Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 20

XIV Seminarium
ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE' 2004
Oddział Gdański PTETiS

TECHNIKI IDENTYFIKACJI OSÓB Z WYKORZYSTANIEM INDYWIDUALNYCH CECH BIOMETRYCZNYCH

Dominika GUTOWSKA[1], Longin STOLC[2]

Politechnika Gdańska, Katedra Automatyki
1. e-mail: gutowska@ely.pg.gda.pl
2. e-mail: lstolc@ely.pg.gda.pl

W pracy przedstawione są różne metody identyfikacji osób w oparciu o ich cechy biometryczne charakterystyczne dla każdego identyfikowanego obiektu. Mogą to być właściwości fizjologiczne, takie jak linie papilarne, kształt dłoni, cechy tęczówki, czy też właściwości behawioralne, jak sposób pisania czy wypowiadania się. Podaje się ich zalety oraz wady jak również błędy mogące wystąpić w trakcie identyfikacji. Znajomość wad i zalet podanych w pracy metod stanowi podstawę dla opracowywanej przez autorów metody oraz algorytmów identyfikacji opartych o rozmyte reguły decyzyjne budowane na bazie odległości pomiędzy punktami charakterystycznymi twarzy.

1. WSTĘP

Autoryzacja użytkownika może być przeprowadzona za pomocą różnych metod uwierzytelniania. Wśród tych metod wyróżniamy:

- metody oparte na wiedzy użytkownika, np. PIN-y i hasła (najbardziej zawodne)
- metody oparte na elektronicznych identyfikatorach, np. karty magnetyczne
- metody biometryczne, które wykorzystują niepowtarzalność wybranych charakterystyk fizycznych użytkownika (człowieka) oraz unikalność jego zachowań [1].

Metody biometryczne to zautomatyzowane metody identyfikacji osoby w oparciu o jego specyficzne właściwości. Mogą to być właściwości fizjologiczne, takie jak linie papilarne, kształt dłoni, cechy tęczówki, jak również mogą to być właściwości behawioralne, jak sposób pisania czy wypowiadania się.

System identyfikacyjny, za pomocą różnych sposobów, „czyta" te właściwości (cechy), a następnie przetwarza je na reprezentacje cyfrową. Kolejnym krokiem jest porównanie uzyskanej reprezentacji cyfrowej użytkownika z przechowywanym biometrycznym „profilem". Stosowanie do identyfikacji nieznanej osoby cechy charakterystycznych twarzy, odcisków palców, cech tęczówki oraz, chociaż rzadziej, DNA pomaga odpowiedzieć na pytanie „Kto jest tą osobą?". Identyfikacja polega na porównaniu biometrycznych szablonów (wzorców) osoby z przechowywanym zbiorem wielu „profili" oraz na znalezieniu najlepszego dopasowania [2].

Istnieją dwie główne funkcje oferowane przez systemy identyfikacyjne, są to:

- identyfikacja (rozpoznanie) – to proces porównania jednego wzoru biometrycznego do wielu przechowywanych w bazie danych (1:M, - one-to-many),
- weryfikacja – to proces, w trakcie którego system dokonuje porównania danego wzoru biometrycznego do wzoru przechowywanego w bazie danych dla konkretnego użytkownika (1:1, - one-to-one).

Termin „weryfikacja" często jest używany zamiennie z „autoryzacją", gdyż w obydwu przypadkach chodzi raczej o ustalenie uprawnień użytkownika do danych zasobów niż o jego identyfikację.

