Abstracts of Dissertations

Institute of Information and Communication Technologies

BULGARIAN ACADEMY OF SCIENCES

4 / 2014

Modular methods for digital data embedding into images for the improvement of security on Internet-based communication platforms

Svetozar Ilchev

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

Светозар Илчев

Автореферати на дисертации

Институт по информационни и комуникационни технологии

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ISSN: 1314-6351

Поредицата ***„Автореферати на дисертации на Института по информационни и комуникационни технологии при Българската академия на науките“*** *представя в електронен формат автореферати на дисертации за получаване на научната степен „Доктор на науките” или на образователната и научната степен „Доктор”, защитени в Института по информационни и комуникационни технологии при Българската академия на науките. Представените трудове отразяват нови научни и научно-приложни приноси в редица области на информационните и комуникационните технологии като Компютърни мрежи и архитектури, Паралелни алгоритми, Научни пресмятания, Лингвистично моделиране, Математически методи за обработка на сензорна информация, Информационни технологии в сигурността, Технологии за управление и обработка на знания, Грид-технологии и приложения, Оптимизация и вземане на решения, Обработка на сигнали и разпознаване на образи, Интелигентни системи, Информационни процеси и системи, Вградени интелигентни технологии, Йерархични системи, Комуникационни системи и услуги и др.*

The series ***Abstracts of Dissertations of the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences*** *presents in an electronic format the abstracts of Doctor of Sciences and PhD dissertations defended in the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences. The studies provide new original results in such areas of Information and Communication Technologies as Computer Networks and Architectures, Parallel Algorithms, Scientific Computations, Linguistic Modelling, Mathematical Methods for Sensor Data Processing, Information Technologies for Security, Technologies for Knowledge management and processing, Grid Technologies and Applications, Optimization and Decision Making, Signal Processing and Pattern Recognition, Information Processing and Systems, Intelligent Systems, Embedded Intelligent Technologies, Hierarchical Systems, Communication Systems and Services, etc.*

e-ISSN: 1314-6351

BULGARIAN ACADEMY OF SCIENCES

Modular methods for digital data embedding into images for the improvement of security on Internet-based communication platforms

Svetozar Valeriev Ilchev

Supervisor: Assoc. Prof. Rumen Andreev

Approved by Supervising Committee:

Prof. Boyan Bonchev
Prof. Radoslav Pavlov
Acad. Ivan Popchev
Assoc. Prof, Pencho Venkov
Assoc. Prof. Rumen Andreev

INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES
Department of Communication Systems and Services

The Ph.D. thesis was discussed and allowed to be defended during an extended session of the Department "Communication systems and services" at IICT-BAS, which was held on 12.12.2013.

The Ph.D. thesis consists of 219 pages including 78 figurers, 7 tables and 10 pages bibliography containing 180 titles.

The defense of the Ph.D. thesis will be held on ……..… at ……. in room …….., building …… of IICT-BAS during an open session of the supervising committee consisting of the following members:

1. ……..
2. ……..….
3. ……..….
4. ……..…….
5. ……..…….

The materials for the defense of the Ph.D. thesis are at the disposal of the interested parties at IICT-BAS, Sofia, Acad. "G. Bonchev" str., Bl. 2.

Author: Svetozar Valeriev Ilchev

Title: Modular methods for digital data embedding into images for the improvement of security on Internet-based communication platforms

Keywords: data hiding, steganography, digital watermarking, image processing, image tampering detection, lossy compression, security, cryptography, signatures, Internet portals, social networks, web services, intellectual property protection

General description of the Ph.D. thesis

Research topic and motivation

The data hiding as a science has been first mentioned in ancient Greece [1]. First, it was known under the name "steganography" (from "steganos" - "covered, hidden" and "graphia" - "writing") [2]. The steganography at that time focused on the theoretical methods and practical applications of data embedding into different media. The end goals were to make the embedded information invisible for any uninformed third party and to do the embedding in such a way, that it was robust against the normal processing of the medium. Classical examples of the application of steganography are watermarks and metal threads hidden in banknotes, invisible inks and microprinting.

The progress of modern communication technologies and digital multimedia have led to a rekindled interest in steganography and its rebirth as a modern science bearing the more general name "multimedia data hiding" [3]. In the course of time, two main research branches of data hiding have been formed. The first research branch has inherited the ancient name of the science "steganography" and it deals with the transmission and storage of secret information. The second branch is called "digital watermarking". Its main topic is the protection of multimedia as intellectual property by embedding suitable additional information into the multimedia content [3], [4].

The research activities described in this thesis are directed mainly towards the hiding of data into compressed digital images. The main reason for this focus is the popularity of images and, in the latest years, short video clips in the global network. The results achieved by the methods for data embedding into images build the foundation for the creation of methods for data embedding into videos because most video formats encode the so called "key frames" using the same formats employed for digital images [5], [6], [7].

To implement effective multimedia data hiding, a good knowledge of a variety of research and application fields is necessary – e.g. signal processing in the frequency domain, compression of multimedia content, image, audio and video processing, number theory, coding theory, software engineering, cryptography, etc. An integral part of the data hiding into JPEG images is the application of the discrete cosine transform (DCT) in particular. Both images and embedded data are subjected to compression by arithmetic coding, run-length coding, Huffman coding, etc. The image processing encompasses the application of different kinds of filters and the creation of histograms used frequently in the algorithms for image analy-

sis/steganalysis. Error-correcting codes and coding techniques such as the quantization index modulation are used during the preparation of the data for embedding.

The software engineering finds application during the creation of the program architecture and the implementation of the program system. It ensures the provision of secure Internet-based communication with other systems. The object-oriented approach and a variety of communication protocols and formats employed in the Internet for data exchange and data storage are used in the creation of the program system in this thesis [8].

With regard to multimedia content, data hiding offers specialized solutions, which have several technological and legal advantages over general cryptographic approaches. Data hiding methods can be developed in such a way, that the embedded data are robust against frequently used transformations of the digital multimedia. The use of data hiding technologies is often invisible to end users. Data hiding methods embed information directly into the multimedia content. This eliminates the necessity of changes of the transmission or storage format caused by the presence of additional signatures, cryptographic hashes, etc. Steganographic data as well as digital watermarks are an integral part of the multimedia itself. In the absence of detailed information about the data hiding method in use, they cannot be removed in a reliable manner by unauthorized third parties without losing a substantial part of the multimedia content, which leads to a rapid decrease of its quality. In contrast to the existence of legal regulations regarding traditional cryptography in some countries, up to now steganography and digital watermarking remain unregulated [9].

One of the main goals of the Internet is its functioning as a universally accessible means of communication between people facilitating e-commerce and knowledge sharing [10]. Tim O'Reilly summarizes: "Network effects from user contributions are the key to market dominance in the Web 2.0 era." [11], [12], [13]. The creation of such global network effects depends to a large extent on the free flow of information and the free access to knowledge. In this context, data hiding complements and enhances existing cryptographic solutions [14] (Fig. 1).

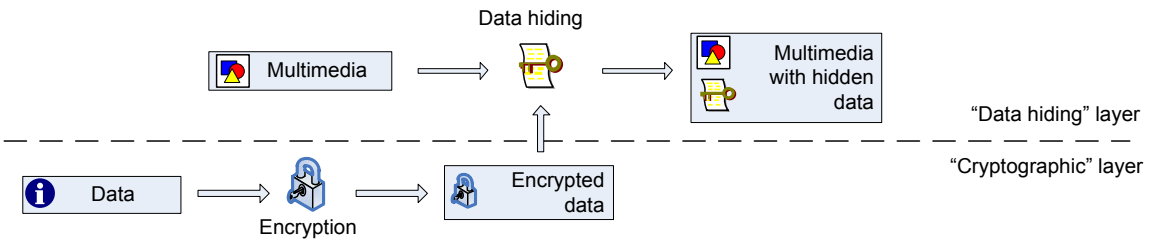


Fig. 1: Embedding of encrypted data into multimedia content

Data hiding methods can embed data or signatures obtained from various cryptographic methods. In this way, data hiding maintains the ease of access to the multimedia content. At the same time, it provides a difficult-to-discover and difficult-to-remove mechanism for the secret transmission of messages, storage of confidential data, tracking of authors, multimedia copies and legal users of the multimedia content. Data hiding web services can be offered and used as an additional enhancement of the cryptographic services used in a company. In contrast to cryptographic services, they ensure compatibility with systems that do not consider any security issues.

Main goal and tasks of the Ph.D. thesis

The main goal of the Ph.D. thesis is the development of a modular approach and modular methods for digital data hiding into images for the purpose of improving security on Internet-based communication platforms. The following tasks are laid down for the achievement of this goal:

1. Definition of the main drawbacks of existing methods for data hiding into multimedia with regard to their application in Internet-based scenarios.

2. Development of a modular approach for data hiding into multimedia for the purposes of network applications. According to this approach, every data hiding method consists of at least two modules – a basic module and an application-specific module.

3. Development of two basic modules and two application-specific modules for application in Internet-based scenarios. The use of the modules in different combinations leads to the creation of a total of four new modular methods for data hiding in multimedia.

4. Creation of the architecture of a program system and realization of the new methods by means of the .NET Framework of Microsoft.

5. Evaluation of the realization of the methods and their properties as well as the quality of the images resulting after the data embedding. This evaluation is used by the end user when choosing a suitable method for a given application scenario.

6. Analysis of the security of the modular methods from the point of view of the statistical steganalysis.

7. Provision of a suitable access to the modular methods by means of suitable web services and data exchange formats. The end goal is to facilitate the integration of the modular methods into general program solutions and infrastructures supporting practical Internet-based scenarios.

Solving the above tasks provides the opportunity to achieve a new higher level of security in different Internet-based scenarios.

List of publications

[1] S. Ilchev, "Accurate Data Embedding in JPEG Images for Image Authentication," *Comptes rendus de l'Acad´emie bulgare des Sciences*, vol. 66, no. 9, pp. 1247-1254, Sep. 2013, ISSN 1310-1331.

[2] S. Ilchev and R. Andreev, "Steganalysis Evaluation of Modular Data Hiding Methods," in *Proceedings of the International Conference "Automatics and Informatics'12"*, Sofia, Bulgaria, 2012, pp. 290-293, CD ISSN 1313-1869.

[3] S. Ilchev and Z. Ilcheva, "Modular Data Hiding as an Alternative of Classic Data Hiding for Web-based Applications," *Information Technologies and Control*, no. 1/2012, pp. 9-15, Jan. 2012, ISSN 1312-2622.

[4] S. Ilchev, "Modular Digital Watermarking Method for Image Tampering Detection," in *Proceedings of the International Conference "Automatics and Informatics'11"*, Sofia, Bulgaria, 2011, pp. B221-B224, ISSN 1313-1850, CD ISSN 1313-1869.

[5] S. Ilchev and Z. Ilcheva, "Protection of Intellectual Property in Web Communities by Modular Digital Watermarking," in *IEEE Signature Conference on Computers, Software and Applications (COMPSAC 2011), 35th IEEE Annual Computer Software and Applications Conference Workshops*, Munich, Germany, 2011, pp. 374-379, E-ISBN 978-0-7695-4459-5, Print ISBN 978-1-4577-0980-7, DOI 10.1109/COMPSACW.2011.69, INSPEC 12288790.

[6] S. Ilchev and Z. Ilcheva, "Modular Data Hiding Approach For Web Based Applications," in *Proceedings of the International Conference "Automatics and Informatics'10"*, Sofia, Bulgaria, 2010, pp. I253-I256, ISSN 1313-1850. **Best presented paper award.**

[7] S. Ilchev and Z. Ilcheva, "Modular data hiding for digital image authentication," in *Proceedings of the IADIS European Conference on Data Mining*, Freiburg, Germany, 2010, pp. 122-127, ISBN 978-972-8939-23-6.

One publication has been published in the journal with impact-factor "*Comptes rendus de l'Acad´emie bulgare des Sciences*", one publication has been published in the specialized journal "*Information Technologies and Control*", two publications have been presented at

specialized international scientific conferences organized by IEEE and IADIS. Three publications, one of which has been awarded a prize, have been presented at specialized national scientific conferences with international participation. Results from the Ph.D. thesis have also been presented at a scientific seminar of IICT.

Project participation

The Ph.D. student has participated in the following projects:

1. "Concerto Premium", financed as a tender of the European Commission Initiative "Concerto", Seventh Framework Programme, Research Theme: "Energy", contract № eu:15620-2011, file reference № ENER/C2/59-1/2010, project coordinator Steinbeis-Europa-Zentrum.
2. "Creation of an office for technology transfer "Information and communication technologies for energy efficiency (ICTEE)", financed by the operative program „Development of the competitiveness of the Bulgarian economy" 2007-2013, contract № BG161PO003-1.2.02-0001-C0001, beneficiary IICT-BAS.

Ph.D. thesis contents

This Ph.D. thesis consists of a total of 7 chapters, acknowledgment, declaration of originality of the results, bibliography and 2 appendices. The main content is laid down on 174 pages. The presentation is accompanied by figures and tables. The bibliography contains 180 titles.

Chapter 1. Introduction

General information about the development and application of multimedia data hiding is presented in this chapter.

1.1 Importance of the topic

This section discusses the modern scientific research branches of data hiding as well as its advantages over classical cryptographic methods with regard to the application in Internet-based scenarios.

1.2 Areas of application

With regard to Internet-based scenarios and applications, there are five main application areas of data hiding technologies [3], [15], which are shown in Fig. 2.

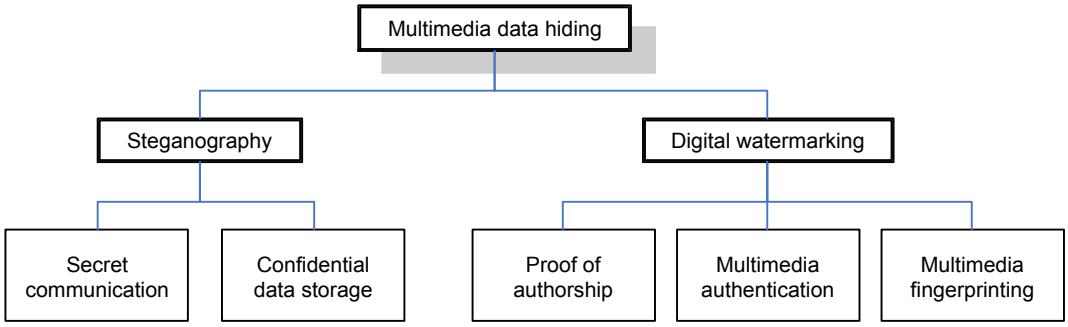


Fig. 2: Application areas of multimedia data hiding

Chapter 2. Analysis of existing methods and program products

In this chapter, several important properties of data hiding methods are defined with regard to their application in Internet-based scenarios. Some of the existing methods and program products for data hiding are reviewed and the realization of the properties is evaluated for each one of them.

2.1 Important properties of multimedia data hiding

Data hiding methods may have different properties such as the robustness against geometric transformations, image format changes or modifications of regions of the multimedia content. [16], [17]. Three properties are of special importance considering Internet-based scenarios: adaptability, robustness against JPEG-based transformations (compression, decompression, recompression) and the capability of working with arbitrary multimedia files and embedded data.

2.2 Existing methods and program products for multimedia data hiding

Because of the large number of existing data hiding methods, only methods based on DCT transformations are examined in this section and their robustness against the different kinds of JPEG transformations is evaluated.

None of the examined methods and products for data hiding considers the adaptability to end users' needs. The existing solutions are monolithic and they are developed for the purposes of specific applications with specific needs and cannot be changed at a later stage. The robustness against JPEG transformations is only partially considered and some JPEG transformations are often not taken into consideration. In addition, some products and methods – especially those built for digital watermarking applications – cannot work with arbitrary images or arbitrary user-defined data.

2.3 Conclusion

The conclusion outlines explicitly the main drawbacks of existing data hiding methods: monolithic construction, only partial robustness against JPEG transformations and inability to work with arbitrary images and embedded data.

Chapter 3. Modular approach for designing data hiding methods

---

In this chapter, the modular design of multimedia data hiding methods is discussed and its advantages are presented. Two modular methods - one for the purposes of steganography and

one for the purposes of digital watermarking – are created for applications in Internet-based scenarios. Their properties are described and discussed in detail.

3.1 Modular design – overview and architecture

During the design of the data hiding methods, they are regarded as composed of two types of modules – a basic module and an application-specific module. The two module types may form different combinations (Fig. 9). The modules are implemented using object-oriented programming (OOP) [8], [18].

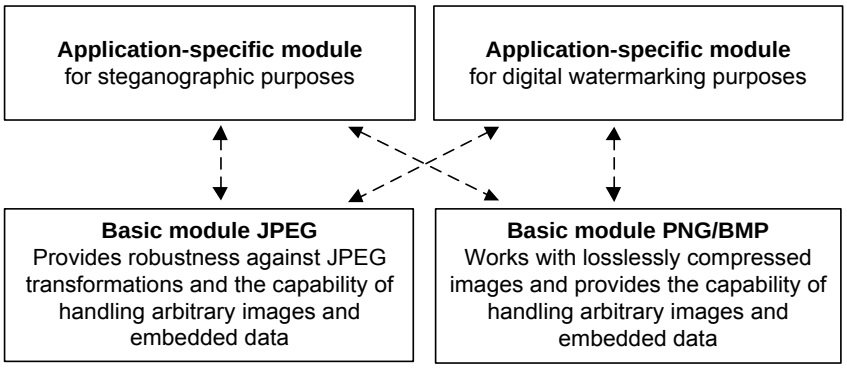


Fig. 9: Modular approach for multimedia data hiding for Internet-based applications

3.2 Basic module robust against JPEG transformations

This basic module is developed specifically for data embedding into images compressed and stored in the JPEG format.

3.2.1 Main goals of the module design and development

The main goals of the design and development of this module are the provision of robustness against JPEG compression, decompression and recompression, the capability of working with arbitrary images and embedded data, the independent extraction of the embedded data without any need of information about the original image as well as the error-free extraction and rebuilding of the embedded data. Good knowledge of the JPEG standard [19] and the JPEG File Interchange Format (JFIF) [20] is essential.

3.2.2 Overview of the JPEG standard

This section describes some of the details of the JPEG standard. The most important detail is the underlying two-dimensional DCT transform applied to each 8×8 pixel block:

$$A_{k,l} = \frac{c_k.c_l}{4} \sum_{m=0}^{7} \sum_{n=0}^{7} P_{m,n}.\, cos\left[\frac{(2m+1).k.\pi}{16}\right].\, cos\left[\frac{(2n+1).l.\pi}{16}\right],$$

where $P_{m,n}$ denotes the pixel block, $A_{k,l}$ denotes the DCT coefficients,

$$c_k = \begin{cases} \frac{1}{\sqrt{2}}, & for\ k = 0 \\ 1, & for\ k \neq 0 \end{cases},\ c_l = \begin{cases} \frac{1}{\sqrt{2}}, & for\ l = 0 \\ 1, & for\ l \neq 0 \end{cases} \text{ and } k, l, m, n \in [0; 7].$$

The image is represented by a standardized set of coefficients $A_{k,l}$. Each of them is subjected to a lossy compression through a division (quantization) by a corresponding element $Q_{k,l}$ of a user-defined quantization table Q and a subsequent rounding.

