POLITECHNIKA ŚLĄSKA W GLIWICACH
WYDZIAŁ AUTOMATYKI, ELEKTRONIKI I INFORMATYKI

Metoda multimodalnego wzmacniania kryptografii w aspekcie biometrii behawioralnej

— AUTOREFERAT ROZPRAWY DOKTORSKIEJ —

AUTOR
mgr inż. Marcin Bugdol

PROMOTOR
dr hab. inż. Andrzej W. Mitas
prof. nzw. w Politechnice Śląskiej

Gliwice 2011

1 Wprowadzenie

Wraz z upowszechnianiem się komputerów i innych urządzeń elektronicznych wprowadzono dodatkowe sposoby identyfikacji i weryfikacji tożsamości człowieka oraz zabezpieczenia treści przesyłanych danych. Opierają sie one głównie na dwóch metodach:

- wiedzy posiadanej przez osoby (ang. *Something You Know – SYK*),
- identyfikatorów (tokenów, żetonów) posiadanych przez osoby (ang. *Something You Have - SYH*).

Praktyka wykazała, iż dotychczas powszechnie stosowane algorytmy zabezpieczeń niejednokrotnie nie spełniają pokładanych w nich nadziei. Przyczyną tego faktu jest sam człowiek, będący najsłabszym ogniwem w systemie zabezpieczeń. Kody dostępu są zapominane, bywają łatwe do odgadnięcia lub ujawniane pochopnie osobom postronnym. Z kolei wszelkiego rodzaju identyfikatory fizyczne mogą zostać zgubione, podrobione, skradzione lub po prostu zniszczone. Należy również podkreślić, że w metodach opartych na posiadanym identyfikatorze lub wiedzy, oceniana jest ich zgodność z wzorcem, a nie autentyczność osoby, której ten wzorzec odpowiada. Z tego powodu od dawna podejmowane są próby zdefiniowania znacznika, który byłby trudny do zgubienia, kradzieży lub podrobienia, a jednocześnie pozwalałby na jednoznaczną i wiarygodną weryfikację tożsamości człowieka.

Rozwiązanie powyżej postawionego problemu tkwi w ludzkim ciele i zaszyfrowanym w nim systemie rekacji i zachowań. Ostatnie dwie dekady to okres intensywnych badań naukowych w dziedzinie analizy cech fizjologicznych i behawioralnych człowieka. Wyniki tych badań jednoznacznie wykazały przydatność biometrii w systemach zabezpieczeń. Osobniczo zmienne wartości cech, czyli tak zwane klucze biometryczne, stały się nieodłącznym atrybutem naszej codzienności. Ich wykorzystanie niesie ze sobą jednak zarówno nowe wyzwania, jak i zagrożenia. Naczelne ryzyko wiąże się z archiwizacją indywidualnych wartości cech biometrycznych. Utrata wzorca, w jego postaci kompatybilnej z wymogami akwizycyjnymi zabezpieczonego systemu, może stanowić poważne zagrożenie (zazwyczaj w kontekście konieczności kradzieży także wielu innych dodatkowych informacji). Lepszym rozwiązaniem wydaje się być odejście od koncepcji centralnej bazy wzorców i wyznaczanie kluczy bezpośrednio z aktualnej wartości biometryki. Wyznaczane tak szyfrogramy byłyby (z uwagi na użyty do rozpraszania informacji ciąg pseudolosowy) trudne do zapamiętania przez człowieka. Koncepcja ta, ujmowana wspólnie pod nazwą „kryptografia biometryczna”, jest nadzwyczaj interesująca, ponieważ wyznaczanie klucza biometrycznego odbywa się w czasie rzeczywistym, a wartość cechy biometrycznej stanowi jedynie jeden z parametrów szyfru. Komfort użytkownika wynika więc ze świadomości posiadania przy sobie „klucza do klucza”.

2 Cele i teza pracy

Prowadzone prace naukowo-badawcze w dziedzinie biocybernetyki i inżynierii biomedycznej stanowią w zamierzeniach autora próbę zastosowania metod matematycznych w asocjacji zasadniczo odmiennych technik biometrycznych. Finalnym celem podejmowanych działań jest określenie metody oraz stworzenie narzędzi sprzętowo-programowych do parametryzacji algorytmu pracy liniowego generatora ciągów szyfrujących.

Celem utylitarnym, wytyczonym w prezentowanej dysertacji, jest przygotowanie sprzętowo-programowego stanowiska laboratoryjnego, desygnowanego zarówno pracom naukowo-badawczym, jak i dydaktyce na kierunku Inżynieria Biomedyczna.

Na podstawie szczegółowej analizy aktualnego stanu wiedzy oraz wyników badań laboratoryjnych sformułowano tezy pracy, które, w podziale warunkowanym oceną ich istotności, przedstawiono poniżej.

Teza główna

Możliwe jest określenie osobniczo stałych mechanizmów reakcji na pobudzenia wzrokowe lub słuchowe (w rozumieniu biometrii behawioralnej), a następnie wyznaczenie na tej podstawie wartości, służących jako stany startowe dla generatorów ciągów pseudo-przypadkowych w logice wielowartościowej, w celu obliczenia biometrycznie wzmacnianego podpisu elektronicznego.

Tezy szczegółowe

1. Możliwe jest wyznaczenie znamiennego osobniczo typu odruchowej reakcji człowieka na kontrolowane pobudzenia dźwiękowe lub wizualne.

2. Możliwe jest wyznaczenie wartości liczbowych parametrów, opisujących sposób odruchowej reakcji człowieka na zadawane pobudzenia testowe, przy czym reakcje te są mierzone technikami pomiarowymi z zakresu inżynierii biomedycznej i biocybernetyki.

3. Możliwe jest zastosowanie ustalonych znaczników biometrycznych do programowania rejestru MVL-LFSR.

3 Biometryczne podstawy koncepcji badawczej

W literaturze przedstawiono wiele podejść do problemu połączenia kryptografii oraz biometrii. Różnią się one zarówno pod względem pola syntezy, jak i sposobu implementacji danej metody. Najważniejsze z podejść obejmują: 1) zabezpieczenie klucza za pomocą biometrii, 2) połączenie klucza kryptograficznego z próbką biometryczną, 3) wykorzystanie całego szablonu biometrycznego, jego części lub wyłonionej próbki do bezpośredniej generacji klucza kodowego, 4) wykorzystanie rozmytych

schematów rekonstrukcji klucza. Prezentowane w pracy rozwiązanie jest autorskim połączeniem pierwszej oraz trzeciej koncepcji.

Wygenerowanie kluczy kodowych na podstawie rozmytej próbki biometrycznej jest zadaniem niezwykle skomplikowanym. Odpowiedni dobór cechy oraz sposobu jej akwizycji pozwala zminimalizować wpływ metody pomiaru na wynikowy kod kryptograficzny. Optymalna cecha biometryczna powinna się charakteryzować:

- odzwierciedleniem zachowania człowieka w reakcji na pobudzenia,
- wysoką stabilnością w długim okresie czasu,
- trudnością kradzieży,
- stosunkowo łatwą akwizycją,
- dużą liczbą parametrów,
- społeczną akceptacją,
- możliwością pobrania tylko od osób żywych.

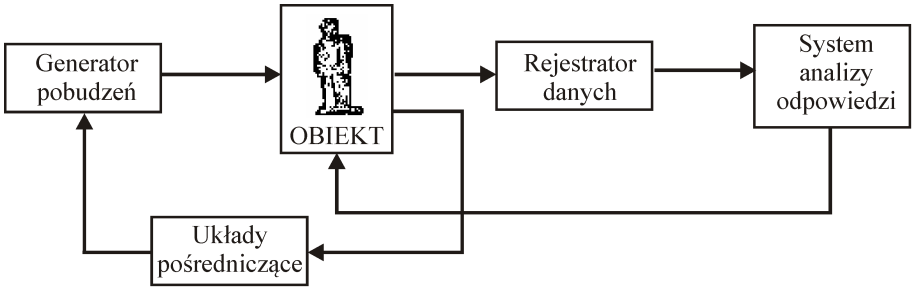
Żadna z obecnie popularnie stosowanych biometryk nie spełnia wszystkich założeń, dlatego też zdecydowano się na dobór dwóch biometryk, ponieważ ich kombinacja pozwala na osiągnięcie wszystkich powyższych warunków równocześnie. Są to: sygnał głosu oraz zapis elektrycznej czynności serca.

4 Autorski system pomiarowy - budowa i oprogramowanie

Podstawowy cel pracy naukowo-badawczej stanowi autorski system kryptografii biometrycznej. Finalne rozwiązanie obejmuje nie tylko sprzęt i oprogramowanie, lecz również odpowiednio dobrany model matematyczny.

