Journal of Shanghai University, **6(4), 2002**

Steganographic Technique Capable of Withstanding RQP Analysis[1]

Wang Shuozhong, Zhang Xinpeng, and Zhang Kaiwen

School of Communication and Information Engineering, Shanghai University, Shanghai 200072

Abstract: A new steganographic approach for 24-bit color images that can resist the RQP steganalysis is described. The technique is based on modification of color triplets such that the existing color palette is not excessively expanded, or even reduced. In this way, numbers of unique colors and pairs of close-colors in the image do not rise significantly. This invalidates the RQP analysis. Experimental results are presented to support the argument.

Key words: steganography, steganalysis, RQP method, LSB embedding

1. Introduction

Since the late 1990s, digital steganography has received a great deal of attention from researchers. The goal is to send secrete information under the cover of a multimedia carrier such as digital image. By embedding the message, called stego data, into a cover image, the very existence of communication is hidden. This is in contrast to cryptography that scrambles the data so that nobody can decode them without the key, but makes no attempt to conceal the presence of secrete communication [1].

Steganography belongs to a broader subject of information hiding. Another important branch of information hiding is digital watermarking, which aims to protect intellectual property rights of multimedia contents [2]. The fundamental difference between steganography and watermarking lies in the primary object of communication. In watermarking, the object to be sent is the host signal, with the embedded data providing IPR protection. The existence of a watermark is often openly declared. The watermark must be robust, meaning that removal or destruction of the embedded mark will render the host object useless. Contrarily, the object to be transmitted in steganography is the embedded message, and the cover image merely serves as a disguise. Therefore, the most crucial requirement for steganography is being undetectable by both perceptual and algorithmic means. Robustness against attacks such as removal, destruction, and signal processing is not of the primary concern.

Techniques used in steganography include LSB embedding, masking and filtering, spread spectrum techniques, etc.[1] In the mean time, anti-steganographic, or steganalytic, methods are also being developed: analysis of pairs of grayscale values (PoVs)[3], the RS technique [4], the raw-quick-pairs (RQP) analysis[5], and high-order statistic methods[6], to name a few. The basic purpose of steganalysis is to reveal the presence of secrete information in an apparently innocuous image. In a sense, some steganographic methods have already been defeated, while countermeasures against steganalysis are quickly emerging [7]. The battle will undoubtedly go on endlessly.

[1] Supported by the Natural Science Foundation of China (60072030), and Key Disciplinary Development Program of Shanghai.

This letter proposes a steganographic countermeasure for 24-bit true color images, which can survive the RQP analysis developed by Fridrich et al. In the following sections, the RQP method is first briefly introduced, and the proposed anti-RQP technique with supporting experimental results is then presented.

2. The RQP Steganalysis

The RQP analysis is based on statistics of the numbers of unique colors and close-color pairs in a 24-bit color image. A pair of colors is said to be close if

$$|R_1 - R_2| \le 1, \quad |G_1 - G_2| \le 1, \quad |B_1 - B_2| \le 1 \tag{1}$$

When stego-data are embedded into a cover image using an LSB-based technique, the number of unique colors, U, usually increases so that the following quotient will rise:

$$Q = \frac{P}{\binom{2}{U}} \tag{2}$$

where P is the number of close-color pairs, and $\binom{2}{U}$ the number of all possible color pairs in the palette.

If the image already contains a hidden message, the increase of Q after embedding some additional data is generally smaller than that for an image without a previously embedded message. Thus, it is possible to detect the presence of hidden data by adding a test message into an image and observing the amount of increase in Q.

Using Q_2/Q_1 as a test statistic, Fridrich et al. described a method for selecting the threshold for a binary decision as to whether or not the image contains a secrete message, where Q_1 is the Q value for the image under test calculated from (2), and Q_2 the value for the image in which a certain amount of test data is embedded. It has been found that the RQP method is quite reliable when the number of unique colors is less than half of the total number of pixels in the image.

3. Anti-RQP Steganography

It is clear that the RQP analysis relies on the fact that steganographic embedding generally causes the number of unique colors to rise due to LSB modifications. An effective countermeasure, therefore, can be devised by maintaining the color palette without creating new colors.

