СТАНОВИЩЕ

от проф. д-р Маргарита Кръстева Тодорова,
ръководител на катедра „Компютърни системи и технологии”,
Факултет „Математика и информатика”, ВТУ „Св. Св. Кирил и Методий”

на дисертационен труд за присъждане на образователната и научна степен „доктор” в област на висше образование 4. Природни науки, Математика и информатика, професионално направление 4.6. Информатика и компютърни науки.

Автор: Христо Иванов Параскевов.
Тема: Методи за стеганографска защита на информация в компютърни мрежи.
Научни ръководители: доц. д-р инж. Станимир Стоянов Станев,
доц. д-р инж. Петър Цветанов Антонов.

Настоящето становище е изготвено въз основа на заповед № РД-16-007/12.02.2014г. на Ректора на ШУ „Епископ Константин Преславски”, с която съм определена за член на научното жури по процедура за защита на дисертационен труд на тема „Методи за стеганографска защита на информация в компютърни мрежи” за придобиване на образователната и научна степен „доктор” в област на висше образование 4. Природни науки, Математика и информатика, професионално направление 4.6. Информатика и компютърни науки с автор Христо Иванов Параскевов – докторант в редовна форма, отписан с право на защита, обучаващ се в катедра „Компютърни системи и технологии” на факултет „Математика и информатика” на ШУ „Епископ Константин Преславски” с научни ръководители: доц. д-р инж. Станимир Стоянов Станев и доц. д-р инж. Петър Цветанов Антонов, както и на основа решение на научното жури от неговото първо заседание (Протокол № 1/14.02.2014 г.).

1. Общо описание на представените материали

Представените от дисертанта материали по защита на дисертационен труд са в съответствие с условията и реда, установени в ЗВО (Глава V), Закона за развитието на академичния състав в Република България и Правилника за неговото прилагане, както и Правилника на Шуменския университет за развитие на академичния състав (Глава II, Раздел I, чл. 4-32).

Извършено е предварително обсъждане на дисертационния труд на кандидата на разширено заседание на катедрата, на което е взето решение за насочването му за публична защита (Протокол № 9/17.01.2014 г.).

Не намирам нарушение в процедурата по защитата на дисертационния труд.

2. Кратки биографични данни за докторанта

Докторантът Христо Иванов Параскевов има завършена магистратура по специалност „Информатика” през 1998 г. в Шуменския университет „Епископ Константин Преславски”. През 2001 г. е назначен като асистент в катедра „Информатика”. В периода

2008-2012 г. е старши асистент в катедра „Компютърни системи и технологии", а от 2012г. е главен асистент.

През 2003 г. е зачислен като редовен докторант при ФМИ на ШУ „Епископ Константин Преславски" – катедра "Компютърни системи и технологии" и отчислен през 2008 г. с право на защита.

Положил е необходимите изпити, съгласно индивидуалния план за обучение.

3. Актуалност на тематиката

Защитата на чувствителна за организациите информация налага разработване на нови усъвършенствани средства за предпазване от несанкциониран достъп. Това определя и актулността на темата на дисертацията - внедряването на съвременни стеганографски методи за защита на информация и създаване на скрити канали за предаване на данни. Прилагането на паралелни стегометоди е слабо изследвана област, като у нас не е известно да са правени изследвания в тази насока, а в световния научен обмен публикациите са малко.

4. Познаване на проблема

Докторантът е извършил задълбочено изследване на проблемната област, което доказва много доброто познаване на състоянието на проблема и специфичната терминология. В следствие на направеното проучване са определени насоките за изследване, които дефинират целта и задачите на дисертацията.

Дълбочината на проучването е демонстрирана и от броя на обработените и използвани източници – 165. Използваната литература може да се представи в обобщен вид, съгласно дадената по-долу таблица:

№ по ред	Език	Брой
1	Български	18
2	Руски	32
3	Английски	115
	ОБЩО	165
4	в т.ч. URL адреси	67

Поради сравнително новото направление, избрано за изследване в дисертацията, литературните източници на български и руски език са малко и приоритетно се използват източници на английски език. Основният брой източници са от последните няколко години и се наблюдава равномерност по време на публикуването им.

5. Методика на изследването

Теория на вероятностите, математическа статистика, цифрова обработка на информацията, емпиричен анализ на ефективността на разработените методи чрез компютърно моделиране и други използвани в дисертационния труд, са адекватни на

поставените цел и задачи и способстват за получаване на достоверни резултати от изследването.