Naukowym problemem jest badanie reakcji człowieka na zadawane pobudzenia. Wybrane cechy biometryczne mają zróżnicowany rodowód:

- fizjologiczny - oznacza to, że biometryka jest stała z zasady i uwolniona od świadomej lub podświadomej reakcji badanego, co odpowiada pośrednio układowi z otwartą pętlą sprzężenia zwrotnego;
- behawioralny - odzwierciedleniem istoty rzeczy jest tu zamknięta pętla biocybernetycznego sprzężenia zwrotnego, w którym stan człowieka, a w szczególności warunkowych jego reakcji, może wpływać na zadawane pobudzenia (rys. 1).



Rys. 1. System pomiarowy z biocybernetycznym sprzężeniem zwrotnym

4.1 Stanowisko pomiarowe - opis konstrukcji

Założenia techniczne projektowanego systemu sformułowano w ogólnej postaci w następującym zestawieniu:

- kontrola procesu akwizycji,
- zadowalająca dokładność pomiaru sygnału mowy, uzyskana dzięki możliwie najlepszej konwersji A/C,
- multimodalność pomiaru uwzględniająca dodatkowy tor pobierania danych, zawierający przenośne urządzenie powszechnego użytku do monitorowania sygnału EKG.

Tor pomiarowy służący do pomiaru sygnału głosu składa się z wysokiej jakości mikrofonu, niskoszumowego wzmacniacza mikrofonowy oraz przetwornika A/C, połączonego z komputerem poprzez interfejs USB.

Świadomie zrezygnowano z użycia standardowej karty dźwiękowej, znajdującej się obecnie praktycznie w każdym zestawie komputerowym. Wynika to z faktu, iż jej parametry są niewystarczające dla pomiarów o dużej precyzji. W szczególności dotyczy to nieliniowości różniczkowej oraz nieliniowości całkowej.

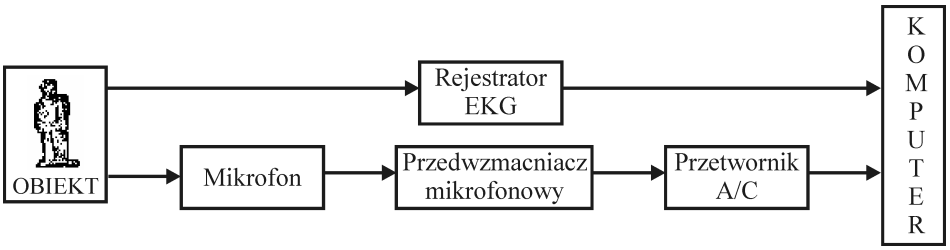
Użyty przetwornik A/C Labjack UE9 charakteryzuje się nieliniowością całkową równą ±0,02% pełnego zakresu, nieliniowością różniczkową równą ±1 LSB dla 12 bitowego przetwarzania, a typowy bezwzględny błąd dokładności wynosi ± 0,025% pełnej skali. Pozostałe parametry, takie jak szybkość próbkowania oraz rozdzielczość, spełniają wymagania opracowanego systemu pomiarowego.

Wykorzystany mikrofon dynamiczny Tonsil MD 268 posiada charakterystykę kierunkową kardioidalną. Dzięki niej mikrofon bardzo dobrze rejestruje dźwięki dochodzące do niego z przodu, natomiast te z boku lub z tyłu są rejestrowane znacznie słabiej lub wcale. Pozwala to na dużą redukcję zakłóceń pochodzących z otoczenia, a tym samym poprawia jakość rejestracji głosu.

Napięcie wyjściowe mikrofonu rzędu kilkunastu mV jest zbyt niskie, aby mogło zostać przesłane bezpośrednio do wejścia przetwornika A/C. W ramach pracy został skonstruowany ultraniskoszumowy wzmacniacz mikrofonowy, którego zadaniem jest zwiększenie sygnału mikrofonowego bez wprowadzania dodatkowych zniekształceń.

Ustalając założenia konstrukcyjne systemu pomiarowego przyjęto multimodalność pomiaru biometrycznego. W związku z tym układ pomiarowy został uzupełniony o równoległy tor, w którym dla badania cechy fizjologicznej wykorzystano podręczny elektrokardiograf ChoiceMed MD100B. Został on wprowadzony w celu rejestracji sygnału EKG w czasie przeprowadzania eksperymentu. Dzięki temu istnieje możliwość określenia wpływu sygnału mowy na zmiany w sygnale EKG badanej osoby. Zapis czynności elektrycznej mięśnia sercowego jest również dodatkowym źródłem cech biometrycznych.

Schemat blokowy systemu dwukanałowej rejestracji cech biometrycznych przedstawiono na rysunku 2.



Rys. 2. Schemat rejestratora próbek

System pomiarowy, poza częścią sprzętową, obejmuje również dedykowane autorskie oprogramowanie, które umożliwia generację pobudzeń, akwizycję próbek sygnału mowy, fali EKG oraz analizę zarejestrowanych danych i przedstawienie wyników pomiarów.

W prezentowanej pracy przyjęto dwa rodzaje bodźców: dźwiękowe oraz wzrokowe. Oba typy pobudzeń można w prosty sposób przetwarzać i emitować w szerokim zakresie przy użyciu komputerów. Tego rodzaju stymulacje nie wymagają zatem specjalistycznego, a przez to często drogiego sprzętu.

Stymulator programowy generuje pojedynczy dźwięk o losowej wysokości. Podawane dźwięki były zapisanymi wcześniej próbkami rzeczywistego instrumentu, w szczególności pianina elektrycznego. Rozkład prawdopodobieństwa częstotliwości generowanych dźwięków został tak dobrany, aby dźwięki przeważnie pochodziły z typowego zakresu mowy ludzkiej (80-900Hz [2]). Pobudzenia spoza wspomnianego zakresu występują trzykrotnie rzadziej. Formalny zapis został zaprezentowany poniżej:

$$P(\xi = x) = \begin{cases} \dfrac{1}{184} & \text{dla} \quad x \in A_1 \\ \dfrac{3}{184} & \text{dla} \quad x \in A_2 \end{cases}, \tag{1}$$

gdzie:

$A_1 = \{a_i : i \in \{1, 2, ..., 12, 61, 62, ..., 88\} \wedge a_1 = 27,5 \wedge a_i = (\sqrt[12]{2})^{i-1} \cdot a_1\}$,

$A_2 = \{a_i : i \in \{13, 14, ..., 60\} \wedge a_1 = 55 \wedge a_i = (\sqrt[12]{2})^{i-1} \cdot a_1\}$.

Zadaniem badanej osoby było dopasowanie się do wygenerowanego dźwięku poprzez zaśpiewanie pojedynczej, ustalonej głoski na podanej wysokości. Poprzednie badania wykazały [3,15], iż w tym celu najlepiej wykorzystać samogłoski (szczególnie samogłoskę „a"). Wynika to z dwóch powodów: można je wypowiadać przez dłuższy czas w niezmienny sposób oraz zawierają informację o cechach fizjologicznych traktu głosowego.

Oprogramowanie modułu pomiarowego rejestruje wypowiadane dźwięki i w czasie rzeczywistym określa stopień ich dopasowania. Porównywane są częstotliwości podstawowe obu sygnałów. Wysokość tonu pochodzącego z instrumentu jest znana, natomiast częstotliwość podstawowa dźwięku śpiewanego przez użytkownika jest obliczana przy użyciu metody opartej o autokorelację sygnału:

$$r(k) = \sum_{n=0}^{N-k-1} x(n)x(n+k), \quad k = 0, 1, 2, \ldots, N-1 \tag{2}$$

gdzie: N - liczba próbek sygnału.

Na podstawie wyniku porównania wyświetlany jest na ekranie odpowiedni obraz. Jest to drugi, wizualny tor stymulacji polisensorycznej. Wyświelany jest kwadrat o jednolitym kolorze, który zmienia się w zależności od stopnia dopasowania pomiędzy przykładowym i emitowanym dźwiękiem. Kolory wyświetlanych obrazów to: zielony, ciemnozielony, żółty, pomarańczowy, ciemnoczerwony oraz czerwony; oznaczają one odpowiednio: prawie idealne dopasowania (zielony), coraz mniejsza zgodność (ciemnozielony, żółty, pomarańczowy i ciemnoczerwony), aż po całkowity brak dopasowania (czerwony). Zgodnie z przyjętymi ustaleniami, celem osoby badanej jest dostrojenie się do podanego dźwięku, a więc uzyskanie koloru zielonego.

