Polski wkład w biometrię

dr inż. Adam Czajka

Z dr. inż. Adamem Czajką z Pracowni Biometrii Naukowej i Akademickiej Sieci Komputerowej oraz Politechniki Warszawskiej rozmawia Andrzej Popielski

Jaki był początek Pracowni Biometrii NASK/PW?

Początków Pracowni Biometrii należy szukać na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej, dokładnie w Instytucie Automatyki i Informatyki Stosowanej. Tam w 1998 r. rozpocząłem pracę nad systemem biometrii podpisu odręcznego jeszcze w ramach mojej pracy dyplomowej kierowanej przez prof. Andrzeja Pacuta. Wyniki weryfikacji przy użyciu tego systemu były na tyle dobre, że profesor Pacut zachęcił mnie do kontynuowania prac w zakresie biometrii. Współpraca naukowa Politechniki z NASK rozpoczęła się natomiast dużo wcześniej i dotyczyła początkowo metod wyceny i regulacji ruchu w sieci Internet. NASK zainteresował się naszymi wynikami w zakresie biometrii, widząc możliwość jej zastosowania do zwiększania bezpieczeństwa w sieci. I tak w roku 2002 powstała wspólna Pracownia Biometrii NASK/PW. Obecnie jest ona częścią Pionu Naukowego NASK, którego dyrektorem jest profesor Krzysztof Malinowski.

W tym czasie w Polsce niewiele się działo w biometrii, natomiast na świecie jest to tematyka prężna od dawna. Stany Zjednoczone przodują, ale w Europie jest również wiele ośrodków badawczych. Na przykład w biometrii tęczówki pionierski, jeśli chodzi o metodę kodowania, jest zespół matematyka Johna Daugmana z Uniwersytetu w Cambridge. Nasze pierwsze osiągnięcia w biometrii tęczówki mieliśmy w 2003 r. Wykonaliśmy system weryfikacji tęczówki z własnymi algorytmami. Ponieważ wyniki były dobre, uznaliśmy, że doświadczenia trzeba spopularyzować, zainwestować w wyjazdy do Brukseli i miejsc „pokrewnych". Na bazie tych prezentacji i naszych publikacji zostaliśmy zaproszeni do udziału w projekcie BioSec.

O BioSecu za chwilę. Czym zajmuje się Pracownia Biometrii NASK/PW?

Pracujemy nad metodami weryfikacji tożsamości przy użyciu różnych metod biometrycznych. Głównie interesujemy się biometrią tęczówki, ale nie tylko. Kontynuujemy prace z zakresu podpisu odręcz-

Przemek Strzelczyk i biometryczna karta mikroprocesorowa

Łukasz Stasiak i prototyp systemu weryfikacji dłoni

nego, autorką aktualnego systemu jest Joanna Putz-Leszczyńska. Mamy swój system weryfikacji geometrii dłoni; autorem jest Łukasz Stasiak. Rafał Wardziński pracuje nad biometrią EEG (elektroencefalogramów) – jest to nowość w skali światowej. Pierwsze eksperymenty z wykorzystaniem wielogodzinnych przebiegów EEG chorych z jednego ze szpitali warszawskich wykazały, że w sygnale EEG można odnaleźć informację niezależną od chorób, a zależną od osoby (indywidualizującą ją). Obecnie mamy własne urządzenie do pomiarów EEG, co umożliwia prowadzenie dojrzałych badań.

Biometria jest tylko częścią całego systemu kontroli dostępu, czy to kontroli logicznej, czy fizycznej. Bardzo istotne są zagadnienia ochrony wzorców biometrycznych. Dlatego w pracowni powstała na bazie karty z maszyną wirtualną Java biometryczna karta mikroprocesorowa, przechowująca i – co bardzo ważne – weryfikująca wzorce tęczówki. Autorem i wykonawcą projektu jest Przemek Strzelczyk.

