Adam Czajka, Andrzej Pacut, "Rozpoznawanie podpisów odręcznych jako przykład systemu weryfikacji tożsamości", *Techniki Komputerowe, Biuletyn Informacyjny*, nr 1/2001, str. 7-24, Instytut Maszyn Matematycznych, Warszawa, 2001

Rozpoznawanie podpisów odręcznych jako przykład systemu weryfikacji tożsamości

Adam Czajka* i Andrzej Pacut*,**

* Politechnika Warszawska, Instytut Automatyki i Informatyki Stosowanej
ul. Nowowiejska 15/19, 00-665 Warszawa
** Naukowa i Akademicka Sieć Komputerowa NASK, ul. Bartycka 18, Warszawa
{A.Czajka,A.Pacut}@ia.pw.edu.pl

Streszczenie

Artykuł przedstawia metodologię weryfikacji i klasyfikacji podpisów odręcznych. Przedstawiony materiał rozumiany jest również jako propozycja systemu weryfikacji tożsamości do zastosowania wszędzie tam, gdzie podpis odręczny jest podstawą akceptacji transakcji. W pracy użyto tabletu graficznego do pomiaru pięciu składników podpisu w dziedzinie czasu, mianowicie położenia na płaszczyźnie, nacisku oraz kątów określających orientację pióra w trakcie pisania (elewacja i azymut, w odniesieniu do płaszczyzny tabletu). Cechy podpisu podzielone zostały na dwie grupy: cechy *widoczne*, związane z obrazem podpisu na płaszczyźnie (i z tego powodu możliwe do skopiowania przez inną osobę) oraz cechy *niewidoczne*, związane z przebiegami w czasie wszystkich składników podpisu. W pracy przeprowadzono następnie analizę skupień podpisów w przestrzeni cech w celu optymalnego podziału zbioru podpisów na podzbiory zawierające „podobne" elementy. Funkcja klasyfikująca aproksymowana została za pomocą dwóch struktur sieci neuronowych, mianowicie dwuwarstwowego nieliniowego perceptronu oraz sieci radialnej RCE. W artykule przedstawiono analizę statystyczną wyjść sieci oraz przykład zastosowania metodologii w systemie kontroli dostępu z użyciem kryptograficznej karty mikroprocesorowej.

1. Wprowadzenie

Według Słownika Języka Polskiego [1] lub Najnowszego Słownika Języka Polskiego [2] podpis oznacza *nazwisko (i imię) napisane własnoręcznie* lub *potwierdzenie pisma, nadanie mu ważności przez napisanie własnego nazwiska; podpisanie* lub *wyrażone pismem (rzadziej znakiem lub znakami) określenie tożsamości piszącego lub stawiającego znaki.* Dla nas najistotniejszymi wydają się być znaczenia drugie i trzecie, które eksponują szersze znaczenia słowa podpis, mianowicie podkreślają fakt o dynamicznym charakterze zjawiska jak również o możliwości określenia tożsamości piszącego na bazie jego podpisu.

Realizacje tego samego podpisu nie są identyczne. Zbiór wszystkich możliwych realizacji tego samego podpisu obejmuje zatem realizacje podpisu różniące się pomiędzy sobą. Różnica między tymi znaczeniami to różnica między elementem zbioru a całym zbiorem. Rozróżnienie pomiędzy tymi dwoma znaczeniami jest istotne w naszej pracy, przy czym zachowamy słowo *podpis* dla zbioru, a jego elementy będziemy nazywać *realizacjami podpisu* (dla skrócenia notacji w dalszej części pracy będziemy używać oznaczenia rp). Innymi słowy

$$Z = \{z\} \tag{1}$$

gdzie z oznacza realizację podpisu, nawiasy klamrowe oznaczają zbiór elementów, zaś Z jest podpisem, a więc rodziną wszystkich możliwych realizacji podpisu. Zauważmy ponadto, że ta sama osoba może mieć kilka różnych typów podpisu, np. „czytelny", „nieczytelny", „długi" (imię i nazwisko), „krótki" (tylko nazwisko), „inicjały", itd. Z naszego punktu widzenia każdy z tych typów stanowi oddzielny podpis.

W zagadnieniach rozpoznawania i klasyfikacji podpisów, realizacje podpisu są obserwowane za pomocą urządzeń pomiarowych. Załóżmy najpierw w najbardziej ogólny sposób, że w trakcie procesu podpisywania jesteśmy w stanie rejestrować szereg wielkości związanych z tym procesem. Należeć do nich mogą nie tylko współrzędne (pozioma i pionowa) końcówki pióra, ale także nacisk pióra na papier, kąt położenia pióra, siła uchwycenia pióra, pozycja chwytu, i inne. Tak szeroko rozumiany podpis można przedstawić jako wielowymiarową funkcję

$$Z = [z_1, z_2, \ldots, z_J] : \; T \mapsto R^I \tag{2}$$

gdzie J oznacza liczbę mierzonych wielkości, zaś T jest zbiorem chwil pomiarowych. Funkcja ta jest jednoznacznie określona poprzez I jednowymiarowych funkcji jednej zmiennej. Wykresem omawianej funkcji jest więc krzywa **z** w przestrzeni $R^{(1+J)}$, przy czym „zerowa" współrzędna odpowiada czasowi, zaś pozostałe J

współrzędnych odpowiada kolejnym wielkościom mierzonym. Oznaczmy przez $z_{p,q,\ldots,r}$ rzut wykresu Z na podprzestrzeń odpowiadającą współrzędnym p, q, ..., r. W rezultacie

$$z_{t,s_1,s_2} \tag{3}$$

odpowiada sytuacji, w której zachowuje się tylko dwie pierwsze wielkości mierzone (np. pomiary współrzędnych z_1, z_2 położenia końcówki pióra na płaszczyźnie), natomiast

$$z_{s_1,\ldots,s_J} \tag{4}$$

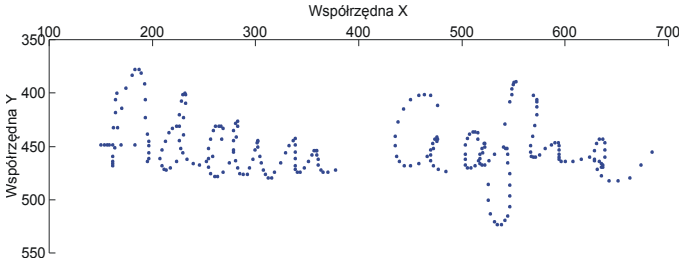
jest krzywą „parametryczną" w której zachowuje się wszystkie wielkości mierzone ale eliminuje czas. W rezultacie

$$z_{s_1,s_2} \tag{5}$$

odpowiada „rysunkowi" standardowego podpisu na płaszczyźnie. Widać tutaj jak ograniczona jest informacja w przypadku podpisu „już napisanego". Zauważmy jeszcze, że kolejność wykonywania operacji rzutowania nie ma znaczenia. Typowo T jest zbiorem dyskretnym, zatem każdą realizację podpisu z można zapisać w postaci macierzy o rozmiarze $J \times N$ gdzie N oznacza liczność T.

