AN ADAPTIVE DCT-BASED MOD-4 STEGANOGRAPHIC METHOD

Xiaojun Qi and KokSheik Wong

Computer Science Department, Utah State University
Logan, UT 84322-4205
xqi@cc.usu.edu and kswong@cc.usu.edu

ABSTRACT

This paper presents a novel Mod-4 steganographic method in discrete cosine transform (DCT) domain. A group of 2×2 quantized DCT coefficients (GQC) is selected as the valid embedding area if more than two DCT coefficients are outside the interval of $[-1, 1]$. The modulo 4 arithmetic operation is further applied to all the valid GQCs to embed a pair of binary bits using the shortest-route modification scheme. Each secret message is also encrypted to provide the system with more security. The proposed system has been extensively tested on a variety of images with different textures. Experimental results demonstrate that our system successfully preserves the quality of the images and stays undetected by the well-known steganalysis methods.

1. INTRODUCTION

Steganography is a data hiding technique that has been widely used in information security applications. It is similar to watermarking and cryptography techniques. However, these three techniques are different in some aspects. 1) Watermarking mainly prevents illegal copy or claims the ownership of digital media. It is not geared for communication. 2) Cryptography scrambles the data to be communicated so that unintended receivers cannot perceive the information. However, the fact that the communication has been carried out is known to everyone. 3) Steganography transmits data by embedding messages into innocuous-looking cover objects, such as digital images. As a result, the presence of communication is hidden.

Machado [1] develops EzStego to embed information into an image in the GIF format. This method sorts the palette to ensure the difference between two adjacent colors is visually indistinguishable. Tseng and Pan [2] present a data hiding scheme in 2-color images. This approach embeds the information in any bit where at least one of the adjacent bits is the same as the original unchanged bit. Kawaguchi and Eason [3] propose a bit plane complexity segmentation (BPCS) method to embed information into the noisy areas of the image. This embedding process is not limited to the least significant bit (LSB) and therefore provides high carrier capacity. Provos [4] develops OutGuess to embed information into the quantized DCT coefficients. The embedding is followed by a correction to ensure that the distributions of any related pair of the quantized DCT coefficients are unchanged. Consequently, Outguess is robust against histogram analysis. Chu et al. [5] apply the quantization step in the JPEG compression scheme to embed information. Each embedded information bit is matched with the quantized value of the LSB of the differences between DCT coefficients from adjacent blocks.

However, several steganalysis tools have been developed to detect the presence of secret messages embedded in images using the above steganographic methods. Specifically, Westfeld and Pfitzmann [6] use the color arrangement in the palette for stego detection in EzStego. Kim et al. [7] apply complex blocks to measure the replacement of LSB-planes in BPCS for stego detection. Fridrich et al. [8] create a macroscopic measure to determine the length of the embedded message based on the increment of the blockiness.

In this paper, we propose a novel steganographic method Mod-4 for DCT-based images. It applies the modulo 4 arithmetic to the valid GQC so that its result matches with the pair of bits to be embedded. The experimental results show that the proposed system preserves the quality of the image and resists some of the well-known statistical attacks. The remainder of the paper is organized as follows. Section 2 presents the Mod-4 steganographic method. Section 3 shows the statistical analysis of the cover and stego images. Section 4 demonstrates the experimental results. Conclusions are given in section 5.

2. MOD-4 METHOD

The block diagram of the proposed system is shown in Fig. 1. A secret message is first encrypted by any cryptographic technique (e.g., 128-bit public key RSA) to ensure more security. This resulting message is further converted to binary bit stream for embedding. Two important components, namely valid GQC selection and Mod-4 embedding, are detailed in the following sub-sections.

0-7803-9134-9/05/$20.00

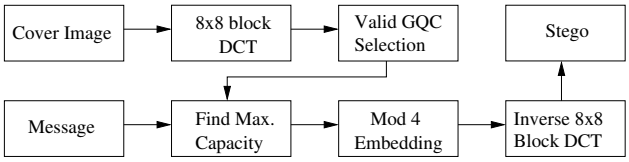


Fig. 1. Block diagram for Mod-4

2.1. Valid GQC - Definition and Order of Selection

GQC is defined to be a group of 2×2 non-overlapping spatially adjacent quantized DCT coefficients. A GQC is called *valid* if $|\{x|x \in \text{GQC}, |x| > 1\}| \geq 2$. By definition, a valid GQC (vGQC) is associated with part of a noisy area in the image. Therefore, when the image resolution is fixed, the number of vGQC's depends on the texture of the image. A noisy image (e.g., baboon) will have more vGQC's while a relatively smooth image (e.g., airplane) will yield a lower number of vGQC's.

