PRZEGLĄD TELEINFORMATYCZNY
NR 1-4, 2020

Wybrane metody rozpoznawania osób na podstawie odcisków palców

Leszek GRAD

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, WAT
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
leszek.grad@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono zagadnienie rozpoznawania tożsamości osób na podstawie odcisków palców. Przedstawiono aktualny stan wiedzy, wybrane metody i techniki zarówno opisu obrazu linii papilarnych, jak i metody klasyfikacji.

SŁOWA KLUCZOWE: biometria, rozpoznawanie odcisków palców, identyfikacja, weryfikacja tożsamości

Wstęp

Obecnie obserwuje się gwałtowny rozwój elektronicznych systemów zabezpieczeń wykorzystujących techniki biometryczne w procesie uwierzytelniania. Ze wszystkich dotychczas stosowanych metod zabezpieczeń techniki biometryczne należą do najbezpieczniejszych oraz najwygodniejszych dla użytkowników. Bezpieczeństwo wynika z tego, że człowiek dysponuje wieloma unikatowymi cechami, które mogą być agregowane w celu osiągnięcia żądanego poziomu bezpieczeństwa. Systemy dostępu bazujące na biometrii są wykorzystywane powszechnie zarówno w dostępie do systemów o bardzo wysokim poziomie zabezpieczeń (systemy bankowe, bankomaty, laboratoria), jak i do zabezpieczeń personalnego sprzętu komputerowego (laptopy z czytnikami biometrycznymi, myszki, pamięci flash, smartfony). Jedną z ważniejszych charakterystyk biometrycznych są odciski palców. Oprócz zastosowań w systemach dostępu odciski palców od dawna były i są nadal wykorzystywane w kryminalistyce do identyfikacji przestępców (daktyloskopia). Systemy automatycznego rozpoznawania odcisków palców są z języka angielskiego określane skrótem AFIS (*Automated Fingerprint Identification System*).

Podstawowe pojęcia biometrii

Biometria (ang. *biometrics*) jest nauką zajmującą się identyfikacją lub weryfikacją tożsamości osoby na podstawie jej cech fizycznych lub behawioralnych. Owe cechy nazywane są cechami biometrycznymi (ang. *biometric traits*) [33] lub krótko biometrykami [5]. Dokonuje się systematyki biometryk. Są one dzielone na rejestrowane w sposób statyczny, nazywane fizycznymi lub fizjologicznymi (ang. *physiological traits*) oraz rejestrowane w pewnym przedziale czasu, zwane behawioralnymi (ang. *behavioral traits*), obejmujące cechy wykształcone lub wyuczone. Do pierwszej kategorii zaliczane są, będące przedmiotem rozważań niniejszego artykułu, odciski palców. Przykładem charakterystyki behawioralnej jest głos. Zestawienie podstawowych charakterystyk biometrycznych przedstawione zostało w tabeli 1, szczegółowy zaś opis poszczególnych biometryk można znaleźć w pracach [5], [18], [33].

Tab. 1. Podstawowe charakterystyki biometryczne

Cechy fizyczne	Cechy behawioralne
Odciski palców	Głos
Tęczówka oka	Składanie podpisu
Układ naczyń krwionośnych siatkówki oka	Ruch ust
Układ naczyń krwionośnych dłoni	Chód
Geometria dłoni	
Obraz twarzy	
Termogram	
Profil DNA	
Kształt ucha	

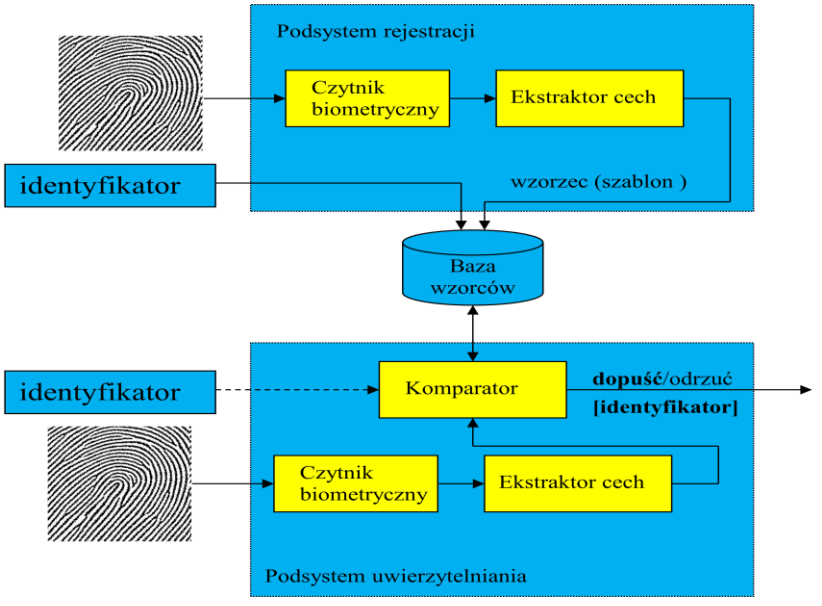
Przydatność danej biometryki jest oceniana na podstawie pięciu cech: unikatowości (ang. *unigueness*), uniwersalności (ang. *univesality*), trwałości (ang. *permanence*), mierzalności lub ściągalności (ang. *collectability*), akceptowalności (ang. *acceptance*). W tym świetle idealną cechą jest taka, która pozwala na jednoznaczną identyfikację osobnika w ramach określonej populacji, każdy osobnik ją posiada, łatwo ją zmierzyć oraz jej zdejmowanie nie budzi kontrowersji ani nie jest inwazyjne. Z wymienionych w tabeli 1 największe znaczenie praktyczne obecnie posiadają: odciski palców wraz z układem naczyń krwionośnych dłoni, tęczówka oka oraz głos (z biometryk behawioralnych).

