DOI: 10.15199/ELE-2014-015

Analiza technik biometrycznych do uwierzytelniania osób

mgr inż. MIROSŁAWA PLUCIŃSKA, JAROSŁAW WÓJTOWICZ
Instytut Maszyn Matematycznych, Warszawa

Elektronizacja administracji (e-administracja), upowszechnienie transakcji i usług internetowych (e-usługi) wymagają jednoznacznej weryfikacji osoby korzystającej z tych udogodnień. Wydaje się, że takie jednoznaczne potwierdzenie tożsamości osoby może zapewnić biometria. W związku z tym należy rozpatrzyć dostępne techniki biometryczne, przyjrzeć się im i wybrać te, które będą najbardziej przydatne do uwierzytelniania. Ogólny przegląd technik biometrycznych istniejących i rozwijanych obecnie na rynku z krótkim opisem metody działania i najważniejszymi wadami i zaletami został umieszczony w artykule pt.: „Krótki przegląd technik biometrycznych do rozpoznawania osób" autorstwa M. Plucińskiej i w związku z tym w obecnym artykule nie będzie przypomnienia technik jakie są obecnie na rynku, a jedynie ich porównanie.

Najważniejsze cechy technik biometrycznych

Analizę i porównywanie technik biometrycznych można przeprowadzić w różnych aspektach. Do najważniejszych cech charakteryzujących poszczególne techniki biometryczne opisanych parametrami urządzeń biometrycznych należą – wiarygodność techniki, akceptowalność społeczna i łatwość użycia, przepustowość określona czasem weryfikacji, wielkość wzorca, wielkość urządzenia, cena i inne.

Akceptowalność społeczna

Jedną z ważnych cech dotyczących technik biometrycznych jest akceptowalność społeczna biometrii. Strach przed przyłożeniem palca czy oka do urządzenia skanującego oraz obawa przed zostawianiem swoich danych biometrycznych są ciągle duże, ale ogólne podejście społeczeństwa do biometrii zmienia się. Z danych przytoczonych na Konferencji Naukowej Biometria 2010 (organizator Instytut Maszyn Matematycznych, Warszawa) w prezentacji prof. A. Koziczak z Uniwersytetu Kazimierza Wielkiego w Bydgoszczy, aż 77% ankietowanych studentów Wydziału Prawa i Administracji w wieku od 22 do 30 lat było za stosowaniem cech biometrycznych do szybkiego sprawdzenia tożsamości. Ankietowani godzili się na udostępnienie swojej cechy biometrycznej ze względu na zwiększenie bezpieczeństwa oraz dla wygody i ułatwień z tym związanych. Badania te wykazują, że stosunek młodych ludzi do rozwiązań biometrycznych ulega zmianie w stronę większej akceptowalności.

Badania społecznej akceptowalności podstawowych technik biometrycznych przeprowadzano w różnych ujęciach. Najlepiej akceptowalną metodą biometryczną jest badanie głosu, nie budzi większych zastrzeżeń przyłożenie palca do skanera, chociaż metoda ta uważana jest za metodę policyjną. Dalej plasuje się rozpoznawanie kształtu dłoni, rozpoznawane wzoru tęczówki i podpis odręczny. W innym podejściu metody biometryczne podzielono na nieinterakcyjne i interakcyjne, czyli wymagające kontaktu z urządzeniem pobierającym próbkę cechy biometrycznej. Najbardziej akceptowalne są metody nieinterakcyjne takie jak: analiza głosu, analiza rysów twarzy i analiza tęczówki. Metody interakcyjne budzą z różnych względów szereg wątpliwości. I tak np. dobrze akceptowalna w innych badaniach interakcyjna metoda analizy kształtu dłoni budzi wątpliwości ze względów higienicznych. Te same uwagi użytkownicy mają do pobierania obrazu linii papilarnych i wzoru naczyń krwionośnych palca. Największe obawy przez swoją inwazyjność rodzi metoda badania siatkówki.

Łatwość użycia

Na akceptowalność społeczną ma wpływ łatwość użycia danej techniki biometrycznej. Kolejność metod biometrycznych według łatwości użycia przedstawia się następująco: analiza głosu, analiza rysów twarzy, analiza kształtu dłoni, analiza wzoru naczyń krwionośnych, analiza linii papilarnych, analiza tęczówki, analiza siatkówki.

