Biometryczna Identyfikacja Tożsamości

Wykład 11: Bezpieczeństwo sensorów biometrycznych

Adam Czajka

Wykład na Wydziale Elektroniki i Technik Informacyjnych
Politechniki Warszawskiej

Semestr letni 2014

Wykład 11: Bezpieczeństwo sensorów biometrycznych

- Podatność urządzeń biometrycznych na ataki
- Testowanie żywotności palca
- Testowanie żywotności oka

Wykład 11: Bezpieczeństwo sensorów biometrycznych

Podatność urządzeń biometrycznych na ataki

Testowanie żywotności palca

Testowanie żywotności oka

Ochrona fizyczna urządzeń i danych w urządzeniach

1. Obudowy odporne na ingerencje (ang. *tamper-proof*)
2. Kasowanie i zamazywanie pamięci w przypadku ingerencji
3. Szyfrowanie i podpisywanie danych przesyłanych do dalszych komponentów systemu
4. Uwierzytelnianie urządzeń
5. Certyfikacja urządzeń

Podatność biometrii na ataki

Przykład: iPhone 5s (2013)

theguardian

News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment | Tech | TV | Video | Dating | Offers | Jobs

News › Technology › iPhone

iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club

Biometrics are not safe, says famous hacker team who provide video showing how they could use a fake fingerprint to bypass phone's security lockscreen

Follow Charles Arthur by email BETA

Charles Arthur

Follow @charlesarthur Follow @guardiantech

theguardian.com, Monday 23 September 2013 08.50 BST

Jump to comments (306)

An Apple employee instructs the use of the fingerprint scanner technology built into the company's iPhone 5S. German hackers say they can beat it. Photograph: Ng Han Guan/AP

Germany's Chaos Computer Club says it has cracked the protection around Apple's fingerprint sensor on its new iPhone 5S, just two days after the device went on sale worldwide.

Share 2801 Tweet 1,869 247 1 Share 410 Email

Article history

Technology
iPhone · Apple · Hacking · iPhone 5s

More news

More on this story

iPhones 5s and 5c sell 9m in record weekend as Apple shrugs off doubters
Data suggests 5s outsold 5c two to one as high-end smartphone market still shows promise and 200m upgrade to newer iOS 7 software.
By Charles Arthur

iPhone 5S and 5C: the

Today's best video

JFK: former secret service agent relives assassination
Former secret service agent Clint Hill gives his account of the day John F Kennedy died as the US marks 50 years since Kennedy's assassination

Doctor Who theme re-recorded
New recording marks the series' 50th anniversary

Bayern Munich recreate Borussia Dortmund stunt
Players recreate trick on board team bus

Muppets Most Wanted
The Muppets return with a new adventure. Watch the trailer

GuardianWitness

Podatność biometrii na ataki

Przykład: 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

Podatność biometrii na ataki

Przykład: 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

Podatność biometrii na ataki

Imitacje przygotowywane w laboratoriach IAiIS PW oraz NASK

Forma z modeliny

Magnetyczny proszek daktyloskopijny

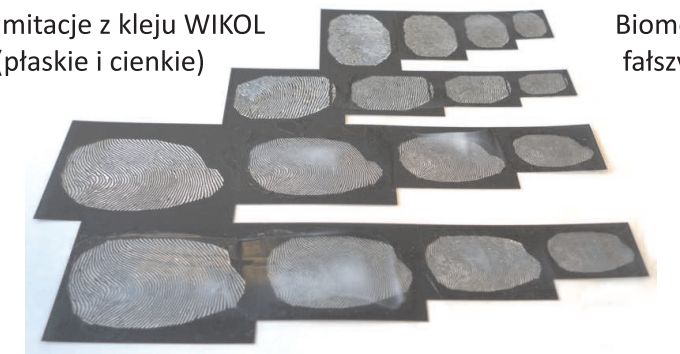
Odcisk utajony w świetle widzialnym

Odcisk utajony w świetle ultrafioletowym

Obraz biometryczny

Imitacje z silikonu, kleju lub żelatyny (3D)

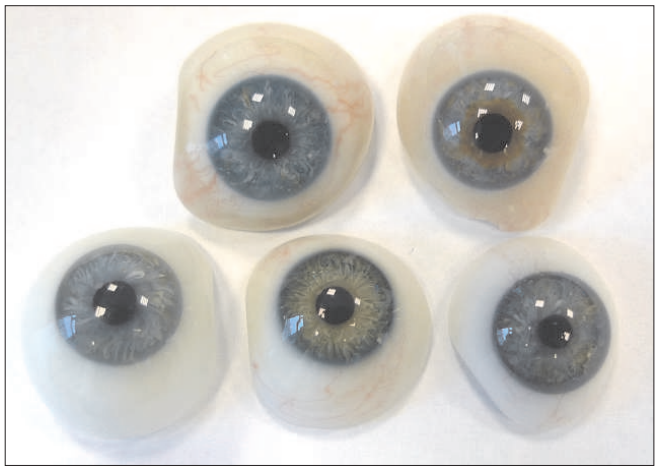
Imitacje z kleju WIKOL (płaskie i cienkie)



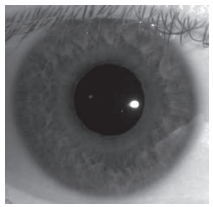
Biometryczny obraz fałszywego odcisku

Podatność biometrii na ataki

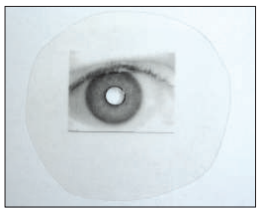
Imitacje przygotowywane w laboratoriach IAiIS PW oraz NASK



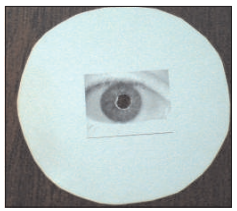
Modele oka (protezy)



Obraz biometryczny autentycznej tęczówki



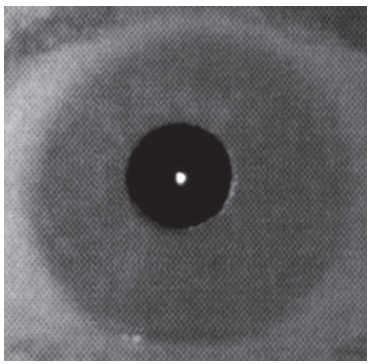
Wydruk na folii



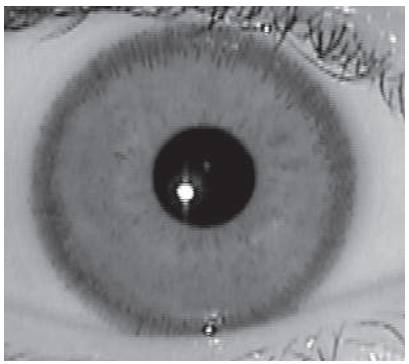
Wydruk na papierze

Obrazy biometryczne falsyfikatów:

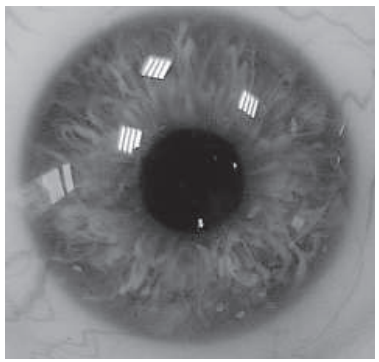
Wydruk papierowy



Wydruk na szkle kontaktowym



Model oka (proteza)



