International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 6 (2015) pp. 14489-14496

http://www.ripublication.com

High Capacity Robust Image Steganography In The DCT Domain Using Spread Spectrum Technique

A Nagalinga Rajan[a], P Eswaran[b]
[a]Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, pincode: 627 012, India email: nagalingarajan@gmail.com
[b]Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamilnadu, pincode: 630003, India, email:eswaranperumal@gmail.com, telephone: 91 - 4565 - 227831, fax: 91 - 4565 - 225202

Abstract

Steganography is one of the emerging techniques for covert communication in the modern networked age. High capacity of embedding and the high prevalence of images in the internet make images as the medium of choice for steganography. For effective communication the hidden message must withstand a variety of image modifications that arise in the medium such as compression, noise addition, blurring etc. Hence this paper proposes a high capacity robust image steganography method using spread spectrum technique in the Discrete Cosine Transform domain. The middle frequency band of 22 coefficients in the discrete cosine transform of 8×8 image blocks is selected. Spread spectrum technique is used for the embedding. In order to improve capacity of embedding, messages are encoded in a higher base representation. The visual stealth, measured using the peak signal to noise ratio of the marked cover with respect to the cover image is improved by using adaptive strength for embedding. The extraction stage is simulated during the embedding to ensure that the strength of embedding is sufficient for successful retrieval after compression. This procedure allows the use of lower strengths where possible and thereby improves the visual stealth. Experimental results show that the method is robust to JPEG compression, noise addition and blurring. The error rate of reconstructing the message is shown to be more than 80% which is high enough for the technique to be useful in conjunction with error correcting methods. Thorough analysis is presented for the various cases. It is also shown that the method is reasonably effective against steganalysis by histogram analysis and subtractive pixel adjacency matrix.

Keywords : Information hiding, Steganography, Watermarking, Spread Spectrum, Steganalysis

Introduction

Steganography is a modern technique for covert communication where secret message bits are embedded inside another digital medium. In addition to hiding the message, steganography has the added advantage over cryptography in that the communication does not cause any suspicion [1]. Images are suitable as the medium due to several reasons. Image data has a lot of redundancies [2] which can be exploited to hide large amounts of data. Since images are present in the internet in vast numbers the communication is least likely to evoke suspicion in a passive observer. This allows communication between individuals and organizations without interference by a hostile censorship authority

The objectives of a good steganographic technique are listed as follows:-

1. The visual similarity between the cover and the embedded images must be high enough to be indistinguishable to a human observer.
2. The technique must evade detection by steganalysis.
3. The embedding capacity must be high enough relative to the number of pixels in the image. Usually there is a tradeoff between capacity and stealth.
4. The message must be preserved when the image is transmitted through a communication channel. A method that is robust to common image modifications is needed in this case [1]. Message integrity requirements could be relaxed if it can be recovered through redundancies built into the system such as error correcting codes [5]. Common image modifications include compression, noise addition, resizing etc. Robustness is measured using Message Integrity which is defined as the percentage of message bits correctly retrieved at the receiver side after passing through the image modifications.

The objectives mentioned above have been taken into consideration in developing the proposed method.

The next section presents a literature survey of common steganographic methods.

Review of Related Work

Several steganographic methods have been proposed in the last few decades. The simplest technique called Least Significant Bit (LSB) substitution replaces the least significant bits of the cover image with the secret message[6]. But it is not effective against steganalysis techniques such as the pair of values analysis by Westman & Pfitzmann in [7], RS-Steganalysis by Fridrich et al. in [8] and primary sets technique introduced by Dumitrescu et al. in [9]. The LSBs are very sensitive to simple transformations such as JPEG compression and noise addition [2].

Several transform domain techniques are also proposed where the message bits are hidden in the DCT coefficients. Some of the techniques that fall under this category are F5 [14], Outguess [15], and JSteg [16] etc which offer some robustness against JPEG compression. Many of the common steganographic methods have their implementation available online [17].

Several watermarking methods have been proposed which has robustness to image transformation as the main objective. In general robust watermarking methods fall under one of two categories. In 1997 Cox et al [18] introduced the spread spectrum

(SS) watermarking methods in which a pseudo-random noise-like watermark is added to the host feature sequence. In 2003 Malvar & Florencio have introduced the improved SS (ISS) method [18] which overcomes the host interference problem of the SS methods.

