



Krótki przegląd technik biometrycznych do rozpoznawania osób

MIROSLAWA PLUCIŃSKA, Instytut Maszyn Matematycznych, Warszawa

Biometria zajmuje się pomiarem i selekcją indywidualnych, fizjologicznych lub behawiorystycznych cech organizmów żywych oraz udoskonalaniem metod pomiaru i wyboru najbardziej niepowtarzalnych osobniczo parametrów.

Obecnie istnieje na rynku szereg technik biometrycznych wykorzystywanych w systemach kontroli dostępu i uwierzytelniania osób. Techniki te są ciągle rozwijane i ulepszone, a także pojawiają też nowe techniki. Najnowszym trendem są multibiometrie, czyli łączenie kilku technik biometrycznych, co zwiększa pewność prawidłowego rozpoznawania osoby i podwyższa bezpieczeństwo systemów je wykorzystujących.

Prace nad wykorzystaniem biometrii do celów rozpoznawania osób koncentrują się głównie na łatwo dostępnych cechach fizycznych. Wstępnie techniki biometryczne przydatne do uwierzytelniania osób można podzielić na trzy podstawowe grupy:

1. Techniki biometryczne znane od dawna:
 - rozpoznawanie rysów twarzy,
 - rozpoznawanie odcisku palca,
 - rozpoznawanie kształtu dłoni,
 - rozpoznawanie siatkówki oka,
 - rozpoznawanie tęczówki oka,
 - rozpoznawanie głośno.
2. Techniki biometryczne obecnie preferowane:
 - rozpoznawanie naczyń krwionośnych palca,
 - rozpoznawanie naczyń krwionośnych dłoni.
3. Techniki biometryczne przyszłości:
 - rozpoznawanie głosu (nowej generacji),
 - multibiometrie, w tym rozpoznawanie odcisku palca + naczyń krwionośnych palca.

Interesujące są również techniki rozpoznawania cech behawioralnych takich, jak:

- sposób pisania odręcznego (prędkość, nacisk, kąt),
- sposób uderzania w klawisze klawiatury,
- sposób mówienia (ruch ust), mimika.

Prowadzone są także badania nad uwierzytelnianiem osób za pomocą rozpoznawania np.: geometrii uszu, odcisku kostek dłoni, chodu danego człowieka.

Opis technik biometrycznych

Rozpoznawanie rysów twarzy

Rozpoznawanie geometrii twarzy jest wygodnym środkiem rozpoznawania – „swoją twarz masz zawsze ze sobą”. Użytkownik spogląda w kamerę, która rejestruje obraz. Po obróbkę i matematycznym przekształceniu obrazu twarzy jest on porównywany ze wzorcem wcześniej zarejestrowanym. Najczęściej jest zapamiętywanych kilka wzorców rysów twarzy, a pomiar jest dokonywany za pomocą kilku kamer, aby uzyskać obraz przestrzenny.

Analiza zarejestrowanego obrazu polega na zlokalizowaniu w pierwszej kolejności twarzy i oczu. We wstępnym przetwarzaniu zarysów stosuje się sieci neuronowe. Następnie jest analizowana pozycja oczu w stosunku do siebie i do całej twarzy. Wyznacza się także takie zadania, jak rozpoznanie okularów czy zarostu.

Dopiero po tych czynnościach jest tworzona geometryczna siatka charakterystycznych punktów twarzy i dokonywane automatyczne porównywanie ze wzorcem. Porównywanie nigdy nie jest dokonywane między obrazami, a między punktami charakterystycznymi rysów twarzy, które są niezmiennie.

W celu uniknięcia prób podsunięcia kamery zdjęcia stosuje się odczyt termiczny wykrywający różnice niewidoczne optycznie. W tym celu wykonuje się pomiary w różnych przedziałach częstotliwości w bliskiej podczerwieni. Obraz termiczny można zarejestrować bez oświetlenia, nie podlega on zmianom wynikającym z kierunku padania światła, czy występowania cieni. Nie da się go sfalszować przebraniem, nie zależy od procesu starzenia się.