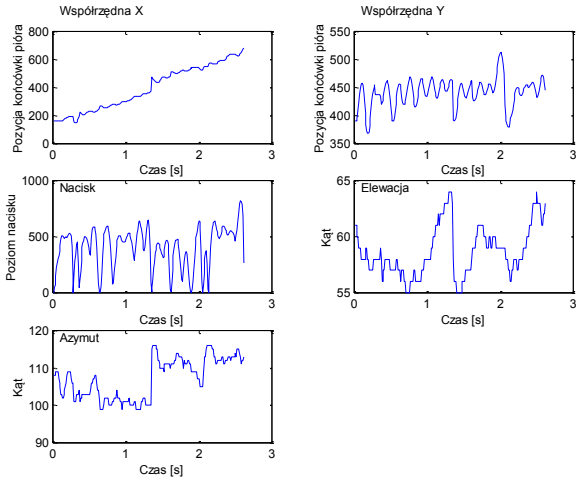
Reasumując powyższe rozważania podkreślamy, że istotne jest rozróżnianie podpisu (zbioru) od realizacji podpisu (elementu zbioru). Realizacje podpisu są wielowymiarowymi krzywymi jednowymiarowego argumentu (czas). Każda z tych krzywych jest jednoznacznie określona przez jej wykres, zaś znaczenie praktyczne mają także rzuty wykresów rp na wybrane podprzestrzenie. W szczególności, „podpis skanowany" jest rzutem wykresu rp na płaszczyznę xy.

Rysunek 1 prezentuje podpis skanowany jednego z autorów pracy, na rysunku 2 przedstawione są natomiast wykresy wszystkich składników rp w dziedzinie czasu, czyli - stosując przyjętą w artykule terminologię - są to rzuty tego samego wykresu rp na podprzestrzenie dwuwymiarowe, gdzie każda podprzestrzeń reprezentowana jest przez czas i jeden składnik rp (położenie, nacisk, orientacja).



Rysunek 1 Przykład rzutu rp na podrzestrzeń s_1,s_2 (podpis skanowany).

Oprócz podpisu, rozumianego jako zbiór wszystkich realizacji podpisów danego typu danej osoby, wprowadzimy dodatkowo specjalizowane podzbiory tego zbioru. Przez podpis referencyjny Z_r będziemy rozumieli zbiór (jednego lub kilku) rp złożonych przez tę osobę jako podpisy odniesienia, względem których należy oceniać inne podpisy tej osoby. Przez podpis testujący Z_t rozumiemy zbiór rp złożonych przez tę osobę, a nie zawartych w podpisie referencyjnym. Przez podpis sfałszowany Z_f będziemy rozumieć zbiór rp które wykonane zostały przez inną osobę niż ta związana z podpisem Z.



Rysunek 2 Wykresy składników realizacji podpisu z rys. 1.

Dla porównania wyników klasyfikacji i weryfikacji będziemy stosować kilka standardowych wskaźników. Wskaźnik *FRR* (ang. ***F**alse **R**ejection **R**ate)* oznacza stopień błędnego odrzucania przez system podpisów właściwych, *FAR* (ang. ***F**alse **A**cceptance **R**ate)* oznacza stopień błędnej akceptacji

przez system podpisów sfałszowanych, natomiast *CCR* (ang. ***C**orrect **C**lassification **R**ate*) oznacza stopień poprawnej klasyfikacji podpisów właściwych ale nieznanych w procesie uczenia systemu. Wskaźniki te są zależne od siebie. Punkt przecięcia FAR oraz FRR jako wykresów w funkcji parametru oznaczany jest przez *ERR* (ang. ***E**qual **E**rror **R**ate*).

W pracy rozpatrujemy dwa zagadnienia: klasyfikacji oraz weryfikacji podpisów. W obu procesach zakładamy znajomość przynależności rp do odpowiednich podpisów. Jednakże w procesie *klasyfikacji* musimy estymować przynależność każdej realizacji ze zbioru Z_t na wejściu systemu do odpowiedniego podpisu Z, natomiast w procesie *weryfikacji* każda realizacja z Z_t oraz z Z_f jest opatrzona hipotezą przynależności do danego podpisu Z, a następnie hipoteza ta jest testowana. Oba problemy były już rozwiązywane [3,6,9,10] z zastosowaniem podpisów skanowanych. Jednakże do stworzenia systemu weryfikacji, któremu postawiono wysokie wymagania co do minimalnej liczby akceptacji podpisów fałszywych (czyli małej wartości współczynnika *FAR*), należy posiadać informacje nt. samego procesu podpisywania. Stąd też w pracy użyto tabletu graficznego, za pomocą którego rejestrowanych jest pięć składników podpisu w czasie, mianowicie: położenie (s_1,s_2), nacisk (s_3) i orientacja pióra (elewacja s_4 i azymut s_5) w odniesieniu do powierzchni tabletu. Pomiary te pozwalają na wyekstrahowanie cech podpisów umożliwiających zarówno na ich klasyfikację jak i weryfikację. Zbiór cech jest poddawany wstępnej analizie, dzięki której następuje eliminacja cech liniowo skorelowanych. Przestrzeń cech podzielona została na regiony, w obrębie których aproksymowane są funkcje klasyfikujące, po jednej dla każdego regionu. Podczas podziału przestrzeni cech zastosowano analizę skupień bazującą na drzewach rozpinających (ang. *spanning trees*) oraz hierarchicznych drzewach skupień (ang. *hierarchical cluster trees*).

2. Istniejące rozwiązania

Rozwiązania problemów weryfikacji i klasyfikacji podpisów podzielić można na bazie wymiarowości informacji dostępnej podczas procesu pisania, mianowicie: podejście *statyczne* bazujące na analizie skanowanych podpisów, oraz podejście *dynamiczne*, zakładające dostępność informacji zależnej od czasu w formie danych w p-wymiarowej przestrzeni, gdzie $p=\{3,4,5,6\}$.

