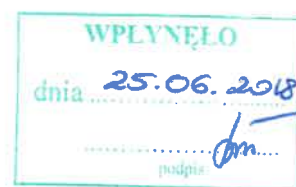


Dr hab. inż. Janusz Jeżewski, prof. ITAM
Instytut Techniki i Aparatury Medycznej ITAM
janusz.jezewski@itam.zabrze.pl

Zabrze, 18 czerwca 2018



RECENZJA

rozprawy doktorskiej magister inżynier Agnieszki Świerkosz

pt.: "Kodowanie informacji dodatkowych w strukturze cyfrowego elektrokardiogramu"

Promotor: prof. dr hab. inż. Piotr Augustyniak

Opiniowana rozprawa doktorska dotyczy problematyki steganografii, czyli przekazywania informacji w taki sposób, aby jej treść nie została wykryta. Postawione zagadnienie jest ważne z punktu widzenia poufności danych medycznych, wymaganej obecnie przez szereg dyrektyw UE. Autorka skupia się na kodowaniu poufnych informacji dodatkowych w sygnale elektrokardiogramu, czyli na problemie szeroko opisywanym w piśmiennictwie już od wielu lat. Dodatkowe informacje diagnostyczne lub administracyjne, które zostają dołączone do struktury elektrokardiogramu cyfrowego, nie mogą zakłócać podstawowych jego informacji diagnostycznych. Integracja w strukturze elektrokardiogramu danych do identyfikacji pacjenta, przy jednoczesnym zabezpieczeniu jej przed nieuprawnionym dostępem, może w przyszłości wspomóc rozwój telemedycyny. Przeprowadzone badania stanowią czynnik wzbogacający stan wiedzy w zakresie kodowania informacji towarzyszących, które mogą rozszerzyć interpretację sygnału elektrograficznego bez potrzeby definiowania nowych struktur danych i kanałów transmisji.

W celu rozwiązania problemu skutecznego dołączania do struktury elektrokardiogramu informacji dodatkowych, zaproponowano dedykowaną metodę kodowania, która umożliwia adaptacyjny dobór parametrów kontenera danych do bieżącej zawartości diagnostycznej elektrokardiogramu. W metodzie tej bardzo ważny jest dobór bitowej głębokości kodowania, która pozwala na uzyskanie rozkładu wartości przypominającego szum. Do oceny jakości steganografii z wykorzystaniem opracowanych metod, użyto przemysłowego standardu stosowanego dla automatycznej diagnostyki elektrograficznej (IEC60601-2-51). Przeprowadzone testy weryfikacyjne stosowalności metody dotyczyły różnych parametrów składowych procesu kodowania: sposobu dekompozycji

sygnału EKG, gęstości strumienia i typu danych dodatkowych. Dla większej głębokości bitowej charakterystyka częstotliwościowa informacji dodatkowej przypominała charakterystykę szumu, stąd kodowanie praktycznie nie miało żadnego wpływu na wartości wyznaczanych podstawowych parametrów diagnostycznych. Rodzaj bazy dekompozycji czy typu informacji sekretnej był pomijalny. Interesujące było wskazanie klasy sygnałów EKG, zawierających widoczne zakłócenia szumem wysokoczęstotliwościowym czy przydźwiękiem sieci, które okazały się być bardziej wrażliwe na wprowadzoną informację sekretną.

Przedstawiona do recenzji rozprawa (bez wykazów) obejmuje 78 stron druku. Zawiera wstęp, pięć rozdziałów i podsumowanie. Cały wywód rozprawy doktorskiej przeprowadzono w oparciu o wybrane i właściwie cytowane 60 pozycji piśmiennictwa. Należy podkreślić fakt, że w cytowanej literaturze znajduje się 7 publikacji naukowych współautorstwa Doktorantki, dotyczących tematyki rozprawy. Świadczy to o tym, że prezentowana rozprawa jest naturalną kontynuacją i konsekwencją jej ukierunkowanych zainteresowań.

Postawiona w rozprawie teza „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” jest oryginalna i istotna z naukowego punktu widzenia, a opracowane dla wykazania (uprawdopodobnienia) tej tezy metody i algorytmy z pewnością przyczynią się do poprawy efektywności automatycznego kodowania w sygnale informacji towarzyszących. Zastosowana przez Doktorantkę metodologia i narzędzia programistyczne do osiągnięcia celu postawionego w rozprawie, są zgodne z ogólnie panującymi trendami panującymi w dziedzinie współczesnych metod przetwarzania sygnałów.