3.2.3 Basic module: encoding

The data encoding in the basic module consists of two stages: a *preparation stage* and a *finishing stage*. After the processing of the algorithm stages is complete, the resulting image containing the embedded data is passed to the application-specific module.

3.2.4 Guaranteeing robustness against JPEG compression, decompression and recompression

The embedding of data into the least significant bits of the DCT coefficients ensures the intrinsic robustness against JPEG compression and provides relatively good image quality for embedded data of a relatively large size [3]. The decompression of a JPEG image is almost always accompanied by errors caused by rounding errors or the limited representation of the respective color spaces – most often as a subset $S = \{0,1,2,\ldots,255\}$ of the set of natural numbers. The recompression is also almost always associated with information loss due to the differences in many coefficients of the JPEG quantization tables. An algorithmic description achieving robustness against the lossy decompression and recompression is presented.

3.2.5 Basic module: decoding

In contrast to the encoding, the decoding process consists of only one stage, which is similar to the *preparation stage* of the encoding process. The decoding process needs significantly less time in comparison to the full encoding process.

3.3 Application-specific module for steganographic purposes. Modular steganographic method

The application-specific module for steganographic purposes is developed for the embedding of a maximum quantity of data into a given image.

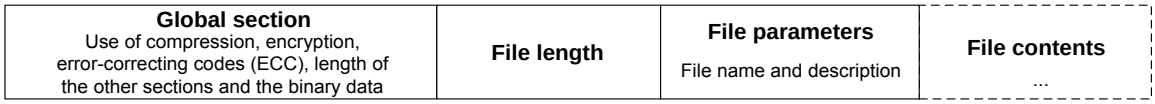


Fig. 20: Modular steganographic method – file headers

3.3.1 File headers

The file headers for the steganographic method are presented in Fig. 20.

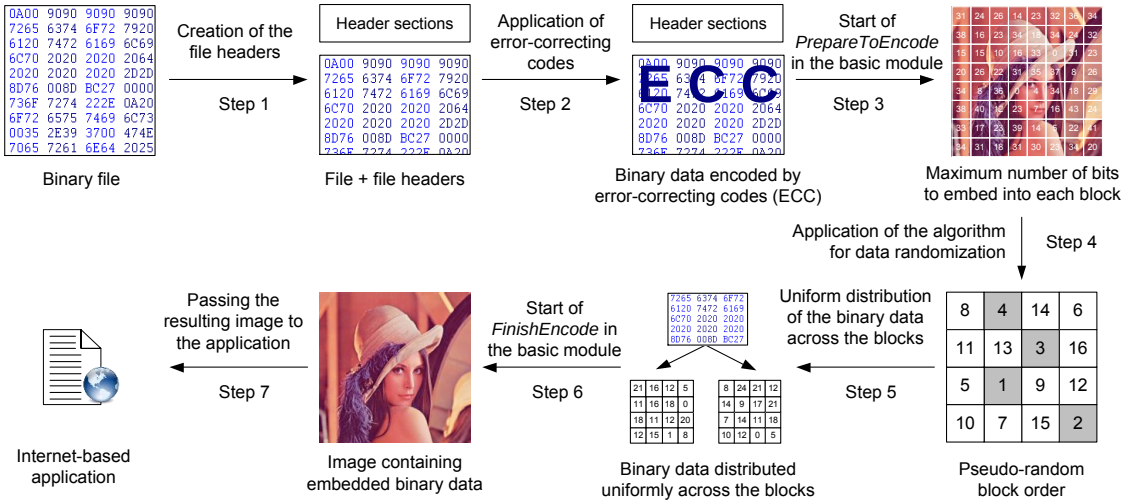


Fig. 24: Steganographic method - encoding

3.3.2 Error-correcting codes

The error-correcting codes used in this method are based on the algorithm of Hamming and allow the reliable discovery and correction of single-bit errors in each segment of the embedded data. Not relying on the optional use of such error-correcting codes, the developed basic module independently guarantees the robustness of the embedded data against JPEG transformations. This section also provides an algorithmic description of the used error-correcting scheme.

3.3.3 Data randomization

The data randomization uses a generator of pseudorandom numbers to generate permutations [21]. These permutations determine the blocks, into which data is embedded.

3.3.4 Data encoding

Besides the embedding of a maximum amount of data into the image, the encoding process also includes the creation of the file headers and the application of the algorithms for generating error-correcting codes and data randomization (Fig. 24).

3.3.5 Data decoding

The decoding process reverses the steps of the encoding process to extract and rebuild the embedded data and its file headers.

3.4 Application-specific module for digital watermarking purposes. Modular digital watermarking method

The application-specific module for digital watermarking purposes embeds small watermarks in such a way that they are robust against image modifications. The modified image regions can be identified by the method (Fig. 27).

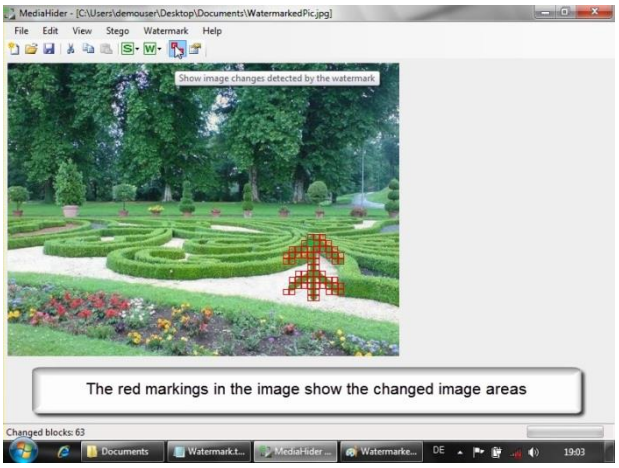


Fig. 27: Examination of an image containing unauthorized modifications of some JPEG blocks

3.4.1 File headers and error-correcting codes

The digital watermark file headers are simplified versions of the file headers used by the steganographic method. The error-correcting codes are identical. Their use is not obligatory.

3.4.2 Macroblocks

The algorithm for digital watermarking divides the image into several large areas called macroblocks. Each macroblock consists of a matrix of microblocks and contains a copy of the watermark.

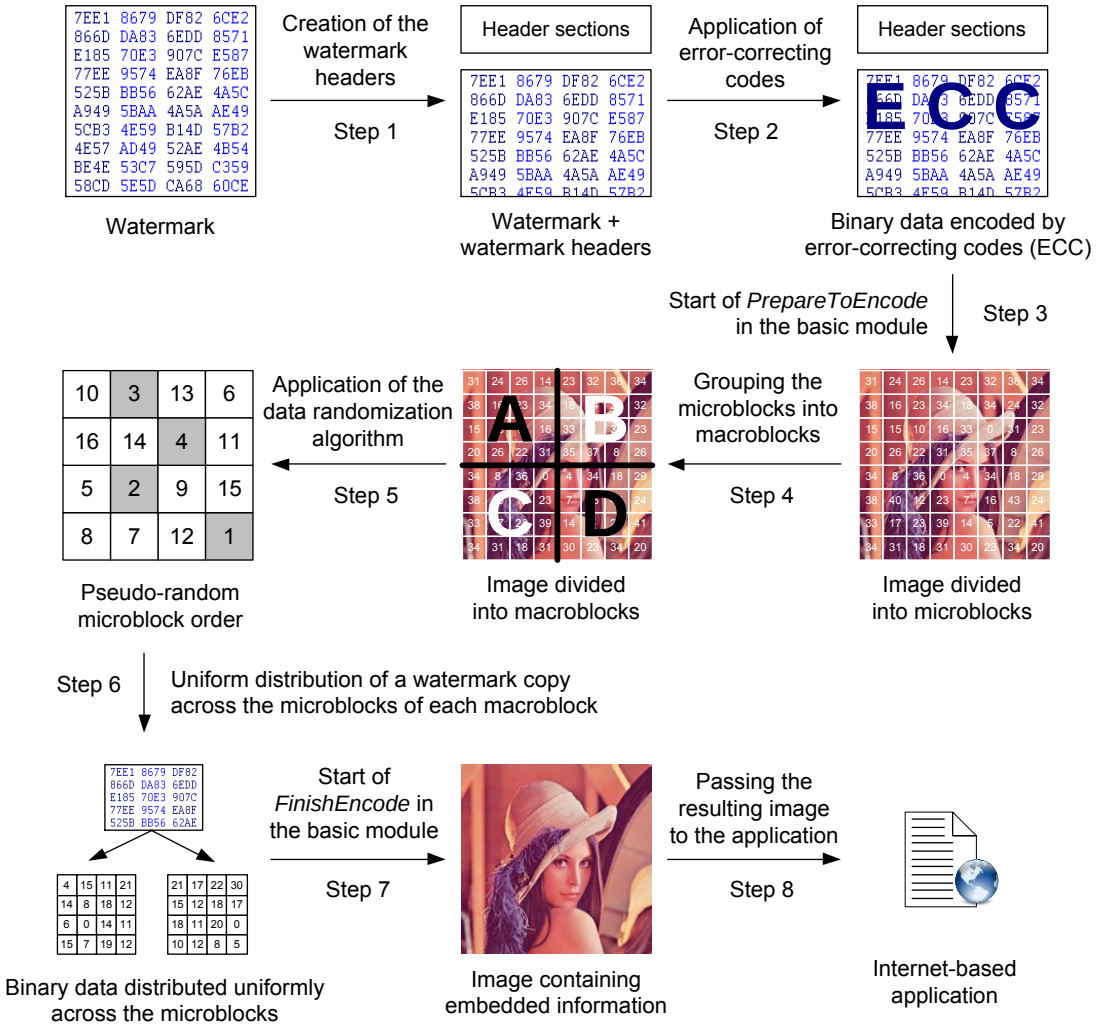


Fig. 32: Digital watermarking method - encoding

3.4.3 Discovery of image modifications and extraction of the watermark

During the decoding process, the watermark copies embedded into the individual macroblocks are extracted and compared to one another. If the size of the modified image regions is not too big, most copies will be identical to the original watermark. The remaining copies will contain differences, whose relative positions correspond to the modified microblocks of the macroblocks containing the changed watermark copy. As the basic module provides ro-

bustness against JPEG transformations, the embedded watermarks will remain unchanged after image modifications caused by JPEG compression, decompression or recompression. These modifications will not be regarded as such by the algorithm.

3.4.4 Watermark encoding

The encoding process which realizes the embedding of the watermark into the image macroblocks, consists of the steps shown in Fig. 32.

3.4.5 Watermark decoding

The decoding process reverses the steps of the encoding, extracts and rebuilds the watermark and discovers any image modifications.

3.5 Basic module for losslessly compressed images

The basic module presented in this section is developed for the verification of the modular approach and for the use of the steganographic and digital watermarking application-specific modules in conjunction with uncompressed (e.g. BMP) or losslessly compressed (e.g. PNG) images.

3.6 Conclusion

According to the modular approach for the design of data hiding methods, every property of a given method is realized either in the basic or the application-specific module constituting the method. This allows the addition or modification of properties of the methods thus achieving a degree of flexibility needed for their application in different Internet-based scenarios.

Chapter 4. Programming realization of the modular methods

The architecture of the program system is shown in Fig. 40.

In addition, a series of filters and tools for histogram image analysis have been implemented in the program system for use in the steganalysis. Among the implemented filters are the

mean, the Gaussian and the median filters, the Wiener-Kolmogorov filter and the Laplacian of Gaussian in the *RGB*, *Greyscale* and YC_bC_r color spaces.

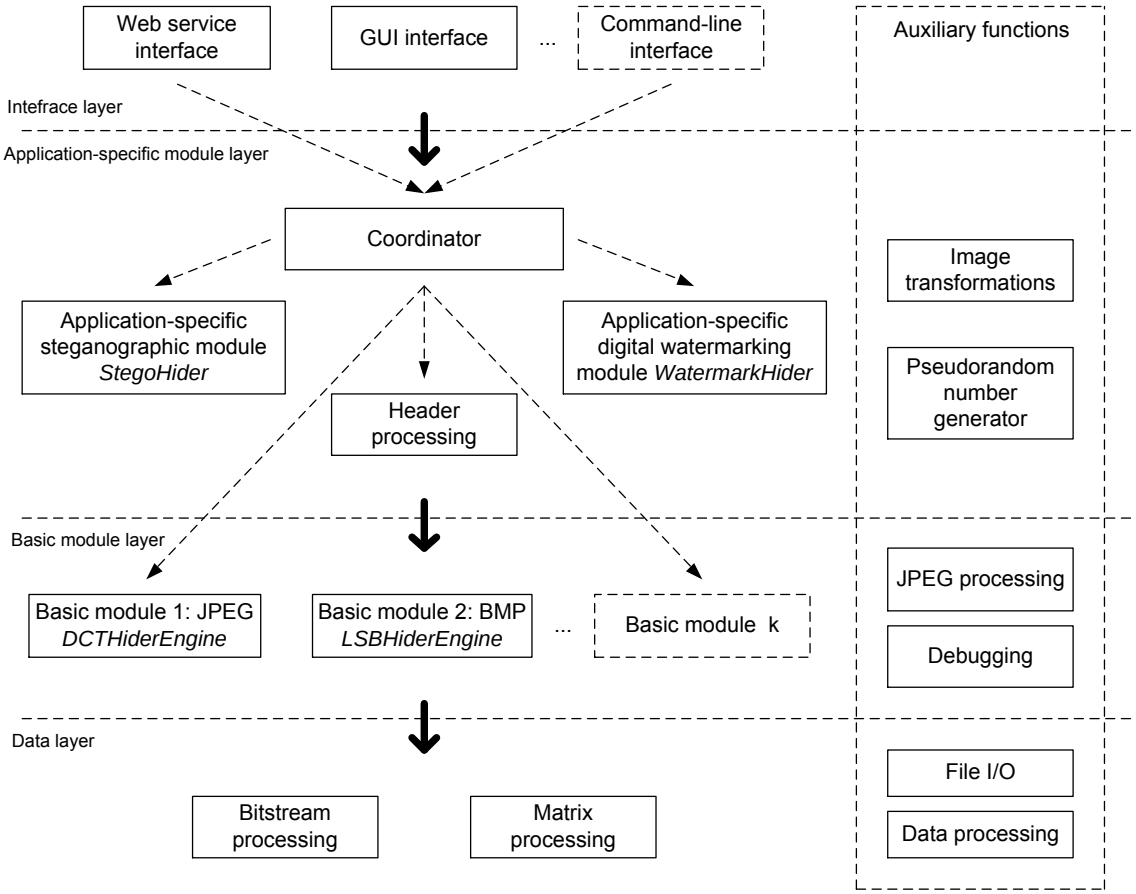


Fig.40: Program architecture - overview

The application programming interface for web services is implemented on the basis of the ASP.NET technology of Microsoft. The communication between the client and the server utilizes the SOAP protocol or regular HTTP GET or POST queries.

Chapter 5. Evaluation and steganalysis of the developed methods

---

The evaluation of the methods is made according to the following three criteria: i*mage quality, embedded data size* and *method properties*. One method cannot be optimized with regard to all three criteria simultaneously. As different application scenarios have different require-

ments, there is no single best data hiding method. The results of the evaluation of the two modular methods are summarized in Fig. 61.

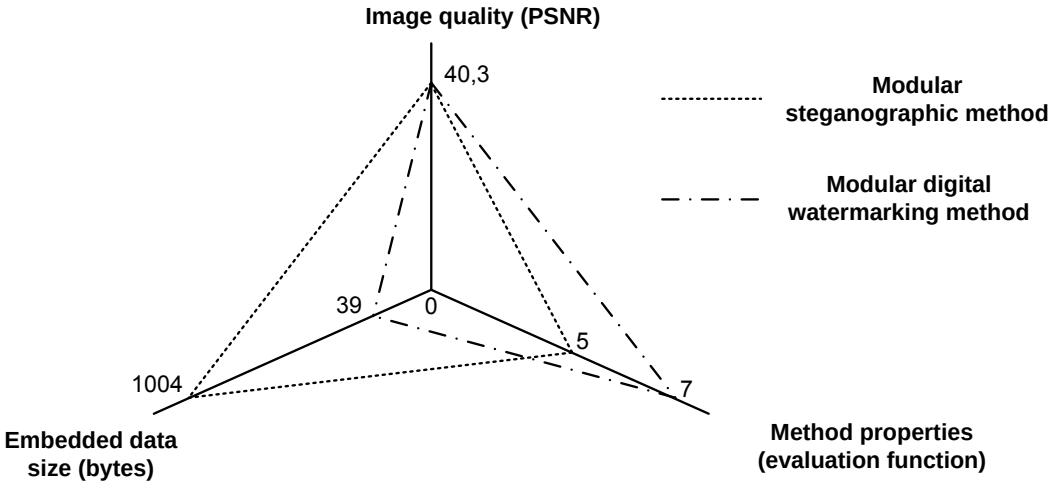


Fig. 61: Modular data hiding methods – evaluation results

This chapter also examines the invisibility of the embedded data to automated steganalysis methods and tools, which is one of the major requirements for the practical applicability of data hiding methods. The results obtained from some popular algorithms for steganalysis by using the open source program *Stegdetect* [22] show that existing statistical methods cannot discover the presence of data embedded by the modular methods. In addition, two principal approaches to steganalysis are examined. The first approach is based on the evaluation of correlations in the image and the second approach is based on noise level evaluations by image filtering. Both approaches show that the images resulting from the modular data hiding methods approximate natural images with very high degree of success.

Chapter 6. Application of the methods in Internet-based scenarios

This chapter discusses the practical application of the developed methods in several specific Internet-based scenarios: *phishing prevention for web portals*, *multimedia intellectual property protection for news agencies*, and *improvement of the legal use of multimedia content in Internet-based societies*, e.g. social networks and forums such as Facebook or DevianArt. In addition, an Internet-based data hiding certification service for multimedia content is designed and implemented in form of program code (Fig. 63). Its use in the above scenarios is

discussed in detail (Fig. 77). As the embedded signatures can be based on cryptographic approaches for protection, data hiding methods do not substitute but rather enhance traditional cryptography and give more latitude for its application.

