DOI: 10.15199/13.2016.9.23

Obszary zastosowań biometrii

(Biometry areas applications)

mgr inż. KRZYSZTOF DZIK, mgr inż. ELŻBIETA GOMULSKA, mgr inż. LECH NAUMOWSKI, mgr inż. MIROSŁAWA PLUCIŃSKA

Instytut Maszyn Matematycznych, Warszawa

Streszczenie

Postęp w zastosowaniach biometrii w identyfikacji jest stały i konsekwentny. Artykuł przedstawia i podsumowuje ten zakres zastosowań biometrii, z uwzględnieniem najnowszych osiągnięć w tej dziedzinie.

Słowa kluczowe: potwierdzanie tożsamości, uwierzytelnianie biometryczne, kontrola dostępu

Abstract

Progress in the biometrics applications to identify is stable and consistent. The article presents the latest applications of biometrics identification.

Keywords: confirmation of identity, biometric authentication, access control

Biometria to dziedzina zajmująca się pomiarami cech fizycznych i behawioralnych człowieka. Wiele cech człowieka jest unikalnych w skali całej populacji (np. linie papilarne, układ naczyń krwionośnych) i charakterystycznych dla każdego z nas. Tę właściwość można wykorzystać do potwierdzenia tożsamości poszczególnych osób.

W ostatnich dwudziestu latach nastąpił bardzo szybki rozwój urządzeń biometrycznych opartych o rozpoznawania różnych cech fizycznych i behawioralnych. Są one wykorzystywane w następujących celach:

- do potwierdzania tożsamości,
- do dostępu do usług, zasobów i pomieszczeń,
- do tworzenia systemów śledzących zachowanie człowieka i sygnalizujących stany niepożądane lub niepokojące.

Rys. 1. Najczęściej spotykane obszary zastosowania technik biometrycznych w praktyce
Fig. 1. The most common areas of use of biometric techniques in practice

Potwierdzanie tożsamości

Potwierdzenie tożsamości może zostać dokonane przez innego człowieka (np. urzędnika, pracownika banku) z wykorzystaniem informacji biometrycznych zawartych w dokumentach drukowanych na papierze (zdjęcie, PESEL itp.) lub w sposób automatyczny przez urządzenia techniczne. Aby potwierdzić biometrycznie czyjąś tożsamość należy porównać pobraną wcześniej próbkę wzorcową cechy z próbką prezentowaną w procesie weryfikacji tożsamości. Zawsze pobieranie próbki wzorcowej musi być przeprowadzone po starannej weryfikacji tożsamości przez osobę uprawnioną w sposób bezpieczny ze ścisłym zachowaniem procedur. Jest to bardzo istotne ze względu na konieczność wykluczenia fałszowania tożsamości. Próbka wzorcowa może być przechowywana w bazie danych systemu informatycznego lub na karcie będącej w posiadaniu właściciela cechy. Zależnie od celu weryfikacji tożsamości systemy takie są tworzone w oparciu o prawo międzynarodowe lub krajowe przez państwa lub wyspecjalizowane instytucje. Karta zawierająca m.in. wzorzec biometryczny stała się w wielu krajach dokumentem potwierdzającym tożsamość obywatela i może pełnić funkcję dokumentu tożsamości, paszportu lub karty wykorzystywanej wyłącznie w określonym systemie (np. ochrona zdrowia, wypłata zasiłków etc.).