Systemy biometryczne

Systemem biometrycznym nazywany jest system rozpoznawania (identyfikacji lub weryfikacji), w którym klasyfikacja odbywa się na podstawie

charakterystyk biometrycznych (zapisanych w postaci wektorów cech). Architekturę typowego biometrycznego systemu rozpoznawania przedstawiono na rysunku 1. Składa się on z dwóch podsystemów: rejestracji oraz identyfikacji/weryfikacji. Zadaniem pierwszego jest dokonanie rejestracji użytkownika. W trakcie jednorazowej rejestracji w bazie danych (lub ogólniej w systemie) zapisywany jest identyfikator oraz wzorzec (szablon) biometryczny. Zadaniem podsystemu identyfikacji/weryfikacji jest dokonanie identyfikacji poprzez porównanie pobranej próbki biometrycznej ze wzorcami zapisanymi w bazie lub zweryfikowanie tożsamości poprzez porównanie pobranej próbki ze wzorcem osoby, której tożsamość jest deklarowana.

Działanie biometrycznych systemów rozpoznawania oceniane jest na podstawie dwóch podstawowych wskaźników. Pierwszym z nich jest stopa fałszywej akceptacji (ang. *False Acceptance Rate* – FAR) wyznaczana jako procent zdarzeń polegających na pozytywnej weryfikacji fałszywej próbki. Drugim jest stopa fałszywego odrzucenia (ang. *False Rejection Rate* – FRR) wyznaczana jako procent zdarzeń polegających na stwierdzeniu niezgodności badanej próbki ze wzorcem w sytuacji, kiedy zgodność występuje. Do porównywania jakości działania systemów rozpoznawania wykorzystuje się wskaźnik EER (ang. *Equal Error Rate*) wyznaczany jako wartość wskaźnika FAR lub FRR dla takiego progu decyzyjnego, kiedy FAR = FRR.



Rys. 1. Architektura typowego biometrycznego systemu uwierzytelniania

System biometryczny jest systemem rozpoznawania wzorców. Wykorzystuje zatem znane metody klasyfikacji (klasyfikatory minimalno-odległościowe, sztuczne sieci neuronowe) [18], [23], [33], [47].

1. Odcisk palca jako charakterystyka biometryczna

Jak zaznaczono we wstępie, odciski palców należą do podstawowych charakterystyk biometrycznych. Są wykorzystywane do identyfikacji osób od dawna. Już w XVIII zostały wykorzystane przez Galtona do identyfikacji tożsamości [33]. Na początku XX wieku opracowany został system identyfikacji Sir Edwarda Henry'ego, udoskonalony przez FBI (stosowany w kryminalistyce do ręcznej identyfikacji tożsamości) [5]. Wykorzystuje on podział wszystkich odcisków na pięć podstawowych klas: pętla lewa (ang. *left loop*), pętla prawa (ang. *right loop*), wir (ang. *whorl*), łuk (ang. *arch*), łuk wyostrzony namiotowy, (ang. *tented arch*) (rys. 2). Wzorzec zawiera opis wszystkich dziesięciu palców wg schematu: [*łuk, pętla lewa, łuk namiotowy, wir...*]. Obecnie, w systemach automatycznego rozpoznawania klasyfikacja typów odcisków jest stosowana do wstępnego filtrowania bazy odcisków [9]. W obrazie linii papilarnych można wskazać dwa charakterystyczne miejsca (punkty, ang. *Singular points*). Pierwszym jest tzw. rdzeń (ang. *Core*) [12]. Jest to miejsce o największej zmienności kierunku przebiegu grzbietów[1] [4], [40]. Drugim jest miejsce, gdzie linie tworzą układ delty (ang. *Delta point*). Obydwa charakterystyczne punkty pokazane zostały na rysunku 3.

Rys. 2. Pięć podstawowych klas odcisków. Od lewej: pętla lewa (ang. *left loop*) (34%), pętla prawa (ang. *right loop*) (31%), wir (ang. *whorl*) (28%), łuk (ang. *arch*) (4%), łuk wyostrzony (namiotowy) (ang. *tented arch*) (3%). W nawiasach podano częstość występowania, obrazy z bazy FVC2002

[1] W obrazie linii papilarnych wyróżniamy grzbiety (ang. *ridge*), czyli miejsca w których palec przylegał do skanera oraz doliny albo bruzdy (ang. *valley*), czyli miejsca pomiędzy grzbietami.

Charakterystyka odcisku palca w świetle pożądanych cech

Unikatowość: bardzo niska powtarzalność – szacowane ok. 1 : 64 miliardów [5].

Uniwersalność: nieliczny odsetek nie posiada tej cechy (utrata kończyny, wady genetyczne).

Trwałość: wysoka – obraz linii papilarnych kształtuje się w okresie prenatalnym i nie zmienia się do końca życia, dość duża jednak podatność na uszkodzenia przy ranach prowadzących do blizn (można je jednak traktować jako zmianę charakterystyki).

Mierzalność: łatwa – skanowanie obrazu odcisku palca zabiera mało czasu i jest jedną z najmniej inwazyjnych metod biometrycznych.

Akceptowalność: w kryminalistyce cecha nieistotna, w systemach ochrony jest akceptowalna.