Instead of embedding data by modifying LSB of individual color components of the pixels, we base our technique on modifying each triplet, [RGB], of the pixel color value as an entirety. The triplet is modified to a new point in its close vicinity in the color space, which is a valid color in the palette of the cover image. A new color is created only if such a color is not available. This is realized in the following way.

1) Assume that a pixel A is chosen to carry one bit of the stego data. If a “0” is to be embedded, and the sum of the 3 color components in A, R+G+B, is even, the pixel does not need to be changed. Similarly, if a “1” is to be embedded and R+B+G is odd, the pixel is also unchanged.
2) If the above condition is not satisfied, the least significant bits of each color component of the pixel are set to 0, resulting in a base color denoted A000. The 8 colors that are closest to A are then obtained, and they can be divided into two groups:

   Even colors: A000=A000+[000], A011=A000+[011], A101=A000+[101], A110=A000+[110]

Odd colors: A001=A000+[001], A010=A000+[010], A100=A000+[100], A111=A000+[111]

3) If a "0" is to be embedded, a search in the cover palette is performed to find a match with any one of the 4 colors in the even group. Once a match is found, search is terminated and the pixel is modified to the matched color with an error at most 1 level in 256 in any one of the 3 color components.
4) In case none of the 4 even colors is in the cover palette, set A=A000, and a new even color is thus created.
5) Similarly, if a "1" is to be embedded, the search is done to find a match with a color in the odd group.
6) In case a match is not found, set A=A001 to create a new odd color.
7) Pick the next cover pixel and the next stego data bit, and start over from Step 1.

The probability of creating a new color in each embedded pixel is difficult to calculate. However, it can be estimated experimentally by counting the increased number of unique colors in the new palette.

As the search of matched colors is carried out within unit cubes in the color space, modifications of the pixel colors are confined to the LSB plane. By taking LSBs of the sum R+G+B of all modified pixels, the stego data are easily extractable.

In order to reduce the chance of creating new colors in the embedding process, the cubic searching space may be expanded to a size of 3×3×3. The expanded cubic space consists of 64 colors, 32 even and 32 odd, therefore the search is done within 32 colors instead of 4. Table 1 gives all the possible increments to the base color triplet A000 for steganographic embedding. The quantity δ in the first column indicates the number of color components in a pixel to be modified that are beyond LSB. For example, if a pixel value is modified to A000+[2 2 1], components R and G are increased by 2 that will affect the second least significant bits, and B increased by 1, therefore $\delta = 2$. Colors with a small δ are tested first in the search in order to minimize the color distortion. A new color is created each time when a match cannot be found in all 32 colors.

Obviously, expansion of the search cube substantially reduces the number of new colors at the cost of increased distortion and a rise in computational complexity, while extraction method remains unchanged. In fact, due to overlap of the large test cubes of adjacent pixels, it is usual that the variety of colors is even slightly reduced after steganographic embedding. For convenience in the discussion, the schemes with different cube sizes will be referred to in the following as ARQP111 and ARQP333 respectively.

Table 1 Increments in RGB components with respect to A000 in steganographic embedding

δ	Even group: for embedding a "0"	Odd group: for embedding a "1"
0	0 0 0 0 1 1 1 0 1 1 1 0	0 0 1 0 1 0 1 0 0 1 1 1
1	2 0 0 0 2 0 0 0 2 2 1 1 1 2 1 1 1 2 –1 1 0 1 –1 0 –1 0 1 1 0–1 0 –1 1 0 1 –1	1 2 0 2 1 0 1 0 2 2 0 1 0 1 2 0 2 1 –1 0 0 0 –1 0 0 0 –1 1 1 –1 1 –1 1 –1 1 1
2	2 0 2 2 2 0 0 2 2 –1 –1 0 0 –1 –1 –1 0 –1 –1 1 2 1 –1 2 –1 2 1 1 2 –1 2 –1 1 2 1 –1	2 2 1 1 2 2 2 1 2 –1 1 –1 1 –1 –1 –1 –1 1 –1 2 0 2–1 0 –1 0 2 2 0 –1 0 –1 2 0 2 –1
3	–1 –1 2 2 –1–1 –1 2 –1 2 2 2	–1 2 2 2 –1 2 2 2 –1 –1 –1 –1

4. Experiments

Two image databases, each consisting of 100 true-color images sized 300×400 (pictures of people) and 200×267 (landscapes) respectively, were used in the experiment. These images were generated using a digital camera and stored in the JPEG format. Numbers of unique colors ranged from 30% to 55% of the total number of pixels in each image so that any stego contents embedding in these images with an LSB embedding technique would be vulnerable to the RQP steganalysis.