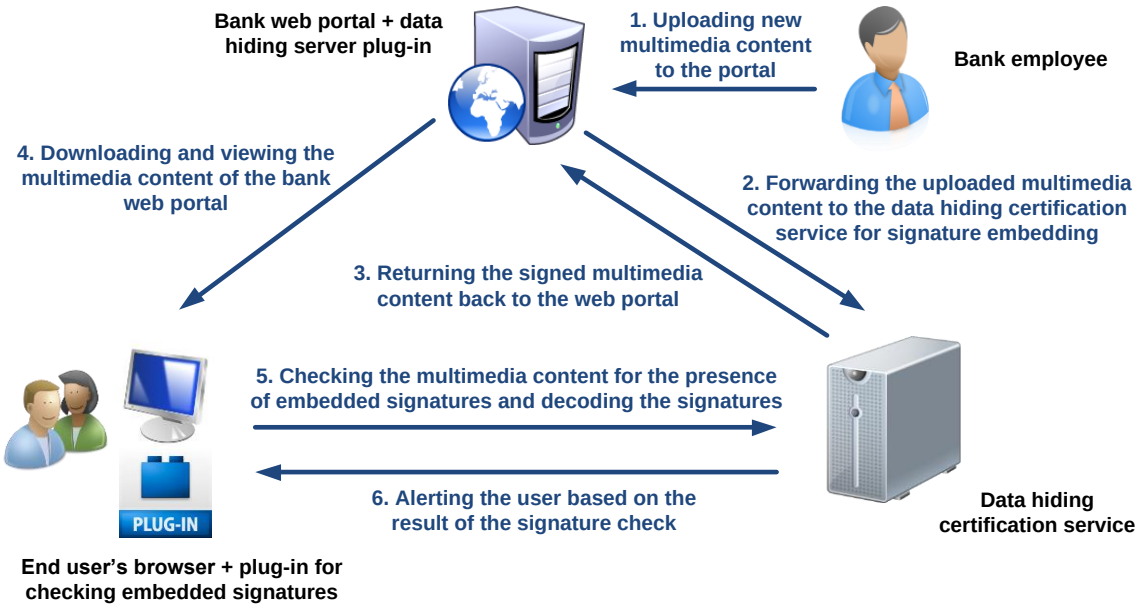


Fig. 63: Application of the modular methods as a data hiding certification service

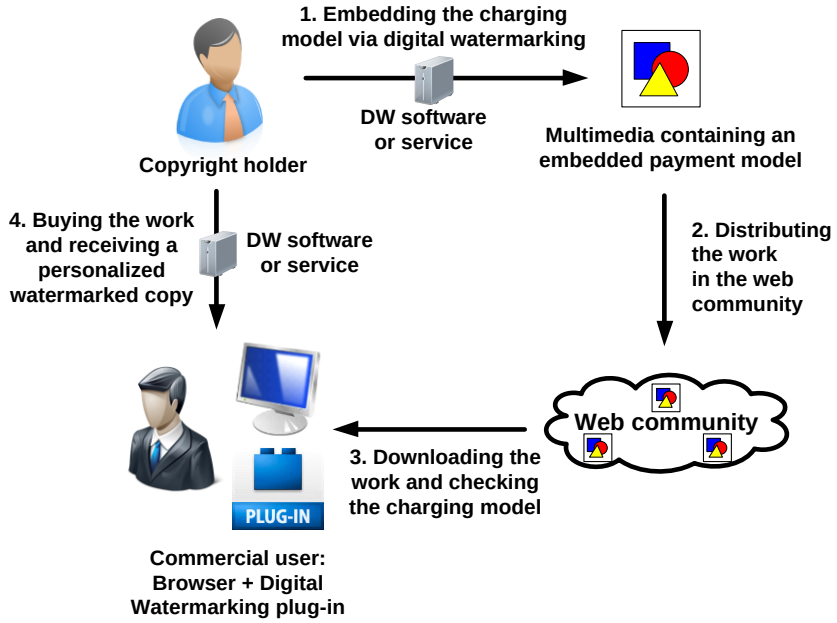


Fig. 77: Micropayment for multimedia works

Chapter 7. Conclusion – main results

The modular approach to data hiding makes possible the creation of extendable and adaptable data hiding methods robust against JPEG transformations and steganalysis. Because of the possibility for module reuse and adaptation to changes in the application requirements, modular data hiding methods can be created relatively quickly and at an affordable price. The web service communication interface and the characteristics of the methods developed specifically for use in Internet-based scenarios help with the integration of the data hiding technology in scenarios important for Internet users.

The future work on the modular data hiding approach may encompass the creation of a sufficiently large pool of modules that support popular and frequently used image formats, transformations, etc. In addition, a modular approach to steganalysis may be developed and a standardized suite of web service interfaces may be created for use with various possible Internet-based scenarios. The multimedia content is already an essential part of the Internet. Data hiding methods offer an effective way to protect this content. In the near future, they will become an indispensable part of the security mechanisms ensuring the users' safety.

Contributions

The main research and development contributions of the Ph.D. thesis are:

1. Creation of the concept of a modular approach to data hiding and definition of the communication process between the modules.

2. Design of a context-independent basic module which realizes a new method for the achievement of robustness against JPEG compression, decompression and recompression and works with arbitrary images and embedded data. Furthermore, it guarantees the recovery of the embedded data with single-bit accuracy.

3. Design of a context-independent basic module for use with losslessly compressed images. It is based on the quantization index modulation and works with arbitrary images and embedded data and guarantees the recovery of the embedded data with single-bit accuracy.

4. Design of a steganographic data hiding method which includes a steganographic application-specific module, file headers for the embedded files as well as error-correcting codes and data randomization.

5. Design of a digital watermarking method which includes a digital watermarking application-specific module, watermark headers as well as the capability of finding modified image regions and the extraction of the watermark in the case of a modified image.

6. Creation of a multi-tier architecture of the prototype program system for the purposes of verification, evaluation and steganalysis of the modular data hiding approach and the developed modular methods.

7. Investigation and evaluation of the effectiveness of some popular and frequently used steganalysis algorithms with regard to the modular data hiding methods. Investigation and evaluation of the effectiveness of two principal approaches to steganalysis: one approach based on the examination of correlations in the image and one approach based on the application of filters for noise level analysis.

The main applied contributions of the Ph.D. thesis are:

1. Implementation of the prototype program system using the programming languages VB.NET, C# and C/C++. It consists of the following layers: data layer, basic module layer, application-specific module layer and interface layer.

2. Design and implementation of tools for group processing and analysis of images as well as for filter and histogram processing in different color spaces.

3. Evaluation of the results of the modular methods by examining the robustness of the embedded data against JPEG transformations and measuring the image quality.

4. Investigation of the application and the advantages of the modular approach and the modular methods for data hiding in three scenarios: a scenario for phishing prevention for bank web portals, a scenario for multimedia intellectual property protection for news agencies and a scenario for the improvement of the legal use of multimedia content in Internet-based societies.

5. Design and program implementation of a data hiding certification service that can be integrated into various Internet-based application scenarios and provides access to the modular data hiding methods developed and evaluated in the Ph.D. thesis.

Bibliography

[1] Herodotus, *Histories, Book 5*., 440 B.C.

[2] J. Peterson. (1997) Steganographia (Secret Writing), by Johannes Trithemius. [Online]. URL: http://www.esotericarchives.com/tritheim/stegano.htm (accessed August 9, 2012).

[3] I. J. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2nd ed.: Morgan Kaufmann Publishers, 2008.

[4] E. Lin and J. Delp, "A Review of Data Hiding in Digital Images," in *Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS '99)*, Savannah, Georgia, 1999, pp. 274-278.

[5] Y. Shi and H. Sun, *Image and Video Compression for Multimedia Engineering*, 1st ed.: CRC Press, 2000.

[6] J. Mitchell, W. Pennebaker, C. Fogg, and D. LeGall, *MPEG Video Compression Standard*, 1st ed.: Kluwer Academic Publishers, 2002.

[7] A. Uhl and A. Pommer, *Image and Video Encryption*, 1st ed.: Springer, 2005.

[8] G. Booch et al., *Object-Oriented Analysis and Design with Applications*, 3rd ed.: Addison-Wesley, 2007.

[9] Electronic Privacy Information Center. Cryptography Policy. [Online]. URL: http://www.epic.org/crypto/ (accessed May 18, 2011).

[10] World Wide Web Consortium. About W3C: Goals. [Online]. URL: http://www.w3.org/Consortium/mission (accessed March 24, 2011).

[11] T. O'Reilly. (2005) What is Web 2.0. [Online]. URL: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html?page=1 (accessed May 9, 2011).

[12] T. O'Reilly. (2006) Web 2.0 Compact Definition: Trying Again. [Online]. URL: http://radar.oreilly.com/2006/12/web-20-compact-definition-tryi.html (accessed May 9, 2011).

[13] T. O'Reilly. (2006) Harnessing Collective Intelligence. [Online]. URL: http://radar.oreilly.com/2006/11/harnessing-collective-intellig.html (accessed May 9, 2011).

[14] M. Backes and C. Cachin, "Public-key steganography with active attacks," in *2nd Theory of Cryptography Conference (TCC)*, vol. 3378 of Lecture Notes in Computer Science, 2005, pp. 210-226.

[15] E. Cole, *Hiding in Plain Sight: Steganography and the Art of Covert Communication*,

1st ed.: John Wiley & Sons, 2003.

[16] S. Voloshynovskiy, F. Deguillaume, O. Koval, and T. Pun, "Information-theoretic Data-hiding: Recent Achievements and Open Problems," *International Journal of Image and Graphics*, vol. 5, no. 1, pp. 1-31, 2005.

[17] E. Lin and E. Delp, "A Review of Fragile Image Watermarks," in *Proceedings of the Multimedia and Security Workshop (ACM Multimedia '99)*, 1999, pp. 25-29.

[18] M. Weissfeld, *The Object-Oriented Thought Process*, 3rd ed.: Addison-Weslez, 2008.

[19] W. B. Pennebaker and J. L. Mitchell, *JPEG Still Image Data Compression Standard*, 1st ed.: Van Rostrand Reinhold, New York, 1993.

[20] E. Hamilton. (1992, September) JPEG File Interchange Format. [Online]. URL: http://www.w3.org/Graphics/JPEG/jfif3.pdf (accessed March 16, 2011).

[21] D. Knuth, *The Art of Computer Programming*, 3rd ed.: Addison-Wesley, 1998, vol. 2.

[22] N. Provos. (2008) Steganography Detection with Stegdetect. [Online]. URL: http://www.outguess.org/detection.php (accessed May 12, 2011).

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

АВТОРЕФЕРАТ НА ДИСЕРТАЦИЯ

за присъждане на образователна и научна степен "доктор" по научна специалност 02.21.04 „Компютърни системи, комплекси и мрежи"

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

Светозар Валериев Илчев

Ръководител: доц. Румен Андреев

Научно жури:

Проф. Боян Бончев
Проф. Радослав Павлов
Доц. Пенчо Венков
Акад. Иван Попчев
Доц. Румен Андреев

Институт по информационни и комуникационни технологии
Секция "Комуникационни системи и услуги"

Дисертацията е обсъдена и допусната до защита на разширено заседание на секция „Комуникационни системи и услуги“ на ИИКТ-БАН, състояло се на 12.12.2013 г.

Дисертацията съдържа 219 стр., в които 78 фигури, 7 таблици и 10 стр. литература, включваща 180 заглавия.

Защитата на дисертацията ще се състои на …… от ……. часа в зала …….. на блок …… на ИИКТ-БАН на открито заседание на научно жури в състав:

1. ……..
2. ……..
3. ……..
4. ……..
5. ……..

Материалите за защитата са на разположение на интересуващите се в ИИКТ-БАН, София, ул. „Акад. Г. Бончев“, бл. 2.

Автор: Светозар Валериев Илчев

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

Обща характеристика на дисертацията

Област на изследване и мотивация

Криене на данни (англ. data hiding) е модерното име на класическа наука, водеща началото си от древна Гърция [1]. Първоначално тя е известна под името стеганография – съставено от гръцките думи “steganos“ (“покрит, таен”) и “graphia” (“писане”) [2]. Стеганографията по това време е наука, фокусирана върху теоретичните методи и практическите приложения на скриването на тайна информация в различни видове носещи среди. Целта е скритата информация да бъде невидима за неинформирания потребител и да не се влияе от нормалните обработки на носещата среда, в която е вградена. Класически примери за приложението на стеганографията са водните знаци и защитните метални нишки, скрити в банкнотите, невидимите мастила и микро-печатът, който използва шрифтове с изключително малък размер (< 0.5 мм.), възприемани като тънка линия от невъоръженото човешко око.

Прогресът на модерните комуникационни технологии и цифровата мултимедия са причината за възобновяването на интереса към стеганографията и формирането ѝ като модерна наука, носеща вече по-общото наименование „криене на данни в мултимедия“ (англ. multimedia data hiding) [3]. С течение на времето се оформят две основни научноизследователски направления: първото направление наследява древното име на тази наука – стеганография, а второто направление е наречено цифрово маркиране (англ. digital watermarking) [3], [4].

Модерната стеганография изучава кодирането и откриването на тайни съобщения, предавани през цифрови комуникационни канали и платформи. Стеганографските методи скриват наличието на произволни цифрови съобщения посредством тяхното кодиране като обичайна част от съдържанието на друго цифрово мултимедийно съдържание. По този начин те правят откриването на тези съобщения от потенциални неоторизирани трети лица много трудно [5]. В последните няколко години значението на стеганографията се преосмисли от редица правителства с оглед на рисковете от обмен на информация между терористични организации с цел терористични атаки [6], [7].

Цифровото маркиране, за разлика от стеганографията, има за основна цел да подобри защитата на интелектуалната собственост и да позволи проверка на автентичността на цифровите медии [8]. По подобие на стеганографските методи, методите за цифрово маркиране крият информация като неразделна част от съдържанието на съответната цифрова мултимедия. Разликата се състои в целта, постигана от скритата информация – тя не е произволно съобщение, а характеризира цифровата мултимедия, в която е скрита, като идентифицира нейния автор, купувач или потвърждава автентич-

ността на мултимедийното съдържание. Методите за цифрово маркиране помагат при проследяване на разпространението на цифровата мултимедия в глобалната мрежа. Те предоставят нови начини за адекватна защита на притежателите на авторски права в процеса на разпространение на интелектуалната собственост [9].

Научноизследователската дейност, описана в тази дисертация, е насочена основно към криене на данни в компресирани цифрови изображения. Основната причина за този акцент е огромната популярност на изображенията, а в последните години и на кратките видео клипове, в глобалната мрежа. Резултатите, постигнати от методите за криене на данни в изображения, образуват основата, на която се базират методите за криене на данни във видео, тъй като повечето видео формати кодират своите т. нар. „ключови кадри" (англ. key frames) във формати за кодиране на цифрови изображения [10], [11].

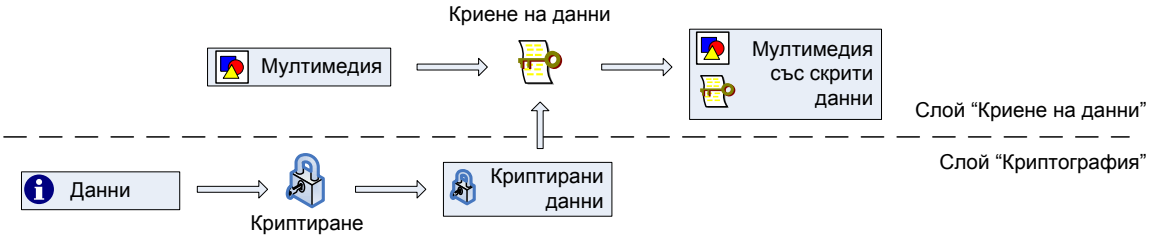
За реализирането на ефективно криене на данни в мултимедия е необходимо доброто познаване на редица научни и приложни области като обработка на сигнали в честотната област, компресия на мултимедийно съдържание, обработка на изображения, аудио и видео, теория на числата, теория на кодирането, софтуерно инженерство, криптография и др. Неделима част от криенето на данни в JPEG изображения е прилагането в частност на дискретната косинусова трансформация (англ. discrete cosine transform, DCT), характерна за формата на компресия JPEG. Както изображенията, така и вгражданите данни се подлагат на компресия чрез аритметично кодиране, кодиране с дължини на сериите (англ. run-length coding), Хъфман кодиране и др. Обработката на изображения включва прилагането на различни видове филтри и построяването на хистограми, използвани често при алгоритмите за анализ/стеганализ на изображенията. При подготовката на данните за вграждане се използват кодове за корекция на грешки и техники на кодиране като модулацията на индекса на квантизация.

Софтуерното инженерство намира приложение при изготвянето на архитектурата и реализацията на програмната система, както и при осигуряването на надеждна Интернет-базирана комуникация с други системи. В дисертацията се използва обектно-ориентирания подход за създаване на програмни системи [12], както и редица протоколи и формати за обмен и съхранение на данни, характерни за Интернет.

По отношение на мултимедийното съдържание криенето на данни може да предложи специализирани решения, които имат редица технологични и правни предимства пред общоприложимите криптографски подходи. Методите за криене на данни могат да бъдат разработени така, че скритите данни да са устойчиви на често прилагани трансформации на цифровата мултимедия. Приложението на технологии за криене на данни в мултимедия обикновено е незабележимо за потребителите. Методите за криене на данни вграждат информация директно в мултимедийното съдържание. При тях не се налага промяна във формата за запомняне и предаване на мултимедията поради наличие на допълнителни сигнатури, криптографски хеш-стойности и др. Стеганографската информация, както и вградените цифрови маркери са интегрална част от самата мул-

тимедия и не могат да бъдат надеждно премахнати (без информация относно използваните методи) от неоторизирани трети лица, без да се загуби значителна част от мултимедийното съдържание, което води съответно до рязко влошаване на неговото качество. На този етап стеганографията и цифровото маркиране не подлежат на правно (законово) регулиране, характерно за традиционната криптография в някои страни [13].

Една от основните цели на Интернет е предоставянето на универсално достъпно средство за комуникация между хората, търговия и споделяне на знание [14]. Тим О'Райли обобщава: "Мрежовите ефекти от приносите на потребителите са ключът към доминирането на пазара в ерата на „Уеб 2.0" [15], [16], [17]. Създаването на такива глобални мрежови ефекти зависи до голяма степен от свободния поток на информацията и свободния достъп до знанието. Криенето на данни в мултимедия може да допълни и подобри съществуващите криптографски решения [18] (Фиг. 1). Методите за криене на данни могат да вграждат данни или сигнатури, получени от различни криптографски методи. По този начин криенето на данни в мултимедия запазва възможността за лесен достъп до мултимедийното съдържание и осигурява труден за откриване и отстраняване механизъм за предаване на тайни съобщения, за съхраняване на поверителна информация, както и за проследяване на авторите, цифровите копия и законните притежатели на мултимедийно съдържание. Мрежови услуги за криене на данни в мултимедия могат да бъдат предоставени и използвани в допълнение и като надграждане на криптографските услуги, използвани в дадена компания. За разлика от криптографските услуги, те осигуряват съвместимост със системи, които не вземат предвид проблеми, свързани със сигурността.



Фиг. 1: Криене на криптирани данни в мултимедия

Цел и задачи на дисертацията

Целта на дисертацията е разработването на модулен подход и модулни методи за вграждане на цифрова информация в изображения за подобряване сигурността на Интернет-базирани комуникационни платформи. За постигането на тази цел са формулирани следните задачи:

1. Определяне на основните недостатъци на съществуващите методи за криене на данни в мултимедия по отношение на тяхното приложение в Интернет-базирани сценарии.
2. Разработване на модулен подход за криене на данни в мултимедия за целите на мрежовите приложения. Съгласно този подход всеки метод за криене на данни се състои от най-малко два модула – базов модул и приложно-специфичен модул.
3. Разработване на два базови и два приложно-специфични модула, подходящи за приложение в Интернет-базирани сценарии. Използването на модулите в различни комбинации води до създаването на общо четири нови модулни метода за криене на данни в мултимедия.
4. Създаване на архитектура на програмна система и програмно реализиране на новите методи с помощта на т.нар. .NET платформа (.NET Framework) на Майкрософт.
5. Оценяване на реализацията на методите и техните свойства и на качеството на получените в резултат от тяхната работа изображения. Оценката се използва от крайния потребител при избор на подходящ метод в даден приложен сценарий.
6. Анализ на сигурността на модулните методи от гледна точка на статистическия стеганализ.
7. Осигуряване на подходящ достъп до модулните методи за криене на данни чрез предоставянето на подходящи мрежови услуги и формати за обмен на данни. Цели се лесно включване на модулните методи към цялостни програмни решения и инфраструктури за реализиране на практически насочени Интернет-базирани сценарии.

