*Lecture Notes in Computer Science*, 2776, 2003: 395-406

# Steganography with Least Histogram Abnormality

Xinpeng Zhang, Shuozhong Wang, and Kaiwen Zhang

Communication & Information Engineering, Shanghai University, Shanghai 200072, China
zhangxinpeng@263.net shuowang@yc.shu.edu.cn ztszkwzr@sh163.net

**Abstract.** A novel steganographic scheme is proposed which avoids asymmetry inherent in conventional LSB embedding techniques so that abnormality in the image histogram is kept minimum. The proposed technique is capable of resisting the $\chi^2$ test and RS analysis, as well as a new steganalytic method named GPC analysis as introduced in this paper. In the described steganographic technique, a pair of mutually complementary mappings, $F_1$ and $F_{-1}$, is used, leading to a balanced behavior of several statistical parameters explored by several steganalytic schemes, thus improved security. Experimental results are presented to demonstrate the effectiveness of the method.

## 1 Introduction

Digital watermarking and steganography are two major branches of information hiding [1]. While watermarking aims to protect copyright of multimedia contents, the purpose of steganography is to send secret messages under the cover of a carrier signal. Despite that steganographic tools only alter the most insignificant components, they inevitably leave detectable traces. The primary goal of attack on steganographic systems, termed steganalysis, is to detect the presence of hidden data [2,3].

A widely used technique with low computational complexity and high insertion capacity is LSB steganography that replaces the least significant bits of the host medium with a binary sequence. Many steganalytic approaches have been developed to attack it. The $\chi^2$ analysis [4,5] detects the presence of hidden data based on the fact that the occurrence probabilities of adjacent gray values tend to become equal after LSB embedding. The method can also be used against other steganographic schemes such as J-Steg in which pairs of values are swapped into each other to embed message bits. RS steganalysis proposed by Fridrich et al. utilizes sensitive dual statistics derived from spatial correlations [2,6]. In addition, the RQP steganalysis for color images [7] is based on statistics of the numbers of unique colors and close-color pairs.

If the cover image was initially stored in the JPEG format, message insertion may alter the quantization characteristics of the DCT coefficients, leaving a clear sign for successful steganalysis [2,8]. If the DCT coefficients are modified in data embedding, block effects [9] or histogram distortion [10] can be explored in the analysis against such steganography techniques as used in J-Steg, OutGuess and F5 [11]. Lyu and Farid proposed a universal higher-order statistical method capable of attacking nearly every steganographic technique [12]. But in practice, it is difficult to perform the required training with a large number of stego and cover images.

While the above approaches aim to detect the presence of hidden data, an active warden attack can be performed, overwriting some insignificant contents in the cover to prevent message extraction. A game model between data-hider and data-attacker and the game equilibria are given in [13].

As opponents of attackers, data-hiders always try to design steganographic strategies for resisting statistical analyses [14]. For example, by carefully choosing replacement of the host pixel values, an LSB-based method can effectively withstand the RQP analysis [15]. In the present paper, a novel steganographic approach is proposed, which avoids the asymmetric characteristic inherent in conventional LSB embedding techniques so that distortion to the image histogram is kept minimum. The proposed technique is capable of resisting several powerful steganalytic methods including the RS analysis, the $\chi^2$ test, and a new technique termed GPC analysis as introduced in Section 2 of this paper.

## 2 Analyses of steganographic techniques

### 2.1 Chi-Square Test [4, 5]

Secret message for encoding or encryption can be considered a pseudo-random bit stream consisting of 0s and 1s. After replacing the LSBs of a cover image with these hidden bits, occurrences with gray values $2i$ and $2i+1$ tend to become equal. Supposing that $n_j$ is the number of pixels with a gray value $j$, the $\chi^2$ test calculates

$$\chi^2 = \sum_{i=1}^{k} \frac{\left[n_{2i} - \left(n_{2i} + n_{2i+1}\right)/2\right]^2}{\left(n_{2i} + n_{2i+1}\right)/2} . \tag{1}$$

and

$$p = 1 - \frac{1}{2^{(k-1)/2}\Gamma\left[(k-1)/2\right]} \int_0^{\chi^2} \exp\left(-\frac{t}{2}\right) t^{\frac{k-1}{2}-1} dt , \tag{2}$$

where $p$ represents the probability that the distributions of $n_{2i}$ and $n_{2i+1}$ are equal. This can be used to decide the presence of secret information.