The vGQC's are used as the secret message carriers. All vGQC's are extracted from the image and stored in a buffer, β, according to the order determined by a pseudo random number generator (PRNG), which in turn depends on a state (i.e., password). Furthermore, the maximum capacity, MC, of the cover image is computed to be twice the number of vGQC's.

2.2. Mod-4 Embedding Algorithm

The embedding phase is carried out right after the quantization of DCT coefficients by a specific quantization table. Let μ be the encrypted message coded in some binary representation. For simplicity, we employ the usual binary representation (i.e., 11_2 represents 3_{10}). Also, given a vGQC $\mathcal{Q}$, define $\sigma_{\mathcal{Q}}$ and $\S(\cdot, 4)$ to be:

$$\sigma_{\mathcal{Q}} := \sum_{x \in \mathcal{Q}} x, \quad \text{and} \quad \S(\sigma_{\mathcal{Q}}, 4) := (\sigma_{\mathcal{Q}} \mod 4)_2$$

The subscript 2 in the definition of $\S(\sigma_{\mathcal{Q}}, 4)$ indicates to convert the resulting value into the binary representation. It is obvious that the range of $\S(\sigma_{\mathcal{Q}}, 4)$ is $\{00, 01, 10, 11\}$. With the notations introduced, the general embedding procedure is as follows:

1. If $|\mu| > MC$, the embedding process halts. Otherwise, random bits of length $MC - |\mu|$ are padded to the secret message.
2. To embed the first pair of binary message bits xy_1, the first vGQC from β, $\mathcal{Q}_1$, is modified. The coefficients of $\mathcal{Q}_1$ are modified so that $\S(\sigma_{\mathcal{Q}_1'}, 4) = xy_1$.
3. For $i \leq MC$, the embedding process continues by modifying the quantized DCT coefficients of $\mathcal{Q}_i$ so that $\S(\sigma_{\mathcal{Q}_i'}, 4) = xy_i$, where $\mathcal{Q}_i$ is the i^{th} vGQC from β, and xy_i is the i^{th} pair of message bits.
4. When $i > MC$, the process stops. The modified vGQC's are re-injected into the locations where they were originally extracted. The rest of the standard JPEG compression scheme is carried out, i.e., zigzag scan, entropy coding and etc.

The most important part of Mod-4 embedding algorithm is in the modification of quantized DCT coefficients. The following rules are enforced during modifications of the quantized DCT coefficients in a vGQC:

- Coefficient with magnitude less than 2 is ignored.
- Magnitude of a coefficient is always increased, i.e., addition to positive coefficient, and subtraction from negative coefficient.
- Coefficients with larger magnitudes are modified first.
- The *shortest-route* scheme is used to ensure the minimum number of modifications per DCT coefficient.

The shortest-route scheme is demonstrated in Table 1 where the pair of message bits to be embedded is $xy = 00$. The extensions to $01, 10$, and 11 could be easily derived.

Table 1. Modification Scheme - Shortest Route

$\S(\sigma, 4)$	$\oplus$	$\ominus$	Route	Shortest
0	0	0	No Change	N/A
1	3	1	-1 or +3	-1
2	2	2	$+2$ or -2	*
3	1	3	-3 or +1	+1

Let $\mathcal{Q}$ be the vGQC under consideration. In Table 1, the $\oplus$ column denotes the value to be added to the positive coefficients in $\mathcal{Q}$ to obtain $\S(\sigma_{\mathcal{Q}'}, 4) = 00$. The $\ominus$ column is defined similarly. The last column indicates the shortest-route, which uses the least number of modifications to get $\S(\sigma_{\mathcal{Q}'}, 4) = 00$. We further define $p := \{x|x \in \mathcal{Q}, x > 1\}$ and $n := \{x|x \in \mathcal{Q}, x < -1\}$. The positive coefficients in $\mathcal{Q}$ are sorted in a decreasing order and labeled by p_1, p_2, p_3, and p_4 if $|p| = 4$. On the contrary, the negative coefficients are sorted in an ascending order and labeled by n_1, n_2, n_3, and n_4 if $|n| = 4$. Based on the values listed in the $\oplus$ and $\ominus$ columns, the shortest-route is chosen as follow:

1. If $\oplus = \ominus = 0$, no changes are made. Done!
2. If $\oplus > \ominus$, subtracting 1 from n_1 is the shortest subtraction route. However, if $|n| = 0$ (i.e., there are no items in the set n), unity has to be added to each of p_1, p_2, and p_3. If p_3 does not exists (i.e., $|p| = 2$), we will add 2 to p_1.
3. If $\oplus < \ominus$, adding 1 to p_1 is the shortest addition route. Similarly, when $|p| = 0$ (i.e., there are no items in the set p), unity has to be subtracted from each of n_1, n_2, and n_3. Again, we might run into the case $n_1' = n_1 - 2$ if $|n| = 2$.
4. If $\oplus = \ominus = 2$, there are 4 cases to consider:
   - $(|p| > |n|)$: Unity is added to each of p_1 and p_2.

