Elektroniczne rozpoznawanie odcisków palców

Systemy automatycznej identyfikacji osób staną się w najbliższym czasie powszechne. Największą szansę podboju rynku mają systemy biometryczne, wykorzystujące charakterystyczne cechy części ludzkiego ciała: palców, dłoni, twarzy, siatkówki, itd. Obecnie największą popularnością cieszą się systemy identyfikacji analizujące odciski palców. Okazuje się, że coś do powiedzenia w tej dziedzinie mają także Polacy!

Pokusa opracowania własnego oprogramowania, zdolnego skutecznie rozpoznawać odciski palca, była ogromna, dlatego podjęliśmy to wyzwanie. Zanim przedstawię szczegóły, krótkie wprowadzenie w dziedzinę.

Dostępne technologie

Czujniki pozwalające na odczyt linii papilarnych wykorzystują różne technologie:

Czujniki optyczne

Pierwszymi czujnikami były niewielkie kamery CCD lub CMOS. Palec przykładano do szklanej powierzchni, pod którą znajdował się pryzmat. Zastosowanie pryzmatu wymagało kompensacji zniekształceń trapezowych. Zaletą takiego rozwiązania jest możliwość skanowania dużych obszarów palca, co w przypadku innych technik jest kosztowne. Wadą jest łatwość „oszukania" układu poprzez podłożenia zdjęcia palca i wynikająca z tego konieczność stosowania dodatkowych zabezpieczeń.

Czujniki pojemnościowe

Zasada działania czujnika pojemnościowego polega na pomiarze pojemności między płaszczyzną czujnika a powierzchnią palca (**rys. 1**). Wartość pojemności zależy od odległości między obiema płaszczyznami, tak więc linie papilarne i przerwy między nimi wykazują różną pojemność. Wadą czujników tego typu jest ich spora wrażliwość na wilgotność palca. Wszelkie zawilgocone fragmenty mogą być widoczne jako ciemne „plamy", natomiast – w skrajnych przypadkach – palce suche nie będą w ogóle rejestrowane. Zaletą czujników pojemnościowych jest duża odporność na próby „oszukania" czujnika.

Czujniki ultradźwiękowe

Zaletą tych czujników jest wysoka jakość uzyskiwanych obrazów i niewielka wrażliwość na wilgotność skóry. Wadą natomiast wysoka cena i czujniki te mają niewielki obszar skanowania.

Czujniki RFww

Istnieje rodzina czujników wykorzystująca zjawisko propagacji fal radiowych. Czujnik stanowi układ wielu setek anten wytworzonych na powierzchni krzemu. Krawędzie czujnika otoczone są pierścieniem przyłączonym do generatora w.cz., a palec musi mieć z nim kontakt w czasie akwizycji obrazu. Czujnik wykrywa różnice kształtu, nie naskórka, ale warstw znajdujących się pod naskórkiem. Warstwy wewnętrzne odwzorowują jednak naskórek. Nie ma więc znaczenia, czy palec jest mokry, suchy, czy też ma wręcz uszkodzony naskórek. Wadą takiego rozwiązania jest niższa rozdzielczość w stosunku do czujników pojemnościowych, zwykle o połowę.

Czujniki termiczne

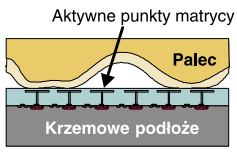
Firma Atmel jest jedynym producentem czujników wykorzystujących różnicę temperatury linii i zagłębień w strukturze papilarnej palca. Jakkolwiek różnice te są niewielkie, czujniki dają dobre obrazy odcisków. Dzięki wbudowanemu układowi stabilizacji temperatury mogą pracować w szerokim zakresie temperatur otoczenia.

Czujniki pełnowymiarowe i sweepery

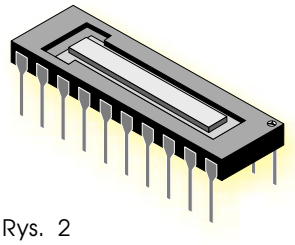
Bez mała każdy producent półprzewodnikowych czujników odciska palca produkuje dwie odmiany czujników:

– pełnowymiarowe, które odczytują obraz palca przyłożonego, widzianego na powierzchni czujnika oraz
– *sweepery* (**rys. 2**, **fot. 3**) wymagające przeciągnięcia palca nad czujnikiem.

