dr hab. inż. Marek Natkaniec, prof. AGH
Katedra Telekomunikacji
Akademia Górniczo-Hutnicza w Krakowie

Kraków, 13 grudzień 2020 r.

RECENZJA ROZPRAWY DOKTORSKIEJ

Tytuł rozprawy: **Efektywne metody skrytej synchronizacji akustycznych kanałów steganograficznych**

Autor rozprawy: **kpt. mgr inż. Jarosław Wojtuń**

Promotor rozprawy: **płk dr hab. inż. Zbigniew Piotrowski, prof. WAT**

Promotor pomocniczy: **ppłk dr inż. Jerzy Dołowski**

1. Jakie zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora?

Opiniowana rozprawa doktorska poświęcona jest zagadnieniom zapewniania synchronizacji przy realizacji steganografii akustycznej w rzeczywistych kanałach telekomunikacyjnych. Poprzez steganografię akustyczną rozumiemy w tym przypadku proces ukrywania informacji w sygnale mowy. Zaproponowane przez Autora pracy metody i rozwiązania pozwalają na uzyskanie synchronizacji po stronie odbiornika. Tematyka pracy jest aktualna i istotna zarówno dla sektora ICT jak i sektora wojskowego w kontekście wzrastającej roli steganografii radiowej i sieciowej. W ostatnich latach obserwujemy stały wzrost zainteresowania różnymi metodami ukrywania informacji w sygnałach dźwiękowych, wizyjnych jak i zintegrowanych materiałach audiowizualnych. Wiele prac związanych jest z analizą metod ukrywania informacji w obrazach cyfrowych. W takich przypadkach algorytmy ukrywające informację przy użyciu transformacji Fouriera dają zwykle dobre wyniki. Niestety, kiedy nośnikiem informacji jest sygnał dźwiękowy większość metod opartych na transformacie Fouriera daje znacznie gorsze rezultaty, gdyż odbierany dźwięk po modyfikacji współczynników transformaty Fouriera jest wyraźnie zniekształcany, co jest bezpośrednio związane z możliwościami percepcyjnymi ludzkiego wzroku i słuchu. Wynika to z faktu, że słuch jest dużo bardziej wrażliwy na zmiany częstotliwości niż obraz. Przekształcenie to stosuje się jednak z powodzeniem w metodach znakowania wodnego utworów. Wykorzystuje się w tym celu zjawisko maskowania, którego

działanie opiera się na wykorzystaniu ułomności ludzkiego słuchu, który nie jest w stanie poprawnie zarejestrować wszystkich dźwięków docierających do ludzkiego ucha. Zjawisko to oczywiście silnie zależy od indywidulanych cech człowieka, który może mieć też różną zdolność do rozpoznawania dźwięków w zakresie częstotliwości akustycznych do 20 kHz. Niemniej jednak w wyniku maskowania nie słyszymy niektórych dźwięków cichszych, które są zagłuszane przez dźwięki głośniejsze znajdujące się na sąsiednich częstotliwościach. Maskowania może mieć miejsce zarówno w dziedzinie częstotliwości jak i w dziedzinie czasu z możliwością występowania wstecz jak i wprzód, kiedy to dźwięki występują zaraz po sobie. Wszystkie wymienione zjawiska powodują, że sygnału maskowanego nie słyszymy. Zakłada się, że znak wodny wstawiany do sygnału dźwiękowego w dziedzinie częstotliwości nie powinien wykraczać ponad krzywą maskowania, zaś w dziedzinie czasu wymaga stosowania odpowiedniego filtru percepcyjnego. Kluczowym problemem staje się jednak kwestia właściwej synchronizacji w systemach steganograficznych. Bez zapewnienia odpowiedniej synchronizacji po stronie odbiorczej, prawidłowa detekcja i wydobycie informacji skrytej są praktycznie niemożliwe, gdyż trudno jest określić w sposób jednoznaczny moment rozpoczęcia procedury ekstrakcji danych skrytych. W konsekwencji powoduje to niską efektywność skrytej transmisji z uwagi na losowy charakter odbieranych danych. Autor zaproponował w recenzowanej pracy cztery autorskie metody gwarantowania synchronizacji w odbiorniku. Trzy pierwsze metody synchronizacji działają wprost na sygnale akustycznym, a działanie czwartej metody związane jest z analizą pakietów na poziomie warstwy transportowej poprzez wykorzystanie struktury zdekodowanego strumienia danych steganograficznych. Analiza różnych metod skrytej synchronizacji akustycznych kanałów steganograficznych, szczególnie dla rzeczywistych kanałów telekomunikacyjnych, zarówno przewodowych jak i bezprzewodowych może stanowić duże wyzwanie, dlatego też w rozprawie wykonano szereg eksperymentów praktycznych, aby osiągnąć postawiony w pracy cel. W szczególności:

