

## Nauka w Polsce

---

**PAP**

English

**Strona główna / Uczelnie i instytuty / Projekty badawcze**

2006-02-06

### **Polscy naukowcy uczestnikami europejskiego projektu dotyczącego biometrii**

Biometria tęczówki, wykorzystująca jej indywidualne cechy określone za pomocą metod matematycznych, jest coraz powszechniej stosowana do weryfikacji osób. Umożliwia m.in. kontrolę dostępu do ważnych obiektów, na przykład budynków wojskowych, laboratoriów badawczych czy elektrowni jądrowych. Nad jej unowocześnianiem pracują także polscy badacze z Pracowni Biometrii **Naukowej Akademickiej Sieci Komputerowej** (NASK) oraz **Politechniki Warszawskiej**.

Biometria to dziedzina nauki wykorzystująca metody statystyki matematycznej do pomiarów organizmów żywych. Techniki biometryczne znajdują zastosowanie m.in. w nowoczesnych technologiach i w informatyce.

#### **WZORCE BIOMETRYCZNE TRUDNE DO PODROBIENIA**

Popularność biometrii wśród specjalistów zajmujących się szeroko pojętym bezpieczeństwem związana jest z faktem, że wzorce biometryczne są niezwykle trudne do zmiany, w przeciwieństwie do popularnych kodów PIN i haseł.

"Daje to zwiększoną pewność identyfikacji osób. Cecha ta szybko staje się jednak istotną wadą, gdy wyobrazimy sobie możliwość niepowołanego użycia identyfikujących nas danych, których zmiana jest niemożliwa bądź bardzo ryzykowna dla naszego zdrowia. Stąd ogromną uwagę poświęca się ochronie danych biometrycznych, np. zapisując je w karcie elektronicznej" - tłumaczy uczestniczący w projekcie dr inż. Adam Czajka z Pracowni Biometrii NASK/PW.

Przez ostatnie dwa lata naukowcy z Pracowni Biometrii NASK/PW brali udział w pracach badawczych europejskiego projektu BioSec (Biometrics and Security). Projekt realizowany w ramach Szóstego Programu Ramowego Unii Europejskiej

dotyczył biometrycznych systemów bezpieczeństwa.

Polscy naukowcy odpowiadali za badania dotyczące biometrii tęczówki oraz rozpoznawania osób z wykorzystaniem fal EEG (elektroencefalografia), natomiast badacze z innych krajów, m.in. Hiszpanii, Francji, Niemiec, Finlandii i Grecji, realizowali zadania dotyczące biometrii twarzy, odcisku palca, głosu czy sposobu chodzenia.

"Przy współpracy z partnerami BioSec stworzyliśmy kartę elektroniczną weryfikującą wzorce tęczówki (weryfikacja danych biometrycznych odbywa się na pokładzie karty). Działa ona znacznie szybciej niż jedyna dostępna obecnie na rynku tego typu karta. Prawdopodobnie jako pierwsi na świecie opracowaliśmy także urządzenie, które weryfikuje +żywołność+ oka dla celów biometrii tęczówki (chodzi o badanie autentyczności obrazu tęczówki - czy obserwowana jest żywa tkanka czy jej plastikowa kopia - PAP). W tym celu zaproponowaliśmy trzy niezależne metody weryfikujące +żywołność+ oka" - wyjaśnia dr inż. Adam Czajka.

Naukowiec mówi, że duża wiarygodność biometrii tęczówki związana jest m.in. z niepowtarzalnością układu mięśni tęczówki. "Bogactwo mięśni jest tu tak ogromne że rozpoznanie osób odbywa się z dużą dokładnością. Warunkiem jest jednak odpowiedni pomiar tęczówki i sposób przetworzenia tych danych" - zaznacza Czajka

Najpowszechniejszą metodę służącą weryfikacji osoby za pomocą obrazu tęczówki : algorytmy angielskiego naukowca Johna Daugmana z Uniwersytetu w Cambridge. Polscy naukowcy zaproponowali własne metody przetwarzania obrazu tęczówki oraz własną metodę kodowania.

Jak tłumaczy Adam Czajka, proces rozpoznawania tęczówki rozpoczyna się od wykonania zdjęcia oka w podczerwieni. Praca w podczerwieni pozwala na rejestrację struktury mięśnia, jednocześnie pomijając zbędne informacje, np. o kolorze tęczówki. System automatycznie wyszukuje niezakłócony obszar oka, który następnie poddawany jest kodowaniu.

"Kodowanie opracowane w Pracowni Biometrii NASK/PW wykorzystuje dekompozycję obrazu tęczówki w szereg liczb. Każda z tych liczb opisuje lokalne właściwości struktury tęczówki" - wyjaśnia naukowiec.

Polscy naukowcy opracowali dodatkowo algorytmy dostosowujące sposób kodowania tęczówki dla obrazów o różnej jakości. Pozwala to na osiągnięcie maksymalnej dokładności rozpoznawania osoby, nawet jeśli zdjęcia tęczówki wykonywane są przez telefon komórkowy.

"Otrzymany wzorzec tęczówki, który może następnie zostać zapisany na karcie elektronicznej, jest ciągiem binarnym, o identycznej strukturze dla każdego oka. Skonstruowany w Pracowni Biometrii NASK/PW prototyp systemu weryfikuje tęczówkę w około 3 sekund" - mówi naukowiec.

## BIOMETRIA I KARTY MIKROPROCESOROWE

Szybka i skuteczna weryfikacja danych osobowych niezbędna jest zarówno w bankach, instytucjach bezpieczeństwa publicznego czy laboratoriach badawczych. Obecnie najczęściej wykorzystywanym zabezpieczeniem są karty magnetyczne, które ze względu na m.in. mniejszą pojemność pamięci, niewielką odporność na zakłócenia

elektromagnetyczne, brak zabezpieczeń przed ich kopiowaniem i brak możliwości dokonywania obliczeń na karcie, wypierane są przez karty mikroprocesorowe.

