Modular Data Hiding as an Alternative of Classic Data Hiding for Web-based Applications

S. Ilchev, Z. Ilcheva

Key Words: *Data hiding; digital steganography; digital watermarking; web-based applications; modularity.*

Abstract. *Data hiding methods improve the security of the transmission and storage of information by embedding digital data inside the content of multimedia files. Classic data hiding methods, products and services reviewed in this paper are optimized for a specific purpose and have a monolithic design. Usually, they do not take into consideration some important requirements of the contemporary World Wide Web. Modular data hiding and a corresponding SaaS approach are being developed as a viable alternative oriented towards the needs for adaptability and reliability of modern web-based applications and their users.*

1. Introduction

In the course of the last twenty years, data hiding has established itself as an important innovative security technology. It can be used independently but it is usually applied in combination with traditional security technologies such as cryptography in order to assist in the protection of digital documents and multimedia content [1,2,3,4,5] (*figure 1*).

The essence of data hiding is the embedding of digital data as an integral part of the content of digital multimedia files. The embedding may serve two distinct purposes and thus it may be used in two different ways. First, it may target the protection of the embedded digital data (e.g. an important classified document). Second, it may target the protection of the multimedia file (copyright protection, identification of the buyer or the owner, protection from unauthorized modifications such as photoshopping a picture, etc). The first way of usage of data hiding is known as steganography and the second one is known as digital watermarking.

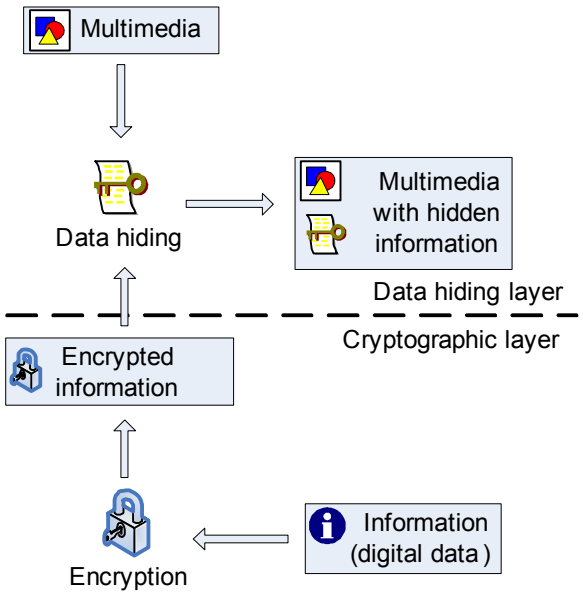

Figure 1. Data hiding of encrypted information

Some significant advantages of data hiding protection include:

- Invisibility (transparency) of the protection - the application of a data hiding protection is difficult to detect and usually involves a lengthy and difficult development of sophisticated steganalysis methods [6].
- Backward compatibility - a data hiding protection is often backward compatible with any cryptography-based security measures that are already in use.
- Absence of legal regulations - attempts to regulate cryptography by law and to define an upper limit to the strength of cryptographic protection allowed for civil use have already been made [7]. So far, data hiding is outside the purview of lawmakers.
- Flexibility and reliability - the embedded data becomes an integral and inseparable part of the multimedia content. It is difficult to remove without authorization and can be made robust against common transformations like compression, cropping, etc.

In this discussion, we will focus on data hiding methods and algorithms designed to process images intended for web-related use - distribution via web channels (web portals - e.g. *nytimes.com*, art - *devianart.com*, social networks - *facebook.com*, etc.).

2. Important Data Hiding Requirements for Web-based Applications

Different requirements may be imposed on data hiding methods such as the robustness against geometric transformations, compression and format changes or the detection of a replacement of parts of the multimedia host, etc ([8,9]). Three requirements are especially important and essential if data hiding is to be applied successfully in the World Wide Web.

The first requirement is the possibility for extension and enhancement of the methods. The inherent openness and volatility of the World Wide Web in combination with the rapid changes in the contemporary social, business and technological environment lead to frequent modifications in user requirements. Some of them pertain to the application areas of data hiding technology. For this reason, data hiding methods should be adaptable to new user requirements and they should be capable

of incorporating new features, while still providing certain basic functionality expected by the end user.

