P3057/01

ISSN 0239-8044

1
2001

Techniki Komputerowe

BIULETYN INFORMACYJNY

INSTYTUT MASZYN MATEMATYCZNYCH
WARSZAWA 2001

P3057/01

Techniki Komputerowe

BIULETYN INFORMACYJNY

Rok XXXVI, Nr 1, 2001

INSTYTUT MASZYN MATEMATYCZNYCH
WARSZAWA 2001

P 3057/01

Wydaje:

INSTYTUT MASZYN MATEMATYCZNYCH
UL. KRZYWICKIEGO 34
02-798 WARSZAWA
TEL. 621.84.41, TLX 81.78.80, FAX 629.92.70
E-MAIL: imasmat@imm.org.pl
INTERNET: http://www.imm.org.pl

Copyright © by Instytut Maszyn Matematycznych, Warszawa 2001

Druk: Zakład Poligrafii Ośrodka Przetwarzania Informacji, al. Niepodległości 186

Niniejsze, specjalne wydanie Biuletynu poświecone jest Konferencji Naukowej BIOMETRIA 2001 *Technika biometryczna – podstawy teoretyczne i praktyka*, która odbyła się 8 listopada 2001 r. w Warszawie. Podobnie jak w ubiegłym roku wygłoszone na Konferencji referaty prezentujemy w formie artykułów, co miedzy innymi dało sposobność Autorom do szerszego ujęcia omawianych zagadnień; była to jednak dodatkowa praca, za którą Redakcja dziękuje wszystkim Autorom.

Z satysfakcją zwracamy uwagę naszych Czytelników na to, że Konferencja zgromadziła słuchaczy i reprezentantów wielu ośrodków uczelnianych i jednostek badawczo-rozwojowych prowadzących badania lub zainteresowanych stosowaniem technik biometrycznych. W wielu wystąpieniach, po omówieniu zagadnień teoretycznych, przedstawiano propozycje wykorzystania w praktyce wyników prac badawczych. Konferencja wykazała, co też było jednym z jej celów, że wykorzystując krajowe zaplecze badawcze wdrażanie techniki biometrycznej w kraju w wielu dziedzinach jest możliwe i może być efektywne.

W imieniu organizatora, Instytutu Maszyn Matematycznych, składamy podziękowanie Ministerstwu Gospodarki za dofinansowanie Konferencji BIOMETRIA 2001.

Redakcja

Warszawa, listopad 2001

TECHNIKI KOMPUTEROWE

Rok XXXVI Nr 1 2001

Spis treści

Str.

Metody weryfikacji tożsamości na bazie dynamicznych cech podpisów odręcznych oraz wzoru tęczówki oka, Adam Czajka, Andrzej Pacut 7

Warunki akceprtacji biometrycznego badania podpisu, Anna Koziczak 25

Dane biometyczne w dowodach osobistych, Małgorzata Andrzejkowicz 31

Dyskryminacja niepełnosprawnych w dowodach tożsamości, Mirosław Owoc 39

Biometryczne wspomaganie niepełnosprawnych, Mirosław Owoc 43

Wybor parametrów sygnału mowy użytecznych w rozpoznawaniu głosów, Jerzy Sawicki 47

Ochrona zasobów własnych za pomocą ciągów losowych, parametryzowanych biometrycznie, Andrzej Mitas 57

Metody neuronowe w kodowaniu i kompresji informacji, Waldemar Graniszewski 67

Bezpieczeństwo handlu elektronicznego, Henryk Krawczyk Michał Wielgus, ... 79

Analiza porównawcza wybranych biometrycznych rozwiązań sprzętowo-programowych wykorztystujących badanie linii papilarnych w procecie uwierzytelniania, Adrian Kapczyński 103

Biometria – techniki, zastosowania, rynek w latach 2000-2001, Jan Ryżko, Jerzy Sławiński 115

ADAM CZAJKA*, ANDRZEJ PACUT*,**
* INSTYTUT AUTOMATYKI I INFORMATYKI STOSOWANEJ
POLITECHNIKA WARSZAWSKA
** NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA
NASK, WARSZAWA

Rozpoznawanie podpisów odręcznych jako przykład systemu weryfikacji tożsamości
Recognition of Human Signatures as the Identity Verification System

Streszczenie

W pracy użyto tableto graficznego do pomiaru pięciu składników podpisu w dziedzinie czasu, mianowicie położenia na płaszczyźnie, nacisku oraz dwóch kątów określających orientację pióra w trakcie pisania. Cechy podpisu podzielone zostały na dwie grupy: cechy widoczne związane z obrazem podpisu na płaszczyźnie oraz cechy niewidoczne związane z całym dynamicznym procesem podpisywania. W pracy przeprowadzono analizę skupień podpisów w przestrzeni cech, natomiast funkcja klasyfikująca aproksymowana została za pomocą dwóch struktur sieci neuronowych. W artykule przedstawiono zastosowanie metodyki w systemie kontroli dostępu z użyciem kryptograficznej karty mikroprocesorowej.

Abstract

A digitizing tablet is used to collect handwritten signatures. Five quantities are recorded, namely, horizontal and vertical pen tip position, pen tip pressure, and pen azimuth and altitude angles. Signature features are divided into visible features related to the „image on paper", and hidden features that depend on the entire time-related process of signing. Cluster analysis is applied to segment the features space into sub-regions of „similar" signatures to simplify classifying functions. The classifying functions are approximated with the use of neural networks. The methodology is applied in an identity verification system with the use of the microprocessor card.

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 *podpisem* a *realizacją podpisu* 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 dla realizacji podpisu. 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

$$Z = [z_1, z_2, ..., z_J]: T \mapsto R^J \tag{2}$$

gdzie J oznacza liczbę mierzonych wielkości, zaś T jest zbiorem chwil pomiarowych. Funkcja ta jest jednoznacznie określona poprzez J 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 $z_{p,q,...,r}$ 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 s_1, s_2 położenia końcówki pióra na płaszczyźnie), natomiast

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

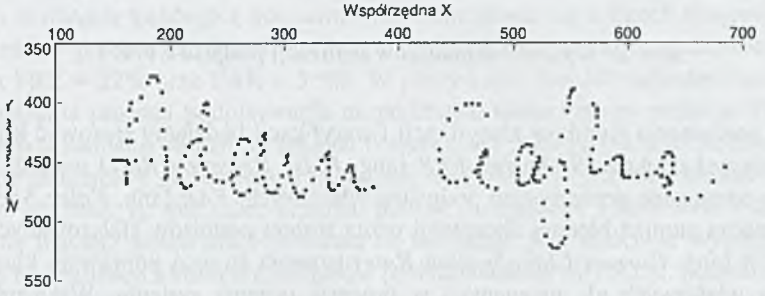
jest krzywą „parametryczną" w której zachowuje się wszystkie wielkości mierzone ale eliminuje czas. W rezultacie

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

‚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.

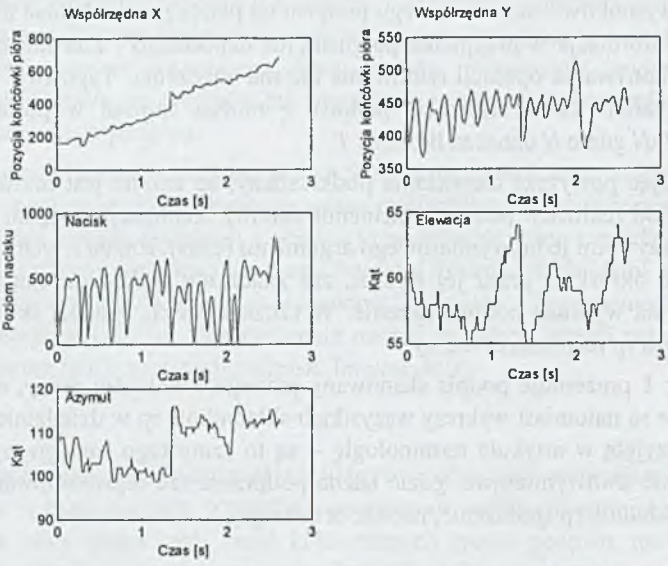
Reasumując powyższe rozważania podkreślamy, że istotne jest rozróżnianie podpisu (zbioru) od realizacji podpisu (elementu zbioru). Realizacje podpisu są wielowymiarowymi krzywymi jednowymiarowego argumentu (czas). Każda z tych krzywych jest jednoznacznie określona przez jej wykres, zaś znaczenie praktyczne 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).



Rys. 1. Przykład rzutu rp na podprzestrzeń s_1,s_2 (podpis skanowany)

Oprócz podpisu, rozumianego jako zbiór wszystkich realizacji podpisu 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.



Rys. 2. Wykresy składników realizacji podpisu z rys. 1

Dla porównania wyników klasyfikacji i weryfikacji będziemy stosować kilka standardowych wskaźników. Wskaźnik *FRR* (ang. *False Rejection Rate)* oznacza stopień błędnego odrzucania przez system podpisów właściwych, *FAR* (ang. *False Acceptance Rate)* oznacza stopień błędnej akceptacji przez system podpisów sfałszowanych, natomiast *CCR* (ang. *Correct Classification Rate*) 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. *Equal Error Rate*).

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_r na wejściu systemu do odpowiedniego podpisu Z, natomiast w procesie *weryfikacji* każda realizacja z Z_r 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 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 metodykę 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).

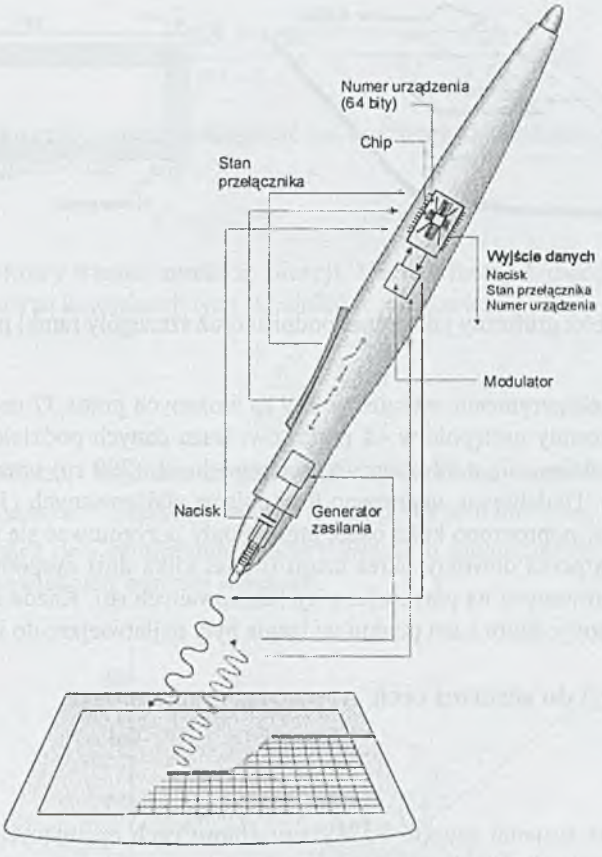
Podejścia dynamiczne klasyfikować można na bazie wymiarowości obserwacji. Metodyka w ogólności nie zależy natomiast od wymiaru przestrzeni obserwacji. Ciekawą pracą wykorzystującą pomiary wyłącznie położenia pióra w czasie pisania ($z_{t,s1,s2}$) jest modelowanie procesu fałszowania podpisu. Brault i 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% naprzeciw 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

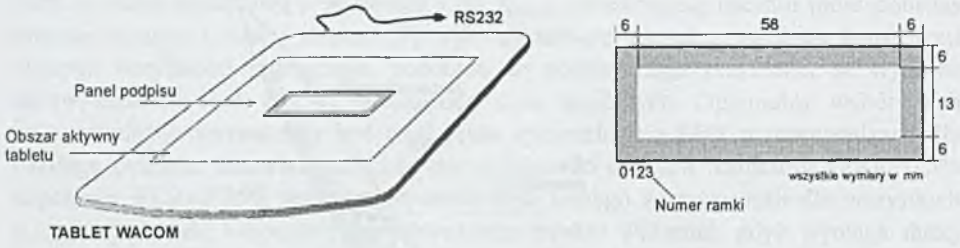
Pomimo tego, że proces podpisywania zależny jest od osobowości, przyzwyczajeń osoby czy też podświadomego wyćwiczenia pewnych ruchów realizowanych przez układ nerwowo-mięśniowy, kolejne realizacje podpisu będą różniły się od siebie w zależności od istniejących warunków pisania. Z drugiej strony te właśnie 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.

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.



Rys. 3. Tablet WACOM wraz z bezprzewodowym piórem

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 100 Hz. 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.



Rys. 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

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

Odchylenia standardowe składników rp

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

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

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

gdzie

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

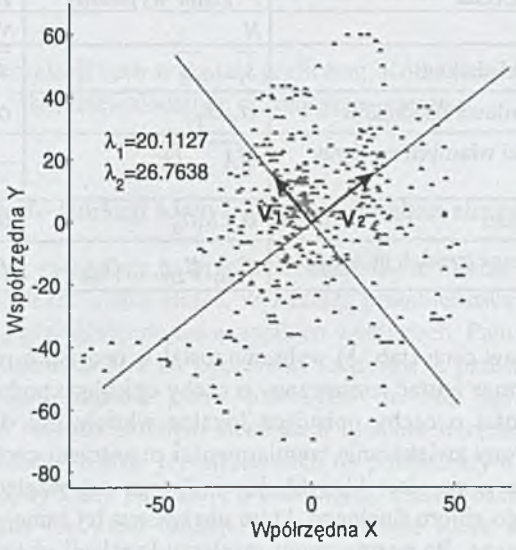
W dalszych obliczeniach posługiwać się będziemy składnikami podpisu z usuniętym trendem, mianowicie

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

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.



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

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

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

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 ($\beta_{p,q,r}$).

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*.

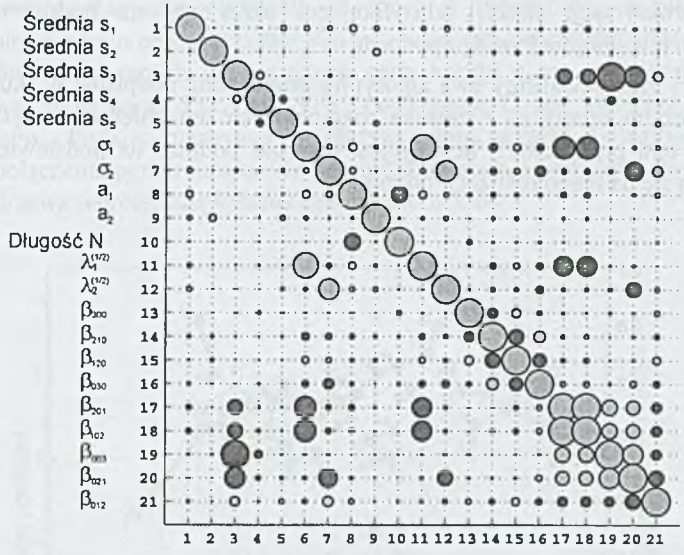
4.2. Minimalny zestaw cech

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.



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

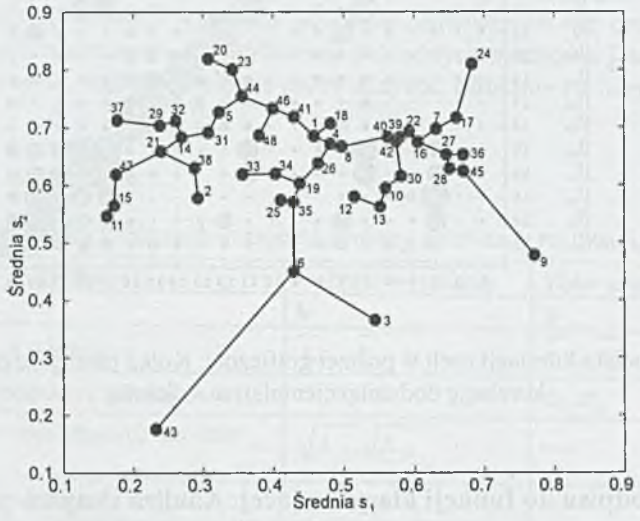
5. Od cech podpisu do funkcji klasyfikującej. Analiza skupień podpisów

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.

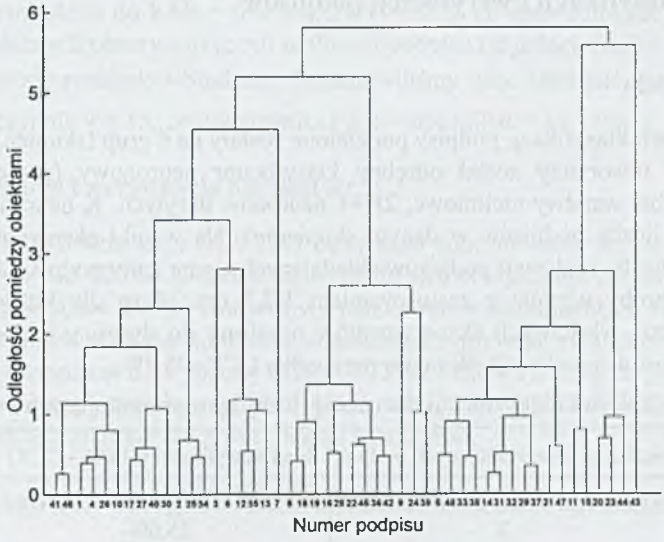


Rys. 7. Drzewo rozpinające w przestrzeni dwóch cech (położenie s_1,s_2)

Pierwszy z algorytmów konstruuje drzewo rozpinające nieskierowany 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. Rysunek 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 $d^2(x,y)=(x-y)^T C^{-1}(x-y)$ 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.



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

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 $\kappa = 0$. 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 w drzewie rozpinającym, 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

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

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 t_N, mianowicie $P\{|t_N| \geq t_\alpha\} = \alpha$ 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

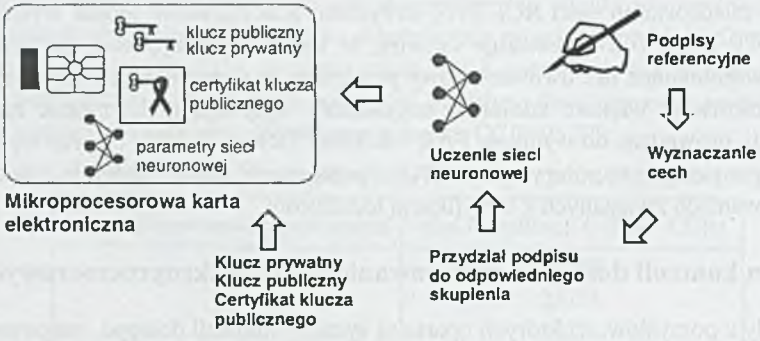
Przy zastosowaniu sieci RCE [11] otrzymano zdecydowanie lepsze wyniki klasyfikacji (CCR bliski 100%). Okazuje się więc, że sieć ta wykazuje znacznie lepsze właściwości uogólniające niż dwuwarstwowy perceptron o sigmoidalnych funkcjach aktywacji. Aczkolwiek większe zdolności uogólniania wpływają niekorzystnie 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

Każdy z pomysłów, na których 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 (*Gemplus Public Key Card*) jest jedną z najlepszych dostępnych kart dla systemów opartych na PKI. Karty mikroprocesorowe zgodne są z normą ISO 7816 (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).



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

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 – *Security Access Module* 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.

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.

Literatura

[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*

ANNA KOZICZAK
KATEDRA KRYMINALISTYKI
UNIWERSYTET IM. A. MICKIEWICZA, POZNAŃ

Warunki akceptacji biometrycznego badania podpisu
The acceptance conditions of biometric examination of a signature

Streszczenie

W artykule wskazano cechy graficzne, które powinny być wykorzystane w systemach biometrycznych, aby systemy te mogły w sposób wiarygodny identyfikować osoby składające podpis.

Abstract

The paper describes the graphical characteristics which ought to be used in biometric systems in order that these systems could faithfully identify the signing persons.

Spośród wielu różnorodnych danych o charakterze biometrycznym, które nadają się do wykorzystania jako podstawa identyfikacji człowieka, własnoręczny podpis należy do tych, które wydają się łatwe do zaakceptowania przez użytkowników automatycznych systemów identyfikacyjnych. Wynika to z faktu, iż podpis jest od bardzo dawna, powszechnie i w najróżniejszych okolicznościach wykorzystywany do celów identyfikacyjnych, a jego składanie na różnorodnych dokumentach nie budzi żadnych negatywnych skojarzeń (inaczej ma się sprawa np. z odciskami palców, których pobieranie u wielu osób budzi niechęć, kojarząc się ze ściganiem i identyfikacją przestępców[1]).

[1] Związane z tym opory przed poddaniem się daktyloskopowaniu powodują, że odciski palców – choć bez wątpienia stanowią znacznie pewniejszą i łatwiejszą do zweryfikowania podstawę identyfikacji niż podpis – zapewne nieprędko znajdą powszechne zastosowanie w obrocie cywilnym, gospodarczym i życiu codziennym.

Oczywiście brak negatywnych skojarzeń nie wystarczy, aby dany system identyfikacji biometrycznej mógł uzyskać akceptację potencjalnych użytkowników – musi nadto charakteryzować się skutecznością stosowną do celu, jakiemu ma służyć.

W zależności od tegoż celu (przeznaczenia, miejsca zainstalowania systemu) należy stosownie dobrać proporcje między wielkością dopuszczalnego współczynnika błędnych akceptacji i dopuszczalnego współczynnika błędnych odrzuceń. Wydaje się, że w większości systemów wskazane jest zmniejszenie tego pierwszego współczynnika (kosztem zwiększenia drugiego). Jednakże w niektórych systemach – np. instalowanych w bankach – błędne odrzucenia (błędna odmowa dostępu) są niemal równie niekorzystne jak błędne akceptacje; zarówno jedne, jak i drugie mogą działać na klientów banku odstraszająco, co bank winien uwzględnić podejmując decyzję o zakupie konkretnego systemu.

Idealnym systemem identyfikacji biometrycznej – niezależnie od tego, do jakich celów ma on służyć – byłby oczywiście system, w którym zarówno FAR, jak i FRR są zredukowane do zera. Należy jednak wyraźnie stwierdzić, że w przypadku systemów opartych na analizie podpisu osiągnięcie owego ideału nie jest możliwe, z przyczyn wskazanych niżej.

Podstawowa reguła badań pismoznawczych głosi, że żadna cecha podpisu (pisma) nie jest cechą „indywidualną", charakterystyczną tylko dla jednej osoby – indywidualny jest dopiero odpowiednio duży **zespół** cech. Zarówno w „tradycyjnych" badaniach pismoznawczych, jak i w systemach automatycznych, analizie podlegać powinna zatem jak największa liczba cech graficznych. W przypadku gdy liczba badanych cech jest niewielka – obejmuje jedynie fragment owego indywidualnego zespołu – szanse na poprawną identyfikację człowieka maleją. Innymi słowy, w miarę zmniejszania się liczby badanych cech podpisu (pisma), rośnie ryzyko pomyłki w identyfikacji wykonawcy.

W automatycznych systemach biometrycznych analiza podpisu ma zawsze charakter niekompletny (nie obejmuje pełnego zespołu cech charakteryzującego danego wykonawcę, lecz tylko jego fragment). Wynika to z dwojakiego rodzaju przyczyn. Po pierwsze, wiele podpisów (nie tylko podpisy skrócone, ale niekiedy także podpisy pełnobrzmiące) to twory „niepełnowartościowe" z identyfikacyjnego punktu widzenia, tj. na tyle krótkie i proste, że nie prezentują w pełni zespołu cech charakteryzującego konkretnego wykonawcę – takie podpisy nie stanowią wystarczającej podstawy identyfikacji człowieka, niezależnie od przyjętej metody ich badania. Po drugie, nawet jeśli dany podpis jest dostatecznie skomplikowany, aby teoretycznie mógł stanowić podstawę jednoznacznej identyfikacji wykonawcy, to i tak w systemach automatycznych analizowana jest jedynie niewielka część jego cech. Z reguły są to cechy należące do jednej z dwóch grup: tzw. grupy cech dynamicznych, mierzonych w trakcie składania podpisu (takich jak kierunek kreślenia, dynamika, siła nacisku, tempo, przyspieszenie, łączny czas kreślenia), albo do grupy cech „statycznych" (obejmujących szeroko rozumianą konstrukcję podpisu, kształt tworzących go krzywych). Analiza podpisu ma więc charakter wybiórczy: ogranicza się jedynie do wybranej części cech graficznych, dających się w podpisie wyróżnić i zbadać. Efekt działania takich systemów

(zidentyfikowanie albo niezidentyfikowanie człowieka) musi być więc wysoce zawodny[2], tym bardziej że:

- istnieją pewne możliwości udatnego naśladowania cech podpisów innej osoby – głównie cech statycznych, ale w pewnym zakresie także cech dynamicznych (naśladownictwo takie jest tym łatwiejsze, im mniejsza jest liczba cech podlegających analizie),
- coraz częstsze są przypadki autofałszerstw podpisów (celowej zmiany cech graficznych przez „właściciela" podpisu po to, aby zakwestionować jego autentyczność i wykazać, że np. gotówka z konta została podjęta przez inną, nieuprawnioną osobę),
- w praktyce zdarzają się przypadki niezamierzonego, niekiedy zaskakująco dużego podobieństwa podpisów różnych osób (dotyczy to głównie podpisów o prostej formie i wysokim stopniu skrócenia),
- u każdej osoby występują naturalne, często dość duże wahania cech podpisów, zarówno statycznych, jak i dynamicznych (spowodowane np. zmianami samopoczucia, warunków pisania i wieloma innymi przyczynami wewnętrznymi lub zewnętrznymi).

Brak możliwości całkowitego wyeliminowania błędów w działaniu systemów opartych na analizie podpisu nie oznacza, że nie należy dążyć przynajmniej do przybliżenia ich do ideału. Wydaje się, że istnieje przynajmniej kilka działań, których podjęcie mogłoby poprawić funkcjonowanie systemów identyfikacji biometrycznej na podstawie podpisu.

Po pierwsze, należy dążyć do uwzględnienia w analizie tak wielu cech graficznych, jak to tylko jest w danym przypadku możliwe. Narzucającym się rozwiązaniem jest łączne analizowanie w biometrycznych systemach identyfikacyjnych zarówno cech statycznych, jak i cech dynamicznych podpisu (zgodność dynamiki kreślenia przy odmienności konstrukcji podpisu może wskazywać, iż dany podpis jest tworem wykreowanym przez fałszerza, przypadkowo kreślonym z podobną prędkością, naciskowością itd.; zgodność konstrukcji przy zasadniczej odmienności dynamiki kreślenia może świadczyć o tym, że dany podpis jest sfałszowany w drodze naśladownictwa; poddanie pomiarom tylko cech jednej lub drugiej grupy może doprowadzić do błędnych wniosków).

---

[2] Opisując IBM-owski program pod nazwą „Sival 2" (opracowany z myślą o zainstalowaniu go w bankach) podano, iż skuteczność jego działania sięga 99,5%, „gdy fałszerz **nie wie**, jak wygląda autograf", czyli w sytuacji, gdy osoba usiłująca uzyskać dostęp do cudzego konta, nie wiedząc jak wygląda autentyczny podpis właściciela, tworzy wymyśloną przez siebie „namiastkę" podpisu (Skudelny H., Mueller P., Komputer – grafologiem, CHIP nr 11/1994 s. 27). Określenie powyższego wyniku mianem „żenująco niskiego" (Owoc M., Komputerowe wspomaganie ekspertyzy pismoznawczej, Kraków 1997 – publikacja wydana na krążku CD) jest w tej sytuacji całkowicie uzasadnione. W pierwszej z cytowanych publikacji nie podano niestety, jak wygląda skuteczność działania systemu, gdy fałszerz **wie**, jak wygląda podpis autentyczny i stara się go naśladować; nie ulega jednak wątpliwości, że musi być znacznie gorsza.

Po drugie, cechy dotychczas uwzględniane w systemach automatycznej analizy podpisów warto uzupełnić o grupę tzw. cech topograficznych. Należą do nich takie cechy podpisów jak: układ liter względem siebie, układ poszczególnych znaków i całego podpisu względem liniatury, rozmieszczenie podpisu w „okienku" wyznaczającym miejsce na podpis (np. na czeku), kształt linii podpisu, tj. linii łączącej minima poszczególnych znaków, kierunek (tendencja) linii podstawowej (linii łączącej minima pierwszego i ostatniego znaku śródlinijnego), odstępy między znakami, wzajemny układ członów podpisu itp. O analizie cech topograficznych wspomina się w publikacjach z zakresu biometrii rzadko, a jeśli już, to w odniesieniu do badań obszernych tekstów, a nie podpisów.[3] Tymczasem cechy topograficzne są szczególnie istotne w badaniu autentyczności podpisów, ponieważ są wyjątkowo rzadko uwzględniane (naśladowane) przez fałszerzy; jednocześnie należą do cech najrzadziej zmienianych przez osoby dokonujące autofałszerstwa podpisu.

Po trzecie, ze względu na wspomniane wyżej zjawisko naturalnej fluktuacji podpisu, jako wzorzec do późniejszej identyfikacji należy wykorzystywać nie jeden, lecz co najmniej kilka, kilkanaście podpisów tej samej osoby; korzystne byłoby, gdyby były to podpisy składane w różnym czasie, a nie jeden po drugim. Wartość pojedynczego podpisu jako wzorca do późniejszych analiz porównawczych jest znikoma (jeśli bowiem podpis ten byłby akurat składany w szczególnych, nietypowych dla danej osoby okolicznościach, to może się okazać, że znakomita większość „normalnych" podpisów tej osoby obiega od niego grafizmem). Dopiero analiza większej liczby podpisów pozwala ustalić, jaki jest zakres naturalnej fluktuacji grafizmu u danej osoby.

Spełnienie powyższego warunku nie wiąże się z jakimiś szczególnymi trudnościami, a znacznie zmniejsza ryzyko popełnienia błędu; umożliwia także zastosowanie w systemach automatycznej identyfikacji analiz o charakterze statystycznym.

Po czwarte, warto rozważyć, czy jest sens obejmować systemem automatycznej identyfikacji podpisy wszystkich osób, które potencjalnie mogłyby z niego skorzystać (np. wszystkich klientów danego banku), czy raczej zastosować swego rodzaju kwalifikację wstępną. Efekty działania automatycznych systemów byłyby znacznie lepsze (liczba popełnianych błędów obu rodzajów byłaby zdecydowanie mniejsza), gdyby eliminować z nich te podpisy, z których poprawnym rozpoznawaniem systemy miewają kłopoty. Należy bowiem założyć, że automatyczne rozpoznawanie części podpisów będzie skuteczne, tzn. będzie z reguły przebiegać bezbłędnie (dobrze powinny być rozpoznawane podpisy zawierające wystarczającą do identyfikacji liczbę cech, a jednocześnie ustabilizowane, mało różniące się między sobą grafizmem), natomiast

[3] V.S.Nalwa, autor rozdziału poświęconego automatycznej weryfikacji podpisów w wydanej niedawno książce dotyczącej biometrycznych metod identyfikacji człowieka, przytacza stosunkowo liczne publikacje na ten temat i opisuje koncepcje innych autorów; nie wspomina jednak, aby którykolwiek z nich uwzględniał w analizie podpisów cechy topograficzne (Nalwa V.S., Automatic on-line signature verification, w: Biometrics. Personal Identification in Networked Society, Boston, Dordrecht, London 1999, s. 143-163). O wykorzystywaniu niektórych cech topograficznych pisma (tekstu) w automatycznej identyfikacji wykonawcy wspomina się w publikacji: Arazi B., Automatic Handwriting Identification Based on the External Properties of the Samples, IEEE Transactions on Systems, Man and Cybernetics, vol. SMC-13, no 4, July/August 1983, s. 635-642.

w rozpoznawaniu pewnej grupy podpisów szczególnie często będą zdarzać się błędy (do grupy tej należeć będą parafy i podpisy o wysokim stopniu naturalnej fluktuacji grafizmu). Osoby posługujące się takimi właśnie podpisami (parafami i podpisami o nieustabilizowanym grafizmie) musiałyby być identyfikowane w inny sposób, np. metodą daktyloskopijną.

MAŁGORZATA ANDRZEJKOWICZ
KATEDRA KRYMINALISTYKI
UNIWERSYTET IM. A. MICKIEWICZA, POZNAŃ

Dane biometryczne w polskich dowodach tożsamości
Biometric data in Polish authentication documents

Streszczenie

Omówiono nowe polskie dokumenty tożsamości: dowód osobisty i paszport, zwracając uwagę na zawarte w nich dane o charakterze biometrycznym (zdjęcie i podpis posiadacza). Oceniono, iż dane te w niedostatecznym stopniu zabezpieczają dokumenty tożsamości przed użyciem przez osoby nieuprawnione. Postulowano skuteczniejsze rozwiązanie.

Abstract

The new Polish authentication documents are described, namely identification card and passport. The biometric data included in these documents (the photograph and the signature of the owner) are underlined. It was estimated that these data are not sufficient to secure the documents against the illegal use. The better solution is proposed.

Można się spotkać przynajmniej z dwojakim rozumieniem biometrii. Tradycyjnie termin ten oznacza naukę dokonującą pomiarów organizmów żywych i opisującą zmienność cech populacji zgodnie z zasadami statystyki matematycznej[1]. Obecnie jednak coraz częściej tłumaczy się biometrię jako zautomatyzowaną technikę pomiaru unikalnych, fizycznych lub behawioralnych cech jednostki i porównywania tak uzyskanej charakterystyki z bazą danych w celu rozpoznania tej jednostki[2].

W niniejszej pracy termin biometria rozumiany będzie w tym drugim znaczeniu.

---

[1] Encyklopedia Powszechna PWN, Warszawa 1983, t. III, s. 302.

[2] Np. J. D. Woodward, Biometrics: identifying law & policy concerns, w: Biometrics. Personal Identification in Networked Society, Boston, Dordrecht, London 1999, s. 387. Takie zawężanie terminu jest jednym z efektów prężnego rozwoju nowoczesnych metod i technik pomiaru owych cech oraz rozkwitu przemysłu wykorzystującego zdobycze badań biometrycznych.

Z rozmaitych względów organizacja państwowa rejestruje swoich obywateli, gromadząc o nich różne dane. Podstawowe z nich, przede wszystkim identyfikujące osobę, uwidaczniane są w urzędowych dokumentach stwierdzających tożsamość – dowodach osobistych i paszportach. Nie wymaga szczególnego komentarza fakt częstego używania, a więc dużego znaczenia tych dokumentów w stosunkach publiczno- i prywatnoprawnych. W związku z dużym zaufaniem do autentyczności tych dokumentów i prawdziwości zawartych w nich danych, walka z podrabianiem, przerabianiem oraz posługiwaniem się cudzym dowodem przez osobę nieuprawnioną jest niezwykle ważna. Stosowane są coraz nowocześniejsze elementy zabezpieczające dowód przed sfałszowaniem, jeżeli jednak dokument nie zawiera informacji o niepowtarzalnych cechach fizycznych i behawioralnych posiadacza, posługiwanie się nim przez oszustów jest bardzo łatwe.

W związku z wprowadzeniem w Polsce od 1 stycznia 2001 r. dowodu osobistego w formie spersonalizowanej karty identyfikacyjnej o standardowych wymiarach (54 × 85 mm)[3] oraz, od 27 maja 2001 r., paszportu nowego wzoru (jak dotychczas, jest to książeczka o wym. 125 x 87 mm)[4], warto przyjrzeć się, w jakim zakresie polskie dowody tożsamości (w sensie dokumentów) wykorzystują dane o charakterze biometrycznym, których zgodność także jest dowodem tożsamości osoby (tym razem w sensie rezultatu wnioskowania). Umieszczanie w dowodach osobistych i paszportach danych biometrycznych jest więc niejako naturalne.

Jako przyczyna wprowadzenia nowych wzorów dokumentów (oraz zbudowania nowego systemu ich wydawania) wskazywana jest wadliwość techniczna i łatwość fałszowania dotychczasowych (szczególnie „stare" polskie paszporty cenione są na nielegalnym rynku dokumentów), a także konieczność dostosowania wzorów do standardów Unii Europejskiej. Jakie jednak przyczyny przyświecały wybraniu właśnie takiej formy, jak opisana poniżej – nie wiadomo.

System wydawania dokumentów tożsamości zbudowało konsorcjum Drukarni Skarbowej p. p., węgierskiej firmy MultiPolaris Kft oraz Hewlett-Packard Polska. Produkcja kart plastikowych i książeczek paszportowych odbywa się w warszawskiej Drukarni Skarbowej. W urzędach gmin (wydawanie dowodów) oraz urzędach

---

[3] Rozporządzenie Rady Ministrów z dnia 21 listopada 2000 r. w sprawie wzoru dowodu osobistego oraz trybu postępowania w sprawach wydawania dowodów osobistych, ich wymiany, zwrotu lub utraty (Dz.U. Nr 112, poz. 1182).

Nad projektem wprowadzenia nowych wzorów dokumentów pracowano od dawna. Po raz pierwszy wymianę starych dowodów osobistych na nowe (zatopione w plastiku blankiety z podpisem i zdjęciem) zaproponowano na początku 1993 r. Potem termin przesunięto na koniec 1995 r. (dowody plastikowe o wymiarach 105 x 75 mm). Następny rząd zdecydował o wprowadzeniu dowodów na początku 1999 r., potem 2000, wreszcie 2001. Jak informowało MSWiA, zadaniem firmy, która zajmie się produkcją nowych dowodów osobistych, będzie wytwarzanie kart wyposażonych w pasek magnetyczny bądź mikroprocesor oraz wprowadzanie do nich informacji o posiadaczu.

