Romuald Swarcewicz

Identyfikacja biometryczna – blaski i cienie

Natura wyposażyła człowieka w unikatowe cechy, które współczesna technika coraz częściej wykorzystuje jako identyfikatory tożsamości. Identyfikacja biometryczna to obecnie jedna z najszybciej rozwijających się technologii automatycznej identyfikacji w aplikacjach kontroli dostępu. Technika identyfikacji biometrycznej stanowi obszerną kategorię systemów zapewniających precyzyjne potwierdzenie tożsamości jednostki przez wykorzystanie cech fizjologicznych i sposobów zachowania. Charakterystyka fizjologiczna jest względnie stabilną cechą fizyczną taką jak: linie papilarne, obraz siatkówki oka, geometria dłoni lub rysy twarzy. Charakterystyka zachowania natomiast, silnie zależy od osobowości jednostki.

Większość systemów identyfikacji biometrycznej stosuje kartę lub PIN do wstępnej identyfikacji. W ten sposób system nie przegląda całej bazy do wykonania potencjalnego dopasowania. System zmierza bezpośrednio do wzorca odpowiadającego karcie lub PIN. Pomiar biometryczny wykorzystuje się do weryfikacji autentyczności właściciela karty lub PINu.

Powszechne aplikacje techniki biometrycznej weryfikacji są następujące:

- Kontrola fizycznego dostępu
- Weryfikacja automatycznej transakcji finansowej
- Zabezpieczenie przed oszustwami opieki społecznej
- Stosowanie w dziedzinie egzekucji prawa
- Sprawdzanie statusu emigracyjnego przy wjeździe do kraju
- Klucz do domu lub samochodu

Ryc. 2. Terminal do czytania wzoru siatkówki oka

- Inteligentny włącznik urządzeń.

O wykorzystaniu poszczególnych technik w aplikacjach decyduje nie tylko ich charakterystyka techniczna, ale i stopień akceptacji przez użytkowników. Poniższy przegląd technik identyfikacji biometrycznej przybliży ich zalety i wady.

Daktyloskopia

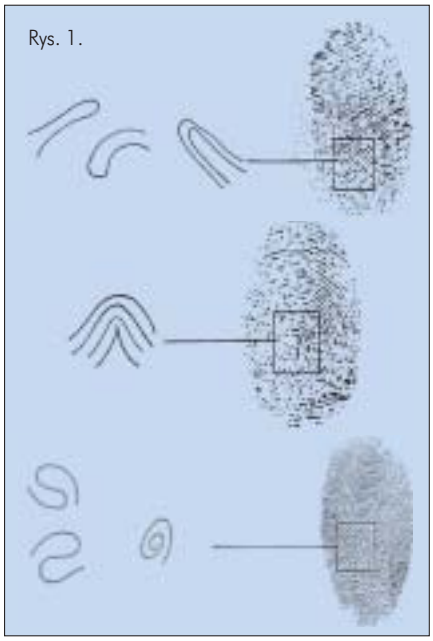
Najczęściej stosowaną techniką biometrycznej identyfikacji jest porównanie linii papilarnych palca. Od ponad stu lat w praktyce sądowej daktyloskopia była uznawana jako dowód rzeczowy zawierający bogactwo informacji unikalności wzoru linii papilarnych. Większość systemów techniki daktyloskopijnej polega na klasyfikacji grzbietów i bruzd wzoru odcisku linii papilarnych wg specyficznych drobnych szczegółach. Odcisk linii papilarnych palca jest charakteryzowany poprzez różne łuki, pętle, spirale, które z różnymi mniejszymi szczegółami tworzą tzw. rysy, rys. 1. Ilość różnych charakterystycznych rys na określonej powierzchni jest unikalnym identyfikatorem. Porównanie danych z tabelą dla identyfikowanych osób pozwala zidentyfikować indywiduum.

W zależności od projektu urządzenia i wymaganego poziomu zabezpieczenia, składowanie wzorca wymaga pojemności ok. 1000 bajtów.

