ISPACS 2006

2006 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS2006)
Yonago Convention Center, Tottori, Japan

Graphical Comparative Study on DCT-based Steganographic Methods

KokSheik Wong
Faculty of Engineering,
Shinshu University,
4-17-1 Wakasato, Nagano,
380-8553 Japan.
Email: koksheik@shinshu-u.ac.jp

Kiyoshi Tanaka
Faculty of Engineering,
Shinshu University,
4-17-1 Wakasato, Nagano,
380-8553 Japan.
Email: ktanaka@shinshu-u.ac.jp

Xiaojun Qi
Department of Computer Science,
Utah State University,
4205 Old Main Hill,
Logan, UT 84322-4205, USA.
Email: xqi@cc.usu.edu

Abstract— **This paper presents a graphical comparative study of steganographic methods in the DCT domain. This graphical representation allows at-one-glance comparison among steganographic methods, showing the relative performance of each method with respect to the ideal methods for the metrics considered. Six representative DCT-based steganographic methods are selected and fairly compared in terms of six significant evaluation criteria. From the comparison results, we found some trends in recent evolution of steganographic methods and possible future development directions.**

I. Introduction

Derived from the Greek literature, steganography is an ancient technique for covert communication. Even from the earlier days, imagery steganography plays an important role in secret communication. Classically, two images are generated so that when superimposing one on top of another reveals the third (secret) image. In the digital world, imagery steganography includes the techniques to hide information, and to detect the presence of the embedded message in a suspicious image [1]. Its applications are not limited for covert communication, but also for history recording, authentication, signature, and so on [2].

In recent years, many imagery steganographic methods are invented to hide information utilizing redundancies in digital image representation. Along with the evolution of steganographic methods, many steganalyzers are equally smartly invented to detect the presence of data embedded in an image[1], [3]. While the battle between hiding and seeking continues, comparison among methods in the same domain is neglected. In particular, when a steganographic method Ψ is proposed, a fair comparison between Ψ and other existing methods is important but generally difficult to carry out. Unlike watermarking where there is a set of standard benchmarking criteria (e.g., robustness against compression, cropping, rotation, and etc.) for comparing two or more watermarking systems, there is almost no guideline for benchmarking a steganographic method. Nevertheless, steganalysis is usually (or solely) used as the evaluation tool to compare two or more steganographic methods.

Seeing the necessity of such comprehensive comparative study using various aspects of evaluation criteria, we present a graphical approach to fairly compare two or more steganographic methods. "A picture tells a million words" - this graphical representation allows at-one-glance comparison among steganographic methods instead of looking at the dull tables. This representation also show the relative performance of each method with respect to (w.r.t.) the ideal method for the metrics considered. In particular, we consider six significant evaluation criteria, and the graphical comparative study is carried out with six representative steganographic methods in the DCT domain.

II. Methodologies

In this section, we review several representative steganographic methods in the DCT domain. To ease the discussion, let $\Omega(\epsilon)$ denote the carrier capacity of method ϵ.

A. JSteg (JS)

Upham invents JSteg that hides information in the least significant bits (LSB) of the quantized DCT coefficients (qDCTCs) of a JPEG image in a sequential manner [4]. Let $qDCTC(y)$ denote a qDCTC with value y. JS skips all $qDCTC(y = 0, 1)$, and embeds information using three fields:

1) Field X (5 bits) expresses the length of field Y.
2) $Y \in [0, 2^{31}]$ expresses the message length.
3) Z is the actual secret message bits.