Решаването на горните задачи дава възможност за постигането на ново по-високо ниво на сигурност в различни Интернет-базирани сценарии.

Списък на публикациите по дисертацията

[1] S. Ilchev, "Accurate Data Embedding in JPEG Images for Image Authentication," *Comptes rendus de l'Acad´emie bulgare des Sciences*, vol. 66, no. 9, pp. 1247-1254, Sep. 2013, ISSN 1310-1331.

[2] S. Ilchev and R. Andreev, "Steganalysis Evaluation of Modular Data Hiding Methods," in *Proceedings of the International Conference "Automatics and Informatics'12"*, Sofia, Bulgaria, 2012, pp. 290-293, CD ISSN 1313-1869.

[3] S. Ilchev and Z. Ilcheva, "Modular Data Hiding as an Alternative of Classic Data Hiding for Web-based Applications," *Information Technologies and Control*, no. 1/2012, pp. 9-15, Jan. 2012, ISSN 1312-2622.

[4] S. Ilchev, "Modular Digital Watermarking Method for Image Tampering Detection," in *Proceedings of the International Conference "Automatics and Informatics'11"*, Sofia, Bulgaria, 2011, pp. B221-B224, ISSN 1313-1850, CD ISSN 1313-1869.

[5] S. Ilchev and Z. Ilcheva, "Protection of Intellectual Property in Web Communities by Modular Digital Watermarking," in *IEEE Signature Conference on Computers, Software and Applications (COMPSAC 2011), 35th IEEE Annual Computer Software and Applications Conference Workshops*, Munich, Germany, 2011, pp. 374-379, E-ISBN 978-0-7695-4459-5, Print ISBN 978-1-4577-0980-7, DOI 10.1109/COMPSACW.2011.69, INSPEC 12288790.

[6] S. Ilchev and Z. Ilcheva, "Modular Data Hiding Approach For Web Based Applications," in *Proceedings of the International Conference "Automatics and Informatics'10"*, Sofia, Bulgaria, 2010, pp. I253-I256, ISSN 1313-1850. **Best presented paper award.**

[7] S. Ilchev and Z. Ilcheva, "Modular data hiding for digital image authentication," in *Proceedings of the IADIS European Conference on Data Mining*, Freiburg, Germany, 2010, pp. 122-127, ISBN 978-972-8939-23-6.

Една публикация е публикувана в списание с импакт фактор „*Доклади на БАН*“, една публикация е публикувана в специализирано списание „*Information Technologies and Control*“, две публикации са докладвани на специализирани международни конференции на IEEE и IADIS. Три публикации, една от които е отличена с награда, са докладвани на специализирани национални научни конференции с международно участие. Резултати от дисертацията са представени и на научен семинар на ИИКТ.

Участие в проекти

Докторантът е взел участие в следните проекти:

1. „Concerto Premium”, финансиран като тендър по инициативата „Кончерто“ на Европейската комисия, Седма Рамкова Програма, Научна Тема: „Енергия“, договор № eu:15620-2011, референтен № ENER/C2/59-1/2010, координатор на проекта Steinbeis-Europa-Zentrum.
2. „Създаване на офис за технологичен трансфер „Информационни и комуникационни технологии за енергийна ефективност (ИКТЕЕ)“, финансиран по оперативна програма „Развитие на конкурентоспособността на българската икономика“ 2007-2013, договор № BG161PO003-1.2.02-0001-C0001, бенефициент: ИИКТ – БАН.

Съдържание на дисертацията

Настоящата дисертация се състои от общо 7 глави, благодарности, декларация за оригиналност на резултатите, списък на цитираната литература и 2 приложения. Основното съдържание е поместено на 174 страници, а изложението е придружено с фигури и таблици. Списъкът на цитираната литература включва 180 заглавия.

Глава 1. Увод

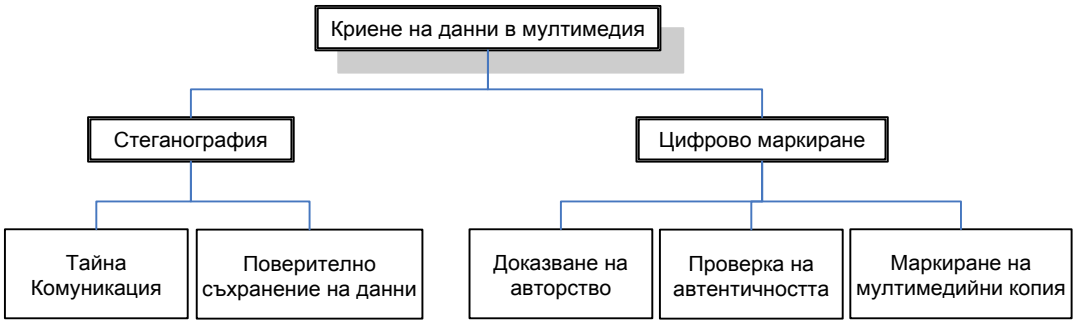
В тази глава е представена обща информация за развитието и приложението на криенето на данни в мултимедия.

1.1 Актуалност на проблема

Този раздел дискутира съвременните научни направления на криенето на данни както и предимствата пред класическите криптографски методи за приложения в Интернет-базирани сценарии.

1.2 Области на приложение

По отношение на Интернет-базираните сценарии и приложения, съществуват пет основни приложни области на технологиите за криене на данни в мултимедия [3], [6], които са показани на Фиг. 2.



Фиг. 2: Области на приложение на криенето на данни в мултимедия

В следващите раздели се разглеждат няколко примера, показващи практическата полза от криенето на данни и възможностите за интеграция в модерните Интернет-базирани бизнес процеси, включващи мрежова комуникация и разпространение на интелектуална собственост.

1.2.1 Тайна комуникация

Този пример дискутира сливането на две акционерни дружества, чиито акции се търгуват на фондовите борси. Подобно сливане обикновено има голямо въздействие върху финансовите пазари и двете компании се опитват да го запазят в тайна. Те трябва да комуникират една с друга, за да договорят условията на сливането, но дори самото наличие на повишена комуникация между тях може да послужи като индикатор за

предстоящо сливане на компаниите, от което финансовите спекуланти да се възползват. Интернет е несигурна комуникационна среда и двете компании не са сигурни кой би могъл да наблюдава техните комуникации и с каква цел.

Традиционните криптографски подходи не са полезни в тази ситуация, тъй като те не могат да скрият факта, че значителна по обем информация се обменя между компаниите. На базата на повишения обем на комуникацията и текущото икономическо положение, предстоящото сливане лесно може да бъде предвидено.

1.2.2 Доказване на авторство

Този пример се отнася до новинарската агенция *A*, която поддържа и обновява информационен портал в Интернет. Конкурентната новинарска агенция *B* сваля снимките, придружаващи новинарските статии от Интернет портала на *A*, и ги използва в изданията на своя собствен Интернет вестник. *A* би желала да докаже, че тя е законният собственик на снимките и да изобличи действията на *B* като нарушения на авторското право. Тъй като цифровите данни, описващи снимките могат лесно да бъдат променени, шансът за успех на *A* не е голям.

Традиционните криптографски подходи не могат да предотвратят незаконното присвояване на авторско съдържание или да помогнат при доказването на авторски права върху снимките, ако те вече са направени публично достъпни в Интернет..

1.2.3 Проверка на автентичността на мултимедия

Да разгледаме пример, в който водеща машиностроителна компания, е внедрила мрежа от камери за наблюдение в свое предприятие. Камерите са свързани към Интернет и автоматично архивират всички изображения на централен сървър. Един ден в една от производствените сгради е установена липсата на нов прототип. Записът от камерите показва как нарушители са влезли неправомерно в сградата. Заснето е също така лицето на един от работниците, който твърди, че е невинен.

За да се гарантира, че записът от камерите е надеждно доказателство, компанията се нуждае от средство за проверка, че записът е оригинален и не е бил променян от момента на неговото създаване. Това би могло да се направи с помощта на криптографски подходи [19], но цифровото маркиране предлага допълнително възможността за откриване на точните региони от записа, които са били неправомерно променени. Това се постига чрез вграждането (в записите от камерите) на специални сигнатури, наречени крехки водни знаци, които се разрушават в случай на промяна на изображението, в което са вградени. В допълнение към откриването на променени региони, съществуват специализирани методи за цифрово маркиране, които позволяват частичното възстановяване на оригиналното съдържание [20].

В този пример методите за цифрово маркиране могат да потвърдят, че регионът от записа на камерите, съдържащ лицето на работника, е бил неправомерно променен. Възможно е дори да се възстанови лицето на реалния извършител и това да доведе до заключението, че работникът е невинен. Останалата информация относно начина, по който е била извършена кражбата, е автентична и може да се използва в хода на разследването.

1.2.4 Маркиране на мултимедийни копия

Този пример е вдъхновен от истински случай, описан в Интернет [21].

Художник създава цифрови картини (интелектуална собственост). Той има агент, който се грижи за показването на картините в (Интернет) галерии и тяхната продажба на индивидуални клиенти. Художникът записва своите нови творби на сървъра на агента си и получава от него известия за хода на продажбите. Един ден художникът намира част от своите произведения свободно достъпни в Интернет, въпреки клаузи в договора с галериите и крайните клиенти, които забраняват разпространението на творбите. Художникът би искал да предотврати подобни инциденти в бъдеще, както и да съди нарушителя за щети, изисквайки материална компенсация.

Традиционните криптографски подходи не могат да помогнат в такава ситуация. Те не могат да предотвратят надеждно разпространението на творбите или да идентифицират нарушителя. Всяка оторизирана галерия или краен купувач могат да разгледат криптирана картина, което означава, че те могат да репродуцират творбата и премахнат криптографската защита. Това им дава свободата да разпространяват картината в Интернет, без да оставят следи, водещи до разкриването на тяхната самоличност.

Глава 2. Анализ на съществуващите методи и програмни продукти

В тази глава се дефинират някои важни свойства на методите за криене на данни в мултимедия по отношение на приложението им в Интернет-базирани сценарии. Разглеждат се някои от съществуващите методи и програмни продукти в областта, като се оценява реализацията на свойствата във всеки един от тях.

2.1 Важни свойства на криенето на данни в мултимедия

Методите за криене на данни в мултимедия могат да имат различни свойства като устойчивост срещу геометрични трансформации, промени на формата, промяна на ре-

гиони от мултимедийното съдържание и др. [22]. Три свойства са особено важни по отношение на Интернет-базираните сценарии: адаптивност, устойчивост срещу JPEG-базирани трансформации и работа с произволна мултимедия и вградени данни.

Присъщата отвореност и непредсказуемост на глобалната мрежа в комбинация с бързите и резки промени в съвременните социални, бизнес и технологични среди водят до постоянни изменения на потребностите и изискванията на клиентите. Поради тази причина методите за криене на данни трябва да могат да бъдат лесно адаптирани към промени в изискванията на клиентите – т.е. те трябва да могат да променят част от свойствата си (в зависимост от конкретното приложение и цели на клиента), като в същото време запазват една основна функционалност, която потребителите очакват от всички такива методи.

Важно изискване към методите за криене на данни в мултимедия, особено ако се цели тяхното приложение в Интернет, е запазването на вградената информация след компресия на мултимедийното съдържание [3]. Най-често се използва т.нар. загубна компресия [23], при която се губи част от мултимедийното съдържание, но се постига с пъти по-високо ниво на компресия от стандартните беззагубни методи за компресия. Един от най-важните формати за загубна компресия на изображения, намиращ широко приложение и при кодиране на видео кадри, е JPEG, който е базиран на т.нар. дискретна косинусова трансформация (DCT) [24]. Съществуват три основни типа JPEG трансформации:

1. Компресия – кодиране на матрица от пиксели в JPEG формат. Всяко цифрово изображение трябва да се представи под формата на правоъгълна матрица от пиксели преди извършването JPEG компресия.
2. Декомпресия – декодиране на JPEG формат до матрица от пиксели.
3. Рекомпресия – промяна на степента на компресия или други параметри на компресията на изображение, което е вече кодирано в JPEG формат.

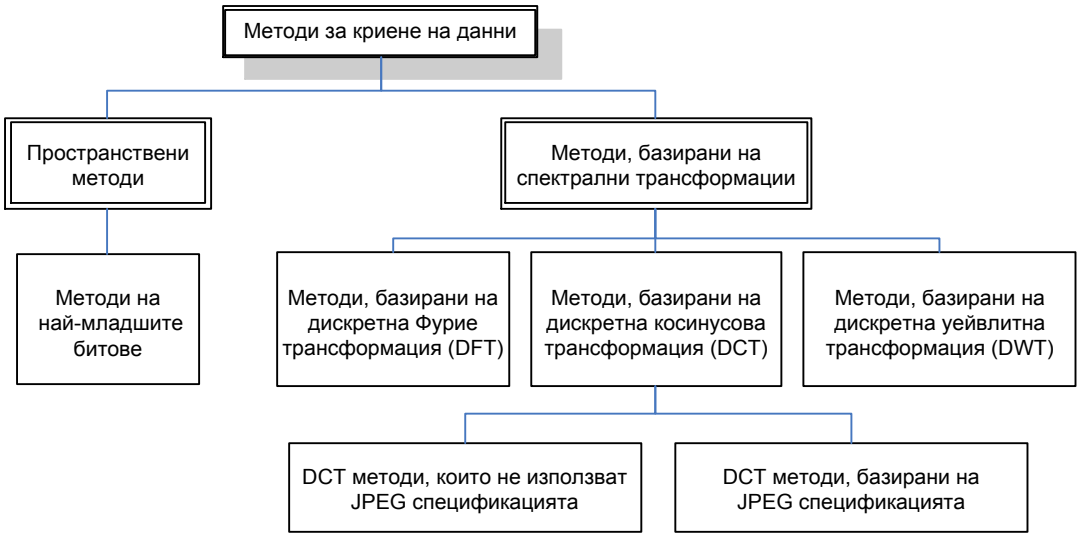
Методите за криене на данни трябва да бъдат достатъчно гъвкави, така че да могат да обработват произволна мултимедия, предоставена от крайните потребители. Също така оригиналното изображение или статистическа информация, която го описва не трябва да бъдат необходими за декодиране на вградените данни.

Тъй като методите за криене на данни за приложения в глобалната мрежа често работят с криптирани или компресирани данни, предоставени от крайния потребител, то тези методи не трябва да налагат ограничения върху формата или последващата употреба на вградените данни. Възстановяването на вградените данни без наличие на грешки трябва да бъде възможно с оглед на тяхната последваща употреба от други произволни технологии.

2.2 Съществуващи методи и програмни продукти за криене на данни в мултимедия

Най-важните типове методи за криене на данни могат да се класифицират както е показано на Фиг. 3 ([4], [25]). Поради големия брой съществуващи методи за криене на данни и важното значение на JPEG формата за обмен на изображения в Интернет, в този раздел се разглеждат само *методите, базирани на DCT трансформацията*, като се изследва тяхната устойчивост срещу различните видове JPEG трансформации.

Никой от разгледаните методи за криене на данни в мултимедия не дискутира свойството адаптивност. Тези методи са монолитни решения, разработени за целите на специализирани приложения със свои собствени конкретни изисквания относно свойствата на методите. Авторите не дискутират как тези методи биха могли да бъдат интегрирани като част от вече съществуващи решения и инфраструктури.



Фиг. 3: Класификация на методите за криене на данни

Устойчивостта срещу JPEG трансформации и възможността за работа с произволна мултимедия и вграждани данни са само частично взети под внимание. Повечето методи разглеждат само определени аспекти на тези свойства. Потенциалът за подобрение се състои в едновременното реализиране на всички значими аспекти на свойствата.

Вследствие на силния академичен и корпоративен интерес към криенето на данни в мултимедия, съществуват редица практически насочени програмни продукти и услуги в областта на стеганографията и цифровото маркиране. Те са добили популярност в последните години и се предлагат в Интернет или като част от по-големи програмни пакети.

Продуктите, създадени за стеганографски цели, могат да работят с произволни носещи изображения и данни за вграждане, но не са толкова устойчиви срещу JPEG трансформации колкото разгледаните продукти за цифрово маркиране. От друга стра-

на, продуктите за цифрово маркиране могат да вграждат само малки по размер, предварително дефинирани типове данни – най-често идентификационни номера, но с добра степен на устойчивост срещу JPEG трансформации.

Нито едно от съществуващите програмни решения не взема предвид адаптивността към нуждите на клиентите. Тези решения са изградени монолитно, на базата на конкретни и завършени методи и не могат да се адаптират към променящите се изисквания на потребителите в Интернет, които налагат промени в свойствата на методите за криене на данни в мултимедия.

2.3 Заключение

В резултат на направения обзор могат да се идентифицират следните недостатъци на съществуващите методи за криене на данни в мултимедия, базирани на DCT трансформации:

1. Съществуващите методи и продукти за криене на данни в мултимедия са монолитни и с конкретна приложна насоченост.
2. Много малко на брой методи са разработени, за да бъдат устойчиви срещу JPEG декомпресия или рекомпресия и те не винаги могат да работят с произволни изображения и вградени данни.

Глава 3. Модулен подход за проектиране на методи за криене на данни

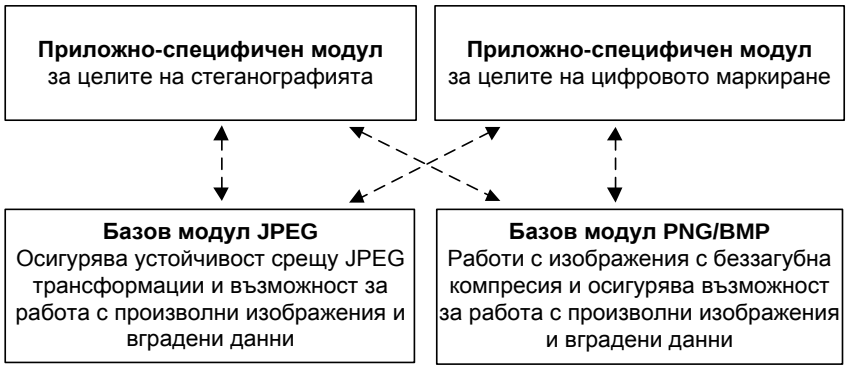
В тази глава се дискутира модулното проектиране на методите за криене на данни в мултимедия и се представят неговите предимства. Един модулен метод за целите на стеганографията и един модулен метод за целите на цифровото маркиране се създават специално за приложение в Интернет-базирани сценарии и техните свойства се описват и дискутират в подробности.

3.1 Модулно проектиране – общ поглед и архитектура

При реализацията на методите за криене на данни те се разглеждат като съставени от два вида модули –базов модул и приложно-специфичен модул. Двата вида модули могат да се комбинират в различни конфигурации (Фиг. 9).

Предложената модулна архитектура за реализация на методите за криене на данни позволява създаването и адаптирането на приложно-специфичните модули според

променящите се изисквания на потребителите, като в същото време се запазват всички свойства, реализирани от базовия модул. Следователно, базовият модул трябва да предостави основни свойства, които са от голямо значение за всички използвани методи за криене на данни и не се променят. Приложно-специфичният модул трябва да предоставя специализирани и често пъти по-сложни за реализиране свойства от високо ниво на методите за криене на данни, които са зависими от конкретното приложение и конкретните нужди на потребителя. По този начин свойствата, реализирани от целия метод, представляват комбинация от свойствата, осигурени от базовия и от приложно-специфичния модул. Гарантирано, че методи, използващи един и същ базов модул, разполагат с еднаква реализация на свойствата, които този базов модул предоставя. Това подобрява надеждността на методите и улеснява тяхната употреба. Модулите се проектират с помощта на обектно-ориентираното програмиране (англ. object-oriented programming, OOP) [12].