[4] Rozporządzenie MSWiA z dnia 11 maja 2001 r. zmieniające rozporządzenie w sprawie wzorów oraz trybu wydawania paszportów, dokumentów wymaganych do ich otrzymania, a także trybu postępowania funkcjonariuszy Straży Granicznej w przypadku ujawnienia w czasie kontroli granicznej wad w paszportach (Dz.U. Nr 48, poz. 505).

wojewódzkich (wydawanie paszportów) znajdują się jedynie terminale do wprowadzania danych. Jest to sprzęt wysokiej klasy: silny komputer PC, wyposażony w drukarkę i skaner. System uruchamiany jest w środowisku Windows NT 4.0. Oprogramowanie dostarczone przez MultiPolaris to proste aplikacje: *IDL System*, inaczej System Obsługi Obywatela (ewidencja wydanych i utraconych dowodów osobistych) oraz *System Obsługi Paszportów*. Rekordy złożone z danych osobowych (ręcznie wprowadzonych z wniosku) oraz zeskanowanego zdjęcia i podpisu petenta przesyłane są siecią teleinformatyczną PESEL-NET z urzędów wojewódzkich do MSWiA – Centrum Personalizacji Dokumentów CPD[5].

W Centrum następuje proces personalizacji, czyli nadania dokumentom cech indywidualnych przez laserowe wygrawerowanie w poliwęglanie imienia, nazwiska i innych danych osobowych posiadacza oraz tzw. danych graficznych: zdjęcia i podpisu. Dokumenty mają zawierać ponad 40 elementów zabezpieczających przed sfałszowaniem i być pod tym względem, zdaniem przedstawicieli MSWiA, jednymi z najlepszych na świecie. Pierwsze spostrzeżenia służb granicznych nt. paszportów nowego typu są jednak mniej optymistyczne[6].

Pośród zamieszczanych w dokumentach tożsamości danych (nazwisko, imię, nr PESEL – „stały symbol numeryczny jednoznacznie identyfikujący określoną osobę fizyczną" i inne), jedynymi danymi o charakterze biometrycznym są zdjęcie i podpis posiadacza.

Poniżej rozważono możliwość potwierdzenia albo zanegowania tożsamości osoby posługującej się dowodem (paszportem) z osobą, której dane uwidocznione są w tym dokumencie.

Dla przeprowadzenia weryfikacji tożsamości przez komputer, wizerunki twarzy i podpisu, których nośnikiem jest dowód, muszą zostać przekształcone w postać cyfrową. Analizując szanse powodzenia zautomatyzowanej weryfikacji tożsamości nie wnikano w szczegóły algorytmów i podstawy matematyczne.

ROZPOZNANIE TWARZY I UCHA

Ubiegający się o wydanie dokumentu musi złożyć m.in. dwie aktualne, wyraźne fotografie o wymiarach 35 × 45 mm (do dowodu) albo 40 × 50 mm (do paszportu), przedstawiające osobę bez nakrycia głowy i okularów z ciemnymi szkłami w taki

---

[5] P.T.C. Centertel sp. z o. o., za pomocą sieci telefonii komórkowej Idea, ma zapewnić sprzęt teletransmisyjny oraz bezpośrednie przesyłanie drogą radiową danych z urzędów gmin do CPD; na razie jednak w całej Polsce system działa w tzw. trybie awaryjnym (zapis rekordów na dyskietkach i przewiezienie ich do wojewódzkiego ośrodka informatyki, który transmituje dane do Warszawy z wykorzystaniem sieci PESEL-NET).

[6] D. Augustyniak, W. Palemba, Możliwości weryfikacji autentyczności paszportu RP serii AB w ramach procedur kontroli granicznej, referat wygłoszony na 3. Konferencji *Techniczno-kryminalistyczne badania autentyczności dokumentów publicznych*, Poznań 27-28 września 2001 r.

sposób, aby ukazywały głowę w pozycji lewego półprofilu i z widocznym lewym uchem, z zachowaniem równomiernego oświetlenia twarzy[7].

Zdjęcie naklejane jest na formularz, a następnie wykonywana jest procedura „przekształcania cyfrowego zdjęcia i podpisu", czyli skanowanie. Rozdzielczość, z jaką skanowane są dane graficzne, nie jest znana przez obsługujących system; program określa ją automatycznie. Przeprowadzone próby pozwalają przypuszczać, że jest to wielkość ok. 200 dpi[8]. Niezależnie od tego, czy zdjęcie jest kolorowe, czy czarno-białe, przetwarzane jest na obraz w skali szarości.

Zdjęcia umieszczone w spersonalizowanym dokumencie są mniejsze niż w oryginale: 20 × 27 mm w dowodzie (ilustr. 1) i 30 × 35(37) w paszporcie (ilustr. 2). Wizerunki powinny w większości przypadków okazać się wystarczająco wyraźne dla wzrokowej identyfikacji posiadacza karty (paszportu).

Ilustracja 1

Ilustracja 2

Automatyzacja czynności rozpoznania polegać będzie na porównaniu obrazu twarzy – oryginału (zarejestrowanego np. przez kamerę) z matematyczną reprezentacją wzorca z dokumentu przez komputer.

Co do kryteriów porównawczych, to niewłaściwe byłoby zastosowanie metody opartej na pomiarze odległości między określonymi punktami anatomii twarzy[9]:

---

[7] Z uwagi na interwencje związków wyznaniowych oraz Polskiego Związku Niewidomych można odstąpić od żądania przedkładania fotografii bez nakrycia głowy w przypadku osób noszących nakrycie głowy zgodnie z wymogami wyznawanej religii oraz dopuścić możliwość dołączenia fotografii w ciemnych okularach przez osoby niewidome.

[8] Dla porównania: fotografia i podpis kierowcy, w celu nadrukowania na prawie jazdy, skanowane są z rozdzielczością 600 dpi. R. Domagała, D. Nowakowski, A. Pawlak, Rozwój systemu centralnej personalizacji praw jazdy, referat wygłoszony na 3. Konferencji *Techniczno-kryminalistyczne badania autentyczności dokumentów publicznych*, Poznań 27-28 września 2001 r.

[9] J. J. Weng, D. L. Swets, Face recognition, w: Biometrics, s. 69.

automatyczne wyszukiwanie tych punktów nie zawsze jest wiarygodne, a liczba możliwych pomiarów za mała, by była selektywna. Efektywność metody pomiarowej polegającej na lokowaniu i porównywaniu cech wewnątrz siatki[10] uzależniona jest od gęstości siatki, ta zaś musi być skorelowana z rozdzielczością obrazu. Powodzeniem natomiast powinna zakończyć się weryfikacja oparta na technologii sieci neuronowych, bowiem metoda przeszła pozytywne testy także dla obrazów zakłóconych („szum" rysunku gilosza na zdjęciach) i o niskiej rozdzielczości. Przy stosowaniu metod statystycznych (wektorowa reprezentacja obrazu) najlepsze możliwe rezultaty nie zostaną zapewne osiągnięte ze względu na istnienie tylko jednego wzorca[11].

Trudnością nie do pokonania dla systemu rozpoznawania twarzy może okazać się próba rozróżnienia osób bardzo podobnych (w tym upodabniających się w celu „kradzieży tożsamości" – niekiedy dzięki operacji plastycznej), zwłaszcza przy ograniczonej rozdzielczości obrazów. Ponadto, mogą istnieć bardzo różne wizerunki twarzy tej samej osoby (np. gdy radykalne zmienia uczesanie lub makijaż), na co systemy zazwyczaj nie są odporne.

Rozpoznanie osoby na podstawie obrazu ucha jest metodą obiecującą, ale ciągle na etapie prób badawczych[12]. Podejmowane są również kroki w celu potwierdzenia niepowtarzalności i niezmienności kształtu ucha[13]. Z dwóch metod identyfikacyjnych prezentowanych w *Biometrics*[14], technika antropometryczna (system Iannarelli'ego) nie nadaje się do wykorzystania ze względu na wymaganą precyzję lokalizacji punktów pomiarowych, niemożliwą do zrealizowania przez maszynę, zaś metoda oparta na topologicznych relacjach pomiędzy wyekstrahowanymi krzywymi – najprawdopodobniej ze względu na niewystarczającą rozdzielczość obrazu.

WERYFIKACJA PODPISU

Podpis na formularzu (druku sporządzanym na podstawie wniosku o wydanie dowodu osobistego), jak i na wniosku paszportowym, składany jest w obecności urzędnika, co ma zapobiec podpisaniu podania przez inną osobę.

Ze względu na dużą liczbę starających się o paszport, zdarza się przyjmowanie wniosków już wypełnionych w całości. Przy sprawdzaniu prawidłowości ich wypełnienia, od czasu wprowadzenia nowego wzoru paszportu stwierdza się, że najwięcej błędów popełnianych jest przy składaniu podpisu. Podpis musi zmieścić się w wyznaczonym polu o wym. 14 × 73 mm. Osoby o wydatnie zautomatyzowanym sposobie kreślenia podpisu zazwyczaj wykraczają poza tak wąską ramkę. Konieczność ponownego wypełnienia formularza jest dla większości na tyle odstręczająca, że zakreślają korektorem zbyt długie elementy podlinijne i linie adiustacyjne, odpowiednio je

[10] J. Ashbourn, Biometrics - Advanced Identity Verification. The complete guide, London 2000, s. 53.

[11] Systemy oparte na sieciach neuronowych i metodach statystycznych opisują: J. J. Wen, D. L. Swets, Face recognition, w: Biometrics, s. 65-86.

[12] Survey: Ear, eye, gait, keystroke, lip and nailbed biometrics. Biometric Technology Today, Luty 2000, s. 8-10.

[13] Ear Identification Research, http://www.forensic-evidence.com/site/ID00004_4.html.

[14] M. Burge, W. Burger, Ear biometrics, w: Biometrics, s. 273-285.

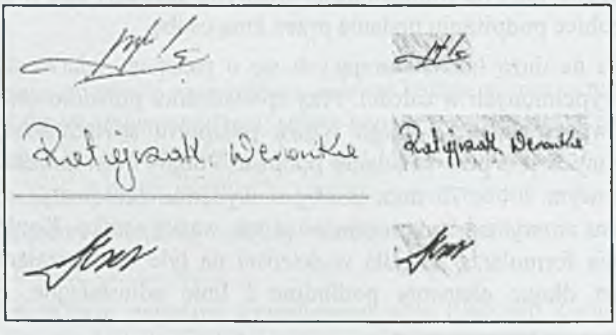
skracając. Niektórzy wnioskujący zauważają, że tak skorygowany podpis „to już nie jest ich podpis". Wypełniają więc wniosek ponownie – czasem nawet kilkakrotnie – aż do złożenia podpisu w sposób prawidłowy; nie można jednak wykluczyć, że część takich podpisów jest również zniekształcana (by nie „wykroczyć" poza pole). Ponadto, istnieje tendencja do traktowania dolnej krawędzi ramki jako liniatury. Niestety, złożenie podpisu na linii i tylko nieznacznie nad nią (do ok. 2 mm) skutkuje „obcięciem" dolnych partii podpisu przy skanowaniu (nie wolno skanować krawędzi ramki).

Na formularzach stosowanych przy wydawaniu dowodów osobistych na podpis przeznaczono pole o wym. 16 × 70 mm. Przy składaniu podpisu obowiązują warunki jw., a ponieważ formularze są drukami ścisłego zarachowania, urzędnicy aktywnie „asystują" przy tej czynności. Z tego oraz wyżej przytoczonych względów podpis nie zawsze jest dla danej osoby reprezentatywny.

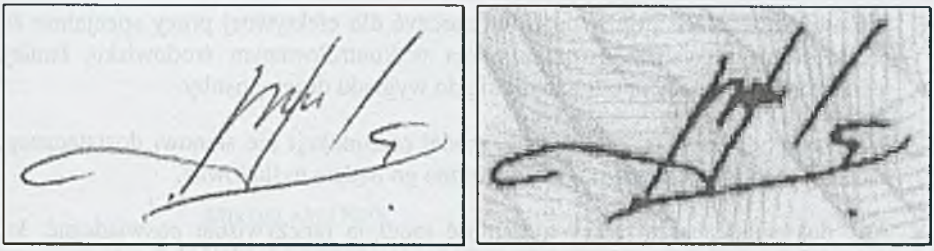
Nie ma wymogu, aby podpis był pełnobrzmiący lub chociaż czytelny, ale musi on zostać złożony długopisem (mazakiem) czarnym, ew. niebieskim (ze względu na przeznaczenie podpisu do skanowania).

Nie udało się ustalić rozdzielczości skanowania, najprawdopodobniej jednak nie przekracza ona 100 dpi (w *IDL System* wydaje się być nieco gorsza). Niemożliwe jest zatem odzwierciedlenie większości cech wiązania pisma ani szczegółów budowy znaków jak w oryginale. W obu systemach podpis konwertowany jest do postaci cyfrowej jako obraz w skali szarości. *System Obsługi Paszportów* poddaje ten obraz dalszej transformacji, którą można określić jako pogrubienie linii oraz zwiększenie kontrastu. Potęguje to zmiany we wzorcu (np. zmianę wyglądu początków i zakończeń linii, wypełnienie mniejszych pętli).

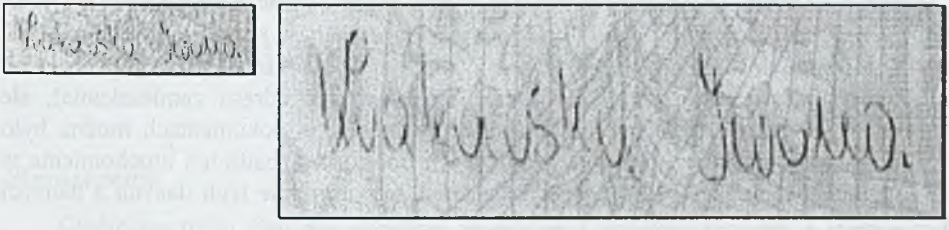
Wzorzec podpisu umieszczany w dokumencie jest mniejszy od oryginału: największe spotkane rozmiary to 6 × 33 mm w dowodzie i 7 × 28 mm w paszporcie.



Ilustracja 3. Podpisy na wnioskach paszportowych i paszportach – wielkość oryginalna



Ilustracja 4. Ten sam podpis na wniosku i w paszporcie – w powiększeniu



Ilustracja 5. Podpis w dowodzie osobistym – wielkość oryginalna i w powiększeniu

Możliwości zautomatyzowanej weryfikacji gotowych tworów graficznych są ograniczone. Po znormalizowaniu rozmiaru wzorca i porównywanej próbki mierzone są cechy geometryczne; brak możliwości analizy cech dynamicznych podpisu.

Należy także pamiętać, że ilość informacji zawarta w jednym podpisie, zwłaszcza skróconym i nieczytelnym, zazwyczaj nie wystarcza do identyfikacji wykonawcy przez biegłego, a tym bardziej przez komputer[15]. Badanie samego kształtu tak specyficznej reprodukcji, zważywszy na fakt, że nawet autentyczne podpisy potrafią się różnić, może nie wystarczyć do przeprowadzenia weryfikacji tożsamości.

REASUMUJĄC:

I. W porównaniu z podrabianiem i przerabianiem dokumentów, podszywanie się obecnie pod inną osobę nie będzie szczególnie trudne. Skradziony albo zgubiony dowód osobisty w postaci karty może zostać z powodzeniem użyty przez oszusta (będzie to nowy rodzaj „oszustwa karcianego").

[15] A. Koziczak, Bankowy wzorzec podpisu jako podstawa identyfikacji klienta, w: Współczesna przestępczość. Problemy prawnokarne, kryminalistyczne i kryminologiczne, Szczecin 1996, s. 100-102.

II. Wprawdzie wzorzec twarzy może wystarczyć dla efektywnej pracy specjalnie zaprojektowanego systemu rozpoznawania w kontrolowanym środowisku, istnieją jednak proste sposoby upodobnienia się do wyglądu drugiej osoby.

III. Wzorzec podpisu w postaci pomniejszonej reprodukcji nie stanowi dostatecznego zabezpieczenia przed oszustami – nietrudno go będzie naśladować.

IV. Aby dokument stwierdzający tożsamość mógł ją rzeczywiście poświadczać, konieczne jest umieszczenie w nim dodatkowych danych biometrycznych w postaci odcisków palców[16]. Przetwarzana i przechowywana informacja powinna być niedostępna dla osób postronnych, zatem zeskanowany wzorzec należy zapisać w mikroprocesorze, bez uwidaczniania na dokumencie. W mikroprocesorze mogłyby się znaleźć również wzorce twarzy i podpisu wykonane w większej niż obecnie rozdzielczości. Technicznie rozwiązanie takie może okazać się realne już wkrótce, ponieważ, jak twierdzi dyrektor Drukarni Skarbowej, „w perspektywie roku, 2 lat do nowego dowodu osobistego zapewne zostanie wprowadzony procesor". Pozwoli to na umieszczanie danych, które się zmieniają (np. adresu zamieszkania), ale wymagać będzie takiej modyfikacji przepisów, aby w dokumentach można było umieszczać informacje niewidoczne dla ich posiadacza, bądź też uruchomienia w urzędach stanowisk pozwalających każdemu na odczytanie tych danych z pamięci karty[17].

[16] Przykłady wykorzystania odcisków palca i innych danych biometrycznych w dowodach tożsamości podaje: J. Ryżko, Zastosowanie metod biometrycznych w dziedzinie prawa i porządku, Informatyka 10/2000, s. 24-28.

[17] http://www.computerworld.pl/online/2001/03/temat/Dowody_za_piec_dwunasta.asp.

MIROSŁAW OWOC
KATEDRA KRYMINALISTYKI
UNIWERSYTET IM. A. MICKIEWICZA, POZNAŃ

Dyskryminacja niepełnosprawnych w dowodach tożsamości
Discrimination of disabled persons in identity cards

Streszczenie

Omówiono różne realizacje dowodów tożsamości i problemy związane z wydawaniem nowych dowodów osobistych niepełnosprawnym. Rozwiązaniem byłoby tu wprowadzenie odcisku palca.

Abstract

Different realisations of authentication documents are described and problems of endow disabled persons with new identity cards are outlined. Introduction of the fingerprint to these cards seems to be solution of that.

1. Zasadniczą funkcją wszelkiego rodzaju dowodów tożsamości jest administracyjna identyfikacja posiadacza.

Tzw. „dowody osobiste" winny identyfikować osobę [pojedynczego obywatela] w populacji generalnej; podobnie jak paszporty. Jednakże zespół cech wybranych do tej identyfikacji może być zmienny w szerokim zakresie – zależnie od aktualnych celów przyświecających wystawcy oraz uwarunkowań dodatkowych. Skrajnym przypadkiem było numerowanie więźniów w hitlerowskich obozach koncentracyjnych i tatuowanie ich tymi numerami. Na drugim biegunie bliskich nam [terytorialnie] przykładów umieścić można dowody osobiste PRL. W nich to oprócz niepowtarzalnego numeru – już nie tatuowanego, lecz drukowanego [ale z obowiązkiem noszenia przy sobie] – zawarte były m. in. informacje o:

- dacie i miejscu urodzenia,
- imionach rodziców,
- stanie cywilnym i rodzinnym [dzieci],
- zawodzie,
- miejscu pracy i miejscu zamieszkania,

- wyglądzie zewnętrznym [fotografia, wzrost, kolor oczu, cechy szczególne],
- obrazie graficznym własnoręcznego podpisu

a także o:

- pobranych kartach na mięso lub na benzynę i
- wydanej książeczce walutowej.

Widać więc, iż hitlerowców charakteryzowało minimalistyczne utylitarne podejście do procesu dokumentacji indywidualności osoby, natomiast ambicje władców PRL-u były na wskroś humanistyczne. Dowód osobisty był wręcz książką opisującą życie obywatela.

Najnowszy wzór DOWODU OSOBISTEGO[1] jest wersją pośrednią, która ani nie jest tak skrajnie minimalistyczna jak wersja obozowa ani nie wnika tak głęboko w szczegóły życia osobistego posiadacza jak wersja PRL-owska, choć w jednym miejscu ją prześciga: zawiera oznaczenie płci posiadacza[2].

2. Wprowadzony Rozporządzeniem Rady Ministrów z dnia 21.11.2000 r. „Tryb postępowania w sprawach wydawania dowodów osobistych" przewiduje, iż „wniosek wypełnia i podpisuje osoba ubiegająca się o wydanie dowodu osobistego" [§ 1 ust. 3], podczas gdy poprzednio wniosek mogła **wypełnić** osoba trzecia, a sam zainteresowany tylko się podpisywał. Miało to swoje plusy i minusy, jednak te pierwsze przeważały.

Obecnie, już w momencie składania wniosku, dyskryminacji podlegają osoby nie mogące normalnie pisać: niewidomi, ociemniali, dysgraficy, cierpiący na chorobę Parkinsona, z niedowładami rąk rozmaitego pochodzenia. Interesujące, iż Rada Ministrów przewidziała tryb składania wniosków przez osoby małoletnie [choć piśmienne][3], lecz zapomniała o wymienionej grupie osób mających istotne trudności z pisaniem. A jest to grupa dość liczna i – ostatnio – niepokojąco się rozrastająca.

Uzasadnione jest, by w niniejszym omówieniu ograniczyć się do grupy dysgraficzków, bowiem – jeśli wierzyć publikacjom psychologów [a brak podstaw do niewiary w tym względzie, gdy pracuje się w szkolnictwie lub zawodowo zajmuje badaniami pismoznawczymi], blisko 20% dzieci szkolnych cierpi na dysleksję[4] a 30% ubiegłorocznej populacji polskich maturzystów przedstawiło zaświadczenia o posiadaniu przynajmniej jednej z trzech postaci zaburzeń: **dysgrafii** [objawiającej się zaburzeniami

---

[1] Wprowadzony Rozporządzeniem Rady Ministrów z dnia 21.11.2000 r., które weszło w życie z dniem 01.01.2001 r.

[2] Nie można wykluczyć, iż dyskryminacyjny charakter tej informacji będzie podnoszony na innych konferencjach niż poświęcone BIOMETRII, bowiem płeć nie jest zaliczana [jak dotąd] do cech biometrycznych.

[3] Przewidziany jest udział opiekunów ustawowych lub prawnie ustanowionych.

[4] Rypiński P., Dysgrafia - możliwość identyfikacji, w: Badania dokumentów. Kształtowanie się osobniczych cech pisma, Warszawa 1999, s. 97-137 [Zeszyty Metodyczne nr 3, Wyd. CLK KG Policji];
Korneć M., Możliwości identyfikowania pisma dysgraficznego, PROBLEMY KRYMINALISTYKI nr 229/2000, s. 27-35;
http://www.bpp.com.pl/ptd/prawny.htm z dnia 06.09.2001 r.;
http://dysleksja.univ.gda.pl/o_dysl.htm z dnia 06.09.2001 r.

w piśmie i dlatego najłatwiejszej do stwierdzenia], dysortografii [objawiającej się niemożnością opanowania ortograficznych zasad pisowni; kwestia owej „obiektywnej niemożności" jest trudna do zbadania] bądź wąsko rozumianej dysleksji [objawiającej się zaburzeniami w samym czytaniu][5]. To właśnie ta populacja będzie w najbliższym czasie otrzymywała dowody osobiste nowego wzoru. Jak małą wartość identyfikacyjną będą miały ich podpisy – można sobie wyobrazić.

3. Jeśli nawet jakiś uproszczony podpis osoby wyżej wymienione złożą, to nie będzie on miał charakteru nawykowego [nie będzie odwzorowaniem wystarczająco stabilnego wzorca wewnętrznego] i nie będzie możliwy do ponownego odtworzenia w razie potrzeby weryfikacji tożsamości okaziciela dowodu tożsamości. W przypadku utraty dowodu tożsamości zaopatrzonego w podpis osoby niepełnosprawnej w pisaniu, nieuprawniony posiadacz łatwo może przejść procedurę weryfikacyjną naśladując krańcowo uproszczony twór graficzny.

4. Zaopatrzenie dowodów tożsamości w odcisk palca kładzie kres opisanej dyskryminacji, a przy okazji podnosi pewność identyfikacji w odniesieniu do wszystkich obywateli.

5. Na zakończenie, by oddać sprawiedliwość twórcom projektu nowego wzoru dowodu osobistego [którzy byli zapewne artystami-plastykami wysokiej klasy] oraz samej Radzie Ministrów [w skład której nie wchodzą ani pracownicy Policji, ani pracownicy Straży Granicznej, ani kasjerzy bądź urzędnicy bankowi, ani pismoznawcy ani w ogóle nikt, kto będzie się zajmował weryfikacją tożsamości na podstawie wprowadzanego właśnie nowego dowodu osobistego] trzeba zauważyć, iż wszyscy Oni usiłowali jakoś zrównać wartość identyfikacyjną podpisów osób pełnosprawnych i niepełnosprawnych. Uczyniono to poddając jedne i drugie miniaturyzacji [około 3-krotnemu pomniejszeniu]. Najnowocześniejszą technologię komputerową zastosowano w złym kierunku i zarazem nieudolnie, niszcząc cechy identyfikacyjne wszystkich podpisów. W rezultacie użyteczność identyfikacyjna podpisów na dowodach osobistych została sprowadzona do poziomu bliskiego bezużyteczności.

---

[5] Często mianem dysleksji określa się zbiorczo wszystkie trzy postacie zaburzeń. Bierze się to zapewne stąd, iż mają one wspólną etiologię i z reguły współwystępują.

MIROSŁAW OWOC
KATEDRA KRYMINALISTYKI
UNIWERSYTET IM. A. MICKIEWICZA, POZNAŃ

Biometryczne wspomaganie niepełnosprawnych
Biometric assistance of disabled persons

Streszczenie

Omówiono skutki niepełnosprawności przy procedurach identyfikacyjnych oraz przyczyny narastającego aktualnie swoistego analfabetyzmu przy jednoczesnym starzeniu się społeczeństwa. Zaproponowano ustawowe wprowadzenie odcisku palca w procedurach weryfikacji tożsamości.

Abstract

The results of disability at identification procedures are described and causes of peculiar illiteracy observed now in Poland is discussed. Introduction of the fingerprint to legal authentication of people is postulated.

1. Potoczne rozumienie niepełnosprawności uwzględnia w pierwszym rzędzie trudności typu lokomocyjnego. Tymczasem ograniczenia równego dostępu przy korzystaniu ze współczesnych zdobyczy cywilizacyjnych mogą wynikać z niepełnosprawności przy procedurach identyfikacyjnych rozmaitego rodzaju. Wymienić tu warto w pierwszym rzędzie procedury składania podpisu na:

- poleceniach wypłaty (czekach),
- poleceniach przelewu,
- fakturach,
- rachunkach obciążeniowych (płatnych coraz powszechniej stosowaną kartą płatniczą),
- potwierdzeniach odbioru.

2. Na początku XXI wieku narasta (nie tylko w Polsce) fala swoistego analfabetyzmu. Ma on kilka niezależnych od siebie przyczyn, których skutki po części kumulują się. Wymienić tu należy:

- niski poziom motywacji uczniów (słabo rozwiniętych ruchowo przez nadmiar oglądania telewizji oraz niedomiar zajęć wychowania fizycznego w szkołach), którym wszelkie ruchy sprawiają trudność, a tym bardziej ruchy precyzyjne (istotne przy pisaniu),
- systematyczne obniżanie poziomu wymagań szkolnych w zakresie sprawności psychomotorycznej pisania,
- wzrost liczby dysgrafików[1], których liczba sięga 20% populacji dzieci w wieku szkolnym[2],
- zwiększoną możliwość korzystania z maszynopisania („komputeropisania").

Jeśli ktoś w wieku szkolnym nie wytworzył sobie automatyzmu pisania, to z wiekiem sprawność jego w tym zakresie raczej spada niż wzrasta. W rezultacie pojawia się tzw. analfabetyzm wtórny, objawiający się m. in. redukcją podpisu do postaci dziecięcych bazgrot lub „podpisywaniem się" literami na wzór druku. Towarzyszy temu brak rozeznania co do faktu oczywistej dysfunkcji i wynikająca stąd psychiczna niemożliwość podniesienia swej sprawności. Osoby takie stają się ofiarami licznych przestępstw (ich „podpisy" na dokumentach są często podrabiane). Ratunkiem dla tej grupy osób może być stosowanie odcisku palca obok podpisu na wszelkich dokumentach o doniosłości wyższej niż znikoma.

3. Systematycznie wzrasta w społeczeństwie procentowy udział emerytów. Osoby w podeszłym wieku częściej niż dawniej zmuszone są podpisywać różnego rodzaju dokumenty (wynika to z realiów funkcjonowania we współczesnym społeczeństwie), a wiadomo nie tylko pismoznawcom i urzędnikom bankowym, iż tzw. pismo starcze jest trudne do badania i dlatego łatwiejsze do skutecznego sfałszowania. Nadto starszych ludzi łatwiej okraść, co bezwzględnie wykorzystują złodzieje kieszonkowi kradnący dokumenty „na zamówienie" (wg rysopisu). Mało tego – starsi ludzie częściej są nieroztropni i noszą ze sobą całe książeczki czeków ROR i przez nieuwagę je gubią. Nie mogą jednak zgubić palca ani żaden złodziej nie może ukraść odcisku palca.

Dlatego istotną pomocą dla wymienionej grupy osób może być stosowanie odcisku palca zamiast albo obok podpisu.

4. Obecny poziom rozwoju sprzętu biometrycznego oraz systemów łączności jest dostatecznie zaawansowany, by postulować ustawowe wprowadzenie odcisku palca zamiast (lub przynajmniej obok) podpisu przy urzędowych procedurach weryfikacji tożsamości.

---

[1] Dysgrafia objawia się zaburzeniami w piśmie. Dysortografia objawia się niemożnością opanowania ortograficznych zasad pisowni. Wąsko rozumiana dysleksja objawia się zaburzeniami w samym czytaniu.

[2] Rypiński P., Dysgrafia - możliwość identyfikacji, w: Badania dokumentów. Kształtowanie się osobniczych cech pisma, Warszawa 1999, s. 97-137 [Zeszyty Metodyczne nr 3, Wyd. CLK KG Policji];
Korneć M., Możliwości identyfikowania pisma dysgraficznego, PROBLEMY KRYMINALISTYKI nr 229/2000, s. 27-35;
http://www.bpp.com.pl/ptd/prawny.htm z dnia 06.09.2001 r.;
http://dysleksja.univ.gda.pl/o_dysl.htm z dnia 06.09.2001 r.

Od zaraz, w pierwszej kolejności i najniższym kosztem społecznym można wprowadzić obowiązek składania odcisku palca (obok podpisu) na aktach notarialnych. Równie niewielkim kosztem można pobierać odcisk palca obok bankowego wzoru podpisu.

W obu wymienionych przypadkach odcisk palca byłby wykorzystywany pomocniczo, w razie zaistnienia trudności z identyfikacją na podstawie podpisu. Taki etap pośredni, bezinwestycyjny, pozwoliłby oswoić się ludziom z nową procedurą i poznać jej zalety. Etap zastosowania biometrycznego badania odcisków palców w procedurach identyfikacyjnych najczęściej powtarzanych byłby etapem następnym, przygotowującym powszechną rejestrację monodaktyloskopijną ([wymagającą powszechnego stosowania biometrii).

JERZY SAWICKI
INSTYTUT ELEKTRONIKI, TELEKOMUNIKACJI
I INFORMATYKI, POLITECHNIKA SZCZECIŃSKA

Wybór parametrów sygnału mowy użytecznych w rozpoznawaniu głosów
Choice of speech signal parameters useful for speaker recognition

Streszczenie

W referacie przedstawiono model wytwarzania mowy przez człowieka, będący podstawą do wyróżnienia parametrów sygnału pobudzenia krtaniowego i charakterystyki częstotliwościowej kanału głosowego. Omówiono podstawowe parametry niosące informację osobniczą: obwiednię widma, częstotliwości formantów, kształt i częstotliwość impulsów tonu krtaniowego. Zaprezentowano wyniki badań zmienności osobniczej i czasowej położenia formantów samogłosek na płaszczyźnie F1-F2.

Abstract

In this paper we present a human speech production model that forms a basis for determining the parameters of the excitation signal and of the vocal tract transfer function. The basic parameters that convey the speaker individuality are discussed: spectral envelope, formant frequencies, shape and frequency of excitations impulses. Results of the speaker variablity and variability of formant location over time on the F1-F2 plane are also presented.

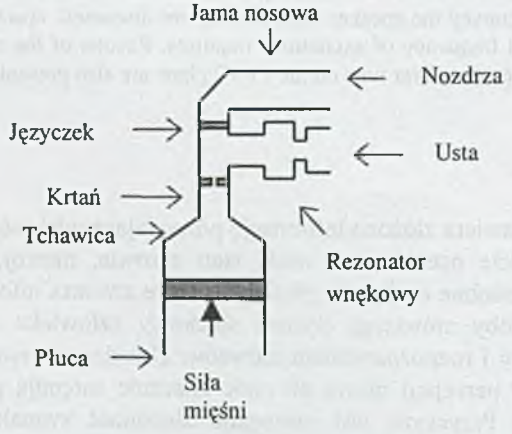
1. Wstęp

Sygnał mowy zawiera złożoną informację pozwalającą odebrać nie tylko znaczenie wypowiedzi, ale także ocenić płeć, wiek, stan zdrowia, nastrój, pochodzenie, wykształcenie i inne podobne cechy. W głosie jest także zawarta informacja pozwalająca na identyfikację osoby mówiącej. System słuchowy człowieka dobrze radzi sobie z rozumieniem mowy i rozpoznawaniem mówców. Urządzenia techniczne starające się naśladować procesy percepcji mowy na razie znacznie ustępują pod względem skuteczności działania. Przyczyną jest niezwykła złożoność sygnału mowy oraz jego zmienność czasowa i sytuacyjna. Niewielkie, ale odbierane przez słuch człowieka zmiany parametrów akustycznych niosą rozmaite przydatne informacje. Z drugiej strony ciągła zmienność parametrów akustycznych utrudnia określenie takich cech

akustycznych głosu, które mogłyby stanowić podstawę do rozpoznawania mówców. Naturalność i powszechność komunikacji głosowej skłaniają do poszukiwania w sygnale mowy cech osobniczych, gdyż wypowiedzi tej samej treści dowolnych dwóch osób zawsze różnią się od siebie pod względem mierzalnych cech fizycznych. Problem stanowi jednak fakt, że także dwie wypowiedzi tej samej osoby zarejestrowane w różnym czasie różnią się od siebie. Sygnał mowy może być opisany za pomocą bardzo wielu różnych parametrów zmieniających się w trakcie wypowiedzi. Różne techniki pomiaru głosu zastały opracowane dla potrzeb fonetyki akustycznej, foniatrii, logopedii, automatycznego rozpoznawania mowy, kompresji objętości informacyjnej w telekomunikacji i w wielu innych zastosowaniach. Wydaje się zatem, że nie ma potrzeby poszukiwania nowych metod reprezentacji sygnału mowy, ale należy skoncentrować się na zbadaniu użyteczności już istniejących. Znalezienie odpowiednich parametrów zadecyduje o skuteczności automatycznych systemów rozpoznawania mówców, które mogłyby stać się systemami biometrycznymi do identyfikacji lub weryfikacji tożsamości osoby mówiącej.

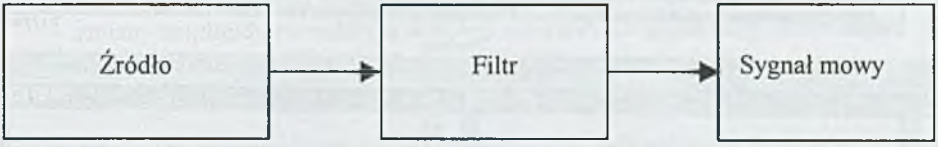
2. Model wytwarzania mowy

Analiza głosu człowieka musi uwzględniać jego strukturę czasowo-częstotliwościową, ta zaś zależy od zjawisk towarzyszących wytwarzaniu tego sygnału. Wytwarzanie mowy jest złożonym procesem, w który zaangażowane są miedzy innymi: płuca, oskrzela i tchawica, tworzące drogę doprowadzającą strumień powietrza do krtani, w której znajdują się fałdy głosowe (potocznie zwane strunami głosowymi) wytwarzające tak zwany ton krtaniowy, który jest następnie filtrowany w dalszej części traktu głosowego składającego się z odpowiednio ułożonych następujących narządów: języka, języczka, podniebienia twardego i miękkiego, zębów i ust, a w przypadku niektórych dźwięków także nozdrzy. Narządy te tworzą naturalny rezonator wnękowy wzmacniający pewne częstotliwości tonu krtaniowego. Uproszczony schemat wytwarzania mowy przedstawiono na rys. 1.



Rys. 1. Uproszczony schemat narządów mowy człowieka

W wielu przypadkach użyteczne jest przedstawienie procesu wytwarzania głosu za pomocą prostego modelu źródło-filtr (rys. 2), w którym dokonuje się umownego podziału na proces wytwarzania energii dźwięku (fonacja) i kształtowania jego charakterystyki częstotliwościowej (artykulacja).



Rys. 2. Model wytwarzania głosu typu źródło-filtr

Zaletą takiego modelu jest rozdzielenie dwóch etapów produkcji mowy oraz możliwość definiowania i pomiaru parametrów obydwu bloków: źródła i filtru. Zasadniczym problemem ograniczającym dokładność jest niedostępność samego sygnału źródła. Jedynym dostępnym pomiarowo sygnałem jest wyjściowy sygnał mowy, który jest splotem sygnału pobudzenia źródła i odpowiedzi impulsowej filtru. Istnieją jednak takie metody cyfrowego przetwarzania sygnału mowy (na przykład analiza homomorficzna), które pozwalają korzystając z przedstawionego modelu dokonać rozdzielenia obydwu tych funkcji. Omówiony model jest także właściwy dla opisu wytwarzania głosek bezdźwięcznych (wytwarzanych bez udziału krtani).