Weryfikacja biometryczna jest wysoce niezawodna. Wskaźnik fałszywej akceptacji wynosi jak jeden do miliona. Pomiary odrzucone stanowią w przybliżeniu 3% prób. Przyczynami są niedokładne umieszczenie palca, rana na palcu, jakość zdjęcia obrazu i jakość algorytmu porównującego.

Obraz siatkówki oka

Ta technologia bazuje na analizie obrazu siatki naczyń krwionośnych siatkówki oka. Do oświetlenia siatkówki oka używa się źródła światła podczerwieni. Energia podczerwieni jest szybciej absorbowana przez naczynia krwionośne siatkówki niż przez otaczającą tkankę. Powiększony obraz siatki naczyń krwionośnych analizuje się pod względem charakterystycznych punktów. Terminal ze skanerem siatkówki przedstawiono na rys. 2.



Rys. 1.

Skanowanie siatkówki pozwala uzyskać prawie taka samą ilość danych co analiza daktyloskopijna. Wielka ilość danych odpowiada wysokiemu poziomowi dyskryminacji (wysokiemu stopniu identyfikacji), skanowanie siatkówki może być alternatywą dla identyfikacji daktyloskopowej.

Technologia skanowania siatkówki posiada jednak kilka mankamentów, których nie ma identyfikacja daktyloskopowa, a mianowicie:

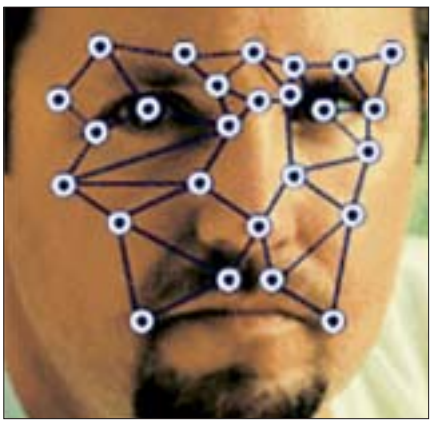
1. Skanowanie siatkówki jest bardziej wrażliwe na choroby (szczególnie kataraktę itp.) zmieniające charakterystykę oka.
2. Skanowanie siatkówki jest metodą inwazyjną dla identyfikowanego – światło lasera lub innego źródła spójnego światła musi być kierowane bezpośrednio przez rogówkę oka.
3. Otrzymanie prawidłowego skanowanego obrazu siatkówki w poważnym stopniu zależy od umiejętności operatora i zdolności osoby identyfikowanej do postępowania wg wskazówek.

Zapis wzorca siatkówki wymaga tylko 35 bajtów.

Geometria dłoni

System identyfikacji wg geometrii dło-

Rys. 3. Terminal identyfikacji geometrią dłoni



Rys. 4. Rozkład punktów pomiarowych umożliwiających identyfikację podpisu

ni opiera się na fakcie, iż dłoń każdej osoby jest ukształtowana odmiennie i że kształt dłoni po osiągnięciu pewnego wieku nie zmienia się w sposób znaczący. Do pomiaru kształtu dłoni używa się kilku metod, które ogólnie można zakwalifikować do dwu kategorii: detekcji mechanicznej lub zarysu obrazu. Każda z tych metod ocenia wg pewnych kluczowych pomiarów dłoni (długość palców i kciuka, szerokość itp.); dane te są używane do klasyfikacji osób.

Identyfikacja geometrii dłoni w porównaniu z innymi metodami identyfikacji biometrycznej (w szczególności daktyloskopią) nie dostarcza dużej ilości danych. Dlatego też przy dużej liczbie rekordów identyfikacja geometrii dłoni może nie odróżnić jednego indywiduum od drugiego o podobnej charakterystyce. Gdy wielkość bazy danych rośnie konieczne jest użycie większej ilości cech charakterystycznych aby umieścić sprawdzanego w wąskim zakresie osobników posiadających podobne charakterystyki biometryczne.

