodra)
- analiza parametrów, np. wzajemnego położenia głowy i nóg, ocena kątów nachylenia

Analiza ichnogramu – ścieżki chodu

- dzięki porównywaniu kierunku i linii chodu, długości i szerokości kroku oraz sposobie ułożenia stopy możliwe jest identyfikowania osób
- badania pokazują, że około 80% ludzi ma stopy z wrodzonymi lub nabytymi zniekształceniami, które powodują indywidualne zmiany w chodzie



Tafazzoli F., Bebis G., Louis., Hussain M., Genetic feature selection for gait recognition, Journal of Electronic Imaging, Volume 24, 2015.

Biometria naczyń krwionośnych dłoni

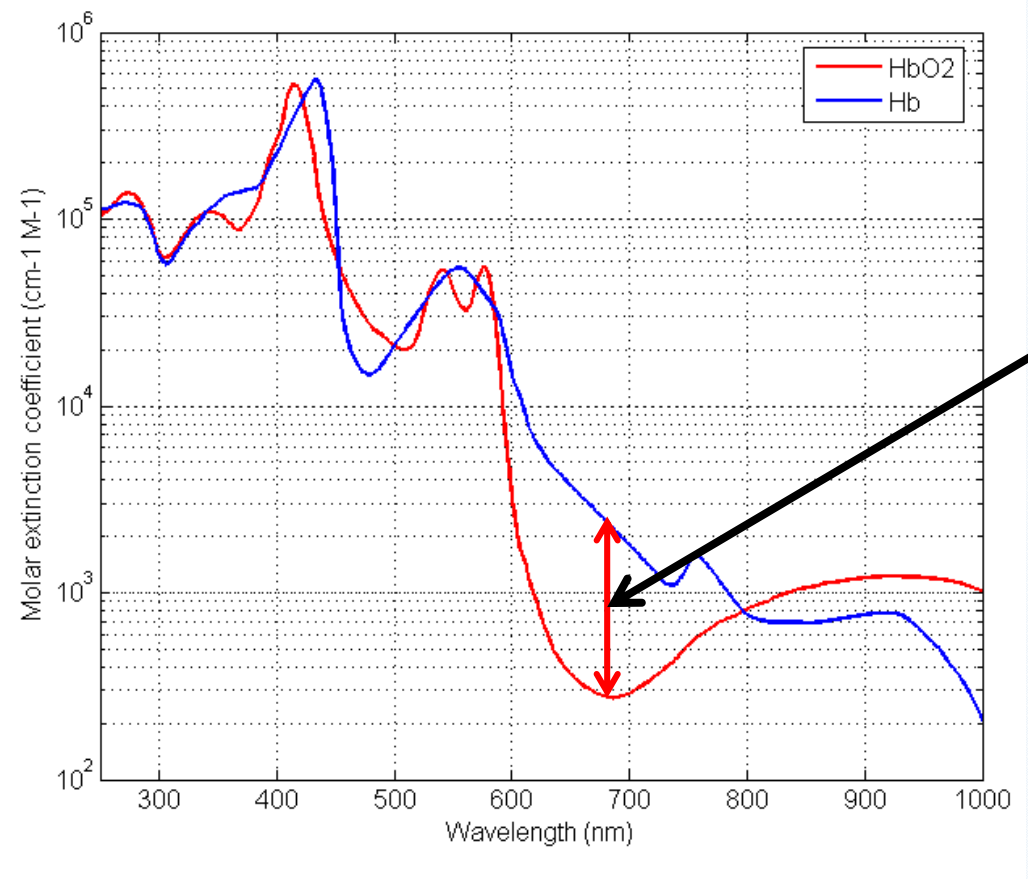
- Analiza rozkładu naczyń krwionośnych dłoni
- Cecha biometryczna ukryta pod powierzchnią skóry dłoni
- Osobniczy rozkład naczyń krwionośnych
- Cecha stabilna od 18 roku życia
- Możliwość nieinwazyjnej analizy z wykorzystaniem podczerwieni
- Wykorzystanie efektu absorpcji fal podczerwonych przez komórki ciała/skórę/tłuszcz/hemoglobinę