A conservative estimation of $\Omega(JS)$ is

$$\min\left\{2^{31}, \sum_{y\neq 0,1} qDCTC(y)\right\} - 36 \text{ bits}. \quad (1)$$

B. OutGuess (OG)

Provos invents OG that hides information by replacing the LSB of qDCTCs by the message bits to be embedded [5]. OG scatters information in a random manner with some key, skipping $qDCTC(k = 0, 1)$. After data embedding, OG carries out a distribution correction phase so that qDCTCs of the resulting stego are distributed 'similarly' to the original distribution. Let $h(y)$ denoted frequency of $qDCTC(y)$. Based on the code downloaded from *www.OutGuess.org*,

$$\Omega(OG) = \frac{2 \times (\sum_{y\neq 0,1} h(y)) \times h(-2)}{h(-1) + h(-2)} \quad (2)$$

C. F5

Westfeld invents F5 that utilizes matrix encoding to represent the secret message with LSB of $qDCTC(y \neq 0)$ [6]. Depending on the cover image and the secret data length, F5 chooses a $(1, j, 2^j)$-matrix encoding scheme, which requires at most 1 modification for embedding j bits, using 2^j $qDCTCs(y \neq 0)$. Whenever a modification is required, the magnitude of the selected qDCTC is decremented. In case an $qDCTC(y = 1, -1)$ is shrunk to zero, the message bits are re-embedded. $\Omega(F5)$ could not be estimated accurately because it is both message and image dependent.

D. Model Based Steganography (MB)

Sallee proposes MB that treats a cover medium as a random variable X that obeys some parametric distribution (e.g., Cauchy or Gaussian) [7]. The medium is divided into 2 parts, i.e., the deterministic part $x_D \in X_D$, and the indeterministic part $x_I \in X_I$ where the secret message is embedded. Low precision histograms of qDCTCs are first obtained, and the offsets of qDCTCs (w.r.t. the original histogram bin) are employed for data embedding. $\Omega(MB)$ is computed with the entropy of the modeled conditional distribution $\hat{P}_{X_I|X_D}$.

E. ZS

Iwata et al. define *diagonal bands* within a block of 8×8 qDCTCs in [8]. There are at most 9 diagonal bands in a block, and each band holds exactly one secret bit. Denote each diagonal band by D_i, and let r_i denote the number of consecutive zeros in band D_i. The zero sequence in D_i is modified so that $\mod(r_i, 2)$ matches the message bit to be embedded. In the extended version,

$$\Omega(ZS) = \frac{N_x N_y (L_b + \alpha + L_s)}{64}, \tag{3}$$

where L_b and L_s[1] represent the number of bands employed in each block, α denotes the fixed length of secret message bits stored in the nonzero part of D_i, and $N_x \times N_y$ is the dimension of the image.

F. Mod4

Qi et al. propose Mod4 that stores information in a valid group of 2×2 spatially adjacent qDCTCs (vGQC) [9]. A vGQC contains at least τ_1 number of $qDCTC(y > \phi_1)$, and at least τ_2 number of $qDCTC(y < -\phi_2)$. Each vGQC holds exactly two bits, and qDCTCs in a vGQC are modified so that the sum of all qDCTCs, when mod'ed with 4, matches with the pair of bits to be embedded. During modification, Mod4 uses the shortest route modification scheme, skipping $qDCTC(y), y \in [-\phi_2, \phi_1]$, and modifies coefficients with larger magnitude first. $\Omega(\text{Mod4}) = 2 \times$ number of vGQC. For the rest of this paper, unless specified otherwise, let $\phi_i \in \{0, 1, 2\}$ and $\tau_i \in \{1, 2\}$, i.e., random parameter.

[1] L_b determines the number of D_i-bands to consider in the zero sequence-based embedding scheme, and L_s determines the number bands to consider in the summation of absolute value-based embedding scheme.

III. Metrics

To carry out graphical comparative study among the aforementioned steganographic methods, we rely on metrics. Each metric is briefly reviewed in the following subsections, along with the scaling procedure when necessary. 500 hundred 8-bit grayscale images, each of size 800×600 pixels, were collected using Sony Digital camera DSC-828 for experimental use.

A. Carrier Capacity

For the rest of the paper, set JPEG quality factor to 80. We express $\Omega(\epsilon)$ for an image A_k in terms of bits per nonzero qDCTCs (bpc) [10]. To assign the final value, we compute the average of $\Omega(\epsilon)$ for $A_k, k = 1, 2, ..., 500$. If the average value $\bar{\Omega}(\epsilon) > 1$, we set $\bar{\Omega}(\epsilon) = 1$. For Mod4, we set $\phi_i = \tau_j = 1$ for this part.