- W pracy dokonano przeglądu niektórych metod steganografii akustycznej. Na podstawie analizy wybrano jedną metodę, która wykorzystuje działanie w dziedzinie częstotliwości, a jako nośnik danych steganograficznych wykorzystuje sygnał mowy próbkowany z częstotliwością 8 kHz. Kolejno, dokonano jej implementacji przy zastosowaniu krzywej maskowania, wyznaczonej na podstawie standardu MPEG-1.

- Opracowano i zaimplementowano cztery autorskie mechanizmy skrytej synchronizacji akustycznych kanałów steganograficznych.

- Sprawdzono, czy zaproponowana procedura wyznaczania krzywej maskowania nie wpływa negatywnie na opisaną metodę osadzania danych, a następnie wykonano szereg eksperymentów badawczych w oparciu o metody obiektywne oraz subiektywne potwierdzających zarówno poprawność jak i skuteczność działania poszczególnych mechanizmów synchronizacji. Kolejne badania, przeprowadzone do oceny efektywności skrytej transmisji w rzeczywistych sieciach telekomunikacyjnych, zostały przeprowadzone z użyciem środowiska testowego zrealizowanego w oparciu o radiowe łącze VHF (*Very High Frequency*) oraz w kanale VoIP (*Voice over Internet Protocol*).

W pracy sformułowano następujące tezy rozprawy:

- **Zastosowanie skrytej synchronizacji sygnałów akustycznych zwiększa efektywność transmisji danych steganograficznych w kanale telekomunikacyjnym, w którym występują czynniki degradujące sygnał.**

- **Zastosowanie skrytej synchronizacji sygnałów akustycznych nie spowoduje znacznego pogorszenia jakości sygnału będącego nośnikiem informacji.**

Tezy zostały określone prawidłowo. Można jedynie zauważyć, że pierwsza teza pracy wprost nie zawiera informacji o tym, w jaki sposób mierzona będzie efektywność, tym bardziej, że jako miarę efektywności transmisji danych przyjęto wyłącznie bitową stopę błędów BER (*Bit Error Rate*).

2. Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?

Praca ma charakter teoretyczny oraz doświadczalny. W ramach udowodnienia postawionych tez przeprowadzono szereg eksperymentów badawczych, opartych na testach subiektywnych i obiektywnych, również z użyciem rzeczywistych kanałów telekomunikacyjnych, zarówno przewodowych jak i bezprzewodowych, w oparciu o autorskie implementacje mechanizmów synchronizacji zdefiniowanych w rozdziale czwartym rozprawy.

3. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł (literatury światowej, stanu wiedzy i zastosowań w przemyśle) świadczący o dostatecznej wiedzy Autora? Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?

W recenzowanej rozprawie doktorskiej obecny stan wiedzy tzw. *state-of-the-art* w dziedzinie steganografii akustycznej i metod synchronizacji stanowi zawartość rozdziału drugiego. Warto jednak zaznaczyć, że Autor odnosi się do zebranej literatury również w pozostałych rozdziałach rozprawy. W spisie literatury Autor przytacza 104 pozycje, w tym sześć prac współautorskich. Zdecydowana większość cytowanych w spisie literatury pozycji jest anglojęzyczna i obejmuje znane i cenione konferencje międzynarodowe, czasopisma z tzw. listy filadelfijskiej i książki wydane przez uznane wydawnictwa międzynarodowe. W spisie znalazło się również kilka pozycji opisujących strony internetowe, czasopisma o zasięgu krajowym, książki wydane w języku polskim, dwie rozprawy doktorskie i standardy. Można stwierdzić, że cytowana literatura w zasadzie jest wystarczająca, jednak jak słusznie zauważa sam Autor istnieje wiele innych opublikowanych prac, których tematyka dotyczy steganografii akustycznej oraz metod synchronizacji. Autor wskazuje, że na potrzeby rozprawy dokonano również przeglądu innych prac, a w samej rozprawie opisane zostały jedynie metody najpopularniejsze i najbardziej charakterystyczne. Zdaniem recenzenta w spisie literatury mimo wszystko zabrakło kilku istotnych publikacji związanych głównie z analizowanymi przez Autora metodami synchronizacji stosowanymi przy realizacji steganografii akustycznej. Warto tu chociażby wymienić takie pozycje jak:

- P. Gajewski and Z. Piotrowski, "Correspondent authorization in the GSM telephony using watermarking technology," 2006 European Conference on Wireless Technology, Manchester, 2006, pp. 150-153, doi: 10.1109/ECWT.2006.280457.