W pracowni zajmujemy się także biokryptografią. Jest to zagadnienie nowe, zwłaszcza w Polsce. Dziedzina ta dotyczy wykorzystania biometrii do generowania stabilnych kluczy kryptograficznych. Problem jest bardzo trudny, gdyż za każdym razem pomiar biometryczny się różni. Obecnie prace prowadzone w tym zakresie w naszej pracowni przez Marcina Chochowskiego przynoszą dobre efekty z wykorzystaniem naszych systemów biometrii tęczówki i dłoni oraz komercyjnych odcisków palca.

Pracownia korzysta z niezbędnego narzędzia do projektowania i testowania metod biometrycznych, tj. z własnej bazy wielomodalnej (zawierającej różne cechy biometryczne tej samej osoby). Została ona zarejestrowana w GIODO (Generalny Inspektor Ochrony Danych Osobowych). Zawiera zdjęcia tęczówek, odcisków palców, twarzy, dłoni oraz podpisy odręczne. W momencie tworzenia w 2003 r. była to jedna z pierwszych tego typu baz na świecie i pierwsza w Polsce. Baza taka jest zdecydowanie lepsza od tzw. baz pseudowielomodalnych, które istniały już na świecie i były syntezą wielu baz jednomodalnych.

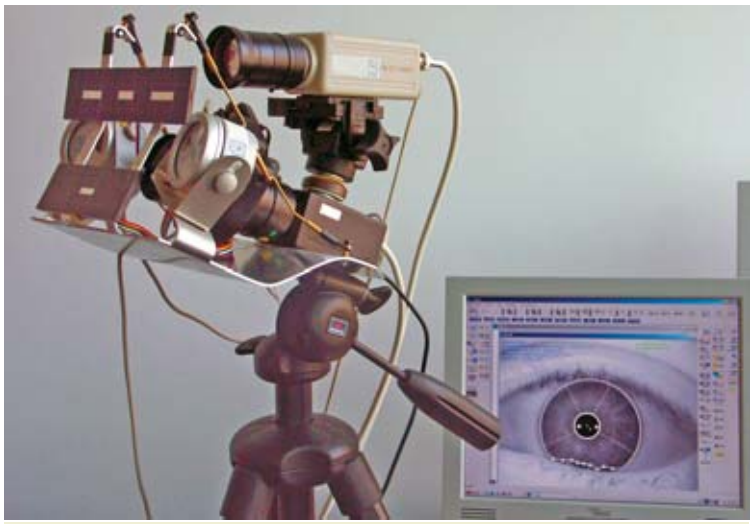
Pomówmy o BioSecu...

To największy, jak do tej pory, europejski projekt poświęcony biometrycznym systemom bezpieczeństwa i w ogóle biometrii. Zaczął się grudniu 2003 r. i trwał 2 lata. Jego budżet wyniósł około 10 mln euro. W konsorcjum realizującym BioSec uczestniczyło 23 partnerów z 9 krajów: Hiszpanii, Włoch, Niemiec, Francji, Belgii, Finlandii, Izraela, Grecji i Polski. Partnerami BioSec byli m.in. Telefonica Research and Development, Siemens, MediaScore, Giesecke & Devrient, VCON Telecommunications Ltd, VTT Electronics, Linie Lotnicze Finnair, MSW Finlandii, Ibermatica, Etra R&D, Biometrika, ATMEL i kilka placówek badawczych. Sumując: były firmy telekomunikacyjne i biometryczne, ośrodki rządowe, linie lotnicze i uniwersytety. Partnerzy wielcy... co nie oznacza, że ich wielkość przekładała się na rozmiar wkładu pracy. NASK był trzecim, co do rozległości nałożonych zadań, partnerem konsorcjum. Całość prac projektu koordynowała hiszpańska firma Telefonica I+D.

