POLITECHNIKA ŚLĄSKA W GLIWICACH
WYDZIAŁ AUTOMATYKI, ELEKTRONIKI I INFORMATYKI

Metoda multimodalnego wzmacniania kryptografii w aspekcie biometrii behawioralnej

— ROZPRAWA DOKTORSKA —

AUTOR
mgr inż. Marcin Bugdol

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

Gliwice 2011

Za możliwość otwartej wymiany poglądów, czasami leżących na przeciwnych biegunach, cierpliwość, wyrozumiałość i nieocenioną pomoc, a także za zwracanie uwagi na pozytywne aspekty wielu codziennych spraw chciałbym podziękować Panu Profesorowi Andrzejowi W. Mitas.

Serdecznie dziękuję mojej Rodzinie za wsparcie i motywację do osiągania kolejnych celów.

Spis treści

Wprowadzenie 6

1. Struktura pracy 9

2. Technologie biometryczne i ich podstawowe właściwości - krótka charakterystyka nowoczesnych rozwiązań 11
2.1 Podstawowe techniki biometryczne 11
2.1.1 Biometria fizjologiczna 11
2.1.2 Biometria behawioralna 12
2.1.3 Biometria multimodalna 15
2.2 Wskaźniki jakości technik biometrycznych 16
2.2.1 Błędy dopasowania 17
2.2.2 Błędy decyzji 17
2.2.3 Błędy akwizycji 19
2.2.4 Podsumowanie problematyki oceny jakości systemów biometrycznych 20
2.3 Obszary stosowalności 20
2.4 Psychologiczne bariery biometrii 22

3. Cele i teza pracy 23

4. Biometryczne podstawy koncepcji badawczej 24
4.1 Wprowadzenie do kryptografii biometrycznej 24
4.2 Kryteria wyboru cech biometrycznych 30
4.3 Sygnał głosu - analiza właściwości wybranej biometryki behawioralnej 32
4.3.1 Powstawanie sygnału mowy 32
4.3.2 Głos w biometrii 34
4.4 Elektrokardiogram - analiza właściwości biometrycznych 36
4.4.1 Mechanika EKG 37
4.4.2 EKG jako cecha biometryczna 38

5. Autorski system pomiarowy - budowa i oprogramowanie 47
5.1 Stanowisko pomiarowe - opis konstrukcji 48
5.1.1 Układ rejestracji głosu 49
5.1.2 Tor EKG 52

5.2 Oprogramowanie systemu pomiarowego 53
5.2.1 System generowania pobudzeń 54
5.2.2 Akwizycja danych 62

6. Metody ekstrakcji rzeczywistych biometryk 65
6.1 Analiza sygnału EKG 65
6.1.1 Przetwarzanie wstępne informacji o pracy serca 65
6.1.2 Ekstrakcja cech biometrycznych 73
6.2 Analiza sygnału głosu 80
6.2.1 Przetwarzanie wstępne sygnału mowy 80
6.2.2 Ekstrakcja cech biometrycznych 81
6.3 Połączenie modalności 86
6.3.1 Dyskryminacja Fisher'a 88
6.3.2 Analiza składowych głównych 91

7. System multimodalnego klucza biometrycznego z MVL–LFSR 101
7.1 Generatory MVL-LFSR 102
7.2 Propozycja systemu kryptograficznego wzmocnionego biometrycznie . 105

8. Praktyczna weryfikacja koncepcji kryptografii biometrycznej 109
8.1 Algorytm wyznaczania powtarzalnego klucza kodowego 110
8.2 Algorytm pracy generatora klucza kodowego - charakterystyka rozwiązania technicznego 111
8.3 Dyskusja wyników dla posiadanej bazy danych 114

9. Podsumowanie 118

Wnioski 120

Bibliografia 123

Spis rysunków 136

Spis tabel 139

Spis algorytmów 140

Wykaz skrótów i oznaczeń 141

Wprowadzenie

Od zarania dziejów podstawą sprawnego działania i rozwoju społeczeństwa jest możliwość nienegowalnego potwierdzenia tożsamości człowieka. Obserwowana ostatnimi laty wszechobecna globalizacja jest przyczynkiem zmniejszania się dystansu interpersonalnego i zacierania się granic między krajami. Procesowi temu towarzyszy gwałtowny wzrost liczby udogodnień i ułatwień, uprzyjemniających użytkownikom wykonywanie codziennych czynności. Jednak pomimo przejęcia wielu naszych obowiązków przez najprzeróżniejsze maszyny i urządzenia, wszystkie umowy, czy to cywilnoprawne czy też kupna-sprzedaży, są zawierane pomiędzy konkretnymi osobami, których tożsamość, tak jak wieki temu, powinna być bezsprzecznie potwierdzona.

W przeszłości podstawową metodą weryfikacji osoby był podpis odręczny składany na dokumencie. Nieliczne jednostki wzmacniały zabezpieczenie oficjalnych dokumentów za pomocą pieczęci, wytwarzanych przez zaufane osoby i pilnie strzeżonych. Wraz z upływem czasu te proste w gruncie rzeczy metody weryfikacji nie nadążały za zmianami cywilizacyjnymi. W społeczeństwie informacyjnym potwierdzenie tożsamości przebiega w wielu przypadkach na odległość i musi być przeprowadzone niezwłocznie, przy czym bezpośredni kontakt z uwierzytelnianą osobą jest często niemożliwy. Osobną kwestią jest zapewnienie poufności danych, przesyłanych przez media transmisyjne w celu zawarcia umowy.

Wraz z upowszechnianiem się komputerów i innych urządzeń elektronicznych wprowadzono dodatkowe sposoby identyfikacji i weryfikacji tożsamości człowieka oraz zabezpieczenia treści przesyłanych danych. Opierają się 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 reakcji 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. Gdyby surowe wzorce biometryczne miały być przechowywane w repozytoriach centralnych, to musiałyby być zabezpieczone w ponad przeciętnym stopniu, znacznie lepiej niż powszechne dziś identyfikatory alfanumeryczne. Utrata wzorca, w jego postaci kompatybilnej z wymogami akwizycyjnymi zabezpieczonego systemu, może stanowić poważne zagrożenie (najczęściej w kontekście konieczności kradzieży także wielu innych dodatkowych informacji). Świadomość ryzyka lub tylko intuicyjna obawa depozytariuszy osobistych biometryk implikuje zazwyczaj wielki sceptycyzm użytkowników. Dla ochrony kluczy biometrycznych można wykorzystać metody znane z kryptografii, które umożliwiają zaszyfrowanie wzorca. Sposób ten prawdopodobnie nie gwarantuje pełnej ochrony, ponieważ dysponentem szyfru jest podmiot odpowiedzialny za przechowywanie danych w repozytorium. 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".

Na co dzień przychodzi nam jednak zmierzyć się z problemem rozpowszechniania przez producentów systemów biometrycznych rozwiązań przez to najlepszych,

że najtańszych, w sensie rzeczywistego kosztu materiałów i pracochłonności. Dystrybutorzy prześcigają się w przekonywaniu potencjalnych klientów o domniemanej doskonałości ich produktów, jednocześnie nie informując o niesionych przez nie potencjalnych zagrożeniach. Nasuwa się tu analogia do systemów bezpieczeństwa biernego użytkowników pojazdów samochodowych, w przypadku których producenci szeroko omawiają problem ochrony, jaką dają poduszki powietrzne oraz strefy zgniotu. Tylko nieliczni z nich informują o fakcie, że jedynie obrażenia zewnętrzne osób przebywających w samochodzie w czasie wypadku są faktycznie ograniczane. Uszkodzenia organów wewnętrznych mogą być natomiast potencjalną przyczyną śmierci poszkodowanych pasażerów. Stopień zagrożenia i ewentualne skutki wynikają jedynie z przeciążenia, na które systemy ochrony biernej nie mają wpływu. Warto nadmienić, iż użytkownicy nie mają przeważnie wystarczającej wiedzy o tym, jak działa wykorzystywany przez nich system, już choćby dlatego, że do rozumienia jego funkcjonowania wymagany jest nieelementarny poziom wiedzy z fizyki.

Przenosząc dywagacje o rzetelności informowania użytkowników na temat rzeczywistych cech funkcjonalnych oferowanych produktów z powrotem na grunt biometrii, warto poruszyć problem tak zwanego skrótu biometryki. Archiwizacja wzorców stanowiących obrazy graficzne, także w postaci zredukowanej w wyniku kompresji informacji, nie umniejsza radykalnie możliwości ich nadużyć. Podnoszony często wskaźnik zmniejszenia ilości informacji, rzędu 10 i więcej (na przykład z mapy bitowej do formatu jpg w przypadku zdjęcia fotograficznego), nie implikuje całkowitego bezpieczeństwa. Każdy z nas ze zdjęcia jpg rozpozna postaci i miejsca równie efektywnie, jak na podstawie obserwacji pierwotnej mapy bitowej. W zredukowanym zbiorze graficznym danej biometryki są bowiem zachowane kluczowe informacje, niezbędne zwłaszcza w automatycznym rozpoznawaniu obrazu. Można jedynie optymistycznie zakładać, że w aplikacji, w której użyte byłyby skompromitowane biometryki w ich zredukowanej postaci, system rozpoznawania obrazu wymagałby wyższej jakości. Występująca tu sprzeczność semantyczna podważa zasadność optymizmu.

Zadaniem badacza, jako osoby uprawnionej do posiadania odpowiedniego poziomu wiedzy, jest więc pozostawanie w opozycji do przedstawicieli rynku zabezpieczeń biometrycznych i krytyczna ocena wdrażanych rozwiązań. Stopień złożoności współczesnych rozwiązań technicznych w dziedzinie biometrii (sprzęt do rejestracji i archiwizacji obrazów oraz skomplikowane algorytmy ich rozpoznawania) praktycznie wykluczają możliwość heurystycznej oceny kwalitatywnej stosowanych technik. Rzeczowa translacja, nierzadko niejawnych parametrów technologicznych na język potoczny, zrozumiały dla przeciętnego użytkownika, to szczególne wyzwanie.

1. Struktura pracy

W rozdziale 2 przedstawiono analizę literaturową najważniejszych zagadnień z zakresu biometrii. Porównano najważniejsze cechy obu grup biometryk: fizjologicznych i behawioralnych, a także wskazano na zalety oraz zagrożenia płynące z połączenia kilku cech biometrycznych w ramach jednego systemu. Opisano najważniejsze wskaźniki jakościowe wykorzystywane do porównywania systemów biometrycznych oraz problemy z oceną tychże systemów. Przedstawiono najważniejsze obszary zastosowań biometrii jak również obawy współczesnego człowieka przed systemami biometrycznym w życiu codziennym.

Na podstawie rozpoznanego stanu wiedzy w dziedzinie biometrii określono w rozdziale 3 podstawowe cele z wyróżnieniem zadań naukowo-badawczych, utylitarnych i pośrednio poświęconych dydaktyce. W tym rozdziale postawiono główną tezę dysertacji.

Rozdział 4 otwiera proces dowodowy tezy pracy. Opisano aktualny stan w dziedzinie kryptografii biometrycznej oraz uzasadniono dobór cech użytych w dalszych rozważaniach. Zawarto w nim także podstawowe informacje na temat fizjologicznych aspektów generacji mowy ludzkiej wraz z modelem matematycznym opisującym ten proces. Przedstawiono również najpopularniejsze współczynniki, ekstrahowane z sygnału głosu oraz wykorzystywane metody klasyfikacji. Opisano mechanikę powstawania sygnału EKG. Dokonano także analizy dotychczasowych rozwiązań z zakresu metodyki przetwarzania i ekstrakcji cech z przebiegu EKG w biometrycznym rozpoznawaniu osób.

Autorska propozycja multimodalnego systemu biometrycznego została szczegółowo przedstawiona w rozdziale 5. Zamieszczono opis poszczególnych elementów sprzętowych systemu wraz z uzasadnieniem ich użycia. Szczególną uwagę zwrócono na minimalizacją błędów związanych z procesem akwizycji oraz uzyskaniem możliwie jak największej kontroli nad etapem rejestracji. Przedstawiono również autorską koncepcję generacji pobudzeń dźwiękowych i wizualnych oraz pomiaru reakcji użytkownika w odpowiedzi na te wymuszenia. Zarejestrowane odpowiedzi były interpretowane jako biometryki behawioralne.

Rozdział 6 zawiera opis poszczególnych etapów analizy zarejestrowanych próbek sygnałów w celu wyłonienia unikalnych znaczników biometrycznych. Przedstawiono zaimplementowaną metodę detekcji załamków R w sygnale EKG, która umożliwiła określenie interwałów czasowych pomiędzy kolejnymi uderzeniami serca. Dzięki temu określono współczynniki, które zawierały informację o unikalnej reakcji osoby na zadane pobudzenie. Opisano także zaproponowane parametry wyłonione z mowy ludzkiej. Wyznaczone parametry odzwierciedlały umiejętność dopasowania się osoby do usłyszanego dźwięku. Dodatkowo opisano zaimplementowany algorytm wyznaczania wartości współczynników mel-cepstralnych, powszechnie wykorzystywanych w analizie głosu. Przedstawiono metody poszukiwania optymalnych zestawów parametrów oraz zaprezentowano wyniki testów dokładności zaproponowanego rozwiązania.

W rozdziale 7 wyartykułowano koncepcję biometrycznie wzmacnianego systemu kryptograficznego, wykorzystującego autorski system multimodalny oraz strukturę generatora sekwencji psudolosowych MVL-LFSR. Zasugerowano połączenie powszechnych obecnie metod identyfikacji opartych na wiedzy i posiadaniu z wyłonionymi współczynnikami biometrycznymi. Przedstawiono ideę parametryzowania generatora z użyciem wartości rozproszonych pomiędzy wspomniane identyfikatory.

Praktyczną weryfikację koncepcji systemu kryptograficznego przedstawiono w rozdziale 8. Zebrane w trakcie eksperymentów wyniki pomiarowe podzielono na część wzorcową i testową oraz zbadano efektywność dwóch wariantów składania finalnego klucza.

Rozdział 9 podsumowuje rezultaty uzyskane w pracy. Zebrano tu ponadto wnioski płynące z przeprowadzonych badań. Wskazano wady i zalety proponowanych rozwiązań oraz przedstawiono kierunki dalszych badań.

2. Technologie biometryczne i ich podstawowe właściwości - krótka charakterystyka nowoczesnych rozwiązań

W początkowym okresie swojego rozwoju nazwa *biometria* odnosiła się do badania i oceny zmienności cech w populacji organizmów żywych. W tak pojemnej definicji zawierała się zarówno analiza statystyczna sygnałów biomedycznych, których źródłem był człowiek [134], jak również ocena wpływu różnorodnych czynników na uprawy i hodowle rolnicze [153]. Z tym pierwotnym ujęciem spotkać się można już coraz rzadziej. Wpływ na to miał dynamiczny rozwój urządzeń i metod wykorzystywanych w przetwarzaniu sygnałów i obrazów biologicznych, dzięki czemu możliwa stała się ich efektywna akwizycja i analiza. Dlatego też pod współczesną nazwą biometria (lub biometryka [76], raczej w odniesieniu do aktualnej wartości konkretnej cechy biometrycznej) będziemy rozumieli metody automatycznej identyfikacji i weryfikacji osób na podstawie ich unikalnych cech fizjologicznych lub behawioralnych [11, 51].

2.1 Podstawowe techniki biometryczne

2.1.1 Biometria fizjologiczna

Dominującymi współcześnie systemami rozpoznawania lub potwierdzania tożsamości są technologie oparte na cechach fizjologicznych człowieka, takich jak kształt twarzy, odcisk palca czy wzór tęczówki oka. Jest kilka istotnych powodów takiego stanu rzeczy. Pierwszym z nich jest to, że nieinwazyjna rejestracja i analiza fizykalnych cech organizmu ludzkiego jest przedmiotem badań naukowych od wielu lat. Podstawowym deskryptorem jest na przykład używany po dziś dzień w dowodach osobistych znacznik biometryczny wzrostu człowieka, a w mowie potocznej także waga czy obfitość owłosienia. Dalece bardziej dystynktywna daktyloskopia ma po-

nad stuletnią historię, a weryfikacja tożsamości na podstawie odręcznego podpisu sięga nawet czasów starożytnych.

Tak długie zainteresowanie tą grupą technologii biometrycznych wynika z faktu, iż cechy fizjologiczne są względnie łatwo dostrzegalne „gołym okiem" i dzięki temu ich akwizycja oraz analiza jest możliwa przy użyciu prostych narzędzi. Jednakże techniki te mają również swoje wady, wśród których najważniejsza polega na tym, że wzorce biometryczne są „jednorazowe" - skradziona biometryka (na przykład odcisk palca) nie może zostać przywrócona lub zmieniona tak jak hasło lub żeton i dlatego nie może ona zostać ponownie użyta. Należy w tym miejscu podkreślić konsekwencje, jakie płyną z tego faktu. Człowiek, którego cechy biometryczne dostały się w niepowołane ręce, może mieć istotnie ograniczone możliwości w dzisiejszym, zinformatyzowanym społeczeństwie, o ile do zawierania transakcji wymagane będzie użycie technologii biometrycznej.

W poniższej tabeli 2.1 znajduje się zestawienie najważniejszych fizjologicznych cech biometrycznych wykorzystywanych współcześnie w systemach identyfikacji i weryfikacji tożsamości. Oczywiście poniższe zestawienie nie wyczerpuje katalogu elementów fizjologii człowieka przydatnych w biometrii. Dodatkowo systematyczny rozwój urządzeń biometrycznych daje dodatkowy impuls do kreowania nowych podejść do biometrii fizjologicznej. Jako przykład można podać odcisk palca, w którym początkowo skupiano się tylko na wzorze listewek linii papilarnych i ich nieciągłościach (minucje). Zwiększenie rozdzielczości czytników do 500-1000 dpi [115] pozwoliło na wykorzystanie położenia porów [131] do identyfikacji tożsamości, a użycie kilku kamer umożliwiło dokładną rejestrację obrazu 3D palca [20].

Nieostra klasyfikacja technik w tabeli 2.1 służy jedynie wstępnej charakterystyce metod biometrycznych, a użyte deskryptory opisują funkcjonalność w wymiarze fizykalnym i społecznym. Mimo to cytowana tabela stanowi cenne źródło informacji.

2.1.2 Biometria behawioralna

Biometria behawioralna, związana ze sposobem zachowywania się człowieka, wykazuje pewne zalety w stosunku do technologii biometrycznych uznawanych za tradycyjne, wzmiankowanych w punkcie 2.1.1. Wzorce behawioralne rozumiane jako sposób naszego zachowywania się (świadomego lub podświadomego) są zazwyczaj kształtowane długookresowo i mogą być zdeterminowane przez wiele czynników takich, jak środowisko, wychowanie czy edukacja. Co więcej, nasze zachowanie jest modyfikowane wraz z nabywaniem doświadczenia życiowego. Zmienność cechy może być także postrzegana jako wada, ponieważ trudno wyekstrahować jeden stały wzorzec z tak rozmytej próbki. Z drugiej strony biometria behawioralna ma ogromną

Tab. 2.1. Porównanie wybranych technik biometrii fizjologicznej. Oznaczenia: $*$ - niska, $**$ - średnia, $***$ - wysoka (źródło: [53])

Technika	Powszechność	Dystynktywność	Niezmienność	Pobieranie	Wydajność	Akceptowalność	Odporność
Twarz	***	*	**	***	*	***	*
Odcisk palca	**	***	***	**	***	**	***
Geometria dłoni	**	**	**	***	**	**	**
Geometria żył dłoni	**	**	**	**	**	**	***
Tęczówka oka	***	***	***	**	***	*	***
Siatkówka oka	***	***	**	*	***	*	***
Termografia twarzy	***	***	*	***	**	***	***
Zapach	***	***	***	*	*	**	*
DNA	***	***	***	*	***	*	*
Kanał ucha	**	**	***	**	**	***	**

zaletę - w przypadku utraty wzorca człowiek może wykształcić nowe sposoby zachowania, które zostaną użyte do weryfikacji jego tożsamości. Cechy behawioralne mogą być pobrane w nieinwazyjny sposób, często nawet bez wiedzy osoby badanej. Niestety ta grupa biometrii charakteryzuje się niską dystynktywnością w porównaniu z metodami fizjologicznymi. Można zatem przypuszczać, że obszarem zastosowań biometrii behawioralnej będzie raczej weryfikacja niż identyfikacja, wymagająca z definicji znaczącej rozdzielczości. Zestawienie najpopularniejszych technik biometrii behawioralnej przedstawiono za literaturą źródłową w tabeli 2.2.

W dyskusji o taksonomii technik biometrycznych można przyjąć również i takie stanowisko, że niektóre techniki behawioralne mają także swój fizjologiczny kontekst. Ostatecznie dynamika chodzenia immanentnie wiąże się z układem kostno-stawowym lub mięśniowym człowieka, a wydawanie głosu ewidentnie zależy od budowy krtani i strun głosowych oraz rezonatorów. Na uwagę zasługuje wysoki poziom akceptowalności i łatwości pobierania, co wynika prawdopodobnie z powszechnego wymiaru tych czynności. Techniczne atrybuty wyszczególnionych metod współcześnie plasują się na słabych pozycjach, choć z drugiej strony wiadomo, jak niska jest stopa błędów w identyfikacji behawioralnej, wykonywanej autonomicznie przez człowieka z wykorzystaniem jego naturalnych zmysłów.

Tab. 2.2. Porównanie wybranych technik biometrii behawioralnej. Oznaczenia: $*$ - niska, $**$ - średnia, $***$ - wysoka (na podstawie: [53, 149])

Technika	Powszechność	Dystynktywność	Niezmienność	Pobieranie	Wydajność	Akceptowalność	Odporność	Identyfikacja
Dynamika pisania na klawiaturze	$*$	$*$	$*$	$**$	$*$	$**$	$**$	N
Podpis	$*$	$*$	$*$	$***$	$*$	$***$	$*$	T
Mówienie/śpiew	$**$	$*$	$*$	$**$	$*$	$***$	$*$	T
Dynamika chodzenia	$**$	$*$	$*$	$***$	$*$	$***$	$**$	N

Yampolskiy [149] zaproponował następujący podział biometrii behawioralnej na 5 kategorii, ze względu na rodzaj rejestrowanej informacji o użytkowniku:

- wykorzystująca indywidualny styl w czasie takich czynności, jak pisanie czy rysowanie,
- wykorzystująca bezpośrednią obserwację działań człowieka przy komputerze z wykorzystaniem urządzeń wejściowych (mysz, klawiatura) lub użytkowania popularnych aplikacji,
- wykorzystująca pośrednią obserwację niskopoziomowych zdarzeń (zapis w pamięci masowej, wpisy do rejestru itp.), występujących wewnętrznie w komputerze podczas wykorzystywania tego komputera przez człowieka,
- bazująca na zdolnościach motorycznych człowieka (wykonywanie różnych, oczywistych zadań, takich jak śpiewanie czy mówienie),
- czysta biometria behawioralna (z angielskiego „pure behavioral biometrics"), w której pomiary nie są skupione na jednej konkretnej części ciała, ale na pewnych zespołach czynności w ujęciu holistycznym (sposób prowadzenia samochodu).

Przyjęty w niniejszej pracy system biometryczny jako podstawa dyskusji merytorycznej jest rozwiązaniem opartym na wymuszonych reakcjach człowieka w odpowiedzi na określone bodźce zewnętrzne. Osoba badana, poddawana odpowiedniej stymulacji, wykonuje oczekiwane zadania. W konkretnym rozwiązaniu, opisywanym

w dalszych rozdziałach, jest to wydawanie dźwięku, klasyfikowane jako śpiew. System ten wykorzystuje więc biometrię behawioralną, opartą na motoryce człowieka (czwarty punkt powyższego podziału).

2.1.3 Biometria multimodalna

Dotychczasowe poszukiwania „doskonałej" cechy biometrycznej nie przyniosły rezultatu. Wszystkie, obecnie proponowane biometryki, mają swoje wady. Niektóre z nich nie są społecznie akceptowane, inne są niewystarczająco unikalne lub zmienne w czasie. Stąd też pojawił się pomysł na wykorzystanie w systemach biometrycznych kilku koncepcji równocześnie. Dzięki takiemu połączeniu technik, określanemu wspólną nazwą *biometria multimodalna*, rozwiązania wynikowe wykazują nowe zalety w stosunku do systemów opartych na pojedynczych cechach.

Pierwszą, oczywistą i najczęściej najbardziej chyba pożądaną, jest większa dokładność. Heurystyka podpowiada, że cechy behawioralne mogą być klasyfikowane jako zdarzenia niezależne. Na podstawie elementarnych reguł matematycznych prawdopodobieństwo popełnienia błędu jest dane za pomocą następującej zależności:

$$P(A \cap B) = P(A) \cdot P(B), \tag{2.1}$$

gdzie: A, B - zdarzenia niezależne, czyli biometryki, $P(A)$, $P(B)$ błąd danej metody, a $P(A \cap B)$ oznacza wynikowe prawdopodobieństwo błędu klasyfikacji przy użyciu zestawu cech biometrycznych.

Nie każdy system multimodalny łączy cechy statystycznie niezależne. Jako przykład można podać takie rozwiązania, w których występuje ewidentna zależność pomiędzy biometrykami:

- wykorzystanie cech fizycznie ze sobą powiązanych - mowa oraz ruch warg,
- wykorzystanie tych samych danych przez wiele wyodrębnionych klasyfikatorów - analizatory chodu,
- n-krotne użycie różnych próbek tej samej cechy - dwa obrazy tęczówki oka [99].

Dzięki biometrii multimodalnej projektowane rozwiązania cechuje również większa uniwersalność, to znaczy, że można uwzględnić większą część populacji, która w przypadku pojedynczej cechy byłaby nierozróżnialna [120].

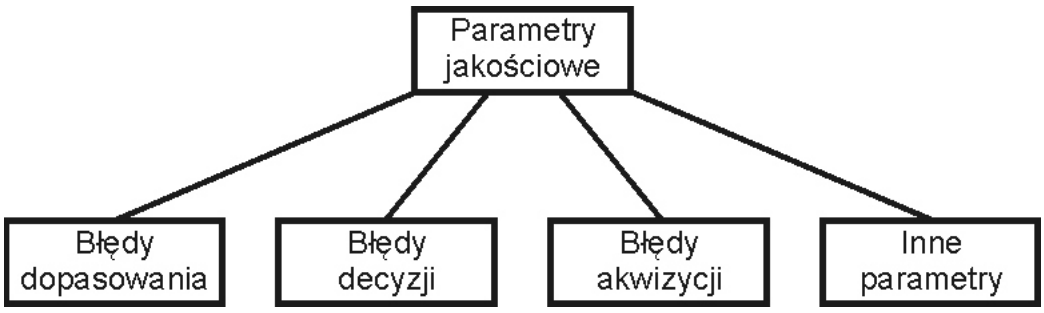
Prawdopodobieństwo skutecznej kradzieży wartości pojedynczej cechy biometrycznej przez potencjalnego intruza jest zależne od wielu trudnych do zdefiniowania czynników. Jest oczywiste, że administrator systemu informatycznego, zawierającego repozytorium wzorców, dołoży starań, by było ono możliwie małe. Można przyjąć, że próba nielegalnego pozyskania dwóch lub więcej cech wymagałaby znacznie

większego wysiłku lub poważniejszych środków. Prawdopodobieństwo sukcesu takiej operacji jest wyrażone również iloczynem prawdopodobieństw zdarzeń, jeśli są one niezależne. Połączenie biometryk podnosi więc poziom bezpieczeństwa, a w przypadku koincydencji cech stosunkowo prostych do przetwarzania (np. obraz twarzy) z takimi, które wymagają do rejestracji specjalistycznego sprzętu (np. sygnał EKG) znacząco wzrasta jakość systemu biometrycznego. Skutkuje to wzrostem poziomu zaufania dla jego użytkowników.

Biometria multimodalna ma również i wady. Najważniejszą z nich jest potrzeba przechowywania wielu wzorców biometrycznych [98]. Ewentualne włamanie i skopiowanie zawartości repozytorium niesie za sobą dużo poważniejsze konsekwencje. Problem odpowiedniego zabezpieczania baz danych próbek stanowi więc nie lada wyzwanie dla administratorów systemów. Dodatkowym problemem, całkowicie nieistotnym w przypadku systemów z pojedynczą cechą, jest potrzeba stworzenia odpowiedniego modułu decyzyjnego, który poprawnie sklasyfikuje otrzymane wzorce. Liczba oraz różnorodność rozwiązań, jakie można znaleźć w literaturze [88, 93, 96, 97, 119], wskazuje jednoznacznie, iż nie jest to zadanie trywialne.

2.2 Wskaźniki jakości technik biometrycznych

Popularność danej metody biometrycznej oraz systemu, który korzysta z tej metody, zależy między innymi od poziomu dokładności najczęściej przeprowadzanych przez system czynności: autentyfikacji i rejestracji użytkowników. Z każdym z tych procesów wiążą się błędy, które mogą wpłynąć na akceptację lub przeciwnie - całkowitą nawet dezaprobatę danego rozwiązania. Na rys. 2.1 przedstawiono umowny podział parametrów jakościowych systemów biometrycznych. Poniżej zostaną zaprezentowane współczynniki należące do poszczególnych grup.



Rys. 2.1. Podział parametrów jakościowych

2.2.1 Błędy dopasowania

Współczynnik fałszywego dopasowania (ang. *False Match Rate - FMR*) jest to oczekiwane prawdopodobieństwo, iż próbka danego użytkownika zostanie sklasyfikowana jako pasująca do losowo wybranego wzorca innego użytkownika znajdującego się w bazie.

Współczynnik fałszywego niedopasowania (ang. *False Non Match Rate – FNMR*) – prawdopodobieństwo, iż próbka danego użytkownika nie zostanie dopasowana do wzorca, pobranego w czasie rejestracji tego samego użytkownika. W przypadku systemów 1:1, parametr FNMR oznacza, że próbka nie została poprawnie zweryfikowana względem własnego wzorca. Natomiast w przypadku systemów 1:N, wskaźnik ten określa prawdopodobieństwo, że dany wzorzec nie zostanie odnaleziony w bazie.

2.2.2 Błędy decyzji

Błędy decyzji są najpowszechniej wykorzystywanymi parametrami jakościowymi, zarówno przez producentów sprzętu, jak i badaczy zajmujących się biometrią. Zostały one tu przytoczone dla porządku oraz w celu wskazania różnicy pomiędzy tą grupą parametrów, a parametrami przedstawionymi w poprzednim akapicie.

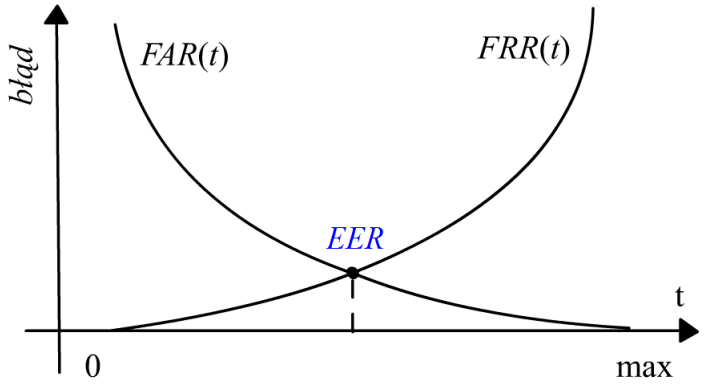
Współczynnik fałszywego odrzucenia (ang. *False Reject Rate – FRR*) – parametr określa procent transakcji, w czasie których dochodzi do niepoprawnego odrzucenia osoby, która poprawnie przedstawiła swoją tożsamość. Transakcja może zawierać jedną lub więcej niepoprawnych prób w zależności od polityki decyzyjnej. Współczynnik ten jest często określany jako błąd I rodzaju.

Współczynnik fałszywej akceptacji (ang. *False Accept Rate – FAR*) – parametr ten określa procent transakcji, w czasie których dochodzi do niepoprawnego zaakceptowania osoby, która nie posiada odpowiednich uprawnień. Transakcja może zawierać jedną lub więcej niepoprawnych prób w zależności od polityki decyzyjnej. Współczynnik ten jest często określany jako błąd II rodzaju .

W literaturze dość często można spotkać się ze stwierdzeniem, że współczynnik FAR (FRR) odpowiada współczynnikowi FMR (FNMR). Należy jednak odróżnić te współczynniki od siebie, ponieważ błędy decyzji mogą powstać zarówno na skutek błędnego dopasowania, jak również z powodu złej akwizycji cechy biometrycznej. Dodatkowo, jak wspomniano w definicjach, FNMR oraz FMR dotyczą pojedynczych dopasowań, natomiast FAR oraz FRR dotyczy transakcji, które mogą zawierać jedną lub więcej prób autentyfikacji użytkownika.

Współczynniki błędnych decyzji oraz błędnego dopasowania zależą silnie od ustawień progu czułości danego systemu. Zbyt wysoki próg zgodności wzorców powoduje, iż wzrasta liczba błędnych odrzuceń (niedopasowań). Z kolei zaś zbyt niski próg

skutkuje dużą liczbą fałszywych akceptacji (dopasowań). Bardzo często charakterystyki błędów FAR oraz FRR są prezentowane na jednym wykresie właśnie w funkcji progu czułości t (rys. 2.2).



Rys. 2.2. Przykładowy wykres współczynników FAR oraz FRR z zaznaczonym punktem EER

Wartości parametrów FRR oraz FAR, podawane w postaci wyodrębnionej z kontekstu przez producentów rozwiązań biometrycznych (zarówno urządzeń jak i algorytmów), nie powinny być traktowane jako wyznaczniki poziomu dokładności tych systemów. Podanie współczynnika FAR bez podania odpowiadającej mu wartości FRR może oznaczać, iż system pomimo niskiego poziomu błędu typu FAR charakteryzuje się błędem FRR na nieakceptowalnym poziomie.

Również podanie obu tych parametrów nie rozwiązuje problemu, ponieważ nie ma dobrej metody na określenie, czy lepszy jest system z wysokim FAR i niskim FRR, czy też system posiadający niską wartość FAR, a wysoką FRR, wobec czego wykorzystuje się dodatkowo jeszcze jeden parametr określający dokładność systemu biometrycznego.

Wartość błędu zrównoważonego (ang. *Equal Error Rate – EER*) to punkt na wykresie, w którym następuje przecięcie charakterystyk parametrów FAR oraz FRR (rys. 2.2). Oznacza to, iż przy takim ustawieniu progu czułości statystycznie taka sama liczba osób zostanie błędnie odrzucona i jak błędnie zaakceptowana. Parametr ten jest bardzo często wykorzystywany do określenia dokładności danego rozwiązania biometrycznego oraz do przeprowadzenia analizy porównawczej kilku urządzeń. Im niższa wartość tego współczynnika, tym urządzenie lub algorytm zyskuje lepszą ocenę.

W niektórych analizach porównawczych systemów biometrycznych bierze się także pod uwagę wartości jednego ze współczynników, przy założonej wartości innego parametru. Na przykład w konkursie FVC 2006 [28] brano pod uwagę m.in. takie

parametry jakościowe, jak FMR100, FMR1000, ZeroFMR i ZeroFNMR, oznaczające odpowiednio: najniższą wartość współczynnika FNMR dla FMR $\leqslant 1\%$, najniższą wartość współczynnika FNMR dla FMR $\leqslant 0{,}1\%$, najniższą wartość FNMR dla zerowej wartości FMR oraz najniższą wartość FMR dla FNMR $= 0\%$. Parametry te mają na celu zaprezentowanie dokładności rozwiązań przy ustalonych warunkach brzegowych.

Wartości parametrów FNMR ora FMR mogą być również zaprezentowane za pomocą charakterystyk. Pierwszym typem jest krzywa ROC (*Receiver Operating Characteristic*), która przedstawia zmierzoną dokładność systemu. Przebieg tej krzywej jest wykreślany jako prawdopodobieństwo weryfikacji (1-FNMR) w funkcji parametru FMR. Innym przykładem charakterystyki jest krzywa DET (*Detection Error Trade-off*). Przedstawia ona współczynniki błędów na obu osiach, dając lepsze wyobrażenie o zachowaniu systemu. Często stosowana jest skala logarytmiczna, dzięki czemu poszczególne systemy są lepiej rozróżnione. Krzywa ta może zostać wykreślona zarówno dla współczynników błędnego dopasowania (FNMR w funkcji FMR) jak również dla współczynników błędnych decyzji (FRR w funkcji FAR). Przykłady takich krzywych można znaleźć w pracy [144].

2.2.3 Błędy akwizycji

Przy wyborze konkretnego rozwiązania w pierwszej kolejności brane są pod uwagę parametry określające dokładność systemu biometrycznego. Jednak przydatność systemu może zostać zakwestionowana w przypadku, gdy użytkownik nie jest w stanie się w nim zarejestrować lub też w późniejszym użytkowaniu systemu wystąpią problemy na skutek niemożności pobrania próbki o odpowiedniej jakości. Poniżej przedstawiono dwa parametry opisujące jakość procesów akwizycji próbki.

Niepowodzenie rejestracji (ang. *Failure to Enrollment Rate - FTE*) – odsetek populacji, dla której system nie jest w stanie wygenerować powtarzalnego wzorca. Błąd ten może wynikać:

- ze zbyt małego zróżnicowania cech biometrycznych,
- ze znacznego zniekształcenia biometryk,
- z braku odpowiedniego przeszkolenia użytkowników systemu, którzy nie eksponują odpowiednio dane cechy,
- z niemożności wygenerowania próbki o wystarczającej jakości do procesu rejestracji.

Niepowodzenie pobrania próbki (ang. *Failure to Acquire Rate - FTA*) – odsetek transakcji, dla których system nie był wstanie pobrać i wyekstrahować odpowiedniej informacji z biometrycznej próbki. Parametr ten może zależeć od przyjętego progu jakości pobieranych próbek.

2.2.4 Podsumowanie problematyki oceny jakości systemów biometrycznych

Wśród pozostałych parametrów, nie należących do żadnej z wyżej wymienionych grup, należy przede wszystkim wspomnieć o złożoności czasowej procesów rejestracji oraz autentyfikacji użytkowników. W szczególności powinien być brany pod uwagę czas potrzebny na weryfikację lub identyfikację użytkownika. Jest to kluczowy, z funkcjonalnego punktu widzenia, parametr doboru rozwiązania biometrycznego do miejsca jego zastosowania.

Przedstawione powyżej parametry nie stanowią zamkniętego zbioru możliwych wskaźników jakościowych, lecz tylko niewielką część zestawów współczynników spotykanych w literaturze. Ich mnogość jest głównym problemem w jednoznacznej ocenie jakościowej rozwiązań proponowanych zarówno przez naukowców jak i firmy komercyjne. Innym problemem jest niejednoznaczność definicji stosowanych w różnych publikacjach oraz tworzenie zupełnie nowych, które mają na celu pokazanie danego rozwiązania w pozytywnym świetle. Przykłady wspomnianych różnic zostały opisane w [79]. Podejmowane są prace na rzecz standaryzowania oceny systemów biometrycznych prowadzonych przez takie organizacje jak NIST [102], NCITS [101] czy ISO. Jednak według wiedzy autora nie ma na tę chwilę jednego obowiązującego standardu.

2.3 Obszary stosowalności

Weryfikacja tożsamości jest w chwili obecnej jednym z kluczowych elementów społeczeństwa informacyjnego. Stąd też wynika szerokie zainteresowanie systemami biometrycznymi, które umożliwiają potwierdzenie deklaracji uczestnika transakcji. Biometria wkracza w coraz to nowe dziedziny zastosowań i obecnie bardzo trudno znaleźć miejsca, w których nie może zostać ona wykorzystana [136]. Obszary zastosowań technik biometrycznych można podzielić na trzy główne kategorie [15, 113]:

- komercyjne,
- rządowe,
- sądownicze.

Policja jako pierwsza zwróciła uwagę na możliwość wykorzystania biometrii (głównie odcisków palców oraz DNA) do identyfikacji przestępców, jak również ofiar przestępstw lub wypadków. Utworzono centralne bazy danych odcisków na początku w postaci papierowych kartek (analogowych), a obecnie jako cyfrowe obrazy, które są automatycznie przeszukiwane za pomocą systemów AFIS (ang. *Automated Fingerprints Identification System*). Dzięki długiej historii to właśnie systemy AFIS są dominującymi obecnie rozwiązaniami i w najbliższych latach sytuacja ta prawdopodobnie nie ulegnie znaczącym zmianom [111].

Rządowe zastosowania biometrii skupiają się głównie na wszelkiego rodzaju dokumentach tożsamości (dowody osobiste, paszporty, prawa jazdy...) oraz procesach związanymi z kontrolą tych dokumentów, w szczególności na przejściach granicznych, lotniskach lub w przypadku udzielania pomocy społecznej. Przykładem globalnego wykorzystania biometrii są paszporty biometryczne, które w chwili obecnej zostały wprowadzone w całej Unii Europejskiej, części Azji, Australii, USA jak i w wielu innych krajach [148]. Zawierają cyfrową informację o twarzy, a często również o odciskach palców, tęczówce lub inny rodzaj biometrii zgodnie ze standardem opracowanym przez ICAO [39].

Najbardziej różnorodny obszar zastosowań technik biometrycznych jest bez wątpienia związany z ich komercyjnym użyciem. Systemy biometryczne pełnią rolę „inteligentnych" zamków, które kontrolują dostęp do newralgicznych miejsc przedsiębiorstwa, a równocześnie pozwalają na rejestrację czasu pracy [110] (niemożliwym staje się tak zwane „odbicie karty" za inną osobę). Są one również szeroko wykorzystywane w bankowości przy zdalnym dostępie (głos, dynamika pisania na klawiaturze [136]), a także przy autoryzacji transakcji lokalnie (bankomaty, okienko bankowe). Użytkownikami biometrii są nie tylko osoby dorosłe, ale także dzieci. W Wielkiej Brytanii wprowadzono systemy biometryczne do szkół, dzięki czemu można kontrolować obecność dzieci na zajęciach, jak również usprawnić takie czynności jak płatność za posiłki w stołówkach lub wypożyczanie książek w bibliotece [25, 138]. Biometria wkracza także do codzienności przeciętnych użytkowników komputerów, które często posiadają możliwość autoryzacji dostępu poprzez weryfikację odcisku palca lub obrazu twarzy użytkownika.

Powyższy rozdział nie wyczerpuje wszystkich zastosowań technik biometrycznych, które są obecnie wykorzystywane. Gwałtowny rozwój tej dziedziny powoduje, iż każde zestawienie w chwili druku jest już w jakimś wymiarze nieaktualne. Celem autora nie była próba marketingowej analizy tematu, lecz raczej przybliżenie czytelnikowi złożoności i różnorodności problematyki.

2.4 Psychologiczne bariery biometrii

Wykorzystanie biometrii niesie ze sobą wiele korzyści dla przeciętnego człowieka, zarówno finansowych (brak fizycznych identyfikatorów, które można zgubić) jak i użytkowych (szybsze procedury obsługi klientów). Biometria daje nam bowiem szanse na zachowania klucza dostępowego „przy sobie". W każdym innym systemie, ktoś inny (administrator systemu, bank) wymaga od nas zdeponowania swoich uprawnień.

Jednak pomimo wszystkich niezaprzeczalnych zalet identyfikatorów biometrycznych, powszechne stosowanie biometrii (dostępnej w zastosowaniach cywilnych od ponad 20 lat) napotyka na problemy, które nie istniały w przypadku tradycyjnych metod rozpoznawania tożsamości. Jednym z najważniejszych jest brak społecznej akceptacji dla rozwiązań biometrycznych wynikający przede wszystkim z bariery psychologicznej oraz niezrozumienia korzyści płynących z ich użycia [35].

