dr hab. inż. Janusz Stokłosa
prof. nadzw.
w Wyższej Szkole Bankowej w Poznaniu

Poznań, 12 sierpnia 2018 r.

Recenzja rozprawy doktorskiej mgr. inż. Katarzyny Koptyry

pt. „**Zaawansowane techniki steganografii wielu sekretów**"

wykonana dla

Rady Wydziału Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej

Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie

1. Przedłożona mi do recenzji rozprawa doktorska mgr. inż. Katarzyny Koptyry dotyczy projektowania systemów ochrony steganograficznej stosowanych w kontenerach cyfrowych (nośnikach danych). Przedmiotem zainteresowań steganografii cyfrowej jest ukrywanie przed osobami postronnymi faktu istnienia dodatkowego kanału komunikacyjnego między nadawcą i odbiorcą wiadomości. Wiadomość chroniona jest za pomocą klucza steganograficznego wykorzystywanego w procesie jej osadzania i wyodrębniania. W przypadku steganografii wielu sekretów mamy do czynienia z umieszczeniem kilku niezależnych wiadomości w jednym nośniku danych.

Teza rozprawy została sformułowana następująco:

„Możliwe jest opracowanie nowej klasy algorytmów steganografią cyfrowej, umożliwiających bezkolizyjne ukrywanie wielu niezależnych sekretnych informacji w jednym nośniku danych".

2. Rozprawa składa się z pięciu rozdziałów i wykazu literatury – razem 109 stron. Rozdziałem 1 jest wstęp do rozprawy. W rozdziale 2 Autorka scharakteryzowała techniki steganografii cyfrowej. Rozdziały 3 i 4 zawierają główne osiągnięcia Autorki. Rozdział 5 jest podsumowaniem rozprawy.

W rozdziale 3 zaproponowano algorytmy użyteczne w steganografii obrazowej wielu sekretów. Autorka zreferowała wyniki eksperymentów wykonanych przez siebie na obrazach cyfrowych jako nośnikach danych.

W pierwszym eksperymencie w każdym kontenerze ukrywano dwie wiadomości: prawdziwą w postaci zdjęcia satelitarnego pewnego obiektu oraz fałszywą w postaci fotografii o charakterze neutralnym. Piksele przechowujące wiadomość tajną wybierano zgodnie z kluczem steganograficznym określającym permutację indeksów pikseli. Do osadzania wiadomości fałszywej wybrano algorytm najmniej znaczącego bitu. Kluczem był skrót fałszywej wiadomości wyznaczony za pomocą algorytmu SHA-256. W rezultacie przeprowadzonych badań zauważono, że nietypowy kształt histogramu kontenera wskazuje na ukrytą w nim wiadomość. Może to stanowić podstawę do przeprowadzenia przez intruza analizy steganograficznej.

Drugi eksperyment dotyczył nośników w postaci plików w formacie JPEG, w których – jak wiadomo – stosuje się kompresję stratną. W przypadku plików JPEG można manipulować jakością obrazu poprzez dobór współczynnika kwantyzacji. Jego zmiana powoduje pojawienie się widocznych różnic w obrazie oraz wpływa na rozmiar pliku. Algorytmem służącym do ukrywania wiadomości był algorytm F5 z kluczem (tak jak poprzednio) w postaci skrótu SHA-256 wiadomości fałszywej. Prawdziwy sekret będący obrazem zapisano jako grafikę wektorową SVG i zaszyfrowano. Sekret fałszywy, w postaci tekstu ASCII, umieszczano w nagłówku. Wyniki eksperymentu wskazują, że osadzanie fałszywego sekretu nie wpływa na wygląd kontenera, wpływa jednak na jego rozmiar.

Algorytm F5 wykorzystano w kolejnym eksperymencie do ukrycia dwóch różnych wiadomości za pomocą techniki przeplatania. Przeplatanie polega na wymieszaniu fragmentów wiadomości, a następnie ukryciu ich w nośniku. Zaproponowano algorytm mieszania sekretów (algorytm 3.1) oraz algorytm odzyskiwania sekretów (algorytm 3.2). Wyniki eksperymentu zilustrowano na rysunku 3.8. Na podstawie jego oglądu można wysnuć wniosek o skuteczności takiego podejścia.

Dalsze badania dotyczyły steganografii wielopoziomowej polegającej na umieszczeniu każdej wiadomości na innym poziomie. W pierwszym kroku zaszyfrowany plik SVG ukryto w kontenerze i tak utworzony obiekt – w kroku drugim – osadzono jako sekret w kolejnym kontenerze.