Podatność biometrii na ataki

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

Podatność biometrii na ataki

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

Podatność biometrii na ataki

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

Podatność biometrii na ataki

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

Podatność biometrii na ataki

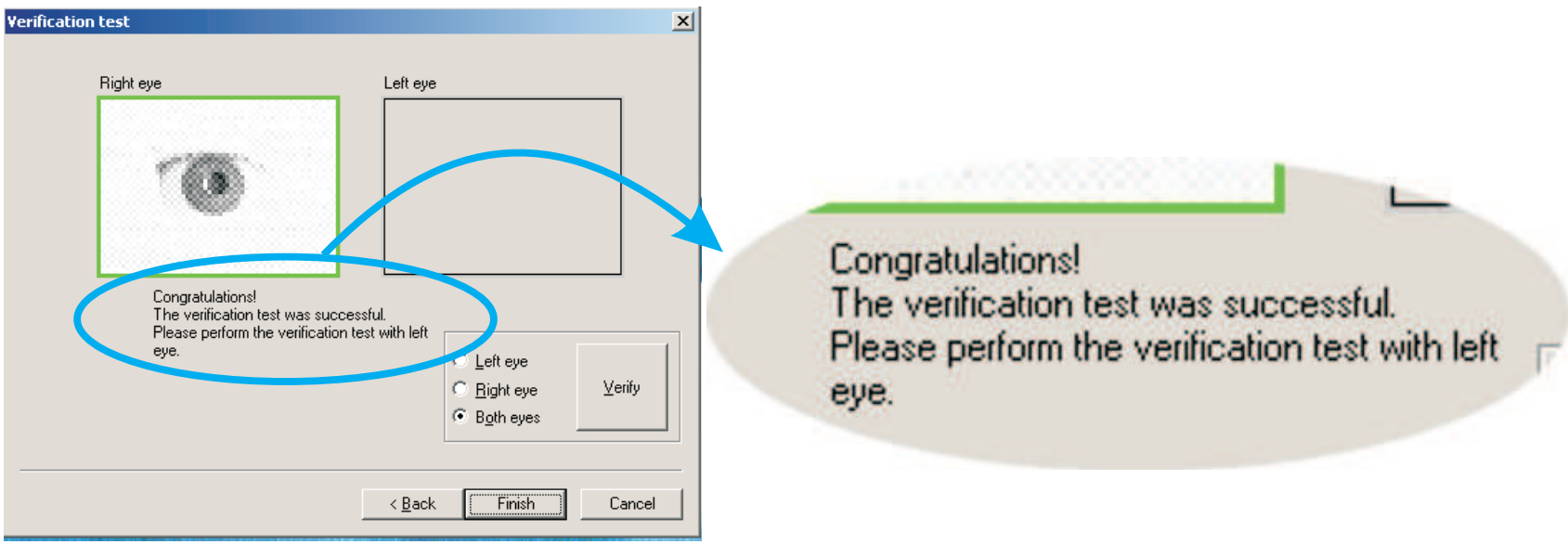
Eksperymenty PW/NASK, 2005 r. (tęczówka)

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
   - testowane systemy: Panasonic ET100, Panasonic ET300, OKI IrisPass-M
   - weryfikacja: **wszystkie** kamery zaakceptowały wydruki (ET100 73,1%, ET300 15,6%)

Podatność biometrii na ataki

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



Podatność biometrii na ataki

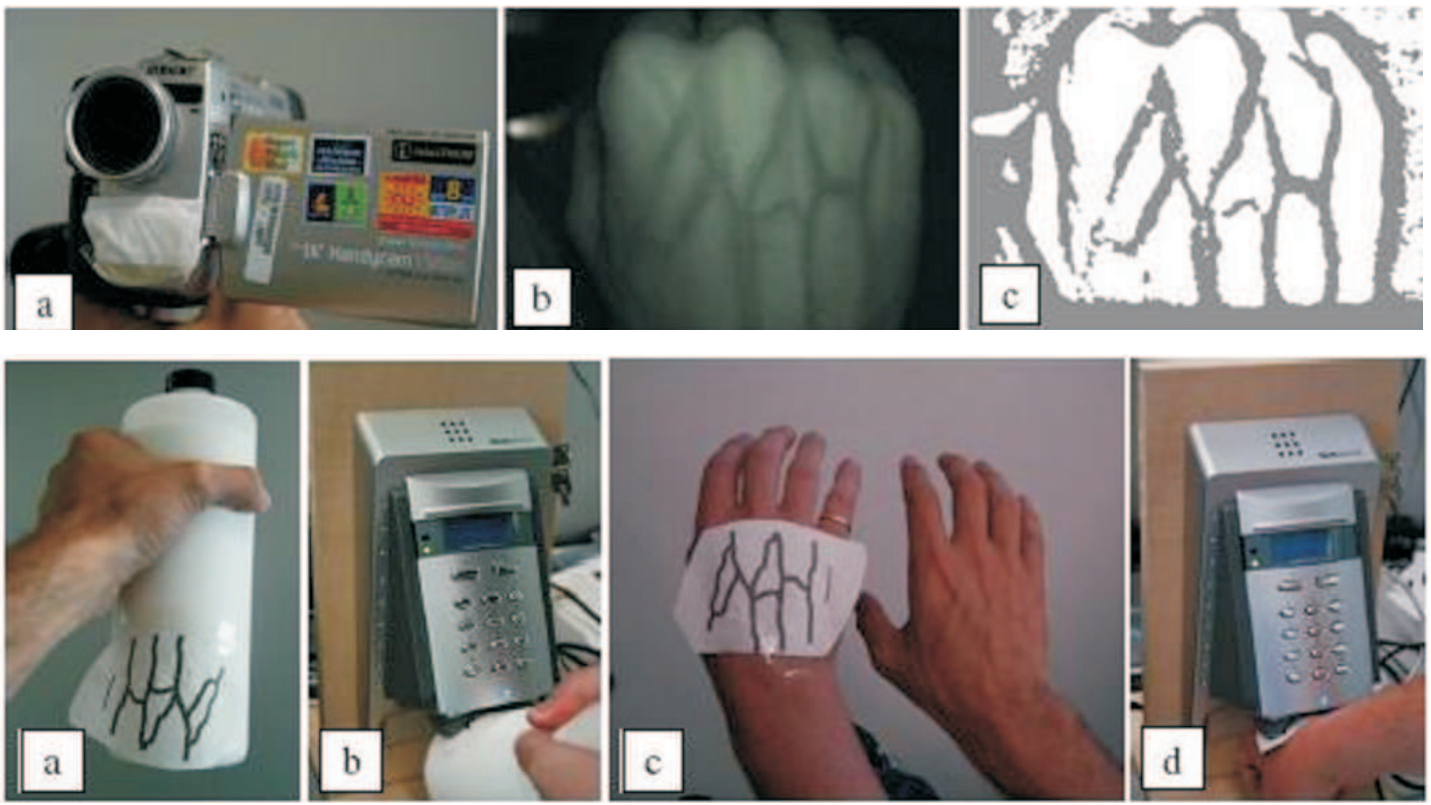
Eksperymenty FIDIS, 2006 r. (żyły dłoni)

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

Podatność biometrii na ataki

Eksperymenty FIDIS, 2006 r. (żyły dłoni)



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

Podatność biometrii na ataki

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

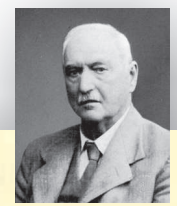
źródło: T. Matsumoto, How to measure security of embedded black-box systems, 9th Global Business Dialog on Electronic Commerce Summit, 9 November 2007, Tokyo, Japan

Podatność biometrii na ataki

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?"

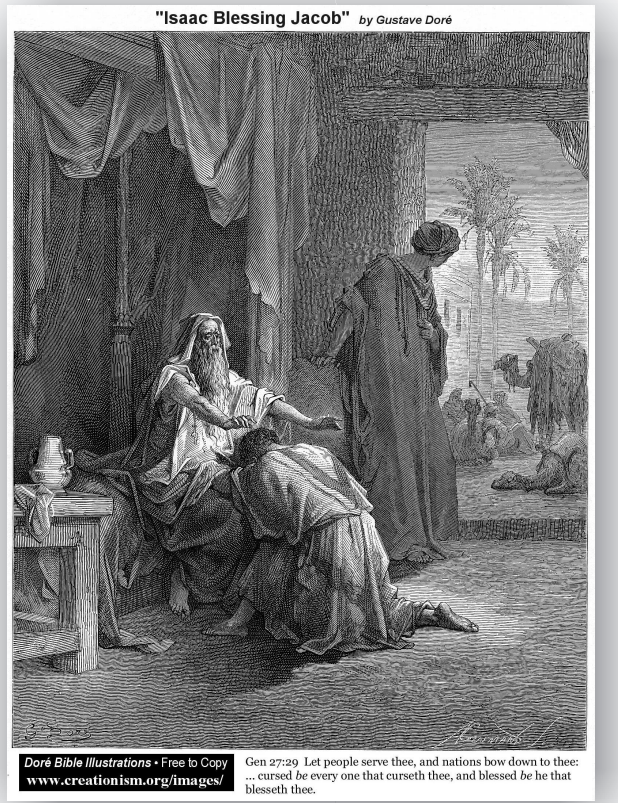
"Much more so, and infinitely more secure. A signature, being written with a pen, requires that the forgery should also be written with a pen, a process demanding very special skill and, after all, never resulting in an absolute *facsimile*. But a finger-print is a stamped impression—the finger-tip being 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."