B. Image Quality Measures

For image quality evaluation, we employ Universal Image Quality Index (UQI) by Wang and Bovik [11]. UQI consider linear correlation between corresponding pixels, the mean luminance difference, and the contrast difference between cover A_k and stego A'_k. UQI is computed using the following equation:

$$UQI(A_k, A'_k) := \frac{\sigma_{xy}}{\sigma_x \sigma_y} \cdot \frac{2\bar{x}\bar{y}}{(\bar{x})^2 + (\bar{y})^2} \cdot \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2} \tag{4}$$

where

$$\sigma_{xy} = \frac{1}{N-1} \sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y})$$

Here, x (y) is the linearized pixel array of A_k (A'_k). $\bar{x}$ is the mean pixel value of x, and σ_x^2 is the variance of pixel values of x. Eq. (4) is computed for local regions using a sliding window of size $B \times B$, and the value is store in Q_j. We set $B = 16$ in this paper, and there are $\mathcal{M} := 800 \times 600 \div 256 = 1875$ windows. The overall quality index is calculated as

$$UQI(A_k, A'_k) = \frac{1}{1875} \sum_{j=1}^{1875} UQI_j(A_k, A'_k). \tag{5}$$

To carry out the experiment, we embed at rate $0.05bpc$ into A_k using each method ϵ, and these A'_k are used for the rest of the paper unless specified otherwise.

C. Filesize Ratio

Let $FS(A_k^J)$ be the filesize of A_k^J in bytes, where A_k^J is the JPEG compressed version of A_k. We consider the ratio of $|FS(A_k^J) - FS(A'_k)|$ to the amount of information embedded, computed by Eq. (6). Here $bpc = 0.05$. The closer FSR gets to 1 raises less suspicion in steganalysis (better performances):

$$FSR(A_k, A'_k) = 1 - \frac{8 \times |FS(A'_k) - FS(A_k)|}{bpc \times (\sum_{k \neq 0} h_k) \times 2} \tag{6}$$

D. Histogram Product

Let $\mathcal{P}_{ij}(A_k^J), i, j \in \{0, 1, ..., 7\}$ denote the distribution of the (i, j)-mode qDCTCs for A_k^J. Let $\mathcal{P}(A_k^J) := \sum_{i,j} \mathcal{P}_{ij}(A_k^J)$, i.e., the global histogram. Let $h_{ij}^k(y)$ be the frequency of the bin labeled y in $\mathcal{P}_{ij}(A_k^J)$. Finally denote the frequency of the bin labeled y in $\mathcal{P}(A_k^J)$ by $h^k(y)$. We drop the superscript k to ease the presentation. To quantify how close the histograms are (JPEG A^J and stego A') w.r.t. one and another, we calculate the product of ratios for the frequency of some selected bins. We denote this product by HP, and it is computed as follows:

$$HP := \prod_{\substack{y=-1 \\ ,0,1}} \left[\frac{\min\{h(y), h'(y)\}}{\max\{h(y), h'(y)\}} \prod_{\substack{i,j=1,2 \\ i=j\neq 1}} \frac{\min\{h_{ij}(y), h'_{ij}(y)\}}{\max\{h_{ij}(y), h'_{ij}(y)\}} \right] \tag{7}$$

E. Blind Steganlyzer

We consider Fridrich's feature based blind steganalyzer to quantify the robustness of each method against steganalysis. Instead of receiver operation characteristic curve, we consider stego detection rate,

$$SDR := \frac{\text{Number of Detected Stego}}{\text{Number of Stego} = 200} \tag{8}$$