Pierwszy pakiet zadaniowy – największa część BioSecu – był poświęcony rozwojowi algorytmów weryfikacji tożsamości na bazie cech biometrycznych. My kierowaliśmy zadaniami związanymi z tęczówką. W tej dziedzinie współpracowaliśmy z Uniwersytetem Karola III z Madrytu, z Raulem Sanchezem-Reillo od dawna zajmującym się tą problematyką. W pakiecie poświęconym algorytmom brał udział również Siemens z własnym systemem weryfikacji twarzy wykorzystującym trójwymiarowe (3D) obrazy oraz między innymi grupa Dawida Maltoniego z Uniwersytetu w Bolonii z problematyką odcisku palca. Finowie z VTT zbudowali system rozpoznawania osób z wykorzystaniem dynamiki chodu.
Wyniki tego pierwszego pakietu przeplatały się z resztą. Nie wspomniałem o sprawie, na którą Unia bardzo liczyła. Chodziło o opracowanie testów

Rafał Wardziński przy systemie pomiarów EEG

Joanna Putz-Leszczyńska i system weryfikacji podpisu odręcznego



Prototyp systemu weryfikacji tęczówki

autentyczności i żywotności mierzonych obiektów dla biometrii tęczówki i odcisku palca (odróżniania żywego oka i palca od podróbek). Maltoni zajmował się odciskami palców, my tęczówką. Osiągnęliśmy wyniki, które teraz patentujemy.

Drugi pakiet zadań dotyczył kart elektronicznych i miniaturowych urządzeń biometrycznych. Tego typu inteligentna karta zwiększa bezpieczeństwo, pozwalając na rezygnację z centralnych baz danych biometrycznych – poważnego źródła obaw potencjalnych użytkowników. Karta mająca wzór biometryczny tęczówki i geometrii dłoni po włożeniu do zewnętrznego czytnika sama weryfikuje właściciela karty. Wszystko odbywa się na jej pokładzie i nie ma potrzeby przenoszenia wzorców z karty do zewnętrznej jednostki obliczeniowej (jest to tzw. technologia *match-on-token*).

W tym zadaniu NASK współpracował z firmą Giesecke & Devrient z Niemiec i Hiszpanami z Madrytu. Opracowane w pakiecie pierwszym algorytmy dotyczące tęczówki zostały przeniesione na te właśnie karty. Do tej pory była na świecie tylko jedna karta tego typu zrobiona dla odcisków palców, ale proces weryfikacji trwał ponad minutę. Nasz system z kartą weryfikuje tęczówkę w czasie 8–9 sekund, przy czym sama weryfikacja trwa ułamek sekundy. Pozostałych około 8 sekund wynika z potrzeby transmisji i szyfrowania danych (zgodnie ze standardem ISO 7816). Poważnym problemem w przypadku stosowania kart mikroprocesorowych do przechowywania i porównywania wzorców biometrycznych jest ich mała pamięć, moc obliczeniowa i prosta architektura. Stąd równolegle były wykonywane specjalizowane urządzenia biometryczne wykorzystujące silniejsze mikrokontrolery.

W czwartym pakiecie zadaniowym stworzyliśmy razem z Telefonicą nowy protokół BEAP do weryfikacji zdalnej przez Internet przy użyciu biometrii. To jest biometryczne rozszerzenie znanego protokołu EAP *(Extensible Authentication Protocol)* o różne informacje związane z biometrią *(Biometric EAP)*. Są to np. wybór metody biometrycznej, transmisja cech biometrycznych, parametryzacja biometrii i dane związane z testem żywotności. Całość prac zakończyły udane próby weryfikacji biometrycznej pomiędzy Warszawą, Madrytem i Barceloną. Zalogowaliśmy się do zasobów na serwerze w Hiszpanii za pomocą naszego urządzenia do tęczówki i linii papilarnych (to ostatnie otrzymaliśmy od Włochów). Świadomość sprawdzenia, iż działa to między Hiszpanią a Polską, a nie między np. dwoma sąsiednimi pokojami, ma pewne zalety perspektywiczne.

Co w BioSecu było innowacyjnego?