Podatność biometrii na ataki

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

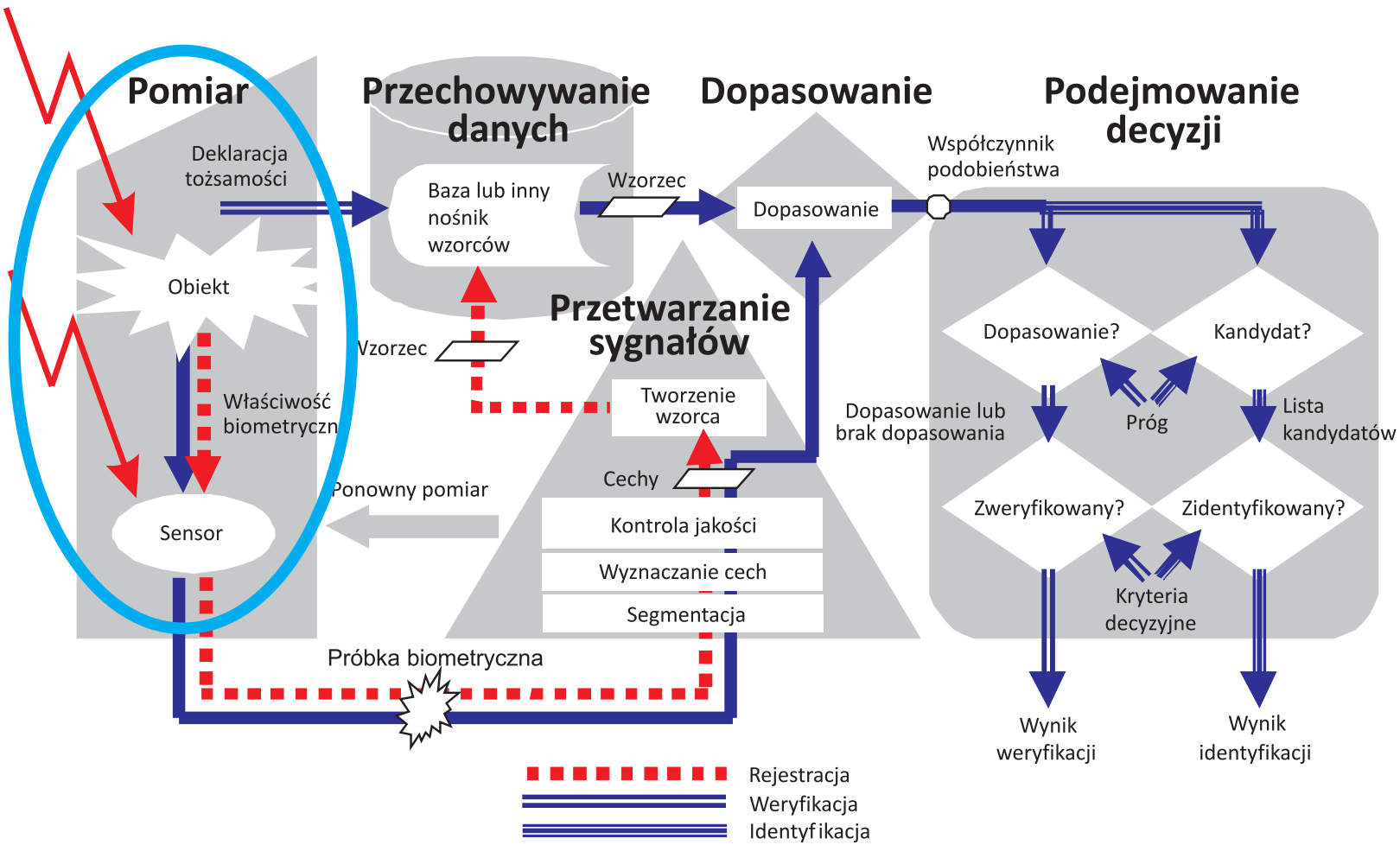


Testowanie bezpieczeństwa biometrii

1. 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)
2. Zagrożenia
   - Ograniczona dokładność biometrii
   - Wykorzystanie imitacji charakterystyki biometrycznej
   - Modyfikacja charakterystyki biometrycznej
   - Wykorzystanie syntetycznych danych biometrycznych
   - Kradzież charakterystyki biometrycznej
   - Kradzież i modyfikacja danych biometrycznych
   - Działanie w nieprzyjaznym środowisku
   - Błędy proceduralne procesu rejestracji

Podatność biometrii na ataki

System biometryczny wg ISO/IEC 19794-1:2011



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

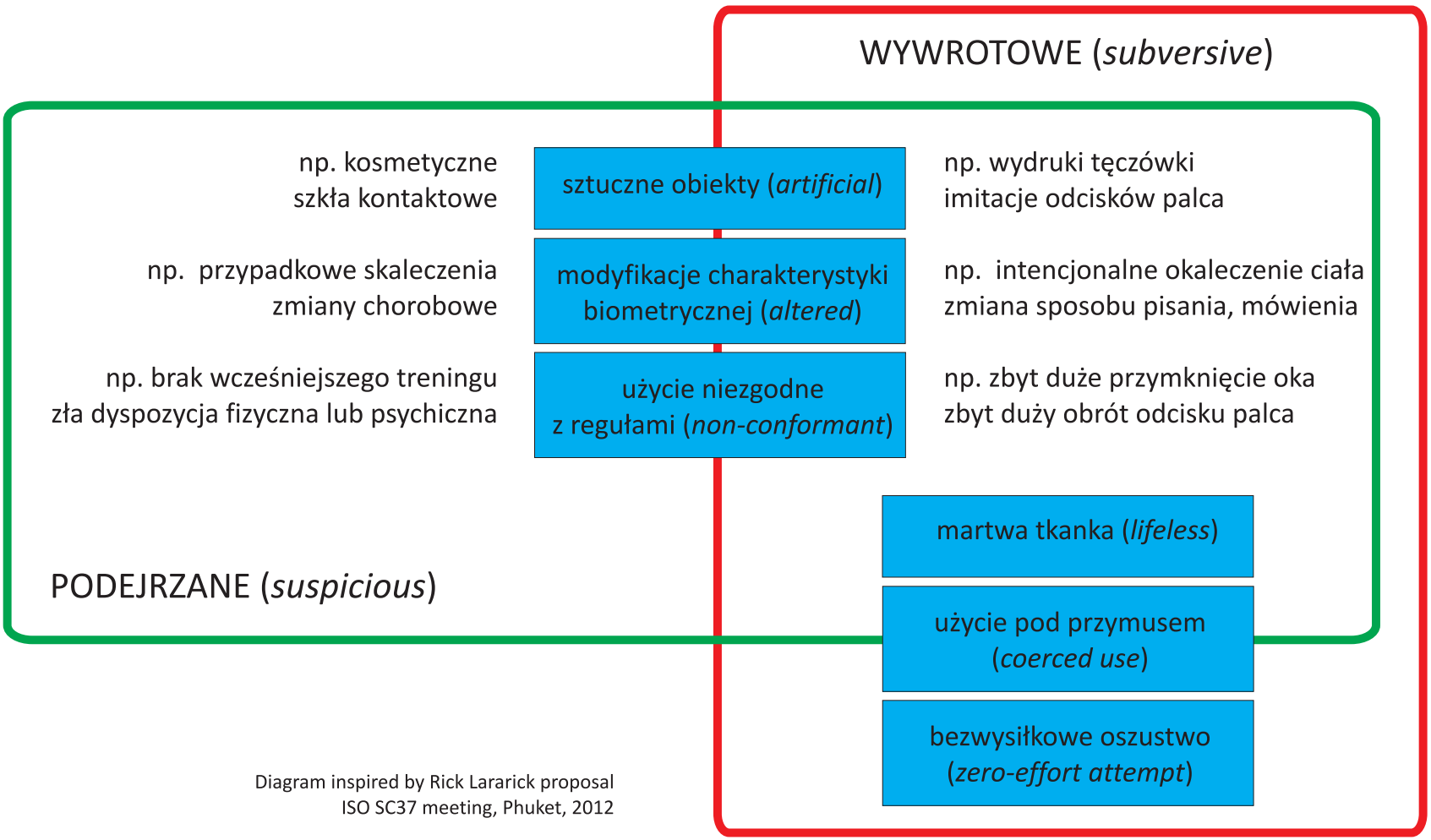


Diagram inspired by Rick Lararick proposal
ISO SC37 meeting, Phuket, 2012

Wykład 11: Bezpieczeństwo sensorów biometrycznych
Podatność urządzeń biometrycznych na ataki
Testowanie żywotności palca
Testowanie żywotności oka

Rozpoznawanie imitacji przez urządzenia

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 $\longrightarrow$ testowanie żywotności lub (ogólniej) testowanie autentyczności (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

Obraz falsyfikatu czy żywego palca?

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

Obraz falsyfikatu czy żywego palca?