- $(|p| = |n| = 1)$: If $|p_1| > |n_1|$, then $p_1' = p_1 + 2$, otherwise, $n_1' = n_1 - 2$.
- $(|p| = |n| = 2)$: If $|p_1| > |n_1|$, then unity is added to each of p_1 and p_2, otherwise, unity is subtracted from each of n_1 and n_2.
- $(|p| < |n|)$: Unity is subtracted from each of n_1 and n_2.

Note that coefficients with values $-1, 0$, and 1 stay unchanged. Also, a vGQC always satisfies the condition of $2 \leq |n| + |p| \leq 4$. The shortest route is always preferred whenever possible because the less we modify the coefficients of the image, the more it resembles the original copy.

The extraction process is similar to the embedding process except that $\S(\sigma_{\mathcal{Q}}, 4)$ of each selected vGQC is computed. All pairs will be combined and decrypted to get the final message.

3. STATISTICAL ANALYSIS : STEGO VS. COVER IMAGE

3.1. Expected number of modifications per coefficient

In order to calculate the expected number of modifications per coefficient, π, we define two terms θ_1 and θ_2. θ_1 is the probability that the shortest route is used for case $\oplus = 3$, and $\ominus = 1$ (the second row in table 1) and θ_2 is the probability that the shortest route is used for case $\oplus = 1$, and $\ominus = 3$ (the last row). Since μ (RSA encrypted secret message) is randomly distributed, the probability for all kinds of modifications is equal. In our case, the total number of modifications can be 0, 1, 2, or 3. As a result, the probability to have each kind of modifications is 0.25. Table 2 shows the probability of each kind of modifications for one fixed pair of message bits xy.

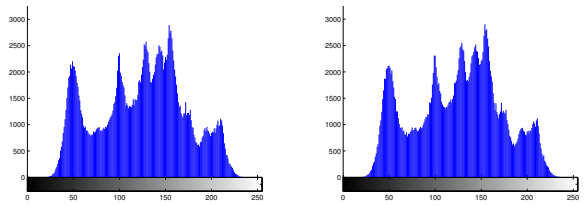
Table 2. Modification probability

Num. of modi.	Probability
0	0.25
1	$0.25(\theta_1 + \theta_2)$
2	0.25
3	$0.25(1 - \theta_1 + 1 - \theta_2)$

The expected number of changes is $\pi = 2 - (\theta_1 + \theta_2)/2$. Since $\theta_1, \theta_2 \in (0, 1)$, $\pi \in (0.25, 0.50)$. In the case of $\theta_1 = \theta_2 = 0.5, \pi = 0.375$. Therefore, we can conclude that π in our scheme is less than π in the LSB embedding scheme in the DCT domain, where $\pi = 0.5$.

3.2. Histogram analysis

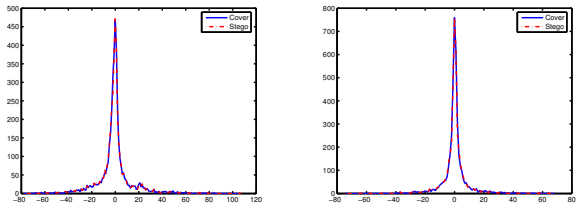
The histograms of the cover and stego images are shown in Fig. 2. It clearly shows the two histograms are identical. This effect is mainly due to the fact that the modifications are made at the DCT coefficients with large magnitudes, which correspond to the noisy areas in the original image.



(a) Cover Image (b) Stego

Fig. 2. Histograms of cover and stego images.

Fig. 3 shows the (1,2) and (2,1)-DCT distributions for cover and stego images. Both distributions are identical. This effect is ensured by the Mod-4 embedding scheme where no flipping of the LSB occurs. These identical distributions make the steganalysis less successful.



(a) (1,2)-DCT coefficient (b) (2,1)-DCT coefficient

Fig. 3. DCT coefficient distirubtion for (1,2) and (2,1).

3.3. Blockiness

When embedding messages of different lengths into an image, the blockiness of the stegos are about the same since the message is padded with a sequence of random bits to fill up the unused spaces. The assumption on the increase of blockiness made in [8] does not fit into our scheme. Thus, the linear model in Outgess attack [8] fails to detect the stegos created by our steganographic scheme.

4. EXPERIMENT RESULTS

To date, our algorithm has been tested on a variety of images with different textures. The experimental results illustrate the effectiveness of our proposed algorithm.

