International Journal of Computing and Business Research
(IJCBR)
ISSN (Online) : 2229-6166

Volume 3 Issue 3 September 2012

High Capacity Data Embedding System in DCT domain for Colored Images

Navdeep Kaur, Sukhjeet K. Ranade

Abstract— **In this paper, we propose a high capacity data-embedding system in DCT domain for colored images and review the existing high capacity data embedding systems both in spatial domain as well as transform domain. The embedding is done on the quantized DCT coefficients using the concept of Hadamard Matrix. The system has very high capacity as comparable to the existing techniques of DCT domain. The system is highly robust and secure.**

Key Words— **data embedding, high-capacity data hiding, information hiding, hiding capacity, DCT transformation.**

I. INTRODUCTION

Nowadays, daily communications of all kinds over the Internet have become incredibly popular and convenient. However, message transmissions over the Internet still have to face all kinds of security problems. To the best of our knowledge, all the most popular forms of security protection heavily rely on encryption, which refers to the process of encoding secret information in such a way that only the person with the right key can successfully decode it. However, encryption leaves obviously noticeable marks on the message, making it suspicious enough to attract eavesdroppers' attention. A practical way to solve this problem is to hide the secret information behind some kind of a cover such as a digital image or sound clip so that it draws no special attention. Image, audio, video, and many other kinds of data are nowadays mostly passed from person to person or from place to place in digital form. The data hiding is the process of hiding the very existence of the data into some cover medium so that the malicious user cannot tamper with it. The embedding of data in digital contents is done for authentication, copyright control, or for secret data hiding. Data-embedding techniques designed to take care of such tasks are commonly classified as watermarking or steganographic techniques in accordance with their functionalities. We know that, with the use of steganographic techniques, it is possible to hide information within digital audio, images and video files which is perceptually and statistically undetectable. The method of embedding secret message (which can be plain text, cipher text, or even images) is usually based on replacing bits of useless or unused data in the source cover (can be audio files, sound, text, Disk space, hidden partition, network packets, digital images, software, or circuitry).

There are two common methods of embedding: Spatial embedding in which messages are inserted into the LSBs of image pixels, and Transform embedding in which a message is embedded by modifying frequency coefficients of the cover image (result is called the stego-image).Transform embedding methods are found to be in general more robust than the Spatial embedding methods which are susceptible to image-processing type of attacks. However with respect to steganography the perceptibility (i.e., whether the source cover is distorted by embedding information to a visually unacceptable level) is a critical property. There is another important issue of steganography, namely, capacity, i.e., how much information can be embedded relative to its perceptibility. We will use digital images as the cover object in this paper in which we embed the hidden information. The challenge of using this data embedding method in cover images is to hide as much data as possible with the least noticeable difference in the output-image and to obtain high robustness.

In this paper we propose a data embedding system in DCT domain that uses the Hadamard matrix as base vectors for data embedding.

The rest of the paper is organized as follows: Section (II) describes the existing high capacity data embedding techniques both in spatial domain as well as DCT domain. In section (III) Hadamard Matrices are described, in section (IV) we describe our proposed system. Section (V) shows Experimental results. The conclusion is given in section (VI).

II. EXISTING HIGH CAPACITY DATA EMBEDDING TECHNIQUES

Many data embedding methods for hiding data in still images have been proposed [1]-[3]. In order to maintain the secrecy of important data in an image, only a small amount of data can be encoded therein (called the data payload). To obtain higher payloads, image-hiding methods based on least-significant-bit (LSB) substitution have been proposed [6]–[8]. These methods typically utilize some mapping rules to embed the important image in certain LSB planes of the cover image and apply additional pixel-adjustment procedures to reduce the errors

introduced in the embedding process. Meanwhile, some studies [5], [9] have considered the characteristics of the human vision system when evaluating the number of bits that can be hidden in an image. Given that human eyes are most sensitive to edges, these methods usually hide more data in areas with higher spatial variations. The data payload and the imperceptibility are the two most important properties of a steganography system. Intrinsically, these requirements contradict each other, since a high data payload introduces more artifacts into the cover image and hence, increases the perceptibility of the hidden data. So, there is always a trade-off between the capacity and the visual imperceptibility of the data embedding system. Previous attempts [3], [5], [9] to maintain both the imperceptibility and a high data payload have worked from the imperceptibility metric: estimating the degree of alterations that are imperceptible to viewers and then embedding data within this constraint. In military and commercial applications, a large amount of communication by a site tends to expose its position and value. Moreover, due to physical constraints and security concerns, the bandwidth of a communication channel where stego-images are used tends to be low.