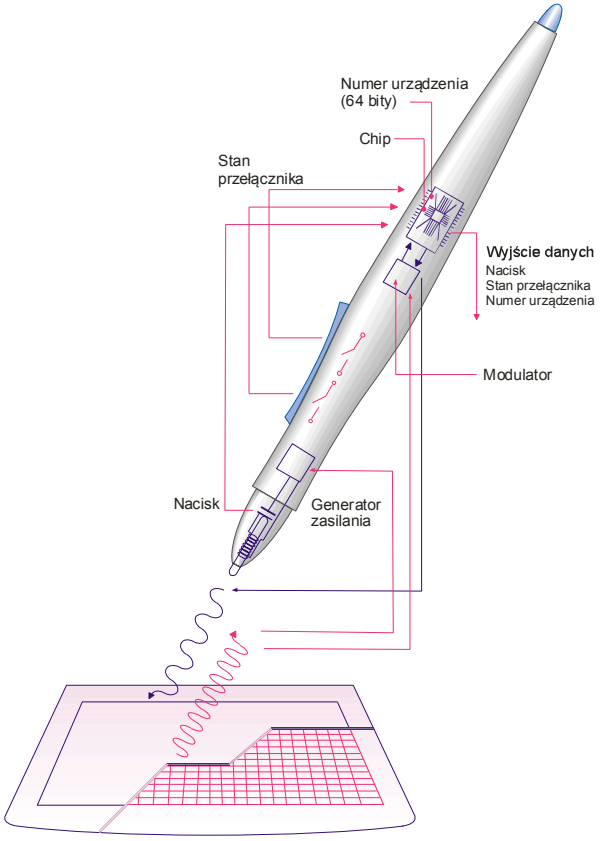
Podejście statyczne stosowane jest z reguły bez użycia specjalistycznego sprzętu. Danymi wejściowymi są tu podpisy skanowane ($z_{s1,s2}$). W pracy Dimauro *et al.* [3] zaprezentowano system weryfikacji podpisów składanych na czekach bankowych. Pierwszym krokiem jest lokalizacja skanowanego podpisu, następnie przekształcenie obrazu tak aby był on niezależny od orientacji i skali. Każdy przekształcony w powyższy sposób obraz dzielony jest następnie na spójne segmenty. Weryfikacja przeprowadzana jest na bazie 6 globalnych cech (wyliczanych dla całego obrazu) i 16 cech wyliczanych w obrębie każdego z segmentów. System składa się z trzech ekspertów głosujących za lub przeciw przyjęciu hipotezy o oryginalności złożonego podpisu. Rezultatem jest FRR = 22% oraz FAR = 3.9%. W pracy Lee i Pan [4] zaprezentowano metodologię śledzenia procesu podpisywania na podstawie skanowanego podpisu. Pierwszym krokiem jest zamiana obrazu na szkielet o szerokości jednego piksela. Szkielet ten jest następnie zamieniany na sekwencję krzywych, w obrębie których znajdowane są punkty charakterystyczne, tj. maksima, minima, punkty początkowe i końcowe. Punkty te, a dokładnie macierz kowariancji powstała na ich bazie, jest następnie wykorzystywana podczas normalizacji każdego z podpisów (uniezależnienie od rotacji, przesunięcia oraz skali).

Podejścia dynamiczne klasyfikować można na bazie wymiarowości obserwacji. Metodologia w ogólności nie zależy natomiast od wymiaru przestrzeni obserwacji. Ciekawą pracą wykorzystującą pomiary wyłącznie położenia pióra w czasie pisania ($z_{t,s1,s2}$) jest modelowanie procesu fałszowania podpisu. Brault i Plamondon [5] zaproponowali model bazujący na systemie nerwowo-mięśniowym. Zadanie fałszowania podpisu jest tutaj modelowane jako sekwencja podzadań. W obrębie każdego podzadania imitowany jest jeden *element fundamentalny podpisu*, definiowany jako sekwencja trzech pociągnięć pióra: krzywoliniowe – ostrokątne – krzywoliniowe. Podzadanie składa się natomiast z przestrzennej percepcji celu danego podzadania (układ nerwowo-wzrokowy), przygotowania podzadania (mózg) oraz jego wykonania (układ nerwowo-mięśniowy). Z racji nakładania się części podzadań w czasie, zapewniona jest ciągłość modelowania. W pracy Lee *et al.* [6] zaprezentowano system weryfikacji podpisów bazujący na indywidualnych cechach definiowanych dla każdego $z_{t,s1,s2}$ (10-15 cech) dających ich najlepsze zróżnicowanie w przestrzeni cech. Cechy indywidualne wybierane są ze zbioru 40 cech wspólnych dla wszystkich podpisów, opisujących zarówno ich statyczne jak i dynamiczne właściwości. W pracy zastosowano system podejmujący decyzję o oryginalności realizacji podpisu na bazie kilku kryteriów rozpatrywanych osobno przez zespół głosujących ekspertów. Pomiary $z_{t,s1,s2,s3}$ otrzymujemy poprzez dodatkową - w stosunku do $z_{t,s1,s2}$ - obserwację nacisku pióra podczas procesu pisania. Crane i Ostrem [7] wykorzystali ten typ obserwacji do konstrukcji systemu weryfikacji bazującego, podobnie do poprzedniego przykładu, na wyborze indywidualnych cech $z_{t,s1,s2,s3}$ spośród 44 cech wspólnych. Optymalny wybór cech indywidualnych wyznaczany jest tutaj przez minimalizacją ERR przeprowadzaną dla każdego podpisu.

Rozwiązanie, choć prowadzące do dobrych rezultatów (ERR=0.5% na przeciw ERR=1.75% przy zastosowaniu tego samego zestawu cech dla wszystkich $z_{t,s1,s2,s3}$) jest dość kłopotliwe z praktycznego punktu widzenia, gdyż wymaga dużej liczby realizacji podpisu (około 100 dla jednego podpisu) do prawidłowego rozpoznania najlepszego (w sensie minimalizacji ERR) zestawu cech. Dwa komercyjne systemy weryfikacji podpisów, Signplus [9] i Cybersign [10] również bazują na obserwacjach trzech składników podpisu w czasie. Jednakże największą wiedzę o procesie podpisywania otrzymujemy obserwując proces w pięciu wymiarach, mianowicie obok położenia i nacisku obserwowana jest również orientacja pióra, wyrażona za pomocą dwóch kątów (względem powierzchni tabletu): elewacji i azymutu. Pięciowymiarowe obserwacje użyto w pracy Wessels i Omlin [8], w której zaproponowano, podobnie jak w kilku poprzednich pracach, system hybrydowy składający się tutaj z ukrytych modeli Markowa (ang. *Hidden Markov Model*) oraz samoorganizujących się sieci Kohonena (ang. *Kohonen Self Organizing Map*). Po ustaleniu parametrów systemu dla których FRR=0%, system zaakceptował 13% fałszywych podpisów (FAR=13%).

3. Stanowisko badawcze oraz kolekcja podpisów

Pomimo tego, że proces podpisywania zależny jest od osobowości, przyzwyczajeń osoby czy też podświadomego wyćwiczenia pewnych ruchów realizowanych przez układ nerwowo-mięśniowy, kolejne realizacje podpisu będą różniły się od siebie w zależności od istniejących warunków pisania. Z drugiej strony te właśnie zmiany powodują że nasz estymowany model procesu podpisywania jest pełniejszy. Z tej przyczyny każdy podpis powinien być kolekcjonowany przez możliwie najdłuższy okres, a każda nowa realizacja podpisu powinna reprezentować inną sytuację. Chcielibyśmy również aby przykładów przeznaczonych do uczenia systemu było jak najwięcej. Musimy jednak mieć na uwadze fakt, że rzadko mamy możliwość kolekcjonowania dużej liczby realizacji składanych przez jedną osobę, dlatego projektowany przez nas system powinien zachowywać jak najlepsze właściwości również w przypadku gdy jesteśmy ograniczeni dostępnością bądź cierpliwością użytkowników, co prowadzi do arbitralnego ograniczenia od 3 do 6 dostępnych realizacji podpisu od jednej osoby. Może się zdarzyć, że osoba podpisuje się na kilka sposobów (czyli odpowiadają jej dwa różne podpisy, nie realizacje podpisu). Jak wcześniej już powiedzieliśmy, w takim przypadku definiujemy kilka różnych podpisów dla tej samej osoby.

