Biometryczna Identyfikacja Tożsamości

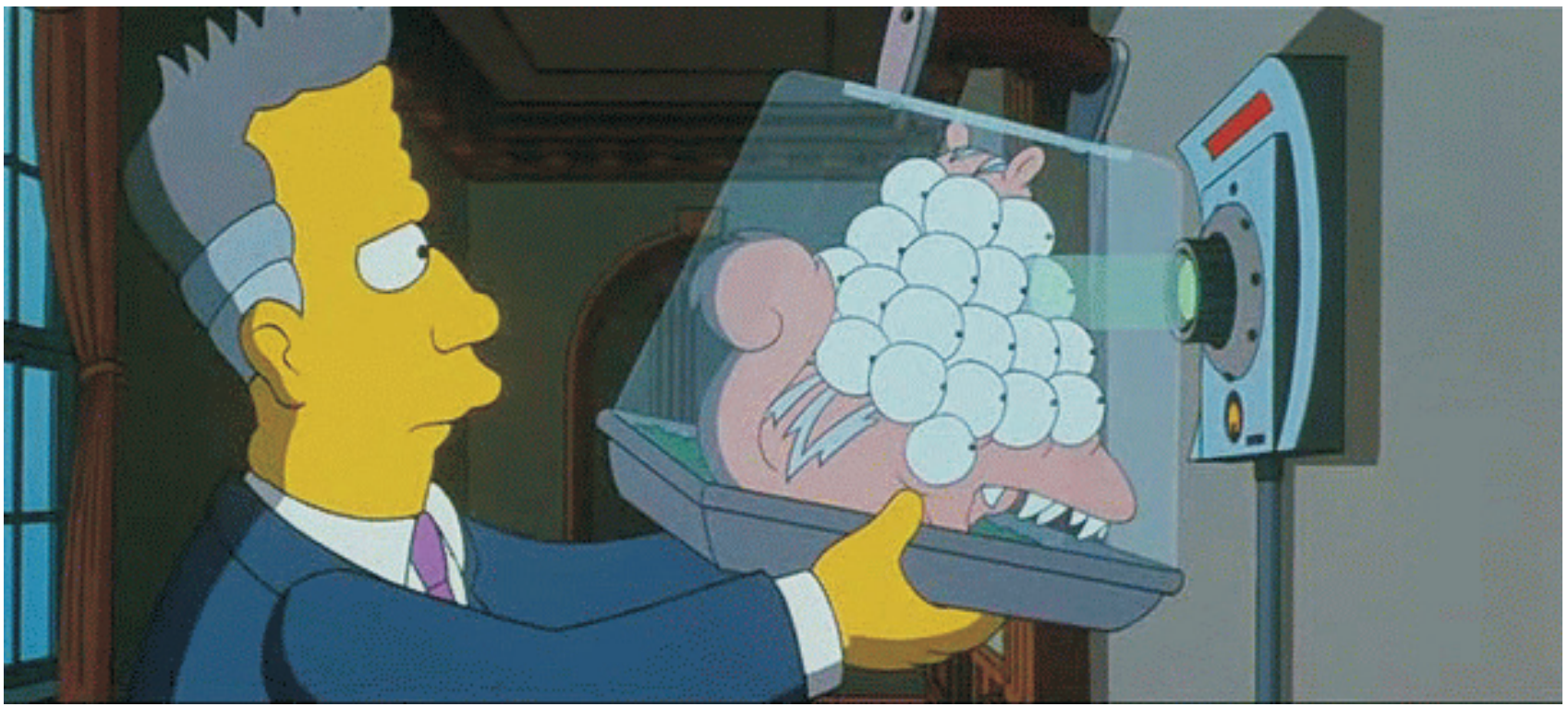
Wykład 3: Bezpieczeństwo sensorów odcisku palca

