BIOMETRIA W DOKUMENTACH IDENTYFIKACYJNYCH

Maciej Kiedrowicz

Wojskowa Akademia Techniczna

Streszczenie. W opracowaniu opisane zostały podstawowe zagadnienia związane z możliwością wykorzystania dokumentów identyfikacyjnych w systemach informatycznych, w szczególności zastosowania danych biometrycznych w tych dokumentach. Celem opracowania jest zwrócenie uwagi na konieczność określenia trwałego związku pomiędzy dokumentem identyfikacyjnym a osobą, której ten dokument dotyczy. Jest to podstawowy problem, który wymaga rozwiązania, tzn. przypisanie właściwej osoby do dokumentu, który jest wykorzystywany do identyfikacji tej osoby. W dalszej części opracowania scharakteryzowane zostały różnorodne biometrie, mogące znaleźć zastosowanie w zabezpieczaniu dokumentów identyfikacyjnych (zarówno cechy fizyczne, jak i behawioralne), określając równocześnie możliwości i ograniczenia w masowym ich zastosowaniu. Możliwość, a w niektórych sytuacjach konieczność zastosowania danych biometrycznych, wynika z coraz szerszego wykorzystania technologii informatycznych (w szczególności internetowych) w życiu codziennym i coraz częstszych prób kradzieży tożsamości osób korzystających z tych technologii.

Z identyfikacją osób mamy do czynienia począwszy od wystawienia aktu urodzenia, a skończywszy na akcie zgonu. W trakcie tego okresu osoba jest wyposażana w wiele dokumentów, które zawierają dane identyfikacyjne – książeczkę zdrowia, legitymację szkolną, dowód osobisty, legitymację studencką, paszport, prawo jazdy, legitymację służbową, identyfikator pracowniczy, kartę dostępową, imienną kartę członkowską, kartę pobytu (…) – ogólnie można stwierdzić, że zbiór ten obejmuje wszelkie dokumenty, które zawierają dane związane z imionami, nazwiskiem, datą urodzenia oraz zdjęcie. Zarówno dowód osobisty, jak i paszport są dokumentami stwierdzającymi tożsamość. Dotyczy to przede wszystkim osób pełnoletnich, dzieci i młodzież (osoby poniżej 18 roku życia) również mogą otrzymać dowód osobisty lub paszport, ale obowiązek posiadania dowodu osobistego dotyczy tylko osób pełnoletnich. Pozostałe dokumenty traktuje się raczej jako dokumenty potwierdzające tożsamość (częstym przypadkiem potwierdzania tożsamości jest okazanie przez daną osobę jednego lub dwóch dowolnych dokumentów ze zdjęciem). Z tego też względu dowód osobisty i paszport są traktowane w sposób szczególny. Dane identyfikacyjne umieszczone na/w dowodzie osobistym lub paszporcie są chronione w bardzo restrykcyjny sposób. Służą temu zarówno zabezpieczenia samych „czystych" blankietów (np.: rodzaj materiałów, z jakich są wykonane, zabezpieczenia przed próbami zmian ich zawartości), zabezpieczenia związane z procesem zbierania i nanoszenia danych

identyfikacyjnych na blankiety (tzw. personalizacja) oraz zabezpieczenia związane z dystrybucją i użytkowaniem dowodów osobistych i paszportów.

Dokumenty identyfikacyjne w systemach informatycznych

Procesy zbierania, umieszczania i wykorzystywania danych identyfikacyjnych podlegają bardzo restrykcyjnym regułom. Systemy informatyczne, wykorzystywane do automatyzacji tych procesów, są projektowane i wytwarzane ze szczególnym naciskiem na aspekty bezpieczeństwa danych w nich przetwarzanych. Z jednej strony mamy ograniczenia wynikające z Ustawy o Ochronie Danych Osobowych, z drugiej zaś – ustawy i przepisy związane z bezpieczeństwem obywateli i szeroko rozumianym bezpieczeństwem kraju. Wszelkiego rodzaju przypadki kradzieży i wykorzystywania „cudzych" tożsamości są podstawową przyczyną takiego traktowania danych identyfikacyjnych w dokumentach stwierdzających tożsamość.