The second important requirement is the robustness against JPEG transformations. A typical requirement for data hiding methods is that they ensure the preservation of the information embedded into the multimedia host after compression ([1,2]). Compression is applied to reduce the size of the transmitted multimedia content and most often lossy compression formats are utilized due to their higher compression ratio. One of the most important compressed image formats is JPEG, which utilizes the discrete cosine transform (DCT) [10]. Its universality and good compression ratio have made it a preferred choice for storing color and grey-scale images. For this reason, it is important for hidden data not to be destroyed by JPEG-related transformations such as compression (encodes a matrix of pixels in a JPEG image file), decompression (decodes a matrix of pixels from a JPEG image file) or recompression (changes the compression ratio or other parameters of a JPEG image file). The robustness against all three transformation types is important for the flexible use of data hiding algorithms in web. Compression is used to reduce the size of newly created images and to make them readable by browsers. Decompression is used to extract the image content, so that it can be shown on screen, modified or recoded in another image format. Recompression is used mainly to reduce the image size. It is often applied to existing JPEG images prior to their distribution via web-related channels (sending by e-mail or uploading to a web site).

It is also important to achieve robustness against the execution of the above transformations by arbitrary programs. For this purpose, intimate knowledge of the JPEG image compression standard itself as well as its specific implementations by software vendors ([10,11]) is needed.

The third important requirement is the capability of the methods to work on arbitrary image content and to embed arbitrary data. The image content is widely used on the web in different varieties. Data hiding methods need to be flexible enough to cope with arbitrary host images supplied by users. This requirement has two important implications. First, data hiding methods should be able to handle black&white, grey-scale and color images and they should not be dependent on any characteristics, which are specific for a particular class of images. Second, the original host image or any statistical information describing it should not be necessary for the decoding of the embedded information. Data hiding methods having this property are referred to as blind ([2]) and provide maximum flexibility.

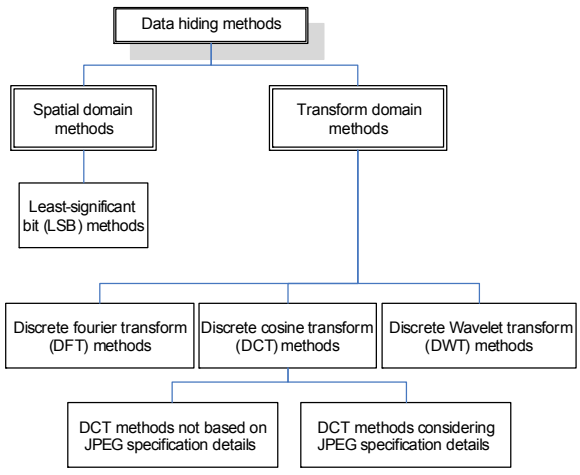

Figure 2. Data hiding method classification

As data hiding methods in the web often work on encrypted or compressed user-defined data, they should not impose any restrictions on the form or the future use of the hidden data. Two considerations are important: the embedded data should be regarded as an arbitrary stream of binary data and an error-free retrieval of the embedded data should be possible in order to permit its subsequent use by other technologies.In the remaining sections of this paper, we will focus on these three requirements and we will analyze the state-of-the-art of academic research and commercial products.

3. Data Hiding for Web-based Applications: State-of-the-art

Both academic research and practical data hiding implementations are considered and their suitability for web-related applications is discussed. A classification of the most important types of data hiding methods is presented in *figure 2* ([2,9,12,13]).

Spatial domain methods work directly on image pixels. Most often they fall into the group of the so-called least-significant bit (LSB) methods, which modify the LSBs of image pixels. Transform domain methods, on the other hand, work on the output of various mathematical transforms of the image. As lossy image compression is often based on such mathematical transforms, these methods perform well if the hidden information has to withstand image compression. Three widely used transforms are the discrete Fourier transform (DFT), the discrete cosine transform (DCT) and the discrete wavelet transform (DWT). DCT data hiding methods are based on the same mathematical transform used by the JPEG standard [10]. They can be further divided into two groups: DCT methods which are not based on the JPEG specification and DCT methods which follow JPEG specification details.

Due to the large number of existing data hiding methods and the importance of the JPEG image format for the web, only DCT methods are reviewed in the paper. Their capability of handling JPEG transformations is examined and the conformity to the requirements presented in the previous section is evaluated.

3.1. Academic Research

The first JPEG-based data hiding method was JSTEG, developed in 1993 by Derek Upham ([14,15] and [16]). It is a steganographic method which hides arbitrary binary data by replacing the LSBs of the DCT coefficients of JPEG images. Another early data hiding method for digital watermarking was proposed by Zhao and Koch, Fraunhofer institute, Darmstadt in 1995 ([17] and [18]). It hides one bit per DCT block by creating a special relationship among the elements of a set of three DCT coefficients.