Metoda rozpoznawania rysów twarzy jest łatwa w użyciu, nieinwazyjna i akceptowalna przez użytkowników. Współczesne algorytmy rozpoznawania opierające porównanie na analizie punktów charakterystycznych twarzy powodują, że metoda jest niezależna od używania szkieł kontaktowych, zmian fryzury, miny i jest bardziej skuteczna niż subiektywne decyzje osób sprawdzających dokument. Zaletą metody jest dostępność, niski koszt kamer i łatwość ich instalacji w komputerach. Obecnie większość laptopów posiada wbudowane kamery. Do zrobienia zdjęcia twarzy i przesłania go do analizy można wykorzystać również telefony komórkowe.

Metoda ta (bez odczytu termicznego) jest podatna na fałszerstwa, takie jak fotografia, czy maska. Zakłócają ją zmiany oświetlenia, cienie, czy ruchy osoby rozpoznawanej. Termiczne rozpoznawanie twarzy, które umożliwia rozróżnianie nawet bliźniaków, jest kosztowne i przez to nie jest stosowane masowo.

Rozpoznawanie wzoru linii papilarnych

Najczęściej używaną techniką biometrycznego rozpoznawania jest badanie wzoru linii papilarnych. Historycznie w kryminalistyce metoda ta jest znana i stosowana od ponad 150 lat.

Do rozpoznawania odcisku palca wykorzystuje się techniki numeryczne korelacji i transformacji obrazu lub techniki oparte o analizę lokalnych nieciągłości we wzorze linii papilarnych, czyli minucji. Można wyróżnić około 100 charakterystycznych punktów (początki, zakończenia, rozwidlenia, oczka, haczyki itp.) w jednym odcisku palca. Jednakże najczęściej przy analizie wykorzystywane są początki, zakończenia, rozwidlenia oraz złączenia linii papilarnych.

Najważniejszym krokiem w rozpoznawaniu linii papilarnych jest rejestracja wzoru linii papilarnych, czyli uzyskanie obrazu odcisku palca z głowicy rejestrującej. Początkowo do realizacji tego zadania były używane wyłącznie układy optyczne, gdzie obraz oświetlonych linii papilarnych padał na matrycę CCD (*Coupled-Charge Device*). Obecnie głównie są stosowane układy sensorowe, dające na wyjściu informację graficzną od razu w postaci cyfrowej. Palec dotyka bezpośrednio do powierzchni dwuwymiarowej tablicy maleńkich sensorów. Wzór linii papilarnych jest rejestrowany jako zmiany pojemności lub temperatury między zróżnicowaną powierzchnią palca (rowki i grzbiety), a powierzchnią sensorów. Każdy piksel tablicy jest reprezentowany przez jednobajtową liczbę



bę proporcjonalną do odległości sensora od najbliższego elementu powierzchni palca. Układy elektroniczne towarzyszące sensorom, z których składa się tablica, na bieżąco wyłapują i usuwają typowe niedokładności występujące przy zdejmowaniu linii papilarnych i z układu wychodzi sygnał cyfrowy.

Po wstępnym przetwarzaniu – filtracji, normalizacji, digitalizacji (poprawianie czytelności, podniesienie kontrastu, wygładzanie, wydobywanie konturów) w celu uzyskania standardowej, wygodnej do dalszej obróbki postaci są analizowane minucje i jest tworzony matematyczny wzorec, który może podlegać jeszcze kompresji i kodowaniu. Dopiero wtedy następuje rozpoznawanie – weryfikacja lub identyfikacja, czyli porównywane z przechowywanym wzorcem i podjęcie odpowiedniego działania, zależnego od wyniku porównania. Obsługa urządzenia weryfikującego osobę na podstawie wzoru linii papilarnych sprowadza się do wprowadzenia z klawiatury kodu i przyłożenia palca do okienka skanującego.

Badanie linii papilarnych jest metodą znaną od dawna, popularną i najczęściej używaną. Odciski palców są łatwe do pobrania, a ich przetwarzanie w obrazy cyfrowe jest coraz prostsze. Metoda jest wysoce niezawodna i nieszkodliwa, chociaż pojawiają się głosy kwestionujące niepowtarzalność linii papilarnych. Wiarygodność metody jest wysoka, zależy od liczby minucji branych pod uwagę (ok. 12). Rozmiar i cena czytników linii papilarnych maleje. Czytniki linii papilarnych zwykle dodatkowo wyposażone są w mechanizm rozpoznawania imitacji (manekina) palca. Coraz częściej są one standardowym wyposażeniem laptopów i komputerów. Pojawiają się też telefony komórkowe z sensorem linii papilarnych.