W klasycznym systemie, w którym wykorzystuje się jakiekolwiek dokumenty zawierające dane identyfikacyjne (imię, nazwisko, data urodzenia, zdjęcie, numer identyfikacyjny PESEL, etc.), po zarejestrowaniu odpowiednich danych klienta/użytkownika takiego systemu zostaje mu wydany odpowiedni dokument – może to nastąpić bezpośrednio po rejestracji – lub dokument ten jest wydawany z pewnym opóźnieniem. Jeśli dokument zawiera tylko dane opisowe (np. imię, nazwisko, datę urodzenia, adres) i nie zawiera zdjęcia, to nie ma możliwości sprawdzenia, czy osoba nim się posługująca jest rzeczywiście tą osobą, za którą się podaje. Mogą w takim przypadku wystąpić dwie „niepożądane" sytuacje: posługiwanie się dokumentem wystawionym dla innej osoby (np. w wyniku kradzieży lub „pożyczenia" dokumentu) lub pozyskanie dokumentu przez osobę podszywającą się pod kogoś innego (w wyniku kradzieży lub „pożyczenia" tożsamości tej osoby). W chwili obecnej, gdy coraz więcej tego typu systemów funkcjonuje w oparciu o technologie informatyczne, istnieją coraz lepsze metody weryfikacji osób starających się o dokument (chociażby poprzez weryfikację większego zakresu danych osobowych, przykładowo – w oparciu o takie dane jak imię ojca lub nazwisko panieńskie matki). Niemniej możliwość pozyskania dokumentu przez inną osobę istnieje.

Zakładając, że bezpieczeństwo danych identyfikacyjnych w systemach informatycznych jest na odpowiednio wysokim poziomie, podstawowym problemem, z którym mamy do czynienia, jest kwestia **przypisania osoby do dokumentu**, który jest wykorzystywany do identyfikacji tej osoby.

W tym właśnie celu wykorzystuje się dane biometryczne, które są umieszczane w dokumencie identyfikacyjnym. Dane te mogą być dwojakiego rodzaju. Z jednej strony są to dane, które można zweryfikować bezpośrednio – bez korzystania ze specjalistycznych urządzeń (np. zdjęcie biometryczne), z drugiej – dane zapisane w części elektronicznej dokumentu (mikroprocesorze), które można zweryfikować

tylko i wyłącznie korzystając z odpowiednich urządzeń (np. czytników linii papilarnych).

Rozwój technologii w tym obszarze daje więcej możliwości wykorzystania coraz to nowych cech biometrycznych. Przykładowo, „tradycyjny" odcisk linii papilarnych może być zastąpiony układem naczyń krwionośnych palca (z równoczesnym badaniem przepływu krwi).

Biometria w dokumentach identyfikacyjnych

Za biometrię uważa się zbiór technik służących pomiarom cech fizycznych i behawioralnych człowieka w celu automatycznego rozpoznania danej osoby, czyli potwierdzenia lub odrzucenia jej tożsamości dla celów bezpieczeństwa.

Największy rozwój systemów biometrycznych rozpoczął się w latach 90. ubiegłego wieku. Obecny poziom rozwoju technologii sprawił, iż w tej chwili systemy biometryczne prezentują nieporównywalnie wyższy poziom, w wielu przypadkach potrafią być całkowicie automatyczne. Prowadzone są ciągłe prace nad ich rozwojem i udoskonalaniem, przede wszystkim w zakresie zabezpieczeń (przed możliwościami oszustw przez osoby nieuprawnione). Praktyka pokazuje, że w większości systemów (czy to opartych na biometrii, kartach, kluczach, czy też hasłach) najbardziej zawodnym elementem bywa człowiek. Nieustające badania i doskonalenie istniejących systemów oraz konstruowanie nowych ma m.in. na celu jeśli nie wyeliminowanie tego czynnika, to przynajmniej jego minimalizację. Badania pokazują również, że systemy wykorzystujące biometrię dają większą gwarancję właściwego określenia tożsamości klienta/użytkownika systemu (w przeciwieństwie do systemów, które korzystają z jego wiedzy (np. hasło) lub zawartości portfela (np. karta)).

Systemy wykorzystujące biometrię mają kilka zasadniczych korzyści, których nie posiadają systemy zbudowane w oparciu o inne metody, również w dużym stopniu udoskonalane w ostatnich latach, czyli oparte o hasła i karty dostępu. O części z nich jest mowa powyżej, istnieje natomiast jedna podstawowa różnica pomiędzy tymi systemami – **danych biometrycznych nie można pożyczyć, ukraść ani zapomnieć**.