RGB

IR

Wzorzec Biometryczny

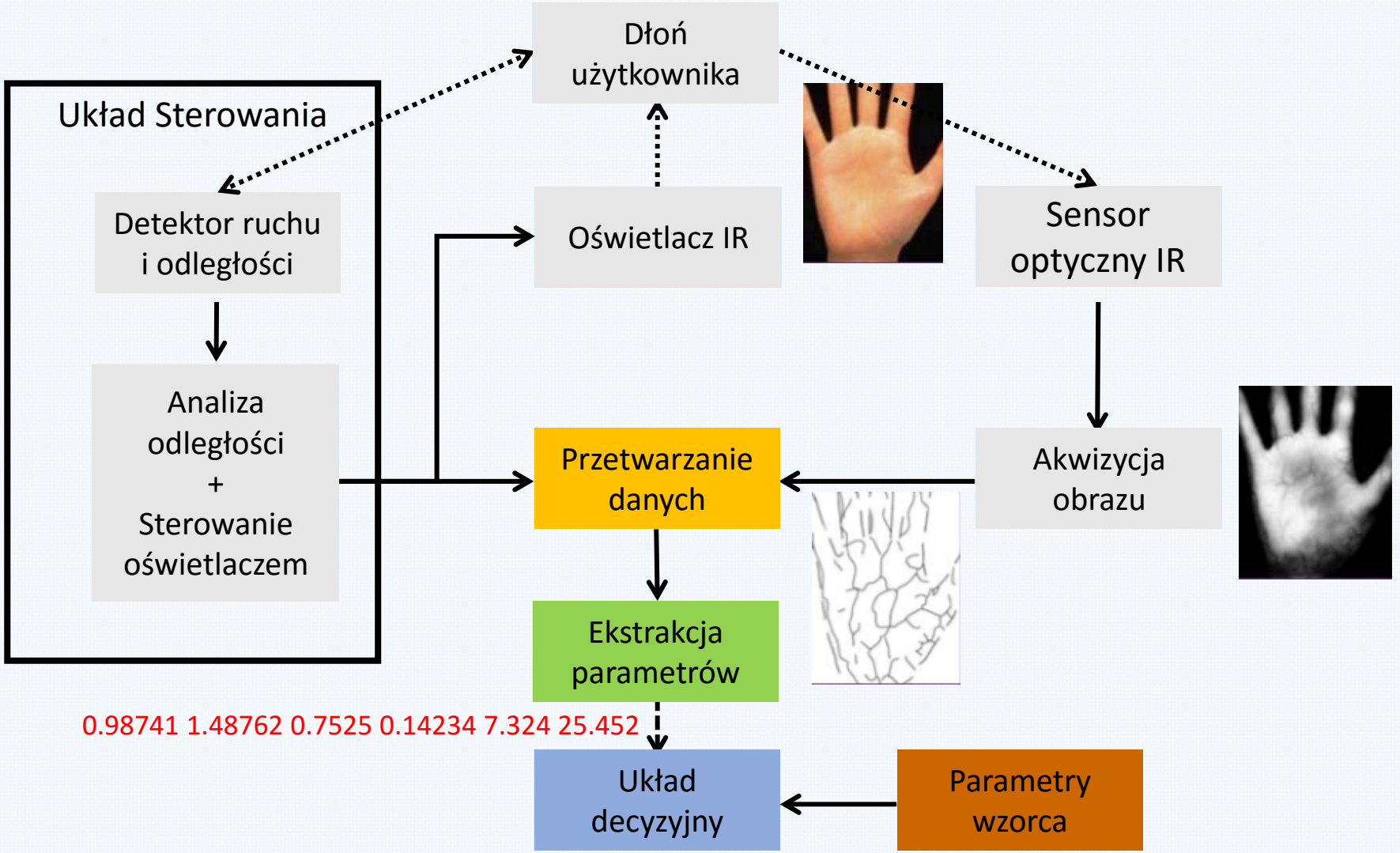
Biometria naczyń krwionośnych dłoni



wzrost absorpcji fal podczerwonych (600nm – 700nm) przez hemoglobinę nasyconą tlenem

http://upload.wikimedia.org/wikipedia/commons/thumb/c/c0/HbAbs_v3.png/300px-HbAbs_v3.png