Analiza głosu i rysów twarzy ze względu na powszechność mikrofonów i kamer staje się ogólnie dostępna i nie wymaga od użytkownika dodatkowych nakładów. Techniki rozpoznawania kształtu dłoni, wzoru naczyń krwionośnych, czy linii papilarnych potrzebują do pobierania cechy biometrycznej urządzeń odpowiednio zaprojektowanych, ułatwiających w sposób naturalny ułożenie palca, czy dłoni na czytniku. Analiza tęczówki i siatkówki wymaga współpracy użytkownika i odpowiedniego pozycjonowania.

Wrażliwość na zakłócenia

Dla wyboru techniki biometrycznej jest ważne dobranie techniki odpowiedniej do warunków jej stosowania. Należy wziąć pod uwagę kto będzie z niej korzystał i jakie będą warunki środowiskowe, na przykład oświetlenie w miejscu jej stosowania.

Przykłady zakłóceń dla różnorodnych technik:

- analiza linii papilarnych – skaleczenia, brud
- analiza kształtu dłoni – opuchnięcie dłoni
- analiza siatkówki – okulary, zmiany chorobowe
- analiza tęczówki – okulary, złe oświetlenie, niewłaściwe pozycjonowanie
- analiza naczyń krwionośnych – złe oświetlenie zewnętrzne, bardzo brudne palce
- analiza głosu – chrypka, hałas
- analiza sposobu pisania na klawiaturze – naderwanie ścięgna
- analiza rysów twarzy – okulary, wąsy, broda, oświetlenie (lub temperatura ciała)

Przepustowość

Na zastosowanie wybranej metody biometrycznej w systemie duży wpływ ma przepustowość urządzenia ją realizującego, w tym czas pomiaru i podjęcia decyzji o wyniku uwierzytelnienia. W tym celu analizuje się:

- czas wprowadzania nowego wzorca,
- czas weryfikacji, obejmujący czas przygotowania do pomiaru, pomiar danych, czas porównania z określonym wzorcem,
- czas identyfikacji, obejmujący czas przygotowania do pomiaru, pomiar danych, czas porównania z wszystkimi zapamiętanymi wzorcami.

Przykładowe czasy trwania weryfikacji

– analiza linii papilarnych	0,5–1 s
– analiza naczyń krwionośnych palca	0,5–1,23 s
– analiza tęczówki	0,8–4,22 s
– analiza kształtu dłoni	< 1 s
– analiza naczyń krwionośnych dłoni	2,13 s
– analiza siatkówki	4–7 s
– analiza głosu	10–14 s

Rozmiar wzorca

Następnym ważnym parametrem branym pod uwagę przy porównywaniu technik biometrycznych jest rozmiar wzorca cechy biometrycznej, który rzutuje na wielkość pamięci potrzebnej do jego przechowywania oraz na czas weryfikacji lub identyfikacji. Proces identyfikacji jest dłuższy, ze względu na to, że identyfikacja wymaga porównania badanego wzorca z wieloma wzorcami przechowywanymi w pamięci, co jest czasochłonne i np. w systemach AFIS (*Automated Fingerprint Identification System*) proces identyfikacji wskazuje kilka najbardziej prawdopodobnych wzorców, a ostatecznego wyboru dokonuje człowiek.

Przykładowe rozmiary wzorców:

- kształtu dłoni 9 bajtów
- siatkówki 96 bajtów
- tęczówki 256 bajtów
- linii papilarnych 270–1500 bajtów
- naczyń krwionośnych palca 400 bajtów
- sposobu pisania na klawiaturze 1000–1500 bajtów
- głosu 1000–10000 bajtów
- naczyń krwionośnych dłoni 1300–2500 bajtów

Wiarygodność

Wiarygodność technik biometrycznych jest charakteryzowana przez wskaźniki:

- fałszywej akceptacji nieuprawnionej osoby (FAR – *False Acceptance Rate*),
- fałszywego odrzucenia uprawnionej osoby (FRR – *False Rejection Rate*),
- równowagi (EER – *Equal Error Rate*) między FAR i FRR.

Współczynnik FAR oznacza pozytywne rozpoznanie osoby nieuprawnionej, a współczynnik FRR – fałszywe odrzucenie osoby uprawnionej. Im współczynnik FAR jest lepszy i urządzenie nie wpuszcza nieuprawnionych osób, tym współczynnik FRR jest gorszy i więcej jest odrzucanych osób uprawnionych i odwrotnie. Poziom równowagi pomiędzy tymi parametrami określa współczynnik EER. Odpowiednie ustawienie współczynników jest zależne od zastosowania i wymaganego poziomu bezpieczeństwa.