Several standard grayscale images (Airplane, Baboon, Lena, and Pepper) have been used in this section to illustrate the effectiveness of our approach.

4.1. Quality of stego

The invisibility of the embedding message is shown in Fig. 4. It clearly shows that there is no obvious visual distortion in the stego image. The PSNR values of four stego objects are listed in Table 3. They are all greater than 35 db, which

is the empirical value for the distortion invisibility requirement.

(a) Cover Image (b) Stego

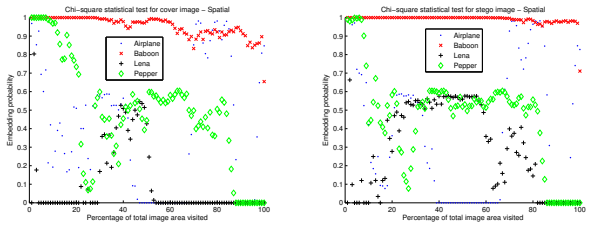
Fig. 4. Cover and stego images.

Table 3. The PSNRs of the stego images.

Images	PSNRs
Airplane	48.01
Baboon	42.69
Lena	48.44
Pepper	48.51

4.2. χ^2-attack in Spatial and DCT Domains

Fig. 5 and Fig. 6 demonstrate the results of the χ^2-test on four original and stego images in spatial and DCT domains, respectively. Both figures show that the χ^2-test fails to detect stegos since the embedding probabilities never remain unity for some percentage of the areas of the image. Baboon image is an exception since the χ^2-test on the original image leads to the unity for certain areas and the image itself is too noisy and hence may not be suitable to be used as a cover image.

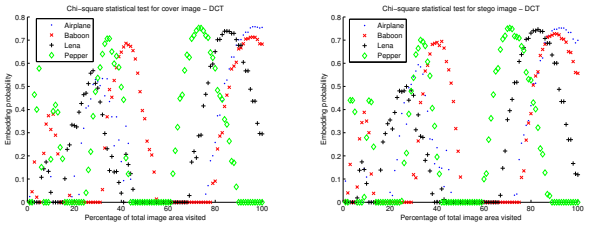


(a) Cover Image (b) Stego

Fig. 5. χ^2-statistical test on spatial domain.

5. CONCLUSIONS

In this paper, we propose a novel adaptive DCT-based Mod-4 steganographic method. It is able to withstand some statistical attacks. The main contributions are:



(a) Cover Image (b) Stego

Fig. 6. χ^2-statistical test on DCT domain.

- Define the vGQC's, which relate to noisy areas in the image, as embedding regions.
- Use the modulo 4 arithmetic to embed a pair of bits into a valid GQC.
- Apply the shortest-route scheme to ensure the expected number of modifications is minimal.
- The DCT coefficients with larger magnitudes are given higher priority for adaptive modification.
- A 128-bit public key RSA method encrypts the scret message for more security.

Our future work includes: 1) refine the definition of vGQC by adding more specific constraints, 2) analyze the properties of Mod-4 stegos when the DC coefficients are ignored during modification, 3) analyze the corresponding changes in spatial domain for each modification done by Mod-4, and 4) mathematically prove that Mod-4 is secure with respect to the existing steganalysis tools. We hope that our Mod-4 method will stimulate the steganography community in search of new and efficient steganalysis methods.

6. REFERENCES

[1] R. Machado, *http://www.securityfocus.com/tools/586/scoreit*, "EzStego", Nov. 1996.

[2] Y. C Tseng and H. K Pan, "Data Hiding in 2-color Image", *IEEE Transactions on computers*, Vol. 51, No. 7, pp. 873-878, July 2002.

[3] E. Kawaguchi and R. O. Eason, "Principle and applications of BPCS-Steganography", *SPIE Int'l Symp. on Voice, Video, and Data Communications*, pp. 464-473, 1998.

[4] N. Provos, "Defending Against Statistical Steganalysis," *Proc. of the 10th USENIX Security Symp.*, pp. 323-335, 2001.

[5] R. Chu, X. You, T. Kong, and X. Ba, "A DCT-based image steganographic method resisting statistical attacks," *IEEE Int'l Conf. on Acoustics, Speech, and Signal Processing*, Vol. 5, pp. 953-956, 2004.

[6] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," *Proc. of 3rd Int'l Workshop on Information Hiding*, pp. 61-76, 1999.

[7] C. Kim, S. Chul, S. Lee, W. Yang, and H. Lee, "Steganalysis on BPCS Steganography," *Pacific Rim Workshop on Digital Steganography*, 2002

[8] J. Fridrich, M. Goljan and D. Hogea. "Attacking the OutGuess", *Proc. of the ACM Workshop on Multimedia and Security*, Dec 2002.