Akademia Górniczo-Hutnicza
Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej
Katedra Automatyki i Inżynierii Biomedycznej

Rozprawa Doktorska

KODOWANIE INFORMACJI DODATKOWYCH W STRUKTURZE CYFROWEGO ELEKTROKARDIOGRAMU

Mgr inż. Agnieszka Świerkosz

Promotor:
Prof. zw. dr hab. inż. Piotr Augustyniak

Kraków 2018

Spis treści

1. Wstęp

1.1 Sygnał fizjologiczny jako nośnik informacji ukrytej

Kodowanie informacji w systemach transmisji i archiwizacji jest przedmiotem badań od wielu lat. Jego celem są zwykle: kompresja danych, zwiększenie odporności na zakłócenia oraz ochrona przed nieuprawnionym dostępem. W tym ostatnim zastosowaniu używane są techniki kryptograficzne, wykorzystujące szyfrowanie informacji oraz steganograficzne polegające na ukrywaniu istnienia informacji. Wbrew przyrostkowi '*grafia*', nośnikami informacji poufnej są nie tylko obrazy, ale również sygnały, w tym sygnały pochodzenia biologicznego. Kilka doniesień naukowych porusza tematykę wykorzystania zapisu elektrokardiograficznego jako nośnika informacji dodatkowych (metrykalnych, fizjologicznych lub środowiskowych).

Niniejsza rozprawa dotyczy ukrywania (steganografii) informacji dodatkowych w sygnale EKG. Autorka prezentuje analizę obecnego stanu wiedzy, własne propozycje algorytmów steganograficznych oraz wyniki ich testów. Badania kardiologiczne przeważnie wykonywane są w szpitalach i klinikach, w ustalonych warunkach, przez wykwalifikowany personel medyczny. Coraz częściej, dzięki rozwojowi telemedycyny oraz zminiaturyzowaniu i uproszczeniu sprzętu elektrokardiologicznego, można te pomiary wykonywać w domu. Tu rodzi się potrzeba poprawy kontroli warunków pomiaru. Można to osiągnąć między innymi poprzez:

1) identyfikację i eliminację czynników zakłócających,
2) interpretację składników elektrokardiogramu związanych z podstawową aktywnością elektryczną serca w kontekście aktywności i środowiska osoby badanej.

Ważne jest, aby dołączona wiadomość nie zmieniała wartości diagnostycznej sygnału. Zatem interpretacja medyczna zapisu z dołączoną wiadomością przeprowadzona przez lekarza lub oprogramowanie powinna być jednoznaczna z interpretacją zapisu oryginalnego. Kodowane informacje mogą służyć między innymi do identyfikacji pacjenta. Wiadomym jest, iż informacje można wysyłać jako osobny tekst. Integracja informacji metrykalnej w strukturze elektrokardiogramu, przy jednoczesnym zabezpieczeniu jej przed nieuprawnionym dostępem może być w przyszłości innowacyjnym narzędziem wspomagającym rozwój telemedycyny. Na tym polu nauki w przyszłości można wymyślić nowe narzędzia oraz algorytmy szyfrowania oraz odszyfrowywania danych. Przeprowadzone badania stanowią wkład do upowszechnienia stosowania steganografii w cyfrowym elektrokardiogramie.

Kodowanie informacji towarzyszących może wzbogacić interpretację zapisu EKG bez potrzeby definiowania nowych struktur danych i kanałów transmisji.

1.2 Cele i teza pracy

Podejmując badania Autorka założyła następującą tezę:

W reprezentacji czasowo-częstotliwościowej sygnału EKG można wskazać obszary niewykorzystane przez składniki kardiogenne, które mogłyby być użyte do ukrycia informacji dodatkowych bez wpływu na jego zawartość diagnostyczną.

Teza ta mówi, że dodatkowe informacje diagnostyczne lub administracyjne mogą być dołączone do struktury elektrokardiogramu cyfrowego nie zakłócając jego podstawowych informacji diagnostycznych. Celem przeprowadzonych badań jest zaproponowanie reguł kodowania, wdrożenie przykładowej procedury testowania oraz poznanie charakterystyki tego procesu dla różnych parametrów: sposobu dekompozycji sygnału nośnika (tzn. EKG), gęstości strumienia i rodzaju danych dodatkowych. W konkluzji Autorka przedstawia uzasadnienie wyboru parametrów kodowania, przy których informacje diagnostyczne pozostają niezmienione i oszacowanie wpływu przekroczenia tych granic.

Autorka przyjęła następujący plan działania:

1) Uruchomienie wersji rozwojowej (ang. *debug*) oprogramowania do automatycznej interpretacji EKG w zakresie niezbędnym do określenia punktów początkowych i końcowych załamków i diagnostyki elektrokardiogramu spoczynkowego. Modyfikacja oprogramowania w celu uzyskania dostępu do informacji opisujących poszczególne ewolucje serca (punkty detekcji zespołu QRS, granic załamków i klasyfikacja pobudzeń).

2) Zapoznanie się z bazą danych CSE (ang. *Common Standard for Quantitative Electrocardiography*), formatem danych i zawartością plików.

3) Zaproponowanie kilku wariantów bezstratnej transformacji umożliwiającej analizę lokalnych własności sygnału i kodowanie informacji dodatkowych w dziedzinie czasowo-częstotliwościowej.

4) Zaproponowanie sposobu podziału informacji dodatkowej i metody jej kodowania w reprezentacji czasowo-częstotliwościowej z wykorzystaniem informacji o lokalnych własnościach nośnika.

5) Zaproponowanie sposobu zapisu kodowanej informacji oraz jej opisania. Ponieważ miejsce z zakodowanymi danymi czyli kontener danych, może mieć zmienną lokalizację, długość oraz głębokość bitową, to jego opis powinien być ustandaryzowany.

6) Implementację wszystkich procedur zaproponowanych w 4) i 5) w programie Matlab. Elementem standardowych pakietów dostarczanych przez producenta są np. transformacje falkowe.

7) Testowanie metod kodowania informacji dodatkowych dla zmiennych: treść dodatkowa, głębokość bitowa, długość kontenera danych. Dla każdej z tych zmiennych przeprowadzono test w całej bazie CSE i zarejestrowano wyniki detekcji granic załamków i interpretacji.

8) Przeprowadzenie interpretacji testów w aspekcie ilościowym - dla każdej zmiennej wyznaczono, w jaki sposób zmienia się położenie punktów granicznych załamków i kiedy informacja dodatkowa wpływa na rezultaty pomiarów.

1.3 Układ pracy

Niniejsza rozprawa zawiera 7 rozdziałów. Teza pracy i cel oraz jej główne tematy zostały omówione w rozdziale pierwszym. Rozdział drugi wprowadza tematy badawcze oraz zawiera wyniki prac opublikowanych we wcześniejszych doniesieniach. Rozdział trzeci poświęcony został materiałom i narzędziom niezbędnym do wykonania eksperymentu, który został opisany w rozdziałach czwartym oraz piątym niniejszej rozprawy. Ostatnie dwa rozdziały opisują wyniki badań oraz podsumowanie.

2. Przegląd stanu wiedzy

2.1 Kodowanie informacji

Steganografia jest metodą utajniania informacji, w której zakodowany np. obraz może być przykryty inną, nieznaczącą treścią, aby odwrócić uwagę od sekretu i ukryć jego istnienie. Metody steganograficzne są na tyle skuteczne, że postronny odbiorca nie domyśla się, że pod jawną treścią nośnika skrywana jest tajemnica. Informacja dołączona jest w taki sposób, aby jawny obraz nie zdradzał, iż może zawierać zakodowany tekst lub inne treści dodatkowe. W przypadku steganografii z użyciem EKG, postronny odbiorca nie odróżni sygnału oryginalnego od nośnika z zakodowaną informacją i będzie w stanie przeprowadzić pełnowartościową i jednoznaczną interpretację każdego z nich nie domyślając się, iż poza sygnałem EKG, cyfrowy zapis kryje możliwość odkodowania z niego jeszcze jakichkolwiek innych informacji dodatkowych. Nośnik z zakodowaną informacją nie jest identyczny z sygnałem oryginalnym, ale pozostaje z nim jednoznaczny z punktu widzenia interpretacji zarówno wizualnej jak i maszynowej.

Kryptologia to nauka zajmująca się szyfrowaniem i kodowaniem informacji [Grajek M. i Gralewski L., 2009]. Dzieli się na kryptologię (dotyczy ona szyfrowania wiadomości) oraz kryptoanalizę (czyli łamanie szyfrów). O historii kryptologii można przeczytać w [Kahn D., 2004] i [Singh S., 2001]. W tych książkach autorzy opisali najważniejsze metody i problemy dotyczące szyfrowania i łamania szyfrów. Opisali konsekwencje tych poczynań na tle historycznym. Więcej na temat algorytmów kodowania można znaleźć w [Buchmann J. A., 2006] i [Kwiatkowski W., 2009]. Można obie te książki nazwać podręcznikami do kryptologii, ponieważ zawierają wstęp do kodowania, czyli opisują szyfry od strony matematycznej. Jest również książka poświęcona kryptografii i bezpieczeństwu w sieci [Stallings W., 2012]. Autor tej publikacji opisuje metody szyfrowania stosowane w Internecie. Zwraca również uwagę na możliwość dostępu osób niepowołanych do poufnych danych, np. przejęcia kontroli kont w sieci.

Autorka tej pracy doktorskiej poświęciła publikację sekretnemu, progowemu podziałowi obrazów, czyli kodowaniu informacji w obrazach [Świerkosz A., 2016a]. Napisała również kilka prac dotyczących modelowania w inżynierii biomedycznej [Świerkosz A., 2015] [Holewa K. i in., 2015].Ostatnimi opracowaniami Autorki były projekty kodowania informacji w cyfrowym elektrokardiogramie opublikowane jako materiały konferencyjne [Augustyniak P. i Świerkosz A., 2015], [Świerkosz A., 2016b], [Świerkosz A., 2016c],

[Świerkosz A., 2017]. Wyżej wymienione prace są ściśle związane z rozprawą i zawierają cząstkowe rezultaty prac badawczych przedstawionych w rozprawie. Przygotowując metody steganografii dla EKG Autorka przeglądnęła i przedstawiła poniżej metody stosowane w utajnianiu informacji w obrazach:

1. sekretny podział obrazu z odwracalną steganografią [Chan C. S. i in., 2009],
2. sekretny podział obrazu ze zdolnością wstępnego podglądu [Chen T. S. i Yang C. N., 2007],
3. sekretny podział obrazu i ukrywanie z autentykacją [Li P. i in., 2010],
4. sekretny podział obrazu z ulepszonym losowym podziałem [Nabiyev V. V. i in., 2008].

Sekretny podział (ang. *Secret Sharing* – SS) obrazu [Blakley G. R., 1979], [Shamir A., 1979], [Noar M. i Shamir A., 1995] polega na zastosowaniu odpowiedniego klucza, składającego się z *n* części. Może on odtworzyć utajniony obraz. Potrzeba do tego użyć *t* z *n* części klucza. Warunkiem jest, aby wartość *t* była mniejsza bądź równa *n*. Zazwyczaj $t > 1$, czyli pojedyncza osoba posiadająca jeden element sekretu nie może odtworzyć oryginalnego obrazu. Aby to uczynić, *t* uczestników musi współpracować przy jego rekonstrukcji stosując przy tym części kluczy, które otrzymali przy utajnianiu obrazu. Jest to metoda zabezpieczająca przed złośliwymi intruzami [Chan C. S. i in., 2009].

W parze z wynalezieniem (*t*, *n*) – progowej koncepcji Noar'a i Shamir'a [Noar M. i Shamir A., 1995], [Chan C. S. i in., 2009], powstała technika sekretnego podziału obrazu znana jako wizualny podział sekretu obrazu (ang. *Visual Secret Sharing* – VSS) [Su C. H. i Wang R. Z., 2006]. Posiada ona następujące cechy [Chan C. S. i in., 2009]:

- każdych *t* spośród *n* uczestników może współdziałać aby odtworzyć sekretny obraz,
- żaden z *t* - 1 uczestników eksperymentu nie może odtworzyć oryginału,
- kamuflaż musi być skuteczny,
- jakość podzielonych obrazów musi być dobra,
- odtworzony obraz musi być wolny od zniekształceń.

Jedną z technik utajniania obrazu jest sekretny podział obrazu z odwracalną steganografią. Metoda ta maskuje ukryty obraz tworząc tzw. stegoobraz. Nie można tu dostrzec sekretnego obrazu, ponieważ jest on schowany w strukturze innego.

Poniżej została opisana koncepcja Shamir'a (*t, n*)-progowego podziału [Shamir A., 1979], [Chan C. S. i in., 2009]. Mając podzielony sekret *s*, uczestnik posiadający część sekretu wyznacza pierwszą wartość *m* i wytwarza wielomian (*t*-1)-stopnia:

$$F(x) = (s + a_1 x + ... + a_{t-1} x^{t-1}) \bmod m \qquad (2.1)$$

gdzie składowe a_1, a_2, a_{t-1}, są losowo ustalane spośród liczb całkowitych z przedziału [0, m-1]. Uczestnik oblicza składowe sekretu:

$$y_1 = F(1), y_2 = F(2),..., y_n = F(n) \qquad (2.2)$$

i rozdziela składowe y_i wtajemniczonym uczestnikom. Obraz jest nieczytelny dla każdego uczestnika. Żaden z nich nie może zrekonstruować ukrytego obrazu, używając wielomianu Lagrange'a. Zestaw jest kompletny jeżeli liczba jego elementów jest większa lub równa *t.* Posiadający składowe sekretu powinni zebrać *t* z jego *n* części aby otrzymać obraz oryginalny $F(x)$ [Chan C. S. i in., 2009].

Mając podzielony sekretny obraz *S*, utajnia się i tworzy *n* stegoobrazów (steganografię). Ta procedura jest odwracalna, czyli ze stegoobrazów można otrzymać sekretny obraz *S*. Kodowanie i odkodowanie obrazu tą metodą wykonuje się w kilku etapach, które są opisane poniżej:

1) Faza tworzenia nieczytelnych obrazów. Można przyjąć, iż podzielone (t-1) liczby *S* są elementami ciągu: s_1, s_2, …, s_{t-1}. Przypuśćmy, iż *O* jest obrazem nośnika w skali szarości z $H \times W$ pikselami a *p* jest pikselem z *O*. Celem odwracalnego procesu jest odzyskanie sekretnych liczb s_1, s_2, …, s_{t-1}. jak również zachowanie wartości *p*.
2) Faza ukrywania. Aby osiągnąć cel steganografii, większość procedur bazuje na zamianie bitów [Chan C. S. i in., 2009], [Hsueh N. L., Lin C. C., 2008], [Rodriguez J. J. i Thodi D. M., 2007], [Ansair N. i in., 2008], co prowadzi do zniekształcenia nośnika. Oznacza to, że takie metody są niezdolne do rekonstrukcji pierwotnego obrazu nośnika na podstawie stegoobrazu. Aby zapewnić własność odwracalności, proponowany schemat może zachować funkcję oryginalnego piksela nośnika *p* przez wykorzystanie operacji kwantowania.
3) Procedura odzyskiwania sekretnego obrazu. Mając *t* spośród *n* stegoobrazów (O_j') i klucz (K_j) od wtajemniczonych uczestników, można zrekonstruować zarówno sekretny obraz *S*, jak i wolny od zniekształceń, kryjący obraz *O* (nośnik).

Kolejną metodą jest sekretny podział obrazu ze zdolnością wstępnego przeglądnięcia sekretu [Chen T. S. i Yang C. N., 2007] przy użyciu jednej z dwóch technik sekretnego podziału: opartej na wielomianie sekretnego podziału obrazu lub technice wizualnego podziału sekretu (ang. *Visual Secret Sharing*, VSS). Niektóre stegoobrazy (nośniki z zakodowaną informacją) można podzielić na *n* nieczytelnych części o rozmiarach *t*- krotnie mniejszych od oryginału podczas progowego podziału. Ich małe rozmiary powodują, że

technika ta jest odpowiednia do szybkiej transmisji, gdzie każda składowa sekretu jest rozdzielona po stronie nadawcy, a następnie gromadzona przez odbiorcę. Autorzy wymienionej powyżej publikacji dołożyli starań, aby ta technika progowego podziału obrazu spełniała wszystkie wymogi schematu sekretnego podziału. Potrzeba tylko *t* cieni dla odbiorcy, aby przesłać oraz całkowicie zrekonstruować sekretny obraz. Pominięcie (*n*– *t*) części składowych podczas transmisji nie będzie zakłócało fazy rekonstrukcji. Aby uzyskać sekretny podział obrazu ze zdolnością wstępnego przeglądnięcia można połączyć dwie sekretne strategie: bazujący na wielomianie sekretny podział i wizualny podział sekretu (ang. *Visual SecretScharing*, VSS), [Noar M. i Shamir A., 1995], [Chen T. S. i Yang C. N., 2007], [Laih C. S. i Yang C. N., 2000], [Eisen P. A. i Stinson D. R., 2002], [Lin C. C. i Tsai W. H., 2003], [Cimato S. i in., 2006], [Shyu S. J., 2006], [Chen T. S. i Yang C. N., 2006]. Korzyścią schematu VSS jest nie wymagające dużo czasu i wysiłku odkodowanie znaków poprzez ludzki wzrok bez jakichkolwiek obliczeń. Można użyć własności techniki wizualnego podziału sekretu w wielomianie sekretnego podziału, uzyskując z sukcesem wcześniejszy podgląd. Odbiorca może w prosty sposób sprawdzić (dokonać podglądu) bezpośrednio nie dokonując obliczeń. Po uprzednim sprawdzeniu uproszczonej treści sekretnego obrazu, można użyć obliczeń interpolacji Lagrange'a do jego pełnego odzyskania [Chen T. S. i Yang C. N., 2007], [Lin J. C. i Thien C. C., 2002].

Osobną metodą progowego kodowania jest sekretny podział obrazu i ukrywanie z autentykacją [Li P. i in., 2010]. Sekretny obraz jest dzielony, a powstałe części są ukrywane w kilku stegoobrazach tak, aby transmisja była bezpieczna. Niestety wadą tej techniki jest to, że każdy stegoobraz musi być zredukowany wielokrotnie, w stosunku do sekretu. Jako przykład zostanie przytoczony (*t*, *n*)- progowy schemat z obrazem zredukowanym do 3,5/*t*- krotności sekretnego obrazu z dobrą jakością obrazu, lepszą niż w poprzednim schemacie opisanym w publikacji [Li P. i in., 2010]. Dwa piksele sekretnego obrazu osadza się w siedmiopikselowym bloku obrazu-nośnika, obraz nośnika musi więc mieć 3,5-krotnie większy rozmiar niż obraz sekretny. W rezultacie można otrzymać lepszą wizualną jakość obrazu używając proponowanego schematu [Li P. i in., 2010].

Przykładowy schemat kodowania stegoobrazu zawiera dwie czynności:

1) Procedurę podziału i ukrycia. Przed podziałem, sekretny obraz należy zaszyfrować przy pomocy sekretnego klucza *K*. Jest on podzielony na *n* podkluczy dla każdej z *n* osób.
2) Autentykację i procedurę ujawnienia przeprowadzaną w oparciu o następujące postępowanie:
   - Do ujawnienia sekretnego obrazu potrzeba zgromadzić *t* lub więcej stegoobrazów.

- Najpierw sekretny klucz *K* można ujawnić przez interpolację Lagrange'a z *t* podkluczami.
- Następnie wyznacza się bity znaków wodnych (stanowiących ukrytą informację) wygenerowanych w oparciu o klucz *K*. Później, każdy stegoobraz jest dzielony na odrębne sekcje przy użyciu wzoru (2.3), a każda z nich posiada 128 bloków.

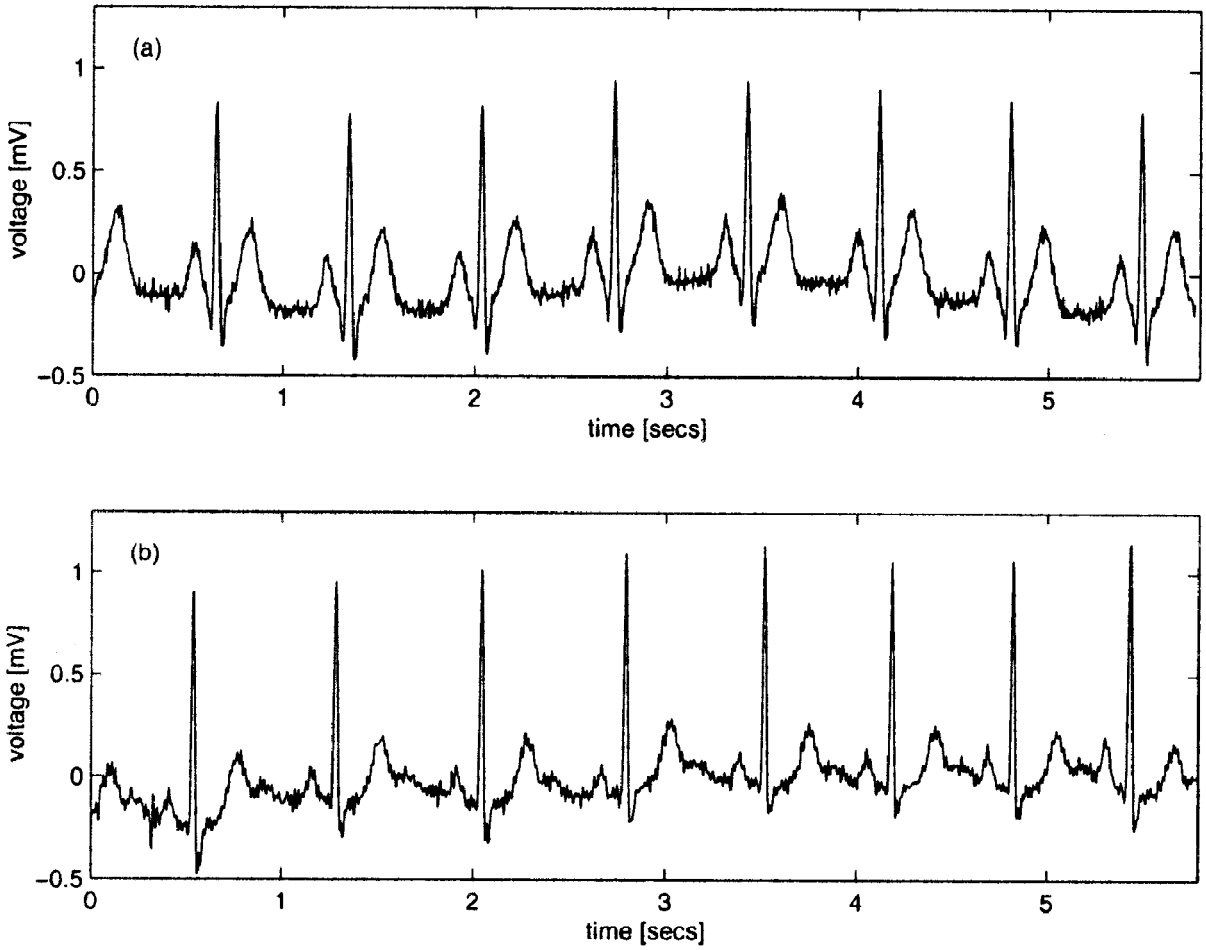
$$h_1 h_2 ... h_{128} = MD5((B_1^{'} - p_1) \| (B_2^{'} - p_2) \| ... \| (B_{128}^{'} - p_{128}) \| K) \qquad (2.3)$$

  gdzie funkcja MD5 generuje bity autentykacyjne.
- Kolejnym krokiem jest obliczenie bitów kontrolnych ($p_1^{'} p_2^{'} ... p_{128}^{'}$) bieżącej sekcji. Jeśli są równe tym osadzonym bitom $p_1 p_2 ... p_{128}$, wtedy bieżąca sekcja jest weryfikowana pomyślnie.
- Proces autentykacji i ujawniania jest powtarzany dopóki można odzyskać *t* nieczytelnych obrazów z *t* stegoobrazów. Ostatecznie ujawnia się obraz sekretny przy użyciu interpolacji Lagrenge'a [Li P. i in., 2010].

Ostatnią metodą jest sekretny podział obrazu z ulepszonym podziałem losowym. Jest ona szczegółowo zaprezentowana w [Nabiyev V. V. i in., 2008] i bazuje na schemacie Chen i Wu [Chen L. H. i Wu C. C., 1998]. Metoda ta wykorzystuje rotację (o 90° w prawo) do osadzenia dwóch zestawów sekretnych obrazów w dwie części nośnika. Wizualny podział sekretu (VSS) to metoda rozpraszająca sekret w losowo podzielone fragmenty, by po złączeniu ich w całość zrekonstruować oryginalny obraz. Każda pierwsza ukrywana część tajemnicy jest losowym wzorem czarno- białych pikseli. Drugi sekret jest tworzony zależnie od pierwszego. Muszą one być ułożone razem w stertę, jeśli trzeba zrekonstruować pierwszy, ukryty obraz. Sterta dwóch części zrekonstruuje drugi sekret podczas obracania pierwszej o 90° w lewo (tj. przeciwnie do kierunku wskazówek zegara). Nowość algorytmu, polega na utworzeniu obydwu części obrazu z dwóch sekretów. Dzielący algorytm można utworzyć przez wybieranie rozszerzonych wzorów przypadkowych pikseli w celu poprawnego kontrastu wymaganego od obu tajemnic zrekonstruowanych przez składową nie obróconą i obróconą układane w stertę. Ta metoda jest bezpieczna ze względu na losowość składowych tajemnicy [Nabiyev V. V. i in., 2008].

2.2 Sygnał EKG

Sygnał elektrokardiograficzny (EKG) bada się w celu rozpoznania chorób serca na podstawie jego aktywności elektrycznej. Synchroniczna aktywność komórek mięśnia serca prowadzi do wytworzenia wypadkowego potencjału elektrycznego, który można zarejestrować za pomocą elektrod używając do tego celu urządzenia zwanego elektrokardiografem. Na rysunkach 2.1 i 2.2 przedstawiono odpowiednio wynik badania u zdrowego człowieka oraz zespół QRS, natomiast rysunek 2.3 przedstawia umiejscowienie elektrod potrzebnych do rejestracji zapisu elektrycznej aktywności serca.



Rys. 2.1. Porównanie (a) syntetycznego sygnału EKG z dodatkiem błędów pomiaru o rozkładzie normalnymi (b) rzeczywistego sygnału EKG od zdrowego człowieka [McSharry P. E. i in., 2003]

Przykładowymi chorobami obserwowanymi w elektrokardiogramie są:

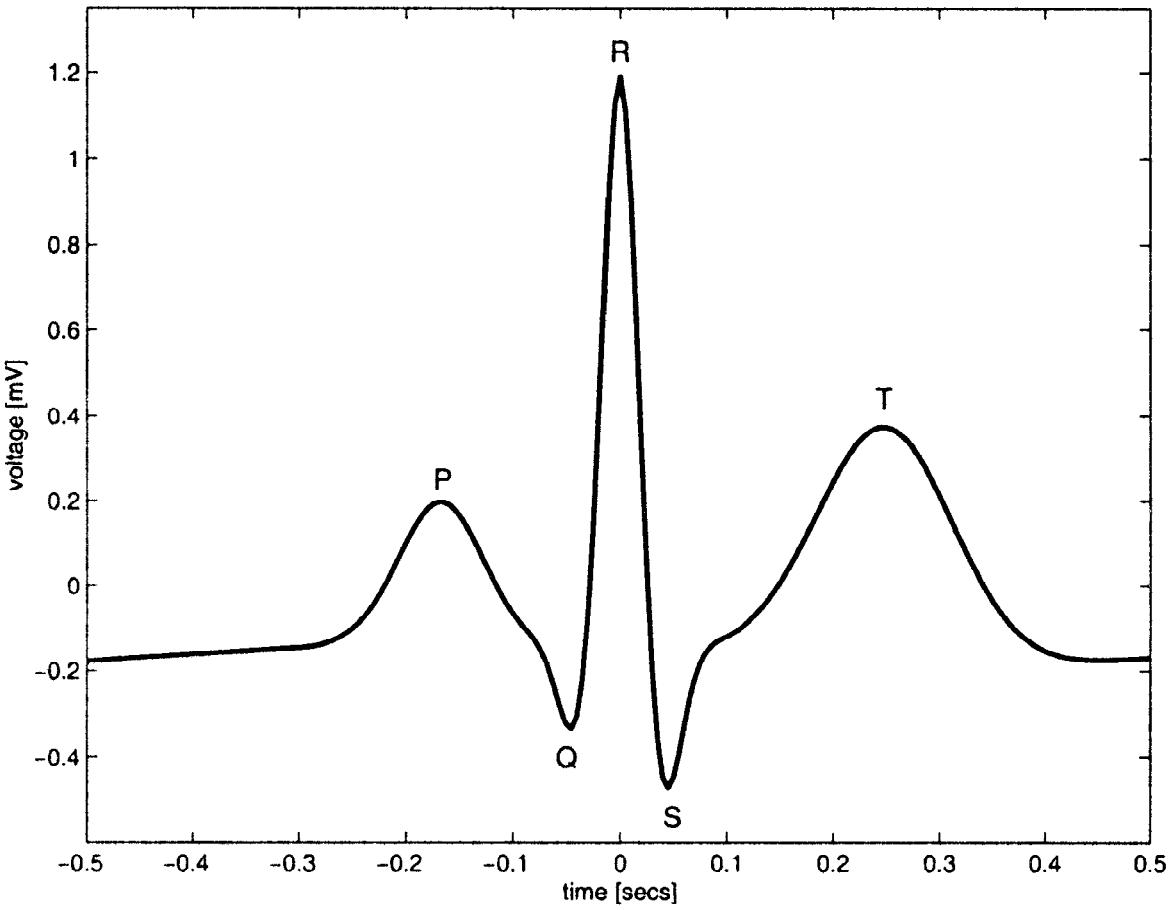
- Zaburzenia rytmu serca spowodowane nieregularną pracą komórek rozrusznikowych lub uaktywnieniem dodatkowych ośrodków bodźcotwórczych; zaburzenia te są obserwowane jako zmiany długości interwału międzyuderzeniowego RR,

- Niedokrwienie mięśnia sercowego spowodowane przez niewydolność krążenia wieńcowego (chorobę niedokrwienną serca); zmiana ta objawia się odmiennym przebiegiem repolaryzacji, który w elektrokardiogramie manifestuje się przez zmianę kształtu odcinka ST.

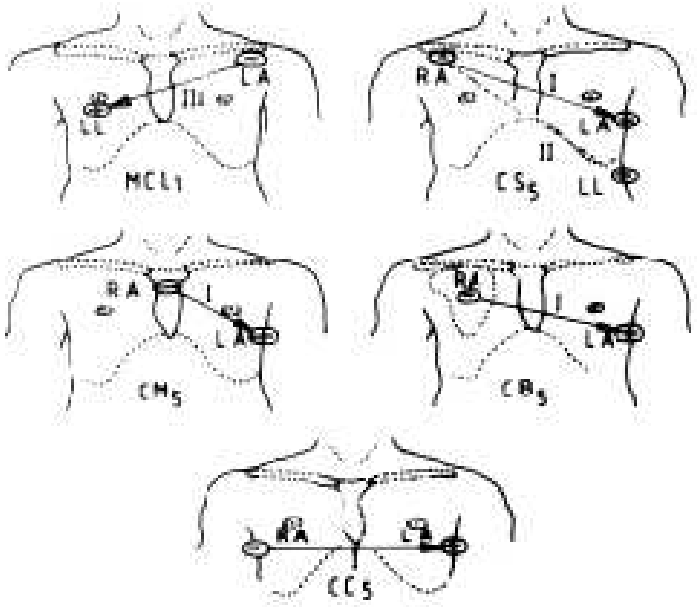
Elektrokardiogram reprezentuje cykliczną pracę poszczególnych części serca: załamek P odpowiada skurczowi przedsionków, zespół QRS – skurczowi komór, a załamek T – fazie repolaryzacji komór. Każdy z tych odcinków wnosi inny wkład do diagnostyki serca i charakteryzuje się inną istotnością diagnostyczną. Dodatkowo, w każdym z nich zjawiska elektryczne zachodzą w tkankach o innych własnościach, w rezultacie składowe kardiogenne sygnału EKG podlegają innym ograniczeniom. Ponieważ sygnał EKG jest próbkowany ze stałą częstotliwością dostosowaną do składowych kardiogennych występujących jedynie na krótkim odcinku zespołu QRS, składowe w obrębie załamków P i T wypełniają tylko część użytecznego pasma dyskretnej reprezentacji sygnału. Dodatkowo, linia izoelektryczna, której odcinki łączą załamki nie zawiera składowych kardiogennych, a jej znaczenie diagnostyczne sprowadza się do wyznaczenia długości odcinków między załamkami. Fragmenty zapisu EKG, w których składowe kardiogenne nie wypełniają całego pasma dyskretnej reprezentacji sygnału zostały nazwane luką pasmową (ang. *band gap*) i mogą zostać wykorzystane do kodowania informacji dodatkowej.

W niektórych przypadkach, może zdarzyć się że luka pasmowa, czyli miejsce o najmniejszej wartości diagnostycznej, w zapisie elektrokardiogramowym może być zbyt mała aby zakodować w sygnale EKG informacje dodatkowe. Niestety niektóre choroby mogą uniemożliwiać wkodowanie danych dodatkowych w strukturze cyfrowego zapisu EKG. O ile celem odgórnym jest to aby dane dodatkowe nie zniekształcały informacji diagnostycznych w zapisie na tyle, aby możliwa była prawidłowa diagnoza, to w przypadku chorób takich jak np. arytmia, kodowanie nie będzie miało sensu, ponieważ luka pasmowa jest zbyt wąska, żeby można byłoby wkodować do niej dodatkowe informacje.