Przykładowe porównanie współczynnika EER dla realizacji różnych metod biometrycznych:

- analiza tęczówki < 0,5%
- analiza siatkówki 1,5%
- analiza sposobu pisania na klawiaturze 1,6%
- analiza kształtu dłoni 2,2%
- analiza głosu 3–19,6%
- analiza linii papilarnych 5,0%

Porównanie technik biometrycznych

Wartości parametrów są związane nie tylko z zastosowaną metodą, ale również z danym rozwiązaniem technicznym, czyli urządzeniem. Dla przykładu w *tabeli 1* umieszczono wartości parametrów konkretnych urządzeń działających w oparciu o wybrane techniki.

Analizując dane z *tabeli 1* można zauważyć na przykładzie czytników UBReader firmy Hitachi i IMMSkan opracowanych w IMM, że kolejne wersje urządzeń opartych na tej samej technice biometrycznej charakteryzują się lepszymi parametrami.

W *tabeli* nie umieszczono techniki rozpoznawania głosu, gdyż jej parametry są ściśle związane z zastosowanym mikrofonem, kodekami, językiem i samym testem. Jakość tej metody najlepiej odzwierciedla błąd EER, czyli wskaźnik równowagi między wskaźnikiem fałszywego odrzucenia i fałszywej akceptacji. Badania przeprowadzone przez The U.S. *National Institute of Standards and Trademarks* (NIST) nad metodą rozpoznawania głosu firmy Nuance/PerSay wykazały dużą zależność metody od języka. Lepsze parametry EER są osiągane dla testów wykonywanych w języku angielskim (zależnie od testu 3–19,6%), niż dla innych języków (6,7–21,5%).

Jak pokazano w poprzednim rozdziale można rozpatrywać techniki biometryczne analizując ich parametry pod kątem różnych wymogów (*tabela 2, 3*). Ostateczny wybór techniki biometrycznej zależy od celu i wymagań aplikacji – wymaganego poziomu bezpieczeństwa, szybkości weryfikacji, wielkości pamięci potrzebnej do przechowywania wzorca, łatwości pobierania próbki biometrycznej oraz zapewnienia prywatności, a także możliwości finansowych. Należy więc na istniejące techniki popatrzeć pod kątem ich najlepszej użyteczności dla zewnętrznej aplikacji i stawianych przed nią celów – inne wymagania będzie miało uwierzytelnienie dostępu do danych bankowych, a inne np. do siłowni.

W systemach o wysokim poziomie bezpieczeństwa najlepsze wydaje się rozpoznawanie osoby na podstawie wzoru siatkówki oka. Metoda ta nie nadaje się jednak do masowego stosowania. Jest trudna do użytkowania, droga i mało akceptowalna społecznie. Jest przeznaczona do specjalnych systemów i aplikacji, które muszą zapewniać maksymalne bezpieczeństwo. Rozpoznawa-

Tab. 1. Zestawienie podstawowych parametrów wybranych urządzeń biometrycznych

Tabl. 1. The basic parameters of the selected biometric devices

Źródło: Hitachi Europe Ltd., Oddział w Polsce, Instytut Maszyn Matematycznych (IMM)

Biometria	Naczynia krwionośne palca	Naczynia krwionośne palca	Naczynia krwionośne dłoni	Tęczówka	Podpis odręczny	Linie papilarne	Linie papilarne
Producent	*Hitachi*	*Hitachi*	*Fujitsu*	*IrisGuard*	*NASK*	*IMM*	*IMM*
Urządzenia	*UBReader 1*	*UBReader 2*	*PalmSecure*	*H100*	*BiomOnline Signature*	*IMMSkan 100*	*IMMSkan 300*
FRR	1,26%	0,01%	4,23%	1,76%	1,82%	1%	0,1%
FAR	0,01%	0,0001%	0,0118%	0,01%	1,74%	0,1%	0,01%
Czas weryfikacji [s]	1,23	0,5	2,13	4,22	–	<1	<1
Czas rejestracji [s]	33,3	<20	61,7	44,5	–	<3	<3

Tab. 2. Ocena parametrów wybranych technik biometrycznych. Tabl. 2. Assessment of selected biometric technologies

