Nowa metoda do badania dynamiki ruchów myszy do celów identyfikacji

Marek Tabędzki[(1)], **Khalid Saeed**[(2)]
Wydział Informatyki Politechniki Białostockiej*
ul. Wiejska 45A
15-351 Białystok, Polska
[(1)] <tabedzki>, [(2)] <aida>@ii.pb.bialystok.pl

Streszczenie: Niniejsza praca przedstawia opis nowej metody badania cech biometrycznych dla celów identyfikacji osób oraz wyniki pierwszych eksperymentów z nią przeprowadzonych. Metoda ta polega na analizie dynamiki ruchów kursora myszy – rytm tych ruchów jest indywidualny i charakterystyczny dla każdego człowieka, dlatego może zostać wykorzystany do celów identyfikacji. Badanym sygnałem była prędkość kursora zmieniająca się podczas wykonywania przypadkowych ruchów myszą. Sygnał ten był przenoszony do dziedziny częstotliwości przy użyciu Dyskretnej Transformaty Fouriera i analizowany przy użyciu metody minimalnych wartości własnych macierzy Toeplitza. Uzyskany wektor cech stanowił opis wejściowego sygnału i mógł być podstawą do klasyfikacji, którą przeprowadzono dwiema metodami: *k* najbliższych sąsiadów oraz z użyciem sztucznych sieci neuronowych. Uzyskane wyniki są obiecujące i wskazują, że metoda ta może być z powodzeniem wykorzystana w celu identyfikacji osób.

Summary: This paper presents a description of a new method for analyzing biometric features for human identification, and results obtained from the first experiments performed with it. This method analyzes the dynamics of the mouse cursor movement. The rhythm of this movement is individual and characteristic for each person, so it can be used for identification. The processed signal is the cursor changing speed, obtained during random movement of a mouse. This signal is transformed into frequency domain with Discrete Fourier Transform and then analyzed by the method of Toeplitz matrix minimal eigenvalues. The resulting feature vector is used for classification performed by two methods: *k* nearest neighbors and artificial neural networks. The obtained results are promising and show that this method can be used for human identification successfully.

1. Wstęp

Metody biometryczne stają się coraz popularniejszą i chętnie stosowaną metodą identyfikacji osób, nawet jeśli nie zadomowiły się jeszcze na dobre w naszym kraju. Cechuje je wysoka skuteczność i bezpieczeństwo – w przeciwieństwie do haseł, kart magnetycznych, czy numerów PIN cechy biometryczne (czyli np. odcisk palca, geometria dłoni, czy obraz tęczówki oka) nie mogą być zgubione, skradzione lub zapomniane. Z ich użyciem wiąże się jednak pewien kłopot – do badania cech biometrycznych konieczne są specjalizowane urządzenia (skanery, kamery, etc.), które mogą być kosztowne i nie są typowym wyposażeniem komputera, co uniemożliwia wykorzystanie tych technologii np. w warunkach domowych. Stąd poszukiwania metody pomiarów biometrycznych możliwych do przeprowadzenia przy użyciu standardowego interfejsu. Jedna z takich metod polega na badaniu dynamiki pisania na klawiaturze [1, 2]. Ta stosunkowo nowa metoda polega na analizie odstępów między naciśnięciami poszczególnych klawiszy w trakcie pisania na klawiaturze i badaniu rytmu tych odstępów, który jest indywidualny i charakterystyczny dla każdego człowieka – pozwala to na identyfikację piszącego z wysoką skutecznością.

Metoda zaproponowana w niniejszej pracy opiera się na podobnym pomyśle i polega na analizie prędkości ruchów myszy. Prędkość ta nigdy nie jest jednostajna, lecz zmienia się, choćby w momencie zmiany kierunku ruchu. Również w wypadku wykonywania jednostajnego, zdawałoby się, ruchu dłonią, faktyczna prędkość kursora myszy podlega pewnym, nieznacznym zmianom. Te zmieniające się prędkości tworzą sygnał o indywidualnym dla każde-

* Praca została sfinansowana przez Rektora Politechniki Białostockiej, grant nr W/WI/3/04

go człowieka rytmie i przebiegu, podobnie jak indywidualny jest rytm pisania na klawiaturze. Mogą być one zmierzone z dużą dokładnością, a następnie zbadane przy użyciu odpowiedniego aparatu matematycznego. Przedstawione tutaj eksperymenty mają za zadanie stwierdzić na ile może być to podstawą do identyfikacji danej osoby.