Metody tej nie można wykorzystywać tam, gdzie osoby rozpoznawane mają brudne palce lub łatwo mogą się kaleczyć. Łatwa dostępność odcisków palców budzi obawy, że zostaną pobrane i wykorzystane bez zgody i wiedzy właściciela. Ze względu na wykorzystywanie odcisków palców w kryminalistyce, metoda ta ma negatywne psychologiczne konotacje z policyjnymi metodami śledczymi.

Rozpoznawanie kształtu dłoni

Badanie geometrii dłoni jest łatwe w użyciu i społecznie akceptowalne. Umieszczona w urządzeniu skanującym dłoń jest oświetlana promieniami podczerwieni, a trójwymiarowy obraz jest odczytywany kamerą CCD, co umożliwia pomiar geometrycznych parametrów dłoni – długości i grubości palców, szerokości i grubości śródrezcza, proporcji śródrezcza lub palców. Istniejące urządzenia wykorzystują obrazy dłoni zrobione z boku i z góry. Oba obrazy są uzyskiwane za pomocą jednej kamery i lustra umieszczonego pod kątem 45 stopni. Na podstawie zmierzonych parametrów jest tworzony wzorec – wektor cech, zajmujący wyjątkowo mało miejsca w pamięci – zwykle od kilku do kilkunastu bajtów. Do porównania badanej dłoni z wzorcem najlepsze rezultaty daje zastosowanie ważonej metryki euklidesowej.

Technika badania geometrii dłoni lub palca jest łatwa do wykorzystania, nieinwazyjna i społecznie akceptowalna. Metoda ta jest podatna na oszustwa, ponieważ kształt dłoni bliźniaków może być identyczny, a krewnych bardzo zbliżony. Pomiar u wielu osób budzi wątpliwości związane z higieną publiczną, bo dłoń należy przyłożyć do płyty czytnika. Do wad należy także zaliczyć duże rozmiary urządzenia rozpoznającego kształty dłoni ograniczające jego zastosowania, jak również wysoką cenę.

Rozpoznawanie siatkówki i tęczęwki oka

• **Wzór naczyń krwionośnych siatkówki** jest unikalny dla każdego człowieka i, za wyjątkiem stanów chorobowych, niezmienny w ciągu całego życia. Wykorzystywanie cech charakterystycz-

nych siatkówki oka (rozkładu jej naczyń krwionośnych) do rozpoznawania rozpoczęto wcześniej niż badania nad tęczęwką. Po oświetleniu dna oka promieniowaniem bliskiej podczerwieni, kamerą jest odczytywany wzór siatkówki i porównywany ze wzorcem. W czasie pomiaru są wykrywane soczewki, transplanty, czy sztuczne oko. Do rejestracji siatkówki trzeba zdjąć okulary.

Siatkówka jest doskonale chroniona dzięki jej usytuowaniu wewnątrz oka i z tego względu rozpoznawanie wzoru siatkówki jest najbardziej pewną i niepodatną na oszustwa metodą. Skonstruowanie fałszywej siatkówki jest wręcz niemożliwe z powodu własności optycznych, które trzeba imitować. Metoda nadaje się głównie do weryfikacji i ma zastosowanie tam, gdzie wymagany jest najwyższy poziom bezpieczeństwa – np. w obiektach wojskowych. Aparatura do badania dna oka jest rozbudowana (kamera, układ optyczny, oświetlenie, mocny komputer do filtracji i analizy) i kosztowna. Metoda jest trudno akceptowalna przez ludzi, gdyż mimo braku fizycznego kontaktu z urządzeniem (jedynie konieczność zbliżenia oka na odległość kilku centymetrów), jest w pewnym stopniu inwazyjna i użytkownik obawia się o swoje zdrowie przy skanowaniu oka.

• **Tęczęwka** – jest to kolorowy pierścień tkanki otaczający źrenicę, zabezpieczony przez spojówkę. Nie jest możliwe jej sztuczne odtworzenie.

Tęczęwka zawiera największą liczbę informacji charakterystycznych dla danego osobnika. Posiada około 250 miniaturowych zmarszczek, rowków, punktów, które są charakterystyczne dla danego człowieka i nie zmieniają się wraz z jego wiekiem.