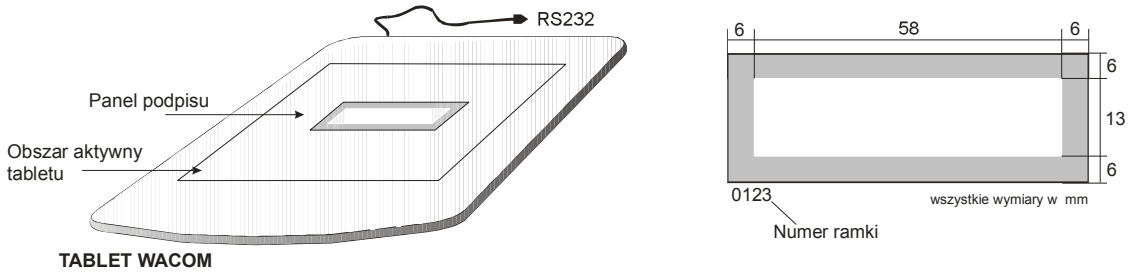


Rysunek 3 Tablet WACOM wraz z bezprzewodowym piórem

Podczas naszych eksperymentów zbieraliśmy nie więcej niż dwie realizacje podpisu od jednej osoby w ciągu dnia. W większości przypadków podczas rejestracji nowej realizacji występowały inne warunki procesu pisania, mianowicie zmęczenie pod koniec dnia, energia o poranku, zdenerwowanie przed egzaminem i odprężenie po nim, zmęczenie po ćwiczeniach fizycznych, pośpiech, radość i smutek.

Realizacje podpisu rejestrowane są za pomocą tabletu graficznego WACOM oraz piszącego, bezprzewodowego pióra (rys.3). Na tablecie umieszczono specjalnie przygotowaną *ramkę*, tworząc w ten sposób *panel podpisu* (rys.4). Jej wymiary zbliżone są do wymiarów ramek występujących na potwierdzeniach transakcji dokonanych kartą płatniczą. Poza tym, biały prostokąt wewnątrz większego szarego oraz czarna ramka obejmująca oba prostokąty sugeruje miejsce złożenia podpisu. Te zasady nie były jednak obligatoryjne dla uczestników eksperymentu i nie były im przedstawiane, każdy mógł złożyć podpis w dowolnym miejscu obszaru aktywnego tabletu. Kilku uczestników złożyło podpisy, które wyraźnie i świadomie wykraczały poza czarną ramkę. Urządzenie umożliwia pomiary położenia, nacisku i orientacji pióra z częstotliwością 100Hz. Przy każdej

rejestracji nowej rp właściciel podpisujący się na kilka sposobów deklarował rodzaj podpisu, mianowicie nazwisko, imię + nazwisko lub inicjały. Każdy wariant jest traktowany jako odrębny podpis tej samej osoby.



Rysunek 4 Tablet graficzny jako panel podpisu oraz szczegóły ramki podpisu

Na potrzeby eksperymentu zebraliśmy 359 rp złożonych przez 37 osób. Realizacje te pogrupowane zostały następnie w 48 podpisów. Baza danych podzielona została na zbiór uczący, składający się z 48 podpisów referencyjnych (299 rp) oraz 48 podpisów testowych (48 rp). Dodatkowo, utworzono 9 podpisów sfałszowanych (12 rp). Do fałszowania podpisów poproszono kilka osób, które mogły przygotować się do ostatecznej próby fałszowania przez dowolny okres czasu (nawet kilka dni) dysponując bazą 299 wykresów rp zrzutowanych na płaszczyznę xy (skanowanych rp). Każda osoba wybrała jeden lub dwa podpisy, które z ich punktu widzenia były najłatwiejsze do imitacji.

4. Od obserwacji do zestawu cech

4.1 Wybór cech

Projektowanie systemu zaczęto od wyboru zbioru cech opisujących jak najlepiej podpis każdej z osób. Z racji dążenia do jak najmniejszego zbioru (ze względów praktycznych), rozpatrywano następujące cechy

Długość podpisu rozumiana jako liczba punktów pomiarowych *N* dla każdej rp.

Wartości średnie składników rp odpowiadające wartościom średnim wyliczonym dla każdego składnika $s_1,...,s_5$ realizacji *z*, mianowicie

$$\overline{s_j} = \frac{1}{N}\sum_{k=1}^{N} s_j(k), \quad j = 1,...,5 \tag{6}$$

Odchylenia standardowe składników rp

$$\sigma_j = \sqrt{\overline{s_j^2} - \overline{s_j}^2}, \quad j = 1,...,5 \tag{7}$$

Współczynniki trendu składników rp, mianowicie współczynniki nachylenia α_j prostej regresji dla każdego składnika rp. Prosta regresji dana jest wzorem

$$s_j^0 = \overline{s_j} - \alpha_j k, \quad j = 1,...,5 \tag{8}$$

gdzie

$$\alpha_j = 12\frac{\overline{\overline{s_j}} - 0.5(N+1)\overline{s_j}}{N^2 - 1} \qquad \overline{\overline{s_j}} = \frac{1}{N}\sum_{k=1}^{N} k s_j(k)$$

W dalszych obliczeniach posługiwać się będziemy składnikami podpisu z usuniętym trendem, mianowicie

$$s_j^* = s_j - s_j^0, \quad j = 1,...,5 \tag{9}$$

Wartości i wektory własne macierzy inercji. Macierz inercji **Γ** dwóch składników jest tożsama z macierzą kowariancji tych składników, mianowicie

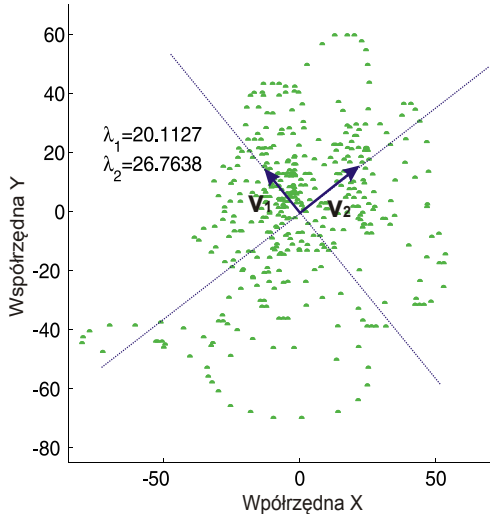
$$\Gamma = \begin{bmatrix} \overline{s_1^{*2}} & \overline{s_1^* s_2^*} \\ \overline{s_1^* s_2^*} & \overline{s_2^{*2}} \end{bmatrix} \tag{10}$$

Jako cechy podpisów używane są pierwiastki kwadratowe wartości własnych $\lambda_1 \geq \lambda_2$ macierzy **Γ.** Rysunek 5 przedstawia rzut rp na podprzestrzeń s_1^*, s_2^*. Na rysunku zaznaczono również dwa ortogonalne wektory własne o długościach pierwiastków kwadratowych odpowiednich wartości własnych.