Rozpoznanie twarzy

Jest to najbardziej naturalny sposób biometrycznej identyfikacji. Ta metoda odróżniania jednej osoby od drugiej jest wrodzoną zdolnością każdego człowieka.

Policyjni artyści próbowali kategoryzować różne części twarzy (linię podbródka, linię owłosienia, cechy nosa i ust itp.) w zbiory wzorców, które mogły być zestawione w kompozytową twarz (portret pamięciowy), która była podobna do twarzy poszukiwanej osoby.

Technologia rozpoznawania twarzy obecnie jest rozwijana w dwu kierunkach: pomiaru twarzy i tzw. metody eigenface.

Technologia pomiaru twarzy polega na pomiarze specyficznych cech twarzy (np. odległość pomiędzy wewnętrznymi kącikami oczu, odległość pomiędzy zewnętrznymi kącikami oczu i zewnętrznymi kącikami ust itp.) i relacji pomiędzy tymi pomiarami. Punkty pomiarowe pokazano na rys. 4.

W ostatnich dwóch latach przeprowadzono testy z kategoryzacją twarzy stosownie do stopnia dopasowania do zbioru eigenfaces (właściwych twarzy). Jest to technologia opatentowana w MIT używająca dwu wymiarowych globalnych obrazów w skali szarości reprezentujących wyróżniające się cechy obrazu twarzy. Zakłada się, że każdej twarzy można przypisać pewien „stopień dopasowania" do każdej ze 150 eigenfaces a nawet, że tylko 40 wzorców eigenfaces z najwyższym stopniem skali dopasowania wystarczy do rekonstrukcji jakiejś twarzy z dokładnością ponad 99%. Różnica pomiędzy metodą kategoryzacji eigenface i metodą artysty policyjnego budującego twarz z wzorców fragmentów jest taka, że metoda eigenface bazuje na rzeczywistych fotografiach osobników i że ta informacja pochodzi z analizy komputerowej cyfrowego obrazu fotografii. Eigenfaces są wysoce powtarzalne i nie poddane ludzkiej subiektywności. Jest to technologia w początkowym stadium rozwoju, bardzo obiecująca i brak jeszcze danych o jej niezawodności. Wzorce do analizy podstawowych elementów twarzy pokazano na rys. 5.

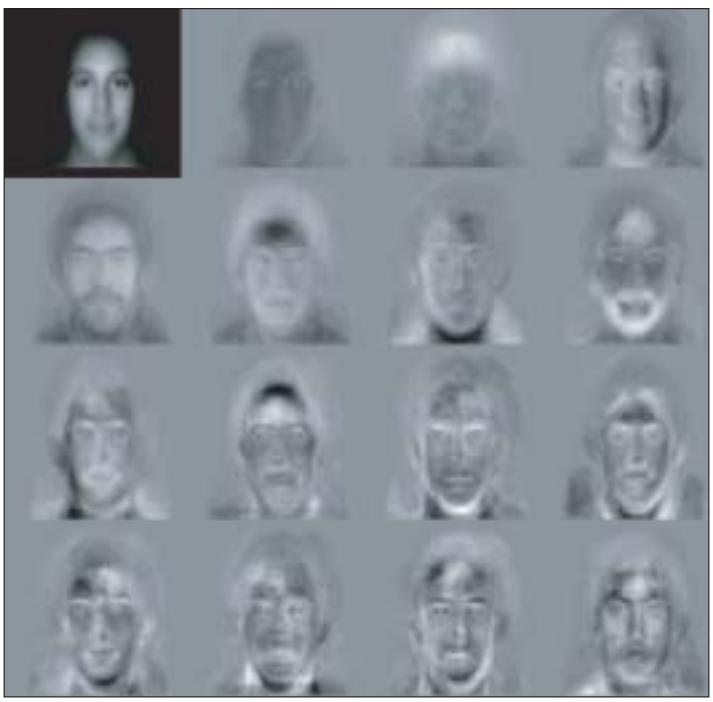
Rys. 6. Skaner tęczówki oka

Istnieje odmiana rozpoznawania twarzy wykorzystująca termiczny obraz twarzy (Thermal Recognition System). Rozpoznanie dokonuje się przez wykonanie termogramu twarzy i porównanie go z termogramem wzorcowym.