Pomiar dokonywany jest z odległości kilku do kilkudziesięciu centymetrów z wykorzystaniem kamer naprowadzających. Głównym problemem przy rejestracji jest lokalizacja tęczęwki. Istnieją dwa sposoby rejestracji obrazu tęczęwki. W pierwszym kamera jest naprowadzana na oczy po zrobieniu zdjęcia, zlokalizowaniu na nim głowy i wykryciu ich pozycji. Drugi sposób wymaga od użytkownika umieszczenia oczu w odpowiedniej pozycji w polu widzenia wąskokątnej kamery. Urządzenie pobierające obraz musi znaleźć kierunek spojrzenia w szerokim zakresie warunków świetlnych i musi również radzić sobie z odbiciami sferycznymi wewnątrz oka.

Proces ekstrakcji cech rozpoczyna się od zlokalizowania tęczęwki w otrzymanym obrazie przez określenie położenia środka źrenicy. Metody ekstrakcji cech nie biorą pod uwagę koloru tęczęwki i analizują monochromatyczny obraz z kamery. Następnie stosuje się metodę falek kwadratu Gabora do wyekstrahowania charakterystycznych informacji z wyizolowanej tęczęwki. Do porównania wzorów tęczęwek wykorzystuje się znormalizowaną odległość Hamminga. Wzorce tęczęwki zajmują zwykle około 512 bajtów.

Charakterystyczne punkty tęczęwki są najbardziej matematycznie rozróżnialną cechą ludzkiego ciała i dzięki temu metoda daje trafność identyfikacji lepszą, niż przy użyciu linii papilarnych, a nawet DNA. Jest łatwa do użycia i niezawodna. Jest to również metoda nieinwazyjna i bezdotykowa. Metoda jest czuła na ruchy oczu użytkownika i refleksy światła. Wymaga dużej współpracy użytkownika lub drogich urządzeń pobierających obraz. Wymaga zdjęcia okularów.

Rozpoznawanie układu naczyń krwionośnych dłoni

Sprawdzanie tożsamości osoby odbywa się przez analizę wzoru układu naczyń krwionośnych. Bada się liczbę naczyń krwionośnych, pozycję i punkty w których się krzyżują. Wzór naczyń krwionośnych dłoni, palca, a nawet całego ciała każdej osoby jest niepowtarzalny (różnice istnieją nawet pomiędzy bliźniętami jed-



nojąowymi oraz np. pomiędzy prawą i lewą dłonią jednej osoby). Wzór ten nie zmienia się także (poza rozmiarami) w ciągu życia danego człowieka.

Technologia została stworzona przez Josepha Rice'a. Pierwszy prototyp rozpoznający układ naczyń krwionośnych powstał w 1985 r., a pierwsze urządzenia komercyjne wyprodukowano dopiero kilka lat temu.

Podstawą działania czytników rozpoznających wzór naczyń krwionośnych dłoni jest prześwietlenie jej światłem o częstotliwości odpowiadającej bliskiej podczerwieni, które jest częściowo absorbowane przez hemoglobinę zawartą we krwi. Otrzymany wzór jest niezwykle trudny do podrobienia, a promieniowanie podczerwone nie oddziałuje negatywnie na nasze ciało. Ten sposób obrazowania jest także całkowicie odporny na obecność zmarszczek, linii dłoni, wilgotność, szorstkość i inne niedoskonałości powierzchni skóry.

Proces skanowania trwa bardzo krótko. Rozpoznanie następuje poprzez porównanie obrazu z czytnika z zarejestrowanym wcześniej i przechowywanym wzorcem.

Metoda jest skuteczna i akceptowalna społecznie. Zaletą metody jest możliwość prawie bezkontaktowego pobierania danych biometrycznych. Przyczynia się to do łatwości obsługi urządzenia i dużej trwałości głowic sensorowych. Nie ma też znaczenia wiek użytkownika systemu. Wadą jest duży rozmiar urządzeń skanujących dłoni.

Rozpoznawania układu naczyń krwionośnych palca

Rozpoznawanie naczyń krwionośnych palca, tak jak przy rozpoznawaniu naczyń krwionośnych dłoni, opiera się na oddziaływaniu światła o częstotliwości odpowiadającej bliskiej podczerwieni z hemoglobiną we krwi.

Opracowano trzy metody naświetlenia palca przy wykorzystaniu diod LED:

- odbicia światła,
- transmisji światła,
- bocznego naświetlenia.