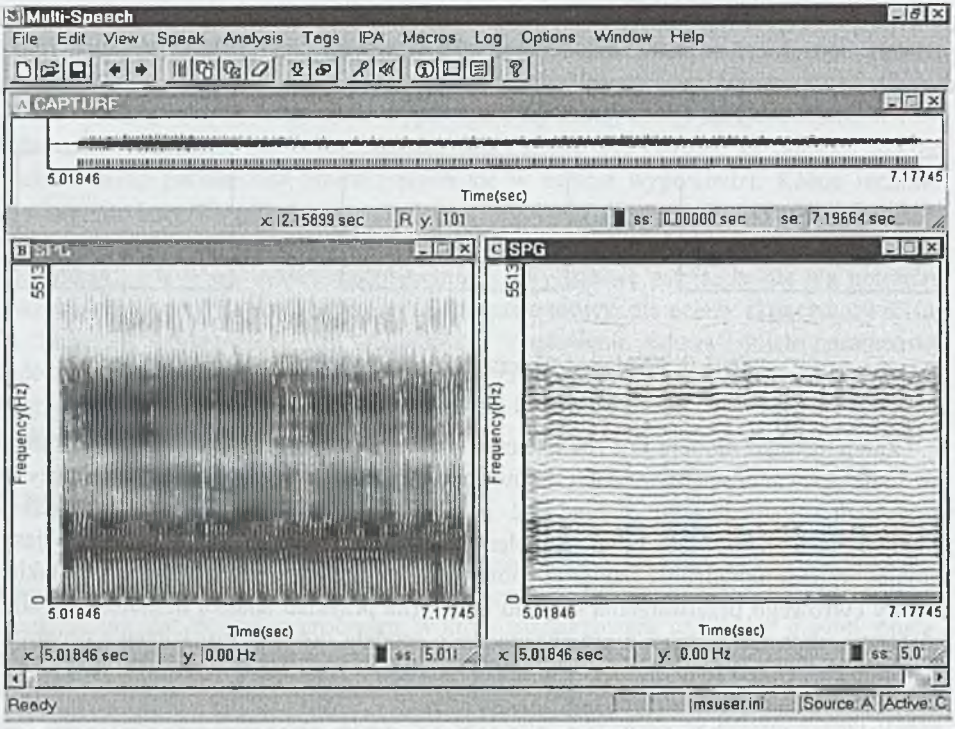
Uważa się, że parametry akustyczne źródła zawierają cechy osobnicze mówcy wynikające z indywidualnych cech anatomicznych narządu fonacyjnego oraz specyficznego sposobu sterowania zmianami wysokości głosu (zmiany tak zwanej częstotliwości podstawowej głosu F_0). Parametry akustyczne źródła odzwierciedlają zatem zarówno warstwę fizyczną, jak i psychiczną układu wytwarzania mowy. Należy także zauważyć, że analiza źródła nie zajmuje się treścią wypowiedzi (ta jest nadawana w układzie filtru), zatem może bazować na dowolnych próbkach wypowiedzi.

Parametry filtru także zawierają cechy osobnicze wynikające z budowy anatomicznej traktu głosowego. Wykorzystanie tej informacji do identyfikacji mówcy wymaga jednak posiadania próbek wypowiedzi o tej samej treści (tym samym składzie fonetycznym).

Model źródło-filtr jest użytecznym sposobem rozumienia procesu wytwarzania mowy, chociaż należy zastrzec, że stanowi znaczne uproszczenie w stosunku do rzeczywistych zjawisk i interakcji zachodzących w procesie mówienia.

3. Parametry opisujące sygnał mowy

Pierwsze próby rozpoznawania głosów w inny sposób niż za pomocą słuchu bazowały na porównaniu obrazów akustycznych wypowiedzi, tak zwanych spektrogramów. Istotnie każdy spektrogram (rys. 3) zawiera dużą ilość informacji w układzie współrzędnych czas-częstotliwość-amplituda.



Rys. 3. Dwa spektrogramy (SPG) głoski [a]: po lewej spektrogram szerokopasmowy, po prawej spektrogram wąskopasmowy, nad rysunkami spektrogramów pokazano przebieg czasowy sygnału z zaznaczonymi impulsami tonu krtaniowego

Obraz spektrogramu jest wynikiem dość złożonych obliczeń, w których należy zdecydować między innymi, czy chcemy uzyskać większą rozdzielczość czasową czy częstotliwościową. Zależnie od tego zmienia się obraz spektrogramu. Prawy spektrogram z rys. 3 prezentują dobrą rozdzielczość częstotliwościową pozwalającą porównywać częstotliwości harmoniczne tonu podstawowego oraz określić położenie tak zwanych formantów (charakterystycznych dla danej głoski), natomiast niedokładnie oddaje strukturę czasową wypowiedzi. Wynika to z faktu, że dokładna analiza częstotliwościowa wymaga użycia do obliczeń dużej ilości próbek przebiegu czasowego, co powoduje uśrednienie wyników w dziedzinie czasu. Dokładniejszą analizę w dziedzinie czasu można uzyskać zmniejszając ilość próbek w obliczeniach FFT – efektem jest jednak zmniejszenie dokładności w dziedzinie częstotliwości (lewy spektrogram na rys. 3). Porównując obydwa rodzaje spektrogramów z modelem wytwarzania mowy widać, że spektrogram wąskopasmowy reprezentuje przede wszystkim właściwości filtru, natomiast spektrogram szerokopasmowy lepiej odzwierciedla właściwości źródła. Porównywanie spektrogramów nie jest obecnie stosowane w rozpoznawaniu głosów, chociaż zastosowanie nowoczesnych metod analizy i przetwarzania obrazów może zmienić ten stan rzeczy.

Bardziej użyteczne jest posługiwanie się parametrami akustycznymi wynikającymi z modelu wytwarzania głosu typu źródło-filtr. Źródło pobudzenia krtaniowego może być opisane za pomocą następujących parametrów:

- wartość częstotliwości podstawowej F_0,
- przebieg zmian F_0 w trakcie wypowiedzi (tak zwany kontur intonacyjny),
- zmiany częstotliwości w kolejnych (sąsiednich) okresach drgań (ang. *jitter*),
- zmiany amplitudy pobudzenia w kolejnych okresach drgań (ang. *shimmer*),
- kształt przebiegu czasowego funkcji pobudzenia krtaniowego,
- widmo pobudzenia krtaniowego.

Parametry filtru kształtującego charakterystykę częstotliwościową wypowiedzi, które mogą mieć zastosowanie biometryczne to przede wszystkim:

- transmitancja filtru, która może być w dużym uproszczeniu reprezentowana przez tak zwane częstotliwości formantowe (maksima obwiedni),
- wyniki analizy przejść przez zero przebiegu czasowego w określonych pasmach częstotliwości,
- wyniki pasmowej analizy widmowej.

Ponadto w sygnale mowy można badać takie parametry, które trudno jednoznacznie zaklasyfikować do któregoś z bloków modelu, takie jak:

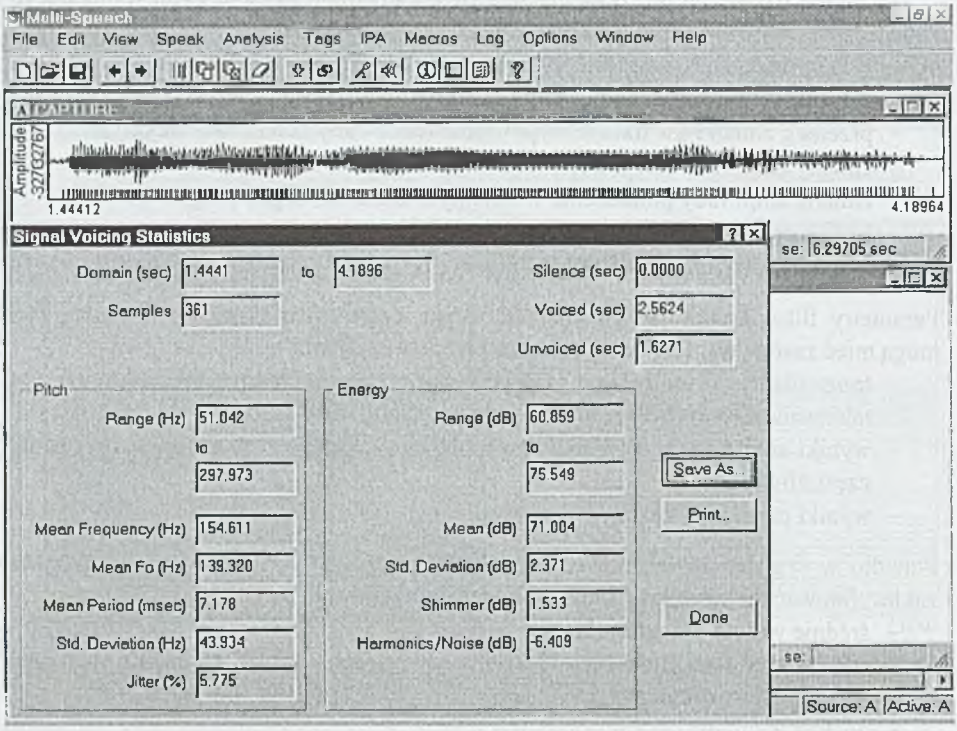
- średnie widmo długoterminowe,
- relacje czasowe elementów językowych (głosek, sylab, wyrazów) charakterystyczne dla każdego mówcy,
- analiza wyników akcentowania wyrazów.

Przy wyborze parametrów należy pamiętać, jakie próbki wypowiedzi będą rozpoznawane. Jeśli mają to być próbki dowolnej treści, to parametry stosowane w opisie filtru nie będą właściwe, gdyż silnie zależą od treści wypowiedzi. Konieczne jest w takich przypadkach ograniczenie się do parametrów opisujących źródło, które funkcjonuje w taki sam sposób przy różnych wypowiedziach. Jeżeli natomiast tekst wypowiedzi może być wcześniej ustalony jako tak zwane hasło, wtedy możemy korzystać z wszystkich wymienionych parametrów.

Pozostają jednak do rozwiązania problemy:

- synchronizacji czasowej wypowiedzi (różne tempa mówienia),
- zgodności analizowanego pasma częstotliwości (wpływ charakterystyk tłumieniowych urządzeń elektroakustycznych zastosowanych do rejestracji, przechowywania lub transmisji sygnału).

Zdaniem autora warto koncentrować się badaniach parametrów źródła. Z fizycznego punktu widzenia źródłem tonu krtaniowego są fałdy głosowe tworzące wraz z układem mięśni i nerwów generator aerodynamiczny napędzany energią wydychanego z płuc powietrza. Wymiary geometryczne i szczegóły budowy anatomicznej decydują o parametrach akustycznych sygnału pobudzenia. Chociaż sygnał ten nie jest bezpośrednio dostępny pomiarowo, wiele jego cech może być określonych na podstawie zarejestrowanego przez mikrofon głosu. Na rys. 4 przedstawiono przykładowe wyniki analizy komputerowej częstotliwości podstawowej F_0.



Rys. 4. Automatyczna analiza pobudzenia krtaniowego krótkiego fragmentu (około 2,75 sekundy) wypowiedzi

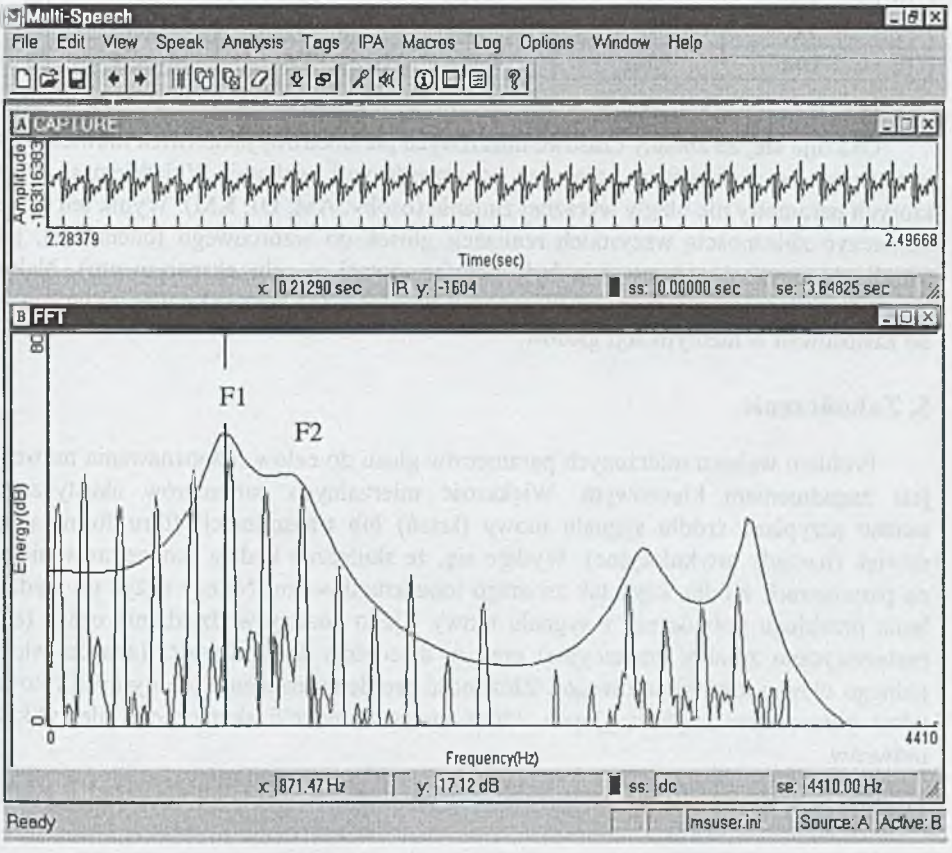
Analiza komputerowa dostarcza między innymi informacji o zakresie zmian wartości F_0 w trakcie mówienia, wartości średniej, parametrach *jitter* i *shimmer* wraz z ich analizą metrologiczną. Jeszcze więcej informacji powinno przynieść badanie czystego przebiegu pobudzenia. Jak wcześniej wspomniano sygnał ten nie jest bezpośrednio dostępny, gdyż przechodząc przez dalsze części traktu głosowego ulega modyfikacji zależnej od treści wypowiedzi. Problem z odtworzeniem sygnału pobudzenia nie został jeszcze dobrze rozwiązany. Obecnie stosowane metody to:

- dzielenie zespolonego widma sygnału mowy przez jego obwiednię (w niej zawarte są bieżące informacje artykulacyjne),
- analiza kepstralna, pozwalająca na zamianę operacji mnożenia sygnałów na ich sumowanie i w efekcie usunięcie (poprzez tak zwaną liftrację) funkcji odpowiedzi impulsowej kanału głosowego, a pozostawienie sygnału pobudzenia.

W warstwie szczegółowej pojawia się jednak szereg trudnych do rozwiązania problemów, które nie mogą dziwić, jeśli weźmie się pod uwagę, że model źródło-filtr to znaczne uproszczenie rzeczywistych interaktywnych procesów fonacji i artykulacji.

4. Wyniki badania zmienności czasowej i osobniczej parametrów głosu

Podstawowym problemem w analizie głosu jest zmienność jego parametrów wynikająca z tak wielu przyczyn, że nie sposób ich wymienić. Najpoważniejsze i najczęstsze wynikają z chorób układu oddechowego – zwykłe przeziębienie znacząco zmienia parametry sygnału pobudzenia wskutek obrzmienia narządów fonacyjnych. Także zmiana sytuacji, miejsca, upływ czasu zmieniają parametry głosu. Aby przekonać się o wielkości tych zmian przeprowadzono eksperyment, który polegał na rejestracji i porównaniu głosów dwunastoosobowej grupy studentów (wyłącznie mężczyźni) w odstępie jednego miesiąca. Materiał dźwiękowy stanowiły samogłoski podstawowe języka polskiego, z których do prezentacji wyników wybrano wypowiadaną w izolacji głoskę [a]. Dokonano pomiaru częstotliwości formantów F1 i F2. Wartości częstotliwości dwóch pierwszych formantów F1 i F2 zostały wykonane na podstawie obwiedni widma uzyskanej metodą predykcji liniowej (rys. 5).



Rys. 5. Analiza częstotliwości formantowych: w dolnym oknie widmo sygnału oraz obwiednia widma uzyskana techniką LPC, w górnym oknie przebieg czasowy (głoska [a])

Wyniki pomiarów zostały przedstawione w tabeli.

Tabela: Zmiany częstotliwości formantowych w głosce [a]

		Pierwsza analiza		Po miesiącu	
Lp.	Osoba	F1 [Hz]	F2 [Hz]	F1 [Hz]	F2 [Hz]
1	MP	781	1312	789	1257
2	TF	796	1250	835	1257
3	AM	843	1296	843	1289
4	KK	765	1054	757	1125
5	BG	804	1132	671	1117
6	TR	718	1117	710	1132
7	TC	750	1242	742	1304
8	MO	789	1210	820	1234
9	DJ	695	1210	695	1257
10	KM	937	1320	929	1320
11	PC	757	1304	781	1320
12	DM	742	1164	726	1179

Okazuje się, że zmiany czasowe mierzonych parametrów, jakkolwiek niewielkie, są porównywalne z różnicami pomiędzy poszczególnymi osobami. Wyjątkiem są głosy, których parametry nie uległy wyraźnej zmianie (osoby: AM, DJ, KM). Wynik ten należy tłumaczyć zbieżnością wszystkich realizacji głosek do wzorcowego fonemu [a], jaki starali się uzyskać mówcy (nie byli poinformowani o celu eksperymentu). Należy zaznaczyć, że według informacji literaturowych głoski [a] oraz [o] najlepiej nadają się do zastosowań w identyfikacji głosów.

5. Zakończenie

Problem wyboru mierzonych parametrów głosu do celów rozpoznawania mówców jest zagadnieniem kluczowym. Większość mierzalnych parametrów akustycznych można przypisać źródłu sygnału mowy (krtań) lub transmitancji filtru formującego dźwięk (narządy artykulacyjne). Wydaje się, że skuteczne będzie skoncentrowanie się na parametrach źródła, czyli tak zwanego tonu krtaniowego. Należy dążyć do wydzielenia przebiegu pobudzenia z sygnału mowy i jego analizy w dziedzinie czasu (charakterystyczne zmiany intonacyjne) oraz w dziedzinie częstotliwości (analiza widma jednego okresu tonu krtaniowego). Złożoność problemu nakazuje nie dyskwalifikować także parametrów artykulacyjnych, które mogą wzmocnić skuteczność identyfikacji mówców.

Literatura

[1] Ortega-Garcia, J., Gonzalez-Rodriguez J., Cruz-Llanas S.: Speech variability in automatic speaker recognition systems for commercial and forensic purposes, IEEE Aerospace and Electronics Systems Magazine, Volume: 15 Issue: 11, Nov. 2000, pp.: 27–32.

[2] Ben-Yacoub S., Abdeljaoued Y., Mayoraz E.: Fusion of face and speech data for person identity verification, Neural Networks, IEEE Transactions on, Volume: 10 Issue: 5, Sept. 1999, pp.: 1065–1074.

[3] Campbell J.P., Jr.: Speaker recognition: a tutorial, Proceedings of the IEEE, Volume: 85 Issue: 9, Sept. 1997, pp.: 1437–1462.

[4] Miller B.: Vital signs of identity [biometrics], IEEE Spectrum, Volume: 31 Issue: 2, Feb. 1994, pp.: 22–30.

ANDRZEJ W. MITAS
POLITECHNIKA ŚLĄSKA
UNIWERSYTET ŚLĄSKI

Ochrona zasobów własnych za pomocą ciągów losowych, parametryzowanych biometrycznie

Own resources protection by biometrically parametrised random sequences

Streszczenie

W artykule przedstawiono przykładowe zastosowanie techniki rozpraszania informacji w celu ochrony danych w pamięci masowej komputera. Problem ten ma szczególne odniesienie do komputerów personalnych, funkcjonujących w otwartej sieci teleinformatycznej. Dostęp do danych, specyfikowany hasłem, jest narażony na nadużycie. Obecny stan technologii oraz przede wszystkim stan prawny nie sprzyja lokalizacji i ukaraniu złodzieja informacji lub terrorysty, niszczącego bezkarnie cudzą własność. W artykule przedstawiono kompromisowe rozwiązanie problemu takiego włączenia komputera do sieci za pomocą standardowych środków technicznych, by bez obaw o integralność informacji uznanej przez posiadacza za niejawną, udostępnić pozostałe dane.

Abstract

In the paper exemplary application of the information dissipation to data protection in mass memory of computer is presented. The problem has particular reference to personal computers working in the open telecommunication computer network. Data access, defined by password, is exposed to abuse. The current state of technology and the legal status not favour the location and punishment of information thief or terrorist, destroying with impunity other property. The paper presents the compromise solution of the problem of such computer connection to the network with standard technical facilities, to without fear of integrity of the information declared by the owner as secrete, make available remaining data.

1. Wprowadzenie

Niezwykłe znaczenie przypisywane rozległej sieci teleinformatycznej Internet wynika z potrzeby szybkiego dostępu do informacji. Dostawca usług lub towaru może znacznie zintensyfikować własne obroty poprzez odpowiednią reklamę oraz błyskawiczny kontakt z potencjalnym klientem. Dotyczy to w zbliżonym stopniu osób

skłonnych do propagowania własnych poglądów i przekonań, co naturalnie w efekcie finalnym jest również formą reklamy, zachęcającej do nabycia pomysłu czy koncepcji, choćby filozoficznej. W historycznej już postaci handlu towarami, usługami i ideologiami dopracowano się przez tysiąclecia wypróbowanych mechanizmów samoobrony – w sklepie jest lada, czy zaplecze, albo hermetyczna dla klienta kasa, gdzie intruz nie ma dostępu, a „chętny" do wypróbowania eksportu towaru zabezpieczonego elektronicznie z dużego domu towarowego jest przy wyjściu „zagadywany" przez osoby, u których stosunek masy mięśniowej do objętości mózgu jest czasami ponadprzeciętny. W czasach propagacji poprzedniej ideologii był komitet, czy przydział talonów, ale chętny spoza „rodziny" do pobrania talonu nie miał szans – to także doskonały sposób ochrony zasobów własnych. Przykłady można mnożyć, ale w gruncie rzeczy postępowanie dostawcy jest proste – na stół wystawia towar, a wyposażenie osobiste ma odłożone w miejscu niedostępnym. Klient naruszający zasadę podziału na towar dostępny i niedostępny jest karany, w pewnych kulturach nawet bezlitośnie. Sytuacja sprzedawcy jest o tyle komfortowa, że wyraźnie wyodrębnia towary dostępne i niedostępne, przyznając im zupełnie odrębne miejsca przechowywania. Przepływ informacji, towaru lub usługi jest przez dystrybutora kontrolowany „osobiście", w szczególności za pomocą receptorów, których działanie jest zrozumiałe dla człowieka. Osoba lub instytucja nadużywająca uprawnień, na przykład zabierając ze sklepu masło do kieszeni miast do koszyka jest identyfikowana, zatrzymywana i karana; wszystko to dzieje się za pośrednictwem zmysłowych środków. Podobnie ma się rzecz w sensie kolejności wydarzeń w przypadku studenta próbującego wykraść pytania egzaminacyjne z zeszytu wykładowcy.

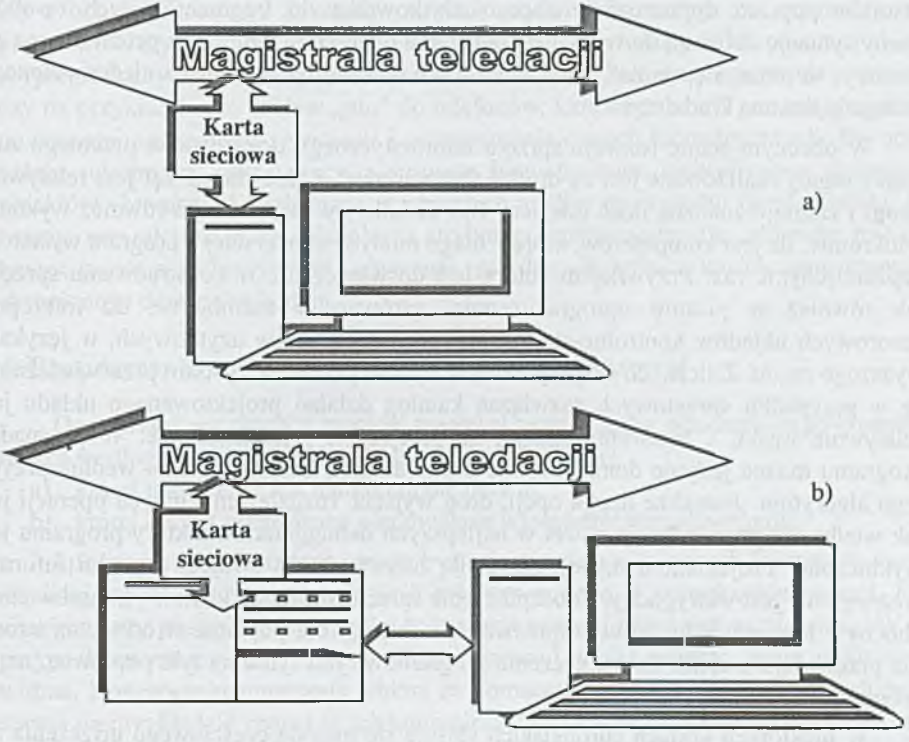
We wszystkich wzmiankowanych powyżej przypadkach istnieje nie tylko wyraźny podział na produkty własne i dostępne publicznie, lecz także podział ze względu na miejsce przechowywania produktów własnych i dostępnych publicznie.

Zupełnie innym zagadnieniem jest wypracowany system dozorowania naruszania integralności własnych zasobów w dystrybucji o tradycyjnym wymiarze (obserwacja, wyekstrahowanie złoczyńcy, ukaranie) wobec początkowej fazy takich środków w systemach teleinformatycznych. Dla pocieszenia tych, którym wymiana informacji jawi się jako wirtualny taniec nierzeczywistych „bitów" po przewodzie sieciowym, dołączonym do komputera, wystarczy przypomnienie, że osobisty, domowy komputer podłączamy do gniazda telefonicznego, a kasuje pieniądze za obsługę tego gniazda dystrybutor usług telekomunikacyjnych. Kiedy zaś uświadomimy sobie, że w obecnej skomputeryzowanej postaci sieci telekomunikacyjnej nawet a posteriori możemy uzyskać dane o rozmowach zarówno przychodzących jak i wychodzących, to teza o trudności identyfikacji połączeń internetowych, które także polegają na przepływie takiego samego rzeczywistego prądu elektrycznego, jest co najmniej wątpliwej jakości. Rodzi się wówczas naturalne pytanie: jakie są prawdziwe przyczyny braku należytej ochrony danych?

2. Ocena możliwości technicznych kompleksowego bezpieczeństwa w teledacji

Względy ekonomiczne wymuszają minimalizację nakładów sprzętowych. Najłatwiej zaoszczędzić w tych miejscach, których się nie rozumie, a więc w szczególności w systemach zabezpieczeń. Podobnie w warunkach domowych instalujemy zamki

i systemy alarmowe „kompatybilne" z zabezpieczeniami atestowanymi o wysokich walorach technicznych. Gdyby właściciel zabezpieczanej posesji pojmował szczegóły techniczne oferowanych rozwiązań, wówczas wyrobiłby sobie zdanie o tej „kompatybilności". Na podobieństwo systemów ochrony stosowanych w codziennym życiu można również w teledacji zainstalować dodatkowy terminal interfejsowy do komunikacji komputera osobistego z siecią. Na rysunku 1a zilustrowano typowe rozwiązanie z kartą sieciową. O tym, jak wiele szkód powstaje w tego rodzaju konfiguracjach wiadomo powszechnie. Dodatkowy komputer sterujący wymianą informacji pomiędzy otoczeniem i systemem personalnym – rys. 1b – pełni rolę czytelni w bibliotece publicznej. Do pomieszczenia czytelni może dostać się każdy obywatel z ulicy, natomiast dostarczanie wybranych (także zamawianych) czasopism czy książek jest w gestii personelu, który ma prawo wejścia do magazynu bibliotecznego. O niezawodności takiego systemu nie trzeba nikogo przekonywać. Nie ma również potrzeby argumentowania, że w realnych warunkach niektórych krajów europejskich nadanie czytelnikowi uprawnień penetracji magazynów w krótkim terminie doprowadziłoby do postawienia składu w stan likwidacji.



Rys. 1. Dołączenie komputera osobistego do sieci teleinformatycznej:
a) bezpośrednie, b) pośrednie

Adaptacja wypróbowanych modeli administrowania detalami życia codziennego do specyfiki informatycznej jest możliwa naturalnie nie tylko w kontekście powyższego przykładu. Wysokie zazwyczaj koszty takiej aplikacji wynikają po prostu stąd, że świat wirtualny w binarnym ujęciu jest prymitywny, a życie codzienne jest skomplikowane i przede wszystkim wielowartościowe. W dalszej części artykułu przedstawiono propozycję takiej techniki samoobrony, która nie ma precedensu w innych dziedzinach życia i polega na czasowym zaburzeniu struktury danych, przechowywanych we własnej pamięci masowej.

3. Koncepcje ochrony zasobów informatycznych

Zabezpieczenia biometryczne znane są od dawna (np. odcisk palca w dowodzie osobistym). Genetycznie uwarunkowana unikalność kodu jest gwarantem niezawodnej identyfikacji. Stosowane współcześnie algorytmy rozpoznawania obrazu (w tym przypadku parametrów biometrycznych) są czasami jeszcze zawodne – mówi się przecież o współczynniku błędnych zakwalifikowań lub błędnych odrzuceń. Zastosowania biometrii w ochronie koncentrują się obecnie na weryfikacji uprawnień dostępu lokalnego lub zdalnego do komputera. Trzeba jednak mieć na uwadze, że w chwili udostępnienia zasobów poprzez dopuszczenie obcego użytkownika do fragmentów tych zasobów mamy sytuację zbliżoną do wpuszczenia petenta na teren urzędu. Jeśli petent ów ma złe zamiary, to może się okazać, że mimo zakazu uda się on w miejsca niedozwolone, a następnie dokona kradzieży.

W obecnym stanie rozwoju sprzętu informatycznego dozorowanie przebiegu zdarzeń z reguły realizowane jest na drodze programowej, ponieważ **sprzęt jest** relatywnie **drogi** i zajmuje znaczną ilość miejsca. Ten dodatkowy sprzęt trzeba również wykonać tylokrotnie, ile jest komputerów, które z niego miałyby skorzystać, a program wystarczy napisać jedynie raz. Przywilejem autora jest doświadczenie w konstruowaniu sprzętu, jak również w pisaniu oprogramowania, zarówno w asemblerze, do mikroprocesorowych układów kontrolno-sterujących jak i programów użytkowych, w językach wyższego rzędu. Z licznych eksperymentów wynika przede wszystkim przeświadczenie, że w przypadku sprzętowych rozwiązań katalog działań projektowanego układu jest relatywnie wąski, a konkretne funkcje są przejrzyste i jednoznaczne. W przypadku programu można jedynie domniemywać o poprawnym funkcjonowaniu według przyjętego algorytmu. Jednakże liczba opcji, dróg wyjścia, rozgałęzień i innych operacji jest tak wielka, że prześledzenie nawet w najlepszych debuggerach struktury programu jest wykluczone. Projektant uznający całkowitą niezawodność swojego wyrobu informatycznego nie jest wiarygodny. Zabezpieczenie sprzętowe jest ewidentne i konsekwentne, choćby z tego powodu, że w półprzewodnikach prąd nie popłynie w odwrotną stronę, niż przewiduje projekt. Zabezpieczenie programowe jest tylko na tyle poprawne, na ile programista rozumie jego działanie.

W niektórych krajach europejskich stosuje się metodę częściowego niszczenia zasobów w celu ochrony przed kradzieżą (autor ma tu na myśli wypalanie inskrypcji na desce klozetowej itp.). Ten nieco drastyczny sposób można próbować przenieść do dziedziny ochrony danych, koncentrując wysiłek raczej na takim zmodyfikowaniu własnych zasobów, by stały się one nieatrakcyjne dla złodzieja, stanowiąc mimo to dla właściciela nadal pełnowartościowy towar.

Informacja w komputerze może przyjąć dowolną postać, w szczególności zgodną z umowami, stanowiącymi podstawę międzynarodowego funkcjonowania informatyki. Kompatybilność oprogramowania i funkcji sprzętowych jest wprawdzie pojęciem względnym (jak wiadomo istnieją takie firmy, które po wprowadzeniu własnych redundantnych formatów same się w nich gubią), niemniej jednak wraz z rozwojem informatyki wyraźnie zarysowuje się tendencja unifikacji, zwłaszcza przy dostępie do sieci rozległej. Coraz rzadziej na ekranie pojawiają się irytujące znaczki w miejsce liter „nietypowych" w języku angielskim. Standaryzacja jest przecież podstawą efektywnej reklamy i atrakcyjności przekazu własnych treści w sieci. Tym atrybutem wyróżnia się informacja udostępniana innym, przypadkowym użytkownikom. Przez inwersję można przyjąć, że informacja osobista może mieć zupełnie oryginalną postać, w szczególności zakodowaną. Zastosowanie techniki rozpraszania widma pozwala na totalne zaburzenie informacji niejawnej. Omawiane zagadnienie można by odnieść do codzienności za pomocą absurdalnego przykładu, że właściciel tartaku przechowuje deski na swojej posesji i przed kradzieżą zabezpiecza je w ten sposób, iż tnie je na drobne, nikomu nieprzydatne kawałki. W celu użycia desek stosuje czynność odwrotną do cięcia i odzyskuje całe, zdrowe deski. W zarządzaniu informacją taki algorytm jest jednak możliwy. Mówimy wówczas o szyfrowaniu danych, a o sposobach szyfrowania można dowiedzieć się z bogatej literatury. Z reguły problem użytkownika polega na zapamiętywaniu parametrów szyfrujących. W celu oceny ilości zapamiętywanych na co dzień danych kryptograficznych zaleca się pobieżne obliczenie ilości kart magnetycznych w portfelu, czy na przykład liczby kodów „pin" do telefonów, kart, kont etc. Z pomocą przychodzi nowoczesna technologia rejestracji i przetwarzania danych biometrycznych. Do normy należą rejestratory czasu pracy, sterowane biometrycznie, identyfikatory dostępu do obiektów chronionych, działające w oparciu o analizę np. kształtu dłoni, rysunku linii twarzy, czy odcisku palca. Wspólnym atrybutem, znamiennym dla człowieka jest relatywnie proste przechowywanie i używanie tych danych, które w konkretnym przypadku chronionego dostępu są kodem.

4. Rozpraszanie widma informacji w pamięci masowej

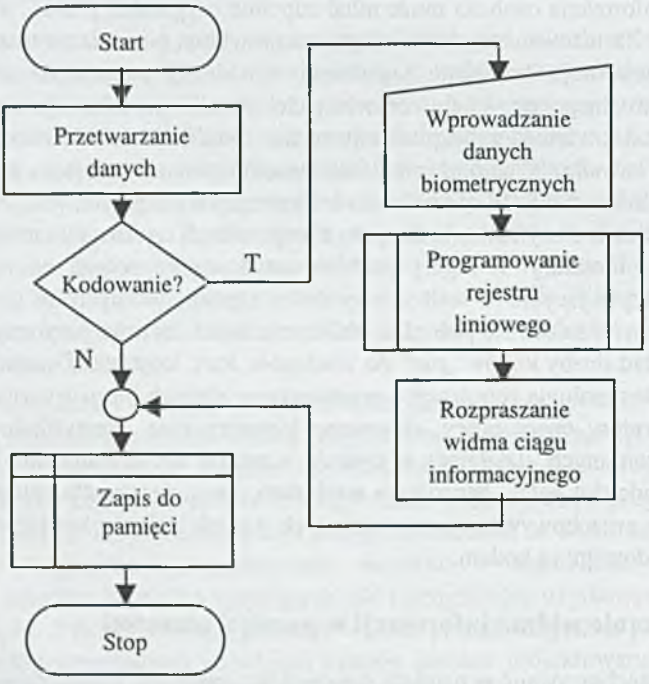
Dane przechowywane w pamięci masowej przeciętnego, standardowego komputera można według własnego uznania podzielić na informację:

a) której ujawnienie jest nam obojętne oraz tę,
b) której odczyt przez osobę niepowołaną wywołałby niezadowolenie.

Informacja ogólnodostępna może być rejestrowana w typowych formatach danych. Złodziej, wykradający naszą własność zobaczy te dane w znanej sobie postaci. Przeciwnie należy postąpić w przypadku informacji uznanej przez nas za niejawną. W tym przypadku wystarczy w trakcie realizacji operacji zapisu wybrać opcję rozpraszania widma. Koncepcję rozpraszania widma za pomocą ciągu liczb pseudolosowych przedstawia na przykładzie znanej w telekomunikacji metody wielodostępu kodowego pozycja [5]. Na rysunku 2 przedstawiono w skrócie algorytm preparacji zbioru danych w trakcie operacji zapisu z alternatywnym wyborem opcji szyfrowania. Dane, stanowiące rozproszone widmo informacji, będą oczywiście zupełnie nieczytelne dla złoczyńcy, a ich postać będzie taka, jak w przypadku zbiorów binarnych, np. danych pomiarowych z urządzenia przemysłowego – na pozór nie skorelowanych. Oczywiście dane te włamywacz może próbować po prostu zniszczyć, dlatego że jego działanie jest

zorientowane na destrukcję w ogóle (podobnie jak u każdego innego złodzieja, który nic nie znajdując w mieszkaniu, niszczy w złości cokolwiek). Znacznie łatwiej jednak zablokować zdalne wykonywanie jednej konkretnej funkcji – np. otwierania zbioru do zapisu – niż kontrolować, czy dane przetwarzane przez osobę trzecią pochodzą z właściwych zasobów.

Informacja poddana celowemu zaburzeniu w trakcie zapisu, po jej spreparowaniu, odróżnia się od danych zapamiętanych w formatach typowych. Poza tym istnieje możliwość wprowadzenia dodatkowego znacznika, po to by w trakcie otwierania zbioru do odczytu zastosować odpowiedni dekoder.