Ochrona granic

Potwierdzenie tożsamości jest szczególnie istotne przy przekraczaniu granic państwowych. Rozwój poligrafii i duża dostępność wysokiej jakości urządzeń drukujących sprawia, że coraz częściej są fałszowane tradycyjne papierowe dokumenty tożsamości. Wykorzystanie biometrii w decydującym stopniu uniemożliwia posługiwanie się sfałszowanymi dokumentami. Aby zapewnić większą kontrolę przepływu osób i ułatwić kontrolę graniczną Międzynarodowa Organizacja Lotnictwa Cywilnego (*International Civil Aviation Organization – ICAO*) opracowała standardy paszportu odczytywanego maszynowo a następ-

nie rozszerzonego o warstwę elektroniczną i dane biometryczne (Dokument Doc 9303). Ze względu na rozwój systemów zabezpieczeń standardy te są stale uzupełniane i aktualizowane. Wytyczne zawarte w tym dokumencie są implementowane w paszportach na całym świecie. Uwzględniając wyżej przytoczone uregulowania, 13 grudnia 2004 roku Rada Unii Europejskiej wydała *Rozporządzenie Rady [We] Nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie* zobowiązujące państwa członkowskie do wydawania paszportów zawierających w warstwie elektronicznej obraz twarzy oraz – od 2009 r. – linii papilarnych palców wskazujących.

Biometria została także wykorzystana w systemach wydawania wiz. W 2002 r. Stany Zjednoczone aktem „Enhanced Border Security and Visa Entry Reform Act" postanowiły, że od 26 października 2004 r. władze amerykańskie będą wydawać wizy do odczytu maszynowego z danymi biometrycznymi oraz, że posiadanie paszportu biometrycznego będzie jednym z warunków zwolnienia z obowiązku wizowego przy wjeździe do USA. Obecnie wiele państw na świecie pobiera dane biometryczne od osób ubiegających się o wizę, np. Australia (obraz twarzy + odciski linii papilarnych). Niektóre, kierując się bezpieczeństwem narodowym np. Japonia, USA, Kanada (od 2013 r.), pobierają dane biometryczne obywateli innych państw przekraczających granice i przechowują je we własnych bazach.

Systemy automatycznej kontroli dokumentów znacznie usprawniają i przyspieszają (średnio z kilku, kilkunastu minut do 6–10 sekund) odprawę pasażerów oraz zapobiegają lub znacznie utrudniają przekraczanie granic państwowych przez osoby niepożądane lub posługujące się sfałszowanymi dokumentami. Często są stosowane na lotniskach. Z reguły ten sposób odprawy jest dedykowany tylko dla obywateli pochodzących z niektórych państw i obowiązkowo posiadających paszport biometryczny, np. automatyczne bramki instalowane na lotniskach: Gatwick, Heathrow, w Birmingham, Bristolu , Cardiff, East Midlands, Luton, Manchester oraz Stansted w Wielkiej Brytanii są przeznaczone tylko dla obywateli ze strefy Schengen. Często – jak np. w Dubaju czy Nowym Jorku wymagana jest dodatkowo rejestracja pasażerów w dedykowanych systemach informatycznych. Ten typ odprawy paszportowej jest stosowany i szczególnie przydatny dla osób często podróżujących.

Inne przykłady:

W Hiszpanii na pięciu największych lotniskach – w Madrycie, Barcelonie (od 2010 r.), Gironie, Palma de Mallorca i Alicante oraz na Teneryfie i w Maladze z powodzeniem wdrożono system Indra, obejmujący 124 kioski automatycznej kontroli granicznej wyposażone w czytniki linii papilarnych i kamery pobierające obraz twarzy, przeznaczony dla pasażerów Europejskiego Obszaru Gospodarczego (obszar Schengen) powracających z państw trzecich. Weryfikacja tożsamości odbywa się na podstawie danych zawartych w warstwie elektronicznej paszportu biometrycznego. System ten działa również w porcie w Algeciras, z którego korzystają turyści z całej Europy podróżujący do Afryki.

W Australii w Sydney jest możliwa automatyczna kontrola dla turystów z Australii, Nowej Zelandii, Wielkiej Brytanii, Szwajcarii, Singapuru i Stanów Zjednoczonych, którzy posiadają paszport biometryczny (system SmartGate). Na podobnej zasadzie – wykorzystując obraz twarzy – działa system zainstalowany na lotnisku w Dubaju (dla obywateli USA, Australii i niektórych państw Europy i Azji, którzy zarejestrowali się w systemie wizowym i po raz kolejny odwiedzają Emiraty Arabskie).