Część promieniowania podczerwonego zostaje zaabsorbowana przez hemoglobinę (rys. 1), reszta promieniowania jest wyla-

pywana kamerą CCD. W ten sposób powstaje obraz pokazujący układ naczyń krwionośnych w postaci ciemnych linii.

Technika ta jest skuteczna i akceptowalna społecznie. Umożliwia otrzymywanie obrazów wzorów naczyń krwionośnych o wysokim kontraście, co pozwala na szybką analizę i porównanie z wzorcem. Różnorodność obrazów naczyń krwionośnych zapewnia wysoką dokładność rozpoznania. Metoda nie ma negatywnych psychologicznych odniesień do policyjnych metod śledczych. Nie ma też znaczenia wiek użytkownika systemu.

Rozpoznawanie układu naczyń krwionośnych palca należy do technik „nieprzechwytywalnych” (*non-traceable biometrics*). Metoda ta opracowana przez firmę Hitachi jest rekomendowana do użycia w systemach „bezkartowych” przez francuską organizację Commission nationale de l'informatique et des libertés CNIL (francuski odpowiednik Głównego Inspektora Ochrony Danych Osobowych GłODO), według której „*Finger Vein jest systemem nie prezentującym żadnego określonego ryzyka dotyczącego prywatności danych osobowych, zważając na fakt braku możliwości przechwycenia wzorców biometrycznych człowieka bez jego woli*”.

Wadą tej techniki są ciągle wysokie ceny czytników układu naczyń krwionośnych palca.

Rozpoznawanie głosu

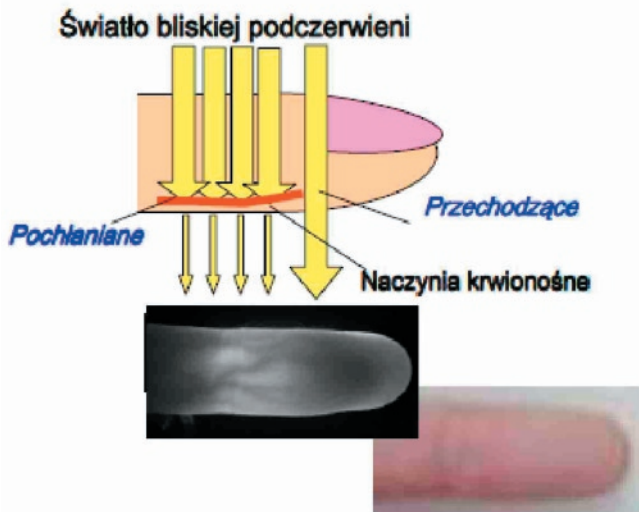
Istnieje kilka sposobów rozpoznawania tożsamości osób na podstawie głosu. Najprostsze i najstarsze oparte są na badaniu ustalonego tekstu lub żądanej dłuższej frazy. W tych przypadkach rozpoznawanie polega na porównaniu wzorca zwykle konkretnych nagranych słów z aktualnie analizowanym głosem. Jeżeli głos rozpoznawany jest na podstawie jednej frazy, łatwo można go zastąpić taśmą magnetofonową. Rozpoznawanie na podstawie kilku zmieniających się fraz jest trudne. Frazy muszą być stanowcze, skończone i odpowiednio długie, co wydłuża czas rozpoznawania.

Nowszy sposób rozpoznawania głosu opiera się na identyfikowaniu mówiącego na podstawie analizy brzmienia jego głosu. Głos jest cechą behawioralną i jego parametry zależą od fizycznych cech indywidualnych danej osoby. W trakcie rozpoznawania rozpatruje takie parametry jak częstotliwość podstawowa, dźwięk nosowy, kadencja itp. Metoda jest atrakcyjna ze względu na możliwość przeprowadzania pomiaru na odległość i szeroką dostępność mikrofonów (np. w telefonach komórkowych). Może być wykorzystana w zastosowaniach takich jak: aplikacje na telefony komórkowe, internetowe usługi bankowe czy handel elektroniczny.

Najnowsze metody analizy głosu przetwarzają na bieżąco dowolną wypowiedź mówiącego i pozwalają na ciągłe sprawdzanie tożsamości osoby w trakcie trwania rozmowy, co utrudnia fałszowanie. W niektórych rozwiązaniach (systemy konwersacyjne) metody te są łączone z weryfikacją wypowiedzianej wiedzy.