Właśnie na takich kartach możliwe jest zapisywanie wzorca biometrii tęczówki, należącego do posiadacza karty. Pozytywna weryfikacja wzorca przez kartę umożliwia dostęp do odpowiednich informacji czy zdeponowanych w banku pieniędzy.

Karty elektroniczne posiadają specjalny system operacyjny (tzw. COS - Card Operating System), a niektóre z nich także maszynę wirtualną JAVA (są to tzw. Jav Cards). Pozwala to na uruchomienie na pokładzie karty odpowiednich programów umożliwiających dokonywanie różnorodnych obliczeń, np. weryfikację biometryczną.

"Nasza karta weryfikuje zawarty w niej wzorec tęczówki i przesyła decyzję po około 8 sekundach. To sukces biorąc pod uwagę, że jedyna dostępna w tej chwili tego typu karta potrzebuje na to ponad minutę - zaznacza Adam Czajka. "Nie jest łatwo stworzyć kartę biometryczną, która będzie działała szybko i niezawodnie" - dodaje.

Karta opracowana została w tzw. technologii match-on-token, tzn. że porównanie wzorca z dostępnym "żywym obrazem" tęczówki realizowane jest na karcie. Oznacza to, że karta jest zarówno nośnikiem, na którym zapisano dane jak i platformą, na której dokonywane jest porównanie wzorców biometrycznych.

"Jest to bardzo ważne, gdyż w takim scenariuszu dane biometryczne właściciela karty nie są odczytywane przez urządzenie zewnętrzne, co istotnie zwiększa ich bezpieczeństwo. W scenariuszach weryfikacji tożsamości znika więc potrzeba konstruowania centralnych baz danych - jednej z największych obaw użytkowników i projektantów systemów biometrii" - wyjaśnia Czajka.

Wykorzystana karta odpowiada standardom ISO (International Organization for Standardization - Międzynarodowa Organizacja Normalizacyjna - PAP) oraz GlobalPlatform (organizacja zajmująca się m.in. promocją rozwoju technologii kart elektronicznych - PAP). Oznacza to, że zagwarantowana jest m.in. poufność informacji przesyłanych między kartą i terminalem oraz dwustronne uwierzytelnianie (karta i urządzenie udowadniają sobie nawzajem, że dysponują tymi samymi kluczami).

## TERMINAL, KTÓREGO NIE MOŻNA OSZUKAĆ

Polscy naukowcy, współrealizujący projekt BioSec, stworzyli także prototypowe urządzenie - terminal do rozpoznawania osób, który wykorzystuje zdjęcie oka. Przystawiając np. takie zdjęcie do zainstalowanej w terminalu kamery, urządzenia nie można oszukać.

"Stworzony przez nas prototyp systemu ma zaimplementowane trzy metody sprawdzania +żywołności+ oka" - wyjaśnia Adam Czajka. To pierwsze na świecie tego typu badania, które doprowadziły do stworzenia metod chroniących przed nieuprawnionym dostępem z wykorzystaniem tęczówki".

"Pierwsza metoda bazuje na analizie częstotliwościowej tego, co obserwuje kamera. Druga analizuje dynamikę źrenicy oka, a trzecia mierzy pewne cechy fizyczne gałki ocznej i porównuje je z właściwymi cechami dla oka człowieka" - wyjaśnia.

## BIOMETRIA PRZEZ INTERNET

Efektem współpracy naukowców z Pracowni Biometrii NASK/PW z Hiszpańską Telefoniką jest także projekt pierwszego na świecie protokołu (BEAP - Biometric Extensible Authentication Protocol) pozwalającego na wykorzystanie biometrii w zdalnym uwierzytelnieniu w celu tworzenia połączeń VPN (Virtual Private Network Wirtualna Sieć Prywatna, sieć bezpiecznych tuneli komunikacyjnych w Internecie, zapewniających poufność przesyłanych danych i wiarygodność uczestniczących w połączeniu stron - PAP). Obecnie połączenie takie zestawiane jest z wykorzystaniem haseł, a nie np. obrazu tęczówki.

Można więc wyobrazić sobie osobę chcącą uzyskać dostęp do ważnych danych instytucji, w której jest zatrudniona. Serwer tej instytucji, np. laboratorium badawczego, żąda od pracownika weryfikacji biometrycznej. Pracownik, wyposażony w czytnik biometryczny, przesyła bezpiecznym łączem wzorec swojej tęczówki (podczas każdej transakcji wzorce tworzone są w inny sposób, co zapobiega atakom nielegalnego wykorzystania wzorców - tzw. biometric replay attack), a serwer instytucji weryfikuje tę informację i na tej podstawie zezwala bądź nie na połączeniu VPN.

W przyszłości weryfikacja za pomocą biometrii tęczówki będzie być może dostępna w telefonach komórkowych. "Pozwoli to na korzystanie z telefonu jedynie osobom posiadającym zapisany na karcie SIM wzorec biometryczny. Karty SIM to bowiem jeden z typów kart elektronicznych, a wiele aparatów telefonicznych już teraz posiada aparat cyfrowy umożliwiający wykonywanie zdjęć" - wyjaśnia naukowiec. Zatem aparat zrobi zdjęcie naszego oka i zweryfikuje jednocześnie, czy możemy z niego telefonować.

To przyszłość, a na razie dostępne są aparaty umożliwiające weryfikację użytkowników za pomocą odcisków palców.

PAP - Nauka w Polsce, Bogusława Szumiec-Presch

we