Adam Czajka

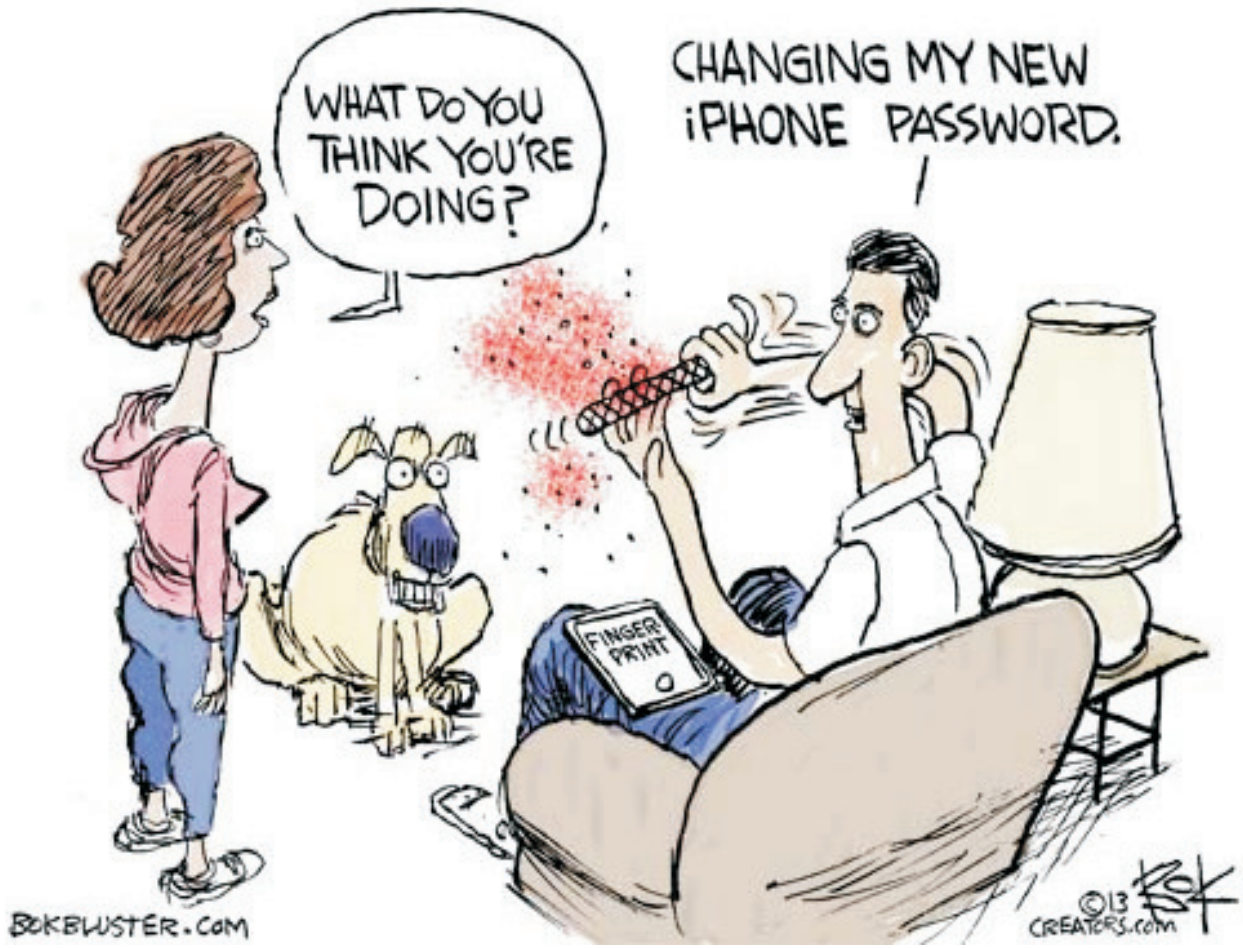
Wykład na Wydziale Elektroniki i Technik Informacyjnych
Politechniki Warszawskiej

Semestr zimowy 2015/16

Czy możemy zastąpić czymś charakterystykę biometryczną?



Czy możemy zmienić naszą charakterystykę biometryczną?