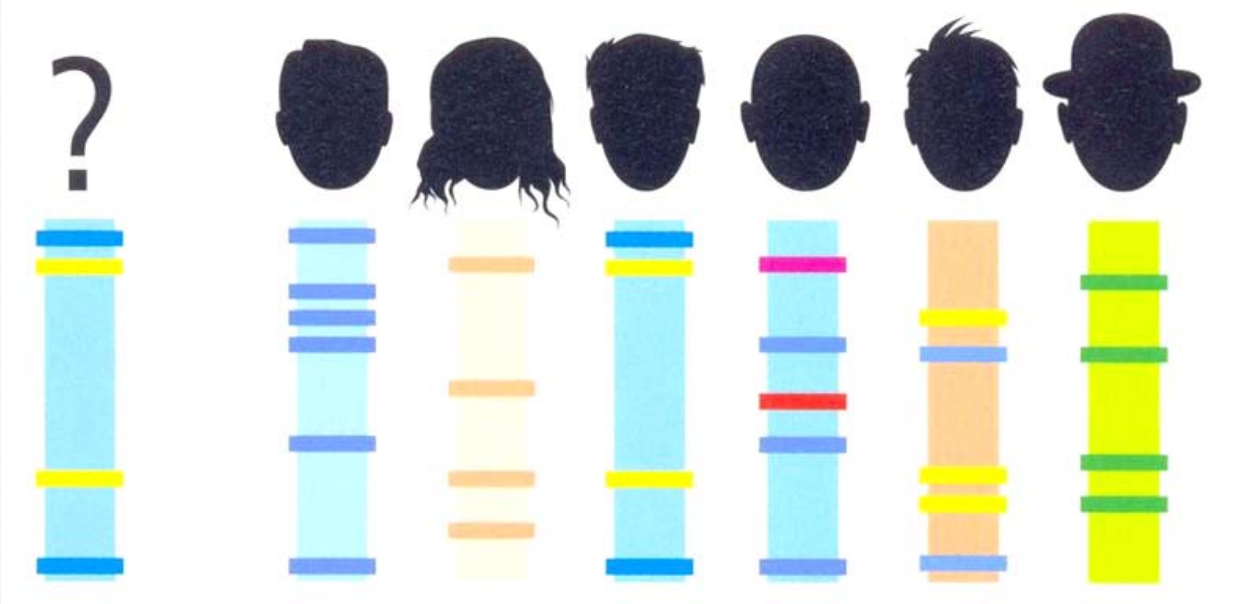
Biometria naczyń krwionośnych dłoni



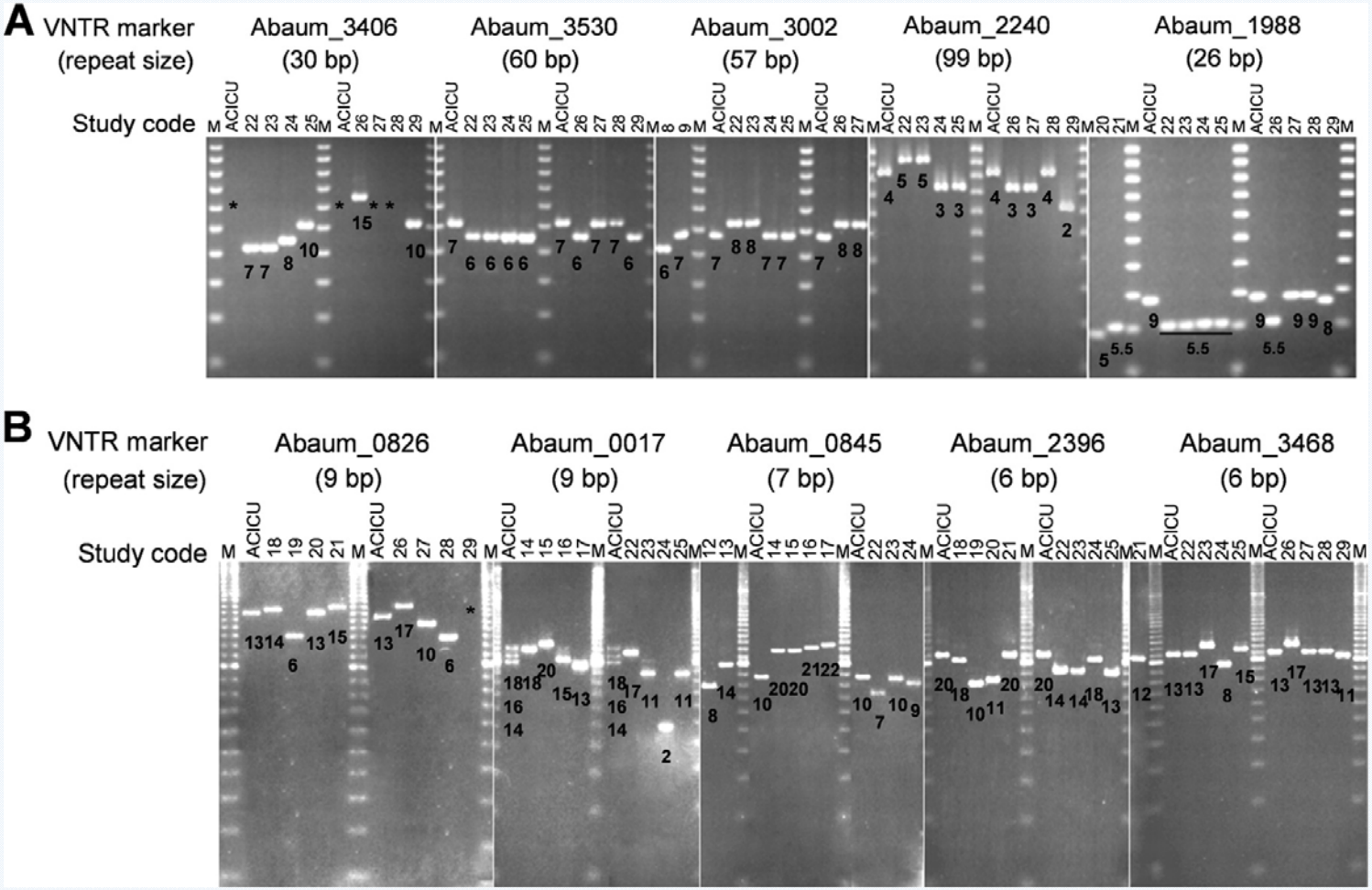
Badanie DNA

DNA w biometrii to jedno z głównych narzędzi kryminalistyki

- Blisko 3 miliony elementów DNA definiują różnice międzyosobnicze
- Różnicowanie polega na badaniu polimorfizmu sekwencji i ich długości
- Cechy biometryczne to liczby powtórzeń konkretnych sekwencji nukleotydów (tzw. VNTR – Variable Number Tandem Repeats)