W najbliższym czasie planuje się wdrożenie systemu wstępnej weryfikacji tożsamości na podstawie obrazu twarzy na lotnisku John F. Kennedy w Nowym Jorku dla obywateli państw mających prawo do wjazdu do USA bez posiadania wizy (Visa Waiver Program, VWP) zarejestrowanych w systemie elektronicznym autoryzacji podróży (Electronic System for Travel Authorization ESTA).

W wielu portach lotniczych na świecie testuje się technologie biometryczne w instalacjach pilotażowych (np. Ataturk Airport w Instambule, Haneda w Tokio, Amsterdam).

W Kanadzie wdrożono System CANPASS (Canadian Passenger Accelerated Service System) stosowany przez urzędy celne Kanady i USA wykorzystujący technologię biometryczną w celu ułatwienia przepływu osób i towarów między tymi państwami. System CANPASS obejmuje osoby często przekraczające granice (np. kierowcy ciężarówek) i stanowiące minimalne ryzyko dla bezpieczeństwa państwa i dotyczy ruchu granicznego między USA i Kanadą, w tym małych samolotów korporacyjnych (do 15 osób) oraz łodzi prywatnych.

Na terenie Europy po zniesieniu kontroli granicznych wewnątrz państw strefy Schengen zaistniała konieczność zapewnienia bezpieczeństwa i nie dopuszczania do wjazdu w strefę osób niepożądanych. Dlatego też utworzono bazę danych Systemu Informacyjnego Schengen (SIS), w której są gromadzone dane biometryczne osób poszukiwanych, niejawnie nadzorowanych lub objętych zakazem wstępu na terytorium państw strefy Schengen. Dostęp do bazy ma straż graniczna, policja i wydziały konsularne ambasad.

Biometria w dowodach osobistych

Prawie we wszystkich krajach na świecie są wydawane dla obywateli karty tożsamości (dowody osobiste). Wiele z tych dokumentów posiada warstwę elektroniczną, a wśród tej grupy tylko w niektórych z nich zostały zapisane dane biometryczne (najczęściej obraz twarzy, linii papilarnych lub siatkówki oka, rzadziej podpis odręczny). W niektórych państwach dane biometryczne zamiast w dokumencie tożsamości są umieszczane w centralnych bazach danych.

Największym biometrycznych projektem na świecie jest system UIDAI (Unique Identification Authority of India) prowadzony przez agendy rządowe Indii. Celem działania systemu jest nadanie każdemu obywatelowi Indii tylko jednego, unikalnego numeru identyfikacyjnego AADHAR i uniemożliwienie jakiegokolwiek fałszerstwa lub duplikowania tożsamości i udostępnianie wielu usług publicznych. Indie są klasycznym przykładem kraju, gdzie ze względu na olbrzymią biedę i analfabetyzm znacznej części społeczeństwa oraz występowanie dużych obszarów niezurbanizowanych o bardzo niskim poziomie rozwoju technologicznego i infrastruktury dochodzi do olbrzymiej korupcji środków publicznych, szczególnie w zakresie zasiłków opieki społecznej i służby zdrowia. W takich warunkach nie sprawdzają się typowe sposoby potwierdzania tożsamości beneficjentów programów pomocowych – ludzie bardzo często nie mają żadnych dokumentów. Równocześnie poziom rozwoju społecznego i znajomość praw obywatelskich jest niski, dlatego, w odróżnieniu od wielu państw wysokorozwiniętych, pobieranie wzorców biometrycznych nie jest postrzegane jako naruszenie prywatności. W procesie nadawania numeru AADHAR od każdej osoby są pobierane i zapisywane do centralnej bazy obrazy cech biometrycznych (linie papilarne, twarz, siatkówka oka) i w procesie identyfikacji jest sprawdzane, czy nie została już wcześniej zarejestrowana osoba o takich ce-

chach. W każdej chwili uprawnione instytucje (urzędy, banki etc.) mogą zależnie od potrzeb potwierdzić tożsamość obywatela na jednym z pięciu poziomów bezpieczeństwa (w tym trzy poziomy wymagają pobrania próbki biometrycznej jedno- lub wielomodalnej) – dane z bazy nie są nikomu udostępniane, jedynie uzyskuje się odpowiedź typu tak-nie. Karta AADHAR nie zawiera danych biometrycznych. Niedawno poinformowano, że w kwietniu 2016 r. było zarejestrowanych w bazie ponad 1 mld numerów AADHAR.