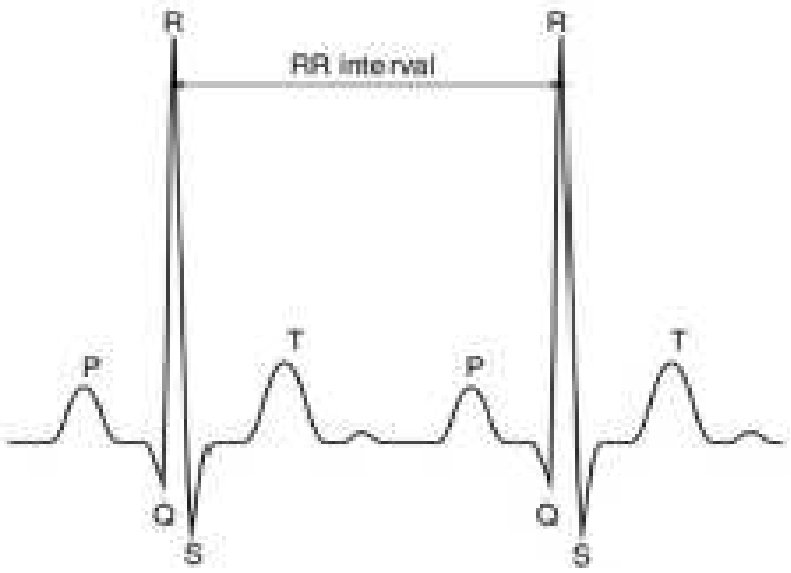
W metodach opisywanych w tej pracy wkodowanie informacji w sygnale było zależne od położenia i długości interwału RR i od typu ewolucji serca. Jego graficzny opis jest przedstawiony na rysunku 2.4.



Rys. 2.2. Morfologia jednej ewolucji serca zawierająca załamek P, zespół QRS i załamek T w EKG [McSharry P. E. i in., 2003]



Rys.2.3.Umiejscowienie elektrod w zmodyfikowanym systemie trzech elektrod [Dash P. K., 2002]



Rys. 2.4. Odcinek sygnału EKG, który zawiera dwa uderzenia serca oraz informacje leżące na załamkach P, Q, R, S i T w każdym uderzeniu serca i długość interwału RR między nimi [Singh Y. N. i in., 2012]

2.3 Wykorzystanie rozkładu informacji diagnostycznych w EKG

W artykule [Abo-Zahhad M. M i in., 2014] przedstawiono hybrydową technikę kompresji sygnałów EKG opartą na dyskretnej transformacji falkowej (ang. *Discrete Wavelet Transform*, DWT) i wykorzystaniu techniki korelacji między próbkami sygnału. Praca ta zawiera technikę dekompozycji DWT, różnicową modulację kodowo-impulsową (ang. *Differential Pulse Code Modulation*, DPCM) i techniki kodowania przebiegu do kompresji różnych części sygnału, gdzie przyjęto kompresję bezstratną w częściach o znaczeniu klinicznym i zastosowano kompresję stratną w tych częściach, które nie mają znaczenia klinicznego. Zaproponowany algorytm kompresji rozpoczyna się od segmentacji sygnału EKG na jego główne komponenty (fale P, zespoły QRS, załamki T, fale U i odcinki izoelektryczne). Wynikiem są fale pogrupowane w części oznaczone jako: region zainteresowania (ang. *Region of Interest, RoI*) i region bez zainteresowania (ang. *Non Region of Interest, NonRoI*). W związku z tym bezstratny i stratny schemat kompresji są stosowane odpowiednio do części RoI i NonRoI. Idealnie byłoby kompresować sygnał bezstratnie, ale w wielu zastosowaniach nie jest to możliwe. Tak więc, biorąc pod uwagę stały budżet bitowy, warto wydawać więcej bitów, aby reprezentować te części sygnału, które należą do określonego RoI, a zatem zrekonstruować zapis EKG z wyższą dokładnością diagnostyczną, pozwalając w innych częściach na większe zniekształcenia. W tym celu korelacja pomiędzy kolejnymi próbkami części RoI jest wykorzystywana przez zastosowanie metody DPCM. Jednakże w zakresie non RoI sygnał jest kompresowany przy użyciu technik DWT,

progowania i kodowania. Transformacja falkowa stosowana jest do skoncentrowania energii sygnału w niewielkiej liczbie współczynników transformacji. Osiąga się to poprzez wybór takiej bazy dekompozycji w której maksymalna część energii sygnału będzie reprezentowana przez niewielką liczbę funkcji bazowych. Działanie proponowanego algorytmu było przetestowane pod kątem współczynnika kompresji CR i wskaźnika zniekształceń PRD dla kompresji 10 sekundowego odcinka danych wyodrębnionych z rekordów 100 i 117 bazy danych MIT-BIH. Uzyskane wyniki wykazały, że proponowana technika ma wyższy stopień kompresji i niższe wartości współczynnika PRD w porównaniu do innych technik transformacji falkowej. Główne zalety proponowanego podejścia to:

1) wdrażanie różnych schematów kompresji do kompresji różnych części EKGw celu zmniejszenia korelacji między kolejnymi próbkami sygnału; i

2) uzyskanie wysokiego współczynnika kompresji przy akceptowalnej jakości zrekonstruowanego sygnału w porównaniu do ostatnio opublikowanych wyników [Abo-Zahhad M. M i in., 2014].

Algorytm ten [Abo-Zahhad M. M i in., 2014] składa się z następujących czynności:

a) Strona pacjenta

1) Otrzymanie sygnału EKG od pacjenta lub przygotowanie nieskompresowanego sygnału z bazy danych.
2) Jeśli sygnał jest przechwytywany od pacjenta, trzeba oczyścić go z artefaktów, usunąć średnią sygnału i znormalizować go. W przypadku pobrania sygnału z bazy danych należy usunąć jego średnią i znormalizować wynikowy sygnał z usuniętą średnią. Wszystkie rozważane sygnały zostały pobierane z bazy danych MIT-BIH.
3) Podzielenie sygnału na część RoI (zespół QRS i ewentualnie fale P-T i U) i część NonRoI (pozostałe części stanowią różnicę między oryginalnym sygnałem EKG a częścią RoI).
4) Kompresja części RoI, na bazie metody kompresji bezstratnej DPCM i przy zastosowaniu zgrubnej kwantyzacji.
5) Zakodowanie pozostałej reszty sygnału w strumieniu binarnym za pomocą algorytmu RLE (ang. *Run-Lenght Encoding*).
6) Kompresja części NonRoI za pomocą techniki kompresji stratnej DWT i przy zastosowaniu odpowiednio dobranych parametrów progowania i kwantyzacji.
7) Zakodowanie uzyskanych skwantyzowanych współczynników falkowych w strumień binarny za pomocą przebiegu algorytmu kodowania.
8) Spakowanie pakietów danych i przygotowanie nagłówków danych.

b) Strona transmisji

1) Nawiązanie połączenia sieciowego (Intranet lub Internet) i / lub skomunikowanie urządzeń transmisji bezprzewodowej.
2) Transmisja nagłówków danych, binarnego strumienia kolejno części RoI i części NonRoI.

c) Strona recepcji

1) Rozpakowanie z odebranego strumienia binarnego nagłówka oraz strumieni binarnych części RoI i części NonRoI.
2) Konwertowanie binarne strumieni nagłówka na podstawowe informacje ważne dla rekonstrukcji sygnału EKG, takie jak długość strumienia RoI, długość strumienia NonRoI, początek i koniec każdej fali w częściach RoI i NonRoI.
3) Konwertowanie binarnych wartości strumieni obu części RoI i NonRoI na ich równoważne liczby dziesiętne.
4) Zastosowanie odwrotnej DPCM dla części RoI i zastosowanie odwrotnej transformacji falkowej dla części NonRoI.
5) Rozłożenie powstałych w czasie elementów RoI i NonRoI na fale QRS, załamki T, fale P, fale U i odcinki izoelektryczne.
6) Użycie uzyskanych w powyższych krokach danych, aby zrekonstruować sygnał EKG.
7) Obliczenie współczynnika kompresji i pomiar błędów dla oceny i porównania.
8) Wyprowadzenie zrekonstruowanego sygnału EKG do badań medycznych [Abo-Zahhad M. M i in., 2014].

W artykule [Mamaghanian H i in., 2011] autorzy określili ilościowo potencjał metody próbkowania oszczędnego (ang. *Compressed Sensing*, CS) sygnału wobec oczekiwań nisko złożonej energooszczędnej kompresji EKG w najnowocześniejszej technologii Shimmer sieci bezprzewodowej (ang. *Wireless Body Sensor Network* WBSN). Ich wyniki pokazują, że CS stanowi konkurencyjną alternatywę dla najnowocześniejszych rozwiązań do kompresji opartych na transformacjach falkowych (DWT). Bardziej konkretnie, chociaż oczekuje się gorszej wydajności kompresji niż w przypadku metod opartych na DWT dla danej zrekonstruowanej jakości sygnału, jej znacznie mniejsza złożoność i mniejsze obciążenie procesora (ang. *Central Processing Unit*, CPU), pozwala jej ostatecznie przewyższyć kompresję EKG opartą na DWT pod względem ogólnej efektywności energetycznej. W rezultacie metoda kompresji EKG oparta na CS pozwala na wydłużenie czasu autonomicznej pracy o 37,1% w stosunku do jego odpowiednika opartego na DWT w celu uzyskania "dobrej" jakości rekonstrukcji. W tym artykule zaproponowano kompletne porównanie na

poziomie systemu pomiędzy nowymi opartymi na CS i najnowocześniejszymi algorytmami kompresji ECG opartymi na DWT. Zgodnie z oczekiwaniami okazało się, że nieadaptacyjna kompresja oparta na CS wykazuje gorszą wydajność kompresji w porównaniu z jej adaptacyjnym wariantem opartym na DWT dla danej zrekonstruowanej jakości sygnału. Przedstawione wyniki uzyskano jednak za pomocą domyślnego algorytmu śledzącego podstawowy przebieg zapisu EKG i nie podjęto próby wykorzystania wysoce strukturalnej natury tego sygnału. Wyniki potwierdziły przydatność CS do energooszczędnej kompresji EKG w czasie rzeczywistym dla ograniczonych zasobów WBSN. Co ważniejsze, sugerują one przydatność wdrożenia "analogowego CS" do wspólnego pobierania próbek i kompresji EKG w kontekście aplikacji WBSN [Mamaghanian H i in., 2011].

2.4 Kodowanie informacji dodatkowych w sygnale EKG

Telemedycyna rozwinęła się przez ostatnią dekadę na dużą skalę, co pociąga za sobą konieczność dbałości o bezpieczeństwo danych. Dane medyczne wymagają ochrony przed nieuprawnionym dostępem i/lub modyfikacją podczas transmisji i archiwizacji. Różne rodzaje sygnału (EKG, EEG, ...) mające wszystkie unikalne właściwości i formaty danych muszą być oznaczone znakiem wodnym i chronione w bezprzewodowym systemie opieki zdrowotnej [Ibaida A. i in, 2011].

Opatrzenie znakiem wodnym to proces, w którym w transmitowanej informacji ukrywany jest strumień danych (znak wodny). Techniki ukrywania informacji zostały opracowane przede wszystkim w celu ochrony praw autorskich w odniesieniu do danych. Mogą być one również bardzo przydatne do uwierzytelniania sygnału biologicznego. W tych technikach osadzone dane były "niewidoczne" w celu utrzymania jakości sygnału będącego nośnikiem. Obecnie oczekuje się, że w najbliższym czasie systemy opieki zdrowotnej doświadczą drastycznej zmiany struktury i organizacji. Ponieważ ilość danych dotyczących opieki zdrowotnej wzrasta, konieczne jest archiwizowanie przechowywanie informacji medycznych. Jednym z głównych problemów technologicznych i etycznych jest prywatność danych. Ochrona przed nieuprawnionym dostępem do danych np. historii choroby i danych osobowych jest bardzo ważna. Proces oznaczania znakiem wodnym został już z powodzeniem zastosowany w cyfrowych przekazach audio, graficznych lub wideo, z wykorzystaniem różnych metod takich jak transformacja Fouriera, transformacja falkowa i schemat oparty na analizie składowych niezależnych [Ahuja B. S. i in., 2010].

Cyfrowy znak wodny to adaptacja papierowych znaków wodnych do cyfrowych nośników danych. Jego implementacja stosuje różne metody i technologie ukrywania informacji w nośniku cyfrowym. Pożądane jest, aby znaki wodne cechowały się następującymi własnościami [Ahuja B. S. i in., 2010]:

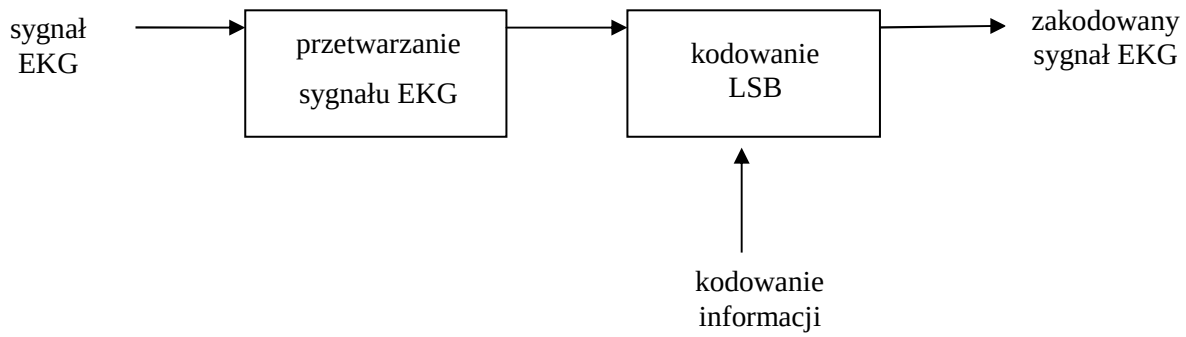
1. Nieprzewidywalność,
2. Czytelność,
3. Niska złożoność,
4. Bezpieczeństwo.

W typowym scenariuszu telemonitoringu bezprzewodowego pacjent nosi czujniki bezprzewodowe zdolne do odczytywania próbek EKG, temperatury, ciśnienia krwi itd. Informacje biomedyczne różnego rodzaju mogą stać się znakiem wodnym w sygnale EKG w urządzeniu pacjenta. W rezultacie są wysyłane bezprzewodowo do centralnego serwera, który sprawdza znak wodny i wyodrębnia meta-informację ukrytą w sygnale. Serwer następnie rozprowadza otrzymane rozpakowane informacje dla tzw. e-lekarzy (np. lekarzy, którzy korzystają z urządzeń przenośnych), którzy mogą szybko podjąć działania zgodnie z ich priorytetem [Ibaida A. i in., 2011]. W tym scenariuszu algorytm znakowania musi zachowywać główne cechy sygnału EKG dla typowego normalnego lub nieprawidłowego EKG. Ponadto musi zagwarantować, że prawidłowa diagnostyczna interpretacja sygnału EKG może odbywać się bezpośrednio bez usuwania znaku wodnego. Znak wodny musi więc być idealnie niewidoczny [Ibaida A. i in., 2011].

W [Ibaida A. i in., 2011] autorzy opisują jedną z metod znakowania wodnego w EKG. Ten algorytm jest połączeniem dwóch z trzech metod używających sygnałów w telemedycynie:

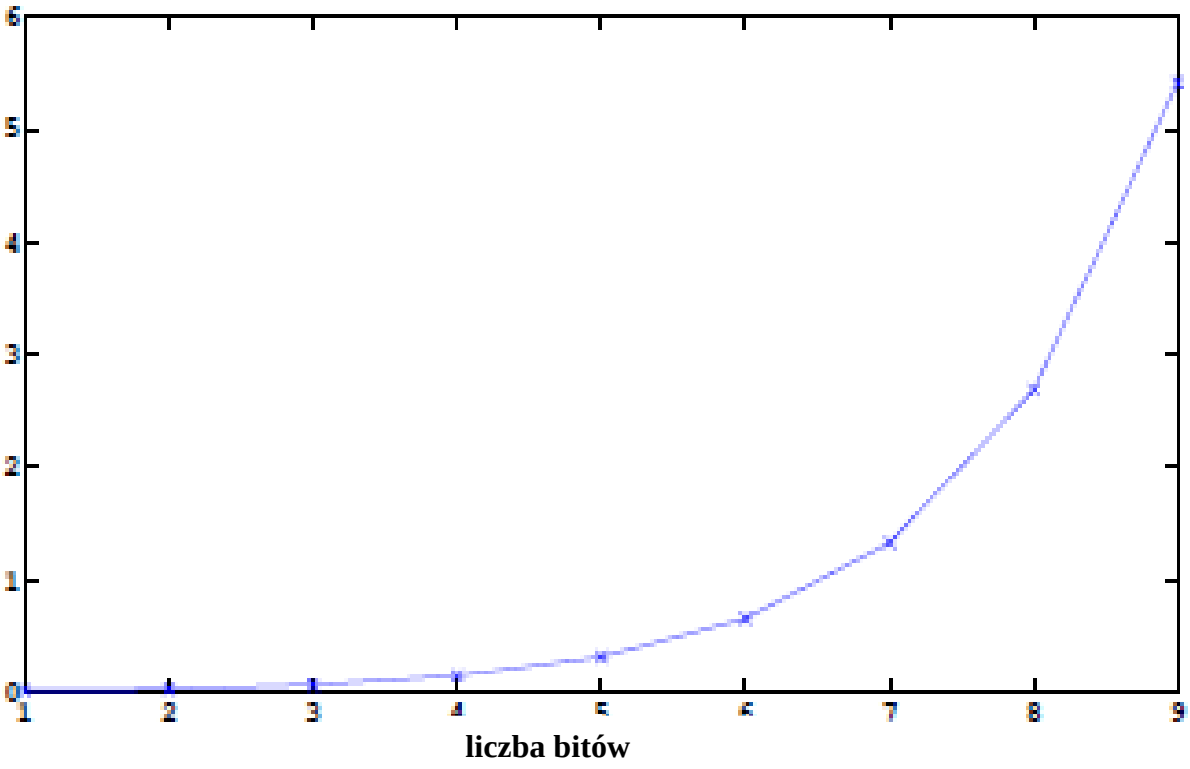
1. Modulacja Indeksu Kwantyzacji (ang. *Quantization Index Modulation*, QIM) Chen B. I Wornell G. W., 2001] Szczegółowy opis metody steganograficznej znajduje się w [SANS Institute],
2. Metoda Kodowania w zakresie Najmniej Znaczącego Bitu (ang. *Least Significant Bit*, LSB)
3. Technika kodowania patchwork [Bender W. i in., 1996]

Ta proponowana metoda znakowania składa się z dwóch etapów, jak pokazano na rysunku 2.5. Pierwszy odpowiada za wstępne przetwarzanie sygnału. Drugi etap to proces znakowania. Ta metoda kodowania sygnału EKG jest opisana w [Ibaida A. i in., 2011].



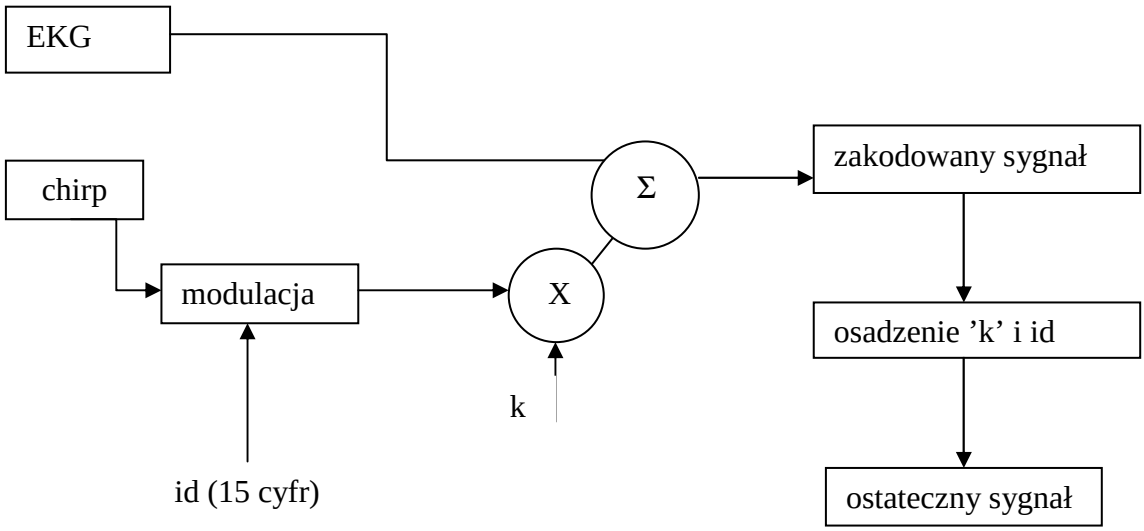
Rys. 2.5.Schemat blokowy proponowanego systemu do osadzania znaku wodnego w sygnale EKG [Ibaida A. i in., 2011]

Porównanie powstałego znaku wodnego z pierwotnym sygnałem odbywa się przy użyciu różnicy średniokwadratowej (ang. *Percent Root-Mean-Square Difference*, PRD), powszechnie używanej jako miara błędu pomiarów EKG. Wynik jest pokazany na rysunku 2.6.

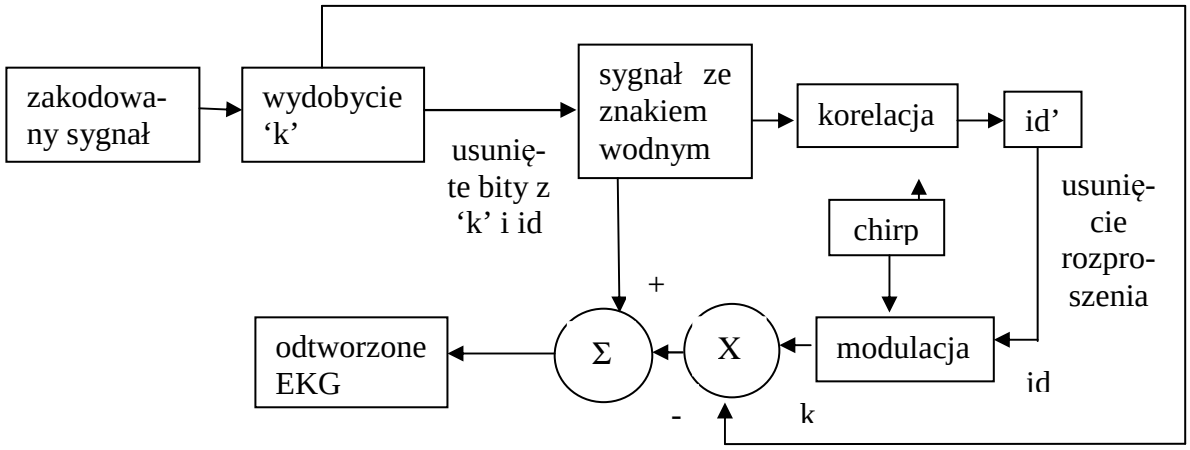


Rys. 2.6. Zależność pomiędzy PRD i ilością bitów [Ibaida A. i in, 2011]

W [Ahuja B. S. i in., 2010] autorzy opisują inną technikę procesu kodowania informacji, przedstawioną na rysunkach 2.7 i 2.8. Jest ona wykorzystywana do znakowania sygnałów biomedycznych, na przykład EKG.



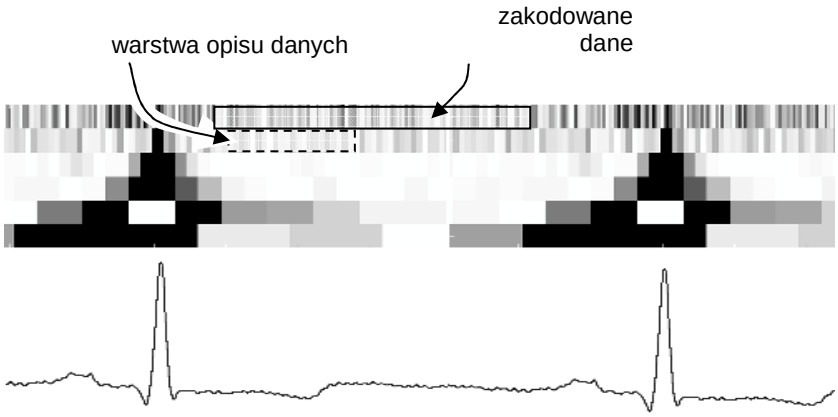
Rys. 2.7. Schemat osadzania znaku wodnego dla sygnału EKG [AhujaB. S. i in., 2010]



Rys. 2.8. Schemat ekstrakcji znaku wodnego z sygnału EKG [Ahuja B. S. i in., 2010]

W pracach [Augustyniak P., 2012] i [Augustyniak P., 2014] autor skupił się zwłaszcza na znakach wodnych w sygnale EKG. Służył on do kodowania informacji o przekształceniu za pomocą dyskretnej transformacji falkowej (DWT), co pokazuje schemat przetwarzania na rysunku 5.1 (w rozdziale 5).. Na podstawie opisu sygnału EKG opisano określone parametry kontenera danych, które przedstawiono na rysunku 5.1 i 5.2 (w rozdziale 5):

- początek względem poprzedniego szczytu R,
- długość i
- maksymalna bitowa głębokość kodowania.



Rys. 2.9. Schemat osadzania danych w luce pasmowej zapisu EKG [Augustyniak P., 2014]

Autor tych publikacji użył klucza do szyfrowania. Składa się on z trzech opisanych poniżej sekcji:

- specyfikacja używanej falki,
- określenie odległości RK,
- unikatowy ciąg klucza.

Autor zwrócił uwagę na trzy cechy zaproponowanej metody:

1. Metoda dostosowuje rozmiar kontenera i głębokości modulacji tak, aby uzyskać najlepsze wyniki w znakowaniu wodnym i najlepiej zamienić informację ukrytą w ciąg o parametrach statystycznych podobnych do parametrów szumu obecnego w pierwotnym sygnale EKG. Można go zmierzyć i zastąpić przez zakodowaną wiadomość. W ten sposób metoda ta jest bardzo ekonomiczna, a wkodowanie informacji - bardzo precyzyjne.
2. Każde uderzenie serca stanowi niezależny kontener danych, lokalizacja kontenerów omija każdy zespół QRS jako szerokopasmowy i potencjalnie najistotniejszy diagnostycznie składnik elektrokardiogramu. Dlatego też ważna jest lokalizacja luki pasmowej w interwale RR. Pod tym pojęciem kryje się miejsce do którego można wkodować dane ukryte bez zniekształcenia istotnych informacji kardiologicznych.
3. Kodowanie ukrytych wiadomości nie powinno mieć wpływu na najbardziej informacyjne sekcje elektrokardiogramu. Oznacza to, że znak wodny nie powinien mieć wpływu na wartość diagnostyczną.

W [Augustyniak P., 2012] i [Augustyniak P., 2014] autor przedstawił dwa potencjalne scenariusze zastosowania metody:

1. do transmisji danych multimodalnych (demograficznych, środowiskowych) za pośrednictwem kanału EKG,

2. w celu ukrycia poufnych danych (np. lokalnie poprawiających jakość zapisu) w standardowym zapisie.

Diagnostyka przyłóżkowa (ang. *Point of Care Testing*, POCT) u pacjentów z chorobą niedokrwienną serca jest stosowana w związku z koniecznością szybkiego dostarczenia, konkretnych i dokładnych wyników niezbędnych dla natychmiastowego rozpoczęcia terapii [Devi A. i Kumar S., 2016]. Diagnostyka przyłóżkowa oparta na rejestracji EKG jest zalecana w celu natychmiastowego i wygodnego przeprowadzenia testu u pacjentów kardiologicznych. Jej stosowanie zwiększa prawdopodobieństwo szybszej wymiany informacji pomiędzy pacjentem, lekarzem i zespołem opieki, co ułatwia natychmiastowe podejmowanie trafnych decyzji dotyczących postępowania terapeutycznego. W bezprzewodowym trybie komunikacji dane biomedyczne mogą być podatne na potencjalne ataki stawiając przed konstruktorami systemów wyzwania związane z bezpieczeństwem:

1) ochrona prywatności i integralności danych biomedycznych,
2) zapewnienie dostępu do informacji wrażliwych dla jedynie autoryzowanych osób.

W artykule [Devi A. i Kumar S., 2016] autorzy proponują pięciopoziomową, falkową dekompozycję zapisu na potrzeby steganografii z użyciem sygnałów EKG, szyfrowaniem RSA i kodowaniem opartym na macierzy szyfrowania. Aby ocenić efektywność proponowanego algorytmu na sygnale EKG pacjenta, dwa parametry opisujące zniekształcenia: takie jak wartość procentowa RMSE (różnica PRD) i PSNR (szczytowy stosunek sygnału do szumu) były badane wraz z wynikami efektywności algorytmu i energią znaku wodnego dla falek Coiflet, Biortogonalnych i Symlet. Stwierdzono, że proponowany algorytm zapewnia bardzo wysoką ochronę dla informacji związanych z pacjentem, a także z mniejszą ilością zniekształceń sygnału EKG, dzięki czemu zachowuje on wartość diagnostyczną po ekstrakcji tajnych informacji związanych z pacjentem (znaku wodnego).

Autor kolejnej publikacji [Engin M. i in., 2005] opisuje, że znak wodny stał się jedną z podstawowych technologii wybieranych do ochrony praw autorskich dla szerokiej gamy aplikacji multimedialnych. Znaki wodne zostały przez niego użyte do osadzenia wcześniej określonych danych w sygnałach biomedycznych, co czyni je odpornymi na niektóre ataki na jakie są narażone w sieciach komputerowych. W pracy [Engin M. i in., 2005] przedstawiono dyskretną technikę znaków wodnych wykorzystującą transformację falkową. Została ona zastosowana do weryfikacji integralności sygnału w elektrokardiogramie w celu monitorowania stosowania chorób sercowo-naczyniowych. Proponowana technika jest oceniana w różnych warunkach zaszumienia sygnału dla różnych funkcji falkowych. Autor

ocenia różne falki macierzyste i konkluduje, że technika bazująca na funkcjach falkowych db2 działa lepiej niż wariant oparty na funkcji falkowej bior5.5 [Engin M. i in., 2005].

Podobnie kolejna publikacja [Ibaida A. i Khalil I., 2013] tematycznie związana jest z kodowaniem informacji dodatkowych w EKG. Autorzy uważają, iż wraz zestarzeniem się populacji i znaczną liczbą osób cierpiących na choroby serca, można sobie wyobrazić, że zdalne systemy monitorowania pacjenta do EKG będą szeroko stosowane jako aplikacje do punktów opieki (ang. *Point of Care*, PoC) w szpitalach na całym świecie. Dlatego też ogromna ilość zapisów EKG zebranych przez sieci czujników od odległych pacjentów w domach będzie transmitowana wraz z innymi odczytami fizjologicznymi, takimi jak ciśnienie krwi, temperatura, poziom glukozy itp. i diagnozowana przez zdalne systemy monitorowania pacjenta. Niezwykle ważne jest, aby poufność danych pacjentów była chroniona podczas przesyłania danych przez sieć publiczną, a także kiedy są one przechowywane w serwerach szpitalnych używanych przez systemy zdalnego monitorowania. W artykule [Ibaida A. i Khalil I., 2013] wprowadzono technikę steganografii opartą na falkach, która łączy technikę ukrywania i szyfrowania w celu ochrony poufnych danych pacjentów. Proponowana metoda pozwala ukryć odpowiednie dane poufne pacjenta i inne informacje fizjologiczne w sygnale EKG, gwarantując w ten sposób integrację między EKG a pozostałymi danymi. Aby ocenić skuteczność proponowanej techniki na sygnale EKG, zastosowano dwie miary zniekształceń: procentową różnicę średniokwadratową – PRD w wariancie standardowym i ważoną w dziedzinie reprezentacji falkowej. Stwierdzono, że proponowana technika zapewnia wysoki poziom ochrony danych pacjentów przy niskim (mniej niż 1%) zniekształceniu, a dane EKG pozostają rozpoznawalne zarówno po zakodowaniu znakiem wodnym (tj. ukrywają poufne dane pacjenta), jak i po usunięciu znaków wodnych [Ibaida A. i Khalil I., 2013].

W pracy [Jero S. E. i Ramu P. , 2016] autorzy stwierdzają, że sygnały biomedyczne przesyłane przez Internet są zwykle oznaczone informacjami o pacjencie. Techniki ukrywania danych, takie jak steganografia, zapewniają bezpieczeństwo takich danych poprzez ukrywanie danych w sygnałach. Jednak ukrywanie danych skutkuje pogorszeniem sygnału, które może wpływać na diagnostykę. Przedstawiono nowatorską technikę, która wykorzystuje transformaty typu curvelet do ukrywania informacji o pacjencie w ich sygnale EKG. Transformacja Curvelet rozkłada sygnał EKG na podpasma częstotliwości. Metoda kwantowania jest stosowana do osadzania danych pacjenta we współczynnikach, których wartości są w pobliżu zera w podpaśmie wysokiej częstotliwości. Metryki wydajności zapewniają miarę niedostrzegalności proponowanego podejścia. Bitowy współczynnik błędu w transmisji cyfrowej (ang. *Bit Error Rate*, BER) służy do pomiaru zdolności do

wyodrębniania danych pacjenta. Proponowane w [Jero S. E. i Ramu P., 2016] podejście przetestowano na bazie danych MIT-BIH, a obserwacje potwierdzają, że jego skuteczność jest lepsza w porównaniu z metodą losowego wyboru współczynników. Chociaż wydajność proponowanego podejścia maleje wraz ze wzrostem rozmiaru strumienia informacji o pacjencie, szczytowe wartości stosunku sygnału do szumu związanego z informacją ukrytą są wysokie. Dlatego proponowane podejście można wykorzystać do bezpiecznego przesyłania danych pacjenta [Jero S. E. I Ramu P. , 2016].