Wykład 3: Bezpieczeństwo sensorów odcisku palca

Podatność sensorów biometrycznych na ataki

Testowanie żywotności palca – metody

Wykład 3: Bezpieczeństwo sensorów odcisku palca

Podatność sensorów biometrycznych na ataki

Testowanie żywotności palca – metody

Imitacje wykorzystywane w laboratoriach IAiIS PW oraz NASK

Forma z modeliny

Magnetyczny proszek daktyloskopijny

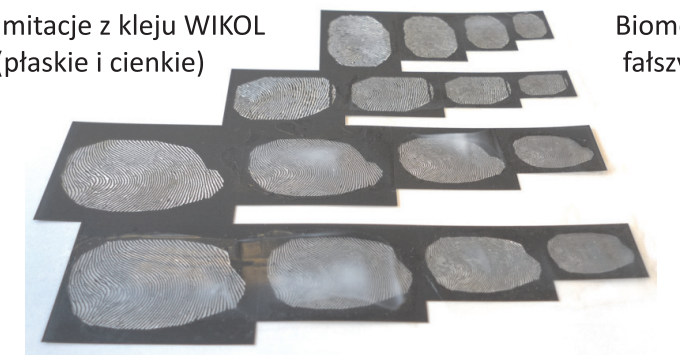
Odcisk utajony w świetle widzialnym

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

Przykłady

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

theguardian

Google™ Custom Search

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

Share 2801 Tweet 1,869 +1 247 Pin it 1 Share 410 Email

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)

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

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.

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

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.