Systemy biometryczne kojarzą się przede wszystkim z pobieraniem odcisków linii papilarnych palców lub skanowaniem tęczówki oka. Tymczasem wciąż poszukuje się coraz to nowych cech fizycznych i behawioralnych człowieka, unikalnych dla niego, a zatem odróżniających go od każdej innej osoby. Niektóre z nich dostępne są już w formie gotowych rozwiązań na rynku, inne znajdują się w fazie badań i testów.

Do cech fizycznych, które mogą być wykorzystane w systemach biometrycznych, można zaliczyć:

- barwę głosu,
- zapach,

- linie papilarne palców („odcisk palca" i odcisk opuszki palca),
- naczynia krwionośne palców,
- geometrię dłoni,
- geometrię i rysy twarzy, rozkład temperatury twarzy, analizę faktury powierzchni twarzy – skóry,
- geometrię ucha,
- geometrię ust,
- cechy charakterystyczne tęczówki oka,
- cechy charakterystyczne siatkówki oka,
- układ żył nadgarstka,
- strukturę włosów/paznokci,
- EEG,
- ECG,
- identyfikację DNA (bliźnięta jednojajowe mają identyczne DNA).

Biorąc pod uwagę cechy behawioralne, można wymienić:

- charakterystykę głosu, mowy,
- charakterystykę ruchu ust,
- charakterystykę ruchów gałki ocznej,
- pismo (podpis odręczny),
- sposób pisania na klawiaturze,
- charakterystykę chodu.

Niektóre z przedstawionych powyżej cechy są już wykorzystywane, niektóre są na etapie badań i prób wdrażania, nie wszystkie z tych cech znajdą praktyczne zastosowanie. Pojawiają się również nowe propozycje cech, które spełniają opisane poniżej właściwości i mogą być w przyszłości wykorzystane jako cechy biometryczne. Zalicza się do nich:

- kształt całego ciała człowieka,
- analizę wibracji twarzy lub głowy w czasie mówienia,
- badanie wewnętrznej struktury ciała i jego funkcji życiowych (np. przepływu krwi),
- analizę pól magnetycznych lub elektrycznych (generowanych przez ciało człowieka lub reakcji na takie pola).

Systemy, w których wykorzystuje się charakterystyczne dla danej osoby zachowania i odruchy, wymagają dłuższego czasu uwierzytelniania, który jest konieczny do wprowadzenia wymaganych danych do tego systemu. Znikomo małe prawdopodobieństwo powtarzalności danej cechy biometrycznej (w niektórych przypadkach nie można mówić o niepowtarzalności cech) stanowi jedno z podstawowych (ale nie jedyne) wymagań stawianych przed tymi systemami. Uważa się, że aby cecha biometryczna mogła być wykorzystana w systemie biometrycznym, to:

- cechę tę powinna posiadać każda osoba (lub prawie każda),
- cecha ta musi być niezmienna w czasie (co najmniej względnie stała),

– cecha ta musi być mierzalna,
– cecha ta nie powinna być podatna na próby podrobienia/zafałszowania.

Istotnym elementem zwiększającym szanse na zaprojektowanie i wdrożenie systemu biometrycznego jest akceptacja pomiaru i sposobu „pobierania" danej cechy biometrycznej (klasycznym przykładem jest tutaj pobieranie odcisków linii papilarnych, co jest jednoznacznie kojarzone z popełnieniem przestępstwa i koniecznością pobrania tych linii przez policję). Drugą stronę zagadnienia stanowią urządzenia i sposoby kontroli biometrii, wszelkiego rodzaju czytniki i bramki kontrolne. Powinny one być łatwe i szybkie w użyciu, precyzyjnie działające (poziom błędów w odrzuceniach i akceptacji), odporne na próby zakłóceń oraz oczywiście niezbyt kosztowne na etapie zakupu i eksploatacji. W przypadku urządzeń, które miałyby służyć do zdalnej lub lokalnej autoryzacji, konieczne może okazać się rozpoznanie nie tylko osoby, lecz także jej woli. Może to powodować, że urządzenia będą musiały mieć możliwość rozpoznawania akcji, służących jako odzwierciedlenie woli danej osoby. Można w takich przypadkach wykorzystać, na przykład, podpis tej osoby: specyficzne ruchy dłoni, oka lub innych części ciała; wypowiedziane słowo lub zdanie.