2. Proponowana metoda badania dynamiki ruchów myszy

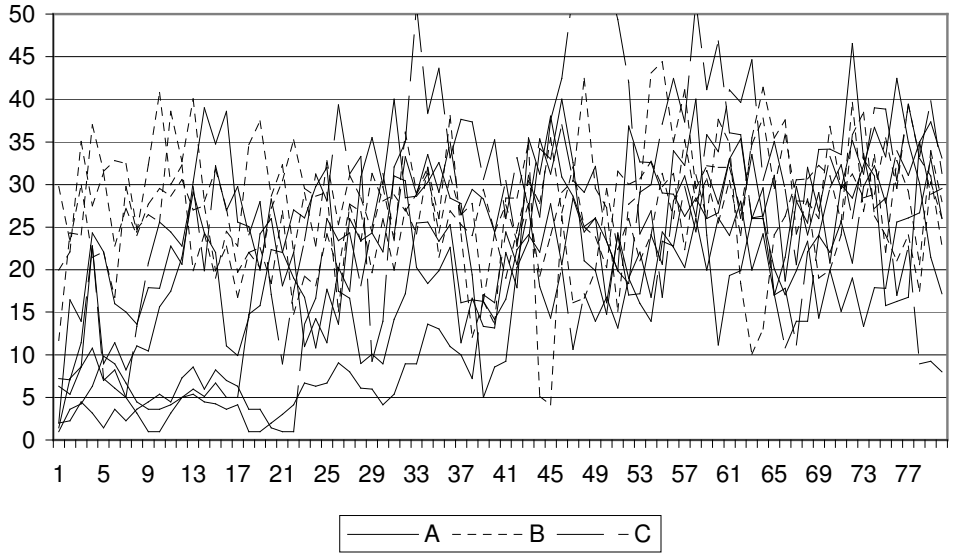
Poniżej przedstawiono szczegółowy opis proponowanej metody. W poszczególnych podrozdziałach omówione są kolejne kroki algorytmu – począwszy od zebrania danych, poprzez niezbędna analizę i wydobycie cech charakterystycznych, aż po klasyfikację.

2.1. Zbieranie danych

Pierwszym etapem było pobranie danych do badania. W tym celu co ustalony przedział czasu (zazwyczaj jest to kilka milisekund, choć może się to zmieniać w zależności od systemu operacyjnego, czy użytych sterowników) pobierane jest położenie kursora myszy. Badaniu nie będzie jednak podlegać samo położenie, lecz aktualna prędkość. Jest ona obliczana na podstawie odległości między kolejnymi położeniami kursora oraz czasu w jakim kursor tam się przemieścił.

Przemieszczanie się kursora było badane w trakcie wykonywania przypadkowych ruchów myszą. Zawsze pobierano próbki tej samej długości – czyli tę samą, z góry określoną ilość punktów pomiarowych. Przedstawione eksperymenty przeprowadzono dla 80-cio elementowych ciągów punktów, co odpowiada mniej więcej ruchowi trwającemu jedną sekundę.

W ten sposób uzyskujemy ciąg wartości reprezentujących zmieniającą się prędkość. Na rysunku (rys. 1) przedstawiono przykłady takich ciągów, uzyskanych dla trzech różnych osób.



Rys. 1. Przykładowe próbki danych zebrane dla trzech różnych osób

2.2. Dyskretna transformata Fouriera

Uzyskany w poprzednim etapie ciąg wartości $[v_0, v_1, \ldots, v_n, \ldots]$ reprezentuje funkcję prędkości w czasie. Celem jej dalszej analizy i zbadania rytmu zmian musimy przenieść ją do dziedziny

częstotliwości. W tym celu posłużymy się dyskretną transformatą Fouriera, zdefiniowaną w postaci [3]

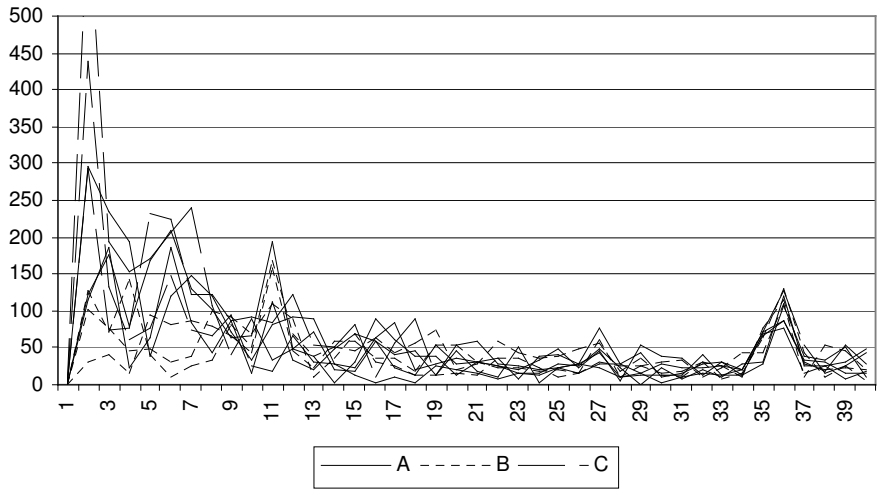
$$F_k = \sum_{n=0}^{M-1} v_n \exp\left(-j\frac{2\pi}{M}kn\right) \tag{1}$$

