Prof. dr hab. inż. Zbigniew Kotulski,
Instytut Telekomunikacji Politechniki Warszawskiej

Warszawa, 14 sierpnia 2018 r.

RECENZJA ROZPRAWY DOKTORSKIEJ DLA
RADY WYDZIAŁY ELEKTROTECHNIKI, AUTOMATYKI, INFORMATYKI
I INŻYNIERII BIOMEDYCZNEJ
AKADEMII GÓRNICZO-HUTNICZEJ im. STANISŁAWA STASZICA W KRAKOWIE

Tytuł rozprawy: Zaawansowane techniki steganografii wielu sekretów

Autor rozprawy: mgr inż. Katarzyna KOPTYRA, Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej, AGH w Krakowie

Omówienie treści rozprawy

Praca jest napisana w języku polskim i liczy 109 stron. Treść pracy podzielona jest na pięć rozdziałów. Rozdział 1 (str. 9-12) zawiera wiadomości wstępne wprowadzające podstawowe idee związane z poufnością informacji, motywację prowadzonych badań, sformułowanie tezy rozprawy i celu prowadzonych badań oraz omówienie jej struktury. Teza rozprawy została sformułowana jako:

„Możliwe jest opracowanie nowej klasy algorytmów steganografii cyfrowej, umożliwiających ukrywania wielu niezależnych sekretnych informacji w jednym nośniku danych,"

a odpowiada jej nadrzędny cel, jakim jest opracowanie nowych algorytmów steganograficznych. W rozdziale 2 (strony 13-31) zostały scharakteryzowane podstawowe techniki steganografii. Przedstawiono wybrane przykłady zastosowań steganografii, zdefiniowano steganograficzny kanał komunikacyjny i opisano jego własności, w tym cechy pożądane dla jego praktycznej użyteczności i spodziewanej odporności na wykrycie. Scharakteryzowano tez krótko popularne metody steganografii rozróżniane ze względu na rodzaj nośnika danych i sposób kodowania w nim ukrywanej informacji. Omówiono tu kilka znanych metod, jednak brak wśród nich metody wykorzystującej popularne języki znaczników, np. html, XML, tex,..., por. np.

- Iman Thannoon Sedeeq, *HTML Steganography Algorithms and Detection Methods*, Thesis submitted in accordance with the requirements of the University of Liverpool for the degree of Doctor in Philosophy, May 2018,
- Iman Sedeeq, Frans Coenen and Alexei Lisitsa, *Attribute Permutation Steganography Detection Using Attribute Position Changes Count*, ICISSP, 2017,
- Lipi Kothari, Rikin Thakkar, *A Survey on Techniques of Data hiding on Web*, February 2016 | IJIRT | Volume 2 Issue 9 | ISSN: 2349-6002.

Rozdziały 3 i 4 zawierają wyniki oryginalne rozprawy. Rozdział 3 (str. 33-57) zawiera propozycje nowych algorytmów steganografii wielu sekretów w nośniku będącym obrazem graficznym. Przedstawiono sformalizowany opis schematu steganografii wielu sekretów. Wykorzystując trzy metody umieszczania sekretu w nośniku (nazwanym kontenerem) przedstawiono propozycje różnych sposobów wykorzystania steganografii wielu sekretów do przesyłania wielu informacji lub do zwiększania jej poufności przez wykorzystanie fałszywych sekretów. Skuteczność nowych algorytmów zweryfikowano eksperymentalnie. W końcowej części rozdziału zaproponowano efektywny algorytm generowania kluczy steganograficznych służących do określenia miejsca położenia fragmentów przesyłanej informacji w kontenerze.