In order to improve the capacity of the hidden secret data and to provide an imperceptible stego-image quality, a steganographic method based on least-significant-bit (LSB) replacement and pixel-value differencing (PVD) method [10] is presented. As compared with the PVD method being used alone, the method can hide much larger information and maintains a good visual quality of stego-image. Meanwhile a method based on Discrete Cosine Transform (DCT), Vector Quantization (VQ), and a Pseudo Random Number Generator (PRNG) have been developed that can embed more information than traditional algorithms without compression and provides good imperceptibility and robustness in terms of both JPEG compression and other signal processing attacks.

Another steganography method is that utilizes a two-way block-matching [12] procedure to search for the highest similarity block for each block of the important image. The bases and indexes obtained together with some not-well-matched blocks are recorded in the least significant bits of the cover image using a hop scheme. The method exhibits a high data payload, which reduces the storage and transmission-time requirements and also provides a method that prevents an observer from selectively blocking the transmission of the important image.

There are many scholars pay attention to increase hiding capacity of information hiding algorithm based on DCT transformation in order to spread its application to wider territory. The fast and efficient high-capacity embedding algorithm [13] in DCT domain is developed which is based on Quantized Projection embedding method. It provides good trade-off between robustness, data capacity, and visual quality and achieves very high hiding ratio and a low Bit error rate (BER) under JPEG compression.

Because human vision system is much more sensitive to signal in low frequency than in high frequency, hiding information in low frequency of DCT has better robustness while hiding in median and high frequency has better imperceptibility. In standard quantization matrix commended by JPEG, high frequency has bigger quantization value, thus information embedded in high frequency will be easily filtered by JPEG compression. Then according to that, an information hiding algorithm [16] that can embed information in DCT median and high frequency coefficients is developed which provides strong robustness against lossy compression.

Four-pixel differencing method is implemented as given in [17] and it is based on LSB substitution method. Another method to increase the hiding capacity is using mod-4 embedding method [18] which is based on the image contrast.

III. HADAMARD MATRICES

A Hadamard matrix H of order n is an $n \times n$ matrix of 1s and -1s in which $HH^T = nI$. (I is the $n \times n$ identity matrix.)
Equivalently, a Hadamard matrix is an $n \times n$ matrix of 1s and -1sin which any two distinct rows agree in exactly $n/2$ positions(and thus disagree in exactly $n/2$ positions.

A Hadamard matrix can exist only if n is 1, 2, or a multiple of 4.If H is a Hadamard matrix of order n, then

$$\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

is a Hadamard matrix of order 2n.

Examples of Hadamard Matrices:

$$H2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Similarly, the other Hadamard matrices of higher order can be generated using the lower order Hadamard matrices.

IV. THE PROPOSED SYSTEM

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166

Volume 3 Issue 3 September 2012

The procedure of our embedding scheme is described as follows:

1) First of all, convert the colored image to single layer.
2) Then masking over Hadamard matrix is done.
3) Divide the host image into 8x8 blocks.
4) Calculate the DCT coefficients of 8x8 blocks of the host image.
5) Then quantization of DCT coefficients is done.
6) See the data masked where positive 1, put there any random coefficient generated.
7) If there is no 1 in data masked, then put dct coefficient of specific pixel at that point.
8) Now, take inverse dct and de-quantization
9) Then recombining the layers we get the final embedded image.

The extraction process can be done in similar way. For more security the data to be embedded can be encrypted using some encryption mechanism such as RSA or DES. This encrypted data can be decrypted using the decryption mechanism to obtain the original plain data.

V. Experimental Results

The Peak Signal to Noise Ratios (PSNR) is used to measure the distortion of watermarked image.

$$PSNR = 10 \log_{10} \frac{255^2}{\frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{i,j} - x'_{i,j})^2}$$

where $x_{i,j}$ and $x'_{i,j}$ denote the pixels of the original and reproduced images, and the images are the size MxN.

The Bit Error Rate(BER) is calculated as:

$$BER = \frac{1}{PSNR}$$

Lena image is used in testing this algorithm. The host image as shown in Fig. 1(a) size is 512x512. The images obtained after embedding are shown in the figures below. The system can embed 4095 bits into the host image of size 512x512 without losing visual imperceptibility.