dla $k = 0, 1, 2, \ldots, M-1$, gdzie M oznacza liczbę wartości pobranych w poprzednim kroku algorytmu. Poszczególne składowe transformaty Fouriera tworzą wektor $\boldsymbol{F}$

$$F = [F_0, F_1 \ldots F_{M-1}] \tag{2}$$

Wektor ten opisuje nasz sygnał wejściowy przeniesiony do innej przestrzeni parametrów. Składowa zerowa F_0 transformaty Fouriera reprezentuje wartość średnią próbek pomiarowych v_n. Wyzerowanie tej wartości spowoduje przesunięcie sygnału do standardowej pozycji układu odniesienia współrzędnych. Dla wejścia rzeczywistego (jak w naszym przypadku) wartości $[F_{M/2+1}, \ldots, F_{M-1}]$ są redundantne, gdyż $\overline{F_k} = F_{M-k}$. Z tego powodu wystarczy, jeśli badaniu będzie podlegać tylko pierwsza połowa uzyskanych składowych transformaty.

Składowymi transformaty są wartości zespolone. Metoda minimalnych wartości własnych macierzy Toeplitza w przedstawionej tutaj postaci opiera się na badaniu wartości rzeczywistych. Dlatego do dalszej analizy użyte zostaną moduły poszczególnych składowych. Przykłady uzyskanych w ten sposób ciągów przedstawiono na poniższym rysunku (rys. 2).



Rys. 2. Moduły poszczególnych składowych transformaty Fouriera dla przykładowych danych

2.3. Metoda minimalnych wartości własnych macierzy Toeplitza

Klasyfikacja na podstawie uzyskanego w poprzednim kroku wektora byłaby bardzo trudna, dlatego celem lepszego wydobycia cech dokonamy jego przekształcenia zgodnie z metodą minimalnych wartości własnych macierzy Toeplitza – pozwoli to na lepszą separację wektorów z odrębnych klas, co znacznie ułatwi etap klasyfikacji.

Zgodnie z metodą opisaną we wcześniejszych pracach [4, 5, 6] sygnał podlegający rozpoznaniu zostaje przedstawiony w postaci szeregu Taylora:

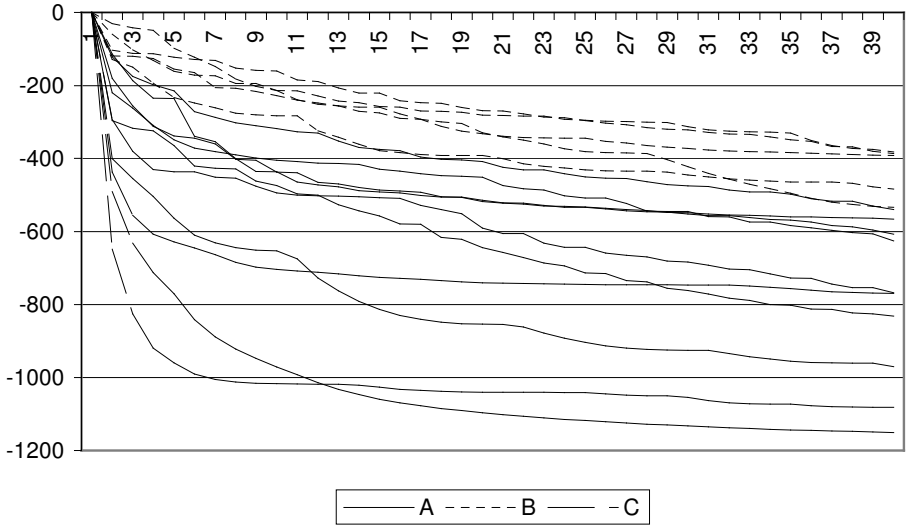
$$T(p) = c_0 + c_1 p + c_2 p^2 + \ldots + c_n p^n + \ldots \tag{3}$$

