

РЕЦЕНЗИЯ

на дисертация за присъждане на образователна и научна степен “Доктор”
в област на висше образование 5. Технически науки,
професионално направление 5.3 „Комуникационна и компютърна техника“
научна специалност 02.21.04 „Компютърни системи, комплекси и мрежи“

Тема на дисертационния труд: Модулни методи за вграждане на цифрова информация в изображения за подобряване сигурността на Интернет-базирани комуникационни платформи

Автор на дисертационния труд: Светозар Валериев Илчев

Научен ръководител: доц. д-р Румен Андреев, ИИКТ - БАН

Рецензент: проф. д-р Боян Бончев, ФМИ - СУ "Св. Кл. Охридски"

Тази рецензия е написана и представена на основание на Заповед № 13/28.01.2014год. на Директора на Института по Информационни и Комуникационни Технологии – БАН, както и на решение на научното жури по процедурата съгл. Протокол №1 от 30.01.2014год.

Като член на научното жури получих за рецензиране следните документи в електронен вид:

- Дисертация за придобиване на образователна и научна степен „Доктор“ с приложена Декларация за оригиналност на резултатите съгласно чл. 27(2) от ППЗ;
- Автореферат на дисертационния труд (на български и английски език);
- Копия на научните трудове по темата на дисертацията.

При рецензирането на дисертационния труд съм се ръководил от изискванията на Закона за развитието на академичния състав в Република България, Правилника за прилагане на Закона за развитието на академичния състав в Република България, Закона за висшето образование и Правилника за специфичните условия за придобиване на научни степени и за заемане на академични длъжности в Института по информационни и комуникационни технологии (ИИКТ) при Българската академия на науките (БАН).

1. Актуалност на проблема и целесъобразност на поставените цели и задачи

Сигурността на данните при разнообразните процеси на обработка, предаване и съхранение на информация е била, е и ще остане ключов проблем в развитието на информационните и комуникационни технологии. Защитата на интелектуалната собственост и механизмите за проверка на автентичността са важни аспекти на проблема на сигурността в цифровите медии. С развитието и популярността на разпространение на мултимедия в глобалната мрежа - най-вече графични изображения и кратки видео клипове

- нараства необходимостта от ефективно криене на данни в мултимедийни ресурси с цел скриване на различни цифрови съобщения и цифрово маркиране на документа с метаданни, описващи автора и защитаващи правата на интелектуална собственост.

Представеният за рецензиране дисертационен труд е насочен основно към криене на данни в компресирани цифрови изображения, посредством вграждане на информация директно в мултимедийното съдържание. Целта му е дефинирана като разработване на *"модулен подход и модулни методи за вграждане на цифрова информация в изображения за подобряване сигурността на Интернет-базирани комуникационни платформи"*. В съответствие с тази цел са формулирани седем задачи, решаването на които прави възможно постигане на по-високо ниво на сигурност в различни Интернет-базирани процеси на обмен на информация. Ето защо намирам темата на дисертационния труд за изключително актуална, а поставените задачи – за логични и целесъобразни с оглед на теоретичните изследвания, решението на проблема и практическата разработка по темата.

2. Познаване състоянието на проблема от страна на дисертанта

Нямам съмнение, че дисертантът е навлязъл много добре в научната проблематика. Списъкът на цитираните литературни източници от една страна е актуален - преобладават публикации от последните десет години, като има източници и от 2013 год., а от друга страна в него присъстват голям брой позовавания на "класически" резултати от деведесетте години на миналия век. Общият брой цитирани източници е относително голям – 180 на брой, като всички от тях са на английски език. С изключение на седемте цитирани авторски публикации, в списъка липсват цитирания на български автори.