2. OBIEKTY IDENTYFIKACJI

2.1 Identyfikacja odcisków palców

Identyfikacja osoby na podstawie odcisków palców ma jak dotąd najdłuższą i najbardziej interesującą historię ze wszystkich biometryków. Archeolodzy odkryli, że odciski palców były używane już przez starożytnych Babilończyków i Chińczyków w celu identyfikacji osób. W XIV wieku w Persji odkryto, że nie ma dwóch identycznych odcisków palców. Pierwsze naukowe badania na temat odcisków palców pochodzą z późnych lat XVII wieku (Marcello Malpighi – 1686r.), jednakże podstawy współczesnych metod identyfikacji opartych o odciski palców zostały ustalone dopiero pod koniec XIX wieku. Badania brytyjskiego antropologa, Sir F. Galtona, prowadzone pod koniec lat 80-tych XIX, nad odciskami palców jako sposobem identyfikacji, zaowocowały publikacją w 1892r. książki pt. „Fingerprints", w której zawarł pierwszy system klasyfikacji odcisków palców. Zarówno badania Sir F. Galtona jak i późniejsze badania Sir E. Henry'ego [4] pozwoliły na opracowanie podstaw prawnych umożliwiających wykorzystanie odcisków palców w identyfikacji.

Pierwszy Automatyczny System Identyfikacji Odcisków Palców (AFIS - ang. Automated Fingerprint Identification Systems) został wdrożony w latach 40-tych XX wieku w FBI (Federal Bureau of Investigation) [4] we współpracy z National Bureau of Standards, Cornell Aeronautical Laboratory i Rockwell International Corp.

Wewnętrzna powierzchnia ludzkiej dłoni (i stopy) pokryta liniami papilarnymi, które często układają się w pętle, spirale i trójkąty. Ilość tych struktur w pojedynczym odcisku palca zależna jest od natury i przez nią regulowana. Zwykle odciski palców dzielą się na 5 podstawowych typów: łuk, rozciągnięty łuk, pętla w prawo, pętla w lewo oraz spirala [6]).

Najstarsze i najlepiej znane techniki pobierania odcisków palców, tak zwane techniki "atramentowe", wymagają, aby palec został pokryty tuszem, a następnie odbity na kartce. Kartka jest skanowana, a obraz odcisku palca zamieniany w postać cyfrową. Standardowa rozdzielczość wynosi 500 dpi. Ta technika może spowodować, że w niektórych miejscach ze względu na zbyt dużą lub małą zawartość atramentu mogą wystąpić zniekształcenia.

Metoda FTIR (ang. Frustrated Total Internal Reflection [5]) jest obecnie najczęściej używaną i najbardziej rozwiniętą metodą skanowania "żywych" odcisków palców.

Oprócz obu wyżej wymienionych metod pobierania odcisku palca stosuje się metody termalne [7] oraz ultradźwiękowe [8].

2.2 Identyfikacja głosu

Jednym z najprostszych systemów identyfikacyjnych jest system rozpoznawania głosu. W tych systemach, użytkownik wypowiada do mikrofonu, podłączonego do systemu, określone słowo. Po tym, specjalny program dokonuje analizy widmowej wypowiedzianego słowa oraz porównuje jej wyniki z przechowywana w bazie charakterystyką. Jeżeli wynik porównania jest pozytywny, użytkownik otrzymuje autoryzację.

Systemy rozpoznawania głosu można podzielić w zależności od charakteru wypowiadanego do mikrofonu tekstu na [9]:

- *Tekst ustalony*: użytkownik wymawia do mikrofonu ustalone z góry słowo lub frazę, które było nagrane podczas rejestrowania użytkownika do systemu. Słowo może być tajnie, działa więc jak hasło.
- *Tekst zależny*: użytkownik musi wypowiedzieć słowo bądź frazę podane przez system w momencie dokonywania autoryzacji. Aby określić użytkownika komputer zestraja jego wypowiedź ze znanym sobie tekstem. W tym przypadku rejestracja jest dłuższa, jednakże podpowiedziany przez system identyfikacyjny tekst może być zmieniany dowolnie. Systemu ograniczone, np. systemy stosujące łańcuchy cyfr, są podatne na ataki „splicing – based".
- *Tekst niezależny*: System identyfikacyjny przetwarza dowolna wypowiedź użytkownika. Wypowiedź może być nakierowana na pewien temat, zadanie. W związku z tym, trudno jest zdobyć wcześniej pożądany tekst wypowiedzi użytkownika. Systemy te są w stanie zidentyfikować użytkownika nawet wówczas, gdy zmieni on język swojej wypowiedzi.