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

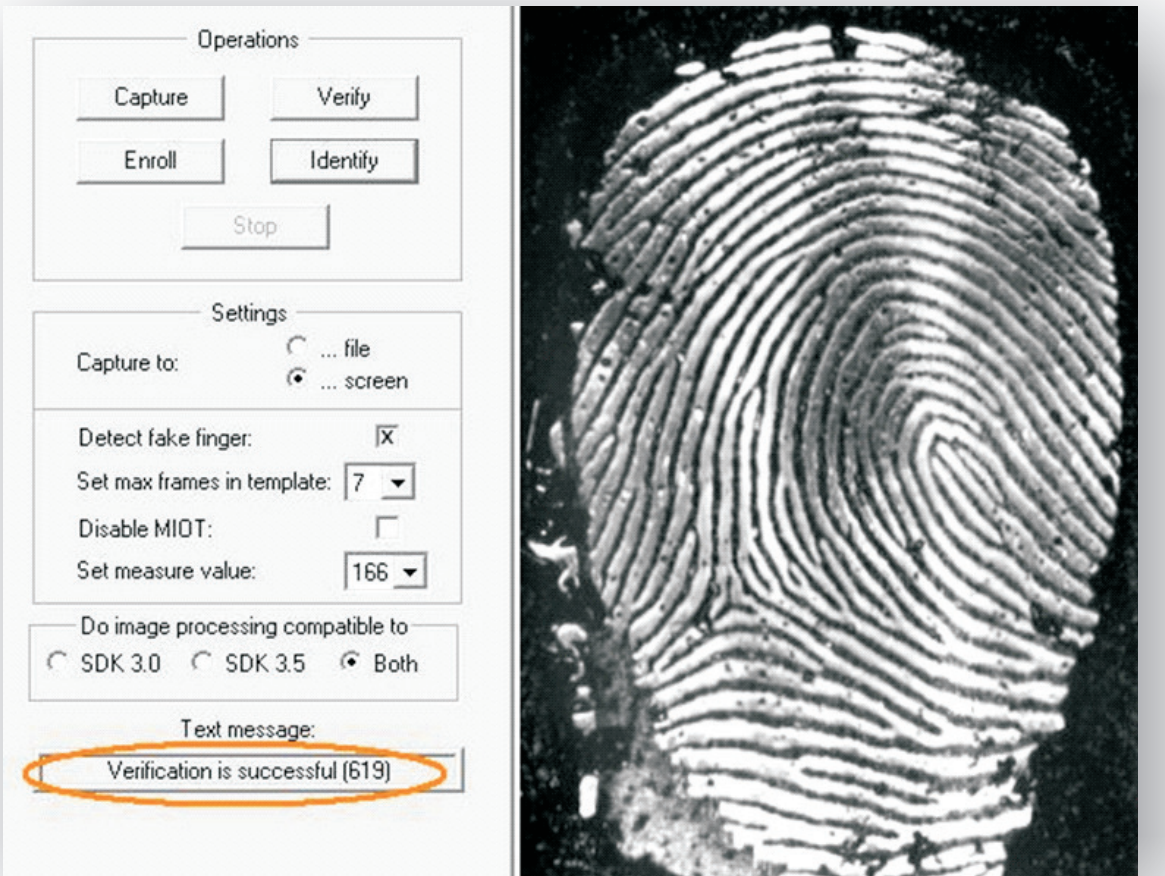
Przykłady

Eksperyment T. Matsumoto, 2004 r.

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

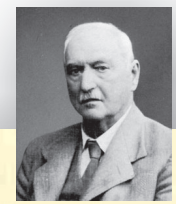
Eksperymenty PW/NASK, 2008 r.



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."

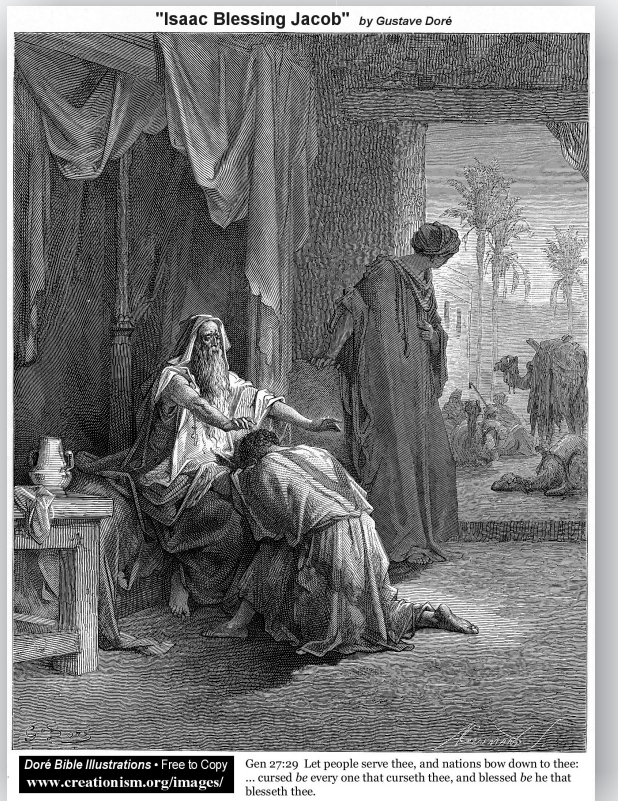
"As easy as to forge a signature, for instance?"