Odległość pomiędzy dwoma dźwiękami jest zdefiniowana w skali muzycznej, brana jest więc pod uwagę nie tylko częstotliwość podstawowa (która określa położenie dźwięku), lecz przede wszystkim wzajemne odległości dźwięku wzorcowego i dźwięku śpiewanego w tej skali. Dzięki temu, nawet jeśli osoba badana nie ma fizycznych możliwości zaśpiewania dźwięku dokładnie na określonej wysokości, może zaśpiewać o oktawę (lub kilka oktaw) wyżej względnie niżej [29]. Zakresy wyświetlanych kolorów definiowane przez różnicę $F_{0_gener} - F_{0_emit}$ są opisane następującym równaniem:

$$\text{kolor} = \begin{cases} \text{zielony} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| \in \left[0, \frac{1}{4}\text{tonu}\right] \\ \text{ciemnozielony} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| \in \left(\frac{1}{4}\text{tonu}, \frac{3}{4}\text{tonu}\right] \\ \text{żółty} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| \in \left(\frac{3}{4}\text{tonu}, \frac{5}{4}\text{tonu}\right] \\ \text{pomarańczowy} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| \in \left(\frac{5}{4}\text{tonu}, \frac{7}{4}\text{tonu}\right] \\ \text{ciemnoczerwony} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| \in \left(\frac{7}{4}\text{tonu}, \frac{11}{4}\text{tonu}\right] \\ \text{czerwony} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| > \frac{11}{4}\text{tonu} \end{cases} . \tag{3}$$

Pierwszym krokiem algorytmu rejestracji danych jest pomiar sygnału EKG przez 30 sekund, w celu określenia rytmu pracy serca w stanie relaksu. Następnie odtwarzany jest pojedynczy dźwięk, który trwa przez około dwie sekundy. Najważniejszą częścią badania jest próba dopasowania się użytkownika do słyszanego tonu. Program w czasie rzeczywistym określa, w jakim stopniu śpiewany dźwięk jest kompatybilny z dźwiękiem, który usłyszała badana osoba i wyświetla na ekranie wynik porównania w postaci jednokolorowych kwadratów. Zmiany prezentowanych kolorów następują co 300 ms. Główna pętla programu (odpowiedź użytkownika - stymulacja wizualna) jest powtarzana przez około pięć sekund. Pojedyncza próba (stymulacja dźwiękowa - dopasowanie się użytkownika) ma czas trwania około siedmiu sekund. W ramach jednego eksperymentu przeprowadza się pięć prób. Całość badania trwa nie więcej niż dwie minuty. Przez cały czas akwizycji dźwięku rejestrowany jest współbieżnie sygnał EKG.

4.1.1 Akwizycja danych

Mierzony sygnał EKG odpowiada różnicy potencjałów pomiędzy elektrodami „lewa ręka” a „prawa ręka” (LA – RA), a więc jest to odprowadzenie I. Użyto standardowych samoprzylepnych elektrod Ag/AgCl. Próbki pomiarowe sygnału EKG zostały pobrane z rozdzielczością 8 bitów przy częstotliwości próbkowania 100Hz. Sygnał mowy został zarejestrowany z dwunastobitową rozdzielczością przy częstoliwości próbkowania 44,1 kHz. Osoba badana otrzymywała słuchawki, w których odtwarzany był dźwięki. Mikrofon ustawiany był w niewielkiej odległości, zapewniającej odpowiedni poziom sygnał przy nagrywaniu. Starano się wprowadzić odbiorców w stan odprężenia, co ze względu na subiektywne definiowanie tego stanu nie jest zadaniem prostym. Zapis pojedynczej próby zawierał także dodatkową informację o charakterystycznych momentach czasu, takich jak: początek stymulacji, początek odpowiedzi (śpiew) oraz koniec próby. Te dane są niezbędne do synchronizacji obu modalności oraz w dalszej analizie, które ma na celu wyłonienie osobniczej reakcji na pobudzenie.

Badania przeprowadzono na 12 osobach w różnym wieku, różnej płci oraz posiadających różne wykształcenie muzyczne. Każdą z osób badano kilkukrotnie w różnych odstępach czasowych, uzyskując w sumie 60 pomiarów.

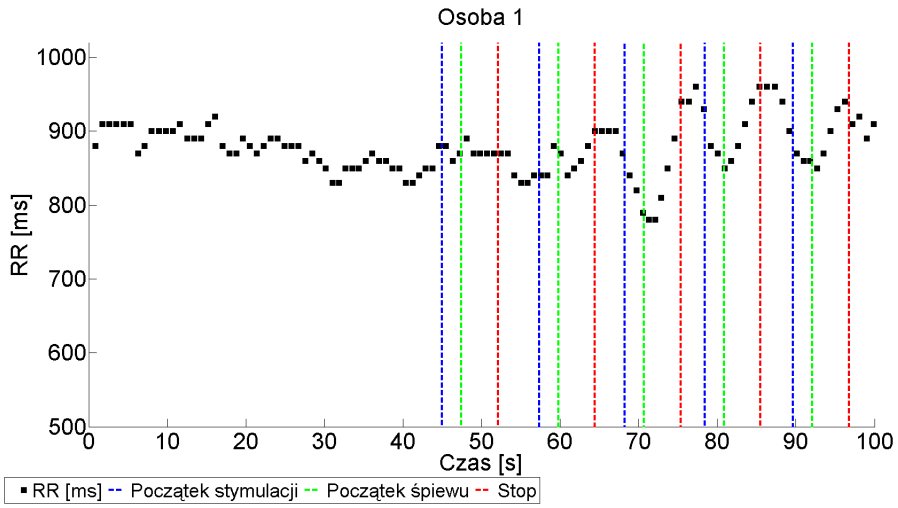
5 Metody ekstrakcji rzeczywistych biometryk

W ramach pracy opracowano metody analizy danych, które pozwalają na wyłonienie zbioru cech biometrycznych. Aktualne, osobniczo znamienne wartości tych cech, przyjmowane w rezultacie odpowiedniego pobudzenia, umożliwiają wyznaczenie biometrycznego znacznika (markera). Ten wynikowy kod posłuży do parametryzacji (wzmocnienia) podpisu elektronicznego.

5.1 Analiza sygnału EKG

Przetwarzanie sygnału EKG obejmowało detekcję załamków R jako punktów najbardziej charakterystycznych elektrokardiogramu oraz wyznaczenie odległości pomiędzy nimi. Zarejestrowany przebieg poddano filtracji wstępnej filtrem górnoprzepustowym w celu eliminacji zakłóceń powstałych w czasie akwizycji. Następnie przeprowadzono lokalizację punktów R, wykorzystując filtrację pasmowoprzepustową (10-17Hz), średnią kroczącą oraz zaprojektowany detektor.

Na podstawie analizy statystycznej dowiedziono, iż zmiany wartości odległości pomiędzy kolejnymi załamkami R są bardziej dynamiczne po stymulacji, aniżeli przed (rys. 3). Wyniki testu dały podstawy do obliczenia cech, które mogą umożliwić rozróżnienie poszczególnych osób biorących udział w eksperymencie. Obliczono odpowiednio: średnią, odchylenie standardowe, medianę, pierwszy kwartyl oraz dominantę przed i po stymulacji.



Rys. 3. Przebieg odległości RR w czasie

Oprócz cech z zakresu statystyki przeanalizowano także przebieg wartości RR użytkownika po oddziaływaniu stymulacji dźwiękowej. Wyznaczono lokalne ekstrema w ciągu RR poprzez obserwację przebiegu wynikowego i badaniu jego monotoniczności. Punkt jej zmiany odpowiada ekstremum lokalnemu. To przekształcenie ujawnia małe zaburzenia, które są interpretowane jako wierzchołki pierwotnego przebiegu. Wprowadzono więc dwie autorskie modyfikacje do algorytmu, aby działał on zgodnie z wymaganiami. Po oznaczeniu położenia wierzchołków w przebiegu RR, wyznaczono następujące cechy związane z tym wykresem:

- liczbę maksimów i minimów lokalnych,
- liczbę ekstremów powyżej i poniżej średniej obliczonej dla całego przebiegu RR,

- pochylenie odcinków pomiędzy kolejnymi ekstremami lokalnymi, obliczonymi na podstawie następującego wzoru:

$$s(n) = \frac{y_n - y_{n-1}}{x_n - x_{n-1}} \tag{4}$$

  gdzie:

  y - wartość ekstremum,

  x - położenie ekstremum,

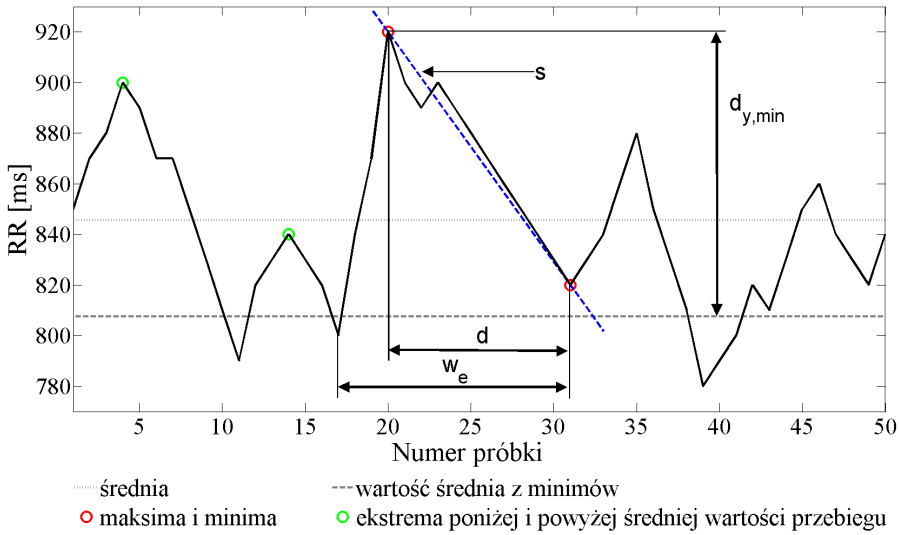
- odległości pomiędzy kolejnymi ekstremami d,
- odległość maksimów lokalnych od wartości średniej minimów $d_{y,min}$,
- szerokości kolejnych ekstremów, obliczone z następującego wzoru,

$$w_e(n) = x_{n+1} - x_{n-1}; \tag{5}$$

  gdzie:

  x - położenie ekstremum.

