POLITECHNIKA WARSZAWSKA
Wydział Elektroniki i Technik Informacyjnych
Instytut Telekomunikacji
ZAKŁAD CYBERBEZPIECZEŃSTWA
ul. Nowowiejska 15/19, 00-665 Warszawa

Warszawa, 4 marca 2025 roku

prof. dr hab. inż. **Krzysztof Szczypiorski**

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY DYSCYPLINY NAUKOWEJ INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA WOJSKOWEJ AKADEMII TECHNICZNEJ IM. JAROSŁAWA DĄBROWSKIEGO

Tytuł rozprawy: ***Metoda steganografii wideo odporna na zniekształcenia analogowe***

Autor rozprawy: mgr inż. **Marcin Pery**

Promotor: dr hab. inż. **Tadeusz Nowicki**, prof. WAT
Promotor pomocniczy: dr inż. **Robert Waszkowski**

1. **Jakie zagadnienie naukowe jest rozpatrzone w pracy /teza rozprawy/ i czy zostało ono dostatecznie jasno sformułowane przez autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?**

   Praca obejmuje zagadnienia bezpieczeństwa w systemach teleinformatycznych w szczególności algorytmy ukrywania informacji za pomocą steganografii wideo. Steganografia jest istotnym elementem cyberbezpieczeństwa, natomiast jej obszar skoncentrowany na obrazach ruchomych należy do najtrudniejszych w realizacji w całym spektrum technik multimedialnych i zastosowania ich w sieciach. Autor postawił sobie trzy cele: pierwszy – dokonanie przeglądu stanu wiedzy w obszarze ukrywania informacji z istotnym akcentem na zagadnienia dotyczące wideo. Drugim celem była pogłębiona analiza steganografii wideo, w której mieści się przedstawiony w pracy algorytm, poszerzona o komplementarną analizę problematyki zniekształceń analogowych pomiędzy komunikującymi się podmiotami. Trzecim, najistotniejszym celem z punktu widzenia rozprawy, było przedstawienie autorskiej metody steganografii wideo RAI (Robust Adaptive Incremental) i dokonanie wszechstronnych badań jej własności.

   Teza badawcza została postawiona w Rozdziale 3.3 i brzmi następująco:

   „Możliwe jest opracowanie nowej metody steganografii wideo spełniającej jednocześnie dwa warunki:

1) Metoda będzie charakteryzowała się tak dużą odpornością, że nawet w przypadku zniekształceń analogowych oryginalnego steganogramu wideo polegających na jednoczesnych przekształceniach geometrycznych, zaszumieniu, transkodowaniu i na końcu utworzeniu przez odbiorcę nowego pliku steganogramu wideo – możliwe będzie przekazanie od nadawcy do odbiorcy tajnego komunikatu.

2) Metoda będzie cechowała się na tyle dużą niewykrywalnością podczas przechodzenia przez kanał analogowy, że fakt ukrycia w steganogramie komunikatu nie będzie możliwy do odkrycia przy pomocy ludzkich zmysłów, w tym przypadku wzroku."

Rozprawa ma charakter teoretyczno-doświadczalny i jest oparta na modelowaniu matematycznym, na symulacjach komputerowych, a także na typowej dla nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja konwencji „proof of concept" (PoC). Dodatkowo prototyp przetestowano na grupie osób, w celu odpowiedzi na pytanie: czy wybrana metoda jest niewykrywalna.

2. **Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł / w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle /świadczący o dostatecznej wiedzy autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?**

Stan wiedzy został przedstawiony wyczerpująco w Rozdziale 2. Przedstawiono wszechstronnie ukrywanie informacji przez omówienie podstaw steganografii i steganoanalizy (ogólnie steganologii). Poddano dyskusji powszechnie używane miary w ukrywaniu informacji (niewykrywalność, pojemność, odporność). W Rozdziale 3 przedstawiono tło badawcze dla każdego ze specyficznych zagadnień omówionych w pracy: ukrywanie informacji w wideo oraz zniekształcenia analogowe.

Wyciągnięte przez Autora wnioski ze stanu wiedzy są logiczne i przedstawiony w sposób klarowny.