Rys. 2. Algorytm kodowania informacji

5. Wielowejściowy rejestr liniowy w funkcji układu modyfikacji informacji

Zasadniczy problem kodowania informacji ma dwa aspekty:

a) metoda szyfrowania,
b) parametry szyfru.

Jedną z metod o znakomitych właściwościach jest naturalnie rozpraszanie widma za pomocą ciągów wyjściowych z generatorów liczb pseudolosowych. Z obszernej literatury dotyczącej struktur i opisu rejestrów liniowych wynika, że znakomitymi

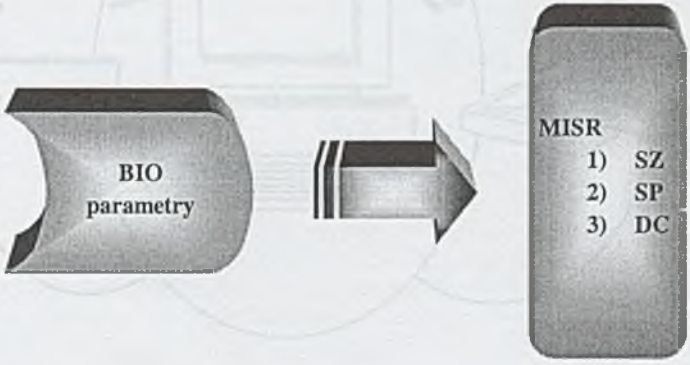
właściwościami charakteryzują się rejestry, których sprzężenia zwrotne opisane są wielomianami pierwotnymi. Katalog tych wielomianów jest naturalnie ograniczony, na podobieństwo zbioru liczb pierwszych w dziedzinie liczb naturalnych. Rejestr liniowy ma kilka parametrów, którym można nadać określone wartości. W szczególności są to:

1) długość rejestru, wyznaczana w zasadzie poprzez wielomian sprzężenia zwrotnego,
2) stan startowy rejestru,
3) długość ciągu rozpraszającego.

Można przyjąć, że dla jakości kodowania (określanej przez trudność wyznaczenia wielomianu sprzężenia zwrotnego) lepiej jest korzystać ze zbioru wielomianów pierwotnych. Wówczas w praktyce można przyjąć, że wielomian charakterystyczny jest określony poprzez numer wielomianu pierwotnego, określający jego pozycję w zbiorze.

Dane biometryczne, znamienne dla użytkownika kodowanej informacji, są unikalne. Ich wprowadzenie w fazie rozpraszania widma kodowanej informacji – zapis niejawnego zbioru na dysku – pozwala zaprogramować rejestr liniowy, bez potrzeby przyporządkowywania danemu zbiorowi danych określonych słów kodowych, haseł etc.

Użytkownik może jedynie wprowadzić sobie własną specyfikę kodowania, polegającą np. na tym, że listy służbowe „programuje" palcem wskazującym prawej ręki, a rodzinne kciukiem lewym lub prawym.

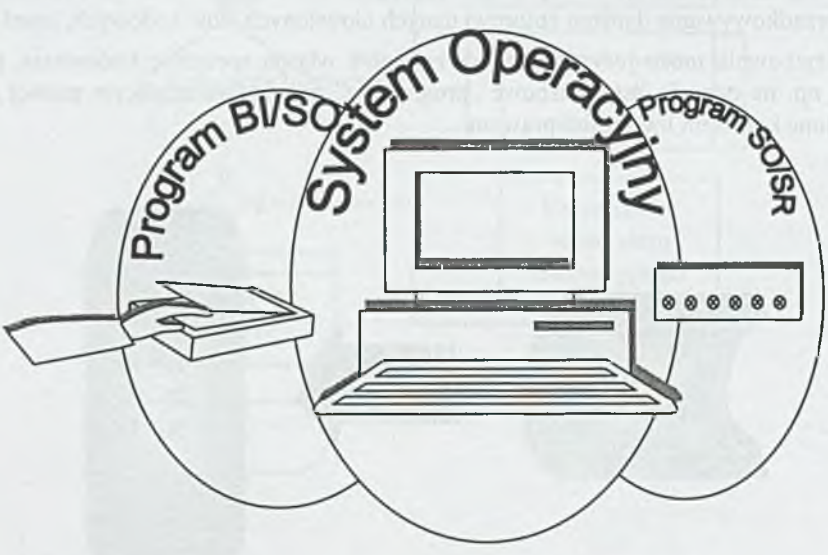


Rys. 3. Programowanie stanu rejestru liniowego

6. Podsumowanie

Obowiązek ochrony własnych danych przed naruszeniem przez złodzieja w obecnej, początkowej fazie rozwoju rozległych sieci teleinformatycznych jest raczej przerzucany na użytkownika komputera personalnego. Przypomina to znane skądinąd przypadki spania w nowo zakupionym, szczególnie wartościowym samochodzie małolitrażowym. Posiadacz informacji może bronić się przed złoczyńcą poprzez separowanie się od sieci teleinformatycznej. Jeśli przyjmiemy uczestnictwo w globalnym

rynku informacji, wówczas możemy zapewnić sobie bezpieczeństwo za pomocą dodatkowego sprzętu. Koszt takiego rozwiązania zmusza nas jednak do poszukiwania innych rozwiązań, w szczególności programowych. Na rysunku 4. przedstawiono w zarysie koncepcję takiego rozpraszania widma informacji, które z jednej strony zapewnia zupełne bezpieczeństwo, a z drugiej zwalnia użytkownika z pamiętania haseł i kluczy. To duże bezpieczeństwo zapewnione jest dzięki temu, że kody liniowe mają charakter sekwencyjny i przy założeniu dowolnego wielomianu charakterystycznego są w praktyce niemożliwe do rozszyfrowania. Dodatkowym wsparciem tego kodu jest programowanie rejestru znamiennymi, osobniczymi parametrami biometrycznymi, dzięki czemu nawet znajomość algorytmu kodowania nie daje możliwości stworzenia ciągu rozpraszającego widmo informacji użytkownika. Dane biometryczne są przetwarzane przez program oznaczony na rysunku BI/SO. Program ten konfiguruje rejestr liniowy. Ciąg wyjściowy tego rejestru w trakcie operacji zapisu do pamięci masowej modyfikuje tę informację, której nie należy udostępniać. System operacyjny czuwa nad całością współpracy tego oprogramowania.



Rys. 4. Oprogramowanie rozpraszania informacji w zasobach własnych

Wymiana informacji z otoczeniem jest realizowana przez program oznaczony symbolem SO/SR, zapewniający udostępnianie wszelkich zasobów. Program ten powinien czuwać jedynie nad zabezpieczeniem systemu przed totalną destrukcją, polegającą na niszczeniu zbiorów, które są dla złodzieja nieczytelne. Dane pobrane nieprawnie są oczywiście dostępne w postaci zbiorów binarnych, nie są jednak wiele warte bez tych samych sekwencji, którymi dokonano rozproszenia widma. Ogromne długości cyklu (okres powtarzalności ciągów losowych) i parametryzowanie za pomocą charakterystycznych dla użytkownika wartości stanowią zalety proponowanej koncepcji ochrony własnych zasobów w komputerze dołączonym do rozległej sieci teleinformatycznej.

Literatura

[1] Andrzej Mitas, Agnieszka Janaszek: System modyfikacji kodu elektronicznego podpisu. Pierwsza Konferencja pn. Metody biometryczne w systemach identyfikacji i kontroli dostępu. Warszawa, 9 listopada 2000.

[2] Andrzej Mitas: Zastosowanie funkcji rejestru liniowego do osobistej ochrony danych w przesyle informacji. I Konferencja pn. Metody biometryczne w systemach identyfikacji i kontroli dostępu. Warszawa, 9 listopada 2000.

[3] Andrzej Mitas, Agnieszka Janaszek: An idea of the test pattern generator for the pseudorandom testing of MVL circuits. The VII Int. Conf. Advanced Computer Systems, Szczecin, Poland 2000.

[4] Ryszard Zieliński: Generatory liczb losowych. Programowanie i testowanie na maszynach cyfrowych. Wydawnictwa Naukowo-Techniczne. Warszawa 1972.

[5] Witold Hołubowicz, Piotr Płóciennik, Andrzej Różański: Systemy łączności bezprzewodowej. Poznań 1997.

WALDEMAR GRANISZEWSKI
INSTYTUT STEROWANIA I ELEKTRONIKI PRZEMYSŁOWEJ
POLITECHNIKA WARSZAWSKA

Metody neuronowe w kodowaniu i kompresji informacji
Neural methods in coding and data compression

Streszczenie

W artykule zostały przedstawione metody kompresji informacji przy wykorzystaniu modeli bazujących na sztucznych sieciach neuronowych (SN). SN posiadają zdolności generalizujące, co umożliwia im eliminacje nadmiarowej i nieistotnej informacji. Zdolności te predystynują je jako efektywne narzędzie do kompresji stratnej. W pracy zostały omówione podstawy redukcji informacji bazującej na przekształceniu PCA oraz metoda kwantyzacji wektorów. Przedstawiono także architektury sieci umożliwiające kompresję w oparciu o ww. techniki: sieć perceptronową z jedną warstwą ukrytą i sieć samoorganizującą się typu topologicznego. Podstawy teoretyczne są zilustrowane przykładem kompresji informacji zawartej w obrazach cyfrowych.

Abstract

Abstract: In this paper methods for the data compression using models based on artificial neural networks (NN) are presented. NN's possess generalisation's ability thanks to which excessive and inessential information can be eliminated. Therefore NN's are an effective tool for loss compression. In this paper the elements of data compression based on Principal Component Analysis (PCA) and Vector Quantisation (VQ) technique are discussed. Author presented also NN architecture enebling compression based on the technique mentioned above, i.e. Multilayer Perceptron Network (MLP) with one hidden layer and self-organising map. The theoretical background is illustrated with an image compression example and results for both NN's are discussed.

1. Wprowadzenie

We współczesnym świecie, przy zastosowaniu komputerów i szeroko rozumianych technik multimedialnych, istnieje ogromne zapotrzebowanie na przepływ i gromadzenie informacji, która zakodowana jest w postaci ciągu bitów. Przesyłanie jej, czy też zapamiętanie wymaga nośników o określonej pojemności. Standardowym przykładem może być tutaj przesyłanie obrazów cyfrowych, które w zależności od rozdzielczości, ilości kolorów, zajmują dużą przestrzeń pamięci. Dla przykładu: obraz o rozmiarze

512 × 512 pikseli, zawierający 256 odcieni szarości, bez kompresji, zajmuje ponad 262 KB. Pomimo zwiększających się możliwości fizycznych przy zapisie i przesyłaniu danych istnieje ciągle wielkie zainteresowanie możliwościami kompresji informacji. Metody kompresji danych można podzielić ogólnie na:

- bezstratne,
- stratne.

Metody bezstratne kompresji to takie, które po kompresji i dekompresji nie powodują utraty informacji. Stosowane są m.in. do archiwizacji danych. Przykładem tych metod są algorytmy Ziv-Lempla, metody Huffmana, Shannona-Fano, kodowanie arytmetyczne i wiele innych.

Metody stratne kompresji to takie, w których w wyniku kompresji i dekompresji danych następuje pewna utrata informacji. Na ogół dąży się do tego, żeby utrata informacji dotyczyła czynników nieistotnych dla danej reprezentacji danych. Często jest to działanie korzystne z punktu widzenia redukcji szumu [16].

Sztuczne sieci neuronowe z zasady swojego działania posiadają zdolności generalizujące – eliminując nadmiarową i nieistotną informację, stąd cieszą się uznaniem jako narzędzie do kompresji stratnej. Dosyć często wykorzystywane są metody kwantyzacji danych (wektorowej i skalarnej) [3][5][10][11][12][21].

Innym sposobem redukcji informacji są metody bazujące na transformacie Karhunena-Loévego [23]. Należą do nich: rozkład wg składowych głównych – PCA (ang. *Principal Component Analysis*) [4][14][17], rozkład SVD (ang. *Singular Value Decomposition*) [8], rozkład względem składowych niezależnych – ICA (ang. *Independent Component Analysis*) [1].

2. Algorytmy kompresji neuronowej

2.1. Sieci jednokierunkowe

2.1.1. Podstawy matematyczne kompresji bazującej na rozkładzie na czynniki główne PCA

Niech dany będzie zbiór P danych pomiarowych (np. próbek z obrazów) w postaci wektorów o długości N, tzn. $\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_P]$, przy czym $\mathbf{x}_i = [x_1, x_2, \ldots, x_N]^T$ dla każdego $i = 1, \ldots, P$. Zależność pomiędzy poszczególnymi danymi pomiarowymi opisuje macierz wartości oczekiwanej macierzy autokorelacji $\mathbf{R}_{xx} = E[xx^T] = \langle \mathbf{x}\mathbf{x}^T \rangle$. Jak podano w pracy [18] wartość tej macierzy można określić z zależności

$$\mathbf{R}_{xx} \approx \frac{1}{P} \sum_{i=1}^{P} \mathbf{x}_i \mathbf{x}_i^T = \frac{1}{P} \mathbf{X}\mathbf{X}^T \tag{1}$$

Oznaczając poprzez λ_i wartości własne, zaś poprzez $\mathbf{w}_i = [w_1, w_2, \ldots, w_N]^T$ ortogonalne wektory własne macierzy $\mathbf{R}_{xx}$, można związek pomiędzy wartościami własnymi, a wektorami własnymi macierzy zapisać zależnością $\mathbf{R}_{xx}\mathbf{w}_i = \lambda_i \mathbf{w}_i$. Porządkując w kolejności malejącej wartości własne w taki sposób, że $\lambda_1 > \lambda_2 > \cdots > \lambda_N \geq 0$ i odpowiednio powiązane z nimi wektory własne, można zdefiniować takie przekształcenie macierzy pomiarowej (obrazu), aby nastąpiła redukcja wymiarów wektora pomiarowego z długości N do długości K, bez utraty jakości poniżej określonego progu. Wybierając K największych wartości własnych i formując z odpowiadających im wektorów własnych macierz $\mathbf{W}$, można zdefiniować przekształcenie PCA: $\Re^N \rightarrow \Re^K$, przy czym $K < N$, w następujący sposób

$$\mathbf{y} = \mathbf{W}\mathbf{x} \tag{2}$$

gdzie: $\mathbf{x} = [x_1, x_2, \ldots, x_N]^T$, $\mathbf{x} \in \Re^N$ wektor przed przekształceniem,

$\mathbf{y} = [y_1, y_2, \ldots, y_K]^T$, $\mathbf{y} \in \Re^K$ wektor K składników głównych PCA,

$\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_K]^T$, $\mathbf{W} \in \Re^{K \times N}$ – macierz wektorów własnych odpowiadających K największym wartościom własnym macierzy $\mathbf{R}_{xx}$. Wektor $\mathbf{y}$ stanowi skompresowaną informację o wektorze $\mathbf{x}$. Wektor pomiarowy może zostać teraz estymowany na podstawie wektora $\mathbf{y}$ z zależności

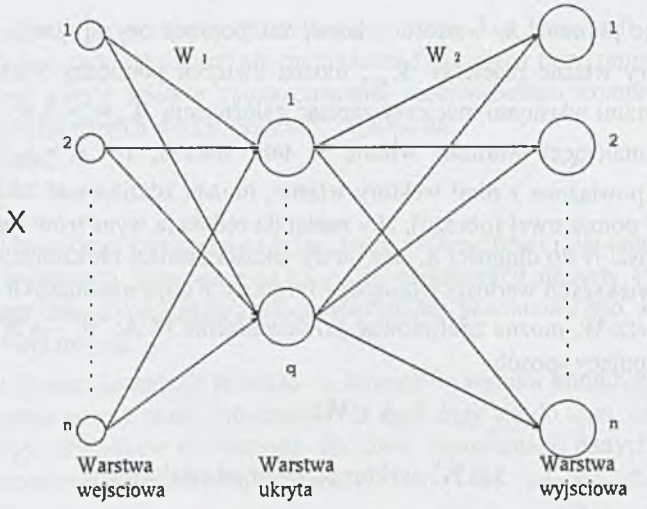
$$\hat{\mathbf{x}} = \mathbf{W}^T\mathbf{y} \tag{3}$$

z błędem przekształcenia PCA, które dla K składników głównych można wyznaczyć na podstawie wzoru

$$E_r = \sum_{i=K+1}^{N} \lambda_i . \tag{4}$$

2.1.2. Architektura sieci realizującej zadanie kompresji w oparciu o metodę PCA

Własności rozkładu macierzy względem wartości głównych – PCA wykorzystane przy budowie sieci neuronowych umożliwiają znaczne zmniejszenie informacji, oczywiście kosztem dokładności, co zostało wcześniej pokazane.



Rys. 1. Architektura sieci perceptronowej do kompresji i dekompresji.

Rys. 1 przedstawia architekturę sieci jednokierunkowej wykorzystanej w pracy [18] do kompresji obrazów w oparciu o rozkład PCA. Liczba węzłów warstwy wejściowej i wyjściowej sieci jest sobie równa i zawiera N jednostek – tyle, ilu elementowy jest wektor podawany na wejście i oczekiwany na wyjściu sieci. W warstwie ukrytej sieci znajduje się q neuronów, które połączone są poprzez macierz wag $\mathbf{W}_1$ z wejściem sieci i poprzez macierz wag $\mathbf{W}_2$ przekazują sygnał na wyjście sieci. Macierz $\mathbf{W}_1$ odpowiada za kompresję informacji, zaś macierz $\mathbf{W}_2$ odpowiada za odtworzenie informacji. Na podstawie przepływu sygnału wartość wyjścia sieci można zapisać równaniem

$$\hat{\mathbf{x}} = \mathbf{W}_2 \cdot \mathbf{W}_1 \cdot \mathbf{x} \tag{5}$$

W procesie uczenia dąży się do takiego doboru macierzy wag $\mathbf{W}_1$ i $\mathbf{W}_2$, aby błąd pomiędzy wyjściem a wejściem sieci był minimalny. W tym celu wprowadza się funkcję celu daną równaniem

$$E = \frac{1}{2}\sum_{i=1}^{P}\sum_{j=1}^{N}(x_j^{(i)} - \hat{x}_j^{(i)})^2 \tag{6}$$

gdzie P jest liczbą wektorów uczących, N – długością wektora.

Istnieje wiele metod adaptacji wag $\mathbf{W}_1$ i $\mathbf{W}_2$, część z nich bazuje na uogólnionej regule Hebba, są też metody wykorzystujące rozkład SVD. Liczba neuronów q w warstwie ukrytej decyduje o liczbie składników głównych przekształcenia PCA i jednocześnie o stopniu kompresji informacji.

2.2. Sieci samoorganizujące się

2.2.1. Architektura sieci

Do najbardziej rozpowszechnionych sieci samoorganizujących się należy Mapa Kohonena. Uczenie takiej sieci opiera się na mechanizmie konkurencji między poszczególnymi neuronami. Niech wzorce uczące v są elementami podprzestrzeni V zawartej w $\Re^N$, co można zapisać $v \in V \subseteq \Re^N$. Miarą przystosowania danego neuronu do wzorca uczącego jest odległość pomiędzy wagą neuronu $\mathbf{w}_i$, a wzorcem uczącym v, oznaczona jako: $d_i(\mathbf{v}, \mathbf{w}_i) = \|\mathbf{v} - \mathbf{w}_i\|$. W zależności od przyjętej metryki odległość ta może być wyrażona w różny sposób. Najczęściej przyjmuje się metrykę Euklidesową. Przy K neuronach, neuron dla którego odległość od podanego wzorca jest najmniejsza, tzn. $d_i(\mathbf{v}, \mathbf{w}_i) \leq d_j(\mathbf{v}, \mathbf{w}_j) \quad j = 1,\ldots,K$, uznawany jest za zwycięzcę. Adaptacja wag neuronów opiera się o jedną z dwóch zasad:

- zwycięzca bierze wszystko – WTA (ang. *Winner Takes All*),
- zwycięzca bierze większość – WTM (ang. *Winner Takes Most*).

W pierwszej z tych reguł uaktualnieniu ulegają tylko wagi jednego neuronu – zwycięzcy, wyłonionego poprzez mechanizm konkurencji. Druga reguła dopuszcza również aktualizację wag innych neuronów. Przy takim sposobie uczenia dla pewnych danych wejściowych $\mathbf{v} \in V$ odwzorowaniem będzie waga tego samego neuronu $\mathbf{w}_i$. Przestrzeń danych wejściowych V zostanie w ten sposób podzielona na K podprzestrzeni, tzn. $V = V_1 \cup V_2 \cup \cdots \cup V_K$, zaś odwzorowaniem każdej z nich będzie waga (położenie) odpowiadającego jej neuronu, tzn. nastąpi przypisanie $V_i \rightarrow \mathbf{w}_i$. Przedstawiona technika nosi nazwę kwantyzacji wektorów (ang. *Vector Quantisation*) i została opisana w pracy [3]. Kwantyzacja taka prowadzi do podziału przestrzeni V w zbiór obszarów

$$V_i = \left\{ \mathbf{v} \in V \mid \|\mathbf{v} - \mathbf{w}_i\| \leq \|\mathbf{v} - \mathbf{w}_j\| \quad \forall j \right\} \tag{7}$$

zwanych wielobokami Voronoja (ang. *Voronoi polygons*) lub wielościanami Voronoja (ang. *Voronoi polyhedra*), wewnątrz których, każdy wektor v odwzorowany jest poprzez odpowiadającą mu wagę neuronu $\mathbf{w}_i$. Przy P danych uczących błąd odwzorowania można zapisać jako

$$E = \frac{1}{P} \sum_{i=1}^{P} \left\| \mathbf{v} - \mathbf{w}_{i(v)} \right\|^2 \tag{8}$$

gdzie $\mathbf{w}_{i(v)}$ jest wagą neuronu leżącego najbliżej danej uczącej v, tzn. neuronu zwycięzcy. W procesie uczenia sieci dąży się do zminimalizowania tego błędu poprzez umiejętne dobranie wag neuronów, które mogą być uaktualniane wg wzoru:

$$\Delta \mathbf{w}_i = \varepsilon \cdot \delta \cdot (\mathbf{v} - \mathbf{w}_i) \quad \text{dla} \quad i = 1,\ldots,K \tag{9}$$

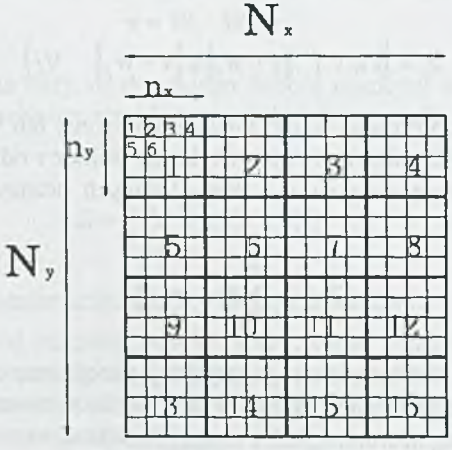
gdzie: $\Delta \mathbf{w}_i$ zmiana wag i-tego neuronu; ε – stała uczenia (na ogół malejąca w procesie uczenia); δ – stała uwzględniająca wpływ zmian wag dla sąsiadów neuronu zwycięzcy.

Jednym ze znanych algorytmów minimalizacji błędu (8) jest metoda spadku gradientu zaproponowana przez Lloyd'a [13]. Jest to metoda typu zwycięzca bierze wszystko i bywa również nazywana metodą *K*-średnich (ang. *K-means*) [3]. Oprócz tego istnieje jeszcze wiele innych algorytmów, m.in. algorytm Kohonena [12], algorytm WTA z mechanizmem „sumienia" lub „zmęczenia" CWTA (ang. *Conscience Winner Takes All*) [6], algorytm gazu neuronowego (ang. *Neural Gas*) [15]. W wyniku procesu uczenia pewna ilość danych uczących zostaje zastąpiona mniejszą liczbą neuronów, a zatem dokonana zostaje kompresja informacji. Wagi neuronów utworzą tzw. książkę kodową (ang. *codebook*).

Podstawowym problemem przy użyciu sieci samoorganizujących się jest odpowiedni dobór liczby neuronów. Zarówno zbyt mała liczba jak i zbyt duża powodują powstawanie dużego błędu. Optymalna zatem wydaje się architektura sieci o zmiennej liczbie neuronów, zwiększana w trakcie uczenia w przypadku niedostatecznej jakości odwzorowania, zaproponowana w [9]. W pracy [2] można znaleźć matematyczne uzasadnienie, że sieć o wzrastającej liczbie neuronów aproksymuje z błędem nie większym niż sieć o zadanej liczbie neuronów.

3. Przykłady zastosowań sieci neuronowych do kompresji informacji

W przypadku wykorzystania sieci neuronowej do kompresji obrazów należy wcześniej dokonać kilka zabiegów „technicznych" np. takich, jak zastosowano w pracy [18]. Obraz przedstawia zwykle informację w postaci zbioru danych 2-D, zapisanych często jako macierz o wymiarach (N_x x N_y), gdzie N_x – jest liczbą pikseli w poziomie, zaś N_y – liczbą pikseli w pionie. Informację zawartą w obrazie należy przekształcić do postaci wektorów, aby móc je zaprezentować sieci neuronowej. Dlatego należy wcześniej dokonać podziału obrazu na mniejsze ramki, tak jak to zostało pokazane na rys. 2.



Rys. 2. Przykład podziału obrazu cyfrowego na ramki

Każda z tych ramek zawiera informację z pewnego obszaru obrazu wyjściowego. Informacja zawarta w każdej z ramek tworzy podmacierz ($n_x \times n_y$) macierzy obrazu. Oczywiście zakłada się, że (N_x / n_x) mod 1 = 0 i jednocześnie (N_y / n_y) mod 1 = 0. Jeżeli taka podmacierz przekształcona zostanie w wektor w ten sposób, że poszczególne wiersze tej podmacierzy utworzą wektor kolumnowy v o długości równej iloczynowi (n_x * n_y), to w wyniku takiego podziału obrazu powstanie zbiór P wektorów uczących, które stanowią zbiór uczący dla sieci neuronowej. W trakcie uczenia sieci, a następnie odtwarzania występuje błąd kwantyzacji, który wpływa na jakość odtworzonego obrazu. Różnicę tę charakteryzuje błąd średniokwadratowy – MSE (ang. *Mean Square Error*), który można wyrazić wzorem

$$MSE(X,\hat{X}) = \frac{1}{N_x \cdot N_y} \sum_{i=1}^{N_x} \sum_{j=1}^{N_y} (x_{ij} - \hat{x}_{ij})^2 \tag{10}$$

gdzie: x_{ij} – jest wartością piksela w i-tym wierszu i j-tej kolumnie obrazu oryginalnego; $\hat{x}_{ij}$ – jest wartością piksela w i-tym wierszu i j-tej kolumnie obrazu odtworzonego. Czasami stosuje się również miarę błędu średniego wartości bezwzględnej – MAE (ang. *Mean Absolute Error*), który opisany jest wzorem

$$MAE(X,\hat{X}) = \frac{1}{N_x \cdot N_y} \sum_{i=1}^{N_x} \sum_{j=1}^{N_y} | x_{ij} - \hat{x}_{ij} | \tag{11}$$

Przy ocenie zdolności systemu do redukcji szumu określa się stosunek sygnału do szumu – SNR (ang. *Signal to Noise Ratio*), mierzony w decybelach, dany wzorem

$$SNR(X,\hat{X}) = 10 \lg \frac{\sigma_x^2}{MSE(X,\hat{X})} \quad [db] \tag{12}$$

lub stosunek maksymalnej wartości sygnału do szumu – PSNR (ang. *Peak Signal-to-Noise Ratio*)

$$PSNR(X,\hat{X}) = 10 \lg \frac{x_{max}^2}{MSE(X,\hat{X})} \quad [db] \tag{13}$$

gdzie: σ_x^2 – jest wariancją, x_{max}^2 jest maksymalną wartością sygnału. W przypadku kompresji obrazów $x_{max}^2 = (2^k - 1)^2$, gdzie k – oznacza liczbę bitów potrzebną do zakodowania stopni szarości obrazu (np. dla obrazu w 256 poziomach szarości k = 8). Wartość współczynnika PSNR podawana jest również w decybelach. Wielkość (wielokrotność) kompresji określana jest przez współczynnik kompresji, wyrażający stosunek ilości informacji potrzebnej do zapisania obrazu oryginalnego do ilości informacji potrzebnej do zapisania obrazu skompresowanego, co można wyrazić wzorem

$$K_r = \frac{P \cdot N \cdot T}{P \cdot q \cdot T + q \cdot N \cdot t} \tag{14}$$

gdzie: q – liczba neuronów w sieci, T – liczba bitów potrzebna do zakodowania danych obrazu (wartości pikseli), t – liczba bitów potrzebna do zakodowania wartości wag

neuronów w sieci, P – liczba wektorów reprezentujących dany zbiór informacji, N – długość wektora.

3.1. Rezultaty badań

Testowano wpływ liczby neuronów, jak również wielkości ramki próbkującej na błąd kompresji. W przypadku sieci perceptronowej konfiguracja została zapisana w postaci N-q-N, gdzie: N - liczba wejść sieci (długość wektora uczącego), q – liczba neuronów warstwy ukrytej. Dla sieci samoorganizującej się konfiguracja podaje liczbę neuronów w sieci. Porównanie wzrokowe otrzymanych obrazów nie wykazywało znaczących błędów kompresji, stąd obiektywną ocenę można wysnuć jedynie na podstawie wyników. W tabeli 1 zestawione zostały rezultaty kompresji obrazów przy różnych konfiguracjach sieci neuronowych. Najlepszą jakość kompresji otrzymano dla sieci samoorganizującej się z 512 neuronami, przy ramce próbkującej wielkości 4×4 piksele.

W przypadku sieci perceptronowej wykorzystującej przekształcenie PCA wielkość błędu MSE i MAE zależy w dużym stopniu od wyboru liczby neuronów w warstwie ukrytej. Jak zostało przedstawione w rozważaniach teoretycznych, błąd który występuje przy tym przekształceniu jest związany z wyborem liczby składników głównych przekształcenia PCA, które służą do odtworzenia oryginału, co jest równoważne z wyborem odpowiedniej liczby neuronów w warstwie ukrytej. W przypadku sieci perceptronowej o konfiguracji 64 – 3 – 64, błąd MSE wynosi 121,53, jest zatem prawie 2 razy większy niż w przypadku sieci o konfiguracji 64 – 5 – 64. Widać zatem, że uwzględnienie dwóch kolejnych składników głównych rozkładu PCA wpływa znacząco na poprawę jakości kompresji. Pewną trudność stanowił odpowiedni dobór wag. Trenowanie sieci wymagało parokrotnego rozpoczęcia ze względu na zatrzymywanie się algorytmu uczącego w minimum lokalnym.

W przypadku sieci samoorganizującej się liczba neuronów również wpływa znacząco na wskaźnik MSE. Dla sieci o 128 neuronach błąd MSE wynosi 109,52. W przypadku zwiększenia liczby neuronów do 512 błąd ten spada ponad dwukrotnie do wartości 51,39. Na taką zmianę wpływa błąd kwantyzacji, który w przypadku większej liczby neuronów jest mniejszy. Przy trenowaniu sieci wykorzystywano algorytm „gazu neuronowego", który jest czasochłonny w przypadku dużej liczby neuronów, ze względu na wyłanianie neuronu zwycięzcy i porządkowanie neuronów. Szybszy jest algorytm CWTA, jednak metoda „gazu neuronowego" charakteryzuje się bardzo dobrą zbieżnością i sieć ta uzyskała najmniejszy błąd MSE.

a)

b)

c)

d)

e)

Rys. 3. Rezultaty kompresji obrazów wielkości 512 × 512 pikseli przez sieci neuronowe. a) Obraz oryginalny przed kompresją; b) obraz skompresowany przez sieć perceptronową z 5 neuronami w warstwie ukrytej, c) negatyw obrazu różnicowego pomiędzy oryginałem a skompresowanym obrazem; d) obraz skompresowany przez sieć samoorganizującą się z 512 neuronami i e) negatyw obrazu różnicowego pomiędzy oryginałem a skompresowanym obrazem.

W przypadku obu sieci ważne znaczenie miał dobór długości wektora próbkującego obraz. W zależności wyboru wielkości ramki próbkującej uzyskano różne rezultaty. Dla ramki wielkości 4 × 4 piksele, błędy MSE i MAE są mniejsze niż w przypadku ramki 8 × 8, jednak w zmniejszanie ramki powoduje również zmniejszanie współczynnika kompresji, co ze względu na cel, którym ma być kompresja, nie jest pożądane. Na rysunku 3 pokazano przykład kompresji obrazu „LENA" o wielkości 512 × 512 pikseli dla sieci perceptronowej i samoorganizującej się. Ramka próbkująca miała rozmiar 8 × 8 pikseli. W przypadku sieci perceptronowej zastosowano 5 neuronów w warstwie ukrytej, co odpowiada 5 wartościom głównym rozkładu PCA. Sieć samoorganizująca się składała się z 512 neuronów i była trenowana za pomocą algorytmu „gazu neuronowego".

Tabela 3. Wyniki badań kompresji obrazu „LENA" przez sieci: perceptronową i samoorganizującą się

	konfiguracja sieci (liczba neuronów)	wielkość ramki próbkującej	MSE	MAE	SNR
Sieć perceptronowa	64 - 3 - 64	8 x 8	121,53	5,71	27,14
	64 - 5 - 64	8 x 8	63,47	4,10	29,97
Sieć samoorganizująca się	128	8 x 8	109,52	6,50	27,60
	256	8 x 8	78,36	5,57	29,05
	512	8 x 8	51,39	4,64	30,89
	256	4 x 4	35,72	3,79	32,46
	512	4 x 4	25,16	3,23	33,97

4. Podsumowanie

W pracy przedstawiono algorytmy kompresji wykorzystujące sieci neuronowe: sieć perceptronową i sieć samoorganizującą się. Otrzymane współczynniki błędów są zadawalające w porównaniu z metodami klasycznymi. Zdolności generalizujące sieci neuronowych pozwalają stosować je efektywnie w kompresji stratnej , przy praktycznie niewidocznej dla odbiorcy różnicy w obrazie. Wzrastające możliwości obliczeniowe komputerów pozwalają na znaczne skrócenie czasu potrzebnego do wytrenowania sieci, jednak dalszy rozwój efektywnych algorytmów wymaga połączenia doświadczeń metod „klasycznych" z neuronowymi. Znakomite możliwości dają techniki przekształceń falkowych, logiki rozmytej, czy też teorii fraktali.

Podziękowania

Autor chciałby podziękować Panu Profesorowi Stanisławowi Osowskiemu i Panu Doktorowi Krzysztofowi Siwkowi za udostępnienie do testowania programów komputerowych NETTEACH [19] i KOHON [22].

Literatura

[1] Amari S., Cichocki A. *Adaptive blind signal processing – neural network approaches*, Proceedings IEEE, vol. 86, No 10, pp 2026-2048, Oct. 1998.

[2] Beliczyński B. *Przyrostowa aproksymacja funkcji za pomocą sieci neuronowych.* Prace Naukowe Politechniki Warszawskiej, Zeszyt 112, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2000.

[3] Buzo A., Gray R., Linde Y. *An algorithm for vector quantizer design.* IEEE Trans. Comm., 28:84-95,1980.

[4] Cichocki A., Kasprzak W., Skarbek W. *Adaptive Learning Algorithm for Principal Component Analysis with Partial Data.* Cybernetics and Systems'96, 13-th European Meating on Cybernetics and Systems Research, Austrian Society for Cybernetics Studies, Vienna, pp 1014-1019.

[5] Cierniak R., Rutkowski L. *On image compression by competitive neural networks and optimal linear predictors.* Signal Processing: Image Communication 15 (2000) pp. 559-565.

[6] DeSieno D. *Adding a conscience to competitive learning.* Neural Networks, 1:117-124,1988.

[7] Diamantaras K., Kung S. *Principal component neural networks, theory and applications.* J.Wiley, New York 1996.

[8] Fołtyniewicz R. *Artificial neural networks for image recognition.* Rozprawa Doktorska. Politechnika Warszawska, 1997.

[9] Fritzke B. *Let it grow – self-organizing feature maps with problem dependent cell structure* . In Proceedings of the International Conferrence on Artificial Neural Networks, Helsinki, 1991. Elsevier.

[10] Gersho A, Gray R.M. *Vector Quantization and Signal Compression,* Kluver Academic Publishers, Boston 1992.

[11] Gray R.M. *Vector Quantization.* IEEE ASSP Mag., 1(2):4-29, 1984.

[12] Kohonen T. *Self-organizing map.* Springer Verlag, Berlin, 1995.

[13] Lloyd S. P. *Least squares quantization in pcm.* IEEE Trans. Inform. Theory., 1(2):2-10, 1982.

[14] Majkowski A. *Zastosowanie transformaty falkowej i obliczeń neuronowych w kompresji sygnałów.* Rozprawa Doktorska. Politechnika Warszawska. 1999.

[15] Martinetz T., Berkovich S., Schulten K. *„Neural-Gas" network for vector quantization and its application to time-series prediction.* IEEE Transaction on Neural Networks, 4(4):558-569, 1993.

[16] Natarajan Balas K. *Filtering Random Noise from Deterministic Signals via Data Compression.* IEEE Transactions on Signal Processing, vol 43, No 11, Nov, 1995.

[17] Oja E. *Principal components, minor components and linear neural networks.* Neural Networks, vol 5, pp. 927-935,1992.

[18] Osowski S. *Sieci neuronowe do przetwarzania informacji.* Oficyna Wydawnicza Politechniki Warszawskiej, 2000.

[19] Osowski S. *Sieci neuronowe.* Oficyna Wydawnicza Politechniki Warszawskiej, 1994.

[20] Rak R. J. *Wybrane metody kompresji sygnałów multimedialnych.* Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 1998.