Fig. 1(b) through Fig. 1(e) show the resultant images obtained after embedding the data at different rates i.e. 1024 bits, 2048 bits, 3072 bits and 4095 bits respectively.

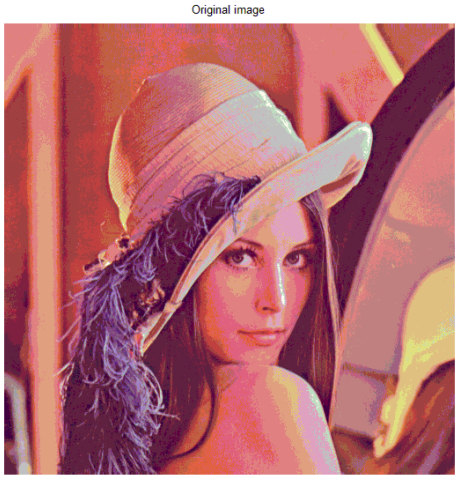

Fig. 1(a) Original Lena Image

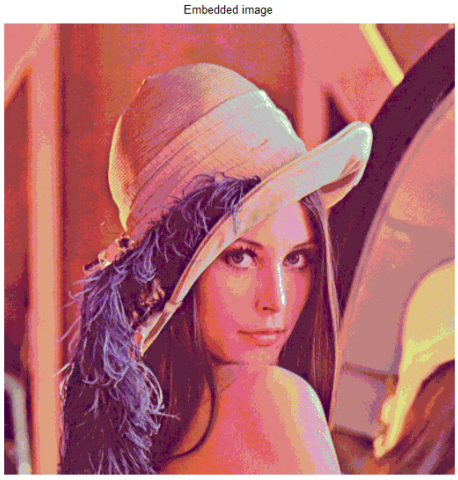

Fig. 1(b) Lena with embedded data 1024 bits

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166

Volume 3 Issue 3 September 2012

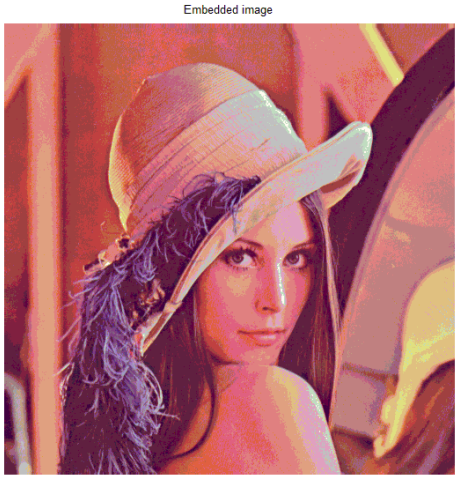

Fig. 1(c) Lena with embedded data 2048 bits

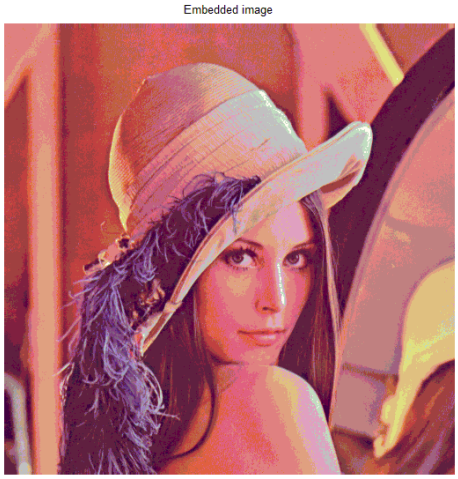

Fig. 1(e) Lena with embedded data 4095 bits

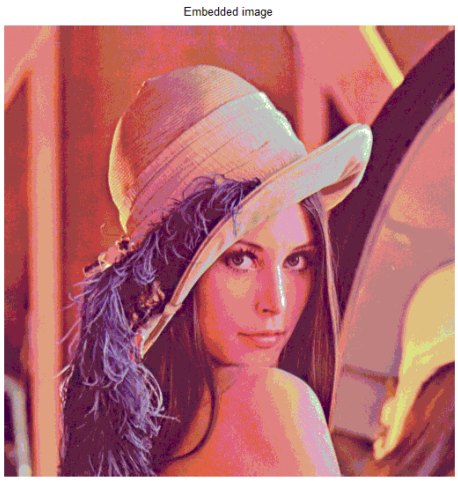

Fig. 1(d) Lena with embedded data 3072 bits

Table I
PERFORMANCE ANALYSIS OF THE EMBEDDED LENA IMAGE WITH VARIOUS CAPACITIES

Data size	BER	MSE	PSNR
1024 bits	0.0212	1.2299	47.2319
2048 bits	0.0208	0.9953	48.1512
3072 bits	0.0203	0.7593	49.3267
4095 bits	0.0197	0.5304	50.8849

The rotation attack is also analyzed in this work. The following table shows the results obtained after rotating the image Fig. 1(e) at different angles.

