Biometryczna Identyfikacja Tożsamości

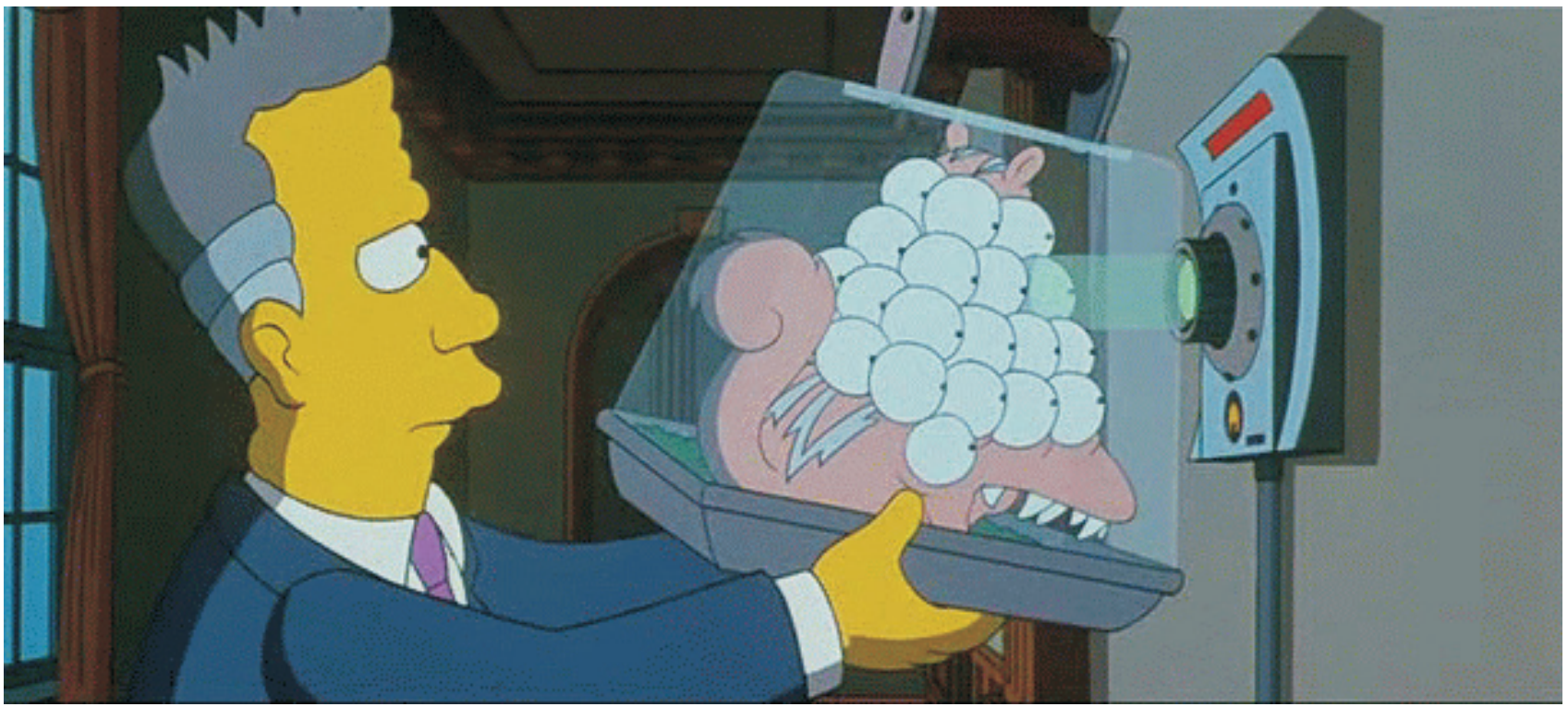
Wykład 5: Bezpieczeństwo sensorów

Adam Czajka

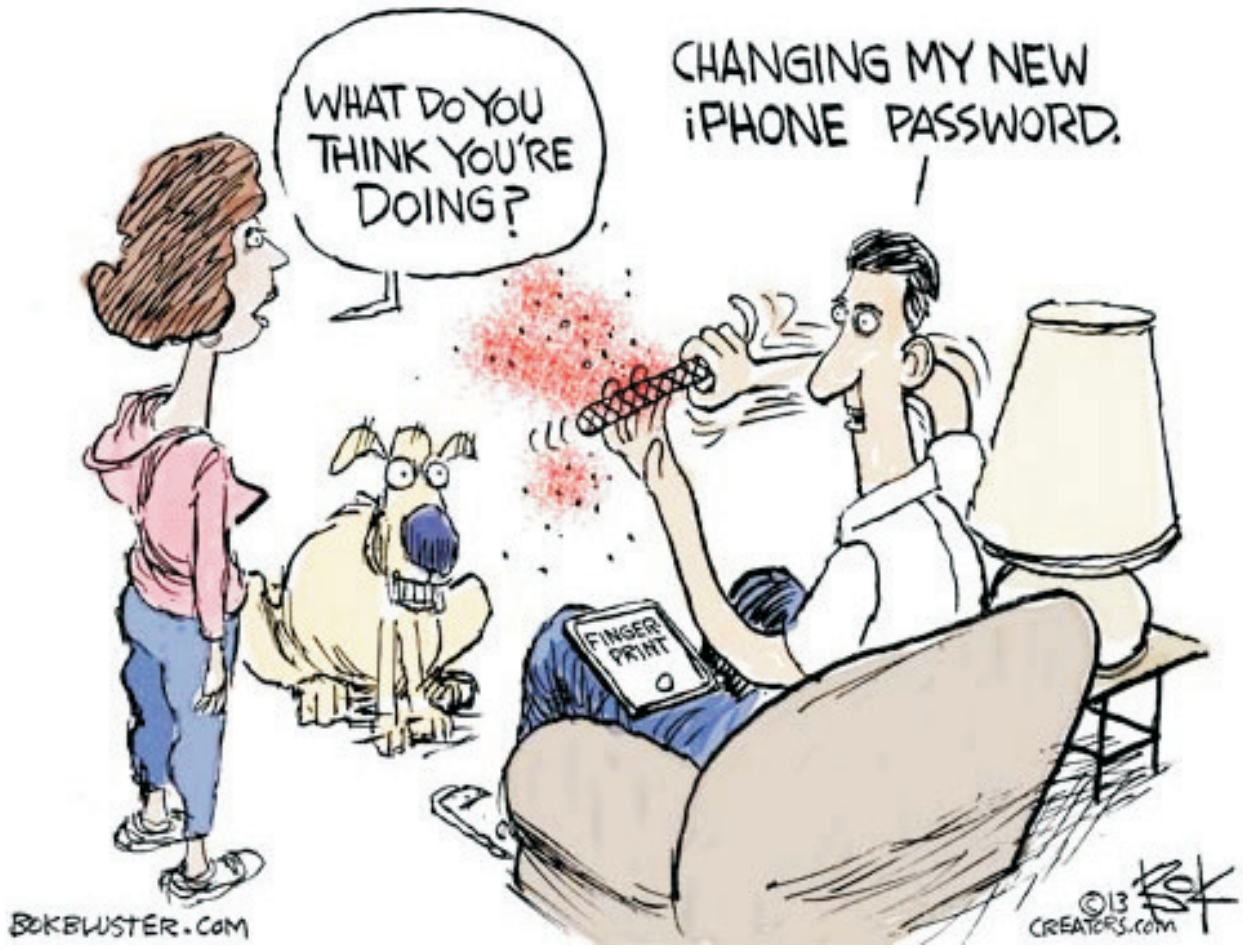
Wykład na Wydziale Elektroniki i Technik Informacyjnych
Politechniki Warszawskiej

Semestr letni 2015

Czy możemy zastąpić czymś charakterystykę biometryczną?



Czy możemy zmienić naszą charakterystykę biometryczną?



Wykład 5: Bezpieczeństwo sensorów

- Podatność biometrii na ataki
- Podatność sensorów biometrycznych na ataki
- Testowanie żywotności palca
- Testowanie żywotności oka

Wykład 5: Bezpieczeństwo sensorów

Podatność biometrii na ataki

Podatność sensorów biometrycznych na ataki

Testowanie żywotności palca

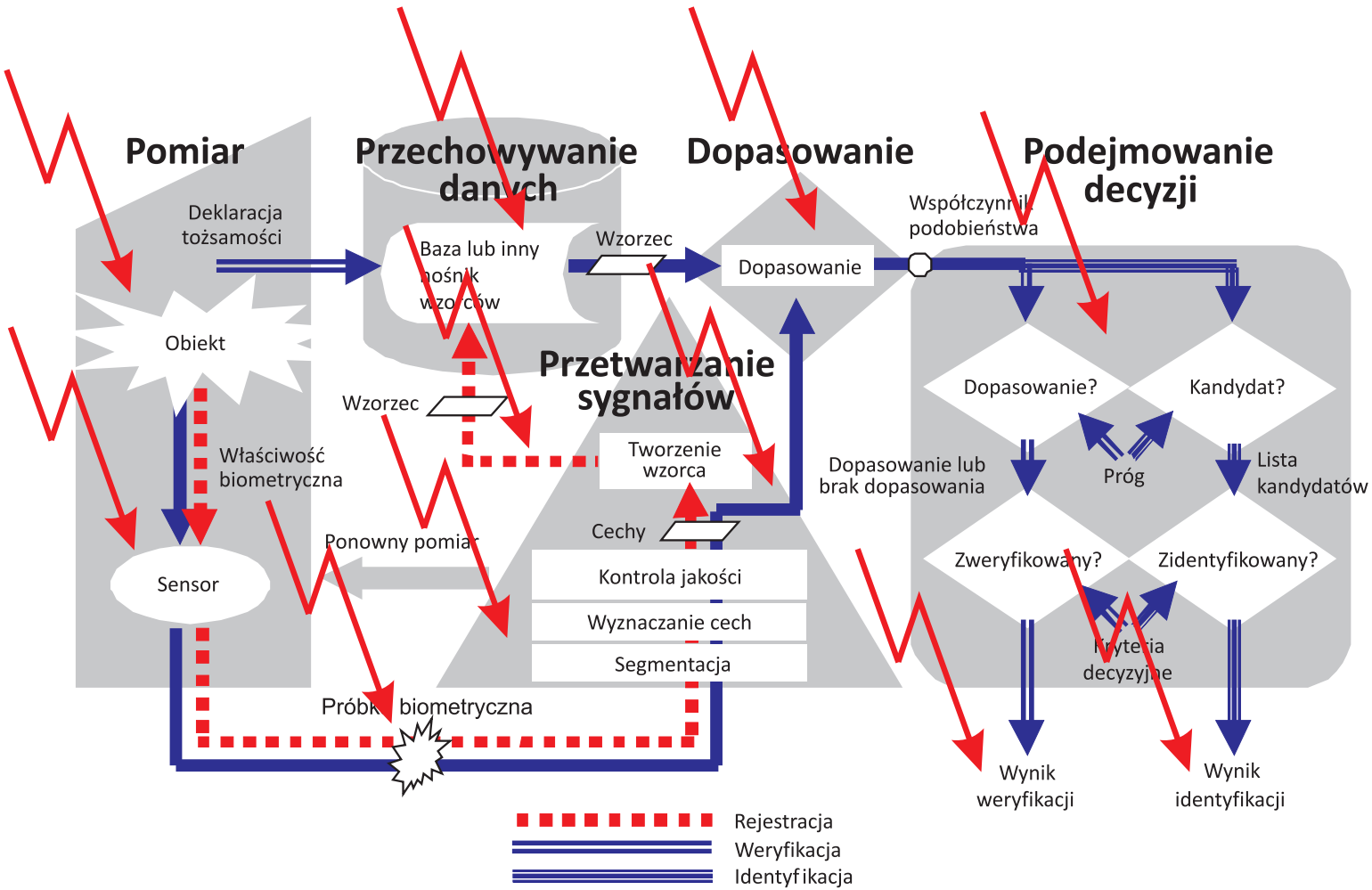
Testowanie żywotności oka

Zagrożenia

1. Ograniczona dokładność biometrii
   (dotyczy w szczególnościwspółczynnika FMR)
2. Wykorzystanie imitacji charakterystyki biometrycznej
   (poważne gdy czytnik nie sprawdza żywotności obiektu)
3. Modyfikacja charakterystyki biometrycznej
   (trudne do wykrycia za pomocą testów żywotności)
4. Wykorzystanie syntetycznych danych biometrycznych
   (nie muszą przypominać danych autentycznych charakterystyk biometrycznych)
5. Kradzież charakterystyk lub danych biometrycznych
   (prezentacja w niezmienionej formie, prezentacja pod przymusem)
7. Błędy proceduralne procesu rejestracji (niska jakość próbek rejestracyjnych lub błędne ich oznaczenie)
8. Działanie w nieprzyjaznym środowisku

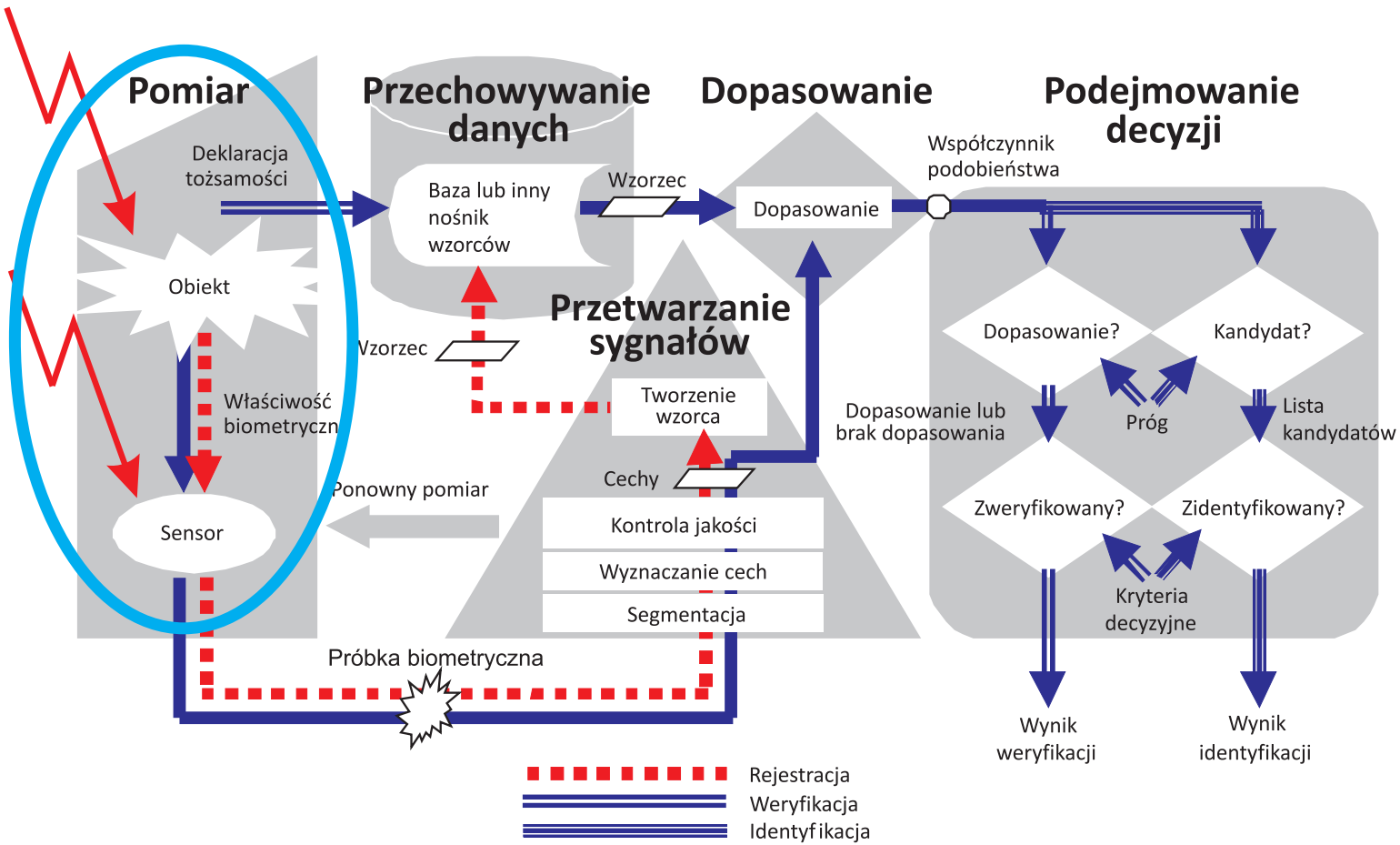
Podatność biometrii na ataki

System biometryczny wg ISO/IEC 19794-1:2011



Podatność biometrii na ataki

System biometryczny wg ISO/IEC 19794-1:2011



Wykład 5: Bezpieczeństwo sensorów

Podatność biometrii na ataki
Podatność sensorów biometrycznych na ataki
Testowanie żywotności palca
Testowanie żywotności oka