Another digital watermarking method was developed in

1997 by Cox, et al., University College London [19]. The method hides watermarks drawn from a Gaussian normal distribution into DCT coefficients by means of scaling functions. In 1998, Wu and Liu, Princeton University, developed another method for digital watermarking [20]. The method hides a visually meaningful binary pattern together with some image content features into the quantized DCT coefficients by means of a specialized look-up table.

A steganographic method designed to hide data, which cannot be detected by statistical steganalysis methods, was developed by Niels Provos, University of Michigan, in 2001 ([21] and [22]). Andreas Westfeld, Technical University Dresden proposed in the same year the F5 method for steganographic applications [23]. It utilizes the so-called matrix coding algorithm [24] in order to minimize the number of necessary changes of DCT coefficients and achieve undetectability by statistical steganalysis methods.

Jessica Fridrich, Binghamton University, and her research group proposed several digital watermarking methods based on DCT transformations. In [25] and [26], the host image is divided into blocks of 64x64 pixels. Each block is transformed to DCT domain and a user-defined watermark is embedded into the DCT coefficients. In [27], the proposed method embeds a highly-specialized watermark which allows a partial reconstruction of image blocks modified by an unauthorized attacker. In [28,29] and [30], the authors propose a method for lossless data embedding. The method embeds a user-defined watermark and allows a full reconstruction of the original unwatermarked image by the receiving side.

Some recent data hiding algorithms rely on a technique called Quantization Index Modulation (QIM), which was first introduced by Costa in 1983 [31] and later analyzed with regard to watermarking applications by Chen and Wornell in 2001 [32]. Li and Cox proposed in 2007 a watermarking method based on QIM and a perceptual model developed by Watson ([33,34]). An improved version of the method was developed in 2008 by Sun, et. al [35]. Another steganographic method utilizing QIM was proposed by Izadinia, et. al. in 2009 [36]. It hides an arbitrary message by applying an algorithm for predictive coding (proposed by Yu, et. al. [37]) to quantized the DCT coefficients. The JPEG decompression or JPEG recompression are not considered.

A brief evaluation of all methods with regard to the requirements discussed in the previous section is presented in *table 1* (N.C. stands for Not Considered). None of the presented methods considers the extensibility. They are monolithic solutions designed for concrete application areas with specific feature requirements. The authors do not discuss how the methods could be integrated into existing solutions.The robustness against JPEG transformations and the arbitrariness of the host image and the embedded data are taken into account only partially. Most methods consider only certain aspects of them (presented in *table 1*). The potential for improvement lies in the simultaneous implementation of all relevant aspects of the requirements.

Table 1. DCT-based data hiding methods - evaluation

Method	Extensibility	Robustness against JPEG transformations			Arbitrariness			
		Compression	Decompression	Recompression	Arbitrary host	Blind method	Arbitrary data	Error-free retrieval
JSteg [14,15,16]	no	yes	N.C.	N.C.	yes	yes	yes	yes
Zhao, Koch [17,18]	no	yes	N.C.	N.C.	yes	yes	yes	yes
Cox, et. al. [19]	no	yes	yes	yes	yes	no	no	no
Wu, Liu [20]	no	yes	N.C.	N.C.	yes	yes	no	yes
Provos [21,22]	no	yes	N.C.	N.C.	yes	yes	yes	yes
Westfeld [23]	no	yes	N.C.	N.C.	yes	yes	yes	yes
Fridrich [25,26]	no	yes	N.C.	N.C.	yes	yes	yes	no
Fridrich [27]	no	yes	N.C.	N.C.	yes	yes	no	yes
Fridrich [28,29,30]	no	yes	N.C.	N.C.	yes	yes	yes	yes
Li, Cox [33]	no	yes	N.C.	N.C.	yes	yes	yes	no
Sun, et. al. [35]	no	yes	N.C.	N.C.	yes	yes	yes	no
Izadinia, et. al. [36]	no	yes	N.C.	N.C.	yes	yes	yes	yes

* N.C. = Not Considered

3.2. Data Hiding Products and Services

In accordance with the strong academic and corporate interest in data hiding, there are some popular data hiding products and services offered over the Internet or as part of larger software bundles.

One of the most well-known steganographic solutions on the market is the Steganos Privacy Suite [38] (*figure 3*). The *File Manager* tool can embed data into compressed or uncompressed host images. The hidden information is robust against JPEG compression at low compression rates but not against JPEG decompression or recompression. The steganographic method is blind and can work with arbitrary data files and host images. A major advantage is the excellent host image quality.