### 2.2 RS Analysis [2, 6]

This method defines two mappings: $F_1$ for $0\leftrightarrow1$, $2\leftrightarrow3$, …, $254\leftrightarrow255$ and $F_{-1}$ for $-1\leftrightarrow0$, $1\leftrightarrow2$, …, $255\leftrightarrow256$. In other words, $F_1$ is used when the LSB of cover image is different from the hidden bit. Also, the following function is defined to measure the smoothness of a pixel group $(x_1, x_2, \ldots, x_n)$:

$$f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n-1} \left| x_{i+1} - x_i \right| . \tag{3}$$

Divide the received image into small blocks of the same size. Define $R_M$ as the ratio of blocks in which $f$ increases when $F_1$ is applied to a part of each block, and $S_M$ as the ratio of blocks with decreasing $f$. In general, $R_M + S_M < 1$. Similarly, another two parameters $R_{-M}$ and $S_{-M}$ can be defined when $F_{-1}$ is applied to a part of each block.

If the received image does not contain secret data, $F_1$ and $F_{-1}$ should equally increase the $f$ value of blocks in a statistical manner. So,

$$R_M \approx R_{-M} > S_M \approx S_{-M} . \quad (4)$$

When secret bits are embedded, the difference between $R_M$ and $S_M$ decreases whereas the difference between $R_{-M}$ and $S_{-M}$ increases. Thus,

$$R_{-M} - S_{-M} > R_M - S_M . \quad (5)$$

Therefore, an attacker can use the relation among the four parameters to detect the presence of secret information.

### 2.3 Gray-Level Plane Crossing (GPC) Analysis

In this subsection, an alternative steganalytic approach against LSB embedding is described. This, together with the $\chi^2$ and RS analysis, will be used in the following to examine the anti-steganalysis performance of a new LHA approach proposed in this paper. By viewing an image as a landscape in a 3D space with the $z$ coordinate representing the pixel gray-level, each pixel in the image is identified as a triplet ($x$, $y$, $z$). Define two interlaced families of odd and even gray-level planes, $\mathbf{P}_O$ and $\mathbf{P}_E$, parallel to the XY plane, each containing planes between $z = 2i+1$ and $2i+2$, and $2i$ and $2i+1$, respectively, where $i$ =0, 1, … , 127. The odd planes in $\mathbf{P}_O$ may be designated $z = 1.5$, $z = 3.5$, $z = 5.5$, …, $z = 255.5$, and the even planes in $\mathbf{P}_E$ as $z = 0.5$, $z = 2.5$, $z = 4.5$, …, $z = 254.5$. The numbers of planes in the two families crossed by all lines connection adjacent pixels are summed up, and denoted $N_O$ and $N_E$ respectively.

Clearly, if the received image does not contain any secret data, $N_O$ and $N_E$ should roughly equal. LSB embedding will not change $N_O$ because swapping between $2i$ and $2i+1$ does not cross any plane in $\mathbf{P}_O$. In contrary, $N_E$ will be raised since each modified pixel traverses one plane in $\mathbf{P}_E$ and the smoothness between adjacent pixels is reduced. For example, if the two adjacent gray values of original image are equal, and one of them is modified by LSB embedding, $N_E$ will increase. Therefore a parameter $R = N_E / N_O$ can be used to detect the presence of inserted data. If $R$ is greater than a given threshold $T$, the image is judged as containing a secret message. In order to enhance sensibility of $R$, the number of crossings is not counted when the difference between adjacent gray values is greater than a predefined value $D$, say, 4 or 5.

Fig.1 shows the relationship between $R$ and the amount of secret bits in 3 test images, all sized 512×512. Note that $R$ increases approximately linearly with the payload $L$, the ratio between the embedded bit number and the total number of host pixels. Also, the less the high-frequency components in a cover image, the more sensitive the value of $R$ is with respect to the payload. The usefulness of the $R$-$L$ relationship is demonstrated in the following experiment. A total of 385 images captured with a digital camera were used to establish statistical distributions of $R$ at different payloads.

Fig.2 shows the results where the ordinate is the image number corresponding to $R$ on the abscissa. When smoothed and normalized, these curves can be used to represent PDF of $R$. Choosing a threshold $T$ for detecting LSB steganography, the probability of missing a secret-data carrying image, $P_m$, and the probability of false alarm, $P_f$, may be determined. In Table 1, $P_m$, and $P_f$ under different $T$ are given. Obviously, a large $T$ results in a small $P_f$ and large $P_m$. When the payload is large enough and a suitable threshold chosen, the two types of error become fairly small.