The second category of robust watermarking methods are quantization index modulation (QIM) introduced by Chen & Wornell, 2001 [20]. In QIM-based watermarking methods, a set of features extracted from the host signal are quantized so that each watermark bit is represented by a quantized feature value. QIM methods yield larger capacity than SS methods.

In 2004, Michael Buchanan proposed creating a robust form of steganography called STEM which is a DCT transform domain technique [21].

DCT domain offers potential robustness against JPEG compression. The lower frequencies cannot be changed without significantly altering the image visually. The higher frequencies are not robust enough. Therefore the middle frequencies are ideal candidates as cover features.

Proposed Method

The proposed method embeds the message digits into the *22* middle frequency coefficients using spread spectrum with adaptive weights. The embedding method is detailed below. The cover *I* is a grayscale image of size $m \times n$. The message *M* is converted as digits of a suitable base *B*. The chip sequences *S* are generated as mentioned in the previous section and it consists of *B* columns one for each of the message digit.

Secret Embedding Algorithm

1. Rescale the image pixel values to the range of *[15-240]*in order to avoid underflows and overflows.
2. Divide I into distinct blocks b_i of size 8×8.
3. Decompose each block using DCT and let $\boldsymbol{x}$ denote the middle 22 coefficients.
4. Visit the blocks according to a pseudo-random sequence parameterized by a secret key*K*.
5. Embed the secret message digit$m_i$in $\boldsymbol{x}$ as

$$y = x(1 + \alpha S_{m_i}) \quad \ldots \tag{5}$$

Here $S_{mi}$is the column of *S* corresponding to m_i. Here α is chosen as mentioned above in an adaptive fashion.

1. The DCT coefficients are replaced and inverse DCT is applied and the image block is replaced with the result.
2. Steps 4 and 5 are repeated for every message digit with the remaining image blocks.

Secret Extraction Algorithm

The image is divided into blocks of size 8×8. The image blocks are visited in the same pseudo-random sequence generated using *K* and DCT is applied to the blocks

and the middle frequency coefficient vector $\boldsymbol{x}$ is taken. The chip sequences S are reproduced using K. The Pearson Correlation is calculated for each of the columns of S and the most correlated column index is taken as the message digit.

Performance Analysis and Validation

The proposed method is implemented in MATLAB 7.9 using the image processing toolbox. In the following subsections the results of experiments are presented along with analysis. The experiments are conducted on a database comprising of 100 uncompressed grayscale test images.For the purpose of illustration, only six images listed in Table 1 are taken and the image modification parameters are listed in Table 2.

Table 1: Test Images

Image Name	**Size**
Cameraman.tif	256×256
Barbara.tif	256×256
Boats.tif	256×256
Lena.tif	256×256
Mandril.tif	256×256
Lake.tif	256×256

Table 2: Image Modifications Applied

Modification Type	Parameters
JPEG Compression	Quality 50%
Gaussian Noise	Mean = 0 Variance = 0.01
Impulse Noise	Density = 0.02

Visual Distortion

The visual integrity of the stego images are measured in Peak Signal to Noise Ratio (PSNR) which is defined as

$$PSNR(S,C) = 10\log_{10}\left(\frac{255^2}{\frac{\sum(S-C)^2}{N}}\right)\ldots \quad (6)$$

Here S and C are the pixel intensities of Stego and Cover images respectively. A higher value of PSNR usually above *30* indicates that the images are visually indistinguishable to a human observer.

The average PSNR values for the database images with varying $B$are displayed in Table 3. The values for the proposed method are compared against the method with a fixed $\boldsymbol{\alpha}$. It can be clearly seen that adaptive $\boldsymbol{\alpha}$ yields better performance.

Table 3: PSNR of Embedding with Fixed and Adaptive α

α	***B*** = 2	***B*** = 3	***B*** = 4	***B*** = 5
PSNR $\alpha = 4$	33.82	32.12	30.98	27.11
PSNR Adaptive $\alpha_{max} = 4$	42.72	40.78	38.25	35.60
Capacity (bpp)	0.0156	0.0248	0.0313	0.0363

The stego images are not subjected to any attack. The PSNR values are quite high and the message was extracted without significant error. The capacity of embedding is good enough for a robust steganographic method [25]. A direct comparison with spread spectrum based methods may not be appropriate because of the difference in objectives.