A classic steganographic program for embedding arbitrary data files into JPEG images is JPHide [39]. Its steganographic method is robust against JPEG compression at low compression ratios but not against JPEG decompression or recompression. The method is blind and can work with arbitrary JPEG host images. It also delivers excellent host image quality.

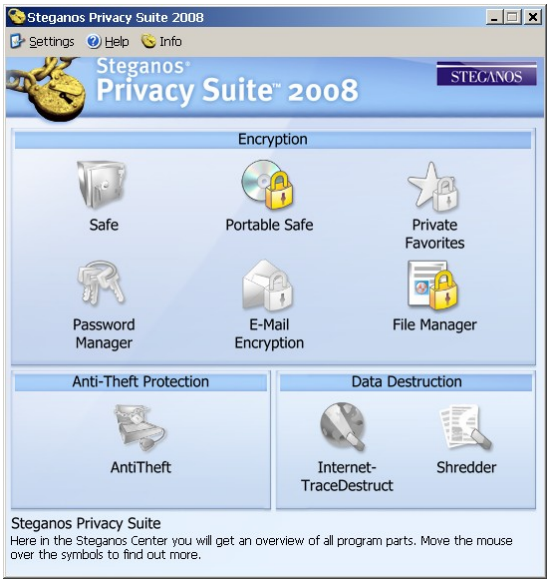

Figure 3. Steganos Privacy Suite

A new steganographic development is the InvisibleSecrets stand-alone GUI program [40] (currently version 4). It has a very nice user interface and supports compressed and uncompressed image formats. With regard to JPEG, it hides the information in the JPEG comment segments (see [10]). This approach has the advantage of not placing any limits to the size of the embedded data but negates many of the advantages of data hiding.

Digimarc [41] is one of the leading data hiding companies that specializes in digital watermarking. The Photoshop plug-in (*figure 4*) which signs digital images is the company's most well-known product. The plug-in embeds a short identification number (ID) along with three Boolean image attributes into the digital content. The identification number plays a central role in the solutions offered by Digimarc - the Digimarc search service, which scans the Internet for images containing the client's ID number, and the integration with digital asset and content management systems targeted at enterprise users.

The Digimarc search service [42] scans web portals for digital images belonging to the Digimarc customers. First, it parses the web portals for images. Then, it tries to read a previously embedded ID number out of each image. If the ID number exists and matches a current customer of the search

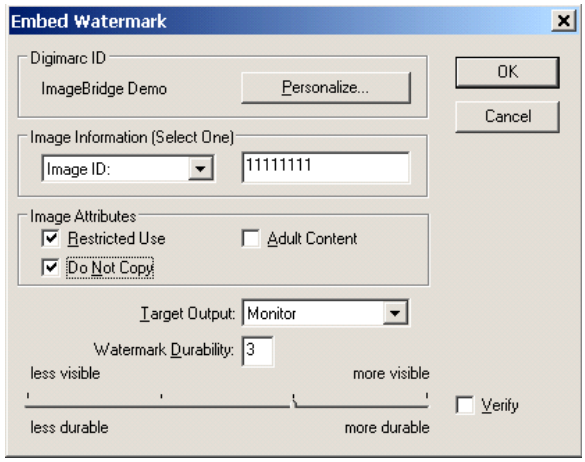

Figure 4. Digimarc's Photoshop plug-in

service, then the location of the image is reported to this customer. In this way, the search service helps customers to keep track of the locations where their digital images are published online.The digital watermarking method used by Digimarc is fairly robust against JPEG compression, decompression and recompression. The end user has the flexibility of changing the trade-off between robustness and image quality via the slider at the bottom of the plug-in window (*figure 4*). In addition, the method is blind and works with arbitrary host images.

Another digital watermarking service provider is Photopatrol [43] (*figure 5*), which uses a digital watermarking technology developed by Fraunhofer Institute SIT, Darmstadt [44]. Photopatrol provides two major online services - a service for signing digital images and a service for scanning images on predefined web portals for the presence of embedded signatures. The image signing service relies on a combination of modern browser technologies and Java applets. It is fairly complex to use and should not be recommended to inexperienced web users. The portal scanning service is similar to the Digimarc search service. It scans web portals for the presence of images belonging to Photopatrol customers. If such images are found, their location is reported back to the customer. The technology used by Photopatrol provides robustness against JPEG transformations. In addition, the method is blind and can work on arbitrary host images.

Figure 5. Photopatrol's browser interface

Another stand-alone program for digital watermarking is SignMyImage (currently version 3.06) [45]. The program has a nice user interface and can embed an identification string consisting of up to 10 characters. The author also offers a web portal scanning service similar to those provided by Digimarc and Photopatrol [46]. The digital watermarking method used in the program is robust to JPEG compression and decompression for low compression ratios. It is blind and can operate on arbitrary host images.