Weryfikacja użytkownika za pomocą głosu jest szczególnie narażona na „ataki zwrotne" ze względu na wszechobecne urządzenia nagrywające i odtwarzające.

2.3 Identyfikacja tęczówki oka

Tęczówka [10, 11] jest stosunkowo nowym biometrykiem i jest bardzo precyzyjna oraz stabilna ze względu na brak elastycznego zniekształcenia (oprócz rozszerzenia źrenicy) w obrazie tęczówki, między jednym próbkowaniem, a następnymi. Tęczówka to kolorowy pierścień tkanki otaczającej źrenicę chroniony przez rogówkę i ciecz wodnistą. Kształtuje się w ciągu 2 pierwszych lat życia i nie zmienia się do śmierci. Jednakże od momentu śmierci ulega zniszczeniu zaledwie w przeciągu 5 sekund.

Wzór tęczówki każdego oka jest absolutnie unikatowy, nawet w przypadku bliźniaków jednojajowych mających podobnie (lub tak samo) brzmiący głos, kształt dłoni, odcień skóry czy twarz. Co więcej, nie tylko wzór tęczówki jednej osoby różni się od wzoru drugiej osoby, ale również wzór tęczówki prawego oka rożni się od wzoru lewego u jednej i tej samej osoby. Ta unikalność u każdej osoby ma swoje źródło w różnicach cech takich jak: bruzdy, dołki, prążkowanie, włókna kolagenowe, zacienione pola (tzw. krypty), plamki, pierścienie. Rozpoznanie wzoru tęczówki jest szybkie, nieinwazyjne, a przede wszystkim nie jest groźne dla użytkownika. Identyfikacja użytkownika jest możliwa pod warunkiem, że ma on nieuszkodzoną rogówkę.

System biometryczny oparty o rozpoznanie tęczówki składa się z czułej, w zakresie bliskiej podczerwieni, kamery, układu optycznego, źródła podczerwieni, karty akwizycji obrazu oraz stacji roboczej [1]. Możemy wyróżnić kilka etapów weryfikacji pobranego materiału:

- Wykonanie zdjęcia.
- Lokalizacja tęczówki.

- Analiza, najczęściej falkowa, obrazu tęczówki w celu przekształcenia pozyskanego obrazu do przestrzeni cech.
- Porównanie wektorów cech (np. XOR w systemie Daugmana).

Identyfikacja użytkownika na podstawie wzoru tęczówki jest niezmiernie użyteczna. Wzorce ludzkiej tęczówki są niezmienne w przeciągu całego życia, dzięki odpada proces starzenia się wzoru biometrycznego, poza tym tęczówka posiada 6 razy więcej rozpoznawalnych cech charakterystycznych od odcisku palca. Funkcją tęczówki jest regulacja dopływu światła do oka w zależności od jego natężenia, dzięki temu ludzkie oko oferuje dodatkową właściwość zmniejszająca prawdopodobieństwo ataku, a co za tym idzie oszukanie systemu identyfikacyjnego. Chodzi o zmianę rozmiaru źrenicy, a więc i samej tęczówki w zależności od natężenia światła. Zwężenie źrenicy w zależności od natężenia światła jest odruchowe, niezależne od świadomości.