O ile matryca czujnika pełnowymiarowego może składać się z np. 300 linii po 240



Rys. 1



Rys. 2

pikseli, o tyle *sweeper* będzie posiadał np. 8 linii po 240 pikseli. Składaniem pełnego obrazu palca zajmuje się oprogramowanie. Pierwszy *sweeper* był produkowany przez firmę Atmel.

Sweepery, jakkolwiek bardziej kłopotliwe, mogą wymagać równomiernego przesuwu palca, składania obrazu itd., są jednak znacznie tańsze. W technologii CMOS cena układu scalonego w dużej mierze zależy od zajmowanej powierzchni krzemu. Niebagatelną zaletą *sweeperów* jest także to, że na powierzchni czujników pełnowymiarowych pozostaje ślad odcisku palca i można go skopiować do późniejszego wykorzystania. Na *sweeperze* taki obraz nie zachowa się, ponieważ jest wycierany podczas akwizycji.

Jakość systemów rozpoznawania odcisków palców

Skuteczność działania systemów rozpoznawania odcisków palców określa się za pomocą trzech współczynników:

FAR – *false acceptable rate* – współczynnik fałszywej akceptacji – jest to procentowa liczba niezarejestrowanych w systemie osób, które system rozpoznał jako uprawnione. Im jest on mniejszy, tym większe jest bezpieczeństwo systemu.

FRR – *false rejection rate* – współczynnik fałszywych odrzuceń – jest to procentowa liczba osób uprawnionych, które nie zostały dopuszczone przez system. Im jest on mniejszy, tym większa jest wygoda użytkowania.

Zatem istnieje dość prosta zależność: im większe bezpieczeństwo systemu (mniejszy procent fałszywych akceptacji FAR), tym mniejsza jego wygoda użytkowania, gdyż wzrasta poziom fałszywych odrzuceń.

Fot. 3

Określa się także punkt środkowy (EER – *equal error rate*), który definiowany jest jako punkt przecięcia charakterystyk FAR i FRR, tzn. procent fałszywie odrzuconych i błędnie zaakceptowanych użytkowników jest zbliżony (**rys. 4**).

Funkcje użytkowe systemów

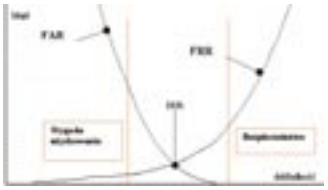
Funkcjonalnie pełen system identyfikacji powinien umożliwiać:

- Rejestrację nowego użytkownika – wygenerowanie pliku cech nowego użytkownika i zapisanie ich w bazie systemu.
- Weryfikację – sprawdzenie, czy pobrany odcisk należy do użytkownika podającego np. znany w systemie kod dostępu.
- Identyfikację użytkownika – sprawdzenie, czy użytkownik jest zarejestrowany w bazie.

Plik cech odcisku palca – template

Systemy rozpoznawania odcisków palca nie mogą w swojej pamięci trwale przechowywać całego, pełnego obrazu odcisku palca. Odciski palców może gromadzić jedynie policja. Popularne systemy identyfikacji starają się odszukać w obrazie palca istotne cechy charakterystyczne. Następnie tworzą unikalny plik cech, zwany w literaturze *template*, który jest opisem danego odcisku palca na podstawie jego charakterystycznych cech, nie zaś fotografią odcisku. Plik *template* ma rozmiar znacznie mniejszy niż rozmiar obrazu palca odebrany przez czujnik. Każdy system rozpoznawania odcisków generuje unikalny plik cech, rozumiany jedynie w ramach systemu. Znając plik cech, nie mamy żadnych szans na odtworzenia linii papilarnych palca, z którego on powstał. Najbardziej powszechną metodą tworzenia pliku *template* jest wywodząca się z kryminalistyki detekcja minutii. Minutie to zakończenia (*end points*) bądź rozgałęzienia (*bifurcation*) linii papilarnych. Dodatkowo definiuje się tzw. *core-point* i *delta-point*, czyli punkt środkowy i punkty delty (**rys. 5**).