3. **Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?**

Autor rozwiązał postawione zagadnienia naukowe i użył właściwych do tego metod przy uzasadnionych założeniach. Udowodnił, bez cienia wątpliwości, że zaproponowana w rozprawie metoda RAI charakteryzuje się wystarczającą odpornością oraz akceptowalnym poziomem niewykrywalności.

Osiągnięta skuteczność metody steganograficznej RAI definiowana jako procent steganogramów, dla których przy jakimkolwiek poziomie kodowania z zakresu od 1 do 5 udało się zdekodować zakodowany komunikat średnio wyniosła prawie 98%. Wyznaczone w badaniach parametry pokazała, że pomiędzy poziomem kodowania wystarczającym do automatycznego zdekodowania komunikatu ze steganogramu a poziomem kodowania, który jest wykrywalny przez osoby badane występuje istotna odległość wynosząca dwa poziomy kodowania. Oznacza to, że proponowana metoda RAI przy zastosowaniu odpowiednio dobranych poziomów kodowania jest techniką steganografii wideo niewykrywalną przez człowieka.

4. **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?**

   Oryginalność rozprawy dotyczy szeregu aspektów: pierwszym, a zarazem głównym, jest zaproponowanie nowej metody steganografii wideo RAI odpowiadającej na problem zniekształceń analogowych wraz z definicją formalnego modelu. Drugim jest zaproponowanie algorytmów kodujących c-RAI wykorzystujących do zapisywania informacji koncepcję masek kodujących oraz algorytmów dekodujących d-RAI wykorzystujących koncepcję adaptacyjnej inkrementacji ilości informacji w kolejnych iteracjach dekodujących. Trzecim: zdefiniowanie dla metody RAI metryk miar odporności, pojemności oraz niewykrywalności, a następnie przeprowadzenie szczegółowych systematycznych badań wpływu różnego typu przekształceń i zniekształceń steganogramów wideo na te metryki. Czwartym: zastosowanie kodów QR do ochrony komunikatu w steganogramach wideo. Ostatnim, piątym, przeprowadzenie badań nad niewykrywalnością metody RAI na grupie osób wraz z ustaleniem rzeczywistych progów detekcji dla ludzkiej percepcji wzrokowej.

   W stosunku do stanu wiedzy znanego z literatury bardzo wysoko oceniam algorytm RAI i sposób jego badania. Wyniki pracy zostały opublikowane w kilku miejscach, w tym w czasopiśmie z tak zwanej listy filadelfijskiej: Pery, M., & Waszkowski, R. (2024). A Model and Quantitative Framework for Evaluating Iterative Steganography. Entropy, 26(12), 1130. https://doi.org/10.3390/e26121130 [IF=2.1, 100 punktów].

5. **Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników /zwięzłość, jasność, poprawność redakcyjna rozprawy/?**

   Redakcja pracy jest wzorowa, wręcz pedantyczna. Od strony merytorycznej rzadko mam do czynienia z pracami napisanymi tak logicznie i wyczerpująco, mimo że, ostatecznie rozprawa jest dość obszerna. Warto na jej podstawie przygotować książkę, najlepiej w języku angielskim

6. **Jakie są słabe strony rozprawy i jej główne wady?**

   Nie dostrzegłem słabych stron rozprawy. Jedynie niewielkie rozczarowanie, że napisanie jej w języku polskim ograniczyło zasięg odbioru do lokalnych czytelników.

7. **Jaka jest przydatność rozprawy dla dyscypliny informatyka techniczna i telekomunikacja?**

   Praca ma ogromny potencjał w zakresie komercjalizacji i stanowi modelowy przykład pracy, która ma zastosowanie zarówno naukowe, jak i praktyczne. Ciekawą kontynuacją prac wydaje się rozszerzenie jej na audio i stworzenie pełnego systemu audiowizualnego, być może sprzężonego w ukrywaniu informacji na poziomie tych dwóch nośników.

Wniosek końcowy

W mojej ocenie przedłożona przez Pana mgr. inż. **Marcina Pery** rozprawa doktorska spełnia wymagania obowiązujących przepisów prawa i może być podstawą do dalszych kroków niezbędnych do uzyskania stopnia doktora nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja. Jednocześnie, ze względu na jej wybitnie dobry charakter i towarzyszące jej publikacje, wnioskuję o jej wyróżnienie.

Signature Not Verified

Dokument podpisany przez Krzysztof Szczypiorski
Data: 2025.03.04 10:55:47 CET