- P. Dymarski and R. Markiewicz, "Informed algorithms for watermark and synchronization signal embedding in audio signal," 2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO), Bucharest, 2012, pp. 2699-2703.
- K. Hiratsuka, K. Kondo and K. Nakagawa, "On the Accuracy of Estimated Synchronization Positions for Audio Digital Watermarks Using the Modified Patchwork Algorithm on Analog Channels," 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, 2008, pp. 628-631, doi: 10.1109/IIH-MSP.2008.55.
- P. Dymarski and R. Markiewicz, "Informed algorithms for watermark and synchronization signal embedding in audio signal," 2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO), Bucharest, 2012, pp. 2699-2703.
- A. V. Shishkin, "OFDM-based audio watermarking for electronic radiotelephone identification," 2010 East-West Design & Test Symposium (EWDTS), St. Petersburg, 2010, pp. 190-194, doi: 10.1109/EWDTS.2010.5742037.
- B. Bogdan and J. Lopatka, "A Real Time Generator of Watermarking Signal for FM Radios," 2006 European Conference on Wireless Technology, Manchester, 2006, pp. 269-272, doi: 10.1109/ECWT.2006.280488.
- G. Budiman, A. B. Suksmono and D. H. Shin, "A multicarrier modulation audio watermarking system," 2015 International Conference on Electrical Engineering and Informatics (ICEEI), Denpasar, 2015, pp. 154-160, doi: 10.1109/ICEEI.2015.7352487.
- Zhang Li, Chen Li-min and Qian Gong-bin, "Self-synchronization adaptive blind audio watermarking," 2006 12th International Multi-Media Modelling Conference, Beijing, 2006, pp. 4 pp.-, doi: 10.1109/MMMC.2006.1651353.
- Jiwu Huang, Yong Wang and Y. Q. Shi, "A blind audio watermarking algorithm with self-synchronization," 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No.02CH37353), Phoenix-Scottsdale, AZ, USA, 2002, pp. III-III, doi: 10.1109/ISCAS.2002.1010302.
- Shaoquan Wu, Jiwu Huang, Daren Huang and Y. Q. Shi, "Efficiently self-synchronized audio watermarking for assured audio data transmission," in IEEE Transactions on Broadcasting, vol. 51, no. 1, pp. 69-76, March 2005, doi: 10.1109/TBC.2004.838265.

Niemniej jednak można stwierdzić, że Autor zawarł w spisie literatury najistotniejsze pozycje, z każdego z poruszanych przez siebie zagadnień oraz uznać, że cytowana literatura jest wystarczająca. Autor prawidłowo wyciągnął wnioski z przeglądu literatury i przedstawił je w sposób przekonywujący, aczkolwiek szkoda, że miejscami bardzo skrótowo.

4. Czy Autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

Autor posługiwał się wyłącznie badaniami eksperymentalnymi opartymi zarówno na testach subiektywnych jak i obiektywnych, z użyciem rzeczywistych kanałów telekomunikacyjnych, zarówno przewodowych jak i bezprzewodowych, dowodząc zarówno prawdziwości zredagowanych w rozprawie tez, jak i dokonując analizy komparatywnej. Problem dotyczący opracowania sposobu zapewniania synchronizacji przy realizacji steganografii akustycznej w rzeczywistych kanałach telekomunikacyjnych przeprowadzono w rozprawie wieloetapowo. Po pierwsze, Autor określił i zaimplementował jedną metodę steganografii akustycznej, która