Obawy mogą wynikać z powodu złych skojarzeń związanych z niektórymi typami biometrii, jak na przykład odcisk palca, DNA czy obraz twarzy. Inne przyczyny niechęci mogą być związane z potrzebą kontaktu fizycznego z czytnikami biometrycznymi, co w niektórych krajach, takich jak Japonia, jest wielce niepożądane w związku z dużą dbałością o higienę osobistą [121].

Wykorzystanie wzorców w innych celach, niż tylko do weryfikacji tożsamości, przez podmioty uprawnione do ich gromadzenia, również może być powodem braku zgody na powszechne stosowanie biometrii. Próbki biometryczne można w pewnych przypadkach wykorzystać do poszukiwania korelacji pomiędzy cechami a stanem medycznym osoby, w celu oceny poziomu ryzyka polisy ubezpieczeniowej [113].

Część lęków związana jest ze wzmiankowaną powyżej jednorazowością wzorców fizjologicznych. Tego typu wzorce, jak na przykład obraz twarzy, mogą zostać pobrane nawet bez wiedzy użytkownika i wykorzystane bez jego zgody. Co więcej, wiele osób bardzo ceni sobie swoją prywatność lub też ukrywa prawdziwą tożsamość z obawy o swoje życie. W przypadku upowszechnienia takich systemów biometrycznych jest to bardzo trudne, gdyż każdy ruch człowieka może być śledzony [52], a tożsamość w dowolnym momencie odkryta. Wydaje się jednak, iż wraz z rosnącym poziomem wiedzy o systemach biometrycznych grupa osób, które będą skłonne do ich użytkowania, a nawet będą się domagały ich instalacji, stale się poszerza. Świadomość korzyści płynących z użycia biometrii oraz wad tradycyjnych systemów weryfikacji przekonuje kolejnych sceptyków do rozwiązań, które pozwolą w sposób jednoznaczny potwierdzić swoją tożsamość [12]. W przypadku bariery psychologicznej, dyskusja o racjonalnych przesłankach i cechach pozytywnych jest oczywiście niezbędna, lecz należy uwzględnić długi czas kreowania przemian świadomości zbiorowej.

3. 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.

4. Biometryczne podstawy koncepcji badawczej

Sformułowanie problemu naukowego, stanowiące meritum 3. rozdziału pracy, określa również bezpośrednio tę subdyscyplinę biocybernetyki i inżynierii biomedycznej, która stanowi oparcie dla prowadzonych badań. Twórczą część dysertacji stanowi analiza możliwości wykorzystania wielokanałowej biometrii o zdywersyfikowanym pochodzeniu.

Jednym z najciekawszych kierunków aplikacyjnego rozwoju tej dziedziny nauki wydaje się być kryptografia biometryczna, łącząca w sobie zalety obu dziedzin składowych. Aparat algebraiczny, stanowiący matematyczny grunt kryptografii, pozwala na uzyskanie takiego stopnia złożoności kodów szyfrujących, który jest adekwatny dla rozważanej aplikacji. Z drugiej strony parametr biometryczny, zależny immanentnie od dysponenta szyfru, pozwala na unikalne rozproszenie widma informacji kodowej, prowadząc do takiego zróżnicowania wynikowych ciągów kodowych, które zasadniczo wyróżnia uprawnionych użytkowników zabezpieczanego systemu. W przedmiotowej literaturze spotyka się równie często pojęcie „biokryptografia", które w niniejszym opracowaniu stosowane bywa zamiennie dla kryptografii biometrycznej. Wydzielonym zagadnieniem badawczym jest połączenie zjawiska absolutnie deterministycznego, jakim jest kod algebraicznie definiowany, oraz rozmytej z zasady informacji o biologicznym pochodzeniu.

4.1 Wprowadzenie do kryptografii biometrycznej

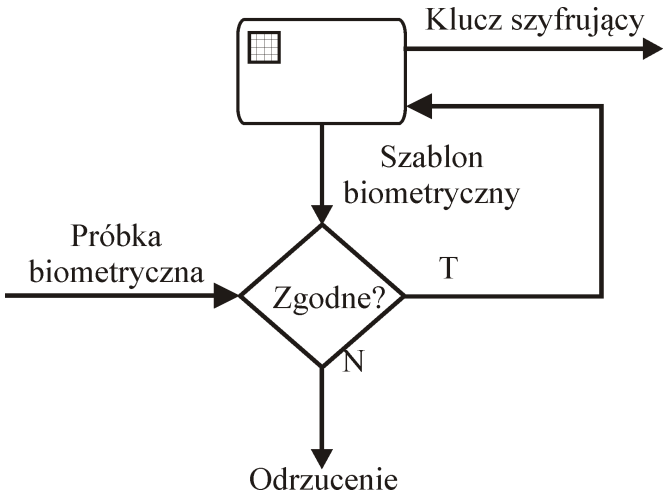
Podstawowym problemem klasycznych systemów kryptograficznych jest fakt, iż w rzeczywistości systemy te autoryzują klucz kryptograficzny, a nie tożsamość jego posiadacza. Istnieje więc, przynajmniej w teorii, możliwość zaprzeczenia przez osobę, przypisaną do danego klucza, podpisanych w ten sposób dokumentów. Jednak, zgodnie z ustawą o podpisie elektronicznym [140], właściciel klucza jest odpowiedzialny za każde jego użycie, co wyklucza praktycznie możliwość zakwestionowania złożonej sygnatury. Takie przepisy nakładają na posiadacza obowiązek bezpiecznego przechowywania i użytkowania fizycznych kluczy szyfrujących. Skutkuje to niechęcią oraz małą popularnością kwalifikowanych podpisów elektronicznych wśród osób prywatnych. Powyższe problemy nie występują w przypadku identyfikatorów biometrycznych, a rozwój nowoczesnych metod autentyfikacji w oparciu o biometrię

przyczynił się do powstania koncepcji połączenia mocnych stron obu dziedzin. Idealny bioklucz kryptograficzny musiałby posiadać następujące właściwości [139]:

- **unikalność** - nie może być identyczny z kluczami innych użytkowników,
- **reprodukowalność** - możliwe jest stworzenie wielu ciągów szyfrujących na podstawie tej samej cechy,
- **bezpieczeństwo** - niemożliwe jest odtworzenie oryginalnej wartości cechy z klucza kryptograficznego,
- **dokładność** - usunięcie pewnych punktów charakterystycznych cechy nie powinno zmniejszyć entropii cechy.

Okazuje się, iż opracowanie metod, które pozwoliłyby na osiągnięcie wszystkich powyższych celów równocześnie nie jest zadaniem trywialnym. Dlatego też istnieje co najmniej kilka sposobów połączenia biometrii i kryptografii [82, 83, 90, 126]. Metody najbardziej interesujące i rozpowszechnione zostaną opisane poniżej.

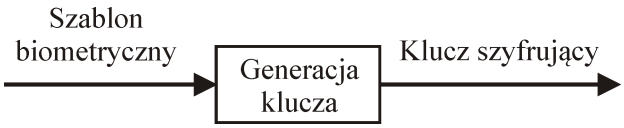
Jednym z najprostszych sposobów wykorzystania biometrii w kryptografii jest zabezpieczenie kluczy szyfrujących za pomocą próbek biometrycznych. Użycie kluczy możliwe jest tylko w wypadku pozytywnej weryfikacji posiadacza klucza na podstawie przedłożonej cechy [114, 129] (rys. 4.1). Takie podejście jest najbardziej zbliżone do klasycznych systemów biometrycznych, z ich wszystkimi wadami i zaletami. Dodatkowo możliwe jest wygenerowanie dowolnej liczby kluczy, co ma niebagatelne znaczenie w przypadku ich ujawnienia. Z drugiej jednak strony w takim rozwiązaniu klucz nie jest w żaden sposób powiązany z cechą biometryczną posiadacza, a próbka biometryczna musi być przechowywana na fizycznym nośniku (karta, komputer, serwer...), a przez to może być narażona na potencjalną kradzież.



Rys. 4.1. Zabezpiecznie klucza za pomocą biometryki

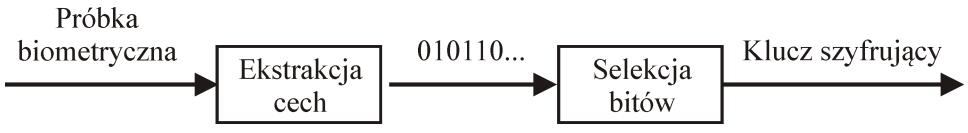
Pierwszą propozycję powiązania próbki biometrycznej z kluczem szyfrującym przedstawił i opatentował Bodo [14]. W tym rozwiązaniu cały szablon biometryczny

lub jego część jest kluczem (rys. 4.2). Jednak w przypadku utraty klucza bezużyteczna staje się także wykorzystana cecha. Niemożliwa jest również okresowa zmiana kluczy, co jest polityką często zalecaną i stosowaną w klasycznych systemach zabezpieczeń. Podobna koncepcja ekstrakcji klucza bezpośrednio z cechy zaproponowana została w [54]. W odróżnieniu od poprzedniej, klucze kryptograficzne mogą zostać zmienione. Poważną wadą tej propozycji jest założenie o stuprocentowej powtarzalności próbki otrzymanej w procesie akwizycji. W warunkach rzeczywistych takie ograniczenie może okazać się zbyt restrykcyjne.



Rys. 4.2. Schemat wykorzystania szablonu biometrycznego jako klucza szyfrującego

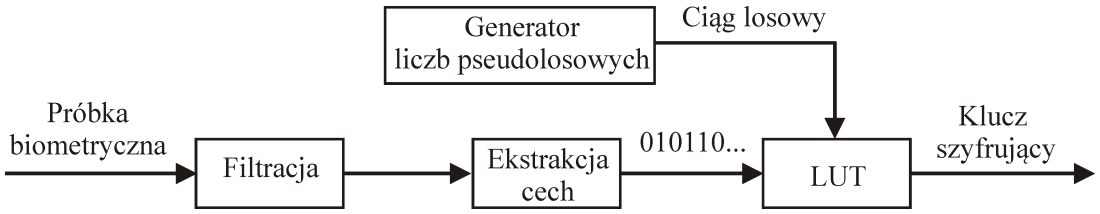
Inną propozycją jest połączenie informacji biometrycznej z pseudolosowym ciągiem generowanym dla każdego użytkownika (rys. 4.3). Istnieje wiele różnych podejść do tego zagadnienia. Jednym z nich jest wykorzystanie pewnych ściśle określonych bitów szablonu biometrycznego pobranego w procesie rejestracji użytkownika w systemie. W pracy [42] wykorzystuje się poufny algorytm służący do ustalenia bitów w szablonie, służących do utworzenia klucza. Wadą tego rozwiązania jest to, iż klucz szyfrujący jest zawsze kodowany przez te same bity z szablonu biometrycznego. Potencjalny napastnik może zdobyć wystarczającą liczbę różnych kluczy i na tej podstawie określić algorytm szyfrujący. Inne podejście przedstawione zostało w pracy [50], gdzie użyto dwóch kluczy szyfrujących, z których jeden s_1 był funkcją skrótu SHA-1 szablonu biometrycznego (odcisku palca oraz tęczówki oka), natomiast drugi s_2 był psudoprzypadkowym ciągiem liczb. System kryptograficzny wykorzystywał architekturę PKI, w której klucz publiczny generowany był na podstawie wspomnianych wcześniej kluczy prywatnych, a jego bezpieczeństwo było zapewnione do momentu ujawniania klucza s_2. Według przedstawionej koncepcji, próbka biometryczna powinna być przechowywana na karcie, co w znaczący sposób obniża bezpieczeństwo tego rozwiązania.



Rys. 4.3. Generacja klucza kodowego na podstawie wybranych bitów próbki biometrycznej

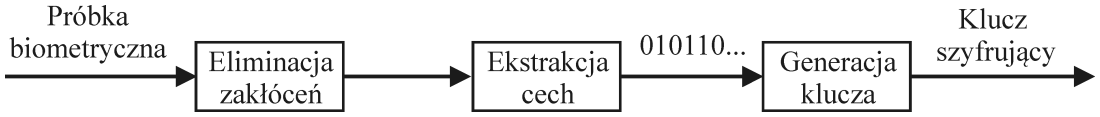
W pracach [18, 127, 128] przedstawiono rozwiązanie, w którym szablon biometryczny zostaje powiązany z ciągiem pseudolosowym w procesie rejestracji użytkownika w systemie (rys. 4.4). Tak utworzony bezpieczny blok danych nazwano

bioscrypt. Próbka biometryczna zostaje poddana transformacji Fouriera w celu redukcji wpływu zmiany położenia prezentowanej cechy, a następnie przefiltrowana specjalnie zaprojektowanym filtrem w celu optymalnej redukcji błędów. Klucz uzyskany w wyniku filtracji zostaje powiązany z blokiem bioscrypt poprzez nadmiarową tablicę LUT (ang. *LookUp Table*).



Rys. 4.4. Schemat powiązania biometrii z ciągiem pseudolosowym

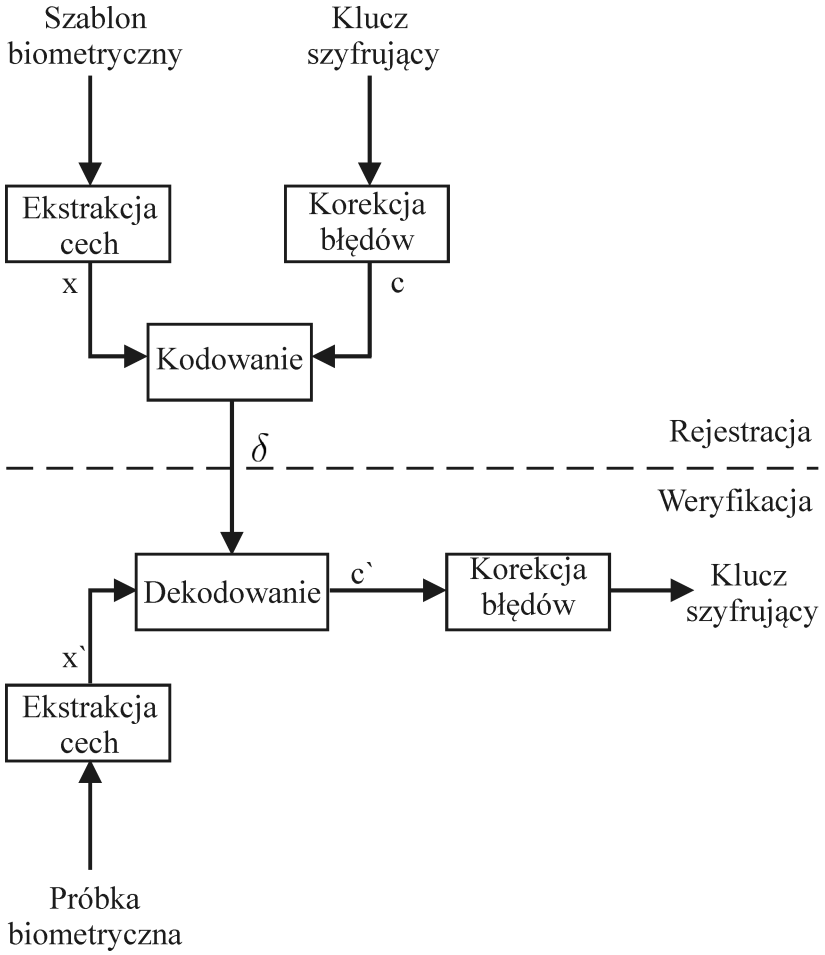
Inne podejście do kryptografii biometrycznej zakłada generację klucza szyfrującego bezpośrednio z próbki biometrycznej (rys. 4.5). W takich rozwiązaniach jednym z etapów przetwarzania jest eliminacja zakłóceń w pobranym szablonie, powstałych w wyniku niedoskonałego procesu akwizycji. W pracach [130, 137] zaproponowano wykorzystanie kluczy tworzonych na podstawie szablonu, w celu ochrony poufnego PIN-u. Przedstawiona koncepcja wykorzystuje transformatę Fouriera do zakodowania próbki biometrycznej, która może być zaimplementowana z użyciem urządzeń optycznych lub cyfrowych.



Rys. 4.5. Wykorzystanie szablonu biometrycznego jako klucza szyfrującego

Monrose i in. [92] zaproponowali wykorzystanie dynamiki pisania na klawiaturze (interwały pomiędzy naciśnięciami klawiszy, czas wciśnięcia klawisza) w celu wzmocnienia hasła podanego przez użytkownika. W innej pracy tych autorów [91] przedstawiono z kolei generację kluczy z sygnału głosu. Z zarejestrowanych próbek wyznaczano współczynniki cepstralne, które określały położenie w przestrzeni. Na podstawie przynależności do odpowiedniego centroidu (wycinka przestrzeni) generowany był klucz szyfrujący.

Wyłonienie niezmiennej reprezentacji próbki biometrycznej w celu wykorzystania jej do utworzenia kluczy kodowych skutkuje redukcją przestrzeni cech. To z kolei powoduje, iż prawdopodobieństwo wygenerowania identycznego klucza dla różnych osób znacząco rośnie. Ten problem można rozwiązać poprzez generację ciągów szyfrujących bezpośrednio z zaszumionej próbki cechy (rys. 4.6). Takie podejście zostało zaproponowane w pracy [56]. Koncepcja nazwana *fuzzy commitment scheme* polega na wygenerowaniu losowego klucza c, utworzeniu szablonu biometrycznego x, a następnie obliczany jest offset $\delta = c - x$. Jeżeli próbka biometryczna x' będzie

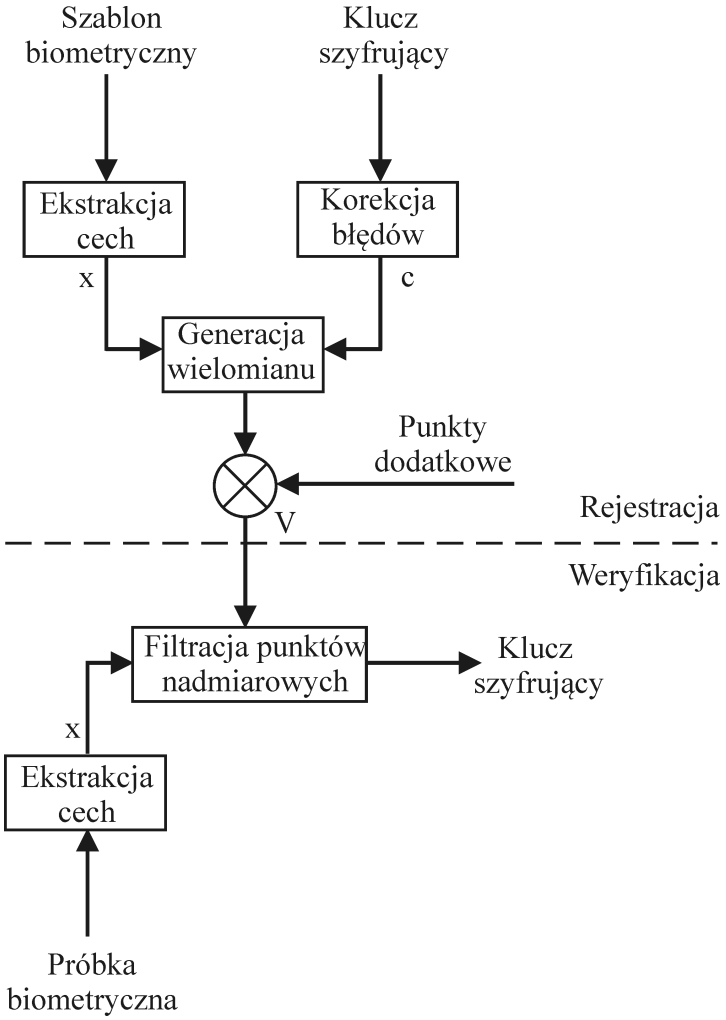


Rys. 4.6. Generacja klucza kodowego z użyciem metody *fuzzy commitment scheme*

wystarczająco podobna do x, to uzyskana wartość $h(c') = h(c)$, gdzie $c' = \delta + x'$, umożliwia ekstrakcję klucza kodowego.

Powyższe podejście zostało rozwinięte w pracy [55] pod nazwą *fuzzy vault*. Koncepcja ta może zostać wykorzystana do przechowywania poufnych informacji. Dane mogą zostać odszyfrowane za pomocą dwóch wystarczająco podobnych kluczy A i B. Informacja jest kodowana za pomocą losowo wygenerowanego wielomianu $p(x)$. W oparciu o klucz kodowy oraz wspomniany wielomian generowane są punkty $(x_i, y_i) = (a(i), p(a(i)), a(x) \in A$ oraz dodatkowe punkty, które nie zależą od wielomianu, a mają za zadanie jedynie ukryć jego postać (rys. 4.7). Odtworzenie zakodowanej informacji z użyciem wystarczająco podobnej próbki jest możliwe dzięki wykorzystaniu kodów korekcyjnych (w szczególności zmodyfikowanej wersji algorytmu Reed-Salomon).

Koncepcja *fuzzy vault* i późniejsze jej modyfikacje wydają się być w chwili obecnej najczęściej stosowanym podejściem w dziedzinie kryptografii biometrycznej (wnioskując po liczbie publikacji, w których została ona wykorzystana [19, 128]).



Rys. 4.7. Generacja klucza kodowego z użyciem metody *fuzzy vault*

Aspekt bezpieczeństwa systemów biokryptograficznych jest zagadnieniem niezwykle istotnym, z racji użycia wrażliwych danych biometrycznych. Analiza omówionych powyżej rozwiązań niestety nie pozwala na stwierdzenie, iż systemy te są całkowicie bezpieczne. W pracach [2, 122] przedstawiono metody ataku na systemy oparte zarówno na koncepcji [127] jak i na schemacie *fuzzy vault*. W pracy [61] autorzy zrealizowali eksperymentalny atak (nazwany *correlation attack*) na system korzystający ze schematu *fuzzy vault* i wykazali, iż byli w stanie odszyfrować ponad 59% wiadomości (w bazie zawierającej ich około 400) za pomocą różnej postaci pojedynczego odcisku palca.

Propozycje zabezpieczenia próbek biometrycznych w systemach kryptograficznych obejmowały między innymi niszczenie próbki po procesie kryptografii [151], możliwość wielokrotnego wykorzystania cechy [124], oraz wykorzystanie dodatkowej funkcji mieszającej, która powinna uodpornić schemat *fuzzy vault* przed atakiem wspomnianym w poprzednim akapicie [108].

4.2 Kryteria wyboru cech biometrycznych

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. Należy także uwzględnić fizjologiczną naturę niektórych cech znacząco ograniczającą ich stosowalność z powodu względnej podatności na kradzież i wynikającej stąd jednorazowości. 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 (lub więcej) biometryk, ponieważ ich kombinacja pozwala na osiągnięcie wszystkich powyższych założeń równocześnie. Dodatkowo wykorzystanie biometrii multimodalnej umożliwia uzyskanie efektu, o którym mowa była w punkcie 2.1.3.

W pracy [74] wskazano na znaczny potencjał poniższych cech:

- tęczówka oka,
- odcisk palca,
- głos.

Stwierdzono również, iż przy odpowiedniej parametryzacji próbek biometrycznych wspomnianych identyfikatorów możliwe będzie wyłonienie niewielkiego, kilkubitowego zestawu informacji dla dalszego wykorzystania w aplikacji kryptograficznej.

W pracy [95] rozważano wykorzystanie wzoru tęczówki oka do parametryzowania ciągów pseudolosowych. Niemniej jednak zwrócono uwagę na dużą zmienność tej biometryki, a co za tym idzie trudność w wyłonieniu niezmiennego markera biometrycznego. W tej samej pracy zaproponowano wykorzystanie odcisku palca, w celu ustalenia stanu początkowego generatora kluczy szyfrujących. Z uwagi jednak na fizjologiczny charakter tejże biometryki w niniejszej pracy nie podjęto się kontynuacji tegoż podejścia.

Ostatnią rozważaną we wspomnianych pracach cechą był sygnał głosu. Wskazano na łatwość akwizycji oraz różnorodność metod analizy w celu wyłonienia odpowiedniego zestawu niezmiennych wartości. Z drugiej jednak strony duża zmienność warunków akwizycji spowodowała, iż w pracy [95] po wstępnych analizach uznano tę cechę ze niewłaściwą w zastosowaniach kryptograficznych. Należy jednak podkreślić, iż biometryka głosu jest powszechnie akceptowaną metodą weryfikacji tożsamości, a dodatkowo zawiera informację zarówno o cechach fizjologicznych jak i cechach behawioralnych osoby badanej. Wydaje się również, iż odpowiednio dobrane warunki akwizycji mogą implikować wysoką stabilność pomiarów. Co więcej, za pomocą odpowiednio dobranego scenariusza eksperymentu możliwe jest zarejestrowanie dźwiękowej odpowiedzi człowieka na zadane wymuszenie. Oczywiście ten rodzaj biometrii nie spełnia wszystkich przyjętych powyżej założeń. Na przykład nietrudno sobie wyobrazić nagranie próbki głosu, a następnie odtworzenie jej w odpowiednim momencie, w celu nieuprawnionego dostępu do danego systemu, ponieważ fizyczna obecność osoby nie jest weryfikowana. Dlatego też należało dobrać dodatkową biometrykę, która uzupełni braki sygnału głosu, a jednocześnie sama będzie źródłem cech biometrycznych.

Jednoznaczną i niepodważalną informację o tym, czy dana osoba żyje, dają nam dwa sygnały biomedyczne, które są powszechnie wykorzystywane w diagnostyce medycznej, a ostatnio także w biometrii. Są to:

- czynność elektryczna serca,
- czynność elektryczna mózgu.

Badania diagnostyczne rejestrujące powyższe sygnały to odpowiednio elektrokardiografia (EKG) w przypadku sygnału elektrycznego serca oraz elektroencefalografia (EEG) dla sygnału pochodzącego z mózgu.

Wykorzystanie sygnału EEG w biometrii zostało zaproponowane stosunkowo niedawno, a wstępne wyniki wydają się być obiecujące [106]. Jednak pomiaru sygnału EEG dokonuje się tylko na powierzchni skóry czaszki, a liczba elektrod niezbędnych do przeprowadzenie tego badania wynosi 21 [1, 41], aczkolwiek zaproponowano również rozwiązanie wykorzystujące mniejszą liczbę podłączeń [117]. W praktycznych zastosowaniach ten rodzaj biometrii może napotykać na bardzo, wydawałoby się, prozaiczne problemy. Osoby, które poświęcają dużo czasu oraz znaczne środki na ułożenie fryzury z całą pewnością odmówią nałożenia ściśle przylegającego czepka, a nawet zwykłej czapki zawierającej elektrody. Dodatkowo, tego typu badanie kojarzy sie często negatywnie z różnego rodzaju zaburzeniami natury psychicznej.

Wymienionych powyżej wad nie posiada badanie EKG. Może ono być wykonywane w sposób dużo mniej inwazyjny aniżeli badanie EEG dzięki mniejszej liczbie elektrod oraz możliwości podłączenia ich na nadgarstkach lub kostkach. Wraz ze wzrostem liczby chorób serca zwiększa się także powszechność tego badania, a co za tym idzie także społeczna akceptacja. Ostatnie prace z zakresu biometrii wskazują także na osobniczą unikalność przebiegu EKG oraz jego stabilność w dłuższym

okresie czasu. Przedstawione metody analizy z zakresu klasycznego przetwarzania sygnału mają już ugruntowaną pozycję. Szerzej zostaną one opisane w rozdziale 4.4.

Na podstawie powyższych rozważań zdecydowano się ostatecznie na wykorzystanie dwóch biometryk: sygnału głosu oraz zapisu elektrycznej czynności serca, dzięki czemu spełnione zostaną wszystkie przyjęte powyżej założenia.

4.3 Sygnał głosu - analiza właściwości wybranej biometryki behawioralnej

Mowa ludzka niesie niezwykle złożoną informację pozwalającą zrozumieć nie tylko sens wypowiedzi, ale także umożliwia ocenić mówcę pod względem płci, wieku, stanu zdrowia, pochodzenia czy też stanu emocjonalnego osoby mówiącej. Co więcej, osoby nam znane są rozpoznawane prawie natychmiast po wypowiedzeniu kilka, a czasem nawet tylko jednego słowa. Narząd słuchu człowieka radzi sobie z tym zadaniem niemal doskonale, bez względu na warunki towarzyszące wypowiedzi.

Urządzenia techniczne radzą sobie niestety z tym problemem dużo gorzej. Wielokrotne badania nad możliwością wykorzystania sygnału mowy w celach biometrycznych zaowocowały jednak rozwiązaniami, które pozwalają z dużym prawdopodobieństwem automatycznie rozpoznawać ludzi.

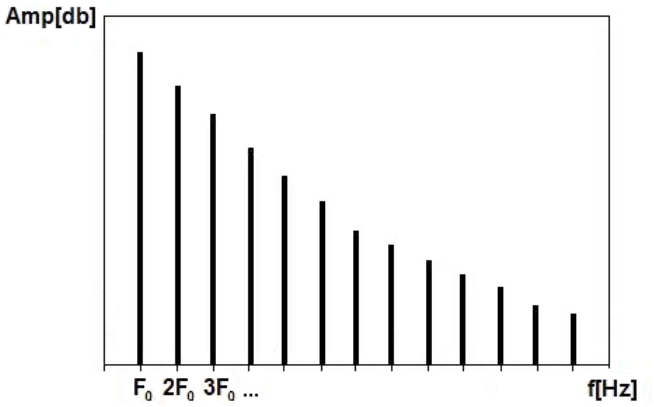
Poniżej omówione są elementy wpływające na generację mowy ludzkiej. W tym rozdziale przedstawiono również przegląd dotychczasowych rozwiązań w dziedzinie biometrycznego wykorzystania sygnału głosu.

4.3.1 Powstawanie sygnału mowy

Na charakterystykę sygnału mowy człowieka mają przede wszystkim wpływ dwa aspekty:

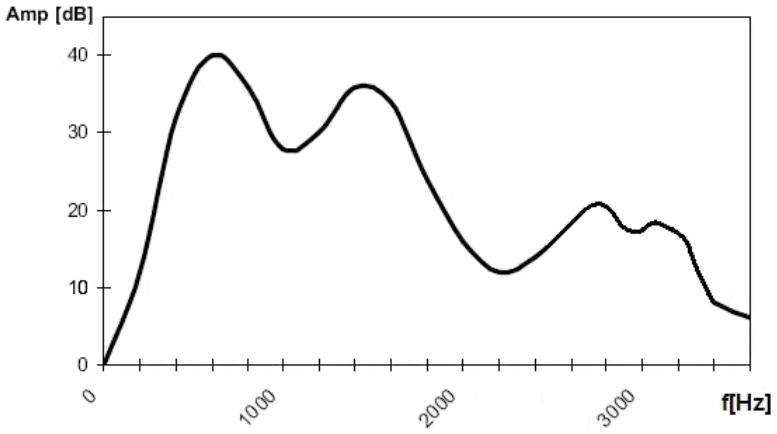
- fizyczny,
- behawioralny.

Aspekt fizyczny zależy w głównej mierze od budowy narządu mowy: gardła, jamy nosowej oraz jamy ustnej. Uwzględniając wszystkie elementy, które biorą udział w procesie tworzenia mowy, należy również wymienić płuca, oskrzela oraz tchawicę. Organy te dostarczają strumień powietrza do krtani. Generacja dźwięku odbywa się poprzez drgania fałd głosowych zwanych również potocznie strunami głosowymi. Są one źródłem sygnału dla głosek dźwięcznych („a”, „i”, „o”,...). Widmo tonu krtaniowego jest okresowe i pomimo, że kolejne harmoniczne są tłumione około 12dB/oktawę (rys. 4.8), to możliwe jest wydobycie nawet do trzydziestej harmonicznej. W przypadku mowy bezdźwięcznej struny głosowe są rozwarte i nie stanowią przeszkody dla strumienia powietrza. Widmo tonu krtaniowego dla głosek bezdźwięcznych posiada charakterystykę szumu białego [133]. Częstotliwość podstawowa



Rys. 4.8. Widmo tonu krtaniowego

mowy dźwięcznej F_0 jest tylko jedną z wielu składowych sygnału akustycznego, który dociera do słuchacza. Jednak determinuje ona odbiór dźwięku jako niski lub wysoki. Bez względu na rodzaj mowy, sygnał ze strun głosowych jest następnie modulowany w kolejnych częściach traktu głosowego takich jak język, języczek, podniebienie twarde i miękkie, zęby i wargi, a w przypadku niektórych dźwięków także nozdrzy [59]. Dźwięk pochodzący z krtani zostaje odbity w wymienionych narządach, co powoduje wzmocnienie niektórych harmonicznych, a tłumienie innych. Wpływ traktu głosowego na sygnał dźwiękowy jest najczęściej modelowany jako filtr liniowy, który posiada cztery maksima zwane formantami (rys. 4.9).



Rys. 4.9. Charakterystyka filtra traktu głosowego

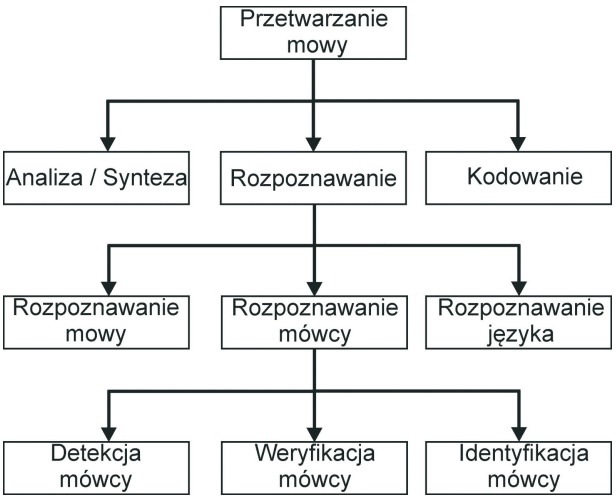
Wyższe częstotliwości sygnału mowy odpowiedzialne są za treść przekazywanej informacji, a także za barwę głosu. Profesjonalni śpiewacy generują dźwięki, które posiadają o wiele bogatszą barwę. Jej bogactwo zależy w dużym stopniu od liczby znaczących harmonicznych oraz tworzonych przez nie formantów. Szczególnie uwypuklone jest pasmo w zakresie ok. 3000 Hz. Jednak w przypadku sopranistek, wyższe formanty (odpowiedzialne za przekaz treści) wykraczają poza zakres sły-

szalności człowieka, przez co głoski są nierozróżnialne dla słuchacza. Wynika to z charakterystyki ucha ludzkiego, która nie jest jednorodna w całym paśmie słyszalności. Człowiek jest bardziej czuły na dźwięki w zakresie średnich częstotliwości (ok. 1000 Hz), natomiast w zakresie niskich (od 20 Hz do 100 Hz) oraz wysokich częstotliwości (powyżej 10000 Hz) natężenie dźwięku musi być o wiele większe, aby ucho ludzkie zarejestrowało taką stymulację [80].

Element behawioralny głosu związany jest ze sposobem mówienia, emocjami, nastrojem czy też statusem społecznym osoby mówiącej. Są to więc cechy będące wypadkowym wynikiem wielu czynników wpływających na nasz rozwój psychiczny i emocjonalny.

4.3.2 Głos w biometrii

Sygnał głosu, a w szczególności jego cyfrowa reprezentacja, jest obecnie powszechnie wykorzystywany w cyfrowych urządzeniach telekomunikacyjnych. Najważniejsze dziedziny przetwarzania mowy ludzkiej zostały przedstawione na rysunku 4.10 [17]. Na polu biometrii interesujące są przede wszystkim dwa z wymienio-



Rys. 4.10. Dziedziny przetwarzania głosu

wych powyżej zastosowań: weryfikacja oraz identyfikacja mówcy. W obu przypadkach można dokonać dalszego podziału ze względu na sposób interakcji użytkownika z systemem. W szczególności wyróżnia się systemy zależne od tekstu oraz niezależne od wypowiadanych słów. W tych pierwszych użytkownik wypowiada wcześniej wybrane przez niego hasło lub też odczytuje podane przez system słowa z pewnego, zazwyczaj niewielkiego, słownika. W systemach zależnych od tekstu oczekuje się pełnej kooperacji użytkownika z systemem, dzięki czemu możliwe jest uzyskanie wysokiej jakości próbek głosu, a co za tym idzie również wysokiej dokładności autentyfikacji.

Systemy przetwarzania głosu niezależne od tekstu cechują się dużo większą elastycznością od poprzednio opisanych. Liczba wypowiadanych słów jest nieograniczo-

na, a dodatkowo można poprawnie rozpoznać osoby, które zmieniły język wypowiedzi. Tego typu systemy mogą być wykorzystywane również w kryminalistyce, dzięki identyfikacji poszukiwanej osoby na podstawie próbki głosu, pobranej bez jej wiedzy. Z drugiej strony systemy niezależne od tekstu cechują się większą stopą błędu, jak również potrzebą użycia dalece bardziej skomplikowanych metod klasyfikacji osób.

Tak, jak i w przypadku innych biometryk, systemy oparte o sygnał głosu składają się zasadniczo z dwóch głównych części: ekstraktora cech oraz klasyfikatora. Ze względu na specyfikę proponowanego modelu generacji mowy (źródło - filtr), możliwe są dwie zasadnicze grupy cech, związanych z sygnałem głosu. Pierwsza grupa jest skojarzona z tonem krtaniowym, bez uwzględniania wpływu traktu głosowego na charakterystykę częstotliwościową tego tonu. W tym zbiorze parametrów analizuje się przede wszystkim wartość częstotliwości podstawowej F_0 oraz jej zmienność w czasie, a także kształt widma tonu podstawowego. W drugiej grupie skupiono się na matematycznym opisie charakterystyki częstotliwościowej filtru traktu głosowego. Istnieją także parametry, związane z akcentem czy intonacją, których nie można jednoznacznie przypisać do żadnej z powyższych grup.

Mnogość współczynników ekstrahowanych z sygnału głosu skłania badaczy raczej do opracowywania bardziej efektywnych metod ich wykorzystania, aniżeli do poszukiwania kolejnych parametrów. Najpopularniejsze obecnie metody analizy głosu wykorzystują współczynniki, które opierają się na dwóch głównych podejściach: liniowego kodowania predykcyjnego LPC (ang. *Linear Predictive Coding*) oraz szybkiej transformacie Fouriera - FFT (ang. *Fast Fourier Transform*). Algorytmy te są podstawą do dalszego przetwarzania, w celu uzyskania współczynników cepstralnych. Jednymi z najpowszechniej wykorzystywanych są parametry mel-cepstralne, które obliczane są w skali mel. Skala ta została wyznaczona w sposób empiryczny i modeluje charakterystykę narządu słuchu człowieka. Cechy te znajdują zastosowanie zarówno w analizie mowy, jak również w rozpoznawania mówcy [17].

W literaturze nie zaproponowano żadnego uniwersalnego podejścia do problemu klasyfikacji osób na podstawie głosu. Zależnie od trybu pracy systemu biometrycznego (zależny albo niezależny od wypowiadanego tekstu), stosowane są inne metody podejmowania decyzji przez system.

W przypadku rozwiązań zależnych od tekstu wykorzystywane są w szczególności techniki bazujące na dwóch typach metod [22, 27]:

- dynamiczne „marszczenie czasu" (ang. *Dynamic Time Warping* - DTW),
- ukryte modele Markova (ang. *Hidden Markov Model* - HMM).

Dobór metod podyktowany jest przede wszystkim faktem, iż w systemach tych porównywane są pewne z góry przewidziane wzorce tekstu mówionego, które mogą się różnić zarówno w czasie, jak również pod względem charakterystyki widmowej poszczególnych części słowa. Metody oparte na HMM przynoszą generalnie lepsze rezultaty, aniżeli te bazujące na DTW, których przewagą z kolei jest dużo mniejszy zbiór uczący potrzebny do wytrenowania klasyfikatora.

W systemach niezależnych od tekstu najpopularniejszymi metodami klasyfikacji są [22, 27]:

- kwantowanie wektorowe (ang. *Vector Quantization* - VQ),
- mieszany model gaussowski (ang. *Gaussian Mixture Models* - GMM).

Ponieważ zasób słów jest nieograniczony, dlatego z każdej zarejestrowanej wypowiedzi użytkownika należy wydobyć pewien charakterystyczny wektor cech, który umożliwi odróżnienie tej osoby od innych. W praktyce niemożliwym jest przechowywanie nieskończonej liczby próbek dla pojedynczego człowieka, dlatego też dokonuje się kompresji, w wyniku której uzyskuje się tzw. książkę kodową w przypadku VQ lub klastry dla metody GMM.

Jeżeli dostępny jest wystarczająco duży zbiór danych uczących, wówczas techniki bazujące na GMM charakteryzują się mniejszą stopą błędu aniżeli te, oparte na VQ. W przeciwnym przypadku należy korzystać raczej z metod wykorzystujących jako podstawę kwantowanie wektorowe.

4.4 Elektrokardiogram - analiza właściwości biometrycznych

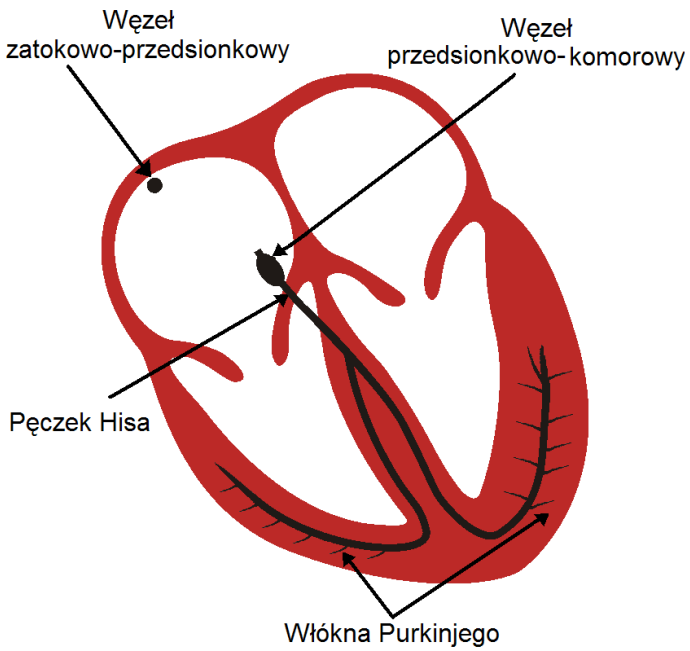
Zapis sygnału elektrycznego związanego z pracą mięśnia sercowego pierwszy raz został przeprowadzony przez Aleksandra Muirhead w 1872, natomiast pierwszego opisu diagnostycznego sygnału EKG, wraz z nadaniem nazw poszczególnym załamkom, wykonał w 1903 roku Willem Einthoven. Od tego momentu, dzięki postępowi technologicznemu w zakresie elektroniki biomedycznej oraz informatyki, wprowadzono liczne modyfikacje i usprawnienia, które pozwoliły na coraz dokładniejsze pomiary.