6. Характеристика и оценка на дисертационния труд

Дисертационният труд съдържа 189 страници, 43 фигури, 9 таблици и 35 страници приложения. Използвани са 165 литературни източници на български, руски и английски език. По темата на дисертацията са направени 6 публикации.

Дисертационният труд е структуриран в увод, пет глави, изводи и получени резултати, използвана литература, списък на публикациите, свързани с темата на дисертацията и приложения.

В **увода** са формулирани целта и задачите на дисертационното изследване.

Първа глава разглежда актуалността на проблема за стеганографска защита на информацията и са формулирани основните понятия в стеганографията. Анализиран е процесът на образуване на стегограма.

Посочени са съставът и функците на подсистема за стеганографска защита. Предложена е класификация на високотехнологичната стеганография. Дефинирани са направленията за развитие на компютърната и мрежова стеганографии. Разработен е общ модел на стеганографията при наличие на пасивен нарушител. Формулирани са изисквания към стегосистемите.

Предложена е структура на модул за стеганографска защита на информацията и са формулирани основните му функции. Чрез него се реализира основната идея в дисертацията, секретната информация да се предава чрез мултимедийни контейнери, а стегоключовете с разработен метод за скрит мрежов канал.

Във **Втора глава** е направен анализ на основните методи в компютърната стеганография и са избрани показатели за оценка.

Разработена е таксономия на методите на компютърната стеганография. По-голямо внимание е отделено на методите в пространствената област с цел търсене на възможност за намаляване на времето на изчислителния процес. На базата на направената класификация на графичните контейнерите са предложени аналитични изрази за избор на контейнер.

На базата на цялостния анализ е избрано направлението за разработване на алгоритми в пространствената област, базирани на метода на най-младшия бит (LSB) във формат BMP, като основни критерии са: висока степен на незабележимост, осигуряване на по-голям стегокапацитет и търсене на възможност за намаляване на времето за обработка.

В **Трета глава** са предложени три стегоалгоритъма за вграждане на скрита информация в BMP файл, базиращи се на метода LSB - два последователни и един паралелен:

- Последователен алгоритъм за стеганографска защита с разпръснато вграждане, базиран на метода LSB, позволяващ сравнение на характеристиките на предложените други алгоритми в дисертацията;

- Последователен алгоритъм с предварително осмично преобразуване, позволяващ увеличение на стегокапацитета, спрямо метода LSB;
- Паралелен стегоалгоритъм, базиран на метода LSB, ускоряващ времето на изчислителния процес, спрямо последователното изпълнение на метода LSB.

Посочено е, че е целесъобразно като вариант за предаване на стегоключа в реално време да се използват методите на мрежовата стеганография.

В **Четвърта глава** са дефинирани основните проблеми при защитата на компютърните мрежи и е показана възможността за използване на мрежови методи за стеганографска защита. Анализирани са способите за реализация на различни видове скрити канали и техните параметри. Разкрита е същността на мрежовата стеганография и е представена нейната таксономия. Анализирани са възможностите на отделните нива на OSI модела за осъществяване на скрит обмен на информация, както и контрамерки срещу тяхното приложение и са предложени два алгоритъма за стеганографска защита на информация с използване на мрежовите протоколи RDP и TCP/IP:

- Мрежов стеганографски алгоритъм, използващ протокол RDP, за реализация на скрит времеви канал, който да предава стегоключ в реално време;
- Мрежов стеганографски алгоритъм, използващ протоколния стек TCP/IP, за реализация на скрит канал с модификация на дължината на TCP-сегмента, който да предава стегоключ в реално време.

В **Пета глава** се изследват предложените алгоритми, извършват се експерименти с разработените програми и се описва разработеният програмен комплекс за стеганографска защита.

Проведените експерименти изследват характеристиките на предложените алгоритми и доказват изпълнението на поставените в дисертацията задачи.

Общата ми оценка на дисертационния труд е положителна. Изложението е добре структурирано и поднесено с достатъчна степен на детайлност. Извършените анализи и експерименти са визуализирани със съответни фигури, таблици и диаграми. Към всяка от главите са представени съответни изводи. Приведени са и обобщени резултати от изследванията.

В приложенията към дисертацията е даден и първичния код на разработените програмни приложения.