Фиг. 9: Модулен подход за криене на данни в мултимедия за целите на мрежови приложения

3.2 Базов модул, устойчив срещу JPEG трансформации

Базовият модул, представен в този раздел, е разработен, за да позволи създаването на модулни методи, които вграждат информация в изображения, компресирани и запаметени във JPEG формат.

3.2.1 Основни цели при разработването на модула

Основните цели при разработването на базовия модул са както следва:

1. Да се осигури устойчивост срещу JPEG трансформации: компресия, декомпресия и рекомпресия.
2. Да се осигури възможност за работа с произволни изображения и данни за вграждане.

3. Да се осигури контекстно-независимо прочитане на вградените данни, т.е. без нужда от допълнителна информация, отнасяща се до оригиналното изображение преди криенето на данните.
4. Да се гарантира безпогрешното прочитане и възстановяване на скритата информация.

Едновременното реализиране на тези четири цели при разработката на базовия модул е комплексна задача, която изисква задълбочено познаване на процесите на JPEG компресия и декомпресия, дефинирани в JPEG стандарта [24] и в описанието на формата JPEG File Interchange Format (JFIF) [26]. Тъй като стандартът не дефинира напълно процеса на JPEG компресия, познаването на основните практически реализации на JPEG е от съществено предимство.

3.2.2 Общ поглед върху стандарта JPEG

В този раздел са представени накратко най-важните особености на стандарта за компресия на изображения JPEG, имащи отношение към методите за криене на данни в мултимедия. Целта е да се подготви и улесни изложението на кодиращите и декодиращите методи, създадени за базовия модул. Важно е да се отбележи, че в основата на JPEG компресиращия алгоритъм лежи двумерната DCT трансформация на всеки 8×8 блок от пиксели посредством следната математическа формула:

$$A_{k,l} = \frac{c_k.c_l}{4} \sum_{m=0}^{7} \sum_{n=0}^{7} P_{m,n}.\cos\left[\frac{(2m+1).k.\pi}{16}\right].\cos\left[\frac{(2n+1).l.\pi}{16}\right],$$

където $P_{m,n}$ обозначава блока от пиксели, $A_{k,l}$ обозначава DCT коефициентите,

$$c_k = \begin{cases} \frac{1}{\sqrt{2}}, & \text{за } k = 0 \\ 1, & \text{за } k \neq 0 \end{cases}, \; c_l = \begin{cases} \frac{1}{\sqrt{2}}, & \text{за } l = 0 \\ 1, & \text{за } l \neq 0 \end{cases} \text{ и } \; k, l, m, n \in [0; 7].$$

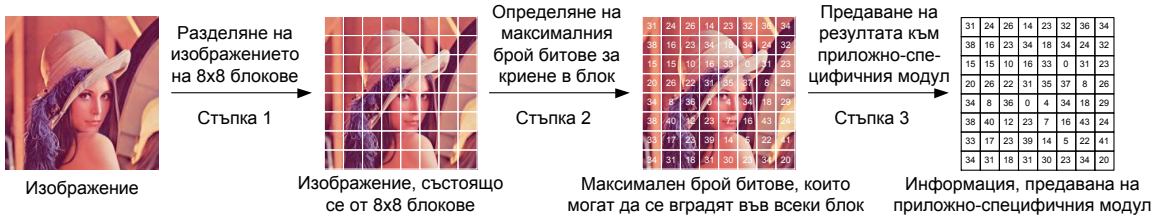
Изображението се представя посредством стандартизиран набор от коефициенти $A_{k,l}$, всеки от които се подлага на загубна компресия чрез деление (квантизиране) със съответния му елемент $Q_{k,l}$ от потребителски определена квантизираща таблица Q и последващо закръгляване.

3.2.3 Базов модул: кодиране

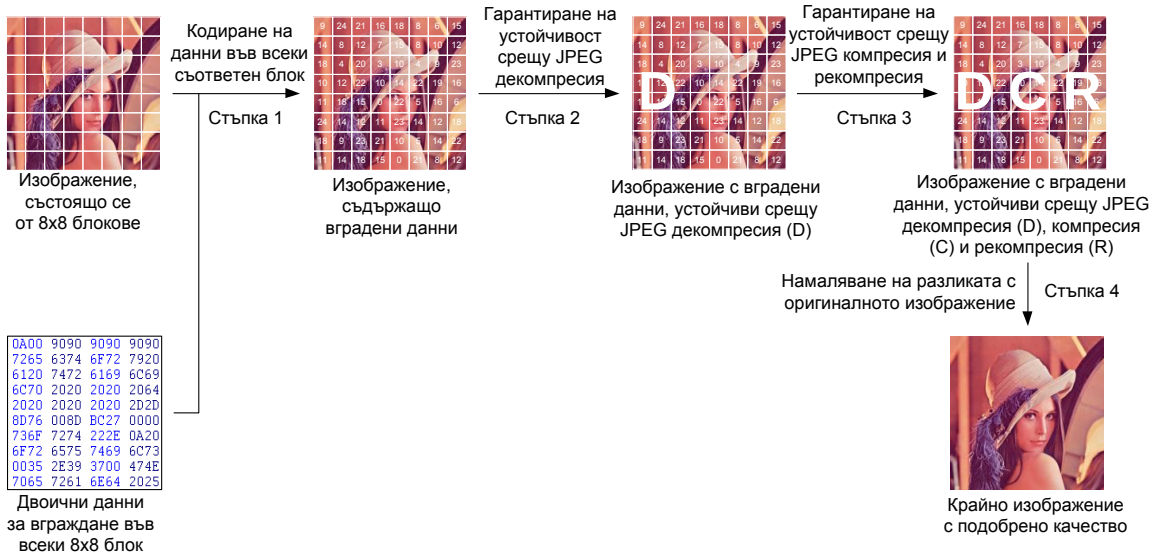
Кодирането на информацията в базовия модул се състои от два етапа. *Етапът на подготовка* се стартира от приложно-специфичния модул и преминава през стъпките на Фиг. 16.

Етапът на завършване на кодирането приема като входни данни (от страна на приложно-специфичния модул) конкретните битове, които трябва да бъдат вградени във всеки блок от изображението. Изпълняват се стъпките, показани на Фиг. 18.

Стъпките за вграждане на данни, описани по-горе, се изпълняват за всеки един блок от изображението. След като алгоритъмът приключи, крайното изображение, съдържащо вградените данни, се предава на приложно-специфичния модул.



Фиг. 16: Базов модул – етап на подготовка (*PrepareToEncode*)



Фиг. 18: Базов модул – етап на завършване на кодирането (*FinishEncode*)

3.2.4 Гарантиране на устойчивост срещу JPEG компресия, декомпресия и рекомпресия

Вграждането на данни в най-младшите битове на квантизираните DCT коефициенти ни дава само по себе си устойчивост срещу JPEG компресия, съпроводена със сравнително добро качество на изображението при сравнително голям размер на вграждането данни [3]. Декомпресията на изображение от JPEG до матрица от RGB пиксели винаги включва грешки, породени от две основни причини:

1. Първата причина е свързана с грешки от закръглявания при целочислените програмни реализации на JPEG трансформациите.
2. Втората причина е свързана с ограниченото представяне на цветовите пространства – често подмножества на множеството на естествените числа $S = \{0,1,2,\ldots,255\}$.

Загубната компресия постига намаляване на информацията чрез изобразяване на множество сходни по стойности блокове от пиксели в един и същи DCT блок. Обратното изображение е уникално. Ако някои от оригиналните стойности на пикселите преди компресията имат стойности, близки до границите на множеството *S*, то някои стойности на пикселите, получени след декомпресия, биха могли да попаднат извън границите на *S*. Повечето програми за обработка на изображения променят тези стойности на 0 или 255. В резултат на това променениият блок от пиксели би могъл да бъде изобразен в друг DCT блок, което води до загуба на вградените данни. Нашето решение е да се скалират предварително стойностите на пикселите, така че обратното изобразяване при декомпресията винаги да дава валидни стойности (стъпки 4 и 5 от алгоритмичното описание по-долу).

JPEG стандартът не дефинира JPEG квантизиращите таблици, отговорни за загубната компресия, и те са различни при отделните производители на програми за обработка на изображения като Adobe, Microsoft, Corel, и др. На този етап се гарантира устойчивостта срещу рекомпресия с $\forall Q^{(j)} | Q_{k,l}^{(j)} \leq Q_{k,l}$ за $\forall k,l \in \{0,1,2,\dots,7\}$, където j е индекс на итерация, покриващ всички комбинации от квантизиращи таблици $Q^{(j)}$, които биха могли да се използват от програмните системи, а квантизиращата таблица Q се определя в зависимост от избраното от потребителя ниво на JPEG компресия. За да се гарантира надеждно възстановяване на данните, в този базов модул се използва изменена техника на Модулация на Индекса на Квантизация [27]. Посредством квантизиращата стъпка $q_{k,l}$ могат да се изберат множество нови стойности $C_{k,l}^{(i)}$ на всеки един квантизиран коефициент $C_{k,l}$, които кодират идентични вградени данни (стъпки 7 и 8 от алгоритмичното описание по-долу). Коефициентът β приема първоначална стойност 1. Ако за дадено $Q^{(j)}$ и $\forall (k,l) \in Z_{data}$ е изпълнено $C_{k,l}^{(i)} = E_{k,l}^{(i,j)}$, то целият JPEG блок се приема за устойчив срещу рекомпресия с $Q^{(j)}$. Изборът и броят на квантизиращите таблици $Q^{(j)}$ зависи от програмните системи и библиотеки, които се използват за генериране на JPEG изображение – например библиотеката с отворен код IJG, програмните системи Adobe Photoshop, Paint Shop Pro, и др. На този етап, прототипната реализация на базовия модул използва всички възможни $Q^{(j)}$ с цел по-доброто изследване на предложения метод.

Алгоритмично описание:

Нека приемем, че коефициентите $C_{k,l}$ вече са пресметнати и данни са вградени в някои от тях. Нека също така дефинираме множеството $Z_{data} = \{(k,l) | C_{k,l} \text{ съдържа вградени данни}\}$, $k,l \in \{0,1,2,\dots,7\}$. Тогава алгоритъмът за постигане на устойчивост срещу JPEG трансформации може да се представи посредством следните стъпки:

0. Определят се първоначалните стойности: $i = 1$, $u^{(0)} = 0$, $v^{(0)} = 255$, $\alpha = 1$.

1. Пресмята се нов блок от пиксели $P_{m,n}^{(1)}$ от блока $C_{k,l}$ чрез извършването на алгоритъма за декодиране на изображение от JPEG формат.
2. Пресмята се нов блок DCT коефициенти $C_{k,l}^{(1)}$ от блока $P_{m,n}^{(1)}$ чрез извършването на алгоритъма за кодиране на изображение в JPEG формат.
3. Ако $\exists(k,l) \notin Z_{data} | C_{k,l} \neq C_{k,l}^{(1)}$, то за $\forall(k,l) \notin Z_{data}$ се присвоява $C_{k,l} = C_{k,l}^{(1)}$ и се преминава на стъпка 1.
4. Пресмята се нов блок от пиксели $P_{m,n}^{(2)}$ от блока $C_{k,l}$ чрез извършването на стъпки 3 до 7 от алгоритъма за декодиране на изображение от JPEG формат.
5. Ако $\exists(m,n) | P_{m,n}^{(2)} \notin \{u^{(0)}, u^{(0)}+1, \dots, v^{(0)}\}$, то за $\forall(m,n) | P_{m,n}^{(2)} < u^{(0)}$ се пресмята:
$$s^{(i)} = \max_{(m,n)|P_{m,n}^{(2)} < u^{(0)}} \left(\alpha \left| P_{m,n}^{(2)} - u^{(0)} \right|\right)$$
и за $\forall(m,n) | P_{m,n}^{(2)} > v^{(0)}$ се пресмята:
$$t^{(i)} = \max_{(m,n)|P_{m,n}^{(2)} > v^{(0)}} \left(\alpha \left| P_{m,n}^{(2)} - v^{(0)} \right|\right)$$
Пресмятат се: $u^{(i)} = u^{(i-1)} + s^{(i)}$ и $v^{(i)} = v^{(i-1)} - t^{(i)}$. За $\forall(m,n) | P_{m,n} < u^{(i)}$ се присвоява $P_{m,n} = u^{(i)}$ и за $\forall(m,n) | P_{m,n} > v^{(i)}$ се присвоява $P_{m,n} = v^{(i)}$. Увеличава се i с 1 и се преминава на стъпка 1.
6. Присвоява се $i = 0$, $\beta = 1$, избира се валиден индекс $j | \exists Q^{(j)}$ и за $\forall(k,l)$ се присвоява $C_{k,l}^{(0)} = C_{k,l}$.
7. Пресмятат се $D_{k,l}^{(i,j)} = \left[C_{k,l}^{(i)} \times Q_{k,l} / Q_{k,l}^{(j)}\right]$ и $E_{k,l}^{(i,j)} = \left[D_{k,l}^{(i)} \times Q_{k,l}^{(j)} / Q_{k,l}\right]$.
8. Ако $\exists(k,l) \in Z_{data} | C_{k,l}^{(i)} \neq E_{k,l}^{(i,j)}$, то се пресмята $C_{k,l}^{(i+1)} = C_{k,l}^{(i)} + (-1)^i \left[(i+1) \times q_{k,l}\right]$, където $q_{k,l} = \beta \times 2^{N_{k,l}}$ и $N_{k,l}$ е броят битове, съдържащ се в коефициента $C_{k,l}$. Увеличава се i с 1 и се преминава на стъпка 7.
9. Повтарят се стъпки 6 до 8 за $\forall(k,l) \in Z_{data}$ и $\forall j | \exists Q^{(j)}$.

3.2.5 Базов модул: декодиране

За разлика от процеса на кодиране, процесът на декодиране (*Decode*) се състои само от един етап, който е подобен на етапа на подготовка (*PrepareToEncode*):

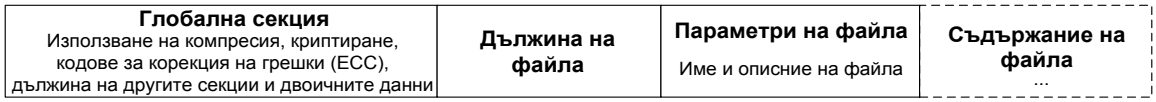
1. Разделяне на входното изображение на блокове с размер 8×8 пиксела.
2. Определяне на максималния брой битове, вградени във всеки блок.
3. Декодиране на съответния брой битове от всеки DCT блок чрез прочитане на най-младшите битове на квантизираните DCT коефициенти на блока $C_{k,l}$.
4. След обработката на всички блокове от изображението, декодираните битове се предават към приложно-специфичния модул.

Процесът на декодиране се нуждае от значително по-малко време за изпълнение в сравнение с пълния процес на кодиране, съставен от етапите на подготовка и завършване на кодирането.

3.3 Приложно-специфичен модул за целите на стеганографията. Модулен стеганографски метод

Представеният приложно-специфичен модул за целите на стеганографията е разработен, за да скрие максимално количество информация в дадено изображение.

3.3.1 Направляващо файлово описание



Фиг. 20: Модулен стеганографски метод – направляващо файлово описание

Направляващото файлово описание съдържа информация относно обработвания файл с данни и някои важни параметри, контролиращи метода за криене на данни. То е разделено на няколко отделни секции (Фиг. 20).

3.3.2 Кодове за корекция на грешки

Кодовете за корекция на грешки, използвани в този метод за криене на данни в мултимедия, се базират на алгоритъма на Хеминг и позволяват надеждното откриване и корекция на грешки с дължина един бит в определен сегмент от двоичните данни. Независимо от незадължителната употреба на такива кодове, разработеният базов модул гарантира устойчивостта на данните срещу JPEG трансформации.

Алгоритмично описание:

Нека с $f_k^{(i)}$ се обозначи стойността на бита на позиция $i, i \in \{0,1,2,\dots,l_{f_k}-1\}$ във фрагмент k от потока на битове f. Нека за опростяване на описанието приемем, че дължината на всеки фрагмент f_k е $l_{f_k} = l_f = 120$ за $\forall k$, и $\sum_{k=1}^{n_f} l_{f_k} = n_f l_f$ е дължината на целия поток от битове, където n_f е броят фрагменти, на които потокът от битове е разделен. Нека с $h = 7$ се обозначи броят на битовете за корекция на грешки в един фрагмент. Нека с $P_{f_k}^M = P(f_k^{(i_1)}, f_k^{(i_2)}, \dots f_k^{(i_m)})$ се обозначи функцията на четност на битовете на позиции $i_1, i_2, \dots, i_m$ във фрагмент f_k, като $M = \{i_1, i_2, \dots, i_m\}$ е множеството, съдържащо тези позиции. По дефиниция: $P(0) = 0,\ P(1) = 1,\ P\left(0, f_k^{(i_1)}, f_k^{(i_2)}, \dots f_k^{(i_m)}\right) = P\left(f_k^{(i_1)}, f_k^{(i_2)}, \dots f_k^{(i_m)}\right)$, $P\left(1, f_k^{(i_1)}, f_k^{(i_2)}, \dots f_k^{(i_m)}\right) = \overline{P\left(f_k^{(i_1)}, f_k^{(i_2)}, \dots f_k^{(i_m)}\right)}$, където $\bar{0} = 1$ и $\bar{1} = 0$. Изпълняват се следните стъпки:

0. Определя се първоначалната стойност на k: $k = 1$.
1. Дефинира се фрагмент g_k с дължина $l_g = l_f + h$. Дефинира се $j = 1$.
2. За $\forall z | z \in \{2^j, 2^j + 1, \dots, 2^{j+1} - 2\}$ се присвоява $g_k^{(z)} = f_k^{(z-1-j)}$. Ако $j < h - 1$, то j се увеличава с 1 и се преминава към стъпка 1. В противен случай се продължава със стъпка 3.
3. Дефинира се $b = 0$.
4. Дефинира се $c = 2^b$. Присвоява се $g_k^{(c-1)} = 0$. Дефинира се множеството $M \subseteq \{0,1, \dots, l_g - 1\}$, съдържащо като елементи следните позиции на битове в g_k: $M = \{c - 1, c, c + 1 \dots, 2c - 2, 3c - 1, 3c, \dots, 4c - 2, \dots, (2d + 1)c - 1, (2d + 1)c, \dots, (2d + 2)c - 2, \dots, l_g - 1\}$, където $d \in \mathbb{N}$.
5. Присвоява се $g_k^{(c-1)} = P_{g_k}^M$. Ако $b < h - 1$, то b се увеличава с 1 и се преминава към стъпка 4. В противен случай се продължава със стъпка 6.
6. Ако $k < n_f$, то k се увеличава с 1 и се преминава към стъпка 1.