Imitacje wykorzystywane w laboratoriach IAiIS PW oraz NASK

Forma z modeliny

Magnetyczny proszek daktyloskopijny

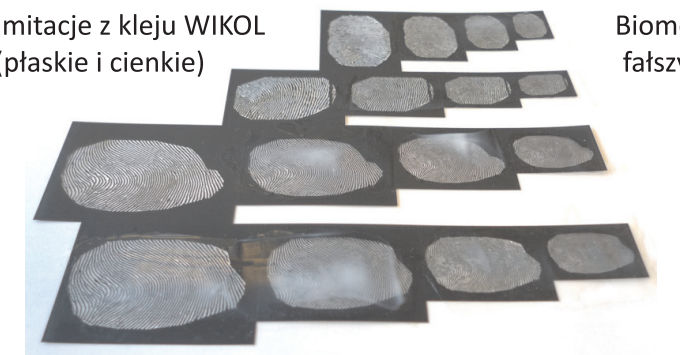
Odcisk utajony w świetle widzialnym

Odcisk utajony w świetle ultrafioletowym

Obraz biometryczny

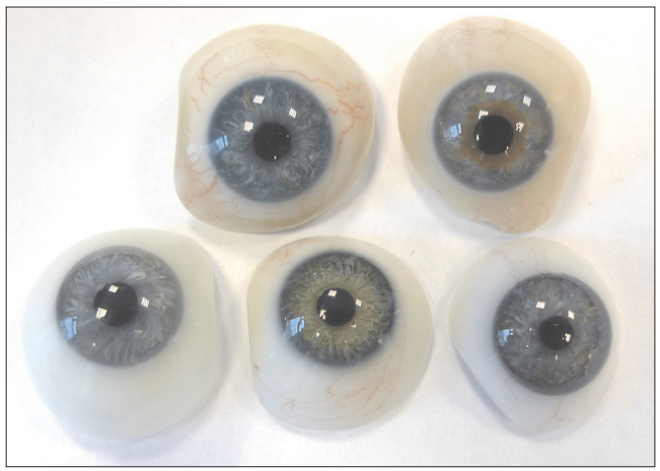
Imitacje z silikonu, kleju lub żelatyny (3D)

Imitacje z kleju WIKOL (płaskie i cienkie)

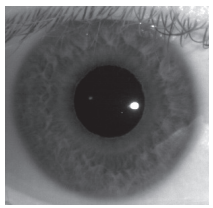


Biometryczny obraz fałszywego odcisku

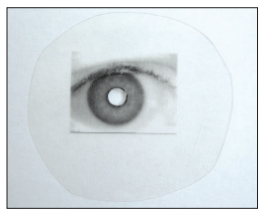
Imitacje wykorzystywane w laboratoriach IAiIS PW oraz NASK



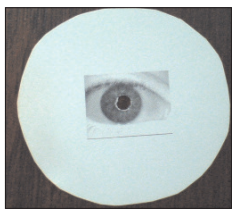
Modele oka (protezy)



Obraz biometryczny autentycznej tęczówki



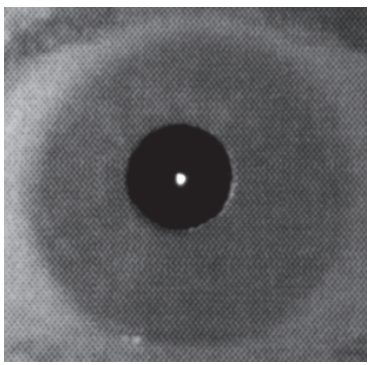
Wydruk na folii



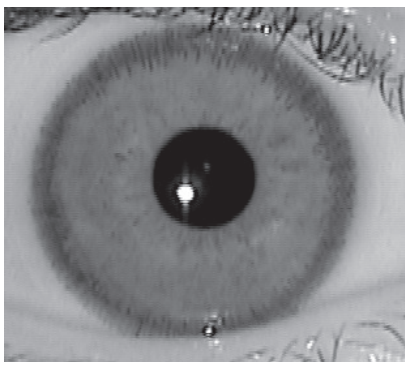
Wydruk na papierze

Obrazy biometryczne falsyfikatów:

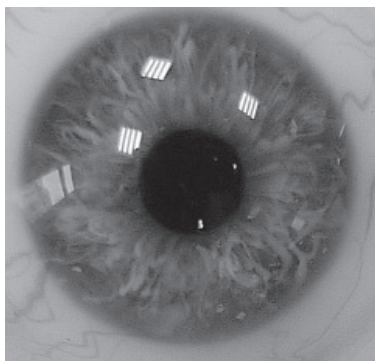
Wydruk papierowy



Wydruk na szkle kontaktowym



Model oka (proteza)



Przykłady

iPhone 6 (2014) i iPhone 5s (2013)

Przykłady

System kontroli czasu pracy w Brazylii (2013)

Brazilian docs fool biometric scanners with bag full of fake fingers

Some fingerprint scanners aren't very discerning.

by **Lee Hutchinson** - Mar 13 2013, 4:35pm

HACKING 60

The BBC is one of several outlets carrying the bizarre story of a Brazilian doctor arrested for allegedly defrauding her employer, a hospital in the town of Ferraz de Vasconcelos, near São Paulo. At the time of her arrest, she was equipped with a total of sixteen fingers—ten of which God gave her, and six of which were crafted of silicone and given to her by coworkers. At least three of the extra fingers bore the prints of fellow doctors at the hospital.

Six silicone fingers, all in a row.

BBC

The doctor, Thaune Nunes Ferreira, 29, claims through her attorney that she was forced to use the silicone fingers to clock in to the hospital's time card system in order to cover for absentee colleagues. "She says she was innocent because it is a condition they imposed on her to keep her job," the attorney notes.

Źródło: http://arstechnica.com

Przykłady

System kontroli granicznej w Japonii (2010)

Japanese biometric border fooled by tape

Published 29 January 2010

Two South Korean women have managed to fool Japan's expensive biometric border-control system by using special tapes on their fingers; the invisible tape carries the finger prints of another person, and the South Korean broker who supplied the tape also provided false passports to go with it; this is the third known case of South Korean women using the fingerprint-altering tape to enter Japan; in all three cases, the women managed to fool the biometric screening, but were later caught because they over-stayed their visas

Japan's million-dollar biometric immigration screening systems are still no match for a little ingenuity — and some tape. Austin Modine writes that two South Korean women have been arrested on suspicion of bypassing a cutting-edge fingerprint reading machine and illegally entering Japan by using special tape bearing the fingerprints other people.

The women slipped past the immigration process at Tokyo's Haneda airport in May and October 2008, according to *the Japan Times*. The two had reportedly laid low as nightclub hostesses, but were spotted after both received deportation orders in 2008 for overstaying their visas and had their fingerprints taken again.

Japan's biometric immigration system was installed in thirty airports in 2007 to improve security by keeping terrorists and foreigners with deportation records away. The country spent more than 4 billion yen ($44 million, £27 million) on the devices, which cross-check visitors' fingerprints with a database of fugitives and lawbreakers.

Źródło: HomelandSecurityNewswire.com

Przykłady

Testy uniwersytetów i niezależnych instytucji (2002→)

1. Fraunhofer Research Institute & German Federal Institute for IT Security (2002)
   - komercyjne biometrie twarzy, odcisku palca i tęczówki
   - wydruki twarzy, ruchome twarze, wydruki oka, odciski ujawniane z urządzeniach (chronionych tymi odciskami)
2. Yokohama National University (2004→)
   - komercyjne biometrie odcisku palca, tęczówki i żył
   - papierowe wydruki oka, imitacje odcisków z żelatyny i silikonu, warzywa i tworzywa polimerowe jako sztuczne palce
3. NASK & Politechnika Warszawska (2004→)
   - komercyjne biometrie odcisku palca i tęczówki
   - papierowe wydruki oka, protezy oka, imitacje odcisków z kleju WIKOL, żelatyny, gumy guar, silikonu

Przykłady

Eksperyment T. Matsumoto, 2004 r. (odcisk palca)

1. Źródła falsyfikatów
   - żywy palec, zdjęcie palca, odciski utajone
2. Rodzaje nośników
   - żelatyna, silikon, silikon z domieszką grafitu
3. Modele: 2D i 3D
4. Testowane systemy: 11 systemów od 9 producentów
   - dwa systemy instalowane w telefonach komórkowych
   - dwa systemy oferowały "test żywotności"
   - optyczna i pojemnościowa technika pomiaru

Przykłady

Eksperyment T. Matsumoto, 2004 r. (odcisk palca)

5. Wyniki
   - wszystkie systemy zaakceptowały żelatynowe falsyfikaty
   - 5/11 systemów zaakceptowało silikonowe falsyfikaty
   - 9/11 systemów zaakceptowało falsyfikaty silikonowe z domieszką grafitu
   - czytniki instalowane w telefonach komórkowych zostały oszukane falsyfikatami wykonanymi z wykorzystaniem odcisków utajonych pozostawionych na tych telefonach

Przykłady

Eksperyment T. Matsumoto, 2004 r. (tęczówka)

1. T. Matsumoto, *Biometrics 2004 Exhibition and Conference*, październik 2004, Londyn
   - wydruk tęczówki: kolorowa drukarka laserowa, obraz pobrany przez kamerę Panasonic ET100 oraz przez mikroskop cyfrowy działający w zakresie podczerwieni
   - testowane systemy: OKI IrisPass-h, Panasonic Authenticam ET100, OKI IrisPass-WG
   - rejestracja: jedynie OKI IrisPass-WG nie zaakceptował wydruków
   - weryfikacja: **wszystkie** kamery zaakceptowały wydruki

Przykłady

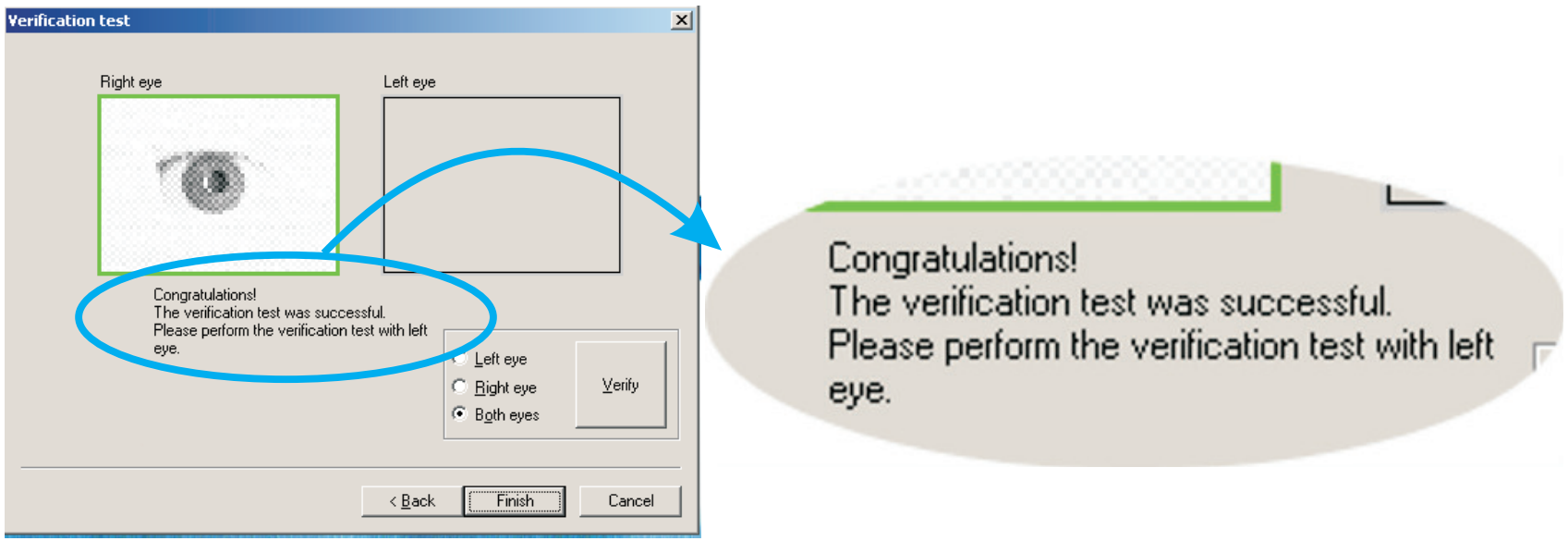
Eksperymenty PW/NASK, 2005 r. (tęczówka)

2. A. Czajka, A. Pacut, "Iris aliveness detection", *BioSec 2nd Workshop*, Bruksela, 20 stycznia 2005
   - wydruk tęczówki: obrazy pobrane kamerą IrisCUBE, wydruk laserowy, atramentowy oraz odbitka fotograficzna
   - testowano dwa komercyjne systemy rozpoznawania tęczówki
   - weryfikacja: **wszystkie** kamery zaakceptowały wydruki (System A: 73,1%, System B: 15,6%)

Przykłady

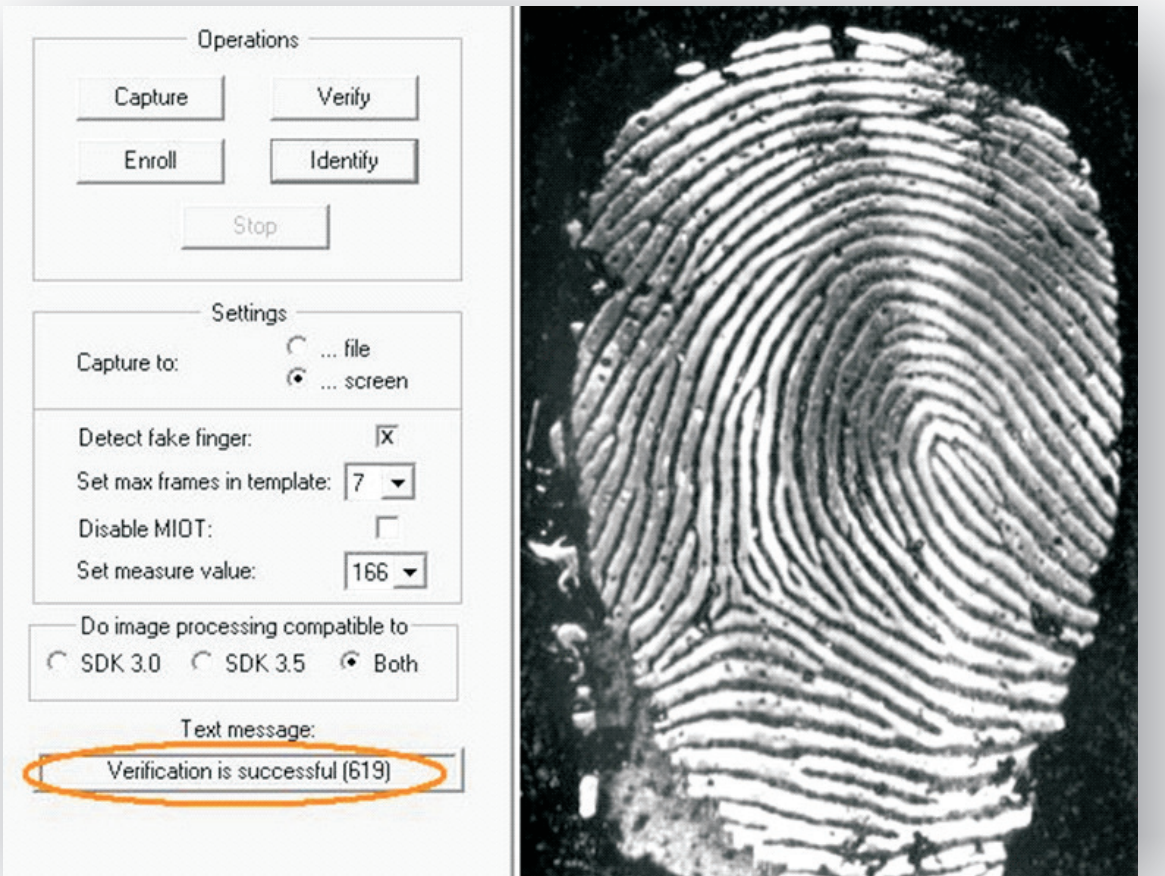
Eksperymenty PW/NASK, 2008 r. (tęczówka)

