ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2012
Seria: ORGANIZACJA I ZARZĄDZANIE z. 61 Nr kol. 1873

Michał SZCZEPANIK, Ireneusz J. JÓŹWIAK
Politechnika Wrocławska
Wydział Informatyki i Zarządzania

SYSTEMY INTELIGENTNEJ BRAMKI BAZUJĄCE NA ROZPOZNAWANIU ODCISKÓW PALCÓW UWZGLĘDNIAJĄCYCH ICH USZKODZENIA

Streszczenie. W artykule przedstawiono istniejące rozwiązania z zakresu rozpoznawania odcisków palców, a także wykazano ich nieskuteczność w przypadku występowania zmian struktury linii papilarnych w wyniku fizycznych uszkodzeń. Zaproponowano nowy algorytm, bazujący na rozkładzie grup minucji, który w analizie odcisku uwzględnia częste uszkodzenia odcisku. Proponowany algorytm może mieć zastosowanie w systemach inteligentnych bramek, ograniczających nieuprawniony dostęp do wrażliwych danych bądź innych zasobów przedsiębiorstwa.

SYSTEMS INTELLIGENT GATEWAY BASED ON FINGERPRINT RECOGNITION TAKING INTO ACCOUNT THE DAMAGE

Summary. In this paper authors present existing solutions for fingerprint recognition, and demonstrated their ineffectiveness in the event of changes in the fingerprint structure as a physical damage result. They propose a new algorithm based on distribution groups minutiae, fingerprint analysis, which takes account of frequent damage to the imprint. The proposed algorithm can be applied in systems of intelligent gateways restrict unauthorized access to sensitive data or other enterprise resources.

1. Wprowadzenie

Artykuł zawiera analizę skuteczności działania istniejących algorytmów rozpoznawania odcisków palców w przypadku wystąpienia uszkodzeń fizycznych. Praktycznie każdy system biometryczny może stanowić inteligentną bramkę, ponieważ ludzi można rozpoznawać na podstawie różnych cech, np.: wyglądu twarzy, sposobu poruszania, odcisków palców,

kształtu twarzy oraz innych cech fizycznych i behawioralnych [2]. Systemem inteligentnej bramki może być czytnik kontroli dostępu, umożliwiający dostęp do pomieszczeń tylko wybranym i upoważnionym osobom, lub systemy rejestracji czasu pracy. Najpopularniejszy, zapewne dlatego, że najtańszy, jest obecnie system rozpoznawania linii papilarnych, który spotykamy w większości sprzedawanych komputerów i nośników informacji. Urządzenia do weryfikacji osób, wykorzystujące ten system, nie należą jednak do najbezpieczniejszych [10] – przestępcy udowodnili to wielokrotnie. Dlatego stosuje się także dodatkową weryfikację, stwierdzającą, czy badany obiekt jest człowiekiem. Wykonano wiele typów urządzeń akwizycyjnych, a najczęściej stosowane to: sensory optyczne (nieodporne na zabrudzenia oraz łatwe do oszukania), sensory pojemnościowe (mało odporne na wyładowania elektrostatyczne, łatwe do oszukania), sensory naciskowe (mała czułość), sensory termiczne (dość odporne na oszustwa) oraz sensory ultradźwiękowe (drogie, ale bardzo dobrej jakość pomiaru).

2. Budowa linii papilarnych

Linie papilarne tworzą charakterystyczny układ bruzd na skórze, w szczególności na opuszkach palców rąk, ale także na innych powierzchniach naszego ciała. Powstają one w czasie życia płodowego i, zgodnie z zasadą sformułowaną przez Galtona, są niepowtarzalne, niezmienne i nieusuwalne. Linie papilarne opisuje się za pomocą charakterystycznych cech, tzw. minucji, których jest ponad 30 rodzajów. Typy minucji wykorzystywane w kryminalistyce w Polsce przedstawiono w tabeli 1.