Cyfrowe termogramy wymagają od 2 do 4 kb pamięci. Kamera na podczerwień jest nieczuła na oświetlenie i tworzy dokładne obrazy nawet w ciemności z odległości do 4 stóp. Ocenia się, że ta technika jest dokładniejsza od wzoru linii papilarnych, druku głosu lub skanowania tęczówki.

Skanowanie tęczówki oka

Technologia skanowania tęczówki oka bazuje na charakterystyce tęczówki. Sprawdzany osobnik musi stać w odległości 12 – 14 cali od kamery pobierającej obraz tęczówki do analizy. Tęczów-



Rys. 5. Wzorce do analizy podstawowych elementów twarzy

ka dostarcza dużej ilości danych – 256 bajtów, co jest równoważne z wysokim stopniem dyskryminacji – identyfikacji. Technologia skanowania tęczówki jest bardziej akceptowalna przez użytkowników niż skanowanie siatkówki oka. Skaner tęczówki przedstawiono na rys. 6.

Weryfikacja głosu

Weryfikacja głosu może łączyć w jednym procesie – zabezpieczenie hasłem i weryfikację biometryczną. Weryfikację realizuje się przez porównanie wymówionego hasła z przechowywanym cyfrowym wzorcem. Dla zbudowania wzorca odnoszenia, osobnik musi powtarzać go kilkakrotnie, aby system utworzył właściwy wzorzec. System identyfikacji głosu uwzględnia kilka zmiennych lub parametrów rozpoznania czyjegoś wzorca głosu takich jak głębia, dynamika i kształt fali. Dla systemu identyfikacji głosu najważniejsze jest, jak uwzględnić zmiany w czyimś glosie przy każdej identyfikacji. Natężenie i głębia mowy osobnika nie są takie same w każdej chwili czasu. Pomocą do wyeliminowania tych zmian w czasie identyfikacji stanowi zastosowanie procesu zawierającego modelowania Markowa. Podstawa tej metody to używanie przez system (oprogramowanie) języka modelowania do określenia, jak wiele różnych słów prawdopodobnie wystąpi po danym słowie, Pozwala to na redukcję wielu słów podobnie brzmiących, a właściwe słowo zostaje rozpoznane.

Głos jest bardzo wygodnym sposobem weryfikacji przy transakcjach telefonicznych. Zakupy telefoniczne, przy których używa się numeru karty kredytowej, mogą również używać systemu głosowego dla potwierdzenia, że osoba dokonująca zakupu jest legalnym właścicielem karty kredytowej.

Badania przeprowadzone na 2000 przypadkach wykazało 0,31% błędnych identyfikacji przy stosowaniu weryfikacji głosu. Technologia ta również cieszy się wysokim stopniem akceptacji użytkowników.

Weryfikacja podpisu

Podpis był przez wiele lat przyjętą ogólną formą stwierdzenia wiarygodności. Istotną właściwością automatycznych systemów identyfikacji podpisu jest zdolność do rozróżniania pomiędzy postacią podpisu nawykowego (regularnego), a postaciami trochę zmienionymi, które pojawiają się za każdym razem, gdy osoba pisze swoje nazwisko. Istnieje ponad 100 patentów na tego rodzaju systemy. Ogólnie sprowadzają się one do tego, że na podstawie treningowego zbioru podpisu tworzony jest prototyp podpisu, jak zilustrowano to na rys. 7 i przy weryfikacji podpisu obraz podpisu jest porównywany z prototypem podpisu.

