РЕЦЕНЗИЯ

на дисертационен труд на
Христо Иванов Параскевов
на тема

"Методи за стеганографска защита на информация в компютърни мрежи"

представен за придобиване на образователна и научна степен "доктор" в
Професионално направление: 4.6 "Информатика и компютърни науки"

от подп. доц. д-р Николай Тодоров Стоянов
Институт по отбрана "Професор Цветан Лазаров"
бул. Тотлебен 34, гр. София, тел. +359 2 9221827, факс: +359 2 9221808, GSM: +359 882110016, e-mail: n.stoianov@di.mod.bg

1. Характеристика на дисертационния труд

Представеният за рецензиране дисертационен труд е разработен на 224 страници включващ увод, пет глави, изводи и получени резултати, научно-приложни приноси в дисертацията, приложни приноси в дисертацията, направления за бъдещи изследвания, списък на публикациите по темата на дисертацията, използвани литературни източници, списък на използваните съкращения, списък на фигурите, списък на таблиците и приложения. Основният текст на дисертационния труд е разработен на 189 страници, в това число 43 фигури и 9 таблици.

1.1. Актуалност на разработвания проблем

Навлизането на информационните технологии във всички сфери на живота има двустранен характер – от една страна ползата от по-лесно и по-бързо управление на различни типове процеси, а от друга– защита на комуникационно-информационната инфраструктура и данните в тези системи. Ето защо, защитата на националните информационни ресурси, в това число и с използване на специално създадени за целта информационни технологии, е от особено значение за националната сигурност.

Актуалността на предложения дисертационен труд се определя от необходимостта от разкриването на същността, съдържанието и специфичните особености на методи за стеганографска защита на информацията и се акцентира върху синтез на алгоритми за стеганографска защита на информацията, които ускоряват изчислителния процес.

Считам, че темата на дисертационното изследване е актуална както от научна, така и от приложна гледна точка. Докторантът е фокусирал своите изследвания върху синтез на алгоритми за стеганографска защита на информацията (в пространствената и мрежова области) и на реализацията на програмен комплекс за експериментално изследване на разработените методи и алгоритми.

1.2 Цели и задачи

Целта на изследването, дефинирана в работата е "разработване на методи и синтез на алгоритми за стеганографска защита на информацията, ускоряващи изчислителния процес". Произтичащите от тази цел задачи са формулирани точно и ясно, целесъобразни са и реализируеми. Работната хипотеза приета в дисертационното изследване "Въвеждането на стеганографска подсистема в системите за защита на информацията (СЗИ) ще повиши сигурността на информацията в компютърните мрежи. Използването на паралелни стегоалгоритми ще повиши бързодействието на методите за стегозащита в мрежите." е коректно формулирана. Предложените подходи за изследване: теория на вероятностите, математическа статистика, цифрова обработка на информацията и емпиричен анализ на ефективността на разработените методи, чрез компютърно моделиране са правилно избрани, адекватни на поставената цел и задачи и позволяват тяхното решаване.

1.3. Структура на дисертационния труд

В Увода авторът описва общата концепция на научното изследване и формулира целта, задачите, обекта и предмета на изследване, работната хипотеза и избраните методи за изследване.

В глава първа от дисертационния труд са разгледани стеганографски системи за защита на информацията в компютърни мрежи, като са определени актуалността на проблема (от гледна точка на автора) и приетите ограничения. Представена е една класификация на подходите за скриване на информация. Направена е класификация на класовете и методите използвани във високотехнологичната стеганография. Дефиниран е обобщен модел на стеганографска система и са определени основните термини. Определена е разликата между компютърна и мрежова стеганография по начина на манипулиране на контейнерите - статични и динамични, като са дадени основните направления и подходи за тяхното използване. Въведено е понятието стегоалгоритъм, чрез използване

на аналитичен израз (1.2 и 1.3) и на основата на възможните преобразувания е дефинирано формално понятието стегосистема (израз 1.1). Чрез използване на дефиниции и понятия от теория на информацията и способите за проверка на хипотези е дефиниран обобщен математически модел на стегосистема. На основата на релациите между заплахите и обекта на защита са определени основните функции на стеганографска система за защита на информацията.