Przebieg sygnału EKG zawiera wiele ważnych informacji o funkcji serca, które są wykorzystywane do celów diagnostycznych. Zmiany, które zachodzą w sercu, zarówno morfologiczne jak fizjologiczne, znajdują swoje odzwierciedlenie w zapisie EKG. Analogowe systemy monitorujące EKG, w których zapis odbywał się tylko i wyłącznie na papierowych taśmach, wymagał każdorazowej oceny wyników przez lekarza specjalistę. W przypadku całodobowych zapisów EKG, była to operacja bardzo nużąca i czasochłonna. Wykorzystanie rosnących możliwości obliczeniowych urządzeń cyfrowych pozwoliło na skonstruowanie systemów wspomagających ten proces [29]. Dzięki urządzeniom cyfrowym upowszechniło się także użycie urządzeń rejestrujących EKG w nowych dziedzinach, nie tylko w diagnostyce medycznej.

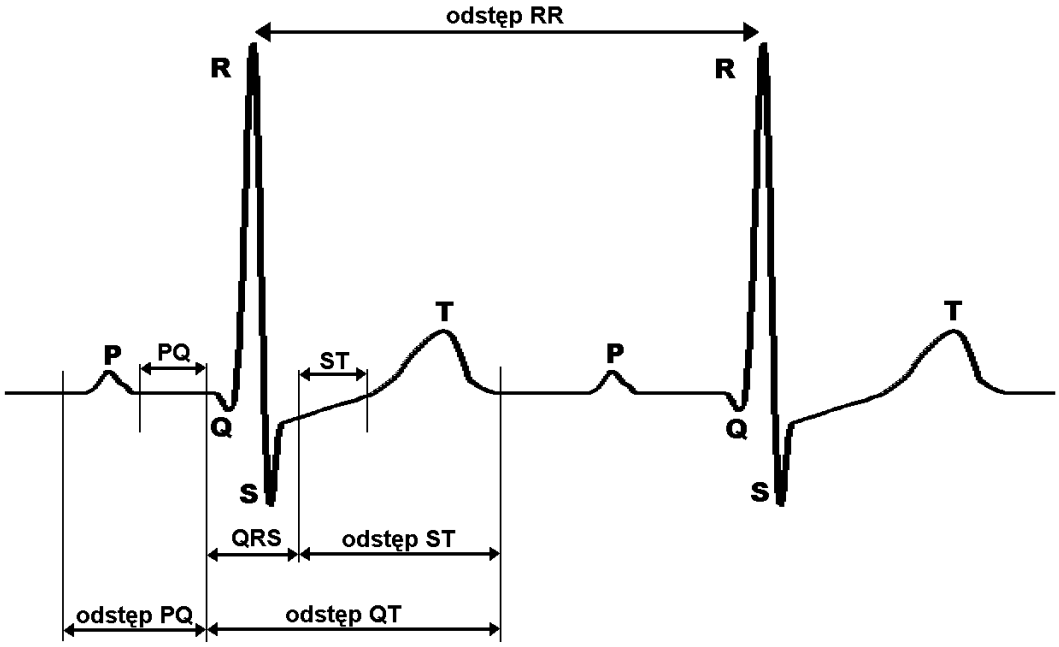
Analiza pracy serca została poniżej przedstawiona w ujęciu skorelowanym z zasadniczym celem pracy, przy czym szczególnie wyartykułowano te aspekty, które, zdaniem autora, istotnie łączą się z zagadnieniem biometrii.

4.4.1 Mechanika EKG

„Bicie serca" jest to skurcz mięśnia sercowego spowodowany różnicą potencjałów w komórkach składowych, zwanych kardiomiocytami. Kardiomiocyty mają ujemnie naładowane wnętrza. Cykl pracy serca rozpoczyna się od wyładowania węzła zatokowo-przedsionkowego. Węzeł ten narzuca swój rytm całemu sercu (rys. 4.11). Sygnał elektryczny rozchodzi się na zewnątrz węzła i powoduje depolaryzacje oraz gwałtowny skurcz przedsionków pod wpływem przemieszczania się jonów sodu (Na^+). Na przebiegu EKG jest to widoczne w postaci załamka P. Jedyną drogą przejścia sygnałów elektrycznych pomiędzy przedsionkami a komorami jest węzeł przedsionkowo-komorowy. Impulsy zostają spowolnione przy przejściu przez ten węzeł, ponieważ sygnały elektryczne są przenoszone przez względnie powolne jony wapnia (Ca^+), dzięki temu skurcz komór nie następuje, zanim krew z przedsionków nie zostanie do nich wpompowana. To spowolnienie jest wyrażone jako przerwa pomiędzy załamkiem P a R. Po przejściu przez węzeł przedsionkowo-komorowy sygnał gwałtownie przyśpiesza przy przejściu przez pęczek Hisa, gdzie w przewodzeniu ponownie biorą udział jony sodu (Na^+), a następnie trafia do lewej i prawej odnogi pęczka złożonego z włókien Purkinjego, gdzie rozchodzi się w komórkach tworzących komory serca. Wtedy następuje gwałtowny skurcz komór, co widoczne jest jako zespół QRS w zapisie EKG. Repolaryzacja komór rozpoczyna się bezpośrednio po zespole QRS (odcinek ST i załamek T) i nie odpowiada dokładnie depolaryzacji ze względu na czynniki chemiczne oraz opóźnienie pomiędzy końcem impulsu elektrycznego a fizycznym przemieszczeniem [23, 24]. Przebieg sygnału EKG wraz zaznaczonymi punktami charakterystycznymi został przedstawiony na rys. 4.12.



Rys. 4.11. Serce i jego stymulatory



Rys. 4.12. Przykład fali EKG z punktami charakterystycznymi

4.4.2 EKG jako cecha biometryczna

Prace dotyczące międzyosobniczej zmienności zapisu EKG zostały przedstawione w [36]. Autorzy udowodnili, iż różnica w zarejestrowanych sygnałach EKG, pochodzących od różnych osób, zależy w dużej mierze od anatomii badanych. Zaproponowali oni metodę redukcji tych różnic dzięki wykorzystaniu modelu geometrycznego klatki piersiowej, serca oraz płuc tworzonego na podstawie zdjęć rezonansu magnetycznego. W pracy tej stwierdzono również, iż nie tylko czynniki geometryczne, ale także różnice w przewodności mięśni szkieletowych, czy też indywidualna budowa tkanek mają wpływ na sygnał EKG.

Na podstawie analizy literaturowej z zakresu wykorzystania elektrokardiografii w biometrii można wyróżnić dwie zasadnicze grupy metod ekstrakcji cech z przebiegu EKG:

- metody wykorzystujące punkty charakterystyczne sygnału EKG (rys. 4.12) oraz te,
- które nie korzystają z wymienionych punktów.

Metody bazujące na punktach charakterystycznych sygnału EKG

Jako jedni z pierwszych możliwość wykorzystania sygnału EKG w identyfikacji osób przedstawili w 1999 roku autorzy opracowań [9, 10]. Zaproponowali oni wykorzystanie zapisu pełnego, wysoce specjalistycznego, dwunasto-odprowadzeniowego

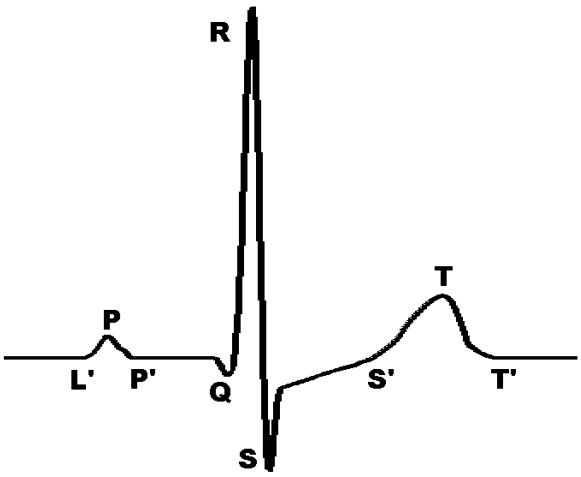
monitora EKG (SIEMENS Megacart), który pozwolił na automatyczną ekstrakcję 360 cech (30 cech wykorzystywanych powszechnie w diagnostyce medycznej dla każdego z odprowadzeń). Jednak ich dalsza analiza pokazała, iż istnieje silna korelacja pomiędzy poszczególnymi odprowadzeniami a cechami. Dlatego też finalnie zdecydowali się oni na użycie tylko trzech elektrod, przypiętych do kończyn, w celu rejestracji poszukiwanych cech. Ostatecznie zaproponowali, jako podstawę klasyfikacji, zestaw 10 cech nieskorelowanych ze sobą. Wykorzystano metodę PCA w celu redukcji przestrzeni cech oraz klasyfikacji i uzyskano wynik 50 poprawnych klasyfikacji na 50 prób przy 20 badanych osobach.

Użycie jedno-odprowadzeniowego EKG do celów biometrycznej weryfikacji tożsamości zaproponowane zostało w [123]. Autorzy przedstawili podejście oparte na siedmiu cechach sygnału EKG, z których pięć związane było z zespołem QRS. W analizie użyto przebiegów EKG 20 osób zarejestrowanych w bazie MIT–BIH. Weryfikację przeprowadzono w oparciu o dwustopniowy klasyfikator, którego pierwszy stopień porównywał wzorce, a drugim była sieć neuronowa. Sieć ta była uczona na podstawie cech wyłonionych z 20 losowo wybranych uderzeń serca każdego użytkownika. Wzorce biometryczne do weryfikacji były tworzone z cech wyekstrahowanych z 20 innych uderzeń serca. Etap porównywania wzorców miał na celu wstępną ocenę zgodności próbek. Te próbki, które okazywały się w wystarczającym stopniu zgodne, były ostatecznie weryfikowane przez sieć neuronową. Według autorów uzyskano stuprocentową dokładność weryfikacji, ale należy podkreślić, iż zarówno zbiór cech uczących, jak i zbiór cech weryfikowanych dla danego użytkownika pochodził z tego samego przebiegu EKG.

W pracy [65], pochodzącej z roku 2001, skupiono się na ekstrakcji i analizie tylko czterech parametrów sygnału EKG w szczególności czasów trwania: załamka P, odstępu PQ, zespołu QRS oraz odstępu QT. Rejestrację sygnału przeprowadzono monitorem EKG, rejestrującym pięćset, dwunastobitowych próbek na sekundę. Jak w uprzednio opisanej pracy wykorzystano zapis pochodzący tylko z jednego odprowadzenia - II. Usunięto składowe sygnału poniżej 0,06 Hz, powyżej 60 Hz, a także w zakresie 50 Hz. Wspomniane cechy wyekstrahowano poprzez dwukrotne zróżniczkowanie sygnału, dzięki czemu wyróżnione zostały punkty charakterystyczne. Z każdego przebiegu EKG uzyskiwano sekwencję cech, na podstawie których wyznaczono ich średnią, wariancję oraz kowariancję. Dyskryminację przeprowadzono poprzez zestawienie cech parami i wykorzystanie odległości Mahalanobisa jako kryterium. Zbadano 18 przebiegów EKG pochodzących od 9 osób i uzyskano dokładność powyżej 90%.

Pierwszą próbę połączenie sygnału EKG z tradycyjną modalnością biometryczną, w szczególności geometrią twarzy, przedstawiono w [49]. Połączenie to miało przede wszystkim na celu wzmocnienie systemu biometrycznego przed atakami za pomocą skradzionych lub podrobionych cech. Pomiaru EKG dokonano komercyjnym urządzeniem, z częstotliwością próbkowania 256 Hz oraz siedmiobitową rozdzielczością. Pomiar trwał 4 minuty. W czasie pierwszych dwóch określano poziom bazowy

sygnału, w następnych dwóch osoba badana miała za zadanie wykonać proste działania arytmetyczne. Wybierano dwuminutową sekwencję w celu określenia średniej fali EKG, a następnie dla każdego uderzenia serca wyodrębniano 15 parametrów związanych z punktami charakterystycznymi fali: P, R oraz T, a także z nowo zdefiniowanymi punktami L' i P' - oznaczającymi początek i koniec załamka P oraz S' i T', stanowiące granice trwania załamka T (rys. 4.13). Wykorzystano dwa frontalne obrazy: przed oraz po pomiarze EKG i wyznaczono cechy z użyciem metody PCA. Przetestowano trzy podejścia łączenia biometryk i uzyskano dokładność około 99% w przypadku prostego połączenia cech. W pozostałych metodach łączenia cech uzyskano gorsze wyniki, a w jednym przypadku połączenie modalności dało gorsze wyniki, aniżeli użycie tylko cech twarzy.



Rys. 4.13. Fala EKG z dodatkowymi punktami charakterystycznymi zaproponowanymi w [49]

Identyfikację osób na podstawie znacznie większego zbioru danych zawierających przebiegi EKG, przeprowadzono w pracy [105]. Sygnały rejestrowane przez 18 godzin od 10 osób, pochodziły z bazy MIT–BIH. Dla każdej osoby wybrano 200 uderzeń serca i poddano je dalszej analizie. Przebiegi zostały przefiltrowane filtrami cyfrowymi Butteworth'a (IIR) w celu usunięcia szumów spoza zakresu 1-60 Hz. Wyłoniono zespoły QRS, bazując na zmodyfikowanym algorytmie Pan'a i Thompkins'a, a następnie obliczono cztery cechy związane z tym zespołem, odległość R-R oraz nowo zdefiniowany współczynnik kształtu, określany w literaturze jako *form factor*. W celu identyfikacji badanych osób użyto dwóch typów sieci neuronowych: wielowarstwowy perceptron ze wsteczną propagacją błędu oraz uproszczone rozmyte sieci ARTMAP. Sieci te były uczone połową zbioru danych (1000 próbek), natomiast druga połowa służyła do celów testowych. Badano różne konfiguracje wspomnianych sieci i uzyskano 97,6% poprawnych identyfikacji.

Bardzo obszerne badania z zakresu wykorzystania EKG do identyfikacji osób przedstawili autorzy opracowań [43, 45, 47, 147]. Podobnie jak w [49], osoby bada-

ne były poddawane różnym zadaniom, w czasie których mierzony był sygnał EKG. Zadania zostały podzielone ze względu na poziom stresu, który wywołują. Zadania o mniejszym poziomie stresu (m. in. medytacja) były rozdzielone fazami odpoczynku od zadań o większym obciążeniu umysłowym (czytanie lub arytmetyka). Przebadano 29 osób podczas dwunastu różnych zadań. Użyto dwóch rejestratorów EKG: o dużej (1000 Hz) częstotliwości próbkowania i dwunastobitowej rozdzielczości oraz standardowego urządzenia o częstotliwości próbkowania 256 Hz i siedmiobitowej rozdzielczości. Przy czym w dalszej analizie wykazano, iż mniejsza częstotliwość próbkowania wpływa na dokładność identyfikacji osób. Zarejestrowane dane poddano obróbce filtrem pasmowo-przepustowym w zakresie 2-40 Hz, a następnie wyłoniono 15 cech związanych punktami charakterystycznymi fali: P, R oraz T, a także ze wspomnianymi wcześniej punktami L', P', S' i T'. Selekcji cech dokonano poprzez krokową analizę dyskryminacyjną wykorzystującą λ Wilkes'a jako miarę rozbieżności. Przeprowadzono doświadczenia, które miały na celu ocenę wpływu poszczególnych zadań na dokładność klasyfikacji. Wykazano, iż poza jednym zadaniem (prowadzenia samochodu w wirtualnej rzeczywistości), udało się zidentyfikować poprawnie tożsamość badanych osób w ponad 97% przypadkach. Udowodniono również, iż lokalizacja elektrod nie wpływa na poprawność klasyfikacji.

W kolejnym artykule Irvine i in. [48] przedstawione są dodatkowe badania na większej populacji (ponad 100 osób). Stwierdzono, że wykorzystanie do identyfikacji tożsamości cech bazujących tylko na punktach charakterystycznych sygnału EKG, nie jest wystarczające w przypadku dużej liczby osób. W tych badaniach dokładność przedstawionej metody spadła do 88%.

Ciekawą propozycję połączenia sygnałów EEG oraz EKG przedstawiono w [117]. Autorzy wykorzystali czujniki umieszczone w czapce do pomiarów EEG oraz jedną elektrodę na nadgarstku do pomiaru EKG. Elektroda referencyjna została podłączona do prawego płatka ucha. Użyte elektrody mogły pracować bez dodatkowego żelu przewodzącego. Informacje o zarejestrowanym sygnale były przesyłane do komputera z użyciem sieci bezprzewodowej. Zarejestrowano cztery trzyminutowe pomiary, następnie dzielono je na czterosekundowe odcinki i dla każdego obliczano pięć cech. Dla każdej badanej osoby wyznaczano najlepszą kombinację cech i klasyfikatorów (spośród 4). Tworzono ten sposób „osobisty klasyfikator" wykorzystywany w procesie weryfikacji. W celu potwierdzenia tożsamości rejestrowano jednominutowe przebiegi. Przetestowano ponad 400 sytuacji: 350 prób oszustwa, 48 prób weryfikacji osób podających prawdziwe dane oraz, 16 prób włamania (brak osoby w bazie). W zależności od sposobu podziału przestrzeni cech uzyskano dokładność 98% oraz 100%.

Metody nie wykorzystujące punktów charakterystycznych

Wszystkie omówione powyżej opracowania bazują na cechach wyekstrahowanych na podstawie punktów charakterystycznych sygnału EKG (fale P, QRS oraz T), ponieważ stanowią one podstawę w przypadku oceny medycznej i próba ich użycia

również w celach biometrycznych jest naturalna. Urządzenia wykorzystywane w tym celu pozwalają na automatyczną lokalizację punktów charakterystycznych, z mniejszą lub większą dokładnością. Jednak w przypadku zastosowań biometrycznych taka rozmyta ocena położenia wspomnianych punktów powoduje, iż weryfikacja lub identyfikacja tożsamości może być obarczona dużym błędem. Dodatkowym problemem jest fakt, iż nie ma żadnej uniwersalnej reguły, która pozwalałaby na jednoznaczne określenie granic poszczególnych fal [70], a liczba opracowań dotycząca metod automatycznej ekstrakcji punktów charakterystycznych (omówione na przykład w pracy [57]) sugeruje, iż kwestia ta wciąż pozostaje przedmiotem badań naukowych.

Inne podejście do wykorzystania sygnału EKG w procesie weryfikacji tożsamości przedstawione zostało w [145]. W przeciwieństwie do prac opisanych powyżej, nie wyodrębniono żadnych cech z zapisów czynności serca, lecz porównywano same przebiegi. Co więcej, wykorzystano stosunkowo krótkie zapisy o długości 10 s, zebrane w długim okresie czasu (średni interwał pomiędzy zapisami wynosił 16,6 miesiąca). Zbiór danych pochodził z bazy Physikalisch-Technische Bundesanstalt (PTB) i zawierał 234 zapisy od 74 osób zarejestrowanych przez urządzenie o częstotliwości próbkowania równej 500 Hz. Wykorzystano odprowadzenia kończynowe Einthovena. Sygnał przefiltrowano filtrem dolno-przepustowym o częstotliwości odcięcia wynoszącej 75 Hz. Porównywano krótkie przebiegi (100 ms) zawierające jeden zespół QRS. Pojedynczy przebieg był wybierany z dziesięciosekundowych zapisów w taki sposób, aby jego odległość euklidesowa od pozostałych uderzeń serca w danym zapisie była jak najmniejsza. Ten sam współczynnik wykorzystano w celu oceny zgodności uderzeń serca pochodzących z dwóch różnych zapisów. Wartość współczynnika EER dla weryfikacji wyniosła 3%. Natomiast identyfikację przeprowadzono z dokładnością 99%.

Wspomniane problemy w ekstrakcji punktów charakterystycznych skłoniły autorów opracowań [142, 143] do poszukiwania innych zestawów cech bazujących na sygnale EKG. W analizie korzystali oni z publicznych baz zawierających zapisy czynności elektrycznej serca. Były to odpowiednio: PTB, przechowująca sygnały zarejestrowane z częstotliwością 1 kHz, z rozdzielczością 0,5 μV, MIT-BIH, zawierająca zapisy próbkowane z częstotliwością 128 Hz. Wybrano zapisy, które nie zawierały arytmii. Sygnały zostały poddane filtracji Butteworth'a w zakresie 1–40 Hz w celu usunięcia zakłóceń. Następnie sygnał został podzielony ma okna o długości 800 ms. Dla tych okien wyznaczono dwa zestawy cech. Jako pierwszy zaproponowano 15 cech przedstawionych w pracach Israel i in. [47, 49], które uzupełniono o dodatkowe 5, reprezentujących różnicę napięć pomiędzy wybranymi punktami. Dokładność rozpoznawania osób wyniosła 85% oraz 100% w zależności od bazy w przypadku 15 cech, natomiast wykorzystanie dodatkowych cech pozwoliło osiągnąć 100% dokładności. W drugim zestawie wyznaczono cechy na podstawie algorytmu PCA. Pojedyncze bicie serca zostało zapisane w M-wymiarowej przestrzeni. Wybrano te wektory własne, których suma wartości własnych stanowiła 99% wszystkich wartości. Zaproponowano hierarchiczny moduł decyzyjny, w którym pierwszy stopień stanowi klasyfikator

oparty na LDA (*Linear Discriminat Analysis*) korzystający z pierwszego zestawu cech, który podejmuje wstępną decyzję. Następnie, jeśli zajdzie taka potrzeba, korzysta się z algorytmu PCA i klasyfikatora opartego na algorytmie k-NN. Osiągnięto dokładność 100%. Celem autorów było nie tylko osiągnięcie stuprocentowej dokładności w identyfikacji osób, ale także jak najlepszej dokładności w identyfikacji pojedynczych uderzeń serca.

W pracach [109, 142] wspomniani autorzy przedstawili również inne podejście do problemu ekstrakcji cech, bazując na tych samych danych i identycznej filtracji wstępnej. Sygnał został podzielony na pięcio- lub dziesięciosekundowe okna, dla których wyliczano wartości współczynników funkcji autokorelacji (AC) dla przesunięcia M, gdzie $M << N$, a N to długość okna. Następnie wyznaczano współczynniki dyskretnej transformaty kosinusowej (DCT) w celu redukcji przestrzeni cech. Przebadano różne kombinacje liczby współczynników DCT, oraz opóźnień funkcji AC korzystając z miary euklidesowej oraz metody k-NN jako klasyfikatorów, ale tylko dla jednego z nich uzyskano idealne dopasowanie. Dodatkowo w pracy [109] testowano również użycie logarytmu naturalnego funkcji gęstości prawdopodobieństwa rozkładu normalnego standardowego jako miary, przyjmując że każda z badanych cech ma rozkład normalny. Nie dowiedziono jednak, iż założenie to jest spełnione.

W późniejszej pracy [3] oprócz połączenia funkcji AC/DCT wykorzystano także kombinację metod AC/LDA w celu wyłonienia zestawu cech. Zaproponowano ponownie wstępną selekcję klas, do których może należeć testowana osoba, bazując na współczynnikach funkcji AC, a następnie dokładną klasyfikację, korzystając ze współczynników DCT lub LDA. Uzyskano całkowitą dokładność dla wszystkich kombinacji, poza połączeniem AC/DCT bez wstępnej klasyfikacji. Przeprowadzono również testy związane z ustawieniem progu czułości klasyfikacji na okoliczność oszacowania wartości współczynników FAR oraz FRR, ale nie przedstawiono wyników w czytelny i przekonywujący sposób.

Powyższą analizę rozszerzono również na zapisy EKG zawierające pewne wybrane typy arytmii [5], w szczególności przedwczesną depolaryzację przedsionkową (ang. *atrial premature contraction* - APC) oraz przedwczesną depolaryzację komór (ang. *premature ventricular contraction* - PVC). W przypadku arytmii AVC przebieg sygnałów nie zmienia się w sposób znaczący, przez co nie było potrzeby wprowadzenia dodatkowych metod przetwarzania w stosunku do tych opisanych w [3, 109, 142]. Natomiast w przypadku arytmii PVC wprowadzono dodatkowy etap, który eliminował segmenty EKG, zawierające te niepożądane zaburzenia. Klasyfikację oparto o miarę euklidesową oraz algorytm najbliższych sąsiadów i otrzymano wyniki na poziomie 96,4% poprawnych identyfikacji tożsamości na próbie liczącej 56 osób w tym 30 mających zaburzenia rytmu serca.

Kolejna praca autorstwa Agrafioti i Hatzinakos [4] zawiera propozycję wykorzystanie dwunasto-odprowadzeniowego EKG jako źródła cech. Do testów wykorzystano zapisy EKG 14 osób pochodzących ze wspomnianej już bazy PTB. Filtracja, podział na okna oraz ekstrakcja cech została przeprowadzona podobnie jak w pracach

opisanych w poprzednim akapicie. Wykorzystano połączenie funkcji autokorelacji oraz LDA w celu redukcji przestrzeni cech. Zbadano dokładność klasyfikacji z użyciem cech wyznaczonych na podstawie zapisów z pojedynczych elektrod. Poza odprowadzeniami V1, V3 oraz V4, w pozostałych przypadkach klasyfikacja była bezbłędna. Przedstawiono różne podejścia do problemu połączenia sygnałów ze wszystkich elektrod. Przetestowano proste połączenie wektorów cech, wyłonionych z poszczególnych odprowadzeń w jeden wektor i uzyskano perfekcyjną dokładność, jednak w przypadku klasyfikacji pojedynczych okien dokładność wynosiła około 95%, co było niższą wartością, aniżeli dokładność uzyskana z wykorzystaniem tylko jednej z elektrod. Inne podejście do połączenia cech polega na wykorzystaniu modułu decyzyjnego. Każde z odprowadzeń miało osobny klasyfikator wyuczony na podstawie cech pochodzących z tej elektrody. Następnie zaproponowane 4 reguły decyzyjne, na podstawie których badana osoba jest zaliczana do jednej z klas: (1) wszystkie klasyfikatory podejmują tę samą decyzję, (2) więcej niż połowa klasyfikatorów podejmuje tę samą decyzję, (3) przynajmniej α klasyfikatorów podejmuje tę samą decyzję ($\alpha \in (0, 1]$, oraz (4) decyzja została podjęta przy odpowiedniej przewadze (również zależne od parametru α) jednej z klas nad pozostałymi. Jeżeli osoba nie została sklasyfikowana odpowiednio z regułami, to zostaje odrzucona. Chroni to system przed próbą włamania ze strony osób nie zarejestrowanych, ale powoduje także odrzucenie osób uprawnionych. Wartość współczynnika odrzucenia osób wahała się od 0 (dla metody (2)) aż do ponad 30 % (dla metody (1) oraz (3) i (4) przy $\alpha > 0,9$). Przeprowadzone badania udowodniły, iż prawie wszystkie odprowadzenia mogą być wykorzystywane do identyfikacji osób (w szczególności odprowadzenia kończynowe), jednak użycie pełnego dwunasto-odprowadzeniowego EKG nie jest dobrym rozwiązaniem dla praktycznych systemów biometrycznych ze względu na trudności z rozmieszczeniem elektrod, zwłaszcza odprowadzeń przedsercowych.

Również w pracy [44] zaproponowano inne podejście do wyznaczania cech, które nie wymaga lokalizacji punktów charakterystycznych. Proces akwizycji danych odbywał się w ten sam sposób, jak w poprzednich pracach tych autorów [43, 45, 47]. Następnie próbki zostały przefiltrowane pasmowo-przepustowym filtrem Fourier'a i posegmentowane na pojedyncze uderzenia serca. Podział odbywał się z użyciem funkcji autokorelacji, a wszystkie uderzenia były wyrównywane do punktu R. Kolejnym krokiem, była normalizacja każdego uderzenia serca składająca się z dwóch kroków. Najpierw normalizowano długość każdego uderzenia serca poprzez próbkowanie w dół do wartości 250, 100, 50, 25 oraz 10 próbek na całe uderzenie, a następnie normalizowano amplitudę EKG w zakresie [0;1]. Na podstawie tak przygotowanych danych dla każdego uderzenia serca wyznaczano macierz kowariancji oraz własności własne i odpowiadające im wektory własne, a więc wykorzystano metodę PCA. Do uczenia, tworzenia kolekcji próbek oraz do weryfikacji wykorzystano ten sam dwuminutowy przebieg EKG podzielony na 3 bloki. W klasyfikacji wykorzystano odległość euklidesową. Otrzymane wyniki klasyfikacji dochodzą do 100%, jednak rozróżnianie pojedynczych uderzeń serca było niższe, niż w oparciu o cechy bazujące na punktach

charakterystycznych EKG. Z drugiej jednak strony ponad 35% osób nie mogło zostać zarejestrowanych, jeżeli cechy wyznaczano tak, jak w przypadkach medycznych.

W kolejnej pracy autorstwa Irvine i Israel [46] zaproponowano wykorzystanie analizy sekwencyjnej do weryfikacji tożsamości w jak najkrótszym czasie. Sygnał EKG został przefiltrowany filtrem pasmowo-przepustowym w zakresie od 0,2 do 40 Hz, a następnie podzielony na segmenty zawierające pojedyncze uderzenie serca. Dla każdego segmentu ekstrahowano wektor składający się z 9 cech związanych z punktami charakterystycznymi przebiegu EKG. W kolejnym kroku wyznaczano średni wektor cech oraz macierz kowariancji. W procesie weryfikacji dla kolejnych uderzeń serca wyznaczane są cechy, a następnie aktualizowana jest wartość średnia wektora cech i sprawdzane jest czy wartość statystyki przekroczyła jeden z dwóch założonych progów, które odpowiadają dwóm hipotezom: badana osoba jest tą za którą się podaje oraz dana osoba nie jest tą za którą się podaje. Jeżeli wartość statystyki nie przekroczy żadnego z tych progów, to przetwarzane jest kolejne uderzenie serca, aż do podjęcia decyzji. Przetestowano dwa zbiory danych. Jeden zawierał 29 przebiegów zebranych w poprzednich pracach [45, 47], natomiast drugi zawierał dane 75 osób zarejestrowanych urządzeniem o częstotliwości próbkowania 256 Hz oraz rozdzielczości 7 bitów. Wyniki eksperymentów pokazały, iż możliwe jest zweryfikowanie osoby nawet po dwóch uderzeniach serca, a w najgorszym przypadku potrzeba ich było 33. Dokładność weryfikacji wyniosła od 70% do 100% w zależności od przyjętego progu czułości, który oscylował od 0,0001 do 0,1. Należy zwrócić uwagę, iż wektor cech po raz kolejny opierał się na punktach charakterystycznych, które nie muszą być łatwe w lokalizacji. Widać to wyraźnie w przypadku drugiego zbioru, zarejestrowanego urządzeniem o niższej dokładności, gdzie wyniki zaprezentowano tylko dla progów czułości o wartości 0,05 oraz 0,01. Dodatkowo, w celu uproszczenia analizy, założono bez dowodu, iż wektor cech ma 9-wymiarowy rozkład normalny, ale nie udowodniono, że założenie to jest spełnione. Otrzymane wyniki sugerują, iż użycie analizy sekwencyjnej jest słusznym podejściem i pozwala na szybkę weryfikację tożsamości.

Transformację sygnału EKG w przestrzeń trójwymiarową zaproponowano w pracy [26]. Pomiaru dokonano jedno- oraz trójodprowadzeniowym EKG podłączonym do klatki piersiowej badanej osoby (odprowadzenia V4, V5 oraz V6) przy częstotliwości próbkowania 250 Hz. Sygnał został przefiltrowany filtrem pasmowo-przepustowym w zakresie 2-50 Hz. Na podstawie pięciu kolejnych uderzeń serca wyznaczano jedno uśrednione uderzenie i stworzono jego rekonstrukcję w przestrzeni fazowej. W przypadku EKG jednoodprowadzeniowego wektor w przestrzeni 3D miał następującą postać $X_0(t) = [x_0(t) \quad x_0(t+\tau) \quad x_0(t+2\tau)]$, gdzie x_0 to uśredniona fala EKG, zawierał więc sygnał EKG oraz jego kolejne przesunięcia w czasie o wartość τ. Dla EKG trójodprowadzeniowego każdy wymiar wektora zawierał uśredniony sygnał z jednego z odprowadzeń. Sygnały były uśredniane na podstawie załamka R, który był jedynym punktem charakterystycznym, ekstrahowanym bezpośrednio z przebiegu EKG. Zaproponowano dwie miary do określenia podobieństwa dwóch obrazów

w przestrzeni fazowej: przestrzenną korelację zależną od liczby sześcianów, na które podzielono przestrzeń (im mniejsza wartość tego współczynnika, tym dwa obrazy są mniej podobne do siebie), oraz wzajemną odległość najbliższych punktów (im mniejsza wartość tym dwa obrazy są bardziej podobne do siebie). Testy przeprowadzono dla różnych długości sygnału EKG (31 oraz 151 punktów wokół punktu R) oraz dla jedno- i trójodprowadzeniowego EKG. Zbadano dwa scenariusze: gdy tylko jedna miara jest wykorzystywana, lub gdy oba współczynniki są użyte w klasyfikacji. Uzyskano dokładność na poziomie około 95% dla 100 badanych osób. Zaletą tego podejścia jest brak potrzeby uczenia klasyfikatora, ponieważ nowy obraz musi tylko zostać zapisany w bazie. Użycie odprowadzeń piersiowych powoduje, iż przedstawione rozwiązanie nie nadaje się do praktycznego zastosowania. Wykorzystanie tylko zespołu QRS do tworzenia obrazu fazowego wydaje się dodatkowo mocno ograniczać przestrzeń cech.

W pracy [6] rozszerzono analizę przedstawioną w [5, 109, 142] o transformację okresowości (*periodicity transform*) w celu określenia współczynnika jakości zarejestrowanego sygnału EKG. Dodatkowo zaproponowano podział uzyskanego przebiegu funkcji autokorelacji sygnału EKG na kilka segmentów i wyznaczania dla każdego z nich jego zestawu cech z użyciem metody LDA. Klasyfikacja sygnału odbywa się na podstawie odległości, będącej sumą iloczynów odległości poszczególnych segmentów oraz wag przypisanych każdemu wycinkowi funkcji autokorelacji i wspomnianego współczynnika jakości. W przypadku weryfikacji uzyskano wartość współczynnika EER na poziomie 2%, natomiast w przypadku identyfikacji uzyskano dokładność 81,5% dla pięciosekundowych zapisów EKG oraz 93,2% dla trzyminutowych przebiegów. Badania przeprowadzono dla 52 osób.

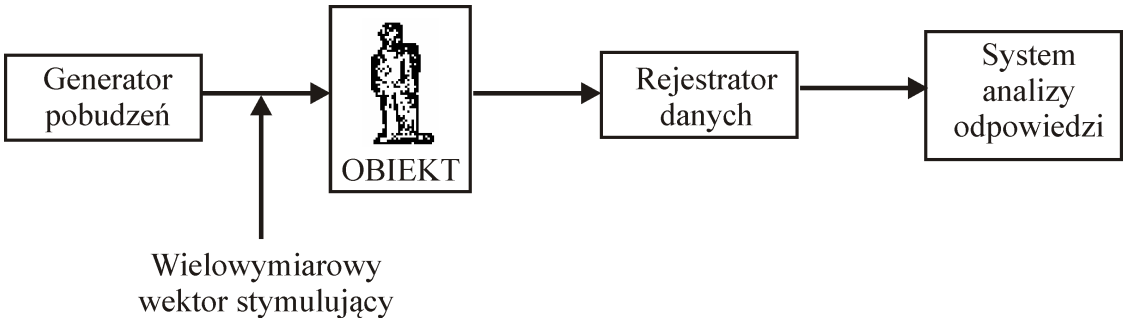
Połączenie cech temporalnych sygnału EKG oraz współczynników cepstralnych zaproponowano w [67]. Bazując na osiemnastu przebiegach EKG zapisanych w bazie MIT-BIH z częstotliwością próbkowania równą 128 Hz, użyto wielomianów Hermite'a (*Hermite Polynomial Extension* - HPE) do zamiany kształtu sygnału EKG na wartości współczynników cech temporalnych. W procesie klasyfikacji z użyciem tych cech wykorzystano maszynę wektorów wspierających (*Support Vector Machine*). Drugim typem cech były współczynniki cepstralne ekstrahowane za pomocą mieszanego modelu gaussowskiego (*Gaussian Mixture Model* - GMM) oraz uniwersalnego modelu tła (*Universal Background Model*) z maksymalizowanym prawdopodobieństwem „a posteriori" (*Maximum A Posteriori*). Wykorzystano również kombinację GMM oraz SVM, znanej pod nazwą gaussowskiego super wektora (*Gaussian Super Vector* - GSV). W celu redukcji cech zaproponowano heteroskedastyczną liniową analizę dyskryminacyjną (*Heteroscedastic Linear Discriminant Analysis* - HLDA). Przetestowano różne konfiguracje wymienionych metod i najlepsze wyniki uzyskano przy połączeniu cech temporalnych (HPE + SVM) oraz cepstralnych (GSV + HLDA). Dokładność identyfikacji wyniosła 98,26% przy EER równym 0,5%.

5. Autorski system pomiarowy - budowa i oprogramowanie

Podstawowy cel pracy naukowo-badawczej, niejako meritum niniejszej dysertacji, stanowi autorski system kryptografii biometrycznej. Finalne rozwiązanie obejmuje nie tylko sprzęt i oprogramowanie, lecz również odpowiednio dobrany model matematyczny, użyty jako podstawa wnioskowania aksjomatyczno-dedukcyjnego. Na podstawie analizy ogólnego stanu wiedzy w przedmiotowej dziedzinie (zaprezentowanego pokrótce we wprowadzającej części opracowania), sprecyzowano zadania, wymagające zarówno realnego wsparcia technicznego jak i jednoznacznego systemu wnioskowania.

Punktem wyjścia dla poszukiwania własnej koncepcji elektroniczno-informatycznego oprzyrządowania jest pogłębiona analiza spotykanych rozwiązań w dziedzinie biometrii. Z uwagi na poziom istotności tej analizy dla powodzenia syntetycznej części pracy naukowej wyodrębniono ją w postaci osobnych podrozdziałów poprzedzających bezpośrednio autorską część pracy.

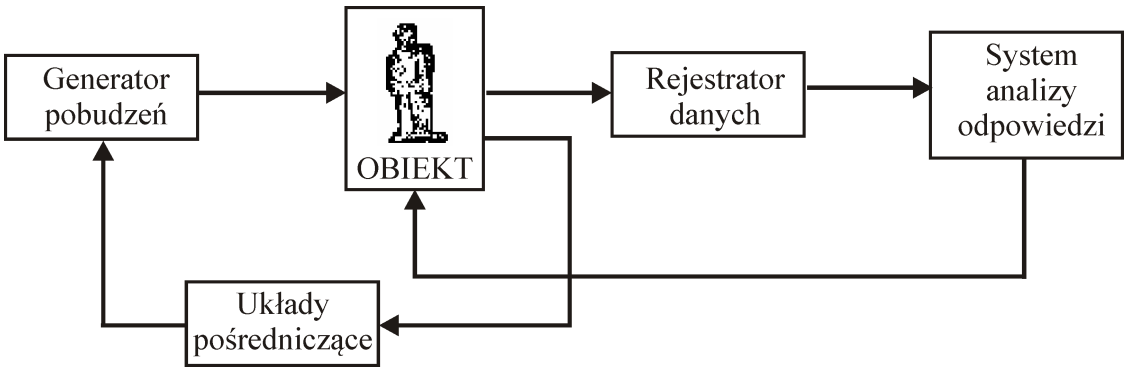
Naukowym problemem, artykułowanym w niniejszej pracy wielokrotnie, w zróżnicowanej postaci, jest badanie reakcji człowieka na zadawane pobudzenia. W największym uogólnieniu prezentuje to rysunek 5.1.



Rys. 5.1. System rejestracji reakcji

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. 5.2).



Rys. 5.2. System pomiarowy z biocybernetycznym sprzężeniem zwrotnym

Odmienność ilustracji układów z biocybernetyczną pętlą sprzężenia zwrotnego od obrazu typowego układu regulacji wynika z faktu, że człowiek występuje tu integralnie, choć inne jego organy (receptory) pełnią rolę obiektu, a inne (umysł, system nerwowy i dalej mięśniowy) rolę sprzężenia zwrotnego.

5.1 Stanowisko pomiarowe - opis konstrukcji

Współcześnie, w dobie tzw. „cyfrowej jakości dźwięku i obrazu", kompletowanie informacji z otoczenia nie wzbudza zazwyczaj należytego respektu. Przeciętny użytkownik sprzętu informatycznego zadowala się cyfrową kamerą i - digitalizującą dźwięk - kartą w komputerze. Nieoczywiste staje się to, iż zasadnicza informacja w ujęciu biocybernetycznym ma analogową ciągłość. Zagadnienie przetwarzania sygnałów biometrycznych, zwłaszcza na etapie badawczym, wymagającym ustalonych progów kwalitatywnego relatywizowania kolekcjonowanych wyników, przestaje być odpowiednio rozumiane w kontekście elektroniki. Dlatego też obiektywizacja i implikująca ją jakość pomiarów stanowiły podstawową przesłankę dla opracowania konstrukcji systemu pomiarowego.

Zadanie skonstruowania systemu pomiarowego do rejestracji i analizy sygnałów biometrycznych ma również swój dydaktyczny wymiar. Urządzenie przeznaczone do akwizycji i wstępnego przetwarzania danych biomedycznych z powodzeniem może być użyte do wspomagania realizacji zajęć laboratoryjnych z przedmiotu *Biometria*.

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, który zawiera przenośne urządzenie powszechnego użytku do monitorowania sygnału EKG.

Szczegółowa specyfikacja technicznych parametrów systemu pomiarowego stanowi przedmiot dalszej części niniejszego rozdziału.

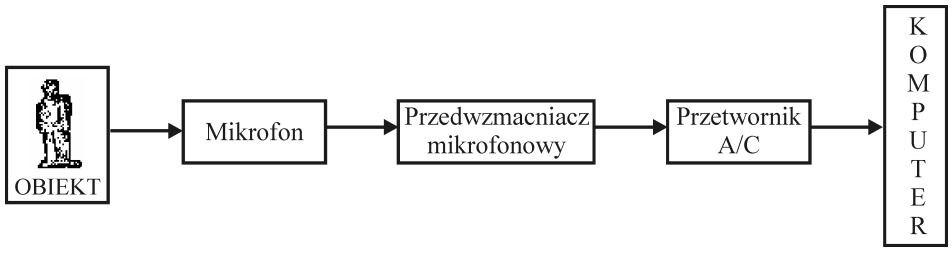
5.1.1 Układ rejestracji głosu

Tor pomiarowy służący do pomiaru sygnału głosu składa się z następujących elementów:

- wysokiej jakości mikrofonu,
- niskoszumowego wzmacniacza mikrofonowego,
- przetwornika A/C, połączonego z komputerem poprzez interfejs USB.

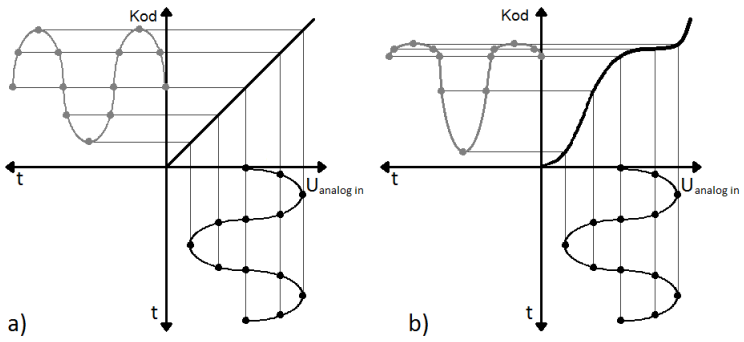
Przetwornik A/C

Schemat układu pomiarowego do przetwarzania sygnału dźwiękowego został przedstawiony na rysunku 5.3.