wykorzystuje działanie w dziedzinie częstotliwości, a jako nośnik danych steganograficznych wykorzystuje sygnał mowy w zawężonym paśmie częstotliwości. Autor zastosował krzywą maskowania, wyznaczoną w oparciu o model psychoakustyczny standardu MPEG-1, która została dodatkowo przekształcona z uwagi na mniejszy zakres obsługiwanych częstotliwości. Po drugie, Autor opracował i zaimplementował cztery autorskie metody skrytej synchronizacji akustycznych kanałów steganograficznych. Wszystkie opracowane metody zostały zaimplementowane na procesorze sygnałowym lub układach mikroprocesorowych i działały w czasie rzeczywistym. Po trzecie, zweryfikowano czy zaproponowana procedura wyznaczania krzywej maskowania nie wpływa negatywnie na zastosowaną metodę osadzania danych. Wykonano szereg badań określających jakość sygnału po osadzeniu w nim informacji steganograficznej oraz wpływu zakłóceń na bitową stopę błędów. Po czwarte, Autor potwierdził poprawność działania wyżej wymienionych mechanizmów z użyciem serii eksperymentów badawczych w oparciu o metody obiektywne oraz subiektywne potwierdzających zarówno poprawność jak i skuteczność działania poszczególnych mechanizmów synchronizacji. Kolejno porównano obie metody, co pozwoliło dowieść drugą tezę rozprawy. W ostatniej części rozprawy przeprowadzono ocenę efektywności skrytej transmisji z użyciem rzeczywistego środowiska testowego zrealizowanego w oparciu o radiowe łącze UKF oraz wykonano badania transmisji steganograficznej w kanale VoIP zarówno w sieci lokalnej jak i rozległej, co umożliwiło potwierdzić pierwszą tezę rozprawy. Badania przeprowadzono wykorzystując trzy różne tryby pracy radiostacji: transmisję sygnału mowy z wykorzystaniem modulacji F3E w analogowym trybie pracy na ustalonej częstotliwości AFF (*Analog Fixed Frequency*), transmisję sygnału mowy (kodowanie CVSD 16 kbit/s z szyfrowaniem) z wykorzystaniem modulacji F1D (modulacja SRC4) w cyfrowym trybie pracy na ustalonej częstotliwości DFF (*Digital Fixed Frequency*) i transmisję sygnału mowy (kodowanie CVSD 16 kbit/s z szyfrowaniem) z wykorzystaniem modulacji F1D (modulacja SRC4) w cyfrowym trybie pracy ze skokowo zmieniającą się częstotliwością FFH (*Fast Frequency Hopping*). Rozpatrywaną metryką zarówno w przypadku sieci bezprzewodowych jak i przewodowych była wartość bitowej stopy błędu. Proponowane przez Autora metody weryfikacji poprawności działania poszczególnych metod jak również analizy wydajności ich pracy należy uznać za spójne i poprawne z metodologicznego punktu widzenia.

5. Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek Autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?
   a. W celu weryfikacji postawionych tez Autor wykonał szereg czynności, m.in. prace projektowe, implementacyjne oraz pomiarowe pozwalające na ocenę zaproponowanych rozwiązań w stosunku do istniejącego stanu wiedzy. Przede wszystkim Autor zdefiniował cztery nowe metody skrytej synchronizacji akustycznych kanałów steganograficznych. W pierwszej metodzie nazwanej *Monotonic Phase Correction* Autor dokonał modyfikacji metody opartej na korekcji dryftu kąta fazowego DCM (*Drift Correction Modulation*) w celu przystosowania jej do działania kodera steganograficznego. Koncepcja działania układu wytwarzającego sygnał synchronizujący polega na wytworzeniu sygnału OFDM, który kolejno podlega korekcji amplitudy w oparciu o krzywą maskowania. Kolejno, dokonywane jest przejście z dziedziny częstotliwości do dziedziny czasu i dodanie otrzymanego sygnału do sygnału steganograficznego. Po stronie odbiorczej sygnał

podawany jest na wejście układu skanera kąta fazowego, który wyznacza wartości rozstrojenia kąta fazowego. Następnie dokonywana jest jego korekcja, która odbywa się dla wszystkich ramek sygnału wejściowego i dla wszystkich harmonicznych. W kolejnym etapie następuje detekcja prążków pilotów. Jeżeli liczba wykrytych prążków jest większą bądź równa cztery, wówczas zakłada się, że sygnał wejściowy jest sygnałem steganograficznym. W ostatniej fazie algorytm przechodzi do etapu synchronizacji czasowej.