Tabela 1

Typy minucji wykorzystywane w kryminalistyce w Polsce [1]

NAZWA MINUCJI		SYMBOL
W języku polskim	**W języku łacińskim**	
Początek	Initium	J
Zakończenie	Terminatio	T
Rozwidlenie pojedyncze	Bifurcatio simplex	B1
Rozwidlenie podwójne	Bifurcatio duplex	B2
Rozwidlenie potrójne	Bifurcatio triplex	B3
Złączenie pojedyncze	Iunctio simplex	Jn1
Złączenie podwójne	Iunctio duplex	Jn2
Złączenie potrójne	Inucito triplex	Jn3
Haczyk	Unculus	U
Oczko pojedyncze	Ocellus simplex	O1
Oczko podwójne	Ocellus duplex	O2

Zwykle odcisk rozpatruje się tylko na podstawie 2 typów mutacji: początku i rozwidlenia bruzd, ponieważ pozostałe, tj. punkt czy odcinek, często mogą pochodzić z błędu odczytu, najczęściej spowodowanego zabrudzeniami. Zgodnie z polskim prawem odciski uznaje się za identyczne, jeżeli 15 punktów charakterystycznych jest jednakowo rozmieszczonych na obu próbkach.

3. Bezpieczeństwo i użyteczność systemów biometrycznych

Prawdopodobieństwo zakwalifikowania wzorca do danej klasy, mimo iż przynależy on do innej, jest nazywane poziomem bezpieczeństwa i określone parametrem FAR (ang. *False Acceptance Rate*) [2]. W systemie biometrycznym poziom bezpieczeństwa jest to prawdopodobieństwo przyznania dostępu do systemu mimo braku stosowanych uprawnień. Poziom użyteczności jest określony przez parametr FRR (ang. *False Rejection Rate*). Jest to prawdopodobieństwo niezakwalifikowania wzorca do danej klasy, mimo iż do niej należy. W systemie biometrycznym poziom użyteczności jest to prawdopodobieństwo nieprzyznania dostępu do systemu mimo posiadania uprawnień.

Zabezpieczenie uprawniające dostęp do zasobów tylko określonym pracownikom jest realizowane za pomocą inteligentnej bramki. Inaczej mówiąc, służy ona do identyfikacji pracowników w przedsiębiorstwie. Dlatego jest istotne, żeby poziomy bezpieczeństwa i użyteczności były wysokie i jednocześnie nie stanowiły utrudnienia w pracy.

Istniejące algorytmy rozpoznawania odcisków palców, mimo iż stosuje je się od lat, nie są odporne na zmiany struktury fizycznej odcisków palców. Wystąpienie uszkodzeń na odcisku znacznie obniża poziom ich użyteczności, często powodując frustrację pracowników i niechęć do ich stosowania.

Problem dopasowania odcisków jest procesem złożonym nawet w warunkach laboratoryjnych, dlatego algorytmy stosowane w inteligentnej bramce powinny być nieczułe na niektóre naturalne zdarzenia, do których możemy zaliczyć:

- niekompletność odcisku – kilka odcisków może się nakładać częściowo,
- skanowany odcisk może być obrócony (rotacja),
- część odcisku może być zamazana lub nieczytelna (np. palec częściowo przyłożony do czytnika),
- nawet przy właściwym pobieraniu odcisku mogą wystąpić elastyczne deformacje,
- palec w obszarze odcisku może być zraniony (skaleczenia).

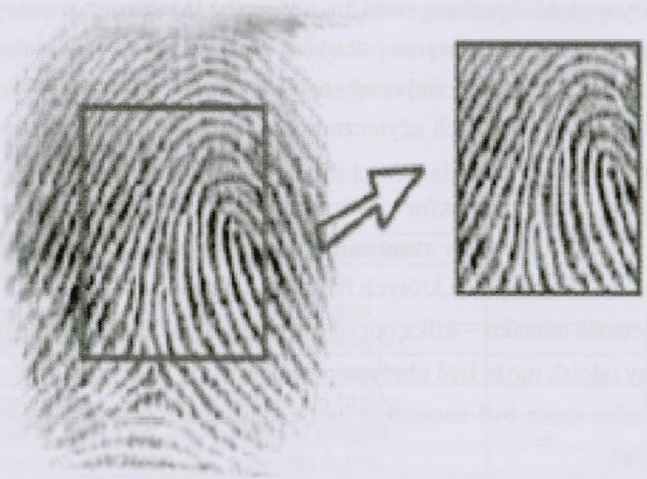
4. Algorytmy rozpoznawania odcisków palców

Najpopularniejszymi algorytmami rozpoznawania odcisków palców są [2]:

- algorytm oparty na wzorcach (ang. *Pattern-Based Templates*),
- algorytm elastycznego dopasowania minucji (ang. *Elastic Minutiae Matching*),
- algorytm oparty na grafie przylegania minucji (ang. *Minutiae Adjacency Graph*),
- algorytm oparty na triangulacji delaunay (ang. *Delaunay Triangulation*).