Rys. 5.3. Schemat rejestratora dźwięku

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. Powyższe stanowisko może budzić zdziwienie, zważywszy, że typowa rozdzielczość przetwornika w karcie dźwiękowej to 16 bitów. Najważniejszymi parametrami każdego przetwornika analogowo-cyfrowego jest jednak nieliniowość różniczkowa oraz nieliniowość całkowa. Wpływ nieliniowości wejścia analogowego przetwornika A/C na wynikowy kod binarny przedstawiony został na rysunku 5.4. Odchylenie charakterystyki przej-



Rys. 5.4. Wpływ liniowości przetwornika A/C na wyjściowy sygnał cyfrowy a) idealna liniowość b) nieliniowość

ściowej przetwornika od linii prostej skutkuje zniekształceniem sygnału mierzonego, a w konsekwencji utratą informacji jaką ten sygnał zawiera. Dla uzasadnienia odpowiedniego doboru właściwych składników konstrukcyjnych przytoczono poniżej określenia kluczowych pojęć z dziedziny przetwarzania analogowo-cyfrowego.

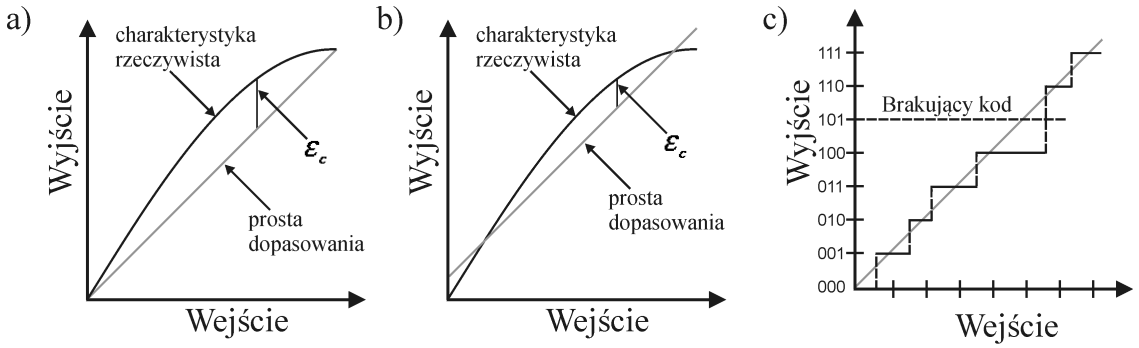
Nieliniowość całkowa

Nieliniowość całkowa (ang. *integral nonlinearity*) określona jest jako maksymalne względne odchylenie $(\Delta U_{we})_{\max}$ rzeczywistej charakterystyki przetwarzania $N = f(U_{we})$ od charakterystyki idealnej, czyli od prostej łączącej skrajne punkty zakresu przetwarzania [40, 63] - rysunek 5.5. Nieliniowość całkowa ε_c jest wyrażona w procentach w stosunku do pełnego zakresu przetwarzania zgodnie ze wzorem [141]:

$$\varepsilon_c = \frac{(\Delta U_{we})_{\max}}{U_{we\max}} * 100\%. \tag{5.1}$$

Innym sposobem określenia nieliniowości całkowej jest tak zwana definicja „najlepszego dopasowania", w której prosta odniesienia jest wyznaczana w taki sposób, aby odległości pomiędzy poszczególnymi punktami charakterystyki a prostą odniesienia były jak najmniejsze. Ten sposób definiowania nieliniowości bywa czasem stosowany przez producentów sprzętu, ponieważ taka definicja daje generalnie

błąd o połowę mniejszy aniżeli wcześniej opisana metoda punktów skrajnych [60] - rysunek 5.5b.



Rys. 5.5. Przykłady błędów nieliniowości a) całkowej - punktów końcowych, b) całkowej - najlepszego dopasowania, c) różniczkowej z brakującym kodem

Nieliniowość różniczkowa

Nieliniowość różniczkowa (ang. *differential nonlinearity*) - określana jest przez wyznaczenie różnic między sąsiednimi wartościami napięcia wejściowego, powodującymi zmianę słowa wyjściowego o wartość najmniej znaczącego bitu. Nieliniowość różniczkowa ε_r jest podawana w procentach jako maksymalne względne odchylenie tej różnicy od jej wartości średniej w całym zakresie przetwarzania lub wyrażana w ułamakch wartości LSB (ang. *less significant bit*) [40, 63].

Jeżeli wartość błędu nieliniowości różniczkowej przekracza ±1 LSB, to w charakterystyce przetwarzania mogą wystąpić brakujące kody - rysunek 5.5c.

Nieliniowość różniczkowa ma szczególne znaczenie w przypadku zastosowań, w których analizuje widma sygnałów, gdyż duża wartość tego błędu może wprowadzać znaczące zniekształcenia uzyskanego widma, przez co jego dalsza obróbka i interpretacja będzie znacząco utrudniona. Przetwarzanie sygnałów mowy, które w znakomitej większości odbywa się w dziedzinie częstotliwości, wymaga więc przetworników A/C o bardzo dobrych parametrach dotyczących nieliniowości charakterystyki przetwarzania.

Użyty przetwornik A/C Labjack UE9 cechuje 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 (±0,05% maksymalnie). Pozostałe parametry, takie jak szybkość próbkowania oraz rozdzielczość, spełniają wymagania opracowanego systemu pomiarowego. Szczegółowy opis wszystkich parametrów wybranego przetwornika można znaleźć w [66]

Mikrofon i wzmacniacz

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.

Głównym elementem wzmacniacza jest układ scalony LM2209, który posiada dynamikę rzędu 100dB, natomiast jego zniekształcenia harmoniczne są poniżej 1% [34]. Został on zamknięty w metalowej obudowie, która efektywnie ekranuje obwód i chroni go przed wpływem zewnętrznych zakłóceń elektromagnetycznych. Wzmocnienie układu zostało dobrane w taki sposób, aby napięcie wyjściowe nie przekraczało wartości ±5V, która jest najwyższą dopuszczalną wartością wejściową dla wejść analogowych zastosowanego przetwornika.

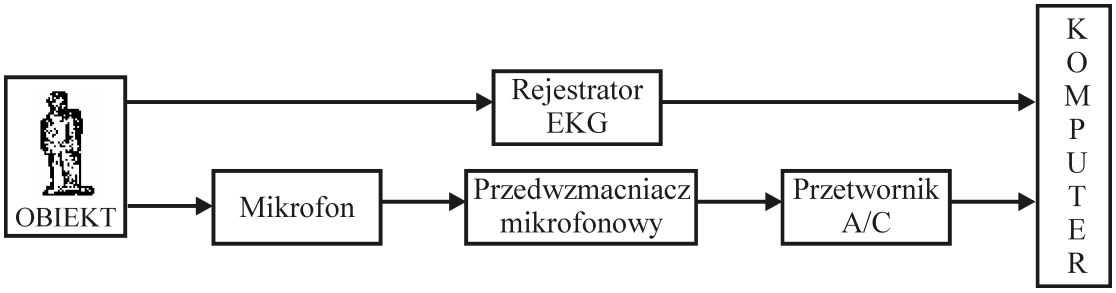
5.1.2 Tor EKG

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. Wprowadzono go w celu rejestracji sygnału EKG w czasie przeprowadzania eksperymentu. To standardowe urządzenie umożliwia:

- całodobową rejestrację sygnału EKG,
- automatyczną ocenę przebiegu EKG,
- pomiar tętna,
- eksport zapisanych danych do komputera.

Dzięki temu istnieje możliwość określenia wpływu sygnału mowy na zmiany w sygnale EKG badanej osoby. Co więcej, jak opisano w rozdziale 4.4, zapis czynności elektrycznej mięśnia sercowego jest dodatkowym źródłem cech biometrycznych.

Schemat blokowy systemu dwukanałowej rejestracji cech biometrycznych przedstawiono na rysunku 5.6.



Rys. 5.6. Schemat rejestratora próbek

5.2 Oprogramowanie systemu pomiarowego

Zaprezentowany w początkowej części niniejszego rozdziału schemat blokowy systemu pomiarowego ujmuje zarówno generator pobudzeń, jak i system akwizycji i analizy próbek oraz przetwarzania wyników. Użyty, w funkcji sterownika, system komputera personalnego umożliwia względnie proste programowanie algorytmów pracy przedmiotowego urządzenia. Przygotowane dla potrzeb niniejszej dysertacji dedykowane oprogramowanie umożliwia więc:

a) generację pobudzeń;

b) akwizycję próbek sygnału mowy oraz fali EKG;

c) analizę zarejestrowanych danych i prezentację wyników pomiarów.

Przeprowadzenie założonych pomiarów oraz wyłonienie osobniczo charakterystycznych, unikalnych znaczników biometrycznych umożliwia przygotowane oprogramowanie w postaci modułowej. Obsługę sprzętu pomiarowego (programowanie oraz zbieranie danych) wykonuje się w czasie rzeczywistym, a dane pomiarowe buforowane są w autonomicznych pamięciach elementów pomiarowych. Analiza pozyskanych danych oraz ich przetworzenie w celu (optymalnie korzystnej dla użytkownika) wizualizacji stanowi przedmiot wydzielonego modułu, który pracuje w trybie off-line.

Zaprojektowane oprogramowanie, wykonane w środowisku MATLAB® [71], jest integralną częścią systemu pomiarowego, stanowiąc w całości pracę autorską. Zostało ono zaimplementowane z wykorzystaniem kwalifikowanych bibliotek, dostarczanych wraz z pakietem.

5.2.1 System generowania pobudzeń

W prezentowanej pracy przyjęto dwa rodzaje bodźców:

- dźwiękowe,
- 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.

Wpływ dźwięków na ciało ludzkie jest przedmiotem badań wielu prac szczególnie z zakresu muzykoterapii [75,100]. Udowodniono, iż rytm serca człowieka dopasowuje się do rytmu słuchanej muzyki [64]. W pracy [118] wykorzystano stymulację dźwiękową generowaną przez osobę badaną. Fala dźwiękowa była rejestrowana zarówno od strony ust jak i od strony ucha, w którym następowało odbicie dźwięku, co posłużyło do określenia budowy ucha, a jego kształt do autentyfikacji użytkownika.

Dotychczasowe prace badawcze potwierdziły, iż pobudzenia wzrokowe również wpływają na reakcje człowieka. W pracy [58] opisano wykorzystanie ruchu gałek ocznych w odpowiedzi na nadzorowane wymuszenia wizualne do identyfikacji tożsamości. Bodźcem były jednokolorowe, migające kwadraty.

W badaniach dotyczących wykorzystania elektroencefalografii (EEG) w systemach biometrycznych, a w szczególności bazujących na zjawisku potencjałów wywołanych (*evoked potentials*), stymulacja stanowi niezbędny komponent. Wśród potencjałów wywołanych można wyróżnić trzy typy, które znajdują zastosowanie w identyfikacji osobniczej: wizualne potencjały wywołane *Visual Evoked Potentials - VEP* (pobudzenia wzorcem, takim jak szachownica [112]), słuchowe potencjały wywołane *Auditory Evoked Potentials - AEP* oraz somatosensoryczne potencjały wywołane *Somatosensory evoked potential - SEP* (proste czynności, jak zamknięcie oka [106]).

Inne podejście do użycia tego typu stymulacji przedstawił Mostowski [94]. Zaproponował on koncepcję wizualnego sprzężenia zwrotnego w systemach biometrycznej autentyfikacji. System ten działał w trybie weryfikacji tożsamości, a więc wymagał zarejestrowania próbek biometrycznych użytkownika. Jako cechę biometryczną zaproponowano sygnał mowy. Zadaniem użytkownika było wygaszenie wyświetlanego obrazu, co oznaczało, iż generowany przez niego dźwięk zgadzał się z próbką zarejestrowaną w systemie. Głos analizowano w dziedzinie częstotliwości z użyciem krótkookresowej transformaty Fouriera. Rozwiązanie to jednak wymagało dużych nakładów obliczeniowych związanych z wielokrotnym obliczaniem wspomnianej transformaty (4 razy w ciągu 30ms). Innym problemem były zmienne warunki akwizycji, które w istotny sposób wpływały na wyniki badań. Przedstawiona koncepcja wizualnego

sprzężenia zwrotnego posłużyła jako podstawa do opracowania autorskiej koncepcji systemu biometrycznego w aspekcie biometrii behawioralnej.

Działanie systemu opiera się na pomiarze reakcji w odpowiedzi na bodźce zewnętrzne. Przed rozpoczęciem eksperymentu osobie badanej podłączane były elektrody do pomiaru sygnału EKG, a następnie rejestrowano falę EKG przez 30 sekund, aby określić stan osoby przed stymulacją. Po okresie relaksu stymulator programowy generował 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 [7]). Pobudzenia spoza wspomnianego zakresu występują trzykrotnie rzadziej. Formalny zapis został zaprezentowany poniżej:

$$P(\xi = x) = \begin{cases} \frac{1}{184} & \text{dla} \quad x \in A_1 \\ \frac{3}{184} & \text{dla} \quad x \in A_2 \end{cases}, \tag{5.2}$$

gdzie:

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

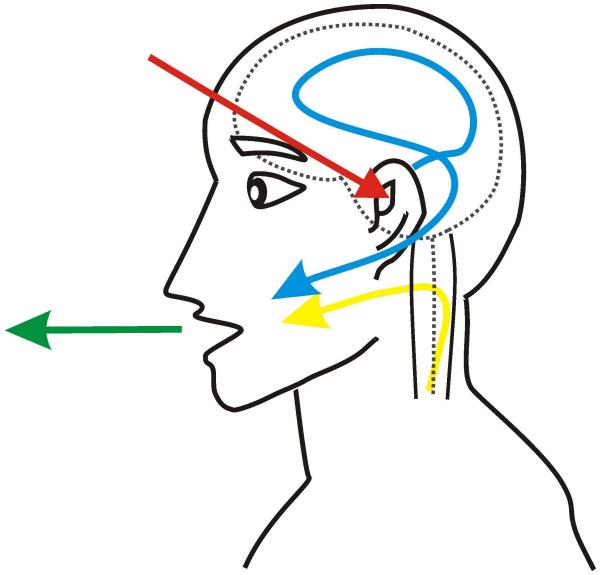
$A_2 = \{a_i : i \in \{13, 14, ..., 60\} \wedge a_1 = 55 \wedge a_i = (\sqrt[12]{2})^{i-1} \cdot a_1\}$.

Zadaniem badanej osoby było dopasowanie się do wygenerowanego dźwięku poprzez zaśpiewanie pojedynczej, ustalonej głoski na podanej wysokości. Poprzednie badania wykazały [16, 80], iż w tym celu najlepiej wykorzystać samogłoski (szczególnie samogłoskę „a"). Wynika to z dwóch powodów:

- można je wypowiadać przez dłuższy czas w niezmienny sposób,
- zawierają informację o cechach fizjologicznych traktu głosowego.

Powyżej scharakteryzowana frakcja dźwiękowa toru stymulacji stanowiła pierwszy obwód biocybernetycznego sprzężenia zwrotnego (rys. 5.7) prezentowanego systemu pomiarowego.

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. Wybór takiego rozwiązania podyktowany był faktem, iż metodę autokorelacji stosuje się w dziedzinie



Rys. 5.7. Schemat sprzężenia dla pobudzenia dźwiękowego

czasu, a więc nie ma potrzeby przechodzenia do dziedziny częstotliwości, które wiążę się z relatywnie złożoną obliczeniowo i czasochłonną transformatą Fouriera.

Funkcja korelacji własnej sygnału $x(t)$ dana jest wzorem:

$$R_{xx}(\tau) = R_x(\tau) = \int_{-\infty}^{\infty} x(t)x^*(t-\tau)dt \tag{5.3}$$

Natomiast dla sygnałów dyskretnych:

$$r(k) = \sum_{n=0}^{N-k-1} x(n)x(n+k), \quad k = 0, 1, 2, \ldots, N-1 \tag{5.4}$$

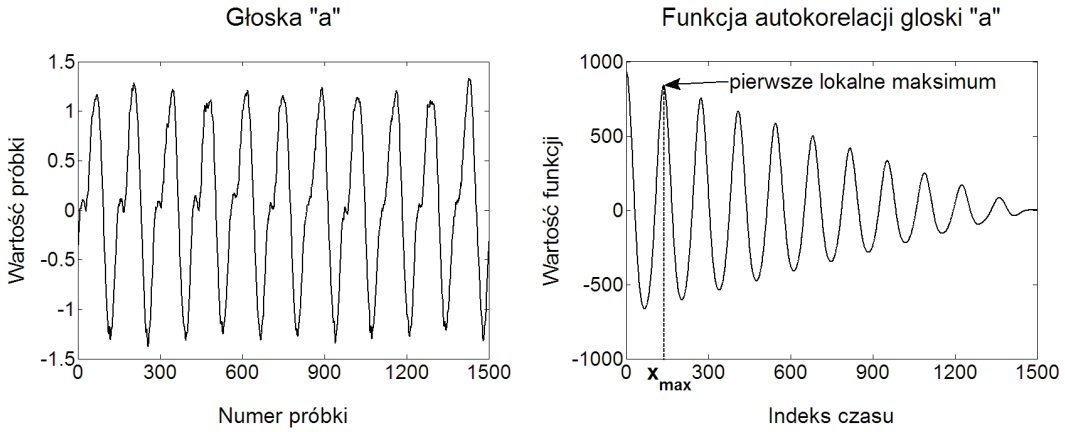
gdzie: N - liczba próbek sygnału.

Funkcja autokorelacji przyjmuje wartość maksymalną dla $k = 0$. Aby wyznaczyć częstotliwość podstawową F_0 sygnału należy najpierw wyznaczyć położenie pierwszego lokalnego maksimum x_{max} funkcji $r(k)$ dla $k > 0$ (rys. 5.8), a następnie obliczyć wysokość generowanego przez daną osobę dźwięku z poniższej zależności:

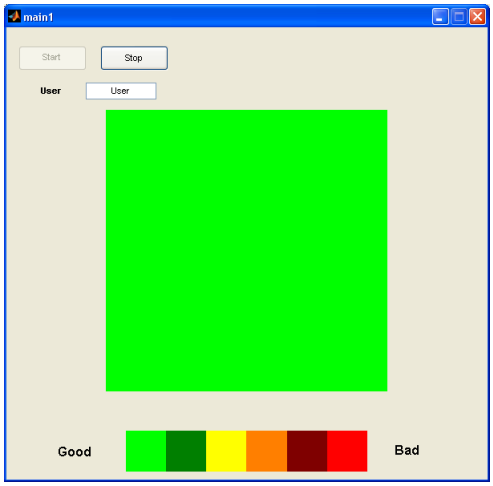
$$F_0 = \frac{F_s}{x_{max}} \tag{5.5}$$

gdzie: F_s - częstotliwość próbkowania sygnału.

Na podstawie wyniku porównania pokazywany jest na ekranie odpowiedni obraz. Prezentowane obrazy stanowią drugi, wizualny tor stymulacji polisensorycznej.



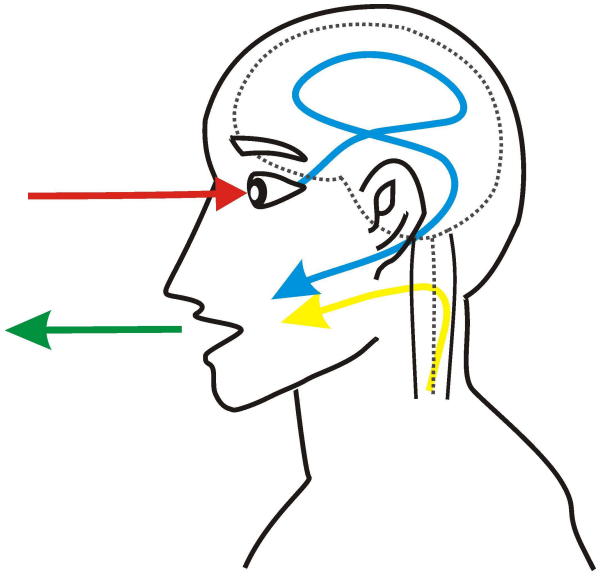
Rys. 5.8. Przykładowe przebiegi sygnału dźwiękowego oraz funkcji autokorelacji dla głoski „a" z zaznaczonym pierwszym lokalnym maksimum x_{max}



Rys. 5.9. Główne okno programu do akwizycji próbek

Wyświetlany jest kwadrat o jednolitym kolorze, który zmienia się w zależności od stopnia dopasowania pomiędzy przykładowym i emitowanym dźwiękiem (rys. 5.9). Zmiany następują co 300 ms. Szybsze nie pozwalałyby na reakcję użytkownika, a w skrajnym przypadku (duża częstotliwość zmian) mogłyby doprowadzić do wywołania ataków epilepsji. Z kolei zbyt długi czas pomiędzy kolejnymi obrazami powoduje, iż użytkownik odnosi wrażenie, że system nie reaguje na jego odpowiedź. Stymulacja wizualna stanowi drugi obwód biocybernetycznego sprzężenia zwrotnego w systemie pomiarowym (rys. 5.10).

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 przy-



Rys. 5.10. Schemat sprzężenia dla pobudzenia wizualnego

jętymi ustaleniami, celem osoby badanej jest dostrojenie się do podanego dźwięku, a więc uzyskanie koloru zielonego. Oczywiście, ze względu na różnice pomiędzy poszczególnymi ludźmi, nie każda osoba jest w stanie osiągnąć taki wynik w każdej próbie.

Zakresy wyświetlanych kolorów zostały zdefiniowane na podstawie odległości pomiędzy dźwiękiem wygenerowanym przez stymulator, a dźwiękiem emitowanym przez badaną osobę. 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 [125]. Pojęcia te oznaczają odpowiednio pomnożenie częstotliwości podstawowej przez wielokrotność liczby 2 (dla jednej oktawy mnożnik wynosi 2) lub podzielenie tej częstotliwości. Z punktu widzenia słuchacza dźwięki odległe o oktawę (lub kilka oktaw) stanowią ewidentny konsonans (współbrzmienie). Zakresy wyświetlanych kolorów definiowane przez różnicę $F_{0_gener} - F_{0_emit}$ są opisane następującym równaniem:

$$\text{kolor} = \begin{cases} \text{zielony} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| \in \left[0, \frac{1}{4}\text{tonu}\right] \\ \text{ciemnozielony} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| \in \left(\frac{1}{4}\text{tonu}, \frac{3}{4}\text{tonu}\right] \\ \text{żółty} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| \in \left(\frac{3}{4}\text{tonu}, \frac{5}{4}\text{tonu}\right] \\ \text{pomarańczowy} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| \in \left(\frac{5}{4}\text{tonu}, \frac{7}{4}\text{tonu}\right] \\ \text{ciemnoczerwony} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| \in \left(\frac{7}{4}\text{tonu}, \frac{11}{4}\text{tonu}\right] \\ \text{czerwony} & \text{dla} \quad |F_{0_gener} - F_{0_emit}| > \frac{11}{4}\text{tonu} \end{cases} . \quad (5.6)$$

Powyższe równanie wyraża odległości pomiędzy dźwiękami w skali muzycznej, która jest skalą nieliniową, gdzie częstotliwość podstawowa dźwięku stanowi $\sqrt[12]{2} \approx 1,0595$ częstotliwości podstawowej dźwięku go poprzedzającego (w stroju równomiernie temperowanym) [8]. Dodatkowo należy wziąć pod uwagę fakt, iż skala muzyczna jest cykliczna, przez co dźwięki znajdujące się w odległości oktawy (8 tonów lub 12 półtonów) lub jej wielokrotności są takimi samymi dźwiękami w sensie muzycznym [146]. W celu wyznaczenia stopnia zgodności generowanych i emitowanych dźwięków należało przeliczyć ich wartości na skalę liniową. Wykorzystano następującą zależność:

$$F_{0_lin} = \log_2\left(\frac{F_0}{27{,}5}\right), \quad (5.7)$$

gdzie:

F_{0_lin} - częstotliwość dźwięku przeliczona na skalę liniową,

F_0 - częstotliwość podstawowa dźwięku.

Wartość 27,5 to częstotliwość podstawowa pierwszego dźwięku pianina użytego do generacji stymulacji wyrażona w hercach. W notacji muzycznej odpowiada to dźwiękowi A w oktawie dolna subkontra.

Otrzymana w wyniku przekształcenia 5.7 wartość jest reprezentowana przez liczbę rzeczywistą. Interpretacja jej fizykalnego sensu wykorzystuje następujące definicje:

- *cecha liczby rzeczywistej*

$$\lfloor x \rfloor = \max\{k \in \mathbb{Z} \colon k \leqslant x\}, \quad (5.8)$$

- *część ułamkowa liczby rzeczywistej*

$$\{x\} = x - \lfloor x \rfloor. \quad (5.9)$$

Część całkowita zawiera numer oktawy pianina (liczoną od 0), natomiast część ułamkowa określa położenie dźwięku w oktawie. Wynikiem porównania a dwóch dźwięków jest więc różnica ich części ułamkowych:

$$a = |(F_{0_emit_lin} - \lfloor F_{0_emit_lin} \rfloor) - (F_{0_gener_lin} - \lfloor F_{0_gener_lin} \rfloor)|. \tag{5.10}$$

Parametr a przyjmuje wartości z zakresu $[0; 1)$. Należy jednak pamiętać, iż dla $a > 0{,}5$ porównywane dźwięki są coraz bardziej do siebie zbliżone. Na przykład stosując równania 5.7 oraz 5.10 dla dźwięków gis^2 (830,6 Hz) oraz h^1 (493,88 Hz) otrzymamy wartość $a = 0{,}75$, co oznacza, iż te dźwięki znajdują się daleko od siebie. Jeżeli przyjmiemy, że dźwięk a jest początkiem oktawy, to okazuje się, iż dźwięk gis jest tylko pół tonu niżej, a dźwięk h o ton wyżej od początku oktawy. Wprowadzono więc poniższą korektę, aby wynik porównania przedstawiał faktyczną odległość pomiędzy dźwiękami w skali muzycznej:

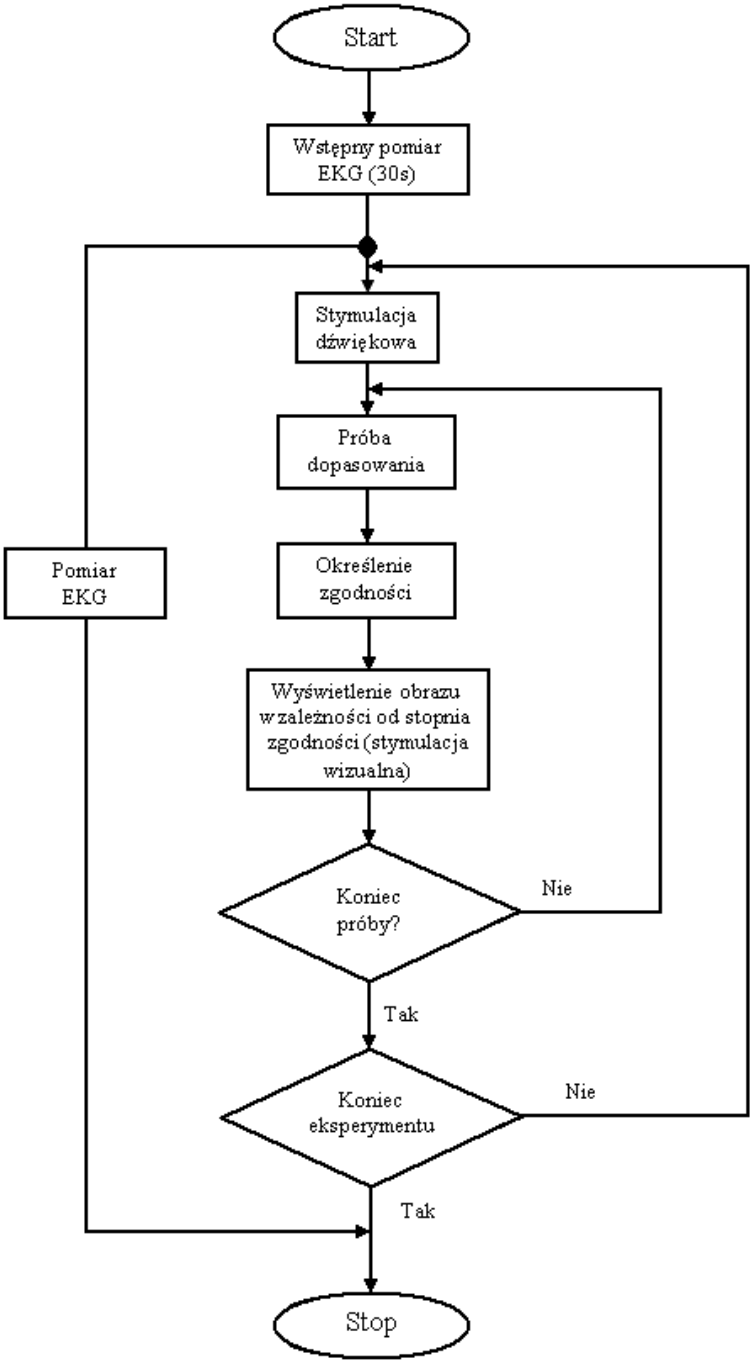
$$\tilde{a} = \begin{cases} a & \text{dla} \quad a \in [0; 0{,}5] \\ |a - 1| & \text{dla} \quad a \in (0{,}5; 1) \end{cases}. \tag{5.11}$$

Wykorzystując powyższe zależności można zakresy wyświetlanych kolorów wyrazić w skali liniowej w następujący sposób:

$$\text{kolor} = \begin{cases} \text{zielony} & \text{dla} \quad \tilde{c} \in [0; 0{,}0416) \\ \text{ciemnozielony} & \text{dla} \quad \tilde{c} \in [0{,}0416; 0{,}125) \\ \text{żółty} & \text{dla} \quad \tilde{c} \in [0{,}125; 0{,}2083) \\ \text{pomarańczowy} & \text{dla} \quad \tilde{c} \in [0{,}2083; 0{,}2917) \\ \text{ciemnoczerwony} & \text{dla} \quad \tilde{c} \in [0{,}2917; 0{,}4583) \\ \text{czerwony} & \text{dla} \quad \tilde{c} \in [0{,}4583; 0{,}5] \end{cases}. \tag{5.12}$$

Schemat blokowy algorytmu eksperymentu został przedstawiony na rysunku 5.11. 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

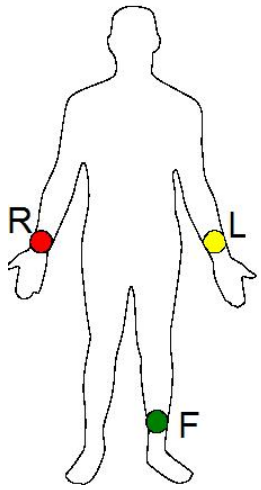
jednego eksperymentu przeprowadza się pięć prób. Całość badania trwa nie więcej niż dwie minuty. Przez cały czas akwizycji dźwięku rejestrowany jest współbieżnie sygnał EKG.



Rys. 5.11. Algorytm eksperymentu

5.2.2 Akwizycja danych

Rejestrator EKG należy podłączyć zgodnie z rysunkiem poniżej (rys. 5.12). Mierzony sygnał 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, co uznano za wystarczającą jakość badania. Sygnał mowy został zarejestrowany z dwunastobitową rozdzielczością przy częstotliwości próbkowania 44,1 kHz. Zdecydowano się na taką jakość, aby nie wprowadzać niepotrzebnych błędów związanych z nieliniowością przetwornika, co (jak opisano wyżej w rozdziale 5.1) ma kluczowe znaczenie w procesie akwizycji sygnałów analogowych. Osoba badana otrzymywała słuchawki, w których odtwarzane były dźwięki. Mikrofon ustawiany był w niewielkiej odległości, zapewniającej odpowiedni poziom sygnału 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 informacją 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. W tabeli 5.1 przedstawiono przykładowy zapis eksperymentu, natomiast na rysunku 5.13 zaprezentowano egzemplaryczne okno autorskiej aplikacji wykorzystywanej do generowania przebiegów z zarejestrowanych danych. Zgodnie z przyjętą standaryzacją okno ma zunifikowany charakter, co determinuje przyjazność obsługi systemu. Do przycisku „Help" jest plik pomocy standardowego środowiska przygotowywania aplikacji.

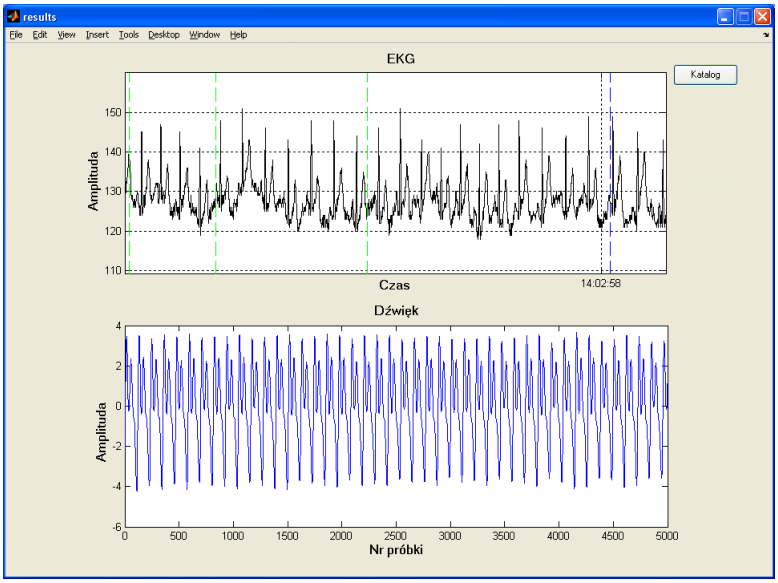


Rys. 5.12. Schemat podłączenia rejestratora EKG

Tab. 5.1. Przykładowe wyniki pomiarów

Dźwięk					
Nr próby	FQ	t_{start}	$t_{start\text{-}śpiew}$	t_{stop}	U_{in}
1	277 Hz	15:44:33:099	15:44:35:562	15:44:40:241	0,454361 V 0,416913 V 0,396942 V ⋮
2	493 Hz	15:44:45:447	15:44:47:908	15:44:52:585	0,057420 V 0,049930 V ⋮
...	...	...	...	...	...
EKG					
t_{start}			Wartość próbki		
15:43:46			138 139 ⋮		

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. Żadna z badanych osób nie miała problemów ze zrozumieniem i wykonaniem postawionego przed nią zadania.

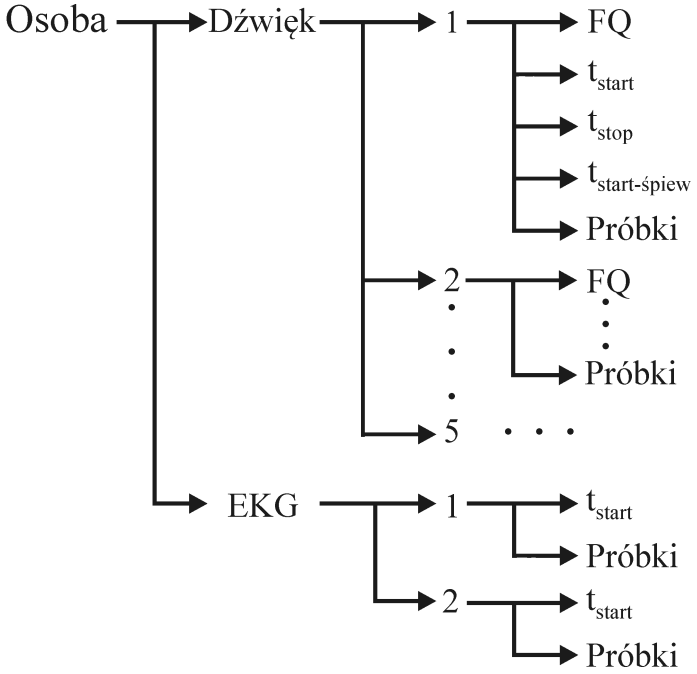


Rys. 5.13. Okno aplikacji do graficznej prezentacji zarejestrowanych danych

Dla każdego badania tworzony jest osobny katalog o unikalnej nazwie i numerze eksperymentu. Znajdują się w nim pliki zawierające zarejestrowane próbki. Użyty monitor EKG zapisuje dane o pomiarze bezpośrednio na dysku lokalnym w postaci plików binarnych. Przebieg sygnału EKG jest dzielony na jednominutowe bloki, natomiast informacja o czasie zarejestrowania danego segmentu danych znajduje się w innym zbiorze, niż wartości próbek.

Dane reprezentujące chwilowe stanu sygnału akustycznego, pobierane w czasie eksperymentu, są zapisywane do plików tekstowych osobno dla każdej próby dopasowania (w katalogu znajduje się więc pięć plików). W nagłówkach tych zbiorów zapisano również informację o częstotliwości podstawowej dźwięku stymulacji, znacznik czasu początku stymulacji, znacznik początku odpowiedzi oraz końca próby.

W ramach utworzonej aplikacji przygotowano moduł, odpowiedzialny za odczyt zapisanych danych oraz przetworzenie ich do postaci dogodnej dla dalszej analizy. Stosując się do dobrych praktyk programistycznych zaproponowano organizację danych spójnych logicznie z ich realnym znaczeniem. Strukturę tę przedstawiono na rysunku poniżej (rys. 5.14).



Rys. 5.14. Schemat struktury danych, w której przechowywano informację o badaniu użytkownika

6. Metody ekstrakcji rzeczywistych biometryk

Kompletowanie rzeczywistych wyników pomiarowych jest bez wątpienia nie tylko metrologicznym zadaniem, lecz także stanowi podstawę dla poszukiwań metod odpowiedniego przetwarzania danych. Dalszym, zasadniczym z naukowego punktu widzenia, etapem jest poszukiwanie uogólnień oraz precyzowanie modelu o heurystycznych podstawach.

W prezentowanym rozdziale zawarty jest opis czynności następujących po akwizycji danych pomiarowych. W dalszej kolejności zaprezentowano więc także 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 służy do parametryzacji (wzmocnienia) podpisu elektronicznego.

6.1 Analiza sygnału EKG

6.1.1 Przetwarzanie wstępne informacji o pracy serca

Pierwszym krokiem przetwarzania jest proces filtracji, który może zostać zapisany następującym równaniem:

$$y(n) = h(n) \otimes x(n), \tag{6.1}$$

gdzie:
$h(n)$ - sygnał filtrujący,
$x(n)$ - sygnał filtrowany.

Wstępna filtracja sygnału EKG ma na celu skonstruowanie takiej funkcji $h(n)$, która pozwoli na usunięcie zakłóceń wolnozmiennych związanych z ruchami mięśniowymi oraz eliminację zakłóceń szybkozmiennych, pochodzących przede wszystkim z sieci zasilającej rejestratory EKG. Wykorzystane urządzenie nie jest wprawdzie

zasilane z sieci elektrycznej (posiada własne źródło napięcia stałego), lecz z uwagi na obecność bardzo silnych pól elektrycznych, o częstotliwości 50 Hz wokół nas (pochodzących z powszechnych i mocnych urządzeń codziennego użytku) tego czynnika zakłócającego nie da się pominąć. Częstotliwość próbkowania równa 100 Hz sprawia, zgodnie z twierdzeniem Kotielnikowa-Shannona, iż częstotliwości powyżej 50Hz nie zostaną zarejestrowane. Z tego powodu nie ma potrzeby filtracji składowych szybkozmiennych. Dlatego też zaprojektowano filtr górnoprzepustowy, zamiast (jak w większości prac, omówionych w rozdziale 4.4.2) filtry pasmowoprzepustowe.

Filtry cyfrowe można podzielić na dwa rodzaje:

- o skończonej odpowiedzi impulsowej (ang. *Finite Impulse Response* - FIR),
- o nieskończonej odpowiedzi impulsowej (ang. *Infinite Impulse Response* - IIR).

Zaletą filtrów IIR jest możliwość uzyskania „stromych" charakterystyk amplitudowych przy niewielkiej liczbie współczynników wagowych. Jednak poważną wadą tych filtrów jest nieliniowa charakterystyka fazowa, która powoduje, iż sygnał po filtracji zmienia swój kształt, co w zastosowaniach biomedycznych nie może mieć miejsca [132]. Powyższy mankament sprawia, że filtry tego typu nie były brane pod uwagę.

Zdecydowano się na użycie filtrów FIR, których najważniejsze zalety to: prostota projektowania, nie wzbudzanie się oraz możliwość uzyskania liniowej charakterystyki fazowo-częstotliwościowej [152]. Pozytywy te okupione są dużo większą liczbą współczynników wagowych w stosunku do filtrów IIR, co wpływa na złożoność przetwarzania, jednak biorąc pod uwagę moc obliczeniową dzisiejszych komputerów, ostatecznie nie stanowi to dużego problemu.

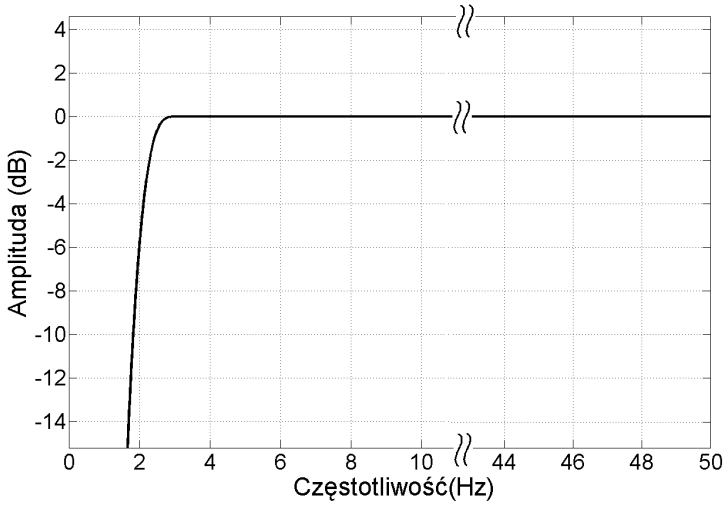
Na potrzeby wstępnej filtracji sygnału EKG zaprojektowano doświadczalnie filtr o następujących parametrach:

$$f_{stop} = 0,01 \text{ Hz}, f_{pass} = 2 \text{ Hz}, A_{stop} = 80 \text{ dB}, A_{pass} = 1 \text{ dB}.$$

Spośród wielu różnych podejść do konstrukcji filtrów cyfrowych wybrano metodę opartą na oknach. Jest ona bardzo prosta pod względem implementacyjnym, a jednocześnie efektywna. W tym przypadku funkcja $h(n)$ jest mnożona przez wybraną funkcję okna czasowego $w(n)$:

$$h_w(n) = h(n) \cdot w(n). \tag{6.2}$$

Wykorzystano okno parametryczne Keisera, ponieważ pozwala ono na kontrolowaną zmianę jego kształtu, a co za tym idzie, także kształtu charakterystyki projektowanego filtra [152]. Charakterystykę amplitudową uzyskanego układu przedstawiono na rys. 6.1.