Познаването на състоянието на проблема от страна на дисертанта е много добре илюстрирано и от глави 2, 3 и 5 на дисертационния труд. Докато в глава 2 са представени свойства на методите за криене на данни в мултимедия по отношение на приложението им в Интернет, както и най-популярните съществуващи методи и програмни продукти в тази област с акцент на устойчивост срещу JPEG компресия, декомпресия или рекомпресия, то в глава 3 са очертани особеностите на стандарта за компресия на изображения JPEG, имащи отношение към методите за криене на данни в мултимедия, а в глава 5 - свойствата на модулните методи с различни изображения и двоични данни за вграждане за стеганографски цели и за целите на цифровото маркиране.

3. Методика на изследването

Методиката за провеждане на научното изследване, избрана от автора, произтича от поставената цел и съответства на произтичащите от целта задачи. Тя напълно адекватна на целта на работата и се основава на три идентифицирани свойства на приложни сценарии в Интернет, именно:

1. Адаптивност на методите към конкретните потребителски нужди;
2. Устойчивост срещу JPEG-базирани трансформации, по-точно JPEG компресия, декомпресия или рекомпресия;
3. Възможност за работа с произволна мултимедия и вградени данни.

Авторът идентифицира съществуващите методи и продукти за криене на данни в мултимедия като монолитни (предлагащи константен набор от свойства) и с конкретна приложна насоченост (без възможност за адаптация към промени в изискванията като напр. качество на крайното изображение, количество вградена информация и свойствата като устойчивост срещу JPEG трансформации или други промени в съдържанието на мултимедията. Ето защо авторът създава нов модулен подход за криене на данни в мултимедия за целите на мрежови приложения, използващ два приложно-специфични модула:

- модул за целите на стеганографията - преследващ максимизирането на размера на вгражданите двоични данни чрез използване на описание на вгражданите файлове, кодове за корекция на грешки и разбъркване на данните;
- модул за целите на цифровото маркиране - позволяващ откриване на променени региони в изображението и надеждно възстановяване на водния знак при такива промени.

Двата приложно-специфични модула се комбинират с други два базови, контекстно-независими модула, отговорни за обработката на графичните формати и реализирането на общи свойства - единият осигурява устойчивост срещу JPEG компресия, декомпресия и рекомпресия, а другият работи с изображения с беззагубна компресия, като използва модуляция на индекса на квантизация. И двата базови модула осигуряват възможност за работа с произволни изображения и вградени данни, като могат да се комбинират по 4 различни начина с двата приложно-специфични модули в рамките на програмно решение с многослойна архитектура, разработено посредством платформата Майкрософт .NET, в зависимост от изискванията на потребителите и с адаптация към приложения в различни области. Така недостатъците на съществуващите методи са преодоляни, като с цел улесняване на поддръжката всяко свойство на даден метод се реализира или в базовия, или в приложно-специфичния модул.

Проведените експерименти с модулните методи за криене и направената оценката на ефективността спрямо различни подходи за стеганализ показват, че стеганализът чрез използване на корелационни алгоритми и чрез прилагане на филтри върху изображението е ненадежден, ако няма достъп до оригиналното изображение. Същевременно модулните методи предлагат отлично качество на изображението и могат да вградят относително голямо количество данни.

Практическата полза от реализираните модули е илюстрирана чрез три реални Интернет сценария: сценарий за предотвратяване на фишинг на банкови портали, сценарий за защита на мултимедийна интелектуална собственост и сценарий за подобряване на законосъобразното използване на мултимедийно съдържание в социални мрежи.

4. Характеристика и оценка на приносите на дисертационния труд

Дисертацията се състои от седем глави (включващи увод и заключение), декларация за оригиналност на резултатите, списък на цитирани публикации (включващ и публикациите на автора), списък с авторски публикации по дисертацията и списък на проекти, в които докторантът е взел участие, използвана библиография и две приложения. Съдържанието е много добре оформено като том от 205 машинописни страници, като е използвано общоприетото форматиране на текста. Приведени са множество таблици и цветни фигури, илюстриращи по адекватен начин тестовото описание.