Obrazy wykonane czytnikiem
optycznym z testem żywotności (Futronic)

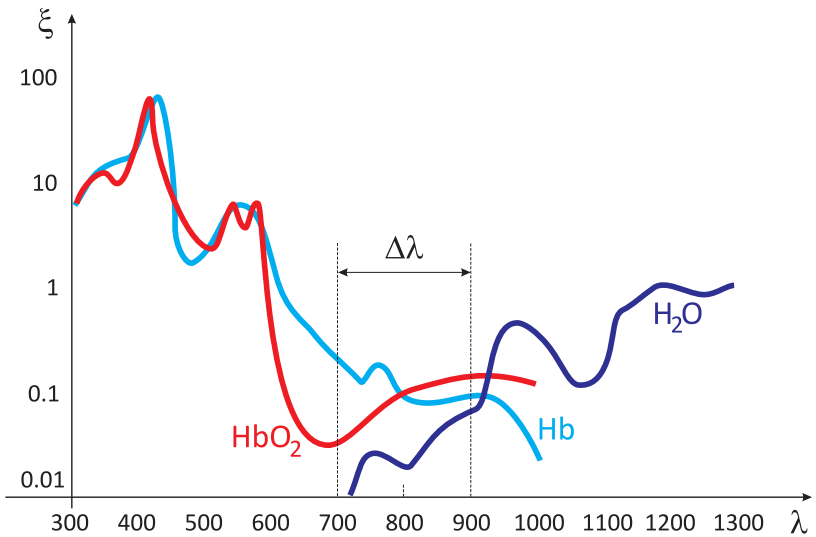
źródło: laboratorium BIT, semestr letni 2010

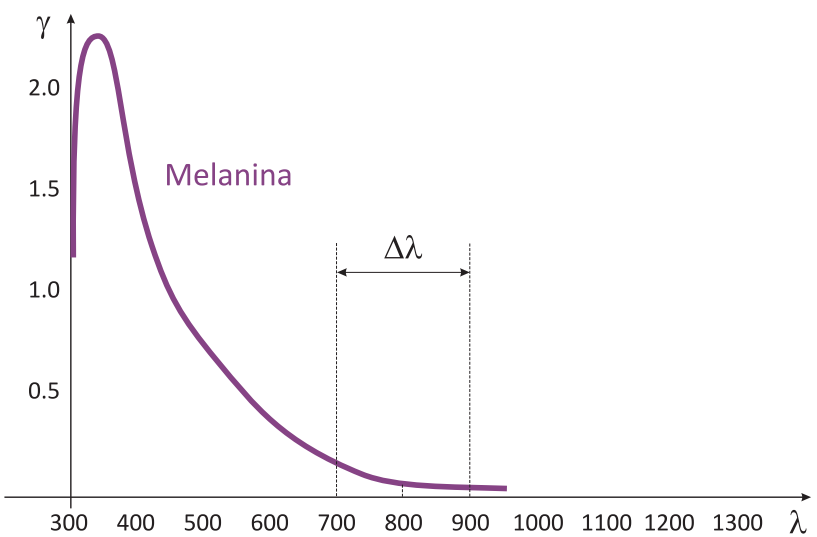
Metody testowania żywotności

▲ 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"

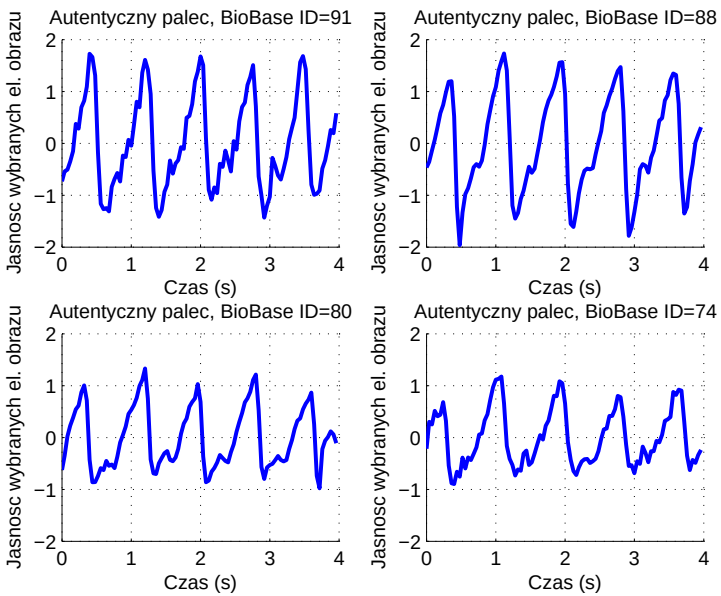
Metody testowania żywotności

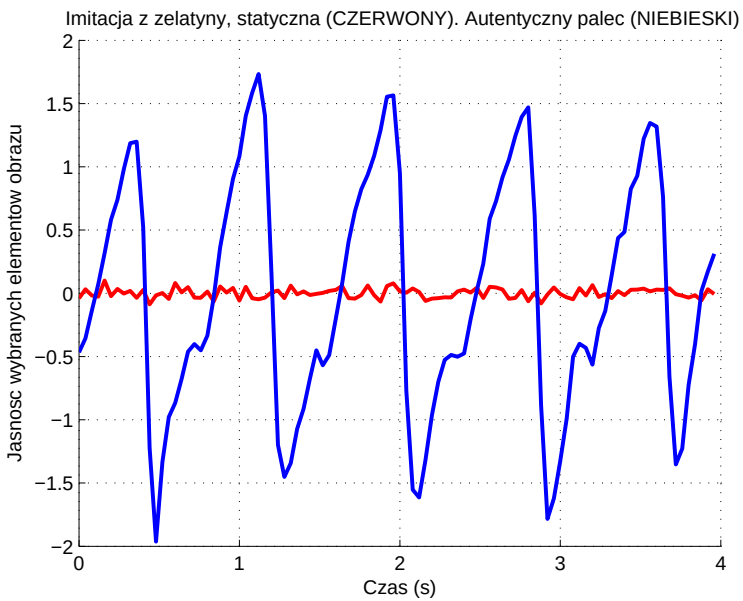
▲ Wodoszczelny czytnik Lumidigm testujący żywotność palca (analiza spektralna)

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

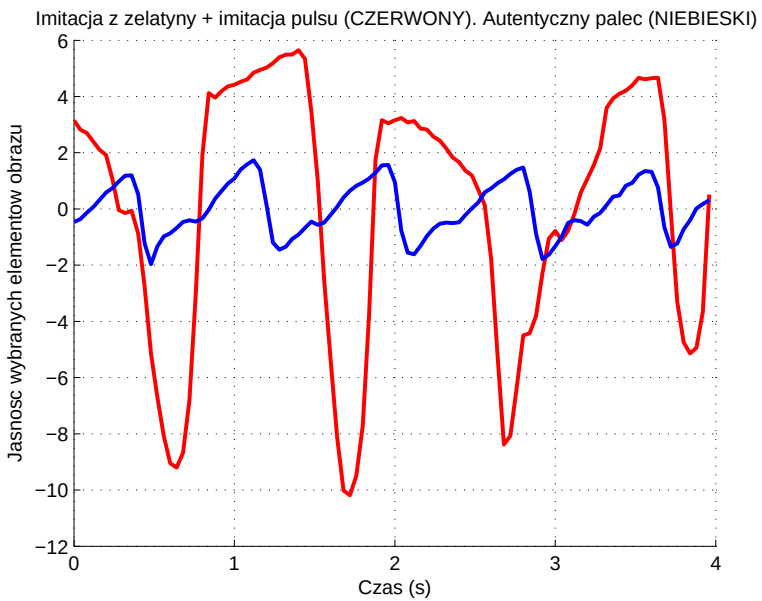
Analiza obrazu po prześwietleniu palca światłem w zakresie podczerwieni. Łatwe rozpoznawanie statycznych obiektów.

