

Odciski palców zazwyczaj kojarzą się nam albo z przestępcą, którego identyfikuje się na podstawie analizy daktyloskopijnej, albo z gehenną ludzi wjeżdżających na teren Stanów Zjednoczonych. Tymczasem identyfikacja dzięki liniom papilarnym może, na przykład, zabezpieczyć nasz komputer przed dostępem niepożądanych osób.

Jest to tylko jeden ze sposobów umożliwiających rozpoznanie konkretnej osoby spośród milionów innych. Jeszcze do niedawna biometria, czyli określanie tożsamości człowieka na podstawie jego indywidualnych cech fizycznych, gościła jedynie w filmach science-fiction.

Prócz odcisków palców, istnieje kilkanaście innych metod „wyłuskiwania” z tłumu bezimiennych ludzi właściwej osoby. Okazuje się, że nasz organizm ma wiele przypisanych tylko jemu elementów, które dzięki programom komputerowym oraz aparaturze pomiarowej można rozpoznać i zapamiętać. Różniemy się nie tylko rysami twarzy i wspomnianymi już odciskami palców. Wyróżnia nas także kształt dłoni, obraz tęczęwki i siatkówki oka, kształt i odcisk ucha. To są cechy fizyczne. Identyfikacja możliwa jest także na podstawie metod behawioralnych, czyli związanych z naszym zachowaniem. Najważniejszy jest podpis, choć prowadzi się także badania nad chodem, barwą głosu, a nawet skojarzeniami, które ponoć są odmienne dla każdego człowieka. Każda z tych cech odznacza się różnym stopniem skuteczności. Niektóre metody zostały już wdrożone i zastosowane przez banki lub fir-

Biometrii, w którym są konstruowane i badane urządzenia pozwalające na identyfikację osobnika na podstawie obrazu tęczęwki oka, kształtu i termiki dłoni oraz odręcznego podpisu. Zespołem kieruje profesor **Andrzej Pacut**.

Do wykonania pomiaru tęczęwki służy specjalna kamera.

– *Aby uzyskać zadowalający obraz, należy najpierw pokonać problemy związane z optyką. Zdjęcie tęczęwki wymaga dużej powiększenia, co jednocześnie powoduje małą głębię ostrości. Prototyp kamery, który*

Prawdopodobieństwo wystąpienia takich samych linii papilarnych jest jak 1:8 000 000 000. A więc przy 6-miliardowej ludzkości wciąż są niepowtarzalne.

jest obecnie udoskonalany, wykonuje sekwencję zdjęć, a następnie wybierane jest najlepsze z nich. Cały proces zajmuje około dwóch sekund – wyjaśnia Adam Czajka, pracownik NASK i Instytutu Automatyki i Informatyki Stosowanej Wydziału Elektroniki PW.

Tęczęwka, która ma zostać sfotografowana, zostaje oświetlona światłem podczerwonym. Pozwala to na bardzo dokładną rejestrację struktury jej mięśnia. Wyodrębnienie właściwe-

Następnie zdjęcie należy porównać z wzorcem przechowywanym w bazie danych lub na innym bezpiecznym nośniku, np. na karcie mikroprocesorowej.

– *Nie odbywa się to na zasadzie porównywania „piksel w piksel” – zastrzega Adam Czajka. – Komputer wyznacza cechy charakterystyczne dla danej tęczęwki. Istnieje kilka sposobów, jednak najlepsza jest metoda oparta na analizie falkowej obrazu.*

Podczas obróbki danych, obraz zostaje zamieniony na współczynniki falkowe dla różnych częstotliwości i skali. W ten sposób uzyskuje się duży zestaw danych, z którego wyodrębniane są elementy najlepiej opisujące daną tęczęwkę. Inna metoda polega na przekształceniu obrazu w mapę charakterystycznych elementów. Są to doliny, wzgórza, pie-

tów. Tyle wystarczy, aby zidentyfikować każdą tęczęwkę.