W naszym wypadku współczynnikami $c_0, c_1 \ldots c_n$ tego szeregu będą wartości uzyskane w poprzednim kroku algorytmu – czyli kolejne składowe transformaty Fouriera $[F_0, F_1 \ldots F_{M/2}]$, gdzie $n = \frac{M}{2}$. Następnie, zgodnie z algorytmem minimalnych wartości własnych [5], używamy ich do zbudowania ciągu macierzy Toeplitza. Ich wyznaczniki dane są wzorem:

$$D_i = \begin{vmatrix} c_0 & c_1 & \ldots & c_i \\ c_1 & c_0 & \ldots & c_{i-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_i & c_{i-1} & \ldots & c_0 \end{vmatrix}, \quad i = 0,\ 1,\ 2, \ldots, n \tag{4}$$

Dla kolejnych macierzy obliczamy ich minimalne wartości własne $(\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_n)$, gdzie λ_i jest najmniejszą wartością własną macierzy D_i. Uzyskujemy w ten sposób ciąg będący wektorem cech opisującym sygnał wejściowy.

Poniższy rysunek (rys. 3) przedstawia wektory charakterystyczne uzyskane dla próbek wprowadzonych przez trzy różne osoby. Jak widać, tym razem różnice między wykresami poszczególnych osób są znaczne i dają się one dobrze wyodrębnić, chociaż część z nich jest nadal nieco rozproszona.



Rys. 3. Ciągi minimalnych wartości własnych dla trzech badanych osób

2.4. Klasyfikacja

Ostatnim krokiem algorytmu jest klasyfikacja. Jest ona dokonywana na podstawie uzyskanego w poprzednim kroku wektora charakterystycznego. „Klasą" będzie konkretna osoba, która wprowadzała dane, zaś klasyfikacja ma polegać na zidentyfikowaniu tej osoby. W typowym wykorzystaniu prezentowana tu metoda może służyć do autoryzacji. Wówczas mamy ustaloną z góry liczbę klas – osób mających dostęp do chronionego zasobu. Na podstawie zarejestrowanego ruchu kursora myszy mamy ustalić tożsamość osoby i wskazać ją spośród dostępnych lub też stwierdzić, że osoby nie da się zidentyfikować.

Najważniejszym elementem tej pracy jest sam pomysł i sposób na badanie ruchów myszy oraz ekstrakcję cech kluczowych. Etap klasyfikacji ma już służyć tylko obliczeniu jej sku-

teczności. Dlatego też wybór konkretnej metody klasyfikacji jest dość dowolny. W naszej pracy wykorzystaliśmy metodę *k* Najbliższych Sąsiadów oraz Sztuczne Sieci Neuronowe.

Każda metoda klasyfikacji będzie wymagać zebrania pewnej grupy przykładów (już sklasyfikowanych próbek danych) tworzących „zbiór uczący". Na jego podstawie dokonywana będzie klasyfikacja wektorów testowych (czyli próbek, dla których przy użyciu określonej metody szukamy właściwej klasy).

Metoda *k* Najbliższych Sąsiadów należy do najprostszych metod klasyfikacji. Mając dany wektor reprezentujący testowany sygnał wyszukujemy w zbiorze uczącym *k* jego najbliższych sąsiadów. Obliczając odległość testowanego wektora od wektorów zbioru uczącego skorzystaliśmy z normy euklidesowej. Następnie stwierdzane jest, która klasa jest najliczniej reprezentowana w grupie jego *k* najbliższych sąsiadów – uznaje się, że badany wektor również zalicza się do tej klasy.

Drugą zastosowaną tutaj metodą są Sztuczne Sieci Neuronowe. To znana i sprawdzona metoda [7, 8, 9]. Pozwala ona znacznie podnieść wydajność procesu klasyfikacji, gdyż zdejmuje z nas potrzebę utrzymania i stałego przeglądania dużej bazy przykładów – są one jedynie konieczne do wytrenowania sieci. Poza tym elastyczność i zdolność do adaptacji, cechująca sieci neuronowe, pozwala radzić sobie również z przykładami, które nie były obecne w zbiorze uczącym. W naszych badaniach skorzystaliśmy z prostej, trójwarstwowej sieci bez sprzężeń zwrotnych, z sigmoidalną funkcją aktywacji. Sieć była uczona metodą propagacji wstecznej. Ilość neuronów w warstwie wyjściowej odpowiadała ilości klas (czyli ilości osób). Obecność pobudzenia na danym neuronie warstwy wyjściowej oznaczała, że badany sygnał zostawał zaliczony do tej właśnie klasy.

W sytuacji, gdy sygnał wejściowy nie może być zaliczony do żadnej z klas, należy uznać, że identyfikacja jest niemożliwa. Może to np. oznaczać, że ktoś niepowołany usiłuje uzyskać dostęp do chronionych zasobów.