Analiza głosu rozpoczyna się od przetworzenia sygnału otrzymanego z mikrofonu na sygnał cyfrowy i dalej na oddzieleniu odcinków mowy od odcinków ciszy. Następnie większość systemów wydziela pewne cechy oparte na częstotliwości sygnału i poddaje je analizie widmowej transformatą Fouriera. Po dalszej obróbce jest tworzony wzorec. Do porównywania wzorca z głosem danej osoby, w celu uzyskania jak najlepszego dopasowania, są wykorzystywane różnorodne algorytmy, np. techniki optymalizacji dynamicznym zakrzywieniem czasu, modele Markowa czy sieci neuronowe.

Metoda jest podatna na błędy związane ze zmianą głosu w czasie, stanem emocjonalnym czy chrypką. Może być zakłócona przez złe warunki atmosferyczne, hałas, szумы kanału transmisyjnego i złe parametry pomieszczenia. Może być oszukana za pomocą np. magnetofonu, czy stworzonej sztucznie mechanicz-



Rys. 1. Zasada obrazowania wzoru naczyń krwionośnych palca
Fig. 1. The principle of imaging a finger blood vessel pattern
(Źródło: Hitachi Europe Ltd., Oddział w Polsce)



nej osobowości. Jednakże analiza głosu jest łatwa w użyciu, społecznie akceptowalna i tania. W wielu zastosowaniach zwłaszcza, gdy jest konieczne użycie telefonu, rozpoznawanie głosu jest rozwiązaniem najlepszym i najtańszym. Widziane są wielkie możliwości w jej stosowaniu i w związku z tym ciągle prowadzone są prace nad jej ulepszeniem.

Rozpoznawanie charakteru pisma i podpisu

Uwierzycielnianie za pomocą podpisu stosowane było od wieków. Podpis jest niestabilny nawet w przypadku tej samej osoby i dlatego automatyczne rozpoznawanie jest skomplikowane. Charakter pisma i podpis osoby mocno zależy od jej emocji i samopoczucia, zmienia się również w czasie. W tej chwili można rozróżnić badanie podpisów pasywnych i badanie podpisów aktywnych.

Podpisy pasywne są skanowane z papierowych dokumentów, gdzie zostały złożone w sposób konwencjonalny. Automatyczne badanie ręcznie pisanych tekstów, podpisów, listów, notatek jest obecnie szeroko stosowane do potwierdzania autentyczności dokumentów finansowych, rozwiązywania specjalistycznych problemów w kryminologii, diagnozowania stanu fizycznego i psychicznego pacjentów w medycynie i w psychologii. Analizując podpis bada się pewne parametry niezmienna dla konkretnej osoby, np. stosunek wysokości małych liter do szerokości podpisu, wysokość dużych liter w odniesieniu do małych, odległości między literami itd.

Podpis aktywny (elektroniczny) wymaga konwersji podpisu ręcznego do postaci cyfrowej, co realizuje się za pomocą specjalnych tabletek i piór elektronicznych. Elektroniczny podpis odręczny zawiera w sobie cechy podpisu tradycyjnego i jest wygodny oraz łatwy do przyswojenia i stosowania przez użytkownika. Użytkownik składa swój własnoręczny podpis na ekranie urządzenia. Taki podpis nie wymaga tłumaczenia, czym jest podpis elektroniczny i na jakich zasadach działa, w związku z czym zmniejsza obawy przed złożeniem go i nie wprowadza strachu przed nową niezrozumiałą techniką.

Podstawą weryfikacji takiego podpisu jest badanie sposobu w jaki został nakreślony. Sprawdza się czas przeznaczony na kreślenie podpisu, prędkość z jaką jest pisany, liczbę przerwania podczas pisania i miejsca, w których to się zdarza. Podpis jest stosunkowo łatwy do sfalszowania, ale sfalszować już fragment tekstu ręcznie pisanego jest znacznie trudniej. Wzorec takiego podpisu nie powinien być robiony na bazie losowo pobranej jednej próbki, ponieważ człowiek nie potrafi podpisać się dokładnie w ten sam sposób drugi raz oraz jego podpis zmienia się przez całe życie.

Obecnie pojawiły się systemy rozpoznawania pisma zdolne do samodzielnego uczenia się w czasie. Korzystają one z zaawansowanych algorytmów tworzących wzorce na podstawie kilku podpisów, jak również modyfikują go wraz z kolejnymi pobieranymi podpisami.