The conformity of the presented products and services to the requirements diiscussed in the previous section is shown in *table 2* (N.C. stands for Not Considered).

The differences between the steganographic and the digital watermarking solutions can be clearly seen. The steganographic solutions can work with arbitrary host images

Table 2. DCT-based data hiding products and services - evaluation

Product / Service	Extensibility	Robustness against JPEG transformations			Arbitrariness			
		Compression	Decompression	Recompression	Arbitrary host	Blind method	Arbitrary data	Error-free retrieval
Steganos Privacy Suite [38]	no	partial	no	N.C.	yes	yes	yes	yes
JPHide [39]	no	partial	no	N.C.	yes	yes	yes	yes
InvisibleSecrets [40]	no	yes	no	yes	yes	yes	yes	yes
Digimarc [41]	no	yes	yes	yes	yes	yes	no	yes
Photopatrol [43]	no	yes	yes	yes	yes	yes	no	yes
SignMyImage [45]	no	partial	partial	N.C.	yes	yes	no	yes

* N.C. = Not Considered

and data but they are not as robust against JPEG transformations as the reviewed digital watermarking solutions. The digital watermarking solutions, on the other hand, can embed only several small predefined data types - most often ID numbers. None of the existing solutions considers extensibility. The solutions are monolithic and cannot be adapted to user requirements, which require changes in the provided method features.

4. Modular Data Hiding

The concept of modular data hiding has been already partially presented in [47] and [48]. Its main idea is to separate complex monolithic methods into several modules (*figure 6*). In this way, the reuse and extensibility of already existing data hiding modules as part of new data hiding methods can be made possible.

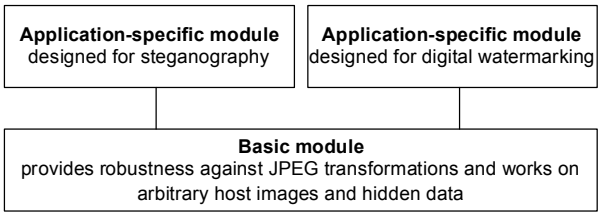

Figure 6. The modular data hiding approach

The basic module is responsible for features closely related to the host image format. In this case, we focus on JPEG and the basic module handles all JPEG transformations. The application-specific module is highly adaptable. It can be suited to different user requirements in the application areas of both steganography and digital watermarking.

This modular approach is specifically designed to answer the need for flexibility and adaptability of data hiding methods in modern web environments. Its advantages lie in the possibility of combining an arbitrary basic module with an arbitrary application-specific module. Thus, if a pool of basic and application-specific modules is created, their combinations will offer end-users a wide variety of data hiding methods with different features. In this way, every end-user (or an automated client application) may assemble, the most appropriate data hiding method.

Furthermore, the individual modules and the communication between them are designed in a manner, which enables the usage of arbitrary host images and data to embed. In the prototype implementation, another major focus is set on the full robustness of one of the basic modules against JPEG transformations. *Figure 7* shows a screenshot of the latest prototype version.

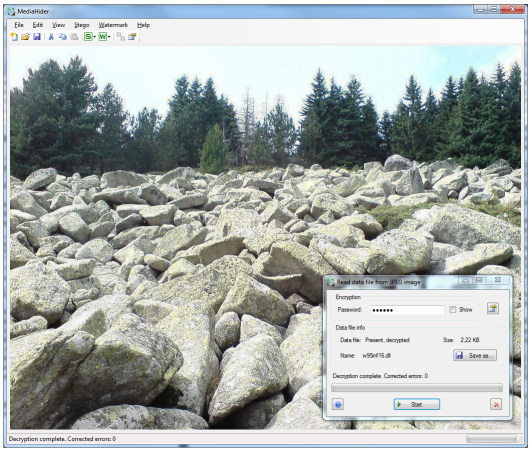

Figure 7. Modular data hiding prototype

The next step of enhancement of the prototype, which we are currently working on, is the implementation of a Software-as-a-Service (SaaS) approach, which can be automated and integrated into web-based applications (*figure 8* and *figure 9*).

In *figure 8*, a simple web form is shown, which controls the web-based server-side embedding of copyright information.