Poza powyższymi cechami systemy rozpoznawania bazujące na obrazach linii papilarnych charakteryzują się wysoką skutecznością rozpoznawania (FAR rzędu 0,01% przy FRR maksymalnie 10% [24], [33]).

Ważną cechą systemu biometrycznego jest odporność na oszustwa. W przypadku odcisków palców wysoką odporność gwarantują nowoczesne skanery odczytujące obraz trójwymiarowy oraz mierzące tętnienie krwi w naczyniach krwionośnych [48]. W zakresie polityki bezpieczeństwa systemów biometrycznych leży także ochrona baz wzorców przed kompromitacją [37][2].

Rys. 3. Punkty charakterystyczne obrazu odcisku palca: rdzeń oraz delta, obraz z bazy FVC2002 DB1_B

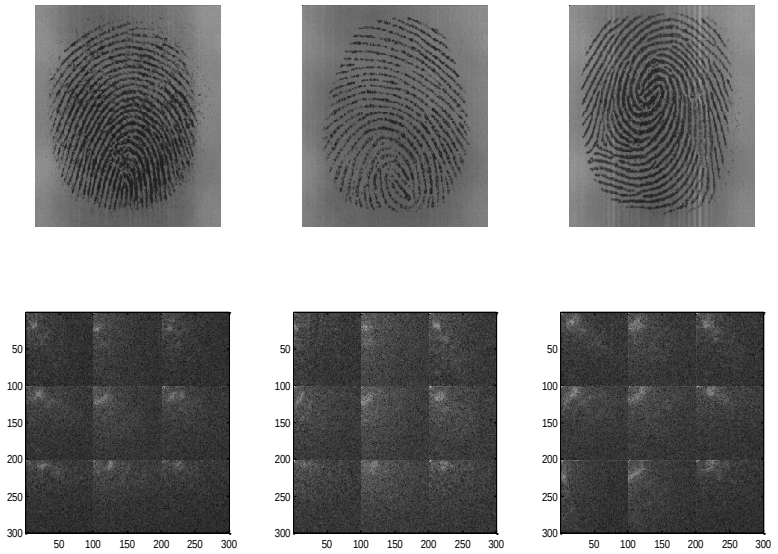
[2] W pracy przedstawiono wysoce bezpieczną technikę komparacji odcisków odporną na ataki DPA (ang. *Differential Power Analysis*), które mogą doprowadzić do kompromitacji wzorca.

Podstawowe metody ekstrakcji cech obrazu linii papilarnych

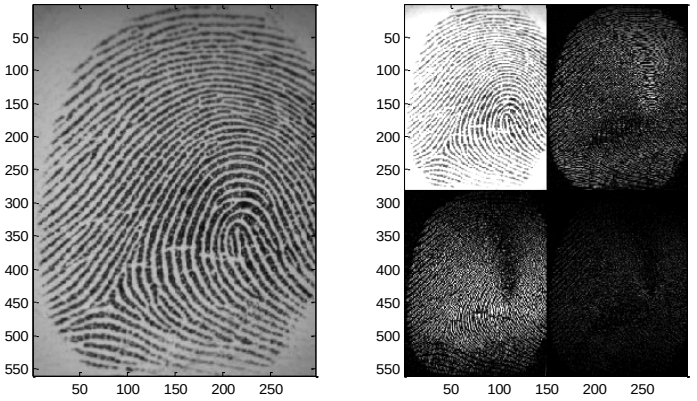
Obraz linii papilarnych poddawany jest analizie mającej na celu wydobycie cech istotnych dla procesu rozpoznawania (cech dystynktywnych) przy jednoczesnej redukcji danych, co pociąga za sobą szybsze działanie systemu rozpoznawania oraz zmniejszenie objętości bazy wzorców.

Obecnie w rozpoznawaniu odcisków palców wykrystalizowały się dwa podejścia. Pierwsze polega na rozpoznawaniu poprzez porównywanie obrazów odcisków (ang. *fingerprint matching*), najczęściej w dziedzinie transformat (przestrzenno-częstotliwościowej). Najczęściej wykorzystywane transformaty to: transformata Fouriera, transformata kosinusowa, transformata falkowa [2], [9], [36]. Na rysunku 4 przedstawione zostały obrazy trzech odcisków oraz transformaty kosinusowe tych obrazów wyznaczone w segmentach (lokalnie), każdy obraz został podzielony na 9 segmentów, wyraźnie widoczny jest zróżnicowany rozkład energii w odpowiadających sobie segmentach transformat związany z kierunkiem przebiegu linii. Z kolei rysunek 5 przedstawia wynik dekompozycji falkowej (pierwszego poziomu) obrazu odcisku. W wyniku dekompozycji uzyskuje się składową niskoczęstotliwościową oraz informację o szczegółach przebiegu linii (poziomych, pionowych oraz przebiegających ukośnie). Analiza kierunku przebiegu linii (rys. 6) stanowi jedną z podstawowych metod opisu obrazu odcisku i jest rozwijana od początku lat dziewięćdziesiątych ubiegłego stulecia [8], [9], [10], [20], [28], [30], [38], [43], [44], [45]. Rozpoznawanie odcisków w dziedzinie transformat cechuje duża odporność na niską jakość obrazu odcisku. Jest preferowane w identyfikacji kryminalistycznej, gdzie ważna jest minimalizacja FRR.