Wynik działania przykładowego systemu dostępnego na rynku (zakupionego w lutym 2008 r.): czas udanej weryfikacji wydruku oka krótszy (!) niż czas weryfikacji oka żywego



Przykłady

Eksperymenty PW/NASK, 2008 r. (odcisk palca)



Przykłady

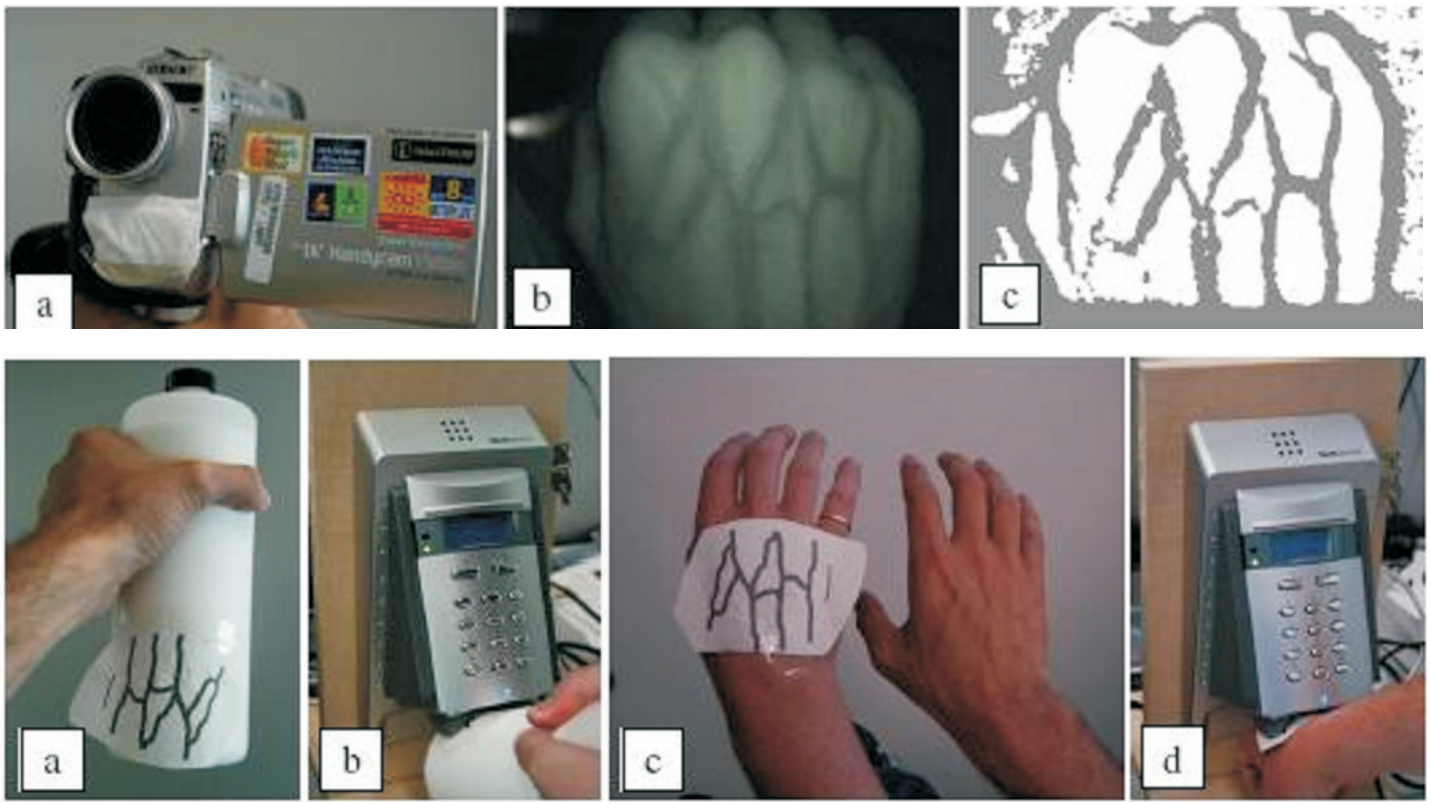
Eksperymenty FIDIS, 2006 r. (żyły dłoni)

FIDIS (*Future of Identity in the Information Society*, `www.fidis.net`), EU Network of Excellence, publikacja w styczniu 2006

- wydruk układu żył na papierze
- nośniki: butelka, rękawiczki silikonowe, żywa ręka
- udane próby weryfikacji pomimo uaktywnienia testu żywotności

Przykłady

Eksperymenty FIDIS, 2006 r. (żyły dłoni)



źródło: State of the Art Biometrics Excellence Roadmap, MITRE Tech. Rep., Vol. 1, 2008

Przykłady

Eksperymenty T. Matsumoto, 2007 r. (żyły palca)

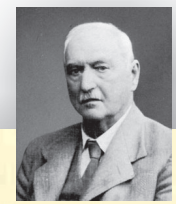
Rejestracja (R) / Weryfikacja (W)	Poziom akceptacji (R/W, %)	Uwagi
A / A	91 / 100	normalne warunki użytkowania
F1 / F1	100 / 100	rzodkiew japońska, R i W tego samego dnia
F2 / F2	98 / 100	rzodkiew japońska, W tydzień po R
F3 / F3	100 / 100	sztuczny śnieg
A / F4 F4 / A	98 (W)	λ=910 nm, wydruk na folii pięciowarstwowy, 192 dpi

Źródło: T. Matsumoto, How to measure security of embedded black-box systems, 9th Global Business Dialog on Electronic Commerce Summit, 9 November 2007, Tokyo, Japan

Oszustwo biometryczne wplecione w fabułę kryminału

R. Austin Freeman, "The Red Thumb Mark", 1907 r.

- idea fałszowania odcisku palca (utajonego)
- odcisk w formie z gliny lub wosku + odlew żelatynowy
- fotografia palca + chromowanie modelu z żelatyny (niechromowane grzbiety pozostawiają ślady po nawilżeniu modelu)



168 THE RED THUMB MARK

"I understand, then," pursued Anstey, "that you consider the [illegible] print, which has been sworn to as the prisoner's, to be a forgery?"

"Yes. It is a forgery."

"But is it possible to forge a thumb-print or a finger-print?"

"It is not only possible, but quite easy to do."

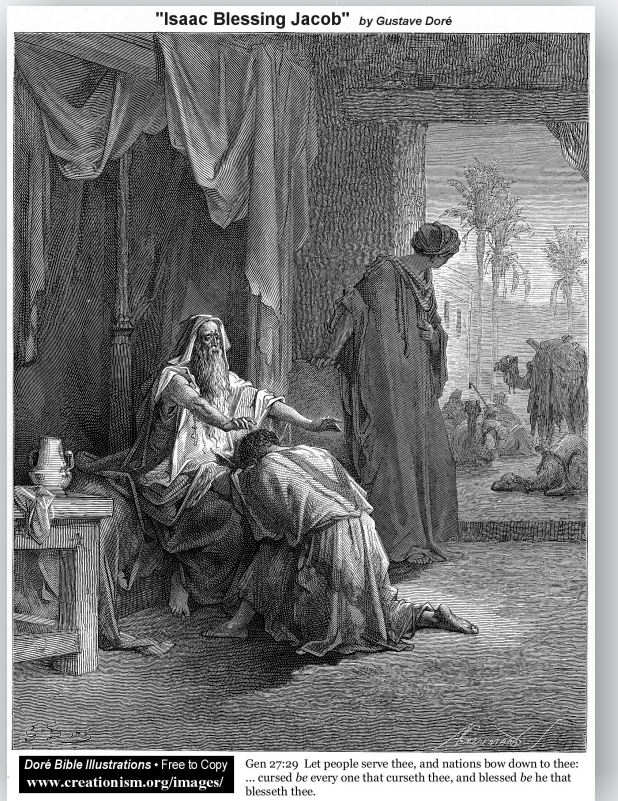
"As easy as to forge a signature, for instance?"

"Much more so, and infinitely more secure. A signature, being written with a pen, requires that the forgery should also be written with a pen, a process demanding very special skill and, after all, never resulting in an absolute *facsimile*. But a finger-print is a stamped impression—the finger-tip being the stamp; and it is only necessary to obtain a stamp identical in character with the finger-tip, in order to produce an impression which is an absolute *facsimile*, in every respect, of the original, and totally indistinguishable from it."

Podstęp “biometryczny” w opowiadaniach biblijnych

Księga Rodzaju, Stary Testament

- podstęp Rebeki i Jakuba: imitacja skóry dłoni i szyi za pomocą skórek z koźlęcia
- cel: podszycie się pod Ezawa i otrzymanie błogosławieństwa od Izaaka



Formy ataków na sensor biometryczny

1. Naśladowanie kogoś (ang. *impersonation*)
   - cel: uzyskanie dostępu do zasobów w imieniu innej osoby
   - kopia charakterystyki biometrycznej, syntetyczne dane biometryczne
   - najczęściej dotyczy schematu pozytywnej weryfikacji/identyfikacji
2. Maskowanie siebie (ang. *disguise*)
   - cel: uniknięcie bycia rozpoznanym
   - zmiana lub ukrywanie charakterystyki biometrycznej
   - najczęściej dotyczy schematu negatywnej identyfikacji
3. Odmowa usługi (ang. *denial of service*)
   - cel: awaria systemu biometrycznego, np. jako prekursor ataku na systemy awaryjne (realizujące zadania uwierzytelnienia w sposób alternatywny, ang. *fallback procedures*)

Rozróżnienie ataku i sytuacji nietypowej

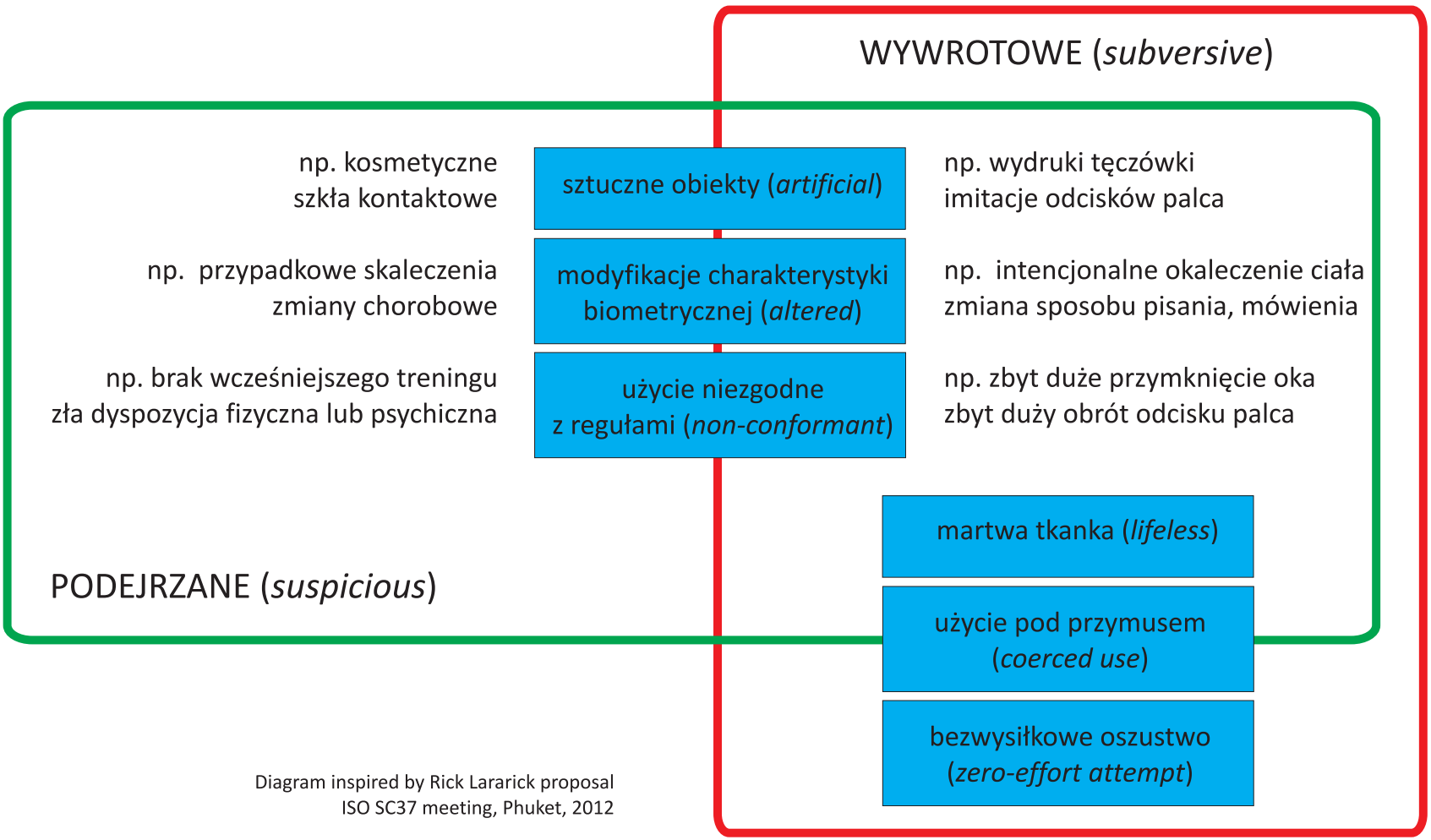


Diagram inspired by Rick Lararick proposal
ISO SC37 meeting, Phuket, 2012

Metody ochrony

1. Biometryczne
   - testowanie żywotności (lub ogólniej: autentyczności) obiektów
2. Systemowe
   - obudowy odporne na ingerencje (ang. *tamper-proof*)
   - kasowanie i zamazywanie pamięci w przypadku ingerencji
   - szyfrowanie i podpisywanie danych przesyłanych do dalszych komponentów systemu
   - uwierzytelnianie urządzeń
   - certyfikacja urządzeń
3. Normalizacja
   - ISO/IEC 19792 (Security evaluation of biometrics)
   - ISO/IEC 30107 (Presentation Attack Detection)
   - ISO/IEC 19795 (Biometric Perf. Testing and Reporting)
   - ANSI/INCITS 409 (Biometric Perf. Testing and Reporting)

Testowanie żywotności

1. Biometria – pomiar cech biologicznych żywego organizmu (nie papierowych, silikonowych lub żelatynowych falsyfikatów)
2. Zapewnienie autentyczności pomiaru
   - + przetwarzane dane muszą być wynikiem pomiaru własności żywej osoby
   - + biometryczne urządzenia pomiarowe (sensory, czytniki) muszą dostarczać właściwe próbki biometryczne
   - + konieczne stosowanie mechanizmów stwierdzających, czy próbka biometryczna jest właściwa $\rightarrow$ testowanie żywotności (obiektów, danych)
3. Źródła informacji o obiektach i danych biometrycznych
   - + kopie oryginalnych danych i obiektów
   - + oryginalne dane i obiekty (np. użycie pod przymusem)
   - + dane syntetyczne, obiekty wykonane z wykorzystaniem danych syntetycznych

Testowanie żywotności

Brak testowania żywotności (autentyczności) w urządzeniu jest słabością tego konkretnego urządzenia, NIE biometrii jako dziedziny nauki

Czy testowanie żywotności jest łatwe?