W [Sankari V. i Nandhini K., 2014] autorzy również bazują na wkodowaniu danych dodatkowych przesyłanych bezprzewodowo. Opisują, iż odsetek osób starzejących się w populacji znacznie rośnie. Zgodnie z Ustawą o Przenoszalności Ubezpieczeń Zdrowotnych i Odpowiedzialności (HIPAA) prywatność i bezpieczeństwo danych pacjenta są ważne w służbie zdrowia. Przepisy bezpieczeństwa są wdrożone w celu zapewnienia integralności danych, poufności i dostępności. W związku z tym sygnał EKG pacjenta i inne odczyty fizjologiczne, takie jak temperatura, ciśnienie krwi, odczyt glukozy, pozycja itp., są gromadzone w domach przy użyciu sieci czujników umieszczonych na powierzchni ciała (ang. *Body Sensor Network*, BSN), a następnie przesyłane i diagnozowane przez zdalne systemy monitorowania pacjenta. Przy tym samym koszcie poufność pacjenta jest chroniona przed intruzami, podczas gdy dane są transmitowane przez otwartą sieć i są przechowywane na serwerach szpitalnych. W projekcie [Sankari V. i Nandhini K., 2014], w celu realizacji aktu HIPAA, zaproponowano technikę steganografii opartej na transformacji falkowej. Technika DWT pozwala ukryć dane poufne pacjenta w sygnale EKG, a tym samym zapewnia pacjentowi prywatność i poufność. Ponadto w projekcie uwzględniono następujące założenia: (1) szyfrowanie i deszyfrowanie poufności i integralności danych (2) trzystopniowe bezpieczeństwo danych (3) użycie steganografiiopartej na EKG do wymiany danych. Metoda zapewnia pacjentowi wysoki poziom prywatności i jednoczesne zapis stegano EKG zachowuje własności diagnostyczne. System [Sankari V. i Nandhini K., 2014] zapewnia również bezpieczeństwo, skalowalność i wydajność.

Kolejną publikacją dotyczącą kodowania informacji dodatkowych w EKG jest praca [Stanković S., 2010]. Przedstawiono w niej przegląd metod analizy czasowo-częstotliwościowej oraz niektóre aspekty ich zastosowań w oznaczaniu sygnałów cyfrowym znakiem wodnym. Omówiono główne zalety i wady różnych rozkładów czasowo-częstotliwościowych. Celem tego teoretycznego przeglądu jest ułatwienie odpowiedniego wyboru rodzaju dekompozycji w konkretnej aplikacji. Następnie przedstawiono różne aspekty analizy czasowo-częstotliwościowej w zastosowaniu do nanoszenia cyfrowego znaku

wodnego. W szczególności szczegółowo omówiono sposób odwzorowywania charakterystyki czasowo-częstotliwościowej sygnału nośnika na sekwencję znaku wodnego o charakterystyce zbliżonej do charakterystyki szumu. To podejście jest prezentowane w wielowymiarowej formie, a następnie stosowane do cyfrowego dźwięku, obrazu cyfrowego i cyfrowego znaku wodnego wideo. Na koniec rozważania teoretyczne są zilustrowane różnymi przykładami liczbowymi dotyczącymi rzeczywistych sygnałów [Stanković S., 2010].

W pracy [Wang H. i in., 2016] autorzy stwierdzają, że obecnie telekardiologia cieszy się dużą popularnością ze względu na to, że coraz więcej osób na świecie cierpi na choroby serca. Dlatego ogromna liczba zapisów EKG, jak również informacje poufne pacjenta są obecnie i będą coraz częściej przesyłane przez Internet. Technika ukrywania danych oparta na technologii falkowej zaproponowanej przez Ibaida ma na celu ochronę poufnych danych pacjentów przy użyciu sygnału EKG jako nośnika. Niestety, nie pozwala ona całkowicie zrekonstruować oryginalnego sygnału EKG. Każda zmiana zapisu EKG może prowadzić do niedokładnego wniosku diagnostycznego postawionego przez lekarza, w zakresie, który nie może być zaakceptowany przez pacjentów. Postulat będący podstawą przedstawionych prac zakładał, aby zarówno informacje o pacjencie, jak i sygnał EKG były przywrócone idealnie, to znaczy na poziomie identyczności bitowej z oryginałem. Najpierw zaproponowano metodę osadzania poufnych danych pacjenta w sygnale EKG, zachowując przy tym jego wysoką jakość wizualną. Następnie autorzy stosują ujednoliconą metodę osadzania-szyfrowania w celu zagwarantowania bezpieczeństwa prywatności pacjenta, jak również samego sygnału EKG. Po dodaniu znaku wodnego struktura sygnału stego EKG została poważnie zmieniona, ale usunięcie znaku wodnego umożliwia dokładne odtworzenie oryginalnego zapisu. Oba eksperymentalne wyniki pokazują, że proponowane przez [Wang H. i in., 2016] metody są odwracalne. Ponadto drugi z zaproponowanych systemów może osiągnąć wysoką efektywność kodowania informacji [Wang H. i in., 2016].

Analiza dostępnych publikacji prowadzi do wniosku, że z rozwojem telemedycyny musi iść w parze bezpieczeństwo transmitowanych danych. W artykule [Wu W. i in., 2015]zaproponowano odwracalny schemat ukrywania danych dla ochrony prywatności pacjentów. W celu zapewnienia odwracalności zastosowano całkowitoliczbową transformację falkową Haara do utworzenia czasowo-częstotliwościowej reprezentacji EKG. Schemat przesuwania histogramu i progowania jest starannie zaprojektowany, aby adaptacyjnie osadzić informacje ukryte zgodnie z lokalną pojemnością nośnika i odzyskać zarówno informację ukrytą, jak i sygnał EKG bez żadnych zniekształceń, czyli w postaci bitowo identycznej z oryginałem [Wu W. i in., 2015].

3. Materiały i narzędzia

3.1 Narzędzia matematyczne

Korelacja (współzależność cech) określa wzajemne powiązania pomiędzy wybranymi zmiennymi. Charakteryzując korelację dwóch cech podawane są dwa czynniki: kierunek (korelacja dodatnia i ujemna jest opisana poniżej) oraz siłę, którą mierzy się od 0 do 1,0, gdzie 0 oznacza brak zależności a 1 praktycznie pełną zależność [Starzyńska W., 2000], [Statystyka_wykład_korelacja].

Korelacja pozwala na porównanie sygnału z przebiegiem odniesienia (wzorcem). Redukuje wpływ składowych losowych oraz pomaga wykryć składowe sygnału podobne do wzorca [Podstawy teorii sygnałów-splot i korelacja].

Ze względu na sposób analizy oraz charakter analizowanych zmiennych można wyróżnić:

- korelację prostą– badającą związek zachodzący pomiędzy dwoma cechami lub zjawiskami (r_{xy}, r_{12}),
- korelację cząstkową– informującą o związku dwóch cech z wyłączeniem trzeciej zmiennej ($r_{xy.z}$, $r_{12.H}$),
- korelację wieloraką– informującą o związku jednej cechy z kilkoma ujętymi łącznie ($r_{x.yz}$, $r_{1.2H}$) [Sobczyk M., 1991], [Statystyka_wykład_korelacja].

Wyrazem liczbowym korelacji jest współczynnik korelacji (r lub R), zawierający się w przedziale [-1; 1]. Istnieją dwa rodzaje korelacji:

- korelacja dodatnia (wartość współczynnika korelacji od 0 do 1) – informuje, że wzrostowi wartości jednej cechy towarzyszy wzrost średnich wartości drugiej cechy,
- korelacja ujemna (wartość współczynnika korelacji od -1 do 0) - informuje, że wzrostowi wartości jednej cechy towarzyszy spadek średnich wartości drugiej cechy[Starzyńska W., 2000], [Statystyka_wykład_korelacja]

Można również wziąć pod uwagę siłę związków korelacyjnych:

- poniżej 0,2-korelacja słaba (praktycznie brak związku),
- 0,2 – 0,4-korelacja niska (zależność wyraźna),
- 0,4 – 0,6-korelacja umiarkowana (zależność istotna),
- 0,6 – 0,8-korelacja wysoka (zależność znaczna),
- 0,8 – 0,9-korelacja bardzo wysoka (zależność bardzo duża),
- 0,9 – 1,0-zależność praktycznie pełna [Statystyka_wykład_korelacja].

Współczynnik korelacji Pearsona wykorzystywany jest do badania związków liniowych badanych zmiennych, w których zwiększenie wartości jednej z cech powoduje proporcjonalne zmiany średnich wartości drugiej cechy (wzrost lub spadek).
Współczynnik ten obliczamy na podstawie wzoru:

$$r_{xy} = \frac{cov(x,y)}{Sd_x \cdot Sd_y}, \qquad (3.1)$$

gdzie

$$cov(x,y) = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{n}, \qquad (3.2)$$

$$Sd_x = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x}_x)^2}{n}}, \qquad (3.3)$$

$$Sd_y = \sqrt{\frac{\sum_{i=1}^{n}(y_i - \bar{y}_y)^2}{n}}, \qquad (3.4)$$

gdzie Sd_x i Sd_y to odchylenia standardowe odpowiednio zmiennej X i Y [Starzyńska W., 2000], [Statystyka_wykład_korelacja].

Do wykonania eksperymentu opisanego w tej pracy zastosowano dyskretną tranformację falkową (ang. *Discrete Wavelet Transform*, DWT). Jej opis wymaga wprowadzenia pojęcia falek, które to według słownika języka polskiego [Słownik języka polskiego-falki] są rodziną funkcji i każda z nich wyprowadzana jest z funkcji macierzystej za pomocą przesunięcia i skalowania. Falki mają zastosowanie w analizie i przetwarzaniu sygnałów cyfrowych [Słownik języka polskiego-falki]. Falki stosuje się przy analizie reprezentowanych przez sygnały procesach przejściowych [Białasiewicz J. T., 2000].

Falką nazywamy funkcję $\Psi(t) \in L^2(R)$ taką, że układ:

$$\Psi_{j,k} = 2^{j/2}\Psi(2^j t - k) \qquad (3.5)$$

gdzie: j i k to dowolne liczby całkowite a Ψ to funkcja matka i $\Psi_{j,k}$ to falka o skali j i przesunięciu k, jest bazą ortonormalną w przestrzeni Hilberta $L_2(\mathbb{R})$ [Wojtaszczyk P., 2000].

Transformacja falkowa jest przekształceniem, które opiera się na wykorzystaniu operacji iloczynu skalarnego badanego sygnału *s(t)* i pozostałej części zwanej „jądrem przekształcenia” [Transformacja Falkowa_Wikipedia].

Transformacja falkowa dla sygnałów analogowych (ciągłych) jest przekształceniem całkowym:

$$\tilde{s}_{\Psi}(a,b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} s(t) \Psi(\frac{\mathrm{t-b}}{\mathrm{a}})\, dt \quad (3.6)$$

gdzie:
a– parametr skali (przesunięcie w dziedzinie częstotliwości),

b– parametr przesunięcia w dziedzinie czasu *t*,

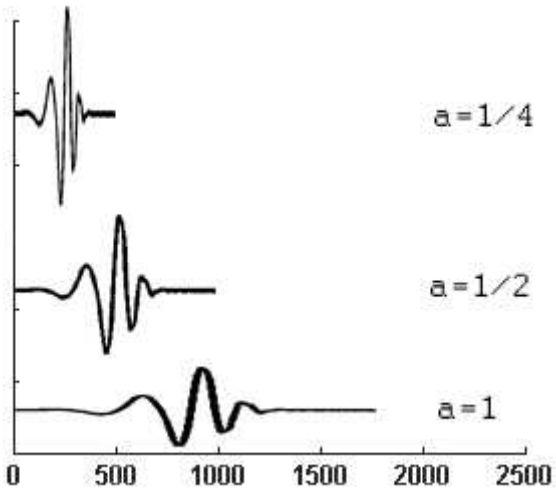
$s(t)$– analizowany sygnał,

$\Psi\left(\frac{\mathrm{t-b}}{\mathrm{a}}\right)$– jądro transformacji falkowej

$\tilde{s}_{\Psi}(a,b)$– transformata Falkowa [Transformacja Falkowa_Wikipedia.

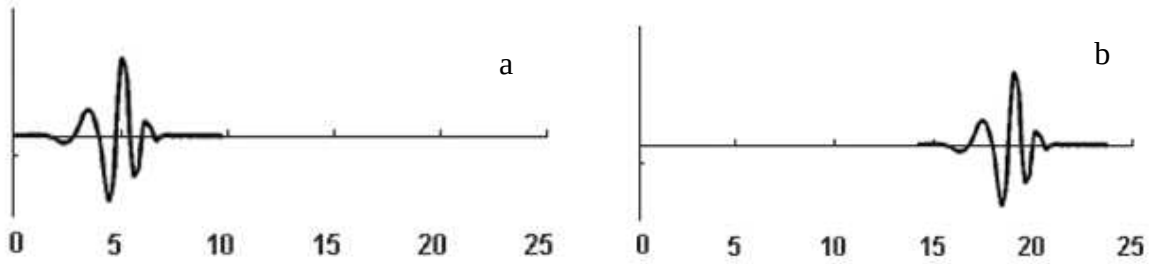
Analogiczny wzór można znaleźć w [Augustyniak P., 2003].

Parametr skali decyduje o zakresie częstotliwości jaką reprezentuje falka. Jego wartości są większe od zera i odwrotnie proporcjonalne do częstotliwości falki. Współczynnik $(\frac{1}{\sqrt{a}})$ występuje przed całką i służy do normalizacji energii falek wszystkich skal. Przedstawia to rysunek 3.1. [Transformacja Falkowa_Wikipedia].



Rys. 3.1.Wpływ współczynnika skali *a* na skalowanie falki w czasie i amplitudzie [Transformacja Falkowa_Wikipedia]

Parametr *b* odpowiada za przesunięcie falki wzdłuż osi czasu, a jego wpływ jest przedstawiony na rysunkach 3.2 [Transformacja Falkowa_Wikipedia]



Rys. 3.2. Opis parametru b: a) pierwotne położenie falki i b) przesunięcie falki o parametr *b* [Transformacja Falkowa_Wikipedia]

Transformacja falkowa ma charakter odwracalny o ile zastosowana baza dekompozycji spełnia warunek ortonormalności. W takim przypadku sygnał oryginalny można uzyskać na podstawie współczynników jego reprezentacji czasowo-skalowej według wzoru:

$$s(t) = \frac{2}{C_y} \int_0^{+\infty} [\int_{-\infty}^{+\infty} CWT(\Gamma, a)\, g\left(\frac{t-\Gamma}{a}\right) d\Gamma] \frac{da}{a^2}, \quad (3.7)$$

gdzie:

$C_y = \int_{-\infty}^{+\infty} \frac{|\Gamma(f)|^2}{|f|} df < \infty \Gamma(0) = 0$ [Heksel K., 2001].

Są różne rodzaje falek. Oto najpopularniejsze z nich:

-Haara - rysunek 3.3 a),

- symlets - rysunek 3.3 b),

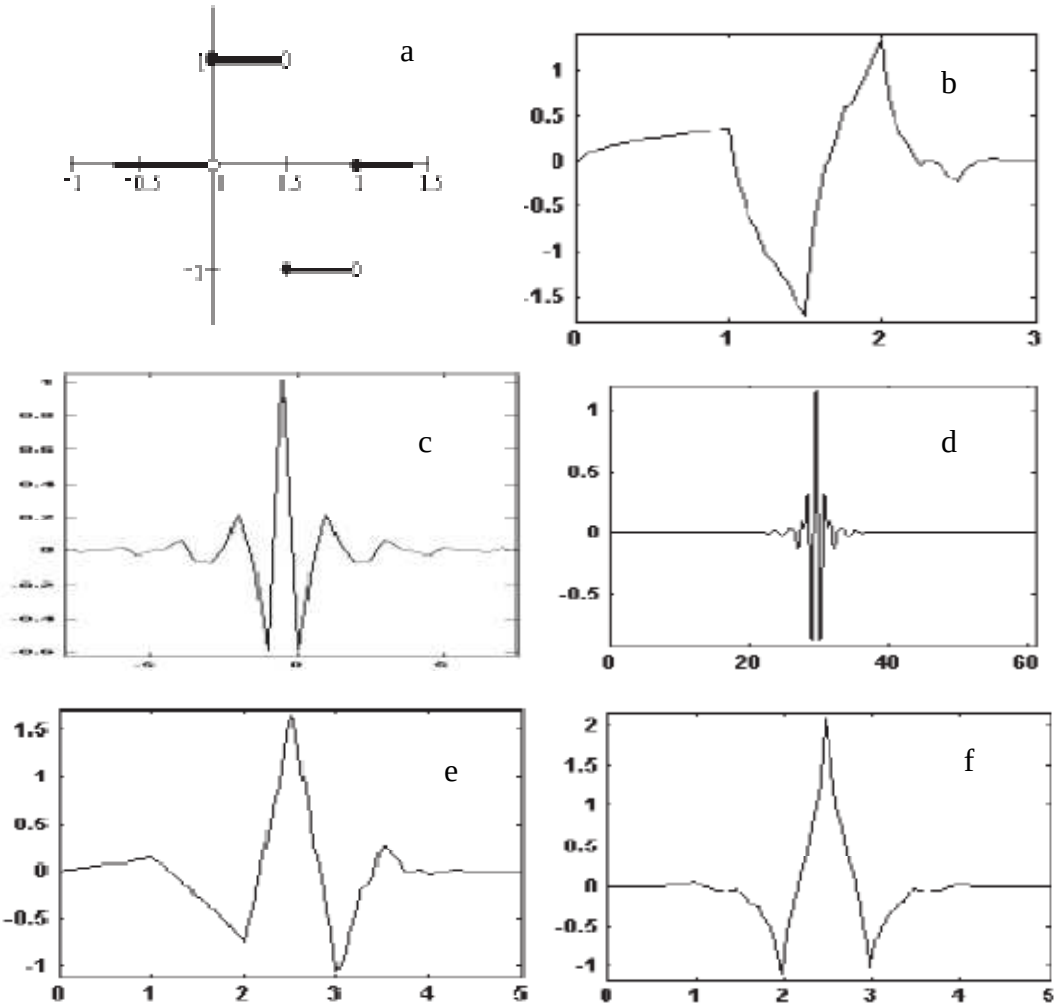
- Meyera - rysunek 3.3 c),

- dyskretna Meyera - rysunek 3.3 d),

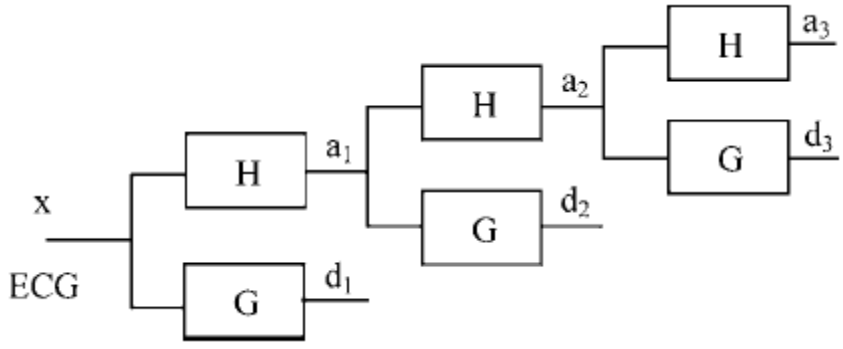
- Daubechies – rysunek 3.3 e),

- Coiflets - rysunek 3.3 f) [Józefczyk I., 2005].

Rysunek 3.4 opisuje stopnie dekompozycji piramidowej podczas dyskretnej transformacji falkowej [Engin M. i in., 2005], gdzie sygnał *x* dekomponowany jest na składowe *a*1 (aproksymacji) i *d*1 (detali) skali pierwszej, a następnie aproksymacja *a*1 jest dekomponowana na składowe *a*2 i *d*2 itd. na kolejnych stopniach dekompozycji.



Rys. 3.3. Różne przykłady falki-matki a) falka Haara, b) falka symlet, c) falka Meyera d) falka dyskretna Meyera, e) falka Daubechies, f) falka Coiflets [Józefczyk I., 2005]



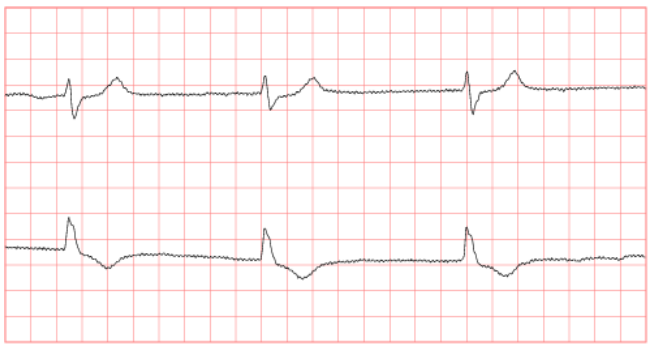
Rys. 3.4. Dyskretna Transformacja Falkowa dekompozycja sygnału EKG [Engin M. i in., 2005]

3.2 Repozytoria fizjologicznych sygnałów referencyjnych EKG

Zainteresowanie komputerowym przetwarzaniem elektrokardiogramów (EKG) w ciągu ostatnich 15 lat gwałtownie wzrosło. Wciąż jednak nie ma standardów komputerowej

interpretacji EKG. Różne techniki są stosowane nie tylko do pomiaru i interpretacji, ale również do przesyłania i przechowywania danych. Aby wypełnić te luki, w 1980 r. rozpoczęto duży międzynarodowy projekt sponsorowany przez Komisję Europejską, którego celem było opracowanie wspólnych standardów w zakresie ilościowej elektrokardiografii (ang. *Common Standards for Quantitative Electrocardiography*, CSE). Głównym celem pierwszego badania CSE było zmniejszenie rozbieżności w pomiarach długości załamków EKG uzyskiwanych w programach komputerowych do interpretacji zapisów. Drugie badanie rozpoczęto w 1985 roku i miało na celu ocenę i poprawę programów interpretacji EKG w zakresie klasyfikacji diagnostycznej. W tym celu opracowano biblioteki dobrze udokumentowanych zapisów EKG i opracowano kompleksowe programy oceny wizualnej i komputerowej analizy EKG. Zadanie to wykonała rada kardiologów w procesie przeglądu Delphi oraz 9 programów VCG i 10 standardowych programów 12-odprowadzeniowych opracowanych przez uniwersyteckie grupy badawcze i przemysł. Trzecie działanie rozpoczęto w czerwcu 1989 r. w celu zharmonizowania pozyskiwania, kodowania, wymiany i przechowywania cyfrowych danych EKG. Tak wykonana akcja stała się międzynarodowo uznanymi kamieniami milowymi dla standaryzacji ilościowej elektrokardiografii [Willems J. L. i in., 1990].

PhysioBank to duże i wciąż rosnące archiwum danych fizjologicznych. Znajdują się tu bazy danych takiejak MIT-BIH. Baza MIT-BIH jest efektem wspólnego działania Massachussetts Institute of Technology oraz Beth Israel Hospital zmierzającego do utworzenia repozytorium do badania oprogramowania do interpretacji długoczasowych (holterowskich) zapisów EKG. W swej podstawowej wersji baza MIT-BIH Arrhythmia Database składa się z 44 zapisów dwuodprowadzeniowych o czasie trwania ok. 30 min każdy, reprezentujących rozmaite patologie. Rys 3.5 przedstawia przykładowy sygnał z bazy MIT-BIH.



Rys. 3.5. Przykładowy rysunek z bazy danych testów kompresji sygnałów EKG [Baza MIT-BIH]

3.3 Przemysłowy standard jakości diagnostyki

W tym rozdziale zostanie opisana norma IEC 60601-2-51, z której korzystała Autorka podczas weryfikacji jakości steganografii opartej na EKG. Normy IEC zostały wprowadzone dla zapewnienia bezpieczeństwa pacjenta i lekarza poprzez standaryzację podstawowych parametrów technicznych elektrokardiografów jedno- i wielokanałowych z interpretacją lub bez.

Sto dziesięciosekundowych sygnałów MA1 do MA 125 (tabela 3.1) będących powieleniem wycinka pojedynczej ewolucji serca z zapisów rzeczywistych MO1 do MO125 pochodzących z bazy CSE wymienionych w Tabeli 1 jest rekomendowanych do użycia w testach dokładności wyznaczania granic załamków i długości interwałów: załamka P, interwału PQ, zespołu QRS i interwału QT. Wartości (numery próbek będących granicami interwałów) wyznaczone dla każdego rekordu przez 12 programów 12-odprowadzeniowych, 8 programów wektokardiograficznych oraz dwóch losowo wybranych ekspertów są zgromadzone narastająco w rekordzie towarzyszącym bazie, co umożliwia wyznaczenie wartości średniej, średniego rozrzutu rezultatów i ustalenie rankingu wartości programów referencyjnych i wartości wyznaczonej przez testowany program. Aby oprogramowanie mogło zyskać nazwę 'oprogramowania do interpretacji EKG' lub urządzenie, którego jest częścią - nazwę 'elektrokardiografu z interpretacją' niedokładności średnie dla 96% spośród 100 plików testowych nie mogą przekroczyć wartości progowych. Dopuszczalne odchyłki zaprezentowano w tabeli 3.2 [Norma IEC].

W dołączonych dokumentach producent urządzenia lub oprogramowania do interpretacji EKG powinien ujawnić, w jaki sposób traktowane są odcinki izoelektryczne wewnątrz zespołu QRS: czy są one włączane czy wyłączane z długości poszczególnych załamków Q, R i S. Powinien on także ujawnić czy części izoelektryczne (I-wave) po globalnym rozpoczęciu zespołu QRS (QRS-ONSET) oraz poprzedzające globalne zakończenie zespołu QRS(QRS-OFFSET) (fala K) są uwzględniane w czasie trwania najbliższego załamka. Jeżeli pomiary są przewidziane dla zapisu EKG, ich dokładność jest testowana [Norma IEC].

Tabela 3.1.Zestaw 100 plików z bazy CSE rekomendowanych przez IEC [Norma IEC] do testowania dokładności pomiaru i rozpoznawania załamków w zapisach biologicznych.

Oznaczenie EKG z bazy pomiarowej CSE serii MA1_ lub MO1_				
1	26	47	74	98
2	27	48	75	99
3	28	49	76	101
4	29	51	77	102
5	30	53	78	103
7	31	55	79	104
8	32	58	80	105
9	33	59	81	106
11	34	60	82	107
12	35	61	83	108
13	36	62	84	110
14	37	63	85	112
15	38	64	86	113
16	39	65	87	114
17	40	66	88	115
19	41	68	90	116
21	42	69	91	118
22	43	71	95	123
24	44	72	96	124
25	46	73	97	125

Tabela 3.2 Dopuszczalne średnie różnice i odchylenia standardowe dla globalnych czasów trwania załamków i odstępów dla zapisów biologicznych [norma IEC].

Pomiar globalny	**Dopuszczalna średnia różnica**	**Dopuszczalne odchylenie standardowe**
Załamek P	±10	15
Interwał PQ	±10	10
Zespół QRS	±10	10
Interwał QT	±25	30

4. Falkowy schemat steganografii w EKG

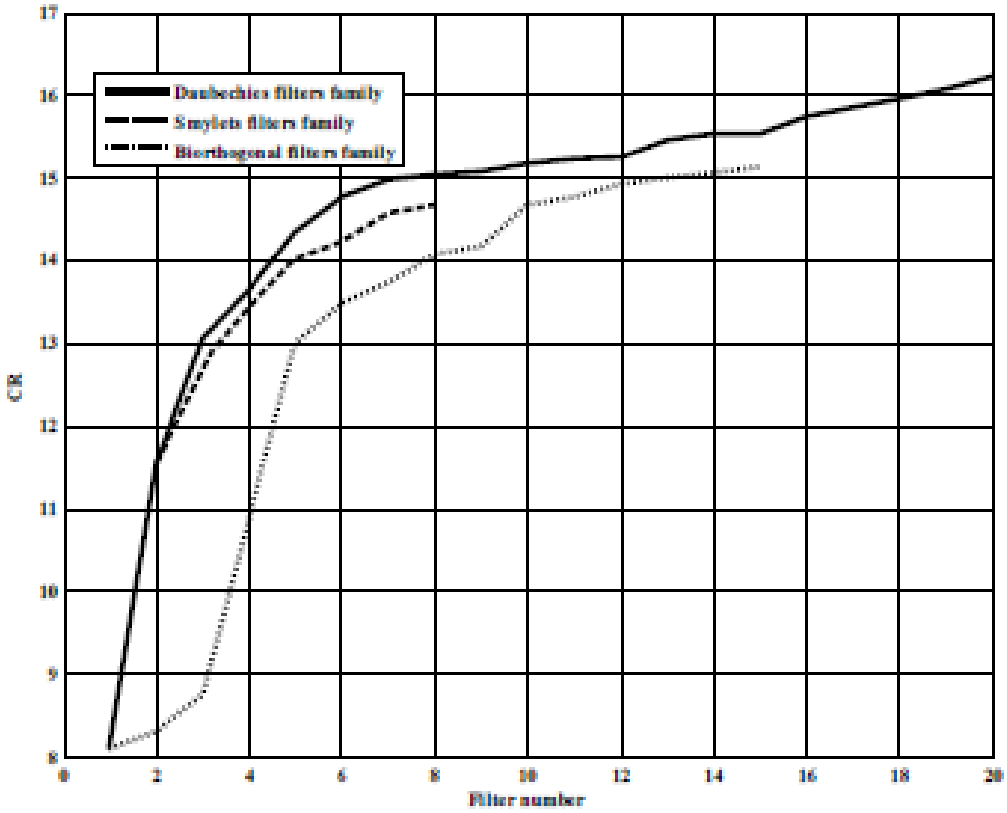
4.1 Wybór dziedziny czasowo-częstotliwościowej

„Tradycyjna analiza widmowa Fouriera jako superpozycja funkcji sinus i cosinus jest niemal wszechobecna w dziedzinie identyfikacji i analizy sygnałów pomiarowych. Użyteczność transformaty Fouriera zawiera się w jej zdolności do analizy przebiegu czasowego sygnału pod kątem jego „zawartości częstotliwościowej". Należy podkreślić, że tradycyjna analiza częstotliwościowa nie nadaje się do obserwacji właściwości sygnałów niestacjonarnych. Wymagana jest tutaj analiza wykorzystująca łączne czasowo-częstotliwościowe (t/f) reprezentacje sygnałów (ang. *Joint Time-Frequency Analysis*, JTFA). Tego rodzaju analizę zapewnia krótkoczasowa transformata Fouriera, czy też transformata Gabora" [Rak R. J. i Majkowski A., 2004].

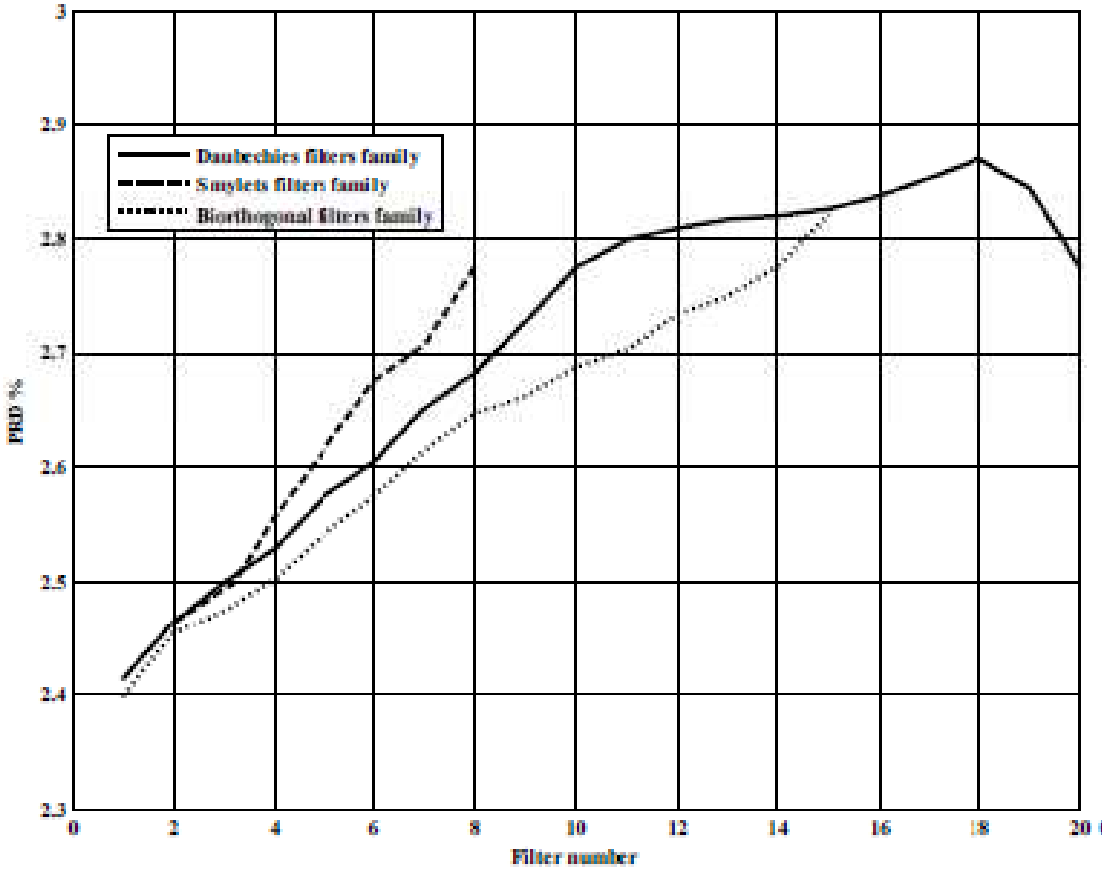
„Rodzajem analizy czasowo-częstotliwościowej jest również transformacja falkowa. Najbardziej charakterystyczne dla transformaty falkowej jest to, że indywidualne funkcje falkowe są dobrze zlokalizowane w czasie (lub przestrzeni – dla obrazów) i jednocześnie dobrze opisują sygnał w dziedzinie częstotliwości, ściśle biorąc tzw. skali. Ponadto w odróżnieniu od funkcji sinus i cosinus, które definiują unikalną transformatę Fouriera, nie ma pojedynczego, unikalnego zbioru falkowych funkcji bazowych. Falki różnią się między sobą zwartością lokalizacji czasowej oraz płynnością i gładkością kształtów. Wynikająca stąd zdolność falek do opisu sygnałów „z nieciągłościami", przy ograniczonej liczbie współczynników oraz z lokalizacją w czasie, stanowi o jej przewadze nad transformatą Fouriera" [Laboratorium wirtualne-Analiza czasowo-częstotliwościowa sygnałów].