W rozdziale 4 (str. 59-89) przedstawiono propozycję nowych systemów steganografii wielu sekretów w środowisku wzorowanym na schemacie bezpieczeństwa „*fuzzy vault*", zaproponowanym przez Ari Juels i Madhu Sudan w 2002 roku. „Fuzzy vault" jest to system kryptograficzny, w którym kluczami są zbiory elementów (a nie uporządkowane ciągi, jak to jest w tradycyjnej kryptografii) i który jest odporny na niewielkie błędy w tych ciągach. System ten (tzn. „*fuzzy vault*") w matematycznym sformułowaniu może być interpretowany w języku wielomianowych schematów podziału sekretu i w taki sposób jest w rozprawie opisywany. W omawianym rozdziale przedstawiono w formalny możliwość wykorzystania schematu do przenoszenia wielu sekretów i propozycje wykorzystania takiego systemu bezpiecznego przechowywania danych do kilku zastosowań informatycznych. Są to: ochrona kluczy steganograficznych, proaktywne udostępnianie danych wielu użytkownikom, system dostępu typu pytanie-odpowiedź oraz system wspomagający

zarządzanie hasłami użytkownika w dostępie do wielu serwisów. Kolejnym oryginalnym elementem tego rozdziału jest wykorzystanie schematu bezpieczeństwa „*fuzzy vault*" w schematach steganograficznych wyższych rzędów, tzn. umieszczania sekretu w sekrecie. Przedstawionych to zostało kilka wariantów takiego zastosowania, takich jak współdzielenie sekretu drugiego rzędu bez dodatkowego klucza i schemat umożliwiający stopniowanie uprawnień. Podsumowaniem rozdziału jest przedstawienie kilku wariantów możliwości wykorzystania danych biometrycznych jako kluczy steganograficznych w schemacie „fuzzy vault". Ten podrozdział ma wprawdzie cechy popularyzatorskie (zastosowania biometrii są bardzo efektowne), lecz ja osobiście nie zalecałbym stosowania takich metod w praktyce. Kompromitacja danych biometrycznych (nieodwracalna, bo właściciel nie może ich już nigdy zmienić) może przynieść dużo większe straty niż potencjalne korzyści wynikające z powyższego zastosowania.

Ostatni rozdział 5 (str. 91-94) stanowi podsumowanie przeprowadzonych badań, zestawienie wyników uzyskanych w poszczególnych rozdziałach i propozycje możliwych kierunków kontynuowania badań w zakresie steganografii wielu sekretów.

Rozprawa doktorska zawiera streszczenia w języku polskim i języku angielskim, nie zawiera natomiast wykazu symboli i oznaczeń, spisu rysunków, spisu tabel i spisu algorytmów. Bibliografia rozprawy liczy 182 pozycje, w tym 19 prac, których współautorką jest pani mgr inż. Katarzyna Koptyra. W pracy umieszczono 26 rysunków, 2 tabele i 9 specyfikacji algorytmów.

Dalszą część recenzji przygotowałem w punktach wzorowanych na zestawie pytań zawartych zwykle w formularzach recenzji rozpraw doktorskich.

Omówienie rozprawy

Jaki jest problem naukowy (teza) rozprawy i czy został on trafnie i jasno sformułowany?

Celem pracy jest skonstruowanie nowych algorytmów steganografii cyfrowej wielu sekretów. Ten jasno sformułowany główny cel pracy został zrealizowany poprzez wykonanie szeregu zadań szczegółowych, do których należą propozycje metod umieszczania kilku różnych sekretów w jednym nośniku, w tym sekretów fałszywych, co utrudnia steganalizę, oraz opracowanie metod generowania kluczy steganograficznych służących do losowego rozpraszania sekretu w nośniku.

Przeprowadzone badanie w pełni wykazały tezę rozprawy, to znaczy Autorka zaprezentowała dwie nowe klasy algorytmów steganografii cyfrowej, umożliwiających ukrywania wielu niezależnych sekretnych informacji w jednym nośniku danych

Czy autor rozwiązał postawiony problem i czy użył do tego właściwych metod dowodząc, że posiadł umiejętności związane z metodyką i metodologią prowadzenia badań naukowych?

Zarówno cel główny, jak też cele szczegółowe będące jego rozwinięciem i doprecyzowaniem, zostały w pełni zrealizowane. Zaproponowane nowe algorytmy steganograficzne zostały poprawnie zdefiniowane i zapisane w formie pseudokodu. Algorytmy te zostały również zaimplementowane, a efekty ich działania zostały zweryfikowane eksperymentalnie. Każdy z zaproponowanych w pracy algorytmów stał się również tematem publikacji naukowej, czyli został poddany zewnętrznej recenzji, a przez fakt upublicznienia – przedstawiony do oceny w środowisku naukowym.

Czy tematyka rozprawy jest aktualna lub dostatecznie ważna?