Rozpoznaj falsyfikaty

Obrazy wykonane czytnikiem optycznym

Obrazy wykonane czytnikiem pojemnościowym

źródło: T. Matsumoto, „Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies. A Case Study for User Identification", ITU-T Workshop on Security, Seoul, 2002

Czy testowanie żywotności jest łatwe?

Rozpoznaj falsyfikat

Obrazy wykonane czytnikiem optycznym z testem żywotności (Futronic)

źródło: laboratorium BIT, semestr letni 2010

Wykład 5: Bezpieczeństwo sensorów

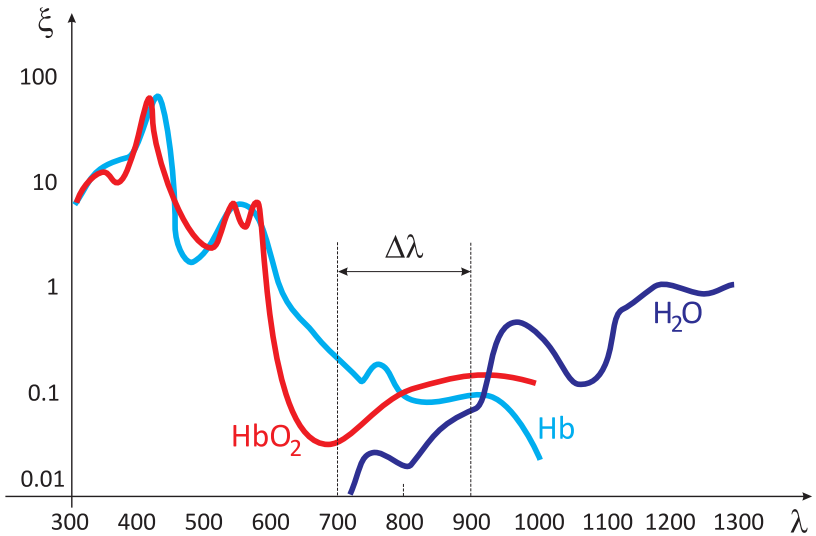
Podatność biometrii na ataki
Podatność sensorów biometrycznych na ataki
Testowanie żywotności palca
Testowanie żywotności oka

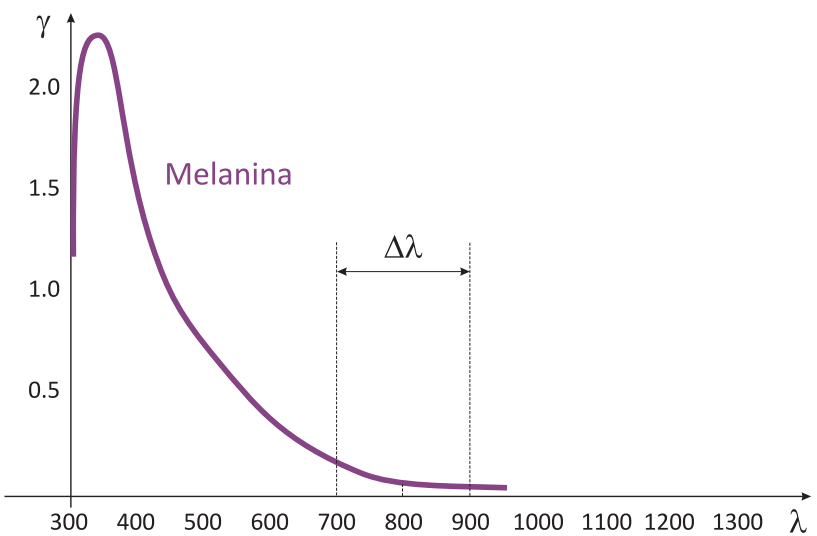
Metody testowania żywotności

▲ Wodoszczelny czytnik Lumidigm testujący żywotność palca (analiza spektralna)

1. Analiza statycznych własności palca
   - impedancja (Setlak, 1999)
   - temperatura (Putte, 2000)
   - ultrasonografia (Bicz, 2003)
   - analiza spektralna – różne długości fali, kierunki oświetlenia i polaryzacje (Rowe, 2005)
   - szczegóły odcisku: struktura skóry (Maltoni, 2003), kształt porów (Moon, 2005), liczność porów (Strzelczyk, Czajka, 2009)

Współczynnik absorpcji hemoglobiny i melaniny





Z lewej: współczynnik absorpcji ξ [cm^{-1}] deoxy-hemoglobiny (Hb), oxy-hemoglobiny (HbO_2) oraz wody (H_2O) w funkcji długości fali λ, dla stężenia hemoglobiny równego 50μM. Rysunek na podstawie: A. Sassaroli, *et al.*, "Near-infrared spectroscopy for the study of biological tissue", Tufts University.

Z prawej: współczynnik absorpcji melaniny z funkcji długości fali. Rysunek na podstawie: J. Daugman, "Absorption spectrum of melanin"

Metody testowania żywotności

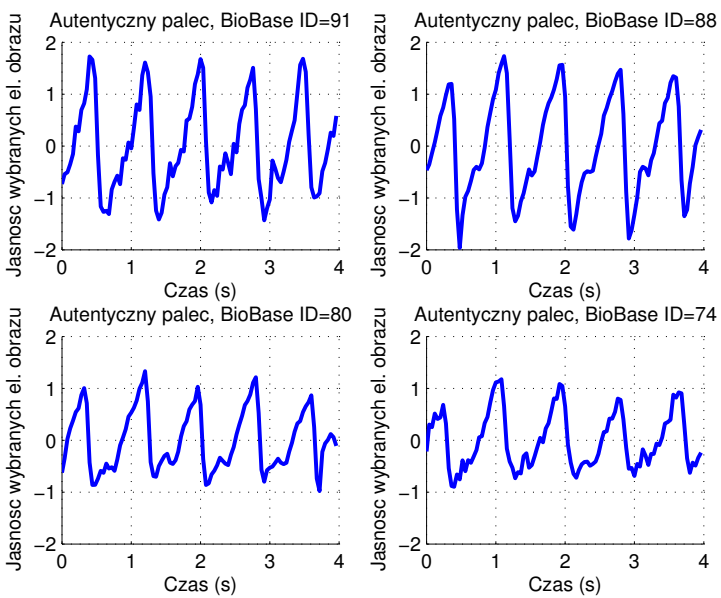
▲ Wodoszczelny czytnik Lumidigm testujący żywotność palca (analiza spektralna)

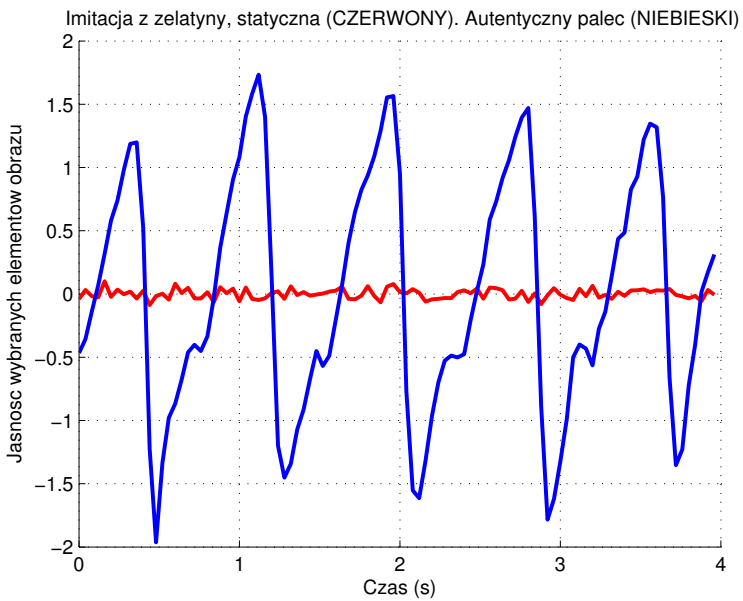
2. Analiza dynamicznych własności palca
   - puls krwi (Lapsley, 1998; A. Czajka, K. Kozioł, 2010)
   - pocenie się skóry (Schuckers, 2004)
   - deformacje palca (Antonelli, 2006)
   - zapach palca (Baldisserra, 2006)

Detekcja pulsu

(A. Czajka, K. Kozioł, 2010)

Analiza obrazu po prześwietleniu palca światłem w zakresie podczerwieni. Łatwe rozpoznawanie statycznych obiektów.

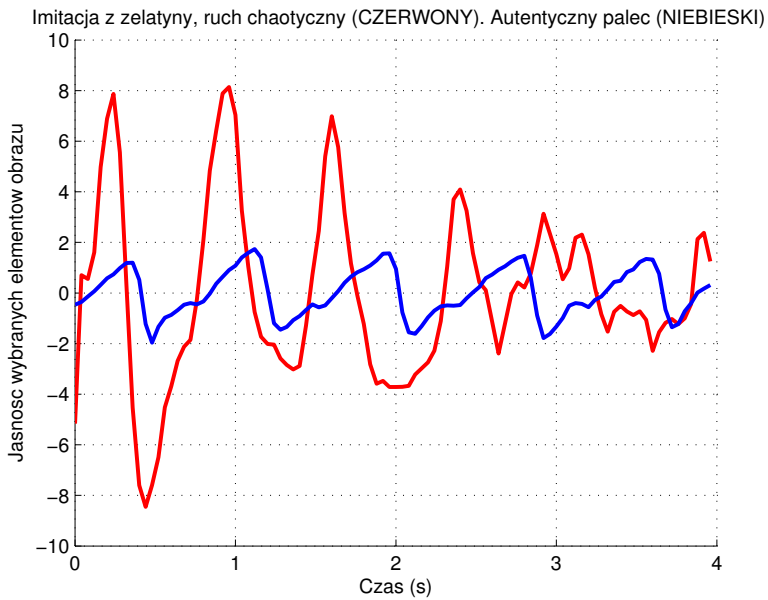




Detekcja pulsu

(A. Czajka, K. Kozioł, 2010)

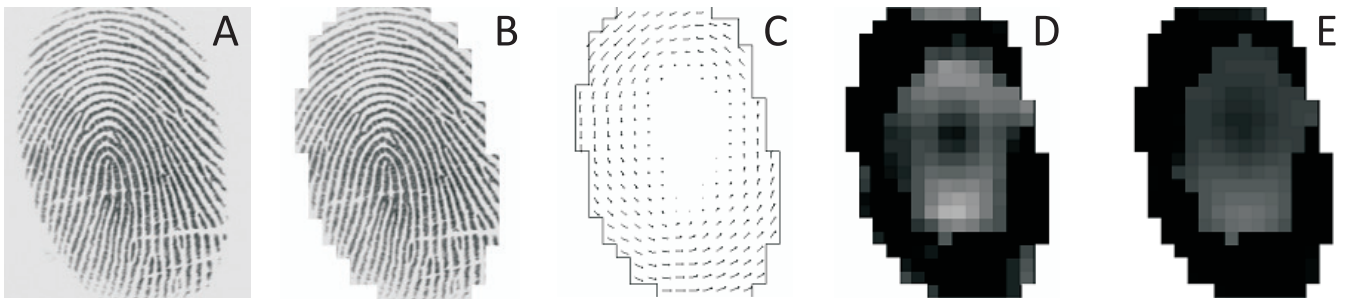
Trudniejsze (ale możliwe) rozpoznawanie obiektów w ruchu (celowa imitacja pulsu lub ruchy chaotyczne dla zaburzania pomiaru).



Analiza deformacji palca

(Antonelli, 2006)

źródło: A. Antonelli et al., A New Approach to Fake Finger Detection Based on Skin Distortion, in: D. Zhang et al., ICB 2006, LNCS 3832, Springer 2005



1. Rejestracja obrazów palca podczas jego obrotu (15°/sek, rys. A)
2. Przetwarzanie obrazów
   - lokalizacja odcisku, rys. B
   - detekcja ruchu, rys. C
   - wyznaczenie i uśrednianie mapy odkształceń
     - mapa odkształceń odpowiadająca obrotowi elementów odcisku względem centroidu, rys. D
     - akumulacja map odkształceń wyznaczonych w poprzednich chwilach, rys. E

Analiza deformacji palca

(Antonelli, 2006)

źródło: A. Antonelli et al., A New Approach to Fake Finger Detection Based on Skin Distortion, in: D. Zhang et al., ICB 2006, LNCS 3832, Springer 2005

3. Wzorzec żywotności: kod reprezentujący odkształcenie (uśrednione w kierunku kątowym mapy odkształceń)
4. Porównywanie wzorców żywotności z wykorzystaniem dynamicznego marszczenia czasu
5. Wyniki
   - baza danych: pomiary 90 żywych palców i 40 falsyfikatów (nośniki: silikon, latex, żelatyna i klej do drewna)
   - EER = 12% (dla indywidualny kodu)
   - EER = 17.5% (dla wspólnego kodu)

Analiza zapachu palca

(Baldisserra, 2006)

1. "Elektroniczny nos"
   - matryca sensorów czułych na molekuły zapachu (odoranty)
   - przetwarzanie stężenia gazów lub składników organicznych w powietrzu na poziom napięcia
   - trzy etapy pomiaru
     - kalibracja (pomiar zapachu otoczenia)
     - rejestracja (pomiar zapachu palca, kilka sek.)
     - powrót do warunków początkowych (10-15 sek.)
2. Wzorzec żywotności
   - funkcja (odcinkowo liniowa) napięcia odpowiadającego stężeniu wybranej substancji w czasie pomiaru

Analiza zapachu palca

(Baldisserra, 2006)

3. Weryfikacja wzorców żywotności – porównanie skalarnego wskaźnika jako ważonej sumy
   - różnicy trendów liniowych funkcji,
   - różnicy pól pod krzywymi, oraz
   - korelacji pomiędzy sekwencjami pomiarów

   z eksperymentalnie dobranym progiem zgodności
4. Wyniki
   - baza danych: pomiary 30 żywych palców i 12 falsyfikatów (nośniki: silikon, latex, żelatyna)
   - EER = 7.48%

Analiza liczności porów

Przykładowe obrazy

obraz żywego palca

obraz falsyfikatu
(klej WIKOL)

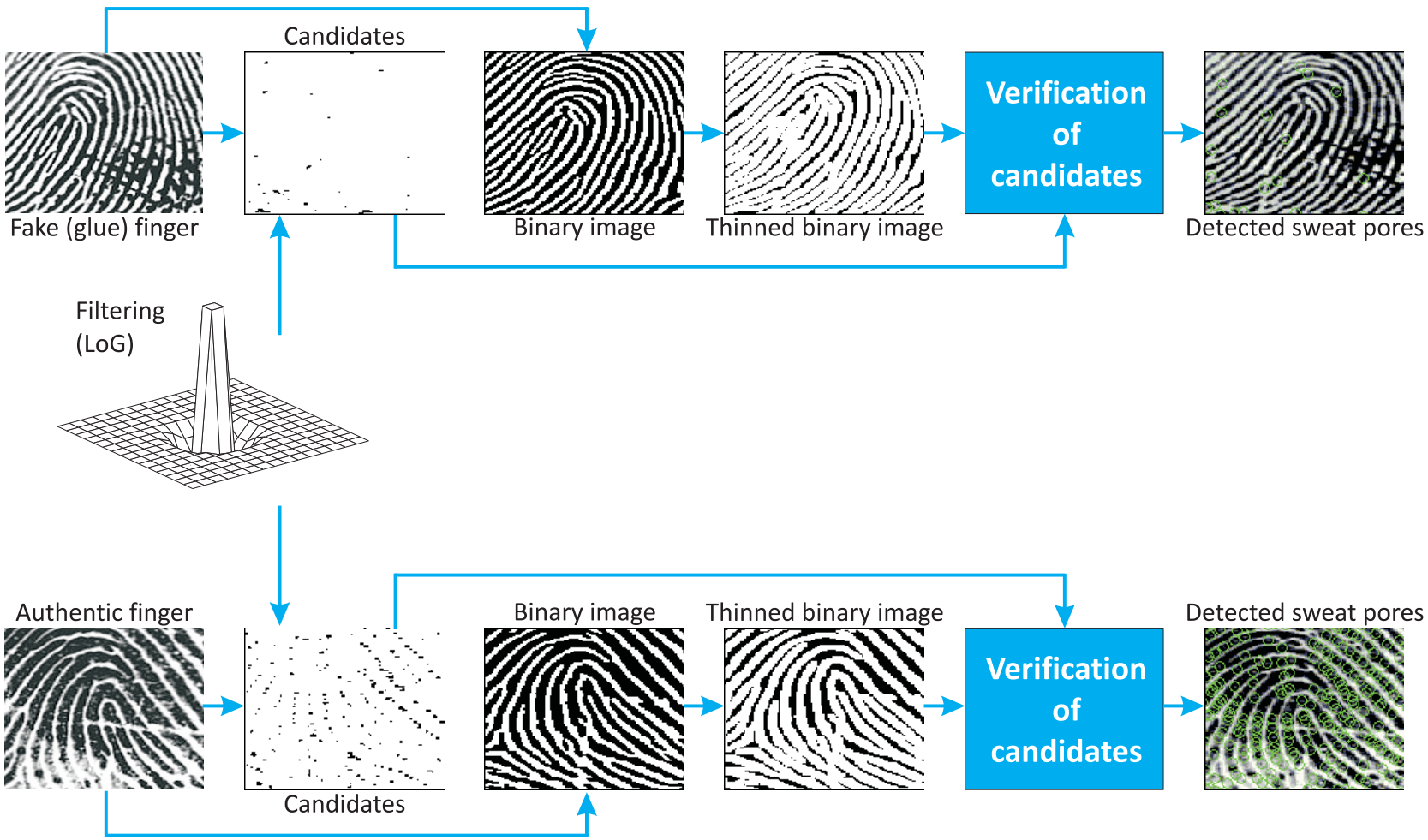
Analiza liczności porów

(P. Strzelczyk, A. Czajka, 2010)