Do szczególnie wartościowych i oryginalnych elementów rozprawy należy zaliczyć:

1. Opracowanie metody kodowania informacji dodatkowej w postaci znaku wodnego w strukturze cyfrowego elektrokardiogramu, która umożliwia adaptacyjny dobór parametrów kontenera danych do bieżącej zawartości diagnostycznej elektrokardiogramu. Dodatkową zaletą jest niezależność kontenerów danych, utworzonych dla tego samego zapisu, w ramach poszczególnych odprowadzeń sygnału EKG czy poszczególnych cykli pracy serca. Może to dotyczyć długości danych, głębokości ich kodowania czy też autoryzacji możliwości ich odczytu przez

użytkowników. Jako bazy dekompozycji wykorzystano sześć funkcji bazowych z trzech rodzin: Daubechies, Symlets i Biortogonalnych. Użyto falek o dwóch różnych rzędach tak dobranych, aby długość falki odpowiadała spodziewanej długości zespołu QRS w środku zakresu dekompozycji. W przypadku rodzin Daubechies i Symlets wybór rzędu falki rzeczywiście okazał się mieć istotny wpływ na własności dekompozycji.

2. Zaproponowanie metody projektowania i opisu kontenerów danych, która uwzględnia wykorzystanie luki pasmowej do zastąpienie składowych sygnału niezwiązanych z reprezentacją pracy serca przez informację sekretną. W metodzie tej ważny jest dobór bitowej głębokości kodowania, większa głębokość kodowania zapewnia większe zniekształcenia sygnału EKG aczkolwiek w krótszym przedziale czasu. Dla sygnałów EKG, które charakteryzuje wyższy poziom szumów, większa głębokość kodowania pozwala na uzyskanie rozkładu wartości kodowanej informacji, który jest bardziej podobny do charakterystyki szumu. Stąd też Autorka wprowadziła procedurę wyznaczania liczby bitów informacji dodatkowej, użytych do jej kodowania w pojedynczym współczynniku falkowym jako funkcję międzyszczytowej wartości szumu wyznaczonej dla sygnału EKG.
3. Zaproponowanie sposobu oceny jakości steganografii dla opracowanych metod, z użyciem przemysłowego standardu stosowanego dla automatycznej diagnostyki elektrokardiograficznej (IEC60601-2-51). Zapewnia on obiektywną ocenę klinicznej istotności zakłóceń zawartości diagnostycznej sygnału EKG, spowodowanych wprowadzaną do nich informacją sekretną. Normy IEC zapewniają standaryzację podstawowych parametrów technicznych elektrokardiografów z automatyczną interpretacją lub bez. Ocena stopnia zachowania informacji diagnostycznej została przeprowadzona przy użyciu rekomendowanej w normie bazy sygnałów CSE. Weryfikacji poddano proces kodowania informacji sekretnej tekstowej i numerycznej, przy użyciu transformacji falkowej dla sześciu różnych rodzajów falek (db5, db10, sym6, sym10, bior2.4, bior4.4) i sześciu wariantów bitowej głębokości kodowania. Zakłócone sygnały analizowano programem Ascard6 (Aspel) w celu wyznaczenia parametrów sygnału EKG (długości odcinków P, PQ, QRS, QT). Aby uniezależnić otrzymane wyniki od niedokładności posiadanego programu interpretacyjnego, jako wartości referencyjnych użyto wyników analizy sygnału bez zakodowanej informacji. Dzięki temu wyznaczono parametry kodowania, dla których uzyskano minimalne wartości błędu wskazujące, że nośnik zawierający informację sekretną nadal może być uważany za medycznie równoważny z oryginalnym (w rozumieniu IEC60601-2-51).

4. Przeprowadzenie analizy statystycznej wyników oceny wpływu na zawartość diagnostyczną sygnału EKG, zakłóceń spowodowanych wprowadzaniem informacji sekretnej. Analiza wykazała, że dla falek db5 i bior4.4 przy głębokości kodowania 3-5 bitów, oraz dla falki bior2.4 przy głębokości kodowania 4-5 bitów, błąd wyznaczania długości zdarzeń w elektrokardiogramie wynosił zero. Oznacza to, że proces kodowania nie miał żadnego wpływu na uzyskiwane wartości podstawowych parametrów diagnostycznych. Z kolei 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 miał niewielki wpływ, aczkolwiek nadal w granicach normy IEC. Podobne testy przeprowadzono dla oceny wpływu użytej bazy dekompozycji czy typu informacji sekretnej.