Na rysunku 4 przedstawiono wszystkie wymienione powyżej cechy.



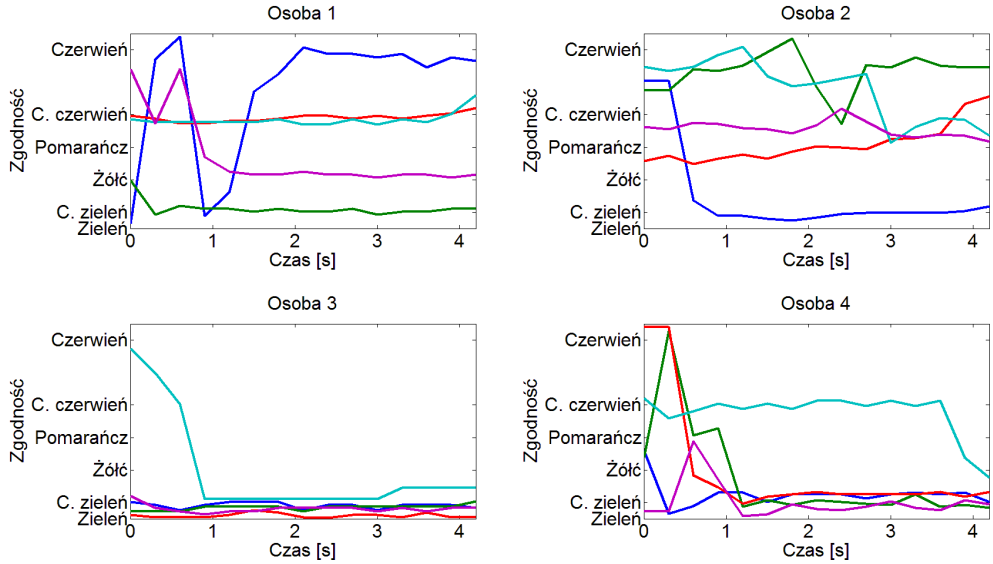
Rys. 4. Przebieg RR z zaznaczonymi, proponowanymi cechami

5.2 Analiza sygnału głosu

W przypadku sygnału mowy przetwarzanie wstępne ograniczało się do podzielenia zarejetrowanego przebiegu na okna czasowe, w których przeprowadzano analizę. Nie zastosowano dodatkowej filtracji, ponieważ założono, iż do dalszych badań należy wykorzystać pełną informację, zarejestrowaną w sygnale.

Głos emitowany przez człowieka zawiera zarówno cechy behawioralne jak fizjologiczne. Dlatego też skupiono się na obu grupach cech, w celu utworzenia jak największego zbioru unikalnych współczynników.

Na podstawie zarejestrowanych próbek głosu sporządzono wykresy stopnia dopasowania (wyrażonego w kolorach) w zależności od czasu trwania eksperymentu dla poszczególnych prób (rys. 5). Czas, po którym obliczano stopień dopasowania, to 300 ms, a więc dokładnie tyle, ile wynosi, interwał pomiędzy kolejnymi zmianami stymulacji wizualnej osoby badanej w trakcie eksperymentu.



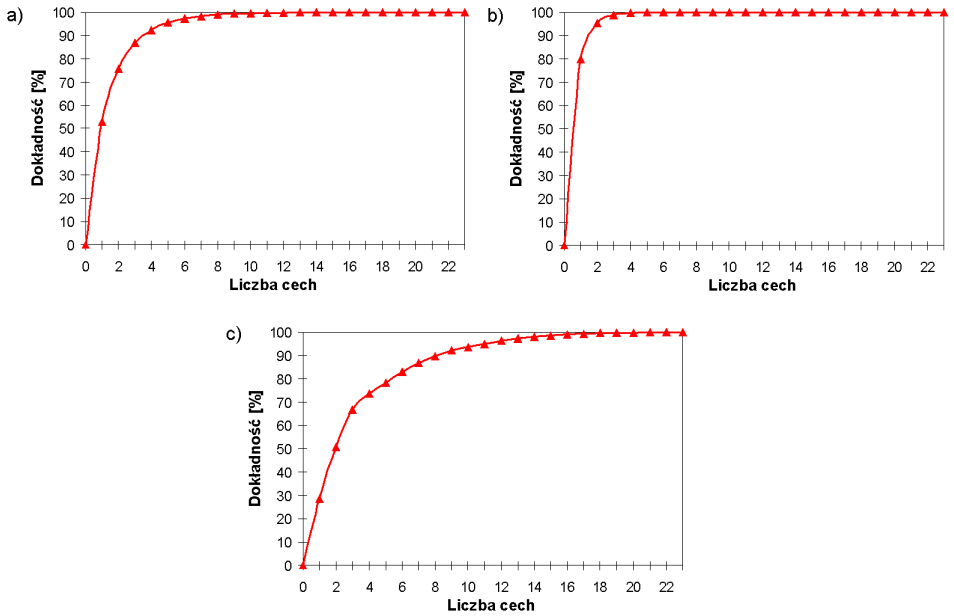
Rys. 5. Przebiegi zgodności dla czterech osób

Bazując na tych spostrzeżeniach zaproponowano obliczenie pewnych współczynników statystycznych i wykorzystanie ich w celu wyłonienia unikalnego znacznika (markera) biometrycznego.

Wybrano jeden przedział czasu o długości 300 ms obejmujący okres pomiędzy 1,2 s, a 1,5 s każdej próby. Selekcji dokonano na podstawie obserwacji wielu przebiegów dopasowania. Wynikało z nich, iż użytkownik w pierwszej sekundzie próby starał się dopasować do usłyszanego dźwięku, a następnie utrzymywał częstotliwość emitowanego dźwięku na względnie stabilnym poziomie przez resztę czasu trwania próby. Dlatego też początek przebiegów charakteryzuje się dużą zmiennością, a więc nie jest odpowiedni, aby wyznaczyć pewne stałe co do wartości współczynniki biometryczne. Z kolei wybranie okna czasowego w późniejszym momencie eksperymentu również nie gwarantuje stałości wartości zaproponowanych cech, ponieważ część osób nie potrafi zaśpiewać dźwięku przez okres dłuższy niż 2 s i po tym czasie milknie. We wspomnianym wyżej przedziale wyliczano następujące współczynniki statystyczne: średnią, odchylenie standardowe, pierwszy i trzeci kwartyl, medianę oraz dominantę. Obliczono także rodzaj głosu.

W zaproponowanym powyżej oknie czasowym (ramce) obliczono 32 współczynniki mel–spektralne oraz 24 współczynniki mel–cepstralne [11, 26, 37].

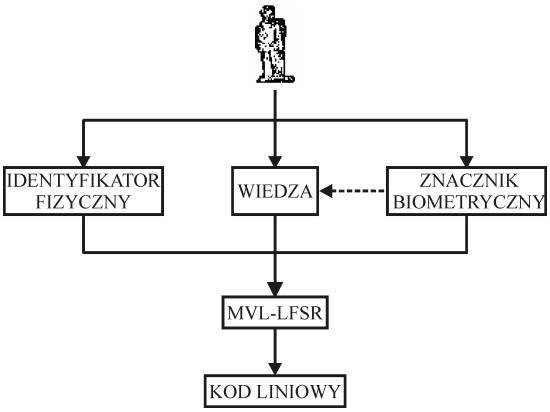
W celu doboru najlepszego zestawu współczynników wykorzystano dwie metody redukcji wymiarowości przestrzeni cech: analizę dyskryminacyjną Fisher'a oraz metodę analizy składowych głównych (PCA). Orzymano 23 współczynniki związane z oboma modalnościami, które reperezentowały zarówno cechy fizjologiczne jak i behawioralne. Przeprowadzone testy w zakresie podziału przestrzeni cech na rozłączne wycinki potwierdziły dokładność proponowanego rozwiązania (rys.6).