1. Filtracja i progowanie obrazu
   - wykorzystanie laplasjanu gaussowskiego $\rightarrow$ wstępna lokalizacja porów (kandydatów)
2. Detekcja grzbietów
   - tworzenie obrazu binarnego
3. Pocienianie grzbietów
   - jednokrotna erozja morfologiczna obrazu binarnego
4. Weryfikacja kandydatów
   - odrzucenie tych kandydatów, którzy znajdują się poza środkowymi częściami grzbietów odcisków palca
5. Określenie liczności porów

Analiza liczności porów

Schemat metody



Wykład 5: Bezpieczeństwo sensorów

Podatność biometrii na ataki
Podatność sensorów biometrycznych na ataki
Testowanie żywotności palca
Testowanie żywotności oka

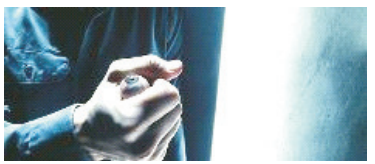
Systematyka fałszerstw

1. Obraz statyczny
   - papierowy wydruk tęczówki
   - obraz na ekranie monitora
   - hologram
2. Obraz dynamiczny
   - off-line: z wykorzystaniem wiedzy *a priori*
   - on-line: z wykorzystaniem wiedzy *a posteriori*
3. Sztuczne oko
   - model z tworzywa
   - żywe oko + szkła kontaktowe
4. Prawdziwe oko
   - martwa tkanka
   - działanie pod przymusem

Dracula (2000)

Demolition man (1993)

Never say never again (1983)


Minority report (2002)

Bad Company (2002)

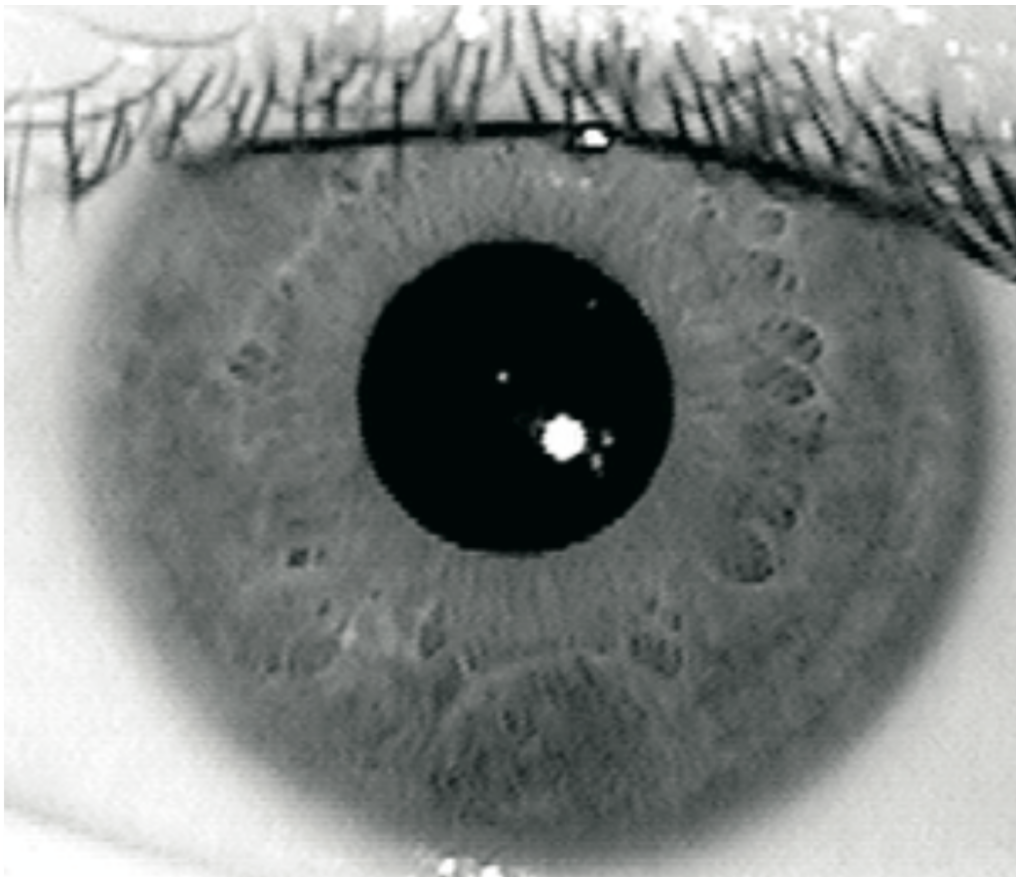
źródło: perso.orange.fr/fingerchip/biometrics/movies.htm

Metody testowania żywotności oka

1. Obiekt statyczny, pomiar pasywny
   - cechy dwuwymiarowe: analiza częstotliwościowa, temperatura
   - cechy trójwymiarowe: analiza kształtu gałki ocznej, struktury mięśnia tęczówki
   - analiza tzw. odbić Purkiniego (odbicia od soczewki i źrenicy)
2. Obiekt dynamiczny, pomiar pasywny
   - spontaniczne ruchy źrenicy (tzw. *hippus*, ok. 0.5 Hz)
3. Obiekt statyczny, pomiar aktywny
   - analiza stymulowanych odbić światła
   - analiza charakterystyki absorpcyjnej tkanki przy oświetlaniu światłem o różnej długości fali
4. Obiekt dynamiczny, pomiar aktywny
   - odruch bezwarunkowy: dynamika zmian wielkości źrenicy pod wpływem zmiany natężenia światła
   - świadome działanie: podążanie za punktem, mrugnięcia

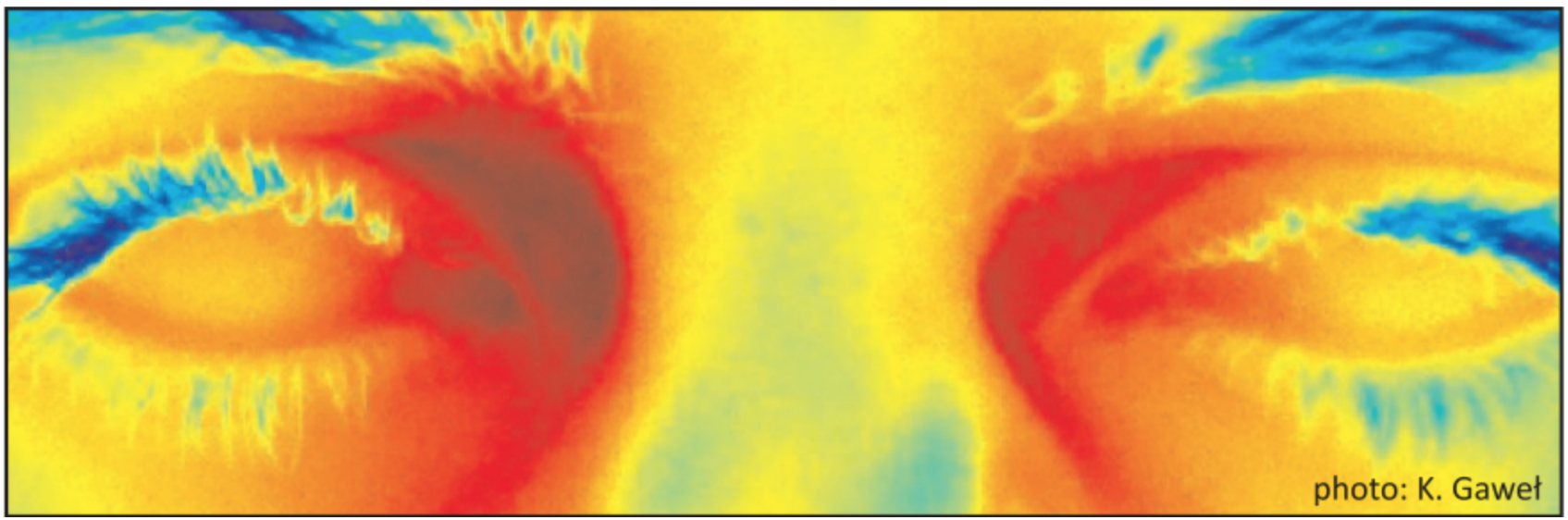
Przykład odbić Purkiniego

(obraz wykonany kamerą LG Iris Access 2000)



Przykład obrazu termicznego oka

(obraz wykonany kamerą FLIR w Laboratorium Biometrii IAiIS PW)



Metody testowania żywotności oka

Omówienie wybranych podejść

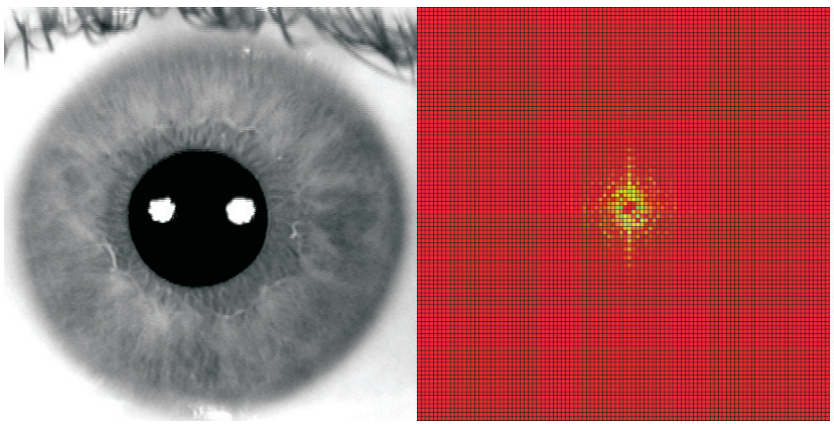
1. Obiekt statyczny, pomiar pasywny
   - cechy dwuwymiarowe: analiza częstotliwościowa

Dodatkowa literatura:

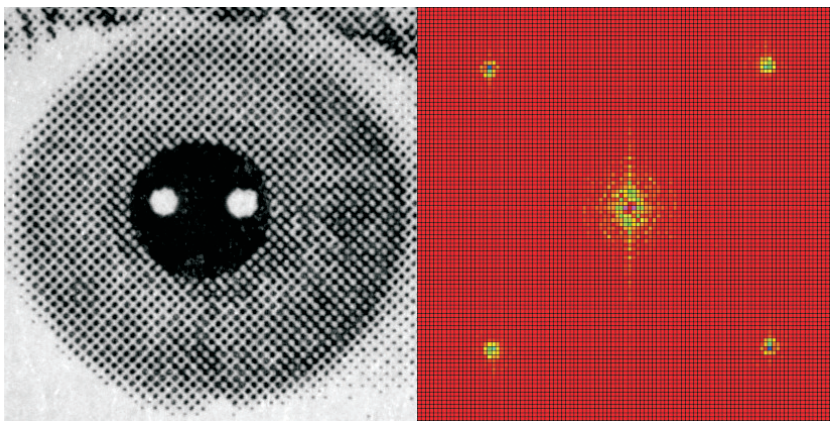
Adam Czajka, "Database of Iris Printouts and its Application: Development of Liveness Detection Method for Iris Recognition", The 18th International Conference on Methods and Models in Automation and Control (MMAR2013), Miedzyzdroje, Poland, August 26-29, 2013

Andrzej Pacut, Adam Czajka, "Aliveness detection for iris biometrics", 2006 IEEE International Carnahan Conference on Security Technology, 40th Annual Conference, October 17-19, Lexington, Kentucky, IEEE 2006

Analiza częstotliwościowa



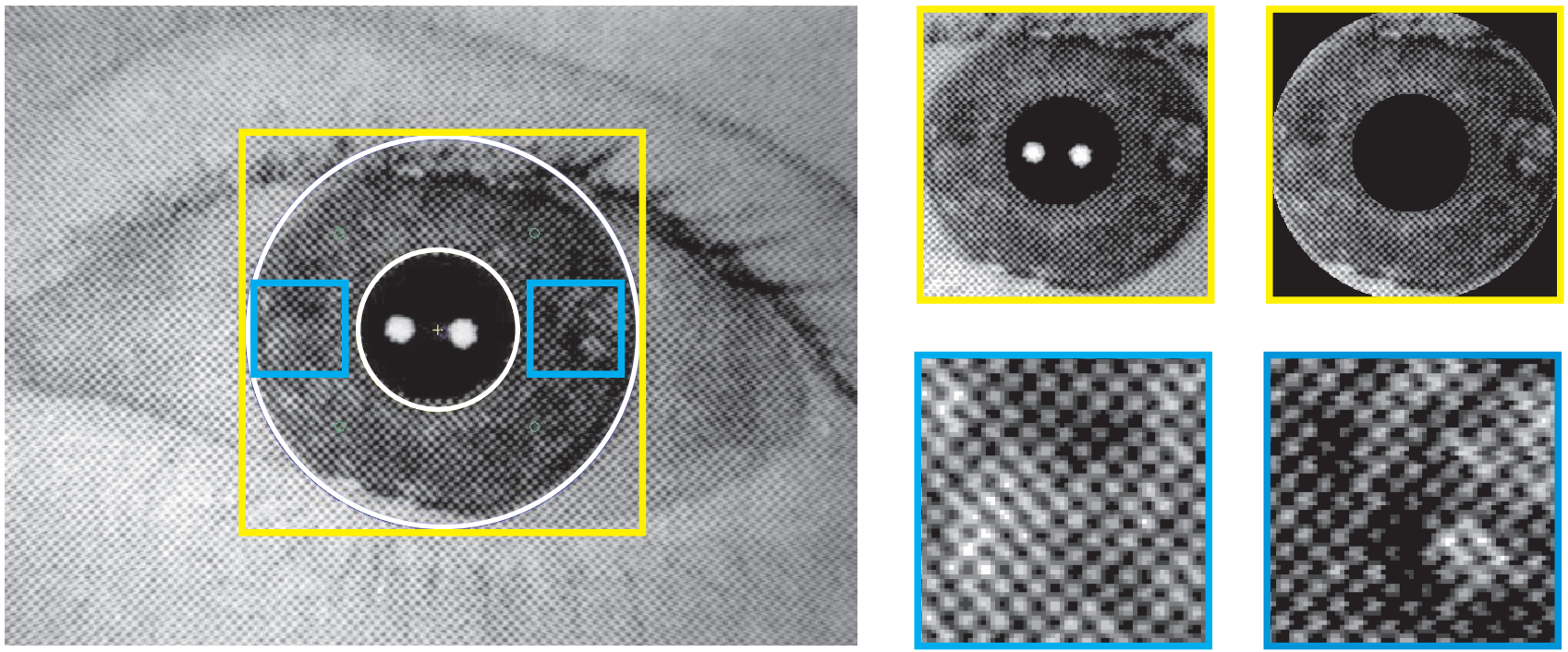
Zdjęcie i widmo amplitudowe autentycznej tęczówki