Praktyczne wykorzystywanie poszczególnych cech biometrycznych przedstawia się następująco: skanowanie odcisków palców – 33%, odciski palców – 25,3%, rozpoznawanie twarzy – 12,9%, tęczówka oka – 5,1%, geometria dłoni – 4,7%, rozpoznawanie głosu – 3,2%, układ żył – 3%, kilka cech jednocześnie – 2,9%, pozostałe cechy – 4%. Natomiast główne obszary zastosowań można sklasyfikować następująco: 1) sprawiedliwość i obronność (identyfikacja zwłok, śledztwa kryminalne, identyfikacja terrorystów, poszukiwania zaginionych, instytucje wojskowe i specjalne, instytucje strategiczne – banki, elektrownie, rafinerie); 2) administracja publiczna (dowody osobiste – tzw. ID karty, prawa jazdy, podpis cyfrowy, świadczenia społeczne, kontrola paszportowa, kontrola graniczna); 3) zastosowania komercyjne (praca przy komputerze, ochrona danych, e-handel, dostęp do Internetu, karty kredytowe i płatnicze, fizyczna kontrola dostępu, telefony komórkowe, zarządzanie dokumentacją medyczną, zdalne nauczanie, zarządzanie czasem pracy, dostęp do bibliotek i publicznych zasobów danych, masowe imprezy).

W ogólności, systemy identyfikacji biometrycznej pracują w dwóch trybach: weryfikacji i identyfikacji. Wybór odpowiedniego trybu wiąże się zarówno z techniką identyfikacji, jak również sposobem i szybkością działania systemu. Praca systemów biometrycznych realizujących funkcje weryfikacji opiera się na potwierdzeniu tożsamości osoby, która poddaje się temu procesowi. Zadaniem systemu jest znalezienie odpowiedzi na pytanie: „Czy dana osoba jest tą, za którą się podaje?". Praktycznie oznacza to rozpoczęcie uwierzytelniania poprzez dokonanie właściwej preselekcji weryfikowanych danych, np. za pomocą podania odpowiedniego kodu lub też podania danych biometrycznych zapisanych na nośniku, jakim może być karta. Odpowiedni wektor cech biometrycznych zostaje porównany ze swoim odpowiednikiem

w systemie i podejmowana jest decyzja o ich zgodności (lub jej braku). Ten tryb nazywany jest trybem 1 : 1 (jeden do jednego). Rozwiązanie takie pozwala dokonywać weryfikacji w systemach o zdecydowanie mniejszych wymaganiach wydajnościowych (wymaga również krótszego czasu na realizację tej funkcji).

Systemy realizujące przede wszystkim funkcje identyfikacji ukierunkowane są na jednoznaczne określenie tożsamości danego użytkownika. Nie potwierdzają przynależności określonych cech biometrycznych dla danej osoby, ale biorąc pod uwagę jej cechy biometryczne, potrafią jednoznacznie ją zidentyfikować. Po odczytaniu zadanych cech biometrycznych i odpowiedniemu przekształceniu ich do postaci cyfrowej, dokonują przeszukania dostępnych zasobów danych w celu znalezienia obiektu najbardziej zbliżonego do badanego. Jest to podstawą ustalenia tożsamości badanej osoby. Biorąc pod uwagę sposób działania tych funkcji, identyfikacja określana jest jako tryb 1 : N (jeden do wielu). Stwierdzenie „najbardziej zbliżonego do badanego" mówi, że pozytywna odpowiedź jest możliwa po osiągnięciu określonego (zadanego parametrycznie) progu zgodności szukanego zestawu cech biometrycznych ze znalezionym.