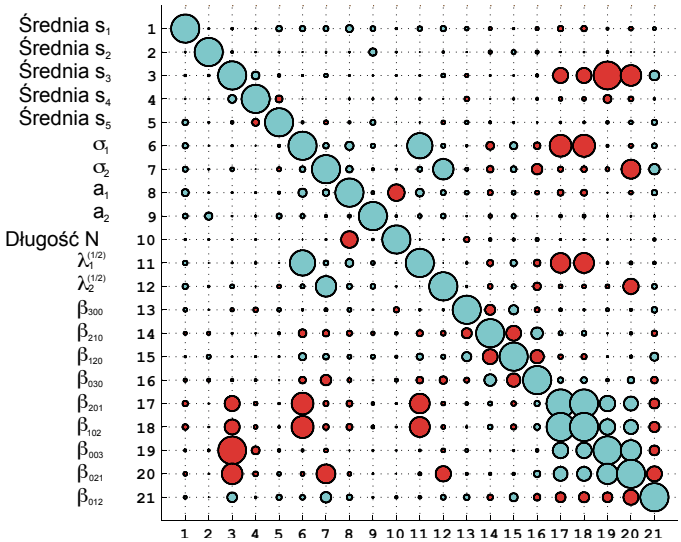
Trzecie momenty centralne. W pracy przebadano również trzecie momenty centralne położenia (s_1^*, s_2^*) i nacisku (s_3^*), mianowicie

$$\beta^3{}_{p,q,r} = \frac{1}{N}\sum_{k=1}^{N}(s_1^*(k))^p(s_2^*(k))^q(s_3^*(k))^r \tag{11}$$

gdzie $p+q+r = 3$, $p,q,r = 0,1,2,3$, które związane są z orientacją krzywej w 3-wymiarowej przestrzeni obserwacji. Aby skalę wszystkich cech zachować na tym samym poziomie, w dalszych badaniach wykorzystano pierwiastki sześcienne wartości trzecich momentów ($\beta_{p,q,r}$).



Rysunek 5 Realizacja podpisu zrzutowana na podprzestrzeń składników s_1^*, s_2^* (po usunięciu trendu liniowego)



Rysunek 6 Macierz korelacji cech w postaci graficznej. Kółka jaśniejsze oznaczają korelację dodatnią, ciemniejsze - ujemną.

Należy zwrócić uwagę, że wyłącznie cztery cechy z powyżej wprowadzonych, mianowicie wartości średnie oraz odchylenia standardowe położenia pióra, mogą być wyznaczone dzięki obserwacji wyłącznie podpisów skanowanych. Te cechy nazywać będziemy *cechami widocznymi*. Do wyliczenia pozostałych niezbędna jest obserwacja procesu podpisywania, stąd też pozostałe cechy nazywać będziemy *cechami niewidocznymi*.

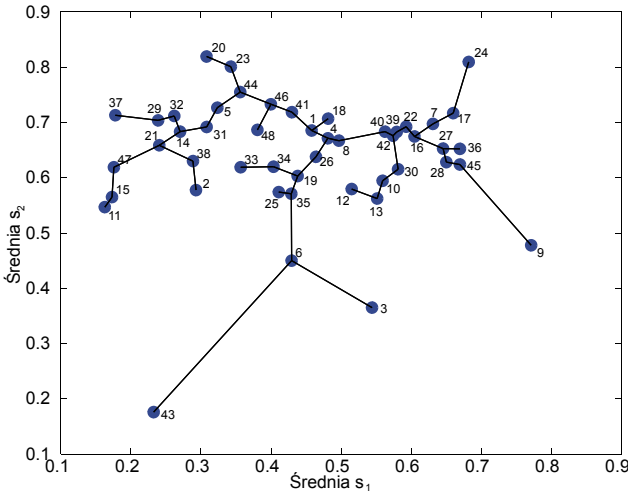
4.2 Minimalny zestaw cech

Tabela 1 Wyjściowy zbiór cech oraz zredukowany zbiór cech realizacji podpisu

Cecha	Zbiór wyjściowy	Zbiór zredukowany
Długość	N	N
Wartości średnie składników	$\overline{s_1},\ldots,\overline{s_5}$	$\overline{s_1},\ldots,\overline{s_5}$
Odchylenia standardowe składników	σ_1,σ_2	σ_1,σ_2
Pierwiastki wartości własnych macierzy inercji	$\sqrt{\lambda_1},\sqrt{\lambda_2}$	—
Współczynniki trendu	$\alpha_1,\ldots,\alpha_5$	α_2
Pierwiastki sześcienne trzecich momentów	$\beta_{300},\beta_{210},\ldots,\beta_{003}$	$\beta_{300},\beta_{120},\beta_{012}$

Pierwotny zestaw cech (tab. 1) wybrany został w oparciu o relatywnie małą bazę danych. Zbiór ten może zostać rozszerzony o cechy opisujące podpis bardziej szczegółowo, w szczególności o cechy opisujące lokalne właściwości dynamiczne podpisu. Z drugiej jednak strony zwiększanie wymiarowości przestrzeni cech powoduje większe trudności podczas uczenia sieci klasyfikującej. Z tego też względu należy starać się dobrać takie cechy do zbioru finalnego, które nie wnoszą tej samej informacji, czyli nie są ze sobą skorelowane. Po wyznaczeniu macierzy korelacji okazuje się, że proponowany zbiór pierwotny zawiera cechy liniowo skorelowane. Rysunek 6 przedstawia macierz korelacji w postaci graficznej. Zbiór ostateczny powstał przez odrzucenie cech, dla których wartość bezwzględna współczynnika korelacji przekraczała, arbitralnie przyjęty, *próg korelacji* wynoszący 0.4. Z racji niejednoznaczności wyboru „silnie skorelowanych" cech, odrzucamy te cechy, których obliczenie jest bardziej złożone. Dla przykładu, wartości własne macierzy inercji oraz odchylenia standardowe odpowiednich składników wykazują korelację na poziomie 0.9; w tym przypadku zrezygnowaliśmy z wartości własnych macierzy. Procedura ta doprowadziła do finalnego zbioru 12 cech (tab. 1). W pracy nie stosowano metod detekcji korelacji nieliniowych, a powstały zbiór cech używany był w procesach zarówno klasyfikacji jak i weryfikacji.