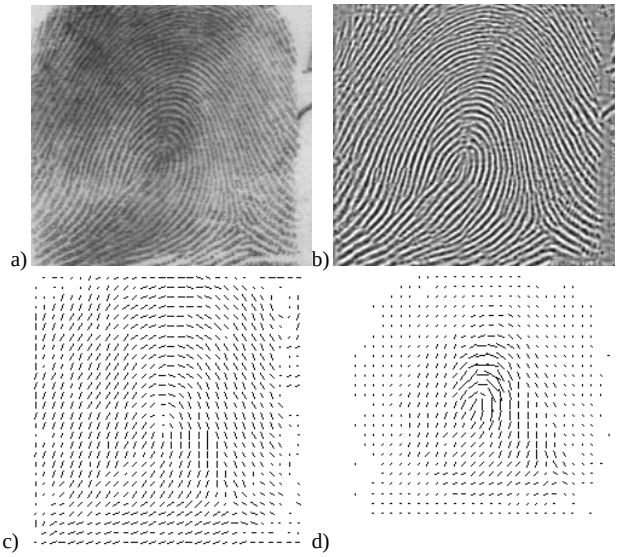
Drugie podejście do rozpoznawania odcisków polega na uwzględnieniu charakterystycznych cech budowy morfologicznej (szczególnych elementów geometrycznego wzoru tworzonego przez linie papilarne) tzw. minucji [18], [19], [29], [32], [33], [46]. Wyszczególniono kilkanaście różnych detali [49] (rys. 7), z których najczęściej wykorzystywane są dwa, tzn. początek/koniec linii oraz rozwidlenie pojedyncze (bifurkacja). W tym przypadku wzorzec odcisku obejmuje wektor minucji, z których każda opisana jest współrzędnymi położenia oraz kierunkiem przebiegu grzbietu. Początek układu współrzędnych umieszcza się w rdzeniu odcisku. Stosowanymi metodami znajdowania rdzenia są: metoda Poincare [17], [30], [31], [34] oraz R92 [31].



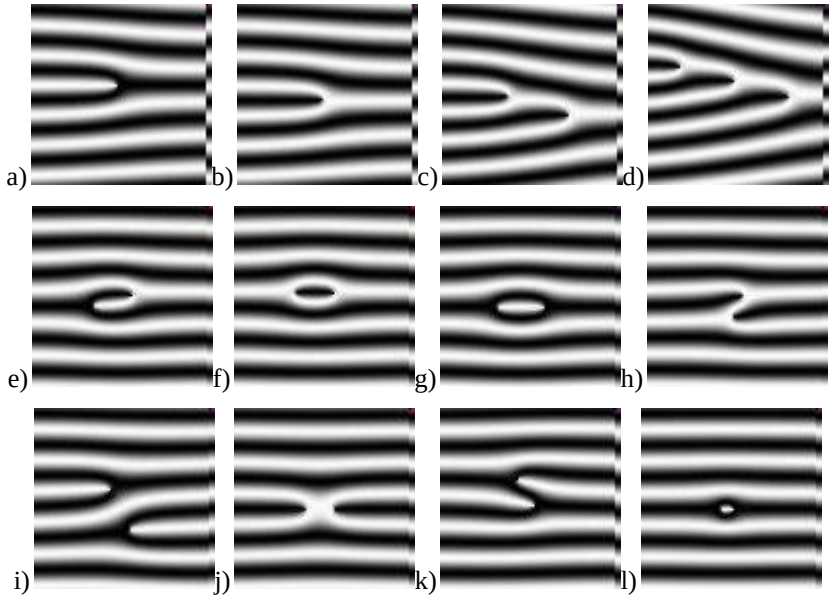
Rys. 4. Odciski trzech palców i odpowiadające im lokalne transformaty kosinusowe. Zastosowano podział obrazu na 9 segmentów, widoczny jest odmienny rozkład energii w odpowiadających sobie segmentach transformat. Obrazy z bazy FVC2002 DB3_B



Rys. 5. Transformata falkowa obrazu linii papilarnych (po prawej), pierwszy poziom dekompozycji. Prawy górny obraz opisuje detale poziome, lewy dolny – detale pionowe, prawy dolny – detale skośne. Obrazy z bazy FVC2002 DB1_B

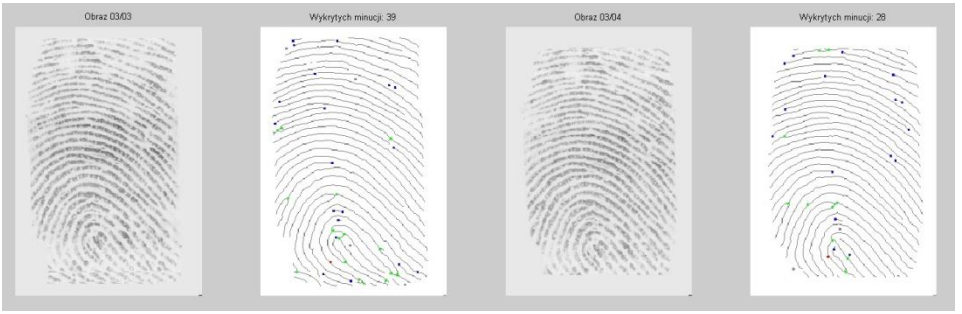


Rys. 6. Ekstrakcja cech w metodzie przedstawionej w pracy [8], a) obraz linii papilarnych, b) obraz o poprawionej jakości (ang. *enhancement*), c) kierunki przepływu bruzd (ang. *directional image*), d) directional image z wycentrowanym rdzeniem odcisku



Rys. 7. Minucje (linie przedstawione są kolorem białym): a) początek/koniec, b) rozwidlenie pojedyncze, c) rozwidlenie podwójne, d) rozwidlenie potrójne, e) haczyk, f) oczko, g) odcinek, h) mostek, i) linia przechodząca, j) skrzyżowanie, k) styk boczny, l) punkt Źródło: www.optel.com.pl

Z reguły w obrazach linii papilarnych wykrywa się 30-40 minucji. Do określenia zgodności odcisku ze wzorcem wystarczy zgodność na poziomie 10-20[3]. Rozpoznawanie na podstawie minucji preferowane jest w weryfikacji biometrycznej, gdzie ważna jest minimalizacja wskaźnika FAR. Detekcja minucji wymaga zastosowania wieloetapowego przetwarzania obrazu[4] [29]. Na rysunku 8 przedstawiono obrazy odcisków przetworzone do postaci szkieletowej z wykrytymi zakończeniami oraz rozwidleniami linii.