Rys. 6.1. Charakterystyka amplitudowa filtra

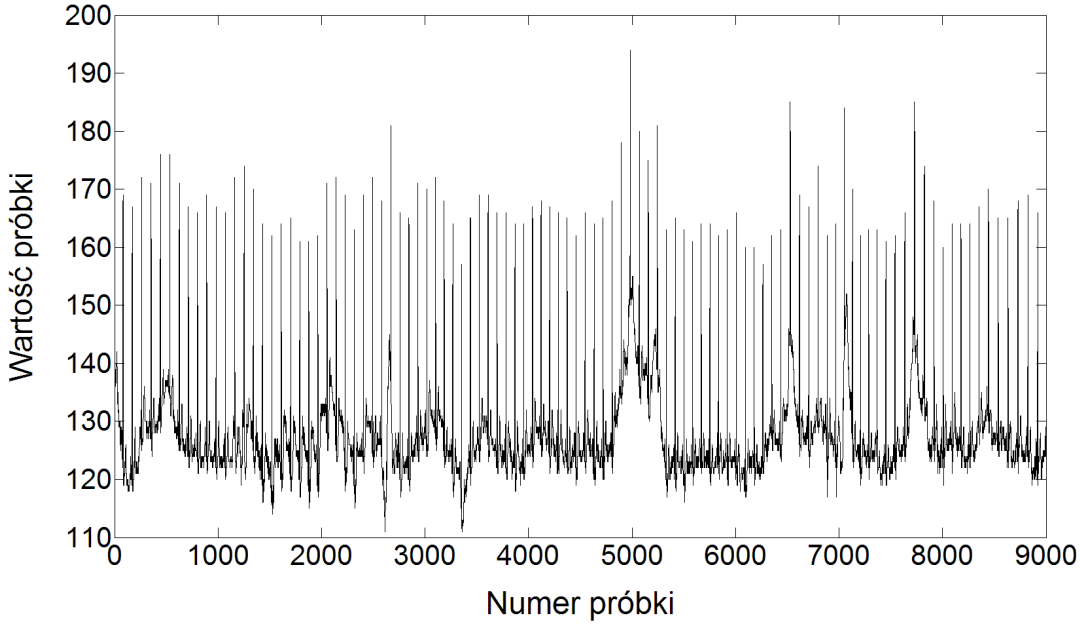
W przypadku użycia filtrów typu FIR próbki wejściowe i wyjściowe są przesunięte względem siebie o $M = (N-1)/2$ [152]. Dlatego też w każdym przypadku posłużenia się filtrem typu FIR należy zsynchronizować sygnały przed i po zastosowaniu filtracji. Liczba współczynników wagowych N uzyskanego filtra wstępnego wynosi 254. Stąd próbki wyjściowe są opóźnione o $M = (254-1)/2 = 126,5$ próbki względem próbek wejściowych. Oznacza to, iż nie jest możliwe dokładne zsynchronizowanie obu sygnałów, a różnica wynosi 0,5 próbki.

Na rysunkach 6.2 oraz 6.3 zaprezentowano przebiegi sygnałów EKG przed oraz po filtracji. Przedstawiono paczki fal zamiast pojedynczych okresów, aby pokazać działania skonstruowanego filtra w dłuższym czasie. Jak można zauważyć w wyniku zastosowania filtra górnoprzepustowego zakłócenia wolnozmienne zostały praktycznie całkowicie wyeliminowane.

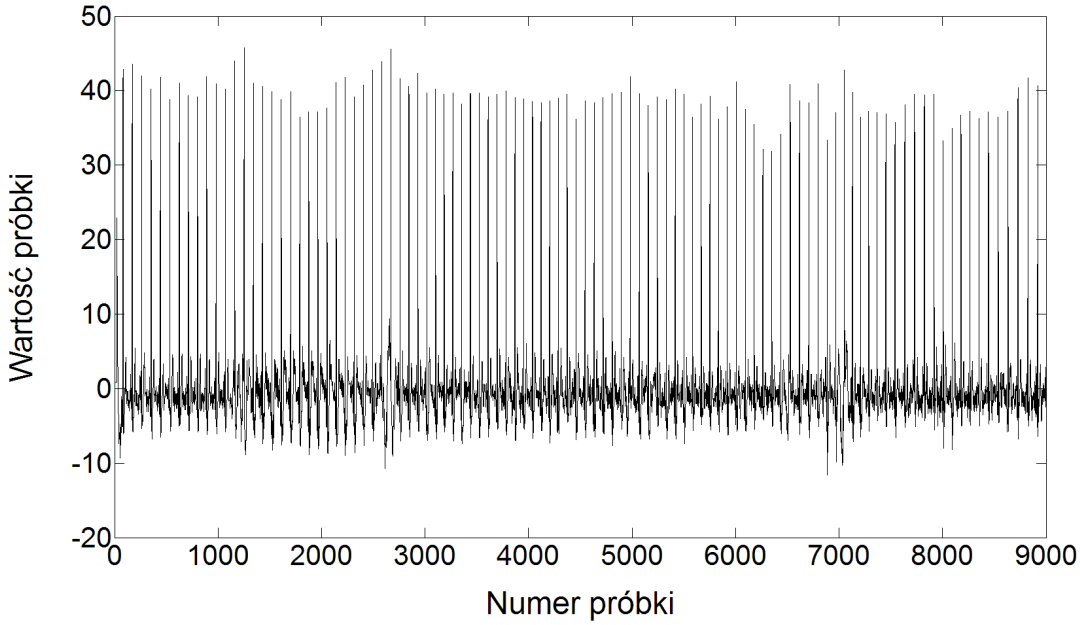
Następnym etapem przetwarzania jest detekcja zespołu QRS. Analiza sygnału EKG, (zarówno w zastosowaniach biomedycznych jak i biometrycznych) rozpoczyna się najczęściej od lokalizacji tego zespołu, a w szczególność punktu R jako punktu najbardziej charakterystycznego w tym sygnale. Każdy z załamków widocznych w zapisie elektrokardiogramu posiada swoje pasmo częstotliwości w widmie. Środek widma częstotliwości zespołu QRS to ok. 17 Hz, widmo załamków T znajduje się poniżej 10 Hz, a załamków P poniżej 7 Hz [135]. Bazując na powyższych informacjach zaprojektowano filtr cyfrowy, pasmowoprzepustowy o następujących parametrach:

$$f_{stop1} = 10 \text{ Hz}, f_{pass1} = 12.1 \text{ Hz}, f_{pass2} = 17 \text{ Hz}, f_{stop2} = 20 \text{ Hz},$$
$$A_{stop1} = 60 \text{ dB}, A_{pass} = 1 \text{ dB}, A_{stop2} = 80 \text{ dB}.$$

Tak, jak w przypadku filtra użytego do wstępnego przetwarzania sygnałów, również i tym razem skorzystano z metody konstrukcji filtrów cyfrowych, wykorzystują-

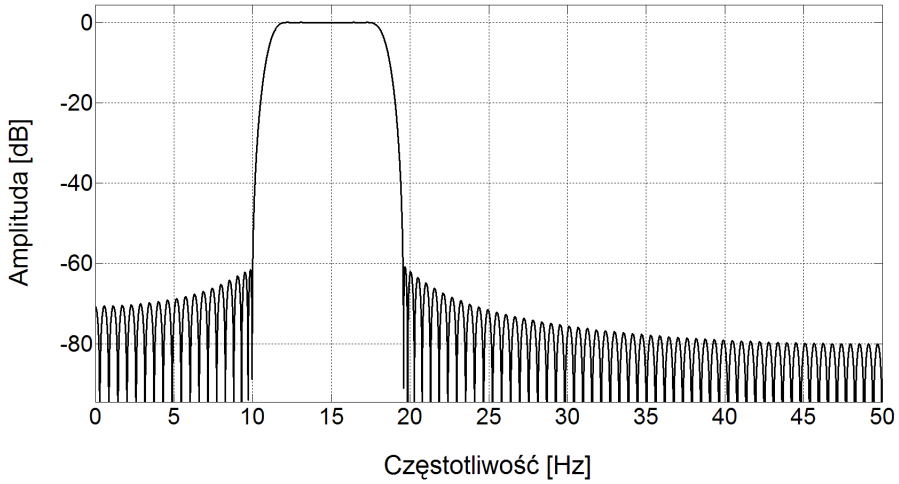


Rys. 6.2. Przebieg sygnału EKG przed filtracją



Rys. 6.3. Przebieg sygnału EKG po filtracji

cych parametryczne okna Keisera. Podobnie jak poprzednio, należało zsynchronizować ze sobą przebiegi wejściowe i wyjściowe. Liczba współczynników wagowych filtra N wynosi 173. Stąd sygnał wyjściowy należy przesunąć o $M = (173 - 1)/2 = 86$ próbki, aby odpowiadał on w fazie sygnałom wejściowym. Charakterystykę amplitudową uzyskanego filtra zaprezentowano na rysunku poniżej (rys. 6.4):



Rys. 6.4. Charakterystyka amplitudowa filtra do detekcji zespołu QRS

Jak widać na rys. 6.5b sygnał na wyjściu filtra pasmowoprzepustowego oscyluje w pobliżu zespołu QRS. Przebieg ten wymaga „prostowania", dzięki czemu zmienia się jego kształt do postaci wygładzonej. W tym celu stosuje się następującą transformację nieliniową, opartą na średniej kroczącej:

$$FO(n) = \frac{1}{2 * N + 1} \sum_{i=-N}^{N} x(n+i)^2, \tag{6.3}$$

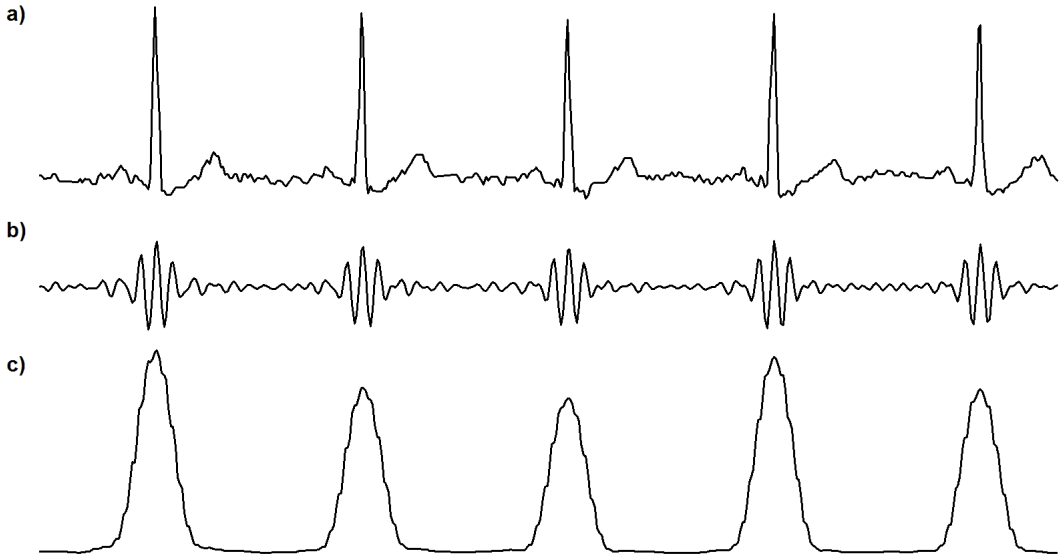
gdzie:

N - długość filtru średniej kroczącej.

Jedynym parametrem powyższej transformacji jest długość filtra średniej kroczącej. Na podstawie doświadczeń wartość parametru N została ustalona na 8. Otrzymane wierzchołki przebiegu wyjściowego nie są zbyt płaskie, a z drugiej strony nie posiadają zazębień, które utrudniają dokładną lokalizację zespułu QRS. Sygnał poddany transformacji 6.3 został przedstawiony na rys. 6.5c.

W celu lokalizacji punktów R należało zaprojektować moduł decyzyjny, którego zadaniem jest oznaczenie położenia tych punktów w sygnale EKG. Konieczne jest zdefiniowanie pewnych reguł decyzyjnych, na podstawie których dokonywano klasyfikacji poszczególnych próbek jako punkty R. Najprostszym sposobem na wyznaczenie lokalizacji tych punktów jest ustalenie pewnego progu, powyżej którego mogły się one znajdować.

Na podstawie obserwacji zarejestrowanych przebiegów zauważono, iż liczba punktów wokół załamka R, których amplituda była znacząco większa niż pozostała część sygnału EKG, wynosi około 3. Przy założeniu, iż zespół QRS występuję przeciętnie raz na sekundę to dla częstotliwości próbkowania 100Hz wynika, że tylko około



Rys. 6.5. Przebiegi sygnału EKG po kolejnych fazach procesu detekcji zespołu QRS a) po wstępnej filtracji b) po filtracji pasmowoprzepustowej c) po zastosowaniu średniej kroczącej

3% próbek sygnału funkcji opisującej FO o największej wartości amplitudy może zawierać załamek R. Na podstawie powyższych rozważań ustalono początkowy poziom detekcji t (poziom, powyżej którego rozpoczynamy poszukiwanie lokalnego maksimum) na wartość kwantyla rzędu $p = 0,97$ sygnału FO.

Jednak stały próg detekcji nie sprawdza się w przypadku przebiegów zmiennych takich jak sygnały biomedyczne. Dlatego też wprowadzono dodatkową regułę decyzyjną, która zapobiegała sytuacji, kiedy amplituda poszukiwanego załamka R była mniejsza niż początkowa wartość t (np. na skutek gwałtownych ruchów osoby badanej). Polega ona na obniżeniu wartości progu detekcji o połowę, w przypadku, gdy przez 2 sekundy nie odnaleziono żadnego punktu R. Czas ten wynika z faktu, iż puls zdrowego człowieka nie powinien wynosić mniej niż 30 uderzeń na minutę, czyli średnio dwa razy na sekundę. Jeżeli pomimo obniżenia progu o połowę punkt R nie został odnaleziony, to poziom detekcji ponownie zostaje zmniejszony o połowę. Ostatnia operacja jest powtarzana, aż punkt R zostanie odnaleziony. Formalny zapis algorytmu znajduje się poniżej (algorytm 6.1).

Na rys. 6.6 zaprezentowano wynik działania detektora punktów R. Jak można zauważyć (rysunek b), punkty R nie w każdym przypadku zostały poprawnie zlokalizowane, pomimo, że punkty będące lokalnymi maksimami przebiegu EKG po przekształceniach (rysunek a) są oznaczone prawidłowo. Jednym z powodów tych

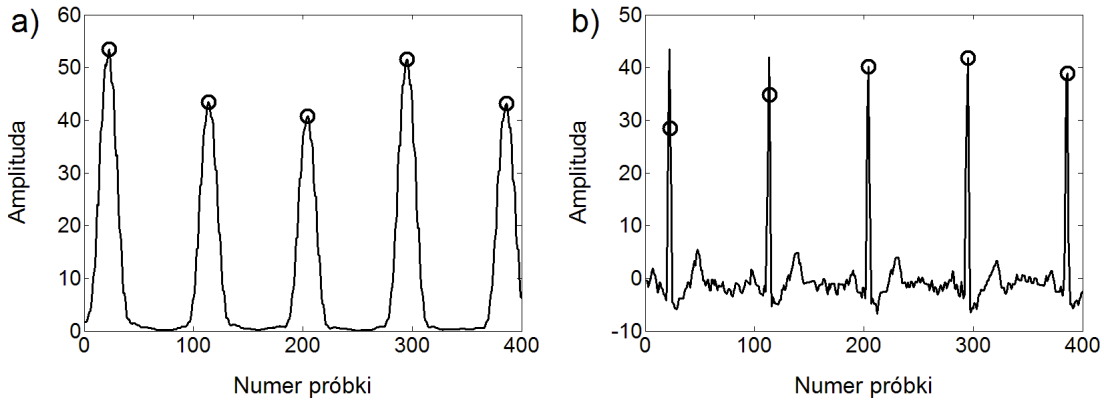
Algorytm 6.1: Wyznaczenie położenia punktów R

Dane wejściowe: Próbki sygnału EKG po średniej kroczącej EKG_{avr}

Dane wyjściowe: Pozycja punktów R

```
1  Ustaw poziom detekcji t na wartość kwantyla rzędu p = 0,97 sygnału EKG_avr
2  DOPÓKI są elementy do przetworzenia w EKG_avr
3      JEŻELI seria punktów w EKG_avr > t
4          Wybierz punkt maksymalny w serii r_max
5          JEŻELI r_max znajduje się dalej niż 250 ms R(n − 1)
6              Oznacz r_max jako kolejny punkt R(n)
7      JEŻELI dana seria została przetworzona ponownie
8          Przywróć próg czułości t do stanu początkowego
9      JEŻELI przez 2 sekundy nie znaleziono punktu R
10         Obniż próg czułości t do t/2
11         Cofnij przetwarzanie do poprzednio znalezionego punktu
           R(n − 1) + 300ms
```

niedokładności jest płaski wierzchołek funkcji opisującej, przez co kilka sąsiadujących ze sobą punktów ma tę samą wartość.



Rys. 6.6. Przebiegi sygnałów a) funkcji opisującej z zaznaczonymi lokalnymi maksimami b) przebieg EKG z zaznaczonymi punktami R

W celu dokładnego wyznaczenia pozycji punktów R zastosowano prosty algorytm korekcyjny. Jego działanie polega na znalezieniu lokalnych maksimów w przebiegu EKG po wstępnej filtracji w otoczeniu punktów wyznaczonych przez detektor opisany powyżej. Szerokość otoczenia wokół punktów R została ustalona doświadczalnie na ±3 próbki. Formalny zapis algorytmu został przedstawiony poniżej (algorytm 6.2).

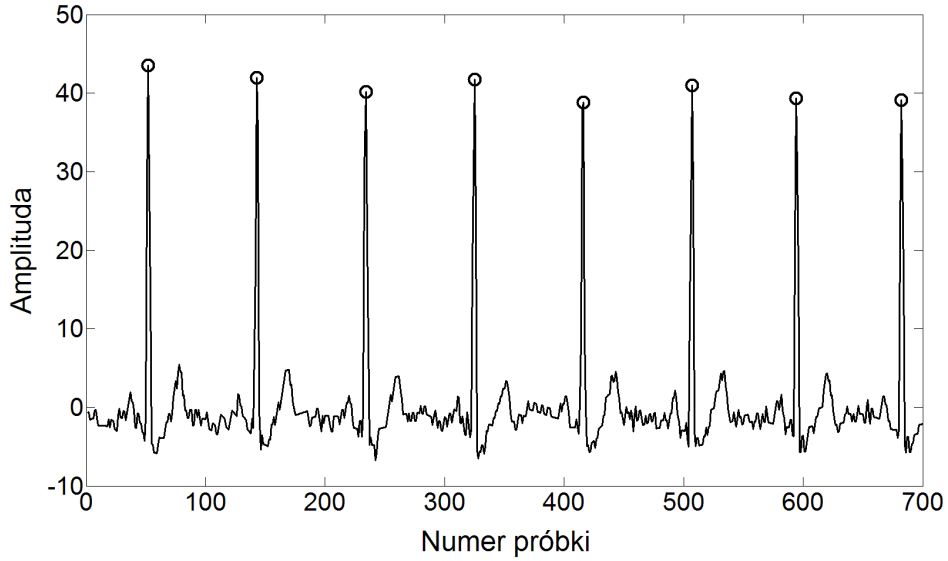
Algorytm 6.2: Korekta położenia punktów R

Dane wejściowe: Próbki sygnału EKG EKG, pozycja punktów R

Dane wyjściowe: Skorygowana pozycja punktów R_{kor}

1 **DLA KAŻDEGO** *punktu* R
2 Znajdź maksymalną wartość r_{max} w sygnale EKG w otoczeniu punktu $R(n)$
3 Oznacz r_{max} jako kolejny punkt $R_{kor}(n)$

Wynik działania algorytmu został przedstawiony na rys. 6.7. Jak widać wprowadzona korekta umożliwiła poprawną lokalizację poszukiwanych punktów charakterystycznych.



Rys. 6.7. Przebieg sygnału EKG z zaznaczonymi punktami R po zastosowaniu algorytmu korekcji

Ostatnim etapem wstępnego przetwarzania zarejestrowanego sygnału EKG jest obliczenie tętna i odległości pomiędzy kolejnym załamkami R. Odległość RR pomiędzy kolejnymi załamkami R obliczano z następującej zależności:

$$RR(i) = \frac{R(i+1) - R(i)}{F_s} * 1000, \quad i = 1, 2, \ldots, N-1, \tag{6.4}$$

gdzie:

F_s - częstotliwość próbkowania,

$R(i)$ - położenie punktu R.

6.1.2 Ekstrakcja cech biometrycznych

Dla porządku przypomina się w tym miejscu podstawowe pojęcia oraz zagadnienia statystyki matematycznej, które zostały wykorzystane w procesie selekcji cech. Należy wymienić przede wszystkim nieobciążone i mocno zgodne estymatory wartości oczekiwanej oraz wariancji populacji.

W przypadku dużej liczności próby można, w celu poprawienia przejrzystości prezentacji danych lub dla skrócenia czasu obliczeń, zebrać dane w tzw. szeregu rozdzielczym. Dzieli się wówczas zgromadzone wyniki według określonej cechy jakościowej lub ilościowej, z podaniem liczebności lub częstości każdej z wyodrębnionych klas. Jeśli liczba wartości, które może przyjmować zmienna losowa, jest niewielka, to buduje się szereg rozdzielczy punktowy. Gdy tych wariantów jest dużo, lub zmienna losowa ma charakter ciągły, buduje się szereg rozdzielczy przedziałowy.

Liczbę klas k estymuje się jako:

$$k \approx [\sqrt{n}], \tag{6.5}$$

gdzie:
n - liczność próby.

Szerokość h każdego z przedziałów to:

$$h = \frac{x_{max} - x_{min}}{k}, \tag{6.6}$$

gdzie:
k - liczba klas, wyznaczona przy użyciu 6.5,
x_{min}, x_{max} - odpowiednio najmniejsza i największa wartość próbki.

Wśród analizowanych cech znalazły się zarówno cechy dyskretne o niewielkim zbiorze wartości, jak i o charakterze ciągłym. W związku z powyższym wyrażenia opisujące poszczególne współczynniki przedstawione zostaną dla obu przypadków.

Ponadto przyjmuje się następujące oznaczenia:
x_{Li}−lewy koniec przedziału i-tej klasy, zawsze należy do przedziału,
x_{Pi}−prawy koniec przedziału i-tej klasy, należy do przedziału tylko w ostatniej klasie,
$\overline{x_i}$−średnia wartość i-tej klasy, wyznaczana jako $(x_{Li} + x_{Pi})/2$,
n_i−liczność i-tej klasy.

Średnią arytmetyczną liczb $x_1, \ldots, x_n$ nazywamy liczbę $\overline{x}$ określaną zależnością:

$$\overline{x} = \frac{1}{n} \sum_{i=1}^{n} x_i, \tag{6.7}$$

natomiast średnia szeregu rozdzielczego wyznaczana jest jako:

$$\overline{x} = \frac{1}{n} \sum_{i=1}^{k} \overline{x_i} \cdot n_i, \tag{6.8}$$

gdzie:
n - liczność próby,
x_i - wartość i-tej zmiennej losowej.

Odchylenie standardowe s próby losowej $x_1, \ldots, x_n$ wyrażone jest wzorem:

$$s = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (x_i - \overline{x})^2}, \tag{6.9}$$

natomiast dla szeregu rozdzielczego zachodzi zależność:

$$s = \sqrt{\frac{1}{n-1} \sum_{i=1}^{k} (\overline{x_i} - \overline{x})^2 \cdot n_i}, \tag{6.10}$$

gdzie:
n - liczność próby (zakłada się, że $n \leqslant 50$),
x_i - wartość i-tej zmiennej losowej,
$\overline{x}$ - średnia wartość z próbki, wyznaczona według wzoru 6.7
$\overline{x_i}$ - średnia wartość w i-tej klasie.

Kwantyl rzędu p zmiennej losowej to wartość taka, że prawdopodobieństwo zdarzenia takiego, że zmienna losowa będzie od niej mniejsza wynosi co najmniej p oraz prawdopodobieństwo zdarzenia takiego, że zmienna losowa będzie większa od tej wartości wynosi co najmniej $1 - p$. Jeżeli $p = 1/4, 1/2$ lub $3/4$, wówczas kwantyle nazywa się kwartylami. Kwartyl rzędu $p = 1/2$ nazywa się także medianą lub wartością środkową próbki $x_1, \ldots, x_n$, uporządkowanej w ciąg niemalejący:

$$x_{(1)} \leqslant x_{(2)} \leqslant \cdots \leqslant x_{(n)}.$$

Mediana jest zatem równa:

$$Q_{0,5} = \begin{cases} x_{(n+1)/2}, & \text{gdy } n \text{ nieparzyste}, \\ \frac{1}{2}(x_{(n/2)} + x_{(n/2)+2}), & \text{gdy } n \text{ parzyste}. \end{cases}, \tag{6.11}$$

natomiast dwa pozostałe kwartyle wyliczane są przy wykorzystaniu $Q_{0,5}$:

$$Q_{0,25} = \begin{cases} x_{(m+1)/2}, & \text{gdy } m \text{ nieparzyste,} \\ \frac{1}{2}(x_{(m/2)} + x_{(m/2)+2}), & \text{gdy } m \text{ parzyste.} \end{cases}, \tag{6.12}$$

$$Q_{0,75} = \begin{cases} x_{(m+n)/2}, & \text{gdy } (n-m+1) \text{ nieparzyste,} \\ \frac{1}{2}(x_{(m+(n-m-1)/2)} + x_{(m+(n-m+1)/2)}), & \text{gdy } (n-m+1) \text{ parzyste.} \end{cases}, \tag{6.13}$$

gdzie:
m - numer próbki, będącej medianą.

Inaczej wyraża się kwartyle w przypadku, gdy konstruowany jest szereg rozdzielczy przedziałowy:

$$Q_{0,25} = x_{L,0,25} + \frac{N_{0,25} - \sum_{i=1}^{m_{0,25}-1} n_i}{n_{0,25}} \cdot h_{0,25}, \tag{6.14}$$

$$Q_{0,5} = x_{L,0,5} + \frac{N_{0,5} - \sum_{i=1}^{m_{0,5}-1} n_i}{n_{0,5}} \cdot h_{0,5}, \tag{6.15}$$

$$Q_{0,75} = x_{L,0,75} + \frac{N_{0,75} - \sum_{i=1}^{m_{0,75}-1} n_i}{n_{0,75}} \cdot h_{0,75}, \tag{6.16}$$

gdzie:
$x_{L,i}$ - lewy koniec przedziału, zawierającego dany kwartyl,
N_i - numer próbki, będącej danym kwartylem ($N_i = n * i$),
m_i - numer klasy, do której należy dany kwartyl,
n_i - liczność klasy, do której należy dany kwartyl,
h_i - szerokość przedziału, do którego należy dany kwartyl.

Z kolei dominanta to wartość najczęściej występująca. Z tej definicji korzysta się w przypadku cechy, mogącej przyjmować wartości z mało licznego zbioru. Jednakże w przypadku cechy o charakterze ciągłym lub niemalże ciągłym, stosowane jest inne podejście.

Dominantą w szeregu rozdzielczym jest liczba obliczona na podstawie wzoru:

$$D(x) = x_{0d} + \frac{(n_d - n_{d-1})}{(n_d - n_{d-1}) + (n_d - n_{d+1})} \cdot h_d, \tag{6.17}$$

gdzie:

x_{0d} - dolna granica klasy dominanty,

n_d - liczebność klasy dominanty,

n_{d-1} - liczebność przedziału poprzedzającego dominantę,

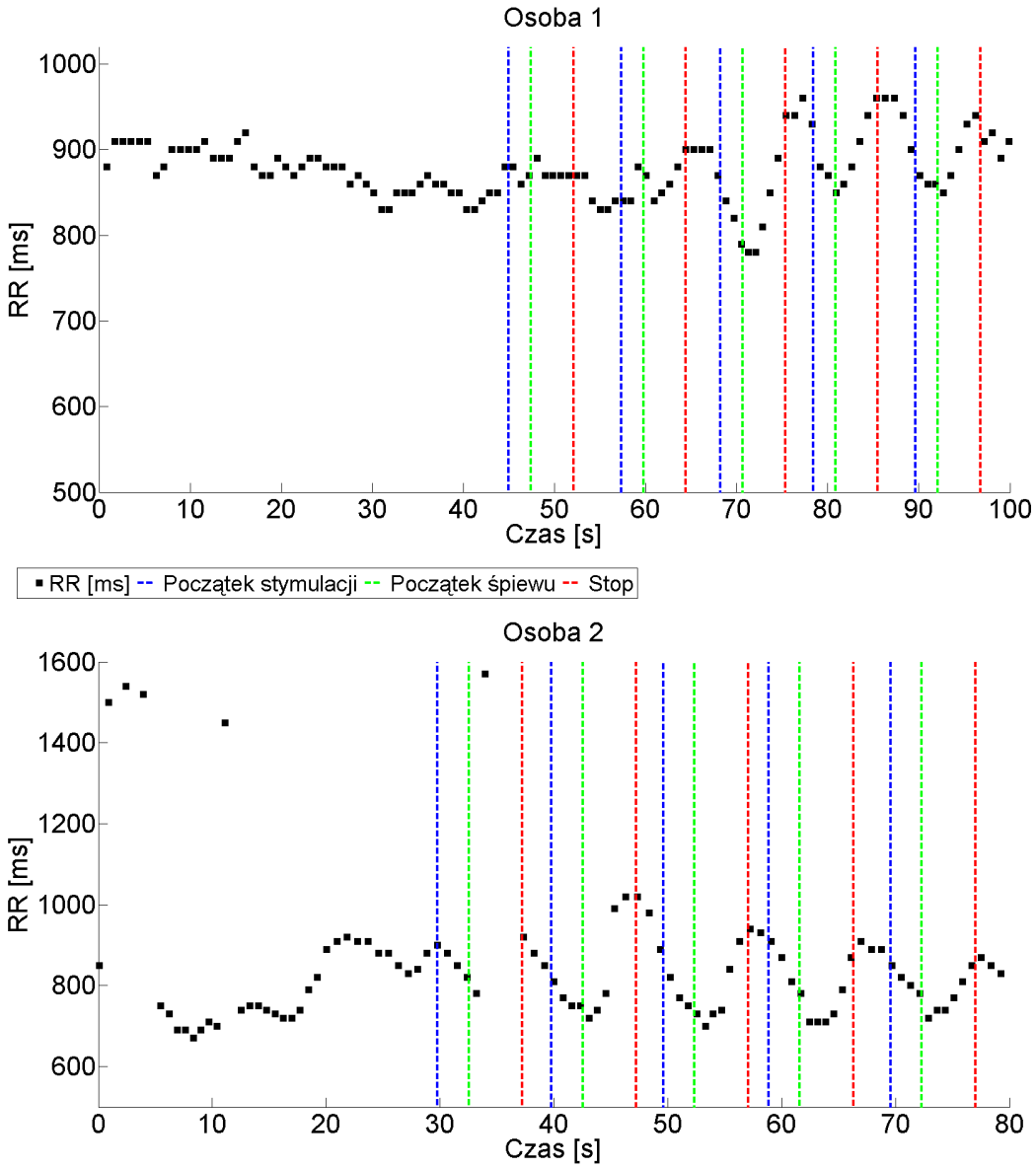
n_{d+1} - liczebność przedziału następującego po dominancie,

h_d - rozpiętość przedziału dominanty.

Obliczone wartości odległości RR pomiędzy kolejnymi punktami R posłużyły od utworzenia charakterystyk tej wielkości w funkcji czasu. Na ilustracji poniżej (rys. 6.8) przedstawiono dwa przykładowe przebiegi wartości RR od czasu dla dwóch różnych osób. Zaznaczono również charakterystyczne momenty czasu związane z pomiarami (początek stymulacji, początek odpowiedzi oraz koniec odpowiedzi). Na podstawie obserwacji otrzymanych przebiegów zauważono, że występuje znacząca zmiana w kształcie charakterystyki przed oraz po stymulacji dźwiękowej. W szczególności odnotowano, iż zmiany wartości odległości pomiędzy kolejnymi załamkami R są bardziej dynamiczne po stymulacji, aniżeli przed.

W celu potwierdzenia dokonanych obserwacji w sposób formalny, posłużono się statystyką matematyczną. Podzielono przebieg na przedziały zawierające po pięć punktów, natomiast ostatni przedział zawierał punktów $N \mod 5$ gdzie N to liczba punktów przebiegu. Szerokość przedziału dobrano doświadczalnie. W każdym przedziale punkty aproksymowane były wielomianem stopnia 1 $w(x) = a_1 x + a_0$, przy użyciu metody najmniejszych kwadratów, która to metoda polega na minimalizowaniu kwadratu odległości funkcji aproksymującej od węzłów aproksymacji. Jeżeli współczynnik a_1 był nieujemny, to wówczas do przedziału został przyporządkowany znak $\oplus$, natomiast w przeciwnym przypadku znak $\ominus$. Dla każdego przebiegu sprawdzano liczbę zmian znaków na jednostkę czasu przed oraz po stymulacji. Korzystając z parametrycznego testu istotności dla średniej zbadano przeciętną różnicę pomiędzy tymi wartościami m. Wykorzystano model, w którym przyjmuje się, że populacja generalna ma dowolny rozkład o średniej wartości m i o skończonej, ale nieznanej wartości wariancji σ^2. Ponadto zakłada się, że liczebność populacji jest duża - co najmniej rzędu kilku dziesiątek [33]. Testowano następującą hipotezę:

$$\begin{aligned} H_0 &: \quad m = 0, \\ H_1 &: \quad m > 0. \end{aligned}$$



Rys. 6.8. Przebieg odległości RR dla dwóch różnych osób

Statystyka testowa wyraża się wówczas jako:

$$u = \frac{\overline{x} - m}{s}\sqrt{n}, \tag{6.18}$$

gdzie:

u - wartość statystyki,

$\overline{x}$ - średnia z próby,

m - hipotetyczna wartość średniej w populacji,

n - liczność próby,

s - odchylenie standardowe z próby,

natomiast zbiór krytyczny wyraża się jako:

$K = [U_\alpha, \infty)$,

gdzie:

$\Phi(U_\alpha) = 1 - \alpha$,

$\Phi(\cdot)$ - wartość dystrybuanty rozkładu normalnego standardowego.

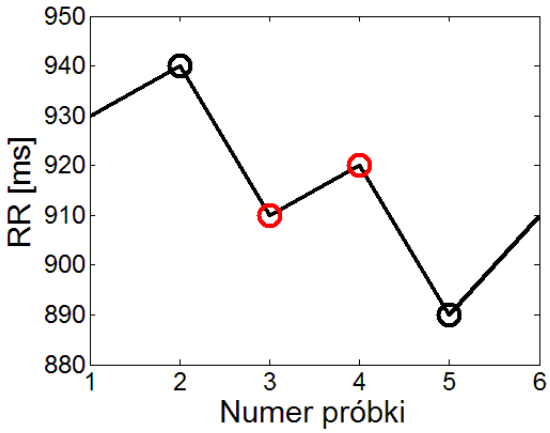
Na podstawie danych zgromadzonych podczas badań, opisanych w rozdziale 5. wyznaczono następujące wartości:

$s = 0{,}0381$,

$\overline{x} = 0{,}0139$,

$n = 63$.

Zbiór krytyczny dla $\alpha = 0{,}05$ jest równy $[1{,}64; \infty)$. Obliczona wartość statystyki to 2,89 i zawiera się w zbiorze krytycznym. Istnieją zatem podstawy do odrzucenia hipotezy zerowej na korzyść hipotezy alternatywnej. W ten sposób wykazano, że zmiany odległości pomiędzy kolejnymi załamkami R są bardziej dynamiczne po stymulacji aniżeli przed. Wyniki powyższego testu dały podstawy do obliczenia cech, które mogą umożliwić rozróżnienie poszczególnych osób biorących udział w eksperymencie. Korzystając ze wzorów 6.7, 6.9, 6.11, 6.12 i 6.17 obliczono odpowiednio: średnią, odchylenie standardowe, medianę, pierwszy kwartyl oraz dominantę przed i po stymulacji.



Rys. 6.9. Przebieg RR z zaznaczonymi poprawnymi (czarne) i błędnymi (czerwone) ekstremami

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. Niestety ten prosty

algorytm jest niewystarczający do poprawnego wyznaczenia punktów, które uznano za wierzchołki przebiegu. To przekształcenie ujawnia małe zaburzenia, które są interpretowane jako wierzchołki pierwotnego przebiegu 6.9. Należy więc wprowadzić kilka modyfikacji do algorytmu, aby działał on zgodnie z wymaganiami.

Pierwsza poprawka polegała na tym, iż dla każdych czterech punktów, które oznaczono jako potencjalne wierzchołki, obliczano różnice pomiędzy wartościami punktów skrajnych (1 i 4) h_{14} oraz pomiędzy wartościami punktów wewnętrznych (2 i 3) h_{23}. Jeżeli wartość różnicy h_{23} była czterokrotnie mniejsza niż h_{14}, oznaczało to, iż wśród tych czterech punktów znajdują się takie, które należy uznać za zakłócenia. W takim wypadku z tej czwórki pozostawiano punkt o wartości maksymalnej oraz minimalnej, a pozostałe dwa usuwano.

Drugie usprawnienie sprawdzało dla każdych trzech kolejnych punktów, czy ich wartości są nierosnące lub niemalejące. Jeżeli warunek był prawdziwy, to oznaczało to, że środkowy punkt oznaczony jako ekstremum jest tylko zakłóceniem i należy go usunąć ze zbioru wierzchołków. Ta modyfikacja została wprowadzona jako uzupełnienie pierwszej, w celu zapewnienia poprawnej eliminacji krótkotrwałych zakłóceń. Pełna postać algorytmu została przedstawiona w algorytmie 6.3.

Algorytm 6.3: Wyznaczanie ekstremów lokalnych na wykresie RR

Dane wejściowe: Punkty RR

Dane wyjściowe: Położenie i amplituda ekstremum w sygnale W

```
1  obliczenie pierwszej pochodnej dRR z przebiegu RR
2  DLA KAŻDEGO punktu w dRR
3      JEŻELI jeżeli zmienił się znak pochodnej
4          Oznacz punkt jako ekstremum
5      W PRZECIWNYM WYPADKU: JEŻELI pochodna w dwóch
       sąsiednich punktach jest zero
6          oblicz środek płaskiego wierzchołka jako ekstremum
7  DLA KAŻDYCH 4 punktów w W
8      JEŻELI 1/4 h14 > h23
9          znajdź wartość minimalną i maksymalną spośród 4 punktów
10         usuń pozostałe dwa punkty ze zbioru W
11 DLA KAŻDYCH 3 punktów w W
12     JEŻELI wartości trzech sąsiednich wierzchołków są niemalejące albo
       nierosnące
13         usuń środkowy wierzchołek
```

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:

$$s(n) = \frac{y_n - y_{n-1}}{x_n - x_{n-1}} \tag{6.19}$$

  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,

$$w_e(n) = x_{n+1} - x_{n-1}; \tag{6.20}$$

  gdzie:

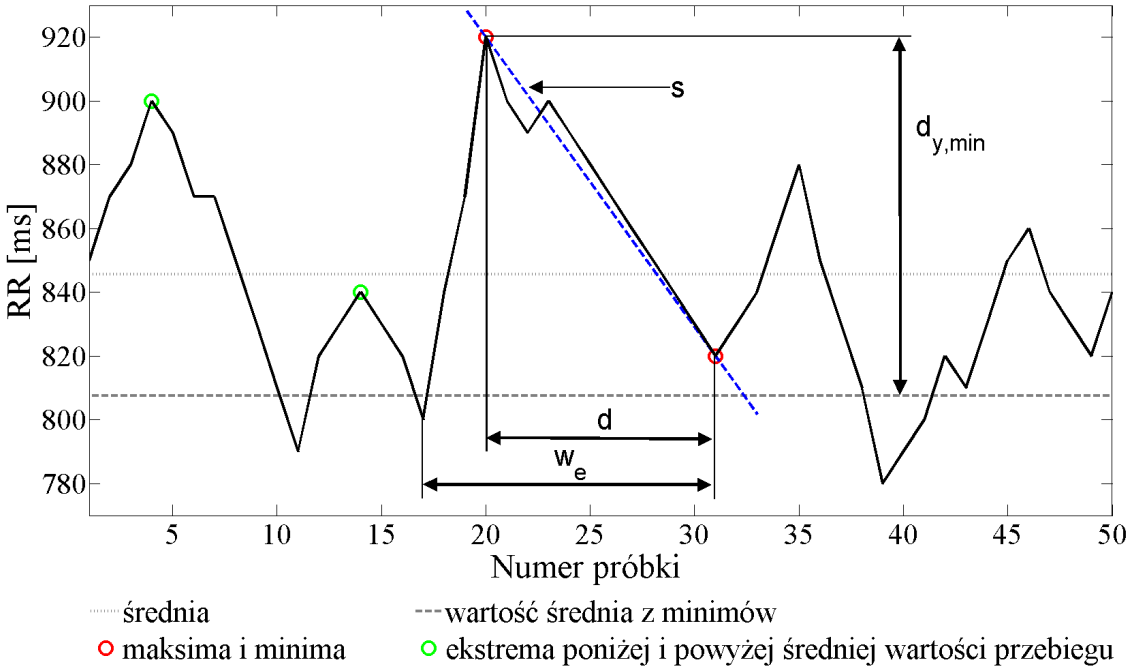
  x - położenie ekstremum.

Na rysunku 6.10 przedstawiono wszystkie wymienione powyżej cechy.

6.2 Analiza sygnału głosu

6.2.1 Przetwarzanie wstępne sygnału mowy

W przypadku sygnału mowy przetwarzanie wstępne ograniczało się do podzielenia zarejestrowanego 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.



Rys. 6.10. Przebieg *RR* z zaznaczonymi proponowanymi cechami

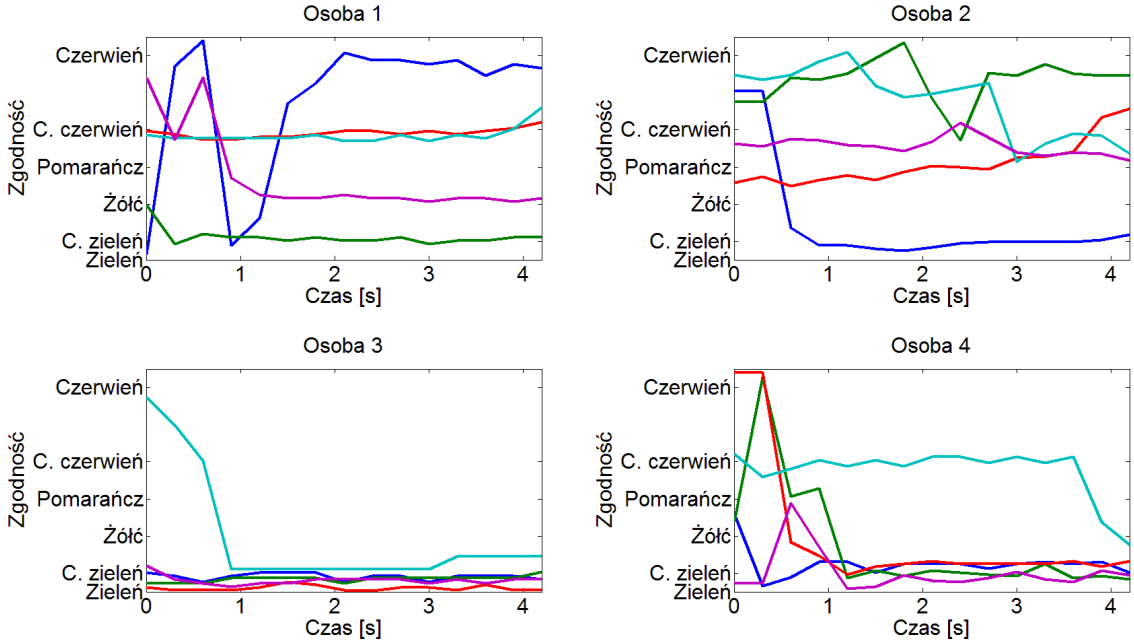
6.2.2 Ekstrakcja cech biometrycznych

Jak wspomniano w rozdziale 4.2, głos emitowany przez człowieka zawiera zarówno cechy behawioralne jak i fizjologiczne. Dlatego też poniżej skupiono się na obu grupach cech, w celu utworzenia jak największego zbioru unikalnych współczynników.