Patrząc na algorytmy weryfikacji – wiele było świeżego. Nasz prototyp systemu weryfikacji tęczówki też był rzeczą nową. Innowacyjne były działania Siemensa (weryfikacja twarzy 3D). Absolutnie nowe w skali światowej są opracowane systemy testowania żywotności, zarówno dla tęczówki, jak i odcisków palców. Jesteśmy autorami trzech metod do weryfikacji żywotności tęczówki. Maltoni natomiast opracował kilka metod oraz prototypowe urządzenia do weryfikacji żywotności palca. Mówiąc o nowościach, powinienem przypomnieć o protokole zdalnej weryfikacji (BEAP), a także stworzeniu biometrycznego interfejsu API – BioSecAPI.

Na koniec rzecz zupełnie nietechniczna, ale z techniką bardzo związana. Są to badania wykonane w ramach BioSec przez Katolicki Uniwersytet z Leuven, poświęcone reakcjom użytkowników podczas kontaktu z urządzeniami biometrycznymi (badacze uzupełniali urządzenia komercyjne ze zwykłej oferty rynkowej dodatkowymi interfejsami ułatwiającymi ich stosowanie).
Wyniki uświadomiły wielu twórcom metod biometrycznych i konstruktorom, jakie pokłady nieufności i bariery tkwią w zwykłym człowieku. Okazuje się, że nie jest istotne, czy urządzenie ma dużą dokładność i jest w 100% bezpieczne. Jeśli użytkownik ma szukać jakiejś lampki na obudowie i trwa to dłużej niż 5 sekund, dla niego to urządzenie jest już stracone. Ludzie boją się nowości. Ta kamera wykonuje zdjęcie mojego oka, ale gdzie ono trafi? A może pomiar uszkodzi mi wzrok? Co ciekawe, wyjaśnienia niewiele pomagają.
Z przykrością muszę powiedzieć, że biometria tęczówki, będąca świetną metodą – i jeśli jest prawidłowo zastosowana, to mająca dobrą dokładność – wzbudza dużą nieufność. Konieczne są edukacja i poprawienie interfejsów pomiędzy człowiekiem a systemem. Cóż, *vox populi, vox dei* (głos ludu głosem boga), rynek będzie musiał się dostosować. Co ciekawe – to wiemy z własnych doświadczeń, bo z BioSecu metodę podpisów odręcznych skreślono z listy za-

dań projektu, ludzie zupełnie nie boją się kradzieży podpisów własnoręcznych, choćby składali je nawet na tabliczkach elektronicznych. Siła przyzwyczajenia?

Co warto powiedzieć o waszym systemie weryfikacji tęczówki?

Nasz prototyp systemu przeprowadza kompletny proces weryfikacji tęczówki, od automatycznego wykonania zdjęcia, poprzez jego przetworzenie, do decyzji co do tożsamości osoby. Proces ten zajmuje około 3 sekund. Kilka dodatkowych sekund pochłania pozycjonowanie oka przez użytkownika do momentu, aż zostanie automatycznie wykryte przez system. Zdjęcie jest wykonywane w podczerwieni, co powoduje pominięcie informacji o kolorze oka – cechy niewyróżniającej osoby, gdyż melanina (barwnik) nie jest widoczny w tym świetle.

Surowy obraz oka zawiera wiele zakłóceń: powieki, rzęsy czy odbicia źródeł światła. System wybiera do analizy jedynie niezakłócone sektory tęczówki. Sektory są następnie kodowane przy użyciu transformaty Zaka-Gabora, dzięki której zamieniamy obraz w szereg współczynników rozwinięcia falkowego. Jest to podejście inne niż filtracja obrazu stosowana w komercyjnych systemach tęczówki, mające wiele zalet. Metoda ta pozwoliła np. na implementację – czego nie było w projekcie BioSec, a było częścią mojej pracy naukowej – algorytmu, który zapobiega kradzieży wzorców biometrycznych tęczówki, bez potrzeby korzystania z kryptografii. Nie wchodząc w szczegóły, zakodowany w ten sposób wzorzec tęczówki jest bezużyteczny w momencie kradzieży.