Rzeczywiste sygnały rzadko mogą być przedstawione przy pomocy jednego współczynnika dekompozycji reprezentującego całą wartość jego energii, podobnie jak nieliczne sygnały mogą być przedstawione przy pomocy pojedynczego prążka widma. Do przedstawienia sygnału potrzeba zwykle kilku – kilkudziesięciu współczynników o znacznych wartościach. Ich liczba, a także postać dekompozycji w dziedzinie czas-częstość zależy od kształtu (przebiegu) falki-matki. W przeważającej liczbie zastosowań istotna jest koncentracja jak największej części energii sygnału w jak najmniejszej liczbie współczynników dekompozycji. Można ją osiągnąć przez właściwy dobór kształtu falki-matki w dziedzinie czasu (poprzez badanie korelacji z sygnałem – im większa tym lepiej) lub w dziedzinie dekompozycji (poprzez badanie spadku entropii – im szybszy tym lepiej). Rysunki 4.1 i 4.2 pokazują efektywność kompresji sygnału EKG i przyrost poziomu zniekształceń dla falek różnych rzędów (oś pozioma) rodzin Daubechies, Symlets i Biortogonalnych. Ich analiza

prowadzi do wniosku, że efektywność kompresji (najwyższy współczynnik CR przy najniższych zniekształceniach PRD) jest największa dla falek Daubechies.



Rys. 4.1. Zależność współczynnika kompresji (ang. C*ompression Ratio*, CR) od zastosowanego filtru falki [Abo-Zahhad M. M i in., 2014]



Rys. 4.2.Zależność współczynnika zniekształceń (ang. *Percent Residual Difference*, PRD) od zastosowanego filtru falki [Abo-Zahhad M. M i in., 2014]

4.2 Badanie właściwości czasowo-częstotliwościowej EKG

Większość parametrów diagnostycznych sygnału EKG jest w postaci czasu, dlatego dla utrzymania ich wysokiej jakości ważne jest dokładne wyznaczenie granic załamków. Przeprowadzono zatem badania mające na celu wyznaczenie spodziewanej wartości i odchyleń standardowych współczynników reprezentacji czasowo-skalowej elektrokardiogramu. Poszukiwane cechy tej reprezentacji zostały odniesione do zawartości diagnostycznej elektrokardiogramu, a ściśle do położenia załamków reprezentujących poszczególne fazy cyklu serca.

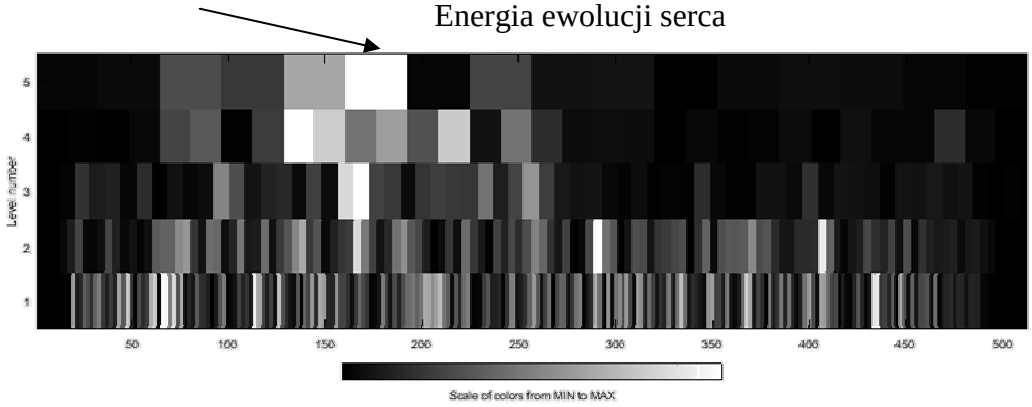
W pierwszym etapie spośród 100 zapisów referencyjnych CSE wyznaczono 29 o najbardziej zbliżonym czasie ewolucji. Czas ten wynosił od 469 do 501 próbek, czyli 938-1002 ms. Numery wybranych plików i odpowiadający im czas pojedynczej ewolucji są przedstawione w tabeli 4.1.

Tabela 4.1. Długość ewolucji i numery wybranych próbek referencyjnych poddanych uśrednieniu.

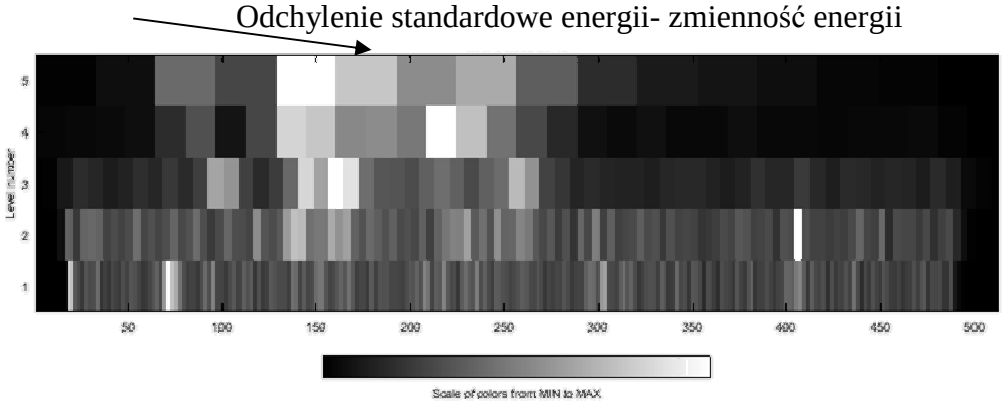
l.p.	**numer zapisu CSE**	**długość ewolucji [próbek]** (częstość próbkowania 500Hz)
1	1	469
2	93	469
3	114	469
4	124	469
5	57	471
6	72	471
7	77	471
8	66	475
9	117	475
10	96	477
11	29	479
12	56	479
13	62	479
14	99	479
15	82	481
16	44	485
17	17	489
18	86	489
19	120	489
20	90	499
21	94	499
22	103	499
23	8	501
24	28	501
25	33	501
26	43	501
27	49	501
28	74	501
29	84	501

Wybrane ewolucje zostały następnie symetrycznie uzupełnione próbkami o wartościach próbek krańcowych do długości 512 próbek i przekształcone do dziedziny czasowo-skalowej. W tej dziedzinie wyznaczono wartości średnie i odchylenia standardowe odpowiadających sobie współczynników w reprezentacjach 29 wybranych zapisów uzyskując czasowo-skalową reprezentację spodziewanej średniej energii (rys. 4.3) i odchylenia standardowego energii (rys. 4.4).

Na obu rysunkach strzałką zaznaczono średnie położenie zespołu QRS. Ponieważ w zastosowanej prezentacji graficznej kolor ciemny określa najmniejszą energię a jasny największą można łatwo dostrzec, iż największa energia przypada na zespół QRS. Główna koncentracja energii przypada w obrębie tego właśnie regionu. Najwyższa częstotliwość, czyli najniższy numer skali to pasmo, w którym i dla energii i zmienności energii można zauważyć ujednolicenie (brak zależności zawartości od zjawisk kardiogennych) co sugeruje, że przeważa tam szum. Widać, że w najwyższej skali (dolna część rysunku) zmienność energii jest taka sama w zespole QRS jak poza nim.



Rys. 4.3. Uśredniony rozkład energii spodziewanej w obrębie pojedynczej ewolucji serca



Rys. 4.4. Uśredniona zmienność energii spodziewanej w obrębie pojedynczej ewolucji serca; znikoma zmienność na początkach i końcach sygnału (czarny prawy i lewy brzeg diagramu dekompozycji) jest rezultatem uzupełniania długości sygnału próbkami o wartościach próbek krańcowych

Zasadnicza konkluzja z przeprowadzonego badania potwierdza istnienie luki pasmowej w dwóch wyższych skalach w przedziałach czasu poza zespołem QRS. Daje to

nadzieję na możliwość kodowania informacji dodatkowej (sekretu) w luce pasmowej bez interferencji z zawartością diagnostyczną elektrokardiogramu.

4.3 Kodowanie i dekodowanie tajemnic w EKG jako nośniku

Ukryta wiadomość jest całkowicie osadzana we współczynniki reprezentacji czasowo-skalowej w najwyższej (pierwszej) skali poza odcinkiem zawierającym zespół QRS. Druga skala (w której czasowa rozpiętość współczynników jest dwukrotnie większa niż w pierwszej) jest następnie używana dla warstwy opisu danych. To umożliwia identyfikację wiadomości i przechowywanie trzech deskryptorów kontenera danych: położenia początku kontenera względem położenia maksimum załamka R (6 bitów), długości kontenera (9 bitów) i identyfikatora głębi bitowej kodowania (3 bity). Zestaw deskryptorów opisujących kontener danych jest poprzedzony wzorcem autoryzacji dostępu (do 12 bitów) tworzącym odpowiednią sekcję kluczową. Tak skomponowany ciąg identyfikacyjny jest zakodowany za pomocą prostej metody LSB we współczynniki drugiej skali reprezentacji czasowo-skalowej elektrokardiogramu i zajmuje 30 kolejnych próbek (tj. 240 ms przy 500 Hz). Ciąg identyfikacyjny rozpoczyna się od próbki położonej w określonej odległości R-to-Key (RK) od szczytu załamka R (rys. 2.9) [Augustyniak P., 2014].

Jak sugeruje termin, klucz jest podstawowym elementem w osadzaniu ukrytej wiadomości w elektrokardiogramie. Aby zwiększyć ochronę danych, zastosowano trzeci system ochrony zgodnie z Kluczową Klasyfikacją Schematów Steganograficznych. W związku z tym klucz składa się z trzech sekcji o następujących funkcjach:

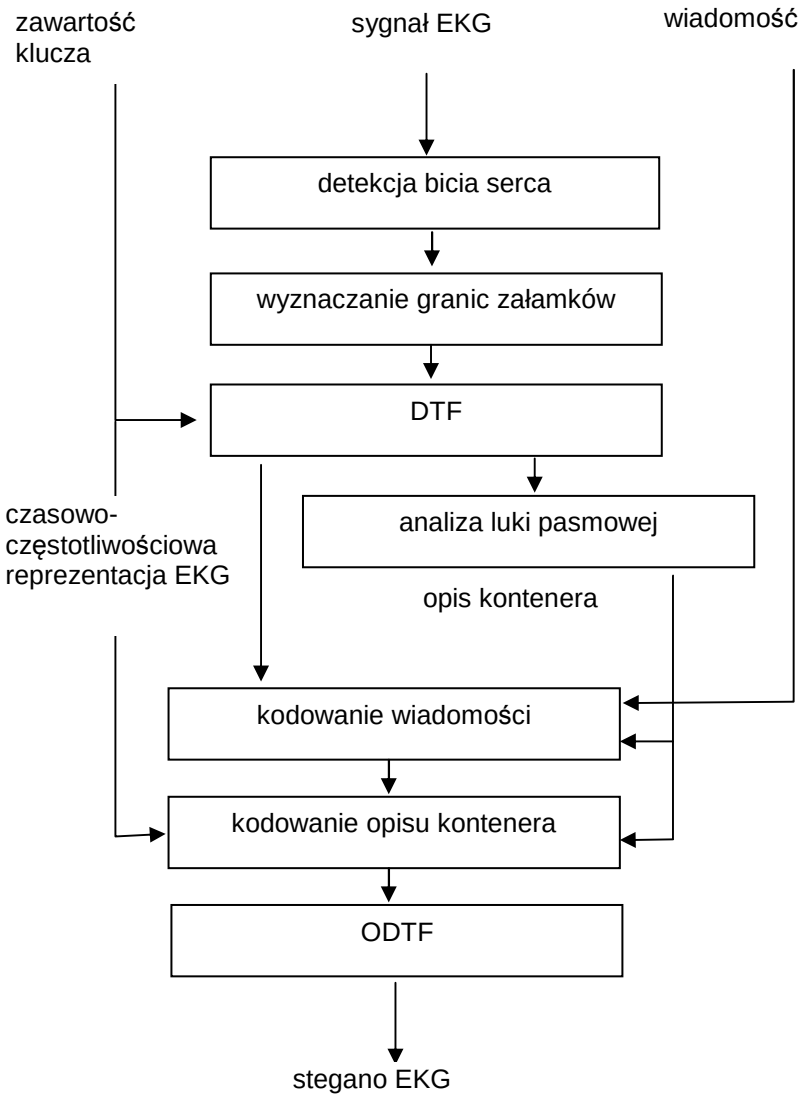
- specyfikacja użytej falki,
- specyfikacja odległości RK,
- wzorzec autoryzacji dostępu [Augustyniak P., 2014].

Warto zauważyć, że przyjęte rozwiązanie umożliwia adaptacyjny dobór parametrów kontenera danych do bieżącej zawartości diagnostycznej elektrokardiogramu. Przykładowo, podwyższenie częstości akcji serca spowoduje automatyczne skrócenie kontenerów danych i zaznaczenie tego faktu w opisie. Dodatkową zaletą przyjętego rozwiązania jest niezależność kontenerów danych utworzonych w ramach poszczególnych ewolucji czy odprowadzeń EKG. W ramach tego samego zapisu mogą one być różnej długości, rozpoczynać się z różnym opóźnieniem względem maksimum załamka R, używać różnej bitowej głębokości kodowania danych, wreszcie – mogą być przeznaczone dla różnych odbiorców w zależności od ciągu bitów stanowiących wzorzec autoryzacji dostępu.

5. Eksperymentalna ocena schematu kodowania

Zaproponowany schemat seganografii z wykorzystaniem sygnału EKG jako nośnika został zaimplementowany w środowisku Matlab i zweryfikowany na drodze eksperymentalnej z użyciem standardowych zapisów wieloodprowadzeniowych z bazy CSE (rozdział 3.3).

Na rysunkach 5.1 i 5.2 przedstawiono schemat działań, użyty w eksperymencie.

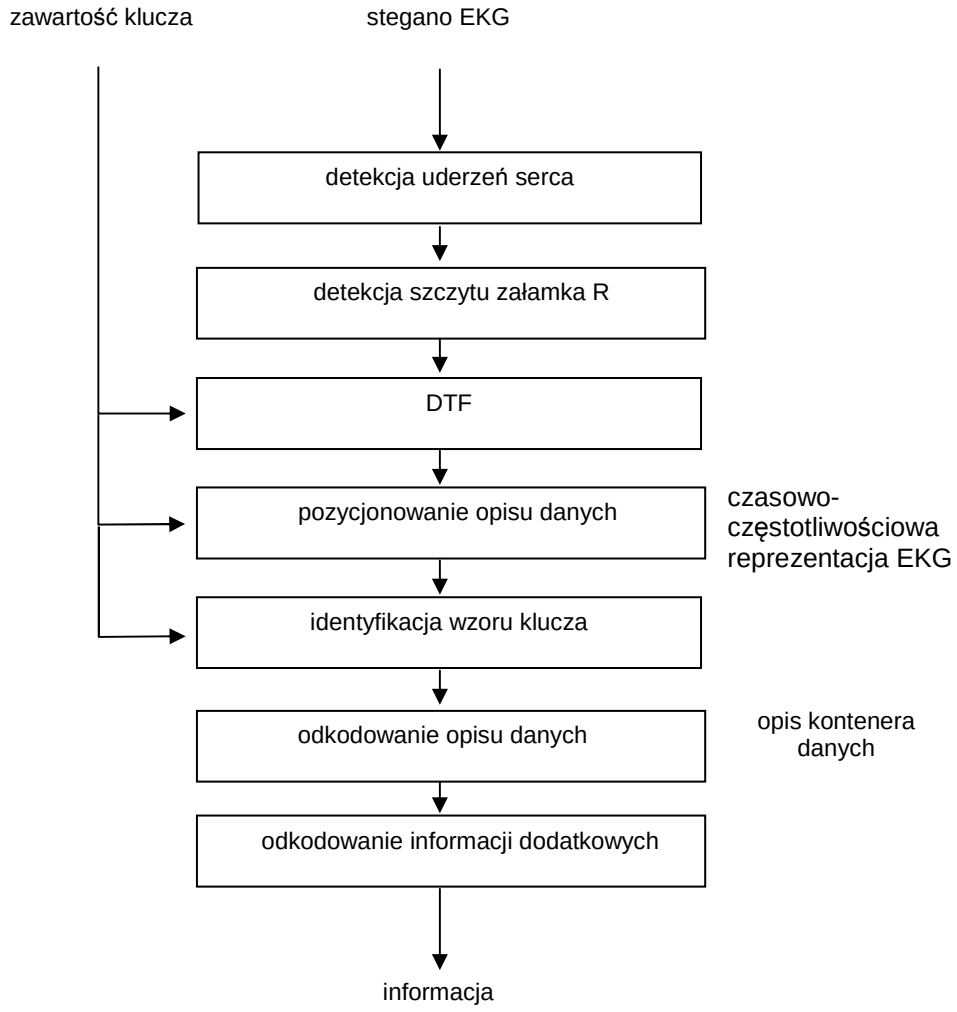


Rys. 5.1. Schemat blokowy schematu przetwarzania dodatkowego kodowania wiadomości cyfrowych [Augustyniak P., 2012]

Zestaw 100 sygnałów rekomendowanych normą IEC60601-2-51 (tab. 3.1) został poddany kodowaniu o różnych parametrach: transformacji falkowej (por. rozdział 5.1), bitowej głębokości kodowania (por. rozdział 5.2) i różnej zawartości sekretu (tekst lub dane liczbowe, por. rozdział 5.3). Dla każdego z wariantów kodowania, a także dla każdego z ‘czystych’ nośników (tzn. oryginalnych sygnałów EKG z bazy) przeprowadzono automatyczną analizę zapisu za pomocą certyfikowanego programu Ascard6 (Aspel s.a.).

Program został nieznacznie zmodyfikowany w celu udostępnienia (zapisu do pliku) wartości zmiennych wewnętrznych zawierających parametry amplitudowo-czasowe punktów granicznych wszystkich załamków w każdym z odprowadzeń EKG. Na wejście programu kierowany był każdy z plików bazy CSE w wersji oryginalnej, a następnie w szeregu wersjach zawierających informację dodatkową (tekstową lub liczbową) zakodowaną z użyciem testowanych transformacji falkowych oraz z różną głębokością bitową. Łącznie wykonano 7300 automatycznych analiz dziesięciosekundowych plików EKG, trudno wyobrazić sobie analizę takiej liczby wariantów zapisów EKG w sposób inny niż automatyczny.

Jako miarę jakości diagnostycznej sygnału, oraz miarę utraty jakości względem zapisu oryginalnego (‘czystego’ nośnika) przyjęto powtarzalność podstawowych parametrów czasowych (długości: załamka P, odcinka PQ zespołu QRS i odcinka QT) wyspecyfikowanych wraz z dopuszczalnymi odchyłkami wartości w normie 60601-2-51 (por. rozdział 3.3).



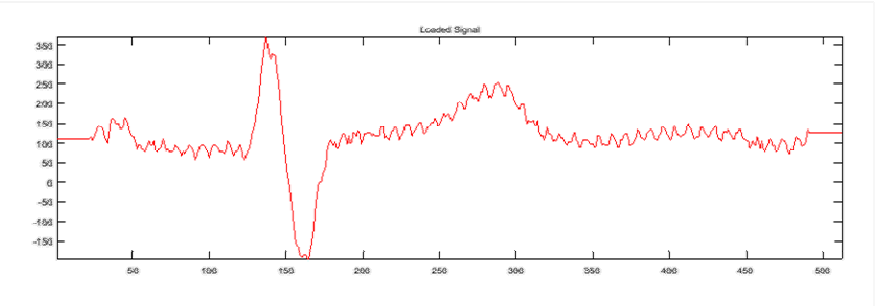
Rys. 5.2. Schemat blokowy schematu odkodowania wiadomości [Augustyniak P., 2012]

5.1 Kodowanie z różnymi falkami macierzystymi

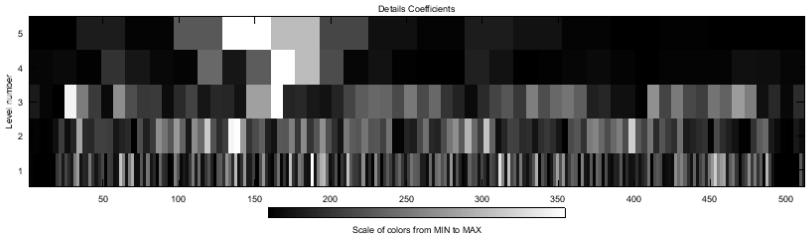
W większości zastosowań falkowej dekompozycji sygnałów uzyskiwany rezultat zależy od właściwego wyboru funkcji bazowej dekompozycji (falki-matki). Wybór ten zwykle podyktowany jest podobieństwem czasowym falki i spodziewanych form sygnału, co zapewnia uzyskanie dużych wartości korelacji wzajemnej i koncentrację energii sygnału w niewielkiej liczbie współczynników o znacznych wartościach. Ze względu na różnorodność form spodziewanych w sygnale EKG trudno było jednoznacznie wskazać falkę, której dobór byłby uzasadniony podobieństwem kształtu. Z tego powodu w badaniach uwzględniono sześć funkcji bazowych z trzech rodzin: Daubechies, Symlets i Biortogonalnych, dla każdej z nich używając falek o dwóch różnych rozpiętościach czasowych (rzędach filtrów). Rzędy te dobrano tak, aby długość falki odpowiadała spodziewanej długości zespołu QRS w środku zakresu dekompozycji tj. w 3 lub 4 skali.

Na rysunkach 5.3 do 5.12 przedstawiono dekompozycje czasowo-częstotliwościowe przykładowego sygnału CSE001 z wykorzystaniem falek: db5 i db10, sym6 i sym11 oraz bior2.4 i bior4.4 i ich korelację z przykładowym sygnałem EKG. Na pierwszym z nich (rys. 5.3) ukazany jest typowy sygnał (tutaj CSE001). Rysunki 5.4 do 5.12 przedstawiają dekompozycje uzyskane za pomocą różnych typów falek z różnych rodzin, a także ich różnice, aby zobrazować odmienność reprezentacji czasowo-skalowych. Im niższy jest rząd falki tym większy jest przeciek energii w dziedzinie widma. Krótsza falka jest bardziej dokładna w dziedzinie czasu natomiast jest mniej dokładna w dziedzinie częstotliwości i na odwrót, gdy rząd jest większy, falka jest bardziej dokładna w dziedzinie częstotliwości natomiast jest mniej dokładna w dziedzinie czasu.

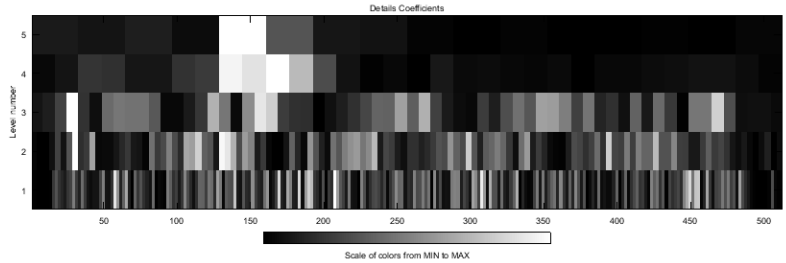
Jakościowe badanie wpływu wyboru rzędu falki na rezultat dekompozycji sygnału przedstawiono dla każdej z trzech rodzin i przykładowego sygnału CSE 001 na rysunkach 5.3 – 5.12. Dla fragmentu sygnału zawierającego pojedynczą ewolucję serca (rys. 5.3) dokonano dekompozycji z użyciem falki niższego rzędu i wyższego rzędu (pary rysunków: 5.4 i 5.5, 5.7 i 5.8 oraz 5.10 i 5.11), a następnie porównano. Wynik tego porównania (rysunki 5.6, 5.9 i 5.12) świadczy o tym, że w przypadku rodzin Daubechies i Symlets wybór rzędu falki ma istotny wpływ na własność dekompozycji, natomiast w przypadku falek Biortogonalnych różnica jest mniej istotna.



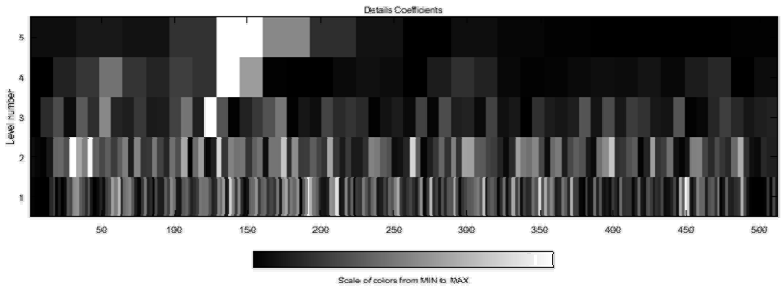
Rys. 5.3. Sygnał (CSE001)



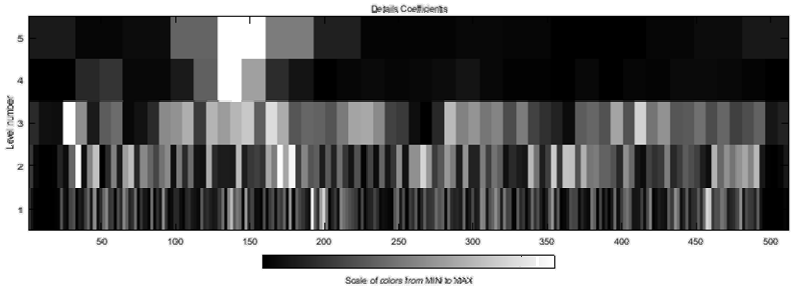
Rys. 5.4. Dekompozycja sygnału EKG (CSE001) z użyciem falki db5



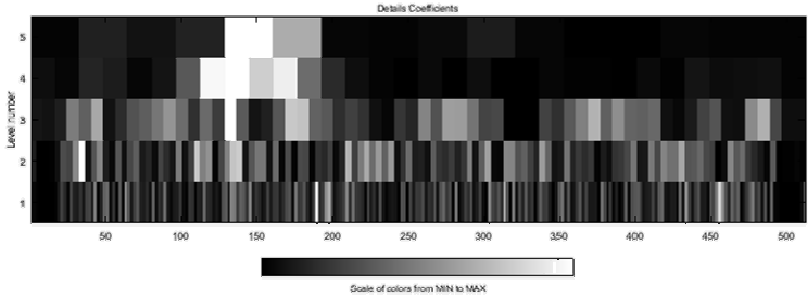
Rys. 5.5. Dekompozycja sygnału EKG (CSE001) z użyciem falki db10



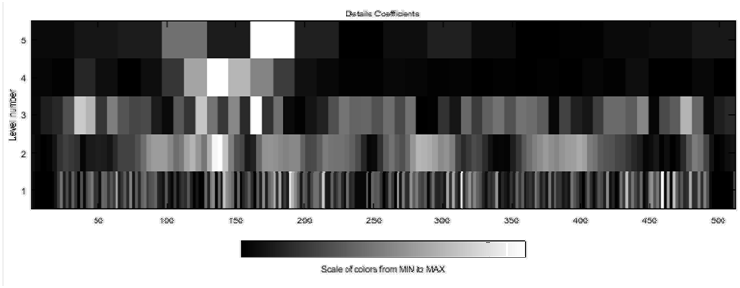
Rys. 5.6. Różnica dekompozycji sygnałów EKG (CSE001) z użyciem falek db5 i db10



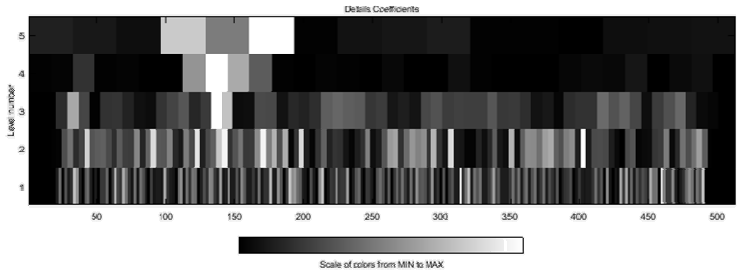
Rys. 5.7. Dekompozycja sygnału EKG (CSE001) z użyciem falki sym6



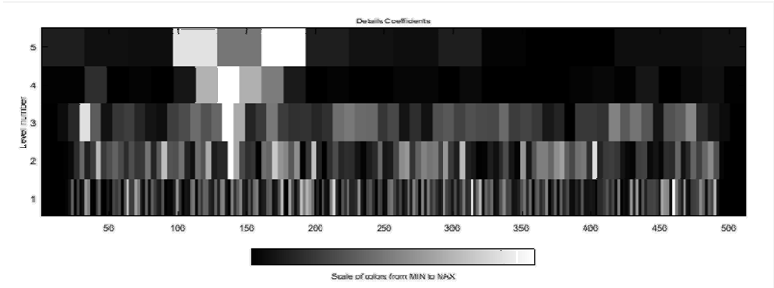
Rys. 5.8. Dekompozycja sygnału EKG (CSE001) z użyciem falki sym11



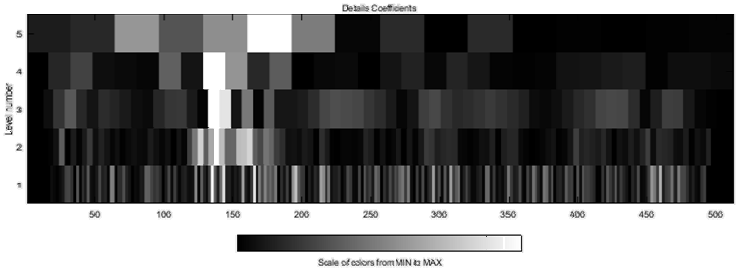
Rys. 5.9. Różnica dekompozycji sygnałów EKG (CSE001) z użyciem falek sym6 i sym11



Rys. 5.10. Dekompozycja sygnału EKG (CSE001) z użyciem falki bior2.4



Rys. 5.11. Dekompozycja sygnału EKG (CSE001) z użyciem falki bior4.4



Rys. 5.12. Różnica dekompozycji sygnałów EKG (CSE001) z użyciem falek bior2.4 i bior4.4

W zależności od zawartości zapisu EKG (tj. dla różnych plików wchodzących w skład bazy CSE) różne falki-matki okazywały się najlepiej skorelowane z sygnałem. Wskazuje to na brak uniwersalnej falki-matki optymalnej dla wszystkich zapisów (co najmniej w odniesieniu do zawartości bazy CSE). Przeprowadzona analiza jakościowa wykazała zależność otrzymywanej dekompozycji czasowo-częstotliwościowej od falki-matki użytej do transformacji. Uzasadnia to potrzebę wykonania pełnej analizy ilościowej, której wyniki zostały przedstawione w rozdziale 6.

5.2 Kodowanie z różną głębokością bitową

W ramach przeprowadzonego eksperymentu była badana zależność jakości sygnału EKG od głębokości bitowej kodowania informacji dodatkowej. Po zakodowaniu informacji w każdym z pięciu wariantów głębokości bitowej parametry diagnostyczne wyznaczone z sygnału stegano EKG zostały porównane z analogicznymi parametrami dla sygnału referencyjnego (‘czystego’ nośnika).

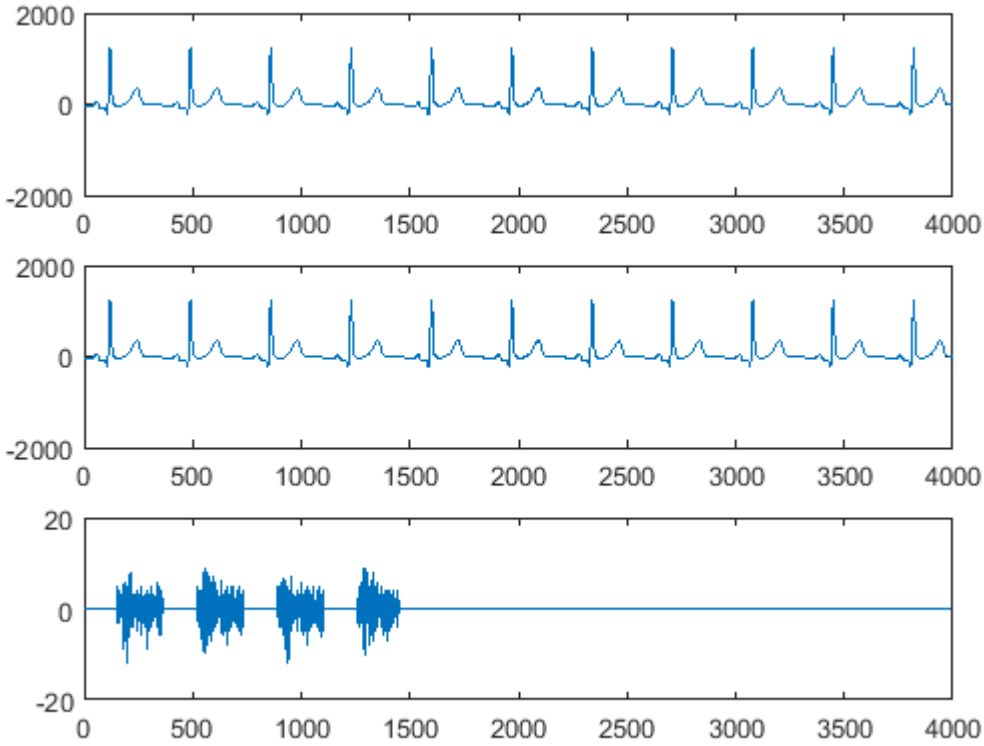
Głębokość bitowa 1 odpowiada kodowaniu jednego bitu strumienia informacji dodatkowej w jednym współczynniku reprezentacji czasowo-częstotliwościowej. Odpowiada to metodzie najmniej znaczącego bitu (ang. *Least Significant Bit*, LSB) opisanej w literaturze [Ibaida A. i in, 2011]. Oczywiście większa głębokość bitowa powoduje wzrost pojemności kontenera danych, ale jednocześnie zwiększa ingerencję w sygnał EKG.