2.4 Weryfikacja geometrii dłoni

Geometria dłoni, jak wskazuje nazwa, odnosi się do struktury geometrycznej ludzkiej dłoni. Typowe cechy obejmują: długość i szerokość palców, szerokość dłoni, grubość dłoni itp. [14]. Istniejące systemy identyfikacyjne działające w oparciu o rozpoznanie geometrii dłoni nie korzystają z jakichkolwiek niegeometrycznych cech dłoni, jakim jest na przykład kolor skóry. Chociaż cechy dłoni nie zmieniają się znacznie w całej populacji, to mogą być użyte do skutecznej weryfikacji osoby. Weryfikacja geometrii dłoni jest bardzo wygodną i wiarygodną metodą, dzięki temu znajduje zastosowanie w systemach kontroli dostępu i rejestracji czasu pracy. Systemy weryfikacji oparte na geometrii dłoni nie są nowe i są dostępne od wczesnych lat 70-tych XX wieku. Pomimo to nie ma zbyt wiele ogólnodostępnej (otwartej) literatury na ten temat poza patentami (np. [15]) czy opisami zorientowanymi na zastosowanie [16].

Zasada działania systemu dokonującego weryfikacji w oparciu o geometrię dłoni (w porównaniu z tęczówką czy siatkówką) jest prosta. Po umieszczeniu dłoni w komorze urządzenia mierzony jest rozmiar i kształt dłoni - długość, szerokość i grubość czterech palców oraz obszar pomiędzy kostkami palców (kciuk nie jest wykorzystywany). Odbywa się to poprzez oświetlenie dłoni promieniami podczerwonymi i odczytanie obrazu macierzą CCD - tworzony jest trójwymiarowy obraz kształtu dłoni (kilka różnych położeń). Z wyników pomiarów tworzony jest wzorzec, który zapisywany jest w pamięci razem z kodem ID osoby. Proces weryfikacji użytkownika polega na wprowadzeniu kodu ID oraz porównaniu aktualnie analizowanego wzorca dłoni ze wzorcem umieszczonym w bazie danych [17].

Geometria dłoni jest tak elastyczna, że można połączyć w całość z innymi biometrykami, w szczególności z odciskami palców. Na przykład system weryfikacyjny może użyć odcisków palców dla bardziej precyzyjnej weryfikacji, a geometrii dłoni dla mniej rygorystycznej. Łatwo jest stworzyć system rejestrujący, który symultanicznie (jednocześnie) zapisuje zarówno odciski palców jak i dokonuje pomiaru geometrii dłoni. Wadą tego typu weryfikacji jest stosunkowo wysokie FA (ang. False Akcept) i FR (ang. False Reject).

2.5 Identyfikacja twarzy

Identyfikacja na podstawie twarzy jest sposobem najbardziej spektakularnym, a jednocześnie najbardziej naturalnym. Pomimo, że prace nad tym sposobem identyfikacji trwają już od 50 lat to jest ona nadal w fazie eksperymentów. Proces identyfikacji twarzy przebiega zwykle w trzech etapach:

- Lokalizacja twarzy,

- Wyodrębnienie cech charakterystycznych,
- Identyfikacja.

Najstarsza spośród technik identyfikacji na podstawie twarzy jest technika „twarzy własnych" (ang. eigenfaces) rozwinięta przez M. Turka i A. Pentlanda [18] w 1991 roku. Podstawowym założeniem tej techniki jest duża liczba obrazów twarzy zawartych w bazie danych systemu identyfikacyjnego. Pierwszym krokiem jest podział przechowywanych obrazów twarzy na podgrupy, które charakteryzują się największym stopniem podobieństwa, krok drugi to stworzenie, na podstawie wyodrębnionej grupy, „twarzy własnej". Wobec tego „twarz własna" to graficzna reprezentacja cech najbardziej i najmniej podobnych w danej grupie. „Twarze własne" traktowane są jako twory złożone z wielu różnych składników, z których przez odpowiednią ich kombinację, system jest w stanie utworzyć twarz dowolnej osoby, by następnie porównać ją z twarzą przechowywana w swojej bazie danych. Im większa liczba „twarzy własnych" tym lepsza skuteczność systemu, chociaż poprawną identyfikacje można uzyskać posiadając „jedynie" ok. 100 „twarzy własnych" (na podstawie:[19]). Wadą tej techniki jest to, że prawidłowa identyfikacja zależy od podobnego (w stosunku do obrazu znajdującego się w bazie danych) oświetlenia, pozy czy miny identyfikowanej osoby. Wystarczy uśmiech, by system identyfikacyjny odrzucił osobę.