3.3.3 Разбъркване на данните

Разбъркването на данните използва генератор на псевдослучайни числа [28] за създаването на псевдослучайни пермутации. Тези пермутации се използват при избора на блок от изображението, в който ще бъде скрит всеки следващ пореден бит на потока от данни. Началните стойности на генератора на псевдослучайни числа могат да са зависими от парола, дефинирана от потребителя, както и от дадени характеристики на изображението, което води до повишаване на нивото на сигурност на предлагания стеганографски метод. Разбъркването на данните подобрява също така общото възприемано качество на изображението. Ако блоковете, в които се вграждат данни, не са поредни, а са разпръснати в изображението, то не съществува област от изображението, в която качеството да се влошава повече, отколкото в останалите области.

3.3.4 Кодиране на данните

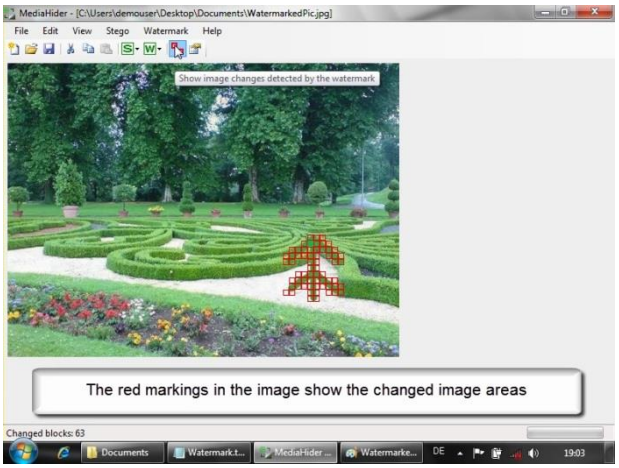
Процесът на кодиране включва създаването на направляващо файлово описание, както и алгоритмите за корекция на грешки и разбъркване на данните, описани в предните раздели. Неговата цел е да постигне устойчиво и визуално недоловимо криене на максимално количество данни в изображението. Състои се от стъпките на Фиг. 24.

3.3.5 Декодиране на данните

Процесът на декодиране обръща стъпките, от които се състои процесът на кодиране, описан в предишния раздел, като възстановява вградените двоични данни заедно с информацията в тяхното направляващо описание.

Фиг. 24: Стеганографски метод - кодиране

3.4 Приложно-специфичен модул за целите на цифровото маркиране. Модулен метод за цифрово маркиране



Фиг. 27: Проверка на изображение, съдържащо неправомерно променени JPEG блокове

Разработеният приложно-специфичен модул за целите на цифровото маркиране използва базовия модул, за да постигне устойчивост срещу JPEG трансформации по начин, подобен на стеганографския приложно-специфичен модул. Вгражданите цифрови водни знаци са значително по-малки по размер от данните, с които работи стеганографският метод и се вграждат в изображението по такъв начин, че да бъдат устойчиви срещу промени в него. На Фиг. 27 е показан резултатът от проверката на изображение (авторска снимка) посредством метода. Изображението съдържа известен брой неправомерно променени JPEG блокове с размер 8 × 8 пиксела, които са маркирани в червено (борчето в долната дясна част на изображението).

3.4.1 Направляващо описание и код за корекция на грешки

Направляващото описание на цифровия воден знак е опростена версия на направляващото описание, използвано от стеганографския метод. Кодовете за корекция на грешки са идентични, като тяхната употреба не е задължителна.

3.4.2 Макроблокове

Алгоритъмът за цифрово маркиране разделя изображението на няколко големи области, наречени макроблокове. Всеки макроблок се състои от матрица от микроблокове и съдържа копие на водния знак. По дефиниция всеки микроблок съдържа B бита вградени данни, които изпълняват ролята на негова сигнатура и се използват за откриването на промени в микроблока. Броят и размерите на макроблоковете зависят от размера на изображението и общата дължина L на водния знак. Нека дефинираме съотношенията RC и $RC^{(i)}$, съответно за цялото изображение и за всеки един макроблок i по следния начин:

$$RC = n_y / n_x \, , RC^{(i)} = M^{(i)} / N^{(i)} \, ,$$

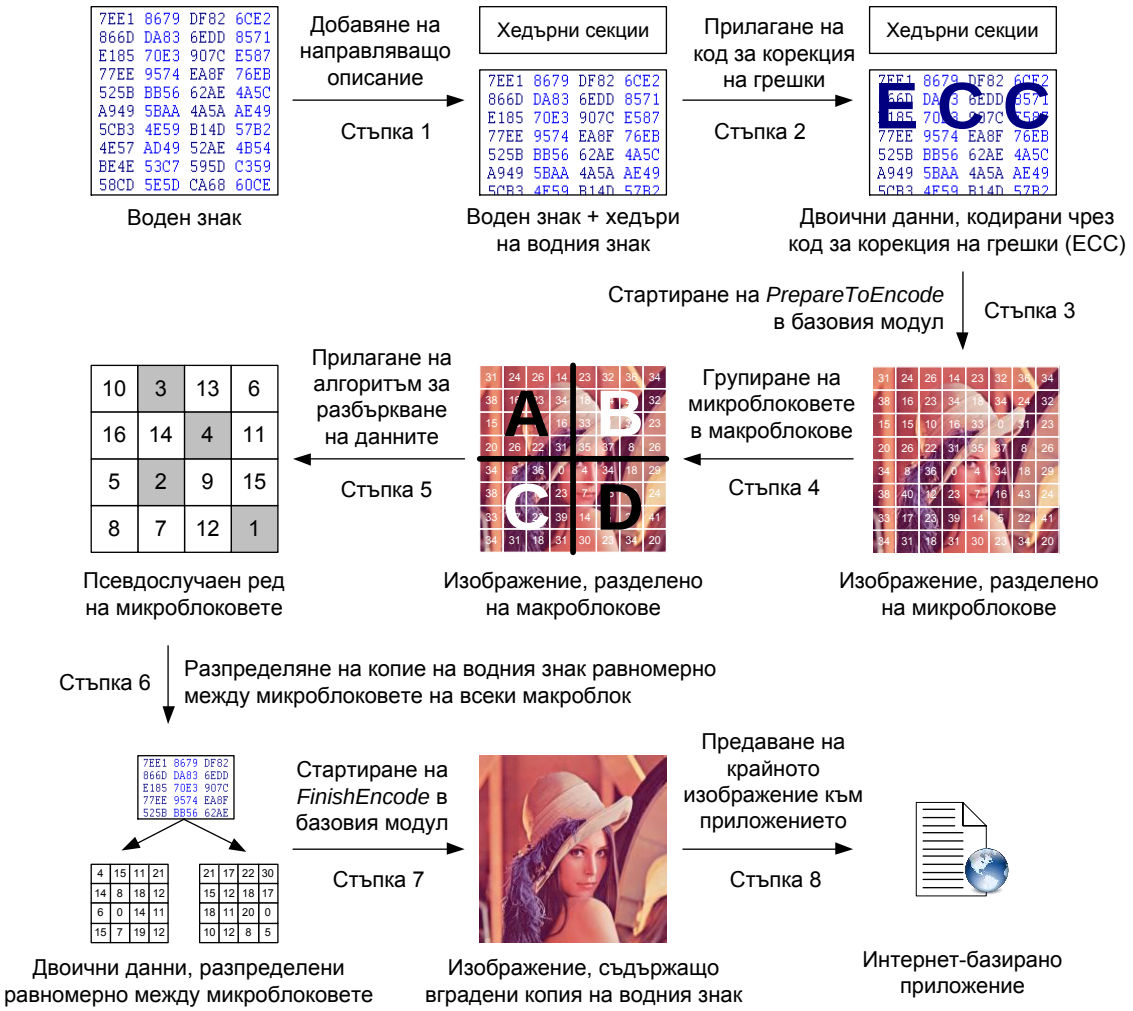
където n_x и n_y обозначават съответно броя микроблокове по хоризонтала и вертикала в изображението, а $M^{(i)}$ и $N^{(i)}$ обозначават съответно броя на редовете и колоните от микроблокове в даден макроблок i. Съотношението $RC^{(i)}$ се избира за всеки макроблок i по такъв начин, че $RC^{(i)} \approx RC$ за $\forall i$. При конструирането на всеки макроблок i се предпочита използването на малки размери. Търсят се:

$$M^{(i)}, N^{(i)} | S^{(i)} = M^{(i)} \times N^{(i)} \approx \min_{a,b | M_a^{(i)} \times N_b^{(i)} \geq L/B \text{ и } M_a^{(i)}/N_b^{(i)} \approx RC} \left(M_a^{(i)} \times N_b^{(i)} \right) ,$$

където с $S^{(i)}$ се обозначава броят на микроблоковете в макроблок i, а с индексите a и b се обозначават съответно различните възможни стойности на броя редове и колони, съставящи макроблока. Това води до по-голям брой макроблокове и съответно по-голям брой вградени копия на водния знак, което увеличава устойчивостта на вграждането.

3.4.3 Откриване на промени в изображението и възстановяване на водния знак

По време на декодирането вградените във всеки макроблок копия на водния знак се прочитат и сравняват помежду си. Ако промените в изображението не са били прекалено големи по размер, повечето копия ще бъдат идентични с оригиналния воден знак. Останалите копия ще съдържат разлики, чието положение ще отговаря на променените микроблокове в макроблока, съдържащ промененото копие. По този начин е възможно да се локализират променените области от изображението и едновременно с това да се възстанови оригиналният вграден воден знак, при положение че са останали достатъчен брой непроменени микроблокове и съответно макроблокове.



Фиг. 32: Метод за цифрово маркиране - кодиране

Тъй като базовият модул осигурява устойчивост срещу JPEG трансформации, вградените водни знаци остават непроменени след промени на изображението, предизвикани от JPEG компресия, декомпресия или рекомпресия. Следователно, тези видове промени на изображението няма да се отчетат като такива от алгоритъма, описан по-горе.

3.4.4 Кодиране на водния знак

Процесът на кодиране, който реализира вграждането на водния знак в макроблоковете на изображението, се състои от стъпките на Фиг. 32.

3.4.5 Декодиране на водния знак

Процесът на декодиране обръща стъпките, от които се състои процесът на кодиране, като открива евентуални промени в изображението и прочита вградения воден знак.

3.5 Базов модул за изображения с беззагубна компресия

Базовият модул, представен в този раздел, е разработен с цел верификация на модулния подход и употреба на приложно-специфичните модули за целите на стеганографията и цифровото маркиране върху некомпресирани изображения (напр. BMP) или изображения, компресирани без загуба на информация (напр. PNG).

3.6 Заключение

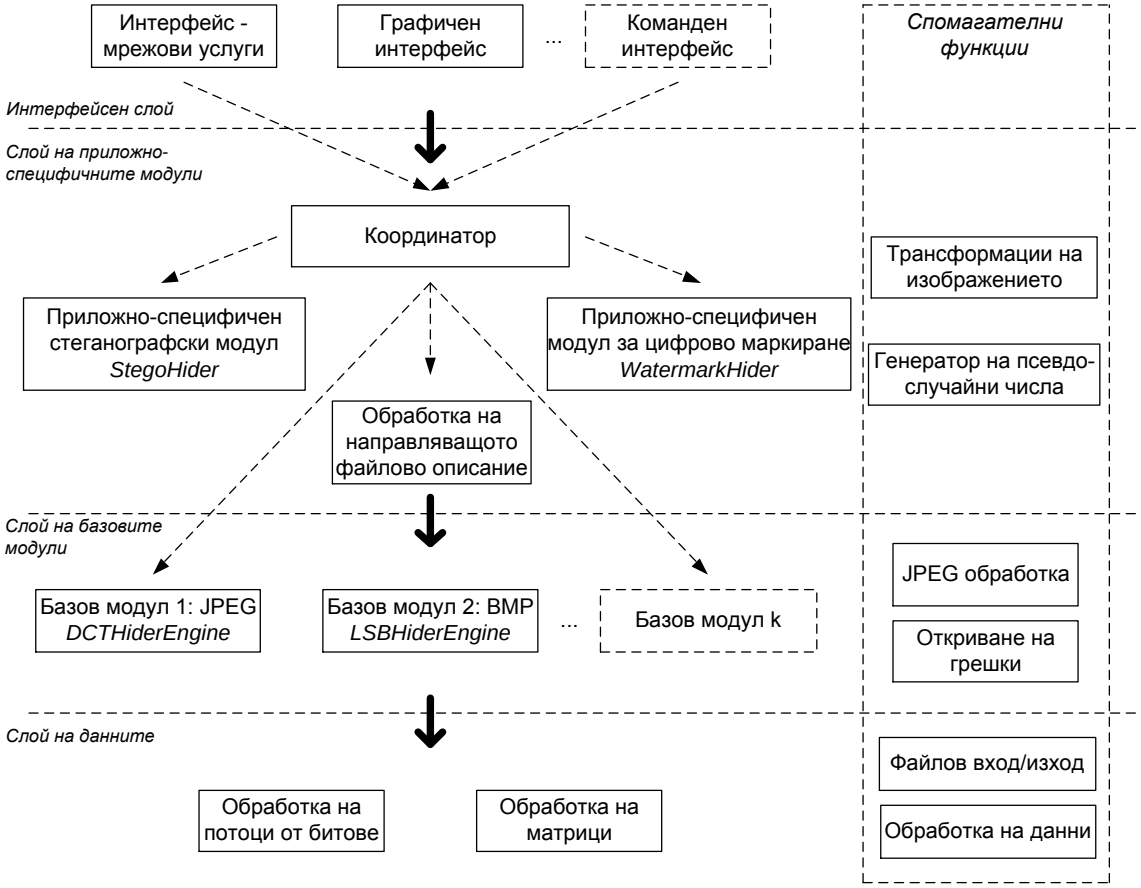
При модулния подход за проектиране на методи за криене на данни всяко свойство на даден метод се реализира или в базовия, или в приложно-специфичния модул, от които методът е съставен. Това улеснява поддръжката на метода и отстраняването на грешки. Също така методите могат сравнително лесно да се подобряват чрез добавяне на нови свойства или усъвършенстване на вече съществуващите такива. Освен това чрез разделянето на методите на модули се постига гъвкавост при прилагането им в различни приложни Интернет-базирани сценарии.

Глава 4. Програмна реализация на модулните методи

Предложените методи за криене на данни в мултимедия са реализирани като програмна система посредством програмната платформа .NET на Майкрософт. Програмната реализация предлага възможност за предварителна обработка на вгражданите данни: компресиране с програмната библиотека с отворен код *zlib* с алгоритъма *LZ77* (Lempel–Ziv 1977) [29] и криптиране според стандартите *3DES* и *AES*.

Архитектурата на програмната система е представена на Фиг. 40. Компонентите, принадлежащи на пространството на имената на *спомагателните функции* реализират някои основни функции, които не са част от .NET платформата или C++, но са необходими за реализацията на модулните методи за криене на данни. Слоят на данните съдържа два компонента, които осигуряват поддръжка съответно на потоци от битове и на матрици. Базовите модули се реализират програмно от класове, написани на VB.NET или C++. Характерно за разработените модули е, че кодирането на данните има по-голяма сложност, по-малка скорост на изпълнение и изисква по-голям обем RAM-памет в сравнение с декодирането. Приложно-специфичните модули се реализират програмно от класове, написани на VB.NET. Производителността на кода в приложно-специфичните модули не е от такова критично значение както при базовите модули. Интерфейсният слой осъществява връзката между методите за криене на данни в

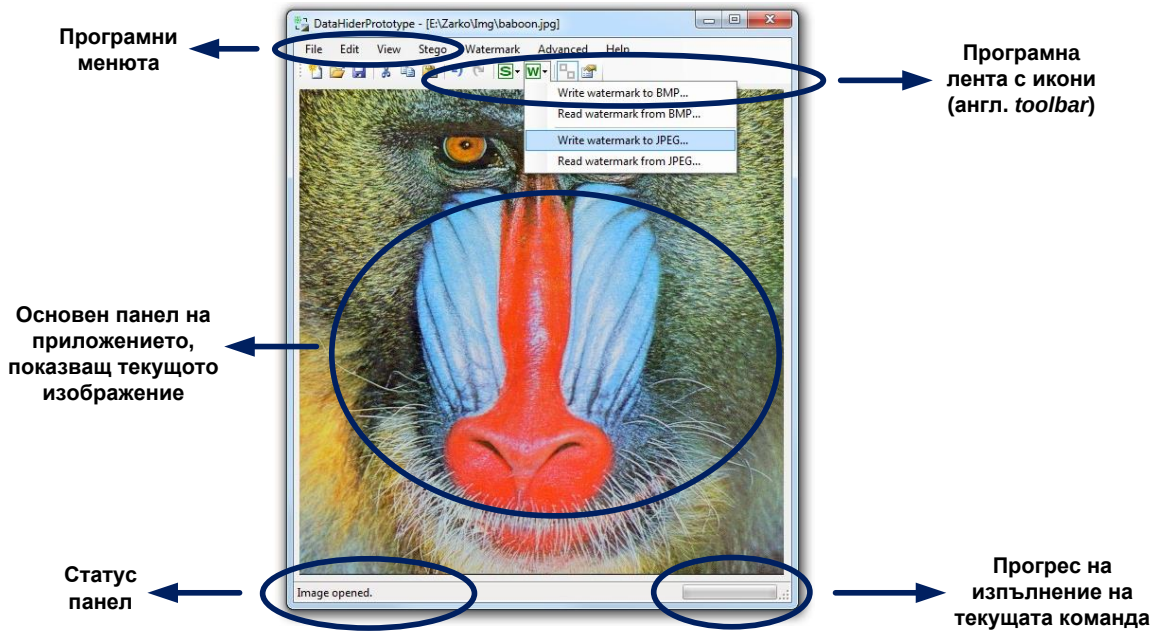
мултимедия и външния свят –автоматизирани мрежови приложения и/или реални потребители. Интерфейсите, реализирани до момента, са:



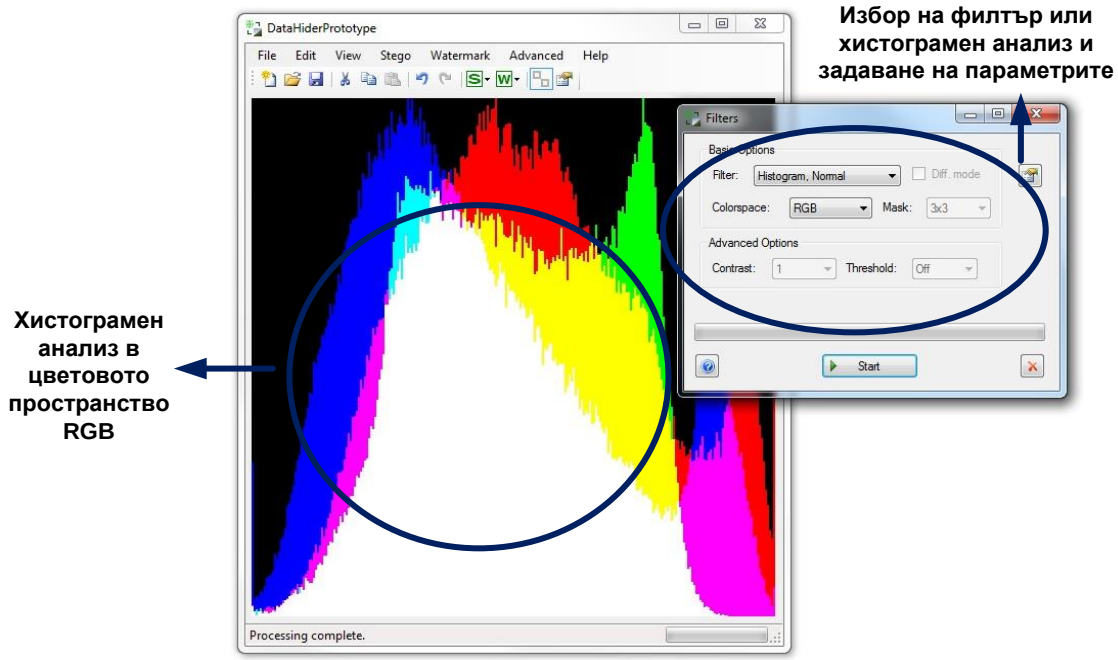
Фиг. 40: Програмна архитектура – общ поглед

1. Графичен потребителски интерфейс за използване на методите за криене на данни под формата на самостоятелно десктоп приложение (Фиг. 45 и Фиг. 27, раздел 3.4);
2. Графичен потребителски интерфейс, позволяващ старт и анализ на групови обработки на мултимедийни файлове и файлове с данни;
3. Приложен програмен интерфейс (англ. application programming interface, API) за мрежови услуги, подходящ за употреба в Интернет-базирани сценарии.