Message Integrity Under Jpeg Compression

The images are subjected to JPEG compression of varying quality and the message integrity is measured. The experiment was conducted for all the database images and the average message integrity is plotted against different qualities of compression in Figure 1 for the cases of *B* = 2, 3 and 4.

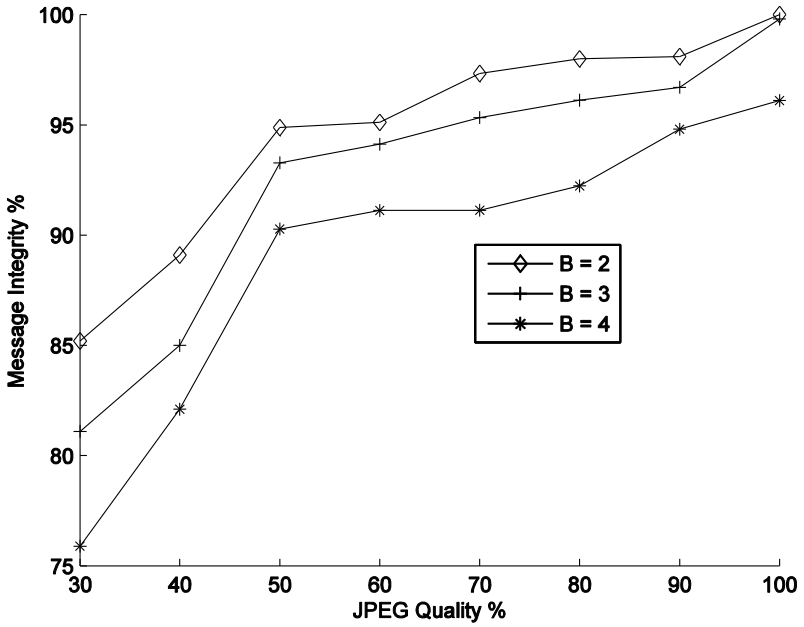

Figure 1: Performance of Message Integrity after JPEG compression

Figure 1 demonstrates that the method is robust to JPEG compression of quality above *40%* with accuracies more than *80%* for *B* = 2, 3 and 4.

Effectiveness Against Steganalysis By Spam

Subtractive Pixel Adjacency Matrix is a modern steganalysis method proposed by T Pevny et al. in [4]. The implementation is available online at [24]. It employs a soft margin support vector machine (SVM) classifier with Gaussian kernel to classify stego images from normal images using a feature set comprising of transition probabilities along eight directions. The total error rate is

$$P_{error} = \frac{1}{2}\left(P_{False\ Postives} + P_{False\ Negatives}\right) \quad \ldots \quad (9)$$

The error rate was calculated for first order SPAM with *T=4* and second order SPAM with *T=3*. The stego images were subjected to JPEG compression of 50% quality before detection. The average error rates were *0.37* and *0.31* respectively. This shows that the method cannot be detected reliably by SPAM technique.

Conclusion

This paper presents a robust steganographic technique which utilizes the middle frequency DCT coefficients to hide message digits. Using several chip sequences which are poorly correlated with each other, the method is able to hide message digits in a higher base. This improves the hiding capacity of this spread spectrum based approach. The proposed method also employs an adaptive scheme to use the smallest embedding strength thereby decreasing the visual distortion. An analysis of message preservation under JPEG compression, Gaussian and impulse noise is also presented. Results indicate that the message can be recovered with an accuracy of more than *80%* with more than 1 bit per block.The visual consistency of the stego images is also shown to be intact. The proposed method can be effectively used to communicate in a public network based scenario that undergoes compression and noise distortions.

The performance of the proposed method under significant amounts of noise suffers due to the sensitivity of the middle frequency coefficients to noise. This could possibly be rectified using ISS principles. Although the method improves the capacity of spread spectrum watermarking, the capacity is still lacking for a steganographic scenario. A possible solution is to use advanced selection strategy in choosing the chip sequences according to the image characteristics.

References

[1]. Ingemar. J. Cox et al, “Digital Watermarking and Steganography”, 2nd ed. Morgan Kaufmann series in computer security.

[2]. R. Chandramouli, M. Kharrazi, and N. Memon, Image steganography and steganalysis: Concepts and practice. In T. Kalker, Y. M. Ro, and I. Cox, editors, Digital Watermarking, 2nd International Workshop, IWDW 2003, Seoul, Korea, October 20–22, 2003, volume 2939 of LNCS, pages 35–49. Springer-Verlag, New York, 2004.