"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

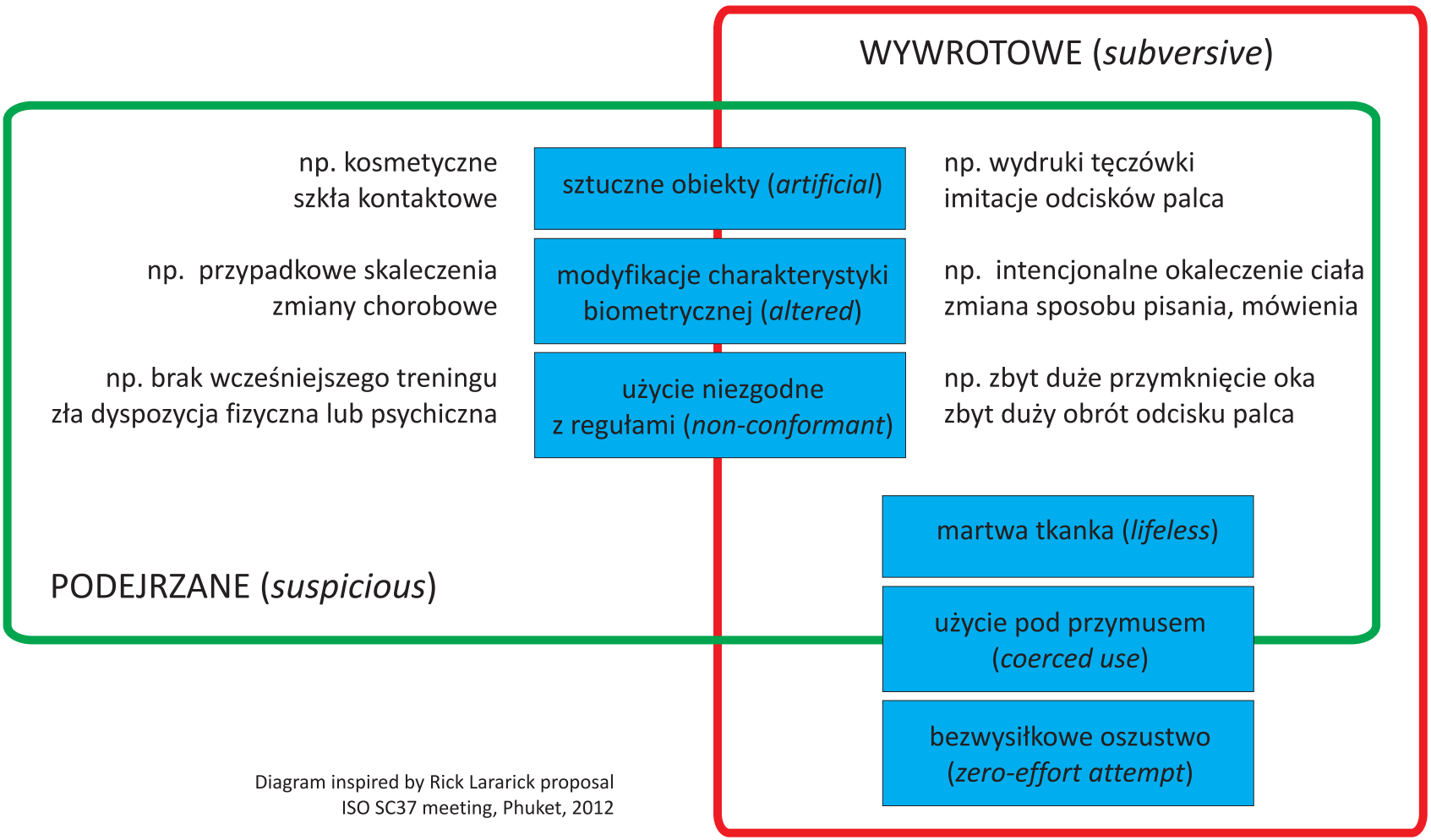


Diagram inspired by Rick Lararick proposal
ISO SC37 meeting, Phuket, 2012

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 3: Bezpieczeństwo sensorów odcisku palca