Podczas lektury recenzowanej rozprawy znalazłem kilka zagadnień niewyjaśnionych lub dyskusyjnych, które zostały zestawione w następujących punktach:

1. Tekst, który można traktować jako Wprowadzenie obejmuje 34 strony i stanowi aż 45% pracy.
2. Na str. 36. Tabela 4 zawiera mało istotne informacje o długościach ewolucji serca w odniesieniu do poszczególnych sygnałów, wystarczający jest sam opis już znajdujący się w tekście,
3. Na str. 39 i 55. W celu wyznaczenia parametrów elektrokardiogramu, zakłócone kodowaną informacją sygnały analizowano przy użyciu programu Ascard6. Jako referencyjne wartości pomiarów tych parametrów posłużyły wyniki analizy tym samym programem sygnału bez informacji zakodowanej. Czy wyniki oceny wpływu wprowadzenia kodowanej informacji do sygnału EKG, nie zależą zbyt mocno od jakości użytego programu analizującego? Czy nie mamy do czynienia z przypadkiem badania „odporności” użytego programu analitycznego na „specyficzne” zakłócenia w sygnale EKG? Czy gdyby użyto innego programu analizy EKG to uzyskane wyniki byłyby całkiem inne? Może należało to sprawdzić przynajmniej dla dwóch różnych programów.
4. Na str. od 45 do 54. Rysunki od 5.13 do 5.30 zawierają niewiele informacji istotnej, brakuje opisu osi i jednostek, górny i dolny sygnał EKG są zawsze identyczne, a także brakuje odpowiedniego komentarza do wykresów. Może zamiast osiemnastu rysunków wystarczyłby jeden ale dobrze opisany.

5. Na str. 57-62, 68, 89. Rysunki 6.1-6.6, 6.10, 6.11 – uwaga jest podobna jak poprzednia, aczkolwiek dotyczy 40 histogramów. Niefortunnie zaproponowany dobór klas sprawia, że histogramy są mało użyteczne do oceny błędów. Prawie wszystkie błędy zawierają się w klasie błędu o wartości zero, więc odnośną syntetyczną informację wystarczyło umieścić w tekście. Jeżeli według Tabeli 3.2 dopuszczalny błąd wynosił $\pm 10\text{ms}$, to ustalenie zakresu histogramu od -250ms do 500ms czy nawet od -500ms do 2000ms wydaje się być nietrafione.
6. Na str. 59 i 60. Ogromna Tabela 6.1 zorganizowana została w sposób nieoptymalny, brakuje opisu jednostek a kropka zamiast przecinka oznacza znak dziesiętny. Zapis wyników z dokładnością 0,1 mikrosekundy (przy zakresie błędu rzędu milisekund) wydaje się być sztuczny. Wystarczająca dokładność 0,1 ms poprawi czytelność i zmniejszy rozmiary tabeli.
7. Na str. 67. Tabele 6.2 i 6.3 zawierają same zera, moim zdaniem tabele są zbędne gdyż w tekście napisano, że zawierają same zera?
8. Na str. 64 i 65. Autorka przedstawiła 6 zespołów QRS z bazy CSE, dla których po wprowadzeniu zakodowanej informacji wystąpiły znaczne rozbieżności w wynikach analizy względem sygnałów „czystych”. Wynika to z faktu, że były one znacznie zaszumione lub miały przydźwięk sieciowy. Moim zdaniem sygnały te powinny być od razu odrzucone. Wpisywanie informacji do sygnału EKG następuje na etapie przekazywania jej przez aparat na interfejs wyjściowy w formie, którą lekarz oglądał na ekranie czy wydruku aby zdecydować czy sygnał nadaje się do dalszej analizy. Sygnał ten jest już po odpowiedniej filtracji i nie powinien zawierać szumu czy przydźwięku sieciowego. Stąd moje pytanie: czy użyta do eksperymentów baza sygnałów CSE została dobrana odpowiednio? Zawiera ona bowiem surowe sygnały EKG przydatne do testowania filtrów i algorytmów detekcji implementowanych bezpośrednio w rejestratorach. Moim zdaniem bardziej odpowiednie byłyby sygnały w postaci jaka jest na wyjściu z urządzenia, gdyż właśnie na tym etapie wprowadzana jest informacja sekretna, a nie do sygnału otrzymanego z toru analogowego do którego podłączone są elektrody EKG.

Wskazane w niniejszej recenzji uwagi krytyczne mają raczej charakter polemiczny, nie wpływają na sformułowanie końcowego wniosku opinii, a służą wyłącznie do poprawy przyszłych publikacji Doktorantki.

Podsumowując przedstawianą opinię stwierdzam, że magister Agnieszka Świerkosz wykazała się wiedzą oraz umiejętnościami wymaganymi do uzyskania stopnia doktora nauk technicznych, gdyż samodzielnie rozwiązała istotne zadanie naukowe z dyscypliny naukowej biocybernetyka i inżynieria biomedyczna. Wymienione powyżej uwagi, nie zmieniają mojej pozytywnej oceny pracy. Przedstawiona rozprawa doktorska spełnia ustawowe wymagania (art. 13, ust.1 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki, Dz. U. z 2003 r., nr 65, poz. 595 z późn. zm.) to jest: stanowi oryginalne rozwiązanie problemu naukowego. W związku z tym stawiam wniosek o przyjęcie tej pracy jako rozprawy doktorskiej i o dopuszczenie jej Autorki – magister Agnieszki Świerkosz do jej publicznej obrony.

