RESEARCH PAPER | Science | Volume : 5 | Issue : 3 | March 2015 | ISSN - 2249-555X

# MODULAR DATA HIDING METHODS FOR IMPROVED SECURITY AND INFORMATION EXCHANGE ON THE INTERNET

KEYWORDS: data hiding, digital watermarking, security, Internet

**Svetozar Ilchev**
IICT, Bulgarian Academy of Sciences, Acad. G. Bonchev Str., Bl

**Zlatoliliya Ilcheva**
IICT, Bulgarian Academy of Sciences, Acad. G. Bonchev Str., Bl

**ABSTRACT** *In this paper, we present the general concept of our modular data hiding methods together with a performance evaluation and comparison of the obtained experimental results to the results achieved by traditional monolithic methods. We begin with a short introduction into the general applications of data hiding and digital watermarking and explain their advantages with regard to the improvement of security in Internet-based communications. We explain the benefits of modularity in a rapidly changing communication environment, which is characteristic of today's Internet. Next, we briefly outline the structure of the modular methods using the example of our application-specific module for digital watermarking purposes. Then, we evaluate the overall efficiency achieved by the modular methods and present the obtained experimental results and numbers comparing them to both traditional research methods and commercial products.*

## INTRODUCTION

In light of recent discoveries regarding the security of digital communications and information exchange, the development of new approaches for information protection is a central topic for both researchers and IT professionals. In this paper, we focus on the presentation of some experimental results regarding the efficiency and the performance of the modular data hiding methods we have developed specifically for use with digital images in Internet-based applications [1,2].

In contrast to traditional monolithic data hiding methods [3,4,5,6,7], our modular data hiding methods consist of two types of modules – a basic module and an application-specific module. The basic module copes with peculiarities of the image format (jpeg, gif, png, etc.), ensures robustness against image changes and lossy image transformations (for jpeg images) and provides a generic storage medium for the application-specific module. The application-specific module provides high-level features such as image authentication, image integrity verification, ownership/copyright proof and others. These features are important when images are a central part of the information exchanged on the Internet – e.g. web newspapers and magazines, online marketing, product and website development, eCommerce, etc. The communicating parties can use the data hiding application-specific modules to guarantee that the images they work with:

1. Really originate from the communication partner,
2. Have not been tampered with during the exchange,
3. Are or are not subject to copyright restrictions imposed by the author. In the case of restrictions, the data hiding module shows contact details embedded by the author into the image (e.g. an e-mail or a website) for the purpose of arranging a new license for a particular use.
4. These applications pertain to the subject of digital watermarking and they discuss the improvement of several security aspects of the exchange of images between the communicating parties. Our digital watermarking application-specific module can also recover information about the image even if some parts of the image have been damaged or intentionally changed by third-parties.

We have also developed an application-specific module for steganographic purposes. In this case, the image does not benefit from any protection. The communicating parties use it as a host medium and transmit messages hidden embedded within its pixels, DCT coefficients, etc. This application-specific module utilizes AES encryption, compression, two types of pseudorandom number generators and error-correcting codes to enhance the security and undiscoverability of the embedded messages.

One major advantage of the modular data hiding methods over traditional approaches is the versatility and easy adaptability to new customer requirements, which is very important for today's Internet-based application scenarios. The basic and application-specific modules form a pool of building blocks which can be used in different combinations and extended. If a new graphics format (e.g. jpeg2000) has to be supported, then a new basic module must be created. By combining the new basic module with existing application-specific modules, we can use existing digital watermarking and steganographic functionality to secure images in the jpeg2000 format. For traditional data hiding methods, the incorporation of a new image format means the creation of a new method leading to potential incompatibilities with existing methods.

## FUNCTIONING OF DATA HIDING MODULES

The structure of the modular data hiding methods is discussed in detail in [8]. Here, we focus on the achieved results and present only a brief example of the functioning of a digital watermarking application-specific module. It illustrates the interaction between the modules during the encoding of a watermark into an image (Figure 1).

