

## СТАНОВИЩЕ

за дисертационен труд за присъждане на образователна и научна степен "Доктор" по специалността 02.21.04. "Компютърни системи, комплекси и мрежи" в професионалното направление 5.3. "Комуникационна и компютърна техника"

**Автор на дисертационния труд:** инж. маг. Светозар Валериев Илчев

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

**Изготвил становището:** доцент д-р Пенчо Георгиев Венков

### **Актуалност на разработвания в дисертационния труд проблем в научно и научно-приложно отношение**

Масовото използване на комуникационните мрежи за обмен на изображения и мултимедийни продукти обуславя повишения интерес към методите за вграждане на цифрова информация с цел тайна комуникация, поверително предаване и съхранение на данни, защита на авторските права. Стеганографията изучава способите за кодиране на тайни съобщения в изображенията, предавани по комуникационни канали и мрежи. Цифровото маркиране се прилага за защита на интелектуалната собственост и за проверка на автентичността на цифровите медии. То позволява да се идентифицира автора, притежателя на продукта и потвърждава оригиналността му. Тези два съвременни подхода са надстройка на криптографските методи за ограничаване на достъпа до мултимедийни продукти и гарантиране на целостта и произхода им. Съвременните методи за вграждане на цифрови данни в изображения се отличават с гъвкавост и независимост към форматирането и обработката на изображения, незабележимост и надежност към отстраняването на кодираните данни от трети лица. Разработеният проблем в дисертацията е актуален в научно и научно-приложно отношение.

### **Степен на познаване състоянието на проблема и творческа интерпретация на литературния материал**

Задачите за стеганография и цифрово маркиране са описани и илюстрирани с примери в Глава 1. Там те са съпоставени с криптографските методи. В Глава 2 са описани съществуващите методи, програмни продукти и услуги за стеганография и цифрово маркиране. Изтъкнати са техните предимства и недостатъци. Тази информация е извлечена от 180 литературни източника и интернет сайтове, повече от които са публикувани след 2000 г. От прегледа на библиографията и описанието на литературните данни в цитираните глави може да се констатира, че авторът на дисертационния труд добре познава състоянието на проблема и интерпретира получените резултати от позициите на специалист в областта на цифровото маркиране на интернет-базирани мултимедийни продукти.

### **Съответствие на избраната методика на изследване и поставената цел и задачи на дисертационния труд с постигнатите приноси**

В дисертацията е предложен модулен подход за криене на данни в изображения и е описан способа за комуникация между модулите. Проектирани са базов модул за вграждане на данни с устойчивост към JPEG компресия и базов модул за

изображения с беззагубни трансформации, които гарантират възстановяването на скритата информация с точност до бит. Разработени са стеганографски модул за криене на данни и модул за цифрово маркиране с възможност за откриване на променени части в изображенията и възстановяване на вградени водни знаци. Предложена е многослойната архитектура на програмна система за проверка, оценка и анализ на модулния подход за криене на данни и разработените приложни алгоритми. Сравнена е ефективността на разработените алгоритми с тази на съществуващи алгоритми за стеганализ, надеждността на подхода за кодиране при изследване на корелациите в изображението и прилагането на филтри. Използваната методика е ефективна и позволява гъвкаво да се балансират обема данни и устойчивостта към трансформации на изображенията в приложните класове задачи.

## **Научни и научно-приложни приноси на дисертационния труд**

### **Научно-приложни приноси**

1. Разработен е модулен подход за криене на данни и е предложен набор от методи за комуникация между модулите.
2. Създаден е метод за постигане на устойчивост срещу JPEG компресия, декомпресия и рекомпресия, който гарантира възстановяването на вградените данни с точност до бит. Методът е реализиран в контекстно-независим базов модул.
3. Проектиран е базов модул за работа с изображения при беззагубна компресия, използващ модулация на индекса на квантизация. Той също гарантира възстановяването на скритата информация с точност до бит.
4. Създаден е стеганографски метод за криене на данни, включващ приложно-специфичен модул, описание на вградените файлове, кодове за корекция на грешки и разбъркване на данните.
5. Създаден е метод за цифрово маркиране, включващ приложно-специфичен модул за маркиране, описание на вградените водни знаци и възможност за откриване на променени части в изображението и възстановяване на вградените водни знаци.
6. Създадена е многослойна архитектура на прототипна програмна система за целите на проверката, оценката и анализа на модулния подход и методи за криене на данни.