5 Od cech podpisu do funkcji klasyfikującej. Analiza skupień podpisów.



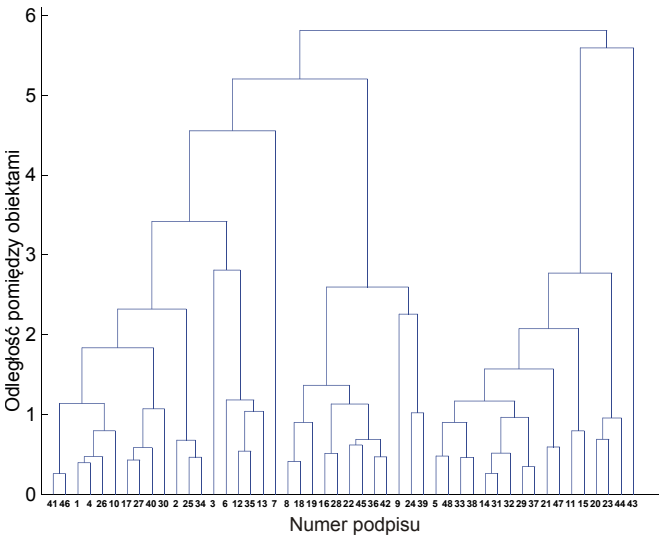
Rysunek 7 Drzewo rozpinające w przestrzeni dwóch cech (położenie s_1,s_2)

Rozkład podpisów, rzutowany na przestrzeń cech, może okazać się niejednorodny. Część podpisów może leżeć blisko siebie, wykazując podobieństwa dla pewnego podzbioru cech, inne zaś będą różnić się we wszystkich wymiarach. Pamiętajmy, że funkcja klasyfikująca aproksymowana jest na podstawie wektorów z przestrzeni cech, i takie niejednorodne ułożenie obiektów może prowadzić do złej aproksymacji funkcji klasyfikującej. Z tego powodu istotnym elementem systemu weryfikacji podpisów jest analiza skupień podpisów. Dzieląc przestrzeń cech na podobszary o zbliżonych wartościach cech, otrzymujemy klasy podpisów o podobnych właściwościach. W ten sposób otrzymujemy nie jedną ale klika funkcji klasyfikujących, które aproksymowane są w obrębie każdego podobszaru, co zapewnia mniejsze błędy aproksymacji i, co za tym idzie, lepszą klasyfikację i weryfikację.

Ważnym elementem analizy skupień jest wybór cech (ze zbioru finalnego) na bazie których dokonywany będzie podział oraz klasyfikacja bądź weryfikacja. Zauważmy, że w obu przypadkach nie muszą to być te same podzbiory cech. Podczas eksperymentów najlepsze wyniki weryfikacji otrzymano dla przypadku podziału podpisów w grupy wyłącznie na bazie cech widocznych, a następnie analizy dyskryminacyjnej w obrębie każdej z grup na bazie cech niewidocznych. Takie postępowanie jest intuicyjnie zrozumiałe: cechy widoczne to, jak wcześniej wspomniano, cechy których estymacja jest możliwa dzięki obserwacji podpisu skanowanego. Fałszerz, starając się upodobnić swoją próbę imitacji do podpisu widniejącego na papierze, nie będzie mógł natomiast sfałszować cech wyznaczanych na bazie pozostałych składników podpisu, czyli nacisku, orientacji

pióra i przede wszystkim czasu. Taki sposób podziału podpisów prowadzi do dobrych aproksymacji funkcji klasyfikującej określonej na podprzestrzeni cech niewidocznych w obrębie każdego podpisu.

W pracy zastosowaliśmy dwa algorytmy grupowania podpisów w skupienia, mianowicie algorytm oparty na drzewach rozpinających oraz hierarchicznych drzewach skupień. W obu przypadkach liczony jest centroid podpisu na podstawie wszystkich składających się na niego realizacji podpisu.



Rysunek 8 Dendrogram podpisów. Analiza dla przestrzeni 12 cech (zbiór finalny cech, tab. 1)

Pierwszy z algorytmów konstruuje drzewo rozpinające nie skierowany graf pełny, którego węzłami są centroidy podpisów a długości łuków odpowiadają odległości (euklidesowej) pomiędzy centrami (rys. 7). Przecięcie *k-1* najdłuższych łuków w tak powstałym drzewie prowadzi do *k* podzbiorów podpisów podobnych. Wybranie arbitralnego progu oznaczającego największą dopuszczalną odległość pomiędzy centroidami podpisów oraz przecięcie wszystkich łuków o długości większej od wybranego progu również prowadzi do poddrzew rozpinających, jednakże ich liczba nie może być z góry określona. Strategia postępowania pozostaje w gestii projektanta systemu, w tej pracy stosowano pierwszą z nich: w procesie weryfikacji przestrzeń cech podzielono na cztery podprzestrzenie, w procesie klasyfikacji natomiast podprzestrzeni jest sześć.

Drugi z algorytmów łączenia podpisów w skupienia, dający w rozpatrywanym zagadnieniu lepsze rezultaty aproksymacji funkcji klasyfikującej, polega na budowie binarnego, hierarchicznego drzewa na bazie macierzy odległości. Liście binarnego drzewa hierarchicznego reprezentują pojedyncze podpisy, stanowiące punkt wyjścia do konstrukcji skupień. Elementy łączone są parami na bazie najprostszego algorytmu najbliższego sąsiada (ang. *nearest neighbor*). Para zgrupowanych podpisów tworzy obiekt, który może zostać dołączony do innego obiektu w dalszych iteracjach algorytmu, tworząc następne skupienie podpisów. Rys. 8 przedstawia wynik algorytmu konstrukcji drzewa binarnego w postaci *dendrogramu*. Macierz podobieństwa (odległości) podpisów zrzutowanych na przestrzeń cech bazuje u nas na odległości d(x,y) Mahalanobisa, mianowicie $d^2(x,y)=(x-y)^T\mathbf{C}^{-1}(x-y)$ gdzie **C** jest macierzą kowariancji cech podpisów. Podając następnie najdłuższą, dopuszczalną odległość pomiędzy obiektami, połączenia przekraczające to ograniczenie zostają przecięte. Powstałe w ten sposób poddrzewa reprezentują kolejne skupienia obiektów.

Innym sposobem podziału drzewa hierarchicznego w skupienia jest wykorzystanie *współczynnika niespójności* κ (ang. *inconsistent coefficient*). Współczynnik ten charakteryzuje każde połączenie w dendrogramie poprzez porównanie jego długości ze średnią długością połączeń w poddrzewie wskazującym przez dany łuk. Wartość κ obliczana jest natępująco

$$\kappa = \frac{L_k - \overline{L_k}}{\sigma_L(k)} \tag{12}$$

gdzie L_k oznacza długość rozważanego łuku *k*, $\overline{L}_k$ oznacza średnią długość wybranych połączeń (liczba połączeń w poddrzewie o korzeniu w węźle wskazującym przez łuk *k*), natomiast $\sigma_L(k)$ oznacza odchylenie standardowe wybranych połączeń w tym poddrzewie. Liściom drzewa przypisana jest wartość κ=0. W algorytmie można dobierać poziom zagłębienia obliczeń, lecz nie trudno zauważyć, że musi on być większy bądź równy 2. Dla „silnie niespójnych" połączeń wartość współczynnika jest bliska 1, dla połączeń charakteryzujących się zbliżoną długością w porównaniu do rozpatrywanych połączeń w poddrzewie, wartość współczynnika jest bliska 0. Określając maksymalną wartość niespójności połączeń, algorytm przecina wszystkie łuki wykraczające poza to ograniczenie. Prowadzi to, podobnie jak w przypadku przecinania najdłuższych połączeń, do poddrzew binarnych reprezentujących skupienia podpisów.