Zdjęcie i widmo amplitudowe wydruku tęczówki

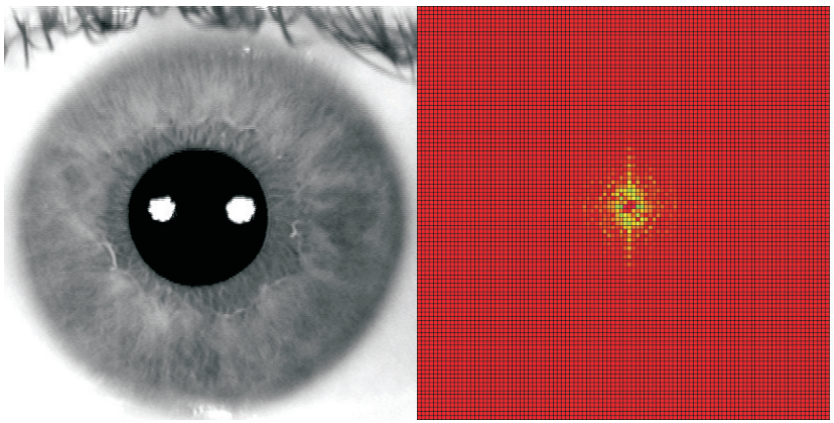
1. Możliwość wykorzystania tego samego zdjęcia, które służy rozpoznawaniu tęczówki
   - testowanie żywotności
   - dodatkowy składnik oceny jakości zdjęcia

Analiza częstotliwościowa

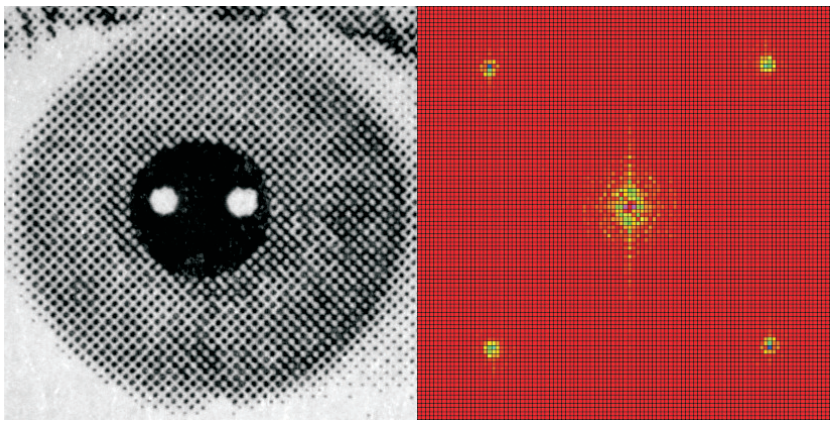


2. Wymagana segmentacja tęczówki
   - 'łatwa' dla zdjęć autentycznych tęczówek
   - nieprzewidywalna dla zdjęć imitacji

Analiza częstotliwościowa



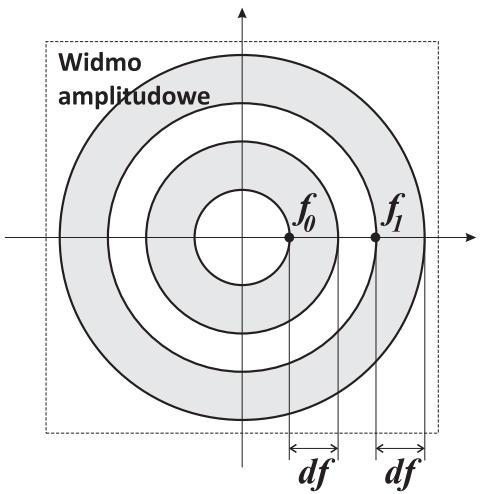
Zdjęcie i widmo amplitudowe autentycznej tęczówki



Zdjęcie i widmo amplitudowe wydruku tęczówki

3. Okienkowanie widma, np. poprzez zdefiniowanie f_0, f_1 oraz df
4. Określenie "wskaźnika żywotności", np.

$$q = \frac{\max |F(f_1, f_1 + df)|}{\max |F(f_0, f_0 + df)|}$$



Analiza częstotliwościowa

* Transformata Fouriera dla obrazów obróconych

Niech $f(\mathbf{x}) : \mathbb{R}^2 \mapsto \mathbb{R}$, gdzie $\mathbf{x} = [x_1, x_2]^T$ reprezentuje obraz, a $f'(\mathbf{x}) = f(\mathbf{R}^{-1}\mathbf{x})$ będzie obróconą wersją tego obrazu, gdzie $\mathbf{R}$ jest macierzą obrotu.

Dwuwymiarowa transformata Fouriera obróconego obrazu:

$$F'(u_1, u_2) = \int \int_{-\infty}^{\infty} f'(x_1, x_2) e^{-2\pi i(u_1 x_1 + u_2 x_2)} dx_1 dx_2$$

lub (upraszczając zapis)

$$F'(\mathbf{u}) = \int_{-\infty}^{\infty} f'(\mathbf{x}) e^{-2\pi i \mathbf{u}^T \mathbf{x}} d\mathbf{x}, \quad \text{gdzie } \mathbf{u} = [u_1, u_2]^T$$

Analiza częstotliwościowa

* Transformata Fouriera dla obrazów obróconych

Wstawmy $f(\mathbf{R}^{-1}\mathbf{x})$ zamiast $f'(\mathbf{x})$, dokonajmy zamiany $\mathbf{u} \rightarrow \mathbf{Ru}$ oraz skorzystajmy z własności $\mathbf{R}^T = \mathbf{R}^{-1}$ dla macierzy obrotu:

$$F'(\mathbf{Ru}) = \int_{-\infty}^{\infty} f(\mathbf{R}^{-1}\mathbf{x}) e^{-2\pi i(\mathbf{Ru})^T \mathbf{x}} d\mathbf{x} =$$

$$= \int_{-\infty}^{\infty} f(\mathbf{R}^{-1}\mathbf{x}) e^{-2\pi i \mathbf{u}^T \mathbf{R}^T \mathbf{x}} d\mathbf{x} =$$

$$= \int_{-\infty}^{\infty} f(\underbrace{\mathbf{R}^{-1}\mathbf{x}}_{\mathbf{y}}) e^{-2\pi i \mathbf{u}^T \underbrace{\mathbf{R}^{-1}\mathbf{x}}_{\mathbf{y}}} d\mathbf{x} = F(\mathbf{u})$$

Czyli:

$$F'(\mathbf{Ru}) = F(\mathbf{u}) \quad \text{lub} \quad F'(\mathbf{u}) = F(\mathbf{R}^{-1}\mathbf{u})$$

Metody testowania żywotności oka

Omówienie wybranych podejść

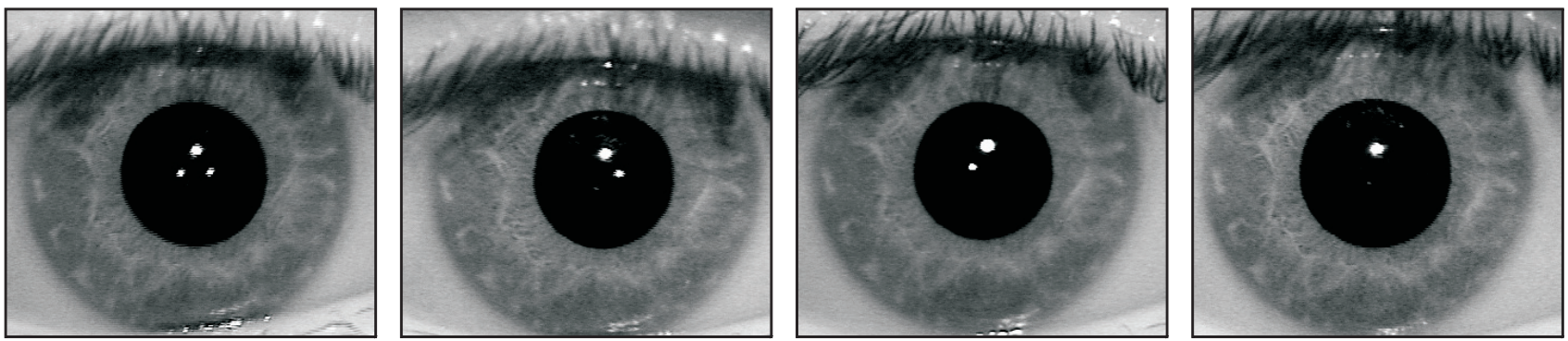
3. Obiekt statyczny, pomiar aktywny
   - analiza stymulowanych odbić światła

Dodatkowa literatura:

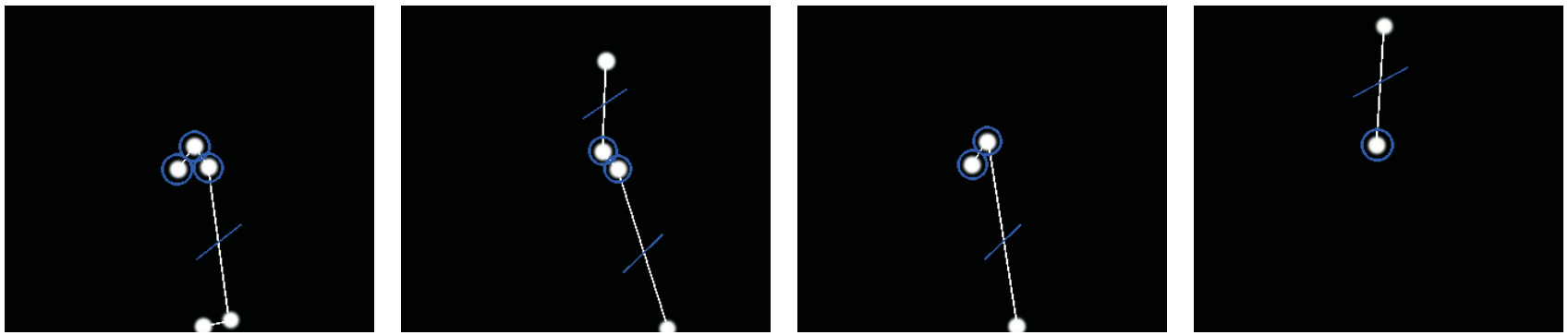
Andrzej Pacut, Adam Czajka, "Aliveness detection for iris biometrics", 2006 IEEE International Carnahan Conference on Security Technology, 40th Annual Conference, October 17-19, Lexington, Kentucky, IEEE 2006

Analiza stymulowanych odbić

1. Oświetlenie dodatkowymi źródłami podczerwieni



Analiza stymulowanych odbić



2. Weryfikacja położenia odbić
   - lokalizacja odbić (filtr LoG – laplasjan gaussowski)
   - indeksacja odbić
   - określenie wzajemnego położenia odbić: konstrukcja drzewa rozpinającego
   - eliminacja "fałszywych" odbić (usunięcie "zbyt krótkich" i "zbyt długich" krawędzi drzewa)
3. Porównanie otrzymanej sekwencji położeń z zadaną przez system

Metody testowania żywotności oka

Omówienie wybranych podejść

4. Obiekt dynamiczny, pomiar aktywny
   - odruch bezwarunkowy: dynamika zmian wielkości źrenicy pod wpływem zmiany natężenia światła

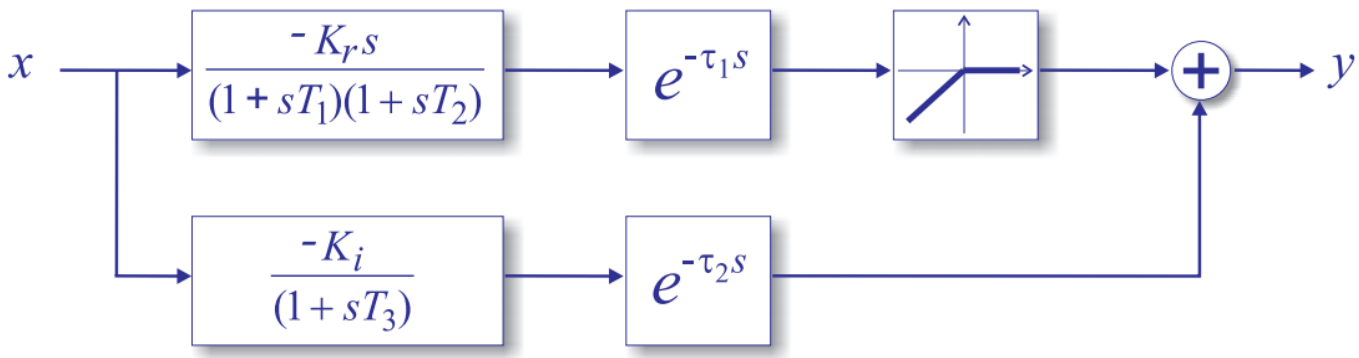
Dodatkowa literatura:

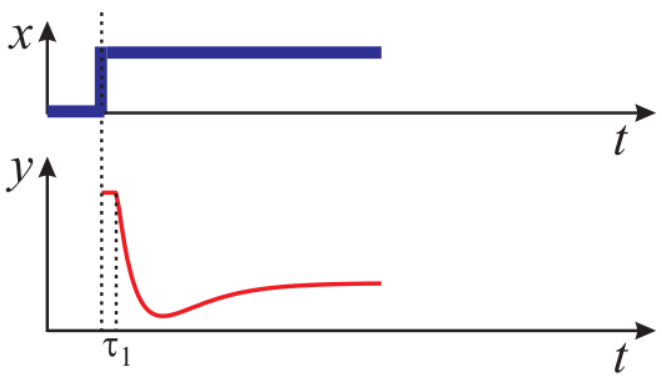
Adam Czajka, "Pupil Dynamics for Iris Liveness Detection", IEEE Transactions on Information Forensics and Security, Vol. 10(4), str. 726-735, kwiecień 2015

Adam Czajka, Andrzej Pacut, Marcin Chochowski, "Method of Eye Aliveness Testing and Device for Eye Aliveness Testing", US Patent No. 8,061,842, 2011

Andrzej Pacut, Adam Czajka, "Aliveness detection for iris biometrics", 2006 IEEE International Carnahan Conference on Security Technology, 40th Annual Conference, October 17-19, Lexington, Kentucky, IEEE 2006