Rys. 6. Dokładność dopasowania dla wszystkich wykorzystanych współczynników w zależności od liczby cech a) średnie b) maksymalne c) minimalne

6 System multimodalnego klucza biometrycznego z MVL–LFSR

Zaproponowane cechy wykorzystane zostały do wzmocnienia systemu kryptograficznego. Wartości uzyskanych współczynników pozwalają co prawda na rozróżnienie poszczególnych osób z dużą dokładnością, lecz nie jest możliwa generacja kluczy szyfrujących bezpośrednio na ich podstawie. W niniejszej pracy proponuje się koncepcję systemu biometrycznego, w którym połączone zostały wszystkie dotychczasowe metody uwierzytelniania: oparte na wiedzy, oparte na posiadaniu oraz biometria. Każdy z identyfikatorów będzie zawierał tylko część informacji niezbędnej do wyznaczenia klucza szyfrującego. Efektem ich integracji będą parametry generatora liczb opartego na rejestrze liniowym w logice wielowartościowej (rys. 7).



Rys. 7. Propozycja systemu kryptograficznego wzmacnianego biometrycznie

6.1 Propozycja systemu kryptograficznego wzmocnionego biometrycznie

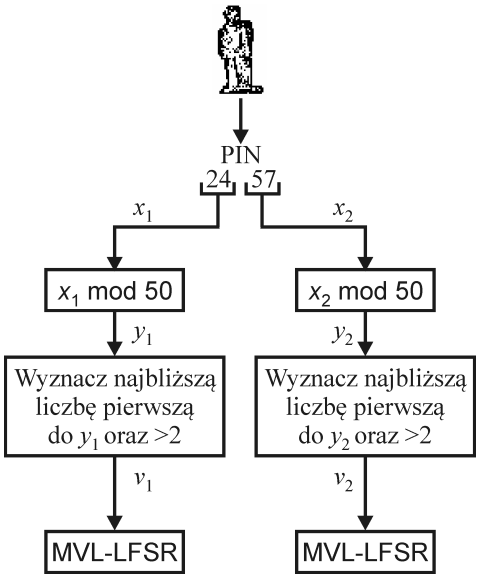
W proponowanym systemie kryptograficznym wykorzystane są dwa generatory MVL-LFSR o niezależnej długości rejestru oraz wartości logik.

Aby zdefiniować generator liczb pseudolosowych działający w oparciu o rejestry przesuwne w logice wielowartościowej, potrzebne są 4 parametry:

- wartościowość logiki v,
- długość rejestru m,
- wielomian charakterystyczny sprzężenia zwrotnego g,
- niezerowy ciąg inicjalizujący s_v.

Pierwszy z wyżej wspomnianych parametrów, określający wartościowość logiki obu generatorów, jest przechowywany w postaci 4-cyfrowego indywidualnego numeru identyfikacyjnego (PIN). Wartościowość logiki musi być liczbą pierwszą, dlatego też zaproponowano następujący algorytm ekstrakcji tej wartości z numeru PIN: na podstawie pierwszych dwóch cyfr będzie wyznaczany parametr v_1, natomiast na podstawie dwóch kolejnych parametr v_2, a więc wartościowość obu rejestrów MVL. Wyłonienie poszukiwanych parametrów w obu przypadkach odbywa się identycznie. Algorytm ekstrakcji przedstawiony został schematycznie na rys. 8.

Dwucyfrowa liczba przyjmuje wartości z zakresu $00, \ldots, 99$. Jak przedstawiono na rysunku 8, jako pierwsza wyliczana jest reszta z dzielenia *mod* 50. Wartość ta została tak dobrana, aby cały zakres (00-99) podzielić na równe części. Dla oceny przydatności ustalono roboczo, iż logika o maksymalnie 47 wartościach (najwyższy możliwy rząd ciała w zakresie [1;50]) będzie wystarczająca, co jednocześnie nie wpływa na ogólność rozważań. Następnym krokiem jest wyznaczenie liczby pierwszej najbliższej otrzymanej reszcie.



Rys. 8. Propozycja ekstracji wartości logiki rejestru MVL z numeru PIN

Niech P będzie zbiorem 14 najmniejszych liczb pierwszych, większych od 2 ($P = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$). Wtedy:

$$v = \arg\min_{p \in P} |y - p|. \tag{6}$$

Na tym etapie, do procesu ekstrakcji wartościowości logik obu rejestrów, wprowadza się element biometrycznej parametryzacji generatora liczb pseudolosowych. Przypisywana użytkownikowi liczba pierwsza jest zależna od rodzaju głosu osoby rejestrowanej/weryfikowanej w systemie:

$$v = \begin{cases} \arg\min_{p \in P} |(y+1) - p| & \text{dla} \quad \text{fem} \\ \arg\min_{p \in P} |(y-1) - p| & \text{dla} \quad \text{masc} \end{cases}. \tag{7}$$

Jeżeli istnieją dwie równoodległe do $y + 1$ liczby pierwsze:

$$|y + 1 - p_i| = |y + 1 - p_j| \quad \text{dla} \quad i \neq j, \tag{8}$$

to korzysta się z poniższej zależności, która ostatecznie określa poszukiwaną wartościowość logiki:

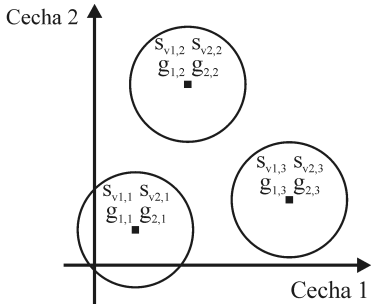
$$v = \begin{cases} \arg\min_{p \in P} |(y+2) - p| & \text{dla} \quad \text{fem} \\ \arg\min_{p \in P} |(y-2) - p| & \text{dla} \quad \text{masc} \end{cases}. \tag{9}$$

Wykorzystana cecha biometryczna wykazuje dużą stabilność na zmienne warunki akwizycji, dzięki czemu możliwa jest powtarzalna generacja klucza kodowego.

Drugim elementem weryfikującym tożsamość w proponowanym systemie biometrycznym jest fizyczny identyfikator (token), w którym przechowywane są parametry rejestrów MVL dotyczące ich długości. Długość rejestru musi zostać tak dobrana, by

nie było zadaniem trywialnym wyznaczenie klejnych stanów bądź ciągu startowego. W przedstawionej koncepcji założono, iż 4 cyfry wystarczą do przechowania długości obu rejestrów. Tak jak w przypadku PIN, dwie pierwsze cyfry oznaczają długość rejestru pierwszego, natomiast dwie kolejne liczbę stopni drugiego z generatorów, przy czym do wartości zapisanej na karcie dodaje się liczbę 10 w celu osiągnięcia minimalnej długości rejestru. Dzięki temu liczba przerzutników tworzących rejestr mieści się w zakresie $m \in [10; 109]$.

Proponuje się również wykorzystanie opracowanego systemu biometrycznego w aspekcie biometrii multimodalnej do wzmocnienia opisywanego systemu kryptograficznego. W chwili rejestracji nowego użytkownika w systemie wyznaczany jest jego wektor cech, który określa punkt w przestrzeni przypisany do tej osoby (rys. 9). Punktowi temu przyporządkowywane są cztery parametry: wartości początkowe rejestrów s_{v1}, s_{v2} oraz współczynniki wielomianów pierwotnych sprzężenia zwrotnego g_1, g_2 dla obu generatorów.



Rys. 9. Przypisanie określonym punktom w przestrzeni cech parametrów generatora MVL

7 Praktyczna weryfikacja koncepcji kryptografii biometrycznej

Zaprezentowana propozycja systemu kryptograficznego wymaga weryfikacji pod kątem poprawności kontroli tożsamości oraz unikalności generowanych kluczy kodowych. W ramach tej części pracy wykonano odrębny moduł autorskiej aplikacji, pozwalający na przeprowadzenie odpowiednich testów przedstawionej koncepcji.

7.1 Algorytm wyznaczania powtarzalnego klucza kodowego

W niniejszej dysertacji proponuje się wykorzystanie wartości biometryk do określania punktu w przestrzeni, któremu zostaną przypisane wartości parametrów startowych generatora MVL-LFSR. Dzięki takiemu rozwiązaniu proces decyzyjny weryfikacji tożsamości jest podobny, jak w przypadku podstawowych systemów biometrycznych, w których zazwyczaj wypracowuje się odpowiedź „Tak/Nie”, na podsta-

wie kwalifikowanego podobieństwa obrazów. W poszukiwaniu rozwiązania kryptografii biometrycznej przyjęto trzy możliwości:

1) osoba została poprawnie zweryfikowana, klucz jest zgodny,

2) osoba została poprawnie zweryfikowana, klucz jest niezgodny,

3) osoba została niepoprawnie zweryfikowana, klucz jest niezgodny.