4.1. Algorytm oparty na wzorcach

Algorytm oparty na wzorcach [3] przechowuje oryginalny obraz odcisku, tzw. wzorzec. Po zeskanowaniu odcisku badanego wyszukiwany jest środek odcisku, tzw. rdzeń, a następnie, po podstawowych przekształceniach graficznych, np. skalowaniu i rotacji, obraz ten porównywany jest ze wzorcem. Taka procedura czyni algorytm praktycznie nieodpornym na uszkodzenia. Ze względu na przechowywanie oryginalnego obrazu odcisku istnieje duże ryzyko, że obraz ten może zostać odczytany z pamięci czytnika bądź bazy danych, dlatego w Polsce algorytm ten został uznany przez Generalnego Inspektora Ochrony Danych Osobowych za niebezpieczny [12]. Prawnie odcisk palca jest uznawany za część danych osobowych i jego przechowywanie bez zgody właściciela jest nielegalne.

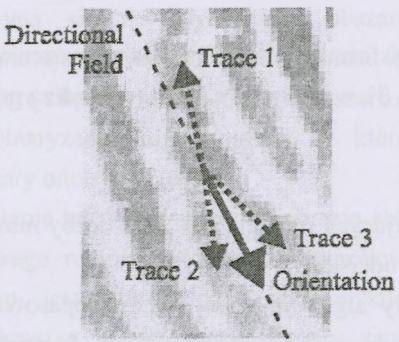


Rys. 1. Algorytm bazujący na wzorcach – lokalizacja rdzenia odcisku [3]
Fig. 1. Based on patterns algorithm [3]

4.2. Algorytm elastycznego dopasowania minucji

Algorytm elastycznego dopasowania minucji wylicza model nieliniowej transformacji w dwóch etapach. Przede wszystkim lokalne dopasowanie określa, które punkty na odciskach prawdopodobnie pasują do siebie. Bazuje ono na cechach lokalnego podobieństwa. Bez tego etapu rozwiązanie problemu wymagałoby więcej stopni swobody. Następnie realizuje się dopasowanie globalne, które wykorzystuje odpowiadające sobie fragmenty do wyznaczenia globalnej transformacji. Odpowiadające sobie punkty są wyliczone przy użyciu metody minimalizacji kwadratów dopuszczalnych błędów, które muszą być dokładnie wybrane, gdyż odległości między odpowiadającymi sobie punktami po elastycznej rejestracji są niewielkie.

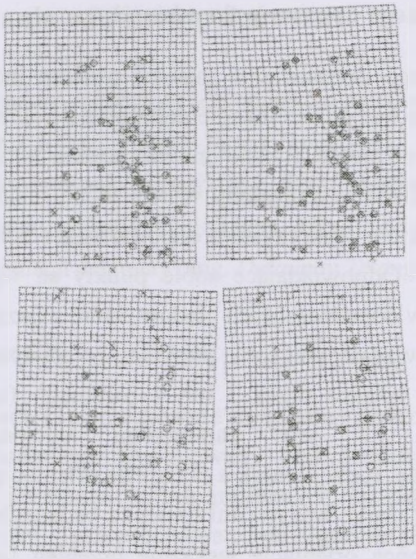
Każda minucja jest opisana przez 3 lub 4 parametry (x, y, T, Θ), gdzie: x i y to współrzędne minucji, T jest parametrem opcjonalnym, określającym typ (np. początek/zakończenie, rozwidlenie), a Θ określa orientację minucji. Poprawna orientacja jest wybierana przez podążanie wszystkimi liniami z badanego punktu przez pewien dystans. Dla punktu początku/końca orientację wskazuje przebieg linii, a dla rozwidlenia – linie rozwidlające się w danym punkcie.