Działanie systemów biometrycznych powinno uniemożliwiać powtórne zarejestrowanie użytkownika/klienta w bazie danych. Innymi słowy, nie powinien umożliwiać zarejestrowania tej samej tożsamości z innymi danymi identyfikacyjnymi. Jest to szczególne istotne w systemach wymagających wysokiego bezpieczeństwa. Zmiana danych osobowych nie ma wpływu na wynik identyfikacji, a osoba raz wprowadzona do bazy danych (jako określony zestaw danych biometrycznych) jest zawsze identyfikowana pod pierwotnie wprowadzonymi danymi. Wynikiem takiego podejścia jest efektywne zabezpieczenie przed próbami ukrywania lub zmiany tożsamości.

Przykłady wybranych cech biometrycznych

Biometria linii papilarnych palca. Biometria linii papilarnych jest cechą anatomiczną, która była wykorzystywana do weryfikacji tożsamości najwcześniej – już w X w. p.n.e. w Babilonie odciski palców służyły potwierdzeniu transakcji handlowych. Linie papilarne zostały sklasyfikowane w XVII wieku, a w roku 1823 opracowano zestaw dziewięciu głównych wzorów linii papilarnych. Do podstawowych wzorów linii papilarnych zalicza się: łuki (*ang. arch*), pętle (*ang. loop*) oraz wiry/spirale (*ang. whorl*). Kluczowe w historii badań nad liniami papilarnymi palców było wprowadzenie pojęcia detali (tzw. minucji). Podstawą klasyfikacji oraz porównywania odcisków palców jest porównanie detali wyróżnionych w obrazach linii papilarnych. Przykładami detali są: zakończenia (*ang. ridge ending*), rozdwojenia (*ang. bifurcation*), ogrodzenia (*ang. enclosure*) oraz wyspy (*ang. island*). W roku 1918 opracowano zasadę, że istnienie dwunastu takich samych detali pozwala wnioskować o identyczności dwóch odcisków palców. Zasada ta obowiązuje do dzisiaj. Pomiar

cechy biometrycznej może być realizowany z wykorzystaniem różnych czytników linii papilarnych – najczęściej stosowane to: czytnik optyczny, pojemnościowy lub ultradźwiękowy.

Wady technologii biometrycznych wykorzystujących wzory linii papilarnych związane są z samą charakterystyką biometryczną. Wynika to z silnego wpływu stanu powierzchni palca na wynik pomiaru (uszkodzenia naskórka, zabrudzenia, stopień nawilżenia). Zdarzają się także przypadki, w których nie ma możliwości pobrania odcisków palców (przypadki losowe – brak palców, schorzenia anatomiczne, efekt ciężkich warunków pracy). Niemniej jest to najczęściej wykorzystywana cecha biometryczna.

Biometria naczyń krwionośnych palca. Dla potrzeb identyfikacji osobniczej mogą być wykorzystywane charakterystyki naczyń krwionośnych palca. Pobieranie charakterystyki naczyń krwionośnych palca następuje przez rozwiązania sprzętowe (czytniki) wykorzystujące światło bliskiej podczerwieni. Ten rodzaj światła pochłaniany jest przez hemoglobinę, co pozwala sensorowi (np. kamerze CCD) na uzyskanie odpowiedniego obrazu naczyń krwionośnych. W klasycznych systemach obrazowania naczyń krwionośnych wykorzystuje się dwie metody naświetlania: opartą o odbicie światła oraz opartą o transmisję światła. Dla pierwszej z nich urządzenia pomiarowe są niewielkich rozmiarów, obszar działań jest otwarty, a uzyskany obraz naczyń krwionośnych posiada niski kontrast. Dla drugiej – urządzenia pomiarowe są większe, obszar operacji zamknięty, a wzorzec posiada wysoki kontrast. Metoda wykorzystywana w przypadku biometrii naczyń krwionośnych palców łączy zalety dwóch powyższych metod – polega na bocznym naświetlaniu naczyń krwionośnych. Po akwizycji obrazu naczyń krwionośnych palca wykonuje się jego normalizację, a w późniejszym etapie ekstrakcję cech charakterystycznych otrzymanego obrazu oraz dopasowywanie wzorców. Zalety rozwiązań opartych o biometrię naczyń krwionośnych palca dają szerokie możliwości zastosowań praktycznych – m.in. w systemach kontroli dostępu (inteligentne budynki), jak również dla potrzeb sektora bankowego – szczególnie do uwierzytelniania transakcji (automaty płatnicze).