Przykład rzeczywistego wyniku badań markerów DNA



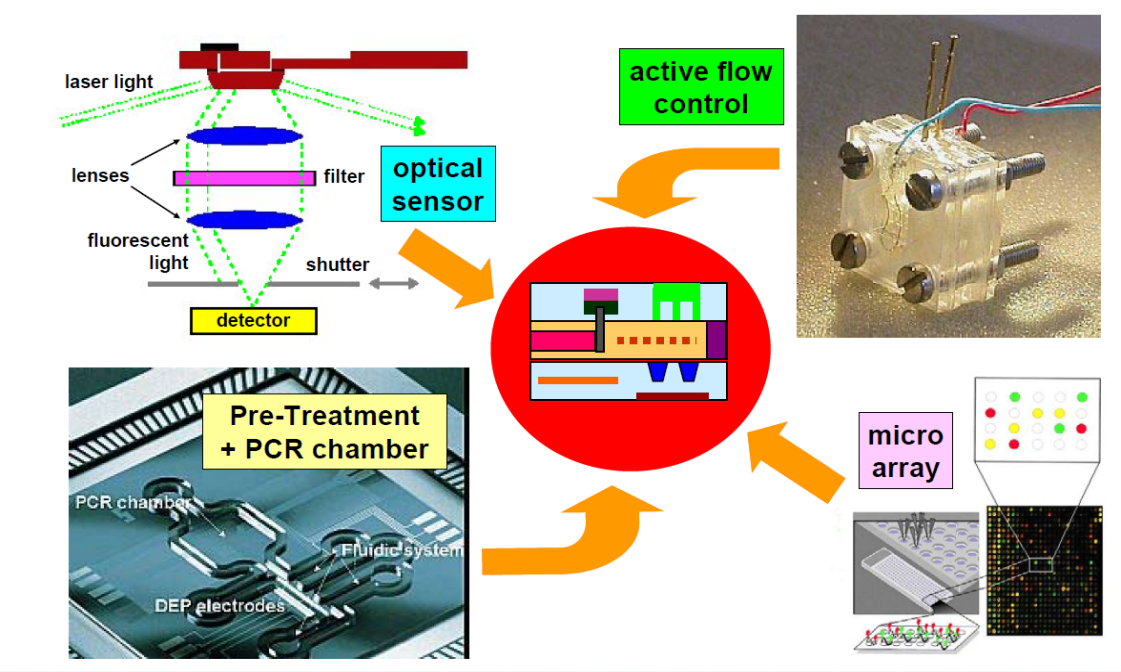
Badanie DNA

- FBI używa 13 lokalizacji z których odczytywane są sekwencje, co daje szansę przypadkowej zgodności na poziomie $0{,}0000000001 = 10^{-10}$

- Główną wadą tej metody jest konieczność posiadania namacalnej próbki do badań, a co za tym idzie łatwość kradzieży lub podrzucenia innych próbek.
- Metodę trudno także zastosować w innym obszarze poza kryminalistyką, ze względu na ogromną ilość informacji dodatkowej jaką niesie DNA, co mogłoby prowadzić do nadużyć

Smart BioMems

- Układ elektro-mechaniczny wykorzystywany do sekwencjonowania genów
- Umożliwia wykrycie błędnych mutacji genów prowadzących do chorób (np. rak)



Development of an Integrated MEMS-based DNA Analysis Chip with Active Flow Control Components for Space Applications, G. Vezzani, D. Palmieri, F. Lagasco, D'Appolonia S.p.A Via Paolo di Dono 223, 00142 Rome, Italy

Kierunki rozwoju biometrii

Biometrię cechuje powszechność, trudność i nieopłacalność fałszowania, wygodny i tani pomiar oraz niezmienność w czasie.

Dzięki swojej innowacyjności może wyprzeć z użycia „klucze dostępu” o charakterze zarówno fizycznym (klucze, karty magnetyczne) jak i logicznym (PIN, token, hasło sms) lub je uzupełnić (a co za tym idzie zabezpieczyć)

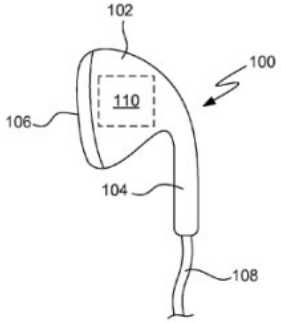
Biometria to coś, co mamy zawsze przy sobie, coś co wiemy, czego nie można zgubić, zapomnieć czy nie da się nam tego ukraść.

Każdy człowiek jest indywidualnym, niepowtarzalnym hasłem.