[21] Rzesiowski D. *Neuronowe metody kwantyzacji wektorowej w zastosowaniu do kompresji obrazów.* Rozprawa Doktorska. Politechnika Warszawska, 1995.

[22] Siwek K. *Implementacja komputerowa wybranych algorytmów uczących i aplikacyjnych sieci samoorganizujących się Kohonena.* Praca Dyplomowa. Politechnika Warszawska, Warszawa, 1995.

[23] Skarbek W. (edytor) *Multimedia – Algorytmy. Standardy kompresji.* Akademicka Oficyna Wydawnicza PLJ. Warszawa, 1998.

HENRYK KRAWCZYK, MICHAŁ WIELGUS
KATEDRA ARCHITEKTURY SYSTEMÓW
KOMPUTEROWYCH
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI
I INFORMATYKI, POLITECHNIKA GDAŃSKA

Bezpieczeństwo handlu elektronicznego
Security of e-commerce

Streszczenie

Rozpatrzono i scharakteryzowano wielowarstwowe architektury systemów informatycznych wspomagających handel elektroniczny. Zasygnalizowano niezbędne różnego typu mechanizmy zabezpieczeń dla podstawowych usług i określonych klas zagrożeń. Główną uwagę zwrócono na podpisy cyfrowe. Na tej podstawie wprowadzono model zaufania oraz zdefiniowano metryki pozwalające na oszacowanie ryzyka przeprowadzanych transakcji.

Zaprezentowano również strategie testowania systemów handlu elektronicznego z uwzględnieniem wymagań bezpieczeństwa, omówiono wybrane procedury testowania oraz przedstawiono narzędzie wspomagające tego typu testowanie.

Abstract

In the paper multi-layer architectures of information systems supporting e-commerce are examined and characterized. Necessary mechanisms of different type securities for basic services and definite classes of threats are mentioned. The main attention is paid on digital signatures. Under the base the confidence model was introduced and metrics allowing estimation the risk of processed transactions are defined.

Strategies of testing e-commerce systems taking into account security requirements are also presented, chosen testing procedures are discussed and the tool supporting this type testing is presenting.

1. Wprowadzenie

W początkowych etapach rozwoju handlu wszystkie konsekwencje wykonywanych operacji spadały na zainteresowane strony. Z czasem funkcję pewnej ochrony gwarantowało państwo (pieniądz papierowy) lub banki (transakcje finansowe). Wymiana danych elektronicznych w tym pieniędzy elektronicznych wymaga dodatkowych zabezpieczeń gwarantowanych również przez odpowiednie organizacje certyfikujące. Zapewniają one wykonanie operacji handlowych w ustalonej z góry formie przez

uprawnione osoby lub organizacje i na odpowiednim poziomie zaufania. W przypadku wykorzystania Internetu decydującą rolę odgrywają takie aspekty:

- pełna autentyfikacja stron biorących udział w transakcji,
- akceptowalność transakcji (wykona się tylko poprawnie lub wcale),
- poufność transakcji (niemożliwość wykonania przez osobę nieupoważnioną),
- prywatność (dostęp do chronionej informacji ma tylko osoba upoważniona),
- integralność danych (informacja kreowana przez nadawcę jest taka sama jak odbierana przez odbiorcę).

Kilka technologii, takich jak zapory ogniwe, VPN (Virtual Private Network), infrastruktura klucza publicznego (Kerberos) czy detekcja intruza (IDES), zapewnia powyższe cechy. Integrując różne rozwiązania dotyczące zabezpieczeń zwiększamy zaufania do handlu elektronicznego. Przykładem jest organizacja ACES (Access Certificates for Electronic Services), która zaleca stosowanie odpowiednich sygnatur certyfikujących opartych o infrastrukturę klucza publicznego.

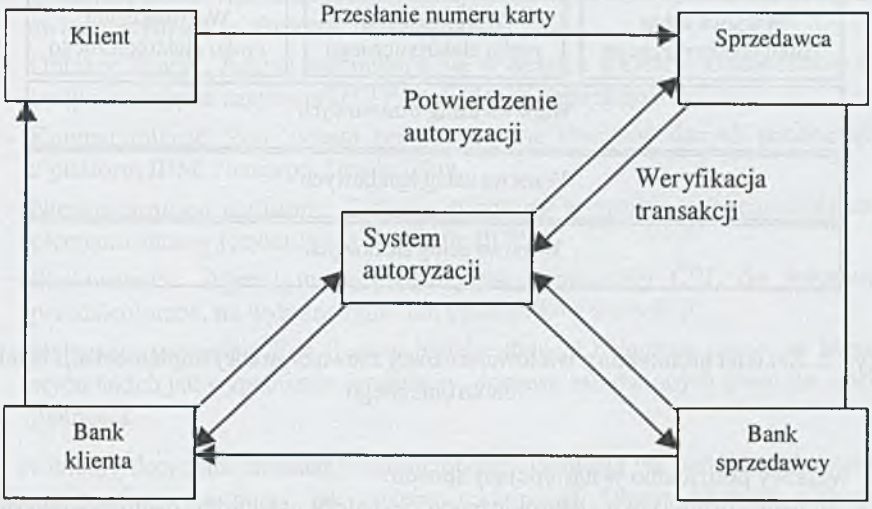
W pracy rozpatrzono i scharakteryzowano wielowarstwowe architektury systemów informatycznych wspomagających handel elektroniczny. Zasygnalizowano niezbędne różnego typu mechanizmy zabezpieczeń dla podstawowych usług i określonych klas zagrożeń. Główną uwagę zwrócono na podpisy cyfrowe. Opisano metody testowania bezpieczeństwa aplikacji. Na tej podstawie wprowadzono model zaufania oraz zdefiniowano metryki pozwalające na oszacowanie ryzyka przeprowadzanych transakcji.

2. Model handlu elektronicznego

Realizacja transakcji handlowych może przebiegać w różny sposób. Zależy to od przyjętego zakresu B2C czy B2B. W najprostszym przypadku (rysunek 1) klient składa zamówienie w sklepie podając dodatkowo dane osobowe i numer karty kredytowej. Sprzedawca po sprawdzeniu poprawności zamówienia i otrzymaniu potwierdzenia co do autentyczności danych podanych przez klienta i wypłacalności, otrzymuje pieniądze od banku pośredniczącego w transakcji i dostarcza towar klientowi za pośrednictwem firmy kurierskiej. Bank pośredniczący rozlicza się z bankiem klienta. W efekcie bank obciąża konto klienta. W opisanej sytuacji sprzedawca nie ma możliwości sprawdzenia prawa klienta do posługiwania się podanym numerem karty. Co więcej, potwierdzenie autentyczności danych osobowych klienta i numeru kary nie oznacza, że osoba posługująca się nimi jest pełnoprawnym właścicielem. Może to oznaczać co najwyżej zapas środków płatniczych na koncie klienta, którego dane i numer karty podano w zamówieniu.

Zaawansowane implementacje handlu elektronicznego wymagają architektury wielowarstwowej. Główne platformy zorientowane obiektowo nie zapewniają kompatybilności i nie pozwalają na wymianę informacji. Dotyczy to następujących platform:

- IBM CommercePoint [19],
- Microsoft Internet Commerce Framework [20],
- Netscape ONE (Open Network Environment) [21],
- Oracle NCA (Network Computing Architecture) [22],
- Sun/JavaSoft JECF (Java Electronic Commerce Framework) [23].

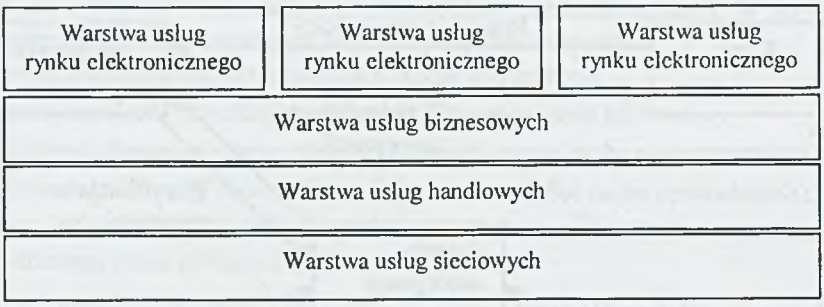


Rys. 1. Model handlu elektronicznego

Wymienione architektury próbowano połączyć opracowując wspólny rozproszony model zorientowany obiektowo w oparciu o protokół CORBA IIOP (Common Object Request Broker Architecture Internet InterORB Protocol). Miało to umożliwić klientom dokonywanie transakcji niezależnie od używanej platformy. Projekt podjęty przez IBM, Netscape, Oracle oraz Sun nie uwzględniał konieczności komunikacji w warstwie aplikacji biznesowych. Kolejną próbę opracowania standardu dla potrzeb budowy systemów handlu elektronicznego podjęto w CommerceNet [9]. Proponowane rozwiązanie w postaci Eco System spełnia trzy podstawowe funkcje:

- warstwa middleware ułatwia współpracę pomiędzy agentami aplikacji dostarczając usług autentyfikacji, przeprowadzania i rozliczania transakcji w oparciu wymianę komunikatów języka CBL (Common Business Language), modelującego procesy zachodzące w rzeczywistym świecie biznesu,
- zorientowane obiektowo środowisko wymusza ponowne użycie modułów handlu elektronicznego (włączając moduły reprezentujące linię produkcyjną przedsiębiorstwa),
- pozwala na wprowadzanie otwartych standardów i pomaga dostawcom technologii w komunikacji zwrotnej z użytkownikami dotyczącej pożądanych cech produktów.

Eco System stanowi szkielet aplikacji modelujących kluczowe procesy i usługi biznesowe. Architektura została zbudowana z czterech warstw, poukładanych jedna na drugiej (rysunek 2). Każda warstwa kolejna korzysta z usług w warstwie niższej.



Rys. 2. Szkielet architektury wielowarstwowej zaawansowanej implementacji handlu elektronicznego

Warstwy podzielono w następujący sposób:

- Warstwa usług rynku elektronicznego. Świadczy usługi dla równoległych rynków w obrębie większych przedsięwzięć handlowych, np. rynek nieruchomości (przegląd ofert, udzielanie kredytów), rynek operacji finansowych (operacje kupna, sprzedaży, notowań giełdowych).
- Warstwa usług biznesowych. Obejmuje podstawowe procesy biznesowe i aplikacje wspólne dla większej liczby rynków np. funkcje sprzedaży detalicznej (dokonywanie zakupów, składanie zamówień, transport towarów), B2B (zarządzanie dostawami, obsługa magazynu, inwentaryzacja towarów). Oferuje mechanizmy komunikacji między kupującymi a sprzedającymi.
- Warstwa usług handlowych. Na tym poziomie dostępne są usługi wchodzące w skład portfela elektronicznego (autentyfikacja, dokonywanie płatności, lokalizacja dostawców). W przyszłości warstwa zostanie uzupełniona o zaawansowane usługi w postaci bezpiecznej poczty, mechanizmy ochrony płatności na bazie inteligentnych kart, zarządzanie przeprowadzanymi transakcjami i zarządzanie agentami aplikacji,
- Warstwa usług sieciowych. Wprowadza mechanizmy podnoszące wydajność, wiarygodność i bezpieczeństwo krytycznych operacji, np. pokwitowania transakcji, inteligentne zapory ogniowe.

Opis szkieletu Eco System wyszczególnia podstawowe usługi, które muszą zostać zaimplementowane w obiektach należących do danej klasy. Dodatkowo należy uszczegółowić interfejs usług sieciowych NSI (Network Services Interface). Jest to zestaw komunikatów zaimplementowanych w języku IDL (Interface Definition Language). Ponadto proponowany szkielet musi uwzględniać specyfikację API dla modułów związanych ze świadczeniem usług. Budowa Eco System na wyłaniającym się standardzie rozproszonych obiektów i przetwarzania sieciowego CORBA 2.0 stwarza kompatybilność z IIOP (zaimplementowanym w Netscape Communicator) na bazie komunikatów CBL. Naturalnie proponowany standard będzie współpracował z HTTP (Hypertext Transfer Protocol), HTML (Hypertext Markup Language) i językiem Java. Przyjęte decyzje projektowe pokrywają się z trendami technologicznymi:

- Usługi sieciowe. Każda aplikacja działająca na bazie Eco System będzie agentem świadczącym usługi dostępne przez sieć.
- Obiekty WWW. Agenci komunikują się w oparciu o system komunikatów CBL i odpowiadają na zapytania HTTP pochodzące z przeglądarek.
- Kompatybilność. Eco System będzie wspierał wymianę danych pochodzących z platform IBM, Netscape, Oracle i Sun.
- Niezależność od platformy. Zostanie osiągnięta w oparciu o mechanizmy zaimplementowane w języku Java i protokole IIOP.
- Skalowalność. Agenci mogą przekazywać komunikaty CBL do wskazanych przedsiębiorstw, na wybrane rynki lub pośredników transakcji.
- Delegacja procesów. Eco System będzie ułatwiał delegację procesów biznesowych takich jak wypełnianie formularzy, dostawa zamówionych towarów, obsługa płatności.

Problemy dotyczące transakcji internetowych pojawiają się podczas dokonywania rozliczeń (zarówno płatności, jak również reklamacji). Obawy klientów wzbudzają również rozbieżności w wyglądzie i jakości produktów prezentowanych na stronach WWW od rzeczywistych, dostarczonych towarów. Rodzaje zagrożeń związanych z dokonywaniem transakcji przez Internet są następujące:

- oszukanie kupującego przez sprzedającego, tzw. spoofing,
- ujawnienie danych przesyłanych pomiędzy kupującym a sprzedającym (dane osobowe, hasła, numery kart kredytowych), tzw. sniffing,
- kradzież danych z serwera,
- zalew serwera sklepowego fikcyjnymi zleceniami, tzw. Denial of Service (DoS).

3. Metody zabezpieczeń

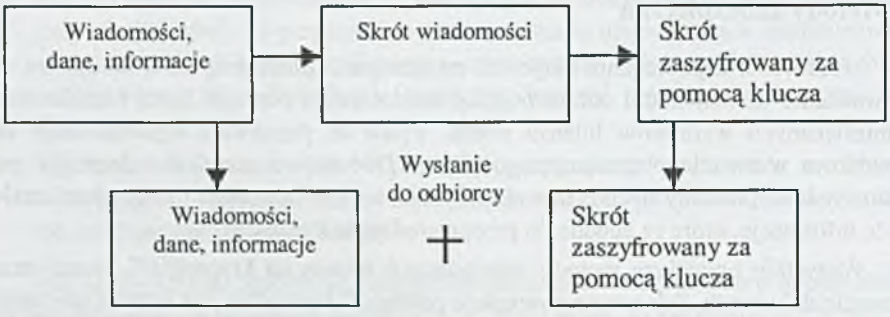
Możliwości zapobiegania kłopotom związanym z płatnością kartą kredytową daje prowadzenie dokumentacji odnotowującej każdorazową płatność kartą i analizowanie comiesięcznych wydruków bilansu konta. Tylko te papierowe wydruki mają moc dowodową w świetle obowiązującego prawa. Dodatkowo wszelkie informacje przesyłane w sieci powinny być szyfrowane. Oprócz tego w Internecie nie powinny znaleźć się te informacje, które są zbędne do przeprowadzenia transakcji [3].

Wszystkie omawiane metody zabezpieczeń bazują na kryptografii. Samo zaszyfrowanie dokumentu cyfrowego gwarantuje poufność. Potrzebny jest jeszcze mechanizm uwierzytelniający nadawcę, gwarantujący autentyczność dokumentu (podpis cyfrowy). Obecne rozwiązania bazują na parze kluczy – publicznym i prywatnym, które gwarantują poufność i autentyczność, oraz stronie trzeciej, tzn. organizacji certyfikującej, do której mamy całkowite zaufanie, potwierdzającej przynależność klucza do danej osoby przez wystawianie specjalnych certyfikatów. Do 1967 r. wykorzystywano szyfrowanie symetryczne oparte na jednym kluczu, a przez to zaszyfrowaną wiadomość mógł odczytać każdy, kto dysponował kluczem. Dużą zaletą takiego szyfrowania jest szybkość, wydajność oraz odporność na próby złamania. Pierwsze algorytmy niesymetryczne pojawiły się pod koniec lat 70. Wiadomość (tekst jawny) szyfruje się jednym kluczem (publicznym, ogólnodostępny), a odszyfrowuje drugim (prywatnym,

przypisany osobie, która go wygenerowała). Klucze uzyskuje się stosując przekształcenia matematyczne. Nie ma możliwości wyznaczenia jednej wartości klucza na podstawie drugiej. Szyfrowanie asymetryczne jest złożone i czasochłonne, jednak nie ma problemu z ujawnieniem klucza publicznego. Rozsądny stopień bezpieczeństwa można osiągnąć stosując klucze o długości 1024 bitów dla szyfrów asymetrycznych lub 128 bitów dla szyfrów symetrycznych.

Omawiany mechanizm działa również w drugą stronę, tzn. kluczem prywatnym szyfruje się skrót wiadomości (funkcja skrótu oparta na skomplikowanych przekształceniach matematycznych gwarantuje podobną niepowtarzalność skrótu jak w przypadku odcisku palca, ponadto mając skrót nie jesteśmy w stanie poznać treści wiadomości), wytwarzając w ten sposób podpis elektroniczny wiadomości (rysunek 3), a osoba odbierająca wiadomość samodzielnie wytwarza nowy skrót wiadomości, deszyfruje kluczem publicznym otrzymany skrót i porównuje oba skróty. Jeżeli wszystko się zgadza, wiadomość jest prawdziwa, a przynajmniej pochodzi od osoby będącej w posiadaniu jednego z pary kluczy [14]. Niezawodność omawianego sposobu poświadczania autentyczności dokumentów zależy od kilku czynników: siły algorytmu użytego do wytworzenia kluczy, złożoności funkcji skrótu oraz autentyczności klucza publicznego (certyfikacja). Podpis elektroniczny musi spełniać takie funkcje [7]:

- niepowtarzalność tzn. musi być wyjątkowy dla osoby, która się nim posługuje,
- możliwość weryfikacji,
- znajdować się pod wyłączną kontrolą osoby, która się nim posługuje,
- dołączony do wiadomości pozwala stwierdzić jej autentyczność i zapewnia integralność,
- zamierzony w użyciu tzn. posiada te same skutki prawne co podpis odręczny.



Rys. 3. Schemat tworzenia podpisu elektronicznego

Ustawa o podpisie elektronicznym została przyjęta przez Sejm 18 września br. Prezydent złożył podpis pod ustawą 11 października br. Skutki prawne podpisu będą odczuwalne za 9 miesięcy.

PKI (Public Key Infrastructure) to struktura powstała na skutek ujednolicenia wymagań i przepisów dotyczących certyfikatów, dostawców usług certyfikacyjnych oraz urządzeń służących do generowania i weryfikacji podpisu elektronicznego dla dużych

firm, chcących handlować przez sieć. Stworzone przez TP Internet, Centrum Certyfikacji SIGNET jest odpowiedzialne za wydawanie i pełną obsługę danych oraz certyfikatów elektronicznych służących do składania i weryfikacji elektronicznego podpisu [13]. Dla potrzeb prywatnych, np. bezpiecznej poczty elektronicznej, starcza mechanizm kluczy publicznego i prywatnego. Certyfikat to ciąg danych zapisanych na odpowiednim nośniku. Najpopularniejszy standard to X.509. Budowa certyfikatu: wersja, numer seryjny, nazwa wydawcy certyfikatu, data ważności, nazwa podmiotu, dla którego certyfikat został wystawiony, jego klucz publiczny oraz podpis cyfrowy organu wydającego certyfikat (Certification Authority, CA). Prawdziwość podpisu można zweryfikować mając klucz publiczny urzędu certyfikującego. Klucz ten znajduje się z kolei w certyfikacie wystawionym przez organ wyższej instancji. Weryfikacja certyfikatu polega na prześledzeniu ścieżki zaufania, na końcu której znajduje się organ nadrzędny (Root CA). Certyfikat wystawia on sam dla siebie, a wszyscy powinni mieć swobodny dostęp do jego klucza publicznego. W Polsce taki certyfikat wystawił sobie urząd Unizeto Certum. Z kolei PolCert otrzymał certyfikat od znanego w Europie urzędu nadrzędnego GlobalSign. PKI pozwala na budowę systemów bezpiecznej wymiany dokumentów (internetowy system przekazu elektronicznych deklaracji dla ZUS obsługiwany przez Unizeto Certum), systemy handlu elektronicznego, VPN oraz zabezpieczać stacje robocze i gromadzone na nich dane poprzez eliminację anonimowości. W strukturach PKI współdziałają SSL (Secure Socket Layer), TLS (Transport Layer Security), S/MIME (Secure Multipurpose Internet Mail Extensions), SET (Secure Electronic Transaction), IPSec (Internet Protocol Security).

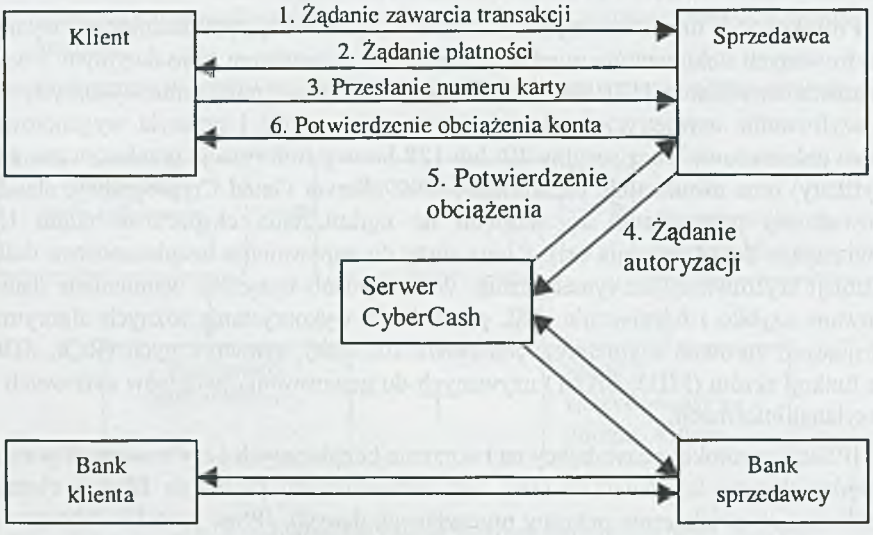
Protokół SSL to zestaw reguł i standardów umożliwiających bezpieczną wymianę zaszyfrowanych dokumentów między przeglądarką a serwerem transakcyjnym z wykorzystaniem certyfikatów [17]. Na początku przy zestawianiu połączenia wykorzystywane jest szyfrowanie asymetryczne, dzięki któremu utajnia się i przesyła wygenerowany losowo jednorazowy klucz sesyjny 40- lub 128-bitowy (informacja przekazywana przez certyfikaty) oraz ewentualnie rozszerzenie SGC (Server Gated Cryptography, standard wprowadzony przez banki ze względu na ograniczenia eksportowe rządu USA obowiązujące do 14 stycznia br.). Klucz służy do zapewnienia bezpieczeństwa dalszej transmisji szyfrowanej już symetrycznie. W ten sposób wszystkie wymieniane dane są kodowane szybko i bezpiecznie. SSL pozwala na wykorzystanie różnych algorytmów szyfrujących zarówno asymetrycznych (RSA 1024-bit), symetrycznych (RC4, 3DES) oraz funkcji skrótu (MD5, SHA1) używanych do generowania podpisów cyfrowych dla przesyłanej informacji.

IPSec to protokół pozwalający na tworzenie bezpiecznych i szyfrowanych połączeń pomiędzy dwoma komputerami [18]. Jest rozszerzeniem protokołu IPv4 o elementy umożliwiające zwiększenie ochrony przesyłanych danych. IPSec umożliwia bezpieczne nawiązywanie połączenia w warstwie sieciowej protokołu IP oraz dostarcza mechanizmy ułatwiające autoryzację, poprawiające integralność przesyłanych danych oraz zapewnia ich poufność.

Najmniej zadawalającym sposobem stwarzającym pozory bezpieczeństwa jest połączenie identyfikatora użytkownika i jego hasła. Daje on słabe zabezpieczenie przed podszywaniem się, tzw. Spoofing, oraz dopuszcza możliwość modyfikacji danych po ich dotarciu do serwera sklepowego, a przed ich przetworzeniem przez główny moduł sklepowy. Dodanie do wspomnianych dwóch elementów uwierzytelniania trzeciego

w postaci cyfrowego tokena eliminuje słabości związane z podszywaniem się, jednak nie zapewnia integralności danych zlecenia od chwili wysłania ich z przeglądarki.

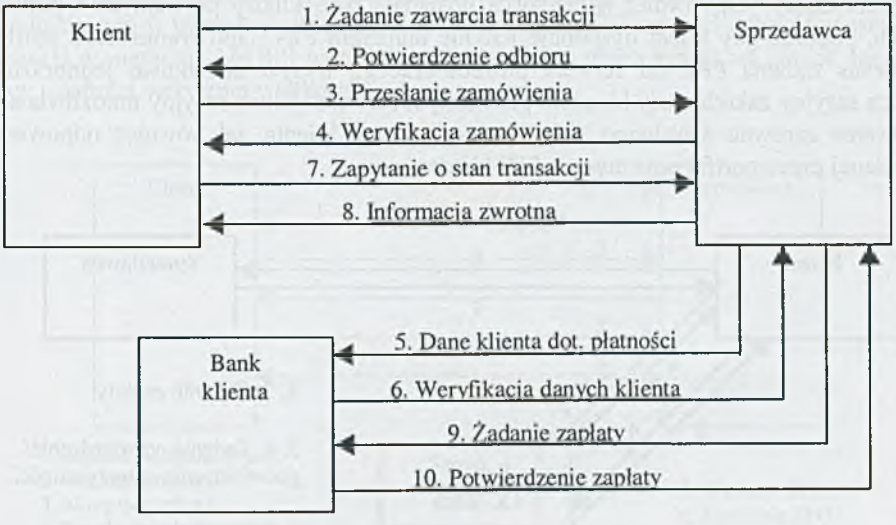
Pierwszym z prezentowanych rozwiązań zabezpieczających handel elektroniczny jest system znany pod nazwą CyberCash (rysunek 4). Składa się on z oprogramowania klienta, które pełni rolę elektronicznego portfela z mechanizmami kryptograficznymi i rejestrującymi przeprowadzane transakcje oraz analogicznego oprogramowania po stronie sprzedawcy [8]. Przesyłane informacje są szyfrowane za pomocą losowego klucza symetrycznego, który jest dołączany do wiadomości zaszyfrowanej kluczem publicznym odbiorcy. Klucz publiczny systemu CyberCash jest wbudowany w dostarczane oprogramowanie, natomiast pary kluczy prywatnych i publicznych są generowane przy rejestracji nowej karty kredytowej w portfelu. Nowo wygenerowany klucz publiczny przesyłany jest do serwera CyberCash, który tym samym uczestniczy w każdej transakcji dokonywanej między klientem a sprzedawcą, potwierdzając autentyczność stron biorących w niej udział. Sam mechanizm transakcji nie odbiega od modelu handlu elektronicznego, a o poprawność i bezpieczeństwo wykonania transakcji dba oprogramowanie CyberCash. Sprzedawca otrzymuje jedynie zaszyfrowany kluczem publicznym CyberCash numer karty kredytowej klienta co teoretycznie podnosi zaufanie do systemu. W praktyce dane klientów przechowywane na serwerach sprzedawców są często posegregowane na podstawie numerów kart, które CyberCash z upoważnienia klienta dostarcza na każde żądanie sprzedawcy.



Rys. 4. Model bezpiecznego handlu elektronicznego. Rozwiązanie CyberCash

SET (Secure Electronic Transaction) to propozycja standardu obsługi zamówień i płatności w Internecie. Został on opracowany jako wspólne przedsięwzięcie Eurocard, Mastercard, Visa, IBM, Microsoft i Netscape [8]. Zapewnia najwyższy obecnie poziom bezpieczeństwa dla klientów i sprzedawców [15]. Przebieg transakcji wygląda następująco (rysunek 5) [16]. Klient składa zamówienie w sklepie i podaje własny certyfikat,

czyli podpis elektroniczny. Asymetryczne szyfrowanie zapewnia identyfikację użytkownika i zabezpiecza przesyłane informacje przed rozszyfrowaniem. Sprzedawca zwraca się do instytucji obsługującej karty kredytowe z zapytaniem o autoryzację klienta, która bierze na siebie pełną odpowiedzialność i zleca bankowi klienta dokonanie płatności na rzecz sprzedawcy. Po potwierdzeniu tożsamości sprzedawca wysyła towar do klienta przez firmę kurierską. Bank obciąża konto klienta. Standard SET pozwala dokonać płatności przy użyciu karty kredytowej bez potrzeby podawania numeru karty, a ponadto wprowadza certyfikaty (podpis elektroniczny) dla stron uczestniczących w transakcji (rejestracja) dzięki czemu eliminuje anonimowość uczestników (przyczyna największych zagrożeń ze strony Internetu). Zasadnicza różnica między CyberCash a SET polega na tym, że w pierwszym przypadku tylko system CyberCash zna klucze publiczne wszystkich stron biorących udział w transakcji. Natomiast SET zakłada istnienie hierarchicznej struktury systemu certyfikatów, które muszą zostać wymienione pomiędzy uczestnikami transakcji. Na tej podstawie wiadomo, który klucz publiczny należy użyć wysyłając wiadomość do konkretnego uczestnika.

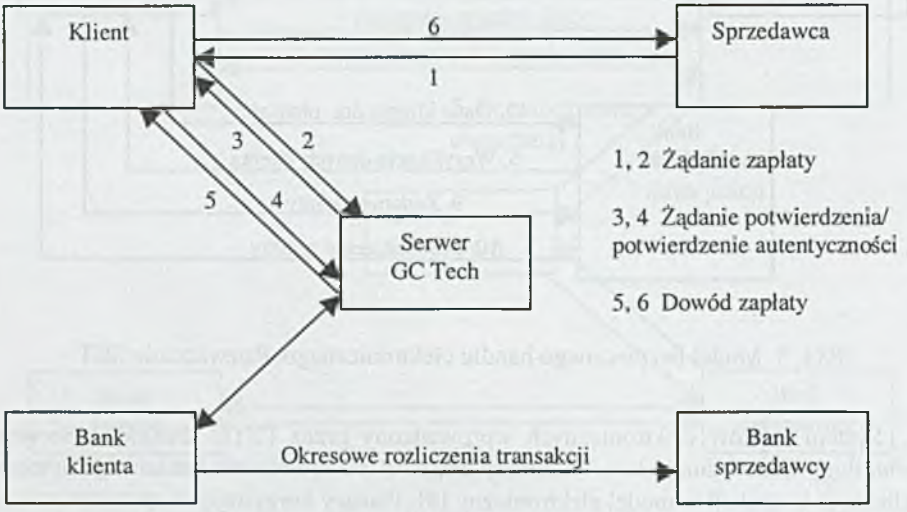


Rys. 5. Model bezpiecznego handlu elektronicznego. Rozwiązanie SET

System czeków elektronicznych wprowadzony przez FSTC (Financial Services Technology Consortium) stanowi kolejny przykład odwzorowania bankowego systemu rozliczania transakcji w model elektroniczny [8]. Płacący korzystając z oprogramowania realizującego operacje kryptograficzne generuje cyfrowo podpisane zlecenie zapłaty, czyli czek elektroniczny, który zostaje przesłany do sprzedawcy. Po cyfrowym podpisaniu przez sprzedawcę, tzw. akceptacja czeku czyli indos, czek trafia do banku sprzedawcy. Za pośrednictwem izby rozrachunkowej następuje uregulowanie należności. Ważną składową modelu czeków elektronicznych jest standaryzacja systemu realizacji przelewów. Ponadto model FSTC zakłada nieograniczony dostęp do kluczy

publicznych i certyfikatów stron uczestniczących w transakcji oraz wzajemne poręczanie pomiędzy stronami.

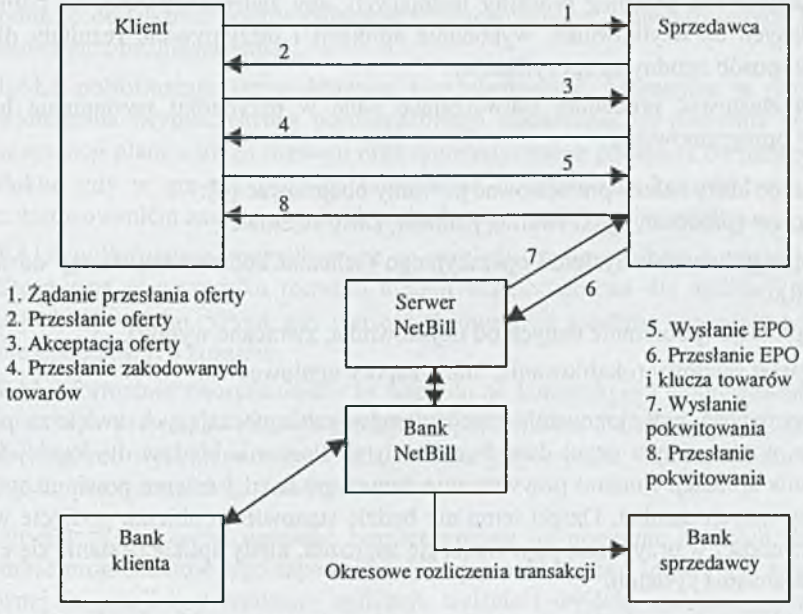
Model z dozorcą wprowadzony przez GC Tech eliminuje potrzebę wystawiania i zarządzania certyfikatami dla klientów [8]. Bazuje podobnie jak CyberCash na oprogramowaniu portfela elektronicznego i serwerze pośredniczącym przechowującym dane o klientach i sprzedawcach (rysunek 6). Klient po dokonaniu wyboru towarów otrzymuje cyfrowo podpisane przez sprzedawcę wezwanie do zapłaty, które po weryfikacji przez oprogramowanie portfela zostaje przesłane na serwer pośredniczący GC Tech. Serwer wysyła żądanie zwrotne do przesłania informacji mogących potwierdzić autentyczność klienta (PIN). Po otrzymaniu poprawnej odpowiedzi serwer obciąża konto klienta przy jednoczesnym udzieleniu kredytu sprzedawcy. Uregulowanie należności następuje po osiągnięciu przez kredyt ustalonej wielkości. Jeżeli klient dysponuje wystarczającymi środkami finansowymi do przeprowadzenia transakcji, serwer wystawia cyfrowo podpisany dowód zapłaty PPT (Proof of Payment), które trafia do portfela klienta, a następnie do sprzedawcy. Zapewnienie zapłaty obliguje sprzedawcę do dostarczenia zamówionych towarów. Model GC Tech zakłada, że zarówno serwer pośredniczący, jak również sprzedawca posiadają parę kluczy prywatnych i publicznych, podczas gdy klient dysponuje jedynie numerem PIN. Oprogramowanie portfela podczas żądania PPT od serwera pośredniczącego wysyła dodatkowo jednorazowy klucz sesyjny zakodowany kluczem publicznym serwera. Klucz sesyjny umożliwia szyfrowanie zarówno zwrotnego żądania autentyfikacji klienta, jak również odpowiedzi wysłanej przez portfel oraz numeru PIN klienta.



Rys. 6. Model bezpiecznego handlu elektronicznego. Rozwiązanie GC Tech

System NetBill został opracowany przez CMU (Carnegie Mellon University) dla potrzeb dostarczania klientom za pomocą Internetu tekstu, obrazów i oprogramowania [8]. Nacisk położono na zagwarantowanie dostarczenia klientom materiałów, za które

po dostawie zapłacą, a sprzedawcy będą mieć pewność, że pieniądze zasilą ich konto. Przepływ sterowania w systemie rozpoczyna autentyfikacja klienta chroniona szyfrowaniem z kluczem publicznym i generacja klucza sesyjnego do szyfrowania przesyłanych komunikatów, a kończy przesłanie klientowi klucza, za pomocą którego będzie miał dostęp do otrzymanych materiałów (rysunek 7). Klient nie jest obciążony finansowo dopóki zakodowane informacje nie zostaną dostarczone. Jednocześnie w przypadku braku na koncie klienta środków finansowych transakcja zostanie przerwana, a klucz, którym zaszyfrowano dostarczone materiały, nie zostanie przesłany klientowi. Dodatkowo podpisane cyfrowo przez sprzedawcę zamówienie EPO (Electronic Payment Order) gwarantuje, że informacja kreowana przez nadawcę jest taka sama jak odbierana przez odbiorcę. W sytuacji błędu polegającego na tym, że oprogramowanie obsługujące transakcję zerwało połączenie po dokonaniu zapłaty, ale przed otrzymaniem przez klienta klucza do odszyfrowania dostarczonych materiałów, może nastąpić ponowienie żądanie dostarczenia kopii klucza, bez naruszenia wymogów bezpieczeństwa. W odróżnieniu od metody GC Tech, w której sprzedawca komunikuje się z serwerem uczestniczącym w transakcji pośrednio przez oprogramowanie portfela klienta, w metodzie NetBill wyłącznie sprzedawca komunikuje się bezpośrednio z serwerem pośredniczącym w transakcji. Podobnie jak w metodzie GC Tech rozliczenie finansowe transakcji w metodzie NetBill następuje po osiągnięciu przez kredyt na koncie sprzedawcy ustalonej wcześniej wielkości.



Rys. 7. Model bezpiecznego handlu elektronicznego. Rozwiązanie NetBill

Polityka ochrony systemów teleinformatycznych zakłada, że bezpieczeństwo całego systemu jest tak mocne, jak jego najsłabszy element. Oprócz stosowania kryptografii

należy zadbać o bezpieczeństwo infrastruktury służącej do przetwarzania i przechowywania gromadzonych danych. Wiąże się to z ograniczeniem fizycznego dostępu do serwerów, oddzielenie sieci wewnętrznej od Internetu, zastosowania zapór ogniowych oraz rejestrację wszelkich wykonywanych operacji.