Biometria podpisu odręcznego. Biometria podpisu odręcznego wykorzystuje bardzo powszechny sposób weryfikacji tożsamości, jest więc łatwo akceptowalną metodą. Systemy weryfikujące podpis mogą badać podpis już złożony (tzw. systemy *off-line*), lecz większą dokładność zapewniają systemy, które „obserwują" podpis w czasie jego składania (tzw. systemy *on-line*). Użycie w takim systemie właściwego urządzenia, np. tabletu graficznego, umożliwia rejestrację podpisu uwzględniającą zarówno jego charakterystykę wizualną (obraz dwuwymiarowy), jak też sposób, w jaki podpis został złożony (szybkość składania podpisu, siłę nacisku na papier, sposób trzymania długopisu/rysika). Każdy złożony podpis jest prezentowany jako ciąg wektorów, zawierających przebiegi wybranych wielkości (zebranych w trakcie podpisywania). Dane te pozwalają modelować dynamikę ruchu z dużą dokładnością

(dynamika ruchu zawiera najwięcej cech osobniczych). Techniki porównywania tak zarejestrowanych podpisów wykorzystują tzw. ukryte modele Markowa oraz tzw. dynamiczne marszczenie czasu, będące modelami wykorzystywanymi do porównywania funkcji. Dynamiczne marszczenie czasu opiera się na spostrzeżeniu, że bezpośrednie porównywanie wartości dwóch funkcji czasu (wynikających ze złożenia dwóch podpisów) dla następujących po sobie chwil czasowych może nie być właściwe, gdyż czas dla każdej funkcji może „biec inaczej" (chociaż obie zachowują następstwo zdarzeń). Dlatego też – dla badanych podpisów – wprowadza się „zindywidualizowane czasy" za pomocą odpowiedniego zniekształcenia („zmarszczenia") czasu rzeczywistego i skonstruowania tzw. funkcji marszczących. W metodzie tej określa się tzw. poziomy błędów zrównoważonych (*EER – Equal Error Rate)*, które określają częstość fałszywych odrzuceń i fałszywych akceptacji przy odpowiednim dobraniu parametrów systemu. Dla najlepszych systemów biometrii podpisu odręcznego on-line plasują się na poziomie 2%. Dla systemów off-line błędy te mogą być nawet o rząd wielkości większe. Pomimo takich poziomów błędów, biometria podpisu odręcznego, zarówno w wersji on-line jak i off-line, stosowana jest bardzo szeroko w bankowości (głównie jako technologia wspomagająca) ze względu na powszechną akceptację tej metody.

Biometria tęczówki. Znalezienie biometrii idealnej, czyli takiej, która bezbłędnie weryfikuje tożsamość, jest odporna na oszustwa, efekty chorób i starzenia się organizmu, nie budzi kontrowersji na tle religijnym, socjologicznym i rasowym oraz – co jest również bardzo ważne – jest przyjazna dla użytkownika, to cel projektantów i producentów systemów biometrycznych. Chociaż trudno jednoznacznie wskazać biometrię posiadającą wszystkie powyższe zalety jednocześnie, biometria tęczówki należy do cech, które można wykorzystać do budowy systemów prawie idealnych. Podstawowe zalety tej biometrii to niezmienność w trakcie życia osoby oraz wysoki stopień zróżnicowania.

Tęczówka jest mięśniem, który kontroluje natężenie strumienia światła docierającego do wnętrza oka, wykształca się w pełni już pod koniec ósmego miesiąca życia płodowego i jest niezmienna w trakcie życia. Pozwala na rozpoznawanie osób blisko spokrewnionych ze sobą (nawet bliźniąt jednojajowych), struktura tęczówki w znikomym stopniu zależy od naszych genów. Do poprawnego rozpoznania osoby wystarczający jest obraz jednego oka, chociaż metody wykorzystujące parę oczu są wygodniejsze w użyciu i cechują się mniejszym stopniem fałszywych odrzuceń. Zakłócenia spowodowane rzęsami, powiekami, odblaskami światła itp. poddawane są procesowi eliminacji zakłóceń oraz przekształcane są do postaci identycznej dla każdego oka. Przetworzony obraz poddawany jest także kodowaniu i filtrowaniu, a wynik tych działań zapisywany jest w postaci odpowiedniego kodu binarnego. Dużą zaletą systemów z biometrią tęczówki jest bardzo duża dokładność weryfikacji. Badania wskazują na błędy fałszywego odrzucenia rzędu 0,1%, a fałszywej akceptacji

na poziomie 0,001%. Problemem jest uciążliwy pomiar tęczówki, wymagający nierzadko wcześniejszego przygotowania.