Figure 1 shows the result of RQP analysis on stego images using the People group as covers. Curve 1 represents values of Q_2/Q_1, where Q_1 is calculated from the 100 cover images without a stego message, and Q_2 is obtained from a corresponding set of stego images each of which containing 17,255 bits of stego data embedded with a simple LSB method, that is a payload of 0.048 bits per color component. In obtaining the stego images, a bit stream of the stego data was used to replace the LSBs of a set of pseudo-randomly chosen color components in each cover image, resulting in peak-signal-to-noise ratios (PSNRs) around 64.4dB for the majority of the images. Curve 2 represents Q_3/Q_2 where Q_3 is obtained by embedding 17,255 additional bits of test data into the stego images using the same LSB method, referred to as LSB-on-LSB. Clearly, the values of Q_3/Q_2 are substantially smaller than Q_2/Q_1 so that a threshold can easily be found [5], making the RQP analysis effective.

Curves 3 and 4 are obtained in the same way except using ARQP111 instead of a conventional LSB embedding method. It is observed that, with the number of newly created colors reduced, both curves for Q_2/Q_1 and Q_3/Q_2 are significantly lowered and become much closer. A decision threshold for images from the same database becomes rather critical, therefore is no longer possible to find a unified threshold for a wider range of images. This means that the RQP steganalysis will fail.

Curves 5 and 6 are the results for ARQP333. These two are very close to each other with $Q_{n+1}/Q_n \approx 1$, meaning that the stego image is indistinguishable from the cover in terms of unique colors and pairs of close colors. This makes the RQP analysis totally impossible.

Experiments were also carried out to embed an additional 17,255 bits of test data using the same basic LSB method into cover images and stego images generated with the anti-RQP techniques. The results are shown in Figure 2, in which the top solid, the lower solid, and the dotted curves correspond respectively to the LSB-on-cover, LSB-on-ARQP111, and LSB-on-ARQP333 cases. It is clear that one cannot distinguish covers from the ARQP-based stego images using a statistical test. Especially, the ARQP333-stego images behave almost the same as the covers in terms of the RQP analysis.

Experiments on the Landscape group have produced similar results that are not shown here due to space limitation.

Assuming Gaussian distributions for both cases as proposed in [5], and estimating the means and standard deviations from the experimental data, the probability density functions of Q_{n+1}/Q_n shown in Figure 3 (scaled to [0, 1] for presentation convenience) can be obtained. With 100 images from the Landscape database and an embedding capacity of 5,299 bits, the results are illustrated in Figure 4.

Invisibility of the stego data is shown in Table 2. Fidelity of the stego image is measured in peak-signal-to-noise ratio (PSNR) with respect to the cover image. By using the anti-RQP algorithm, the loss of fidelity is less

than 3dB and 5dB for ARQP111 and ARQP333 respectively. In any case, however, PSNR is greater than 59dB, representing a very high degree of imperceptibility in comparison with the lower bound of 39dB as accepted for invisible watermarks.