Na podstawie tych informacji – położeniu minutii, ich orientacji, obecność punktów *core* i *delta*, jest generowany



Rys. 4

Rys. 5

plik cech, który następnie służy do identyfikacji lub weryfikacji użytkowników systemu.

Detekcja minutii nie jest banalnym problemem. Często odciski palców są uszkodzone, nieczytelne, tak więc znalezienie minutii, a często i linii papilarnych na tych obrazach jest praktycznie niemożliwe. Co gorsza, można wygenerować fałszywe minutie, niemające odpowiednika na rzeczywistym palcu.

Na lewej części **fot. 6** większa część odcisku jest nieczytelna, co zostało spowodowane dużą wilgotnością palca oraz mechanicznymi uszkodzeniami naskórka. Mimo takich uszkodzeń, napisane w naszej firmie oprogramowanie rozpoznaje odciski jako te same, co świadczy o dużej skuteczności naszego algorytmu. Pokazane zakłócenia występują stosunkowo rzadko i są mimo wszystko względnie łatwe do usunięcia.

Znacznie trudniejszym problem są zniekształcenia struktury linii papilarnych wynikające z odkształceń elastycznych skóry. Powstają one w wyniku różnej lub zmiennej siły nacisku palca na czujnik podczas akwizycji (**fot. 7**), co powoduje zmianę częstotliwości występowania linii papilarnych (odległości między sąsiednimi liniami) oraz nieliniowe przesunięcia punktów charakterystycznych. Z tych powodów stosowanie klasycznych

Fot. 6

Fot. 7

metod, opartych o porównania minutii, nie zawsze daje oczekiwane efekty. Dopiero zastosowanie zaawansowanych technik modelowania umożliwia poprawną identyfikację zniekształconych odcisków, jednak okupione może być wzrostem czasu przetwarzania. Budowanie pliku cech na podstawie kilku obrazów palca oraz przechowywanie cech kilku odcisków palców tej samej osoby także prowadzi do zwiększenia efektywności systemu.

Jak testować systemy?

Wszystko zależy od celu i efektów, jakie zamierzamy osiągnąć. W opisach dostępnych na rynku systemów dość często czytamy: FAR = 0,00001% i FRR=0,001%. Oczywiście, takie wyniki można uzyskać dla określonego użytkownika lub małej, znanej grupy użytkowników, która rygorystycznie przestrzega zalecanych zasad użytkowania systemu. I tylko w takiej grupie!

nik FAR=0,1%, choć nie na wszystkich bazach odcisków, natomiast rezultaty w granicach kilku procent uchodziły za niezłe. Po prostu bazy odcisków używane przez organizatorów zawodów nie są banalne. Najmniejsza „wada" algorytmu zostanie bezlitośnie ujawniona, a jej negatywny wpływ na końcowy wynik jest nie do ukrycia.

Testując oprogramowanie opracowane przez nas, na odciskach pochodzących z baz FVC2002, osiągnęliśmy wyniki na poziomie EER = 0,6% i FRR = 2% przy zerowym FAR, przy rozmiarze pliku cech pojedynczego odciska ok. 2 kB. Czas wprowadzenia obrazu palca był poniżej 200 ms, a czas jego porównanie ze zbiorem cech innego odcisku poniżej 240 ms. Znane implementacje, zrealizowane bez udziału PC, mają czasy porównywania ok. 1,2 s. Skuteczna implementacja analizy

Główne problemy, z którymi muszą zmierzyć się systemy identyfikacji, to:

- **niewrażliwość na zakłócenia struktury linii papilarnych w postaci pęknięcia skóry, zmiennej wilgotności odcisku powodującej powstawanie „plam" itp.,**
- **uwzględnienie efektu elastyczności skóry prowadzącego do ogromnych zniekształceń,**
- **uwzględnienie rotacji palca.**

Pogorszenie jakości odcisku, wynikające z uszkodzeń skóry, wilgotności palca, odkształceń plastycznych skóry, jest głównym powodem pogorszenia współczynnika FRR.

Firmy produkujące czujniki odcisków dysponują własnymi bazami, zwykle nieudostępnianymi publicznie, co utrudnia porównanie własności algorytmów czy oferowanych systemów.