b. Druga metoda została przez Autora nazwana *Direct Spread Spectrum*. Podobnie jak w pierwszej metodzie, do wytworzenia sygnału synchronizującego generowany jest odpowiedni sygnał OFDM. Dodatkowo jednak generowany jest sygnał DSS, gdzie odpowiednio dobrane ciągi kodowe ułatwiają proces synchronizacji nadajnika z odbiornikiem. W tym celu zastosowano ciąg Golda oraz odpowiednie wielomiany pierwotne, które charakteryzują się dużą wartością autokorelacji dla przesunięcia τ=0, oraz bardzo małą wartością we wszystkich pozostałych przypadkach. Następnie, wygenerowany ciąg pseudolosowy podawany jest na wejście bloku filtrów, interpolacyjnego o charakterystyce pierwiastka z podniesionego kosinusa RRC (*Root Raised Cosine*) oraz dolnoprzepustowego filtra typu FIR (*Finite Impulse Response*). Filtry te odpowiednio kształtują impulsy ciągu pseudolosowego oraz zawężają pasmo sygnału. W ostatnim etapie, z uwagi na silne tłumienie częstotliwości poniżej 300 Hz w analizowanych łączach radiowych, sygnał jest przenoszony na wyższy zakres częstotliwości akustycznych - częstotliwość fali nośnej wynosi fc=2000 *Hz*. W ostatnim kroku sygnały DSS i OFDM podawane są na wejście układu korekcji amplitudy w oparciu o krzywą maskowania, a następnie sumowane z sygnałem steganograficznym. W odbiorniku realizowany jest proces synchronizacji. Odbierany sygnał podawany jest na układ skanera kąta fazowego, w którym wyznaczana jest wartość poprawki kąta fazowego, a kolejno realizowana jest procedura korekcji kąta fazowego oraz procedura detekcji prążków pilotów. Tak jak w przypadku pierwszego mechanizmu, jeżeli liczba wykrytych prążków pilotów jest większa bądź równa cztery, wówczas zakłada się, że odebrany sygnał jest sygnałem steganograficznym i można przejść do etapu synchronizacji czasowej, która polega na wyznaczeniu wartości funkcji korelacji wzajemnej pomiędzy sygnałem odebranym, a sygnałem referencyjnym generowanym po stronie odbiorczej. Przejmuje się, że sygnały są zsynchronizowane, gdy wartość funkcji korelacji wzajemnej osiągnie maksimum dla τ=0.

c. Trzecia metoda synchronizacji przeznaczona do osadzania i ekstrakcji danych w strumieniu VoIP została nazwana *Pattern Insertion Detection* i jej działanie polega na wstawieniu do sygnału mowy znacznika synchronizującego. Transmisja steganograficzna wyzwalana jest przez detekcję sygnału mowy, która wykrywana jest na podstawie wartości energii sygnału (powinna przekroczyć -50 dB) oraz liczby przejść przez zero (współczynnik liczby przejść przez zero powinien być mniejszy niż 0,5). Jeżeli trzy kolejne ramki sygnału spełnią te warunki, to następuje korekcja tych ramek zgodnie z określonym empirycznie wzorcem tłumienia. Tłumienie powoduje obniżenie energii sygnału mowy w oknie o czasie trwania 11ms. Następnie, w sygnale mowy osadzana jest informacja steganograficzna, a algorytm wykrywając sygnał mowy rozpoczyna swe działanie od początku. W odbiorniku działanie mechanizmów synchronizacji polega na analizie, czy dany fragment sygnału zawiera w swej strukturze odpowiedni znacznik synchronizujący. W tym celu analizowana jest wartość energii sygnału i liczba przejść przez zero.

d. Ostatnia, czwarta metoda nazwana została *Minimal Error Synchronization* i tak jak trzecia metoda również przeznaczona jest do zastosowania w strumieniu VoIP. W przeciwieństwie do poprzednich metod, działanie tej metody polega na rozpoznaniu transmisji steganograficznej jedynie na podstawie zdekodowanego strumienia bitów, bez użycia dodatkowych znaczników czy unikalnych sekwencji. Założono, że dane steganograficzne posłużą do budowy ramki w taki sposób, że możliwe będzie jej rozpoznanie w strumieniu bitów po ekstrakcji, jak również, że będzie odporna na utratę pakietów RTP na poziomie ok. 5%. W tym celu zastosowano kody detekcyjno–korekcyjne BCH (*Bose–Chaudhuri–Hocquenghem*), które zapewniły zarówno mały narzut informacyjny, jak również zdolność poprawy założonej ilości traconych pakietów RTP. W celu wyznaczenia odpowiedniego kodu BCH przeprowadzono odpowiednie badania symulacyjne. Zaprojektowane zostały dwa modele kanału VoIP: model z kodekiem PCMA i model z kodekiem iLBC wariant 15,2 kbit/s. Jak sygnał wejściowy przyjęto sygnał mowy o czasie trwania około 120 s, zawierający ponad 2000 bitów informacji skrytej. Procent strat pakietów zmieniano w zakresie od 0 do 5% z krokiem 1. Następnie po stronie odbiornika wyznaczono maksymalną liczbę błędów zarejestrowaną w określonym oknie obserwacji. Pozwoliło to na zaproponowanie różnych wariantów kodów BCH z uwzględnieniem sprawności kodowania oraz minimalnego czasu trwania sygnału T pozwalającego na osadzenie w sygnale n bitów wektora kodowego. Następnie oszacowano prawdopodobieństwo wystąpienia błędów pierwszego rodzaju, co pozwoliło na wybór dwóch wariantów kodu o długości n=127. W celu przygotowania do transmisji, wektor kodowy poddano operacji przeplotu. Po stronie odbiornika proces synchronizacji polega na analizie, czy dekoder BCH jest w stanie, w wyodrębnionym strumieniu bitów rozpoznać ramkę danych. Synchronizację uznaje się za osiągniętą, jeżeli dekoder BCH stwierdzi brak błędów lub wykryje i skoryguje błędy. Jak Autor słusznie zauważa dużą wadą tej metody jest spora złożoność obliczeniowa związana z ciągłą pracą dekodera steganograficznego i dekodera BCH. Zaletą jest z kolei brak ingerencji w sygnał steganograficzny, a więc brak pogorszenia jakości sygnału.