Sposób posługiwania się klawiaturą

Ta metoda weryfikacji biometrycznej analizuje sposób posługiwania się klawiaturą przez osobę monitorując wejście klawiatury 1000 razy na minutę. Badania przeprowadzone przez Narodową Fundację Nauki i Narodowy Instytut Standardów i Technologii ustaliły, że wzorzec posługiwania się klawiaturą jest unikalny. W różnych metodach pomiaru schematu posługiwania się klawiaturą przez użytkownika uniwersalna jest koncepcja obsługi klawiszy dwu przyległych znaków. Najpowszechniejszą miarą jest tu pomiar czasu pomiędzy naciśnięciami pierwszego i drugiego klawisza.

Rys. 7. Prototyp podpisu utworzony na podstawie treningowego zbioru podpisów

Weryfikacja posługiwania się klawiaturą jest technologią biometryczną nie wymagającą używania specjalnego sprzętu. Jej zastosowanie to zabezpieczenie komputerów przed nieupoważnionym dostępem. Jest to technologia będąca jeszcze w fazie rozwoju.

Chip DNA

Rewelacyjną technologię biometryczną oferuje chińska firma Biowell. Jest to technologia zabezpieczająca przed fałszowaniem identyfikatorów.

Chip DNA używa sztucznie skonstruowane DNA, które dla każdej grupy użytkowników identyfikatora jest takie same. Personalizacja jest wyróżniana w systemie przez identyfikację kodu przechowywanego w pamięci chipa. Sygnał chipa DNA jest generowany poprzez interakcję ze specjalnie utworzonym sensorem odczytującym. Autentyczny chip DNA po pobudzeniu przez czytnik generuje sygnał analogowy odbierany przez czytnik. Dla identyfikacji użytkownika sygnał jest porównywany w module czytnika z sygnałem z bazy danych uprawnionych użytkowników.

Polymorfizm DNA jest znacznie bardziej skomplikowany niż sygnały kodów elektronicznych i bardziej odpowiedni do systemów zabezpieczających. System chipa DNA nie może być skopiowany lub rozszyfrowany i współpracuje tylko ze specjalnie skonstruowanymi czytnikami. Wiarygodność chipa potwierdza czytnik firmy Biowell rozpoznający specjalny sygnał na interfejsie chipa i głowicy odczytującej.

Firma Biowell nie podaje, jak pracuje sensor DNA, ale jeżeli taki sensor istnieje, to byłby to idealny mechanizm do identyfikacji biometrycznej zwierząt zapobiegającej jakimkolwiek fałszerstwom danych o zwierzęciu.

Problemy stosowania identyfikacji biometrycznej

Użycie biometrycznych identyfikatorów w handlu elektronicznym może oznaczać, że informacja jest globalnie osiągalna, ale dostępna tylko przy pomocy klucza biometrycznego. Taki klucz biometryczny jest rzeczywiście przenośny i może dostarczyć niezbitych dowodów identyczności. Pozostaje problem pewności bezpieczeństwa i prywatności transakcji.

Teoretycznie technologia biometryczna może dostarczyć zarówno perfekcyjne bezpieczeństwo jak i prywatność.

Niemniej jednak zarówno bezpieczeństwo i prywatność może być kompromisem w systemie biometrycznym, jeśli zapis biometryczny lub używanie danych zostanie sprzedane, ukradzione lub użyte do śledzenia ruchów osoby i historii transakcji bez ich wiedzy i zgody. Sam system biometryczny wyczuwa i dopasowuje, ale nie dostarcza zabezpieczenia. System biometryczny musi być zaimplementowany wewnątrz właściwego otoczenia zabezpieczającego, aby był wiarogodny i użyteczny.