We set $\sigma := 2 \times (1 - SDR)$.[2] For each method ϵ and each of the 500 A_k, we generate $A'_k(\epsilon)$ by embedding a message at rate $0.05bpc$. The mixture of 300 A_k and the corresponding 300 $A'_k(\epsilon)$ are fed into the classifier for training purposes. In specific, we employ two discriminant functions f_0 and f_1 after the computation of covariance matrix using 300 pairs of A'_k and A_k. The rest of the 200 $A'_k(\epsilon)$ are used for the computation of SDR. An image A'_k is classified using

$$A'_k = \begin{cases} \text{cover}, & \text{if } f_0(A'_k) \geq f_1(A'_k) \\ \text{stego}, & \text{otherwise.} \end{cases} \tag{9}$$

F. Embedding Efficiency ($\mathbb{E}$)

Embedding efficiency $\ddot{\mathbb{E}}$ is defined to be the ratio of total number of modifications to the number of bits embedded [7]. Here, a modification could be the change in location or magnitude of a coefficient. Since lower $\ddot{\mathbb{E}}$ implies better performances in terms of steganalysis and image quality, we consider the value $\mathbb{E} := 1 - \ddot{\mathbb{E}}$.

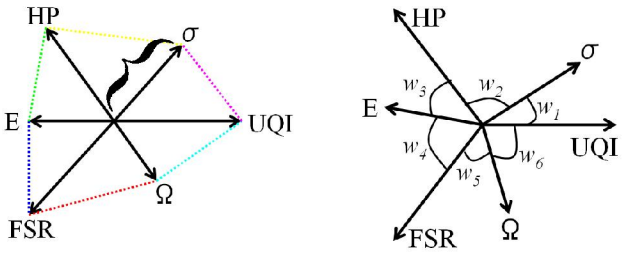
IV. Graphical Representation

To display the result, consider the ordinary polar coordinate system. At a regular angle interval of $\pi/3$, we draw vectors with length equal to the collected metric values. Next, we consider the order in which the metrics should be listed.

In general, the metrics are related to one and another in some manner, but they could be further divided into 3 sets. In specific, we have $G_1 := \{\sigma, \text{HP}, \mathbb{E}, \text{UQI}\}, G_2 := \{\mathbb{E}, \text{FSR}\}$ and $G_3 := \{\Omega, \mathbb{E}\}$. Elements within a set G_i somehow implies one and another. For example, high $\mathbb{E}$ implies that few modifications are done during data embedding, which leads to high UQI, HP and σ. On the other hand, UQI has nothing much to do with FSR when the JPEG quality factor is fixed to some value. Therefore, we group $\mathbb{E}$ and UQI in a new set. Finally, Ω is rather independent, but in F5 [6], $\mathbb{E}$ is inversely proportional to Ω. For that, we group them in a set.

We see that $\mathbb{E}$ appears in all sets. However, it influences FSR and HP more than it does on σ. Thus, we place $\mathbb{E}$ between HP and FSR. Also, in general, bad image quality at a fixed quality factor raises suspicion. Hence, we place UQI next to σ. Fig. 1(a) shows an example for the construction of a graph, where '{' denotes the length of σ.

When the representation is decided, comparison between any two methods could be carried out directly by superimposing the graph for one method on another, and watch which method has a larger enclosed area. We want to clarify that for current implementation, the area enclosed by a method does not represent any entity, but solely used to aide the visual comparison process. Relative performance of each method w.r.t. the ideal method could also be determined visually. That is, the smaller the unfilled region for a method is, the closer it is to the ideal method.