Proszę o autograf

Zespół profesora Pacuta prowadzi również prace nad podpisem odręcznym. Jeszcze do niedawna identyfikacja podpisu była możliwa za pomocą ekspertyzy grafologicznej, ponieważ „parafka” była traktowana jako element statyczny, jako warstwa tuszu na papierze. Zmieniły to specjalne tablety, mierzące nie tylko ruch pisaka, ale także nacisk i kąty opisujące położenie pióra w przestrzeni podczas pisania. Dodatkowym plusem tabletu jest możliwość uporządkowania pomiarów w czasie podpisywania się.

– *Dzięki temu istnieje możliwość identyfikacji za pomocą technik komputerowych. Bardzo ważna jest bowiem kolejność, w jakiej powstają poszczególne elementy podpisu – mówi Adam Czajka.*

Gdy klient dokonuje operacji w banku, rozpoznawany jest między innymi na podstawie podpisu. Zastosowanie tabletu przy okienku kasowym może zwiększyć bezpieczeństwo wypłat.

Najbardziej zaawansowaną metodą jest identyfikacja dzięki porównaniu linii papilarnych. Specjalne czytniki są już do nabycia w sklepach komputerowych. Można tak skonfigurować komputer, żeby uruchamiał się w

100 bajtów wystarcza, by zidentyfikować każdą tęczęwkę.

my telekomunikacyjne, inne wciąż pozostają w fazie badań.

Otwórz oczy

Naukowa i Akademska Sieć Komputerowa współpracuje z Wydziałem Elektroniki i Techniki Informatycznych Politechniki Warszawskiej. Jednym z elementów tej współpracy jest Laboratorium

go fragmentu tęczęwki jest następnym krokiem analizy zdjęcia, ponieważ na fotografii widać też rzęsy i mogą wystąpić odbłaski od oświetlaczy podczerwieni. Poza tym w momencie pomiaru ludzie różnie ustawiają głowę. Otrzymane dane są przetwarzane za pomocą specjalnego algorytmu.



momencie, kiedy zostaną rozpoznane nasze odciski palców. Dotychczasowe zabezpieczenie – za pomocą hasła – nie jest pewne, gdyż może ono zostać podsłuchane lub podpatrzone przez niepowołane osoby.

Tęczówka w sieci

Żadna metoda identyfikacji nie byłaby możliwa bez odpowiedniej bazy danych, z którą można porównać wyniki pomiarów. Na potrzeby badań Laboratorium Biometrii została stworzona pierwsza w Polsce biometryczna wielomodalna baza danych. Wielomodalna – czyli zawierająca wiele metod biome-

trycznych. Od każdej osoby pobrano po pięć parametrów: odciski palców, odręczny podpis, obraz twarzy, tęczę i dion. Dzięki temu można dość dokładnie ustalić jej tożsamość. Była to szeroko zakrojona akcja NASK zarejestrowana w urzędzie Generalnego Inspektora Ochrony Danych Osobowych. Utworzona baza jest wykorzystywana do oszacowania niezawodności metod biometrycznych rozwijanych w Laboratorium.

– Zarejestrowanie takich danych jest konieczne, ponieważ są to dane osobowe. Fakt rejestracji zachęcił wiele osób do wzięcia udziału w eksperymen-

tu. Autorzy tej metody twierdzą, że dla każdej osoby sposób patrzenia jest inny. Niestety, zbyt mała baza danych nie pozwala w pełni oszacować jakości tej metody.

Wyodrębnione metody biometryczne pozwalają z dużą do-

– *Mimo takiego zabezpieczenia pojawiają się liczne wątpliwości: skoro dane są przesyłane do karty, to można je podejrzyc i przechwycić. Jednak istnieją różne techniki zabezpieczeń – takie na przykład, jak szyfrowanie i kryptografia – które w połą-*

Linie papilarne, zdjęcie tęczę, dynamika podpisu, system skójarzeń zastąpią niedługo PIN, który musimy zapamiętać udając się do skrytki bankowej, włączając system alarmowy lub sejf. Wystarczy tylko przyłożyć oko lub palec do czytnika.

kładnością rozpoznać daną osobę. Bliźnięta jednojajowe, które na pierwszy rzut oka wydają się nie do odróżnienia, mają różniące się tęczę. Podobnie jest z odciskami palców. Dzięki temu mogą funkcjonować automatyczne systemy rozpoznawania tożsamości. System komputerowy, opierając się na informacjach z bazy danych, sam może podejmować decyzję o akceptacji, bądź odrzuceniu sprawdzanej osoby.