3. Wyniki

Poniższa tabela prezentuje wyniki całego procesu identyfikacji przeprowadzone na niewielkiej, kilkuosobowej grupie. Poza tym przedstawiono również wyniki próby klasyfikacji (obiema metodami) danych jeszcze nieprzetworzonych oraz danych przetworzonych przy użyciu Transformaty Fouriera. Wyniki, choć znacząco gorsze, wyraźnie wskazują, że te dane pozwalają na identyfikację, zaś metoda minimalnych wartości własnych służy głównie poprawie skuteczności.

Tabela 1. Wyniki identyfikacji z użyciem zaproponowanej metody

	analizowane dane	**metoda klasyfikacji**	
		k Najbliższych Sąsiadów	**Sztuczne Sieci Neuronowe**
mysz	nieprzetworzone dane	53%	42%
mysz	składowe transformaty Fouriera	49%	52%
mysz	**minimalne wartości własne macierzy Toeplitza**	**54%**	**67%**
	klawiatura	52%	62%

Celem porównania w tabeli zawarto również wyniki eksperymentów przeprowadzonych z metodą analizy dynamiki pisania na klawiaturze, która była pierwowzorem metody proponowanej w tej pracy. Aby porównanie było rzetelne, analiza i klasyfikacja były przeprowadzone

dokładnie tym samym algorytmem, co w naszej metodzie i dla tej samej grupy badanych osób, dane zaś pobierano w zbliżony sposób – w trakcie dowolnego naciskania klawiszy.

4. Podsumowanie i plany na przyszłość

Przedstawiona w tej pracy metoda pozwoliła na uzyskanie całkiem obiecujących wyników, które wyraźnie wskazują, że może być ona z powodzeniem użyta w identyfikacji osób. Zastosowanie tej metody w realnych warunkach, dla dużej liczby osób, z pewnością będzie jednak wymagało pewnych usprawnień czy modyfikacji, na szczęście zostawia ona duże pole do dalszego rozwoju i ulepszeń, np. przez dodanie filtrów, które oczyściłyby i poprawiły jakość sygnału, badanie innych parametrów (np. kierunku lub zakresu ruchów) czy też przetestowanie innych metod ekstrakcji cech lub klasyfikacji.

Możliwości wykorzystania tej metody są szerokie – można użyć jej jako samodzielnego testu lub też połączyć z innymi (np. jako dodatkowy test w badaniu podpisu online, gdzie składanie podpisu na tablecie byłoby traktowane jako ruch myszy). Możliwe jest badanie położenia myszy w trakcie zwykłej pracy lub wykonywania z góry określonych ruchów (np. śledzenia obiektu na ekranie czy też zakreślania obwiedni widocznego kształtu), a nawet badanie jej bez wiedzy użytkownika.

Warto też nadmienić, iż jest to nowy, oryginalny pomysł, zaś praca tego typu jeszcze nigdzie nie była dotąd publikowana.

Bibliografia

[1] Joyce Rick, Gupta Gopal: Identity authorization based on keystroke latencies. Communications of the ACM, 33(2):168-176, February 1990.

[2] Monrose Fabian, Rubin Aviel: Authentication via keystroke dynamics. Fourth ACM Conference on Computer and Commmunications Security, pages 48-56, 1997.

[3] Kamen E., Heck B.: Fundamentals of signals and systems using Matlab. Prentice Hall, New York 1997.

[4] Saeed Khalid: Computer Graphics Analysis: A Method for Arbitrary Image Shape Description. MGV – International Journal on Machine Graphics and Vision, Institute of Computer Science, Volume 10, Number 2, 2001, pp. 185-194, Polish Academy of Sciences, Warsaw 2001.

[5] Saeed Khalid: Image Analysis for Object Recognition. Bialystok Technical University Press, 2004.

[6] Saeed Khalid, Tabędzki Marek: Cursive-Character Script Recognition using Toeplitz Model and Neural Networks. ICAISC'04, Lecture Notes in Computer Science, L. Rutkowski, J. Siekmann, R. Tadeusiewicz, L. Zadeh (Editors), Springer-Verlag Heidelberg, Vol. 3070, pp. 658-663, Berlin 2004.

[7] Osowski Stanisław: Sieci Neuronowe do przetwarzania informacji. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2000.

[8] Amari S. I.: Mathematical theory of neural learning. New Generation Computing. 1991. Vol. 8, pp. 281-294.

[9] Haykin S.: Neural Networks, a Comprehensive Foundation. Macmillan College Publishing Company. New York 1994.