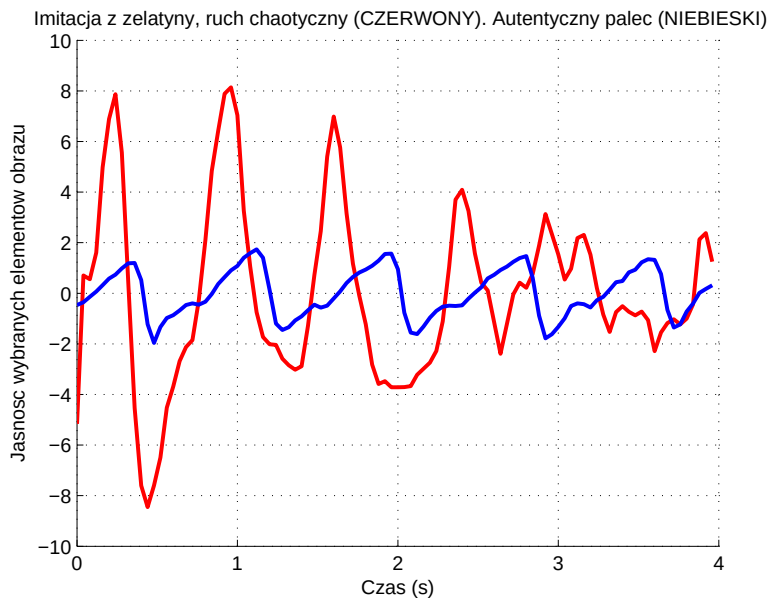




Detekcja pulsu

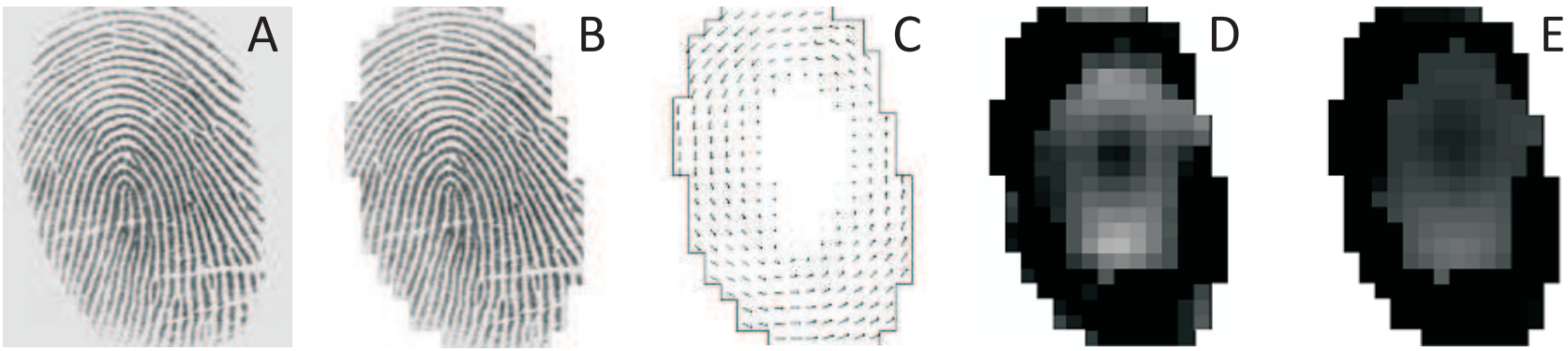
Trudniejsze (ale możliwe) rozpoznawanie obiektów w ruchu (celowa imitacja pulsu lub ruchy chaotyczne dla zaburzania pomiaru).





Analiza deformacji palca

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

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

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

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

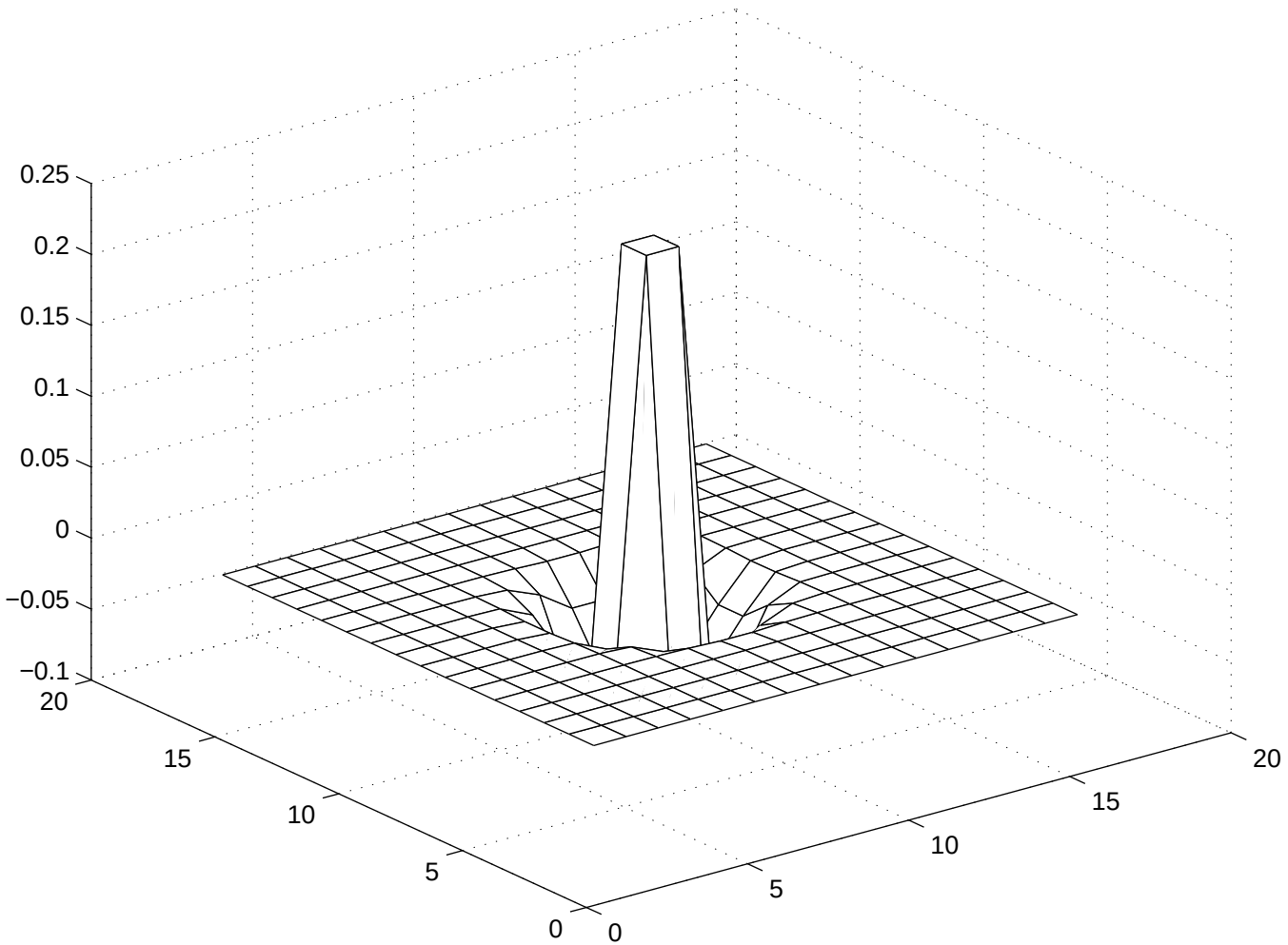
obraz falsyfikatu
(klej WIKOL)

Analiza liczności porów

1. Filtracja i progowanie obrazu
   - wykorzystanie laplasjanu gaussowskiego → 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
6. Wyniki
   - EER bliskie 0% (przy stosowaniu kleju WIKOL do tworzenia fałszywych obiektów)

Analiza liczności porów

Laplasjan gaussowski

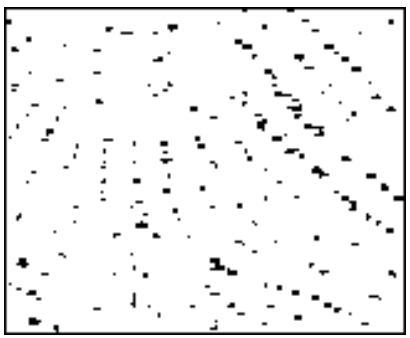


Analiza liczności porów

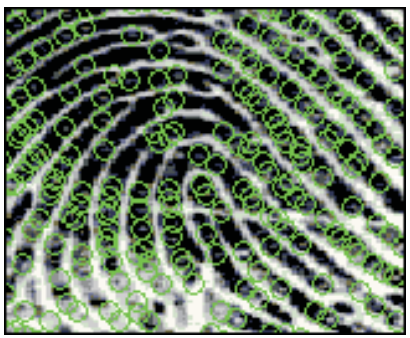
Przykładowy wynik analizy dla obrazu żywego palca

obraz binarny

obraz binarny
po erozji morfologicznej



wstępna lokalizacja
porów (wynik filt. LoG)