Volume : 5 | Issue : 3 | March 2015 | ISSN - 2249-555X

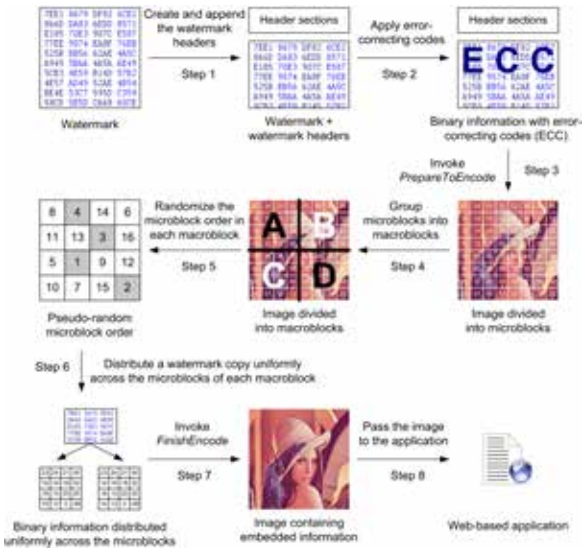


**Figure 1: Digital watermarking data encoding**

In step 1, the application-specific module assembles the binary data to be embedded into the image. It consists of the contents of a watermark file and headers which contain information about the watermark length and the use of error-correcting codes and compression. Step 2 – the application of error-correcting codes – is optional and often omitted due to watermark size constraints. In step 3, the application-specific module invokes a standardized method PrepareToEncode in the basic module, which subdivides the image into microblocks and calculates the amount of data which can be embedded into each block. In step 4, the microblocks are grouped into macroblocks. In step 5, pseudo-random number generators randomize the order of microblocks within each macroblock. In step 6, a watermark copy is embedded into each macroblock according to the randomization order of the microblocks. In step 7, the application-specific module invokes a standardized method FinishEncode in the basic module which performs the actual embedding of the distributed watermark copies into the image. In step 8, the image with the embedded watermark copies is passed back to the Internet-based application.

## EFFICIENCY AND PERFORMANCE RESULTS

The subdivision of our data hiding methods into two modules raises the question about the efficiency of the methods compared to traditional monolithic methods. Our experimental evaluations show that the results achieved by the modular methods are on par and in some cases better than the results obtained from other methods. The modular data hiding methods have been tested with a total of 1520 image/embedded data pairs. The image dimensions averaged 606x583 pixels and the embedded data ranged from 39 bytes to 1004 bytes in a nearly uniform distribution. The achieved average image quality for different JPEG quality ratios is shown in Table 1.

**TABLE – 1**
**MODULAR DATA HIDING METHODS**

| Modular method | JPEG quality ratio | Average Peak Signal-to-Noise Ratio PSNR [dB] |
|---|---|---|
| Steganographic method | 70 | 38,9 |
| | 80 | 40,0 |
| | 90 | 42,2 |
| Digital watermarking method | 70 | 38,3 |
| | 80 | 39,9 |
| | 90 | 42,4 |

The results from some traditional monolithic methods and products are summarized in Table 2. There is some degree of fluctuation in all results due to the different application areas targeted by different steganographic and digital watermarking methods. The embeddable data size often depends not only on the image dimensions but on the content of the particular image itself and on a variety of parameters chosen by the user of the method. The maximum embeddable data size usually ranges from several dozen bytes up to a few kilobytes. The experimental results show that the embeddable data size for the modular data hiding methods is about average in comparison to traditional methods and products.

**TABLE – 2**
**TRADITIONAL MONOLITHIC METHODS AND COMMERCIAL PRODUCTS**

| Method | Embeddable data size for 256x256 to 768x512 images [bytes] | Average PSNR [dB] |
|---|---|---|
| JSteg [9] | 2224 - 2642 | 29,71 - 41,60 |
| Zhao, Koch [10] | 380 | N.C. |
| O'Ruanaidh[11] | 55 - 512 | N.C. |
| Cox, et. al. [12] | 125 | N.C. |
| Wu, Liu [4] | 135 | N.C. |
| Lin, Chang [13] | N.C. | 32,95 – 40,70 |
| Provos [14] | 1462 | N.C. |
| Westfeld [15] | 192 - 1935 | N.C. |
| Chang [16] | 6656 | 27,63 – 39,14 |
| Fridrich [6] | 130 - 1124 | 35,32 – 53,12 |
| Li, Cox [5] | 1536 | 28,00 – 49,00 |
| Izadinia [7] | 8192 | 43,11 – 43,12 |
| Steganos Privacy Suite | N.C. | 52,70 |
| JPHide | N.C. | 56,40 |
| InvisibleSecrets | unlimited | N.C. |
| Digimarc | 3 - 4 | 35,10 |
| Photopatrol | N.C. | 33,00 |
| SignMyImage | 10 | 35,80 |
| Icemark | 20 | 32,60 |
| Eikonamark | 8 | 40,80 |
| * N.C. = Not Considered (no data) | | |

The image quality obtained by the modular data hiding methods is relatively constant with an average PSNR of about 40dB. This is similar to the PSNR achieved by the JPEG compression itself and it is better than the image quality achieved by many of the traditional methods and products.