6 Wyniki klasyfikacji i weryfikacji podpisów

6.1 Klasyfikacja.

Dla potrzeb klasyfikacji, podpisy podzielone zostały na 6 grup (skupień). W obrębie każdej grupy utworzony został odrębny klasyfikator neuronowy (perceptron dwuwarstwowy, obie warstwy nieliniowe, 2K+1 neuronów ukrytych, K neuronów wyjściowych, K jest liczbą podpisów w danym skupieniu). Na wyniki eksperymentów silny wpływ miała liczba realizacji podpisów składających się na dany podpis. Dlatego przeprowadzono próby uczenia z zastosowaniem 1,2,3 oraz 4 rp dla każdego podpisu (tab. 2). Podczas właściwych eksperymentów mieliśmy do dyspozycji podpisy reprezentowane przez 4-8 realizacji. W takim przypadku CCR=95.8%.

Tabela 2 Wyniki klasyfikacji dla różnej liczby rp reprezentujących podpis

liczba rp reprezentujących podpis	błąd klasyfikacji (100% - CCR)
1	36.5%
2	25.0%
3	16.7%
4	12.5%
4-8	4.2%

6.2 Weryfikacja.

W przypadku weryfikacji zbiór podpisów podzielony został na cztery skupienia (w przestrzeni 4-wymiarowej na bazie cech widocznych), a weryfikacja odbywała się z wykorzystaniem wyłącznie cech niewidocznych (w obrębie utworzonego skupienia). Podobnie jak w przypadku klasyfikacji, dla każdego skupienia stworzony został klasyfikator neuronowy. Niezbędnym okazało się zastosowanie analizy statystycznej wyjść sieci neuronowej w celu akceptacji lub odrzucenia hipotezy o przynależności danej realizacji do podpisu. Analizie poddano wyjścia $O^{(1)}$ oraz $O^{(2)}$ dwóch „zwycięskich" neuronów (czyli tych, których wyjścia miały największe wartości). Aby hipoteza *realizacja podpisu na wejściu sieci neuronowej nie jest sfałszowana* została zaakceptowana, wyjścia owych „zwycięskich" neuronów muszą spełniać następujące nierówności

$$\begin{aligned} O^{(1)} &\geq m_1 - \frac{\varsigma_1 t_\alpha}{\sqrt{N}} \\ O^{(2)} &\leq m_2 + \frac{\varsigma_2 t_\alpha}{\sqrt{N}} \end{aligned} \tag{13}$$

gdzie m_k oznacza średnią wartość wyjścia neuronu zajmującego *k*-te miejsce w rankingu dla sieci stymulowanej przez wszystkie rp należące do danego podpisu, ς_k oznacza odchylenie standardowe wyjścia *k*-tego neuronu a *N* jest liczbą rp dla badanego podpisu. Przez t_α oznaczyliśmy α-kwantyl rozkładu t-Studenta o *N* - 1 stopniach swobody zmiennej losowej $\mathbf{t}_N$, mianowicie $P\{|\mathbf{t}_N| \geq t_\alpha\} = \alpha$ dla zadanego poziomu ufności α. Takie podejście prowadziło do FAR = 0% lecz FRR = 22%, co spowodowane jest zbyt małą liczbą niezależnych obserwacji (czyli realizacji podpisu od jednej osoby) wyznaczającej stopień swobody rozkładu t-Studenta. Postanowiliśmy więc zamienić wyrażenie $t_\alpha / \sqrt{N}$ przez stały czynnik $\gamma = 15$ co dało wyniki FAR = 0% i FRR = 11.11%.

6.3 Klasyfikacja i weryfikacja dla sieci RCE

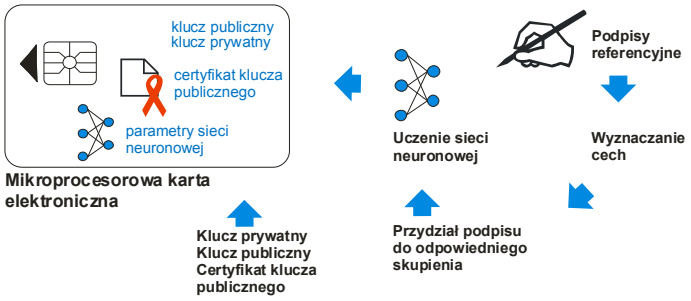
Przy zastosowaniu sieci RCE [11] otrzymano zdecydowanie lepsze wyniki klasyfikacji (CCR bliski 100%). Okazuje się więc, że sieć ta wykazuje znacznie lepsze właściwości uogólniające niż dwuwarstwowy perceptron o sigmoidalnych funkcjach aktywacji. Aczkolwiek większe zdolności uogólniania wpływają niekorzystnie na proces weryfikacji, prowadząc do wyników FAR = 8.33% i FRR = 11.11%, co przy wymaganiu niskiego poziomu współczynnika FAR praktycznie dyskwalifikuje sieć RCE w zastosowaniach związanych z weryfikacją tożsamości.

7 System kontroli dostępu z zastosowaniem kart mikroprocesorowych

Każda metodologia na której oparte są systemy kontroli dostępu ma pewne słabe punkty, dzięki którym zabezpieczenia mogą zostać złamane, z pominięciem tych składników systemu, które bezpośrednio odpowiadają za jego bezpieczeństwo. W systemach opartych na architekturze klucza publicznego (*PKI - Public Key Infrastructure*) korzystanie z klucza prywatnego (generacja podpisu cyfrowego lub deszyfrowanie danych) jest najczęściej zabezpieczone kodem PIN. Wynika z tego, że kod ten, skradziony lub przekazany w jakikolwiek sposób prowadzi do identycznych praw jakie posiada właściciel karty mikroprocesorowej. Widać więc, że dla istotnego zwiększenia bezpieczeństwa systemu należy dodać do niego poprawnie i skrupulatnie zaprojektowany moduł weryfikacji tożsamości na bazie czynników, które nie mogą zostać skradzione czy też przekazane innej osobie. Do tego posłużyć mogą cechy biologiczne człowieka, o ile są to cechy unikatowe. W rozdziale tym użyjemy karty mikroprocesorowej firmy Gemplus do zaprezentowania możliwości połączenia weryfikacji podpisów odręcznych z weryfikacją podpisów elektronicznych.