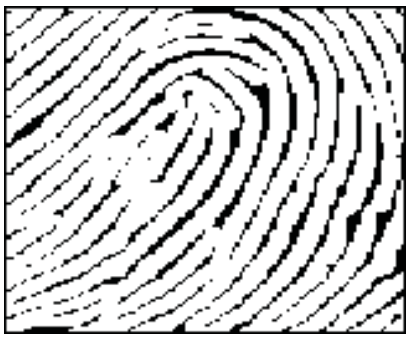


finalna lokalizacja
porów

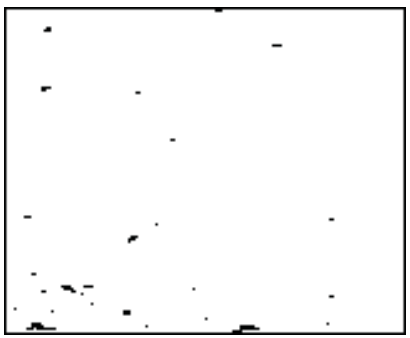
Analiza liczności porów

Przykładowy wynik analizy dla obrazu falsyfikatu

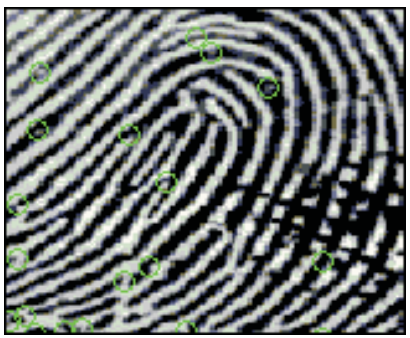
obraz binarny



obraz binarny
po erozji morfologicznej



wstępna lokalizacja
porów (wynik filt. LoG)



finalna lokalizacja
porów

Wykład 11: Bezpieczeństwo sensorów biometrycznych

- Podatność urządzeń biometrycznych na ataki
- Testowanie żywotności palca
- Testowanie żywotności oka

Systematyka fałszerstw

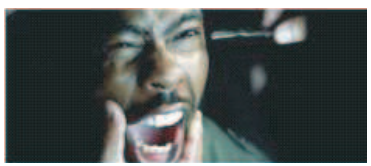
1. Obraz statyczny
   - papierowy wydruk tęczówki
   - obraz na ekranie monitora
   - hologram
2. Obraz dynamiczny
   - off-line: z wykorzystaniem wiedzy *a priori*
   - on-line: z wykorzystaniem wiedzy *a posteriori*
3. Sztuczne oko
   - model z tworzywa
   - żywe oko + szkła kontaktowe
4. Prawdziwe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

Dracula (2000)

Demolition man (1993)

Never say never again (1983)

Minority report (2002)



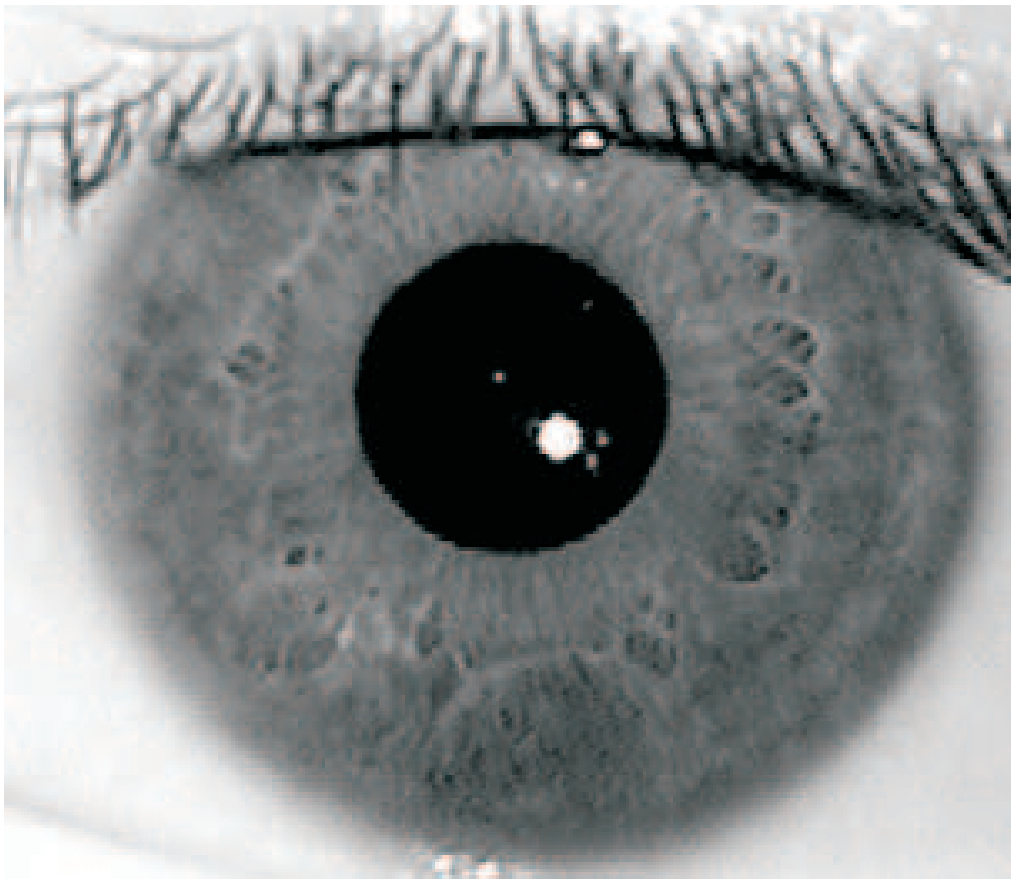
Bad Company (2002)

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

Metody testowania żywotności oka

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



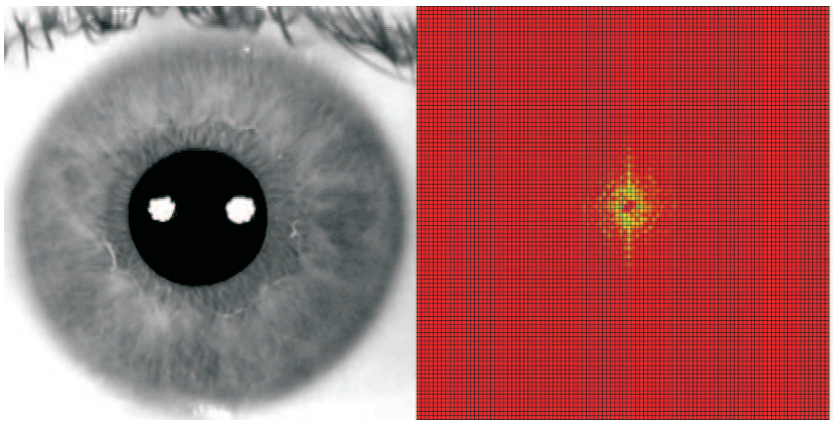
obraz pozyskany kamerą
LG Iris Access 2200

Metody testowania żywotności oka

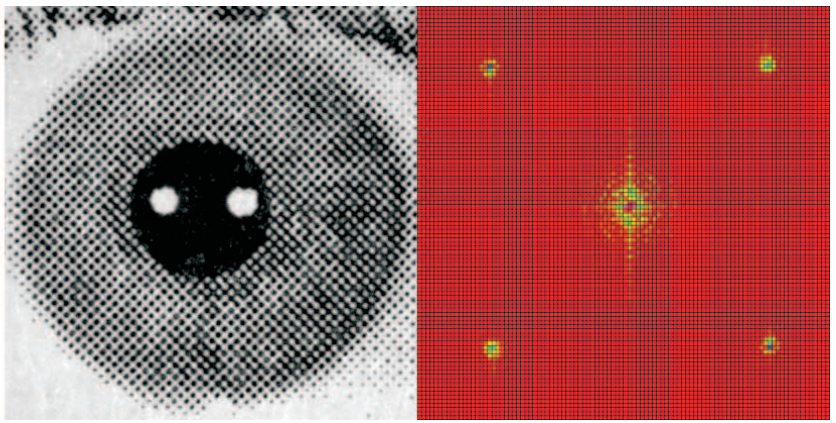
1. Obiekt statyczny, pomiar pasywny
   - cechy dwuwymiarowe: analiza częstotliwościowa
   - cechy trójwymiarowe: analiza kształtu gałki ocznej, struktury mięśnia tęczówki
   - analiza tzw. odbić Purkiniego (odbicia od soczewki i źrenicy)
2. Obiekt dynamiczny, pomiar pasywny
   - spontaniczne ruchy źrenicy (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

Analiza częstotliwościowa

FA – Frequency Analysis [A. Czajka, A. Pacut, 2006, 2012]