Rys. 8. Obrazy odcisków palców oraz obrazy szkieletowe z naniesionymi, wykrytymi minucjami (zakończenia oraz rozwidlenia)[5]

Poważnym problemem, który należy rozwiązać w systemach automatycznego rozpoznawania odcisków palców, jest problem rotacji i translacji. Co prawda skanery w przeważającej mierze są tak skonstruowane, że nie pozwalają na zbyt wielkie odchylenia osi palca od pionowej osi skanera oraz przesunięcie wzdłuż tej osi, ale nawet niewielkie wartości przesunięcia i obrotu mogą skutkować znaczącym pogorszeniem wyników rozpoznawania. Ustalenie osi palca, tym samym rotacji, jest dość łatwe, jeśli zarejestrowany obraz posiada pewien margines. W przeciwnym razie zadanie staje się trudne i stanowi element wielu prac badawczych (punkt 2). W przypadku korekcji błędu przesunięcia wykorzystuje się rdzeń odcisku jako punkt odniesienia.

[3] Na podstawie [48] oraz badań przeprowadzonych w ramach prac dyplomowych prowadzonych przez autora, ciekawe rezultaty badań przedstawiono także w pracy [21].

[4] Typowe fazy ekstrakcji minucji:

1. binaryzacja z progiem adaptacyjnym;
2. wyznaczenie kierunku przepływu linii w każdym pikselu – metody gradientowe;
3. wyznaczenie rdzenia odcisku;
4. szkieletyzacja – metody morfologiczne;
5. lokalizacja minucji;
6. eliminacja minucji fałszywych.

[5] Opracowanie wewnętrzne WAT, autor: Michał Kazimierczak.

W przypadku systemów opartych na minucjach, które są bardzo czułe na rotację i translację, stosuje się najczęściej lekko rozmyte dopasowywanie na etapie wykrywania poszczególnych minucji.

2. Wybrane przykłady metod i algorytmów rozpoznawania tożsamości na podstawie odcisków palców

W tym rozdziale dokonano opisu ciekawszych podejść do rozpoznawania tożsamości osób na podstawie obrazu linii papilarnych. Wybrano zarówno te, gdzie nacisk położono na metodę ekstrakcji cech (opis obrazu), jak i te, w których zaproponowano interesujące systemy klasyfikacji.

W pracy [13] przedstawiono wyniki zastosowania neuronowych sieci rezonansowych ART1 do wstępnej klasyfikacji odcisków. Dla każdej klasy, do ostatecznej identyfikacji jako klasyfikatora użyto również sieci neuronowej. Zbadano wpływ takiego podejścia na czas realizacji procesu rozpoznawania, porównując z działaniem systemu opartego na jednej sieci neuronowej. Otrzymano ponad dwudziestokrotne skrócenie czasu klasyfikacji. Poprawiła się także skuteczność rozpoznawania z 98% do 100% prawidłowych identyfikacji. Również w pracy [26] do weryfikacji zastosowano wielowarstwową sieć neuronową. W tym przypadku sieć neuronowa została wykorzystana jako jeden z trzech algorytmów wykrywania minucji (w metodzie uwzględniono zakończenia i rozwidlenia linii). Do komparacji ze wzorcem zaproponowano własny rozmyty operator, który pozwolił obejść problem różnej liczby wykrywanych minucji w obrazie. Testy wykazały skuteczność takiego podejścia na poziomie 95%.

Problem wstępnej klasyfikacji odcisków był rozważany także w pracach [9] oraz [45]. W pierwszej z nich przedstawiony został dwustopniowy system klasyfikacji wstępnej odcisków (tzn. zaliczania do jednej z podstawowych pięciu klas). W pierwszym stopniu zastosowano klasyfikację minimalnoodległościową opartą na transformacie KL (MKL – Multi-space KL). Wynikiem tego etapu było wytypowanie dwóch najbardziej prawdopodobnych klas. Ostateczne rozstrzygnięcie następowało w klasyfikatorze SPD, który został wytrenowany do rozpoznawania jednej z klas z każdej możliwej pary. Wyekstrahowany wektor cech dla pierwszego etapu liczył 1680 elementów i zawierał opis kierunku przepływu bruzd w 28×30 segmentach, w drugim etapie wektor cech został zredukowany do 80 elementów (poprzez dekorelację). Metodę przetestowano z wykorzystaniem bazy NIST DB4, uzyskano stopę błędnej identyfikacji równą 4,8%, co jest najlepszym wynikiem uzyskanym dla tej bazy [16]. Wcześniejsze prace autorów [6], [7] były również poświęcone zastosowaniu MKL w rozpoznawaniu odcisków. W pracy [45] przedstawiono metodę wstępnej klasyfikacji odcisków na podstawie występowania i położenia rdzenia oraz

delty. Opis parametryczny odcisku zawierał 3 elementy: liczbę rdzeni, liczbę delt, położenie delty (środek, strona lewa odcisku, strona prawa). Wzorce poszczególnych klas zostały opisane w następujący sposób:

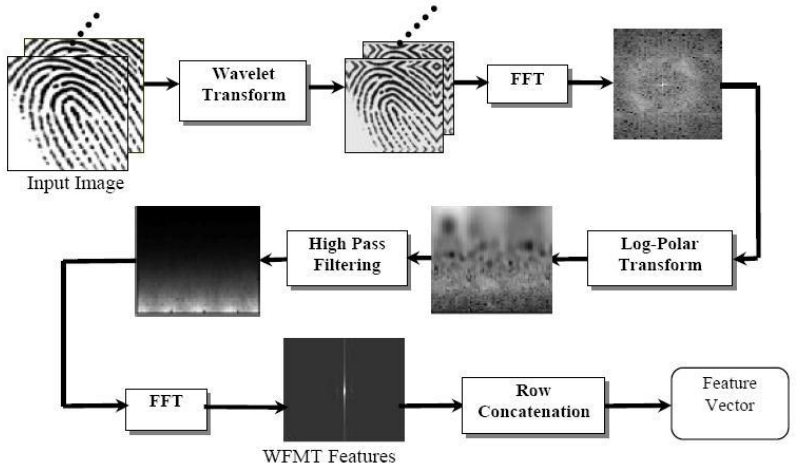
łuk – [0, 0, -], łuk namiotowy – [1, 1, środek], pętla lewa – [1, 1, prawo], pętla prawa – [1, 1, lewo], wir – [2, 2, -]. Do wyznaczenia zarówno rdzenia, jak i delty wykorzystano indeks Poincare. Tak nieskomplikowane określenie wzorców dało dość dobre rezultaty (stopa prawidłowych identyfikacji 84%).

W pracy [2] do parametrycznego opisu odcisku w zadaniu weryfikacji tożsamości zastosowano transformatę falkową oraz transformatę Fouriera–Mellina (WFMT – *Wavelet and the Fourier-Mellin Transform*). Wykorzystana tu została dekompozycja falkowa 2 poziomu w celu wygładzenia i utrwalenia przebiegu linii papilarnych[6]. Pozwala to na uniezależnienie się od zniekształceń kształtu[7] (ang. *shape distortion*). Otrzymano w ten sposób także obraz w mniejszej rozdzielczości, co wpływa na zmniejszenie nakładów obliczeniowych w dalszych etapach przetwarzania. Transformata Fouriera–Mellina zapewnia ekstrakcję cech oraz umożliwia uniezależnienie się od przesunięcia, obrotu i zmiany skali (ang. *invariants features*). Przebieg procesu ekstrakcji cech w proponowanej metodzie przedstawiony został na rysunku 9. W pierwszym kroku algorytmu realizowana jest transformata falkowa. Do dalszego przetwarzania zostaje wzięta jedynie niskoczęstotliwościowa składowa dekompozycji (redukcja przestrzeni, wygładzenie obrazu). W drugim kroku obraz odcisku poddawany jest transformacie Fouriera w celu uzyskania widma amplitudowego. Widmo amplitudowe jest nieczułe na translację.

Kolejny krok to przekształcenie widma do układu planarnego oraz jego zlogarytmowanie. Zabieg ten pozwala na uniezależnienie się od zmiany skali i zastosowanie kwantyzacji nieliniowej uwypuklającej harmoniczne o niższej częstotliwości. Zlogarytmowane widmo amplitudowe przedstawione w układzie biegunowym zostaje poddane filtracji górnoprzepustowej i ponownie transformacie Fouriera (cepstrum, uniezależnienie się od rotacji obrazu pierwotnego). Ostateczny wektor cech uzyskano, sumując wiersze macierzy wynikowej (wektor cech o długości wiersza obrazu odcisku palca po transformacie falkowej). Taka metoda ekstrakcji cech obrazu linii papilarnych została przetestowana na bazie FVC 2002. Dla różnych zbiorów odcisków tej bazy uzyskano ERR od 1,25 do 3,57, co należy uznać za wynik bardzo dobry.

[6] Wykorzystuje niskoczęstotliwościową składową dekompozycji.

[7] Takich jak przerwy w przebiegu linii papilarnych.



Rys. 9. Diagram algorytmu ekstrakcji cech odcisku palca zaproponowany w pracy [2]

Opis innych podejść stosowanych do rozpoznawania obrazów z inwariantnością cech (*integral transforms*, *moment invariants*) można znaleźć w pracy [36].

W pracy [17] opisano metodę opartą także na analizie obrazu odcisku w przestrzeni dwuwymiarowej dyskretnej transformaty Fouriera, z wykorzystaniem jedynie charakterystyki fazowej. Metoda pozwala na skuteczną ekstrakcję cech z obrazów niskiej jakości.

Podsumowanie

Przedstawiona w artykule cecha biometryczna, jaką jest układ linii papilarnych, jest stale wykorzystywana w systemach uwierzytelniana opartych na biometrii. Pomimo, jak się uznaje, lepszych cech, jak np. obraz tęczówki oka, układ żył palca czy śródręcza, odciski palców są stosowane w rozpoznawaniu. Dzieje się to za sprawą wysokiej dystynktywności, uwarunkowań historycznych (zastosowanie w kryminalistyce), rozpowszechnienia układów do akwizycji (niska cena), jak również istnienia ugruntowanych, zaawansowanych metod przetwarzania, analizy i rozpoznawania obrazów linii papilarnych, których przegląd został przedstawiony w niniejszym opracowaniu.