4. Testowanie bezpieczeństwa aplikacji

Polityka bezpieczeństwa prowadzona w każdej organizacji powinna zapewniać, że [1]:

- aplikacja została przetestowana w środowisku odciętym od sieci,
- aplikacja jest ponownie testowana po każdej zmianie w konfiguracji systemu, jak również okresowo po wcześniej ustalonym upływie czasu,
- testy są aktualizowane odpowiednio do pojawiających się nowych zagrożeń,
- oprogramowanie działające na serwerze jest aktualizowane w miarę dostępności nowszych wersji aplikacji pozbawionych błędów i dziur w bezpieczeństwie w odniesieniu do wersji wcześniejszych,
- regularnie monitorowana jest cała sieć, jej komponenty składowe włączając w to zainstalowane oprogramowanie.

W celu sprawdzenia poprawności działania mechanizmów zabezpieczających należy wykonać następujące czynności [2]:

- zaplanować przebieg procedur testujących, aby zademonstrować, że pobieranie danych od użytkownika, wykonanie aplikacji i otrzymywane rezultaty działają w sposób zgodny ze specyfikacją,
- przetestować procedury odtwarzające dane w przypadku wystąpienia błędów w oprogramowaniu.

Cechy, które należy przetestować powinny obejmować [6]:

- sprzęt (procesor, dyski twarde, pamięci, karty sieciowe),
- oprogramowanie systemu operacyjnego (schemat bootowania, dostęp do aplikacji),
- aplikacje (pobieranie danych od użytkownika, zwracane wyniki),
- sprzęt sieciowy (okablowanie, huby, zapory ogniowe).

Poprawność funkcjonowania mechanizmów zabezpieczających zwiększa poziom zaufania, a tym samym czyni dane bezpiecznymi. Poznanie błędów dla każdej ścieżki wykonania aplikacji i metod przywracania danych po każdej usterce powinno stanowić cel opisywanych działań. Dzięki temu nie będzie stanowiło problemu podjęcie właściwych czynności w przypadku pojawienia się zagrożeń, kiedy aplikacja stanie się częścią oprogramowania systemu.

Problem testowania bezpieczeństwa, spełniania przez aplikację określonych wymogów bezpieczeństwa dotyczących funkcjonowania w Internecie wymusił stworzenie standardu znanego obecnie jako CC (Common Cri[illegible]a) [11]. Wytwórcy oprogramowania mogą na tej podstawie zidentyfikować wy[illegible]nia dotyczące bezpieczeństwa, które spełnia ich produkt i dostarczyć odbiorco[illegible]nizmy walidacji pokazujące, że jest tak w rzeczywistości. CC zostało zbudowane [illegible]bazie hierarchicznej modularyzacji

wymagań funkcjonalnych i bezpieczeństwa. Wymagania te zawiera dokumentacja CC lub zostały one stworzone dla potrzeb specyficznych potrzeb klienta. Rezultaty konstruowania wymagań mogą zostać ponownie użyte, służąc za składniki nowych, większych modułów. Poziomy EAL (Evaluation Assurance Levels) zaproponowane w standardzie CC są przykładem konsensusu pomiędzy osiągniętym poziomem bezpieczeństwa a kosztem jego zapewnienia:

- EAL1 przetestowane pod względem funkcjonalnym. Stosowane w przypadku wymagania zaufania do funkcjonowania produktu, ale bez nacisku na zagrożenia dla bezpieczeństwa. Ocenia zgodność implementacji produktu z jego dokumentacją i obecność mechanizmów ochronnych przeciwko zidentyfikowanym zagrożeniom.
- EAL2 przetestowane pod względem strukturalnym. Stosowane w przypadku wymagania bezpieczeństwa potwierdzonego niezależnie na poziomie niskim lub średnim, gdy kompletna dokumentacja nie jest szeroko dostępna.
- EAL3 przetestowane i sprawdzone w sposób metodologiczny. Stosowane w przypadku wymagania bezpieczeństwa potwierdzonego niezależnie na poziomie średnim oraz dokładnej analizy badanego produktu i jego rozwoju, ale bez nacisku na elementy inżynierii oprogramowania.
- EAL4 zaprojektowane, przetestowane i poddane inspekcji w sposób metodologiczny. Stosowane w przypadku wymagania bezpieczeństwa potwierdzonego niezależnie na poziomie średnim lub wysokim, gdy wytwórcy i klienci gotowi są ponieść dodatkowe koszty związane z zastosowaniem zaawansowanych technik testowania bezpieczeństwa.
- EAL5 półformalnie zaprojektowane i przetestowane. Stosowane w przypadku wymagania bezpieczeństwa potwierdzonego niezależnie na poziomie wysokim w sytuacji planowanego rozwoju oraz rygorystycznego podejścia do rozwoju produktu, gdy w grę nie wchodzi poniesienie dodatkowych kosztów związanych z zastosowaniem zaawansowanych technik testowania bezpieczeństwa.
- EAL6 półformalnie zweryfikowane ze względu na konstrukcję i przetestowane. Stosowane w przypadku rozwoju modeli bezpieczeństwa dla aplikacji w sytuacjach wysokiego ryzyka, gdy wartość chronionych zasobów uzasadnia poniesienie dodatkowych kosztów.
- EAL7 formalnie zweryfikowane ze względu na konstrukcję i przetestowane. Stosowane w przypadku rozwoju modeli bezpieczeństwa dla aplikacji w sytuacjach szczególnie wysokiego ryzyka, jak również gdy wysoka wartość zasobów uzasadnia poniesienie dodatkowych kosztów.

Najczęstszą przyczyną naruszeń bezpieczeństwa na poziomie aplikacji jest nieumiejętność programistów jego zapewnienia. Zdając sobie z tego sprawę należy poddać gruntownej inspekcji kod źródłowy aplikacji, wejścia i wyjścia, mechanizmy obsługi błędów i inne [12]. Propozycję metodologii przeprowadzenia testów opisano w dalszej części tej pracy.

Proces testowania powinien obejmować zarówno aplikacje, jak również politykę bezpieczeństwa przyjętą dla całego systemu. Testowanie aplikacji należy rozpocząć od wykonania następujących czynności [1]:

- Sporządzenia listy kluczowych komponentów, których usterki mogłyby w znacznym stopniu obniżyć poziom zabezpieczeń.
- Dla każdego zidentyfikowanego komponentu określenia listy najbardziej prawdopodobnych usterek. Należy oddzielić te elementy, których awarie nie spowodują zagrożeń dla bezpieczeństwa od tych, które nie powinny się popsuć w żadnym wypadku.
- Dla każdej usterki zaprojektowania scenariuszy testowania, które spowodują błąd lub będą go symulowały. Należy rozważyć strategię obronną, która będzie minimalizowała skutki błędów.

Przykład scenariusza testowego. Zadaniem aplikacji jest szyfrowanie połączenia pomiędzy serwerem i klientem w oparciu o mechanizm kluczy szyfrujących. Na skutek błędnego zarządzania kluczami nie jest możliwe ustanowienie bezpiecznego połączenia. Sposobem na przetestowanie takiego przypadku jest czasowe wyłączenie mechanizmu zarządzania kluczami dla celów symulacji.

Przykład strategii obronnej. Dysponujemy zastępczym serwerem kluczy, który jest pozbawiony opisywanego mankamentu. W przypadku stwierdzenia błędnego zachowania należy skorzystać z serwera zastępczego.

Schemat działania powinien obejmować różne przypadki, konfiguracje i przewidywalne rezultaty dla [1]:

- testów wejścia i wyjścia użytkownika oraz opcji zapisu zdarzeń i alarmowania o błędach,
- testów aplikacji jako całości (odzyskiwania danych w przypadku błędów sprzętu lub oprogramowania, właściwym przechowywaniu plików zapisu zdarzeń, monitorowaniu wydajności systemu),
- testów w warunkach operacyjnych, jak również w przypadku występowania anomalii.

W dalszej kolejności należy opisać narzędzia, które będą służyły celom testowania (skanery portów, monitory sieciowe, pakiety wykrywające słabości w konfiguracji, narzędzia śledzące wykonanie aplikacji) oraz właściwe testy, które zostaną przeprowadzone przy użyciu wybranych narzędzi [4].

Testy należy rozpocząć od przygotowania bezpiecznego środowiska testowego, np. połączenia dwóch maszyn pełniących funkcje wewnętrznego serwera organizacji i zewnętrznej maszyny klienta. Mechanizm zapisu zdarzeń najlepiej umieścić centralnie w bezpiecznym miejscu na serwerze. Takie rozwiązanie ułatwi późniejszą analizę plików zapisu zdarzeń. Obydwie maszyny powinny mieć zainstalowane np. narzędzia monitorujące ruch na interfejsach sieciowych i aktywność portów. Przechodząc do właściwych testów należy wykonać następujące czynności [2]:

- Wygenerować losowe wartości wejściowe, który stanowią reprezentatywną próbkę strumieni wejściowych, z wykorzystaniem dostępnych wartości. Podać przygotowane wartości na wejście aplikacji. Upewnić się, że wartości trafiają do celu.
- Poddać analizie wyniki zwracane przez aplikację. Sprawdzić, czy aplikacja nie wysyła danych niewidocznych dla użytkownika. Wykorzystać w tym celu

analizatory plików zapisu zdarzeń oraz narzędzia monitorujące ruch i aktywność portów.

- Sprawdzić, czy opcje zapisu zdarzeń i alarmowania o błędach rzeczywiście działają w zakładany sposób.

Zalecane jest przeprowadzenie testów w gronie dwóch lub więcej osób. Jedna z nich to ta, która projektowała zabezpieczenia, natomiast druga wydaje opinie co do adekwatności mechanizmów zabezpieczających.

Sieć docelowa, w której będzie funkcjonowała aplikacja, łączy maszyny, które odpowiadają na żądania kierowane zarówno wewnątrz organizacji, jak również ze świata zewnętrznego. W procesie testowania należy przeprowadzić następujące czynności [2]:

- Umieścić aplikację na serwerze centralnym.
- Ustalić dostęp do niej dla maszyn wewnątrz organizacji i ze świata zewnętrznego. Prowadzić zapis ruchu wchodzącego i wychodzącego. Do pomocy w obserwacjach można użyć monitora sieciowego.
- Sprawdzić, czy maszyny, które nie powinny mieć dostępu do aplikacji, rzeczywiście go nie posiadają. Wykorzystać w tym celu analizatory plików zapisu zdarzeń i skanery sieciowe.
- Przez skanowanie portów na każdej z maszyn należących do organizacji upewnić się, że informacje, które nie są przeznaczone dla osób z zewnątrz, są dla nich rzeczywiście niedostępne. Sprawdzić, czy nie ma możliwości uruchomienia na danym porcie usługi, która nie powinna się tam pojawić.
- Można skorzystać z narzędzi wykrywających włamania, aby przekonać się, czy nie ma zagrożeń z żadnej znanej strony. Ten krok należy ponawiać iteracyjnie, kiedy okaże się, że zostały opracowane nowe metody włamań.
- Sprawdzić, czy opcje zapisu zdarzeń i alarmowania o błędach rzeczywiście działają w zakładany sposób.

Zalecane jest przeprowadzenie opisywanej fazy testowania przed fizycznym podłączeniem sieci do Internetu. Podobnie powinno się zaczynać od konfiguracji z niewielką ilością maszyn i użytkowników stopniowo zwiększając ich liczbę.

Jeżeli podczas prowadzenia testów wykryto słabości w mechanizmach zabezpieczających aplikacji, należy upewnić się, czy nie istnieją poprawki eliminujące luki w systemie zabezpieczeń lub nowe wersje aplikacji pozbawione wcześniejszych błędów. Jeżeli takie rozwiązania są dostępne, trzeba z nich skorzystać. Jeżeli nie, należy powiadomić autora aplikacji o wynikach testów i jednocześnie podjąć próbę samodzielnego udoskonalenia zabezpieczeń. Nie należy zapominać o ciągłym monitorowaniu zachowania aplikacji. Wymiana doświadczeń i systematyczność stanowią kluczowe aspekty w walce o bezpieczeństwo.

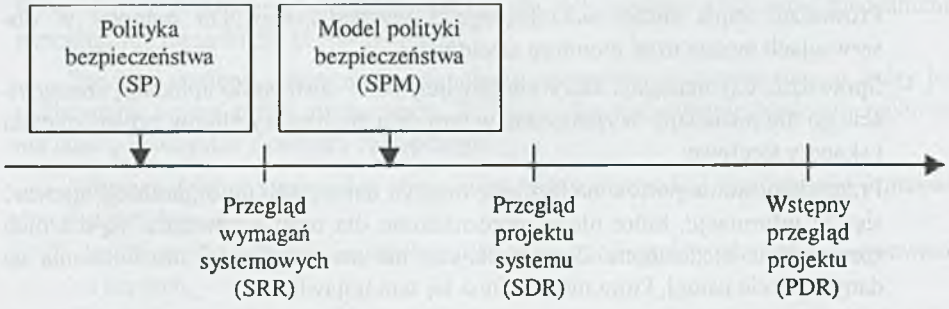
W przypadku zapełnienia plików zapisu zdarzeń należy wybrać jedno z zamieszczonych niżej rozwiązań w celu eliminacji zagrożeń związanych z funkcjonowaniem serwera pozbawionego nadzoru [1]:

- zablokowanie bieżących połączeń z serwerem,
- kontynuacja pracy z nadpisywaniem plików,
- kontynuacja pracy z wyłączoną opcją zapisu zdarzeń.

Pierwsze z proponowanych rozwiązań jest najbezpieczniejsze, ale może się wiązać ze stratami finansowymi dla organizacji. W dalszej kolejności należy wybrać odpowiednią metodę archiwizacji danych zawartych w plikach zapisu zdarzeń. Istotne cechy, które trzeba wziąć pod uwagę, obejmują:

- fizyczną lokalizację archiwum,
- odstępy czasowe pomiędzy archiwizacjami,
- okres przechowywania archiwum.

Rozszerzenie polityki bezpieczeństwa o możliwe zagrożenia dla bezpieczeństwa oraz przypisanie celów polityki i wymagań na poszczególne składowe bezpieczeństwa (fizycznego, personelu) prowadzi do powstania modelu polityki bezpieczeństwa (rysunek 8).

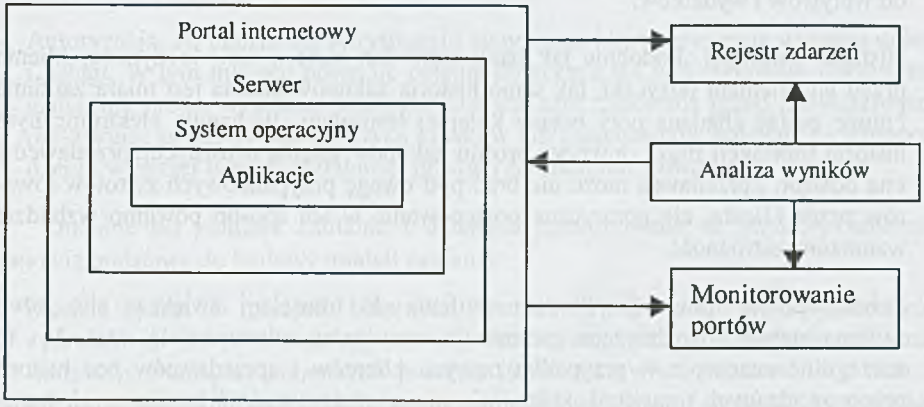


Rys. 8. Model polityki bezpieczeństwa SPM (Security Policy Model) w cyklu życia [5]

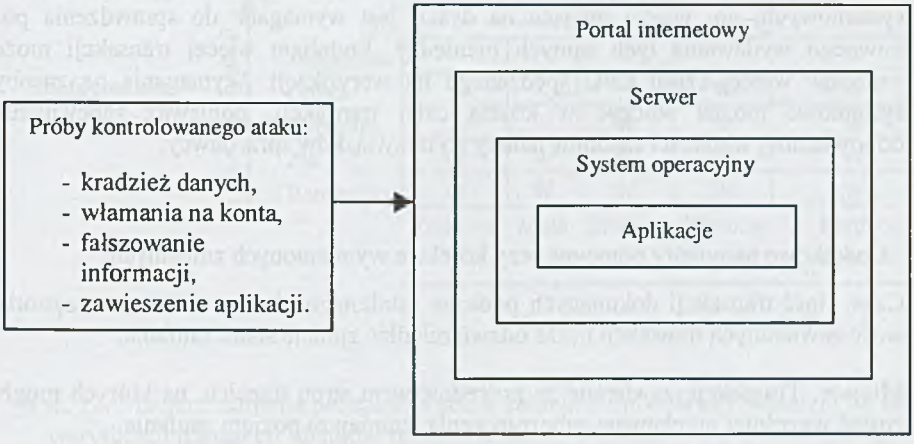
Bazując na informacjach, które pojawiły się do tej pory, można podjąć próbę specyfikacji procedur testujących bezpieczeństwo w dwojaki sposób, tzn. przez analizę bezpieczeństwa (rysunek 9) lub próby kontrolowanego ataku na zabezpieczenia (rysunek 10):

- analizowanie kodu źródłowego aplikacji, adekwatności mechanizmów zabezpieczeń, co do wystarczalności i poprawności, spójności pomiędzy oficjalną dokumentacją i aktualną implementacją,
- analizowanie plików zapisu zdarzeń (zdarzenia i sytuacje wyjątkowe),
- skanowanie aktywności portów (vanilla TCP connect), TCP SYN (half open), TCP FIN lub NULL (stealth), TCP FTP proxy (bounce attack), SYN/FIN przy użyciu IP (packet filters), UDP za pomocą ICMP (ping-sweep), TCP ping, RPC (Remote Procedure Call) w sposób bezpośredni,
- przeprowadzanie ataków specyficznych dla usług sieciowych (TCP/UDP highjacking, IP spoofing),
- przeprowadzanie ataków specyficznych dla oprogramowania systemu (buffer overflow),
- przeprowadzanie ataków odmowy obsługi (SYN flooding, Pentium "F00F" Bug, ping flooding, Email bombing and spamming),

- sprawdzanie zabezpieczeń w DNS (DNS spoofing),
- testowanie zabezpieczeń zapory ogniowej (source routing, source port spoofing oraz routing redirection),
- generowanie raportów podsumowujących poziom bezpieczeństwa.



Rys. 9. Testowanie przez analizę bezpieczeństwa



Rys. 10. Testowanie przez kontrolowany atak

Bezpieczeństwo wiąże się nierozerwalnie z zaufaniem. Problem pomiaru bezpieczeństwa systemu można rozwiązać wprowadzając różne zmienne zależne, np. koszt

jego osiągnięcia. Całkowite ryzyko związane z przeprowadzeniem transakcji jest funkcją tych zmiennych [10]:

- Koszt transakcji. Po pierwsze, ryzyko jest funkcją wartości towarów i usług. Klient poświęca więcej uwagi przy dokonywaniu kosztownych zakupów. Podobnie sprzedawca nie martwi się o straty mogące wyniknąć z drobnej transakcji, ale ryzyko rośnie wraz ze wzrostem wartości transakcji, jak również uwaga sprzedawcy zależnie od wpływów i wydatków.

- Historia transakcji. Podobnie jak bank sprawdza historię linii kredytowej klienta przed udzieleniem pożyczki, tak samo historia zakupów klienta jest miarą zaufania i może zostać zbadana przy ocenie kolejnej transakcji. W handlu elektronicznym historia transakcji może dotyczyć profilu zakupów klienta u różnych sprzedawców i na odwrót. Sprzedawca może nie brać pod uwagę przypadkowych zwrotów towarów przez klienta, ale notoryczne postępowanie w ten sposób powinno wzbudzić wzmożoną ostrożność.

- Zabezpieczenie transakcji. Poziom zaufania do transakcji zwiększa się, jeżeli zaufana strona pośrednicząca gwarantuje ewentualną rekompensatę strat. Ma to szczególne znaczenie w przypadku nowych klientów i sprzedawców bez historii przeprowadzanych transakcji, którzy nie mogą przeprowadzać kosztownych transakcji bez poręczenia.

- Wzory zakupów. W przypadku włamania na komputer, z którego klient przeprowadza transakcje, lub kradzieży karty kredytowej możliwe jest wykrycie podejrzanych zachowań przez obserwację zmian w dotychczasowych zachowaniach (wzorach zakupów) klienta.

- Zasoby systemowe. Zwiększenie ilości transakcji zwiększa zajętość zasobów systemowych, np. więcej miejsca na dysku jest wymagane do sprawdzenia ponownego wydawania tych samych pieniędzy. Podobnie więcej transakcji może oznaczać więcej czasu CPU spędzanego na weryfikacji. Wymagania na zasoby systemowe można wliczyć w koszta całej transakcji, ponieważ zapewnienie odpowiedniej wielkości zasobów należy do obowiązków sprzedawcy.

Dodatkowe parametry pomocne przy korekcie wymienionych zmiennych:

- Czas. Ilość transakcji dokonanych podczas ustalonego okresu, w którym częstotliwość zawieranych transakcji może odzwierciedlać zmianę stanu zaufania.

- Miejsce. Transakcje zawierane za pośrednictwem stron trzecich, na których mogły zostać wcześniej przełamane zabezpieczenia, zmniejsza poziom zaufania.

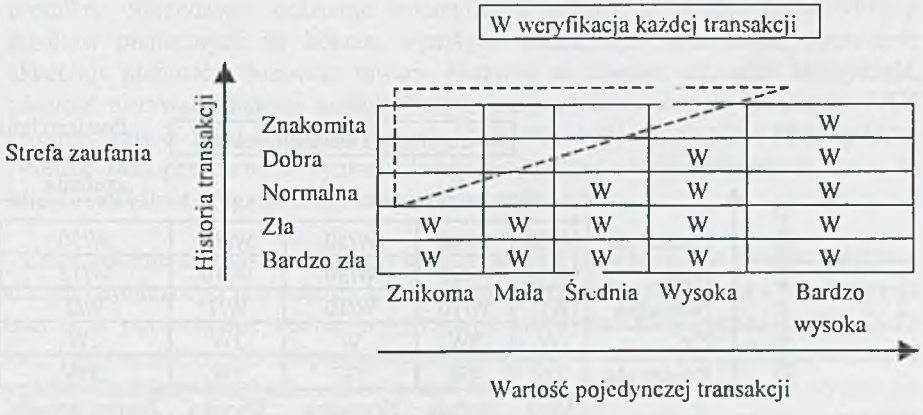
Po zdefiniowaniu zmiennych do pomiaru zaufania, transakcja może zostać zaakceptowana lub odrzucona na podstawie wartości zaufania wyznaczonego w ten sposób. Inne podejście do wyznaczenia zaufania wprowadza działania polegające na weryfikacji zdolności kredytowych klienta lub sprzedawcy i autoryzacji:

- Weryfikacja zdolności kredytowych. Sprzedawcy mają tendencję do weryfikacji każdej płatności klienta. Jeżeli jednak koszt weryfikacji będzie wysoki, pominięta zostanie weryfikacja transakcji o małej wartości. W miarę wzrostu ilości transakcji koszt weryfikacji wyrażony przetwarzaniem i przechowywaniem danych oraz czasem weryfikacji stanie się trudny do zarządzania. Rozwiązaniem może być weryfikacja losowo wybranych transakcji. Podobnie stopień zaufania klientów do sprzedawców jest z góry ograniczony.

- Autoryzacja. Po pomyślnej weryfikacji i autoryzacji klient otrzymuje wybrane dobra i usługi. W tym miejscu powstaje pytanie dotyczące ich wykorzystania i przestrzegania, np. prawa wyłącznej własności. Jedyne zabezpieczenia przed niewłaściwymi praktykami ze strony nieuczciwych klientów lub sprzedawców polegają na wprowadzeniu większej odpowiedzialności prawnej za zakupione towary.

Zmienne do pomiaru zaufania i działania podejmowane do jego wyznaczenia stanowią podstawę do budowy modeli zaufania:

- Modele oparte na relacjach binarnych (rysunek 11). Dwie lub więcej zmiennych i parametrów może zostać użytych do wyznaczenia poziomu zaufania wybranej transakcji. Pomiędzy zmiennymi powinna istnieć oczywista zależność, aby dobrze zdefiniować model zaufania. Zależność najlepiej przedstawić w macierzy wpisując na przecięciu odpowiedniego wiersza i kolumny wymagane działania związane z wyznaczeniem zaufania.

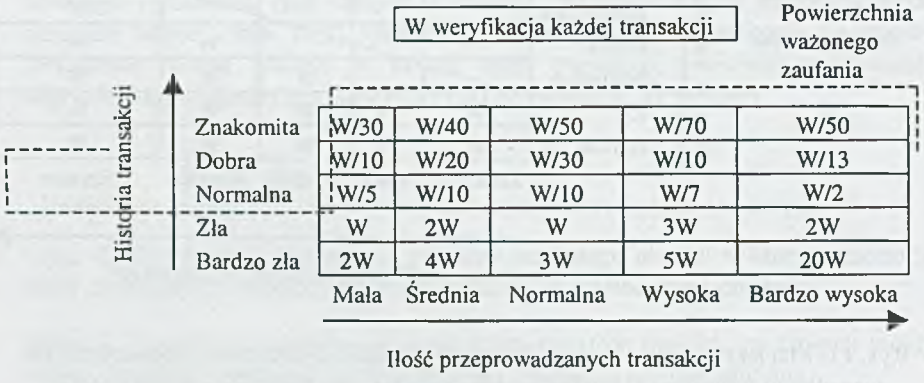


Rys. 11. Macierz zaufania pokazująca strefę zaufania. Sprzedawcy skłaniają się do weryfikacji transakcji klientów ze słabą historią. Dla klientów z dobrą historią prawdopodobieństwo weryfikacji rośnie wraz ze wzrostem wartości transakcji

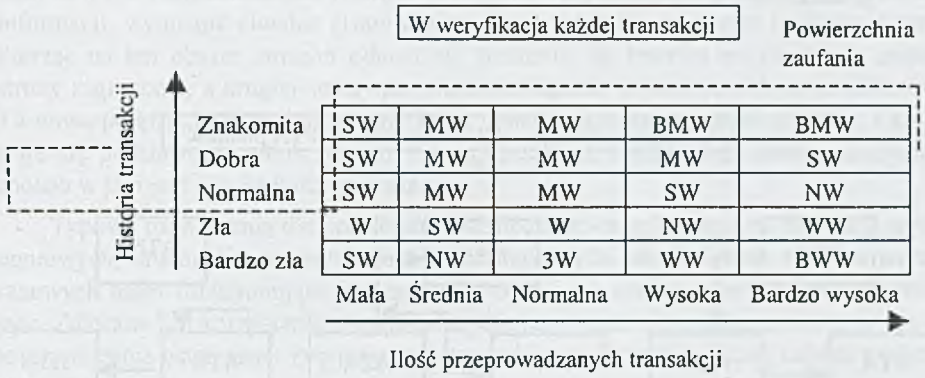
- Modele oparte na automacie stanów transakcji. Dozwolone stany transakcji handlu elektronicznego to zakończona pomyślnie, zakończona błędem, w trakcie wykonywania i w trakcie ataku. Transakcja zostanie zakończona pomyślnie, jeżeli strona

nadzorująca otrzyma potwierdzenia od wszystkich stron biorących w niej udział. Nie oznacza to jednak, że stan transakcji nie może ulec zmianie. Strona nadzorująca przebieg transakcji może uznać, że naruszone zostało zaufanie stron i zmienić stan transakcji z zakończonej pomyślnie na stan w trakcie ataku. Stan w trakcie wykonywania oznacza, że strona nadzorująca transakcję nie otrzymała kompletnego potwierdzenia od przynajmniej jednej ze stron biorących w niej udział. Transakcja zostanie zakończona błędem jeżeli strona nadzorująca nie otrzyma potwierdzeń od stron w niej uczestniczących przed upływem z góry ustalonego czasu (może wówczas nastąpić ponowne wznowienie transakcji) lub potwierdzenia będą błędne (wówczas nastąpi zmiana stanu zakończona błędem na w trakcie ataku). Przejście transakcji w stan w trakcie ataku powoduje przełączenie bieżących zadań w tryb prewencji, co zabezpiecza przed wyrządzeniem dalszych zniszczeń. Tryb prewencji powoduje czasowe zawieszenie działalności stron biorących udział w transakcji. Jeżeli będzie to tylko możliwe nastąpi próba likwidacji wyrządzonych szkód i ponowne wznowienie zawieszonych działań.

- Modele oparte na systemach eksperckich (rysunek 12 i rysunek 13). Różnią się od modeli binarnych tym, że dodają do wpisanych w macierzy działań wagi dla odróżnienia różnego stopnia pomiarów, np. nie jest uzasadnione przeprowadzanie weryfikacji transakcji dla klienta z dobrą historią w tym samym stopniu co dla klienta ze słabą historią nawet w przypadku transakcji o dużej wartości. Takie postępowanie formuje trójwymiarową powierzchnię ważonego zaufania z dolinami i szczytami. Ustalenie progów zaufania i przypisanie wartościom macierzy zrozumiałych terminów (BW – bardzo wysoka, W – wysoka, N – normalna, Ś – średnia, S – niska, M – mała, BM – bardzo mała) umożliwia ich użycie w systemach wiedzy.



Rys. 12. Weryfikacja ważonych transakcji. Im większa liczba transakcji i gorsza historia transakcji klienta tym częstsze weryfikacje



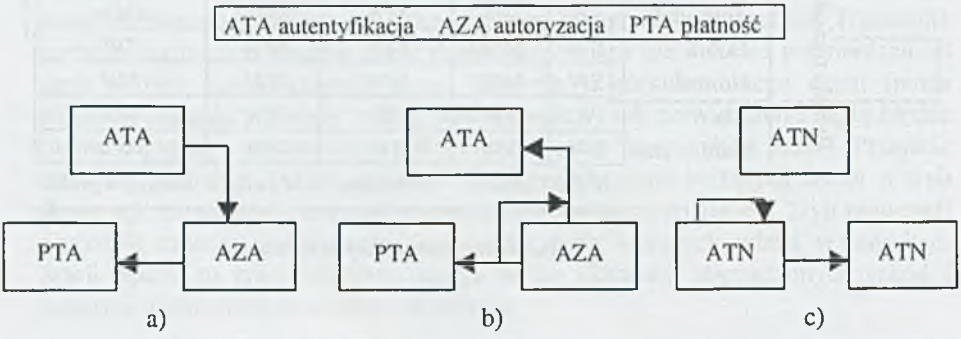
Rys. 13. Macierz zaufania dla systemu wiedzy. Wartości dyskretne zostały zastąpione bardziej zrozumiałymi terminami

- Modele oparte na procesach transakcji. Proces transakcji w handlu elektronicznym przed dostawą towarów do klienta przebiega według schematu autentyfikacja klienta, autoryzacja i płatność AAP (Authenticate; then Authorize and Pay, rysunek 14a). Proces zostaje zainicjowany przez klienta po ustaleniu zaufania do dostawcy na podstawie oferty cyfrowo podpisanej przez zaufaną stronę pośredniczącą. Oferta zawiera stopień zadowolenia innych klientów z kontaktów z dostawcą i specyfikację produktu. Sprzedawca dokonuje autentyfikacji klienta na podstawie weryfikacji środków pieniężnych na koncie, wymagań wieku, itp. Sprzedawca ostatecznie akceptuje płatność i dostarcza towary. Możliwe są również schematy autoryzacja, płatność nazywany inaczej autentyfikacją, jeżeli zaufanie zostało naruszone ATV (Authenticate-if-Trust-Violated, rysunek 14b), oraz najpierw płatność PF (Pay-First, rysunek 14c) przydatne w sytuacji, kiedy nie można ustalić poziomu zaufania do klienta lub klient pragnie zachować anonimowość.

Zastosowanie modeli zaufania do analizy ataków związanych z bezpieczeństwem handlu elektronicznego pozwala na lepsze poznanie metod wykrywania i zapobiegania atakom oraz opracowanie metod przywracania stanu transakcji sprzed ataku. O ile metody kryptograficzne chronią informacje przesyłane w Internecie, są bezużyteczne w przypadku kradzieży haseł lub numerów kart kredytowych. Nawet model PF wydaje się być niewystarczający dla tego typu ataku, a wszystko co pozostaje do zrobienia to próba minimalizacji strat takiej transakcji. Modele zaufania mogą pomóc w zrozumieniu przebiegu możliwego ataku i minimalizacji strat, ale żaden z omawianych modeli nie jest w stanie zapobiec lub wykryć takiego ataku. Zamiast tego zalecane jest wykorzystanie metod:

- detekcji ataku na podstawie analizy zachowania (wzoru zakupów) klienta,
- prewencji na podstawie opóźnienia przekazania klucza odszyfrowującego dane zakupione przez klienta,

– likwidacji szkód wyrządzonych przez atak na podstawie zabezpieczenia transakcji przez firmę ubezpieczeniową.



Rys. 14. Trzy modele oparte na procesach transakcji: a) AAP, b) ATV, c) PF

5. Wnioski końcowe

Bezpieczeństwo systemu można uzyskać poprzez wprowadzenie różnego typu mechanizmów ochrony. Niniejsze opracowanie ma na celu poprawienie bezpieczeństwa przez podniesienie świadomości. Poznanie, dlaczego coś jest problemem, stanowi klucz do sukcesu. Nie jest to natomiast wyczerpujący schemat działań, ale raczej zestaw przykładów mających pobudzić do dyskusji. Bezpieczeństwo Internetu bazuje na zaufaniu i uczciwości użytkowników. Podniesienie poziomu bezpieczeństwa wiąże się z wyeliminowaniem anonimowości użytkowników poprzez wprowadzenie strukturalnego systemu certyfikatów. Sprowadza się to do ustalenia granicy między prywatnością użytkowników a stopniem akceptowalnego ryzyka. Struktura PKI przenosi jedynie środek ciężkości bezpieczeństwa na instytucje rządowe. Metody kryptograficzne rozwijają się w kierunku algorytmów asymetrycznych opierających się na coraz bardziej złożonych operacjach matematycznych (krzywe eliptyczne). W przypadku zaawansowanych systemów handlu elektronicznego nieodzowne staje się zastosowanie technik biometrycznych. Transakcje opiewające na wysokie kwoty wymagają porównania np. wzorów odcisków palców klienta z przechowywanymi w bazie danych, a w przypadku wykrycia podejrzanego zachowania klienta, następuje wstrzymanie przekazania klucza, którym zaszyfrowano towary i zostaje skierowanie żądania dodatkowej identyfikacji poprzez dostarczenie bardziej wiarygodnych i niepowtarzalnych informacji, jak wybranych cech biometrycznych człowieka, np. wzoru tęczówki oka lub charakterystyki głosu.

Przedyskutowano możliwe zagrożenia i wskazano na sposoby pozbycia się ich. Takie konstrukcje zasadniczo wpływają zarówno na metodologie wytwarzania oprogramowania, jak i na politykę bezpieczeństwa systemów. Najsilniejszą bronią jest wieloplaszczyznowa analiza bezpieczeństwa. O skuteczności decyduje szybkość z jaką

następuje reakcja na pojawiające się zagrożenia. Wymaga to ciągłej wymiany doświadczeń na polu bezpieczeństwa. Internet udostępnia w tym zakresie niezastąpione źródło informacji, wymienić chociaż grupy dyskusyjne poświęcone tematyce bezpieczeństwa. Patrząc na ten obszar zmagań odnosi się wrażenie, że Internet przynosząc z jednej strony zagrożenia, z drugiej strony przynosi rozwiązania pojawiających się problemów. Ta nowa potężna broń to informacja, która obecnie dociera wszędzie szybciej, i która staje się podstawową, obok materii i energii, cząstką otaczającego świata. Decyduje sposób w jaki jest ona wykorzystywana.

Typowe rozwiązania dla problemów bezpieczeństwa polegające na instalacji zapór ogniowych, uruchomieniu protokołów kryptologicznych lub używaniu systemu jednorazowych haseł funkcjonujące w oderwaniu od innych zabezpieczeń są niewystarczające. Zalecane jest korzystanie z wymienionych rozwiązań, ale pod warunkiem, że nie są to rozwiązania ostateczne. Powinny one stanowić raczej część większej całości mającej chronić system.

Literatura

[1] National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Generally Accepted Principles and Practices for Securing Information Technology Systems, Marianne Swanson, Barbara Guttman, September 1996.

[2] U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards, FIPS PUB 73, Guidelines for security of computer applications, 1980 June 30.

[3] Getting to Know You (Intimately): Surreptitious Privacy Invasion on the E-Commerce Web, Matt Curtin, Paul Graves, Shaun Rowland, Interhack Corporation, 2000/07/31.

[4] Security for Businesses on the Internet, Marianne Mueller, January 11, 1995.

[5] The Security Policy Model: A Chapter of the Handbook for the Computer Security Certification of Trusted Systems, C.N. Payne, Naval Research Laboratory Technical Memorandum 5540:080A, 24 Jan 1995.

[6] A Guide to Understanding Security Testing and Test Documentation in Trusted Systems, National Computer Security Center, July 1993.

[7] Electronic and Digital Signatures: In Search of a Standard, Thomas O. Wells, IEEE IT Pro, May | June 2000.

[8] Credits and debits on the Internet, Marvin A. Sirbu, IEEE SPECTRUM, FEBRUARY 1997.

[9] Eco System: An Internet Commerce Architecture, Jay M. Tenenbaum, Tripatinder S. Chowdhry, Kevin Hughes, IEEE Computer, May 1997.

[10] E-Commerce Trust Metrics an Models, Daniel W. Manchala, IEEE INTERNET COMPUTING, MARCH • APRIL 2000.

[11] Building an International Security Standard, Kimberly Caplan and James L. Sanders, IEEE IT Pro, March | April 1999.

[12] Raising the Bar on Software Security Testing, Alden Dima, John Wack, and Shukri Wakid, IEEE IT Pro, May | June 1999.