Prototypów systemu weryfikacji tęczówki było już kilka i będą następne. Chodzi nam głównie o poprawę interfejsu i problemów optycznych, np. małej głębi ostrości przy fotografowaniu oka. Chcemy zamienić optykę z aktywnym ustawianiem ostrości na rzecz optyki pasywnej, z dużą głębią ostrości. Pozwoli to na wyeliminowanie mechanicznych elementów systemu, zwiększając tym samym jego niezawodność.

Czy jest szansa, aby nowe pomysły miały przełożenie od teorii do praktyki?

Skonstruowane w pracowni systemy mają wartość praktyczną: zachowują się w taki sposób, jak pełnowartościowe produkty rynkowe. Wiemy jednak, że od prototypu do wdrożenia droga jest długa. Pomimo że ani NASK, ani Politechnika nie są firmami produkcyjnymi, część naszych wysiłków zmierza ku wypromowaniu produktów biometrycznych pod szyldem pracowni. Dla przykładu: protokół BEAP może być stosowany w sieciach bezprzewodowych. Można sobie wyobrazić, że człowiek mający urządzenie mobilne, np. weryfikujące tęczówkę, uzyskuje dostęp do zasobów serwera. Ponieważ NASK jest również dostawcą Internetu bezprzewodowego, jesteśmy bliscy realizacji takiego projektu. Dodać również należy, że w pierwszej kolejności trzeba patentować nowości. Patent tylko w pewnym stopniu chroni nasze wynalazki, ale jest warunkiem koniecznym wdrażania nowych pomysłów. Teraz jesteśmy na etapie uzyskiwania patentu na system testujący żywotność tęczówki.

Czy mógłby Pan odsłonić kulisy ostatniego pomysłu?

Tęczówkowe systemy komercyjne w większości nie mają mechanizmów zabezpieczających przed prezentacją fałszywego oka. Proszę sobie wyobrazić, że najpopularniejsze urządzenia można niestety z łatwością oszukać wydrukiem oka na kartce papieru. Testy z wydrukami tęczówek wykonywano już na świecie (Fraunhofer Institute oraz Yokohama University of Technology). Wykonaliśmy je także u nas. Dwa dobrze sprzedające się systemy tęczówkowe zostały oszukane w 15% i 85% (w zależności od zaawansowania technicznego urządzenia). W pracowni opracowaliśmy – nie tylko w ramach projektu BioSec – trzy niezależne metody weryfikacji żywotności oka. Metody te wykorzystują cechy struktury oka oraz jego dynamiki w celu stwierdzenia, czy mierzony jest żywy obiekt. Testy przeprowadzone na około 30 osobach wykazały o wiele większą skuteczność ochrony niż w przypadku systemów komercyjnych.

Powróćmy jeszcze do biometrycznej karty mikroprocesorowej. Tu również chodzi mi o jej możliwe zastosowania.

Na istniejących kartach elektronicznych ich właściciele nierzadko zapisują PIN flamastrem. Takie słabe ogniwo można wyeliminować biometrią. Karta biometryczna ma pełną funkcjonalność karty elektronicznej, także weryfikację na podstawie kodu PIN. Zatem wprowadzenie takiej karty do istniejących systemów kontroli dostępu jest proste, bo polega nie na ich przebudowie, a na uzupełnieniu funkcjonalności systemu nowymi elementami.

Taką kartę można wyobrazić sobie w użyciu w infrastrukturze podpisu cyfrowego. Podpis byłby tworzony na samej karcie, po weryfikacji biometrycznej, co byłoby gwarancją podpisania się przez osobę uprawnioną i operacją bezpieczniejszą.

Bliskim zastosowaniem, a nad tym pracujemy także, będzie weryfikacja biometryczna w telefonach komórkowych. Używa się w nich karty SIM, która jest przecież kartą inteligentną. Można więc wzorzec biometryczny przenieść do karty. Telefony mają coraz lepsze fotograficzne aparaty cyfrowe, a więc należy się spodziewać, że ich niedroga i na razie kiepska optyka umożliwi niedługo zrobienie zdjęcia tęczówki w wystarczającej jakości do rozpoznania osoby. Są już telefony rozpoznające właścicieli przez czytniki odcisków palców.

Dziękuję za rozmowę