Na podobnej zasadzie, tzn. sprawdzania danych biometrycznych w centralnej bazie działa np. system wydawania prawa jazdy w USA czy dowodów tożsamości w Hiszpanii oraz Izraelu.

W niektórych państwach, szczególnie wysokorozwiniętych, dane biometryczne obywatela są umieszczane wyłącznie w warstwie elektronicznej dowodu tożsamości. Ze względu na długi czas wdrażania i koszty równocześnie są akceptowalne zarówno dowody biometryczne jak i wcześniej obowiązujące rozwiązania. Biometryczne karty identyfikacyjne praktycznie są wydawane zaledwie od kilku lat – to pierwszy krok w celu wprowadzenia na dużą skalę biometrycznej weryfikacji tożsamości.

Obraz twarzy i/lub linii papilarnych jest umieszczony w dokumentach tożsamości wydawanych m.in. przez Belgię, Łotwę, Litwę, Włochy, Portugalię, Mongolię (w dwóch ostatnich przypadkach – porównanie wzorca odbywa się na karcie) .

W celu optymalizacji kosztów niektóre państwa zdecydowały się na wieloaplikacyjne elektroniczne dokumenty tożsamości zawierające m.in. dane biometryczne np. Belgia (potwierdzanie tożsamości w Internecie, kontakt z urzędami administracji publicznej, podpis elektroniczny, potwierdzanie wieku przy zakupach w automatach itp.), czy Hong Kong (klucze podpisu elektronicznego, karta biblioteczna, karta rezerwacyjna, dostęp do e-administracji). Weryfikacja tożsamości zależnie od potrzeb odbywa się z wykorzystaniem certyfikatów lub biometrii.

Także na Filipinach zdecydowano się na korzystanie z dokumentów wielofunkcyjnych (karta tożsamości, karta VISA, dostępu do usług medycznych oraz świadczeń studenckich itp.). W agendach rządowych oraz urzędach ubezpieczeń społecznych (GSIS) zlokalizowano kioski, które za pomocą sieci bezprzewodowej, identyfikacji radiowej, biometrii (linie papilarne) i technologii wirtualnej sieci prywatnej pozwalają na dostęp do wielu e-usług. Turcja wydała dla żołnierzy sił NATO rezydujących na jej terytorium kartę identyfikacyjną, która służą do różnych celów: biometryczna identyfikacja oparta o linie papilarne, e-portmonetka do zakupów bezgotówkowych, składanie podpisu elektronicznego, logiczna kontrola dostępu, e-zdrowie, fizyczna kontrola dostępu).

Innym podejściem, reprezentowanym dotychczas przez np. Norwegię, jest wydawanie numerów identyfikacyjnych i/lub kart elektronicznych dedykowanych konkretnym aplikacjom lub grupom zastosowań. Obywatele Norwegii mogą posiadać paszporty lub/i identyfikatory wydane przez banki, Agencję Zarządzania Publicznego i e-administracji czy Buypass. Ze względów bezpieczeństwa rząd Norwegii planuje jednak wprowadzić dowód tożsamości z danymi jak w paszporcie od 2017 r.