Ponieważ założeniem metody kodowania z wykorzystaniem luki pasmowej jest zastąpienie składowych sygnału niezwiązanych z reprezentacją pracy serca (tj. szumu) przez informację sekretną, trudno oczekiwać, że ustalona *a priori* bitowa głębokość kodowania umożliwi uzyskanie rozkładu wartości przypominającego szum. Dlatego, w jednym z wariantów wprowadzono dodatkowo procedurę pomiaru wartości międzyszczytowej szumu, a górne zaokrąglenie logarytmu (przy podstawie 2) zmierzonej wartości stanowiło liczbę bitów informacji dodatkowej użytych do kodowania jej w pojedynczym współczynniku reprezentacji czasowo-skalowej.

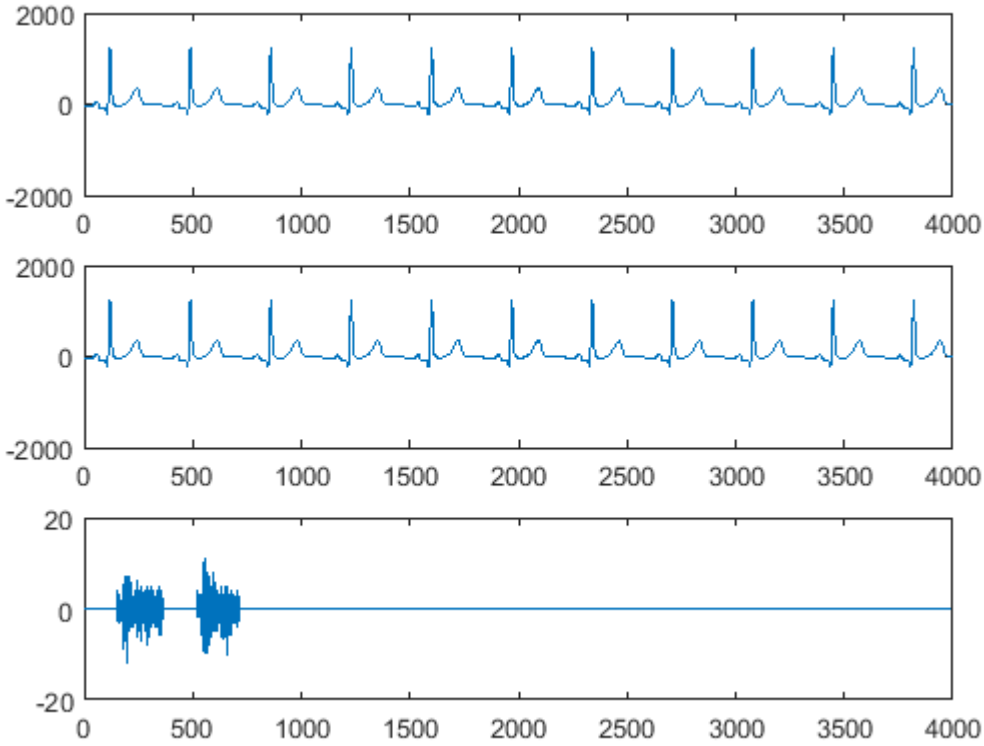
Informacja była tekstem złożonym z 51 znaków. Rysunki 5.13 - 5.17 przedstawiają analizę jakościową kodowania informacji dodatkowej z użyciem falki Daubechies db5 w pliku CSE001 przy głębokości 1-5 bitów. Rysunki 5.18 - 5.22 oraz 5.23 - 5.27 przedstawiają analizę jakościową kodowania informacji dodatkowej z użyciem falek odpowiednio Symlet (sym6) i Biortogonalnych (bior2.4). Rysunki 5.28 - 5.30 przedstawiają analizę jakościową

kodowania informacji dodatkowej przy głębokości dobieranej automatycznie dla falek db5, sym6 i bior2.4. Analiza ilościowa wszystkich zapisów została przedstawiona w rozdziale 6.

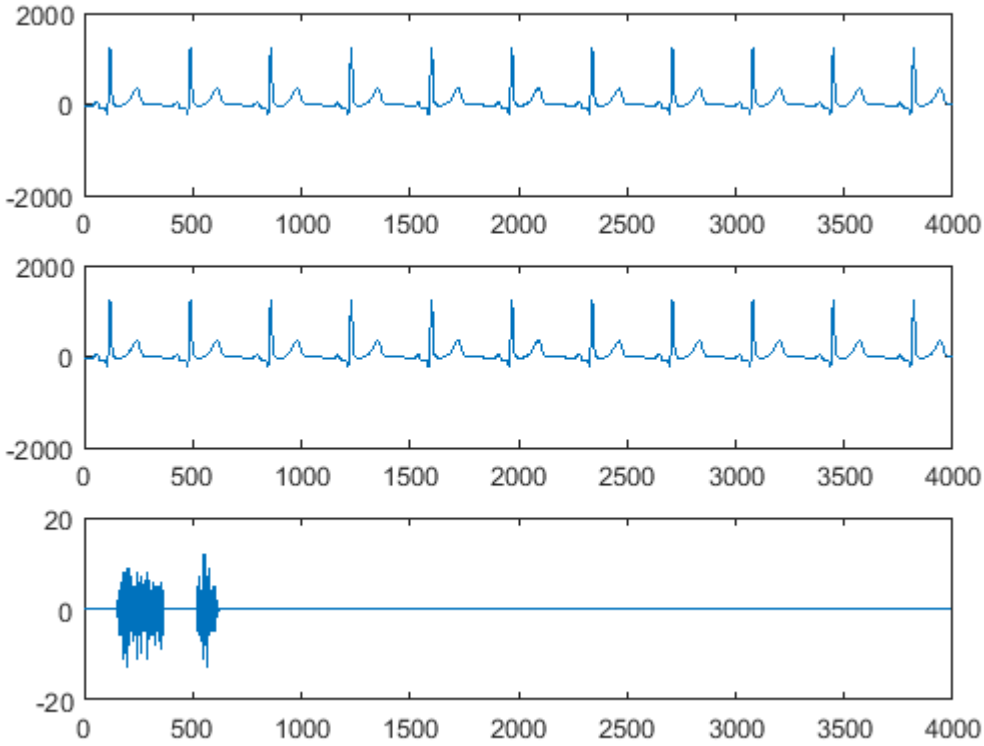
Im większa jest głębokość kodowania tym większa ingerencja procesu kodowania w sygnał EKG i tym większe ryzyko zmiany jego treści diagnostycznej. Jednakże dla sygnałów, które są zarejestrowane z wyższym poziomem szumów, większa głębokość kodowania może być korzystniejsza, bo przy większej głębokości bitowej statystyka wartości kodowanego sekretu jest bardziej podobna do statystyki szumu. Z rysunków 5.13-5.25 wynika również, że zwiększenie bitowej głębokości kodowania zwiększa amplitudę różnicy pomiędzy ‘czystym’ nośnikiem a sygnałem stegano EKG, ale także zwiększa pojemność kontenera danych, dzięki czemu ta sama informacja sekretna może być zakodowana w mniejszej liczbie kolejnych ewolucji serca. Analiza ilościowa procesu kodowania z różną głębokością bitową jest przedstawiona w rozdziale 6.



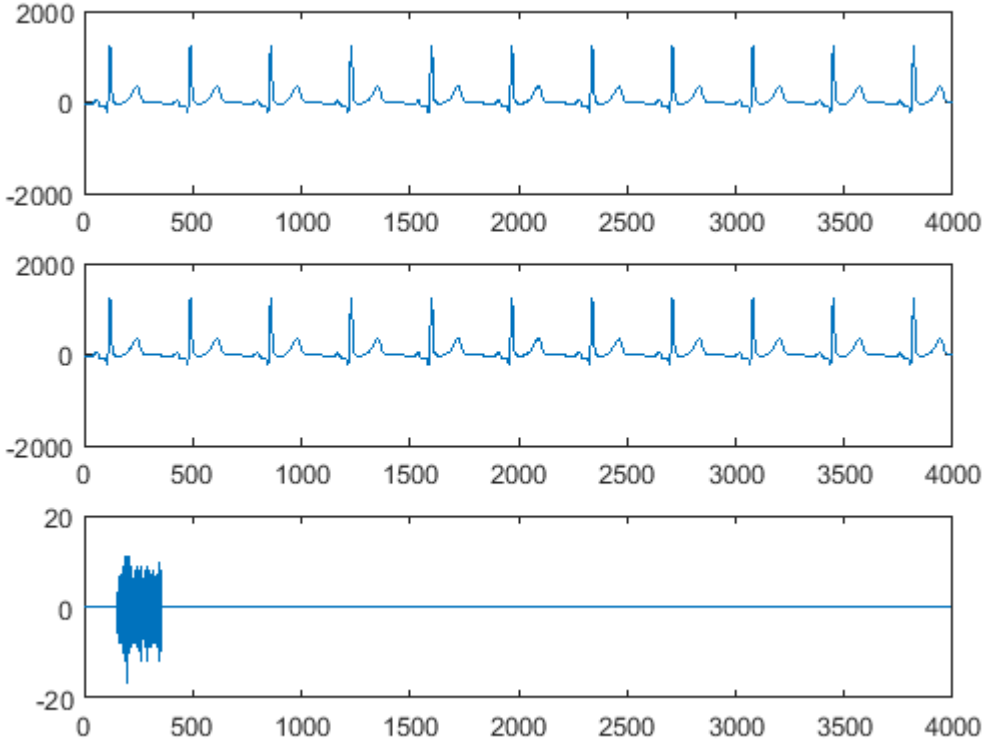
Rys. 5.13. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 1 bit, c) różnica sygnału zakodowanego względem referencyjnego, falka db5



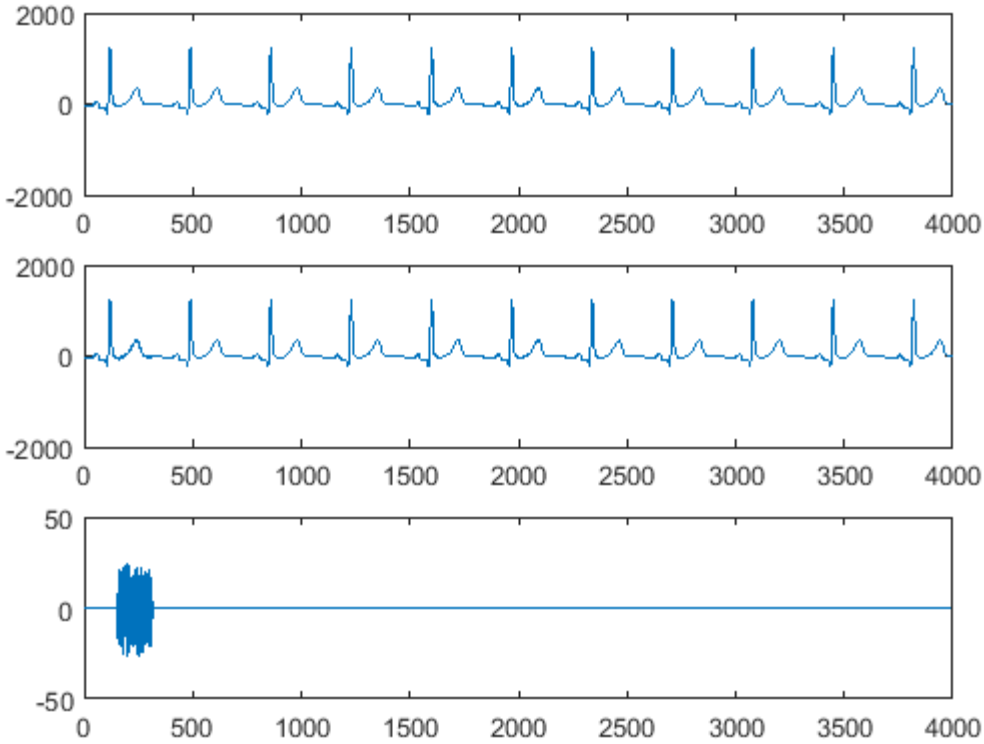
Rys. 5.14. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 2 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka db5



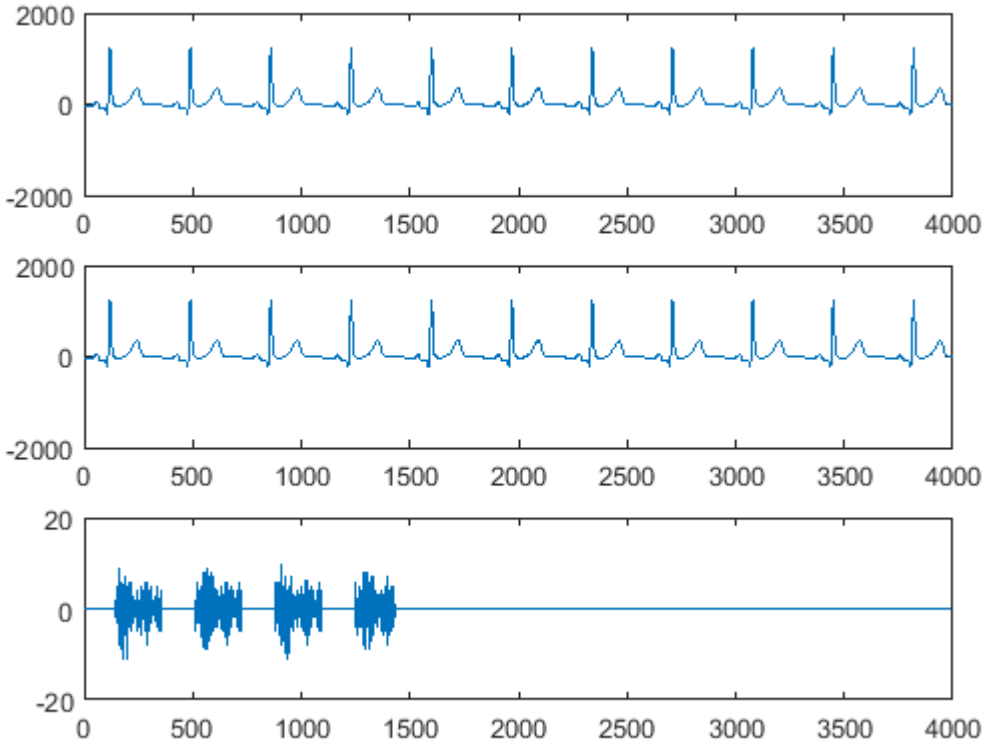
Rys. 5.15. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 3 bitów, c) różnica sygnału zakodowanego względem referencyjnego falka, db5



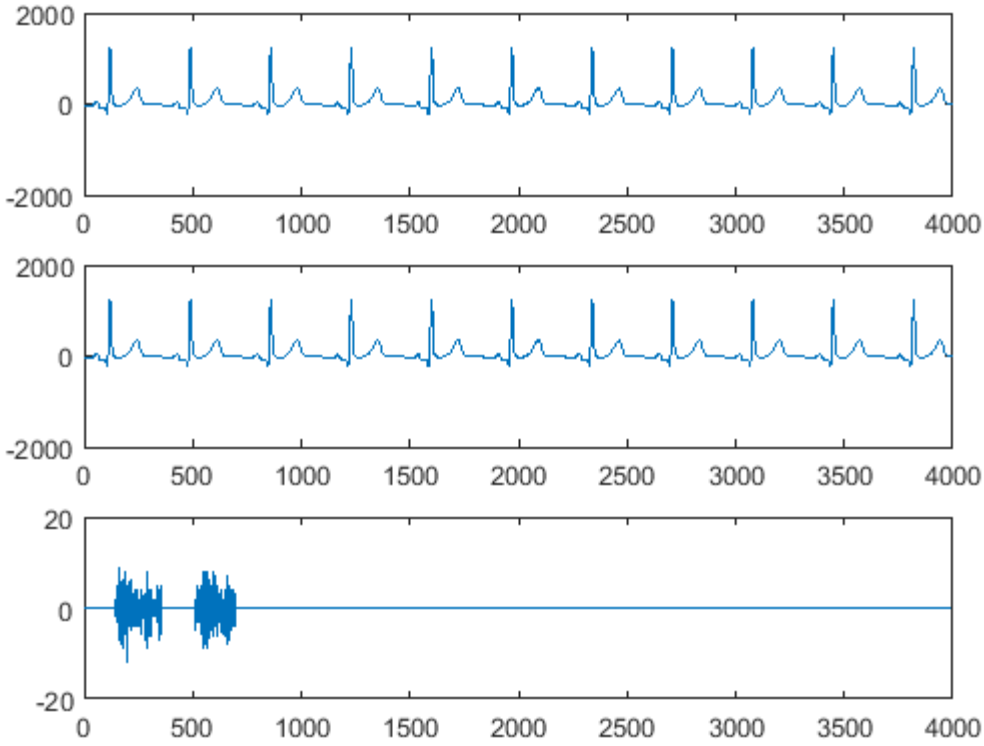
Rys. 5.16. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 4 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka db5



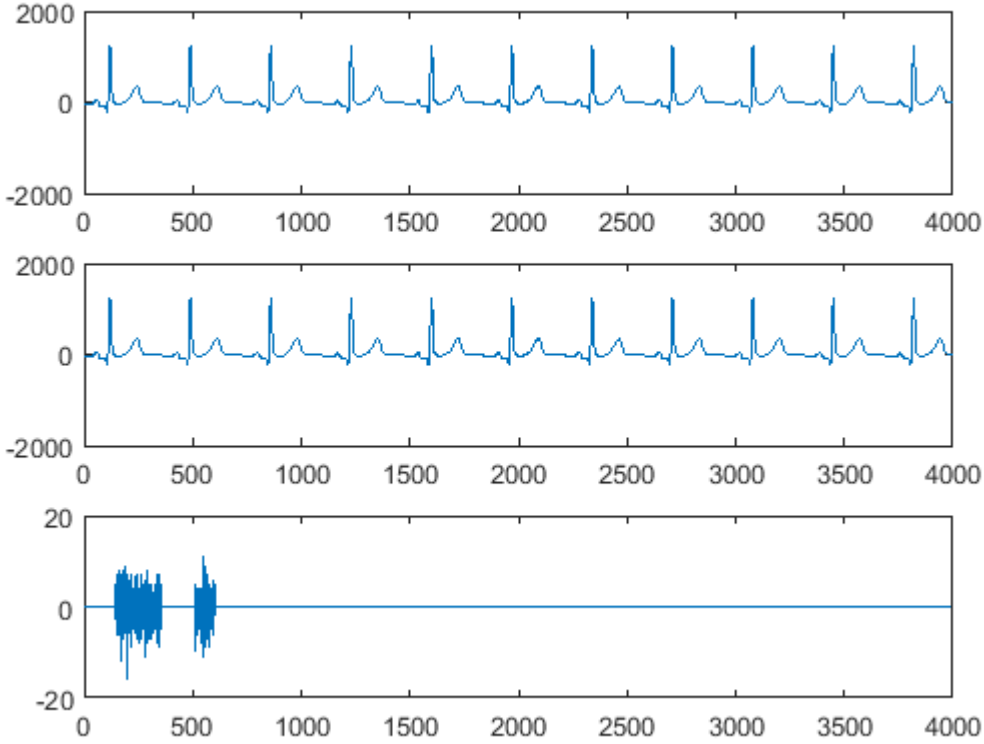
Rys. 5.17. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 5 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka db5



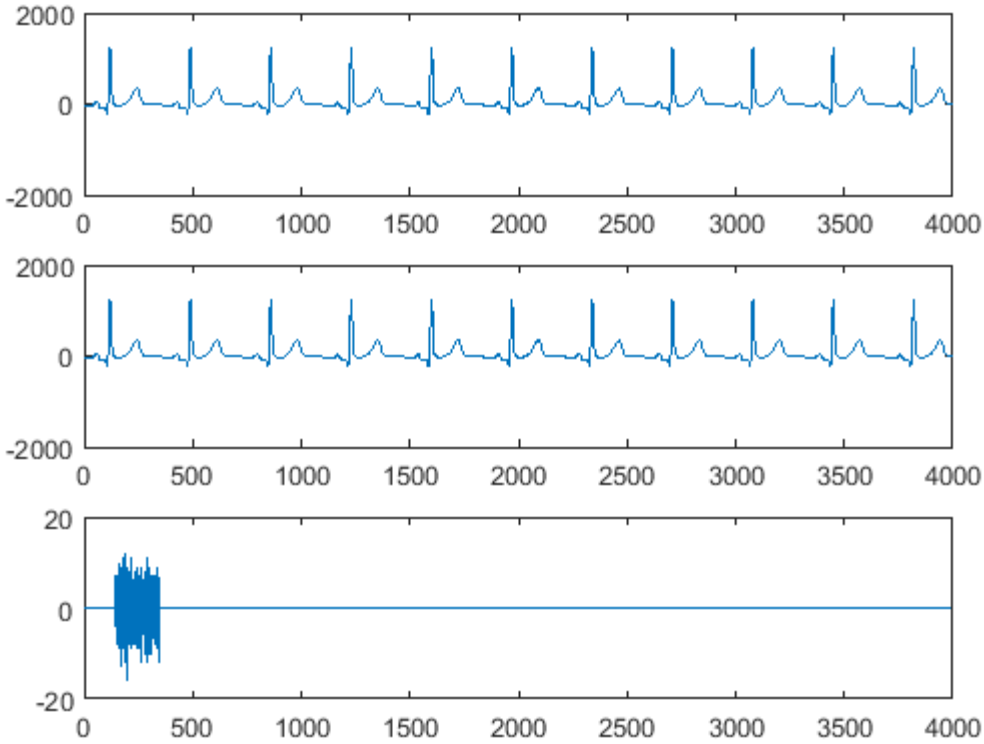
Rys. 5.18. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 1 bit, c) różnica sygnału zakodowanego względem referencyjnego, falka sym6



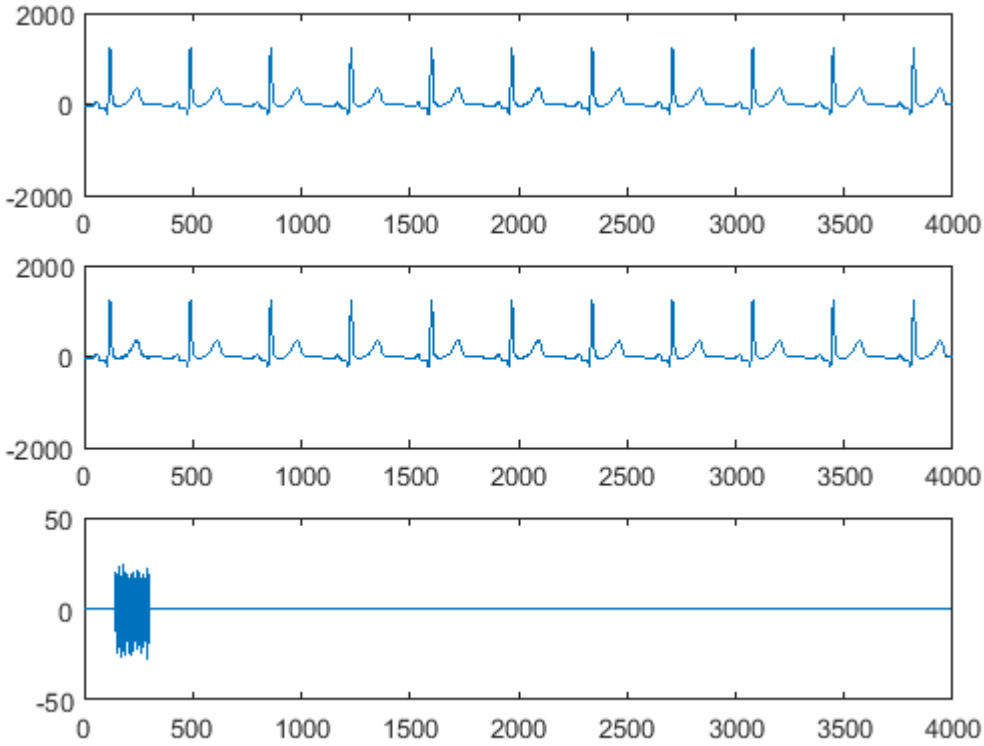
Rys. 5.19. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 2 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka sym6



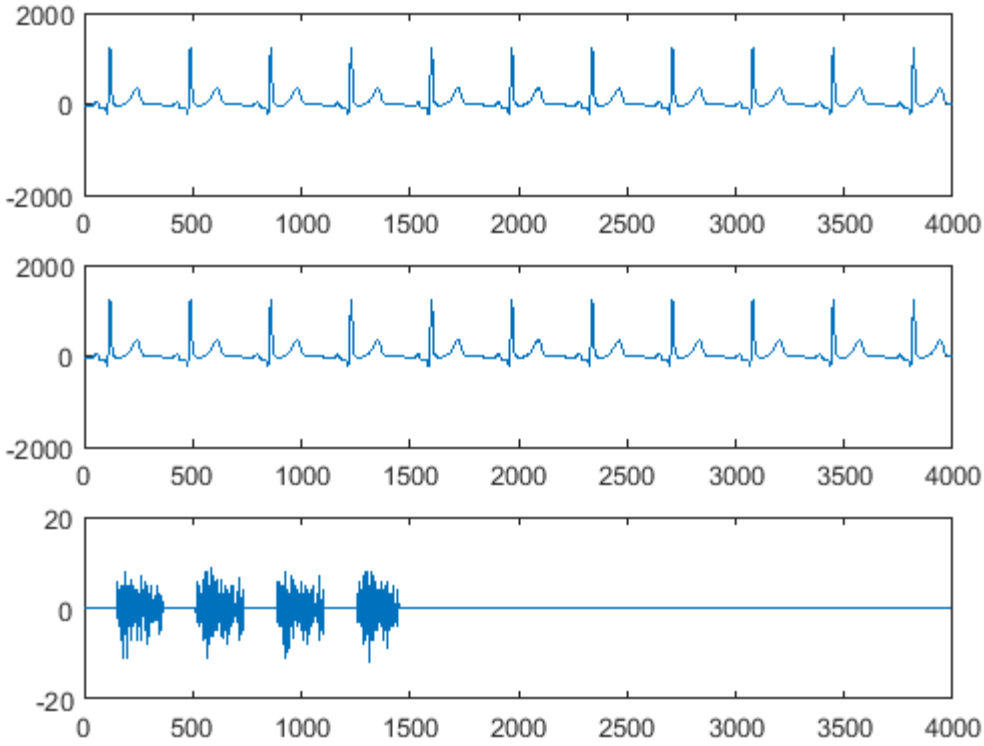
Rys. 5.20. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 3 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka sym6



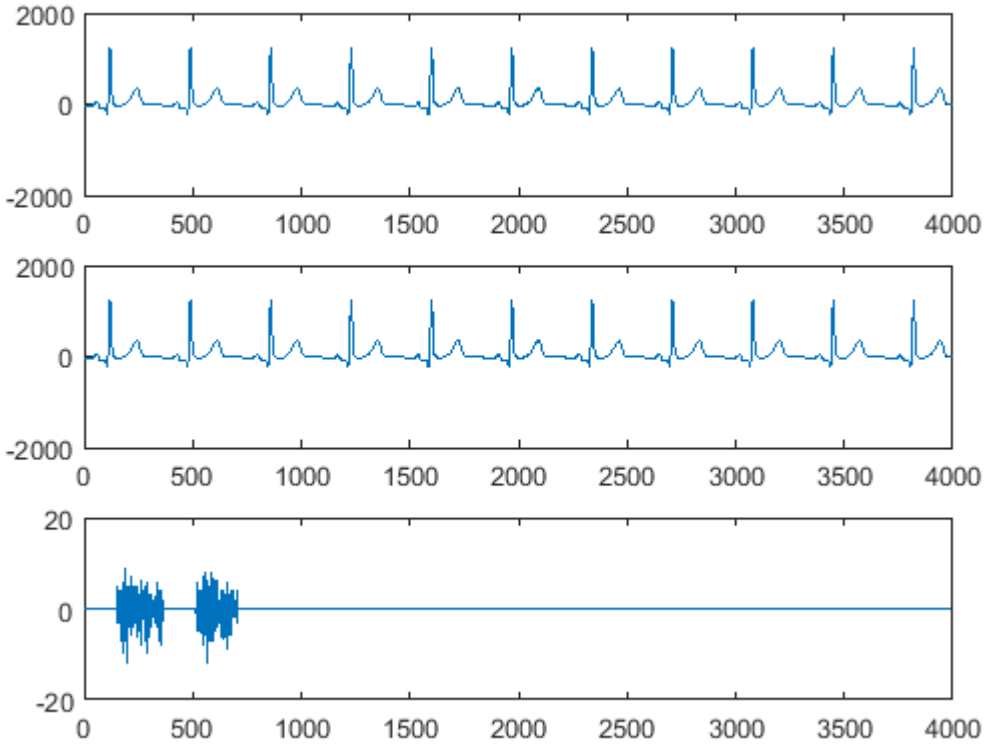
Rys. 5.21. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 4 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka sym6



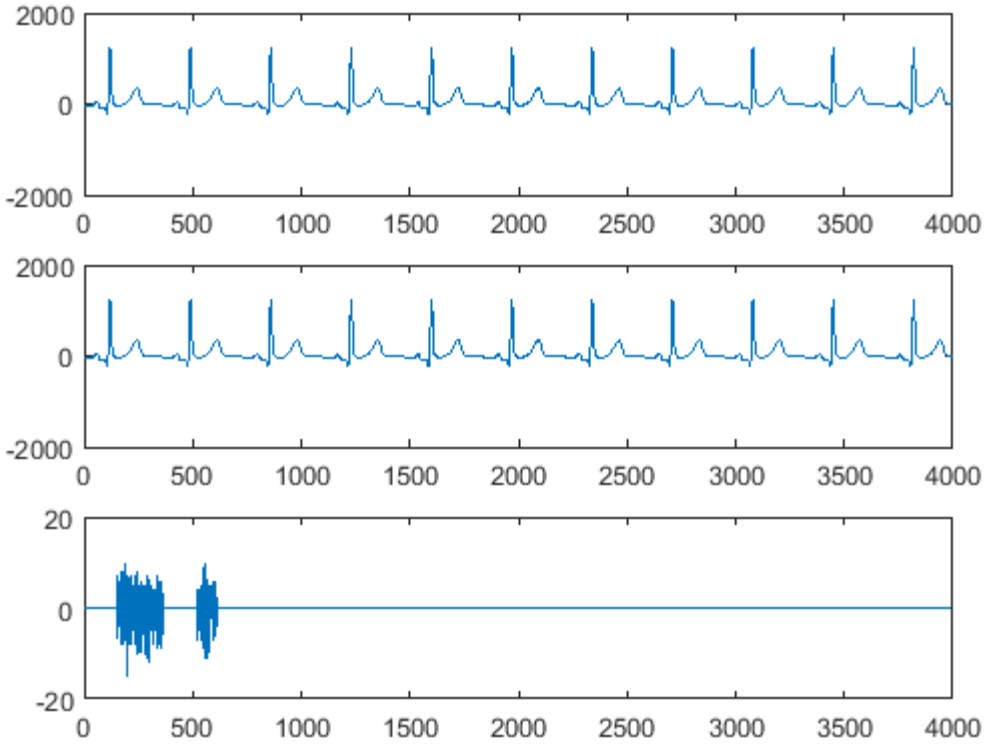
Rys. 5.22. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 5 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka sym6



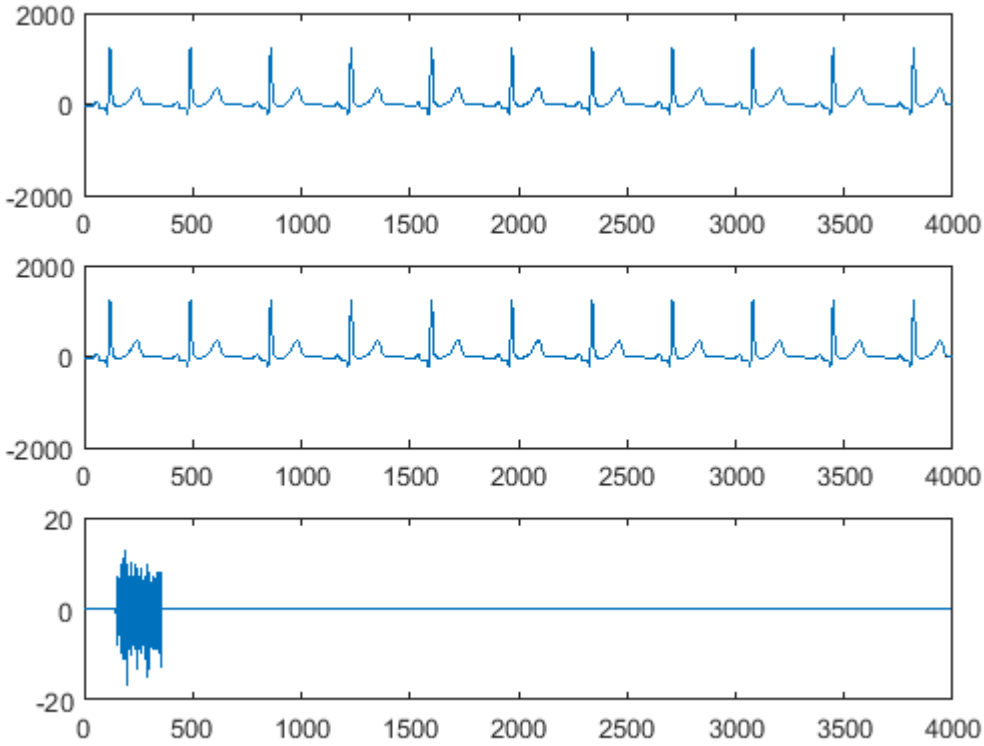
Rys. 5.23. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 1 bit, c) różnica sygnału zakodowanego względem referencyjnego, falka bior2.4