W pierwszym przypadku scenariusz może być następujący: osoba badana wprowadza poprawnie osobisty PIN (z którego zostają wyłonione właściwe wartościowości logik rejestrów), posiada odpowiedni identyfikator, a także pozytywnie przechodzi proces weryfikacji biometrycznej. Wyłonione przez system biometryki określają właściwy punkt w przestrzeni cech, który zawiera parametry startowe generatora. Klucz zostaje poprawnie wygenerowany.

W drugim przypadku możliwy jest następujący przebieg: pomimo poprawnej weryfikacji (podano poprawny PIN, zaprezentowano odpowiedni identyfikator oraz wybrany został właściwy punkt w przestrzeni), dochodzi do sytuacji, gdy wyznaczony na podstawie zarejestrowanych danych rodzaj głosu osoby weryfikowanej jest niezgodny z wzorcem. W tym przypadku klucz kodowy nie zostanie wygenerowany poprawnie.

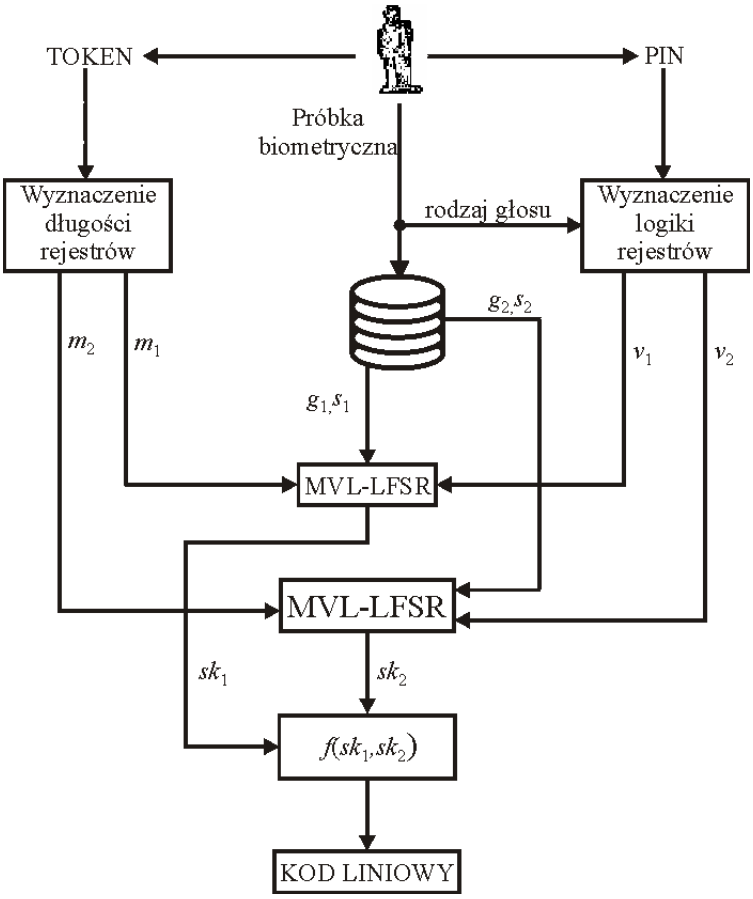
Przypadek trzeci odpowiada scenariuszowi: użytkownik nie został poprawnie zweryfikowany w systemie; wyłonione parametry startowe generatora MVL-LFSR prowadzą w najlepszym wypadku do innego klucza kodowego. Natomiast w przypadku różnych długości rejestru (parametry wyekstrahowane z identyfikatora) oraz sekwencji startowej (pobranej z bazy) generator nie rozpoczyna pracy - klucz nie zostaje wyznaczony.

7.2 Algorytm pracy generatora klucza kodowego - charakterystyka rozwiązania technicznego

Zgodnie z propozycją przedstawioną w rozdziale 6. część parametrów startowych generatora klucza kodowego (podpisu) jest podzielona pomiędzy identyfikatory fizyczne oraz te, oparte na wiedzy. Kluczowym elementem tego rozwiązania jest użycie wyłonionych w niniejszej pracy współczynników biometrycznych, które zabezpieczają pozostałe parametry inicjujące generatora, a także parametryzują jeden z nich. Schemat algorytmu generacji klucza kodowego został przedstawiony poniżej (rys. 10).

Po określonej w algorytmie liczbie kroków, począwszy od zaprogramowanego stanu startowego s_{v1} oraz s_{v2}, uzyskuje się finalne stany końcowe rejestrów $sk_1 = [sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m1}]$ oraz $sk_2 = [sk_{2,1}, sk_{2,2}, \ldots, sk_{2,m2}]$. Długości generowanych sekwencji ds_1 oraz ds_2 są parametrami, które również powinny zostać zapisane w bazie razem z wartościami s oraz g.

Proponuje się utworzenie na podstawie stanów końcowych obu rejestrów jednego ciągu wyjściowego, który utworzy finalny klucz kodowy. Możliwy jest dowolny inny



Rys. 10. Algorytm generacji klucza kodowego

sposób połączenia tych dwóch ciągów i może być to przedmiotem rozważań na gruncie algorytmicznym. W ramach pracy przyjęto jednak wariant najprostszy w celu sprawdzenia proponowanej koncepcji. Klucz kodowy ma następującą postać:

$$kk = [sk_1, sk_2] = [sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m1} sk_{2,1}, sk_{2,2}, \ldots, sk_{2,m2}]. \tag{10}$$

Oba ciągi wyjściowe wyrażone są w innej logice, dlatego w celu wyznaczenia dziesiętnej wartości klucza kodowego należy w pierwszym kroku przeliczyć każdą pozycję klucza na system dziesiętny (w celu ustalenia wspólnego systemu liczbowego, w którym zostaną wykonane dalsze operacje arytmetyczne). Przyjmując, że pozycje po lewej stronie mają najmniejszą wagę, można zapisać tę operację poniższym wzorem:

$$\begin{aligned} kk_{10} = [&sk_{1,1} \cdot v_1^0, sk_{1,2} \cdot v_1^1, \ldots, sk_{1,m2} \cdot v_1^{m_1-1}, \\ &sk_{2,1} \cdot v_2^{m_1}, sk_{2,2} \cdot v_2^{m_1+1}, \ldots, sk_{2,m2} \cdot v_2^{m_1+m_2-1}]. \end{aligned} \tag{11}$$

Finalna wartość klucza kodowego (wyrażona w systemie dziesiętnym) jest sumą wartości poszczególnych pozycji:

$$kk_{10} = \sum_{i=1}^{m_1+m_2} kk_i. \tag{12}$$

7.3 Dyskusja wyników dla posiadanej bazy danych

Zdecydowano się na podział posiadanego zbioru danych na część wykorzystywaną w procesie rejestracji w systemie (oraz na potrzeby związanych z tym obliczeń) i na część, która posłuży do weryfikacji użytkownika. Przyjęto, iż trzy z pięciu zarejestrowanych dla każdej osoby próbek wyznaczają miejsce w przestrzeni cech, do którego są przypisane parametry generatora losowego. Elementy wektora wynikowego są średnimi wartościami cech wektorów wejściowych. Dzięki temu niweluje się w pewnym stopniu niedokładność procesu akwizycji.

Przeprowadzono serię eksperymentów, w których sprawdzono dokładność prezentowanego rozwiązania. W pojedynczym badaniu dla każdej osoby wybierano losowo trzy wektory i rejestrowano ją w systemie. Następnie dokonywano weryfikacji z użyciem pozostałych dwóch wektorów i zapisywano wyniki. Wyszukanie osoby w bazie odbywa się poprzez porównywanie wektora cech aktualnego użytkownika z wektorami cech osób zarejestrowanych. Podobieństwo użytkowników określane jest na podstawie odległości euklidesowej pomiędzy wektorami.

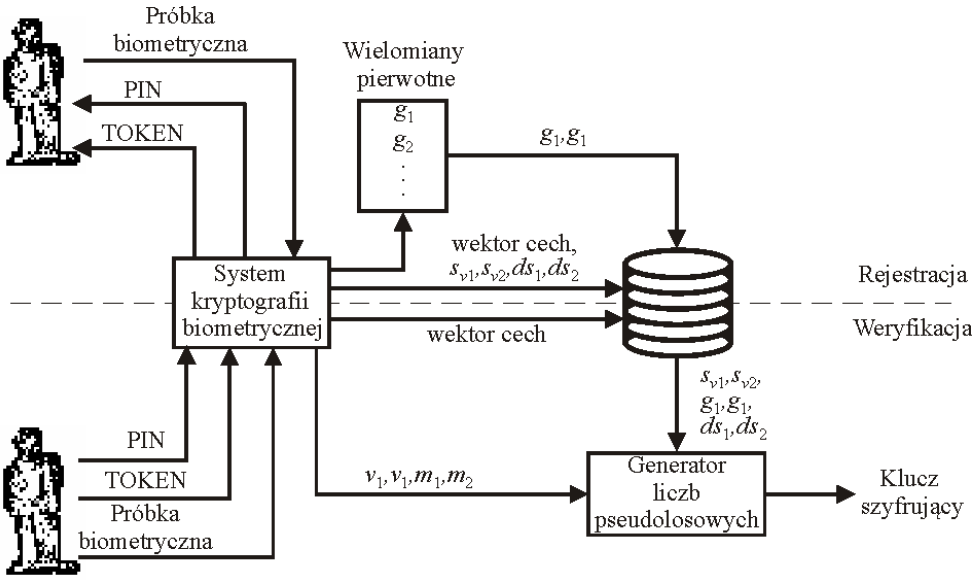
Całość eksperymentu powtórzono dziesięciokrotnie, w celu wyznaczenia średniej dokładności, jak również dla zminimalizowania wpływu pojedynczych, skrajnych wyników. Otrzymano następujące rezultaty: średnia dokładność weryfikacji $\approx$ **8**4%, minimalna osiągnięta dokładność $\approx$ **7**1%, maksymalna uzyskana dokładność $\approx$ **9**3%.