Uwierzytelnianie biometryczne

Automatyczne potwierdzenie tożsamości to podstawa do udostępniania wielu usług zarówno publicznych jak i komercyjnych dla obywatela lokalnie lub w trybie zdalnym przez Internet. Przy burzliwie rozwijającej się informatyzacji otoczenia należy oczekiwać, że w najbliższych latach coraz więcej spraw będzie załatwianych przez obywatela/interesanta w ten właśnie sposób. Przy dostępie zdalnym jedynie biometria pozwala na jednoznaczną, niezaprzeczalną weryfikację tożsamości człowieka – każda inna metoda może być podważona – można przez niefrasobliwość właściciela lub na skutek przestępstwa wejść w posiadanie danych niezbędnych do weryfikacji (np. hasło, karta z certyfikatem itp.).

Informatyzacja kraju, w tym administracji, internetowy dostępu do różnych rejestrów, usług publicznych i komercyjnych, zwłaszcza bankowych wymaga wiarygodnego uwierzytelnienia osób chcących skorzystać z możliwości, jakie daje Internet i komunikacja mobilna. W związku z tym widoczna jest tendencja do szukania tanich rozwiązań technicznych umożliwiających uwierzytelnianie biometryczne, w tym w uzasadnionych przypadkach wykorzystywanie uwierzytelnienia dwuskładnikowego lub biometrii multimodalnej.

Wykorzystanie biometrii w celu uwierzytelniania zdobywa coraz większą akceptowalność wśród społeczeństwa. Na takie rozwiązania otwarci są ludzie młodzi, którzy cenią sobie nowinki techniczne, szybkość i wygodę, ludzie starsi potrzebujący poczucia bezpieczeństwa oraz prostych rozwiązań (bez pamiętania kodów) i biznesmeni, których działalność wymaga niezawodnego, bezpiecznego potwierdzania tożsamości i przeprowadzania transakcji.

Bankowość

Najszerzej uwierzytelnianie biometryczne jest obecnie wykorzystywane w bankowości, a Polska jest jednym z liderów w tej dziedzinie w Europie. Biometrię w oddziałach i bankomatach stosują banki w Japonii, Brazylii, Turcji, Anglii, Włoszech, Słowacji, Czechach, USA itd. Stosowanie uwierzytelnienia biometrycznego w oddziałach bankowych do potwierdzania tożsamości pracowników oraz klientów zmniejsza kradzieże dokonywane przez pracowników banków i ogranicza wyłudzanie pieniędzy za pomocą skradzionych dokumentów. Także coraz więcej bankomatów jest wyposażonych w czytniki biometryczne (np. Bank Bradesco w Brazylii – ponad 30 tys. bankomatów).

Obecnie w bankach stosuje się urządzenia wykorzystujące następujące techniki biometryczne: układ naczyń krwionośnych palca – oddziały i bankomaty w Japonii (m.in. Mizuho Bank, SMBC, Japan Post Bank, Bank of Kyoto, CITI, HSBC) oraz Turcji (IS Bankasi), linie papilarne np. w Brazylii (Bank CAIXA, Itautec,) oraz głos (Barclays Bank w Anglii). Weryfikację klienta w oddziale za pomocą podpisu odręcznego stosują m.in. Tatra Banka na Słowacji, Unicredit Włochy, Intesa San Paolo Bank, GE Money Bank w Czechach, Reiffeisen Bank itd.

Szereg banków australijskich wprowadziło technologie biometryczne, które pozwalają klientom zalogować się do usług bankowych mobilnych wykorzystując swoje odciski palców lub głos (np. Bank of Melbourne 2014, Westpac 2015) zamiast haseł.

Biometrię głosową do komunikacji z Call Center wprowadziły Tatra Banka, Barclays Bank, Eastern Bank (USA).

W Polsce pierwsze prace nad zastosowaniem biometrii (rozpoznawanie naczyń krwionośnych palca) w bankowości podjął Podkarpacki Bank Spółdzielczy (PBS) w 2009 r. Od tej pory uwierzytelnianie biometryczne oparte o naczynia krwionośne w oddziałach i w bankomatach stosuje wiele banków spółdzielczych – Bank Polskiej Spółdzielczości (BPS), Krakowski Bank Spółdzielczy, Bank Spółdzielczy w Kielcach, itd. oraz BPH S.A., Getin Bank, BZ WBK. Smart Bank, Meritum Bank i BZ WBK umożliwiły klientom uwierzytelnianie głosowe w Call Center, a Bank Milennium uwierzytelnianie mobilne za

pomocą linii papilarnych skanowanych przez czytniki wbudowane w smartfony.