Podsumowując wyniki eksperymentów Autorka krótko je scharakteryzowała, zwracając szczególną uwagę na dostępne w badanych metodach pojemności dla wiadomości prawdziwych i fałszywych. Opisała także sytuacje, w których zaproponowane techniki są najbardziej przydatne.

Zwieńczeniem rozdziału 3 jest opisany w nim bezkolizyjny algorytm generacji kluczy steganograficznych. Zadaniem kluczy steganograficznych, wykorzystywanych w algorytmach osadzania i wyodrębniania, jest określenie sposobu rozmieszczenia sekretu w kontenerze. W zaproponowanym algorytmie (algorytm 3.3) wykorzystuje się permutację losową.

W rozdziale 4 zostały przedstawione autorskie metody steganografii wielu sekretów w schematach *fuzzy vault* (rozmytych skarbców?). System taki można traktować jako rodzaj systemu kryptograficznego tolerującego błędy, w którym klucze są zbiorami liczb. W rozpra-

wie Autorka przedstawiła rozszerzenie tego typu systemu, składającego się z algorytmu osadzania i wyodrębniania, pozwalające na umieszczenie w nim wielu niezależnych sekretów.

Takie podejście umożliwia stosowanie w systemach informatycznych różnych technik uwierzytelniania i łączenia ich, czemu poświęcono podrozdział 4.2 rozprawy. W procesie osadzania kontener jest tworzony w trakcie ukrywania wiadomości przedstawionych w postaci punktów prawdziwych i fałszywych. Proces tworzenia punktów prawdziwych został sformalizowany w postaci algorytmu 4.1.

W kolejnym kroku zastosowano schemat *fuzzy vault* do ochrony kluczy steganograficznych. W kontenerze zostaje ukryty jeden klucz kryptograficzny i pewna liczba kluczy steganograficznych. Autorka odniosła się także do sytuacji, w której w trakcie użytkowania systemu zachodzi potrzeba zwiększenia liczby kluczy steganograficznych i rozwiązała ten problem.

W systemie przeznaczonym dla wielu użytkowników każdy z nich dysponuje własnym kluczem oraz przypisanym do siebie sekretem. Osadzanie tych dwóch wartości dokonywane jest w sposób niezależny. W procesie odzyskiwania każdy użytkownik może, korzystając ze swojego klucza, wyodrębnić swój sekret. Zaproponowany system umożliwia dodawanie i usuwanie nowego użytkownika oraz zmianę sekretu użytkownika. W przypadku zmiany sekretu Autorka zaproponowała rozwiązanie polegające na modyfikacji nośnika, jednak z zachowaniem przez wszystkich uczestników ich dotychczasowych kluczy. Rozwiązanie to gwarantuje dostęp każdego użytkownika wyłącznie do swoich kluczy. Konsekwencją tego jest, że wszystkie punkty spoza wybranej puli są traktowane jako fałszywe.

Kolejną sytuacją, w której można wykorzystać rozszerzony schemat *fuzzy vault* jest system typu pytanie-odpowiedź. Użytkownik chcący uzyskać dostęp do sekretu odpowiada na serię pytań. Odpowiedzi są kodowane na zbiór wartości stanowiących klucz. Dzięki tolerancji błędów gwarantowanej przez system *fuzzy vault* odpowiedzi nie muszą idealnie pasować do wzorca; decydujące są w tym przypadku parametry systemu: rozmiar klucza i stopień stosowanego wielomianu.

Do zarządzaniu hasłami odniesiono się w kolejnym fragmencie rozprawy. Omówiono przykładowy rozszerzony schemat *fuzzy vault* dla wielu sekretów. Umożliwia on powiązanie każdej wiadomości z innym kluczem. Takie podejście gwarantuje, że kompromitacja jednego klucza nie powoduje ujawnienia wszystkich haseł.

Współdzieleniu sekretów wyższych rzędów poświeciła Autorka podrozdział 4.3 rozprawy. Tutaj kontener z ukrytą wiadomością jest traktowany jako nowy sekret i umieszczany w innym kontenerze. Współdzielenie polega na podziale wiadomości na fragmenty zwane udziałami i rozdzieleniu udziałów współpracującym użytkownikom. Taki schemat jest znany w kryptografii jako schemat progowy stopnia (k,n), gdzie n oznacza całkowita liczbę uczestników, natomiast k jest liczbę udziałów niezbędną do odtworzenia sekretu. Autorka opracowała i przedstawiła w rozprawie dwa algorytmy współdzielenia sekretów wyższych rzędów opartych na steganografii wielopoziomowej oraz rozszerzeniu kryptosystemu *fuzzy vault*. Algorytm 4.2 jest algorytmem tworzenia wielomianu stopnia n powstałego ze współczynni-