Biometria siatkówki oka. Biometria ta opiera się o zdjęcie wykonywane przy pomocy specjalnej kamery, z niewielkiej odległości od oka, przy równoczesnym naświetlaniu światłem podczerwonym przez około 2 sekundy. Uzyskany obraz pozwala określić współczynniki wchodzące w skład kodu siatkówki (wykorzystuje się w tym celu transformatę Fouriera), długość tego kodu wynosi na ogół 320 bitów. Systemy, które wykorzystują biometrię siatkówki, cechują się wysokim stopniem bezpieczeństwa, małą wygodą użytkowania oraz stosunkowo wysokimi kosztami urządzeń biometrycznych. Z tego też względu zastosowanie biometrii siatkówki nie jest szeroko stosowaną technologią.

Biometria dłoni. Systemy biometryczne, w których wykorzystuje się cechy geometryczne dłoni, zapewniają wysoki poziom bezpieczeństwa, są wygodne w użyciu i stosunkowo tanie. Metoda pomiarowa nie budzi oporów ze strony użytkowników, a łatwość użycia sprawia, że systemy biometrii dłoni odznaczają się jednym z najniższych poziomów błędu fałszywego odrzucenia (w porównaniu z innymi metodami biometrycznymi). Efektem tego jest bardzo częste wykorzystywanie systemów z geometrią dłoni jako systemów kontroli dostępu w różnego rodzaju instytucjach i przedsiębiorstwach. Urządzenie pomiarowe typowego systemu biometrii dłoni składa się z panelu, na którym użytkownik umieszcza dłoń, oraz kamery – za pomocą której wykonywane jest zdjęcie. Panel wyposażony jest w specjalne elementy pozycjonujące, ułatwiające prawidłowe ułożenie dłoni oraz dodatkowe lustra umożliwiające obserwację bocznych krawędzi dłoni i kciuka. Można spotkać również w praktycznych zastosowaniach wykorzystanie rozkładu temperatury dłoni – pozwala to w sposób bardziej precyzyjny dokonywać weryfikacji tożsamości. Jednym z głównych powodów wykorzystywania termiki dłoni jest rozszerzenie tradycyjnych systemów geometrii dłoni o tzw. testowanie żywotności. Ma to na celu przeciwdziałanie oszustwom z wykorzystaniem sztucznych obiektów o geometrii zbliżonej do geometrii dłoni.

Biometria głosu. Technologia biometrii głosu związana jest z weryfikacją mówiącego (a dokładniej – weryfikacją wytworzonego sygnału mowy). Polega ona na stwierdzeniu, czy określona fraza została wypowiedziana przez daną osobę. Do weryfikacji osoby mówiącej wykorzystywane są właściwości akustyczno-fonetyczne dźwięku, a szczególnie podstawowa częstotliwość dźwięku, energia sygnału oraz struktura spektralna fonemów. Wśród systemów weryfikacji mówcy wyróżnia się systemy zależne od wypowiadanej sentencji (ang. *Text-dependent*) oraz systemy weryfikacji niezależne od wypowiadanej sentencji (ang. *Text-independent*), w których pojawia się wymóg utworzenia wektora cech niezależnego od treści wypowiadanego zdania. Do weryfikacji tak wytworzonych zestawów cech wykorzystuje się m.in. takie techniki, jak: dynamiczne zawijanie czasu (*ang. Dynamic Time Warping, DTW*),

kwantyzacja wektorowa (*ang. Vector Quantization, VQ*), ukryte modele Markowa (*ang. Hidden Markov Models, HMM*) czy sieci neuronowe (*ang. Neural Networks*). Biometria głosu ma wysoki stopień akceptacji przez użytkowników, ze względu na wygodę użytkowania, nieinwazyjność, stosunkowo krótki czas poboru charakterystyki oraz niezbyt wysokie wymagania sprzętowe. Błędne odrzucenia wynikają na ogół ze zbyt głośnego/cichego, zbyt szybkiego/powolnego mówienia. Jednym z wymogów tego systemu jest konieczność zapewnienia ciszy w trakcie rejestracji dźwięków. Zastosowania opisywanej technologii są coraz szersze, począwszy od podawania hasła w systemach dostępowych, a skończywszy na zakupach przez telefon, czy też weryfikacji osób korzystających z automatycznych serwisów telefonicznych.