Ponieważ większość ludzi uznaje, że dane biometryczne są najbardziej osobistą formą danych, to istnieje częściowa lecz silna opozycja przed rozpowszechnianiem stosowania systemów biometrycznych. Często przyrównuje się je jako coś mającego wspólnego z technologią „wielkiego brata". W samej branży biometrycznej te obawy są oceniane jako irracjonalne, bo w rzeczywistości zwykła kradzież grupy obrazów linii papilarnych jest bezużyteczna bez znajomości, jak i z kim są połączone. Idea „wielkiego brata" jest rodzajem anonimowego zbierania nadmiernych informacji. Dostępność solidnej ilości danych osobowych może być niebezpieczna, gdy pozwala komuś bez wiedzy osobnika na podjęcie decyzji, które będą miały bezpośredni wpływ na niego. Z drugiej strony system biometryczny może być użyty do zwiększenia prywatności. Może wydawać się to niewiarygodne, ale transakcje biometryczne mogą być całkowicie anonimowe. Dokonuje się tego przez czystą lokalną weryfikację wewnątrz bezpiecznego kanału komunikacyjnego bez użycia jakiegokolwiek logowania lub centralnej bazy danych. Czyniąc pewne dane dostępne tylko osobie przedstawiającej biometryczny identyfikator, możemy rzeczywiście poprawić bezpieczeństwo i prywatność naszych osobistych i publicznych transakcji. Większość naruszeń prawa bezpieczeństwa może być wyeliminowana.

Większość istniejących systemów biometrycznych było zaprojektowanych w kontekście istniejącego prawa. Oznacza to, że istnieje niewielkie zabezpieczenie przed przestępstwem, gdy dochodzi do zbierania, przechowywania i wyszukiwania osobowych i biometrycznych danych. Gdy biometryczne technologie są włączone do aplikacji komercyjnych, powinniśmy być bardziej selektywni w tym, jak te dane są zbierane i przechowywane, gdyż dane mogą być wykorzystania do popełnienia nielegalnego, nieetycznego lub kryminalnego celu.

Legislacja

Innowatorzy technologii komercyjnych zwykle unikają legislacji jak plagi, a firmy biometryczne patrzą na inicjatywy takie jak prawo Europejskiej Prywatności ze strachem i odrazą. Wyważona i rozważna legislacja jest jednak pilnie potrzebna dla zagwarantowania, że dane biometryczne – obecnie zbierane w przyśpieszonym tempie – nie będą nadużywane. Wielu zauważyło, że podobne zagadnienia istnieją w szyfrowaniu danych. Podobnie jak kryptografia może być użyta bezprawnie dla ukrycia nielegalnych transakcji, dane biometryczne mogą uniemożliwić władzy dostęp do biometrycznie zaszyfrowanych danych. Jednocześnie, pewne typy transakcji powinny być zakryte lub zabezpieczone przed wglądem publicznym.

Możemy podsumować zagadnienia prywatności biometrycznej następująco:

- Dobrowolne użycie systemów biometrycznych musi być promowane. Tam gdzie istnieją sprzeciwy z powodów religijnych i osobistych, powinny być dostępne alternatywne środki identyfikacji lub weryfikacji. Dotychczasowe doświadczenia wskazują na bardzo wysoką akceptację systemu po jego implementacji.
- Systemy, które dzielą się informacjami biometrycznymi i relacyjnymi, są czasami konieczne lub wysoko pożądane, powinny być jedyną i niewymuszoną opcją obywateli. Zagadnienia użycia danych biometrycznych dzieci powinny być rozwiązane po rozpoznaniu, że nie będą miały bezpośredniego wpływu jak ich dane będą użyte i że te dane mogą podążać za nimi, gdy będą rosły, dojrzewały aż do wieku dorosłego. Identyfikatory biometryczne mogą być użyte do zapewnienia, że tylko właściwe autoryzowane osoby mogą otrzymać dane biometryczne.
- Powinniśmy mieć świadomość, że systemy biometryczne nie mogą pracować niezależnie od innych zabezpieczeń i technologii udogodnień i że w większości przypadków są tylko częścią rozwiązania.

Technologia biometryczna ma taki potencjał, że byłoby tragedią utopić niepowodzenie ochrony wyników prywatności w generalnych niepowodzeniach i wywołać poślizg jej rozwoju na dużą skalę.