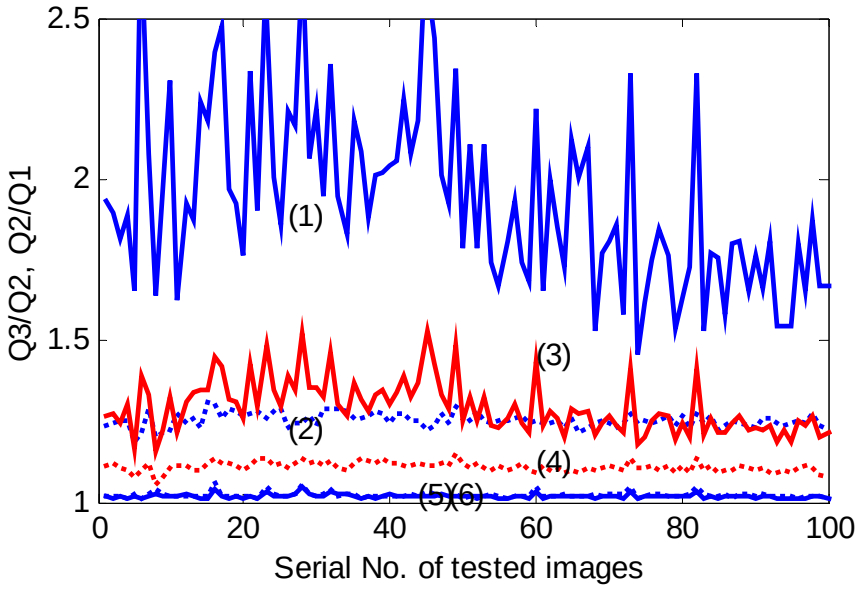

Figure 1 Q_{n+1}/Q_n curves for 100 color images sized 300×400. Curve 1 represents values of Q_2/Q_1, where Q_1 is calculated from 100 cover images without stego data, while Q_2 from stego images each of which containing 17,255 bits of stego data embedded with a basic LSB embedding. Curve 2 represents Q_3/Q_2 where Q_3 is obtained by embedding 17,255 additional bits of test data into the stego images using the same method. Curves 3 and 4 are obtained in a similar way, with ARQP111 instead of the basic LSB. Curves 5 and 6 are obtained using ARQP333.

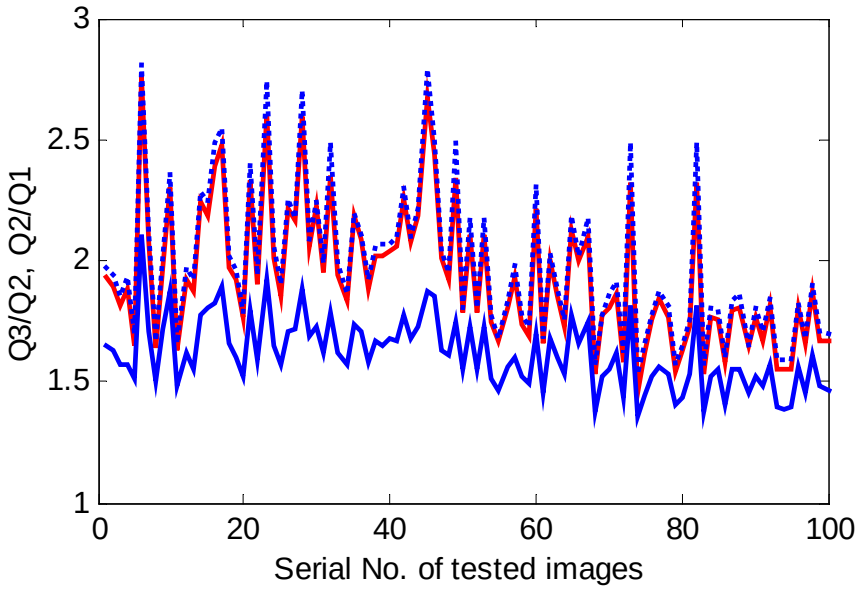

Figure 2 Results for LSB embedding of 17,255 bits test data into cover images (top solid) and stego images generated respectively with ARQP111 (lower solid) and ARQP333 (dotted).

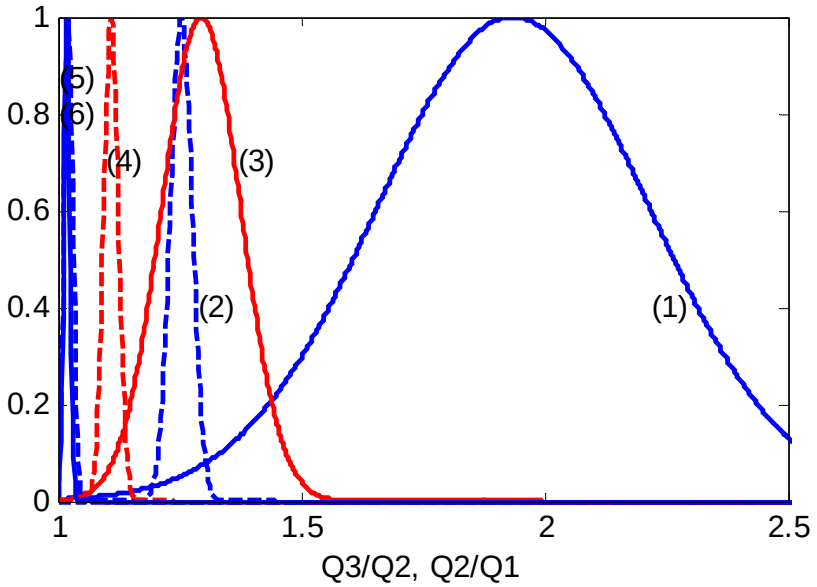

Figure 3 Probability density functions of Q_{n+1}/Q_n scaled to [0, 1]. Curve numbers correspond to those in Figure 1.