Rys. 2. Określanie orientacji minucji typu rozwidlenie [3]
Fig. 2. The orientation of a bifurcation point [3]

W dopasowaniu lokalnym wykorzystuje się sąsiedztwo, czyli najbliższe danej minucji dwa inne punkty charakterystyczne, następnie tak zależne punkty wyszukuje się w zapisie wzorca. Po znalezieniu kilkunastu takich odwzorowań tworzy się globalną transformację obrazu. W zależności od zniekształceń obrazu wykorzystuje się jedną z metod:

- opartą na progu r_0, który określa dopuszczalną różnicę odległości między minucjami w odciskach badanym i wzorcowym,
- opartą na transformacji TSP (ang. *Thin-Plate Spline*).



Rys. 3. Macierze rozkładu minucji w algorytmie elastycznego dopasowania [3]
Fig. 3. Minutiaes distribution matrices in the elastic match algorithm [3]

Po zastosowaniu transformacji macierz rozmieszczenia minucji jest porównywana z macierzą wzorcową (rys. 3), a zgodność s jest określana za pomocą wzoru (1):

$$S = \frac{n_{match}^2}{n_2 n_2}, \tag{1}$$

gdzie: n_{match} to liczba pasujących minucji, n_1 i n_2 to liczby minucji odpowiednio w testowym odcisku i w szablonowym odcisku.

Wielkość S wskazuje, czy algorytm elastycznego dopasowania minucji jest odporny na wystąpienie uszkodzeń oraz czy rozpoznaje odciski, których obraz jest niepełny, np. gdy zeskanowano tylko ¾ odcisku.

4.3. Algorytm z grafem przylegania minucji i z triangulacją delaunay

Algorytm rozpoczyna swoje działanie od utworzenia gwiazd, czyli grafów, łączących sąsiednie minucje. Podobnie jak w przypadku poprzedniego algorytmu minucja jest opisana przez 3 lub 4 parametry v = (x, y, T, Θ), gdzie x i y to współrzędne minucji, T jest parametrem opcjonalnym, określającym typ (np. początek/zakończenie, rozwidlenie), a Θ określa orientację minucji, której definicja jest taka sama jak w rozdziale 4.2. Dodatkowo określa się krawędzie łączące dwa punkty reprezentujące minucje. Każda krawędź jest zdefiniowana następująco: e = (u, v, rad, rc, Φ), gdzie u, v to węzły (minucje) początkowe i krańcowe, rad jest to euklidesowa odległość między minucjami, rc określa tę odległość

przez liczbę bruzd (linii papilarnych) między minucjami, a Φ jest to kąt pomiędzy krawędzią a osią x. Następnie tworzy się grafy łączące tylko sąsiadów. Węzły są uznane za sąsiadów, jeśli odległość między nimi jest mniejsza niż d_{max}. Po tej operacji gwiazdy są łączone i tworzą globalny graf odcisku. Metoda ta jest mało odporna na wielokrotne zranienia palca, głównie skaleczenia, gdyż generują one dodatkowe minucje, które całkowicie zaburzają strukturę grafu.

Algorytm oparty na triangulacji łączy sąsiednie minucje, tworząc w ten sposób trójkąty. Niestety, podobnie jak algorytm grafowy, nie jest odporny na zranienia.

5. Rozwiązanie bazujące na grupach minucji

Proponowane rozwiązanie, w przeciwieństwie do znanych z literatury, nie analizuje minucji pojedynczo, ale wyszukuje się grupy minucji. Taka analiza obrazu odcisku palca jest znacznie bardziej odporna na uszkodzenia, gdyż w przypadku ich wystąpienia taka grupa może tylko nieznacznie (o 1 lub 2) zwiększyć liczność zawartych w niej minucji.

Analiza obrazu rozpoczyna się od wyszukania obszaru zawierającego odcisk z wykluczeniem obszarów zawierających znaczne uszkodzenia. Obraz odcisku jest opisany skalą odcieni szarości, definiującą siłę przyłożenia danego obszaru do czytnika.