Steganografia jest metodą zapewniania poufności informacji istniejącą równolegle z kryptografią od wieków, jednak obecnie jej znaczenie ogromnie wzrosło. Moim zdaniem, są dwa główne powody tego zjawiska (nie jest nim z pewnością wysoki poziom bezpieczeństwa metod steganograficznych). Pierwszym jest pojawienie się wielu możliwości ukrywania informacji w nośnikach cyfrowych i kanałach komunikacyjnych oraz łatwość przesyłania takich informacji. Drugim – powszechna dostępność steganograficznych kanałów komunikacyjnych, nie wymagająca specjalnych technologii, szkolenia i, co najważniejsze, dystrybucji kluczy kryptograficznych. Tak więc rozprawa doktorska pani mgr inż. Katarzyny Koptyry należy do tego aktualnego i ważnego nurtu badań.

Czy rozprawa świadczy o dostatecznej wiedzy autora, wiedzy na zaawansowanym poziomie, o charakterze podstawowym dla dziedziny nauk technicznych oraz o charakterze szczegółowym, odpowiadającym obszarowi prowadzonych badań naukowych?

Czy rozprawa obejmuje najnowsze osiągnięcia nauki i świadczy o znajomości współczesnej literatury z dyscypliny naukowej, której dotyczy?

Autorka rozprawy przygotowała bardzo kompetentny opis stanu sztuki dotyczący różnych metod staganografii klasyfikowanych ze względu na rodzaj nośnika informacji oraz możliwych jej zastosowań. Moja wcześniejsza uwaga o pominięciu języków znaczników w niczym nie podważa tej pozytywnej oceny: możliwości wyboru cyfrowego nośnika danych jest wiele, a lista istniejących możliwych rozwiązań nie jest zamknięta. Metody kodowania sekretnej informacji w obrazie zastosowane w rozprawie są standardowe, ale odpowiadają podobnym współczesnym rozwiązaniom innych autorów. Na podkreślenie zasługuje fakt wykorzystania techniki bezpieczeństwa „fuzzy vault", która wprawdzie również nie jest najnowsza (powstała w 2002 roku), ale nie jest zbyt szeroko stosowana. Jej przypomnienie może być impulsem do nowych oryginalnych badań. Podsumowując, można stwierdzić, że Pani mgr inż. Katarzyna Koptyra ma wiedzę niezbędną do prowadzenia badań na najwyższym poziomie w zakresie steganografii, lub szerzej, bezpieczeństwie informacji, a przeprowadzone w rozprawie badania uwzględniają współczesny stan wiedzy w zakresie steganografii cyfrowej.

Na czym polega oryginalny dorobek autora i jakie jest jego znaczenie poznawcze ?

Jakie są najważniejsze osiągnięcia rozprawy?

Autorka rozprawy doktorskiej przeprowadziła oryginalne badania teoretyczne i doświadczalne, dobrze umotywowane i poprzedzone opisem stanu sztuki. Oryginalne osiągnięcia rozprawy zawarte są w dwóch rozdziałach jednorodnych tematycznie, dotyczących, odpowiednio, klasycznej steganografii w obrazach i ukrywaniu obrazów w schematach „fuzzy vault". Do najważniejszych osiągnięć zaliczyłbym:

- Zaprojektowanie schematów steganograficznych dla wielu sekretów w kilku wariantach;
- Zaproponowanie nowego algorytmu generowania kluczy steganograficznych gwarantującego dobrą losowość klucza i brak kolizji jego elementów;
- Opracowanie metod steganografii wielu sekretów w schemacie bezpieczeństwa „fuzzy vault".

Jakie są wady i słabe strony rozprawy?

Zauważyłem w rozprawie kilka usterek, które jednak zaliczyłbym raczej do usterek redakcyjnych (przedstawię je w następnej części tej recenzji). Pewnym niedostatkiem

pracy jest dla mnie (jako osoby zajmującej się kryptografią) jedynie intuicyjne i jakościowe podejście do bezpieczeństwa prezentowanych algorytmów. Autorka pisze o bezpieczeństwie algorytmów, zwiększaniu tego bezpieczeństwa przez zastosowanie np. fałszywych sekretów, ale nie podaje miar ilościowych poziomu tego bezpieczeństwa i, ilościowo, stopnia jego wzrostu (w kryptografii jest to zwykle liczba operacji potrzebnych do złamania algorytmu, wyrażona długością efektywnego klucza kryptograficznego). Dotyczy to także schematów „fuzzy vault", które są nazywane kryptosystemami.