Table II
PERFORMANCE ANALYSIS OF THE EMBEDDED LENA IMAGE AFTER ROTATION AT DIFFERENT ANGLES.

Rotation Angle	BER	MSE	PSNR
90 degrees	0.0310	38.7408	32.2491
180 degrees	0.0308	36.8107	32.4711
270 degrees	0.0307	35.6845	32.6060

VI. Conclusion

The techniques for embedding data in spatial domain have larger capacity as compared to that of techniques for data embedding in DCT domain. Our system embeds a large amount of data in DCT domain using Hadamard matrix in colored images with minimal distortion. The system achieves hiding ratio of 1/64. The system is highly

robust and secure. The system has low BER and high visual imperceptibility.

ACKNOWLEDGMENT

I would like to thank Mrs. Sukhjeet K. Ranade for her continued support, guidance, inspiration and constant feedback for this study. I am also thankful to the Head of the Department Dr. Jyotsna Sengupta for providing me the opportunity and environment to work on this project.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Liu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, pp. 313–336, 1996.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—a survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[3] L. M. Marvel, C. G. Boncenet, Jr., and C. T. Retter, "Spread spectrum image steganography," *IEEE Trans. Image Procesing,*, vol. 8, no. 8, pp. 1075–1083, Aug. 1999.

[4] M. Alghoniemy and A. Tewfik, "Progressive quantized projection watermarking scheme," *Proc. ACM Multimedia Conf.,* 1999.

[5] Y. K. Lee and L. H. Cheng, "High capacity image steganographic model," *Proc. Inst. Elect. Eng., Vis., Image, Signal Processing*, vol. 147, no. 3, pp. 288–294, Jun. 2000.

[6] R. Z.Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol. 34, pp. 671–683,2001.

[7] C. C. Thien and J. C. Lin, "Asimple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function," *Pattern Recognition*, vol. 36, pp. 2875–2881, 2003.

[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recogniti*on, vol. 37, pp. 469–474, 2004.

[9] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity," *IEEE Signal Procesing Lett*ers, vol. 12, no. 1, pp. 67–70, Jan. 2005.

[10] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEE Proc.Vis. Image Signal Processing,* Vol. 152, No. 5, pp. 611-615, Oct. 2005.

[11] Y. Y. Chung, "A study of High Capacity Image Steganographic System," *Proc. Tencon 2005 IEEE Region 10*, pp. 1-5, Nov. 2005.

[12] R.-Z. Wang and Y.-S. Chen, "High-Payload Image Steganography Using Two-Way Block Matching," *IEEE Signal Processing Letters*, VOL. 13, NO. 3, pp. 161-164, Mar. 2006.

[13] T.-H. Lan and A. H. Tewfik, "A Novel High-Capacity Data Embedding System," *IEEE Transactions on Image Processing*, Vol. 15, No. 8, pp. 2431-2440, Aug. 2006.

[14] K. B. Raja, Vikas, K. R. Venugopal, and L. M. Patnaik, "High Capacity Lossless Secure Image Steganography using Wavelets," *Proc. Advanced Computing and Communications, ADCOM-2006*, pp. 230-235, Dec. 2006.

[15] X. Jianquan, Y. Chunhua, H. Dazu, "High Capacity Information Hiding Algorithm for DCT Domain of Image," *Proc. Intelligent Hiding and Multimedia Signal Processing, IIHMSP-2008*, Aug. 2008, pp. 269-272

[16] X. Jianquan, X. Qing, H. Dazu, "A Robust High Capacity Information Hiding Algorithm Based on DCT High Frequency Domain," *Proc. Computer Network and Multimedia Technology, CNMT-2009*, pp. 1-4, Jan. 2009.

[17] M.B. O. Medeni, E.M. Souidi, "A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution," Proc. IEEE, 2010.

[18] K. Pramitha, L.P.Suresh, K.L. Shunmuganathan, "Image Steganography Using Mod-4 Embedding Algorithm Based On Image Contrast," *Proc. International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011)*, pp. 364-369, 2011.