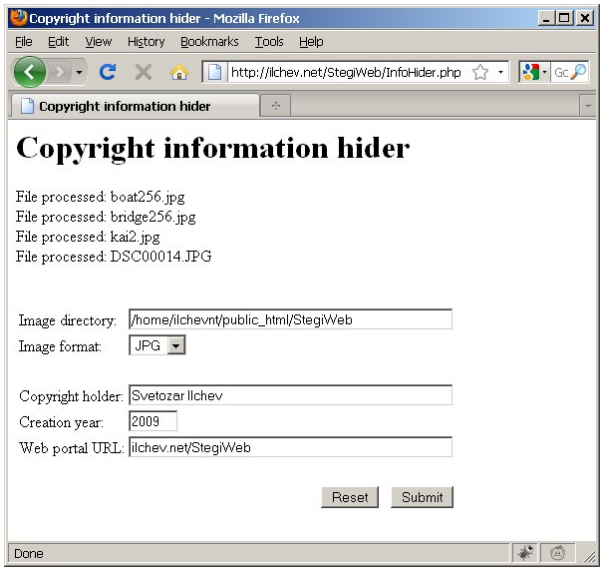

Figure 8. SaaS embedding of copyright data

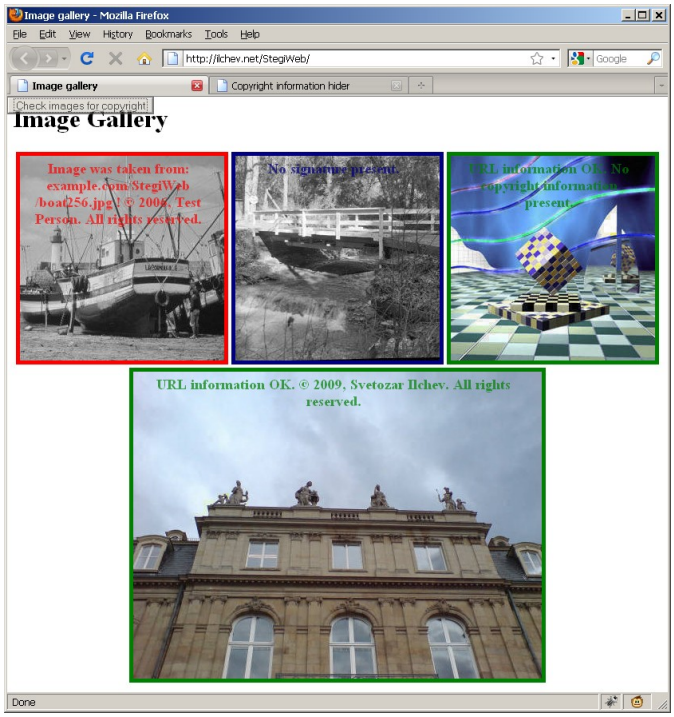

Figure 9. SaaS extraction of copyright data

In *figure 9*, the evaluation of the copyright status of images uploaded on web servers is graphically illustrated. Each image contains embedded information about the author and the URL locations the image may be published at. The copyright status is indicated by the color of the image border: red color indicates a copyright violation - the image has not been authorized for use on this particular web portal. Respectively, green and blue colors indicate an authorized location or absence of copyright information.

The prototype is written in VB.NET and C++ and the impelementation aims at providing maximum flexibility. It consists of a core library of data hiding modules, which can be used in conjunction with a couple of interfaces - a graphical interface (*figure 7*) and a web-service interface (employed in *figure 8* and *figure 9*). In this way, every client can choose the most appropriate way to access the data hiding functionality based on the concrete application requirements.

5. Conclusion

Classic data hiding solutions are created with a specific purpose in mind. They are optimized for solving one single problem and have a monolithic design. Both theoretical research and its practical realizations in form of products and services disregard some important aspects and requirements of the contemporary World Wide Web, which is in the center of today's communications and information distribution and exchange.

The modular data hiding is specifically oriented towards the needs of contemporary web applications. Its main benefits compared to traditional monolithic methods are the flexibility and adaptability to varying user requirements, and the capability of handling different host images and embeddable data. The basic module implemented as part of the prototype offers very good resistance to JPEG transformations - an essential requirement for the majority of web users. Further steps of research and development will consider the better integration of data hiding as a regulatory, preventive and informational mechanism for web applications and multimedia accessed in web-based communities such as social networks and image-sharing web portals.

References

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

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

3. Zeng, W., H. Yu, and C. Lin. Multimedia Security Technologies for Digital Rights Management. 1st ed.: Elsevier, 2006.

4. Peticolas, F., R. Anderson, and M. Kuhn. Information Hiding - A Survey. - *Proceedings of the IEEE*, Special Issue on Protection of Multimedia Content, 87, July 1999, No. 7, 1062 - 1078.