Втора глава от дисертационния труд има теоретико-приложен характер. В нея е направен анализ на методи и алгоритми за компютърна стеганография. За решаване на 2, 3 и 4 задача от дисертационното изследване са избрани показатели за оценка на методите в компютърната стеганография и е предложено за комплексен фактор, формиращ сигурността на дадена стегосистема да се използва устойчивостта на системата (израз 2.1). В тази глава на базата на литературен обзор и анализ е направена една класификация на методите на компютърната стеганография. По-задълбочено внимание авторът е обърнал на методите за компютърна стеганография, в зависимост от начина на вграждане на съобщение: методи в пространствената област, методи използващи трансформация, методи използващи т. нар. разпръснато вграждане, статистически стегометоди, деформиращи методи, изграждащи методи и хибридни методи. На основата на изследването на различните методи в дисертацията е направен сравнителен анализ на тези стегометоди, съгласно предварително дефинираните критерии: незабележимост, стегокапацитет, устойчивост срещу статистически стеганализ, устойчивост срещу промени в изображението, независимост от файловия формат, неподозрителност на стегофайла, ефективност на вграждане и времетраене на изчислителния процес (табл. 2.1). В тази част от изследването, също така, е направен и анализ на методите на компютърната стеганография, в зависимост от използвания контейнер, като подробно са разгледани методите за: оптимално разпределение на елементите на контейнера, методи с аудио файлове, методи с видео файлове. Особено внимание е

обърнато на графичните файлове и тяхната възможност за използване като стегоконтейнери. Подробно са представени подходи за избор на графичен файл, показатели за качество на цифрово изображение и е направен анализ на стеганографските методи с графични контейнери в пространствената област. На основата на извършеното проучване и анализ правилно са формулирани основните изводи към главата.

Трета глава от дисертационния труд е посветена на използваните подходи за разработване на три алгоритъма за компютърна стеганографска защита в пространствената област. Представени са последователен алгоритъм за стеганографска защита с разпръстанто вграждане, базиран на метода LSB; алгоритъм с предварително осмично преобразуване и паралелен стегоалгоритъм, базиран на метода LSB. За така синтезираните и разработени алгоритми са определени входните и изходни параметри, представени са блок-схеми на алгоритмите и е описана последователността на работа на вграждащата и извличащата им част.

В четвърта глава от дисертационния труд са разработени подходи и алгоритми за мрежова стеганографска защита на информацията. Направена е класификация на скритите канали, използвани за предаване на информация и са дадени различните параметри, които ги характеризират. Извършен е семантичен анализ на основните термини в мрежовата стеганография и е представено разпределение на използваните методи по различни нива на OSI модела. На основата на извършения анализ са разработени мрежов стеганографски алгоритъм, използващ RDP протокол и мрежов стеганографски алгоритъм използващ TCP/IP протоколния стек.

Пета глава от изследването разглежда въпроса за създаване и използване на програмен комплекс за експериментално изследване на разработените алгоритми за стеганографска защита на информацията в компютърните мрежи. В изложението е представен съставът на комплекса и е представен избрания метод за изследване на

разработените алгоритми - ефективност на вграждане (израз 5.1). На основата на програмния комплекс са реализирани предложените в трета и четвърта глава алгоритми и са изследвани по критерии ефективност на вграждане, стегокапацитет, процент на запълване, използваемост в локална мрежова среда и в среда на Интернет. На основата на проведените изследвания е направено предложение за състав на стеганографски модул за защита на информацията в компютърни мрежи.

В частта "Изводи и получени резултати" са систематизирани и обобщени резултатите, получени в дисертационното изследване и са формулирани приносите на автора.

1.4. Използвани литературни източници

Докторантът е проучил и използвал значителен брой (165) литературни източници на български, руски и английски езици. Цялостното изложение на дисертационното изследване показва, че докторантът има широк поглед върху състоянието на проблема и говори отлично за неговата висока теоретична и практическа осведоменост.