Usługi publiczne, e-goverment

Wraz z informatyzacją administracji państwowej pojawia się szansa na budowanie e-usług dostępnych dla obywateli. Sprawy urzędowe będziemy załatwiać nie wychodząc z domu. Należy jednak, szczególnie dla działań mających skutek prawny, zapewnić niezaprzeczalne potwierdzenie tożsamości osoby. I tu biometria przychodzi z pomocą. Trzeba jasno powiedzieć – biometria w autoryzacji dostępu do usług jest tylko jednym ze sposobów weryfikacji tożsamości, w niektórych sytuacjach wręcz idealnym, w innych – gdzie wymagany jest niższy poziom bezpieczeństwa lub waga spraw – ze względu na koszty i dostępność nadmiarowym. Obecnie najczęstsze obszary zastosowań biometrii to wybory parlamentarne, zasiłki, służba zdrowia i wojsko.

W wielu krajach szczególnie o niskim poziomie rozwoju demokracji jest trudno przeprowadzić wybory w taki sposób, aby zapobiec manipulacjom głosami wyborców. Często znacząca część wyborców wielomilionowego państwa nie posiada żadnych dowodów tożsamości – tak się dzieje np. w niektórych biednych państwach Afryki czy Azji. Wykorzystanie biometrii – najczęściej linii papilarnych – do tworzenia list wyborców i przeprowadzenia głosowania okazało się efektywne – przykładem wybory prezydenckie 2015 r. w Nigerii, czy parlamentarne w Kirgistanie. Brazylia zamierza przeprowadzić wybory w roku 2018 r. w sposób w pełni zautomatyzowany z wykorzystaniem logowania biometrycznego. System będzie obejmował ok. 155 milionów uprawnionych do głosowania (pilotaż w wyborach 2010 r. na próbie 1.2 mln osób).

Jednym z procesów, w którym bywa stosowane uwierzytelnienie biometryczne to wypłata zasiłków socjalnych (np. Indie, Filipiny). Okazało się, że w specyficznym środowisku (często ludzie o bardzo niskim poziomie wykształcenia) biometria sprawdza się dobrze – zarówno zapobiega oszustwom jak i jest akceptowalna i wygodna dla użytkowników.

Kolejny obszar zastosowań to służba zdrowia i ubezpieczenia społeczne. Istotną okolicznością jest potrzeba ochrony danych wrażliwych dotyczących stanu zdrowia pacjentów. W obecnych czasach występują tendencje do tworzenia dużych baz danych zawierających informacje o procesie leczenia. Aby dobrze chronić prywatność pacjenta wprowadza się rygorystyczne zasady logowania do systemów informatycznych korzystając m.in. z czytników biometrycznych (np. zespół opieki zdrowotnej Sharp Healthcare w San Diego w USA – 1800 łózek, 4000 lekarzy, sieć szpitali i ośrodków zdrowia dla ok. 3 mln osób, biometryczna weryfikacja tożsamości pacjenta w szpitalach).

Jednym z najstarszych zastosowań biometrii jest rozpoznawanie przestępców na podstawie odcisków palców zostawionych na miejscu zbrodni. Dawniej robił to człowiek przeglądając i porównując obrazy, teraz jest to robione wielokroć szybciej i efektywniej automatycznie (systemy AFIS).