Analiza dynamiki źrenicy

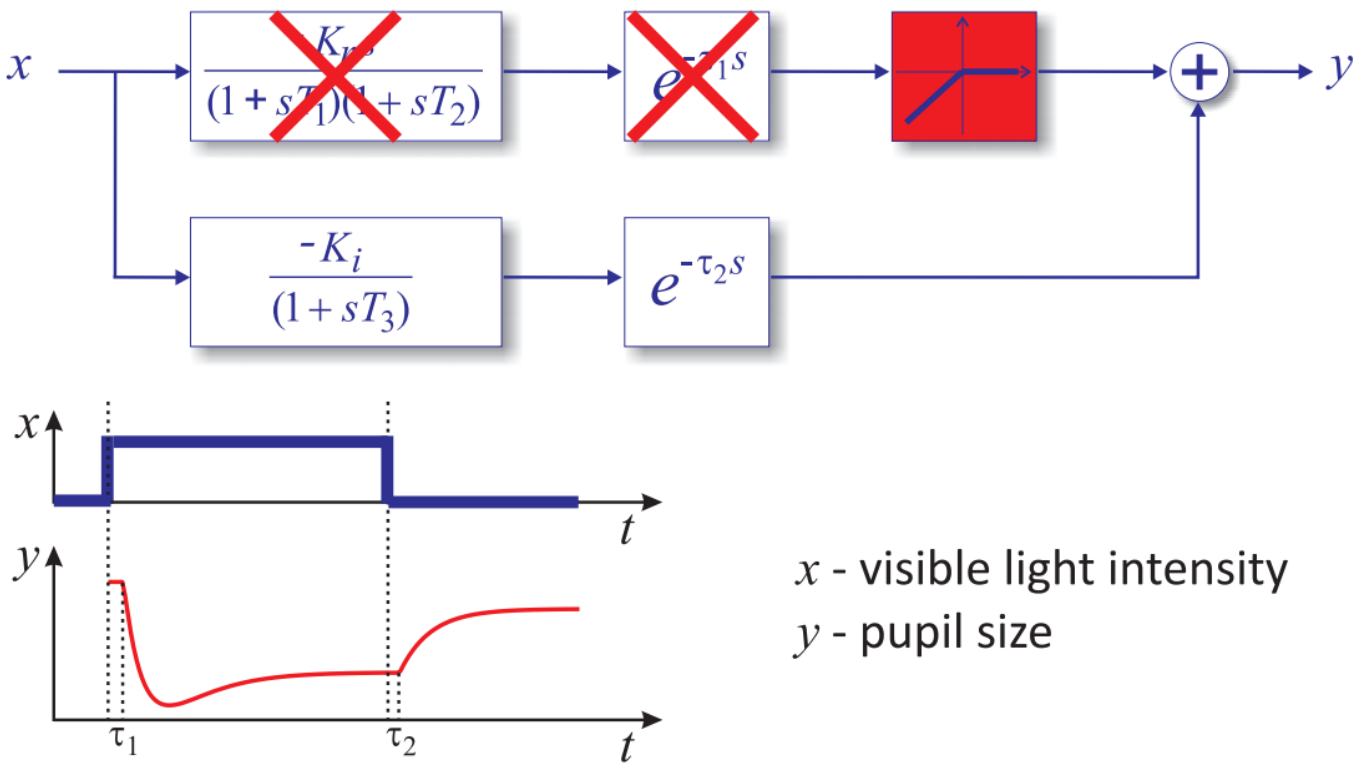




x - visible light intensity
y - pupil size

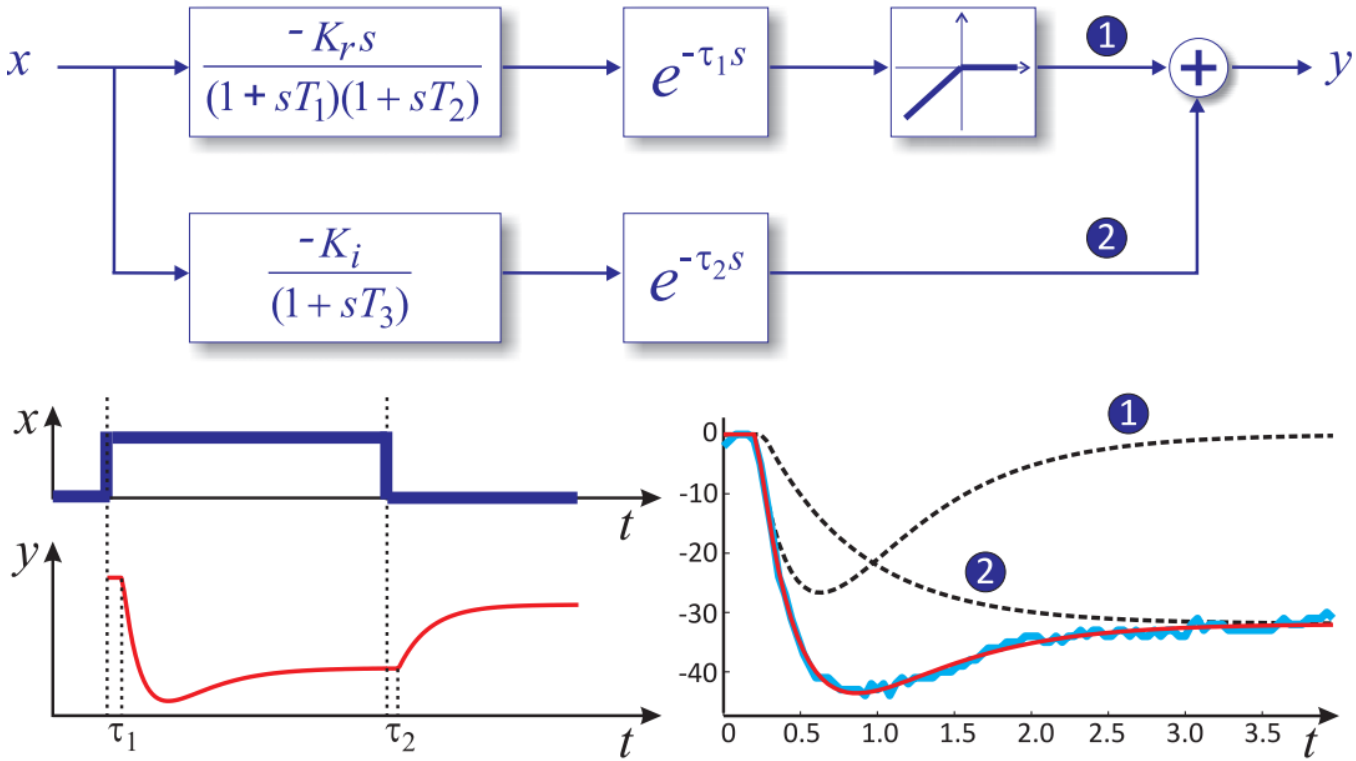
Model Clynes'a i Kohn'a; cechy żywotności: wzmocnienia (K_i, K_r), stałe czasowe (T_1, T_2, T_3) oraz opóźnienia (τ_1, τ_2)

Analiza dynamiki źrenicy



Model Clynes'a i Kohn'a; cechy żywotności: wzmocnienia (K_i, K_r), stałe czasowe (T_1, T_2, T_3) oraz opóźnienia (τ_1, τ_2)

Analiza dynamiki źrenicy



Model Clynes'a i Kohn'a; cechy żywotności: wzmocnienia (K_i, K_r), stałe czasowe (T_1, T_2, T_3) oraz opóźnienia (τ_1, τ_2)

Analiza dynamiki źrenicy

Identyfikacja modelu

$$\widehat{\phi} = \underset{\phi \in \Phi}{\operatorname{argmin}} \sum_{i=1}^{N} (\widehat{y}_{i;\phi} - y_i)^2$$

gdzie:

$\phi = [K_i, K_r, T_1, T_2, T_3, \tau_1, \tau_2]^T$ – cechy żywotności

Φ – zbiór możliwych wartości ϕ

$\widehat{\phi}$ – wyliczone wartości cech żywotności

$\widehat{y}_{i;\phi}$ – wyjście modelu (dla konkretnych wartości ϕ)

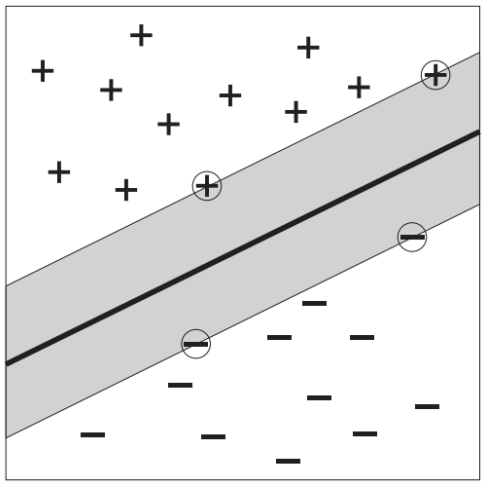
y_i – rzeczywista (zaobserwowana) zmiana wielkości źrenicy

N – długość obserwacji

Analiza dynamiki źrenicy

Przetwarzanie wyjścia modelu

1. Klasyfikacja
   - przykład: wykorzystanie Maszyny Wektorów Podpierających (SVM – Support Vector Machine) w przestrzeni parametrów ϕ (dwie klasy: oko autentyczne lub imitacja)



2. Określenie jakości dopasowania ("goodness of fit")
   - znormalizowana odległość średnio-kwadratowa

$$\text{GoF} = 1 - \frac{\|\widehat{y}_\phi - y\|}{\|\widehat{y}_\phi - \bar{y}\|}$$

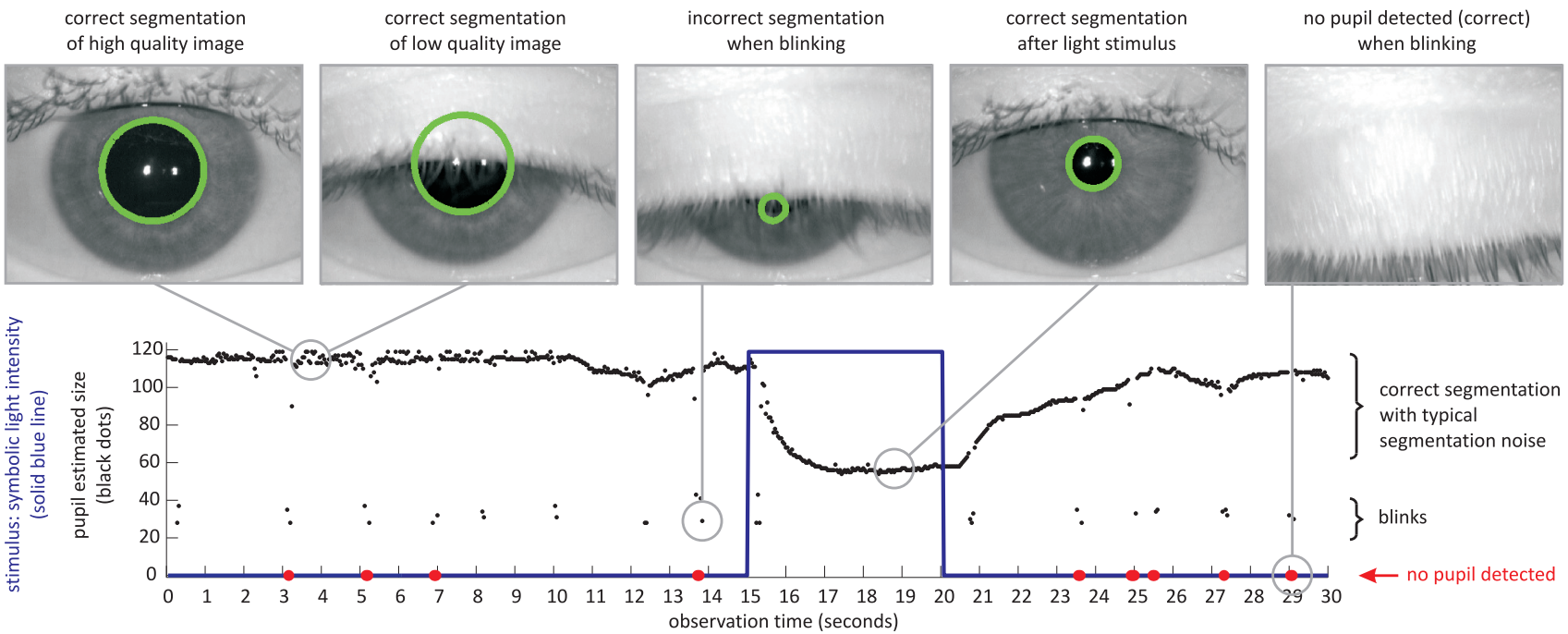
gdzie $\bar{y}$ oznacza średnią y.

Analiza dynamiki źrenicy

1. Pytanie 1: Jak symulować imitacje?
   - statyczne obiekty $\rightarrow$ zadanie trywialne
   - symulacja użycia pod przymusem $\rightarrow$ trudne do wykonania
2. Pytanie 2: Czy powinniśmy polegać jedynie na odpowiedzi klasyfikatora?
   - błędy klasyfikacji (zawsze możliwe) mogą doprowadzić do akceptacji modeli znacznie odbiegających od rzeczywistych obserwacji
3. Pytanie 3: Jak długo musimy obserwować oko?
   - dłuższe czasy obserwacji zwiększają dokładność, ale wydłużają proces rozpoznawania

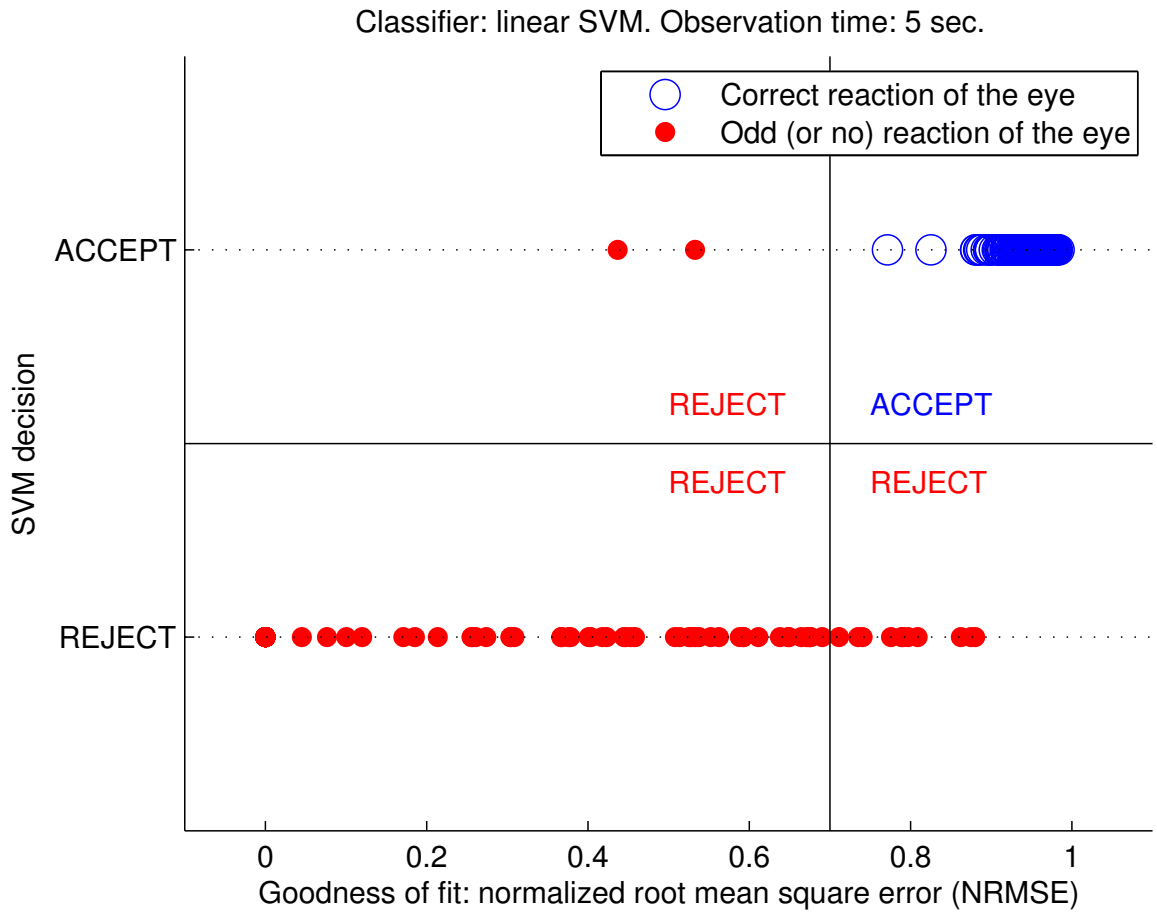
Analiza dynamiki źrenicy

Pytanie 1: Jak symulować imitacje?