Podatność sensorów biometrycznych na ataki

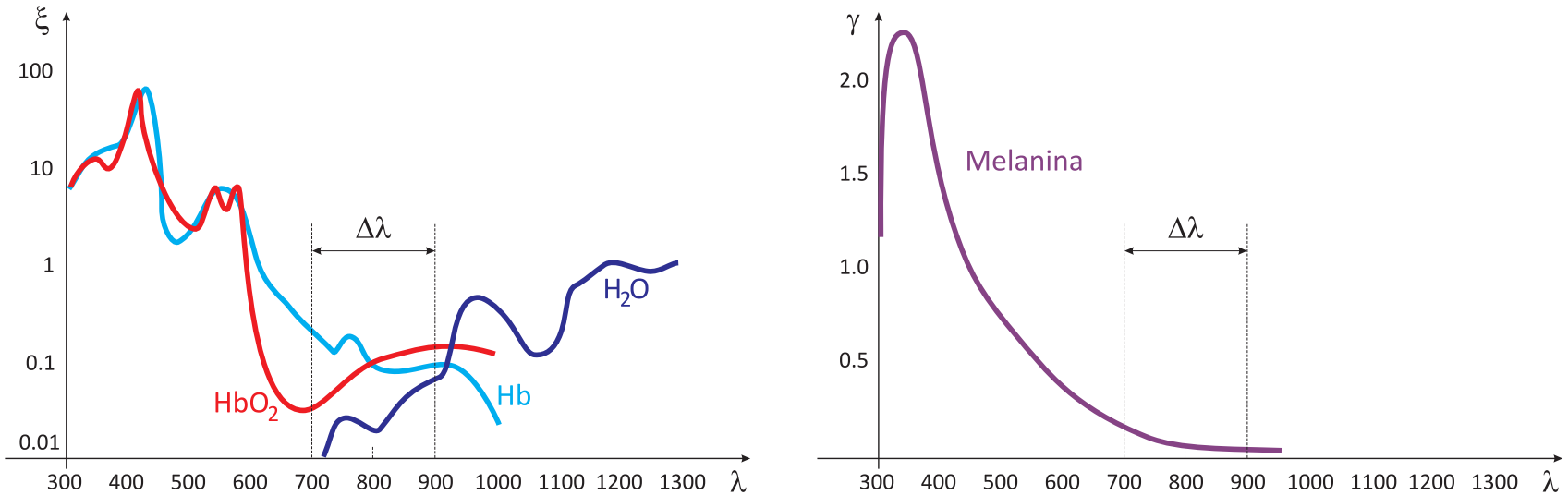
Testowanie żywotności palca – metody

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

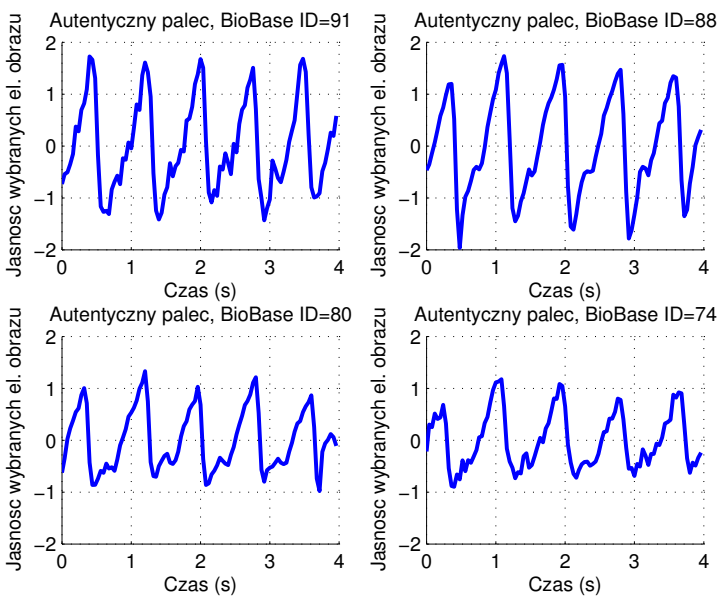
▲ Wodoszczelny czytnik Lumidigm testujący żywotność palca (analiza spektralna)

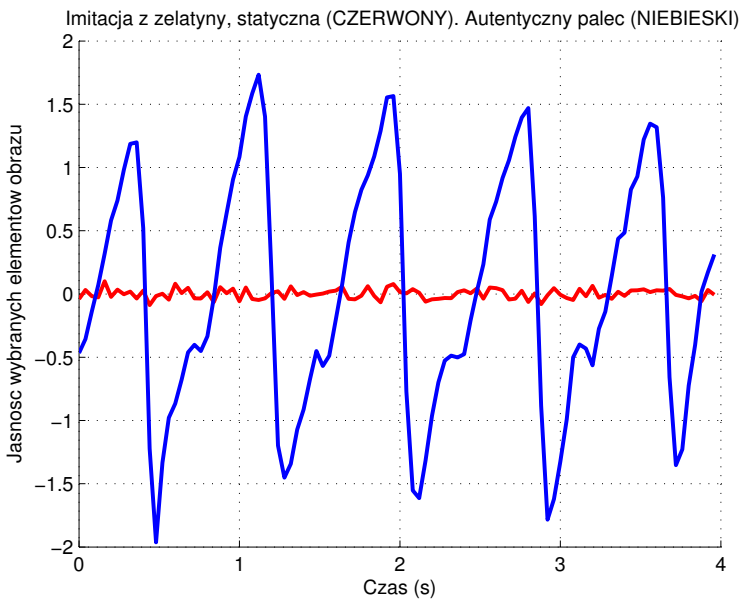
2. Analiza dynamicznych własności palca
   - puls krwi (Lapsley, 1998; A. Czajka, K. Kozioł, 2010)
   - pocenie się skóry (Schuckers, 2004)
   - deformacje palca (Antonelli, 2006)
   - zapach palca (Baldisserra, 2006)