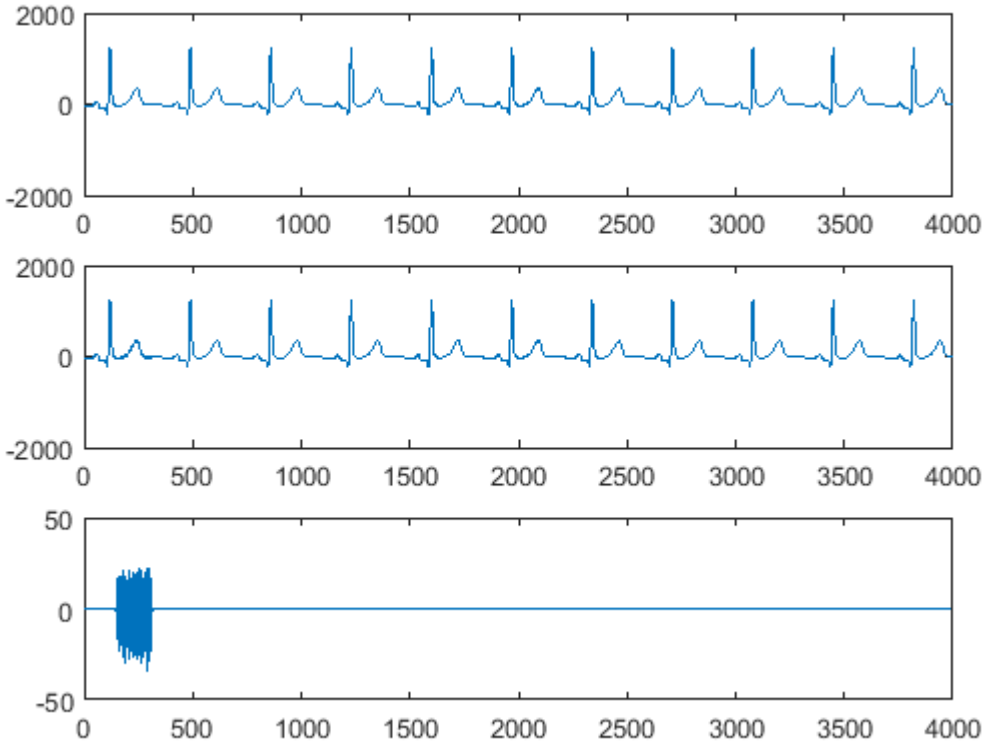
Rys. 5.24. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 2 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka bior2.4



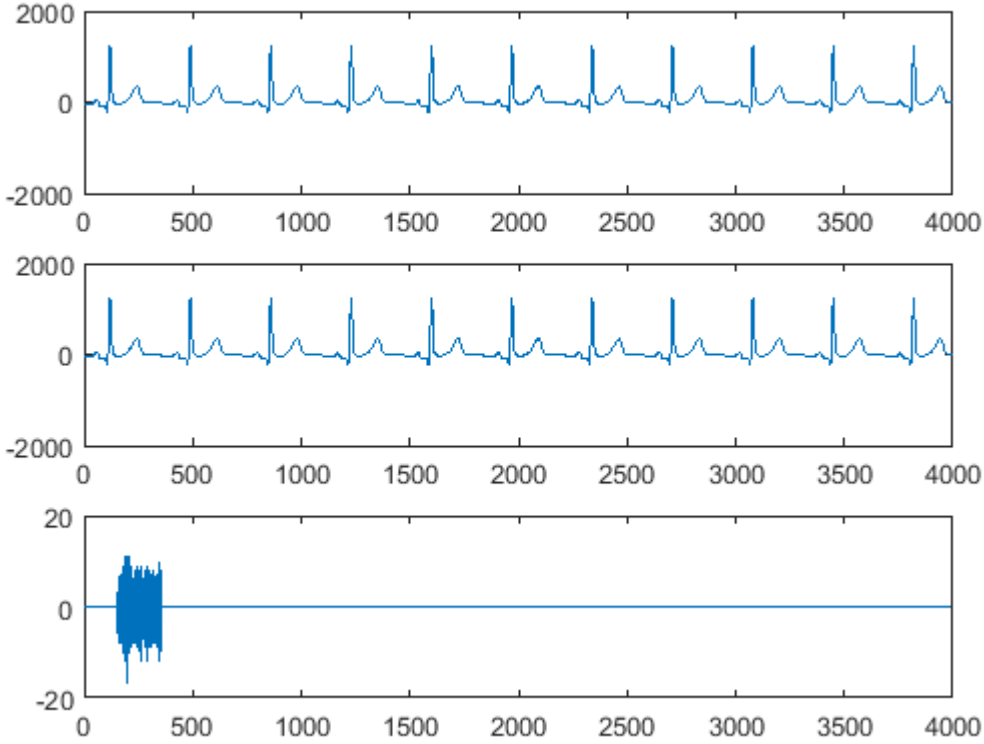
Rys. 5.25. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 3 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka bior2.4



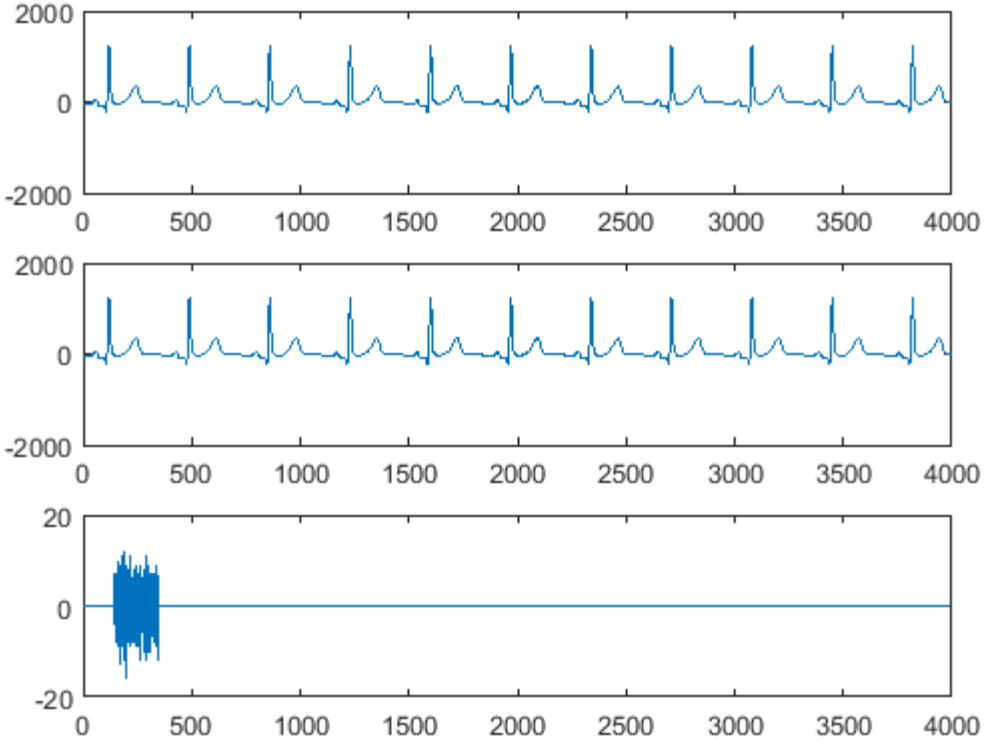
Rys. 5.26. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 4 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka bior2.4



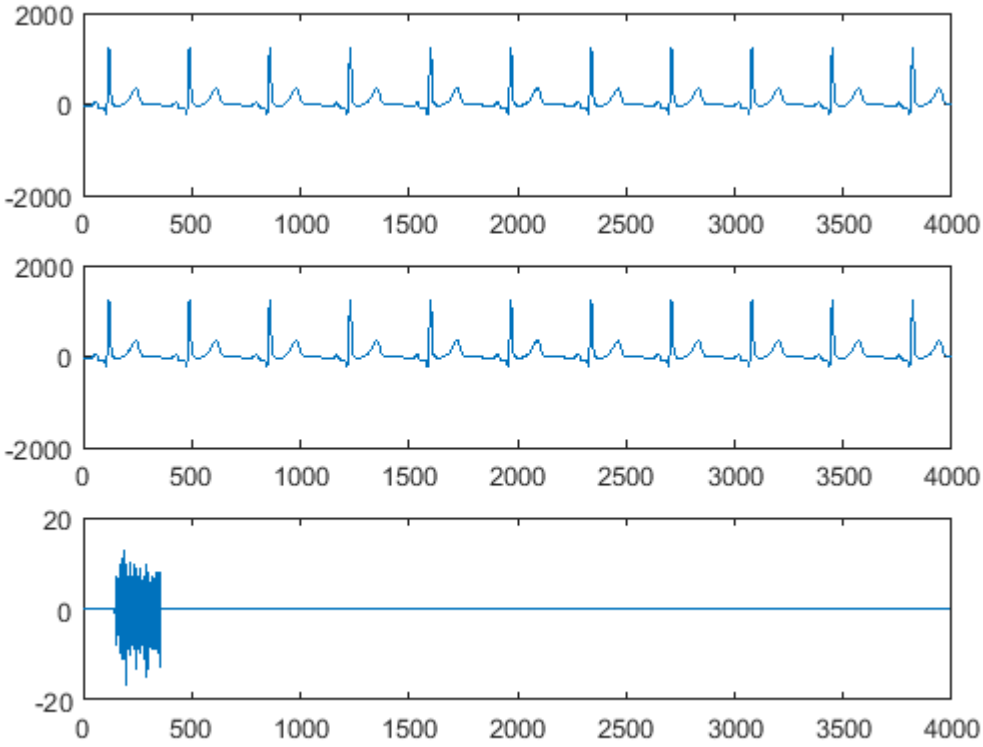
Rys. 5.27. a) sygnał referencyjny, b) sygnał zakodowany na głębokość 5 bitów, c) różnica sygnału zakodowanego względem referencyjnego, falka bior2.4



Rys. 5.28. a) sygnał referencyjny, b) sygnał zakodowany na głębokość dobieraną automatycznie na podstawie analizy poziomu szumu izolinii, c) różnica sygnału zakodowanego względem referencyjnego, falka db5



Rys. 5.29. a) sygnał referencyjny, b) sygnał zakodowany na głębokość dobieraną automatycznie na podstawie analizy poziomu szumu izolinii, c) różnica sygnału zakodowanego względem referencyjnego, falka sym6



Rys. 5.30. a) sygnał referencyjny, b) sygnał zakodowany głębokość dobieraną automatycznie na podstawie analizy poziomu szumu izolinii, c) różnica sygnału zakodowanego względem referencyjnego, falka bior2.4

5.3 Kodowanie sekretu o różnej zawartości

W przykładach podanych w podrozdziałach 5.1 i 5.2 założono, że informacja sekretna jest ma postać zdania języka naturalnego, a jej reprezentacja maszynowa ma postać ciągu kodów ASCII. Z takiego założenia wynikają jednak szczególne własności statystyczne kodowanej informacji: przewaga znaków o kodach 96-127 (#60 - #7F, małe litery), sporadycznie występujące znaki o kodach 64-95 (#40 - #5F, duże litery) i brak pozostałych znaków. Ponieważ jednym z podstawowych zastosowań steganografii sygnału EKG jest przesyłanie dodatkowych parametrów wykonano badania porównawcze kodowania tekstu i kodowania wartości liczbowych, także przedstawionych jako znaki ASCII (kody z zakresu 48 – 57, tj. #30 - #39). Celem przedstawionych badań nie jest wyczerpanie wszystkich możliwych postaci informacji sekretnej (dlatego nie używano reprezentacji binarnej), ale jedynie stwierdzenie, czy inny rozkład statystyczny bitów reprezentacji sekretu wpłynie na własności procesu kodowania.

Rezultaty ilościowe porównania kodowania informacji sekretnej w postaci numerycznej i tekstowej zostały przedstawione w rozdziale 6.

6. Wyniki eksperymentu i ich analiza

Główny eksperyment numeryczny składał się z kodowania informacji sekretnej dwojakiego typu (tekstowego i numerycznego) przy użyciu transformacji czasowo-skalowej dla sześciu różnych rodzajów falek i 6 wariantów bitowej głębokości kodowania. Dodatkowo wykonano analizę dla każdego z sygnałów EKG (nośnika 'czystego'), aby uniezależnić otrzymane wyniki od ew. niedokładności posiadanego programu interpretacyjnego. Całkowita liczba wykonanych interpretacji zapisów EKG o długości 10 s wynosiła 7300.

Zapisy EKG z bazy CSE to sygnały 12 lub 15-odprowadzeniowe, a w poszczególnych odprowadzeniach punkty początkowe (końcowe) załamków nie pokrywają się. W praktyce medycznej jest stosowanych kilka sposobów wyznaczania 'globalnego' punktu początkowego, tj. takiego, który dotyczy całej ewolucji serca, niezależnie od pozycji elektrody. Używany program do interpretacji zapisu jest przeznaczony do 12-odprowadzeniowego przyłóżkowego rejestratora EKG i zawiera procedurę wyznaczania punktów granicznych załamków uruchamianą identycznie dla każdego z odprowadzeń. Aby nie ingerować w funkcjonowanie tego programu (tj. utrzymać jego jakość potwierdzoną certyfikatem), a jednocześnie uniezależnić rezultat pomiaru od lokalnie wyznaczanych punktów granicznych załamków, sygnały CSE zostały zmodyfikowane w następujący sposób:

- wykorzystano sygnały ze zbioru MA (ang. *multilead artificial*), zawierające 10-s powielenie ewolucji typowej w pliku MO (ang. *multilead original*) o odpowiadającym numerze; zapewnia to bitową identyczność wszystkich ewolucji serca i uniezależnia pomiar od wyboru ewolucji,
- wykorzystano odprowadzenie I (Eindhoven-I), którego sygnał powielono zastępując wszystkie pozostałe odprowadzenia; zapewnia to niezależność pomiaru od fluktuacji położenia punktów granicznych załamków w poszczególnych odprowadzeniach, jednocześnie umożliwiając poprawną pracę oprogramowania 12-kanałowego (w zakresie wyznaczania długości załamków).

Dokument IEC 60601-2-51 (por. rozdział 3.3) wymaga, aby dla 96% przypadków odchyłka czterech najistotniejszych parametrów diagnostycznych (długości: załamka P, odcinka PQ, zespołu QRS i odcinka QT) nie przekraczała wartości podanych tab. 3.2. Ponieważ plików testowych jest 100, cztery najgorsze przypadki można odrzucić. W przeprowadzonych badaniach założono, że posiadany program do interpretacji EKG jest idealnie dokładny, nie było celem Autorki testowanie tej dokładności. Założenie to było potrzebne, aby uznać rezultaty otrzymane w wyniku interpretacji 'czystego' nośnika za

wartości referencyjne, służące następnie do oceny wpływu procesu kodowania na zawartość diagnostyczną sygnału stegano EKG. Wartości odchyłki są przedstawione jako różnice wartości otrzymanej w eksperymencie z kodowaniem informacji dodatkowej i wartości referencyjnej. Zatem wartości ujemne oznaczają odcinek krótszy niż referencyjny, a dodatnie – dłuższy.

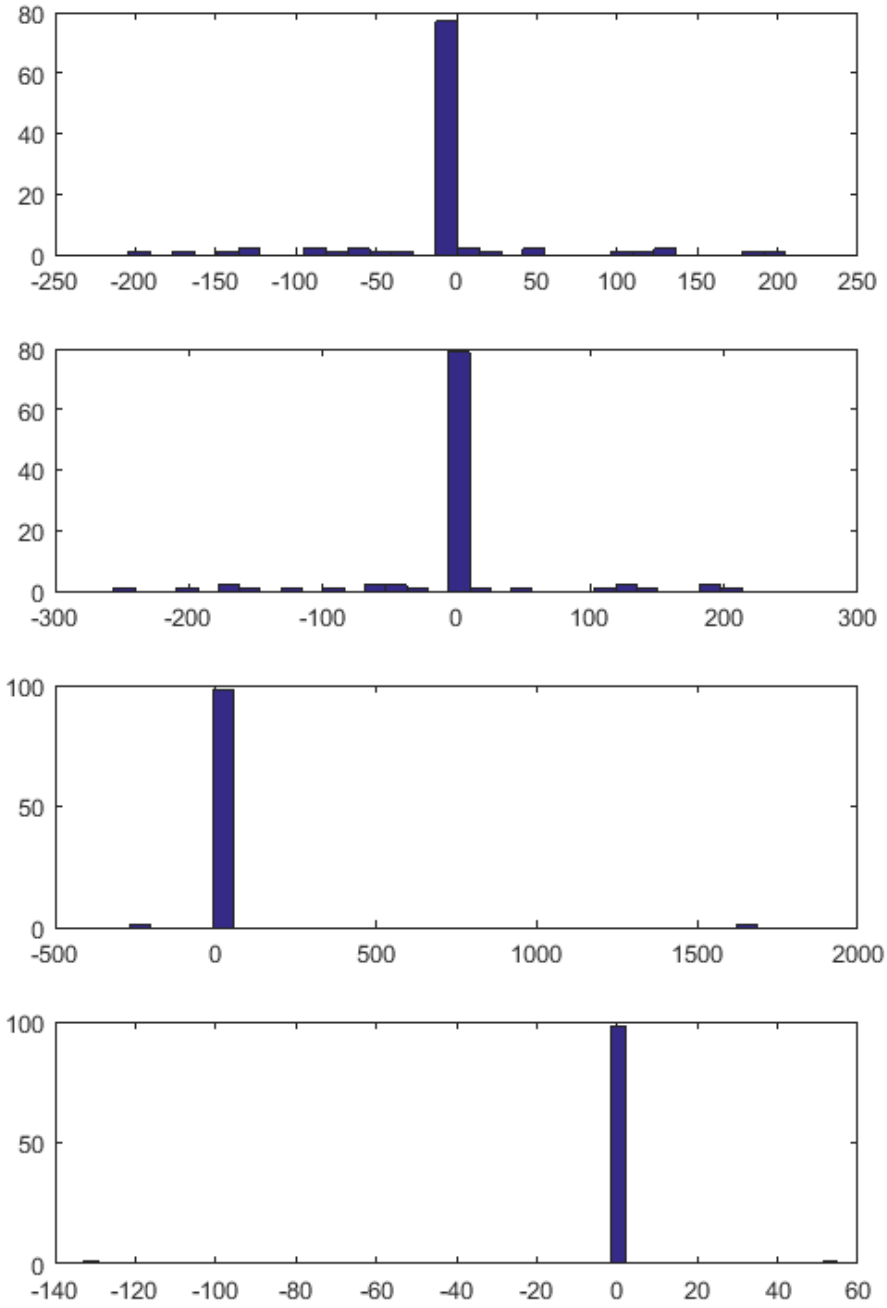
Rysunek 6.1 przedstawia histogramy rozkładu wartości odchyłek dla poszczególnych interwałów dla przypadku użycia falki db5 i głębokości kodowania 1 bit, a rysunek 6.2 - dla falki db5 i głębokości kodowania 2 bity.

Zaproponowany sposób konstruowania kontenerów danych (w 1 skali) i opisu danych (w 2 skali) powoduje, ze ingerencja kodowania w medyczną zawartość elektrokardiogramu jest najbardziej prawdopodobna w obrębie zespołu QRS i załamka T zniekształcając wartości długości zespołu QRS i odcinka QT. Jednocześnie należy zwrócić uwagę, że dokument IEC 60601-2-51 wymaga spełnienia wszystkich czterech warunków podanych tab. 2. Dla uproszczenia prezentacji całościowego rezultatu eksperymentu obliczono więc całościową miarę dokładności wyznaczania długości zdarzeń opartą na interwałach opisywanych przez normę (długości: załamka P, odcinka PQ, zespołu QRS i odcinka QT).

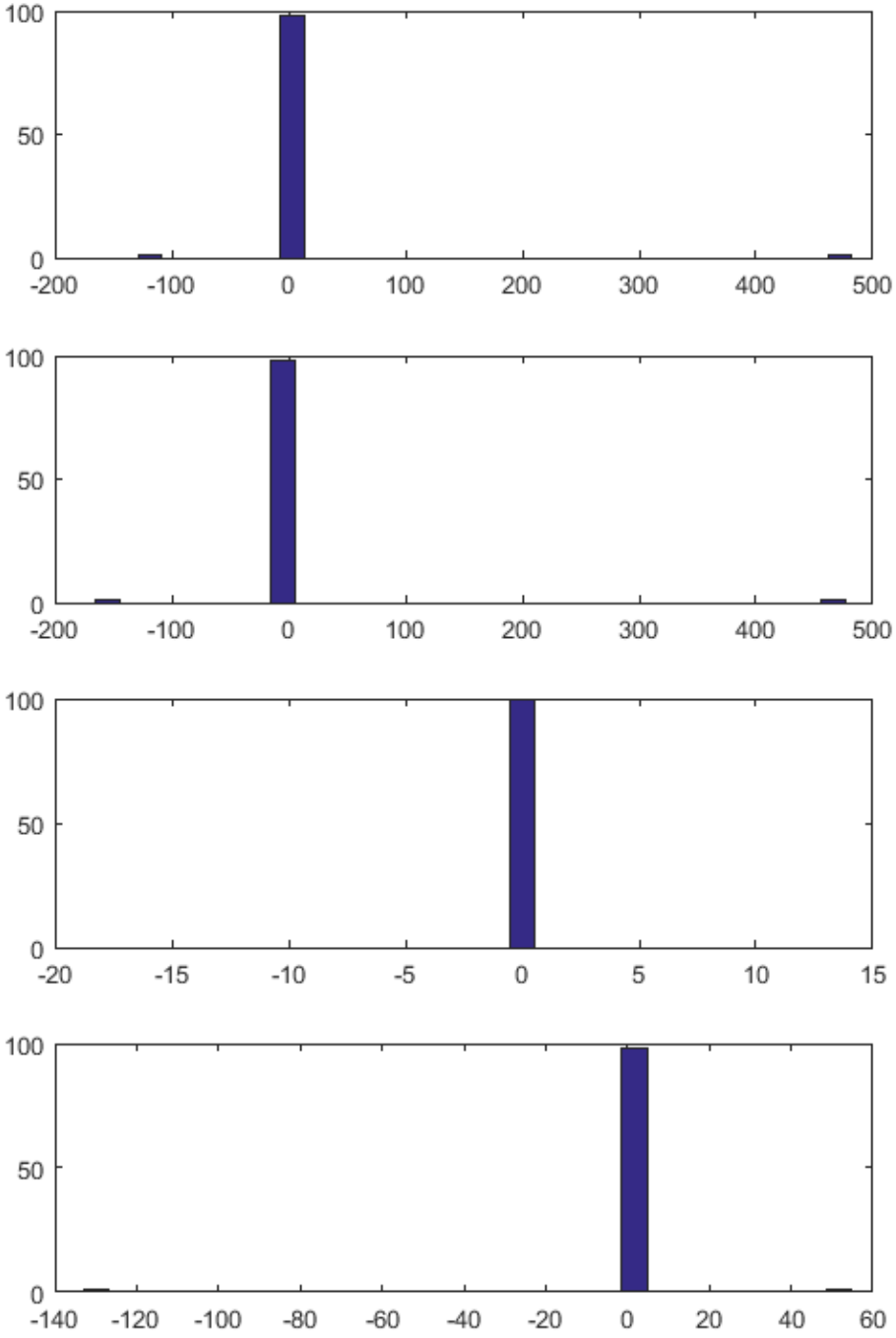
Wartości średnie i odchylenia standardowe tak obliczonej miary dokładności wyznaczania długości zdarzeń dla 100 plików testowych CSE (tab. 1) przedstawia tab. 6.1. Stanowi ona najbardziej syntetyczne podsumowanie przeprowadzonego eksperymentu. Kolorowym tłem wyróżniono falki db5, tekstowy wariant informacji dodatkowej oraz głębokości kodowania 1 i 2 bity dla których histogramy przedstawiają odpowiednio rysunki 6.1 i 6.2.

Rysunek 6.3 przedstawia histogramy rozkładu odchyłek dla 100 plików CSE dla falki Daubechies (db5) i głębokości kodowania 1-5 bitów i głębokości dobieranej automatycznie w zależności od zmierzonego poziomu szumów izolinii. Rysunek 6.4 przedstawia histogramy rozkładu odchyłek dla 100 plików CSE dla falki Symlet (sym6) i głębokości kodowania 1-5 bitów i głębokości automatycznej.

Rysunek 6.5 przedstawia histogramy rozkładu odchyłek dla 100 plików CSE dla głębokości kodowania 1 bit i falek: db5, db10, sym6, sym11, bior2.4 i bior 4.4, a rysunek 6.6 - histogramy rozkładu odchyłek dla 100 plików CSE dla głębokości kodowania 2 bity i falek: db5, db10, sym6, sym11, bior2.4 i bior 4.4



Rys. 6.1. Histogramy rozkładu wartości odchyłek dla długości załamka P, odcinka PQ, zespołu QRS i odcinka QT dla przypadku użycia falki db5 i głębokości kodowania 1 bit



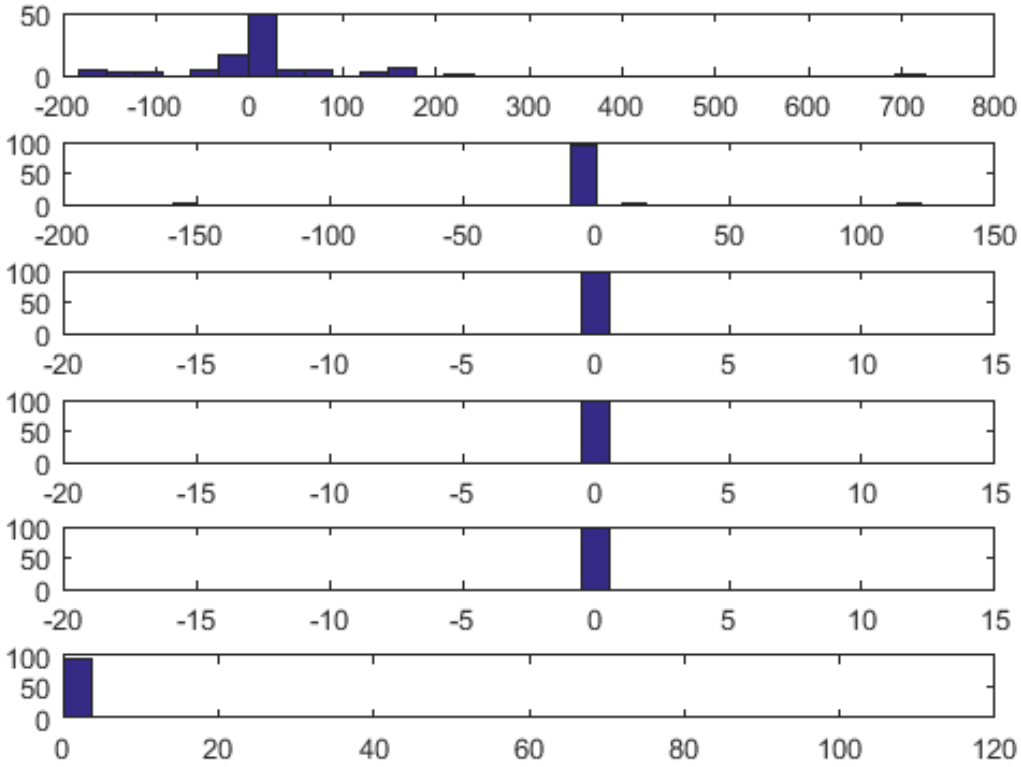
Rys. 6.2 Histogramy rozkładu wartości odchyłek dla długości załamka P, odcinka PQ, zespołu QRS i odcinka QT dla przypadku użycia falki db5 i głębokości kodowania 2 bit

Tab. 6.1 a) Wartości średnie, b) odchylenia standardowe odchyłki długości zdarzeń
a)

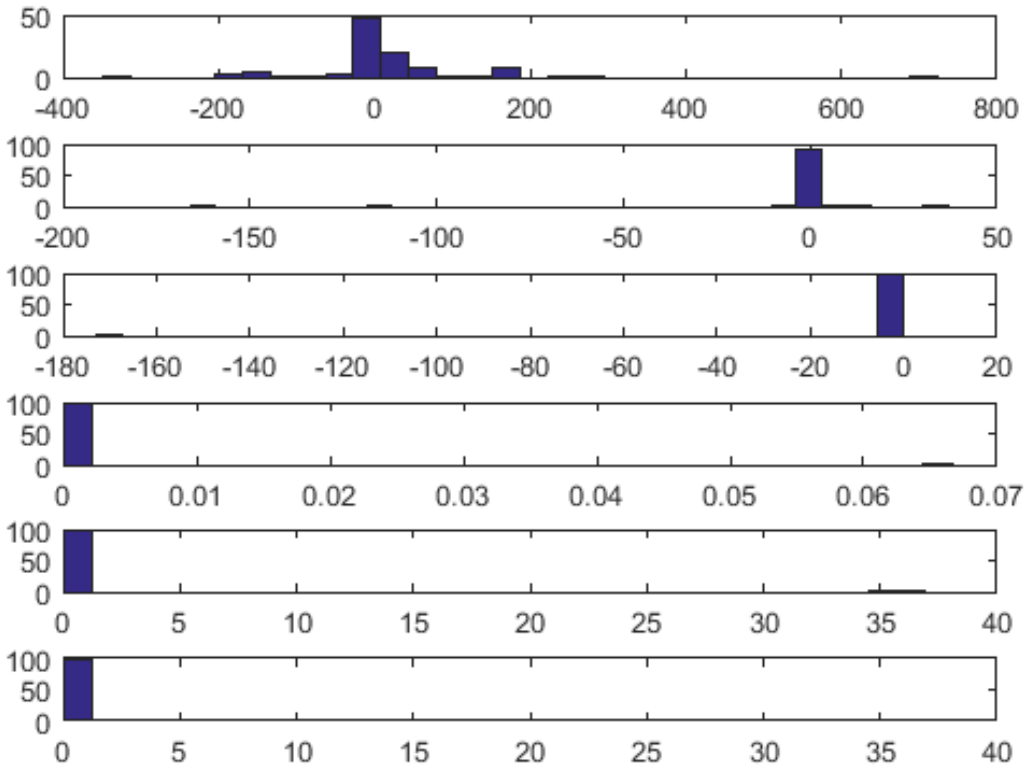
falka	bit	txt/num	P	PQ	QRS	QT	txt/num	P	PQ	QRS	QT
sym6	5	num	0	0	0.0500	-0.0900	txt	0	0	0.0500	-0.0900
sym6	4	num	0	0	0	0	txt	0	0	0	0
sym6	3	num	0	0	0	0	txt	-0.7900	-1.2200	0.1800	0.2500
sym6	2	num	-1.2900	-1.6500	0.1900	0.2000	txt	-1.2900	-1.6500	0.6000	0.0100
sym6	1	num	6.4100	7.2800	12.9400	1.1600	txt	10.5900	10.4000	12.5400	-4.9100
sym6	0	num	0	0	0.0500	-0.0900	txt	0	0	0.0500	-0.0900
sym11	5	num	-0.1400	-0.0900	0.1000	0.0400	txt	0	0	0	0
sym11	4	num	0	0	0	0	txt	0	0	0	0
sym11	3	num	0	0	0	0	txt	0	0	0	0
sym11	2	num	-1.5400	-1.8700	0.9800	0.2000	txt	-0.3000	-0.6000	-0.1200	-0.2700
sym11	1	num	0.7200	0.4500	4.8700	-4.9600	txt	-3.4100	-3.7600	2.3100	-4.4000
sym11	0	num	0	0	0	0	txt	0	0	0.0100	0
bior2.4	5	num	0	0	0	0	txt	0	0	0	0
bior2.4	4	num	0	0	0	0	txt	0	0	0	0
bior2.4	3	num	-0.7900	-1.2200	0.1800	0.2500	txt	-0.7900	-1.2200	0.1800	0.2500
bior2.4	2	num	-2.0800	-2.8700	-1.2100	-1.9200	txt	-1.2900	-1.6500	0.3700	0.2000
bior2.4	1	num	2.8900	2.1800	19.7000	-7.2200	txt	-3.1900	-3.2700	16.4000	-6.6500
bior2.4	0	num	0	0	0	0	txt	0	0	0	0
bior4.4	5	num	0	0	0.0500	-0.0900	txt	0	0	0	0
bior4.4	4	num	0	0	0	0	txt	0	0	0	0
bior4.4	3	num	0	0	0	0	txt	0	0	0	0
bior4.4	2	num	-1.3600	-1.9700	-1.0800	-3.2500	txt	-1.3600	-1.9700	0.5500	-0.9700
bior4.4	1	num	-5.5600	-3.7300	16.7400	-9.7400	txt	-1.5700	-0.9700	16.5000	-2.4800
bior4.4	0	num	0	0	0.0500	-0.0900	txt	0	0	0	0
db5	5	num	0	0	0	0	txt	0	0	0	0
db5	4	num	0	0	0	0	txt	0	0	0	0
db5	3	num	-0.7900	-1.2200	0.1800	0.2500	txt	0	0	0	0
db5	2	num	-2.0800	-2.8700	0.4900	0.6300	txt	3.5300	3.1200	-0.8600	-1.8200
db5	1	num	-0.0300	-0.3000	16.6800	-5.8700	txt	-3.3400	-3.5600	14.1600	-5.0900
db5	0	num	0	0	0	0	txt	0	0	0	0
db10	5	num	0	0	0	0	txt	-0.1400	-0.0900	0.1000	0.0400
db10	4	num	0	0	0	0	txt	0	0	0	0
db10	3	num	-1.2400	-1.2700	0.8300	0.4600	txt	0	0	0	0
db10	2	num	-0.5900	-0.6800	0.0100	-0.1000	txt	-0.5900	-0.6800	-0.0800	-0.9900
db10	1	num	1.0100	-0.3000	7.2600	-15.270	txt	-0.4600	-1.8900	5.5600	-7.7300
db10	0	num	0	0	0.0100	0	txt	0	0	0.0100	0

b)