The experimental results clearly show that the modular structure of the data hiding methods does not compromise their efficiency and performance. The achieved image quality is excellent for embedded data sizes similar to those achieved by traditional methods and products.

## CONCLUSION

With regard to Internet-based applications, the modular data hiding methods provide the opportunity of easily adapting data hiding methods to different customer requirements without sacrificing efficiency and performance. Existing basic and application-specific modules may be assembled statically or on-the-fly into complete data hiding methods for use in a specific Internet-based use case.

Volume : 5 | Issue : 3 | March 2015 | ISSN - 2249-555X

By having a relatively small pool of modules handling specific image formats and high-level user needs, the information exchange on the Internet can be made more secure without the expenses of creating new data hiding methods from scratch.

**REFERENCE** [1] Ilchev, S., and Ilcheva, Z. (2011), "Protection of Intellectual Property in Web Communities by Modular Digital Watermarking," in IEEE Signature Conference on Computers, Software and Applications (COMPSAC 2011), Munich, Germany, 2011, pp. 374-379, E-ISBN 978-0-7695-4459-5, DOI 10.1109/COMPSACW.2011.69. | [2] Ilchev, S., and Ilchev, V. (2012), "Modular data hiding for improved web-portal security," in 13th International Conference on Computer Systems and Technologies (CompSysTech '12), Ruse, Bulgaria, 2012, pp. 187-194, ISBN 978-1-4503-1193-9, DOI 10.1145/2383276.2383305. Best paper award. | [3] Cox, I., Miller, M., Bloom, J., Fridrich, J., and Kalker, T. (2008), "Digital Watermarking and Steganography", 2nd ed.: Morgan Kaufmann Publishers, 2008. | [4] Wu, M., Liu, B. (1998), "Watermarking for image authentication," in IEEE International Conference on Image Processing, vol. 2, Chicago, Illinois, 1998, pp. 437-441. | [5] Li, Q., and Cox, I. (2007), "Using Perceptual Models to Improve Fidelity and Provide Resistance to Valumetric Scaling for Quantization Index Modulation Watermarking," IEEE Transactions on Information Forensics and Security, vol. 2, no. 2, 2007. | [6] Fridrich, J., Goljan, M., and Du, R. (2002), "Lossless Data Embedding - New Paradigm in Digital Watermarking," in Special Issue on Emerging Applications of Multimedia Data Hiding, 2002, pp. 185-196. | [7] Izadinia, H., Sadeghi, F., and Rahmati, M. (2009), "A New Steganographic Method Using Quantization Index Modulation," in International Conference on Computer and Automation Engineering (ICCAE), 2009, pp. 181-185. | [8] Ilchev, S. (2013), "Accurate Data Embedding in JPEG Images for Image Authentication," in Comptes rendus de l'Acad´emie bulgare des Sciences, vol. 66, no. 9, pp. 1247-1254, Sep. 2013, ISSN 1310-1331. | [9] Upham, D., (2011), "JSteg", [Online], URL: http://zooid.org/~paul/crypto/jsteg/ (accessed March 18, 2011). | [10] Zhao, J. and Koch, E. (1995), "Towards Robust and Hidden Image Copyright Labeling," in IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Greece, 1995. | [11] O'Ruanaidh, J., Dowling, W., and Boland, F. (1996), "Watermarking digital images for copyright protection," Vision, Image and Signal Processing, IEEE Proceedings, vol. 143, no. 4, pp. 250-256, 1996. | [12] Cox, I., Kilian, J., Leighton, T., and Shamoon, T., (1997), "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997. | [13] Lin, C., and Chang, S. (2000), "Semi-fragile watermarking for authenticating JPEG visual content," in SPIE International Conference on Security and Watermarking of Multimedia Contents II, vol. 3971, San Jose, California, USA, 2000. | [14] Provos, N. (2008), "OutGuess - universal Steganography", [Online]. URL: http://www.outguess.org/ (accessed May 15, 2011). | [15] Westfeld, A. (2001), "F5—A Steganographic Algorithm," in Proceedings of the 4th International Workshop on Information Hiding, Lecture Notes In Computer Science, vol. 2137, 2001, pp. 289-302. | [16] Chang, C., Chen, T., and Chung, L. (2002), "A steganographic method based upon JPEG and quantization table modification," Information Sciences - Informatics and Computer Science, vol. 141, no. 1-2, pp. 123-138, 2002.