Cechy behawioralne

Na podstawie zarejestrowanych próbek głosu sporządzono wykresy stopnia dopasowania (wyrażonego w kolorach zgodnie ze wzorem 5.6) w zależności od czasu trwania eksperymentu dla poszczególnych prób. 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. Na rysunku poniżej (rys. 6.11) przedstawiono przykładowe przebiegi dla czterech różnych osób. Jak można zauważyć, dla każdego z badanych użytkowników jego charakterystyka dopasowania jest inna od pozostałych.

Następny rysunek (rys. 6.12) przedstawia również przebiegi zgodności dla trzech użytkowników, z których wynika, iż wykresy dla poszczególnych osób są do siebie podobne.

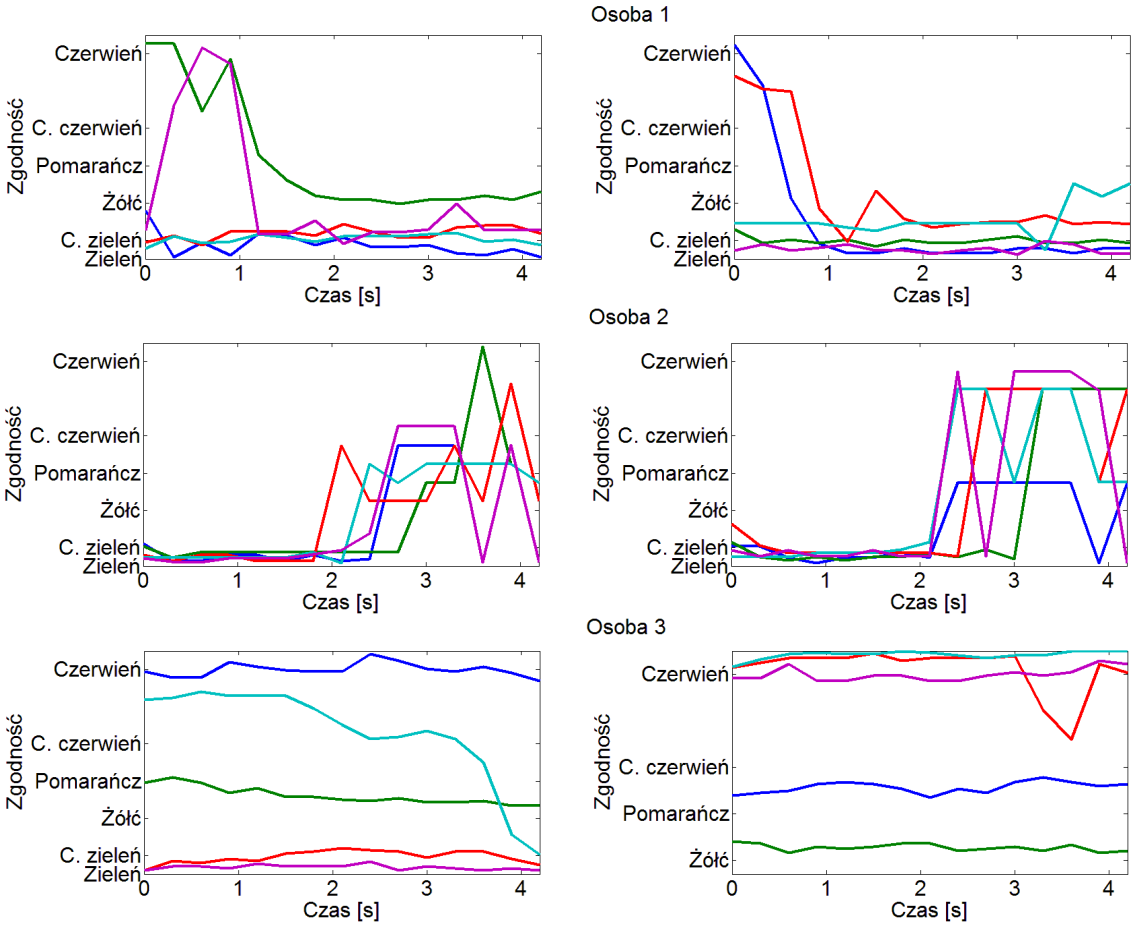


Rys. 6.11. Przebiegi zgodności dla czterech osób

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 (6.7), odchylenie standardowe (6.9), pierwszy i trzeci kwartyl (6.12,6.13), medianę (6.11) oraz dominantę zgodnie z definicją dla cechy przyjmującej wartości z mało licznego zbioru, przedstawioną już uprzednio dla sygnału EKG w rozdziale 6.1.2.

Obliczano także rodzaj głosu w następujący sposób: dla pojedynczego eksperymentu składającego się z pięciu prób (szczegółowy opis warunków eksperymentu zawiera podpunkt 5.2.2) wylicza się najniższą oraz najwyższą częstotliwość podsta-



Rys. 6.12. Przebiegi zgodności dla trzech różnych osób

wową wygenerowaną przez użytkownika w czasie badania. Następnie na podstawie tych częstotliwości przypisuje się danemu użytkownikowi jego rodzaj głosu korzystając z tablicy 6.1. Jeżeli dolna i górna częstotliwość wskazuje na inny rodzaj głosu, to wybiera się głos wyższy. Zapis algorytmu przedstawiono poniżej algorytm 6.4.

Cechy fizjologiczne

W zaproponowanym powyżej oknie czasowym (ramce) obliczono także współczynniki mel–spektralne oraz mel–cepstralne. Algorytm wyznaczania tych cech omówiono poniżej. Na wstępie ramka poddawana jest preemfazie, czyli filtracji filtrem FIR o postaci:

$$\widetilde{x}(n) = x(n) - 0,97x(n-1). \tag{6.21}$$

Dzięki temu przekształceniu wzmacniane są wyższe częstotliwości sygnału.

Tab. 6.1. Zakres częstotliwości poszczególnych rodzajów głosów od najniższego do najwyższego (na podstawie [7, 21])

Głos	**Dolny zakres [Hz]**	**Górny zakres [Hz]**
Bas	≈ 82	≈ 329
Baryton	≈ 87	≈ 349
Tenor	≈ 130	≈ 523
Alt	≈ 174	≈ 698
Mezzosopran	≈ 220	≈ 880
Sopran	≈ 1046	≈ 4186

Algorytm 6.4: Wyznaczanie rodzaju głosu

Dane wejściowe: Wektor próbek sygnału głosu S

Dane wyjściowe: Rodzaj głosu RG

Dane: Minimalna częstotliwość podstawowa $F_{0,min}$, tablica zakresów głosu TZB, maksymalna częstotliwość podstawowa $F_{0,max}$

1 **DLA KAŻDEJ** *Ramki sygnału o długości 300ms* $S(i)$
2 Wyznacznie częstotliwości podstawowej w ramce $F_{0,i}$
3 Aktualizacja wartości $F_{0,min}$ i $F_{0,max}$=0
4 **JEŻELI** $F_{0,min} \in TBZ(i)$ *i* $F_{0,max} \in TBZ(i)$
5 $RG = TBZ(i)$
6 **W PRZECIWNYM WYPADKU: JEŻELI** $F_{0,min} \in TBZ(i)$ *i* $F_{0,max} \in TBZ(i+1)$
7 $RG = TBZ(i+1)$

Ponieważ analiza częstotliwościowa przeprowadzana będzie tylko na podstawie N próbek sygnału, należy wyznaczyć iloczyn sygnału z odpowiednim oknem czasowym, które przyjmuje wartości niezerowe jedynie w zakresie $0, 1, \ldots N-1$.

$$y(n) = \widetilde{x}(n) * w(n), \tag{6.22}$$

gdzie $w(n)$ jest dowolnym oknem czasowym. W przypadku analizy mel–spektralnej wykorzystuje się okno Hamminga w_H, którego funkcja podana jest następującym wzorem:

$$w_H(n) = 0,54 - 0,46\cos\left(\frac{2\pi n}{N-1}\right), \quad n = 0, 1, 2, \ldots, N-1. \tag{6.23}$$

W następnym kroku należy wyznaczyć dyskretną transformatę Fouriera (DFT):

$$Y(k) = F[y(n)], \tag{6.24}$$

gdzie: $Y(k)$ - sygnał uzyskany w wyniku transformacji, $y(n)$ - sygnał oryginalny.

Równanie dyskretnej transformaty Fouriera ma postać:

$$Y(k) = \sum_{n=0}^{N-1} y(n) e^{\frac{-2ikn\pi}{N}}, \quad k = 0, 1, 2, \ldots, N-1. \tag{6.25}$$

Następnie należy obliczyć kwadrat modułu dla każdego zespolonego współczynnika Fouriera:

$$FC(k) = |Y(k)|^2. \tag{6.26}$$

W praktycznych obliczeniach numerycznych zamiennie do obliczeń według wzoru 6.24 wykorzystuje się szybką transformatę Fouriera (FFT).

Uzyskane widmo uśrednia się za pomocą nakładających się na siebie funkcji wagowych o kształcie trójkątnym. Wielkość tego uśrednienia rośnie wraz z częstotliwością. Dzięki temu uwzględnia się podstawy percepcji dźwięku przez człowieka, który lepiej rozróżnia częstotliwości niższe (<1kHz), aniżeli wyższe [59]. Przy projektowaniu zestawu filtrów trójkątnych korzysta się ze skali mel, w której częstotliwość wyraża się w melach. Zależność pomiędzy skalą wyrażoną w hercach a skalą mel przedstawia następujące równanie:

$$f_{mel} = 1127,01048 \cdot \ln\left(1 + \frac{f}{700}\right). \tag{6.27}$$

W skali mel zaprojektowano L identycznych, symetrycznych filtrów trójkątnych D o takiej samej podstawie, pokrywających się w 50% i obejmujących zakres częstotliwości [0;8000Hz]. Następnie należało je przetransformować do skali hercowej za pomocą przekształcenia odwrotnego do (6.27):

$$f = 700 \cdot \left(e^{m/1127,01048} - 1\right). \tag{6.28}$$

Uzyskane w ten sposób filtry trójkątne (już nie symetryczne) stosuje się do uśredniania widma uzyskanego z równania 6.26. Proces ten można zapisać za pomocą poniższej zależności:

$$MFC(l) = \sum_{k=0}^{N-1} [D(l,k) \cdot FC(k)], \quad l = 1, 2 \ldots, L, \tag{6.29}$$

gdzie: l - numer kolejnego filtru trójkątnego. W wyniku powyższego przekształcenia uzyskuje się współczynniki mel–spektralne (ang. *Mel Frequency Coefficients* - MFC), których liczba jest określona przez liczbę trójkątnych filtrów L.

Cepstrum jest to wynik charakterystycznego przekształcenia:

$$cepstrum = FFT^{-1}(log(|FFT(x)|)). \tag{6.30}$$

Analogicznie w przypadku współczynników mel–cepstralnych (ang. *Mel Frequency Cepstral Coefficients* - $MFCC$) należy dokonać transformacji odwrotnej. W tym celu współczynniki mel–spektralne są logarytmowane, a następnie mnożone przez transformatę kosinusową DCT-II [116].

$$MFCC(m) = \sum_{l=1}^{L} \left[\log(MFC(l)) \cdot \cos\left(\frac{m \cdot (2l+1)\pi}{2L} \right) \right], \quad m = 1, 2 \ldots, M, \tag{6.31}$$

gdzie: m - numer współczynnika $MFCC$.

Wyznaczono 32 współczynniki MFC oraz 24 współczynniki MFCC.

Względnie duża liczba wyznaczonych współczynników zasadniczo bywa niekorzystna. Użycie odpowiednio dobranych narzędzi numerycznych redukuje jednakże ten problem do powielania pewnych, schematycznych działań optymalizacyjnych. Z drugiej jednak strony można domniemywać, iż wzrost liczby współczynników opisu cech biometrycznych implikuje zwiększenie prawdopodobieństwa natrafienia na wskaźnik o zadowalającej dystynktywności i oczekiwanej stabilności.

6.3 Połączenie modalności

W tabelach 6.2 i 6.3 zestawiono współczynniki, które zostały wyselekcjonowane z sygnału głosu oraz z sygnału EKG. Zadanie optymalizacyjne polega na wyborze tych wskaźników, które pozwolą na najlepsze rozróżnienie badanych osób.

Tab. 6.2. Zestawienie proponowanych współczynników dla sygnału głosu

Lp.	**Nazwa**	**Miejsce opisu**
1	rodzaj głosu	algorytm 6.4
2	średnia wartość dopasowania	równanie 6.7
3	odchylenie standardowe dopasowania	równanie 6.9
4	I kwartyl dopasowania	równanie 6.12
5	mediana dopasowania	równanie 6.11
6	III kwartyl dopasowania	równanie 6.13
7	dominanta dopasowania	podpunkt 6.1.2
8	32 współczynniki mel–spektralne	równanie 6.29
9	24 współczynniki mel–cepstralne	równanie 6.31

Tab. 6.3. Zestawienie proponowanych współczynników dla sygnału EKG

Lp.	Nazwa	Miejsce opisu
1	średnia EKG przed stymulacją	równanie 6.7
2	odchylenie standardowe EKG przed stymulacją	równanie 6.9
3	I kwartyl EKG przed stymulacją	równanie 6.12
4	mediana EKG przed stymulacją	równanie 6.11
5	dominanta EKG przed stymulacją	równanie 6.17
6	średnia EKG po stym.	równanie 6.7
7	odchylenie standardowe EKG po stymulacji	równanie 6.9
8	I kwartyl EKG po stymulacji	równanie 6.12
9	mediana EKG po stymulacji	równanie 6.11
10	dominanta EKG po stymulacji	równanie 6.17
11	pochylenie ekstremów	równanie 6.19
12	odległość pomiędzy ekstremami	podpunkt 6.1.2
13	wartość ekstremów	podpunkt 6.1.2
14	szerokość ekstremów	równanie 6.20
15	liczba ekstremów powyżej średniej	podpunkt 6.1.2
16	liczba ekstremów poniżej średniej	podpunkt 6.1.2
17	liczba maksimów lokalnych	podpunkt 6.1.2
18	liczba minimów lokalnych	podpunkt 6.1.2
19	wartość maksimów lokalnych względem wartości średniej minimów	podpunkt 6.1.2

Zdecydowano się na analizę poszczególnych zbiorów cech osobno, w celu wyłonienia z każdego z nich najlepszego zestawu. Dzięki temu utworzony wektor cech będzie zawierał zarówno cechy związane z sygnałem EKG, jak również cechy behawioralne i fizjologiczne głosu. W przypadku analizy metodami automatycznymi wszystkich cech równocześnie może zdarzyć się sytuacja, w której te wyłonione na podstawie jednej z rejestrowanych biometryk, zostaną całkowicie odrzucone z powodu niskiej dystynktywności. Sytuacja ta w przypadku biometrii multimodalnej jest dalece niepożądana.

Jako pierwsze poddano analizie cechy EKG oraz behawioralne głosu. Wykorzystano liniową dyskryminację Fisher'a (*Fisher Linear Discrimination* - FLD), która zostanie omówiona poniżej.

6.3.1 Dyskryminacja Fisher'a

Proces klasyfikacji danych testowych może opierać się na wszystkich dostępnych miarach lub tylko na kilku wyselekcjonowanych, które w sposób znaczący różnicują poszczególne klasy. Analiza dyskryminacji służy do rozstrzygania, czy poszczególne współrzędne są istotne w procesie klasyfikacji, czy też wprowadzają jedynie tzw. „szumy".

Dane niech będą w postaci:

$$\forall i \ \in \{1,\ldots,k\}\ X_i = \begin{bmatrix} x_{i,1,1} & x_{i,1,2} & \cdots & x_{i,1,n_i} \\ x_{i,2,1} & x_{i,2,2} & \cdots & x_{i,2,n_i} \\ \vdots & \vdots & \ddots & \vdots \\ x_{i,p,1} & x_{i,p,2} & \cdots & x_{i,p,n_i} \end{bmatrix}. \tag{6.32}$$

Niech:

p - aktualny wymiar wektora danych - tu: liczba wyłonionych współczynników,

k - liczba rozważanych klas - tu: liczba zarejestrowanych osób,

n_i - liczność i-tej klasy,

N - suma liczności wszystkich klas,

$\bar{x}_i$ - p-wymiarowy wektor średni każdej klasy,

$\bar{x}$ - p-wymiarowy wektor średni dla wszystkich danych,

S - wspólna macierz kowariancji, zdefiniowana następująco:

$$S = \frac{1}{N-k}\sum_{i=1}^{k} A_i, \tag{6.33}$$

gdzie: $\forall i \ \in \{1,\ldots,k\}$

$$A_i = \begin{bmatrix} \sum_{j=1}^{n_i}(x_{i,1,j}-\bar{x}_{i,1})^2 & \cdots & \sum_{j=1}^{n_i}(x_{i,1,j}-\bar{x}_{i,1})(x_{i,p,j}-\bar{x}_{i,p}) \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^{n_i}(x_{i,p,j}-\bar{x}_{i,p})(x_{i,1,j}-\bar{x}_{i,1}) & \cdots & \sum_{j=1}^{n_i}(x_{i,p,j}-\bar{x}_{i,p})^2 \end{bmatrix}. \tag{6.34}$$

Algorytm redukcji wymiaru danych przedstawia się w sposób następujący:

1. Wyznaczana jest miara dyskryminacyjna :

$$T^2(y_1,\ldots,y_p) = \frac{1}{N-k}\sum n_i(\bar{x}_i-\bar{x})^T S^{-1}(\bar{x}_i-\bar{x}). \tag{6.35}$$

2. Wyznaczana jest miara dyskryminacyjna przy uwzględnieniu nieobecności i-tej zmiennej:

$$T_i^2(y_1,\ldots,y_p) = T^2(y_1,\ldots,y_{i-1},y_{i+1},\ldots,y_p). \tag{6.36}$$

3. Sprawdzana jest niezbędność każdej współrzędnej:

$$U_i = T^2(y_1, \ldots, y_p) - T_i^2(y_1, \ldots, y_p). \tag{6.37}$$

4. Stawiana jest hipoteza zerowa i hipoteza alternatywna:

$$\begin{aligned} H_0 &: U_{i_{min}} = 0; \\ H_1 &: U_{i_{min}} \neq 0. \end{aligned} \tag{6.38}$$

5. Sprawdzana jest wartość statystyki:

$$F = \frac{N-k-p+1}{k-1} \cdot \frac{U_i}{1 + T^2(y_1, \ldots, y_p) - U_i}. \tag{6.39}$$

6. Wyznaczona statystyka F ma rozkład F-Snedecora o odpowiednio $k-1$ i $N-k-p+1$ stopniach swobody.

7. Przy ustalonym poziomie ufności α tworzony jest zbiór krytyczny.

8. Jeśli wartość statystyki nie należy do zbioru krytycznego, wówczas w procesie klasyfikacji można bez straty informacji pominąć i-tą współrzędną. Algorytm należy powtórzyć, rozpoczynając od kroku pierwszego, pamiętając, że wymiar wektora p zmniejszył się o 1.

9. W przeciwnym wypadku algorytm kończy działanie - pominięcie którejkolwiek z pozostałych współrzędnych może mieć znaczący wpływ na poprawność działania klasyfikatora.

W wyniku powyższej analizy otrzymano 2 cechy związane z behawioryzmem głosu oraz 3 wyznaczone dla EKG. Są to odpowiednio:

1. Głos:
   - rodzaj głosu,
   - mediana.
2. EKG:
   - średnia EKG po stymulacji,
   - odchylenie EKG po stymulacji,
   - mediana EKG przed stymulacją.

Otrzymane wyniki sprawdzono pod kątem ich rozmieszczenia w przestrzeni cech. Miało to na celu dowiedzenie, że odległość pomiędzy wektorami przypisanymi do jednej osoby jest ze statystycznego punktu widzenia mniejsza, aniżeli pomiędzy wektorami odpowiadającymi dwóm różnym osobom.

Mając dane i-te wektory cech dwóch osób x_k oraz y_k, o długości p, wyznaczono odległość euklidesową pomiędzy nimi:

$$d(x_i, y_i) = \sqrt{\sum_{j=1}^{p}(x_{i,j} - y_{i,j})^2}. \tag{6.40}$$

Następnie obliczano średnią odległość pomiędzy wszystkimi wektorami jednej i drugiej osoby:

$$\bar{d} = \frac{\sum_{k=1}^{m}\sum_{l=1}^{n} d(x_k, y_l)}{m \cdot n} \tag{6.41}$$

gdzie: m i n to liczba wektorów cech odpowiednio pierwszej i drugiej osoby.

W przypadku tej samej osoby korzystano z następującego wzoru:

$$\bar{d} = \frac{\sum_{k=1}^{m-1} d(x_k, x_{k+1})}{2k} \tag{6.42}$$

gdzie m to liczba wektorów współczynników danej osoby.

Wyniki obliczeń zebrano w tabeli 6.4. Widać wyraźnie, iż odległości pomiędzy wektorami tej samej osoby są większe, aniżeli średnia odległość pomiędzy daną osobą, a pozostałymi. Tylko w przypadku osób 7 i 12 można zauważyć odstępstwo od tej reguły. Uzyskane rezultaty dają podstawę do wykorzystania wybranego zestawu cech w biometrycznej weryfikacji tożsamości.

Poniżej przedstawiono rozmieszczenie punktów reprezentujących wartości cech badanych osób w przestrzeni trójwymiarowej. Na rysunku 6.13 zaprezentowano wektory cech w przestrzeni, której wymiarami są dwa współczynniki głosu, uzupełnione o jedną miarę związaną z EKG. Jak można zauważyć, punkty związane z poszczególnymi osobami tworzą pewne wydzielone wycinki przestrzeni, aczkolwiek nie w każdym przypadku są one rozłączne.

Rysunek 6.14 pokazuje wartości cech tych samych osób jak na poprzednim rysunku, ale w przestrzeni, której wymiary tworzą współczynniki EKG, otrzymane w wyniku analizy dyskryminacyjnej. Również w tym wypadku można wyodrębnić obszary utworzone przez punkty należące do tych samych osób, lecz tutaj wycinki te nie pokrywają się.

Tab. 6.4. Średnie odległości euklidesowe pomiędzy wektorami cech poszczególnych osób

	u1	**u2**	**u3**	**u4**	**u5**	**u6**	**u7**	**u8**	**u9**	**u10**	**u11**	**u12**
u1	2,7	6,5	6,6	9,5	7,7	8,0	9,5	13,2	9,1	21,3	7,7	9,4
u2	6,5	2,3	4,7	6,1	4,5	3,1	5,8	8,4	5,9	16,1	4,5	6,4
u3	6,6	4,7	5,4	6,5	6,6	5,4	6,7	10,8	6,0	18,0	5,1	7,5
u4	9,5	6,1	6,5	7,9	6,9	6,3	6,5	9,7	6,3	15,2	6,1	7,7
u5	7,7	4,5	6,6	6,9	5,5	5,2	6,8	7,3	6,3	14,4	6,7	6,9
u6	8,0	3,1	5,4	6,3	5,2	3,9	6,0	8,1	6,3	15,4	4,8	6,7
u7	9,5	5,8	6,7	6,5	6,8	6,0	7,6	8,7	6,6	14,1	6,2	7,4
u8	13,2	8,4	10,8	9,7	7,3	8,1	8,7	4,9	7,8	9,3	10,3	8,3
u9	9,1	5,9	6,0	6,3	6,3	6,3	6,6	7,8	6,1	13,7	7,0	7,1
u10	21,3	16,1	18,0	15,2	14,4	15,4	14,1	9,3	13,7	7,8	17,1	13,9
u11	7,7	4,5	5,1	6,1	6,7	4,8	6,2	10,3	7,0	17,1	6,8	7,4
u12	9,4	6,4	7,5	7,7	6,9	6,7	7,4	8,3	7,1	13,9	7,4	9,3
u	10,4	7,0	8,3	8,2	7,3	7,2	7,9	9,1	7,7	14,7	8,0	8,2

6.3.2 Analiza składowych głównych

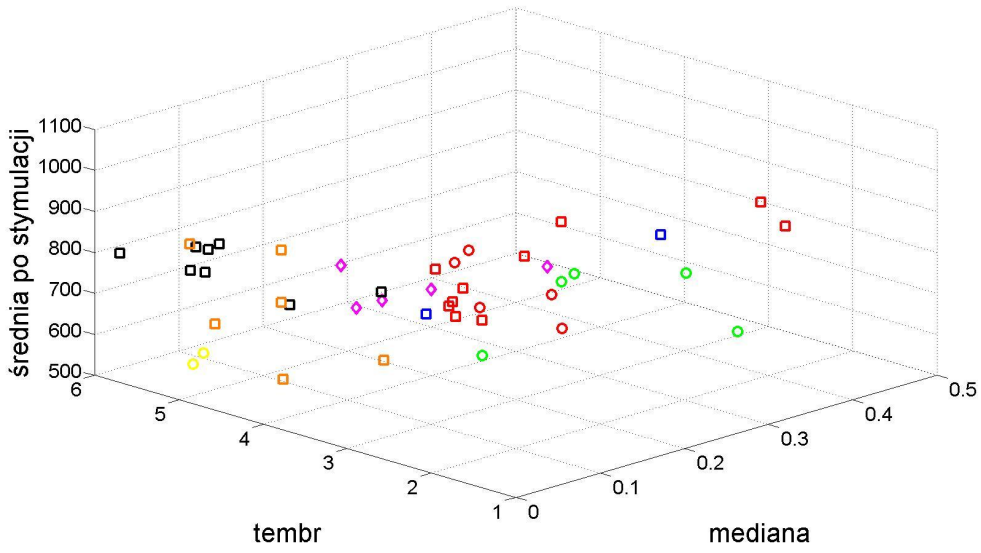
W przypadku parametrów, których długość wektora była większa niż 1 (mel–spektrum oraz mel–cepstrum), każdy z nich był analizowany osobno w celu wyznaczenia najlepszych kombinacji współczynników. Ze względu na stosunkowo dużą liczbę cech zdecydowano się na wykorzystanie jeszcze jednej, poza liniową dyskryminacją, metody redukcji wymiarowości i doboru odpowiedniej kombinacji cech. Wybrano metodę analizy składowych głównych (ang. *Principal Components Analysis* - PCA), ze względu na jej skuteczność oraz popularność wynikającą z prostoty implementacji. Poniżej zostaną opisane kolejne kroki tej metody.

Dane niech będą w postaci:

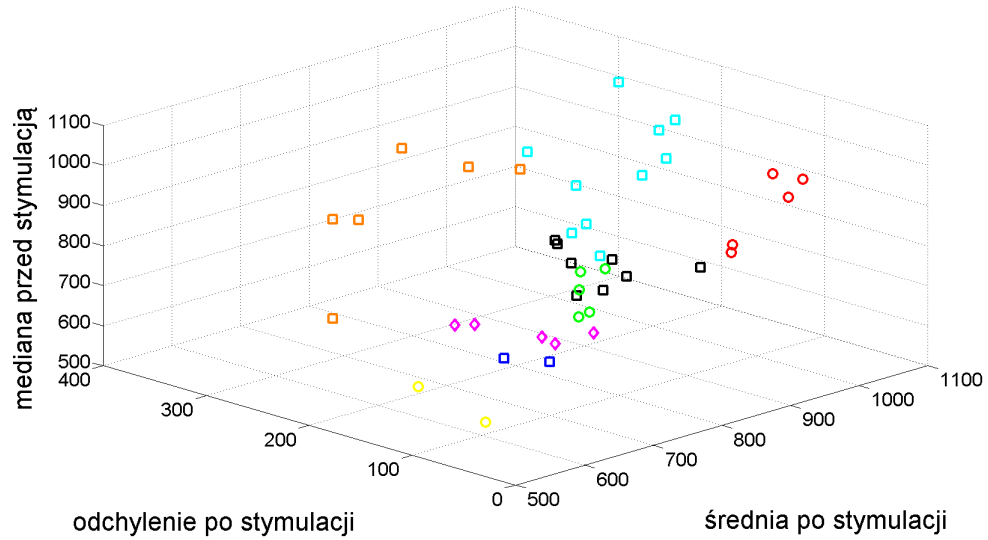
$$X = \begin{bmatrix} x_{1,1} & x_{2,1} & \cdots & x_{m,1} \\ x_{1,2} & x_{2,2} & \cdots & x_{m,2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,n} & x_{2,n} & \cdots & x_{m,n} \end{bmatrix}, \tag{6.43}$$

gdzie:

- n - liczba analizowanych cech,
- m - liczba obserwacji.



Rys. 6.13. Rozmieszczenie w przestrzeni wartości cech behawioralnych głosu



Rys. 6.14. Rozmieszczenie w przestrzeni wartości cech uzyskanych z EKG

Od wartości każdego elementu macierzy należy odjąć wartość średnią danej cechy:

$$X_a = \begin{bmatrix} x_{1,1} - \bar{x}_1 & x_{2,1} - \bar{x}_1 & \cdots & x_{m,1} - \bar{x}_1 \\ x_{1,2} - \bar{x}_2 & x_{2,2} - \bar{x}_2 & \cdots & x_{m,2} - \bar{x}_2 \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,n} - \bar{x}_n & x_{2,n} - \bar{x}_n & \cdots & x_{m,n} - \bar{x}_n \end{bmatrix}. \tag{6.44}$$

gdzie: $\bar{x}_i$ - wartość średnia dla i-tego wiersza macierzy X,

Następnym krokiem jest obliczenie macierzy kowariancji:

$$X_c = \begin{bmatrix} cov(x_1, x_1) & cov(x_1, x_2) & \cdots & cov(x_1, x_n) \\ cov(x_2, x_1) & cov(x_2, x_2) & \cdots & cov(x_2, x_n) \\ \vdots & \vdots & \ddots & \vdots \\ cov(x_n, x_1) & cov(x_n, x_2) & \cdots & cov(x_n, x_n) \end{bmatrix}. \tag{6.45}$$

Kowariancję można obliczyć następującym wzorem:

$$cov(x_i, y_j) = \frac{\sum_{k=1}^{n} (x_{k,i} - \bar{x_i})(y_{k,j} - \bar{y_j})}{(n-1)}. \tag{6.46}$$

Definicja 6.1. *Wektor własny przekształcenia liniowego $T : V \to V$ jest to niezerowy wektor v taki, że $Tv = cv$ dla pewnego skalara c. Wartością własną przekształcenia T jest skalar c taki, że $Tv = cv$ dla pewnego wektora v różnego od 0* [13].

Wyznaczamy wektory własne (ang. *eigenvector*) oraz własności własne (ang. *eigenvalue*) dla macierzy kowariancji. Składowe główne to wektory własne o odpowiadających im najwyższych wartościach własnych.

Kolejnym krokiem algorytmu jest posortowanie wektorów własnych według odpowiadających im wartości własnych (od największej do najmniejszej). Na tym etapie możliwe jest wskazanie tych wektorów własnych, które mają najmniejsze znaczenie. Kryterium doboru najbardziej znaczących wektorów własnych jest wybór takich M wektorów, że suma odpowiadających im wartości własnych stanowi określony procent λ wartości sumy wszystkich N wartości własnych:

$$\frac{\sum_{i=1}^{M} c_i}{\sum_{j=1}^{N} c_j} \geqslant \lambda. \tag{6.47}$$

Mając wybrany zbiór wektorów własnych V należy wyznaczyć nowe wartości cech Y:

$$Y = V^T X'^T, \tag{6.48}$$

gdzie V jest macierzą wektorów własnych, uszeregowanych kolumnami według odpowiadającym im wartościom własnym w porządku malejącym:

$$V = \begin{bmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,n} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m,1} & v_{m,2} & \cdots & v_{m,n} \end{bmatrix}. \tag{6.49}$$

Korzystając z powyższej metody przeanalizowano współczynniki mel–spektralne oraz mel–cepstralne. Dane wejściowe zawierały wektory cech dla każdej odpowiedzi osoby badanej, a więc pięć wektorów dla jednego eksperymentu. Przetestowano zarówno cały zakres danych, jak również zdecydowano się na uśrednienie wektorów otrzymanych dla pojedynczego eksperymentu. W ten sposób otrzymano 4 zbiory danych:

1) współczynniki mel–spektralne (MFC),
2) współczynniki mel–spektralne uśrednione ($\text{MFC}_{\text{śr}}$),
3) współczynniki mel–cepstralne (MFCC), oraz
4) współczynniki mel–cepstralne uśrednione ($\text{MFCC}_{\text{śr}}$).

W przypadku metody PCA badanie przeprowadzono dla dwóch wartości współczynnika λ: 0,95 (oznaczone jako PCA95) oraz 0,99 (oznaczono jako PCA99). Przetestowano również opisaną wcześniej metodę FLD, a także dwustopniowy dobór współczynników z wykorzystaniem metod PCA oraz FLD. Wyniki dotyczące liczby uzyskanych cech przedstawiono w tabeli 6.5. Stopień redukcji zdefiniowano jako iloraz liczby cech uzyskanych w wyniku zastosowania jednej z metod lc_{po} do początkowej liczby cech lc_{przed}:

$$sr = \frac{lc_{po}}{lc_{przed}} \cdot 100\% \tag{6.50}$$

Na podstawie powyższych wyników można zauważyć, iż metoda FLD w większym stopniu zredukowała wymiarowość obu wektorów współczynników MFCC, aniżeli wektor MFC. Metoda PCA dla obu wartości parametru λ znacząco zredukowała wymiarowość wektorów MFC (poniżej 40% początkowej liczby współczynników), natomiast dla MFCC tylko w jednym przypadku długość wektora została zmniejszona o połowę. Oznacza to, iż niewiele z 32 współczynników wektora MFC jest znaczących. Wartość współczynnika λ wpływa na liczbę współczynników otrzymanych w wyniku analizy PCA, z czego wynika, iż wiele z nich może mieć stosunkowo niewielki wpływ na klasyfikację. Kombinacja obu powyższych metod skutkowała w każdym przypadku zmniejszeniem liczby współczynników, zarówno w stosunku do stanu początkowego, jak również w porównaniu z pojedynczymi metodami.

Wykorzystanie metod doboru najbardziej znaczącego zestawu cech nie gwarantuje, iż otrzymane wektory pozwolą bezbłędnie zweryfikować tożsamość badanych osób. Dlatego też zaproponowano algorytm, który pozwolił na ocenę dokładności wyselekcjonowanych parametrów (algorytm 6.5). Pozwolił on również na ocenę dokładności mniej licznych kombinacji cech, w celu określenia minimalnego zestawu współczynników pozwalających na najlepsze rozróżnienie badanych osób.

Tab. 6.5. Liczba cech oraz stopień redukcji wymiarowości uzyskane w wyniku analizy metodami FLD i PCA

Metoda		**Cecha**			
		MFC	**MFC$_{śr}$**	**MFCC**	**MFCC$_{śr}$**
Początkowa liczba cech		**32**	**32**	**24**	**24**
FLD	Liczba cech	12	20	7	3
	Stopień redukcji	37,5%	62,5%	29,1%	12,5%
PCA95	Liczba cech	7	6	16	11
	Stopień redukcji	21,9%	18,8%	66,7%	45,8%
FLD+PCA95	Liczba cech	3	5	6	3
	Stopień redukcji	9,4%	15,6%	25%	12,5%
PCA95+FLD	Liczba cech	4	2	8	2
	Stopień redukcji	12,5%	6,3%	33,3%	8,3%
PCA99	Liczba cech	12	11	21	18
	Stopień redukcji	37,5%	34,4%	87,5%	75%
FLD+PCA99	Liczba cech	4	7	7	3
	Stopień redukcji	12,5%	21,9%	29,2%	12,5%
PCA99+FLD	Liczba cech	5	2	9	2
	Stopień redukcji	15,6%	6,3%	37,5%	8,3%

Przetestowano wszystkie wektory otrzymane dzięki analizie cech fizjologicznych za pomocą wspomnianych metod. Wyniki zostały zaprezentowane w postaci wykresów na rysunku 6.15. Jak można zauważyć, współczynniki MFC (rys. 6.15a) bez względu na użytą metodę doboru cech nie dają dokładności większej, niż 70%. Co więcej, najwyższa wartość została osiągnięta dla metody FDL, która w najmniejszym stopniu zredukowała wymiarowość tego wektora. W każdym innym przypadku, gdy liczba współczynników zmniejszała się jeszcze bardziej, osiągnięte wyniki były jeszcze niższe. Można więc wywnioskować, iż współczynniki te nie będą nadawały się do dalszej analizy, a zaproponowane metody ekstrakcji cech nie dają w tym przypadku oczekiwanej poprawy. Lepsze wyniki uzyskano dla uśrednionego wektora MFC$_{śr}$ (rys. 6.15b), dla którego w kilku przypadkach osiągnięto dokładność powyżej 90% (najlepsze dla metody FDL - 97,5%), z drugiej jednak strony, aż w trzech przypadkach dokładność spadła poniżej 70%. Dodatkowo nie można, tak jak w przypadku wykorzystania pełnego wektora współczynników MFC, dostrzec zależności pomiędzy rosnącym stopniem redukcji wymiarowości, a spadkiem dokładności dopasowania.

Algorytm 6.5: Ocena dokładności wektora cech

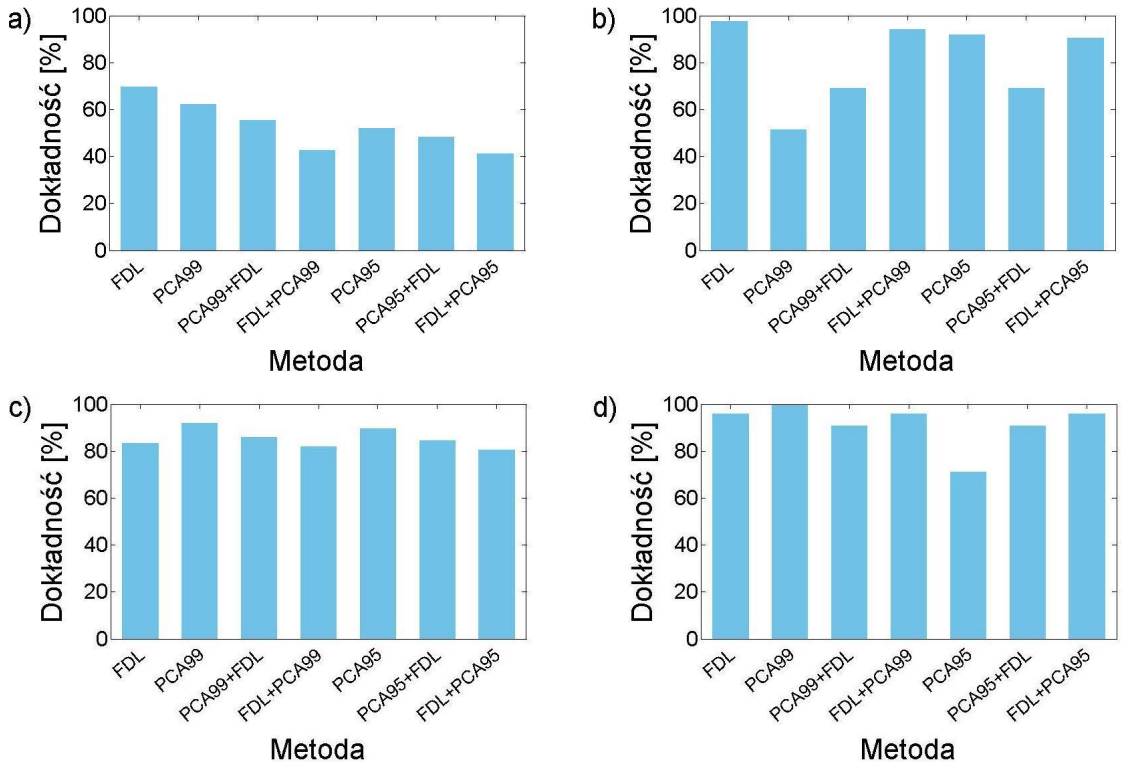
Dane wejściowe: Wektor cech Y, długość wektora cech n, zbiór użytkowników U

Dane wyjściowe: średnia dokładność dla poszczególnych zestawów cech A, minimalna dokładność dla poszczególnych zestawów cech A_{min}, maksymalna dokładność dla poszczególnych zestawów cech A_{max}

Dane: k, *poprawne*

```
1  DLA k := 1, ··· , n
2      DLA KAŻDEJ z C_n^k kombinacji cech
3          poprawne:=0
4          DLA KAŻDEGO użytkownika u ∈ U
5              Określ przestrzeń zajmowaną przez użytkownika u na podstawie
               jego wektora cech
6              DLA KAŻDEGO użytkownika w ∈ U \ {u}
7                  JEŻELI punkty użytkownika w nie wpadają w przestrzeń
                   użytkownika u
8                      INC(poprawne)
9          Wybierz najgorszy i najlepszy zestaw k cech A_min(k), A_max(k)
10     Średnia dokładność dla k-tego zestawu cech A(k) := poprawne/C_n^k
```

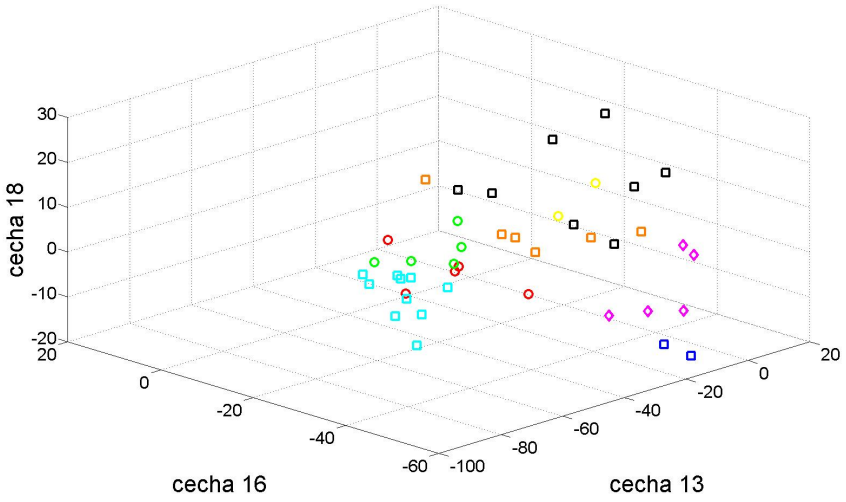
W przypadku analizy na podstawie współczynników MFCC otrzymano dosyć wyrównane rezultaty wahające się w zakresie 80% a 90%. Redukcja wymiarowości dla pełnego wektora MFCC (rys. 6.15c)przyniosła najlepsze rezultaty w przypadku użycia metody PCA dla obu wartości parametru λ. Kombinacja FLD oraz PCA w dowolnej kolejności skutkowała pogorszeniem dokładności dopasowania. Najlepszy wynik uzyskano dla uśrednionego wektora $\mathrm{MFCC}_{\text{śr}}$ (rys. 6.15d) przetworzonego za pomocą metody PCA ze współczynnikiem $\lambda = 0,99$, dla której osiągnięto pełną dokładność. Dla pozostałych metod i ich kombinacji również uzyskano dobre rezultaty, ponieważ, poza jednym przypadkiem, dokładność przekraczała 90%. Tak jak dla wektora $\mathrm{MFC}_{\text{śr}}$, nie można tutaj zauważyć zależności pomiędzy liczbą cech a dokładnością.