Wygenerowane klucze odpowiadały osobom, które zostały poprawnie zweryfikowane. Nie wystąpiła sytuacja, w której osoba inna od uprawnionej doprowadziłaby do wygenerowania odpowiedniego klucza. Podział przestrzeni cech na nie pokrywające się wycinki nie był gwarantem bezbłędnego przebiegu weryfikacji. Wektor cech jednego z użytkowników określa taki punkt w przestrzeni, że jest on poza wycinkiem przestrzeni innego użytkownika, ale mimo to najbliższe mu punkty przynależą do innej osoby.

Przeprowadzono również badania rozkładu wartości generowanych kluczy. W tym celu wygenerowano 10000 kluczy, dla różnych wartości logik oraz długości rejestru. Dla celów testowych ograniczono wartościowość logiki do siedmiu oraz długość rejestru do ośmiu, ze względu na znaczny czas potrzebny na generację tak dużej liczby kluczy. Otrzymano wyniki charakteryzujące się znikomą powtarzalnością (poniżej 0,04%), co wskazuje na to, iż zaproponowane rozwiązanie posiada oczekiwane własności pseudolosowe.

Przedstawiony system może zostać wykorzystany w praktycznym rozwiązaniu kryptografii biometrycznej. Poglądowy schemat został zaprezentowany na poniższym rysunku 11. Wielomiany pierwotne sprzężenia zwrotnego rejestru MVL-LFSR powinny zostać uprzednio zebrane w bazie danych. Wynika to z długiego czasu generowania wielomianów pierwotnych wysokich rzędów (na średniej klasie komputerze osobistym znalezienie pojedynczego wielomianu 19. stopnia dla logiki o wartościowości 47 trwa około 15 minut).

W fazie rejestracji system pobiera próbkę biometryczną od osoby badanej. Następnie nadawany jest użytkownikowi losowy numer PIN oraz przydzielany jest identyfikator fizyczny (token). W kolejnym kroku generowane są wartości stanów



Rys. 11. Propozycja praktycznego wykorzystania wzmacnianego systemu kryptograficznego w aspekcie biometrii behawioralnej

startowych generatorów s_{v1}, s_{v2}, długości generowanych sekwencji ds_1, ds_2, a także pobierane są z tablicy właściwe wielomiany pierwotne g_1 oraz g_2. Na podstawie próbki biometrycznej system wyznacza wektor cech danej osoby. Służy on do określenia punktu w przestrzeni cech, któremu przypisywane są wartości s_{v1}, s_{v2}, ds_1, ds_2, g_1 oraz g_2. Kompletny zestaw informacji zostaje zapisany w bazie danych.

Podczas weryfikacji użytkownik podaje swój PIN, prezentuje identyfikator fizyczny oraz poddaje się akwizycji próbki biometrycznej. System wyznacza wektor cech, na podstawie którego przeprowadzana jest weryfikacja. W przypadku jej pozytywnego wyniku z bazy uwalniane są odpowiednie parametry inicjujące generator (sekwencje startowe, długości sekwencji oraz wielomiany pierwotne). Zgodność numeru identyfikacyjnego oraz autentyczność tokenu jest warunkiem dalszej pracy. Na ich podstawie oraz wektora cech wyznaczane są kolejne parametry generatora (wartościowości logik v_1 i v_2, a także długość rejestrów m_1 i m_2). Kompletny zestaw parametrów inicjuje pracę generatora, który wyznacza finalny klucz kodowy.

8 Podsumowanie

W niniejszej dysertacji przedstawiono autorską propozycję biometrycznego wzmacniania kryptografii w aspekcie biometrii behawioralnej. Zaprezentowane rozwiązanie sprzętowo-programowe pozwala na rejestrację reakcji użytkownika w odpowiedzi na zadawane bodźce słuchowe oraz wizualne i wyznaczenie na tej podstawie unikalnych wartości wektora cech. Utworzony znacznik biometryczny służy do opracowania koncepcji systemu kryptografii biometrycznej, opartego na generatorach liniowych w logice wielowartościowej, łączącego klasyczne metody zabezpieczeń (oparte na wiedzy i posiadaniu) z biometrią.

Scenariusz generowania pobudzeń, zaprezentowany w pracy, jak i dobór typów stymulacji (dźwiękowa i wizualna) okazał się być skutecznym elementem biocybernetycznego sprzężenia zwrotnego, wywołującym unikalną osobniczo reakcję u człowieka. Jednocześnie okazało się, iż system ten jest przyjazny pod względem użytkowym dla osoby badanej.

Skontruowanie specjalistycznego stanowiska pomiarowego dla biometrii mulitmodalnej pozwoliło na realizację badań zgodnie z założonym scenariuszem. Na podkreślenie zasługuje fakt, że odpowieni dobór elementów konstrukcyjnych i podzespołów przyniósł skutek w postaci eliminacji zakłóceń na etapie akwizycji i wysokiej jakości danych pomiarowych, które charakteryzowały się stabilnością, tak przecież pożądaną w systemach biometrycznych.

Dzięki dużej ilości informacji zgromadzonej w czasie równoległego pomiaru dwóch cech biometrycznych - głosu oraz sygnału EKG - możliwe było opisanie reakcji użytkownika na zadawane pobudzenie za pomocą współczynników liczbowych. Spośród tej informacji wyłoniono zestaw parametrów, zarówno behawioralnych jak i fizjologicznych, związanych z oboma modalnościami. Użycie analizy dyskryminacyjnej oraz metody PCA pozwoliło na wyodrębnienie spośród kilkudziesięciu współczynników zestawu tych, które charakteryzowały się największą dystynktywnością.

Zaproponowana metoda biometrycznej parametryzacji generatorów ciągów szyfrujących łączy unikalną, rozmytą informację osobniczą z jednoznacznie określonym kluczem kodowym. Dołączenie tak utworzonego szyfru do innych danych cyfrowych pozwala, w myśl ustawy o podpisie elektronicznym [32], na utworzenie osobistej sygnatury, która będzie jednoznacznie identyfikowała osobę ją składającą.

Za najbardziej znaczące, autorskie osiągnięcia w pracy uważa się:

1. Opracowanie systemu kryptograficznego, wzmacnianego biometrycznie, ujmujące:
   (a) skonstruowanie systemu pomiarowego biometrii multimodalnej, zawierającego:
      i propozycję scenariusza pobudzeń wizualnych i dźwiękowych,
      ii implementację generatora bodźców pracującego według wyżej wspomnianego scenariusza,
      iii pomiar reakcji osób w odpowiedzi na stymulacje;
   (b) wyznaczenie współczynników odzwierciadlających wpływ reakcji na działanie bodźców, a w tym:
      i wyłonienie osobniczo unikalnych współczynników behawioralnych odzwierciedlających wpływ stymulacji na zarejestrowany sygnał EKG,
      ii wyłonienie współczynników behawioralnych opisujących umiejętność dopasowania się osób do usłyszanego tonu,
      iii wykorzystanie analizy dysryminacyjnej Fisher‘a w celu doboru istotnych współczynników biometrycznyh,
      iv użycie metody składowych głównych do wyznaczenia optymalnego zestawu parametrów;

(c) aplikację rejestrów liniowych w logice wielowartościowej parametryzowanych za pomocą dotychczasowych znaczników rozpoznawania tożsamości, a w szczególności przez:

i przechowywanie wartości logiki generatorów w postaci numeru PIN (wiedza),

ii przechowywanie długości generatora w fizycznym identyfikatorze (posiadanie),

iii wykorzystanie wyłonionych współczynników biometrycznych do parametryzowania wartości początkowych oraz współczynników wielomianu sprzężenia zwrotnego rejestru liniowego.

2. Pomiar multimodalny w holistycznym ujęciu, rozumiany jako:

   (a) współbieżne badanie reakcji fizjologicznej i odpowiedzi złożonego systemu nerwowego, z udziałem biocybernetycznego sprzężenia zwrotnego,

   (b) obserwację normalnego przebiegu czynności życiowych, wymagających decyzji w stanie podwyższonego napięcia nerwowego.