### **Приложни приноси**

1. Изследвана е ефективността на някои популярни алгоритми за стеганализ с цел сравнение с модулните методи за криене на данни. Оценена е ефективността на два базови подхода за стеганализ: чрез изследване на корелациите в изображението и чрез прилагане на филтри.
2. Реализирана е програмна система с езиките Visual Basic, C# и C/C++. Тя се състои от слой на данните, слой на базовите модули, слой на приложно-специфичните модули и интерфейсен слой.
3. Реализирани са инструменти за групово обработка и анализ на изображения, за прилагане на филтри и за построяване на хистограми в различни цветови пространства.

4. Оценена е реализацията на модулните методи чрез изследване устойчивостта на вградените данни срещу JPEG трансформации и проверка на качеството на изображенията.

5. Предложен е начин за приложение и са определени предимствата на модулния подход и методите за криене на данни в три сценария: за предотвратяване на фишинг на банкови портали, за защита на мултимедийната интелектуална собственост и за подобряване на законосъобразното използване на мултимедия в Интернет-базирани общества.

6. Разработена е програмна реализация на сертифицираща услуга за криене на данни, която може да се интегрира в различни интернет-базирани сценарии и предоставя достъп до функционалността на модулните методи за криене на данни.

### **Преценка на публикациите по дисертационния труд**

Резултатите от докторантурата са представени в 7 публикации. Една статия е публикувана в списанието „Доклади на БАН“, което е с импакт фактор, друга статия е публикувана в списанието „Information Technologies and Control“. Два доклада са изнесени на международни конференции на IEEE и IADIS. Три публикации, една от които е отличена с награда, са докладвани на национални научни конференции с международно участие. От публикациите 2 са самостоятелни, а в останалите 5 докторантът е на първо място. Не са представени данни за цитиране на публикациите. Считаю, че съществените приноси на дисертационния труд са отразени в публикациите.

Докторантът е участвал в проект от национална програма и в проект от 7-ма рамкова програма.

### **Мнения, препоръки и забележки**

Редакционните забележки не са съществени, но апелират за по-голяма строгост и прецизност на изложението:

- Имената на цитираните автори и техните университети в глави 1 и 2 са изписани на български, което крие възможност за грешно произнасяне. В същото време фигури 10,11 и частично 13,14 в Глава 3 (стр.31,32) са представени с английски термини.
- Макар и рядко се срещат неточни изрази, като "всеки цветови канал се състои традиционно от 8 бита" на стр. 65.

Към теоретичната част имам два въпроса:

- Базовият модул DCTHiderEngine за всеки блок пиксели определя различен брой DCT коефициенти (30-45 от 64). В тях се кодират скритите данни. При ниско ниво на JPEG компресия или рекомпресия на изображенията може да се очаква 100% устойчивост на кодирането (Табл.3 на стр.105). Как се определя граничното ниво на JPEG компресия, при което няма да има загуба на кодираните данни.
- Базовият модул за беззагубна компресия вгражда скритата информация в младшите битове на нивото на сиво във всеки пиксел (стр. 65). Тези битове най-често се променят при предварителната обработка. Може ли да съхрани кодираната информация без загуби след прилагане на гаусова, медианна филтрация на изображенията или изравняване на хистограмата.

Един практически въпрос: Трябва ли новите методи и алгоритми за стеганография да се предлагат от авторите с надеждни методи за стеганализ, за да се предотврати неконтролираното предаване на съобщения от недобросъвестни източници или е по-важно да се запази тяхната прозрачност и недостъпност.

Общото впечатление е, че дисертационният труд се отличава с точен език и добро владение на терминологията. Докторантът притежава задълбочени знания по криптография, стеганография и цифрово маркиране, за комуникационните мрежи и технологии, за цифровите мултимедии, както и за обработката на изображения. Той показва неоспорими умения да прилага тези знания за решаване на инженерни задачи.

### **ЗАКЛЮЧЕНИЕ**

Изпълнени са всички изисквания на ЗРАСРБ, на правилника за неговото приложение, както и специфичните изисквания за придобиване на научни степени в БАН по отношение на обхват, обем и качество на дисертационния труд. На тези основания предлагам на инж. Светозар Валериев Илчев да бъде присъдена образователната и научна степен **доктор** по "Компютърни системи, комплекси и мрежи".

10.03.2014 г.

гр. София