Rys. 6.15. Dokładność dopasowania w zależności od metody dla a) wektora MFC b) uśrednionego wektora MFC c) wektora MFCC d) uśrednionego wektora MFCC

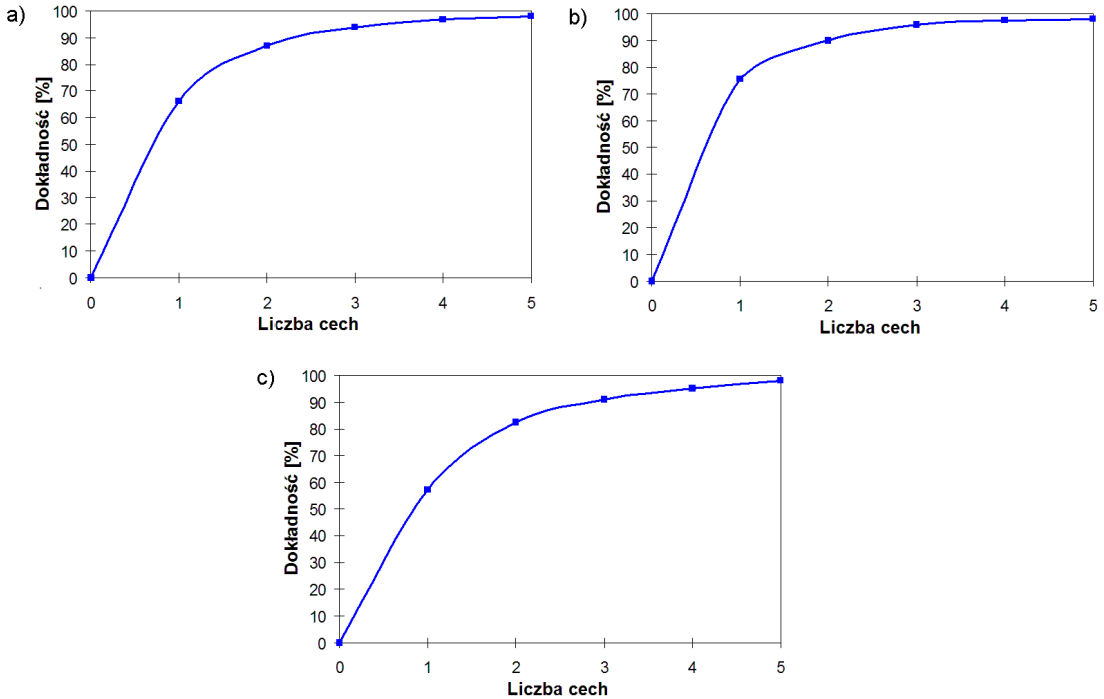
Na podstawie uzyskanych wyników do dalszej analizy wybrano współczynniki wyekstrahowane za pomocą metody PCA, zastosowanej na wektorze cech $\mathrm{MFCC}_{\text{śr}}$ dla $\lambda = 0,99$. Poniżej na rysunku (rys. 6.16) przedstawiono rozmieszczenie punktów w przestrzeni utworzonej na podstawie wartości trzech wybranych współczynników. Jak można zauważyć, poszczególne osoby zostały poprawnie zróżnicowane.

Współczynniki otrzymane z biometryk fizjologicznych połączono z miarami wyekstrahowanymi na podstawie biometryk behawioralnych sygnału głosu oraz EKG. Przetestowano średnią, minimalną oraz maksymalną dokładność dopasowania mniej licznych kombinacji cech za pomocą algorytmu 6.5 opisanego powyżej, w celu określenia minimalnego ich zestawu pozwalającego na rozróżnianie poszczególnych osób. Zbadano dokładność zarówno połączonego wektora cech jak również osobno wektor współczynników fizjologicznych oraz behawioralnych. Otrzymane wyniki przedstawiono na rysunkach 6.17, 6.18 oraz rysunku 6.19.



Rys. 6.16. Rozmieszczenie w przestrzeni wartości współczynników uzyskanych z wektora $MFCC_{śr}$ za pomocą metody PCA

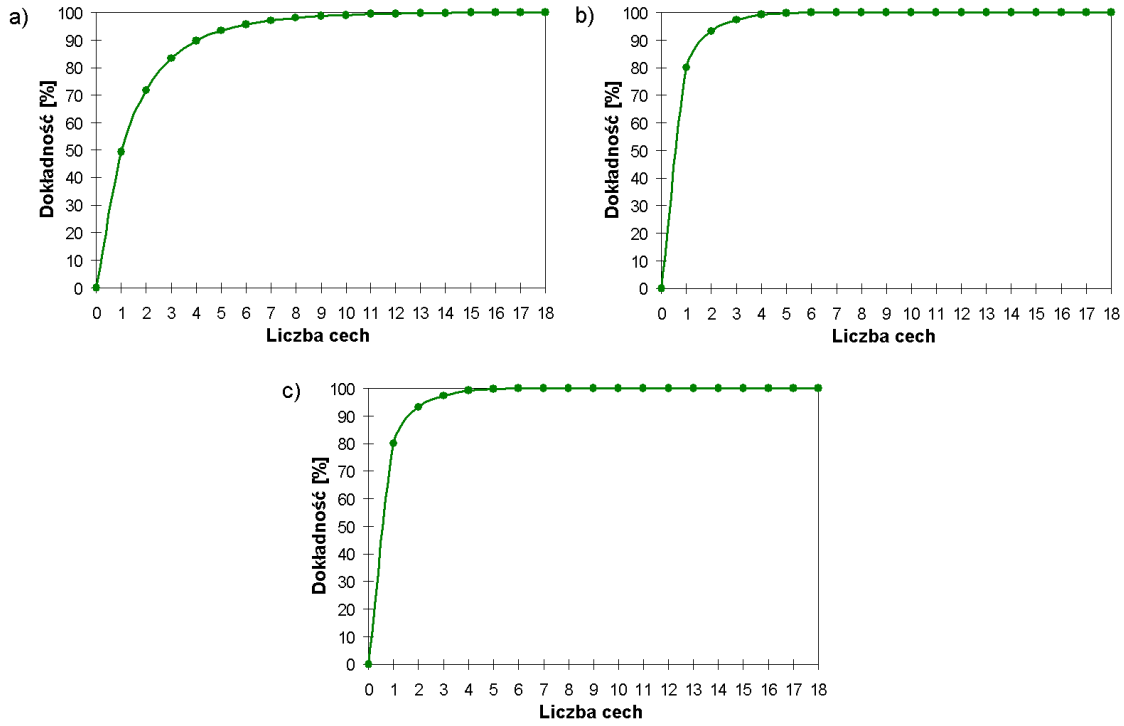
Dla cech behawioralnych (rys. 6.17) najlepszą dokładność na poziomie 98% otrzymano przy wykorzystaniu wszystkich pięciu cech. Wynik ten można uznać za bardzo dobry, biorąc pod uwagę, iż (według wiedzy autora) tego typu badania nie były dotychczas prowadzone. Różnica pomiędzy najlepszymi, a najgorszymi zestawami cech



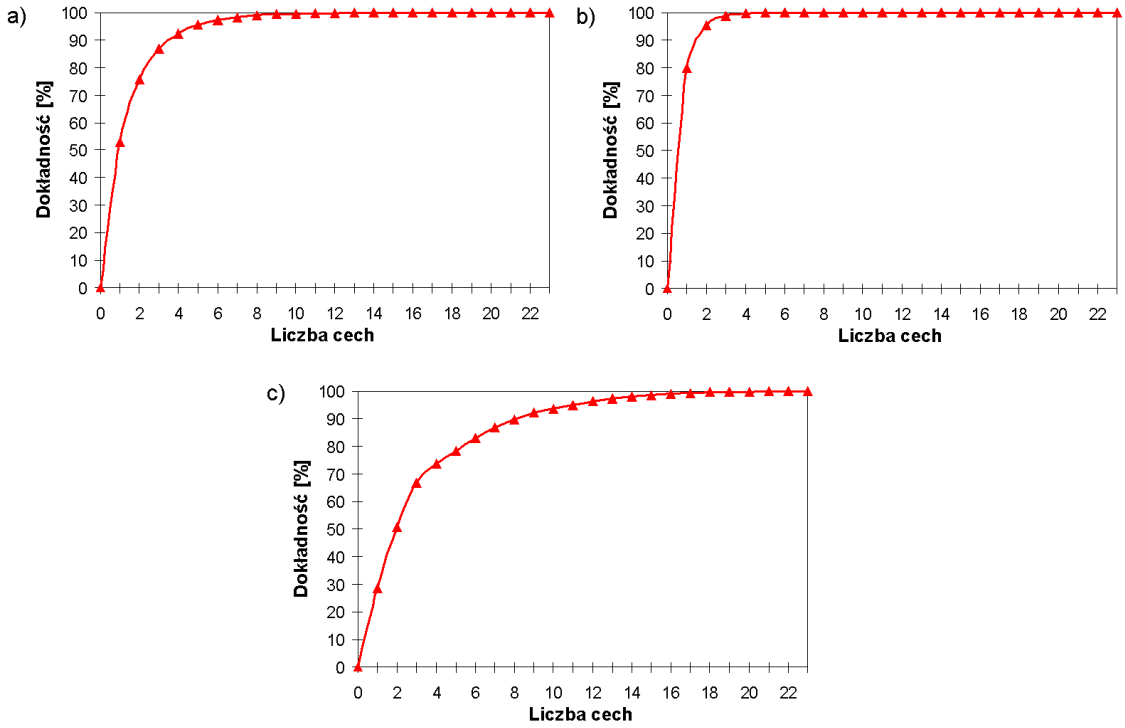
Rys. 6.17. Dokładność dopasowania dla współczynników behawioralnych w zależności od liczby cech a) średnie b) maksymalne c) minimalne

początkowo jest znacząca (około 20% - rys. 6.17b i c), następnie szybko maleje i dla trzech cech wynosi 4% , a przy 4 cechach już tylko 2%. Widać również, iż już dla 3 cech osiągnięto poziom 90% i użycie kolejnych poprawia go o kilka procent. W zastosowaniach biometrycznych jednakże każdy wzrost dokładności jest pożądany, dlatego zastosowanie większej liczby cech jest uzasadnione.

Współczynniki wyekstrahowane z pomocą metody PCA z wektora MFCC pozwoliły na uzyskanie pełnej dokładności, zgodnie z wcześniejszymi badaniami. Należy zwrócić uwagę, iż nawet przy 6 parametrach poziom dokładności osiąga maksimum (rys. 6.18b). Jak widać na rysunkach 6.18b i c, różnica pomiędzy najgorszymi a najlepszymi zestawami cech jest znacząca. W najgorszym przypadku dopiero 9 cech pozwoliło na osiągnięcie dokładności powyżej 90%, a dodawanie kolejnych bardzo powoli poprawia ten wynik. Wydaje się, że najlepszym rozwiązaniem byłoby pozostawienie tylko tych 6 najlepszych cech, z drugiej jednak strony wraz z rosnącą liczbą użytkowników systemu mały zestaw cech mógłby się okazać niewystarczający do poprawnego rozpoznania osób, dlatego nie zdecydowano się na ten krok.



Rys. 6.18. Dokładność dopasowania dla wektora współczynników utworzonego na podstawie MFCC w zależności od liczby cech a) średnie b) maksymalne c) minimalne

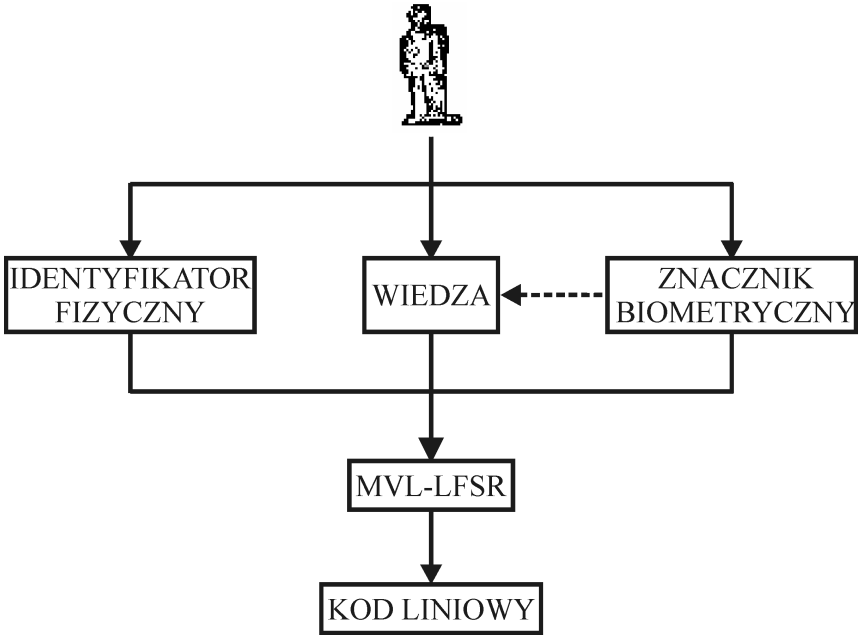


Rys. 6.19. Dokładność dopasowania dla wszystkich wykorzystanych współczynników w zależności od liczby cech a) średnie b) maksymalne c) minimalne

Połączenie obu grup parametrów (rys. 6.19) spowodowało pozytywny skutek. W przypadku najlepszych zestawów (rys. 6.19b) całkowitą dokładność uzyskano już dla pięciu cech, a więc jednej mniej, niż w przypadku samych tylko cech fizjologicznych. Nawet w przypadku najgorszych (rys. 6.19b) zestawów cech pełną dokładność uzyskano już dla 21 cech, co oznacza, iż nie wszystkie parametry muszą zostać użyte w celu optymalnego rozdzielenia przestrzeni cech poszczególnych osób.

7. System multimodalnego klucza biometrycznego z MVL–LFSR

Zaproponowane cechy zawierające informacje zarówno o fizjologii człowieka, jak również o jego reakcjach w odpowiedzi na kontrolowane wymuszenie, 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. Problem ten dotyczy większości cech biometrycznych (za wyjątkiem DNA), co zostało poruszone w rozdziale 4.1.



Rys. 7.1. Propozycja systemu kryptograficznego wzmacnianego biometrycznie

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. 7.1). Szczegóły przedstawionej idei zostaną zaprezentowane poniżej.

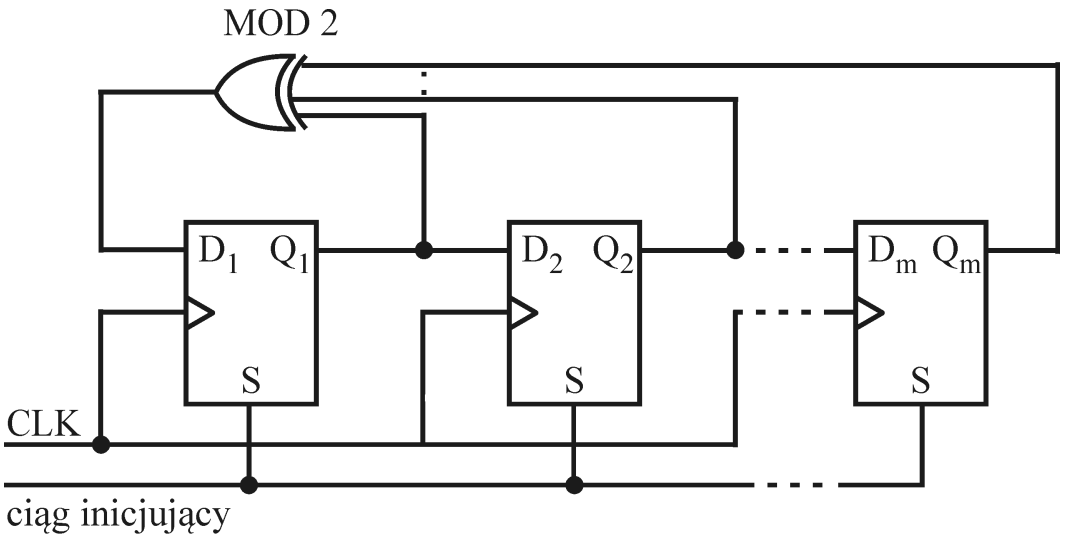
7.1 Generatory MVL-LFSR

W systemach kryptograficznych ważną rolę odgrywają liczby losowe, które w przeważającej większości wykorzystywane są jako klucze kryptograficzne. Liczby generowane przez komputery są *pseudolosowe*, ponieważ zawsze po określonej liczbie sekwencji będą się powtarzały. Odpowiednio skonstruowany generator pozwala na stworzenie wrażenia losowości. Powinien on również gwarantować, iż nie będzie możliwe wyznaczenie n-tej sekwencji wyłącznie w oparciu o wiedzę o poprzednich $n-1$ sekwencjach. Jedynym elementem losowym takiego generatora jest ciąg inicjujący, który powinien być na tyle długi, aby odnalezienie jego wartości nie było możliwe w opłacalnym dla potencjalnego napastnika czasie.

Jedno z podejść do tworzenia generatorów liczb pseudolosowych to takie, w którym wykorzystywane są rejestry liniowe. Zasadnicze różnice w budowie generatorów opartych na tej strukturze dotyczą sposobu realizacji pętli sprzężenia zwrotnego, jak również metody generacji ciągu inicjującego oraz długości samego rejestru.

Koncepcja wielowartościowego (*Multi Value Logic* - MVL) generatora ciągów pseudolosowych oraz jego parametryzacji za pomocą hasła alfanumerycznego przedstawiona została w opracowaniu [72]. W innej pracy zaproponowano z kolei wykorzystanie biometrycznej parametryzacji generatora [38]. Idea ta posłużyła do opracowania generatora parametryzowanego za pomocą odpornej reprezentacji cechy biometrycznej, w szczególności odcisku palca [95].

Podstawą budowy generatora MVL jest rejestr liniowy ze sprzężeniem zwrotnym, składający się z m przerzutników, z których każdy przechowuje w danym momencie jeden bit informacji. Do rozpoczęcia pracy generatora potrzebny jest losowy niezerowy ciąg inicjujący. Schemat układu binarnego rejestru liniowego przedstawiono na rys. 7.2.



Rys. 7.2. Schemat binarnego rejestru liniowego ze sprzężeniem zwrotnym

W każdym cyklu pracy t stan pierwszego przerzutnika jest obliczany jako suma *modulo* 2 wybranych wyjść przerzutników w cyklu poprzedzającym $t-1$. Stan wyjść binarnego rejestru liniowego ze sprzężeniem zwrotnym w chwili t można opisać następującym układem równań:

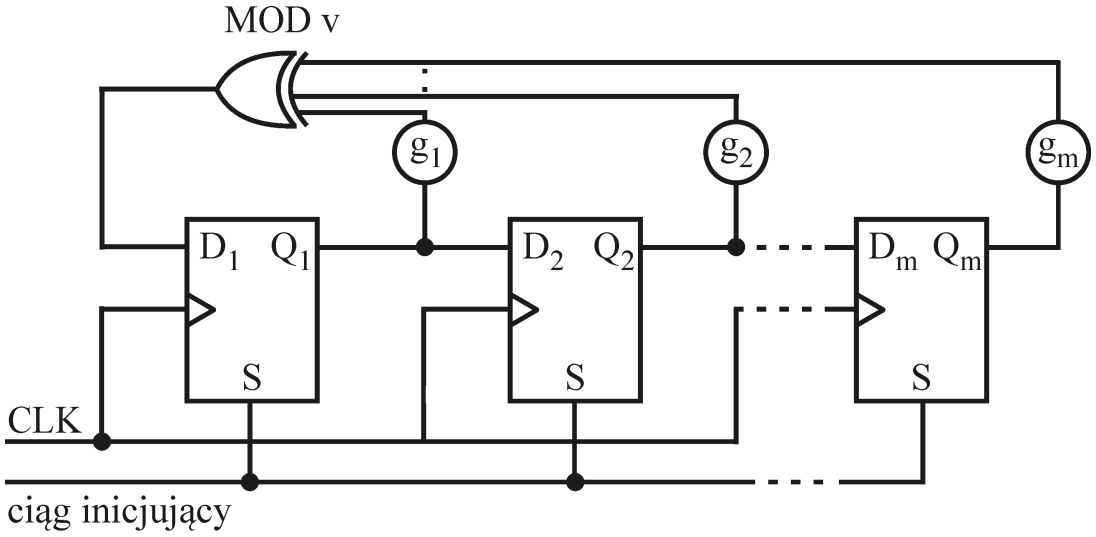
$$\begin{cases} x_1(t+1) = \sum_{k=1}^{m} x_k(t) \cdot g_k \pmod 2 \\ x_2(t+1) = x_1(t) \\ \vdots \\ x_m(t+1) = x_{m-1}(t) \end{cases} \tag{7.1}$$

gdzie:

$x_i(t)$ - stan i-tego przerzutnika w chwili t,

g_i - współczynnik [0;1] określający czy dane wyjście i-tego przerzutnika jest połączone z pętlą sprzężenia.

Przejście z rejestru LFSR, bazującego na logice binarnej, na rejestr MVL-LFSR w logice wielowartościowej polega na zamianie bramek dwuwartościowych na ich v- wielowartościowe odpowiedniki. W tym wypadku wszystkie operacje mnożenia oraz sumowania wykonywane są w rozumieniu logiki *modulo* v. Przykład schematu generatora MVL-LFSR został przedstawiony na rys. 7.3.



Rys. 7.3. Schemat rejestru liniowego v-wartościowego o długości m objętego sprzężeniem zwrotnym

Układ równań opisujący stan przerzutników rejestru MVL-LFSR w chwili t jest następujący:

$$\begin{cases} x_1(t+1) = \sum_{k=1}^{m} x_k(t) \cdot g_k \pmod{v} \\ w_2(t+1) = x_1(t) \\ \vdots \\ x_m(t+1) = x_{m-1}(t) \end{cases} \tag{7.2}$$

gdzie:

$x_i(t)$ - stan i-tego przerzutnika w chwili t,

g_i - współczynnik v-wartościowy, określający wagę połączenia wyjścia i-tego przerzutnika.

Pętla sprzężenia zwrotnego determinuje okres skonstruowanego generatora MVL-LFSR. Wagi sprzężenia zwrotnego mogą być traktowane jako współczynniki wielomianu rzędu co najwyżej m. Jeśli wspomniany wielomian jest wielomianem pierwotnym, to okres takiego generatora jest maksymalny [37,62]. Liczba niepowtarzających się sekwencji wynosi wówczas $v^m - 1$, a generator określa się generatorem MLS (*Maximum Length Sequence generator*).

Wyznaczenia wag wielomianu pierwotnego sprzężenia zwrotnego nie jest zadaniem trywialnym, a problem ten był przedmiotem osobnych prac badawczych [37]. Najwydajniejszy pod względem obliczeniowym algorytm, wyszukujący wielomiany pierwotne nad ciałem $\mathbb{Z}_p$ (gdzie p jest liczbą pierwszą), został przedstawiony w [62].

7.2 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.

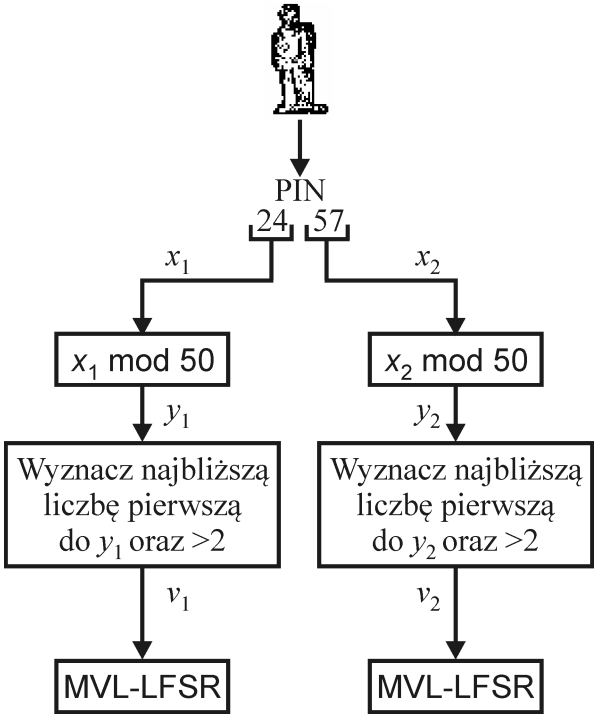
Pierwszy z wyżej wspomnianych parametrów, określający wartościowość logiki obu generatorów, jest przechowywany w postaci 4-cyfrowego indywidualnego numeru identyfikacyjnego (PIN). Zgodnie z opisem przedstawionym w poprzednim rozdziale 7.1, wartościowość logiki musi być liczbą pierwszą, dlatego też zaproponowano 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 rysunku 7.4.

Dwucyfrowa liczba przyjmuje wartości z zakresu $00, \ldots, 99$. Jak przedstawiono na rysunku 7.4, jako pierwsza wyliczana jest reszta z dzielenia *mod* 50. Wartość ta została tak dobrana, aby cały zakres (00-99) podzielić na równe części. W danym zakresie możliwe są również inne podziały na równe przedziały, które zawierają jednak mniej liczb pierwszych. 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.

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:

$$v = \arg\min_{p \in P} |y - p|. \tag{7.3}$$

Na tym etapie, do procesu ekstrakcji wartościowości logik obu rejestrów, wprowadza się pierwszy element biometrycznej parametryzacji generatora liczb pseudolosowych. Przypisywana użytkownikowi liczba pierwsza jest zależna od rodzaju głosu



Rys. 7.4. Propozycja ekstracji wartości logiki rejestru MVL z numeru PIN

osoby rejestrowanej/weryfikowanej w systemie:

$$v = \begin{cases} \arg\min\limits_{p \in P} |(y+1) - p| & \text{dla} \quad \text{fem} \\ \arg\min\limits_{p \in P} |(y-1) - p| & \text{dla} \quad \text{masc} \end{cases} . \tag{7.4}$$

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

$$|y + 1 - p_i| = |y + 1 - p_j| \quad \text{dla} \quad i \neq j, \tag{7.5}$$

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

$$v = \begin{cases} \arg\min\limits_{p \in P} |(y+2) - p| & \text{dla} \quad \text{fem} \\ \arg\min\limits_{p \in P} |(y-2) - p| & \text{dla} \quad \text{masc} \end{cases} . \tag{7.6}$$

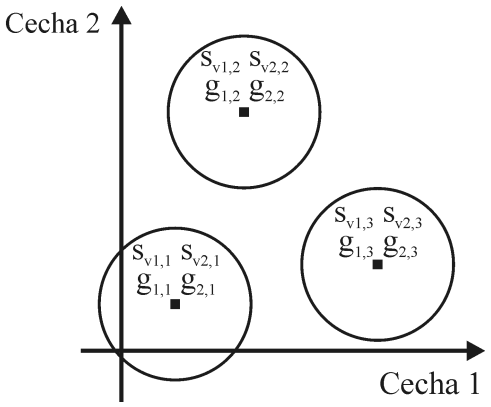
Wykorzystana cecha biometryczna wykazuje dużą stabilność na zmienne warunki akwizycji, dzięki czemu możliwa jest powtarzalna generacja klucza kodowego.

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 kolejnych stanów bądź ciągu startowego.

Proponuje się, aby minimalna długość rejestru została ustalona na 10. Maksymalna długość nie musi być co prawda ograniczona, aczkolwiek znalezienie wielomianów pierwotnych wysokiego stopnia jest zadaniem bardzo kosztownym obliczeniowo. Wobec powyższego w przedstawionej koncepcji założono, iż 4 cyfry wystarczają 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. 7.5). Punktowi temu przyporządkowywane są cztery parametry:

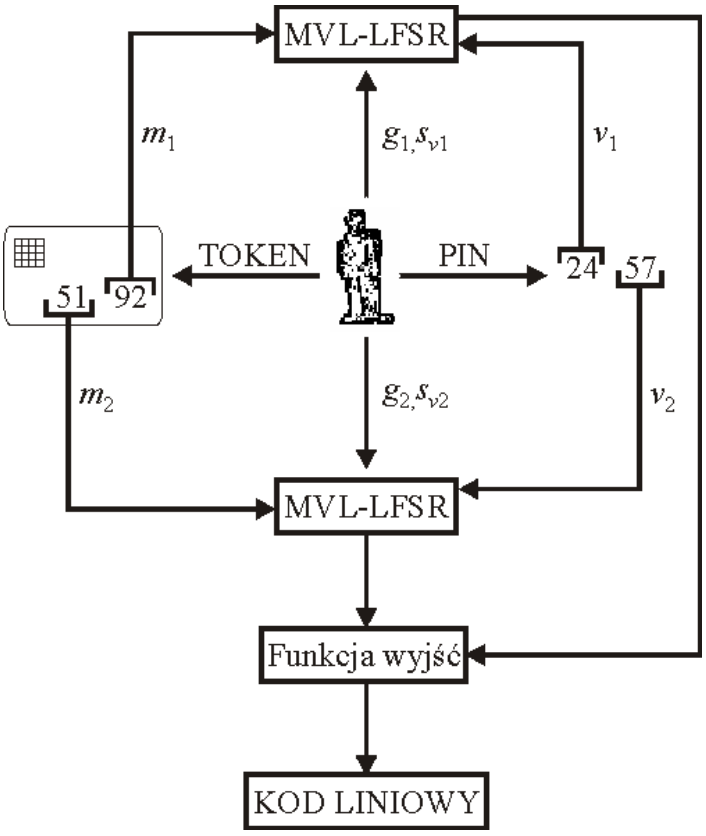
- wartości początkowe rejestrów s_{v1}, s_{v2},
- współczynniki wielomianów pierwotnych sprzężenia zwrotnego g_1, g_2 dla obu generatorów.



Rys. 7.5. Przypisanie określonym punktom w przestrzeni cech parametrów generatora MVL

Zarówno ciągi, jak i wielomiany muszą zostać odpowiednio dobrane do parametrów v_1, v_2, m_1, m_2, zapisanych na karcie oraz w numerze PIN. Wartości pozycji ciągów początkowych mogą zostać wylosowane za pomocą dowolnego generatora o rozkładzie jednostajnym, natomiast dobór wielomianu pierwotnego należy przeprowadzić za pomocą wspomnianego algorytmu przedstawionego w [62]. Wynik działania tego algorytmu musi również wykazywać pseudolosowość.

W procesie weryfikacji osoba okazuje swój identyfikator oraz podaje swój numer PIN. Następnie zostaje przeprowadzona weryfikacja biometryczna, która w przypadku pozytywnego wyniku uwalnia klucze zapisane w bazie. Jeżeli parametry m oraz v są zgodne z ciągami startowymi oraz wielomianami sprzężenia zwrotnego, to następuje rozpoczęcie generacji sekwencji przez oba rejestry MVL. Proponuje się, aby klucz kodowy był funkcją obu wyjść generatorów - rysunek 7.6.

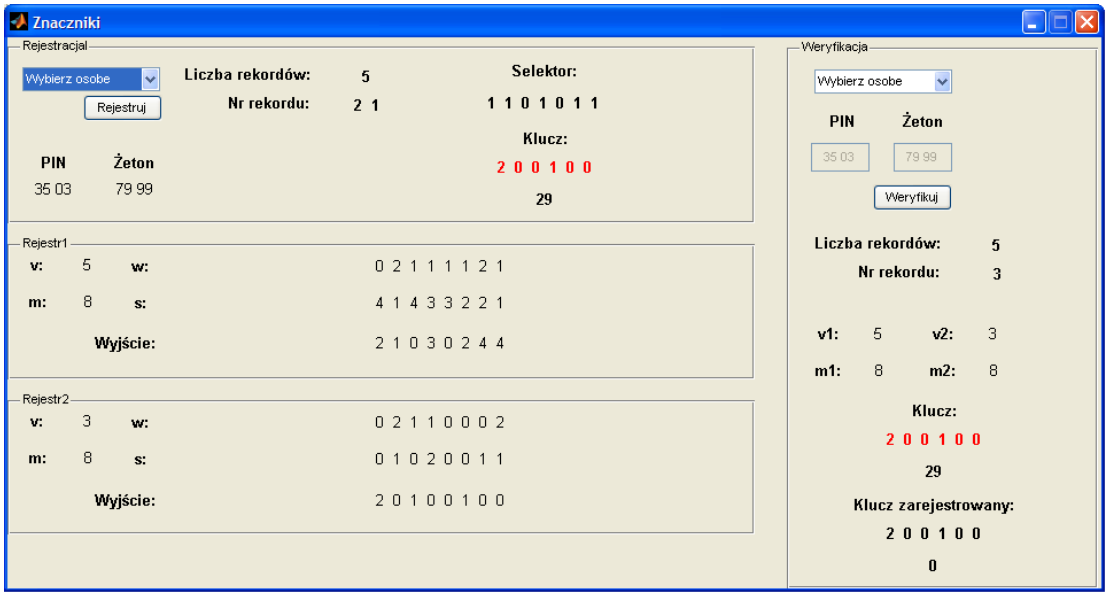


Rys. 7.6. Proces tworzenia klucza kryptograficznego wzmacnianego biometrycznie

Z punktu widzenie teorii rejestrów liniowych zastosowanie dwóch rejestrów o długościach m_1 i m_2 zapewnia identyczny podział przestrzeni zdarzeń na równoliczne podzbiory o takich samych stanach końcowych rejestrów liniowych, jak użycie rejestru pojedynczego o długości równej $m_1 + m_2$. Jednakże wyodrębnienie części szyfrujących, oddzielających poszczególne etapy kryptograficzne, jest uzasadnione przejrzystością rozwiązania technicznego. W rozważanym przypadku jest to zabieg szczególnie korzystny z uwagi na możliwość zdefiniowania niejednakowych wartościowości logiki dla obu rejestrów.

8. Praktyczna weryfikacja koncepcji kryptografii biometrycznej

Zaprezentowana w poprzednim rozdziale 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. Na rysunku 8.1 zaprezentowano okno pochodzące z tego modułu rozwiązania programowego. Do jego zadań należą między innymi: rejestracja nowych użytkowników w systemie, przeprowadzanie procesu weryfikacji tożsamości oraz generowanie kluczy kodowych.



Rys. 8.1. Okno modułu generowania i weryfikacji klucza

8.1 Algorytm wyznaczania powtarzalnego klucza kodowego

W systemach kryptografii biometrycznej najważniejszym wyzwaniem jest powtarzalność generowanych sekwencji losowych, wykorzystywanych jako klucze kodowe. Systemy biometryczne podejmują decyzję na podstawie podobnych, ale w praktyce nie identycznych zestawów cech. Dlatego też w przypadku próby utworzenia klucza bezpośrednio z biometryki występuje problem uzyskania niezmiennych wartości parametrów na wejściu generatora cyfrowego.

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 podstawie 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.

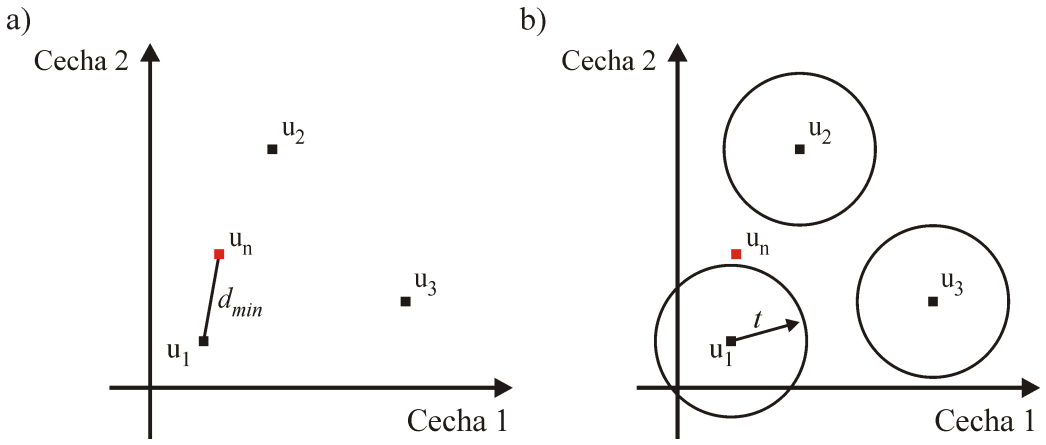
W pierwszym przypadku scenariusz może być następujący: osoba badana wprowadza poprawnie osobisty PIN (z którego zostają wyłonione właściwe wartościowości logik rejestrów), posiada odpowiedni identyfikator, a także pozytywnie przechodzi proces weryfikacji biometrycznej. Wyłonione przez system biometryki 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 następującemu 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.

Proponowana metoda wyznaczania punktów w przestrzeni, przypisanych do zarejestrowanych użytkowników, determinuje dwa możliwe scenariusze weryfikacji (i w konsekwencji generowania klucza). Pierwszy z nich zakłada, iż wektor cech, wyłoniony na podstawie pobranych sygnałów należy do tej osoby, której położenie w przestrzeni cech jest najbliższe (w sensie metryki euklidesowej) punktowi określonemu przez ten wektor. Stwarza to jednak zagrożenie, iż osoba nieuprawniona i nie zarejestrowana w systemie zawsze uwolni parametry startowe jakiejś osoby, która w tym systemie się znajduje (rys. 8.2a). Nie posiadając pozostałych informacji nie będzie ona jednak w stanie wygenerować odpowiedniego klucza. Tym samym tożsamość zarejestrowanego użytkownika pozostanie bezpieczna.

Inną możliwością jest ustawienie pewnej wartości progu czułości rozumianej w proponowanym rozwiązaniu jako ograniczony wycinek przestrzeni wokół punktu wyznaczonego przez wartości cech rejestrowanego użytkownika (rys. 8.2b). Dzięki przyjęciu dodatkowego kryterium prawdopodobieństwo zaakceptowania nieuprawnionej osoby maleje.

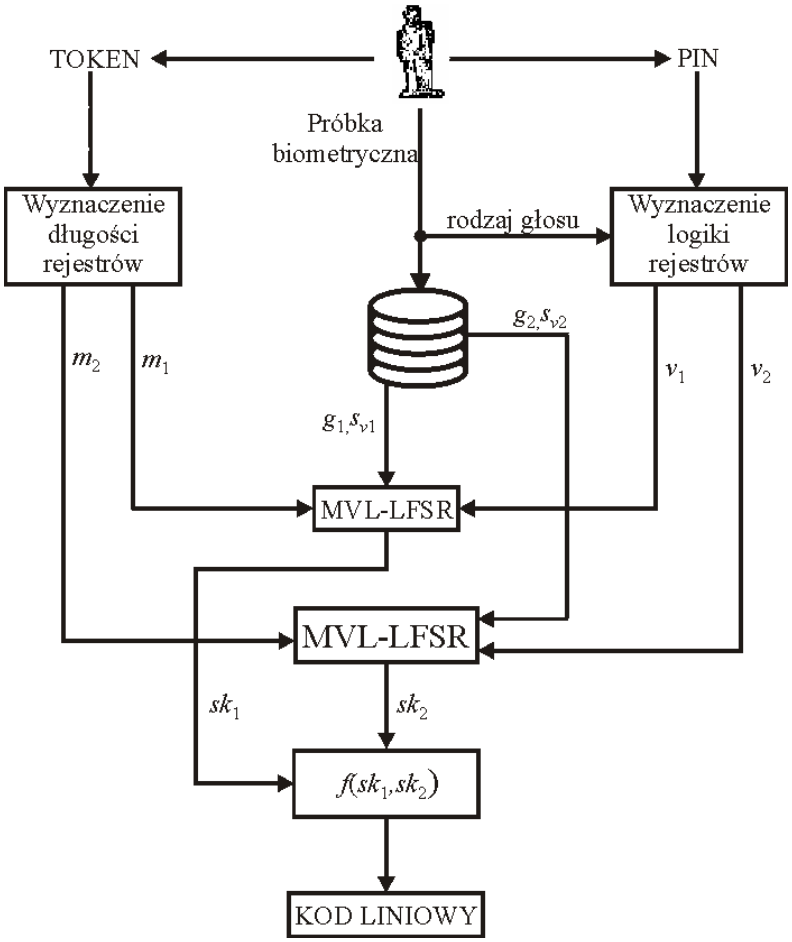


Rys. 8.2. Dwa scenariusze weryfikacji a) nieznany użytkownik u_n zostanie błędnie zweryfikowany jako użytkownik u_1, b) po ustaleniu progu t użytkownik u_n zostanie odrzucony przez system

8.2 Algorytm pracy generatora klucza kodowego - charakterystyka rozwiązania technicznego

Zgodnie z propozycją przedstawioną w rozdziale 7. część parametrów startowych generatora klucza kodowego(podpisu) jest podzielona pomiędzy identyfikatory fizyczne oraz te, które są oparte na wiedzy. Kluczowym elementem tego rozwiązania jest użycie wyłonionych w niniejszej pracy współczynników biometrycznych, które

określają pozostałe parametry inicjujące generatora. Schemat algorytmu generacji klucza kodowego został przedstawiony poniżej (rys. 8.3).



Rys. 8.3. Algorytm generacji klucza kodowego

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 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:

$$kk = [sk_1, sk_2] = [sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m1} sk_{2,1}, sk_{2,2}, \ldots, sk_{2,m2}]. \tag{8.1}$$

Oba ciągi wyjściowe wyrażone są w innej logice, dlatego w celu wyznaczenia dziesiętnej wartości klucza kodowego należy w pierwszym kroku przeliczyć każdą pozycję klucza, aby ustalić wspólny system liczbowy, w którym są wykonywane dalsze operacje arytmetyczne. Przyjmując, że pozycje po lewej stronie mają najmniejszą wagę, można zapisać tę operację poniższym wzorem:

$$\begin{aligned} kk_{10} = [&sk_{1,1} \cdot v_1^0, sk_{1,2} \cdot v_1^1, \ldots, sk_{1,m2} \cdot v_1^{m_1-1}, \\ &sk_{2,1} \cdot v_2^{m_1}, sk_{2,2} \cdot v_2^{m_1+1}, \ldots, sk_{2,m2} \cdot v_2^{m_1+m_2-1}]. \end{aligned} \tag{8.2}$$

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

$$kk_{10} = \sum_{i=1}^{m_1+m_2} kk_i. \tag{8.3}$$

Inną możliwością wykorzystania obu ciągów wyjściowych generatorów może być modyfikacja wartości poszczególnych wyjść drugiego rejestru za pomocą pozycji stanu końcowego rejestru pierwszego. Ponieważ długości obu generatorów są ustalane niezależnie, mogą wystąpić trzy przypadki:

- $m_1 = m_2$,
- $m_1 > m_2$,
- $m_1 < m_2$.

$\widetilde{sk} = [\widetilde{sk}_1, \widetilde{sk}_2, \ldots, \widetilde{sk}_{m2}]$ oznaczają wartości kolejnych pozycji stanu końcowego pierwszego rejestru, które posłużą do zmiany wartości wyjść generatora drugiego.

W pierwszym przypadku nie istnieje potrzeba dodatkowych operacji - wszystkie wyjścia pierwszego generatora są wykorzystywane w obliczeniu klucza kodowego $\widetilde{sk} = sk_1$.

Dla drugiego przypadku rozpatrywanych jest pierwszych m_2 wyjść generatora pierwszego $\widetilde{sk} = [sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m2}]$, które biorą udział w zmianie wyjść generatora drugiego; pozostałe są pomijane.