Kontrola dostępu

Sprawdzonym, istniejącym od lat obszarem stosowania biometrii jest kontrola dostępu fizycznego do pomieszczeń i stref strzeżonych oraz kontrola dostępu logicznego do zasobów danych. Czytniki biometryczne są używane do zabezpieczenia dostępu do wrażliwej infrastruktury np. obiektów zarządzania ruchem lotniczym, serwerowni, miejsc przechowywania tajnych dokumentów. Chronią także tajemnice firmy – urządzenia biometryczne wchodzą często w skład systemów zabezpieczeń dostępu fizycznego do różnych obiektów przemysłowych (np. w energetyce). Prostym, wygodnym i użytecznym rozwiązaniem jest stosowanie zamków biometrycznych w domach mieszkalnych. Biometria jest stosowana w kontroli dostępu do zasobów systemów informatycznych. Ważnym elementem upowszechniania technik biometrycznych jest wbudowywanie czytników biometrycznych w urządzenia powszechnie dostępne (np. laptopy firmy Hewlett-Packard lub niektóre smartfony firmy Samsung, Sharp, iPhone5S Apple). Użytkownik może zablokować dostęp do korzystania z urządzenia osobom postronnym – w ten sposób chroni zarówno często bardzo cenne informacje zgromadzone lokalnie na dysku jak i zapobiega nieuprawnionemu dostępowi zdalnemu do systemów firm).

Inne zastosowania

Od lat znana i stosowana jest w medycynie aparatura do oceny zdrowia pacjenta (np. pomiar tętna, pracy serca, oddechu etc.). Postęp technologiczny w zakresie pobierania, obróbki i przetwarzania danych opisujących bardzo różnorodne cechy człowieka stał się motorem znajdowania nowych, ciekawych zastosowań praktycznych. Z najnowszych rozwiązań – bardzo modne stały się opaski monitorujące różne funkcje życiowe człowieka. Ich zakres wykorzystania jest bardzo szeroki – od ciekawych gadżetów mierzących puls, urządzeń monitorujących treningi sportowców po elementy pomiarowe systemów telemedycyny (zdalny np. monitoring pracy serca, opieka położnicza).

Ciekawym, ciągle jeszcze mało zbadanym obszarem jest wykorzystywanie analizy zachowania człowieka (biometria behawioralna). Na świecie prowadzi się badania nad stworzeniem systemów monitorujących reakcje kierowców prowadzących auta (np. opracowano Pakiet Driver Assistant dla samochodów Ford). Na podstawie m.in. ruchów gałek ocznych próbuje się diagnozować stan zasypiania kierowcy i na tej podstawie jest włączany sygnał alarmu. Testuje się także możliwość wykorzystania niektórych zachowań do potwierdzania tożsamości – np. okazuje się, że szybkość i sposób pisania na klawiaturze jest cechą dość charakterystyczną dla każdego z nas. W przyszłości maszyna – jak obecnie nasze oko – będzie potrafiła być może rozpoznać nas po sposobie chodzenia.

Za pomocą biometrii głosowej przez urządzenia mobilne możliwy jest dostęp do Call Center operatorów sieci telefonii komórkowej, np. T-Mobile.

Czytniki biometryczne często pełniące także funkcję urządzeń kontroli dostępu bywają stosowane w systemach rejestracji czasu pracy. Ze względu na niezaprzeczalność rejestracji ich stosowanie jest bardzo użyteczne w rozstrzyganiu sporów na linii pracownik - pracodawca dotyczących rzeczywistego czasu pracy. Co ciekawe – w praktyce okazało się, że sam fakt zainstalowania tego typu systemu w znaczący sposób wpływa na poprawę dyscypliny wśród pracowników.

Biometryczna identyfikacja człowieka ma także bardzo duże znaczenie w zapewnieniu naszego bezpieczeństwa. Na wielu stadionach piłkarskich istnieją systemy, które na podstawie obrazu twarzy potrafią zidentyfikować osoby niebezpieczne lub niepożądane.

Wcześniej opisano tylko niektóre, najczęściej spotykane zastosowania biometrii – z pewnością nowe, dokładniejsze algorytmy porównywania próbek, miniaturyzacja urządzeń, spadek kosztów czytników, ludzka pomysłowość i inwencja przyczynią się do zastosowania biometrii w nowych, być może zaskakujących obszarach.