[13] Centrum Cerytfikacji, http://www.certum.pl/pl/dokumentacja/slownik
[14] E-podpis, http://www.ipipan.waw.pl/~marians/e-podpis
[15] Globeset Payment System, http://www.globeset.com/products/set/index.html
[16] SETCo, http://www.setco.org/setmark
[17] SSL, http://www.ssl.org
[18] IPSec, http://www.ietf.org/html.charters/ipsec-charter.html
[19] IBM Commerce Point, http://www.internet.ibm.com/commercepoint
[20] Microsoft Merchant Server, http://www.microsoft.com/merchant
[21] Netscape ONE, http://home.netscape.com/comprod/one/white_paper.html
[22] Oracle NCA, http://www.oracle.com/nca/html/nca_wp.html
[23] Sun/JavaSoft JECF, http://www.javasoft.com/products/commerce

ADRIAN KAPCZYŃSKI
POLITECHNIKA ŚLĄSKA GLIWICE

Analiza porównawcza wybranych biometrycznych rozwiązań sprzętowo-programowych wykorzystujących badanie linii papilarnych w procesie uwierzytelniania

Comparative analysis of chosen biometric solutions based on examining fingerprint in authentication process

Streszczenie

W artykule przedstawiono analizę porównawczą rozwiązań biometrycznych badających linie papilarne z punktu widzenia zastosowanego sprzętu oraz oprogramowania. Rozwiązanie sprzętowe Keyboard G81-12000 firmy Cherry GMBH wraz z oprogramowaniem Biologon Security System firmy Identicator Technology zostało porównane z rozwiązaniem sprzętowym firmy Veridicom 5th Sense i oprogramowaniem Veridicom Protector Suite. Uzupełnieniem prezentacji słabych oraz silnych stron badanych rozwiązań stanowi opracowanie preferencji wykorzystania każdego z nich.

Abstract

In presented paper, having in mind applied hardware and software, comparative analysis of biometric solutions examining fingerprints was provided. Hardware solution Cherry GMBH Keyboard G81-12000 with integrated DFR-200 scanner along with software Identicator Technology Biologon Security System was compared with hardware solution Veridicom 5^{th} Sense and software Veridicom Protector Suite. As a result, on ground of list of strong and weak points of each solution, preferred application was suggested.

1. Wprowadzenie

Biometryczne metody identyfikacji zapewniają znacznie wyższy poziom zabezpieczenia niż stosowane obecnie hasła, stanowiąc dla pozostałych mechanizmów uwierzytelniania alternatywę bądź ich uzupełnienie. Współczesne systemy biometryczne wykorzystują w procesie uwierzytelniania cechy anatomiczne oraz behawioralne użytkowników. W ostatnim czasie można zauważyć dynamiczny rozwój systemów biometrycznych bazujących na pomiarach cech anatomicznych w procesie uwierzytelniania.

W roku 1999 ponad 50% firm biometrycznych związanych było z metodą badającą linie papilarne [2].

Obecnie dostępnych na rynku jest szereg urządzeń służących do skanowania struktury linii papilarnych, wykorzystujących w tym celu różne technologie. Na implementację rozwiązań sprzętowych pozwalają zróżnicowane rozwiązania programowe.

Całościowe, sprzętowo-programowe rozwiązania biometryczne bazujące na badaniu linii papilarnych są przedmiotem zainteresowań niniejszego artykułu. Zestawienie słabych oraz mocnych stron każdego z wybranych biometrycznych rozwiązań sprzętowo-programowych, będące wynikiem dogłębnej analizy, pozwoliło na opracowanie preferencji wykorzystania każdego z rozwiązań.

W pierwszej kolejności zostanie przedstawiona istota uwierzytelniania bazującego na badaniu linii papilarnych. Następnie, zostaną scharakteryzowane wybrane rozwiązania biometryczne, stanowiące bazę dla analizy porównawczej, której wyniki zamieszczono w końcowej części artykułu.

2. Uwierzytelnianie na podstawie linii papilarnych

2.1 Ogólna charakterystyka, wady i zalety oraz przykłady zastosowań

Badanie linii papilarnych jest jedną z metod pozwalających na przeprowadzenie identyfikacji (weryfikacji) tożsamości użytkownika. Pobrany obraz linii papilarnych (przedstawiany dalej w postaci zbioru punktów) jest porównywany z zachowanym wzorcem. Niemożliwym jest przeprowadzenie procesu odwrotnego, tj. w wyniku którego na bazie przechowywanych informacji zostanie wykreowany obraz odcisku palca.

Zalety:

- technika badania linii papilarnych należy do najpopularniej stosowanych z uwagi na niewielki koszt oraz rozmiar urządzenia przeprowadzającego pomiar,
- technika badania linii papilarnych jest intensywnie rozwijana,
- w celu jednoznacznego potwierdzenia tożsamości użytkownika wystarczy określić usytuowanie kilkunastu minucji (ang. *Minutiae points*), tj. punktów początkowych lub przecięć linii papilarnych.

Wady:

- wpływ stanu powierzchni palca na wynik pomiaru (zabrudzenie, stopień nawilżenia).

Rozpoznawanie odcisków palców znajduje przykładowo następujące zastosowanie:

- bankomaty,
- kontrola fizycznego dostępu (w obiektach o podwyższonym stopniu bezpieczeństwa),
- kontrola dostępu do stacji roboczych i sieci komputerowych,

– kontrola dostępu w urządzeniach elektronicznych (notebook, telefon komórkowy).

Praktyczne przykłady systemów biometrycznych wykorzystujących omawianą metodę [2]:

- Charles Schwab&Co. (USA),
- Walt Disney World, Orlando (USA).

2.2. Metody odczytywania struktury linii papilarnych

Skanowanie linii papilarnych poprzez urządzenia biometryczne mogą być realizowane przede wszystkim za pomocą metod optycznych, pojemnościowych oraz wykorzystujących ultradźwięki.

Skanery optyczne, wykorzystujące do odczytu obrazu linii papilarnych specjalne matryce CCD (ang. *Coupled charge device*), cechują się wieloma wadami, m.in.: niski kontrast, duża wrażliwość na zabrudzenie powierzchni palca czy też brak pewności, czy obserwowany jest żywy palec, czy też jest to pozostawiony po nim ślad [3]. Tańsze, mniej zawodne od skanerów optycznych, są specjalizowane płytki krzemowe, które pozwalają uzyskać obraz linii na podstawie tworzonej matrycy pojemnościowej. Ostatnią grupę stanowią urządzenia ultradźwiękowe, pozwalające na skanowanie linii papilarnych za pomocą zogniskowanej wiązki ultradźwiękowej lub kamery holograficznej. Skanery ultradźwiękowe nie są wrażliwe na zabrudzenia czy zniszczenia powierzchni palca, pozwalając na skanowanie linii papilarnych nawet przez warstwę materiału.

3. Założenia analizy rozwiązań sprzętowo-programowych

a) Badaniu poddano następujące rozwiązania sprzętowo-programowe:

Rozwiązanie 1:

- Sprzęt: Keyboard G81-12000 firmy Cherry GMBH z czytnikiem linii papilarnych DFR-200 firmy Identicator Technology;
- Oprogramowanie: Biologon Security System 2.0 firmy Identicator Technology.

Rozwiązanie 2:

- Sprzęt: czytniki linii papilarnych 5thSense Sensor firmy Veridicom;
- Oprogramowanie: Protector Suite 3.5 firmy Veridicom.

b) Wybrane rozwiązania zostały przeanalizowane z punktu widzenia zastosowanego sprzętu, oprogramowania oraz właściwości implementacyjnych.

4. Charakterystyka rozwiązania firmy Identicator Technology

4.1. Warstwa sprzętowa

Testom poddany został zintegrowany z klawiaturą czytnik linii papilarnych Identicator Technology DFR-200. Czytnik ten stanowi przykład optycznego skanera linii papilarnych, o rozdzielczości 330 dpi przy powierzchni skanowania 0,72″ × 072″.

Czytniki tej rodziny mogą być osadzane w innych urządzeniach (klawiatura, mysz) lub też mogą być stosowane jako wolnostojące.

Oprócz skanera linii papilarnych w klawiaturze został osadzony czytnik kart elektronicznych zgodny ze standardem GemPlus GemCore. Jednakże przyjęto założenie, iż analizie zostaną poddane implementacje, w których wykorzystywany jest wyłącznie czytnik linii papilarnych.

4.2. Warstwa programowa

W badaniach wykorzystano oprogramowanie Biologon Security System w wersji 2.0., które jest rozwiązaniem przeznaczonym dla środowisk z systemami operacyjnymi firmy Microsoft, tzn.:

- MS Windows 95/98 (wraz z Internet Explorer v. 3.02 lub nowszym),
- MS Windows NT Workstation 4.0 (wraz z Service Pack 3 lub wyższym).

Minimalne wymagania niezbędne do instalacji oraz użytkowania Biologon Security System v. 2.0 obejmują [5]:

- procesor: 486/33DX lub szybszy,
- pamięć RAM: 16 MB (32 zalecane),
- wolna przestrzeń dysku twardego: 10 MB,
- port równoległy: dostępny,
- karta graficzna: standard VGA lub o wyższej rozdzielczości,
- urządzenie wskazujące: mysz lub inne.

W skład pakietu wchodzi Biologon 2.0 Client. Dodatkowo, można nabyć:

- Biologon 2.0 Server (rozwiązanie dla dużych sieci komputerowych),
- Biocard Client: add smart card to Biologon Client (obsługa karty elektronicznej),
- Biosafe (szyfrowanie danych),
- Bioshield (zarządzanie hasłami),
- Biologon SDK (integracja z własnymi aplikacjami).

4.3. Implementacja systemu biometrycznego

Wdrożenie systemu biometrycznego w systemie komputerowym wiąże się z instalacją zarówno na stacjach roboczych, jak i serwerach, stanowiących składniki sieci komputerowej. W niniejszym artykule założono przeprowadzenie jednostanowiskowej (indywidualnej) implementacji systemu biometrycznego na stacji roboczej z systemem MS Windows 9x.

W przypadku implementacji jednostanowiskowej występuje jedna stacja robocza, zatem w celu zaimplementowania systemu identyfikacji opartego o metodę biometryczną, należy jednokrotnie zrealizować procedurę instalacji klawiatury z czytnikiem biometrycznym oraz oprogramowania.

Instalacja sprzętu związana jest z ustawieniem trybu portu równoległego na ECP/EPP oraz podłączeniem klawiatury (podłączenie wtyczki 9-pin SUB-D kabla do

wolnego portu szeregowego, podłączenie wtyczki 25-pin SUB-D kabla do wolnego portu równoległego, podłączenie wtyczki kabla klawiaturowego do gniazda PS/2).

Instalacja oprogramowania biometrycznego jest zbliżona dla klienckich systemów operacyjnych firmy Microsoft (MS Windows 9x/NT Workstation). W trakcie inicjalizacji oprogramowania systemu biometrycznego następuje wybór użytkownika, któremu zostaną przydzielone prawa administratora (wybór jednego z istniejących już kont lub stworzenie nowego konta). Po dostrojeniu czytnika linii papilarnych następuje uruchomienie kreatora poboru wzorca biometrycznego administratora. Pobór wzorca biometrycznego związany jest ze skanowaniem linii papilarnych wybranego palca oraz weryfikacji (powtórne skanowanie odcisku wybranego palca oraz porównanie ze wzorcem pobranym wcześniej).

Po zakończonym etapie instalacji oprogramowania użytkownik pełniący funkcję administratora może zostać zidentyfikowany w systemie poprzez: podanie nazwy użytkownika oraz hasła, podanie nazwy użytkownika oraz dostarczenie odcisku palca, podanie PIN-u oraz dostarczenie karty chipowej. Domyślnie, po instalacji opisywanego oprogramowania wszystkie z wymienionych powyżej metod zalogowania się są dostępne. Z rozwijanego menu, oprócz możliwości wyboru metody logowania, można dostroić czytnik linii papilarnych oraz przeprowadzić test poprawności zainstalowanych komponentów systemu Biologon Security System.

Użytkownik pełniący funkcję administratora za pomocą Biologon Security może ustalić dostępność metod logowania z menu okna logowania do systemu (grupa opcji Workstation Policy). Ponadto, z poziomu grupy opcji Security level może być konfigurowana wielkość wskaźnika błędnych akceptacji (FAR) mogącego przyjąć jedną z trzech wartości: 1/1000 (średni poziom), 1/10000 (wysoki poziom), 1/100000 (bardzo wysoki poziom). Istnieje również możliwość zapisu zdarzeń do pliku log na jednym z trzech poziomów szczegółowości: standardowym, szczegółowym, pełnym [1].

Administrator posiada możliwość operowania na kontach użytkowników. Dla każdego konta administrator może określić, czy użytkownik jest użytkownikiem biometrycznym (ang. *Biometrics User*), czy też pozostaje użytkownikiem niebiometrycznym (ang. *Windows password user*). Zaliczenie danego użytkownika do grupy użytkowników biometrycznych pozwala na sprecyzowanie typu logowania (ang. *logon type*): wyłącznie odcisk palca, odcisk palca lub hasło, odcisk palca i hasło.

W przypadku Microsoft Windows 95/98, instalacja Biologon Security System v. 2.0 podniosła bezpieczeństwo systemu na drodze wprowadzenia wybranych rozwiązań stosowanych w przypadku systemu(ów) Microsoft Windows NT. Za przykład może posłużyć okno bezpieczeństwa (ang. *Windows security*) uruchamiane poprzez naciśnięcie klawiszy CTRL+ALT+DELETE pozwalające (podobnie jak użytkownikom systemów rodziny Microsoft Windows NT) dokonać następujących operacji: Zamknij system, Uruchom menedżer zadań, Zmień hasło, Zablokuj stację. Użytkownik, po zalogowaniu na swoje konto w tradycyjny sposób (hasło), posiada (o ile administrator tego nie zabronił) możliwość przeprowadzenia procedury poboru przez system wzorców biometrycznych.

Niestety, nie występuje możliwość zdalnego zarządzania systemami biometrycznymi poszczególnych stacji przez osobę pełniącą funkcję administratora. Występuje ponadto ryzyko naruszenia integralności mechanizmu bezpieczeństwa związaneg

z identyfikacją użytkowników, z uwagi na niewłaściwe przechowywanie wzorców biometrycznych w rejestrze systemu, co związane jest z następującymi zagrożeniami:

- wszyscy użytkownicy (biometryczni oraz niebiometryczni) posiadają możliwość ustalenia właściwości mechanizmu bezpieczeństwa (akceptowane sposoby logowania, rodzaj audytu, poziom stopy błędnej autoryzacji) obowiązujące dla wszystkich użytkowników danej stacji roboczej,
- naruszenia spójności funkcjonowania systemu, które może przyjąć postać:
  - braku możliwości zalogowania się do systemu użytkowników, którzy nie pozostawili wzorca biometrycznego,
  - możliwości podmiany/usunięcia wzorca biometrycznego użytkownika(ów),
  - możliwości zmiany hasła ustanowionego przez danego użytkownika.

4.4. Wady i zalety rozwiązania firmy Identicator Technology

Poniżej przedstawiono silne oraz słabe strony omawianego systemu, zauważone w trakcie każdego z etapów: instalacji, uruchomienia, konfiguracji oraz użytkowania systemu.

Etap 1. Instalacja oprogramowania oraz sprzętu do identyfikacji biometrycznej.

1. Zalety:
   - szybki, nieskomplikowany proces instalacji, realizowany za pomocą kreatora,
   - wymagana stosunkowo niewielka ilości wolnego miejsca na twardym dysku.

2. Wady:
   - konieczność zapewnienia niezajętego portu równoległego,
   - funkcjonowanie wyłącznie w środowiskach systemowych firmy Microsoft.

Etap 2. Uruchomienie systemu.

1. Zalety:
   - uruchamianie testów diagnostycznych czytnika linii papilarnych po włączeniu systemu,
   - możliwość przeprowadzenia dodatkowych testów diagnostycznych czytnika,
   - możliwość dostrojenia przed zalogowaniem czytnika linii papilarnych,
   - możliwość wyboru z menu sposobu logowania,
   - zamknięcie systemu w wypadku próby logowania przez nieautoryzowanego użytkownika na konto, które nie istnieje.

2. Wady:
   - wydłużony czas oczekiwania na uruchomienie procedury logowania użytkownika do systemu, z uwagi na konieczność połączenia się z odpowiednimi komponentami Biologon Security System v. 2.0.

Etap 3. Konfiguracja i administracja systemem.

1. Zalety:
   - możliwość dostosowania opcji logowania do danej stacji (Workstation policy),

- dodatkowy komponent panelu sterowania centralizujący narzędzia konfiguracji systemu biometrycznego,
- możliwość przeprowadzenia audytu na różnych poziomach szczegółowości,
- możliwość dostosowania poziomu stopy błędnej autoryzacji,
- możliwość administracji kontami użytkowników zarówno biometrycznych, jak i niebiometrycznych z poziomu komponentu Użytkownicy (dzięki modyfikacji tego składnika – dodanie przycisku polecenia „Biometrics"),
- możliwość ustalenia dla każdego z użytkowników z osobna sposobu logowania.

2. Wady:
- wszyscy użytkownicy (biometryczni oraz niebiometryczni) posiadają możliwość ustalenia właściwości mechanizmu bezpieczeństwa (akceptowane sposoby logowania, rodzaj audytu, poziom stopy błędnej autoryzacji) obowiązujące dla wszystkich użytkowników danej stacji roboczej,
- potencjalne zagrożenie naruszenia spójności funkcjonowania systemu.

Etap 4. Użytkowanie systemu.

1. Zalety:
- szybki proces logowania,
- możliwość stosowania więcej niż jednej metody uwierzytelniania,
- implementacja wybranych elementów rozwiązań bezpieczeństwa zastosowanych w MS Windows NT,
- możliwość przeprowadzenia procedury poboru wzorców biometrycznych przez użytkownika,
- szybka, nieskomplikowana procedura poboru wzorców biometrycznych.

2. Wady:
- słabe zabezpieczenie przechowywanych wzorców biometrycznych.

4.5. Zalecenia implementacyjne

W powyższej implementacji zaleca się następujące rozwiązania praktyczne:
- Stosowanie konsekwentnej polityki administrowania systemem, zgodnie z którą:
  - zabrania się samodzielnego przeprowadzania procedury poboru wzorców przez użytkowników, tym samym zezwalając użytkownikowi na skanowanie linii papilarnych jedynie wtedy, gdy administrator uruchomi stosowną procedurę ze swojego konta,
  - regularnie analizowane są logi systemu biometrycznego,
  - stale monitorowany jest status użytkowników biometrycznych oraz niebiometrycznych,
  - ustawiane są jednolite parametry biometryczne dla każdego z użytkowników.
- Wykonywanie dodatkowych działań celem utrzymania spójności systemu:
  - tworzenie kopii bezpieczeństwa gałęzi rejestru gdzie zlokalizowane są wzorce biometryczne:

`KEY_LOCAL_MACHINE\Software\Identicator Technology\Biologon SecuritySystem\BioAccountManager\Database`.

- przeprowadzanie importu do rejestru systemu jedynie słusznych wartości określających parametr m.in. *Workstation policy*, przed uruchomieniem procedury poboru wzorców biometrycznych,
- uniemożliwienie bezpośredniej edycji rejestru systemowego na drodze wyłączenia możliwości uruchomienia aplikacji **Regedit.exe**; zaleca się stosowanie Edytora założeń systemowych (ang. *System policy editor*) pozwalającego administratorowi dostosować środowisko pracy użytkownika, w tym zabraniając mu uruchamiania narzędzi edycji rejestru.

Przedstawione powyżej rozwiązanie wymaga stosowania przytoczonych zaleceń, celem zmniejszenia zagrożeń wynikających z faktu, iż system biometryczny jest integrowany z systemem operacyjnym, którego mechanizmy nie zapewniają wymaganego poziomu bezpieczeństwa.

5. Charakterystyka rozwiązania firmy Veridicom

5.1. Warstwa sprzętowa

Badaniu poddano czytnik linii papilarnych Veridicom Finger Image Scanner 5th Sense skonstruowany przy wykorzystaniu półprzewodnikowego sensora FPS110, tworzącego obraz o rozdzielczości 500 dpi przy powierzchni skanowania 0,60″ × 0,60″. Czytnik ten, w przeciwieństwie do prezentowanego wcześniej, nie posiada wad skanerów optycznych, co przejawia się w braku zniekształceń powodowanych m.in. skomplikowanymi ścieżkami światła. Jako urządzenie półprzewodnikowe czytnik jest bardziej wytrzymały niż prezentowany DFR-200.

5.2. Warstwa programowa

W badaniach wykorzystano oprogramowanie Protector Suite w wersji 3.5. Protector Suite v.3.5 jest rozwiązaniem przeznaczonym dla środowisk opartych o systemy operacyjne firmy Microsoft, tzn.:

- MS Windows 95 OSR 2.1/98,
- MS Windows NT Workstation 4.0/2000.

Minimalne wymagania niezbędne do instalacji oraz użytkowania omawianego oprogramowania, obejmują:

- procesor: Pentium lub wyższy,
- pamięć RAM: 16 MB (Windows 9x), 32 MB (Windows NT),
- wolna przestrzeń dysku twardego: 4 MB,
- port równoległy: dostępny,
- karta graficzna: standard VGA lub o wyższej rozdzielczości,
- urządzenie wskazujące: mysz lub inne.

W skład pakietu Protector Suite v.3.5 wchodzą:

- Logon Protector (zabezpieczenie dostępu do komputera),

- File Disk Protector (szyfrowanie plików),
- Password Protector (zarządzanie hasłami),
- PKI Protector (szyfrowanie i podpisywanie dokumentów).

Oprogramowanie oferowane jest również w wersji Professional Net Edition przeznaczone dla sieci lokalnych oraz w wersji Professional Enterprise Edition, dla sieci rozległych w dużych przedsiębiorstwach. Podobnie jak firma Identicator Technology, Veridicom dostarcza biblioteki dla programistów (SDK). W badaniach wykorzystano wersję podstawową (implementacja jednostanowiskowa).

W przypadku rozwiązania firmy Veridicom oferowane są pakiety oprogramowania skierowane do określonych zastosowań, podobnie jak przypadku rozwiązania programowego firmy Identicator Technology. Różnice pojawiły się w zawartości pakietów podstawowych obu rozwiązań. Odpowiedniki komponentów podstawowych Protector Suite oferowane są już jako dodatkowe, w przypadku drugiego producenta.

5.3. Implementacja systemu biometrycznego

Analogicznie do pierwszego rozwiązania założono przeprowadzenie jednostanowiskowej (indywidualnej) implementacji systemu biometrycznego na stacji roboczej z systemem MS Windows 9x.

Instalacja sprzętu związana jest z podłączeniem czytnika: podłączenie wtyczki 25-pin SUB-D kabla do wolnego portu równoległego, podłączenie wtyczki kabla klawiaturowego do przejściówki mini-DIN6 oraz przejściówki do gniazda PS/2.

Instalacja oprogramowania biometrycznego jest realizowana przez administratora systemu. W trakcie inicjalizacji oprogramowania następuje wybór hasła administratora systemu biometrycznego oraz pobranie wzorca biometrycznego administratora. Po zakończonym etapie instalacji oprogramowania użytkownik pełniący funkcję administratora może zostać zidentyfikowany w systemie poprzez podanie hasła. W przeciwieństwie do rozwiązania firmy Identicator Technology tutaj nie występuje menu wyboru metody logowania. Możliwe jest: (a) logowanie użytkownika z uprawnieniami administratora albo (b) logowanie lokalne lub domenowe. Możliwość (a) stanowi rozwiązanie np. w sytuacji, gdy ulegnie uszkodzeniu czytnik biometryczny (wymagane jest jedynie hasło). Tutaj pojawia się kolejna różnica, w stosunku do rozwiązania pierwszego, gdzie możliwym było ustawienie logowania administratora wyłącznie poprzez czytnik biometryczny i w sytuacji awarii czytnika, logowanie administratora było niemożliwe.

Procedura poboru wzorca biometrycznego różni się od procedury w rozwiązaniu pierwszym. W przypadku rozwiązania pierwszego występowało podwójne skanowanie linii papilarnych, natomiast w przypadku rozwiązania drugiego, obraz linii papilarnych pobierany jest czterokrotnie. W obu rozwiązaniach istnieje możliwość rejestracji obrazu linii papilarnych więcej niż jednego palca, przy czym w przypadku rozwiązania firmy Identicator Technology, możliwym jest pozostawienie wzorców więcej niż trzech palców. Protector Suite oferuje możliwość importu próbki wzorca (pliki z rozszerzeniem *.enr). Możliwym jest wykreowanie (zdalne) przez użytkownika próbki biometrycznej oraz przesłanie jej do administratora, który w trakcie edycji właściwości

użytkownika jest w stanie zaimportować je do bazy. Rozwiązanie firmy Identicator Technology nie oferuje wspomnianych wyżej możliwości.

Podobnie jak w rozwiązaniu poprzednim, administrator może ustalić typ logowania (ang. *Verification type*): nazwa i hasło, nazwa i odcisk palca, nazwa i hasło i odcisk palca. Ponadto (co nie jest możliwe w przypadku Biologon Security System v.2.0) oprócz weryfikacji oferowana jest możliwość identyfikacji (odcisk palca, odcisk palca i hasło).

W przeciwieństwie do rozwiązania pierwszego, dane biometryczne przechowywane są w zaszyfrowanej, własnej bazie danych. Protector Suite oferuje możliwość ustalenia dla każdego z użytkowników, które informacje muszą zostać podane w trakcie logowania. Istnieją trzy poziomy przyporządkowania użytkowników [4]:

- ograniczony – wszystkie informacje przechowywane w bazie danych, brak możliwości zmiany hasła,
- normalny – nazwa użytkownika oraz domeny są przechowywane w bazie danych, istnieje możliwość zmiany hasła,
- uprzywilejowany – wymagane jest wpisanie wszystkich informacji; w przeciwieństwie do poprzednich poziomów, istnieje możliwość logowania na dowolne konto użytkownika.

Ponadto, istnieje możliwość utworzenia kopii zapasowej bazy danych użytkowników. W przypadku Biologon Security System występuje rozbudowa atrybutów konta użytkownika systemu operacyjnego w ramach wewnętrznej bazy kont użytkowników, natomiast w drugim rozwiązaniu, występuje powiązanie identyfikatora użytkownika w bazie systemu biometrycznego z kontem użytkownika w bazie systemu operacyjnego.

Oprogramowanie firmy Identicator Technology jest głęboko zaszyte w system operacyjny, a właściwości biometryczne użytkowników mogą być edytowane z poziomu (rozbudowanych) komponentów Panelu sterowania (np. Użytkownicy).

Rozwiązanie firmy Veridicom oferuje narzędzie do konfiguracji ustawień dostępne w formie oddzielnej aplikacji, a cały system biometryczny nie jest tak głęboko zaszyty w system operacyjny, jak w przypadku pierwszego rozwiązania. Narzędzie administracyjne prezentuje grupy funkcji, przy czym w przypadku użytkowników nie posiadających uprawnień administratora występuje odpowiednio ograniczona wersja tego narzędzia.

W przypadku Microsoft Windows 95/98, instalacja Biologon Security System podniosła bezpieczeństwo systemu na drodze wprowadzenia wybranych rozwiązań stosowanych w przypadku systemu(ów) Microsoft Windows NT, stało się tak również w przypadku Protector Suite. W obu rozwiązaniach występuje chroniony biometrycznie wygaszacz ekranu. Jedynie w przypadku rozwiązania firmy Veridicom, istnieje możliwość odblokowania stacji przez administratora.

W przypadku rozwiązania firmy Veridicom nie występuje ponadto ryzyko naruszenia integralności mechanizmu bezpieczeństwa związanego z identyfikacją użytkowników. Jedynie uprawnieni do tego celu administratorzy posiadają możliwość ustalenia właściwości mechanizmu bezpieczeństwa obowiązujące wszystkich użytkowników danej stacji roboczej.

5.4. Wady i zalety rozwiązania firmy Veridicom

Poniżej zostaną przedstawione silne oraz słabe strony zauważone w trakcie każdego z etapów: instalacji, uruchomienia, konfiguracji oraz użytkowania systemu.

Etap 1. Instalacja oprogramowania oraz sprzętu do identyfikacji biometrycznej.

1. Zalety:
   - szybki, nieskomplikowany proces instalacji, realizowany za pomocą kreatora,
   - wymagana niewielka ilości wolnego miejsca na twardym dysku.

2. Wady:
   - konieczność zapewnienia wolnego portu równoległego,
   - funkcjonowanie w środowiskach systemowych firmy Microsoft.

Etap 2. Uruchomienie systemu.

1. Zalety:
   - wskazówki odnośnie ułożenia palca na powierzchni skanera.

2. Wady:
   - brak możliwości przeprowadzenia testów diagnostycznych czytnika,
   - wydłużony czas oczekiwania na uruchomienie procedury logowania użytkownika do systemu, z uwagi na konieczność połączenia się z odpowiednimi komponentami systemu.

Etap 3. Konfiguracja i administracja systemem.

1. Zalety:
   - dodatkowy komponent centralizujący narzędzia konfiguracji systemu biometrycznego,
   - możliwość zapisu działań do logu,
   - możliwość ustalenia dla każdego z użytkowników z osobna sposobu logowania,
   - brak potencjalnego zagrożenia naruszenia spójności funkcjonowania systemu.

2. Wady:
   - brak.

Etap 4. Użytkowanie systemu.

1. Zalety:
   - szybki proces logowania,
   - możliwość stosowania więcej niż jednej metody uwierzytelniania,
   - implementacja wybranych elementów rozwiązań bezpieczeństwa zastosowanych w MS Windows NT,
   - możliwość przeprowadzenia procedury poboru wzorców biometrycznych przez użytkownika,
   - właściwe zabezpieczenie przechowywanych wzorców biometrycznych.

2. Wady:
   - relatywnie skomplikowana procedura poboru wzorców biometrycznych.

6. Wyniki analizy

Analiza przedstawionego rozwiązania firmy Identicator Technology oraz w odniesieniu do niego, rozwiązania firmy Veridicom pozwoliła na sformułowanie następujących wniosków:

- Z uwagi na niską odporność mechanizmu bezpieczeństwa odpowiedzialnego za składowanie wzorców biometrycznych, nie zaleca się stosowania rozwiązania firmy Identicator Technology w implementacjach jednostanowiskowych.
- Preferencje wykorzystania rozwiązania sprzętowo-programowego firmy Identicator Technology: implementacje wielostanowiskowe (w sieci o strukturze domeny).
- Z uwagi na wysoką odporność mechanizmu bezpieczeństwa odpowiedzialnego za składowanie wzorców biometrycznych, a także wysoką jakość sprzętu oraz rozwiązań programowych, zaleca się stosowanie rozwiązania firmy Veridicom w implementacjach jednostanowiskowych i/lub wielostanowiskowych.
- Preferencje wykorzystania rozwiązania sprzętowo-programowego firmy Veridicom: implementacje jednostanowiskowe, wielostanowiskowe (w sieci o strukturze grupy roboczej oraz domeny) i wielostanowiskowe rozproszone (w sieci o strukturze wielodomenowej).

Literatura

[1] Adrian Kapczyński: Ocena zastosowania wybranej metody biometrycznej w procesie autentykacji użytkowników, Studia Informatica, seria Informatyka nr 1(43) v. 22, Gliwice 2001.

[2] Techniki komputerowe 1/2000, Instytut Maszyn Matematycznych, Warszawa 2000.

[3] Techniki komputerowe 2/2000, Instytut Maszyn Matematycznych, Warszawa 2000.

[4] Veridicom Protector Suite v. 3.5 Manual.

[5] Identix Biologon v. 2.0 User's Guide.

JAN RYŻKO, JERZY SŁAWIŃSKI
INSTYTUT MASZYN MATEMATYCZNYCH WARSZAWA

Biometria – techniki, zastosowania, rynek w latach 2000-2001
Biometrics – technologies, applications, market in 2000-2001

Streszczenie

Przedstawiono sytuację na rynku biometrycznym w latach 2000-2001 zarówno pod kątem najczęściej stosowanych technik jak i wykorzystywanych aplikacji. Omówiono poszczególne techniki, najwięcej miejsca poświęcając liniom papilarnym. Określono tendencje jakie dominują w ostatnim okresie odnośnie stosowanych technik. Wymieniono główne firmy odgrywające istotną rolę na tym rynku i niektóre ich wyroby. Krótko scharakteryzowano też najnowsze tendencje wśród zastosowań.

Abstract

The situation on the biometric market in the years of 2000-2001 is shown both from the viewpoint of most frequently used technologies as well as applications. The particular technologies are described with special attention put on fingerprints. The last tendency about used technologies is pointed. The names of most importants companies and some of their products are mentioned. At the end the newest tendencies in applications are shown.

1. Rynek biometryczny ostatniej dekady

W ciągu ostatnich dziesięciu lat, a zwłaszcza ostatnich kilku lat obserwujemy znaczny wzrost liczby sprzedanych systemów i urządzeń biometrycznych. Według raportu IBIA (International Biometric Industry Association – Międzynarodowe Stowarzyszenie Przemysłu Biometrycznego [1]) w roku 1991 sprzedano około 1600 urządzeń biometrycznych, przy średniej ich cenie około 4400 dolarów. W roku 2001 przewiduje się sprzedaż ponad 400000 tych urządzeń, przy czym przeciętna cena obniżyła się do około 400 dolarów. Liczba wyrobów wzrastała w całym omawianym okresie, ze znacznym przyspieszeniem w ciągu ostatnich trzech lat, natomiast średnia cena spadała mniej równomiernie, wykazując nawet niewielki wzrost w roku 1996 i osłabienie tempa spadku w ostatnich latach. Średni roczny wzrost przychodów wyniósł 36% w omawianym okresie, a w ubiegłych trzech latach ponad 60%. Prognozy na lata następne ocenia autor tego raportu na 25-40% rocznie, co przyniosłoby 1,2 – 2,5 mld.

dolarów w roku 2010, choć inne źródła [2] określają ten raport jako „pesymistyczny". Oceny różnych analityków rynku różnią się znacznie. Według raportu Elsevier Advanced Technology [3] przychody rynku biometrycznego w 2000 roku miały wynieść (bez systemów AFIS) ponad 196 mln dolarów, a według cytowanego raportu IBIA – 170 mln w roku 2001. Mimo tych różnic, wszyscy mówią o znacznym wzroście tej dziedziny.

Jeśli chodzi o udział poszczególnych technik biometrycznych w rynku, to mamy na ten temat dane z ostatnich trzech lat ([3], [4]), oraz podobne dane z lat 1998-99 dla kontroli fizycznego dostępu [5]. Niewątpliwie największy udział ma technika rozpoznawania linii papilarnych, która w 2000 roku stanowiła już 50% rynku [3] wobec 34,7% w grudniu 1999, kiedy już miała większy udział aniżeli technika geometrii dłoni (31%) i 27% w roku 1998 [4]. Należy dodać, że w podziale z 1999 roku jako odrębna technika występowały systemy AFIS, stanowiące 4,4% rynku. Przewidywany jest dalszy wzrost udziału rozpoznawania linii papilarnych do 55% w roku 2004 [6]. Tendencję tę można tłumaczyć faktem, że w tej dziedzinie działa najwięcej firm biometrycznych i możliwe jest uzyskanie obniżenia kosztów całych systemów dzięki niewielkim wymiarom czytników. W dziedzinie kontroli dostępu [5] technika oparta na rozpoznawaniu geometrii dłoni była dominująca zarówno w 1998 jak i 1999 roku, choć udział jej spadł z 48,4% w 1998 do 42,2% w 1999 roku (przy wzroście udziału rozpoznawania linii papilarnych z 19,4% do 21,7% w tym samym okresie). W roku 2000 udział techniki rozpoznawania geometrii dłoni w całym rynku biometrycznym spadł do 15% [3] utrzymując drugą pozycję w tym rankingu. Przewidywania na rok 2004 [6] mówią o 10% udziale. Tutaj, odwrotnie niż w dziedzinie linii papilarnych, nie ma możliwości znacznego zmniejszenia wymiarów urządzeń i tylko nieliczne firmy działają na tym obszarze. Na trzecim miejscu, z 12% udziałem znalazła się w 2000 roku technika rozpoznawania twarzy, która uczyniła znaczne postępy zważywszy że udział ten wynosił tylko 3,9% w marcu 1998 i 7,1% w grudniu 1999 [4]. Również w kontroli fizycznego dostępu udział tej techniki wzrósł ponad 4-krotnie w latach 1998-99 (odpowiednio 2,3 i 15,1% [5]) Sukces ten spowodowany jest rozwojem tej techniki, w tym telewizji przemysłowej i nowych metod rozpoznawania.

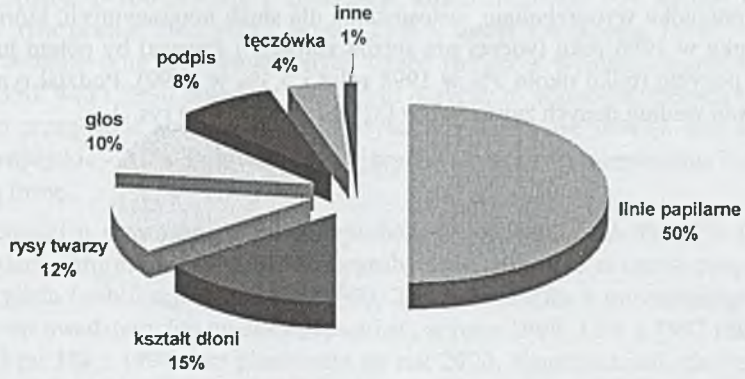
Natomiast udział techniki rozpoznawania głosu, a właściwie mówiącego, wykazuje tendencję spadkową. Według [4] zmniejszył się on z 25% w listopadzie 1996 roku do 15,8% w grudniu 1999 i 10% w roku 2000 [3]. W kontroli fizycznego dostępu udział w rynku zmalał z 28,6% w 1998 roku do 16,3% w 1999 [5]. Dzieje się tak dlatego, że dokładność rozpoznawania głosu ustępuje innym technikom. Prace w tej dziedzinie są jednak intensywnie prowadzone i prognozy na rok 2004 mówią o wzroście udziału techniki rozpoznawania głosu do 15% [6].