Aby w pełni wykorzystać możliwości, jakie daje identyfikacja biometryczna, specjaliści muszą pokonać kilka niemałych problemów. Jednym z nich jest tzw. biometric replay attack, czyli próba ponownego przesłania skradzionych bądź podsłuchanych danych. Jeśli system stwierdzi, że są one w stu procentach identyczne, będzie miał powód, aby odrzucić dane, gdyż może zachodzić próba włamania. Kolejnym ważnym zagadnieniem do rozwiązania przez NASK i PW jest opracowanie metod testujących autentyczność danych biometrycznych, które będą w stanie odróżnić np. żywe oko od jego fotografii.

Kolejnym zagadnieniem, nad którym pracują specjaliści, jest zaprojektowanie systemu bazującego na tzw. kartach inteligentnych. Jest to metoda podobna do podpisu elektronicznego. Wzorce biometryczne pozostają zapisane na karcie w jednym miejscu. Kiedy zachodzi potrzeba porównania danych, są one przesyłane do karty, która dokonuje porównania.

czeniu z biometrią pozwalają zwiększyć bezpieczeństwo. W naszej pracowni wykonaliśmy karty pozwalające identyfikować tęczę. Mogą one być kluczem dostępu do wewnętrznej sieci komputerowej – mówi Adam Czajka.

Część opisanych prac badawczych pokrywa się z tematyką zintegrowanego projektu europejskiego BioSec. Jest to obecnie największy projekt poświęcony technologiom biometrycz-

Nawet jednojajowe bliźnięta – fizycznie identyczne – mają inne linie papilarne i inne tęczę.

nym, prowadzony w ramach Szóstego Programu Ramowego UE. Zespół Laboratorium Biometrii jest jednym z członków konsorcjum BioSec.

Największym problemem mogą być bariery psychologiczne powstające u użytkowników systemów identyfikacji. Ludzie zazwyczaj podejrzliwie podchodzą do pobierania odcisków palców, prześwietleń i pomiarów np. dłoni. Chyba jednak lepiej dać sobie zająrzeć w tęczę, niż zapamiętywać kolejny numer PIN. Jeśli stwierdzimy, że jest to dla nas wygodniejszy sposób identyfikacji – można go będzie stosować na szeroką skalę.

Tylko, czy to nie jest już całkiem blisko do idei Wielkiego Brata i wszczepionego chipa? Ale to temat na odrębny artykuł.

**Tekst i zdjęcia:
MICHAŁ LEŚNIEWSKI**

Zapomnieć PIN



cie. Zgodnie z przepisami nie możemy tych danych nikomu udostępnić. Możemy je wykorzystywać tylko do własnych celów badawczych, o czym zostali poinformowani uczestnicy eksperymentu. W tej chwili baza zawiera dane około 200 osób – tłumaczy Adam Czajka.

Spośród pozostałych technik na uwagę zasługują badania nad skójarzeniami. Każdy człowiek odmienne kojarzy pewne obrazy bądź słowa. Oczywiście nie są one za każdym razem takie same, lecz zbliżone. Zazwyczaj każdy z nas w sobie właściwy sposób łączy pewne wyrazy. Jednak ten sposób identyfikacji znajduje się dopiero w powijakach i na razie nie przynosi konkretnych efektów.

Interesujące wydają się również prace naukowców z Politechniki Śląskiej, którzy pracują nad identyfikacją człowieka na podstawie dynamiki ruchów gał-