Kierunki rozwoju biometrii

- Miniaturyzacja technologii umożliwia umieszczanie czujników biometrycznych w przedmiotach codziennego użytku, by ułatwić procesy autoryzacji, oraz identyfikować użytkownika

Firma Apple umieściła skaner linii papilarnych w smarfonie, a także zgłosiła patent na słuchawki z czujnikiem biometrycznym



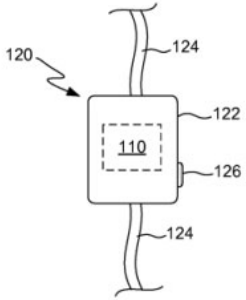


FIG. 1B

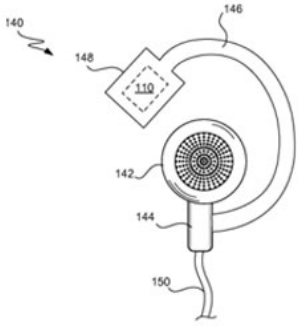


FIG. 1C

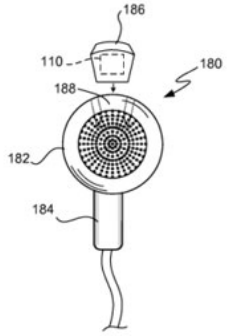
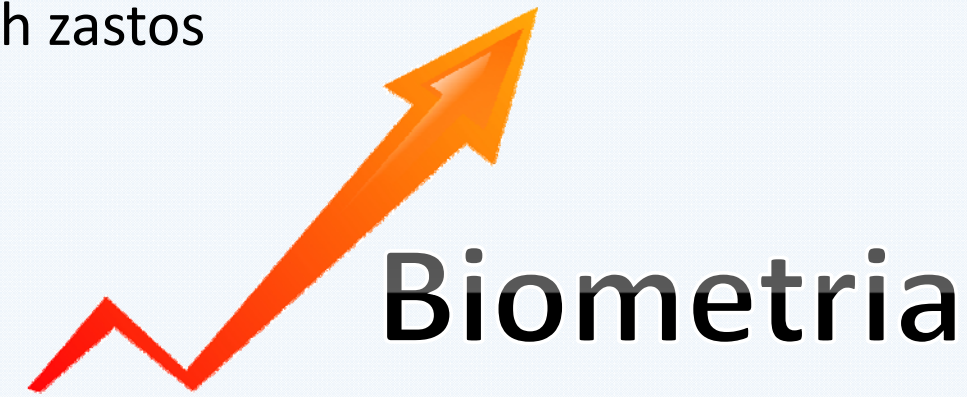


FIG. 1E

Podsumowanie

- Biometria jest bardzo szybko rozwijającą się dziedziną
- Liczne badania potwierdzają, że użytkownicy są gotowi korzystać powszechnie z metod biometrycznych pod warunkiem, że zwiększy to ich bezpieczeństwo
- Obecny rozwój technologiczny umożliwia skorzystanie z wielu metod biometrycznych, dostosowanych do potrzeb użytkowników
- Skuteczność metod biometrycznych stale wzrasta, zwiększając obszar możliwych zastos



Literatura

- Nixon K.A., Aimale V., Rowe R.K., Spoof Detection Schemes, Handbook of Biometrics, Springer, 2007.
- Bobick A.F., Johnson A.Y., Gait Recognition Using Static, Activity-Specific Parameters, Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001.
- White paper Fujitsu Identity Management - Palm Secure: http://www.fujitsu.com/global/solutions/business-technology/security/palmsecure/
- Pourcel, C., Minandri, F., Hauck, Y., D'Arezzo, S., Imperi, F., Vergnaud, G. & Visca, P., Identification of variable-number tandem-repeat (VNTR) sequences in Acinetobacter baumannii and interlaboratory validation of an optimized multiple-locus VNTR analysis typing scheme. J Clin Microbiol 49, 539–548, 2011
- Benesty, J., Sondhi, M., Huang Y., Springer Handbook of Speech Processing, Springer-Verlag Berlin Heidelberg, pp. 725-782, 2008.

POLITECHNIKA GDAŃSKA

Dziękuję za uwagę