Chcąc uzyskać niezależne i obiektywne oceny, można wysłać swoje algorytmy na bezpłatne, odbywające się co dwa lata zawody algorytmów, *Finger Print Verification Competition* – FVC organizowane przez uniwersytet w Bolonii i amerykańskie laboratoria zajmujące się rozpoznawaniem obrazów. Każdy przesłany algorytm testowany jest na czterech różnych bazach odcisków, na tym samym sprzęcie komputerowym, a więc w warunkach umożliwiających bezpośrednie porównanie uzyskanych wyników. Należy jednak pamiętać, że wyniki z różnych edycji FVC nie są ze sobą porównywalne z uwagi na różne warunki, w jakich prowadzono testy i użyte różne zbiory odcisków.

Zwycięzca edycji 2002, firma zajmująca się odciskami palca od 25 lat, uzyskał wy-

odcisków wymaga jednak użycia procesorów sygnałowych lub większych jednostek ARM.

Obecnie najlepsze znane systemy identyfikacji charakteryzuje: EER = 0,1...5 % oraz FRR = 1...50% przy zerowym FAR.

Uzyskano czasy przetwarzania:

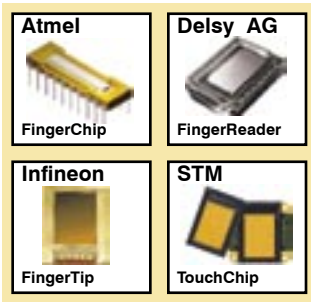
- wprowadzanie nowego użytkownika – 0,1...2 s.
- porównanie informacji o odciskach – 0,1...3 s.

Czasy przetwarzania zmierzono na komputerze z procesorem Pentium III taktowanym sygnałem zegarowym o częstotliwości 933 MHz. Podane czasy nie uwzględniają czasu niezbędnego na wczytanie obrazu odcisku z czujnika.

FVC2004

Wydaje się, że niektórzy uczestnicy konkursu przechytrzyli organizatorów FVC2002 i podczas testów przechowywali w systemie obrazy całych palców, nie zaś pliki cech, przez co mogli uzyskać doskonałe wyniki, dystansując konkurentów. W obecnej edy-

Czytniki odcisków palców są produkowane przez:



cji – FVC2004, wprowadzono ograniczenia na wielkość zbioru cech, który w tzw. kategorii *Light* nie mógł przekraczać 2,5 kB. Wydaje się, że zabieg ten w widoczny sposób spowodował przetasowanie liderów w poszczególnych kategoriach.

W zawodach FVC2004 użyto baz danych zawierających szczególnie „trudne" odciski, na których zwycięzcy osiągali średnie ERR w granicach 2...3 %, a nie jak w poprzedniej edycji 0,1%.

Zastosowanie trudnych odcisków nie było złośliwością organizatorów. Wymagania stawiane systemom identyfikacji będą systematycznie rosły. Skoro mają być one powszechnie stosowane, muszą być uniwersalne i „dostosowane" do potrzeb obsługi np. masowego ruchu na przejściach granicznych, podczas kontroli faktu głosowania.

Nasza firma wzięła udział w zawodach FVC2004, występując pod roboczym, nadanym przez organizatorów, symbolem P027. Uzyskane wyniki ulokowały nas w pierwszej połowie światowej stawki, ulegliśmy m.in. Chińskiej Akademii Nauk.

Resztę informacji i wyników można prześledzić w [1], do czego wszystkich serdecznie zachęcamy. Do udziału w zawodach FVC2006 także.

Jerzy Brzeski,
Zakład Techniki Mikroprocesorowej

Linki internetowe:

1. University of Bologna – turniej algorytmów rozpoznawania palców Fingerprint Verification Competition (FVC) *http://bias.csr.unibo.it*/FVC2004
2. Publikacje dotyczące biometrii:
   http://biometrics.cse.msu.edu/publications.html
   http://dmoz.org/Computers/Security/Biometrics/
   htpp://www.fusa.com/
3. Krzysztof Buczek, Artur Sulkowski – Wyniki testów Samall_Finger, niepublikowane prace Zakładu Techniki Mikroprocesorowej, Poznań 2003, *www.ztm-exe.com.pl*