Zdjęcie i widmo amplitudowe autentycznej tęczówki

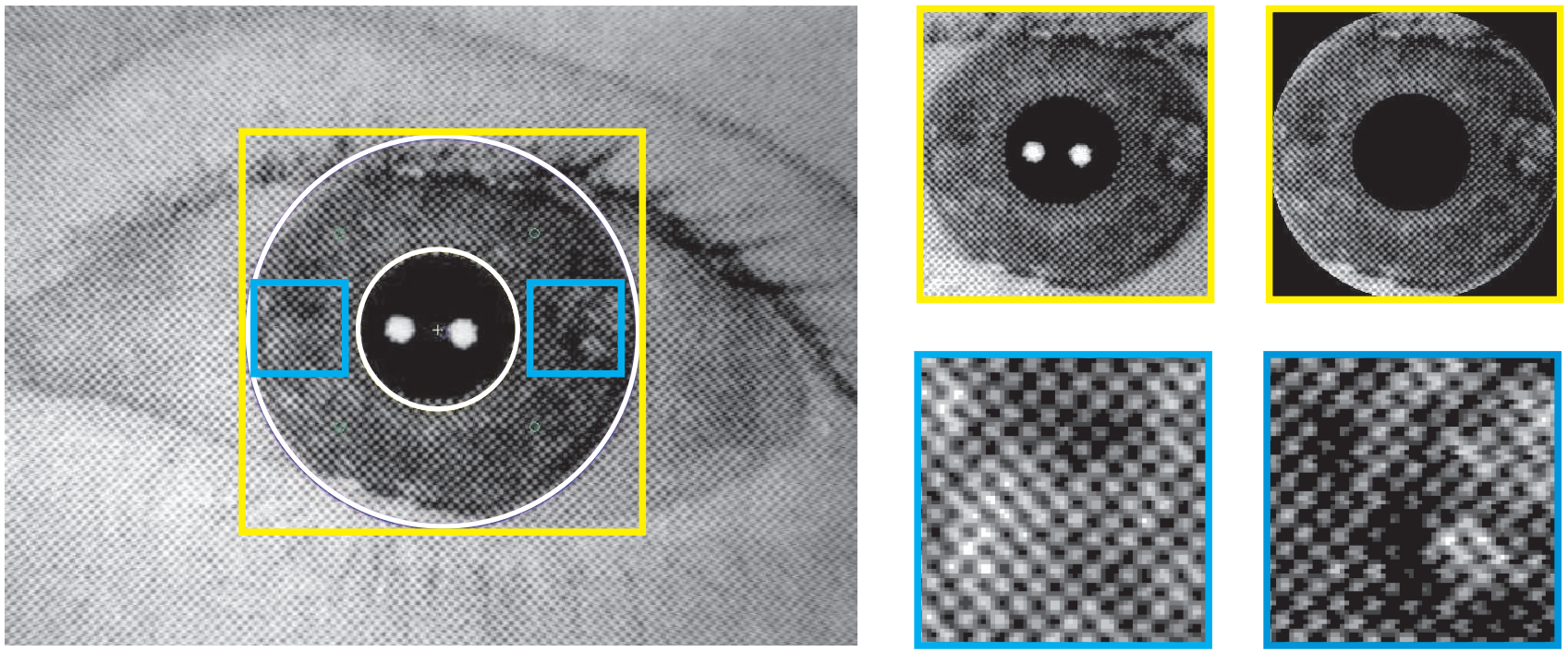


Zdjęcie i widmo amplitudowe wydruku tęczówki

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

Analiza częstotliwościowa

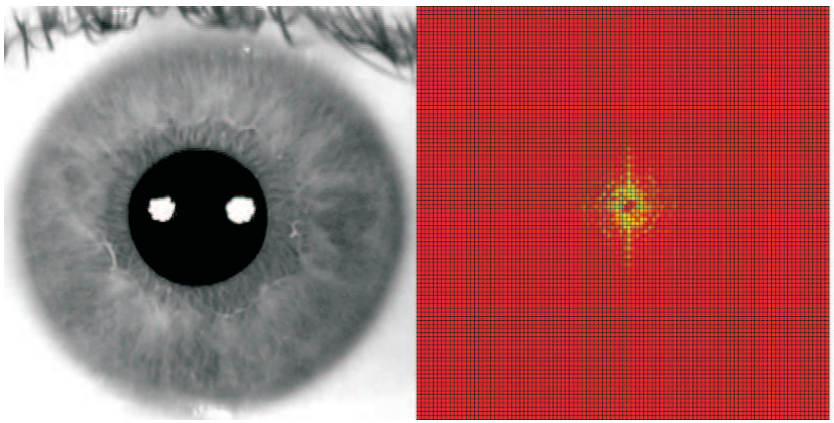
FA – Frequency Analysis [A. Czajka, A. Pacut, 2006, 2012]



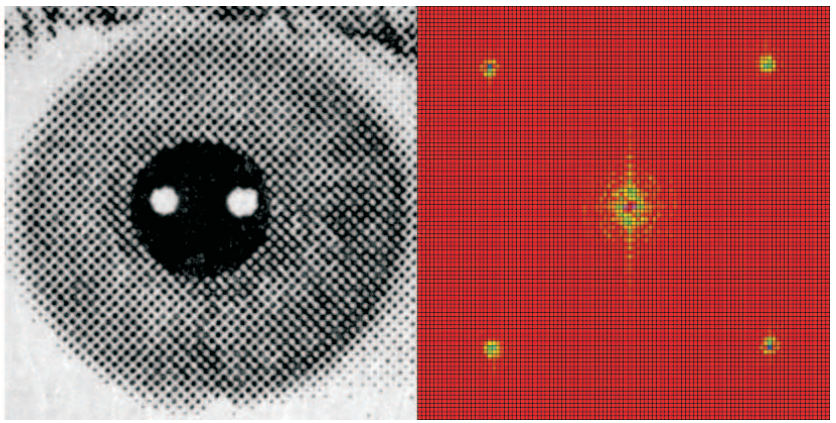
2. Wymagana segmentacja tęczówki
   - 'łatwa' dla zdjęć autentycznych tęczówek
   - nieprzewidywalna dla zdjęć imitacji

Analiza częstotliwościowa

FA – Frequency Analysis [A. Czajka, A. Pacut, 2006, 2012]



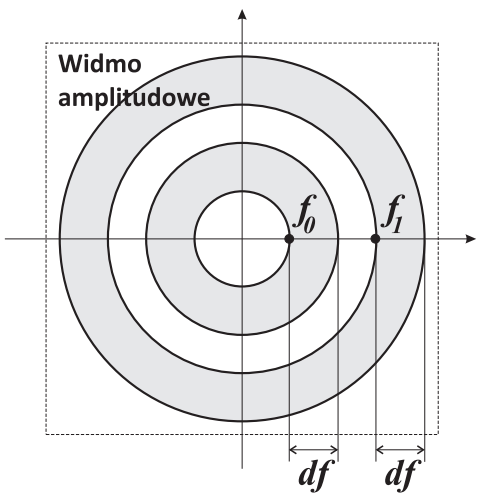
Zdjęcie i widmo amplitudowe autentycznej tęczówki



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:

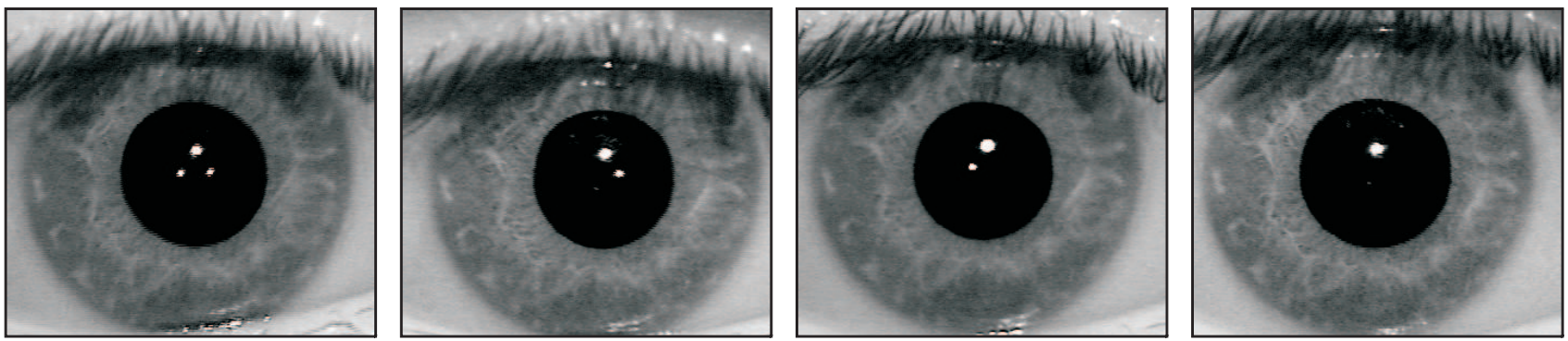
$$F'(\mathbf{Ru}) = F(\mathbf{u}) \quad \text{lub} \quad F'(\mathbf{u}) = F(\mathbf{R}^{-1}\mathbf{u})$$