(a) Graph Construction (b) Weighted Graph

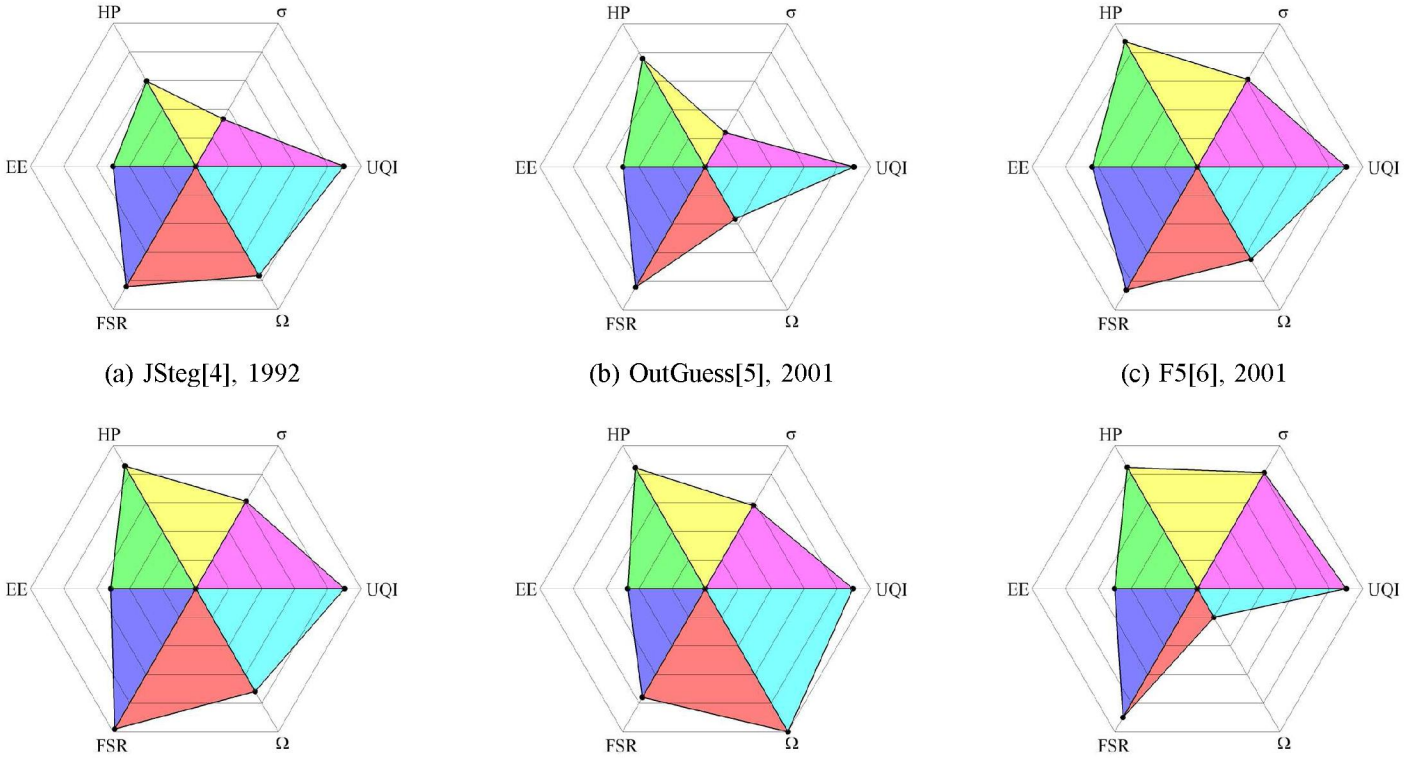
Fig. 1. Graphical Representation

V. Comparison and Discussion

All metric values are collected as described earlier. The graph for JS, OG, F5, MB, ZS, and Mod4 are shown in Fig. 2(a)-(f) in publication order, respectively. Overall, F5 and MB have well-balanced performance based on the graphs. We can also see that each steganographic method is evolving in different directions. The qDCTCs distribution correction phase after data embedding in OG gives better HP value (compared to JSteg) while sacrificing $\Omega(OG)$. Matrix encoding in F5 gives high coding efficiency, but awkward high occurrence of $qDCTC(y = 0)$ leads to bad performance in steganalysis. Arithmetic coding of secret message in MB results in filesize nearly identical to the original JPEG image, but vulnerable to steganalysis. Efficient data representation in ZS results in high $\Omega(ZS)$, but show low average FSR value. Finally, random parameter in Mod4 yields better performance in blind steganalysis but it sacrifices $\Omega(Mod4)$. However, despite its low value in Ω, Mod4 yields comparable results to F5 and MB in terms of UQI, HP and $\mathbb{E}$.