e. Autor przeprowadził cały szereg eksperymentów badawczych umożliwiających określenie efektywności pracy i skuteczności zaproponowanych mechanizmów synchronizacji. Badania przeprowadzano dla różnych sygnałów testowych, a same sygnały zostały celowo odstrojone od stanu synchronizacji. Analizowano również efektywność dekodowania informacji steganograficznej w obecności sygnału synchronizującego. Jako miarę skuteczności wydobywania informacji skrytej zastosowano bitową stopę błędów. Określono również średnią wartość błędu synchronizacji. Ocenie podlegała również jakość przesyłanych sygnałów. Eksperymenty badawcze prowadzone były zarówno w oparciu o metody obiektywne jak i subiektywne z wykorzystaniem grupy słuchaczy testerów, studentów Wojskowej Akademii Technicznej. Obiektywną ocenę jakości sygnałów przeprowadzono w oparciu o zalecenie ITU-T P.862 PESQ (*Perceptual Evaluation of Speech Quality*), a same pomiary wykonano za pomocą dedykowanego testera MultiDSLA. Przyjęto obiektywną miarę jakości sygnału polegającą na wyznaczeniu błędu średniokwadratowego pomiędzy sygnałem oryginalnym i zniekształconym, zakładając przy tym uśrednioną wartość SNR wyznaczoną dla stałych, ale krótkich fragmentów sygnału. Subiektywną ocenę jakości sygnałów przeprowadzono w oparciu o zalecenie ITU-R BS.1116-3. Wynikiem oceny była wartość wyrażona w skali SDG (*Subjective Degradation Grades*), która określa różnicę między oceną stopnia

zniekształcenia dla sygnału oryginalnego i zniekształconego. Ocena dokonywana była z dokładnością do 0,1 przy 5-stopniowej skali stopnia zniekształcenia sygnału.

f. W celu oceny efektywności skrytej transmisji w rzeczywistych sieciach telekomunikacyjnych wykorzystano system bezprzewodowy oparty na falach radiowych oraz telefonię internetową VoIP. Przy realizacji transmisji sygnałów w kanale bezprzewodowym uwzględniono szereg zjawisk takich jak np. interferencje, szumy kwantyzacji i odbiornika, efekty wynikające z różnicy częstotliwości próbkowania, które negatywnie wpływały na przesyłane sygnały mowy. Transmisja steganograficzna w kanale VoIP realizowana była zarówno dla sieci LAN jak i WAN. W pierwszym przypadku użyto infrastrukturę sieci akademickiej WAT, a w drugim dwa publicznie dostępne serwery, do których przyłączono się przez tunel VPN. Zastosowano trzy różne standardy kodowania sygnału mowy: PCMA 64 kbit/s, Speex 24,6 kbit/s i G.729 8 kbit/s. W badaniach telefonii internetowej VoIP wykorzystano te same sygnały testowe, których użyto przy testach w łączu UKF. We wszystkich prowadzonych testach jako miarę efektywności transmisji steganograficznej przyjęto bitową stopę błędu.

Należy podsumować, że proponowane przez Autora oryginalne prace projektowe, implementacyjne oraz pomiarowe pozwoliły na realizację skrytej synchronizacji akustycznych kanałów steganograficznych. Zgodnie z obowiązującym stanem wiedzy dokładnie takie rozwiązania nie były dotychczas proponowane w literaturze światowej. Całokształt rozprawy świadczy o dużej wiedzy Autora w zakresie poruszanej tematyki. Szkoda tylko, że większość swoich prac naukowych Autor opublikował głównie na konferencjach międzynarodowych i w czasopismach o zasięgu krajowym. Szkoda również, że tylko w trzech pracach z prezentowanych dwunastu, doktorant był tzw. 'pierwszym' Autorem.