W ostatnim roku nastąpił wyraźny wzrost udziału techniki rozpoznawania podpisu z 2,7% w grudniu 1999 do 8% w 2000. Inne oceny [7] mówią nawet o 15% udziale tej techniki, co jednak wydaje się przesadą. Wpływ na to ma niewątpliwie przyjmowanie w różnych krajach ustaw o podpisie elektronicznym.

Ostatnią liczącą się techniką jest wykorzystanie do identyfikacji cech oka ludzkiego, przede wszystkim tęczówki. Udział techniki wykorzystującej rozpoznawanie oka wyniósł odpowiednio 3,7% w roku 1999 i 4% w roku 2000. W kontroli fizycznego dostępu udział rozpoznawania tęczówki wzrósł znacznie z 0,5% w roku 1998 do 4,25% w roku 1999. Natomiast udział rozwiązań wykorzystujących siatkówkę oka spadł w tym

samym okresie z 0,9 do 0,45%. Przyczyną tego są specjalne wymagania przy posługiwaniu się tą techniką i wysoka cena urządzeń.

Udział pozostałych, będących w opracowaniu, technik stanowił tylko 1% rynku w 2000 roku. Warto tu tylko zwrócić uwagę na aktywność firmy Net Nanny Software International, która rozpoczęła sprzedaż systemu opartego na technice wykorzystującej sposób uderzania w klawisze (czas przytrzymywania klawiszy i odstępów między uderzeniami), który ma szansę na sukces rynkowy [3]. Udział poszczególnych technik w rynku biometrycznym 2000 roku pokazany jest na rys. 1.

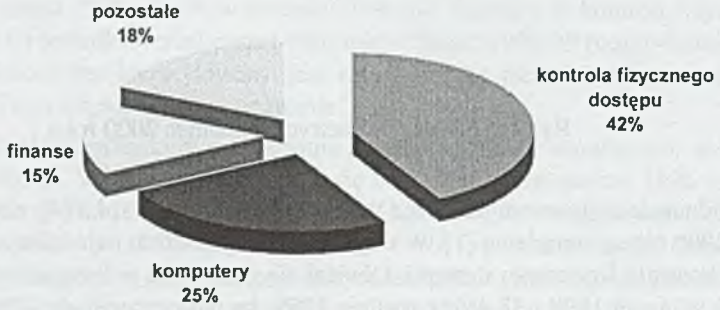


Rys 1. Techniki biometryczne, koniec 2000 roku

Odnośnie zastosowań jest nieco więcej danych od 1996 roku [4], choć informacje z roku 2000 nie są kompletne [3]. W ciągu całego tego okresu największy udział w rynku miała kontrola fizycznego dostępu. Obniżał się on z 63% w listopadzie 1996 roku do 52,8% w marcu 1998 i 38,4% w grudniu 1999, by nieco wzróść do 42% w 2000 roku. Udział ten obejmuje również rejestrację czasu pracy, która w roku 1999 stanowiło około 1/3 całej kontroli dostępu [5]. Na drugim miejscu, z 25% udziałem, znalazły się w 2000 roku szeroko pojęte zastosowania komputerowe [3], podczas gdy w ubiegłych latach bezpieczeństwo komputerów (3,8% w roku 1999) i telekomunikacja (2,8% w tym samym roku) stanowiły niespełna 7% i udział ten nie zmieniał się znacznie od 1996 roku [4]. Na trzecim miejscu, z 15% udziałem, plasuje przegląd [3] zastosowania w finansach, które według [4] w 1999 roku zajmowały tę samą pozycję z nieco większym (17%) udziałem po zastosowaniach w dziedzinie prawa i porządku (19,2%). Udział zastosowań w finansach ciągle rósł w omawianym okresie od około 4,5% w 1996 roku, kiedy zajmował ostatnie miejsce wśród 6 wymienianych tam zastosowań. Dalszy rozwój

tych zastosowań potwierdzają ostatnie doniesienia [8] o ponad 3-krotnym wzroście sprzedaży kiosków, biometrycznie umożliwiających operacje finansowe w roku 2000.

Dane dotyczące pozostałych zastosowań dostępne są jedynie do 1999 roku. Szczegółowe informacje dotyczące roku 2000 można znaleźć w raportach takich jak The Biometric Industry Report (cena 1280 dolarów) lub Biometric Directory (260 dolarów na CD). Jak wspomniano, drugie miejsce wśród zastosowań w roku 1999 zajmowało prawo i porządek obejmujące takie dziedziny jak zastosowania w sądownictwie, więziennictwie, a także w różnego rodzaju dokumentach identyfikujących. Taką samą pozycję, z ponad 12% udziałem, zajmowało to zastosowanie w listopadzie 1996 roku, natomiast na początku 1998 roku nastąpił szybki wzrost zastosowań w służbie zdrowia i opiece społecznej, kiedy one, z około 15% udziałem zajmowały drugie miejsce, by spaść na 4 pozycję (po kontroli fizycznego dostępu, prawie i porządku oraz finansach) w końcu 1999 roku z niewiele zmienionym udziałem. Sama służba zdrowia stanowiła wówczas 9,6% rynku, a ubezpieczenia społeczne 3,9% Z zastosowań w dziedzinie prawa i porządku wyodrębniono zastosowania dla służb imigracyjnych, które stanowiły 6,5% rynku w 1996 roku (więcej niż służba zdrowia i finanse) by potem już spaść na ostatnią pozycję (tylko około 3% w 1998 roku i 5,3% w 1999). Podział rynku według zastosowań według danych zawartych w [3] pokazany jest na rys. 2.



Rys 2. Zastosowania biometrii, koniec 2000 roku
(wg. Biometric Technology Today, styczeń 2001)

Pomimo wspomnianego wysokiego tempa rozwoju sprzedaży wyrobów biometrycznych, kondycja ekonomiczna poszczególnych firm tej branży nie jest najlepsza. Większość z nich przynosi straty, a tylko nieliczne niewielkie zyski. Tłumaczy się to

wysokim stopniem czynionych inwestycji i ogólną stagnacją ekonomiczną, ale ostatnio pojawiły się przykłady znanych firm biometrycznych jak Veridicom [9] i Saflink [10] zagrożonych bankructwem.

W dalszym ciągu dokonany zostanie krótki przegląd najbardziej rozwiniętych technik biometrycznych.

2. Wykorzystanie linii papilarnych

Technice tej poświęcone będzie najwięcej miejsca zarówno dlatego, że jest to dominująca technika rynku biometrycznego, jak i obiekt naszego głównego zainteresowania.

Postęp w tej dziedzinie możemy zaobserwować porównując dwa przeglądy tej techniki opracowane w marcu 1999 roku [11] i w maju 2001 roku [12]. Pierwszy z nich podaje informacje o 100 firmach z 20 krajów, które oferowały 164 wyroby (62% to systemy, w tym prawie 10% AFIS, ponad 23% - sprzęt i niespełna 15% - oprogramowanie). Średnie ceny dla wymienionych trzech rodzajów wyrobów wynosiły odpowiednio: 9350, 440 i 2990 dolarów, przy czym dotyczy to wyrobów, których ceny zostały w tym przeglądzie podane. Firmy amerykańskie stanowiły 56% (w tym z USA – 52%), a europejskie – 31%. Połowa występujących tu krajów reprezentowana była przez tylko jedną firmę.

Jeśli chodzi o czas wprowadzenia wyrobów do sprzedaży, to dla 35% firm, dla których podano informację na ten temat, wyroby były osiągalne w czasie przygotowywania przeglądu (publikacja – marzec 1999); 25% pochodziło z poprzedniego (1998) roku; 24% wprowadzono, lub miano wprowadzić, w roku 1999; 11% z 1997 roku, 3% z 1996 roku i po 1% z 1994 oraz planowano na rok 2000. Natomiast jeśli chodzi o ilość wyrobów oferowanych przez poszczególne firmy to ponad 30% firm przedstawiało tylko jeden wyrób, prawie 13% – dwa wyroby, prawie 7% nie oferowało konkretnych wyrobów, a prawie 4% – trzy wyroby. Najwięcej wyrobów przedstawiły firmy Printrak (10) i Sagem Morpho (7). Pierwsza z nich, obecnie nabyta przez Motorolę, to znany dostawca systemów AFIS i cywilnych systemów identyfikacyjnych. Oferowane wyroby obejmowały systemy i oprogramowanie dla wszystkich etapów identyfikacji: skanowania, przechowywania, przeszukiwania, porównywania... Druga natomiast to wywodząca się z francuskiej firmy Morpho organizacja o podobnym do Printraka profilu, która oferowała również sprzęt i oprogramowanie do weryfikacji. Warto tu przypomnieć, że w przeprowadzonym we wrześniu 2000 roku konkursie FVC2000 weryfikacji linii papilarnych dwa pierwsze miejsca zajęły algorytmy firmy Sagem, dla których testy wykazały współczynniki równego błędu (EER) co najmniej dwukrotnie niższe niż dla innych zgłoszonych algorytmów.

Przeprowadzony ponad 2 lata później przegląd [12] wykazał większą konsolidację tej techniki biometrycznej. Obejmował on już tylko 79 firm (spadek o ponad 20%) z 21 krajów, z których 58% istniało pod tą samą nazwą w poprzednim przeglądzie, nieco ponad 30% to firmy nowe, a reszta to całkowita lub częściowa zmiana nazwy, łączenie się firm lub nabycie przez inną firmę. Udział firm amerykańskich spadł poniżej 50% (firm USA było 45,6%), a firm europejskich wzrósł do 38%. Polskę w obu przeglądach reprezentowała tylko firma Optel z Wrocławia oferująca ultradźwiękowy ekran dotykowy za 400 dolarów. Zwiększyła się natomiast o ponad 54% liczba oferowanych

wyrobów (do 253). Proporcje wśród rodzajów wyrobów nie uległy większej zmianie. Zmniejszył się udział systemów (50%) na rzecz sprzętu (32%), przy czym znacznie mniej było systemów AFIS (tylko 2%). W ofercie znalazły się też usługi (1,6%).

Jeśli chodzi o średnie ceny to tylko w dziedzinie oprogramowania nastąpił wyraźny spadek i to prawie 6-krotny. Natomiast wśród systemów, jeśli nie uwzględnić AFIS, spadek wyniósł około 33%. Uwzględnienie bardzo drogiego (milion dolarów) systemu Pequi AFIS firmy Griaule powoduje prawie 4-krotny wzrost tej ceny w stosunku do przeglądu z roku 1999. Również w sprzęcie, jeśli nie uwzględnimy dwóch drogich skanerów firmy Papillon Systems z 1992 roku, które nie występowały w przeglądzie z 1999 roku, spadek był ponad 3-krotny. Natomiast średnia cena określona dla wszystkich wyrobów sprzętowych była ponad 2-krotnie wyższa niż w 1999.

Co trzeci wyrób występujący w przeglądzie z roku 1999 pojawił się w przeglądzie z roku 2001, przy czym tylko w 13 przypadkach podane były ceny w obu przeglądach. Z tego dla 9 przypadków (69%) ceny nie zmieniły się, a w pozostałych obniżka wynosiła od 35 do 60%, przy czym w jednym wypadku wiązało to się z zakupieniem co najmniej 500 sztuk.

Przegląd z roku 2001 uwzględniał więcej wyrobów z poprzednich lat w związku z tym mniejszy był udział wyrobów aktualnie dostępnych i wyprodukowanych lub planowanych na rok 2001 (po 23%), 19% było wyrobów z poprzedniego (2000) roku, 16% sprzed 2 lat, 9% sprzed 3 lat, po 2% sprzed 4 lub 5, po 1% sprzed 6 lub 7 i 5% sprzed 9 lat.

Zmienili się też liderzy oferujący najwięcej wyrobów. Na pierwsze miejsce z 14 wyrobami wysunęła się tym razem firma Identix. Były to zarówno systemy do skanowania linii papilarnych na żywo, czytniki, jak i systemy do logowania się do komputerów i sieci. Na drugim miejscu z 12 wyrobami znalazła się firma Digital Persona z różnymi odmianami swojego systemu U.are.U. W większości dotyczyło to oprogramowania. Trzecią była nowa koreańska firma Domy & Co z 11 wyrobami w większości sprzętowymi. Dopiero na czwartym miejscu z 8 wyrobami, w większości tymi samymi co przed dwoma laty, reprezentowana była firma Sagem/Sagem Morpho.

Podsumowując rozwój techniki linii papilarnych warto zwrócić uwagę, że większość stosowanych obecnie czytników to rozwiązania sensorowe, najczęściej pojemnościowe, choć firma Atmel Grenoble (dawniej Thomson CSF Semiconductors) wytwarza nadal sensory cieplne podkreślając, że nie ma tu problemów przepięć elektrostatycznych. W przeglądzie ośmiu firm wytwarzających sensory ([13]: AuthenTec, Fingerprint Cards, Who?Vision – obecnie Ethentica, Infineon, Sony, STMicroeelectronics, Atmel i Veridicom) typ pojemnościowy reprezentowało 75% dostawców. Zbliżone rozwiązanie (oparte na polu elektrycznym) oferował Authentec, który oddzielił się od działającej dawniej w tej dziedzinie firmy Harris, a którego wyroby uchodzą za jedne z najlepszych na rynku. Firma ta sprzedała w IV kwartale 2000 roku 50000 sensorów i przewidywała dalszy wzrost sprzedaży w roku 2001. Uzyskała też znaczące fundusze (rzędu 20 milionów dolarów od swych inwestorów, głównie od Texas Instruments.

Ze względów bezpieczeństwa niechętnie przesyła się wzorce linii papilarnych z bazy danych, lecz umożliwia się użytkownikowi by przechowywał swój wzorzec np. na karcie inteligentnej. Jeszcze korzystniej byłoby przeprowadzać proces porównania na tej karcie. Takie rozwiązania zademonstrowały szwedzkie firmy Precise Biometrics,

Miotec i iD2 Technologies [14]. O podobnych rozwiązaniach donosiły też Fingerprints Cards i Veridicom. Natomiast w [15] opisano rozwiązanie niemieckiej firmy Novacard, która na zlecenie holenderskiej firmy ubezpieczeniowej Zorg en Zekerheid opracowała karty inteligentne z wbudowanym w nie sensorem dla pacjentów z chorobą Parkinsona, którzy nie mogą wprowadzać swojego PINu. Zastosowano tu sensor firmy Infineon i karta jest z jednej strony grubsza (1,2 mm) od standardowej (0,81 mm), ale w przyszłości przewiduje się opracowanie sensora o grubości 0,4-0,5 mm, który zmieści się w zwykłej karcie. Cenę takiej karty oszacowano wstępnie na 50 dolarów.

Pod koniec 2000 roku doniesiono [16] o umowie pomiędzy szwedzką firmą Fingerprint Cards i amerykańskim dostawcą Biometric Associates na opracowanie standardowej karty z sensorem w 2001 roku w cenie poniżej 20 dolarów. Fingerprint Cards zamierzała opracować sensor o grubości 0,2 mm, który będzie bardziej elastyczny od dotychczasowych.

Ocenia się [17], że ceny sensorów spadną poniżej 10 dolarów w 2002 roku w porównaniu z 20-30 dolarów, na jakie szacowano je w kwietniu 2001. Fingerprint Cards mówi o możliwości sprzedaży przesuwnego sensora na płytce z elastycznym kablem za 5-6 dolarów [12].

Na rys. 3 pokazano opracowany i aktualnie wdrażany do sprzedaży w IMM nowy czytnik linii papilarnych IMMSkan 200M oparty na sensorze AF-S2 firmy AuthenTec. Czytniki IMMSkan dostosowane są do interfejsu Wieganda, dzięki temu mogą współpracować z dowolnym systemem kontroli dostępu. Współpracują one z oprogramowaniem kontroli dostępu i rejestracji czasu pracy XChronos, które jest oferowane zarówno w wersji jednostanowiskowej jak i sieciowej. Posiadają ponadto możliwość wbudowania głowicy zbliżeniowej, dzięki czemu w miejsce klawiszy można użyć karty do wprowadzenia PINkodu. Warunkiem akceptacji jest wówczas uprawniona karta i weryfikacja osoby.

Rys 3. Czytnik IMMSkan 200M

3. Systemy pomiaru ręki

Jak wspomniano, rozpoznawanie za pomocą pomiaru ręki zdominowane było przez pomiar geometrii dłoni, co stanowiło najbardziej popularną techniką biometryczną jeszcze w 1998 roku, zwłaszcza w systemach kontroli fizycznego dostępu. Przegląd [18] z połowy 1999 roku wymienia 10 firm oferujących swe wyroby na rynku i 14 instytucji opracowujących takie systemy. Największa z nich to Recognition Systems, która do tego czasu sprzedała 27000 swych czytników. Oprócz geometrii dłoni brane są również pod uwagę odciski dłoni, które wprowadzono do standardu ANSI/NIST oraz rozpoznawanie układu żył, gdzie pewne sukcesy mają koreańska firma BK i brytyjska Neusciences, choć ta ostatnia nie miała jeszcze gotowego wyrobu.

Technika geometrii dłoni cieszy się akceptacją użytkowników i znajduje zastosowanie w systemach kontroli dostępu i rejestracji czasu pracy, służbach imigracyjnych, zwłaszcza na lotniskach, a także w systemach płatniczych (banki i świadczenia społeczne). Czytniki tej techniki są dosyć łatwe w użyciu i zapewniają dostateczną dokładność, ale są dosyć duże, ciężkie i raczej drogie. Według ostatniego przeglądu tej techniki [19] dochód uzyskany ze sprzedaży tych systemów wyniósł 29 milionów dolarów w 2000 roku. Z firm, które wycofują się z tej dziedziny wymienione są rosyjska Papillon i węgierska DermoGroup. Amerykańska firma Micro Identification Systems, która opracowała urządzenie FingerPass, oparte na geometrii pojedynczego palca, przerwała działalność w końcu 2000 roku. Również firmy opracowujące nowe rozwiązania, takie jak Talos Technology w USA i Axxess Identification w Wielkiej Brytanii zawiesiły działalność w tym zakresie. Recognition Systems miała już wtedy 35000 instalacji, a sprzedaż wzrosła w 2000 roku o 50%. Przegląd ten podaje dane o 15 firmach działających nadal w dziedzinie rozpoznawania ręki, mniej więcej po połowie w USA i Europie.

4. Rozpoznawanie twarzy

Zajmująca obecnie trzecie miejsce technika rozpoznawania twarzy ma lepsze perspektywy rozwoju od techniki pomiaru ręki. Przegląd tej techniki z października 1999 roku [20] zestawia 17 firm oferujących 34 wyroby, oraz 14 instytucji, które opracowują 11 nowych wyrobów. Najwięcej (7) wyrobów prezentowała firma Miros (obecnie eTrue). Były to różne systemy i oprogramowanie szeregu TrueFace. Na drugim miejscu znalazła się z 6 wyrobami firma Visionics Corporation, która przedstawiała bardzo popularną serię FaceIt, wykorzystywaną przez brytyjską policję do walki z przestępczością i huligaństwem w Londynie i Birmingham. W USA wprowadzenie tego systemu natrafiło na ostry sprzeciw organizacji liberalnych [21]. Trzecie miejsce z 4 wyrobami zajęła firma Viisage. Większość opracowywanych nowych wyrobów miała się pojawić w sprzedaży w 2000 roku. Średnia cena systemów rozpoznawania twarzy była rzędu 3700 dolarów, a wyrobów oprogramowania, nie uwzględniając drogich baz danych – 1350 dolarów.

Na początku 2001 roku [22] Międzynarodowa Organizacja Lotnictwa Cywilnego przyjęła rozpoznawanie twarzy jako najbardziej prawdopodobną technikę biometryczną, która w kombinacji z maszynowym odczytem dokumentów podróży zapewni automatyczną identyfikację pasażerów.

Technika ta jest również powszechnie stosowana w bankowości. Firma Inno Ventry, dostawca urządzeń do realizacji czeków, twierdzi, że jest największym handlowym użytkownikiem biometrii na świecie [23]. Od stycznia do października 2000 roku liczba transakcji realizacji czeków przy pomocy RPM (Rapid Pay Machines – szybkie urządzenia wypłacające) wzrosła 3,5 raza.

Ponadto rozpoznawanie twarzy wykorzystuje się do ochrony różnych klubów i kasyn [24].

5. Rozpoznawanie za pomocą głosu

Czwartą techniką w roku 2000 była metoda weryfikacji mówiącego poprzez rozpoznawanie jego głosu, która była jedną z najwcześniej wprowadzanych metodologii biometrycznych, cieszącą się znaczną akceptacją użytkowników. Ponadto technika ta mogłaby być realizowana w różnych zastosowaniach telefonicznych. Jednakże nie najlepsze wyniki rozpoznawania głosu, związane ze stanem mówiącego (np. choroba) i jakością wykorzystywanego sprzętu, obniżały w ostatnich latach udział tych rozwiązań na rynku. Jednakże liczba firm zaangażowanych w tę technikę była dosyć znaczna.

Pierwszy przegląd z maja 1999 roku [25] podaje 27 nazw firm oferujących swe wyroby na rynku i 7 dalszych, opracowujących nowe wyroby. 62% tych firm pochodziło z USA, a 32% z Europy (w tym 18% z Wielkiej Brytanii). Tanie oprogramowanie dostarczały amerykańskie firmy Veritel i T-Netix, natomiast w sprzęcie dominowały belgijska Keyware i Sensory z USA. Wzorce dla tej techniki mogły być również przechowywane na kartach inteligentnych i w tym zakresie działają takie firmy jak brytyjska Domain Dynamics i amerykańskie Graphco Technologies i VeriVoice.

Przeprowadzony w niespełna rok drugi przegląd [26] obejmował tyle samo firm, z których 74% pozostało sprzed roku. Zwrócono tu uwagę na powiązanie rozpoznawania mowy i weryfikację mówiącego. Osiągnięcia w tej pierwszej dziedzinie wykorzystano do rozwoju tej drugiej. Przodowały w tym takie firmy jak nowopowstała irlandzka Buytel, której wyrób VoiceVault nie wymaga inwestycji sprzętowych i oferuje weryfikację za 0,1-0,2 dolara, czy Nuance z USA. Podobne podejście reprezentował europejski projekt Picasso, mający na celu opracowanie usług bezpiecznych transakcji telefonicznych poprzez identyfikację głosu klienta. Również banki w Belgii, Południowej Afryce i Australii prowadziły próby wdrożenia tej techniki do swej działalności. Podano tu też przykłady nowych zastosowań weryfikacji mówiącego w kontroli dostępu i rejestracji czasu pracy.

Ostatni przegląd [27] z lata 2001 roku podaje dane 40 firm zajmujących się tą techniką (wzrost o 18% w stosunku do przeglądu [26]), z których 55% występowało w tym ostatnim przeglądzie. Świadczy to o wzroście zainteresowania tą metodologią, a niektóre z prognoz mówią o 75% rocznym tempie wzrostu i wartości przychodów 270 milionów dolarów w 2004 roku. Do tego czasu przewiduje się, że 70 nowych, bezprzewodowych telefonów i 80% ręcznych komputerów będzie miało połączenia internetowe poprzez tzw. sieć głosową, której pierwszymi realizacjami są portale głosowe, ale zastosowania te przenoszą się do przedsiębiorstw. Największym rynkiem dla weryfikacji mówiącego jest wymiar sprawiedliwości w sprawach karnych, a w ramach tego nadzór nad warunkowo zwolnionymi.

6. Weryfikacja przez rozpoznawanie podpisu

Jest to, podobnie jak w przypadku głosu, metoda behawioralna i jeszcze bardziej akceptowalna przez użytkowników, gdyż stosowana była od bardzo dawna. Biometryczna weryfikacja uwzględnia jednak nie tylko wygląd podpisu, ale także dynamikę jego składania, a więc takie elementy jak szybkość zapisu poszczególnych fragmentów, nacisk wywierany na narzędzie piszące, czy nawet kąt nachylenia tego narzędzia do płaszczyzny podpisu. Specjalne pióra umożliwiają pomiar tych parametrów. Inną realizacją weryfikacji podpisu jest jego zamiana na postać cyfrową uzyskiwana w odpowiednich urządzeniach (ang. tablets), których cena spadła z 300 do poniżej 100 dolarów. Uzyskujemy wówczas tak popularny ostatnio podpis elektroniczny, posiadający już status prawny w USA i Unii Europejskiej i bliski uzyskania go również u nas. Trzecie rozwiązanie weryfikacji przez rozpoznawanie podpisu jest sprzętowo niezależne, zwykle programowe. Natomiast wśród zastosowań należałoby wymienić zarządzanie przepływem dokumentów, obliczanie z wprowadzaniem danych przy pomocy pióra i handel elektroniczny.

Przegląd z maja 1999 roku [28] wymienia 14 firm oferujących wyroby związane z rozpoznawaniem podpisu na rynku (w tym Politechnikę Szczecińską) i 10 opracowujących nowe systemy, przy czym firmy europejskie stanowiły 48%, a z USA tylko 39%. Wyroby do cyfrowego podpisu dokumentów oferowały firma CyberSign z USA i brytyjska PenOp. Tanie (rzędu 30 dolarów) oprogramowanie szyfrujące do komputerów ręcznych polecała firma Quintet. Zamiast piór niemiecka firma Hesy oferowała podkładki wrażliwe na nacisk do laptopów i urządzeń kasowych. Szyfrowanie jest istotne dla handlu elektronicznego. Firmy biometryczne współpracują tu z organizacjami wydającymi certyfikaty i dostawcami PKI (Public Key Infrastructure – infrastruktura klucza publicznego) dla ustalenia bezpiecznego dostępu do dokumentów, np. Acrobat firmy Adobe przez firmę Communication Inteligence (CIC) z USA.

Drugi przegląd [29] sporządzony niespełna rok później podawał tylko 17 firm, z których 16 występowało w poprzednim przeglądzie. Donosił on o znacznym ożywieniu na rynku rozpoznawania podpisu podając jako przykład 40 milionach podpisów zamienionych do postaci elektronicznej w samej tylko firmie PenOp w 1999 roku, co oznacza ponad 4-krotny wzrost w stosunku do roku poprzedniego. Rozwinęło się bardzo oprogramowanie z tego zakresu jak Easy DSM, Pocket Form i inne. Oprogramowanie to wykorzystywane jest przez wielkie firmy ubezpieczeniowe (na przykład Prudential Singapore), a także do uzyskiwania na bieżąco żądanych informacji. Przede wszystkim jednakże, technika ta służy do zabezpieczenia przesyłanych dokumentów prawnych, medycznych, farmaceutycznych. W związku z ogromnym rozwojem komputerów ręcznych (ponad 5 milionów do końca 1999 roku, a prognozy mówią o prawie 19 mln do 2003) rozwiązania rozpoznawania podpisu są oferowane do tych urządzeń jak również do nowych telefonów komórkowych.

7. Rozpoznawanie tęczówki

Ostatnią liczącą się na rynku biometrycznym techniką jest skanowanie tęczówki oka. Charakteryzuje się ona wysoką dokładnością, co prowadzi do korzystnych parametrów użytkowych systemów, dzięki dużej ilości punktów charakterystycznych tego organu przy dużej trwałości w czasie. Czytniki związane z tą metodologią są jednak

raczej drogie w porównaniu z innymi technikami i po szybkim wzroście w 1999 roku, kiedy na przykład w kontroli fizycznego dostępu udział tej techniki wzrósł 8,5 razy w stosunku do roku 1998, rok 2000 nie przyniósł już tak znaczącego wzrostu. Na początku 2000 roku [30] odnotowano właśnie to wyodrębnienie się techniki rozpoznawania tęczówki spośród grupy metodologii będących na etapie opracowywania i wówczas wiodącą firmą, posiadającą wiele patentów w tej dziedzinie była IriScan, która oferowała licencje takim partnerom jak Sensar, OKI, LG Electronics, Spring Technologies i CitX. W tym okresie ceny wyrobów tej techniki spadły z 10000 dolarów do kilku tysięcy, a nawet poniżej tysiąca. W drugiej połowie 2000 roku Iriscan i Sensar połączyły się [31] tworząc Iridian Technologies [32], która stała się głównym dostawcą wyrobów tej techniki obejmujących również serwery do ich integracji z sieciami komputerowymi przedsiębiorstw [33]. Technikę tę wykorzystuje wiele innych firm. Przykładem może tu być podpisana ostatnio umowa pomiędzy EyeTicket i Unisys, które to firmy procesowały się o wykorzystywanie patentów, a obecnie nawiązały współpracę [34].

Kiedy mówimy o technikach związanych z okiem, nie sposób nie wspomnieć o rozwiązaniach opartych na rozpoznawaniu naczyń krwionośnych siatkówki, która to technika była nawet wcześniej rozwinięta niż rozpoznawanie tęczówki, ale ze względu na konieczność specjalnego ustawiania użytkownika w stosunku do czytnika i niebezpieczeństwa uszkodzenia oka, nie rozwinęła się szerzej. Ostatnio jednakże [35] pojawiły się doniesienia o opracowaniu nowych urządzeń w tej dziedzinie, które mogą okazać się konkurencyjne.

8. Ostatnie tendencje w zastosowaniach

Aby zorientować się, o jakich zastosowaniach najczęściej donoszono w 2001 roku, zestawiono wiadomości na ten temat w dostępnej prasie biometrycznej. Okazało się, że prawie 25% wszystkich doniesień (oparto się na BTT od stycznia do września) dotyczyło zabezpieczeń komputerów i sieci, co potwierdzałoby omówione wcześniej wyniki za rok 2000. Spadek cen systemów biometrycznych i wciąż znaczne koszty zarządzania hasłami powodują [36], iż nawet przy zahamowaniu rozwoju przemysłu komputerowego, jego część zajmująca się zabezpieczeniem rozwija się w szybkim tempie.

Na drugim miejscu (22%) znalazło się zastosowania w dziedzinie prawa i porządku, co nie musi oczywiście określać udziału tego zastosowania w rynku biometrycznym, ale wciąż dużo pisze się o wykorzystaniu rozpoznawania twarzy przy pomocy systemu FaceIt firmy Visionics i telewizji przemysłowej. Po sukcesach w Londynie i Birmingham, wprowadzanie tego rozwiązania w Tampa na Florydzie [37] napotkało na sprzeciw obrońców prywatności. Dużo miejsca poświęca się też przenośnym urządzeniom wykorzystywanym do identyfikacji przestępców, jak system IBIS tej samej firmy Visionics [38]. Wiele informacji dotyczyło imigracji [39], a szczególnie systemów instalowanych na wielkich lotniskach światowych, najwięcej w USA, ale również w Wielkiej Brytanii, Izraelu, Malezji, a nawet Islandii. Często są to inicjatywy międzynarodowych organizacji lotniczych. Wykorzystywane są tu różne techniki od linii papilarnych, poprzez rozpoznawanie tęczówki do kształtu dłoni. Cytowany przegląd zestawia 27 systemów imigracyjnych w 15 krajach i podaje kontakt do 17 firm zajmujących się tym zastosowaniem.

W dalszej kolejności idą zastosowania w dziedzinie finansów (ponad 15%), co znowu zgodne jest z wynikami 2000 roku i kontrola dostępu (niespełna 15%). Mały udział tego ostatniego zastosowania można tłumaczyć tym, że są to rozwiązania masowe, od dawna wykorzystywane i rzadko się o nich pisze mimo prawdopodobnie nadal największego udziału w rynku. Natomiast zastosowania w służbie zdrowia (ponad 10%) wydają się rzeczywiście rosnąć ostatnio po pewnym okresie stagnacji. Przykładem tego może być zabezpieczenie techniką rozpoznawania linii papilarnych sieci amerykańskich instytucji tej służby [40].

Wśród zastosowań, którym nie poświęcono może zbyt dużo miejsca, ale które warto śledzić znajdują się: handel (zwłaszcza elektroniczny [41]), a także specyficzne działy kontroli dostępu jak ochrona kasyn [42] i szkół [43]. Należałoby też wspomnieć o zainteresowaniach biometrią wojska. Pentagon powołał laboratorium testujące [44], które ma sprawdzić 600 wyrobów pod kątem ich wykorzystania dla armii USA.

Jako ciekawostki można wspomnieć wprowadzanie systemów biometrycznych w restauracjach [45], pałacach prezydenckich [46] i w uczelniach dla potwierdzenia tożsamości egzaminowanych [47].

9. Podsumowanie

Wykorzystywanie biometrii staje się coraz bardziej powszechne, a poprawa parametrów i obniżka cen systemów i urządzeń biometrycznych umożliwiają stosowanie ich w coraz to nowych dziedzinach. Dlatego mimo osłabienia tempa rozwoju gospodarczego, co dotyczy również przemysłu komputerowego, kondycja młodego przemysłu biometrycznego wydaje się zupełnie niezła, co potwierdza dwukrotny wzrost sprzedaży w 2000 roku. Nie wszyscy użytkownicy dają się łatwo przekonać do powszechnego stosowania nowych metod, ale stopniowo zyskują one sobie uznanie. Większość firm biometrycznych wykazuje raczej straty niż zysk, ale nawet te zagrożone upadkiem jakoś wybrnęły z kryzysu i działają nadal. Dlatego wydaje się, że jest to dziedzina mająca perspektywy rozwoju.

Literatura

[1] IBIA Biometric Advocacy Report vol. III, no. 7, 20 IV 2001.

[2] IBIA releases pessimistic biometric market figures, Biometric Technology Today (BTT), maj 2001, str. 2.

[3] Survey: 2000 Market Review, BTT, styczeń 2001, str. 9.

[4] Survey: 1999 Market Review, BTT, grudzień 1999 / styczeń 2000, str. 8.

[5] Survey: Physical access control, BTT, wrzesień 1999, str.8.

[6] Biometric Digest, maj 2001, ramka na str. 5.

[7] National Post Business, lipiec 2001.

[8] Real-Time Kiosks & SAFLINK Bring Biometrics to the Credit Union Industry, Biometric Digest, luty 2001, str.1.

[9] Veridicom faces imminent closure, BTT, marzec 2001, str.1.

[10] Saflink warns of company closure, BTT, maj 2001, str. 1.

[11] Survey: Finger technologies point way adead, BTT, marzec 1999, str. 8.

[12] Survey: Taking stock of the fingerprint market, BTT, maj 2001, str. 7.

[13] Survey: Silicon fingerprint sensors, BTT, maj 2000, str. 8.

[14] Smartcard chipd ready for fingerprint matching, BTT, czerwiec 2000, str. 5.

[15] Parkinson's disease amart card project ready to roll out, BTT, lipiec – sierpień 2000, str. 3.

[16] Sensor-on-card deal is struck by Fingerprint Cards, BTT, listopad – grudzień 2000, str. 3.

[17] Chip sensor prices to plunge by 2002, BTT, kwiecień 2001, str. 1.

[18] Survey: Hand measuring systems, BTT, lipiec – sierpień 1999, str. 9.

[19] Survey: Hand measuring systems, BTT, kwiecień 2001, str. 9.

[20] Survey: Face recognition, BTT, październik 1999, str. 8.

[21] Visionics wins controversial order, BTT, lipiec – sierpień 2001, str. 1.

[22] Face recognition chosen for travel, BTT, luty 2001, str. 1.

[23] Innovation at Inno Ventry using facial recognition, j. w., str. 7.

[24] World's biggest casino bets on Viisage technology, BTT, marzec 2000, str. 5.

[25] Survey: Speaker Verification, BTT, maj 1999, str. 9.

[26] Survey: Speaker Verification, BTT, marzec 2000, str. 8.

[27] Survey: Speaker Verification, BTT, lipiec – sierpień 2001, str. 9.

[28] Survey: Signature Verification Technologies, BTT, maj 1999, str. 7.

[29] Survey: Signature Verification Technologies, BTT, kwiecień 2000, str. 8.

[30] Iris gains market recognition, BTT, luty2000, str. 9.

[31] Iriscan and Sensar find synergies in merger, BTT, wrzesień 2000, str. 2.

[32] News in brief: Iris recognition technology..., BTT, listopad – grudzień 2000, str. 6.

[33] Network server announced to integrate iris recogniyion, BTT, kwiecień 2001, str. 5.

[34] Eye Ticket patches up relations with Unisys and prepares for large order, BTT, lipiec – sierpień 2001, str. 12.

[35] Retinal technology revolution arrives, BTT, wrzesień 2001, str. 12.

[36] Survey: Computer security issues, BTT, czerwiec 2001, str. 9.

[37] Tampa project gets vote of approval by Councillors, BTT, wrzesień 2001, str. 2.

[38] Mobile biometric devices help in law enforcement, j. w., str. 6.

[39] Survey: Immigration issues, j. w. str. 8.

[40] Indiana hospital prescribes biometric network security, BTT, kwiecień 2001, str. 2.

[41] Signing up for m-commerce, BTT, maj 2001, str. 4.

[42] API Gaming and Imagis Market Facial Recognition to Casinos, Biometric Digest, czerwiec 2001, str. 2.

[43] Schools learn about the benefits of biometrics, BTT, czerwiec 2001, str. 7.

[44] Pentagon Interested In Biometrics, Biometric Digest, maj 2001, str. 10.

[45] Didital Persona and Digital Dining Revolutionize Restaurant Industry, Biometric Digest, marzec 2001, str. 5.

[46] Lebanese palace uses biometric hand readers, BTT, wrzesień 2001, str. 3.

[47] Colleges across the USA..., Application News, BTT, lipiec – sierpień 2001, str. 3.

BIBLIOTEKA GŁÓWNA
Politechniki Śląskiej
P. 3057/01
Druk: Drukarnia Gliwice, ul. Zwycięstwa 27, tel. 230 49 50