Natomiast, gdy długość generatora drugiego jest większa niż długość generatora pierwszego (ostatni przypadek), to stan końcowy generatora pierwszego jest powielany z razy według następującego wzoru:

$$\begin{aligned} \widetilde{sk} = [&\underbrace{sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m_1}}_{1}, \underbrace{sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m_1}}_{2}, \ldots, \\ &\underbrace{sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m_1}}_{z}, sk_{1,1}, sk_{1,2}, \ldots, sk_{1,z^*}], \end{aligned} \tag{8.4}$$

gdzie:

$z = \lfloor m_2/m_1 \rfloor$,

$z^* = m_2 \bmod m_1$.

Dzięki powyższej operacji wszystkie pozycje stanu końcowego drugiego rejestru zostaną wykorzystane. W przeciwnym wypadku sekwencja wyjściowa będzie zawierała mniej cyfr znaczących, w wyniku czego zmniejsza się także liczba unikalnych kluczy generowanych przez system.

Ostatnim etapem generacji klucza kodowego jest parametryzowanie stanu końcowego rejestru drugiego za pomocą stanu końcowego rejestru pierwszego. Pierwszym krokiem jest przeliczenie każdej pozycji obu ciągów na system dziesiętny (w celu ustalenia wspólnego systemu liczbowego, w którym zostaną wykonane operacje arytmetyczne) zgodnie z poniższym wzorem:

$$\begin{aligned} \widetilde{sk}_{10} &= [\widetilde{sk}_1 \cdot v_1^0, \widetilde{sk}_2 \cdot v_1^1, \ldots, \widetilde{sk}_{m2} \cdot v_1^{m_2-1}], \\ sk_{2\,10} &= [sk_{2,1} \cdot v_2^0, sk_{2,2} \cdot v_2^1, \ldots, sk_{2,m2} \cdot v_2^{m_2-1}]. \end{aligned} \tag{8.5}$$

Wartość klucza kodowego (wyrażona w systemie dziesiętnym) jest iloczynem skalarnym $\widetilde{sk}0_{10}$ oraz $sk_{2\,10}$:

$$klucz = \widetilde{sk}_{10} \circ sk_{2\,10}. \tag{8.6}$$

Poniżej (algorytm 8.1) zaprezentowano przebieg operacji wyznaczania klucza kodowego w proponowanym rozwiązaniu. Koncepcja ta pozwala na utworzenie zwartej i jednorodnej postaci finalnej klucza kodowego.

8.3 Dyskusja wyników dla posiadanej bazy danych

Ostatnim krokiem praktycznej weryfikacji przedstawionej koncepcji systemu kryptografii biometrycznej jest przeprowadzenie eksperymentów dla zgromadzonych danych. Testy składały się z dwóch głównych etapów:

- rejestracji,
- weryfikacji.

Rejestracja danych biometrycznych jest etapem niezwykle ważnym, ponieważ od jej przebiegu zależy w dużej mierze dokładność pomiaru. Zapamiętanie szablonu biometrycznego, pobranego w niekorzystnych warunkach akwizycji (błąd pomiarowy lub gorsza dyspozycja osoby rejestrowanej), skutkuje dużą stopą błędu procesu weryfikacji. Zdecydowano się na podział posiadanego zbioru danych na część wykorzystywaną w procesie rejestracji w systemie (oraz na potrzeby związanych z tym

Algorytm 8.1: Wyznaczanie klucza kodowego

Dane wejściowe: Stany końcowe rejestrów sk_1, sk_2, długości rejestrów m_1, m_2

Dane wyjściowe: Klucz kodowy kk

Dane: z, z^*, sekwencja utworzona na podstawie sk_1 - $\widetilde{sk}$

JEŻELI $m_1 > m_2$
  Wybierz m_2 pozycji z sk_1 $\widetilde{sk} = [sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m2}]$
W PRZECIWNYM WYPADKU: JEŻELI $m_1 < m_2$
  $z = \lfloor m_2/m_1 \rfloor$
  $z^* = m_2 \bmod m_1$
  $\widetilde{sk} = [\underbrace{sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m_1}}_{1}, \underbrace{sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m_1}}_{2}, \ldots,$
    $\underbrace{sk_{1,1}, sk_{1,2}, \ldots, sk_{1,m_1}}_{z}, sk_{1,1}, sk_{1,2}, \ldots, sk_{1,z^*}]$
W PRZECIWNYM WYPADKU
  $\widetilde{sk} = sk_2$
Zamień poszczególne pozycje $\widetilde{sk}$ oraz sk_2 na wartości dziesiętne
$kk = \widetilde{sk}_{10} \circ sk_{2\,10}$

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 $\approx 84\%$,
- minimalna osiągnięta dokładność $\approx 71\%$,

- maksymalna uzyskana dokładność $\approx 93\%$.

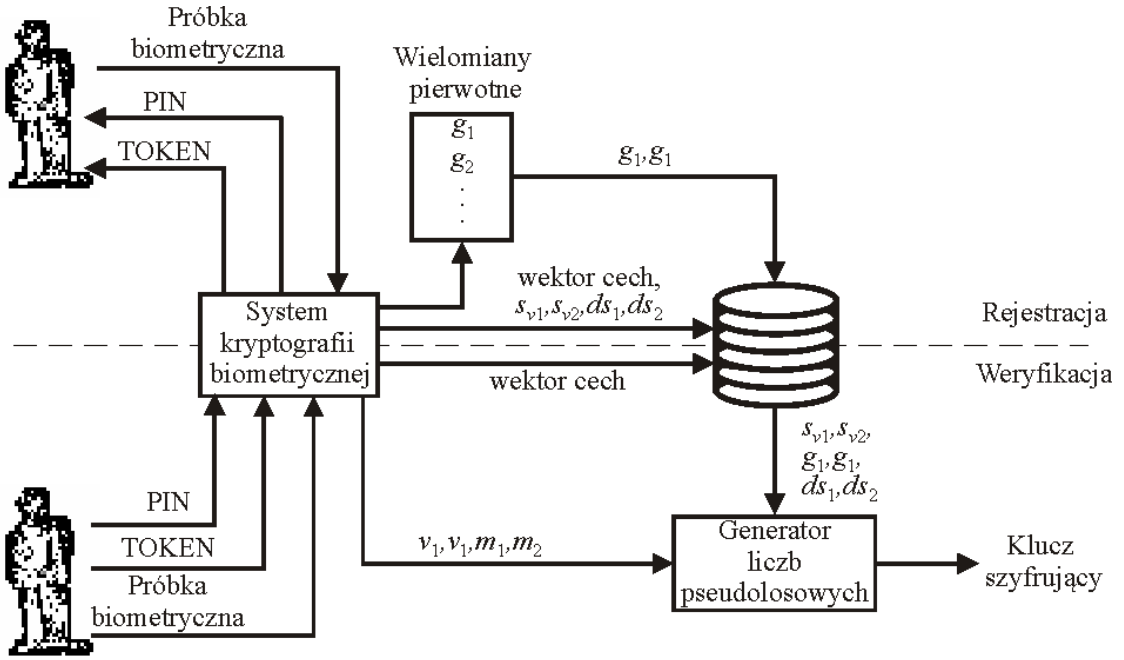
Wygenerowane klucze odpowiadały osobom, które zostały poprawnie zweryfikowane. Nie wystąpiła sytuacja, w której osoba inna od uprawnionej doprowadziłaby do wygenerowania odpowiedniego klucza. Uzyskana dokładność odbiega od wartości otrzymanej w wyniku eksperymentów, przedstawionych w punkcie 6.3 o ponad 10%. Różnica ta jest pochodną odmiennych metod estymacji dokładności. 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. Przetestowano obie koncepcje w celach porównawczych. 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. W przypadku połączenia ciągów wyjściowych w jeden klucz otrzymano wyniki charakteryzujące się znikomą powtarzalnością (poniżej 0,04%), co wskazuje na to, iż zaproponowane rozwiązanie posiada oczekiwane własności pseudolosowe. Dla drugiej propozycji klucze kodowe powtarzały się znacznie częściej ($\approx 2,5\%$). Propozycja ta powinna być więc stosowana jedynie w ograniczonym zakresie.

Przedstawiony system może zostać wykorzystany w praktycznym rozwiązaniu kryptografii biometrycznej. Poglądowy schemat został zaprezentowany na poniższym rysunku 8.4. Wielomiany pierwotne sprzężenia zwrotnego rejestru MVL-LFSR powinny zostać wyznaczone wcześniej i zestawione w odpowiedniej 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 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



Rys. 8.4. Propozycja praktycznego wykorzystania wzmacnianego systemu kryptograficznego w aspekcie biometrii behawioralnej

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 jest punktem wyjścia dla pracy generatora, którego stan po zakończeniu działania wyznacza finalny klucz kodowy.

9. 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.

Skonstruowanie specjalistycznego stanowiska pomiarowego dla biometrii mulitmodalnej pozwoliło na realizację badań zgodnie z założonym scenariuszem. Na podkreślenie zasługuje fakt, że odpowiedni 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 [140], 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 dyskryminacyjnej Fisher'a w celu doboru istotnych współczynników biometrycznych,
      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.

Wnioski

Współczesne narzędzia elektroniczne, wspierane nowoczesnym oprogramowaniem, spełniają rozliczne zadania ukierunkowane na optymalizację codzienności człowieka. Niektóre z nich mają wprawdzie tendencję do dominacji nad użytkownikiem, zaimplementowaną naturalnie przez projektanta, lecz możliwość wyboru ich zastosowania jest na szczęście po stronie odbiorcy. Znaczna część tych ofert ma dyskusyjną przydatność, niektóre z nich mogą być dla sceptyka wręcz natrętne i nieprzyjazne.

Po przeciwnej stronie, w świetle kryterium tzw. społecznego zapotrzebowania, umiejscowione są zastosowania technologii elektronicznej i informatycznej w tych dziedzinach, które immanentnie wiążą się z człowiekiem w jego fizjologicznym i behawioralnym rozumieniu[1]. Można zaryzykować twierdzenie, iż w przypadku biocybernetycznego sprzężenia zwrotnego, gdy człowiek jest obiektem wydającym realne sygnały, poddawane dalszemu przetwarzaniu, odbiór społeczny jest korzystny.

Ważnym wnioskiem, wynikającym z przeprowadzonych badań, jest przeświadczenie o konieczności dalszego poszukiwania takich behawioralnych cech biometrycznych, które byłyby zarówno dystynktywne, jak i bardziej stabilne w czasie. Wielce pożytecznym byłoby badanie rozkładu wartości takiej cechy. Rozkład normalny jest znamienny dla mierzalnych cech człowieka w normie fizjologicznej, natomiast w przypadku analizy zachowań (odruchowych i wyuczonych) istnieje szansa, iż rozkład ten jest jednostajny.

Interdyscyplinarny wniosek, o przypuszczalnie niewielkim stopniu złożoności w przypadku praktycznej aplikacji, to sugestia zbadania za pomocą skonstruowanego systemu liczniejszej grupy osób. Celem tego badania, uśrednionego w dłuższym czasie, byłoby nauczanie poprawnego wyróżniania dźwięków. Efekt ten jest nieoceniony w kształceniu słuchu, dotychczas jednym z trudniejszych przedmiotów w profilowanym kształceniu muzycznym[2].

Realizowane eksperymenty jednoznacznie pouczają, iż w praktyce pomiarowej, kiedy podmiotem jest człowiek, atrybut nieinwazyjności odgrywa dominującą rolę.

[1] Nawet wówczas, gdy rozważa się „wykrywacz kłamstw", odsłaniający przecież obszary celowo skrywane przed otoczeniem, uznaje się jego wysoką użyteczność. [77]

[2] Osoby ze słuchem absolutnym stanowią niekwestionowaną mniejszość, także wśród muzyków; pozostali uczą się rozpoznawania względnego dźwięków. [78]

Wyrażanie sympatii przez osobę poddającą się eksperymentowi naukowemu często determinuje powodzenie wykonania stawianego zadania. W niniejszej pracy przypadek ten odnosi się do pomiaru EKG, wymagającego dołączenia elektrod do nóg. Zastosowanie mniej absorbującej metody pomiaru pracy serca byłoby wielce wskazane. Alternatywnym rozwiązaniem mogłoby być wykorzystanie innej metody pomiaru reakcji człowieka (z zakresu inżynierii biomedycznej).

Nieostatnim i bardzo istotnym problemem, stanowiącym kontynuację linii badawczej prezentowanej dysertacji, jest poszukiwanie specyficznych metod stymulacji, które będą stosowne również dla osób z pewnymi deficytami. Ważne zagadnienie stanowi odpowiedni dobór takich zadań do wykonania w czasie badania, które będą wykonalne przez osoby niepełnosprawne, na przykład przez głuchoniemych.

Biometria jako subdyscyplina biocybernetyki cieszy się społecznym przyzwoleniem, zupełnie uzasadnionym w codzienności wymagającej od nas zapamiętywania PIN-ów, kodów, haseł, czy opanowania hierarchizacji uprawnień. Fizjologiczne cechy biometryczne postrzegamy z odcieniem obaw, nieufni wobec hipotetycznych możliwości nadużyć. Biometria behawioralna, ogniskująca kierunki badań prezentowanej dysertacji, może cieszyć się większym powodzeniem, ponieważ w jej przypadku cechy biometryczne skrywa nasz organizm w sensie wymiernym lub układ nerwowy w sensie centrum sterowania reakcjami. Użycie wartości cech do kodowania informacji stanowi dostateczne rozproszenie widma, by użytkownik mógł nie tylko być bezpiecznym, lecz także bezpiecznym się czuć. Dewaluacja kryptograficznej jakości szyfrów alfanumerycznych, stanowiąca wszakże rezultat niskiej dbałości o nie przez samego użytkownika, może być skompensowana wysokim stopniem złożoności biometrycznie parametryzowanych kodów. Oparcie algebraiczne w postaci logiki wielowartościowej wprowadza dodatkowe stopnie swobody w kształtowaniu mocy kryptograficznej.

Bibliografia

[1] American Clinical Neurophysiology Society `http://www.acns.org`. Stan na dzień 21.11.2010.

[2] A. Adler. Vulnerabilities in biometric encryption systems. *In International Conference on Audio and Video based Biometric Person Authentication*, strony 1100–1109, 2005.

[3] F. Agrafioti, D. Hatzinakos. ECG based recognition using second order statistics. *Communication Networks and Services Research Conference, 2008. CNSR 2008. 6th Annual*, strony 82–87, 5–8 2008.

[4] F. Agrafioti, D. Hatzinakos. Fusion of ECG sources for human identification. *Communications, Control and Signal Processing, 2008. ISCCSP 2008. 3rd International Symposium on*, strony 1542–1547, March 2008.

[5] 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.

[6] F. Agrafioti, D. Hatzinakos. Signal validation for cardiac biometrics. *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*, strony 1734–1737, march 2010.

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

[8] D. Beusa. *Music: a Mathematical Offering.* Cambridge University Press, 2008.

[9] L. Biel, O. Pettersson, L. Philipson, P. Wide. ECG analysis: a new approach in human identification. *Instrumentation and Measurement Technology Conference, 1999. IMTC/99. Proceedings of the 16th IEEE*, wolumen 1, strony 557–561, 1999.

[10] L. Biel, O. Pettersson, L. Philipson, P. Wide. ECG analysis: a new approach in human identification. *Instrumentation and Measurement, IEEE Transactions on*, 50(3):808–812, june 2001.

[11] Biometric Glossary `http://www.biometrics.gov/Documents/Glossary.pdf`. Stan na dzień 04.06.2010.

[12] Biometrics gaining global acceptance. *Biometric Technology Today*, 2009(11):4–5, November–December 2009.

[13] G. Birkhoff, S. Mac Lane. *Przegląd algebry współczesnej*. Państwowe Wydawnictwo Naukowe, Warszawa, 1966.

[14] A. Bodo. Method for producing a digital signature with aid of a biometric feature. german patent de 42 43 908 a1, June 1994.

[15] R. Bolle, J. Connell, S. Pankanti, N. Ratha, A. Senior. *Guide to Biometrics*. SpringerVerlag, 2003.

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

[17] J. Campbell. Speaker recognition: a tutorial. *Proceedings of the IEEE*, 85(9):1437–1462, sep 1997.

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

[19] B. Chen, V. Chandran. Biometric based cryptographic key generation from faces. *Digital Image Computing Techniques and Applications, 9th Biennial Conference of the Australian Pattern Recognition Society on*, strony 394–401, 2007.

[20] Y. Chen, G. Parziale, E. Diaz-Santana, A. K. Jain. 3d touchless fingerprints: Compatibility with legacy rolled images. *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the*, strony 1–6, 2006.

[21] A. Chodkowski red. *Encyklopedia muzyki*. Wydawnictwo naukowe PWN, Warszawa, 1995.

[22] R. A. Cole, J. Mariani, H. Uszkoreit, A. Zaenen, V. Zue. *Survey of the State of the Art in Human Language Technology (Studies in Natural Language Processing)*. Cambridge University Press, mar 1997.

[23] B. Dąbrowska, A. Dąbrowski. *Podstawy elektrokardiografii*. Wydawnicwtwo Lekarskie PZWL, Warszawa, 2007.

[24] D. Dubin. *Interpretacja EKG*. Wydawnicwtwo Lekarskie PZWL, Warszawa, 2008.

[25] Education, education,education... *Biometric Technology Today*, 2010(3):10–11, March 2010.

[26] S.-C. Fang, H.-L. Chan. Human identification by quantifying similarity and dissimilarity in electrocardiogram phase space. *Pattern Recognition*, 42(9):1824–1831, 2009.

[27] S. Furui. Speaker recognition. *Scholarpedia*, 3(4):3715, 2008.

[28] Fingerprint Verification Competition 2006 `http://bias.csr.unibo.it/fvc2006/`. Stan na dzień 03.04.2010.

[29] D. P. Golden, R. A. Wolthuis, G. W. Hoffler. A spectral analysis of the normal resting electrocardiogram. *Biomedical Engineering, IEEE Transactions on*, BME-20(5):366–372, September 1973.

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

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

[32] 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.

[33] J. Greń. *Statystyka matematyczna Modele i zadania*. Państwowe Wydawnictwo Naukowe, Warszawa, 1974.

[34] P. Górecki. Ultraniskoszumny wzmacniacz mikrofonowy do komputera. *Elektronika dla wszystkich*, strony 13–18, marzec 2004.

[35] S. Hilley. When biometrics are far from borderline. *Infosecurity*, 4(8):30–33, 2007.

[36] R. Hoekema, G. J. H. Uijen, A. van Oosterom. Geometrical aspects of the interindividual variability of multilead ECG recordings. *Biomedical Engineering, IEEE Transactions on*, 48(5):551–559, may 2001.

[37] K. Hryńków-Statkiewicz. *Skuteczne metody wykrywania uszkodzeń w układach logiki wielowartościowej.* Praca doktorska, Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki, 2004.

[38] K. Hryńków-Statkiewicz, A. W. Mitas. Generatory psudolosowe w technice mvl w aspekcie zastosowań biometrycznych. *„Techniki Komputerowe", Naukowy Biuletyn Informacyjny Instytutu Maszyn Matematycznych*, strony 49–58, 2003.

[39] ICAO Document 9303, Part 1, Volume 2 (e-passports).

[40] M. Łakomy, J. Zabrodzki. *Scalone przetworniki analogowo-cyfrowe i cyfrowo-analogowe.* Państwowe Wydawnictwo Naukowe, Warszawa, 1985.

[41] International Federation of Clinical Neurophysiology `http://www.ifcn.info`. Stan na dzień 21.11.2010.

[42] H. Imai, K. Kobara, Y. Watanabe. about human-crypto. *IEICE Transaction*, 100(100):57–64, May 2000.

[43] J. Irvine, B. Wiederhold, L. W. Gavshon, S. I. S. McGehee, R. Meyer, M. D. Wiederhold. Heart rate variability: a new biometric for human identification. *Proceedings of the International Conference on Artificial Intelligence (IC-AI '01)*, strony 1106–1111, Las Vegas, 2001.

[44] J. M. Irvine, S. A. Israel, W. T. Scruggs, W. J. Worek. eigenpulse: Robust human identification from cardiovascular function. *Pattern Recognition*, 41(11):3427–3435, 2008.

[45] J. M. Irvine, S. A. Israel, M. D. Wiederhold, B. K. Wiederhold. A new biometric: human identification from circulatory function. *Proceedings of the Joint Statistical Meetings of the American Statistical Association*, strony 1—-7, San Francisco, August 2003.

[46] S. A. Israel, J. M. Irvine. A sequential procedure for individual identity verification using ECG. *EURASIP Journal on Advances in Signal Processing*, 2009, 2009.

[47] 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.

[48] S. A. Israel, J. M. Irvine, B. K. Wiederhold, M. D. Wiederhold. *The heartbeat: the living biometric, w Biometrics: Theory, Methods, and Applications (eds N. V. Boulgouris, K. N. Plataniotis and E. Micheli-Tzanakou).* John Wiley & Sons, Inc., Hoboken, NJ, USA, 2009.

[49] S. A. Israel, W. T. Scruggs, W. J. Worek, J. M. Irvine. Fusing face and ECG for personal identification. *Applied Imagery Pattern Recognition Workshop, 2003. Proceedings. 32nd*, strony 226–231, October 2003.

[50] Y. Itakura, R. H. Tsujii. Proposal on personal authentication system in which biological information is embedded in cryptosystem key. *Joho Shori Gakkai Kenkyu Hokoku*, (45):19–27, 2003.

[51] A. K. Jain, P. Flynn, A. A. Ross. *Handbook of Biometrics.* Springer Verlag, Secaucus, NJ, USA, 2007.

[52] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross. Biometrics: a grand challenge. *Proceedings of International Conference on Pattern Recognition*, strony 935–942, 2004.

[53] A. K. Jain, A. Ross, S. Prabhakar. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image–and Video-Based Biometrics*, 14:4–20, 2004.

[54] P. K. Janbandhu, M. Y. Siyal. Novel biometric digital signatures for internet-based applications. *Inf. Manag. Comput. Security*, 9(5):205–212, 2001.

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

[56] 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.

[57] S. Karpagachelvi, M.Arthanari, T. Shakthi. ECG feature extraction techniques – a survey approach. *International Journal of Computer Science and Information Security*, 8(1):76–80, 2010.

[58] P. Kasprowski, J. Ober. With the flick of an eye. *Biometric Technology Today*, 12(3), 2004.

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

[60] W. Kester. *The data conversion handbook*. Elsevier: Newnes, 2005.

[61] A. Kholmatov, B. Yanikoglu. Realization of correlation attack against the fuzzy vault scheme. *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. Edited by Delp, Edward J., III; Wong, Ping Wah; Dittmann, Jana; Memon, Nasir D. Proceedings of the SPIE*, 6819:68190O–68190O–7, 2008.

[62] D. E. Knuth. *Sztuka programowania. T. 2, Algorytmy seminumeryczne*. WNT, Warszawa, 2002.

[63] Z. Kulka, A. Libura, M. Nadachowski. *Przetworniki analogowo-cyfrowe i cyfrowo-analogowe*. Wydawnictwo Komunikacji i Łączności, Warszawa, 1987.

[64] 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.

[65] M. Kyoso, A. Uchiyama. Development of an ECG identification system. *Engineering in Medicine and Biology Society, 2001. Proceedings of the 23rd Annual International Conference of the IEEE*, wolumen 4, strony 3721–3723, 2001.

[66] LabJack UE9 User's Guide dostępny na `www.labjack.com`.

[67] M. Li, S. Narayanan. Robust ECG biometrics by fusing temporal and cepstral information. *Pattern Recognition (ICPR), 2010 20th International Conference on*, strony 1326–1329, August 2010.

[68] G. Malinowski. *Logiki wielowartościowe*. Państwowe Wydawnictwo Naukowe, Warszawa, 2006.

[69] A. J. Mansfield, J. L. Wayman. *Best Practices in Testing and Reporting Performance of Biometric Devices (Version 2.01)*. NPL Report, August 2002.

[70] J. Martinez, R. A. S., Olmos, A. Rocha, P. Laguna. A wavelet-based ECG delineator: evaluation on standard databases. *Biomedical Engineering, IEEE Transactions on*, 51(4):570 –581, April 2004.

[71] MATLAB® – The Language for Technical Computing `http://www.mathworks.com`.

[72] A. W. Mitas. Zastosowanie funkcji rejestru liniowego do osobistej ochrony danych w przesyle informacji. *„Techniki Komputerowe", Naukowy Biuletyn Informacyjny Instytutu Maszyn Matematycznych*, 35(1):55–61, 2000.

[73] A. W. Mitas. Ochrona zasobów własnych za pomocą ciągów losowych parametryzowanych biometrycznie. *„Techniki Komputerowe", Naukowy Biuletyn Informacyjny Instytutu Maszyn Matematycznych*, 36(1):57–65, 2001.

[74] A. W. Mitas. Podpis elektroniczny. biometryczna parametryzacja podpisu elektronicznego. *W pracy zbiorowej „Biometria – wybrane zagadnienia"*, strony 85–88, 2004.

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

[76] A. W. Mitas. Słowo wstępne. *Techniki Komputerowe, Wydanie Specjalne Monograficzne*, 42(1):7–8, 2008.

[77] A. W. Mitas. Cykl wykładów z przedmiotu Biometria, Gliwice, 2010/11.

[78] A. W. Mitas. Cykl wykładów z przedmiotu Muzyka a Biocybernetyka, Gliwice, 2010/11.

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

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

[81] 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.

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

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

[84] 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.

[85] 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.

[86] 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.

[87] 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.

[88] A. W. Mitas, K. Dudek. Scenariusze i algorytmy biometrii multimodalnej. *Techniki Komputerowe, Wydanie Specjalne Monograficzne*, 42(1):143–152, 2008.

[89] A. W. Mitas, D. Mostowski. Podpis elektroniczny. *„Techniki Komputerowe", Naukowy Biuletyn Informacyjny Instytutu Maszyn Matematycznych*, 40(1):67–79, 2005.

[90] 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.

[91] F. Monrose, M. K. Reiter, Q. Li, S. Wetzel. Cryptographic key generation from voice. *Security and Privacy, 2001. S P 2001. Proceedings. 2001 IEEE Symposium on*, strony 202–213, 2001.

[92] F. Monrose, M. K. Reiter, S. Wetzel. Password hardening based on keystroke dynamics. *Proceedings of sixth ACM Conference on Computer and Communication Security*, strony 202–213, 1999.

[93] M. M. Monwar, M. Gavrilova. Fes: A system for combining face, ear and signature biometrics using rank level fusion. *Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on*, strony 922 –927, 7-9 2008.

[94] 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.

[95] D. Mostowski. *Próbki biometryczne odcisków palców w zastosowaniu do kryptografii oraz parametryzacji bezpiecznego podpisu elektronicznego.* Praca doktorska, Politechnika Śląska, Wydział Automatyki, Elektroniki i Informatyki, 2007.

[96] K. Nandakumar, Y. Chen, S. C. Dass, A. K. Jain. Likelihood ratio-based biometric score fusion. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 30(2):342–347, 2008.

[97] K. Nandakumar, Y. Chen, A. K. Jain, S. C. Dass. Quality-based score level fusion in multibiometric systems. *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, wolumen 4, strony 473–476, 2006.

[98] K. Nandakumar, A. K. Jain. Multibiometric template security using fuzzy vault. *Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on*, strony 1–6, 2008.

[99] K. Nandakumar, A. Ross, A. K. Jain. Biometric fusion: Does modeling correlation really matter? *Biometrics: Theory, Applications, and Systems, 2009. BTAS '09. IEEE 3rd International Conference on*, strony 1–6, 2009.

[100] T. Natanson. *Wstęp do nauki o muzykoterapii.* Zakład Narodowy im. Ossolińskich, Wrocław, 1979.

[101] National Committee for Information Technology Standards `http://www.ncits.org`. Stan na dzień 02.07.2010.

[102] National Institute of Standards and Technology `http://www.nist.gov`. Stan na dzień 02.07.2010.

[103] M. Owoc. Zmierzch podpisu tradycyjnego. *W pracy zbiorowej „Biometria – wybrane zagadnienia"*, strony 78–80, 2004.

[104] M. Owoc. Biometryczne gwarancje praw obywatelskich. *Techniki Komputerowe, Wydanie Specjalne Monograficzne*, 42(1):9–14, 2008.

[105] R. Palaniappan, S. M. Krishnan. Identifying individuals using ECG beats. *Signal Processing and Communications, 2004. SPCOM '04. 2004 International Conference on*, strony 569–572, dec. 2004.

[106] R. Paranjape, J. Mahovsky, L. Benedicenti, Z. Koles'. The electroencephalogram as a biometric. *Electrical and Computer Engineering, 2001. Canadian Conference on*, strony 1363–1366 vol. 2, 2001.

[107] J. N. Pato, L. I. Millett. *Biometric Recognition: Challenges and Opportunities*. The National Academies Press, Washington, D. C., 2010.

[108] T. B. Pedersen, E. Savas. Securing fuzzy vault schemes through biometric hashing. *Turk J Elec Eng & Comp Sci*, 18(4):515–539, 2010.

[109] 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.

[110] M. Plucińska. System kontroli dostępu i rejestracji czasu pracy XChronosBio – wybrane aspekty wdrażania technologii biometrycznych. *Problemy biometrii. Monografia.*, strony 81–96, 2009.

[111] M. Plucińska, J. Ryżko. Development of biometric technologies and applications in 2007–2008. *Biometry – Special Issue*, strony 27–40, 2010.

[112] A. J. Power, E. C. Lalor, R. B. Reilly. Can visual evoked potentials be used in biometric identification? *Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE*, strony 5575–5578, 2006.

[113] S. Prabhakar, S. Pankanti, A. K. Jain. Biometric recognition: security and privacy concerns. *Security Privacy, IEEE*, 1(2):33–42, 2003.

[114] B. Prasanalakshmi, A. Kannammal. Secure cryptosystem from palm vein biometrics in smart card. *Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on*, wolumen 1, strony 653–657, 2010.

[115] Prince, M. Kaur, A. Mittal. Fingerprint matching system using level 3 features. *International Journal of Engineering Science and Technology*, 2(6):2258–2262, 2010.

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

[117] 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.

[118] P. Rodwell, S. Furnell, P. Reynolds. A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head. *Computers & Security*, 26(7-8):468 – 478, 2007.

[119] A. A. Ross, K. Nandakumar, A. K. Jain. *Handbook of Multibiometrics*. Springer Verlag, Secaucus, NJ, USA, 2006.

[120] R. K. Rowe, U. Uludag, M. Demirkus, S. Parthasaradhi, A. K. Jain. A multispectral whole-hand biometric authentication system. *Biometrics Symposium, 2007*, strony 1–6, 2007.

[121] I. Sarkar, F. Alisherov, T. hoon Kim, D. Bhattacharyya. Palm vein authentication system: A review. *International Journal of Control and Automation*, 3(1), March 2010.

[122] W. J. Scheirer, T. E. Boult. Cracking fuzzy vaults and biometric encryption. *in Proceedings of Biometrics Symposium*, strony 1–6, 2007.

[123] 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.

[124] J. Shi, K. yan Lam, M. Gu, H. Li. Reusable set constructions using randomized dissolvent templates for biometric security. *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, strony 1–6, 2009.

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

[126] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. Vijaya Kumar. *Biometric Encryption*. ICSA Guide to Cryptography, Chapter 22 McGraw-Hill, 1999.

[127] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. Vijaya Kumar. Biometric encryption: enrollment and verification procedures. *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, 3386:24–35, March 1998.

[128] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. Vijaya Kumar. Biometric Encryption using image processing. *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, 3314:178–188, April 1998.

[129] C. Soutar, D. B. Roberge, A. Stoianov, R. M. Gilroy, V. Bhagavatula. Method for secure key management using a biometric. US patent no. 6219794, April 2001.

[130] C. Soutar, G. J. Tomko. Secure private key generation using a fingerprint. *Proc. of the CardTech/SecurTech Conference*, 1:245–252, 1996.

[131] J. D. Stosz, L. A. Alyea. Automated system for fingerprint authentication using pores and ridge structure. *Proc. of the SPIE Automatic Systems for the Identification and Inspection of Humans*, 2277:210–223, 1994.

[132] J. Szabatin. *Podstawy teorii sygnałów*. Wydawnictwo Komunikacji i Łączności, Warszawa, 2003.

[133] R. Tadeusiewicz. *Sygnał mowy*. Wydawnictwo Komunikacji i Łączności, Warszawa, 1988.

[134] R. Tadeusiewicz, A. Iworski, J. Majewski. *Biometria*. Wydawnictwa AGH, Kraków, 1993.

[135] 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.

[136] The end of decade. *Biometric Technology Today*, 2010(1):8–11, November–December 2010.

[137] G. J. Tomko, A. Stoianov. Method and apparatus for securely handling a personal identification number or cryptographic key using biometric techniques. US patent no. 5712912, January 1998.

[138] UK schools get lessons in biometric usage. *Biometric Technology Today*, 15(9):8–9, September 2007.

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

[140] Ustawa o podpisie elektronicznym dz.u.01.130.1450.

[141] R. van de Plassche. *Scalone przetworniki analogowo-cyfrowe i cyfrowo-analogowe Wyd. 2.* Wydawnictwo Komunikacji i Łączności, Warszawa, 2001.

[142] 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.

[143] Y. Wang, K. Plataniotis, D. Hatzinakos. Integrating analytic and appearance attributes for human identification from ECG signals. *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the*, strony 1–6, September 2006.

[144] J. Wayman, A. Jain, D. Maltoni, D. M. (Eds). *Biometric Systems: Technology, Design and Performance Evaluation.* Springer, New York, 2005.

[145] 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.

[146] F. Wesołowski. *Zasady muzyki.* Wyd. 9, Polskie Wydawnictwa Muzyczne, Kraków, 1998.

[147] M. D. Wiederhold, S. A. Israel, R. P. Meyer, J. M. Irvine. Identification by analysis of physiometric variation US patent no. 6993378, January 2006.

[148] Wikipedia – The Free Encyclopedia `http://www.wikipedia.org` . Stan na dzień 28.07.2010.

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

[150] 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.

[151] O. Z. Yilmaz, E. Savas. Privacy preserving zero knowledge scheme for biometric authentication. *Signal Processing, Communication and Applications Conference, 2008. SIU 2008. IEEE 16th*, strony 1–3, 20-22 2008.

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

[153] B. Żuk. *Biometria stosowana.* Państwowe Wydawnictwa Naukowe, Warszawa, 1989.

Spis rysunków

2.1 Podział parametrów jakościowych 16
2.2 Przykładowy wykres współczynników FAR oraz FRR z zaznaczonym punktem EER 18

4.1 Zabezpiecznie klucza za pomocą biometryki 25
4.2 Schemat wykorzystania szablonu biometrycznego jako klucza szyfrującego 26
4.3 Generacja klucza kodowego na podstawie wybranych bitów próbki biometrycznej 26
4.4 Schemat powiązania biometrii z ciągiem pseudolosowym 27
4.5 Wykorzystanie szablonu biometrycznego jako klucza szyfrującego . . 27
4.6 Generacja klucza kodowego z użyciem metody *fuzzy commitment scheme* 28
4.7 Generacja klucza kodowego z użyciem metody *fuzzy vault* 29
4.8 Widmo tonu krtaniowego 33
4.9 Charakterystyka filtra traktu głosowego 33
4.10 Dziedziny przetwarzania głosu 34
4.11 Serce i jego stymulatory 37
4.12 Przykład fali EKG z punktami charakterystycznymi 38
4.13 Fala EKG z dodatkowymi punktami charakterystycznymi 40

5.1 System rejestracji reakcji 47
5.2 System pomiarowy z biocybernetycznym sprzężeniem zwrotnym . . . 48
5.3 Schemat rejestratora dźwięku 49
5.4 Wpływ liniowości przetwornika A/C na wyjściowy sygnał cyfrowy . . 50
5.5 Przykłady nieliniowości 51
5.6 Schemat rejestratora próbek 53
5.7 Schemat sprzężenia dla pobudzenia dźwiękowego 56
5.8 Przykładowe przebiegi sygnału dźwiękowego oraz funkcji autokorelacji dla głoski „a” z zaznaczonym pierwszym lokalnym maksimum x_{max} 57

5.9 Główne okno programu do akwizycji próbek 57
5.10 Schemat sprzężenia dla pobudzenia wizualnego 58
5.11 Algorytm eksperymentu 61
5.12 Schemat podłączenia rejestratora EKG 62
5.13 Okno aplikacji do graficznej prezentacji zarejestrowanych danych . . . 63
5.14 Schemat struktury danych przechowującej informację o badaniu użytkownika 64

6.1 Charakterystyka amplitudowa filtra 67
6.2 Przebieg sygnału EKG przed filtracją 68
6.3 Przebieg sygnału EKG po filtracji 68
6.4 Charakterystyka amplitudowa filtra do detekcji zespołu QRS 69
6.5 Przebiegi sygnału EKG po kolejnych fazach procesu detekcji zespołu QRS 70
6.6 Przebiegi sygnałów z zaznaczonymi punktami charakterystycznymi . . 71
6.7 Przebieg sygnału EKG z zaznaczonymi punktami R po zastosowaniu algorytmu korekcji 72
6.8 Przebieg odległości RR dla dwóch różnych osób 77
6.9 Przebieg RR z zaznaczonymi poprawnymi i błędnymi ekstremami . . 78
6.10 Przebieg RR z zaznaczonymi proponowanymi cechami 81
6.11 Przebiegi zgodności dla czterech osób 82
6.12 Przebiegi zgodności dla trzech różnych osób 83
6.13 Rozmieszczenie w przestrzeni wartości cech behawioralnych głosu . . 92
6.14 Rozmieszczenie w przestrzeni wartości cech uzyskanych z EKG 92
6.15 Dokładność dopasowania w zależności od metody 97
6.16 Rozmieszczenie w przestrzeni wartości współczynników uzyskanych z wektora $\mathrm{MFCC}_{\mathrm{śr}}$ za pomocą metody PCA 98
6.17 Dokładność dopasowania dla współczynników behawioralnych w zależności od liczby cech 98
6.18 Dokładność dopasowania dla wektora współczynników utworzonego na podstawie MFCC w zależności od liczby cech 99
6.19 Dokładność dopasowania dla wszystkich wykorzystanych współczynników w zależności od liczby cech 100

7.1 Propozycja systemu kryptograficznego wzmacnianego biometrycznie . 101
7.2 Schemat binarnego rejestru liniowego ze sprzężeniem zwrotnym 103
7.3 Schemat rejestru liniowego v-wartościowego o długości m objętego sprzężeniem zwrotnym 104

7.4 Propozycja ekstracji wartości logiki rejestru MVL z numeru PIN . . . 106
7.5 Przypisanie określonym punktom w przestrzeni cech parametrów generatora MVL . . . 107
7.6 Proces tworzenia klucza kryptograficznego wzmacnianego biometrycznie . . . 108

8.1 Okno modułu generowania i weryfikacji klucza . . . 109
8.2 Dwa scenariusze weryfikacji . . . 111
8.3 Algorytm generacji klucza kodowego . . . 112
8.4 Propozycja praktycznego wykorzystania wzmacnianego systemu kryptograficznego w aspekcie biometrii behawioralnej . . . 117

Wszystkie ilustracje zostały oryginalnie przygotowane przez autora niniejszej pracy, a ewentualne merytoryczne oparcie źródłowe wymieniono w tekście.

Spis tabel

2.1 Porównanie wybranych technik biometrii fizjologicznej 13
2.2 Porównanie wybranych technik biometrii behawioralnej 14

5.1 Przykładowe wyniki pomiarów 63

6.1 Zakres częstotliwości poszczególnych rodzajów głosów od najniższego do najwyższego 84
6.2 Zestawienie proponowanych współczynników dla sygnału głosu 86
6.3 Zestawienie proponowanych współczynników dla sygnału EKG 87
6.4 Średnie odległości euklidesowe pomiędzy wektorami cech poszczególnych osób 91
6.5 Liczba cech oraz stopień redukcji wymiarowości uzyskane w wyniku analizy metodami FLD i PCA 95

Spis algorytmów

6.1 Wyznaczenie położenia punktów R 71
6.2 Korekta położenia punktów R 72
6.3 Wyznaczanie ekstremów lokalnych na wykresie RR 79
6.4 Wyznaczanie rodzaju głosu 84
6.5 Ocena dokładności wektora cech 96
8.1 Wyznaczanie klucza kodowego 115

Wykaz skrótów i oznaczeń

FMR	–	False Match Rate
$FNMR$	–	False Non Match Rate
FRR	–	False Reject Rate
FAR	–	False Accept Rate
EER	–	Equal Error Rate
FTE	–	Failure to Enrollment Rate
FTA	–	Failure to Acquire Rate
$AFIS$	–	Automated Fingerprints Identification System
FRR	–	False Reject Rate
LPC	–	Linear Predictive Coding
DTW	–	Dynamic Time Warping
HMM	–	Hidden Markov Model
VQ	–	Vector Quantization
GMM	–	Gaussian Mixture Models
PCA	–	Principal Components Analysis
LDA	–	Linear Discriminant Analysis
AC	–	Autocorrelation
DCT	–	Discrete Cosine Transform
$k-NN$	–	k-Nearest Neighbor
APC	–	Atrial Premature Contraction
PVC	–	Premature Ventricular Contraction
HPE	–	Hermite Polynomial Extension
SVM	–	Support Vector Machine
GSV	–	Gaussian Super Vector
$HLDA$	–	Heteroscedastic Linear Discriminant Analysis
ε_c	–	nieliniowość całkowa
ε_r	–	nieliniowość różniczkowa

ξ	–	zmienna losowa oznaczająca wysokość generowanego dźwięku
$P(\cdot)$	–	prawdopodobieństwo zdarzenia losowego
$r(\cdot)$	–	funkcja korelacji wzajemnej sygnału dyskretnego
F_s	–	częstotliwość próbkowania sygnału
F_0	–	częstotliwość podstawowa sygnału
a	–	odległość pomiędzy dwoma dźwiękami
$\tilde{a}$	–	skorygowana odległość pomiędzy dwoma dźwiękami
FIR	–	Finite Impulse Response
IIR	–	Infinite Impulse Response
$h(\cdot)$	–	funkcja filtrująca sygnał
$w(\cdot)$	–	funkcja okna czasowego
$h_w(\cdot)$	–	funkcja filtrująca wymnożona przez okno czasowe
$FO(\cdot)$	–	funkcja opisująca sygnał
$R(i)$	–	moment czasu wystąpienia i-tego załamka R
$RR(i)$	–	odległość pomiędzy $i+1$, a i-tym załamkiem R
s	–	pochylenie odcinków pomiędzy ekstremami lokalnymi
d	–	odległości pomiędzy ekstremami
$d_{y,min}$	–	odległość maksimów lokalnych od wartości średniej minimów
w_e	–	szerokości ekstremów
$w_H(\cdot)$	–	funkcja okna Hamminga
MFC	–	Mel Frequency Coefficients
$MFCC$	–	Mel Frequency Cepstral Coefficients
FLD	–	Fisher Linear Discrimination
sr	–	stopień redukcji wymiarowości
$LFSR$	–	Linear feedback Shift Register
MVL	–	Multi Value Logic
v	–	wartość logiki rejestru MVL
m	–	długość rejestru rejestru MVL
g	–	wielomian charakterystyczny sprzężenia zwrotnego rejestru MVL
s_v	–	niezerowy ciąg inicjalizujący rejestru MVL
sk	–	stan końcowy rejestru MVL
ds	–	długość generowanej sekwencji rejestru
kk	–	klucz kodowy