Źródło: Hitachi Europe Ltd., Oddział w Polsce, Instytut Maszyn Matematycznych

Technika	Cena	Akceptowalność	Wiarygodność	Rozmiar urządzenia
Analiza naczyń krwionośnych palca	średnia	wysoka	wysoka	średni/mały
Analiza naczyń krwionośnych dłoni	niska/średnia	wysoka	wysoka	średni
Analiza tęczówki	wysoka	niska	wysoka	duży
Analiza linii papilarnych	niska	średnia	średnia	mały/średni

Tab. 3. Klasyfikacja technik biometrycznych. Tabl. 3. Classification of biometric technologies

Parametr	Biometria
Akceptowalność	głos, rysy twarzy, naczynia palca, linie papilarne, kształt dłoni, tęczówka, podpis odręczny, siatkówka
Łatwość użycia	głos, rysy twarzy, kształt dłoni, naczynia palca i dłoni, linie papilarne, tęczówka, siatkówka
Czas weryfikacji	linie papilarne, naczynia palca, tęczówka, kształt dłoni, naczynia dłoni, siatkówka, głos
Czas rejestracji	linie papilarne, naczynia palca, naczynia dłoni, tęczówka
Wiarygodność – bezpieczeństwo	siatkówka, tęczówka, naczynia palca, linie papilarne, kształt dłoni, głos, sposób pisania na klawiaturze
Wielkość wzorca	kształt dłoni, siatkówka, tęczówka, naczynia palca, linie papilarne, sposób pisania na klawiaturze, głos, naczynia dłoni

nie kształtu dłoni jest wygodne w użyciu i akceptowalne, ale jest podatne na oszustwa, bo kształt dłoni dla bliźniaków może być identyczny, a dla krewnych bardzo zbliżony. Urządzenia do badania kształtu dłoni są również duże i kosztowne. Rozpoznawanie tęczówki i rysów twarzy sprawia szereg problemów technicznych – wymaga pozycjonowania w polu widzenia kamery. Rozpoznawanie rysów twarzy bez pozycjonowania ciągle nie jest metodą wystarczająco dopracowaną. Przyszłościowe nowe podejścia do analizy głosu są w opracowaniu, jednakże pojawiają się już pierwsze zastosowania tej techniki do uwierzytelniania przez telefon. Ostatnio obserwuje się intensywny rozwój systemów opartych o odczyt układu naczyń krwionośnych dłoni lub palca – powstały liczne wdrożenia głównie w bankowości (np. banki japońskie, tureckie i polskie). Jest to rozwiązanie bazujące na wewnętrznej cesze człowieka i pobranie wzorca bez zgody i wiedzy właściciela jest bardzo trudne. Dużą zaletą tych rozwiązań, w porównaniu z tradycyjnie stosowanym odczytem linii papilarnych, jest duża odporność na próby oszustwa systemu oraz bardzo dobre współczynniki jakości weryfikacji, wadą – wyższa cena i wielkość. W USA usankcjonowane prawnie jest korzystanie z elektronicznego podpisu odręcznego. Jest to jednak cecha biometryczna łatwo dostępna, w związku z tym obszar jej zastosowań jest ograniczony. Elektroniczny podpis odręczny zbyt mocno również zależy od emocji i stanu zdrowia.

Podsumowując, rodzaj zastosowanej techniki biometrycznej zależeć będzie od tego, czy dostęp do danej aplikacji ma być masowy, czyli łatwy i tani, czy przede wszystkim bezpieczny. W pierwszym przypadku rozwiązania pójdą w kierunku techniki rozpoznawania głosu lub rysów twarzy jako technik ogólnie dostępnych i tanich, w drugim – rozpoznawania np. naczyń krwionośnych, tęczówki oka, czy nawet siatkówki.

Analiza technik biometrycznych pod kątem zastosowania do uwierzytelniania

Ze względu na założenie, że e-administracja i e-usługi mają być dostępne dla szerokiego grona obywateli, należy dążyć do powszechności dostępu i łatwości korzystania z uwierzytelniania biometrycznego, a więc iść w kierunku wykorzystania technik ogólnie dostępnych i tanich. Jeszcze bardziej radykalnym rozwiązaniem będzie dążenie do tworzenia platform biometrycznych umożliwiających wykorzystywanie różnych technik biometrycznych. Pozwoliłoby to na pozostawienie wyboru techniki biometrycznej w zależności od potrzeb i celów aplikacji zewnętrznej.