Uwagi szczegółowe i redakcyjne

Praca jest zredagowana starannie pod względem językowym i edycyjnym. Niżej przedstawiam kilka uwag, które mogłyby przyczynić do jej jeszcze lepszej prezentacji.

Najważniejsza, moim zdaniem, uwaga redakcyjna dotyczy sposobu cytowania pozycji bibliograficznych i ich odniesienia do treści pracy. Z opisu prezentowanych wyników trudno określić, w jakim stopniu dany fragment tekstu jest opracowany na podstawie literatury, a w jakim oryginalny. Dotyczy to zarówno prac obcych, jak i własnych Autorki. Na przykład, na stronie 59 zamieszczono przykład wprowadzający schemat „fuzzy vault", który jest zaczerpnięty z publikacji [77], co jednak nie wynika z jego opisu, mimo iż wspomniana praca jest cytowana. Podobna sytuacja dotyczy omawiania własnych wyników Doktorantki, gdzie konkretne wyniki były opublikowane w czasopismach i publikacjach konferencyjnych, a nie jest to wyraźnie podkreślone, zarówno w tekście rozdziałów, jak i w podsumowaniu.

- Strona 36, 37, 62, 68, 76, zostało użyte słowo „sekcja" do określenia części rozdziału. Powinno być „podrozdział".
- Strona 15 użyto wyrażenia „funkcja haszująca". Powinno być „funkcja skrótu".
- Strona 18 – Użyto nazwy „Stegaanaliza". Moim zdaniem, lepiej byłoby „steganaliza" albo „steganoanaliza".
- Strona 45, rys. 3.6, strona 47, rys. 3.8 - rysunki o różnych rozmiarach binarnych zostały wydrukowane na stronie jako obrazy tego samego rozmiaru. W ten sposób nie można zaobserwować optycznie efektu umieszczenia obrazu w obrazie, jeśli byłby widoczny.
- Strona 56 – liczbę możliwych kluczy przedstawiono jako skomplikowany

ułamek. Lepiej byłoby to przedstawić jako potęgę liczby 2.

- Strona 65 – Użyto nazwy: „uwierzytelnienie wielopoziomowe". Należałoby raczej powiedzieć „uwierzytelnienie wieloczynnikowe", ang. „multi-factor authentication".
- W spisie literatury Autorka zamieściła kilka własnych prac nie związanych tematycznie z tematyką doktoratu (na temat opisu ruchu człowieka, w szczególności ruchu karateków). Oczywiście, prace te świadczą o wysokich kompetencjach Autorki w dziedzinie informatyki, jednak lepiej byłoby do dokumentacji przewodu przesłanej do recenzenta załączyć CV z wykazem wszystkich publikacji.

Podsumowanie i ocena rozprawy

W swojej rozprawie doktorskiej pani magister inżynier Katarzyna Koptyra sformułowała i zrealizowała oryginalne i aktualne zadanie badawcze, związane z intensywnie rozwijaną tematyką, jaką jest steganografia. Rezultaty uzyskane w pracy związane są z obszarem szczegółowym niezbyt intensywnie badanym w literaturze (steganografia wielu sekretów), lecz o potencjalnie ważnych zastosowaniach. Wyniki uzyskane w rozprawie są tym bardziej cenne. Również schemat bezpieczeństwa „fuzzy vault" nie był dotychczas eksploatowany intensywnie przez badaczy, więc i w tym wypadku wyniki Doktorantki są nowatorskie i ważne.

Reasumując, rozprawę doktorską pani magister inżynier Katarzyny Koptyry oceniam pozytywnie. Uważam, że spełnia ona w całej rozciągłości wymagania stawiane przez *USTAWĘ 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 późniejszymi zmianami, rozprawom doktorskim w **dziedzinie nauk technicznych w dyscyplinie naukowej: informatyka** i wnioskuję o jej dopuszczenie do publicznej obrony.

Prof. dr hab. inż. Zbigniew Kotulski

Z. Kotulski