7. Приноси и значимост на дисертационния труд

Прегледът на дисертацията и получените резултати дават основание да се приемат предложените от докторанта приноси, като ги отнасям към групата на научно-приложни и приложни, които обобщавам по следния начин:

НАУЧНО-ПРИЛОЖНИ ПРИНОСИ В ДИСЕРТАЦИЯТА

1. Доразвито е решаването на проблема за защита на информацията в компютърните мрежи, посредством разработване на подходи и алгоритми за скриване на съобщения чрез създаване на скрит времеви канал с протоколните единици на протокол

RDP и чрез манипулиране дължината на TCP-сегмент при използване на TCP/IP трансфер. Формулирани са основните характеристики и критерии за оптимален избор на контейнер и сравняване на методите на компютърната стеганография.

2. Разработен е алгоритъм, реализиращ вариант на метода LSB с използване на техника за разпръснато вграждане и предварително кодиране на информацията, осигуряващ висока степен на незабележимост.

3. Разработен е последователен стегоалгоритъм на базата на метод LSB за графични изображения с предварителна осмична обработка на скритото съобщение, увеличаващ стегокапацитета близо 3 пъти, спрямо метода LSB.

4. Разработен е стегоалгоритъм за паралелна реализация с клъстерна система за вграждане на скрито съобщение по метода LSB, намаляващ времето на изчислителния процес, спрямо последователната обработка до *n-2* пъти при *n* на брой ядра.

ПРИЛОЖНИ ПРИНОСИ В ДИСЕРТАЦИЯТА

1. Разработени са таксономиите на високотехнологичната стеганография, на методите на компютърната стеганография в пространствената област, на мрежовата стеганография и са дефинирани основните български термини в компютърната и мрежовата стеганография на системите за стеганографска защита на информацията.

2. Разработени са програми за последователна реализация на предложените стегоалгоритми на базата на LSB методи.

3. Разработена е програма за паралелна обработка чрез клъстерна система на предложения стегоалгаритъм.

4. Определен е съставът на подсистема за стеганографска защита на информацията и нейните функции.

5. Разработен е програмен комплекс за оценка на предложените алгоритми и тяхното използвне за обучение по дисциплината „Компютърна стеганография”.

8. Преценка на публикациите по дисертационния труд

По темата на дисертационния труд са публикувани шест статии, публикувани в сборници на научни конференции.

В тези публикации, количеството на които е напълно достатъчно, са отразени основните резултати, получени от дисертанта в процеса на неговите изследвания.

9. Лично участие на докторанта

В пакета документация липсва разделителен протокол относно степента на участие на съавторите в общите публикации. Приемам, че тяхното участие е еднакво.

10. Автореферат

Авторефератът отговаря на изискванията и представя в достатъчна пълнота и съдържателност самия дисертационен труд. Изложението в автореферата следва структурата на дисертацията.

11. Критични бележки и препоръки

- В дисертацията на места има подробни описания, които в подобен труд трябва да не присъстват;
- Дисертацията не е лишена от някои граматически и стилови грешки;
- Би могло да се приложи шумоустойчиво кодиране при методите за мрежова стеганография;
- Би могло да се използват различни графични формати при методите за компютърна стеганография.

12. Лични впечатления

Личните ми впечатления от докторанта се изградиха задочно – на базата на представените от него материали, които говорят за много добра професионална подготовка и натрупан опит за провеждане на научно-приложни изследвания.

13. Препоръки за бъдещо използване на дисертационните приноси и резултати

Препоръчвам на Христо Иванов Параскевов в бъдеще да продължи и задълбочи своите проучвания по проблемите, свързани с използване на паралелни стеганографски методи за защита на информацията в компютърните мрежи, като едно перспективно направление.

Препоръчвам също така да се ориентира към публикуване в реномирани научни списания и участие в международни научни конференции.

ЗАКЛЮЧЕНИЕ

Считам, че представеният дисертационен труд отговаря на изискванията на Закона за развитие на академичния състав в Република България, Правилника за неговото прилагане и Правилника на ШУ „Епископ Константин Преславски" и съдържа научно-приложни и приложни резултати. Докторантът притежава задълбочени теоретични знания и професионални умения, които прилага за извършване на самостоятелни научни изследвания.

Изложеното по-горе ми дава основание да изразя убедително своята **положителна** оценка за проведеното изследване, представено в дисертационния труд. Предлагам на почетаемото научно жури **да присъди** образователната и научна степен „доктор" на Христо Иванов Параскевов в област на висше образование „4. Природни науки, математика и информатика", професионално напрвление „4.6. Информатика и компютърни науки".

05.03.2014 г. Изготвил становището:

/проф. д-р Маргарита Тодорова/