5. Anderson, R. J. and F. Petitcolas. On the Limits of Steganography. - *IEEE Journal on Selected Areas in Communications*, 16, 1998, No. 4, 474-481.

6. Hernandez-Chamorro, A., A. Espejel-Trujillo, J. Lopez-Hernandez, M. Nakano-Miyatake, and H. Perez-Meana. A Methodology of Steganalysis for Images. International Conference on Electrical, Communications, and Computers (CONIELECOMP), Cholula, Puebla, Mexico, 2009, 102-106.

7. Electronic Privacy Information Center. Cryptography Policy. [Online]. URL: http://www.epic.org/crypto/ (accessed January 9, 2012).

8. Voloshynovskiy, S., F. Deguillaume, O. Koval, and T. Pun. Information-theoretic Data-hiding: Recent Achievements and Open Problems. - *International Journal of Image and Graphics*, 5, 2005, No. 1, 1-31.

9. Lin, E. and E. Delp. A Review of Fragile Image Watermarks. Proceedings of the Multimedia and Security Workshop (ACM Multimedia '99), 1999, 25-29.

10. Pennebaker, W. B. and J. L. Mitchell. JPEG Still Image Data Compression Standard. 1st Ed., Van Rostrand Reinhold, New York, 1993.

11. Hamilton, E. (1992, September) JPEG File Interchange Format. [Online]. URL: http://www.w3.org/Graphics/JPEG/jfif3.pdf (Accessed January 9, 2012).

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

13. Kipper, G. Investigator's Guide to Steganography.1st Ed., Auerbach Publications, 2004.

14. Upham., D. JSteg. [Online]. URL: http://zooid.org/~paul/crypto/jsteg/ (accessed January 9, 2012).

15. Wu, M., Z. Zhu, and S. Jin. A New Steganalytic Algorithm for Detecting Jsteg. Lecture Notes in Computer Science, 3619, 2005, 1073-1082.

16. Provos, N. and P. Honeyman. Detecting Steganographic Content on the Internet. Internet Society Network and Distributed System Security Symposium (ISOC NDSS), San Diego, California, 2002.

17. Zhao, J. and E. Koch. Towards Robust and Hidden Image Copyright Labeling. IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Greece, 1995.

18. Zhao, J. and E. Koch. Embedding Robust Labels into Images for Copyright Protection. International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, Austria, 1995.

19. Cox, I. J., J. Kilian, T. Leighton, and T. Shamoon. Secure Spread Spectrum Watermarking for Multimedia. - *IEEE Transactions on Image Processing*, 6, 1997, No. 12, 1673-1687.

20. Wu, M. and B. Liu. Watermarking for Image Authentication. IEEE

International Conference on Image Processing, Chicago, Illinois, 1998, 2, 437-441.

21. Provos, N. Defending Against Statistical Steganalysis. 10th USENIX Security Symposium, 2001.

22. Provos, N. (2008, July) OutGuess - Universal Steganography. [Online]. URL: http://www.outguess.org/ (Accessed January 9, 2012).

23. Westfeld, A. F5-A Steganographic Algorithm. Proceedings of the 4th International Workshop on Information Hiding, Lecture Notes In Computer Science, 2137, 2001, 289-302.

24. Crandall, R. (1998) Some Notes on Steganography. Posted on Steganography. Posted on Steganography Mailing List. [Online]. URL: http://os.inf.tu-dresden.de/westfeld/crandall.pdf (accessed January 9, 2012).

25. Fridrich, J. Image Watermarking for Tamper Detection. IEEE International Conference on Image Processing (ICIP), Chicago, 1998.

26. Fridrich, J. Methods for Detecting Changes in Digital Images. Proceedings of The 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems (ISPACS), Melbourne, Australia, 1998, 173-177.

27. Fridrich, J. and M. Goljan. Images with Self-Correcting Capabilities. IEEE International Conference on Image Processing, Kobe, Japan, 1999.

28. Fridrich, J., M. Goljan, and R. Du. Invertible Authentication Watermark for JPEG Images," in International Symposium on Information Technology (ITCC), Las Vegas, Nevada, 2001, 223-227.

29. Fridrich, J., M. Goljan, and R. Du. Lossless Data Embedding - New Paradigm in Digital Watermarking. Special Issue on Emerging Applications of Multimedia Data Hiding, 2002, 185-196.

30. Fridrich, J., M. Goljan, Q. Chen, and V. Pathak.Lossless Data Embedding with File Size Preservation. Proceedings EI SPIE, San Jose, CA, 2004.