Глава 1 представя увод в предметна област на изследването - криене на данни в мултимедия. В тази глава ясно са формулирани целта и задачите на дисертацията. Описани са както основните научни и приложни области, които са от значение при разработката на нови методи за криене на данни, така и използването на методи за криене на данни в приложни сценарии в Интернет. В глава 2 са описани свойства на методите за криене на данни, които са от съществено значение при използването им в приложни сценарии в Интернет. Анализирани и оценени са известни научно-изследователски методи и програмни продукти по отношение на тези свойства. Глава 3 е посветена на общата концепция и авторски модул подход за проектиране на методи за криене на данни. Описани са графичният формат със загубна компресия JPEG, предложеният нов базов модул с устойчивост на вградените данни срещу JPEG трансформации и втори базов модул, проектиран за използване с некомпресирани изображения и изображения с

беззагубна компресия. Предложени са и два нови приложно-специфични модула – съответно за стеганографски цели и за целите на цифровото маркиране.

В глава 4 е представена софтуерната архитектура на реализираното многослойно приложение с използване на платформата Майкрософт .NET. Описаната програмната система позволява изследване на всеки от модулните методи и провеждането на стеганализ. Достъпът до системата от потребители и външни системи се осъществява през подходящ графичен потребителски интерфейс и приложен програмен интерфейс за мрежови услуги. В глава 5 е дискутирана многокритериална оценка на разработените методи и устойчивостта им спрямо статистически стеганализ с помощта на избрани изображения и данни за вграждане. Описани са недостатъците на съществуващите методи за стеганализ по отношение на модулните методи и е изследвана ефективността на два принципни подхода за стеганализ, реализирани като част от разработената система. Глава 6 се спира на три примерни Интернет-базирани сценария (описани по-горе) за приложение на разработените методи, като за целта е проектирана и реализирана мрежова услуга за сертифициране чрез криене на данни. Глава 7 представлява заключение с обобщение на постигнатите резултати, описва приносите на дисертацията и дава изводи и насоки за бъдеща работа по темата.

Приносите на дисертацията могат да се обобщят така:

А. Приноси с научно-приложен характер:

- Разработен е нов модулен подход за криене на данни и е дефиниран набор от методи, включващ собствен метод за постигане на устойчивост срещу JPEG компресия, декомпресия и рекомпресия, както и контекстно-независим базов модул за работа с изображения с беззагубна компресия, използващ модулация на индекса на квантизация и гарантиращ възстановяването на скритата информация с точност до бит;
- Създаден е стеганографски метод за криене на данни, включващ направляващо описание на вградените файлове, кодове за корекция на грешки и разбъркване на данните, както и метод за цифрово маркиране, включващ направляващо описание на вградените водни знаци и възможности за откриване на променени блокове в изображението и възстановяване на вградения воден знак в случай на промени;
- Създадена е многослойна софтуерна архитектура на прототипна система за целите на проверката, оценката и стеганализа на модулния подход за криене на данни, като е оценена ефективността на някои популярни и разпространени алгоритми за стеганализ по отношение на модулните методи за криене на данни.

Б. Приноси с приложен характер:

- Реализирана е прототипна програмна система, като са проектирани инструменти за групова обработка и анализ на изображенията, за прилагане на филтри и за построяване на хистограми в различни цветови пространства;
- Оценена е реализацията на модулните методи чрез изследване на устойчивостта на вградените данни срещу JPEG трансформации и проверка на качеството на изображенията, както и начинът на приложение и предимствата на модулния подход и модулните методи за криене на данни в три приложни сценария;
- Разработена е програмна реализация на сертифицираща услуга за криене на данни, която може да се интегрира в различни Интернет-базирани приложни сценарии.

5. Значимост на разработката за науката и практиката

Извършената от докторанта работа е много голяма като обем и впечатляваща с нивото си на комплексност и задълбоченост. Практическата реализация свидетелства за

отлични проектантски решения с дълбок замисъл и много възможности за надграждане и използване. В този смисъл намирам работата за особено значима в практикческо отношение.