3. SYSTEMY ROZPOZNAWANIA TWARZY

Poprzez system rozpoznania twarzy należy rozumieć sprzęt i oprogramowanie wraz z algorytmami i danymi, przeznaczone do identyfikacji osób na podstawie obrazu twarzy. Systemy rozpoznawania twarzy dzielimy ze względu na stopień automatyzacji na:

Systemy manualne – wymagają obecności operatora, który dostarcza dane oraz interweniuje w sytuacjach awaryjnych.

Systemy automatyczne – potrafią w skończonym czasie odszukać jedną lub więcej twarzy znajdujących się w obrazie wejściowym, bądź ich sekwencji, oraz zidentyfikować osoby w nim występujące.

Systemy czasu rzeczywistego – mają za zadanie w sposób ciągły sprawdzać występowanie i tożsamość twarzy w obrazie wejściowym.

4. BŁĘDY POPEŁNIANE PODCZAS IDENTYFIKACJI

Głównym wyznacznikiem systemów identyfikacyjnych jest skuteczność rozpoznania. Jednakże, nie bez znaczenia są rodzaje błędów popełnianych przez taki system. Dwa podstawowe błędy popełniane przez systemy rozpoznania to:

- FAR (ang. Falce Acceptance Rate) - błąd fałszywej akceptacji występuje, gdy osoba spoza bazy danych (a właściwie jej dane biometryczne) systemu zostaje rozpoznana jako jedna z bazy,
- FRR (ang. False Rejection Rate) - błąd fałszywego odrzucenia występuje, gdy osoba zarejestrowana w bazie danych (jej dane biometryczne) systemu nie zostaje rozpoznana i jest odrzucona przez system.

Zwiększenie bezpieczeństwa systemu identyfikacyjnego wiąże się ze zwiększeniem FRR. W przypadku, odrzucenia przez system danych biometrycznych osoby zarejestrowanej może okazać się koniecznym wzmocnienie oświetlenia, założenie

klimatyzacji czy też przeszkolenie użytkowników. Natomiast, jeżeli zabezpieczenia systemu ustawione są na zbyt niskim poziomie do czynienia mamy z FAR.

Innym rodzajem błędu jest „błędna klasyfikacja". Błąd ten występuje, gdy osoba zarejestrowana w bazie danych systemu identyfikacyjnego zostaje mylnie rozpoznana jako inna, także występująca w bazie danych.

5. PODSUMOWANIE

Porównania metod identyfikacji przedstawionych w pracy wyłaniają się podstawowe ograniczenia w ich zastosowaniach. Przyjmując za cel podstawowy wyznaczanie ciągu osób w kolejności ich podobieństwa do wzorca („odległość" pomiędzy obiektem a kolejnymi wzorcami) wymaga identycznych warunków powstawania porównywanych modeli obiektów. W praktyce spełnienie tego rodzaju warunków jest wręcz nie do spełnienia.

Autorzy pracują obecnie nad systemem wspomagającym identyfikację na podstawie badania fotografii i porównywania podstawowych cech twarzy. Istniejący obecnie i stosowany przez policje wielu krajów system identyfikacji z porównywania fotografii obarczony jest wieloma ograniczeniami.

Do ograniczeń podstawowych należy zaliczyć:

- Twarz fotografowana en face,
- Fotografie badana i porównywane wykonane muszą być w zbliżonych warunkach (porównywalne aparaty, określona odległości oraz zbliżone oświetlenie obiektów),

W omawianej metodzie na fotografiach wyznaczana jest siarka definiowana przez trzy punkty (środki oczu oraz ust), które są stałe u osób dorosłych. Następnie określa się „odległości" pomiędzy wartościami miar przypisywanych poszczególnym obszarom siatki. Podana metoda nie pozwala porównywać i szeregować podobieństw w przypadkach:

- Duże różnice w kontraście zdjęć: kolor-czarno białe, zdjęcie-ksero,
- Fotografie wykonane pod różnymi katami,
- Znaczne różnice w odległości wykonanych zdjęć.