6. Czy Autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?

Praca została napisana poprawnym językiem polskim z wykresami wysokiej jakości, a także czytelnymi schematami blokowymi. Pewne zastrzeżenia można mieć natomiast do opisów działania poszczególnych procedur skrytej synchronizacji akustycznych kanałów steganograficznych. Zdaniem recenzenta bez dodatkowych informacji, których brakuje także w cytowanej literaturze, trudno jest w całości zrozumieć zasadę działania wybranych mechanizmów, jak również poznać idee jakie przeświecały Autorowi podczas opracowywania niektórych koncepcji, np. sposobu konstrukcji sygnału OFDM, czy też długości kodu Golda. Niezwykle skrótowo przedstawiono także środowisko testowe złożone z radiostacji, jak również sposób prowadzenia w nim testów oraz procedury opracowane dla realizacji testów subiektywnych, czy też sposób gubienia pakietów w testach telefonii internetowej VoIP. Szkoda również, że Autor nie rozszerzył nieco cytowanej bibliografii, zwłaszcza o pozycje wywodzące się właśnie z polskich ośrodków naukowych. Można natomiast pochwalić Autora za poprawność redakcyjną rozprawy. W całej pracy natknięto się jedynie na brak kilku znaków interpunkcyjnych. Należy jednak dodać, że zarówno cele rozprawy, uzyskane wyniki badań jak i tezy przedstawione są w sposób przejrzysty. Zaproponowane przez Autora rozprawy procedury skrytej synchronizacji akustycznych kanałów steganograficznych, jak również przyjęta metoda steganografii akustycznej są spójne wewnętrznie.

7. Jakie są słabe strony rozprawy i jej główne wady?

Recenzowana rozprawa, nie jest oczywiście wolna od drobnych niedociągnięć bądź nieścisłości. W pracy nie zauważono jednak poważniejszych błędów merytorycznych oraz metodologicznych. Szczegółowa analiza pracy umożliwia jednak sformułowanie kilku uwag krytycznych. Należy jednak nadmienić, że są to głównie błędy o charakterze organizacyjno-redakcyjnym oraz drobne uwagi merytoryczne. Wszystkie uwagi zostały podzielone na dwie kategorie: uwagi dyskusyjne oraz mniej istotne uwagi krytyczne.

Uwagi dyskusyjne:

a) Str. 32 - czy Autor rozważał wyznaczenie krzywej maskowania w oparciu o inne, bardziej rozbudowane modele psychoakustyczne?

b) Str. 41 - brakuje uzasadnienia wyboru takiego właśnie sygnału OFDM. Dlaczego przyjęto takie, a nie inne zakresy pasm? Dlaczego przyjęto takie, a nie inne harmoniczne sygnału OFDM? W jaki sposób wybrano prążki pilota? Dlaczego korzystamy właśnie z sygnału OFDM do generowania przebiegu synchronizacyjnego? Dlaczego korzystamy z takich akurat częstotliwości do synchronizacji? Jaki jest poziom sygnału OFDM w stosunku do oryginalnego sygnału?

c) Str. 48 - podobnie jak w przypadku metody MPC brakuje uzasadnienia dla konstrukcji takiego, a nie innego sygnału OFDM. Dlaczego przyjęto takie, a nie inne zakresy pasm? Dlaczego przyjęto takie, a nie inne harmoniczne sygnału OFDM? Dlaczego przyjęto taką długość ciągu Gołda i czy chodzi bardziej o poziom sygnału czy też o czas zbieżności procedury? Czy sygnał pseudolosowy na rysunku 4.15 jest sygnałem basebandowym? Czym ta metoda różni się od klasycznego CDMA znanego z telefonii 3G? Jakie jest uzasadnienie wyboru takich, a nie innych wielomianów pierwotnych? Dlaczego liczność ciągu Golda wykorzystywanego do generacji sygnału DSS została ograniczona do 6096 symboli? Dlaczego częstotliwość wykorzystywanej fali nośnej wynosi fc=2000Hz?

d) Str. 53 - jak często powtarzana jest procedura synchronizacji w metodzie 4.3? Czy stosując metodę PID nie powodujemy znacznej degradacji sygnału dźwiękowego? Czy odbiorca nie słyszy oprócz dźwięku różnych trzasków?