Biometria twarzy. Podstawowym elementem systemów wykorzystujących biometrię opartą na geometrii twarzy jest detekcja oraz lokalizacja twarzy w obrazach otrzymywanych z kamer. Obszar obrazu zawierający wybraną twarz jest traktowany jako wektor elementów o tym samym poziomie ważności. Przy wykorzystaniu metod statystycznych eliminowane są elementy silnie skorelowane, a pozostałe elementy tworzą interesujący nas wektor cech twarzy (najczęściej wykorzystywana jest metoda analizy składowej głównej). Innym sposobem weryfikacji obrazu twarzy jest wykorzystanie punktów charakterystycznych twarzy (takich jak oczy, nos, kąciki ust) oraz obliczanie matematycznych zależności między tymi punktami (np. metodą dopasowania grafu). Biometria geometrii twarzy jest niestety jedną z najmniej skutecznych metod biometrycznych. Wynika to z jej podatności na zniekształcenia obrazu spowodowane czynnikami zewnętrznymi lub związanymi z uwierzytelnianą osobą. Natomiast ma też określone zalety, m.in. nieinwazyjność oraz możliwość zastosowania bez współpracy (często też wiedzy) identyfikowanej osoby. Biometrię tę stosuje się coraz częściej w sytuacjach, gdy mamy do czynienia ze zgromadzeniami dużej liczby osób – np. na stadionach, w trakcie koncertów, czy też na ulicach dużych metropolii.

Podsumowując, można stwierdzić, że możliwości wykorzystania danych biometrycznych są coraz większe, a co za tym idzie – wzrasta również ich praktyczne zastosowanie. Kluczowym elementem, który należy uwzględnić w trakcie projektowania, budowy i eksploatacji systemów wykorzystujących biometrię, jest problem przypisania właściwej osoby do właściwego dokumentu. Oczywiście zakłada się, że systemy spełniają wszelkie wymogi związane z ochroną swoich zasobów danych – czyli danych bardzo wrażliwych, umożliwiających identyfikację i weryfikację osób. Zakłada się, że nie pozwalają na kradzież tożsamości czy też na stworzenie „sztucznej" tożsamości.

BIBLIOGRAFIA

1. R. Anderson, *Inżynieria zabezpieczeń*, wyd. WNT, Warszawa 2007.
2. R.M. Bolle, J.H. Connell, S. Pankanti, *Biometria*, Warszawa 2008.
3. A. Drygajło, wykłady: *Biometrics*, 2006/2007, (http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/).
4. R.W. Kaszubski, *Biometria w bankowości i administracji publicznej*, praca zbiorowa pod redakcją R.W. Kaszubskiego, Związek Banków Polskich, Warszawa 2009.
5. P. Niedziejko, I. Krysowaty, *Biometria. Charakterystyka danych człowieka i ich wykorzystanie w bezpieczeństwie*, „Zabezpieczenia", 4/2006 i 1/2007, wyd. AAT.
6. J.W. Ross, R. Weill, D.C. Robertson, *Architektura korporacyjna jako strategia*, wyd. Studio Emka, Warszawa 2010.
7. A. Wiśniewski, *Metody oceny systemów rozpoznawania mówców*, „Biuletyn IAiR", nr 13 (2000).

The Biometrics and the Identification Documents

Abstract. Using biometrics with the identification documents is an innovation undergoing process of technological adjustments. The possibility of using information systems, especially documents, with biometric features is still at large, but evolving. The goal of this paper is to focus attention on necessity to define firm match between ID document and ID holder. Very crucial in matching is linking right person to correct ID document that is used to authenticate the person. In a subsequent part of the article different biometrics technologies are characterized. Those can be applied to secure identification (ID) documents (with both physical and behavioral biometric technologies). Their capabilities and limitations in the mass usage are, therefore, described. Possibility, but in certain situations necessity, of using biometric data is a result of wide use of information technology in everyday life (especially Internet) and increasing number of attempts of theft, of such identity.