3. Przygotowanie materiałów dydaktycznych do zestawu ćwiczeń laboratoryjnych z przedmiotu „Biometria” dla studiów II-go stopnia na kierunku Inżynieria Biomedyczna (specjalność Informatyka w Medycynie), obejmujących następujące tematy zajęć:

   (a) sygnał głosu w biometrii,

   (b) przetwarzanie sygnału EKG w zastosowaniach biometrycznych,

   (c) optymalny dobór istotnych współczynników biometrycznych.

Tematy ćwiczeń zostały opracowane na podstawie najnowszych materiałów z zakresu fachowej bibliografii. Opisy przeznaczone do pracy dydaktycznej są jednym z efektów prezentowanej dysertacji, dzięki czemu słuchacze kierunku Inżynieria Biomedyczna mają ułatwione zadanie przeszukiwania kwalifikowanych tekstów źródłowych. Zweryfikowane w praktyce autorskie koncepcje stanowią także dobry punkt oparcia dla praktycznie realizowanych (sprzętowo i programowo) ćwiczeń laboratoryjnych.

Motywem przewodnim prezentowanej pracy jest próba stworzenia naukowych podstaw dla ściśle praktycznego, użytkowego, inżynierskiego systemu uwierzytelniania. Obecne rozwiązania, przeważnie rozpoznające atrybuty, zamiast posiadaczy tych atrybutów, stają się niewystarczające wobec rosnącego tempa codziennego życia. Zastosowanie metod biometrycznych personalizuje system, gwarantując tym samym prawo użytkownika do uwierzytelnienia.

Bibliografia

[1] F. Agrafioti, D. Hatzinakos. ECG biometric analysis in cardiac irregularity conditions. *Signal, Image and Video Processing*, 3(4):329–343, 2009. 10.1007/s11760-008-0073-4.

[2] R. J. Baken, R. F. Orlikoff. *Clinical Measurement of Speech and Voice. 2nd edition*. Singular Publishing Group, 2000.

[3] M. D. Bugdol, M. N. Bugdol. Vowels in speaker verification. *Biometrics and Kansei Engineering, IEEE International Conference on*, strony 45–48, 2009.

[4] A. Cavoukian, A. Stoianov. Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy, March 2007.

[5] M. Gorawski, M. D. Bugdol. Kaskadowe operacje ECOLAP. *Studia Informatica*, 28(3A (72)):43–63, 2007.

[6] M. Gorawski, M. D. Bugdol. Model kosztowy x-BR-drzewa w przestrzennych bazach danych. *Studia Informatica*, 29(3A (78)):5–17, 2008.

[7] M. Gorawski, M. D. Bugdol. Cost model for x-BR-tree. *Annals of Information Systems. New trends in data warehousing and data analysis*, 3:203–219, 2009.

[8] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, B. K. Wiederhold. ECG to identify individuals. *Pattern Recognition*, 38(1):133–142, 2005.

[9] A. Juels, M. Sudan. A fuzzy vault scheme. *Proceedings of IEEE International Symposium on Information Theory*, strona 408, 2002.

[10] A. Juels, M. Wattenberg. A fuzzy commitment scheme. *Proceedings of the 6th ACM conference on Computer and communications security*, CCS '99, strony 28–36, New York, NY, USA, 1999. ACM.

[11] W. Kasprzak. *Rozpoznawanie obrazów i sygnałów mowy*. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 2009.

[12] Y. Kusunoki, M. Fukumoto, T. Nagashima. A statistical method of detecting synchronization for cardio-music synchrogram. *IEICE Transactions, Fundamentals*, E86-A(9):2241–2247, 2003.

[13] A. W. Mitas. About the possibilities of the informatics technologies application in music therapy. *Journal of Medical Informatics & Technologies*, 12:189–193, October 2008.

[14] A. W. Mitas, M. D. Bugdol. Techniki biometryczne - podstawowe parametry jakościowe. *Techniki Komputerowe, Wydanie Specjalne Monograficzne*, 42(1):29–37, 2008.

[15] A. W. Mitas, M. D. Bugdol. Biometric aspect of the voice timbre. *Biometry – Special Issue*, strony 93–102, 2010.

[16] A. W. Mitas, M. D. Bugdol. An idea of human voice reaction measurement system under the aspect of behavioral biometric. *Advances in Intelligent and Soft Computing Volume 2*, 69:219–228, 2010.

[17] A. W. Mitas, M. D. Bugdol, M. Plucińska. Biometria a podpis elektroniczny – studium stosowalności. *Elektronika – konstrukcje, technologie, zastosowania*, 49(12):160–163, 2008.

[18] A. W. Mitas, M. D. Bugdol, M. Plucińska. Biometryczne wzmacnianie podpisu cyfrowego - techniczne aspekty zastosowań. *Elektronika – konstrukcje, technologie, zastosowania*, 49(12):164–167, 2008.

[19] A. W. Mitas, M. D. Bugdol, A. Ryguła. Computer aid assessment of driver's fatigue during driving based on eye movements analysis. *Journal of Medical Informatics & Technologies*, 12:195–200, October 2008.

[20] A. W. Mitas, M. D. Bugdol, A. Ryguła. The psychophysiological conditionings and possibilities of driver's work condition assessment under the aspect of traffic safety. *Telematics, logistics and transport safety. TLTS. Proceedings of VIII scientific conference*, strony 122–128, Katowice - Cieszyn, 16-18 października 2008. Silesian Univeristy of Technology.

[21] A. W. Mitas, M. D. Bugdol, A. Ryguła. The psychophysiological determinants of professional driving skills in relation to traffic safety. *Problemy Transportu*, 4(1):87–94, 2009.

[22] A. W. Mitas, M. D. Bugdol, A. Ryguła. Simultaneous analysis of driver's physiological and behavioural parameters under the aspect of transport safety. *Journal of Medical Informatics & Technologies*, 13:241–247, October 2009.

[23] A. W. Mitas, D. Mostowski, M. D. Bugdol. Kryptografia biometryczna w aspekcie wzmacniania podpisu elektronicznego. *Techniki Komputerowe, Wydanie Specjalne Monograficzne*, 42(1):71–81, 2008.

[24] D. Mostowski. Koncepcja wykorzystania wizualnego sprzężenia zwrotnego i sygnału pobudzenia krtaniowego w systemie biometrycznej weryfikacji mówcy. *W pracy zbiorowej „Biometria – wybrane zagadnienia"*, strony 98–106, 2004.

[25] K. Plataniotis, D. Hatzinakos, J. Lee. ECG biometric recognition without fiducial detection. *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the*, strony 1–6, September 2006.

[26] R. Proksa. Visualization of stages of determining cepstral factors in speech recognition systems. *Journal of Medical Informatics & Technologies*, 13:121–128, October 2009.

[27] A. Riera, S. Dunne, I. Cester, G. Ruffini. STARFAST: a wireless wearable EEG/ECG biometric system based on the ENOBIO sensor. *Proceedings of 5th pHealth Workshop on Wearable Micro and Nanosystems for Personalised Health (pHealth'08)*, 2008.

[28] T. W. Shen, W. J. Tompkins, Y. H. Hu. One-lead ECG for identity verification. *Proceedings of the Second Joint EMBS/BMES Conference, 2002*, wolumen 1, strony 62 – 63, 2002.

[29] K. Sikorski. *Harmonia*. Polskie Wydawnictwa Muzyczne, Kraków, 2001.

[30] N. V. Thakor, J. G. Webster, W. J. Tompkins. Estimation of QRS complex power spectra for design of a QRS filter. *IEEE Transaction on Biomedical Engineering*, BME-31(11):702–706, nov. 1984.

[31] U. Uludag, S. Pankanti, S. Prabhakar, A. K. Jain. Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE*, 92(6):948–960, June 2004.

[32] Dz.u.01.130.1450. Ustawa o podpisie elektronicznym.

[33] Y. Wang, F. Agrafioti, D. Hatzinakos, K. N. Plataniotis. Analysis of human electrocardiogram for biometric recognition. *EURASIP Journal on Advances in Signal Processing*, 2008, January 2008.

[34] G. Wübbeler, M. Stavridis, D. Kreiseler, R.-D. Bousseljot, C. Elster. Verification of humans using the electrocardiogram. *Pattern Recognition Letters*, 28(10):1172 – 1175, 2007.

[35] R. V. Yampolskiy, V. Govindaraju. Behavioural biometrics: a survey and classification. *Int. J. Biometrics*, 1(1):81–113, 2008.

[36] S. Yanushkevitch. *Logic Differential Calculus in Multi-Valued Logic Design.* Wydawnictwo Uczelniane Politechniki Szczecińskiej. Institute of Computer Science and Information Systems, Technical University of Szczecin, 1998.

[37] T. P. Zieliński. *Cyfrowe przetwarzanie sygnałów. Od teorii do zastosowań.* Wydawnictwo Komunikacji i Łączności, Warszawa, 2007.