6. Преценка на публикациите по дисертационния труд

Във връзка с дисертационния труд кандидатът е представил седем публикации, от които една публикация е публикувана в списание с импакт фактор („Доклади на БАН“), една - в специализирано списание „*Information Technologies and Control*“, две публикации са докладвани на специализирани международни конференции на IEEE и IADIS, а други три публикации (една от които е отличена с награда) са докладвани на специализирани национални научни конференции с международно участие.

Липсва представен списък с цитирания, показващ отражение на работата от други автори.

7. Лично участие на докторанта

Кандидатът не е представил справка за личното си участие в колективните публикации във връзка с дисертационния труд, но от дългогодишната му работа по темата и от участието му като първи автор в петте колективни публикации оставам с увереността за водещото му участие в тях. Също така съм убеден, че представените в дисертационния труд резултати са лично дело на автора.

8. Автореферат

Като цяло, авторефератът е структуриран в съответствие с традиционните изисквания.

9. Критични забележки

Нямам съществени критични забележки към изложението на дисертационния труд и към постигнатите резултати. Все пак бих искал да отбележа следното към оформлението на дисертационния труд:

- Описанието на стандарта за компресия на изображения JPEG би следвало да бъде поместено преди или в секция 2.1.2, а не в Глава 3;
- Някои от литературните източници са цитирани непълно;

Като съдържателни забележки към работата бих добавил следното:

- Не е представена оценка на бързодействието на създадените алгоритми/методи и сравнението с това на съществуващите методи;
- В списъка на цитираните литературни източници липсват цитирания на български автори;
- Проектите, в които докторантът е взел участие, нямат отношение към дисертацията;
- Не е представен списък на цитирания на публикациите по дисертационния труд – при направена проверка в Google Scholar за тях се указват единствено самоцитирания.

10. Лични впечатления

Нямам лични впечатления за кандидата, но го познавам косвено от разговорите ми с негови колеги от ИИКТ към БАН. От тези разговори съм изградил мнение за Светозар Илчев като ценен колега му изследовател с високи критерии към качеството, но същевременно и обективен и коректен. От представените по процедурата научни статии

лични, че той е също така и задълбочен и амбициозен учен, с отлични приложни познания, способности и опит.

11. Препоръки за бъдещо използване на дисертационните приноси и резултати

Като препоръка бих окуражил авторът да продължи изследванията и практическата работа по усъвършенстване и използване на методите на криене на данни в мултимедия съгласно набелязаните в труда насоки. В тази връзка тя трябва да бъде по-широко популяризирана – напр. чрез Уеб сайт, публикуване в портали като <http://sourceforge.net>, социални и професионални мрежи и др., с цел привличането на нови проектанти и потребители. Такова популяризиране би открило пред него и нови перспективи за развитие на изследванията в избраната научна област, както и за комерсиализация на резултатите.

ЗАКЛЮЧЕНИЕ

Оценката ми за дисертационния труд и описаните в него резултати, автореферата и научните публикации на Светозар Валериев Илчев е **положителна**.

Представеният дисертационен труд съдържа значими научно-приложни и приложни резултати, които представляват оригинален принос в науката и отговарят на изискванията на Закона за развитието на академичния състав в Република България, Правилника за прилагане на Закона за развитието на академичния състав в Република България, Закона за висшето образование и Правилника за специфичните условия за придобиване на научни степени и за заемане на академични длъжности в ИИКТ към БАН. Ето защо предлагам на уважаемото научно жури да присъди образователната и научна степен „Доктор“ на Светозар Валериев Илчев в област на висше образование: 5. Технически науки, професионално направление 5.3 „Комуникационна и компютърна техника“, научна специалност 02.21.04 „Компютърни системи, комплекси и мрежи“.

14.03.2014 год.
София