kami wyznaczonymi z rozwiązania układu n równań n-tego stopnia ze współczynnikami określonymi przez n sekretów. W algorytmie 4.3 odzyskiwania sekretów, na podstawie współdzielonych sekretów, należy utworzyć równanie wielomianowe (obydwa wielomiany są stopnia n) i rozwiązać je, uzyskując w ten sposób sekrety cząstkowe drugiego rzędu. Takie podejście powoduje, że wszystkie informacje konieczne do odtworzenia sekretu rzędu drugiego są ukryte na poziomie pierwszym. Natomiast istnienie sekretów pierwszego rzędu nie wzbudza podejrzeń; ich zadaniem jest maskowanie sekretów rzędu drugiego.

Kolejny algorytm służy do tworzenia udziałów o różnych uprawnieniach. Zaprezentowane rozwiązanie polega na zmodyfikowaniu istniejącego systemu poprzez dodanie do niego ukrytych funkcjonalności dostępnych wyłącznie dla uprawnionych użytkowników. W systemie przewidziano dwa poziomy ukrywania informacji. Pierwszy jest jawny i dostępny dla każdego użytkownika; dane są liczbami, a klucze rozłącznymi zbiorami liczb. Na podstawie wielomianu aproksymacyjnego wyznacza się punkty umożliwiające ukrycie sekretu. Na drugim poziomie obsługuje się użytkowników uprawnionych (algorytm 4.5). Rekonstrukcja udziałów na poziomie pierwszym odbywa się metodą klasyczną, tj. znaną z literatury. Natomiast do odzyskiwania sekretu na poziomie drugim Autorka zaproponowała algorytm 4.6.

Rozdział 4 kończy omówienie możliwości stosowania danych biometrycznych jako kluczy steganograficznych w systemach *fuzzy vault*.

3. Rozprawa ma charakter eksperymentalno-teoretyczny. Autorka trafnie wybrała obszar badań. Głównym osiągnięciem rozprawy – moim zdaniem – jest opracowanie nowych metod steganografii wielu sekretów w schematach *fuzzy vault*.

Praca napisana jest językiem zrozumiałym i zwięzłym. Usterek spostrzegłem niewiele, nie wpływają one na zrozumienie wywodu.

Jako problemy do dyskusji na obronie rozprawy chciałbym prosić Autorkę o rozwinięcie następujących kwestii:

a) W algorytmie 3.3 zabrakło mi kroku oceny jakości wylosowanej permutacji P. Czy jakość tej permutacji jest nieistotna? Czy dowolna permutacja losowa jest tu propozycją najlepszą? Czy permutacja P nie musi się charakteryzować jakimiś cechami szczególnymi?
b) W algorytmie 4.3 (krok 2) konieczne jest rozwiązanie równania n-tego stopnia. Co w przypadku, gdy n jest dostatecznie dużą liczbą? Czy rozwiązanie takiego równania da się uzyskać efektywnie?
c) Na stronie 40 jest informacja o wykorzystaniu do szyfrowania algorytmu Rijndael-256. Domyślać się można, że korzystano z szyfru z kluczem 256-bitowym. Jaki zatem był rozmiar bloku szyfru Rijndael: 128, 192 czy 256 bitów? A może do szyfrowania użyto algorytmu AES-256, czyli standaryzowanej wersji algorytmu Rijndael-256 z blokiem o rozmiarze 128 bitów?

4. Reasumując stwierdzam, że:
   - tematyka rozprawa jest aktualna i bardzo ważna,
   - Autorka rozwiązała zdefiniowany przez siebie problem naukowy i użyła do tego celu odpowiednich metod, tak więc teza rozprawy została wykazana,
   - rozprawa świadczy o dużej wiedzy mgr inż. Katarzyny Koptyry w zakresie steganograficznych metod ochrony danych.

Przedstawiona mi do recenzji dysertacja doktorska, mieszcząca się w dyscyplinie naukowej informatyka, spełnia wymagania stawiane rozprawom doktorskim w *Ustawie o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki* z dnia 14 marca 2003 r. (Dz. U. nr 65, poz. 595; tekst ujednolicony Dz.U. z 2017 r. poz. 1789).

Wnoszę o dopuszczenie mgr inż. Katarzyny Koptyry do publicznej obrony rozprawy.

5. Biorąc pod uwagę znaczące wyniki naukowe oraz fakt, że mgr inż. Katarzyna Koptyra jest współautorką 19 przytoczonych w wykazie literatury publikacji naukowych ogłoszonych na konferencjach międzynarodowych lub opublikowanych w czasopismach naukowych oraz że były one wielokrotnie cytowane, wnoszę o wyróżnienie rozprawy.