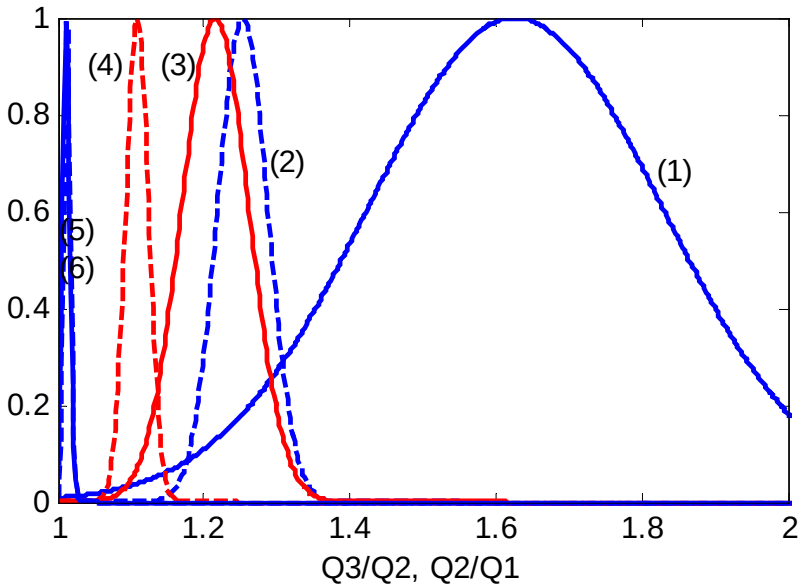

Figure 4 Same as Figure 3, obtained with 100 color images from the Landscape database.

Table 2 PSNR of stego image with different embedding techniques

Image database and payload		Typical PSNR after steganographic embedding (dB)		
Image database	Embedded bits	Basic LSB	ARQP111	ARQP333
People (400×300)	17255	64.4	61.7	59.9
Landscape (267×200)	5299	65.9	63.9	61.5

5. Conclusions

It has been demonstrated that by avoiding creation of new colors in steganographic embedding, steganalysis based on statistics of unique colors can be defeated. The proposed method attempts to find an available color within the existing palette as a replacement of the original cover pixel. Modifications to the cover pixels may occur in the second least significant bit plane, resulting in a slightly increased distortion of the image. This distortion, however, is still well below the human perceptual threshold, therefore ensuring satisfactory invisibility.

Although computational complexity compared to the basic LSB technique is substantially increased, especially with ARQP333, it is not a serious problem as in practical applications the embedding algorithm needs to be executed only on a few images taken from a large database.

References

[1] N. F. Johnson, and S. Lajodia, Exploring Steganography: Seeing the Unseen, *IEEE Computer*, **31**(2), 1998: 26–34

[2] N. Memon, and P. W. Wong, Protecting digital media content, *Communications of the ACM*, **41(**7), 1998: 34–43

[3] A. Westfeld, et al., Attacks on Steganographic Systems, *Lecture Notes in Computer Science*, vol.**1768**, 2000: 61–75

[4] J. Fridrich, et al., Practtical Steganalysis of Digital Images – State of the Art, *Proceedings of SPIE*, vol.**4675**, 2002: 1–13

[5] J. Fridrich, R. Du, and M. Long, Steganalysis of LSB Encoding in Color Images, *2000 IEEE Int. Conf. on Multimedia and Expo*, vol.**3**, 2000: 1279–1282

[6] H. Farid, Detecting Steganographic Message in Digital Images, Report TR2001-412, Dartmouth, Hanover, NH, 2001

[7] A. Westfeld, F5 – Steganographic algorithm: High capacity despite better steganalysis, *Lecture Notes in Computer Science*, vol.**2137**, Springer-Verlag, Berlin, 2001: 289–302