Dla usunięcia powyższych ograniczeń opracowywana jest obecnie metoda wzbogacająca omawiany wyżej system identyfikacji poprzez stosowanie porównania rozmytych ilorazów wybranych odległości charakterystycznych do odległości „stałych". Ponadto wzbogaca system o przetwarzanie obrazu do postaci wymaganej en face.

Przedstawienie i omówienie proponowanej metody i stosowanych w niej algorytmów stanowi osobny temat i będzie przedstawiony w osobnej pracy.

BIBLIOGRAFIA

1. www.4safe.pl
2. www.bio-tech.inc.com/Bio_Tech_Assessment.html
3. Bery J. "The history and development of fingerprinting". In Lee H.C. oraz Gaensslen R.E., redaktorzy, *Advances In Fingerprint Technology*, p. 1-38, CRC Press, Boca Raton, Floryda, 1994
4. FBI, U.S. Department of Justice, Washington, D.C. 20402. *The Science of Fingerprints, Classification and Use*, 1984.
5. Follette D.T, Hultmark E.B. oraz Jordan J.G., *Direct optical imput systemfor fingerprint verification*. IBM Technical Disclousure Bulletin:04-74p3572, Kwiecień 1974
6. www.biometrica.pl
7. Mainguet J-F., Pegulu M. oraz Harris J.B. "Fingerchip^{TM} : thermal imaging and finger sweeping in a silicon fingerprint sensor" *Proc of AutoID 99*, p. 91-94, październik 99.
8. Bicz W., Gurnienny Z. oraz Pluta M., „Ultrasound sensor for fingerprints recognition", *Proc. Of SPIE, Vol 2643, Optoelectronic and electronic sensors*, p. 104-111, czerwiec 1995.
9. Bolle R. M,. Connell J. H, Pankanti S, Ratha N. K, Senior A.: IBM Research Report, Computer Science, RC22481, June 2002
10. Wildes R.P. Iris recognition: An emerging biometric technology. Proceedings of the IEEE, 85(9): 1348-1363, Wrzesień 1997.
11. Wildes R.P., Asmuth G.L., Hsu S.C., Kolczynski R.J, Matey J.R. oraz McBride S.E. A machine-vision system for iris recognition. Machine Applications, 9:1-8, 1996.
12. www.wsp.krakow.pl/whk/posma.html
13. www.znakdlaszkoly.pl/fragmenty/lic_hist_01_podr.pdf
14. Biometric Systems Lab. HaSIS – A Hand Shape Identyfication System.
15. Ernst R.H. Hand ID systems. US Patent No. 3576537, 1971.
16. Miller B. Vital signs of identity. IEEE Spectrum, 31(2):22-30, 1994
17. www.cassini.pl/indexcas.html
18. Turk M., Pentland A. "Eigenfaces for recognition", Journal of Cognitive Neuroscience, vol.3, No.1, 1991
19. www.enter.pl/ent99.12/technologie_tego_asp.

PERSONS IDENTIFICATION TECHNIQUES WITH UTILIZATION THEIR INDIVIDUAL BIOMETRICAL FEATURES.

In this paper different methods of the persons identification are presented based on their biometrical features distinctive for every identified object. It can be physiological properties, like fingerprints, form of palm, iris feature, as well as behavioral properties, as manner of writing or speaking out. Knowledge about disadvantagces and advantages of presented methods is the base of methods and identification algorithm designed by authors. This algorithms and methods are based on fuzzy decision rules. They are designed on the base of distance between characteristic points of face.