Detekcja pulsu

(A. Czajka, K. Kozioł, 2010)

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

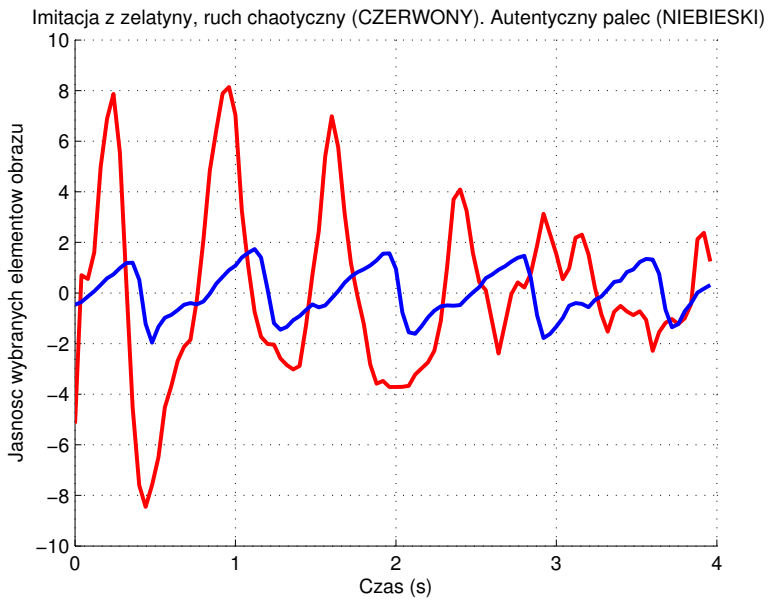




Detekcja pulsu

(A. Czajka, K. Kozioł, 2010)

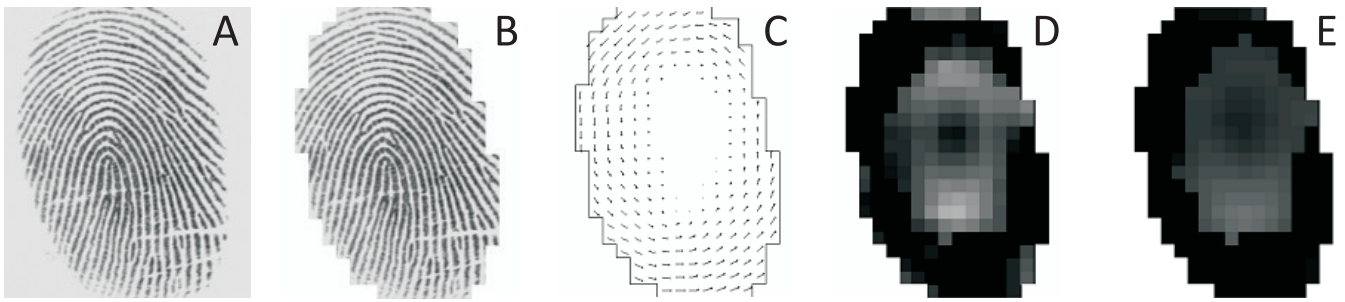
Trudniejsze (ale możliwe) rozpoznawanie obiektów w ruchu (celowa imitacja pulsu lub ruchy chaotyczne dla zaburzania pomiaru).