2. Аналитична характеристика на дисертационния труд

Дисертационният труд има теоретико-приложен характер. Теоретичността се определя от подходите и начините използвани от докторанта за формулиране, формализиране и търсене на решения за стеганографска защита на информацията - пространствена и мрежова. Приложният характер на дисертацията е определен от целта на изследването "Разработване на методи и синтез на алгоритми за стеганографска защита на информацията, ускоряващи изчислителния процес" и подхода за решаване, както и от получените приложни резултати.

3. Приноси в дисертационния труд

Дисертационният труд притежава приноси с научно-приложен и приложен характер. Като научно-приложни приноси приемам, че е доразвито решаването на проблема за защита на информацията в компютърни мрежи, посредством разработване на подходи и алгоритми за скриване на съобщенията, формулирани са основните характеристики и критерии за основнен избор на контейнер и разработените алгоритми за стеганографска защита на информацията (пространствени и мрежови). Получените резултати в изследването показват приложимостта и съдържателността им за решаване на практически задачи, свързани със стеганографска защита на информацията в компютърните мрежи.

4. Публикации и цитирания

Представени са шест публикации на български език, като в една от тях докторантът е самостоятелен автор, в пет – авторът на дисертационния труд е в съавторство. Всичките шест публикации са представени на научни форуми в страната. Нямам сведения за цитирания.

5. Авторство на получените резултати

От представените публикации, може да се направи изводът, че дисертационният труд и получените в него резултати са лично дело на докторанта.

6. Автореферат и авторска справка

Авторефератът вярно и точно отразява дисертационния труд, а именно заглавието, целта, поставените задачи, приносите на автора, получените фактически данни, изводите и списъка на публикациите на автора по темата на дисертацията.

7. Бележки по дисертационния труд

По дисертационния труд могат да бъдат направени следните бележки и препоръки:

- Не е видно дали синтезираните и разработени алгоритми за стеганографска защита на информацията (пространствени и мрежови) са изследвани за пълнота и непротиворечивост.
- При постановка на задачата за приложимост на алгоритъма в Интернет среда, използващ TCP/IP стека не ясно подчертано, дали тази среда съдържа и други хардуерни и софуерни компоненти, имащи отношение към защитата на информацията в компютърните мрежи (firewalls, IDS/IPS и др.).
- Много от използваните литературни източници не съдържат достатъчно информация, за да бъдат намерени и идентифицирани (ISSN, ISBN, стр. и т.н.).
- Изложението на материала се характеризира със строга подреденост. Изследването на съществуващи знания е представено във всяка една от главите и по този начин се добива представа за разпокъсаност между отделните глави.

Посочените бележки по никакъв начин не поставят под съмнения и не омаловажават поучените резултати в дисертационното изследване, те имат единствено за цел подобряване на изложението и бъдещата дейност на автора.

Препоръката която отправям към докторанта е в бъдещата си работа да положи усилия за развитие на работата си чрез участие в национални и европейски научно-изследователски проекти (Horizon 2020) и публикуване на съществуващите и бъдещи резултати в реномирани научни издания у нас и в чужбина.

Цялостната ми оценка за дисертационния труд е положителна. Дисертантът демонстрира отлично познаване на предментната област, добро владеене на апарата на теория на информацията и математическата статистика, и подход и практически знания и умения за реализирането в практиката на предложените от него решения.

Заключение

Като обобщение на гореизложеното, считам, че са изпълнени всички условия и изисквания на Закона за развитие на академичния състав в Република България и правилника към него за присъждане на образователна и научна степен "доктор" и давам с убеждение **положителна оценка** на кандидата **ХРИСТО ИВАНОВ ПАРАСКЕВОВ,** като предлагам на уважаемото научно жури да му присъди **образователната и научната степен „доктор" в професионално направление 4.6 „Информатика и компютърни науки".**

10.03.2014 г. **Рецензент:**

гр. София **подп. доц. д-р Николай Стоянов**