Obraz jest poddawany binaryzacji jednoprogowej, w której parametr t_g wyklucza z analizy słabo odczytane obszary odcisku.

Ostatnim etapem jest nałożenie maski bazującej na obrazie zbinaryzowanym. Maskę dla obszaru kwadratu (X,Y), którego rozmiar wynosi 2,5 szerokości bruzdy, określają dwa paramenty: p_{lo} i p_{hi}. Parametr p_{lo} jest ograniczeniem, które wyklucza obszary ze zbyt małą liczbą pikseli opisujących obraz, a p_{hi} wyklucza obszary zamazane, np. wilgotne. Po zastosowaniu maski otrzymujemy obraz pozbawiony znacznych uszkodzeń, które mogłyby zaburzyć analizę odcisku.

Następnym problemem jest niwelacja uszkodzeń i wyszukiwanie minucji. Niwelację uszkodzeń realizuje się przez obliczenie wariancji punktów i analizę jasności. Na podstawie tych dwóch parametrów obliczana jest częstotliwość występowania bruzd po zastosowaniu filtru Gabora [11] do uwypuklenia bruzd i dolin. Po wprowadzeniu segmentacji, zgodnie z przyjętym rozmiarem segmentu 2,5 szerokości bruzdy, obraz jest przerysowywany. Dzięki temu linie papilarne są ciągłe i niepostrzępione. W przeciwieństwie do rozwiązań znanych z literatury nie wymagają dodatkowych przekształceń, by wyszukać minucje, np. przekształcania wszystkich bruzd do szerokości 1px. Filtr Gabora nie wymaga informacji o orientacji minucji. Wymaga tylko danych o jej położeniu. Dlatego na otrzymanym obrazie stosuje się wyszukiwanie krawędzi, co oznacza, że minucje znajdują się w punktach

przecięcia krawędzi bruzd. Obraz minucji dzielony jest na segmenty, a każdy segment odpowiadający grupie minucji jest opisany przez parametry (*x, y, nom*), gdzie *x* i *y* to współrzędne, a *nom* określa liczbę minucji w grupie. Ponadto w jednej implementacji zastosowano dodatkowy parametr, określający prawdopodobieństwo wystąpienia uszkodzeń w danym segmencie, bazując na rozkładzie obszarów odrzuconych przez maskę. Ostatnim etapem jest utworzenie macierzy euklidesowych odległości pomiędzy grupami minucji. Podczas porównywania stosuje się dwa parametry: d_x – dopuszczalną różnicę odległości między grupami we wzorcu i badanym odcisku i p_x – próg prawdopodobieństwa uszkodzeń (określa, czy dana grupa jest brana pod uwagę w analizie). Podczas porównywania grupy są dzielone zgodnie z wagą, którą definiuje liczba minucji w grupie. Takie działanie zapewnia szybką weryfikację, czy analizowany odcisk jest zgodny ze wzorcem.

6. Wyniki badań

Opracowany i przedstawiony w rozdziale 5 algorytm porównano z innymi algorytmami, opisanymi wcześniej, wykorzystując bazy 120 różnych odcisków palców po 8 próbek każda. Baza zawierała 10% odcisków z uszkodzeniami (25-30% powierzchni), które stanowiły głównie skaleczenia i poparzenia, czyli najczęściej spotykane w życiu codziennym uszkodzenia. Wyniki przedstawiono w tabeli 2.

Tabela 2

Wyniki eksperymentu

	Parametr FAR	**Parametr FRR**
Algorytmy literaturowe		
MAG	1,52%	0,95%
EMM	2,35%	2,55%
PBT	0,30%	8,52%
Opracowane algorytmy		
MGM64	9,25%	0,1%
MGM32	3,12%	0,1%
MGM32_SA	0,33%	0,1%

Zgodnie z przewidywaniami algorytm oparty na wzorcach jest najbardziej wrażliwy na uszkodzenia i nie rozpoznał większości uszkodzonych odcisków. Z istniejących algorytmów najlepszy okazał się ten oparty na grafie dopasowania minucji. W przypadku proponowanego algorytmu bardzo istotny jest rozmiar segmentu. Gdy wynosi on 5 bruzd (MGM64), algorytm

nie zapewnia wymaganego poziomu bezpieczeństwa. Po zmniejszeniu rozmiaru grupy o połowę i zastosowaniu parametru prawdopodobieństwa wystąpienia uszkodzeń w danym segmencie algorytm MGM32_SA okazał się najskuteczniejszy.