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)

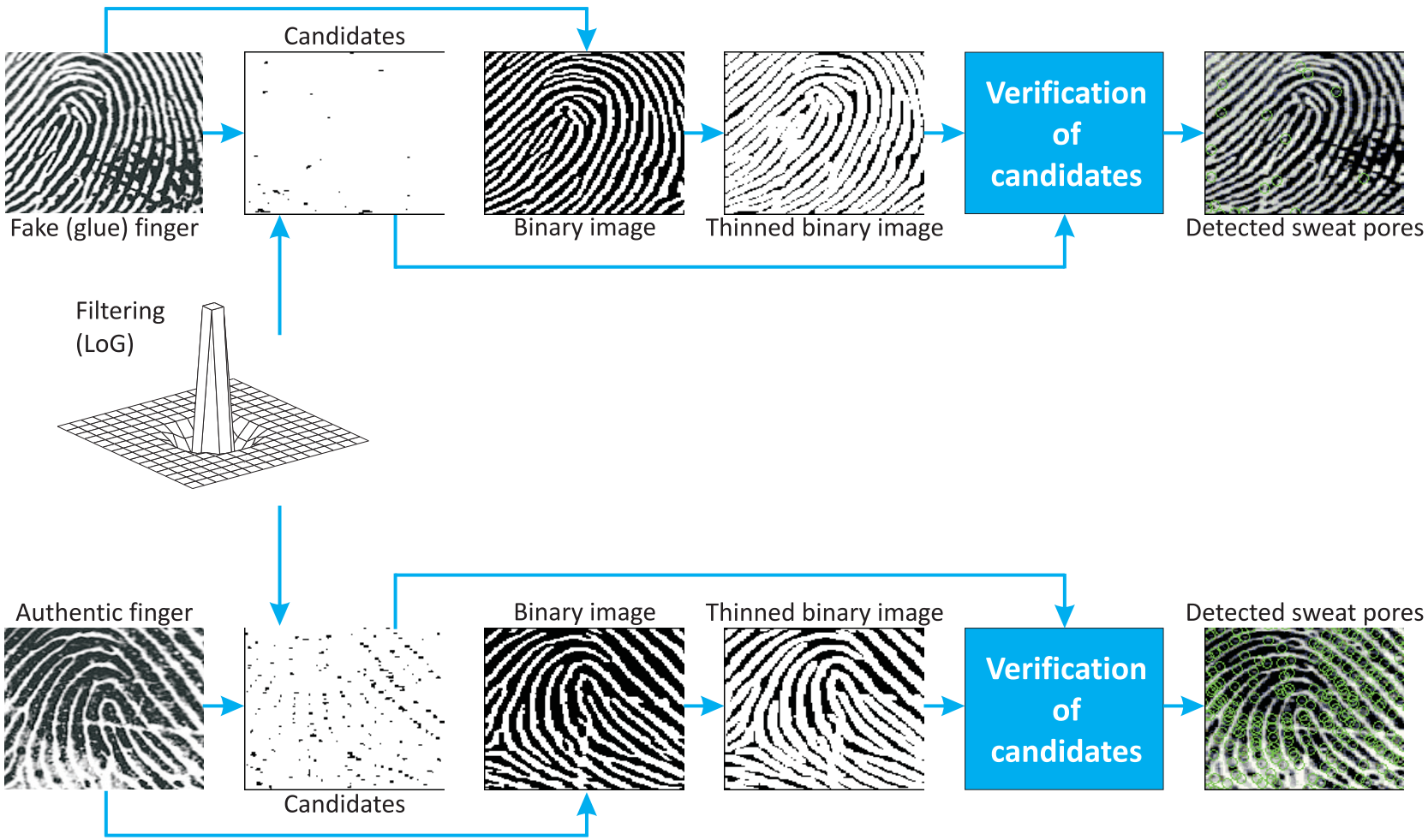
Analiza liczności porów

(P. Strzelczyk, A. Czajka, 2010)

1. Filtracja i progowanie obrazu
   - wykorzystanie laplasjanu gaussowskiego → 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



Przykładowe pytanie egzaminacyjne

Czy wraz ze wzrostem liczby zaakceptowanych fałszywych odcisków palca rośnie FMR?