Literatura

[1] AHMED F., MOSKOWITZ I.S., *Composite signature based watermarking for fingerprint authentication*, MM&Sec ’05: Proceedings of the 7th workshop on Multimedia & Security, ACM, August 2005, pp. 137-142.

[2] ANDREW T.B.J., DAVID N.C.L., *Integrated Wavelet and Fourier-Mellin invariant feature in fingerprint verification system*. WBMA ’03: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, ACM, November 2003, pp. 82-88.

[3] BEY K.B., GUESSOUM Z., MOKHTARI A., BENHAMMADI F., *Agent based approach for distribution of fingerprint matching in a metacomputing environment*. NOTERE ’08: Proceedings of the 8th International Conference on New Technologies in Distributed Systems, ACM, June 2008, pp. 1-7.

[4] BIAN W., XU D., LI O., CHENG Y., JIE B., DING X., *A Survey of the Methods on Fingerprint Orientation Field Estimation*. IEEE Access, 2019, Volume 7, pp. 32644-32663.

[5] BOLLE R.M., CONNELL J.H., PANKANTI S., RATHA N.K., SENIOR A.W., *Biometria*, WNT, Warszawa 2008.

[6] CAPPELLI M., MAIO D., MALTONI D., *Fingerprint Classification based on Multi-space KL*. In proceedings Workshop on Automatic Identification Advances Technologies (AutoID ’99), Summit (NJ), October 1999, pp. 117-120.

[7] CAPPELLI M., MAIO D., MALTONI D., *Multi-space KL for Pattern Representation and Classification*. IEEE Transactions on Pattern Analysis Machine Intelligence, Vol. 23, no. 9, September 2001, pp. 977-996.

[8] CAPPELLI R., LUMINI A., MAIO D., MALTONI D., *Fingerprint Classification by Directional Image Partitioning*. IEEE Transactions on Pattern Analysis and Machine Intelligence 21(5), 1999, pp. 402-421.

[9] CAPPELLI M., MAIO D., MALTONI D, NANNI L., *A two-stage fingerprint classification system.* WBMA ’03: Proceedings of the 2003 ACM SIGMM workshop on biometrics methods and applications, ACM, November 2003, pp. 95-99.

[10] CAO K., JAIN A.K., *Automated Latent Fingerprint Recognition*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2019, Volume 41, Issue 4, pp. 788-800.

[11] CLANCY T.Ch., KIYAVASH N., LIN D.J., *Secure martcardbased fingerprint authentication*. WBMA ’03: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, ACM, November 2003, pp. 45-52.

[12] DOROZ R., WROBEL K., PORWIK P., *An accurate fingerprint reference point determination method based on curvature estimation of separated ridges*, International Journal of Applied Mathematics and Computer Science, 2018, Vol. 28, no. 1, pp. 209-225.

[13] GOUR B., BANDOPADHYAYA T.K., PATEL R., *ART and Modular Neural Network Architecture for Multilevel Categorization and Recognition of Fingerprints.* IEEE Conference, Knowledge Discovery and Data Mining, 2010. WKDD '10, Third International Conference, pp. 536-539.

[14] GUPTA P., RAVI S., RAGHUNATHAN A., JHA N.K., *Efficient fingerprint-based user authentication for embedded systems*. DAC '05: Proceedings of the 42nd annual Design Automation Conference, ACM, June 2005.

[15] HOLZ Ch., BAUDISCH P., *The generalized perceived input point model and how to double touch accuracy by extracting fingerprints*. CHI '10: Proceedings of the 28th international conference on Human factors in computing systems, ACM, April 2010.

[16] HONG L., JAIN A.K., *Classification of Fingerprint Images*. http://www.cse.msu.edu/biometrics/Publications/Fingerprint/clas.pdf

[17] ITO K., MORITA A., AOKI T., HIGUCHI T., NAKAJIMA H., KOBAYASHI K., *A fingerprint recognition algorithm using phase-based image matching for low-quality fingerprints.* Image Processing, 2005, ICIP 2005, IEEE International Conference on, pp. II-33-6.

[18] JAIN A.K., HONG L., PANKANTI S., BOLLE R., *An Identity Autentication System Using Fingerprints*. Proc. of IEEE 85 (9), 1997, pp. 1365-1388, on line at: http://biometrics.cse.msu.edu/Publications/Fingerprint/JainEtAlIdentityAuthUsingFp_ProcIEEE97.pdf

[19] JAIN A.K., HONG L., BOLLE R., *On-Line Fingerprint Verification*. IEEE Transactions on Pattern Analysis and MAchine Intelligence, Vol. 19, no. 4, 1997, pp. 302-314.

[20] JAN H., ALI A., *Optimization of fingerprint size for registration*. Applied Computer Science, vol. 15, no. 2, 2019, pp. 19-30.

[21] KAPCZYŃSKI A., *Quantitative and qualitative characteristics of fingerprint biometric templates*. Zeszyty Naukowe. Organizacja i Zarządzanie / Politechnika Śląska, 2014, z. 74, s. 55-63.

[22] KAWAGOE M., TOJO A., *Fingerprint Pattern Classification*. Pattern Recognition, Vol. 17, no. 3, 1984, pp. 295-303.

[23] KWIATKOWSKI W., *Metody rozpoznawania wzorców*. Bel Studio, Warszawa, 2002.

[24] MALTONI D., MAIO D., PRABHAKAR S., *Handbook of Fingerprint Recognition, SprioSpringre Professional Computing Series*, 2003.