7. Podsumowanie

Proponowane rozwiązanie może znaleźć zastosowanie w identyfikacji osób w przedsiębiorstwach, w których pracownicy są narażeni na uszkodzenia odcisków palców. Zastosowanie inteligentnej bramki znacznie ułatwia weryfikację czasu pracy pracowników i nie wymaga od nich posiadania żadnych dodatkowych kart, które łatwo zgubić. System może także znaleźć zastosowanie w ochronie dostępu do ważnych danych bądź pomieszczeń, do których część pracowników nie powinna mieć dostępu.

Bibliografia

1. Grzeszyk C.: Kryminalistyczne badania śladów linii papilarnych. Legionowo 1992.
2. Wayman J.L., Jain, A.K., Maltoni D., Maio D.: *Biometric Systems*. Technology. Design and Performance Evaluation, 1st Edition. Springer Verlag, 2005, p. 21-59.
3. Maltoni D., Maio D., Jain A.K., Prabhakar S.: Handbook of Fingerprint Recognition. 2nd Edition. Springer Verlag, 2009, p. 97-233.
4. Chikkerur S., Govindaraju V., Cartwright E. N.: K-plet and coupled bfs: A graph based fingerprint representation and matching algorithm. LNCS, Springer Verlag, 2006, p. 309-315.
5. He Y., Ou Z.: Fingerprint matching algorithm based on local minutiae adjacency graph. Journal of Harbin Institute of Technology, No. 10, 2005, p. 95-103.
6. Ross A., Dass S.C., Jain A.K.: A deformable model for fingerprint matching. Pattern Recognition, Vol. 38(1), 2005, p. 95-103.
7. Bebis, G., Deaconu, T., Georgiopoulos, M.: Fingerprint Identification Using Delaunay Triangulation. IEEE ICIIS, 1999, p. 452-459.
8. Huk M., Szczepanik M.: Prawdopodobieństwo błędu klasyfikatorów złożonych dla problemów wieloklasowych. Eksploatacja i Niezawodność – Maintenance and Reliability, nr 3, 2011, s. 12-17.
9. Szczepanik M., Szewczyk R.: Algorytm identyfikacji linii papilarnych tom 1. KNS, Wrocław 2008, s. 131-136.
10. Błoński G.: Hardware Hacking – oszukiwanie zabezpieczeń biometrycznych. Hakin9 – jak się obronić. nr 9, 2007, s. 33-43.

11. Hong L., Wan Y., Jain A. K.: Fingerprint image enhancement: Algorithm and performance evaluation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998, p. 777-789.
12. Strona internetowa Generalnego Inspektora Ochrony Danych Osobowych, http://www.giodo.gov.pl, [dostęp: maj 2011].

Abstract

In this paper authors present existing solutions for fingerprint recognition, and demonstrated their ineffectiveness in the event of changes in the structure of a fingerprint as a result of physical damage. Authors compare three most popular algorithm: Elastic minutiae matching (EMM), Minutiae Adjacency Graph (MAG) and based on patterns algorithm. They use fingerprint base in which 10% of fingerprints have damages. They also create new algorithm (MGM) which recognize fingerprints based on minutiaes groups. In the frist step this algorithm creates matrix of minutiaes groups and choses the biggest groups (number of minutiaes in group is the priority), in second steps determine the weight of each group based on image quality. The last step is to create a matrix of euclidean distances between the groups. To comparing algorithm use the two parameters: dx – the distance, the difference between groups in the pattern and the tested fingerprint px – the threshold probability of damage (determined whether a group is considered in the analysis). When comparing the groups are divided according to the weight which defines the number of minutiaes in the group. This provides quick verification of whether the analyzed fingerprint is consistent with the pattern.

The proposed solution can be used in factories and other enterprises in which workers are exposed to damaging fingerprints. The use of intelligent gateways greatly facilitates the verification of work time did not require them to have any additional cards. The system can also be applied to protect access to important data.