31. Costa, M. Writing on Dirty Paper. - *IEEE Transactions on Information Theory*, 29, 1983, No. 3, 439-441.

32. Wornell, Chen. Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding. - *IEEE Transactions on Information Theory*, 47, 2001, No. 4, 1423-1443.

33. Li, Q. and I. J. Cox. Using Perceptual Models to Improve Fidelity and Provide Resistance to Valumetric Scaling for Quantization Index Modulation Watermarking. - *IEEE Transactions on Information Forensics and Security*, 2, 2007, No. 2.

34. Watson, A. B. DCT Quantization Matrices Optimized for Individual Images. Human Vision, Visual Processing, and Digital Display IV, SPIE-1913, 1993, 202-216.

35. Sun, X., J. Liu, J. Sun, N. Yang, and S. Wu. An Improved Adaptive QIM Watermark Iterative Algorithm. Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP), Harbin, China, 2008, 748-751.

36. Izadinia, H., F. Sadeghi, and M. Rahmati. A New Steganographic Method Using Quantization Index Modulation. International Conference on Computer and Automation Engineering (ICCAE), 2009, 181-185.

37. Yu, Y.-H., C.-C. Chang, and Y.-C. Hub. Hiding Secret Data in Images Via Predictive Coding. - *Pattern Recognition*, 38, 2005, No. 5, 691-705.

38. Steganos GmbH. (2009, August) Steganos Privacy Suite: Overview. [Online]. URL: http://www.steganos.com/us/products/data-security/privacy-suite/overview/ (Accessed January 9, 2012).

39. Latham, A. (1999, August) Steganography. [Online]. URL: http://linux01.gwdg.de/~alatham/stego.html (Accessed January 9, 2012).

40. NeoByte Solutions. Invisible Secrets 4. [Online]. URL: http://www.invisiblesecrets.com/ (Accessed January 9, 2012).

41. Digimarc Corporation. Digimarc. [Online]. URL: http://www.digimarc.com/ (Accessed January 9, 2012).

42. Digimarc Corporation. Digimarc Search Service. [Online]. URL: https://www.digimarc.com/solutions/enterprise_tracking.asp (Accessed January 9, 2012).

43. CSG Copyright Services GmbH & Co. KG. Photopatrol.eu. [Online]. URL: http://www.photopatrol.eu/ (Accessed January 9, 2012).

44. Fraunhofer-Institut SIT. Fraunhofer-Institut SIT. [Online]. URL: http://www.sit.fraunhofer.de/(Accessed January 9, 2012).

45. Krolupper, F. http://www.adptools.com/. (accessed January 9, 2012).

46. Krolupper, F. Image Spider. [Online]. URL: http://www.adptools.com/signmyimage/eng/spider.html (Accessed January 9, 2012).

47. Ilchev, S., Zl. Ilcheva. Modular Data Hiding Approach For Web Based Applications. Proceedings of the International Conference „Automatics and Informatics'10", 3-7 October 2010, Sofia, Bulgaria, I-253-I-256.

48. Ilchev, S. Modular Digital Watermarking Method For Image Tampering Detection. Proceedings of the International Conference „Automatics and Informatics'11", 3-7 October 2011, Sofia, Bulgaria, B-221-B-224.

Manuscript received on 21.01.2012

Mr. Svetozar Ilchev *received a M.Sc. degree in Information Engineering and Management from the University of Karlsruhe in 2009 and a B.Sc. degree in Computer Science from the Technical University, Sofia in 2007. His research interests are in the fields of image processing and Internet security. He is a member of SAI.*

Mr. Ilchev is working as a research associate at the Institute for Information Management in Engineering, Karlsruhe Institute of Technology.

Contacts:
Karlsruhe Institute of Technology (KIT)
Institute for Information Management in Engineering (IMI)
Zirkel 2, Bld. 20.20 (RZ), Room 261
D-76131 Karlsruhe, Germany
e-mail: svetozar@ilchev.net

Doc. Dr. ***Zlatoliliya Ilcheva*** *received a M. Sc. Degree in Automatics and Telemechanics from the Technical University, Sofia (1975). She received her Ph.D. degree from the Bulgarian Academy of Sciences (1980). Her research interests are: Man-Machine Control Systems, Pattern Recognition, Image Processing, Image Compression, Multimedia Data Hiding. She is a member of SAI.*

Dr. Ilcheva is currently working as a docent at the Institute of Information and Communication Technologies, Bulgarian Academy of Sciences.

Contacts:
IICT-BAS
Ac. G. Bonchev Str., bl. 2
Sofia 1113, Bulgaria
e-mail: zlat@isdip.bas.bg