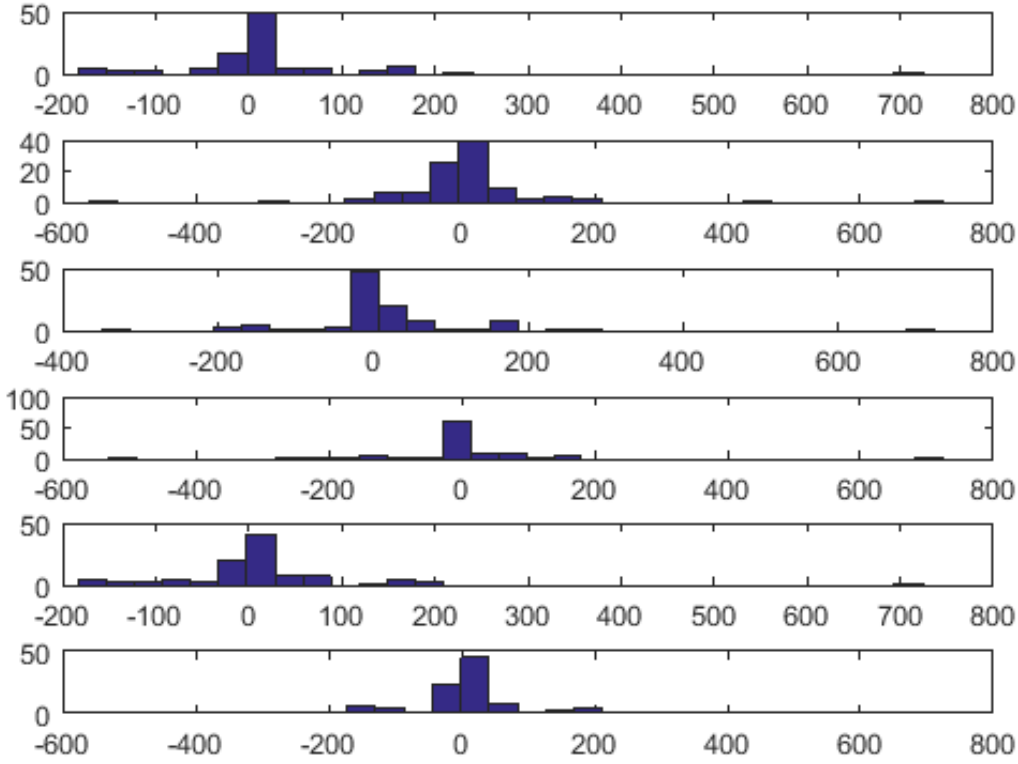
falka	bit	txt/num	P	PQ	QRS	QT	txt/num	P	PQ	QRS	QT
sym6	5	num	0	0	0.5000	0.9000	txt	0	0	0.5000	0.9000
sym6	4	num	0	0	0	0	txt	0	0	0	0
sym6	3	num	0	0	0	0	txt	7.9000	12.2000	1.8000	2.5000
sym6	2	num	12.9000	16.5000	1.8018	1.6143	txt	12.9000	16.5000	3.6763	6.2304
sym6	1	num	79.5317	90.7181	36.9069	57.1195	txt	79.0063	87.1601	38.6289	51.9786
sym6	0	num	0	0	0.5000	0.9000	txt	0	0	0.5000	0.9000
sym11	5	num	1.4000	0.9000	1.0000	0.4000	txt	0	0	0	0
sym11	4	num	0	0	0	0	txt	0	0	0	0
sym11	3	num	0	0	0	0	txt	0	0	0	0
sym11	2	num	20.4941	23.3613	9.4644	14.8834	txt	16.3401	19.6469	2.8259	2.8775
sym11	1	num	46.0946	52.3374	30.5712	57.9620	txt	54.0684	64.3811	30.7971	62.7720
sym11	0	num	0	0	0	0	txt	0	0	0.1000	0
bior2.4	5	num	0	0	0	0	txt	0	0	0	0
bior2.4	4	num	0	0	0	0	txt	0	0	0	0
bior2.4	3	num	7.9000	12.2000	1.8000	2.5000	txt	7.9000	12.2000	1.8000	2.5000
bior2.4	2	num	15.0586	20.4211	14.1345	22.3781	txt	12.9000	16.5000	5.8043	4.5815
bior2.4	1	num	71.3839	81.9864	41.7410	67.6265	txt	57.2949	69.7486	38.6834	65.5577
bior2.4	0	num	0	0	0	0	txt	0	0	0	0
bior4.4	5	num	0	0	0.5000	0.9000	txt	0	0	0	0
bior4.4	4	num	0	0	0	0	txt	0	0	0	0
bior4.4	3	num	0	0	0	0	txt	0	0	0	0
bior4.4	2	num	12.9119	16.7757	14.3708	24.6480	txt	12.9119	16.7757	3.5968	11.0832
bior4.4	1	num	68.1354	83.7035	38.7243	51.2764	txt	66.7579	76.7049	38.4772	58.6306
bior4.4	0	num	0	0	0.5000	0.9000	txt	0	0	0	0
db5	5	num	0	0	0	0	txt	0	0	0	0
db5	4	num	0	0	0	0	txt	0	0	0	0
db5	3	num	7.9000	12.2000	1.8000	2.5000	txt	0	0	0	0
db5	2	num	15.0586	20.4211	2.8867	4.2774	txt	50.0221	50.6304	15.1864	22.5166
db5	1	num	71.1218	79.5817	39.1309	55.3360	txt	57.5037	67.2523	40.8260	52.6828
db5	0	num	0	0	0	0	txt	0	0	0	0
db10	5	num	0	0	0	0	txt	1.4000	0.9000	1.0000	0.4000
db10	4	num	0	0	0	0	txt	0	0	0	0
db10	3	num	12.4000	12.7000	8.4016	10.5977	txt	0	0	0	0
db10	2	num	16.5902	19.6607	1.3521	0.8103	txt	16.5902	19.6607	1.5743	6.2531
db10	1	num	46.1610	54.9627	31.1434	64.5483	txt	47.5570	58.2972	32.4561	55.3138
db10	0	num	0	0	0.0100	0	txt	0	0	0.1000	0



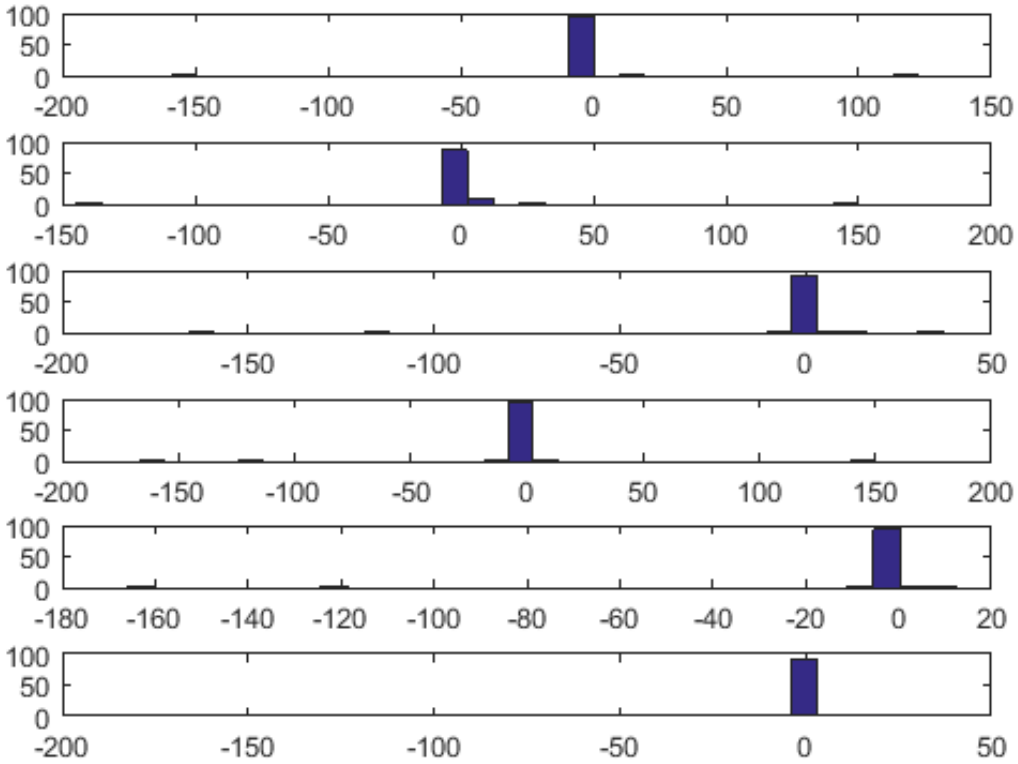
Rys. 6.3.Histogramy rozkładu odchyłek dla 100 plików CSE dla falki db5 i głębokości kodowania 1-5 bitów i głębokości automatycznej



Rys. 6.4 Histogramy rozkładu odchyłek dla 100 plików CSE dla falki sym6 i głębokości kodowania 1-5 bitów i głębokości automatycznej



Rys. 6.5. Histogramy rozkładu odchyłek dla 100 plików CSE dla głębokości kodowania 1 bit i falek: db5, db10, sym6, sym11, bior2.4 i bior 4.4



Rys. 6.6. Histogramy rozkładu odchyłek dla 100 plików CSE dla głębokości kodowania 2 bity i falek: db5, db10, sym6, sym11, bior2.4 i bior4.4

Analiza tab. 6.1 pozwala spostrzec, że dla falek: db5 i bior4.4 przy głębokości kodowania 3-5 bitów, oraz dla falki bior2.4 przy głębokości kodowania 4-5 bitów odchyłka wyznaczania długości zdarzeń w elektrokardiogramie jest zerowa, tzn. proces kodowania sekretu nie ma żadnego wpływu na uzyskiwane wartości podstawowych parametrów diagnostycznych.

Analogiczna analiza prowadzi do wniosku, że dla falek: db10 przy głębokości kodowania 2-4 bitów, falki sym6 przy głębokości kodowania 4 bity oraz sym11 przy głębokości kodowania 3-5 bitów proces kodowania ma wpływ na parametry diagnostyczne pojedynczych plików CSE, ale wartości odchyłki są nieznaczne i nośnik zawierający informację sekretną nadal może być uważany za medycznie równoważny z oryginalnym (w rozumieniu dokumentu IEC60601-2-51).

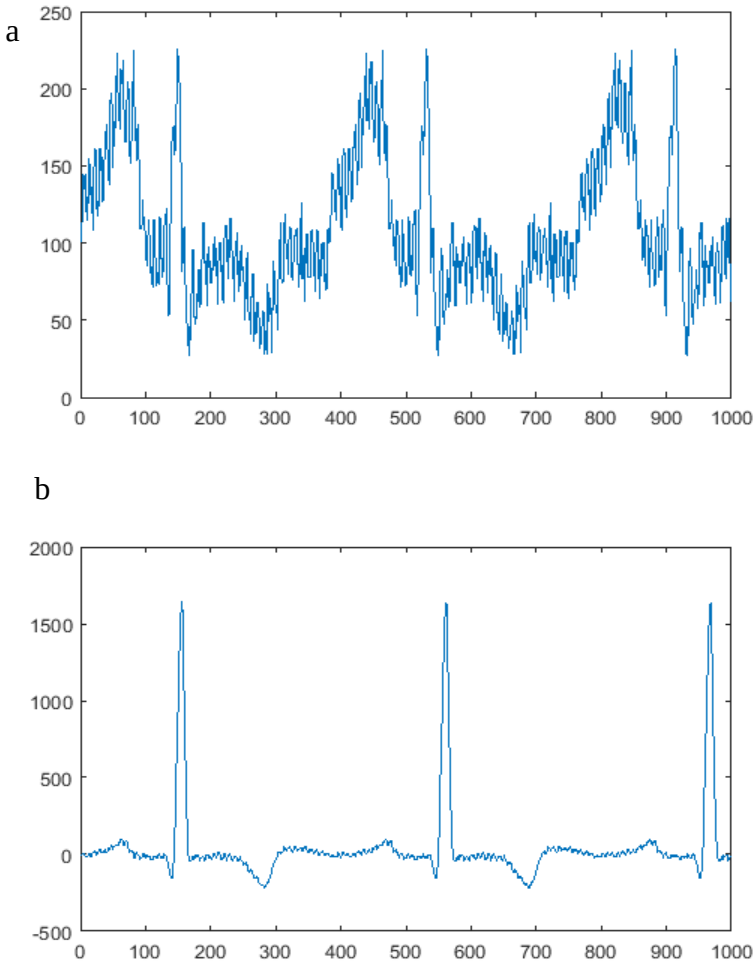
Niestety, dla pozostałych kombinacji falek i bitowej głębokości kodowania odchyłki wyznaczania długości zdarzeń w elektrokardiogramie są zbyt duże, przekraczają wartości podane w tab. 3.2. jako dopuszczalne odchyłki graniczne, co pozbawia zapis EKG wartości diagnostycznej.

Zastosowanie automatycznego doboru bitowej głębokości kodowania informacji dodatkowej na podstawie pomiaru amplitudy szumu przyniósł spodziewany efekt jedynie w przypadku falek biortogonalnych (bior2.4 oraz bior4.4). W przypadku pozostałych falek, odchyłka wyznaczania długości zdarzeń w elektrokardiogramie uzyskana po przeprowadzeniu kodowania z automatycznym doborem bitowej głębokości kodowania była większa niż najmniejsza odchyłka uzyskana z doborem *a priori*.

Analiza przypadków poszczególnych sygnałów z bazy CSE doprowadziła do identyfikacji zapisów szczególnie trudnych. Należą one do trzech kategorii, dla każdej z nich wskazano po dwa przykładowe sygnały i przedyskutowano prawdopodobny mechanizm powstawania błędów:

- duża liczba odchyłek o dużej wartości - nr sygnału CSE 12 i CSE 13,
- duża liczba odchyłek o małej wartości - nr sygnału CSE 7 i CSE 61,
- mała liczba o znacznej wartości - nr sygnału CSE 81 i CSE14.

Pojedyncze ewolucje serca wymienionych zapisów przedstawiono na rysunkach 6.7 – 6.9.

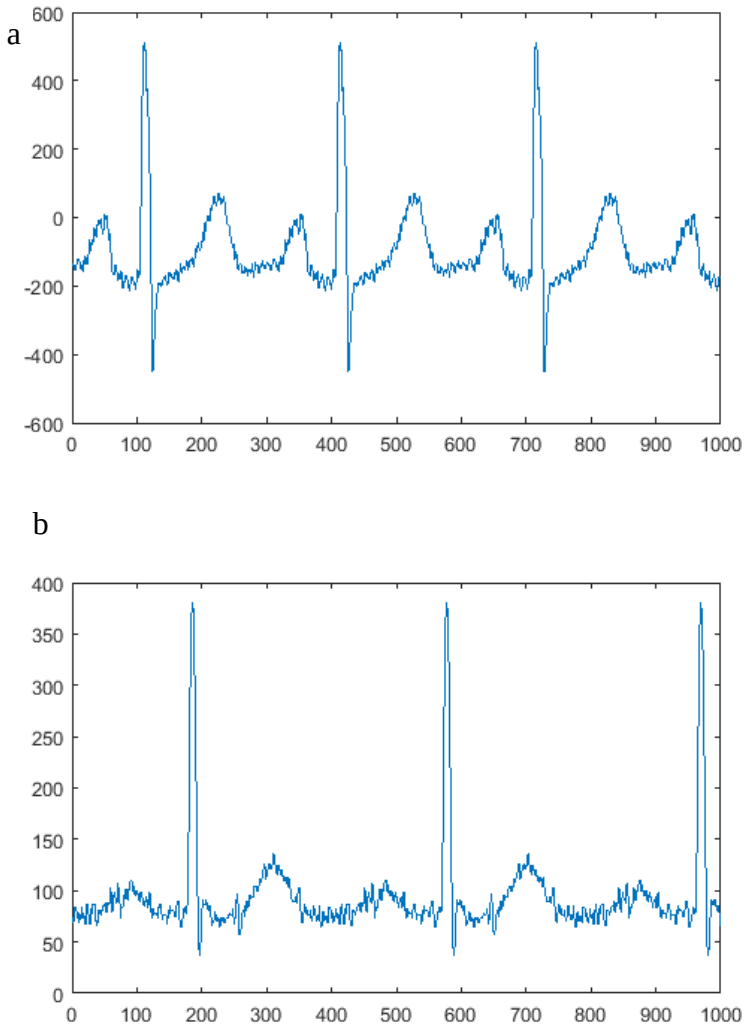


Rys. 6.7. Sygnały a) CSE 12 i b) CSE 13

Zapis CSE 12 charakteryzuje się znacznym poziomem szumu wysokoczęstotliwościowego. Dla bitowej głębokości kodowania 1 i 2, niezależnie od zastosowanej falki, występują istotne rozbieżności w detekcji granic załamków. Automatyczna analiza zapisów ze znakiem wodnym, w których współczynniki reprezentujące szum zostają zamienione przez informację dodatkową, prowadzi do wykrycia granic załamków na granicach odcinków zaszumionych w chwilach niezwiązanych z rzeczywistym występowaniem załamków. Podwyższenie bitowej głębokości kodowania do wartości 3 i powyżej powoduje uzyskanie detekcji bezbłędnej.

Zapis CSE 13 charakteryzuje się niską wartością amplitud załamków P i T. Dla bitowej głębokości kodowania 1 i 2, niezależnie od zastosowanej falki, występują istotne rozbieżności w detekcji granic załamków P i T, podczas gdy granice zespołu QRS o dużej amplitudzie wykrywane są poprawnie. Automatyczna analiza zapisów ze znakiem wodnym powoduje błędną detekcję granic załamków P i T na granicach odcinków odpowiadających

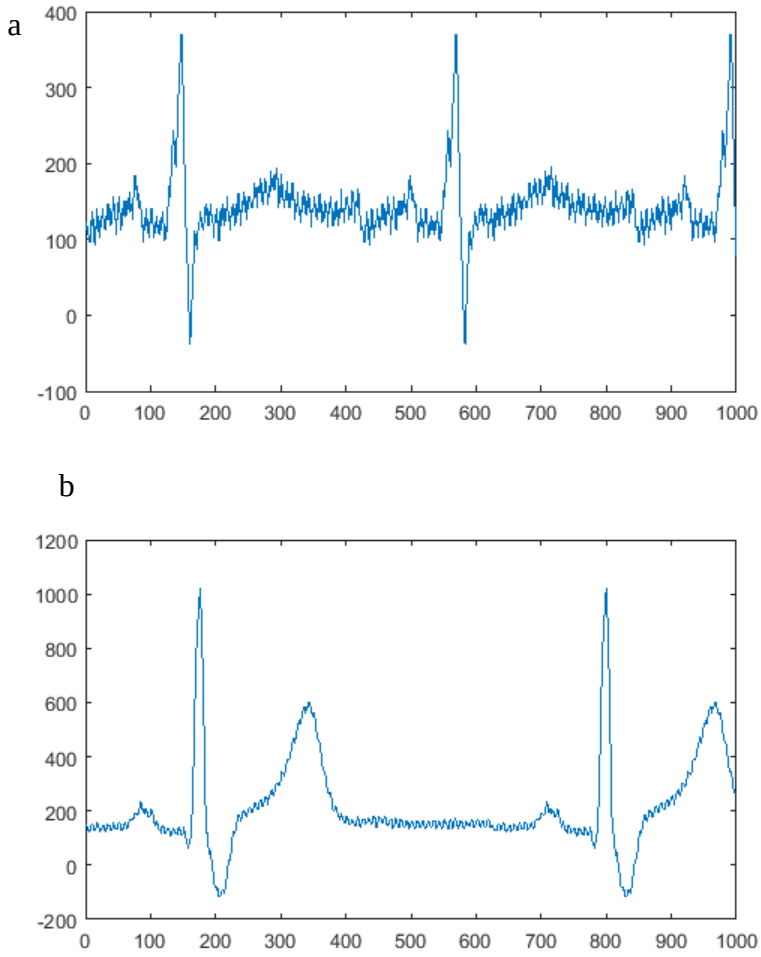
położeniu kontenera danych. Zastosowanie bitowej głębokości kodowania od 3 bitów wzwyż powoduje uzyskanie detekcji bezbłędnej.
W przypadku obu tych sygnałów błędy detekcji granic załamków występujące dla głębokości kodowania 1 i 2 bity przekraczają granice dopuszczone normą IEC.



Rys. 6.8. Sygnały a) CSE 7 i b) CSE 61

Zapis CSE 7 oraz zapis CSE 61 charakteryzują się znacznym poziomem szumu na linii izoelektrycznej (tj. na odcinku PQ). W przypadku zapisu CSE 7 automatyczna analiza prowadzi do detekcji punktów granicznych załamków z niewielką niedokładnością dla falek db5 przy głębokości kodowania 1 i 2 bity, dla bior2.4 - 1 i 3 bity, dla bior4.4 – 1 bit. Dla pozostałych falek niedokładność jest nieco większa dla głębokości 1 bit, ale występuje także dla pozostałych głębokości. W konsekwencji dodanie znaku wodnego dla tego sygnału prowadziło do błędów detekcji granic załamków w 21 na 36 wariantów, ale były to błędy w granicach normy IEC.

Zapis CSE 61 zawiera rytmiczne artefakty i prawdopodobnie ich modyfikacja podczas procesu kodowania powoduje błędne wyznaczanie granic załamków w przypadku głębokości równej 1 i 2 bity niezależnie od użytej falki. Również w tym przypadku, pomimo znacznej liczby niedokładnie wyznaczonych punktów granicznych, wszystkie niedokładności mieściły się w granicach normy IEC.



Rys. 6.9. Sygnały a) CSE 81 i b) CSE 14

Zapis CSE 81 charakteryzuje się obecnością artefaktu, prawdopodobnie przydźwięku sieciowego, o stałej częstotliwości. Powoduje to obecność okresowo powtarzalnego wzorca współczynników w skalach 1 i 2, którego statystyka wartości nie jest podobna do oczekiwanej charakterystyki szumu. Analiza zapisu ze znakiem wodnym prowadzi do błędnej lokalizacji załamków tylko dla głębokości kodowania równej 1 bit. W przypadku falek db10, sym11 i bior2.4 różnice są na granicy normy IEC, natomiast dla db5, sym6 i bior4.4 znacznie ją przekraczają, powodując, że sygnał ze znakiem wodnym jest medycznie bezwartościowy.

Zapis CSE 14 charakteryzuje się niskim poziomem szumu, ale punkt końcowy zespołu QRS jest trudny do wyznaczenia. Wszelkie niedokładności występujące na etapie analizy zapisu oryginalnego powodują niewłaściwe umieszczenie kontenera danych i w efekcie zastąpienie przez informacje dodatkowe istotnej treści diagnostycznej. W konsekwencji analiza zapisu ze znakiem wodnym przynosi błędy lokalizacji załamków tylko dla głębokości kodowania równej 1 bit. W przypadku falek db5 i bior2.4. są to małe błędy, Mieszczące się w granicach tolerancji IEC. W pozostałych przypadkach błędy są duże i dyskwalifikują zapis.

Średnia wartość odchyłki otrzymanej z użyciem poszczególnych rodzajów falek została porównana za pomocą testu parametrycznego *t* dla dwóch zbiorów niezależnych. Przyjęta hipoteza zerowa zakładała stwierdzenie, że zbiory wartości odchyłek uzyskanych z użyciem danej pary falek mają identyczną wartość średnią. Założony poziom prawdopodobieństwa popełnienia błędu polegającego na odrzuceniu hipotezy zerowej p=0,05. Uzyskane wyniki testu parami wszystkich użytych rodzajów falek (tab. 6.2 i 6.3) nie uprawniają do odrzucenia hipotezy zerowej w żadnym z przypadków.

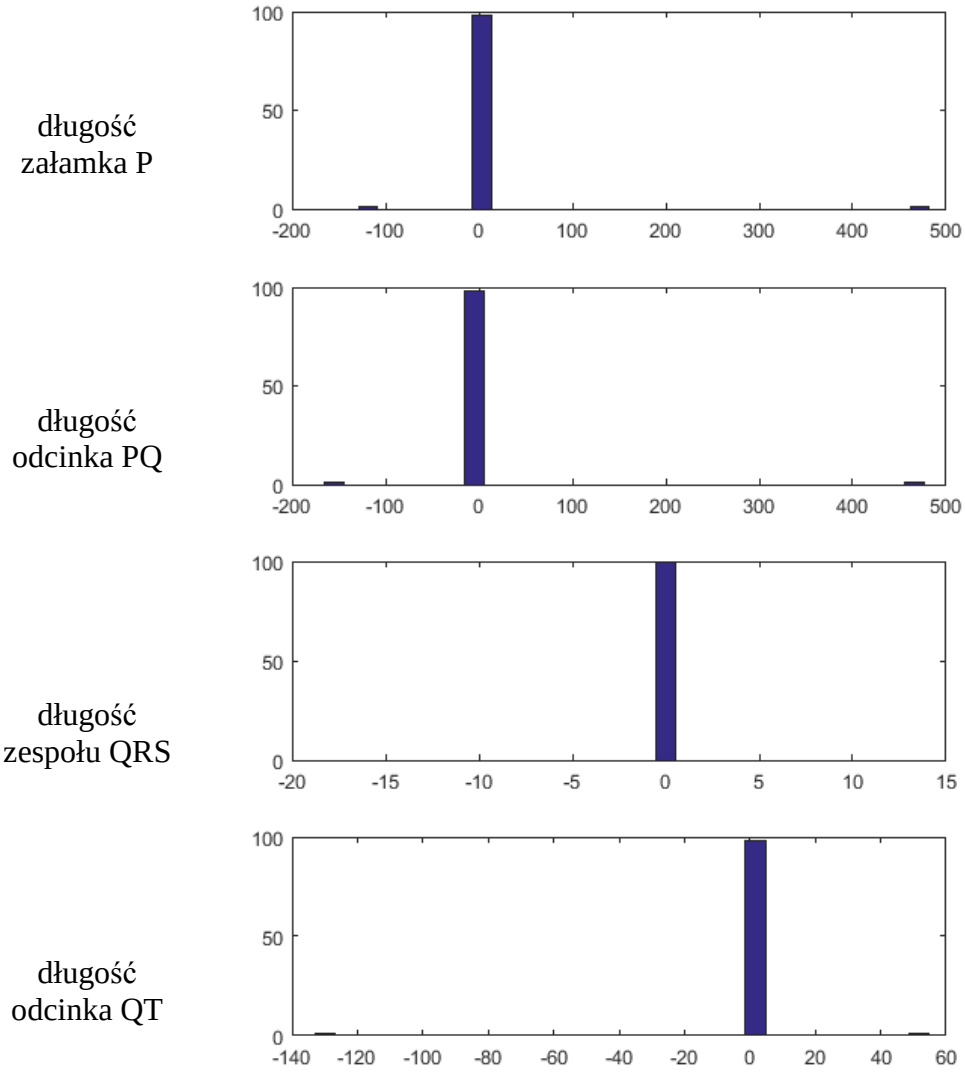
Tab. 6.2. Wynik testu *t* dla dwóch zbiorów niezależnych będących odchyłkami pozycjonowania załamków powstałymi na skutek kodowania informacji dodatkowej z użyciem falek różnych rodzajów dla głębokości kodowania 1 bit

Falka	**db5**	**db10**	**sym6**	**sym11**	**bior2.4**	**bior4.4**
db5	-	0	0	0	0	0
db10		-	0	0	0	0
sym6			-	0	0	0
sym11				-	0	0
bior2.4					-	0
bior4.4						-

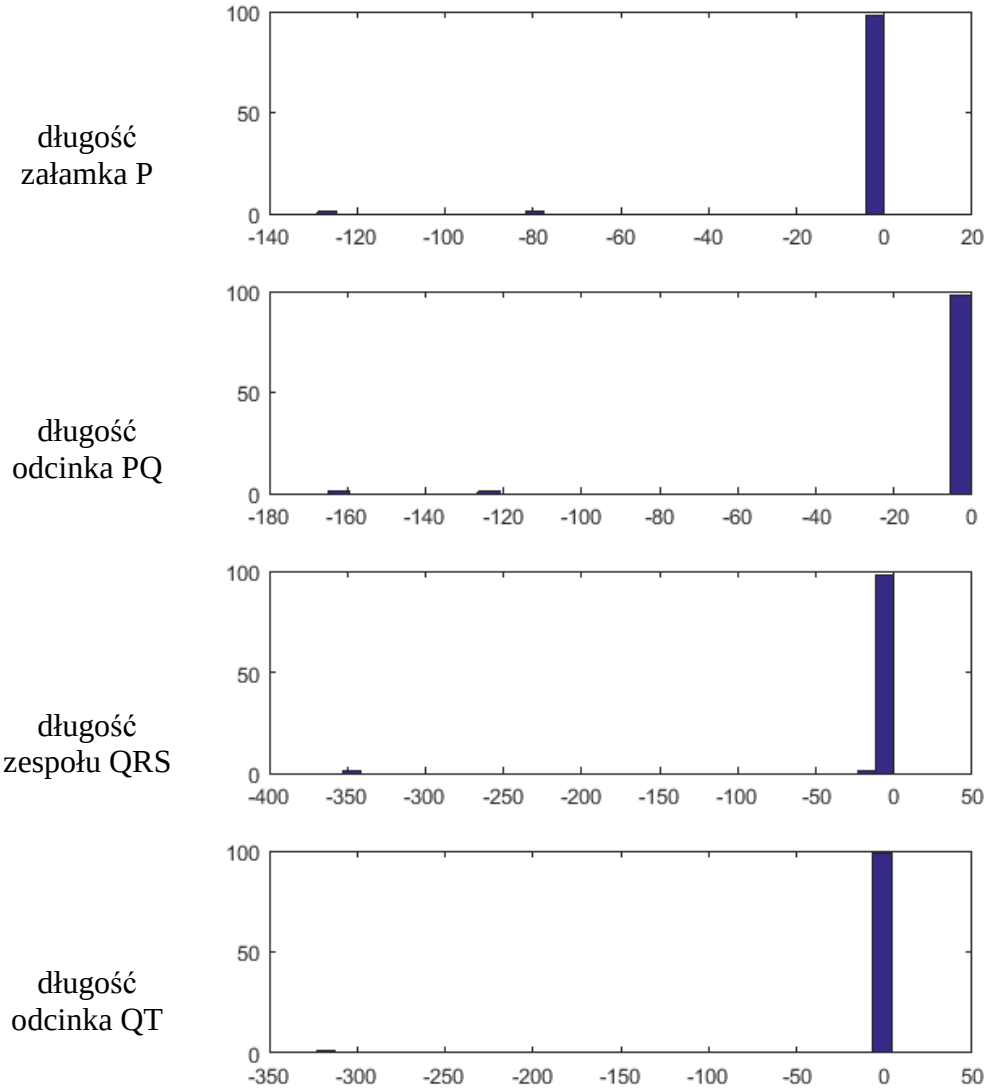
Tab. 6.3. Wynik testu *t* dla dwóch zbiorów niezależnych będących odchyłkami pozycjonowania załamków powstałymi na skutek kodowania informacji dodatkowej z użyciem falek różnych rodzajów dla głębokości kodowania 2 bit

Falka	**db5**	**db10**	**sym6**	**sym11**	**bior2.4**	**bior4.4**
db5	-	0	0	0	0	0
db10		-	0	0	0	0
sym6			-	0	0	0
sym11				-	0	0
bior2.4					-	0
bior4.4						-

Dodatkowy test opisany w podrozdziale 5.3 został przeprowadzony w celu zbadania wpływu rozkładu statystycznego w ciągu kodów informacji sekretnej. Otrzymane rezultaty przedstawia tab. 6.1 powyżej. Rysunki 6.10 i 6.11 przedstawiają porównanie przykładowych histogramów rozkładu odchyłek dla 100 plików CSE dla głębokości kodowania 2 bity i falki db5 dla informacji sekretnej w postaci ciągu znaków i ciągu cyfr.



Rys. 6.10. Histogramy rozkładu odchyłek dla 100 plików CSE dla głębokości kodowania 2 bity i falki db5 dla informacji sekretnej w postaci ciągu znaków



Rys. 6.11. Histogramy rozkładu odchyłek dla 100 plików CSE dla głębokości kodowania 2 bity i falki db5 dla informacji sekretnej w postaci ciągu cyfr

Dla sprawdzenia czy zbiory wartości odchyłek uzyskanych dla informacji sekretnej w postaci ciągu znaków i ciągu cyfr różnią się. Wykonano test istotności t-Studenta dla każdej kombinacji bitowej głębokości kodowania i rodzaju użytej falki [t-distribution]. Rezultaty tego testu dla parametrów długość zespołu QRS oraz długość odcinka QT przedstawia tab. 6.4. Parametry te wybrano ze względu na ich największą podatność na zniekształcenia spowodowane osadzaniem znaku wodnego.