Разработена е и програмна реализация на редица филтри и средства за хистограмен анализ на изображението, използвани като инструменти при провеждането на стеганализ (Фиг. 52). Предлаганите филтри са усредняващ филтър, Гаусов филтър, медианен филтър, Винер-Колмогоров филтър и Лапласиан на Гаусиана (разгледани подробно в [23]). Поддържаните маски на филтрите варират от 3×3 до 11×11. Поддържаните цветови пространства са *RGB, Greyscale* (нива на сивото) и YC_bC_r . Поддържа се и създаването на т. нар. диференчни изображения (англ. difference images).



Фиг. 45: Графичен потребителски интерфейс



Фиг. 52: Резултат от хистограмен анализ в цветовото пространство RGB

Приложният програмен интерфейс за мрежови услуги е реализиран на базата на технологията ASP.NET на Майкрософт, която е част от платформата .NET. Комуникацията между клиента (произволно Интернет-базирано приложение) и сървъра (съдържащ модулните методи за криене на данни) може да се осъществи чрез т.нар. SOAP

протокол (версия 1.1 или 1.2) [30] или обикновени HTTP GET или POST заявки [31] (Фиг. 55).

```
POST /StegiWeb/StegiWeb.asmx/hideDCT HTTP/1.1
Host: xxx.xxx.xxx.xxx
Content-Type: application/x-www-form-urlencoded
Content-Length: length

sourceImage=string&destinationImageFormat=string&
informationToHide=string&informationToHide=string&
errorCorrection=string&saveFileName=string&
dataStreamFileName=string&withstandJPEGCompressionRatio=string
```

Фиг. 55: Примерна HTTP POST заявка

Глава 5. Оценка и стеганализ на разработените методи

Оценката на методите се извършва по следните три критерия:

1. *Качество на изображението* – показва степента на подобие на изображенията преди и след процеса на кодиране на данните, измерена чрез средната квадратична грешка (MSE) и отношението на пиковия сигнал към шума (PSNR) [32].
2. *Размер на вгражданите данни* – дава представа за максималната големина на данните, които могат да се вградят в изображението.
3. *Свойства на метода (функция на оценяване)* – своеобразен вид оценъчна функция, която представя степента на значимост на свойствата на метода за дадено приложение. Тя взема под внимание модулността и адаптивността на методите, устойчивостта срещу JPEG трансформации, способността за вграждане на произволни, дефинирани от потребителя двоични данни и възможността за откриване на неправомерно променени области в изображението.

Даден метод не може да се оптимизира по трите критерия едновременно. Тъй като различните сценарии на приложение имат различни изисквания, не съществува универсален метод за криене на данни, подходящ за всички възможни сценарии.

5.1 Експериментални множества от носещи изображения и двоични данни за вграждане

Оценката на модулните методи се осъществява чрез тяхното прилагане върху специално подбрани множества от изображения и файлове с двоични данни за вграждане. Те са избрани така, че да покриват широк спектър от възможни комбинации между различни видове изображения (цветни, черно-бели, снимки, комикси, и т.н.) и двоични данни (текстови, изпълними, компресирани файлове и др.) (Фиг. 58). Експерименталното множество от изображения е едно и също при всички извършвани експерименти. Поради различното максимално количество на вгражданите данни при стеганографския приложно-специфичен модул и приложно-специфичния модул за цифрово маркиране се използват две различни експериментални множества от двоични данни.

Лена | *Цветна снимка* | *Сканирана снимка в нива на сивото* | *Цветна рисунка* | *Сканиран текст*

Фиг. 58: Примерни изображения, принадлежащи на експерименталното множество

5.2 Оценка на модулните методи

В този раздел се описва как се изпитват свойствата на модулните методи с различни изображения и двоични данни за вграждане и се измерва качеството на получените изображения. Основно свойство, което трябва да се изпита поради естеството на разработените алгоритми, е устойчивостта на вградените данни срещу JPEG компресия, декомпресия и рекомпресия. То се гарантира от базовия модул *DCTHiderEngine*. Качеството на крайните изображения се измерва с помощта на индикаторите средна квадратична грешка $e^{(MSE)}$ и отношение на пиковия сигнал към шума $e^{(PSNR)}$:

$$e^{(MSE)} = \frac{1}{3d_x d_y}\sum_{i=0}^{d_y-1}\sum_{j=0}^{d_x-1}\left(R_{i,j}^{(1)} - R_{i,j}^{(2)}\right)^2 + \left(G_{i,j}^{(1)} - G_{i,j}^{(2)}\right)^2 + \left(B_{i,j}^{(1)} - B_{i,j}^{(2)}\right)^2,$$

$$e^{(PSNR)} = 10.log_{10}\left(\frac{P_{max}^2}{e^{(MSE)}}\right) = 10.log_{10}\left(\frac{255^2}{e^{(MSE)}}\right) = 20.log_{10}\left(\frac{255}{\sqrt{e^{(MSE)}}}\right),$$ където

с d_x и d_y се обозначават съответно ширината и височината на изображението, а с $R_{i,j}^{(1)}$, $G_{i,j}^{(1)}$, $B_{i,j}^{(1)}$, $R_{i,j}^{(2)}$, $G_{i,j}^{(2)}$ и $B_{i,j}^{(2)}$ се обозначават съответно червената, зелената и синята компоненти на пиксела с координати (i, j) съответно от първото и второто изображение.

Табл. 3: Модулен стеганографски метод – постигнати резултати

Параметри на експерименталните процедури				Постигнати резултати				
Експе-рименталн двойки	Фактор на JPEG компр.	Среден размер на изобр. [пиксели]	Среден размер на данните [байтове]	Устойчивост срещу JPEG трансформации			Средна стой-ност на MSE	Средна стой-ност на PSNR [dB]
				Комп-ресия [%]	Деком-пресия [%]	Рекомпре-сия [%]		
1500	*70*	*606x583*	*1004*	*100*	*100*	*100*	*26,5*	*38,9*
1500	*80*	*606x583*	*1004*	*100*	*100*	*100*	*15,5*	*40,0*
1500	*90*	*606x583*	*1004*	*100*	*100*	*100*	*7,5*	*42,2*

Методът за стеганографски цели и за методът целите на цифровото маркиране се изпитват отделно поради разликата в максималния размер на използваните двоични данни. Изпитанията се провеждат чрез описаната в Глава 4 програмна система и нейния графичен потребителски интерфейс за групова обработка и анализ. Всички възможни комбинации от два елемента – един елемент от експерименталното множество от изображения и един елемент от експерименталното множество от двоични данни, се обработват от избрания модулен метод с подходящо подбрани параметри на процесите на кодиране и декодиране. По време на обработките на изображенията се използва библиотеката с отворен код IJG. След като всички експериментални двойки бъдат обработени, се изчисляват средни стойности $e_{avg}^{(MSE)}$ и $e_{avg}^{(PSNR)}$, даващи обща характеристика за работата на метода върху избраните експериментални множества от изображения и двоични данни или водни знаци:

$$e_{avg}^{(MSE)} = \frac{1}{K} \cdot \sum_{i=1}^{K} e_i^{(MSE)} \text{ и } e_{avg}^{(PSNR)} = \frac{1}{K} \cdot \sum_{i=1}^{K} e_i^{(PSNR)}, \text{ където}$$

K обозначава броя на обработените двойки, а $e_i^{(MSE)}$ и $e_i^{(PSNR)}$ са изчислените стойности съответно на MSE и PSNR за експерименталната двойка с пореден номер i.

Експерименталните резултати за двата метода са дадени на Табл. 3 и Табл. 4.

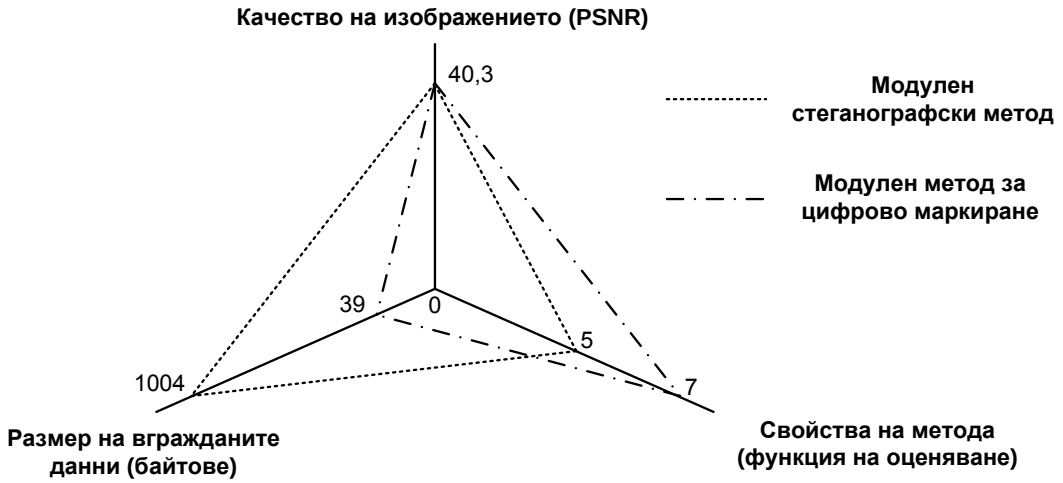
Табл. 4: Модулен метод за цифрово маркиране – постигнати резултати

Параметри на експерименталните процедури				Постигнати резултати				
Експе-рименталн двойки	Фактор на JPEG компр.	Среден размер на изобр. [пиксели]	Среден размер на данните [байтове]	Устойчивост срещу JPEG трансформации			Средна стой-ност на MSE	Средна стой-ност на PSNR [dB]
				Комп-ресия [%]	Деком-пресия [%]	Рекомпре-сия [%]		
750	*70*	*606x583*	*39*	*100*	*100*	*100*	*26,3*	*38,3*
750	*80*	*606x583*	*39*	*100*	*100*	*100*	*15,0*	*39,9*
750	*90*	*606x583*	*39*	*100*	*100*	*100*	*7,0*	*42,4*

Експерименталните резултати от проверката на устойчивостта срещу JPEG компресия, декомпресия и рекомпресия са отлични и показват *100%* устойчивост. Средните

стойности на PSNR лежат в тесни граници около *40 dB*, което надминава много от съществуващите методи, продукти и Интернет-базирани услуги за криене на данни при използваните средни размери на изображението и количество на вгражданите данни.

Резултатите от оценката на двата модулни метода са обобщени на Фиг. 61. Подчертан е компромисът, който се прави между размера на вгражданите данни и новите свойства (запазване на водния знак при промени в изображението и разпознаване на променените региони), предоставени от метода за цифрово маркиране. Компромиси от този вид променят площта и положението на триъгълника, който описва графично общата оценка на метода. Това води до промяна в практическите приложения, за които е подходящ съответният метод.



Фиг. 61: Модулни методи за криене на данни – резултати от оценката

5.3 Оценка на ефективността на съществуващите подходи и методи за статистически стеганализ

Едно от важните изисквания към практическата приложимост на методите за криене на данни е способността за вграждане на данните по такъв начин, че те да са невидими не само за реалните потребители, но и за съществуващите автоматизирани методи за стеганализ. Методите за стеганализ могат да бъдат разделени на същите категории като методите за криене на данни. Тук фокусът е основно върху методите за стеганализ, работещи в DCT-спектралната област.

За разлика от други инженерни и информационни области, приложението на формални модели в стеганографията и цифровото маркиране е силно затруднено поради специфичния начин на използване и обработка на вгражданите данни и техните носители. В стандартния случай не може да се създаде подходящ формален модел на използваните носители на информация (напр. изображения) или вграждани данни (напр.

двоични файлове или водни знаци), тъй като по дефиниция те са изцяло под контрола на отделните потребители, чиито нужди са различни и се променят във времето.

Този раздел представя някои от по-значимите методи за стеганализ, които работят директно с пикселите на изображението както и методи, които анализират DCT спектралната област, за да установят наличие на данни, устойчиви на загубна компресия. Интересна особеност е, че част от подходите, разработени с цел откриване на наличие на вградени данни в DCT спектралната област, се базират на друг вид трансформация - дискретната уейвлитна трансформация (DWT), като се използват различни статистически характеристики на уейвлитните коефициенти [33].

Ефективността на някои по-популярни и разпространени алгоритми за стеганализ при откриването на данни, вградени от модулните методи е оценена чрез програмата с отворен код *Stegdetect* [34], създадена от Нилс Провос. *Stegdetect* може да провежда четири различни вида статистически стеганализ, които откриват присъствие на данни, вграждани от класически програми за криене на данни като *JSteg, JPHide* и *OutGuess*. Чувствителността на статистическите експерименти, която влияе на допуснатите грешки при откриването на данни (вж. [3]), се контролира чрез специален команден параметър на програмата, наречен *Sensitivity*. При оценката се пресмята процентът P_c на изображенията, в които *Stegdetect* не е открил данни:

$$P_c = \frac{n_c}{n_a} \times 100\% ,$$

където n_c е броят на изображенията, в които *Stegdetect* не е открил данни, а n_a е общият брой на изображенията в дадено множество (Табл. 7).

Табл.7: Резултати от анализа, проведен със *Stegdetect*

Stegdetect чувствителност	P_c за множеството от оригинални изображения [%]	P_c за множеството от изображения, съдържащи данни, вградени от стеганографския метод [%]	P_c за множеството от изображения, съдържащи данни, вградени от метода за цифрово маркиране [%]
1,0	91,5	97,7	93,0
2,0	73,2	91,7	88,0

* Стойността по подразбиране на чувствителността на *Stegdetect* е равна на 1,0

Високите процентни стойности на P_c водят до извода, че съществуващите статистически методи за откриване на вградени данни не могат да откриват надеждно присъствието на данни, вградени от модулните методи. Нещо повече – процентните стойности на P_c за двете множества от изображения, съдържащи вградени данни, са дори по-високи от стойностите за множеството от оригинални изображения,. Това показва, че модулните методи се справят добре със задачата да наподобят естествени, необработвани изображения. Най-вероятните причини за този на пръв поглед леко изненадващ резултат се крие във възможни статистически деформации, съществуващи в оригиналните изображения и предизвикани напр. от многократна компресия. Някои от тези деформации могат да бъдат погрешно интерпретирани от стеганализ алгоритмите,

като индикатори за наличие на вградени данни. Модулните методи коригират голяма част от тези деформации и по този начин постигат по-голяма процентна стойност на P_c.

5.4 Реализация и оценка на ефективността на два принципни подхода за стеганализ

В този раздел се разглеждат няколко различни варианта на два принципни подхода при създаването на общи методи за стеганализ:

1. Първият принципен подход се базира на изследването на корелации в изображението, като се очаква корелацията в рамките на един блок, както и между блоковете, да е по-малка в изображения, съдържащи скрита информация, в сравнение с техните оригинали.
2. Вторият подход се базира на прилагане на филтър върху изображението и изследването на разликите между резултата от филтрирането и изображението, което се филтрира, чрез построяването на диференчно изображение. Тъй като вграждането на данни би следвало да увеличи нивата на шум в изображението, то се очаква диференчните изображения, получени от изображенията, съдържащи скрита информация, да се отличават с по-високи стойности на интензитета на пикселите в сравнение с диференчните изображения, получени от оригиналите.

Основната цел е да се оцени практическата приложимост на двата подхода по отношение на модулните методи. Трябва да се отбележи, че модулният подход за криене на данни утежнява разработката на методи за стеганализ поради факта, че всеки модулен метод е съставен от комбинация от модули, всеки от които има влияние върху статистическите свойства на мултимедийното съдържание, като базовите модули имат по-голямо влияние в сравнение с приложно-специфичните модули.

Реализирани са общо четири алгоритъма за изследване на корелации и други статистически характеристики в изображенията, като се използва корелацията на Пиърсън [35], [36], която в дискретния случай приема вида:

$$r_{X,Y} = \frac{\sum_{i=0}^{n-1}(X_i - E(X))(Y_i - E(Y))}{\sqrt{\sum_{i=0}^{n-1}(X_i - E(X))^2}\sqrt{\sum_{i=0}^{n-1}(Y_i - E(Y))^2}},$$

където $E(X)$ и $E(Y)$ са съответно средните стойности (математическите очаквания) на случайните променливи X и Y. Анализът на получените резултати от различните алгоритми показва, че провеждането на стеганализ за модулните методи без наличие на оригиналното изображение е ненадежден. В частност, големите разлики в стойностите на коефициентите на корелация, изчислени за оригиналните изображения и силно променливият знак и ниските абсолютни стойности на величините в колоните „(μ-o)/σ" са

решаващи фактори, определящи до голяма степен неуспеха на корелационните алгоритми.

За целите на стеганализа е възможно прилагането на различни филтри върху изображението - усредняващ филтър, Гаусов филтър, медианен филтър, Винер-Колмогоров филтър, Лапласиан на Гаусиана, описани подробно в [23]. Получените резултати за различните филтри показват сходство с резултатите, получени при изследването на корелациите. Наблюдават се големи разлики в стойностите на метриките, изчислени за оригиналните изображения и силно променливи знаци и абсолютни стойности на величините в колоните „(μ-o)/σ", които определят до голяма степен неуспеха на стеганализа.

Подобрение на резултатите би могло да се получи, ако бъдат намерени допълнителни зависимости между метриките и други характеристики, напр. размерите и текстурите на изображението, с цел намаляване на разликите на стойностите. Получените таблици не дават индикации за съществуването на такива зависимости.

5.5 Заключение

Експериментите и оценката на модулните методи за криене на данни предоставят емпирично доказателство за качеството на тяхното проектиране и програмна реализация. Методите успешно реализират свойствата, необходими за приложение в Интернет-базирана среда, и постигат целта и задачите на дисертацията. Описаните и изследвани в тази глава подходи и методи за стеганализ не са ефективни по отношение на модулните методи за криене на информация.

Глава 6. Приложение на методите в Интернет-базирани сценарии

В тази глава се дискутира практическото приложение на разработените методи в няколко конкретни Интернет-базирани сценария:

1. Предотвратяване на фишинг (англ. phishing) при използване на портали за Интернет-банкиране;
2. Защита на мултимедийната интелектуална собственост на информационни агенции;

3. Подобряване на законосъобразното използване на мултимедийно съдържание в Интернет-базирани общества, например социални мрежи и форуми като Facebook и DevianArt.