Rozpoznawanie samego podpisu odręcznego jest szybkie i nie zależy od języka, w którym został wykonany. Metoda ta jest podatna na fałszerstwa, zwłaszcza że podpis odręczny jest cechą biometryczną łatwo dostępną. Ogranicza to obszar zastosowań tej metody.

Rozpoznawanie dynamiki uderzeń w klawiaturę

Każdy ma swój typowy rytm i prędkość uderzania w klawiaturę komputera. Stanowią one indywidualną cechę wyróżniającą daną osobę. Tak jak dynamika podpisu, tak i dynamika siły nacisku

jest trudna do powtórzenia. Rozpoznawanie dynamiki uderzeń w klawiaturę jest techniką biometryczną szeroko rozwijającą się w ostatnim czasie i predysponowaną do rozpoznawania osoby piszącej na klawiaturze komputera.

Dynamika nacisku na klawisze przy wprowadzaniu osobistego hasła, czy określonego tekstu z klawiatury, może być rozłożona na pojedyncze komponenty, takie jak czas ukrycia, siła nacisku klawisza, czas naciśnięcia klawisza i przemieszczanie nacisku, które mogą być oszacowane i użyte do weryfikacji tożsamości piszącej osoby. Wzór nacisku jest nazywany sygnaturą. Sygnatura nacisku ma cechy podobne do cech pisma ręcznego, różni się nieznacznie za każdym razem. Do zbadania siły nacisku dołącza się metody interpretacji wizualnej, co pozwala uprościć analizę, a także wykorzystać dobrze znane metody przetwarzania obrazu.

Rozpoznawanie osoby piszącej na klawiaturze jest łatwe, wygodne i nie wymagające dodatkowych urządzeń – wystarczy klawiatura. Jednakże wprowadzenie np. kodu wyłącznie z klawiatury komputera jest bardzo podatne na nieuprawnione przechwycenie.

Inne metody

W obecnej chwili istnieją metody rozpoznawania kształtu ucha, kostek dłoni, badanie DNA itd. Pojawiły się również nowe metody, głównie behawioralne, które nie odgrywają, jeszcze znaczącej roli w praktycznych rozwiązaniach takie jak: rozpoznawanie ruchu oczu, ruchu warg. Prowadzone są również prace nad weryfikacją sposobu chodzenia. Badanie stylu chodzenia pozwala na rozpoznawanie ludzi na odległość, poprzez analizę obrazu video. Dużym utrudnieniem w analizie jest powierzchnia po której osoba idzie, prędkość poruszania, samopoczucie, a nawet ubiór (długa spódnica). Innym podejściem do tej problematyki jest badanie siły nacisku i sposobu stawiania stóp. Wymaga to jednak specjalnych czujników rozmieszczonych na podłożu i nakierowania na nie rozpoznawanej osoby.

Techniką rozpoznawania ludzi na odległość, bez ich wiedzy, jest również metoda badania kształtu uszu. W metodzie tej oprócz wydobycia z obrazu podstawowej struktury kształtu ucha, proponuje się również korzystanie z obrazu termicznego, co eliminuje wpływ oświetlenia i przykrycie ucha włosami.

Badanie ruchu ust należy do technik behawioralnych. W odpowiednich warunkach oświetleniowych można odczytać pozycję ust i ich wyraz. Technikę tę można łatwo połączyć z rozpoznawaniem rysów twarzy i głosu mówiącego.

Do metod biometrycznych należy także zaliczyć EKG, badanie tętna i ciśnienia krwi, pomiar temperatury ciała. Nie są to jednak metody stosowane obecnie do rozpoznawania osób.

Literatura

- [1] Boll R., Connell J., Pankanti S., Ratha N., Senior A.: TAO Biometria – Warszawa, WNT
- [2] Woszczyński T.: Finger Vein ID Systemy biometryczne Hitachi – materiały informacyjne
- [3] Hitachi Europe Ltd., Oddział w Polsce – materiały informacyjne
- [4] Bechelli L., Bistarelli S., Martinelli F., Petrocchi M., Vaccarelli A. – Integrating Biometric Techniques with an Electronic Signature for Remote Authentication
- [5] PerSay's position in the NIST 2008 Speaker Recognition – Evaluation – Industry Report
- [6] www.nist.gov/speech/tests/sre/2008/index.html
- [7] www.persay.com