e) Str. 58 - jak realizowana była strata pakietów w zakresie od 0 do 5% - czy pakiety były gubione według określonego rozkładu? Czy możliwa była utrata kilku kolejnych pakietów?

f) Str. 62 - z czego wynikają odczucia autora rozprawy odnośnie minimalnego stosunku sygnału do znaku wodnego? Skąd przekonanie zawarte w rozprawie, że 20 dB jest wartością niewystarczającą?

g) Str. 69 - w pracy zabrakło szczegółów na temat warunków przeprowadzania testów QoE, np. warunków przeprowadzania testów: liczby testów, szczegółowego profilu testerów, mechanizmów wykrywających celowe fałszowanie przez słuchaczy wyniku, czyli z premedytacją udzielających niewłaściwych odpowiedzi itp.

h) Str. 92 - na jaką odległość były oddalone stacje podczas wykonywania testów? Ile razy realizowana była transmisja? Jaki był zbiór sygnałów testowych?

i) Str. 94 - z rysunków 5.41-5.45 oraz 5.49-5.52 wynika, że odchyłki błędów dla uzyskanych wartości BER są dosyć duże. Czy Autor może wskazać w jaki sposób można je zmniejszyć?

Mniej istotne uwagi krytyczne:

j) Str. 38 - szkoda, że na rys. 3.9 średnia bitowa stopa błędów w funkcji odstrojenia w dziedzinie częstotliwości została wyznaczona zaledwie dla 5 wartości odstrojenia w Hz? Uniemożliwia to obserwację zachowania się BER w przedziale -6; -12 Hz i 6; 12 Hz.

k) Str. 61 – szkoda, że Autor wykorzystał jedynie najprostszą miarę jakości sygnału polegają na wyznaczeniu błędu średniokwadratowego pomiędzy sygnałem oryginalnym i zniekształconym. W literaturze spotyka się również takie miary jak: szczytowa wartość odległości sygnału od znaku wodnego, znormalizowana średnia bezwzględna różnica pomiędzy sygnałami, przezroczystości znaku wodnego itd.

l) Str. 69 – w pracy zabrakło informacji o typie i parametrach słuchawek użytych w trakcie przeprowadzania eksperymentu. Jest to o tyle istotne, że jak sam Autor zauważa, podczas testów dźwięk powinien być odtwarzany przez wysokiej klasy system elektroakustyczny w specjalnie przygotowanym do tego celu pomieszczeniu.

8. Jaka jest przydatność rozprawy dla nauk technicznych, przemysłu, obronności kraju itp.?

Recenzowana rozprawa ma charakter teoretyczno-doświadczalny. W pracy zaproponowano i zaimplementowano kilka nowych metod skrytej synchronizacji akustycznych kanałów steganograficznych, możliwych do wykorzystania w sieciach telekomunikacyjnych o różnym zasięgu, zarówno przewodowych jak i bezprzewodowych. Wykonane prace koncepcyjne wszystkich opisanych w rozprawie mechanizmów w niewątpliwy sposób przyczyniają się do rozwoju steganografii. Wszystkie zaproponowane przez Autora rozwiązania zostały z sukcesem przebadane w oparciu o metody obiektywne oraz subiektywne. Przyjęte metryki potwierdziły zarówno poprawność jak i skuteczność działania poszczególnych mechanizmów synchronizacji. Przedstawione rozważania teoretyczne, jak również praktyczna implementacje wykonane na procesorze sygnałowym lub układach mikroprocesorowych, które działały w czasie rzeczywistym, jak również analiza doświadczalna opracowanych mechanizmów świadczą o wysokiej użyteczności wykonanej pracy. Stwierdzam więc, że niniejsza rozprawa wnosi znaczący wkład do aktualnego stanu nauki w zakresie metod skrytej synchronizacji akustycznych kanałów steganograficznych. Ponieważ tematyka steganografii radiowej oraz sieciowej odgrywa coraz większe znaczenie zarówno w kraju jak i na świecie, zaprezentowane w pracy wyniki mogą okazać się przydatne dla zwiększania bezpieczeństwa teleinformatycznego Polski, jak również obronności naszego kraju.

9. Podsumowanie. Do której z następujących kategorii Recenzent zalicza rozprawę:

   a. niespełniająca wymagań stawianych rozprawom doktorskim przez obowiązujące przepisy,

   b. wymagająca wprowadzenia poprawek i ponownego recenzowania,

   c. spełniająca wymagania,

   d. spełniająca wymagania z wyraźnym nadmiarem,

   e. wybitnie dobra, zasługująca na wyróżnienie.

Marek Natkaniec