From the result, we also see some trends in the development of steganographic method. First, in general, the venerability to steganalysis is improving over recent years, which agrees with the observation that steganalysis is usually (solely) used as the evaluation criteria of a steganographic method. Even

[2]The multiplication of two is for the fact that all methods are detectable by the blind steganalyzer at embedding rate $0.05bpc$, i.e., $SDR(\epsilon) > 0.5$.



(a) JSteg[4], 1992 (b) OutGuess[5], 2001 (c) F5[6], 2001

(d) MB[7], 2003 (e) ZS[8], 2004 (f) Mod4[9], 2005

Fig. 2. Graphical Comparison among DCT-based Steganographic Methods

Mod4 yields the highest value in σ, the performance against steganalysis should be further improved. At the same time, having high performance only in steganalysis itself is not enough, and other evaluation criteria should also be taken into consideration. Next, the result also suggest that there maybe room for improvement in terms of $\mathbb{E}$, HP and image quality UQI. From the graphs, these metric values stay almost constant after year 2001, and they should be further improved in future development of steganographic method.

Last but not least, for presentation purposes, we have chosen uniform weight for each metric (i.e., regular angle of $\pi/3$) and relied on the area enclosed to aide the comparison process. Since the area enclosed changes w.r.t. the angle between any two metrics, a user could put different weights w_i on each evaluation metric according to the purpose of the comparison. However, the condition $w_1 + w_2 + ... + w_6 = 2\pi$ must hold. An example of graph construction is shown in Fig. 1(b).

VI. Conclusions

A graphical comparative study for six DCT-based steganographic methods utilizing six significant evaluation criteria is presented. Through the graphical comparison process, some trends in evolution of steganographic methods and possible future development directions are observed. Also, the graphical representation allows visual comparison between two or among more steganographic methods, and it shows the relative performance of each method with respect to the ideal method.

Our future works include the exploration of weight assigned to each evaluation criteria to effectively express the performance of each method. We should also consider more evaluation metrics in the graphical representation to carry out a more thorough comparison among steganographic methods in the same domain.

References

[1] H. Wang and S. Wang, "Cyber warfare: Steganography vs. steganalysis," *Communication of the ACM*, vol. 47, pp. 76–82, 2004.

[2] S. Katzenbeisser and F. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House Publishers, 2000.

[3] K. Mehdi, S. H. T, and M. Nasir, "Benchmarking steganographic and steganalysis techniques," in *Human Vision and Electronic Imaging*, vol. 5681, March 2005, pp. 252–263.

[4] D. Upham, "JSteg V4 - JPEG steganography," 1992. [Online]. Available: http://www.jjtc.com/Steganography/

[5] N. Provos, "Defending against statistical steganalysis," in *Proceeding of the 10th USENIX Security Symposium*, 2001, pp. 323–335.

[6] A. Westfeld, "F5 - a steganographic algorithm - high capacity despite better steganalysis," *Information Hiding. 4th International Workshop. Lecture Notes in Computer Science*, vol. 2137, pp. 289–302, 2001.

[7] P. Sallee, "Model based steganography," in *International Workshop on Digital Watermarking*, Seoul, October 2003, pp. 154 – 167.

[8] M. Iwata, K. Miyake, and A. Shiozaki, "Digital steganography utilizing features of JPEG images," *IEICE Trans. Fundamentals*, vol. E87-A, pp. 929–936, 2004.

[9] X. Qi and K. Wong, "An adaptive DCT-based mod-4 steganographic method," in *Proceedings of IEEE International Conference on Image Processing*, vol. 2, Genoa, Italy, September 2005, pp. 297 – 300.

[10] J. Fridrich, "Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes," in *6th Information Hiding Workshop, LNCS*, vol. 3200, New York, 2004, pp. 67–81.

[11] Z. Wang and A. Bovik, "A universal image quality index," *IEEE Signal Processing Letters*, vol. 9, pp. 81 – 84, March 2002.