[25] MIL'SHTEIN S., PILLAI A., SHENDYE A., LIESSNER C., BAIER M., *Fingerprint Recognition Algorithms for Partial and Full Fingerprints*. 2008 IEEE Conference on Technologies for Homeland Security, pp. 449-452.

[26] MONTESANTO A., BALDASSARRI P., VALLESI G., TASCINI G., *Fingerprints recognition using Minutae extraction: a fuzzy approach*, Image analysis and processing, ICIAP 2007, 14th International Conference, pp. 229-234.

[27] PARK C.H., LEE J.J., SMITH M., PARK S., PARK K.H., *Directional filter bank-based fingerprint feature extraction and matching*. IEEE Trans. On Circuits and Systems for Video Tachnology, Vol. 14, 1, 2004, pp. 74-78.

[28] RAO A.R., *A Taxonomy for Texture Description and Identification*. Springer-Verlag, New York, 1990.

[29] RAPTA P., SAEED K., *A new algorithm for fingerprint feature extraction without the necessity to improve its image*. Bio-Algorithms and Med-Systems, 2010, Vol. 6, no. 12, pp. 25-29.

[30] SRINIVASAN V.S., MURTHY N.N., *Detection of Singular Points In Fingerprint Images.* Pattern Recognition 25(2), 1992, pp. 139-153.

[31] SURMACZ K., SAEED K., RAPTA P., *An improved algorithm for feature extraction from a fingerprint fuzzy image.* Optica Applicata, 2013, Vol. 43, no. 3, pp. 515-527.

[32] SZCZEPANIAK M., JÓŹWIAK I., *Data management for fingerprint recognition algorithm based on characteristic points group*. Foundations of Computing and Decision Sciences, 2013, Vol. 38, no. 2, pp. 123-130.

[33] ŚLOT K., *Wybrane zagadnienia biometrii*. WKŁ, Warszawa, 2008.

[34] TANG T.Y., MOON Y.S., CHAN K.C., *Efficient implementation of fingerprint verification for mobile embedded systems using fixed-point arithmetic*. SAC ’04: Proceedings of the 2004 ACM symposium on Applied Computing, ACM, March 2004, pp. 821-825.

[35] TARDOS G., *Optimal probabilistic fingerprint codes*. STOC '03: Proceedings of the thirty-fifth annual ACM symposium on Theory of computing, ACM, June, 2003, pp. 116-125.

[36] TICO M., IMMONEN E., RAMO P., KOUSMANEN P., SARINNEN J., *Fingerprint Recognition Using Wavelet Features*. Proc. of IEEE international Symposium on Circuits and Systems 2, 2001, pp. 21-24.

[37] YANG S., VERBAUWHEDE I.M., *A secure fingerprint matching technique*. WBMA ’03: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, ACM, November, 2003, pp. 98-94.

[38] WANG S., ZHANG W.W., WANG Y.S., *Fingerprints Classification by Directional Fields.* ICMI'02: Proceedings of the 4th IEEE International Conference on Multimodal Interfaces, IEEE Computer Society, October, 2002, pp. 395-399.

[39] WEGSTEIN J.H., *An automated fingerprint identification system*. U.S. National Institute of Standards and Technology, NBS Special Publication 500-89, 1982.

[40] WIECLAW L., *Gradient based fingerprint orientation field estimation*. Journal of Medical Informatics & Technologies, Vol. 22, 2013, pp. 203-207.

[41] WOOD J., *Invariant Pattern Recognition: A Review*. Pattern Recognition, 29 (1), 1996, pp. 1-17.

[42] WÓJTOWICZ W., *A Fingerprint-Based Digital Images Watermarking for Identity Authentication.* Annales Universitatis Mariae Curie-Skłodowska. Sectio AI, Informatica, Vol. 14, no. 1, 2014, pp. 85-96.

[43] VALDES-RAMIREZ D., MEDINA-PÉREZ M.A.;MONROY R., LOYOLA-GONZÁLEZ O., RODRÍGUEZ J., MORALES A., HERRERA F., *A Review of Fingerprint Feature Representations and Their Applications for Latent Fingerprint Identification: Trends and Evaluation*. IEEE Access, Volume 7, 2019, pp. 48484-48499.

[44] VIZCAYA P.R., GERHARDT L.A., *A Nonlinear Orientation model for Global Description of Fingerprints.* Pattern Recognition 29 (7), 1996, pp. 1221-1231.

[45] ZHANG Q., HUANG K., YAN H., *Fingerprint classification based on extraction and analysis of singularities and pseudo ridges.* VIP '01: Proceedings of the Pan-Sydney area workshop on Visual information processing, Volume 11, Australian Computer Society Inc., May, 2001.

[46] ZHAO F., TANG X., *Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction*. Pattern Recognition 40, 2007, pp. 1270-1281, online at: www.sciencedirect.com

[47] ŻURADA J., BARSKI M., JĘDRUCH W., *Sztuczne sieci neuronowe*. Wydawnictwo Naukowe PWN, Warszawa, 1996.

[48] http://www.biometriclabs.pl/index.php?id=57&Itemid=112 (dostęp 17.09.2019).

[49] http://www.optel.com.pl/software/polska/metody.htm (dostęp 16.06.2019).

Fingerprint recognition – review of used methods

ABSTRACT: The paper considers the issue of the identity recognition of persons on the basis of fingerprints. The current state of knowledge, selected methods and techniques of fingerprint image description and classification methods are presented.

KEYWORDS: biometrics, fingerprint recognition, identification, verification

Praca wpłynęła do redakcji: 22.11.2019 r.