Jak już powiedziano powyżej, usługa uwierzytelniania realizowana przez dany system powinna być szeroko dostępna dla usługobiorców. Należałoby więc wykorzystać do uwierzytelniania cechę biometryczną łatwo dostępną i której pobieranie nie wymagałoby dużych nakładów finansowych.

Na bazie przeprowadzonego przeglądu i analizy różnorodnych technik biometrycznych można stwierdzić, że:

- takimi preferowanymi metodami są rozpoznawanie głosu i rysów twarzy, gdyż:
  - obie te cechy biometryczne są łatwo dostępne,
  - mikrofony i kamery są ogólnie stosowane i tanie,
  - w mikrofony i kamery jest wyposażona większość nowych komputerów,
  - nastąpił znaczny rozwój techniki rozpoznawania głosu,
- obiecującą techniką jest rozpoznawanie pisma odręcznego, ze względu na to, że jest to naturalna, utrwalona w praktyce metoda potwierdzania tożsamości, a tablety dotykowe są urządzeniami coraz częściej używanymi,
- duże zalety ma technika rozpoznawania układu naczyń krwionośnych, której głównymi zaletami są:
  - dobre parametry funkcjonalne,
  - nieprzechwytywalność cechy,
  - małe rozmiary urządzeń do pobierania układu naczyń krwionośnych palca.

Idąc dalej, najlepszym rozwiązaniem byłaby możliwość wykorzystania w danym systemie uwierzytelniania z różnych technik biometrycznych, takich jakimi dysponuje użytkownik, a dopuszczalnych ze względów bezpieczeństwa w danej aplikacji. W obecnym momencie jednak stworzenie takich platform uwierzytelniania jest bardzo trudne, gdyż producenci urządzeń biometrycznych opracowują własne standardy i biblioteki komunikacyjne. W ramach prac normalizacyjnych Komitet 37 ISO/IEC opracował w wieloczęściowej normie ISO/IEC 19794 znormalizowane formaty danych biometrycznych do przesyłania i przechowywania danych dla różnych technik biometrycznych. Opracowano również (ISO/IEC 19784-1:2006) wysokopoziomowy programistyczny model uwierzytelniania biometrycznego, czyli standard BioAPI. Aby więc uzyskać uniwersalność systemów uwierzytelniania biometrycznego należałoby dążyć do standaryzacji formatów danych i bibliotek urządzeń biometrycznych, co powinno rozszerzyć funkcjonalność systemów o korzystanie z szerokiej gamy technik biometrycznych.

Byłby to również duży krok w kierunku zwiększenia bezpieczeństwa w systemach tego wymagających przez oparcie uwierzytelniania o techniki multimodalne (równoczesne rozpoznawanie w oparciu o kilka cech biometrycznych).

Na koniec można stwierdzić, że przyszłości uwierzytelniania należy szukać w wykorzystaniu technik ogólnie dostępnych i akceptowalnych, dających możliwość szerokiej powszechności, łatwości użycia i bezpieczeństwa, a ich wybór warunkować potrzebami danego zastosowania.

Literatura

[1] Bechelli L., Bistarelli S., Martinelli F., Petrocchi M. and Vaccarelli A. – Integrating Biometric Techniques with an Electronic Signature for Remote Authentication.
[2] Boll R., Connell J., Pankanti S., Ratha N., Senior A.: TAO Biometria – Warszawa, WNT.
[3] Kapczyński A. – Wprowadzenie do biometrii Podstawy. Definicje, Konferencja Spring Biometric Summit 2011, Warszawa, 14–15.04.2011.
[4] Koziczak A. – „Społeczna akceptacja identyfikacji biometrycznej", prezentacja, Konferencja Biometria 2010, 1.12.2010, Warszawa.
[5] Opinia porównawcza systemu uwierzytelniania na podstawie elektronicznego podpisu odręcznego i systemu opartego o rozpoznawanie układu naczyń krwionośnych palca, IMM, Warszawa, 10.02.2012.
[6] PerSay's position in the NIST 2008 Speaker Recognition – Evaluation – Industry Report.
[7] Woszczyński T. – Finger Vein ID Systemy biometryczne Hitachi, 22.09.2008.
[8] http://biosys.pl/kontrola-czasu-pracy/BioT-5000Tplus.html
[9] www.compas.com.pl/zip/as990.pdf
[10] www.nist.gov/speech/tests/sre/2008/index.html
[11] www.persay.com
[12] www.reset2.pl/oferta/pro/oferta-specjalna/iclock680