Karta GPK16000 (***G**emplus **P**ublic **K**ey Card*) jest jedną z najlepszych dostępnych kart dla systemów opartych na PKI. Karty mikroprocesorowe zgodne są z normą ISO7816 (części 1,2,3,4), co powoduje że posiadają te same wymiary, elastyczność, położenie styków mikroprocesora, procesory kart taktowane są tą samą częstotliwością (3.56 MHz) jak również interpretują ten sam ustalony zestaw poleceń (w formie kilkubajtowych ciągów), niejednokrotnie rozszerzany przez producentów kart w celu uatrakcyjnienia swojej oferty. Na pokładzie karty GPK16000 znajduje się koprocesor do obliczeń modulo, niezbędnych w algorytmie RSA. Poza tym karta jest w stanie szyfrować dane algorytmem 3DES i dokonywać skrótów MD5 i SHA-1. Karta ma wbudowany generator liczb pierwszych (prawdopodobieństwo wylosowania liczby nie pierwszej wynosi 10^{-78}) co umożliwia generację pary kluczy RSA (o długości modułu 1024 bity) na pokładzie karty (operacja trwa do 10 sek.). Fakt generacji kluczy RSA przez kartę jest bardzo istotny gdyż tylko w takim przypadku klucz prywatny nie opuszcza karty, nie jest on znany nawet jej właścicielowi mimo znajomości kodu PIN, co minimalizuje prawdopodobieństwo złamania zabezpieczenia. Uniemożliwienie odczytania klucza prywatnego z pamięci karty jest możliwe, gdyż procesor GPK16000 generuje samodzielnie podpis cyfrowy na podstawie dostarczonych danych i klucza prywatnego zaszytego w pamięci EEPROM karty (dokładniej, plik zawierający klucz prywatny jest na stałe zablokowany do odczytu na poziomie systemu operacyjnego, zmiany są możliwe, ale wyłącznie przez wykonanie ponownie operacji generacji kluczy).

Pomysł polega na umieszczeniu parametrów nauczonej sieci neuronowej (dla danego skupienia zawierającego podpis właściciela karty) na karcie mikroprocesorowej. Plik zawierający parametry sieci powinien być zabezpieczony dwojako: kluczem symetrycznym znanym przez system kontroli dostępu i kartę oraz hasłem (lub kodem PIN) znanym przez użytkownika. Kod PIN nie jest jednak wymagany i można z niego zrezygnować. Weryfikacja klienta odbywa się tutaj w dwóch etapach. Pierwszy polega na odczytaniu z karty zapisanych parametrów sieci neuronowej (pamiętajmy, że parametry te mogą być odczytane przez urządzenia posiadające klucz symetryczny zabezpieczający plik, dla bezpieczeństwa praktykuje się umieszczanie takich kluczy w dodatkowej karcie mikroprocesorowej SAM – ***S**ecurity **A**ccess **M**odule* zainstalowanej w urządzeniu). Następnie składany jest podpis (z użyciem tabletu graficznego), który zostaje zweryfikowany za pomocą sieci o odczytanych z karty parametrach. Po pomyślnej weryfikacji właściciela karty przechodzimy do drugiego etapu, który polega na dobrze znanej weryfikacji podpisu elektronicznego na bazie kluczy RSA i certyfikatu.



Rysunek 9 Karta mikroprocesorowa jako bezpieczne miejsce kluczy oraz podpisu w formie parametrów sieci neuronowej

Do dyspozycji mamy 12.5 kB pamięci EEPROM karty. Należy rozważyć czy taki rozmiar pamięci jest wystarczający do zapisania parametrów sieci z dokładnością zapewniającą poprawną aproksymację funkcji klasyfikującej. Dla przykładu załóżmy, że każda liczba zapisana będzie na 4 bajtach w pamięci karty. Zgodnie z teorią Kołmogorowa, aby poprawnie aproksymować funkcję w przestrzeni n=12 cech warstwa ukryta sieci powinna składać się z 2n+1 neuronów. Neuron składa się z m+1 liczb dla m wejść, przy założeniu, że nie parametryzujemy funkcji aktywacji. Dla sieci skonstruowanej dla skupienia k=20 podpisów oraz m_1=n (liczba wejść do warstwy ukrytej), m_2=2n+1 (liczba wejść do warstwy wyjściowej) otrzymujemy więc $4*[(m_1+1)*(2n+1)+(m_2+1)*k] = 3380$ bajtów. Mając na uwadze, że plik zawierający klucz publiczny i prywatny

(o module 1024 bity i wykładniku publicznym 24 bitowym) pochłania 144B (część publiczna) + 344B (część prywatna) = 486B oraz certyfikat klucza publicznego, w zależności od danych w nim zawartych oraz po 20% kompresji dokonywanej zwykle przez biblioteki obsługujące komunikację z kartą, pochłania około 700B otrzymujemy sumę 4566B. Oznacza to, że do dyspozycji pozostaje około 8kB pamięci karty, którą można przeznaczyć na zwiększenie dokładności reprezentacji liczb będących parametrami sieci.

Bibliografia

[1] Słownik Języka Polskiego, redaktor naczelny: Witold Doroszewski, PWN, Warszawa 1964
[2] Najnowszy Słownik Języka Polskiego, redaktor naukowy: prof. dr hab. Bogusław Dunaj, WILGA 1999
[3] G. Dimauro, S. Impedevo, G. Pirlo, A. Salzo: „A Multi-Expert Signature Verification System for Bankcheck Processing", *International Journal of Pattern Recognition and Artificial Intelligence,* vol. 11, No. 5 (1992) pp. 827-844
[4] S. Lee, J. C. Pan: „Offline Tracing and Representation of Signatures", *IEEE Trans. On Systems, Man and Cybernetics,* vol. 18, no. 6, June 1996
[5] J.-J. Brault, R. Plamondon: „A Complexity Measure of Handwritten Curves: Modelling of Dynamic Signature Forgery", *IEEE Trans. On Systems, Man and Cybernetics,* vol. 23, no. 2, March/April 1993
[6] L. L. Lee, T. Berger, E. Aviczer: „Reliable On-Line Human Signature Verification System", *IEEE Trans. On Pattern Analysis and Machine Intelligence,* vol. 18, no. 6, June 1996
[7] H. Crane, J. S. Ostrem: „Automatic Signature Verification Using a Three-Axis Force-Sensitive Pen", *IEEE Trans. On Systems, Man and Cybernetics,* vol. SMC-13, No. 3, May/June 1983
[8] T. Wessels, C. W. Omlin: „A Hybrid System for Signature Verification", *Transactions of IJCNN,* Como, Włochy 2000
[9] Internet: *www.signplus.com*
[10] Internet: *www.cybersign.com*
[11] MATLAB Statistics Toolbox User's Guide
[12] D. L. Relly: "The RCE Neural Network", *Nestor, Inc., 1989*
[13] "GPK8000 Reference Manual", *Gemplus, http://www.gemplus.com*
[14] "GPK8000 Application Notes", *Gemplus, http://www.gemplus.com*