[3]. A. D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005.

[4]. T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixeladjacency matrix," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2,pp. 215–224, Jun. 2010.

[5]. W. Cary Huffman and Vera Pless, Fundamentals of error-correcting codes, Cambridge University Press 2003.

[6]. N. F. Johnson, S. Katzenbeisser, "A Survey of steganographic techniques", in S. Katzenbeisser and F. Petitcolas (Eds.): Information Hiding, pp. 43-78. Artech House, Norwood, MA, 2000.

[7]. A. Westfeld and A. Pfitzmann. Attacks on steganographic systems. In A. Pfitzmann, editor, Information Hiding, 3rd International Workshop, IH'99, Dresden, Germany, September 29–October 1, 1999, volume 1768 of LNCS, pages 61–75. Springer-Verlag,New York, 2000.

[8]. Reliable Detection of LSB Steganography in Grayscale and Color Images, with M. Goljan and R. Du, Proc. of the ACM Workshop on Multimedia and Security, Ottawa, Canada, October 5, 2001, pp. 27-30.

[9]. S. Dumitrescu, X. Wu, and N. Memon. On steganalysis of random LSB embedding in continuous-tone images. In Proceedings ICIP, Rochester, NY, September 22–25, 2002, pages 324–339, 2002.

[10]. T. Sharp, "An implementation of key-based digital signal steganography," in Proc. Information Hiding Workshop, Springer LNCS 2137, pp. 13–26, 2001.

[11]. J. Harmsen and W. Pearlman, "Steganalysis of additive-noise modelable information hiding," in Proc. SPIE Security Watermarking Multimedia Contents, vol. 5020, 2003, pp. 131–142.

[12]. Mielikainen,J, "LSB Matching Revisited", IEEE Signal Processing Letters, vol 13, Issue 5pg285-287, May 2006.

[13]. Shunquan Tan, "Steganalysis of LSB matching revisited for consecutive pixels using b-spline functions", IWDW'11 Proceedings of the 10th international conference on Digital forensics and Watermarking, Pages 16-29, Springer-Verlag Berlin, Heidelberg @ 2012

[14]. Andreas Westfeld: The Steganographic Algorithm F5, 1999. http://wwwrn.inf.tu-dresden.de/˜westfeld/f5.html

[15]. OutGuess. Steganography Detection with Stegdetect [Online]. (December 29, 2003). Available: http://www.outguess.org/detection.php.

[16]. JPEG-Jsteg-V4, http://www.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz

[17]. Available Online : [Hide and Seek]: ftp://ftp.funet.fi/pub/crypt/ mirrors/idea.sec.dsi.unimi.it/cypherpunks/steganography/hdsk41b.zip [S-Tools]: ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip [Stella] : http://wwwicg.informatik.uni-rostock.de/~sanction/ stella/ [Hide in Picture]: http://sourceforge.net/projects/hide-in-picture/ [Revelation]: http://revelation.atspace.biz/ [Camouflage]: http:// camouflage.unfiction.com/ [JpegX]: http://www.freewarefiles.com/

Jpegx_program_19392.html [Data Stash]: http://www.skyjuicesoftware.com/software/ds_info.html [Other Tools]: http://www.jjtc.com/Security/stegtools.htm [F5]: http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html [OutGuess]: http://www.outguess.org/

[18]. Cox, I., Kilian, J., Leighton, F. & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia, IEEE Trans. on Image Proces. 6(12): 1673 –1687.

[19]. Malvar, H. & Florencio, D. (2003). Improved spread spectrum: a new modulation technique for robust watermarking, IEEE Transactions on Signal Processing 51(4): 898 – 905.

[20]. B. Chen and G.W.Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," IEEE Trans. Info. Theory, vol. 47, no. 4, pp. 1423–1443, May 2001.

[21]. Joshua Michael Buchanan, Creating a Robust form of Steganography, Thesis submitted to Wake Forest University , May 2004.

[22]. Ahmed, N. (January 1991). "How I came up with the discrete cosine transform". *Digital Signal Processing***1** (1): 4–9. doi:10.1016/1051-2004(91)90086-Z.

[23]. J. R. Hemandez, M. Amado, "DCT domain watermarking techniques for still images as detector performance analysis and a new structure," in IEEE Transactions on Image Processing, 2000, vol. 9, pp. 55-68.

[24]. Available Online: http://dde.binghamton.edu/download/spam/