Концепцията и програмната реализация на Интернет-базирана услуга за сертифициране на мултимедийно съдържание посредством методи за криене на данни е подробно разгледана и нейната употреба в сценариите е представена в следващите раздели.

6.1 Предотвратяване на фишинг на банкови портали

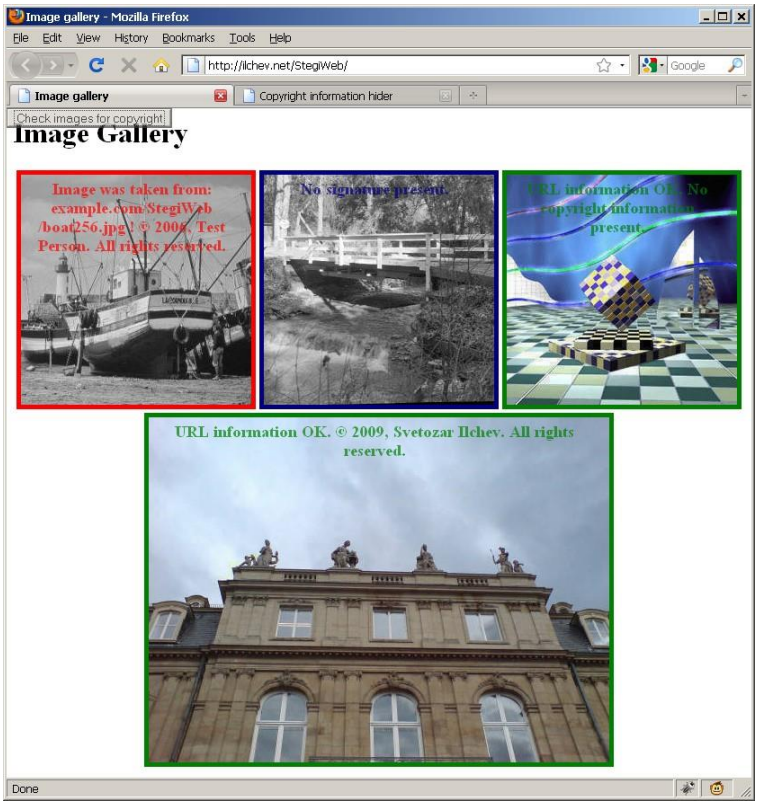
Този сценарий разглежда как сигурността на порталите за Интернет-банкиране може да се подобри чрез използването на методи за криене на данни в допълнение към традиционните технологии за сигурност, които банките използват. Сценарият е от значение и за други корпорации с Интернет портали, които дават достъп на крайни клиенти до част от корпоративната инфраструктура – мобилни оператори като М-Тел, големи Интернет-базирани търговски платформи като Amazon и eBay или услуги за плащане като PayPal.

Фиг. 63: Приложение на модулните методи като мрежова услуга за сертифициране

Традиционните технологии за сигурност разчитат на криптографски подходи и третират съдържанието на Интернет портала като пасивен обект, регулирайки единствено нивото на достъп до него. То не се използва за подобряване на сигурността и служи единствено на крайните потребители. Технологиите за криене на данни позволяват активната употреба на съдържанието за подобряване на цялостната сигурност и предотв-

ратяване на различните вариации на фишинг. Така самото съдържание става допълнително средство за проверка на автентичността на портала и информацията, която той предоставя.

Модулните методи за криене на данни могат се предложат под формата на мрежова услуга чрез използването на подходящ интерфейс за мрежови услуги. Тази мрежова услуга е по същество сертифицираща услуга, даваща възможност за надеждна проверка на автентичността на мултимедийни файлове в корпоративен интранет или в глобалната мрежа (Фиг. 63). Прототипната реализация на сертифициращата услуга за криене на данни използва Microsoft Internet Information Server (IIS), инсталиран на отделна машина, която предоставя необходимата изчислителна мощност за изпълнение на модулните методи за криене на данни.



Фиг. 73: Графичен интерфейс на потребителски скрипт след проверка на сигнатурите

Интеграцията на сертифициращата услуга за криене на данни с Интернет браузърите на крайните потребители зависи до голяма степен от разширяемостта на различните браузъри, съществуващи на пазара, с нова функционалност. Прототипната реализация в тази дисертация се базира на потребителски скрипт, написан на JavaScript, който работи с широко разпространения Интернет браузър Mozilla Firefox и браузърното разширение GreaseMonkey [37] (Фиг. 73). Други широко разпространени браузъри, които поддържат потребителски скриптове са Internet Explorer, Opera и Safari [38].

Когато крайният потребител посети легитимния портал на банката, потребителският скрипт ще маркира всички изображения със зелени рамки, което означава, че сигнатурите съответстват на банковия портал. Ако потребителят посети фалшив банков портал вследствие на опит за фишинг, потребителският скрипт ще маркира изображенията на портала с червени или сини рамки, което е индикатор съответно за грешни или липсващи сигнатури (Фиг. 73). Потребителският скрипт (или браузърно разширение) може да предприеме и други действия освен добавянето на подходящо оцветени рамки към изображенията. Той може да забрани достъпа до Интернет портали, чиито изображения не са снабдени с правилните сигнатури. Ако подписани изображения бъдат намерени на фалшив Интернет портал, потребителският скрипт може да използва информацията от сигнатурите, за да пренасочи Интернет браузъра на потребителя към адреса на истинския банков портал. Също така той може да уведоми съответните органи на властта за откритите нарушения.

6.2 Защита на мултимедийната интелектуална собственост на информационни агенции

Фиг. 76: Откриване на нарушения на авторските права

Този сценарий разглежда предимствата на модулните методи за криене на данни и сертифициращата услуга за криене на данни, представена в предишния раздел, по отношение на защитата на мултимедийно съдържание, публикувано в Интернет. Това е класически случай на приложение на цифровото маркиране. Основни целеви групи на подобрената защита са новинарски агенции, фотожурналисти, филмови продуценти - потребителски групи, предоставящи онлайн достъп до мултимедия в глобалната мрежа. Използването на сертифициращата услуга за криене на данни за тази цел е илюстрирано на Фиг. 76.

6.3 Подобряване на законосъобразното използване на мултимедийно съдържание в Интернет-базирани общества

Предложените методи са подходящи за използване в рамките на Интернет-базирани общества – социални мрежи като Facebook и мултимедийни форуми като DevianArt, които се характеризират с формално нерегулирано разпространение и създаване на връзки (англ. linking) към мултимедийно авторско съдържание. Това поражда *два* принципни проблема:

1. Интернет потребителите трудно могат да определят правния статус на дадена мултимедийна творба и да установят контакт с нейния автор, за да получат разрешение за ползване, ако това е необходимо. При липсата на бърза и ефективна възможност за установяване на лицензия на ползване на мултимедийната творба, потребителите често допускат, че тя е свободна за ползване, тъй като вече се намира в Интернет.
2. Някои Интернет потребители целенасочено нарушават авторското право и претендират за авторство върху разпространявани в цифров вид творби, които не са създадени от тях. В случай,че реалните автори потърсят правата си, те трудно могат да докажат кой е истинският автор.

Фиг. 77: Микроплащане на мултимедийни творби

За ефективното решение на гореспоменатите два проблема и за постигане на по-добро прилагане на законовите регулации е нужен нов технически подход, който би повлиял върху съществуващата Интернет култура и би довел до промяна в навиците на

Интернет потребителите. Сценарий за примерното използване на методите за криене на данни за определяне на правния статус и заплащането на мултимедийни творби (микроплащане, англ. micropayment) е показан на Фиг. 77.

Цифровото маркиране трудно може да се използва като защитен механизъм за предотвратяване на извършването на нарушения на авторското право, но то може да улесни тяхното бързо откриване от участниците в Интернет-обществото. Саморегулацията в Интернет-базираните общества и социалните мрежи би могла да бъде високо ефективна, подобно на малките населени места в реалния свят. Ако информация за неморално поведение - в този случай неспазването на авторското право - стане публично достояние, то тогава е неизгодно за всеки, които иска да остане част от обществото, да извършва нарушение, дори и при липса на формални наказателни механизми. Цифровото маркиране предоставя техническите средства за публично оповестяване на нарушения на авторското право в децентрализирани Интернет-базирани общества. Тази роля на технологията допълва първия сценарий, дискутиращ улесняването на легалната употреба. По този начин цифровото маркиране подобрява придържането към правилата на поведение в Интернет-базираните общества чрез едновременното намаляване на усилията за добро поведение и увеличаване на значимостта на последствията от нарушения.

6.4 Заключение

Това, което обединява различните приложни сценарии, е използването на самото мултимедийно съдържание за подобряването на различни аспекти на сигурността и защитата на участниците. Тъй като вгражданите сигнатури могат да реализират криптографски подходи на защита, то методите за криене на данни не заменят, а по-скоро допълват и дават нова свобода за ползване на традиционната криптография.

Глава 7. Заключение – основни резултати

Разработеният модулен подход за криене на данни позволява създаването на разширяеми и адаптируеми методи за криене на данни, устойчиви срещу JPEG трансформации и стеганализ. Поради възможността за повторно използване на модулите на методите и лесното напасване към промени в изискванията на сценария, модулните методи за криене на данни могат да бъдат създавани бързо и на достъпна цена. Комуникационният интерфейс за мрежови услуги и характеристиките на методите, разработени специално за употреба в Интернет-базирани сценарии, помагат за внедряването на тех-

нологията за криене на данни в мултимедия в сценарии от непосредствено значение за Интернет потребителите.

Бъдещата работа по модулния подход за криене на данни би включвала създаването на достатъчно голям набор от модули, които предлагат поддръжка на разпространени и често използвани графични формати, трансформации и др. Допълнителна част от насоките за бъдеща работа би било създаването на модулна концепция за стеганализ, която е огледално копие на модулния подход, разработен в дисертацията. Тя би позволила разделянето на методите за стеганализ на модули, които могат да бъдат разработвани паралелно с модулите на методите за криене на данни. Друга важна предпоставка за практическия успех на методите е свързана със създаването на единен набор от добре обмислени стандартизирани интерфейси за мрежови услуги, които гарантират удобно внедряване на услугата за сертифициране в различни видове Интернет-базирани сценарии.

Мултимедийното съдържание вече е основна съставна част на Интернет. Методите за криене на данни предоставят ефективен начин за защита на това съдържание. В близко бъдеще те ще станат неотменима част от механизмите за сигурност, които осигуряват безопасността на потребителите.

Приноси

Основните научно-приложни приноси на настоящата дисертация са:

1. Разработен е нов модулен подход за криене на данни и е дефиниран наборът от методи за комуникация между модулите.
2. Създаден е собствен метод за постигане на устойчивост срещу JPEG компресия, декомпресия и рекомпресия, който работи с произволни изображения и данни за вграждане, като гарантира възстановяването на вградените данни с точност до бит. Методът е реализиран в контекстно-независим базов модул.
3. Проектиран е контекстно-независим базов модул за работа с изображения с беззагубна компресия, използващ модулация на индекса на квантизация. Той работи с произволни изображения и данни за вграждане и гарантира възстановяването на скритата информация с точност до бит.
4. Създаден е стеганографски метод за криене на данни, включващ стеганографски приложно-специфичен модул, направляващо описание на вгражданите файлове, кодове за корекция на грешки и разбъркване на данните.
5. Създаден е метод за цифрово маркиране, включващ приложно-специфичен модул за цифрово маркиране, направляващо описание на вгражданите водни знаци и въз-

можности за откриване на променени блокове в изображението и възстановяване на вградения воден знак в случай на промени.

6. Създадена е многослойна архитектура на прототипна програмна система за целите на проверката, оценката и стеганализа на модулния подход за криене на данни и разработените модулни методи.
7. Изследвана и оценена е ефективността на някои популярни и разпространени алгоритми за стеганализ по отношение на модулните методи за криене на данни. Освен това е изследвана и оценена ефективността на два принципни подхода за стеганализ: подход, базиран на изследване на корелациите в изображението, и подход, базиран на прилагане на филтри.

Основните приложни приноси на настоящата дисертация са:

1. Реализирана е прототипна програмна система посредством програмните езици VB.NET, C# и C/C++. Тя се състои от следните слоеве: слой на данните, слой на базовите модули, слой на приложно-специфичните модули и интерфейсен слой.
2. Проектирани и реализирани са инструменти за групова обработка и анализ на изображенията, за прилагане на филтри и за построяване на хистограми в различни цветови пространства.
3. Оценена е реализацията на модулните методи чрез изследване на устойчивостта на вградените данни срещу JPEG трансформации и проверка на качеството на изображенията.
4. Изследван е начинът на приложение и са определени предимствата на модулния подход и модулните методи за криене на данни в три сценария: сценарий за предотвратяване на фишинг на банкови портали, сценарий за защита на мултимедийната интелектуална собственост на информационни агенции и сценарий за подобряване на законосъобразното използване на мултимедийно съдържание в Интернет-базирани общества.
5. Разработена е програмна реализация на сертифицираща услуга за криене на данни, която може да се интегрира в различни Интернет-базирани приложни сценарии и предоставя достъп до функционалността на модулните методи за криене на данни.

Библиография

[1] Herodotus, *Histories, Book 5*., 440 B.C.

[2] J. Peterson. (1997) Steganographia (Secret Writing), by Johannes Trithemius. [Online]. URL: http://www.esotericarchives.com/tritheim/stegano.htm (accessed August 9, 2012).

[3] I. J. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2nd ed.: Morgan Kaufmann Publishers, 2008.

[4] E. Lin and J. Delp, "A Review of Data Hiding in Digital Images," in *Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS '99)*, Savannah, Georgia, 1999, pp. 274-278.

[5] K. Curran and K. Bailey, "An Evaluation of Image Based Steganography Methods," *International Journal of Digital Evidence*, vol. 2, no. 2, 2003.

[6] E. Cole, *Hiding in Plain Sight: Steganography and the Art of Covert Communication*, 1st ed.: John Wiley & Sons, 2003.

[7] Interagency Working Group (IWG) On Cyber Security and Information Assurance (CSIA). (2006) Federal Plan for Cyber Security and Information Assurance Research and Development. [Online]. URL: http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf (accessed May 18, 2011).

[8] D. Feng, W. Siu, and H. Zhang, *Multimedia Information Retrieval and Management*, 1st ed.: Springer, 2003.

[9] C. Lu, *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*, 1st ed.: Idea Group Publishing, 2005.

[10] Y. Shi and H. Sun, *Image and Video Compression for Multimedia Engineering*, 1st ed.: CRC Press, 2000.

[11] J. Mitchell, W. Pennebaker, C. Fogg, and D. LeGall, *MPEG Video Compression Standard*, 1st ed.: Kluwer Academic Publishers, 2002.

[12] G. Booch et al., *Object-Oriented Analysis and Design with Applications*, 3rd ed.: Addison-Wesley, 2007.

[13] Electronic Privacy Information Center. Cryptography Policy. [Online]. URL: http://www.epic.org/crypto/ (accessed May 18, 2011).

[14] World Wide Web Consortium. About W3C: Goals. [Online]. URL: http://www.w3.org/Consortium/mission (accessed March 24, 2011).

[15] T. O'Reilly. (2005) What is Web 2.0. [Online]. URL: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html?page=1 (accessed May 9, 2011).

[16] T. O'Reilly. (2006) Web 2.0 Compact Definition: Trying Again. [Online]. URL: http://radar.oreilly.com/2006/12/web-20-compact-definition-tryi.html (accessed May 9, 2011).

[17] T. O'Reilly. (2006) Harnessing Collective Intelligence. [Online]. URL: http://radar.oreilly.com/2006/11/harnessing-collective-intellig.html (accessed May 9, 2011).

[18] M. Backes and C. Cachin, "Public-key steganography with active attacks," in *2nd Theory of Cryptography Conference (TCC)*, vol. 3378 of Lecture Notes in Computer Science, 2005, pp. 210-226.

[19] G. Friedman, "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image," *IEEE Transactions on Consumer Electronics*, vol. 39, no. 4, pp. 905-910, 1993.

[20] J. Fridrich and M. Goljan, "Protection of Digital Images Using Self Embedding," in *Symposium on Content Security and Data Hiding in Digital Media*, New Jersey Institute

of Technology, 1999.

[21] S. Meyer. (2008) Midnight Sun: Edward's Version of Twilight. [Online]. URL: http://www.stepheniemeyer.com/midnightsun.html (accessed June 18, 2011).

[22] S. Voloshynovskiy, F. Deguillaume, O. Koval, and T. Pun, "Information-theoretic Data-hiding: Recent Achievements and Open Problems," *International Journal of Image and Graphics*, vol. 5, no. 1, pp. 1-31, 2005.

[23] R. Gonzalez and R. Woods, *Digital Image Processing*, 2nd ed.: Prentice Hall, 2002.

[24] W. B. Pennebaker and J. L. Mitchell, *JPEG Still Image Data Compression Standard*, 1st ed.: Van Rostrand Reinhold, New York, 1993.

[25] E. Lin and E. Delp, "A Review of Fragile Image Watermarks," in *Proceedings of the Multimedia and Security Workshop (ACM Multimedia '99)*, 1999, pp. 25-29.

[26] E. Hamilton. (1992, September) JPEG File Interchange Format. [Online]. URL: http://www.w3.org/Graphics/JPEG/jfif3.pdf (accessed March 16, 2011).

[27] H. Izadinia, F. Sadeghi, and M. Rahmati, "A New Steganographic Method Using Quantization Index Modulation," in *International Conference on Computer and Automation Engineering (ICCAE)*, 2009, pp. 181-185.

[28] D. Knuth, *The Art of Computer Programming*, 3rd ed.: Addison-Wesley, 1998, vol. 2.

[29] J. Gailly and M. Adler. (2012) zlib Home Site. [Online]. URL: http://www.zlib.net (accessed Feb. 04, 2012).

[30] W3C. (2013, January) SOAP Specifications. [Online]. URL: http://www.w3.org/TR/soap/

[31] Network Workiing Group. (2013, Jan.) RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1. [Online]. URL: http://tools.ietf.org/html/rfc2616

[32] K. R. Rao and P. C. Yip, *The Transform and Data Compression Handbook*, 1st ed.: CRC Press, 2001.

[33] T. Holotyak, J. Fridrich, and S. Voloshynovskiy, "Blind statistical steganalysis of additive steganography using wavelet higher order," in *International Conference on Communications and Multimedia Security*, 2005, pp. 273-284.

[34] N. Provos. (2008) Steganography Detection with Stegdetect. [Online]. URL: http://www.outguess.org/detection.php (accessed May 12, 2011).

[35] M. Spiegel, J. Schiller, and R. Srinivasan, *Probability and Statistics*.: McGraw-Hill, 2001.

[36] P. Hoel, *Introduction to Mathematical Statistics*, 3rd ed.: John Wiley & Sons, 1966.

[37] Aaron Boodman. (2010) Greasespot. [Online]. URL: http://www.greasespot.net (accessed Nov. 02, 2010).

[38] K. Dsouza. (2008, August) Run Greasemonkey User Scripts in IE, Opera and Safari. [Online]. URL: http://techie-buzz.com/tips-and-tricks/greasemonkey-alternatives-for-ie-opera-and-safari.html (accessed August 26, 2011).

Abstracts of Dissertations

Number 4, 2014

INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

BULGARIAN ACADEMY OF SCIENCES

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Брой 4, 2014

Автореферати на дисертации