Tab. 6.4 a) Porównanie zbiorów odchyłek długości **zespołu QRS** dla informacji sekretnej w postaci ciągu znaków i ciągu cyfr (na poziomie istotności p=0,05)

falka/bit	**1**	**2**	**3**	**4**	**5**	**auto**
db5	1	1	0,8413	0	0	0
db10	1	1	1	0	0,1587	0,5
sym6	1	0,1585	0,1587	0	0,5	0
sym11	1	1	0	0	0,8413	0,1587
bior2.4	1	0	0,5	0	0	0
bior4.4	1	0	0	0	0,8413	0,8413

Tab. 6.4 b) Porównanie zbiorów odchyłek długości **odcinka QT** dla informacji sekretnej w postaci ciągu znaków i ciągu cyfr (na poziomie istotności p=0,05)

falka/bit	**1**	**2**	**3**	**4**	**5**	**auto**
db5	0	1	0,8413	0	0	0
db10	0	1	1	0	0,1587	0
sym6	1	1	0,1587	0	0,5	0
sym11	0	1	0	0	0,8413	0
bior2.4	0	0	0,5	0	0	0
bior4.4	0	0	0	0	0,1587	0,1587

W większości przypadków na poziomie istotności p=0,05 brak podstaw do odrzucenia hipotezy zerowej mówiącej o braku różnic pomiędzy odchyłkami spowodowanymi przez informację dodatkową w postaci tekstu i w postaci cyfr. Jest tak dla wszystkich wariantów kodowania z głębokością 4 bitów, dla falek biortogonalnych przy głębokości 2 bitów, dla falek sym11 i bior4.4 przy głębokości 3 bitów oraz dla falek db5 i bior2.4 przy głębokości 5 bitów. Rozróżnienie wpływu zawartości informacji dodatkowej na parametr długości zespołu QRS i długości odcinka QT jest możliwe właściwie tylko przy głębokości kodowania 1 bit. W pozostałych przypadkach wpływ ten jest bardzo podobny, a często – identyczny.

7. Podsumowanie

7.1 Weryfikacja tezy rozprawy doktorskiej

W rozdziałach 4-7 zaproponowano metodę kodowania informacji dodatkowej znaku wodnego) w strukturze cyfrowego elektrokardiogramu oraz opisano przeprowadzone badania stopnia zachowania informacji diagnostycznej nośnika EKG ze znakiem wodnym w rozmaitych wariantach bazy dekompozycji (falki-matki), bitowej głębokości kodowania, rodzaju informacji dodatkowej. Ocena stopnia zachowania informnacji diagnostycznej została przeprowadzona przy użyciu przemysłowego standardu IEC60601-2-51 i bazy sygnałów CSE. Badania te wskazują w jakich przypadkach możliwe jest kodowanie informacji dodatkowej bez zakłócenia zawartości diagnostycznej oraz wskazują w jakich okolicznościach kodowanie może prowadzić do zniekształceń. Przeprowadzone badania numeryczne wskazały na zalety, a także ograniczenia zaproponowanej metody.

Teza dotycząca tego, że dodatkowe informacje diagnostyczne lub administracyjne mogą być dołączone do struktury cyfrowego elektrokardiogramu w sposób nie zniekształcający informacji diagnostycznej została udowodniona. Co prawda były przypadki, kiedy to zakodowana wiadomość mogła wpłynąć na zawartość diagnostyczną, ale zostały one zidentyfikowane i wyjaśnione. Wśród czynników mających wpływ na jakość nośnika EKG z zakodowanym znakiem wodnym można wyróżnić:

- Głębokość bitową kodowania informacji dodatkowej; gdy zastosowano głębokość bitową powyżej 3 bitów na próbkę, statystyka wartości informacji dodatkowej przypominała statystykę szumu i zniekształcenia praktycznie nie występowały.
- Rodzaj informacji; zakładając hipotezę o braku istotnej statystycznie różnicy odchyłek podczas kodowania ciągu znaków tekstowych i numerycznych sporadycznie otrzymywano podstawy do jej odrzucenia, a praktycznie nie dostrzega się różnicy.
- Zawartość elektrokardiogramu; w niektórych przypadkach dla niektórych sygnałów EKG wartość diagnostyczna zakodowanej informacji jest gorsza a w niektórych przypadkach pozostaje bardzo dobra.

Zasadnicze osiągnięcie naukowe przeprowadzonych prac polega na:

- zaproponowaniu metody kodowania informacji dodatkowej w postaci znaku wodnego w strukturze cyfrowego elektrokardiogramu w dziedzinie czasowo-skalowej z użyciem różnych baz dekompozycji,
- zaproponowanie metody projektowania i opisu kontenerów danych oraz zależności ich parametrów od lokalnych własności elektrokardiogramu nośnika,

– weryfikacja zaproponowanej metody z użyciem przemysłowego standardu jakości stosowanego dla automatycznej diagnostyki elektrokardiograficznej (IEC60601-2-51),
– analiza statystyczna wyników eksperymentu numerycznego i sformułowanie wniosków dotyczących zakresu stosowalności proponowanej metody.

Ponadto, niniejsza praca doktorska oprócz badań przeprowadzonych przez Autorkę, zawiera również przegląd publikacji dotyczących tematu kodowania informacji w EKG. Są tu opisane metody kodowania, jak również narzędzia matematyczne, bazy danych z których można pobrać sygnał EKG jak również część informacji dotyczących telemedycyny.

7.2 Dalsze plany badawcze

Mimo iż Autorka starała się wyczerpać temat kodowania informacji w cyfrowym elektrokardiogramie, podczas badań dostrzeżono nowe możliwości dalszych prac badawczych. Przykładowo, badania przeprowadzono jedynie na sygnałach nadkomorowych, zgodnie z wymaganiami normy IEC, podczas gdy w bazie CSE są także zapisy innych morfologii z punktami referencyjnymi granic załamków. Warto zatem w przyszłości ponowić badania i przeprowadzić analizę co najmniej dla ewolucji komorowych z bazy CSE, pominiętych w tabeli 3.1.

Również zważywszy na sam fakt ciągłego rozwoju telemedycyny warto zastanowić się nad tym w jakim kierunku jej rozwój może być wsparty przez kodowanie informacji dodatkowych w strukturze cyfrowego EKG. Jak już zostało opisane w innych pracach (które zostały przytoczone przez Autorkę w niniejszej rozprawie) ich autorzy zauważyli, że kodowanie dodatkowych informacji w strukturze cyfrowego elektrokardiogramu ma liczne zalety, np. łatwość przesyłania spowodowana integralnością informacji z oryginalnym sygnałem, łatwość archiwizacji, oraz ograniczenie ryzyka dezintegracji np. informacji na temat danych osobowych, w porównaniu z systemami, w których zostaną one przesłane osobno.

Niniejsza rozprawa jest zbiorem informacji dotyczących kodowania informacji dodatkowych w sygnale EKG ale nie tylko. Autorka tej pracy ma nadzieję, że jej wkład w postaci wniosków dotyczących warunków utrzymania jakości zakodowanego sygnału zainspiruje innych badaczy zajmujących się w przyszłości tematem steganografii. Wśród możliwych ulepszeń warto zwrócić uwagę na poprawę procedury detekcji szumu i automatycznego doboru bitowej głębokości kodowania.

Ważne będzie także uważne obserwowanie rozwoju telemedycyny pod kątem usprawniania transmisji jak również dokładności przesyłanych danych używając ciągle ulepszanych podręcznych urządzeń. Pod kątem tych obserwacji można w pewnym momencie zastanowić się czy jest miejsce na wdrożenie takiego zintegrowanego kodowania dodatkowych informacji w strukturze cyfrowego sygnału.

Autorka niniejszej rozprawy skupiła się głównie na kodowaniu w strukturze EKG. Jej badania prowadzone były pod kątem tego właśnie obszaru. Nie sprawdzała czy takie kodowanie można wykorzystać w innych cyfrowych sygnałach medycznych, np. w EEG. Ewentualne zastosowania opisanych metod do innych biosygnałów wymagają odrębnych badań.

Można również w przyszłości zastanowić się jak kodować informacje. Może trzeba tu użyć osobnego urządzenia kodującego albo wpisać algorytm do cyfrowego elektrokardiografu, a po stronie odbiorcy odtworzyć za pomocą dekodera.

8. Literatura

[Abo-Zahhad M. M. i in., 2014] Abo-Zahhad M. M.: Abdel-Hamid T. K., Mohamed A. M.: Compression of ECG Signals Based on DWT and Exploiting the Correlation between ECG Signal Samples. Int. J. Communications, Network and System Sciences, 7, str.53-70, 2014.

[Ahuja B. S. i in., 2010] Ahuja B. S., Frooq O., Kaur S., Singhal R.: Digital watermarking of ECG data for secure wireless communication, International Conference on Recent Trends in Information, Telecommunication and Computing, IEEE Computer Society, 2010.

[Ansair N. i in., 2008] Ansair N., Lin X., Ni Z., Shi Y. Q., Su W., Sun Q.: Robust lossless image data hiding designed for semi-fragile image authentication. IEEE Transactions on Circuits and Systems forVideo Technology, vol. 18, no. 4, pp. 497-509, 2008.

[Augustyniak P., 2012] Augustyniak P.: Analysis of ECG bandwidth gap as a possible carrier for supplementary digital data.Proceedings of the 39th Computing in Cardiology conference pp. 73-76, 2012.

[Augustyniak P., 2014] Augustyniak P.: Encoding the electrocardiogram details in the host record's bandgap for authorization-dependent ECG quality. Computing in Cardiology, vol. 41, 465-468, 2014.

[Augustyniak P., 2003] Augustyniak P.: Transformacje Falkowe w zastosowaniach elektrodiagnostycznych. Uczelniane Wydawnictwa Naukowo-Dydaktyczne AGH, ISBN 83-89388-10-3, Kraków, 2003.

[Augustyniak P. i Świerkosz A., 2015] Augustyniak P. i Świerkosz A.: Kodowanie informacji dodatkowych w strukturze cyfrowego elektrokardiagramu - projekt metody [Appending auxiliary information within the digital ECG structure - concept of metod]. Warszawa: Biocybernetyka i inżynieria biomedyczna : XIX krajowa konferencja naukowa; s.21, 2015.

[Bender W. i in., 1996] Bender W., Gruhl D., Morimoto N., Lu A.: Techniques for dataHiding, IBM Systems Journal, Vol 35, Nos 3&4, str. 313-336,1996.

[Białasiewicz J. T., 2000] Białasiewicz J. T.: Falki i aproksymacje. Wydawnictwo Naukowo-Techniczne, 2000.

[Blakley G. R., 1979] Blakley G. R.: Safeguarding cryptographic keys. Proceedings of AFIPS National Computer Conference, vol. 48, pp. 313-317, 1979.

[Buchmann J. A., 2006] Buchmann J. A.: Wprowadzenie do kryptografii. Warszawa: Wydawnictwo Naukowe PWN, 2006.

[Chan C. S. i in., 2009] Chan C. S., Chang C. C., Lin P. Y.: Secret Image Sharing with Reversible Steganography, 2009 International Conference on Computational Intelligence and Natural Computing. IEEE 2009.

[Chen L. H. i Wu C. C., 1998] Chen L. H., Wu C. C.: A study on visual cryptography. Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.

[Chen T. S. i Yang C. N., 2006] Chen T. S., Yang C. N.: Reduce Shadow Size in Aspect Ratio Invariant Visual Secret Sharing Schemes using a Square Block-wise Operation. Patter Recognition, Vol. 39, Issue 7, pp. 1300-1314, 2006.

[Chen T. S. i Yang C. N., 2007] Chen T. S., Yang C. N.: An image secret sharing scheme with the capability of previewing the secret image. IEEE 2007.

[Chen B. i Wornell G. W., 2001] Chen B., Wornell G. W.: Quantization Index Modulation Methods for Digital Watermarking and Information Embedding of Multimedia. Journal of VLSI Signal Processing 27, str. 7–33, 2001.

[Cimato S. i in., 2006] Cimato S., Prisco R., Santis A.: Probabilistic visual cryptography schemes. The computer Journal, Vol. 49, pp. 97-107, 2006.

[Dash P. K., 2002] Dash P. K.: Electrocardiogram monitoring. Indian :J Anaesth;46 (4) : s. 251-260, 2002.

[Devi A. i Kumar S., 2016] Devi A.,Kumar S.: Novel Audio Steganography Technique for ECGSignals in Point of Care Systems(NASTPOCS).IEEE International Conference on Cloud Computing in Emerging Markets.

[Eisen P. A. i Stinson D. R., 2002] Eisen P. A., Stinson D. R.: Threshold visual cryptography schemes with specified whiteness. Designs, Codes and Cryptography, Vol. 25, Issue 1, pp. 15-61, 2002.

[Engin M. i in., 2005] Engin M., Cidam O.,Engin E. Z.: Wavelet Transformation Based WatermarkingTechnique for Human Electrocardiogram (ECG). Journal ofMedical Systems, Vol. 29, No. 6, December 2005.

[Grajek M. i Gralewski L., 2009] Grajek M., Gralewski L.: Narodziny kryptologii matematycznej. Warszawa: Wydawnictwo Naukowe Semper, 2009.

[Heksel K., 2001] Heksel K.: Metody kompresji EKG z wykorzystywaniem dekompozycji czasowo – częstotliwościowej. Rozprawa doktorska, AGH 2001.

[Holewa K. i in.,2015] Holewa K, Izworski A., Łatas W., Nawrocka A., Orzechowski T. S., Pachana T., Panek D., Stojek J., Świerkosz A., Wesół J.: Wybrane zagadnienia analizy sygnałów, modelowania i sterowania w układach mechanicznych i biomechanicznych.Monografie Katedry Automatyzacji Procesów AGH w Krakowie,2015.

[Hsueh N. L. i Lin C. C., 2008] Hsueh N. L., Lin C. C.: A lossless data hiding scheme based on three-pixel block differences, Pattern Recognition, vol. 41, no. 4, pp. 1415-1425, 2008.

[Ibaida A. i in, 2011] Ibaida A., Khalil I.,VanSchyndel R.: A low complexity high capacity ECG signal watermark for wearable sensor-net health monitoring system, Computing in Cardiology; 38:393-396, 2011,ISSN 0276-6574.

[Ibaida A. i Khalil I., 2013] IbaidaA., Khalil I.: Wavelet-Based ECG Steganography for ProtectingPatient Confidential Information in Point-of-Care Systems. IEEE Transactions On Biomedical Engineering, Vol. 60, No. 12, December 2013.

[Jero S. E. i Ramu P., 2016] Jero S. E., Ramu P.: Curvelets-Based ECG Steganography For Data Security. Electronics Letters 18th February 2016 Vol. 52 No. 4 Pp. 283–285.

[Józefczyk I., 2005] Józefczyk I.: Dyskretna transformata Falkowa dla wybranego modelu symulacyjnego sygnału wibroakustycznego. Diagnostyka '34, str. 137-141 vol. 34, 2005.

[Kahn D., 2004] Kahn D.: Łamacze kodów. Warszawa: Wydawnictwo Naukowo-Techniczne, 2004.

[Kwiatkowski W., 2009] Kwiatkowski W.: Wprowadzenie do kodowania. Warszawa: Wydawnictwa Wojskowej Akademii Technicznej, 2009.

[Laih C. S. i Yang C. N., 2000] Laih C. S., Yang C. N.: New colored visual secret sharing schemes. Designs, Codes and Cryptography, Vol. 20, Issue 3, pp. 325-335, 2000.

[Li P. i in., 2010] Li P., Ma P., Su X.: Image secret sharing and hiding with authentication. 2010 First International Conference on Pervasive Computing, Signal Processing and Applications, IEEE 2010.

[Lin C. C. i Tsai W. H., 2003] Lin C. C., Tsai W. H.: Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, pp. 349-358, 2003.

[Lin J. C. i Thien C. C., 2002] Lin J. C.,Thien C. C.: Secret image sharing. Computers & Graphics, Vol. 26, pp. 765-770, 2002.

[Mamaghanian H i in., 2011] Mamaghanian H, Khaled N., Atienza D., Vandergheynst P.: Compressed Sensing for Real-Time Energy-Efficient ECG Compression on Wireless Body Sensor Nodes. IEEE Transactions On Biomedical Engineering, Vol. 58, No. 9, September 2011, str. 2456-2466.

[McSharry P. E. i in., 2003] McSharry P. E., Clifford G. D., Tarassenko L., Smith L. A.: A Dynamical Model for Generating Synthetic Electrocardiogram Signals. IEEE Transactions On Biomedical Engineering, vol. 50, no. 3, march 2003.

[Nabiyev V. V. i in., 2008] Nabiyev V. V., Ulutas G., Ulutas M., Yazici R.: (2, 2)-Secret Sharing Scheme with Improved Share Randomnes. IEEE 2008.

[Noar M. i Shamir A., 1995] Noar M., Shamir A.: Visual cryptography. Advances in Cryptology: Eurocrypt' 94, Spring-Verlag, Berlin, pp. 1-12, 1995.

[Rak R. J. i Majkowski A., 2004] Rak R. J., Majkowski A.: Czasowo-częstotliwościowa analiza sygnałów. Przegląd Elektrotechniczny R. 80 NR 5/2004.

[Rodriguez J. J. i Thodi D. M., 2007] Rodriguez J. J., Thodi D. M.: Expansion embedding techniques for reversible watermarking IEEE Transactions on Image Processing, vol. 16, no. 3, pp. 721-730, 2007.

[Sankari V. i Nandhini K., 2014] Sankari V. i Nandhini K.:Steganography Technique to Secure Patient Confidential information using ECG Signal. ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India, IEEE, 2014.

[Shamir A., 1979] Shamir A.: How to share a secret. Communications of the ACM, vol. 22. no. 11, pp. 612-613, 1979.

[Shyu S. J., 2006] Shyu S. J.: Efficient visual secret sharing scheme for color images. Patter Recognition, Vol. 39, Issue 5, pp. 866-880, 2006.

[Singh S., 2001] Singh S.: The code book.New York: Delacorte Press, 2001.

[Singh Y. N. i in., 2012] Singh Y. N., Singh S. K.: Evaluation of Electrocardiogram for Biometric Authentication. Journal of Information Security, 3, s. 39-48, 2012.

[Sobczyk M., 1991] Sobczyk M.: Statystyka. Państwowe Wydawnictwo Naukowe, Warszawa, 1991.

[Stanković S., 2010] Stanković S.:Review Article Time-Frequency Analysis and Its Application in Digital Watermarking. Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2010, Article ID 579295, 20, s. 1-20.

[Stallings W., 2012] Stallings W.: Kryptografia i bezpieczeństwo w sieci. Gliwice: Wydawnictwo Helion, 2012.

[Starzyńska W., 2000] Starzyńska W.: Statystyka praktyczna. Wydawnictwo Naukowe PWN SA, Warszawa, 2000.

[Su C. H. i Wang R. Z., 2006] Su C. H. Wang R. Z.: Secret image sharing with smaller shadow images. Pattern Recognition Letters, vol. 27, no. 6, pp. 551 – 555, 2006.

[Świerkosz A., 2015] Świerkosz A.: Modeling of metabolic diseases – a review of selected methods. Bio-Algorithms and Med-Systems (Print), vol. 11 iss. 4, s. 205–209, 2015.

[Świerkosz A., 2016a] Świerkosz A**.:** Digital watermarking in telemedicine an example from ECG – review of challenges, methods and applications. Innovations in biomedical engineering, Switzerland : Springer International Publishing; s. 248–255, 2016.

[Świerkosz A., 2016b]Świerkosz A.: Charakterystyka wybranych technik ukrywania obrazu. Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska, t. 6 nr 4, s. 43–48, 2016.

[Świerkosz A., 2016c] Świerkosz A.: Charakterystyka wybranych technik ukrywania obrazu [Characteristic of selected image hiding techniques]. Lublin: WD 2016 : Warsztaty Doktoranckie : New Technologies & Their applications : innovation strategy : konferencja naukowa s.212–213, 2016.

[Świerkosz A., 2017] Świerkosz A.: Information coding and decoding using Discrete Wavelet transform. Kraków: 20-th Polish conference on Biocybernetics and biomedical engineering : with the honorary patronage of His Magnificence Rector of the University of Science and Technology, prof. Tadeusz Słomka, abstract book s. 33, 2017.

[Wang H. i in., 2016] Wang H. Zhang W., Yu N.: Protecting patient confidential information based on ECG reversible data hiding. Springer Multimed Tools Appl 75:13733–13747, 2016.

[Willems J. L. i in., 1990] Willems J. L., van Bemmel J. H., Degani R., Macfarlane P.W., Zywietz C.: Common standards for quantitative electrocardiography: goals and main results. CSE Working Party. Methods Inf Med. Sep;29(4): str. 263-71, 1990.

[Wojtaszczyk P., 2000] Wojtaszczyk P.: Teoria Falek. Wydawnictwo Naukowe PWN, 2000.

[Wu W. i in., 2015] Wu W., Liu B., Zhang W., Changwen Chen Ch.: Reversible data hiding in ECG Signals Based on Histogram Shifting and Thresholding. IEEE, 2015.

[Norma IEC]International Standards, IEC 60601-2-51: Medical electrical equipment- Part 2-51: Particular requirements for safety, including essential performance, of recording and analyzing single channel and multichannel electrocardiographs. IEC 2003.

Źródła internetowe:

[Baza MIT-BIH] https://www.physionet.org/physiobank/database/cdb/

[Laboratorium wirtualne-Analiza czasowo-częstotliwościowa sygnałów]
http://wazniak.mimuw.edu.pl/index.php?title=Laboratorium_wirtualne_1/Modu%C5%82_5_-_%C4%87wiczenie_5
Tę stronę ostatnio zmodyfikowano o 09:37, 27 sie 2006

[Podstawy teorii sygnałów-splot i korelacja]
http://gdr.geekhood.net/gdrwpl/heavy/studia/Lecture2007%238__Splot_Korelacja.pdf

[SANS Institute] http://www.sans.org/

[Słownik języka polskiego-falki] https://sjp.pl/falki

[Statystyka_wykład_korelacja] http://zsi.tech.us.edu.pl/~nowak/odzw/korelacje.pdf]

[t-distribution] http://stattrek.com/online-calculator/t-distribution.aspx

[Transformacja Falkowa_Wikipedia] https://pl.wikipedia.org/wiki/Transformacja_falkowa

Spis rysunków

Spis tabel

Dodatek. Wydruki wybranych procedur

Procedura podziału znaku wodnego i osadzania fragmentów w kolejnych kontenerach

```
function [SuccMk, OutSig] = EncodeProc(InSigNr, Text, BitDepth, WaveType)
% InSigNr - sygnał nosnika 1 kanał
% RMax, WriteTo, StartFrom,
% RMax - polozenie maksimum R w sygnale oryginalnym (względem początku
% sygnału)
% WriteTo - dopuszczalne położenie końca kontenera (względem początku
% sygnału)
% StartFrom - opóźnienie punktu startowego wkodowania (=20)
% Text - tekst do zakodowania np 'Agnieszka'
% BitDepth - bitowa głębokość kodowania 0 - wyznaczana automatycznie
% WaveType - typ falki matki przekształcenia np. 'db5'
% CodedCnt - faktyczna ilość zakodowanych bajtów)


Delay=30; % parametr opóźnienia kontenera względem końca QRS
SIn=cseread_as(InSigNr);
SIn=SIn(:,1);
m=CseFidPts(InSigNr); %macierz punktow charakterystycznych
m1=FidPts2Mx(m);
BeatsCnt=length(m1(1,:)); % wyznaczenie liczby uderzeń serca
TextLen=length(Text);
OutSig=SIn;
SuccMk=1;
for (i=1:BeatsCnt)
   if(SuccMk==1)
      m2=m1(i,:);
      RMax=m2(4); % koniec zespołu QRS
      WriteTo=m2(5);
      if (i<BeatsCnt)
         WriteTo=m1(i+1,1);
      end;
      [SOut, CodedCnt]=DatEncode(SIn, RMax, WriteTo, Delay, Text, BitDepth, WaveType);
%       SOut=SIn;
      Text=Text(CodedCnt+1:TextLen);
      TextLen=length(Text);
      OutSig(RMax:WriteTo)=SOut(RMax:WriteTo);
      if (TextLen <1)
         SuccMk=0;
      end;
   end;
end;
plot([SIn, OutSig])
y=plotvertical(10, 4000, m); %przygotowanie linii znaczników
%plot([SIn OutSig y']) % wyświetlenie EKG i linii znaczników
plot([abs(SIn-OutSig) y'])
title(['numer pliku: ', num2str(InSigNr)]);
```

Procedura osadzaniaznaku wodnego w kontenerze pojedynczej ewolucji serca

```
function [SOut, CodedCnt]=DatEncode(SIn, RMax, WriteTo, StartFrom, Text, BitDepth, WaveType)
% SIn - sygnał nosnika 1 kanał
% RMax - polozenie maksimum R w sygnale oryginalnym (względem początku
% sygnału)
% WriteTo - dopuszczalne położenie końca kontenera (względem początku
% sygnału)
% StartFrom - opóźnienie punktu startowego wkodowania (=20)
% Text - tekst do zakodowania np 'Agnieszka'
% BitDepth - bitowa głębokość kodowania 0 - wyznaczana automatycznie
% WaveType - typ falki matki przekształcenia np. 'db5'
% CodedCnt - faktyczna ilość zakodowanych bajtów
%-------------
%Text='Pawel';
%WaveType='db5';
%RMax=CodeP(1);
%WriteTo=CodeP(2);
%StartFrom=CodeP(3);
%BitDepth=CodeP(4);
%--------------
[b11, L]=wavedec(SIn, 2, WaveType);
p=0.5*length(SIn)+ceil(0.5*(RMax+StartFrom)); %poczatek górnej skali (cD1) + połowa położenia
końca QRS
NoiseMax=-inf;
NoiseMin=inf;
CodedCnt=length(Text);
for i=p:p+20 % analiza poziomu szumu na odcinku S-T (20 kolejnych próbek skali 1)
   if(b11(i)<NoiseMin)
      NoiseMin=b11(i);
   end;
   if(b11(i)>NoiseMax)
      NoiseMax=b11(i);
   end;
end;
if(BitDepth<1) % automatyczny wybór głębokosci kodowania
   BitDepth=Number2Bits(NoiseMax-NoiseMin);
end;
t=bittailor(Text,BitDepth); % przygotowanie tekstu do wkodowania na poziomie 3 bity
BitDataLength=length(t); % długość kontenera danych
AllowedContLength=floor((WriteTo-(RMax+StartFrom))/2);
if (BitDataLength>AllowedContLength)
   BitDataLength=AllowedContLength;
   CodedCnt=floor(BitDataLength*BitDepth/8);
end;
for i=1:BitDataLength; b11(p+i)=t(i); end; % zamiana szumu na wkodowana treść kontenera
% wkodowanie opisu kontenera do skali 2 (18 bitów):
ContParams=[];
% RtoC - maxR do poczatku kontenera 6 bitów czyli 0-63
ContParams=[ContParams bitget(StartFrom, 6:-1:1)];
% LenC - długość kontenera 9 bitów czyli 0-511
ContParams=[ContParams bitget(BitDataLength, 9:-1:1)];
% BitD - głębokośc kodowania 3 - 0-7
ContParams=[ContParams bitget(BitDepth, 3:-1:1)];
p=0.25*length(SIn)+ceil(0.25*(RMax))+ceil(0.5*StartFrom); %poczatek drugiej skali (cD2)
for i=1:18; b11(p+i)=ContParams(i); end; % zamiana szumu na wkodowana treść opisu
SOut=waverec(b11, L, WaveType);
```

Procedura podziału znaku wodnego na wartości o zadanej reprezentacji bitowej

```
function DecRep=BitTailor(a, BitDepth)
%DecRep - reprezentacja dziesiętna wartości wyjściowych
%a - ciąg symboli wejściowych
% BitDepth - głębokość kodowania bitowego
a1=double(a);
s1=length(a1);
DecRep=[];
BitTable=[];
for i=1:s1; BitTable=[BitTable bitget(a1(s1), 8:-1:1)]; end;
pBitTable=0; %wskaznik w tablicy bitów
sBitTable=length(BitTable);
% uzupełnienie długości ciągu bitów do najbliższej podzielnej przez
% BitDepth
while (mod(sBitTable, BitDepth)>0)
   BitTable=[BitTable 0];
   sBitTable=sBitTable+1;
end;
while (pBitTable<sBitTable)
   CurDecRep=0;
   for i=1:BitDepth
      CurDecRep=CurDecRep+BitTable(pBitTable+i)*2^(BitDepth-i);
   end;
   DecRep=[DecRep CurDecRep];
   pBitTable=pBitTable+BitDepth;
end
```

Procedura osadzania tekstowego znaku wodnego we wszystkich plikach CSE (przykład dla falki bior4.4 i głębokości kodowania dobieranej automatycznie na podstawie zmierzonego poziomu szumu).

```
for FileNbr=1:125 % dla całej bazy CSE
   if((FileNbr~=67)&&(FileNbr~=70))
         [SuccMk, OutSig] = EncodeProc(FileNbr,
         'Katarzyna_i_Joanna_Konstantynopolitańczykiewiczówny', 0, 'bior4.4');
      %pause
   end
   fname=['..\SYGNALY_STG\Stego_', num2str(FileNbr), '.txt'];
   a=csewrite_fname(fname, OutSig);
  % fileID = fopen(fname,'w');
   %fwrite(fileID, OutSig,'int16');
  % fclose(fileID);
end;
```

Eksperyment numeryczny, procedura ekstrakcji parametrów zapisów testowych z bazy CSE

```
function y=iec_par(res, mode)
% funkcja zwraca parametry czasowe wymagane normą IEC60601-2-51 tab. 104
% mode - przełącznik mode=0 parametry globalne, inna wartość - parametry
% lokalne poszczególnych QRS
% res - wertor rezultatów przetwarzania dla pojedynczego odprowadzenia
% y -wartość wyjściowa jeden wiersz (dla mode=0 lub 1) lub wartości w wierszach dla kolejnych QRS:
% P-duration
% PQ interval
% QRS - duration
% QT interval

if (mode==0) % czasowe parametry globalne
   p=0
   m1=res(p+2)-res(p+1);
   if(m1>0)
      m2=res(p+3)-res(p+1);
   else
      m2=0;
   end;
   y=[m1 m2 res(p+4)-res(p+3) res(p+5)-res(p+3)];
end;
if (mode==1) % czasowe parametry ewolucji reprezentatywnej
   p=20;
   m1=res(p+2)-res(p+1);
   if(m1>0)
      m2=res(p+3)-res(p+1);
   else
      m2=0;
   end;
   y=[m1 m2 res(p+4)-res(p+3) res(p+5)-res(p+3)];
end;
if (mode==2) % czasowe parametry kolejnych ewolucji
   y=[];
   p=40;
   while ((p+9)<length(res))
      m1=res(p+2)-res(p+1);
      if(m1>0)
         m2=res(p+3)-res(p+1);
      else
         m2=0;
      end;
      y=[y; [m1 m2 res(p+4)-res(p+3) res(p+5)-res(p+3)]];
      p=p+20;
   end
end;
```

Eksperyment numeryczny, procedura porównania długości interwałów zgodnie z IEC60601-2-51

```
Differ=zeros(100,4);
%[P, PQ, QRS, QT]
for i=1:100;
  FNum=QRStypeN(i);
  if(FNum>99)
     FNstr=num2str(FNum);
  elseif(FNum>9)
      FNstr=['0' num2str(FNum)];
  else
      FNstr=['00' num2str(FNum)];
  end;
  path='c:\Users\aswierk\Desktop\eksperyment\ECG_PROC\';
  CfName=[path 'tmp\res' FNstr '.res'];
  Cur=load(CfName);
  RfName=[path 'ref\res' FNstr '.res'];
  Ref=load(RfName);
  Differ(i, 1)=Cur(1,6)-Ref(1,6); %P
  Differ(i, 2)=Cur(1,7)-Ref(1,7); %PQ
  Differ(i, 3)=Cur(1,3)-Ref(1,3); %QRS
  Differ(i, 4)=Cur(1,4)-Ref(1,4); %QRS
end;
```

Eksperyment numeryczny, procedura zapisu wartości parametrów załamków w programie do automatycznej interpretacji elektrokardiogramu

```
FILE *iFile = fopen (szAnalysisFile , "wb" );
IN16 RepQrs=0;
IN16 CurVal=0;
EKG_Interpretation_Data* ptabCurBeat=ptabDispInfo;
for(int CurCh=0; CurCh<12; CurCh++)
        {
        // parametry globalne: 30 kolumn
        for(CurVal=0; CurVal<10; CurVal++) // zapis globalnych parametrów czasowych
                fprintf(iFile, "%d ", (int)(DispInfo.mark_positions[CurVal])/*ms*/);
        for(CurVal=0; CurVal<10; CurVal++) // zapis amplitud lokalnych dla ewolucji reprezentatywnej
                fprintf(iFile, "%d ", (int)(1000*DispInfo.tab_amp[CurCh][CurVal])/*uV*/);
        for(CurVal=0; CurVal<10; CurVal++) // zapis czasów lokalnych dla ewolucji reprezentatywnej
                        fprintf(iFile, "%d ", (int)(DispInfo.tab_tim[CurCh][CurVal])/*ms*/);
        // parametrylokalne: QrsCnt*20 kolumn
        for (RepQrs=0; RepQrs<g_pParAnal->QrsCnt; RepQrs++)
                {
                ptabCurBeat=ptabDispInfo+RepQrs;
                for(CurVal=0; CurVal<10; CurVal++) // zapis amplitud lokalnych dla kolejnych ewolucji
                        fprintf(iFile, "%d ", (int)(1000*ptabCurBeat->tab_amp[CurCh][CurVal])/*uV*/);
                for(CurVal=0; CurVal<10; CurVal++) // zapis czasów lokalnych dla kolejnych ewolucji
                        fprintf(iFile, "%d ", (int)(ptabCurBeat->tab_tim[CurCh][CurVal])/*ms*/);
                }
        fprintf(iFile, "\n");
        }
fprintf(iFile, "\n");
fclose (iFile);
```