Metody testowania żywotności oka

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

Analiza stymulowanych odbić

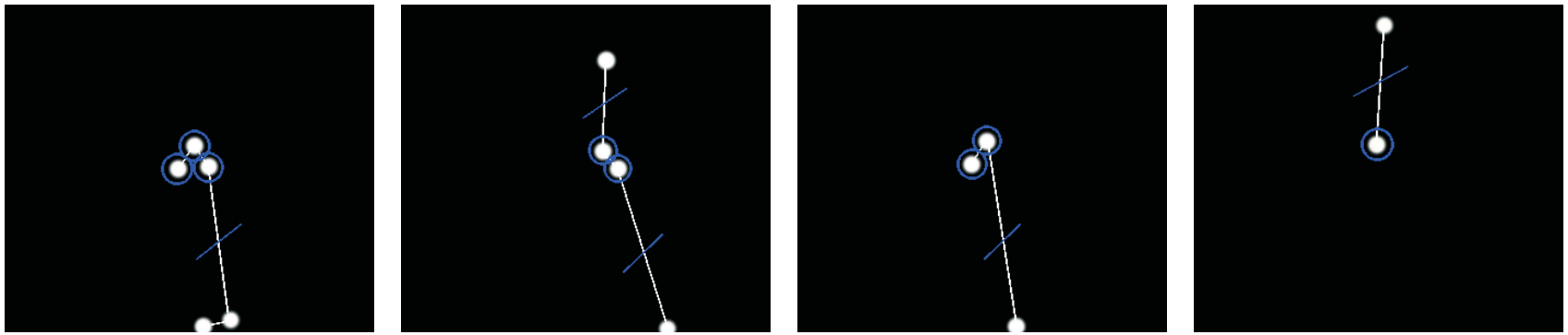
CLR – Controlled Light Reflection [A. Czajka, A. Pacut, 2006]



1. Oświetlenie dodatkowymi źródłami podczerwieni

Analiza stymulowanych odbić

CLR – Controlled Light Reflection [A. Czajka, A. Pacut, 2006]



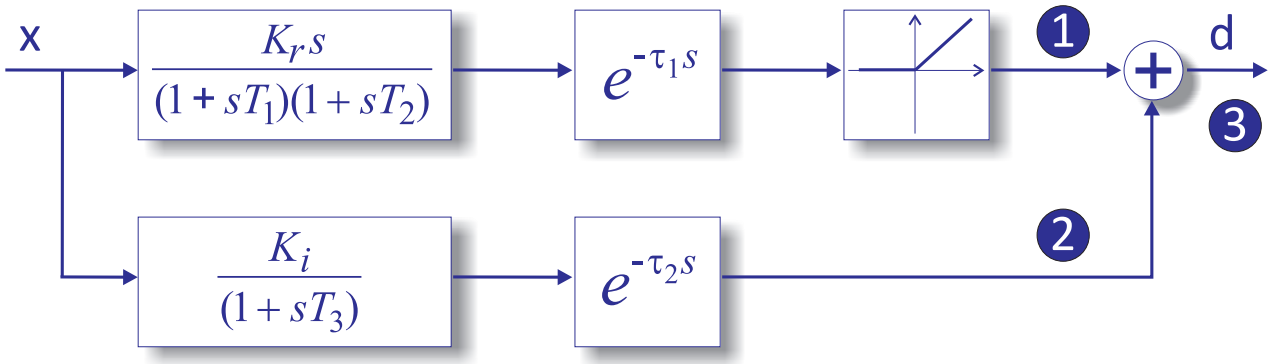
2. Weryfikacja położenia odbić
   - lokalizacja odbić (filtr LoG – laplasjan gaussowski)
   - indeksacja odbić
   - określenie wzajemnego położenia odbić: konstrukcja drzewa rozpinającego
   - eliminacja "fałszywych" odbić (usunięcie "zbyt krótkich" i "zbyt długich" krawędzi drzewa)
3. Porównanie otrzymanej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

Metody testowania żywotności oka

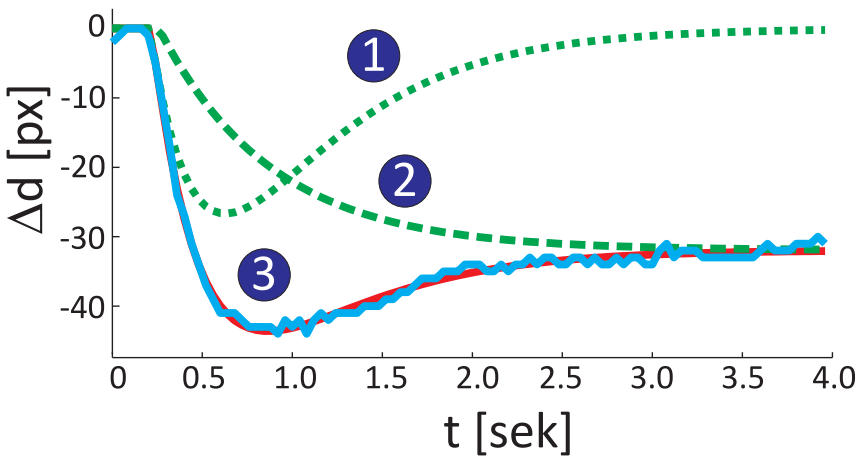
1. Obiekt statyczny, pomiar pasywny
   - cechy dwuwymiarowe: analiza częstotliwościowa
   - cechy trójwymiarowe: analiza kształtu gałki ocznej, struktury mięśnia tęczówki
   - analiza tzw. odbić Purkiniego (odbicia od soczewki i źrenicy)
2. Obiekt dynamiczny, pomiar pasywny
   - spontaniczne ruchy źrenicy (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

Analiza dynamiki źrenicy

PD - Pupil Dynamics [A. Czajka, A. Pacut, 2006]



źródło: A. Czajka, A. Pacut, M.Chochowski
"Method of Eye Aliveness Testing
and Device for Eye Aliveness Testing"
US Patent No. 8,061,842



1. Stymulacja oka światłem widzialnym o zmiennej intensywności i modelowanie reakcji oka (zmian wielkości źrenicy)

Analiza dynamiki źrenicy

PD - Pupil Dynamics [A. Czajka, A. Pacut, 2006]

2. Identyfikacja modelu
   - wzorzec żywotności: wektor ϕ parametrów wzmocnienia (K_r, K_i), stałe czasowe (T_1, T_2, T_3) oraz opóźnienia torów (τ_1, τ_2)
   - minimalizacja błędu dopasowania

$$\widehat{\phi} = \underset{\phi \in \Phi}{\operatorname{argmin}} \sum_{i=1}^{N} (\widehat{d}[i;\phi] - d[i])^2$$

gdzie Φ – zbiór dopuszczalnych wartości ϕ, $\widehat{d}[i;\phi]$ – wyjście modelu, $d[i]$ – rzeczywista (zaobserwowana) zmienność wielkości źrenicy

Analiza dynamiki źrenicy

PD - Pupil Dynamics [A. Czajka, A. Pacut, 2006]

3. Weryfikacja wzorca żywotności (parametrów modelu)
   - etap I – weryfikacja hipotezy
     "testowany obiekt zmienia się w czasie"
   - etap II – weryfikacja hipotezy
     "testowany obiekt zmienia się w czasie jak ludzkie oko"

Testowanie wybranych metod

1. Dane estymacyjne
   - 569 wydruków dla 29 różnych tęczówek
   - drukarki (laserowe): Konica Minolta C350, Xerox WorkCentre 24, Cannon IRC 3200
   - nośniki: papier matowy, błyszczący oraz folia
   - rozdzielczość: 300 dpi, 600 dpi
   - rodzaj wydruku: odcienie szarości, pełny kolor
2. Dane testowe
   - 144 wydruki dla 12 różnych tęczówek
   - nośnik: papier matowy
   - rozdzielczość: 600 dpi rodzaj wydruku: pełny kolor
3. Testowane metody
   - Panasonic ET100
   - Panasonic ET300
   - Laboratorium Biometrii NASK/PW

Testowanie wybranych metod

Wyniki [A. Czajka, A. Pacut, 2006, 2012]

Ocena przykładowych systemów komercyjnych (ET-100 i ET-300) oraz proponowanych metod

System	Metoda	Stopień akceptacji imitacji (%)	Stopień odrzucenia żywych oczu (%)	Możliwości wykrycia fałszerstwa			
				Obraz statyczny	Obraz dynamamiczny	Model oka	Działanie pod przymusem
ET-100	?	73,1	0,0	–	–	–	–
ET-300	?	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	+	+/–	+/–	?

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

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

Co powinniśmy zapamiętać

1. W jaki sposób możemy zabezpieczyć sensor biometryczny?
2. Co daje nam stosowanie metod testowania żywotności?
3. Czym różnią się widma żywej tęczówki i jej wydruku?
4. W jaki sposób możemy wykorzystać zjawisko zmiany wielkości źrenicy w zwiększeniu niezawodności biometrii tęczówki?
5. W jaki sposób możemy wykorzystać istnienie porów na powierzchni palca w celu zwiększenia niezawodności biometrii odcisku?