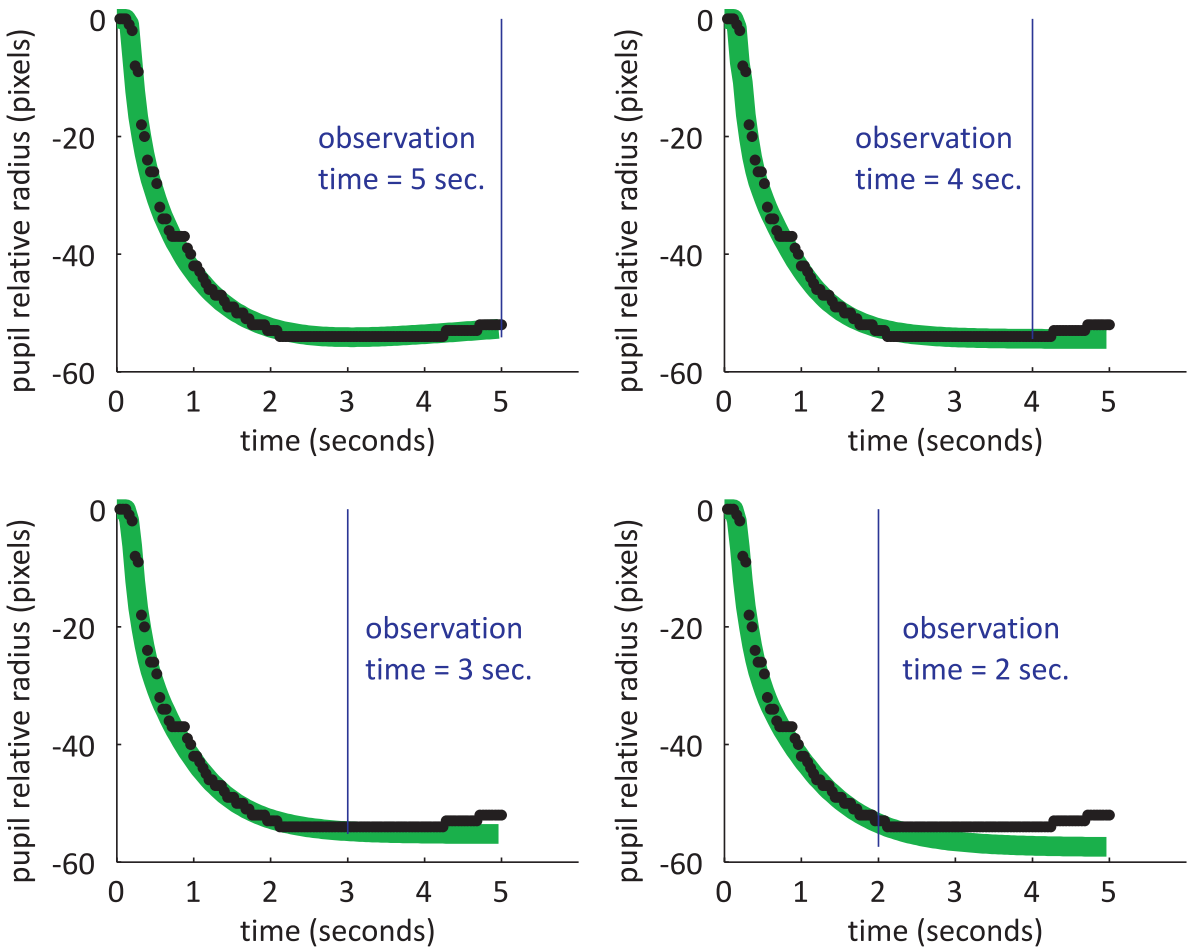
Analiza dynamiki źrenicy

Pytanie 2: Czy powinniśmy polegać jedynie na odpowiedzi klasyfikatora?



Analiza dynamiki źrenicy

Pytanie 3: Jak długo musimy obserwować oko?



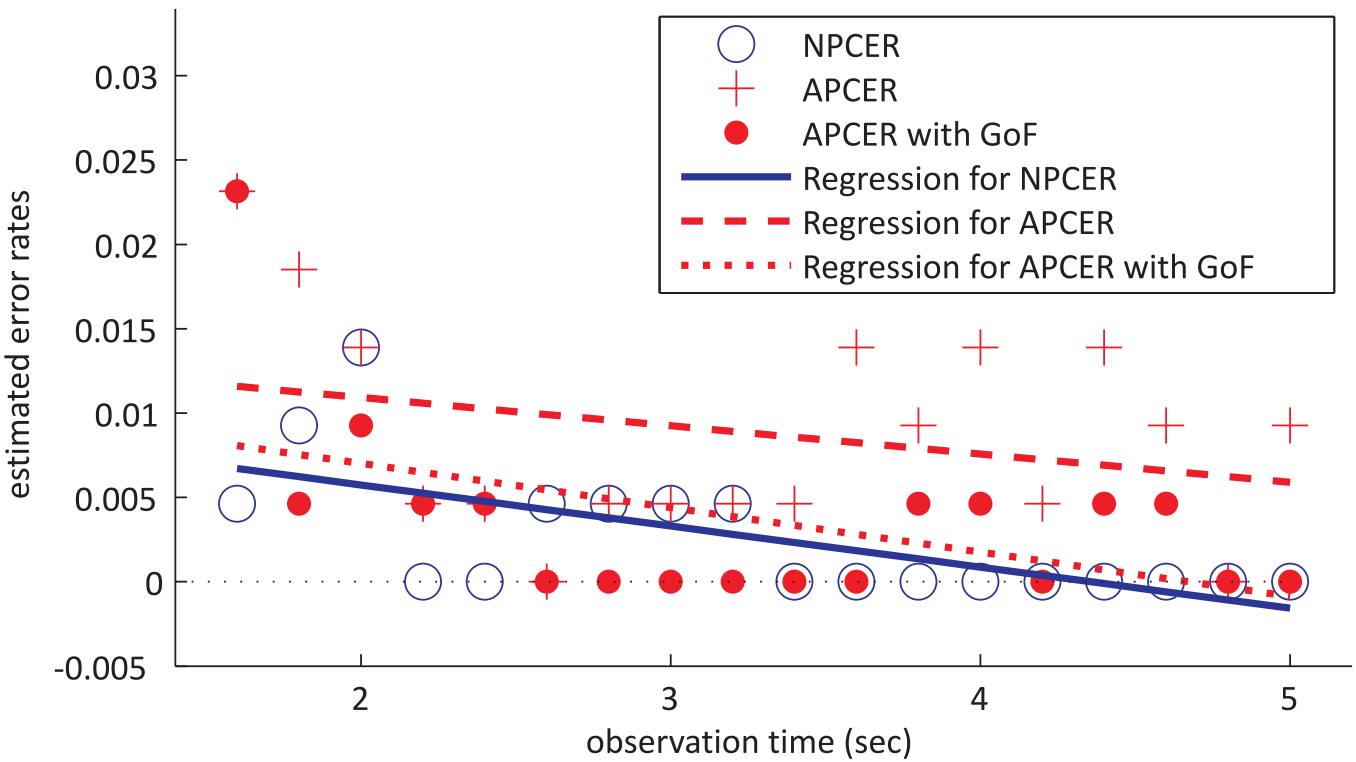
Ocena błędów w testowaniu żywotności

Propozycje zawarte w ISO/IEC 30107

1. APCER: Attack Presentation Classification Error Rate
   - proporcja liczby prezentacji będących atakami ale nierozpoznanych przez system do całkowitej liczby ataków
   - odpowiada wskaźnikowi FMR w rozpoznawaniu biometrycznym
2. NPCER: Normal Presentation Classification Error Rate
   - proporcja liczby autentycznych prezentacji błędnie uznanych za ataki do całkowitej liczby autentycznych prezentacji
   - odpowiada wskaźnikowi FNMR w rozpoznawaniu biometrycznym

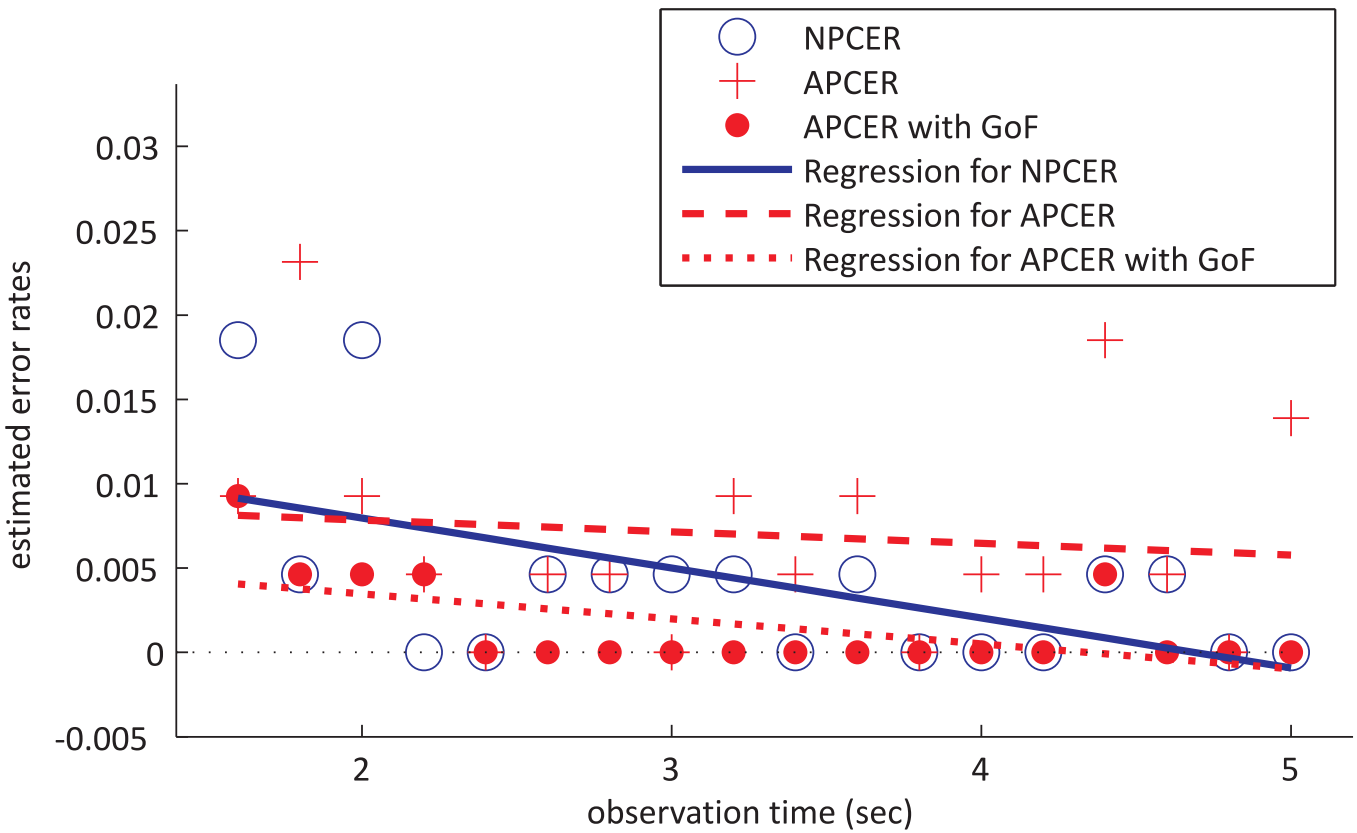
Analiza dynamiki źrenicy

Wyniki dla liniowej SVM



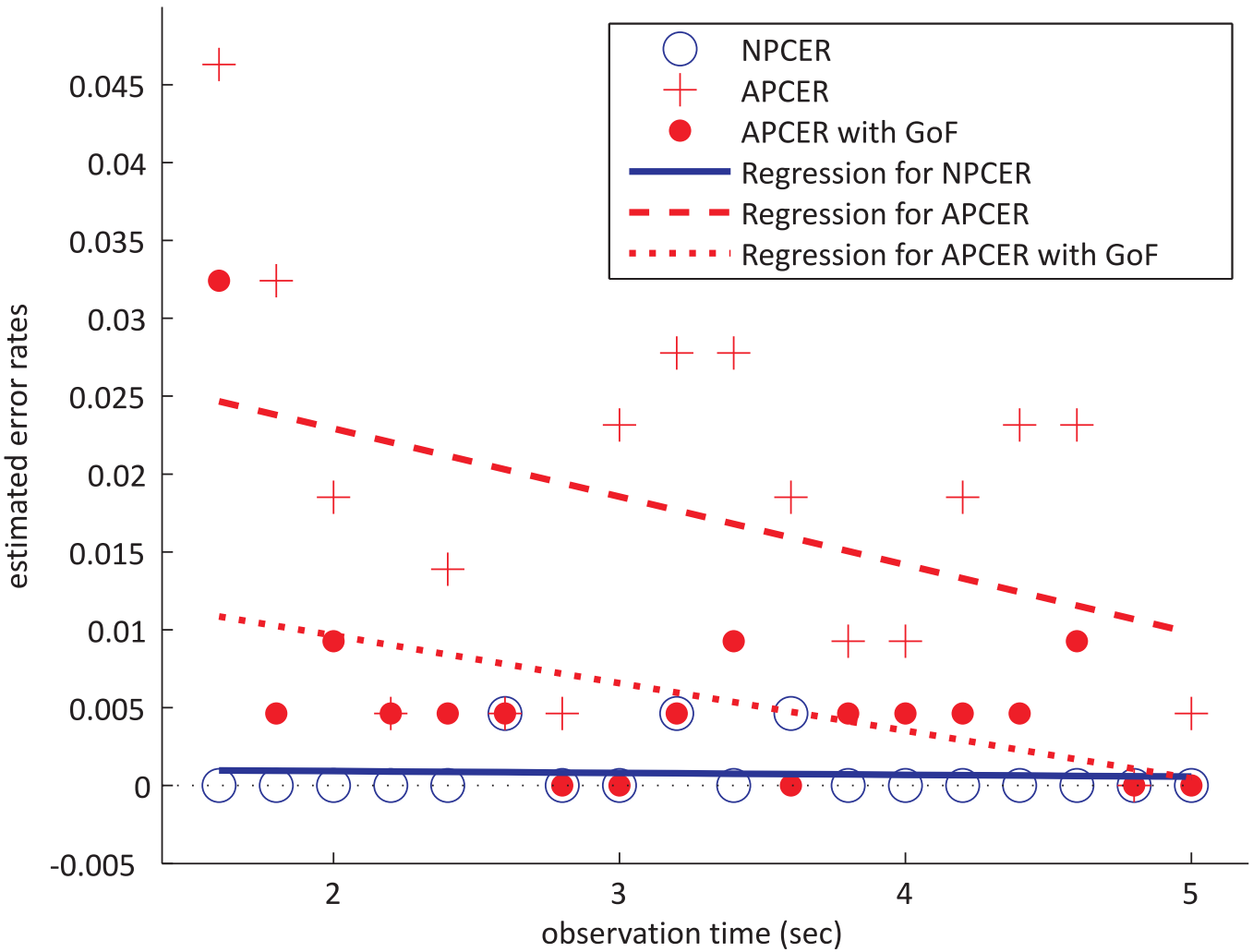
Analiza dynamiki źrenicy

Wyniki dla SVM z jądrem wielomianowym



Analiza dynamiki źrenicy

Wyniki dla SVM z jądrem gaussowskim



Testowanie wybranych metod

Ocena przykładowych systemów komercyjnych (System A, System B) oraz metod NASK/PW

System	Metoda	Stopień akceptacji imitacji (%)	Stopień odrzucenia żywych oczu (%)	Możliwości wykrycia fałszerstwa			
				Obraz statyczny	Obraz dynamiczny	Model oka	Działanie pod przymusem
System A	?	73,1	0,0	–	–	–	–
System B	?	15,6	0,0	–	–	–	–
PW/NASK	FA	0,0 / 5,0*	2,80 / 0,0*	+	–	–	–
PW/NASK	CLR	0,0**	0,0	+	–	–	–
PW/NASK	PD	0,0***	0,0	+	+/–	+/–	?

Baza danych: 569 wydruków w rozdzielczościach 300 oraz 600 dpi dla 29 różnych tęczówek + imitacje dynamiczne: spontaniczne oscylacje (*hippus*) dla 50 różnych tęczówek

* wyniki oceny z wykorzystaniem dodatkowych wydruków tęczówek, które w 100% zostały zaakceptowane przez komercyjny system A

** wynik uzyskany dla konfiguracji, w której odblaski pojawiały się poza źrenicą

*** wynik uzyskany zarówno dla wydruków jak i spontanicznych oscylacji źrenicy

Przykładowe pytanie egzaminacyjne

Zmiana wielkości źrenicy jest czynnikiem zmniejszającym dokładność biometrii tęczówki. W jaki sposób tę własność oka można wykorzystać do zwiększenia dokładności rozpoznawania tożsamości?