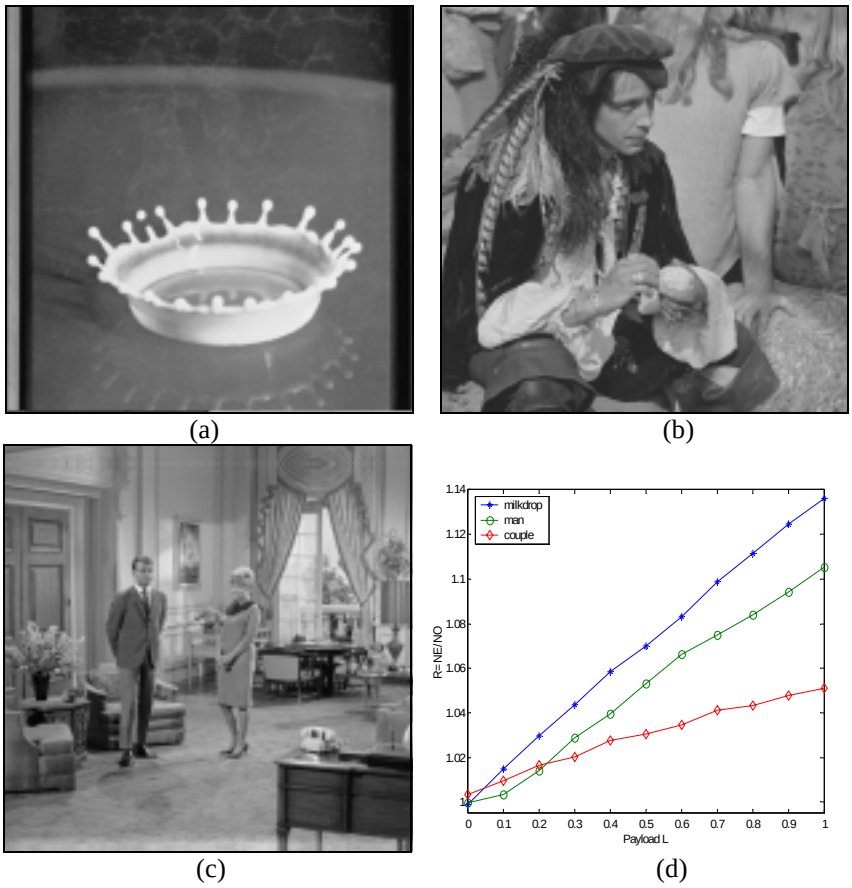



**Fig. 1.** Images Milkdrop (a), Man (b), Couple (c), and relation between $R$ and payload (d).

**Table 1.** Detection performance with different threshold $T$.

| $T$ | False alarm probability $P_f$ (%) | Missing probability $P_m$ (%) | | | |
|---|---|---|---|---|---|
| | | $L$=0.25 | $L$=0.50 | $L$=0.75 | $L$=1.0 |
| 1.010 | 11.69 | 5.97 | 1.04 | 0.52 | 0.26 |
| 1.015 | 5.45 | 10.39 | 3.38 | 1.56 | 0.52 |
| 1.020 | 2.86 | 19.48 | 4.68 | 2.08 | 0.52 |
| 1.025 | 1.82 | 29.61 | 8.31 | 4.16 | 1.82 |
| 1.030 | 1.04 | 43.38 | 12.21 | 5.97 | 2.86 |

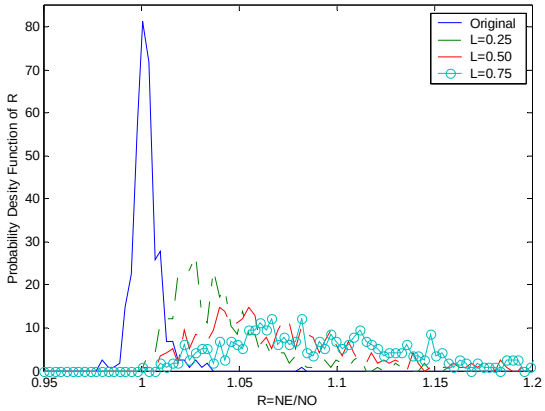



**Fig. 2.** Distributions of $R$ with different payload $L$.

## 3 LHA Steganography

### 3.1 Steganographic Algorithm

In the basic LSB steganography, a gray value is not altered if its LSB is the same as the bit to be hidden. Otherwise $2i$ is changed to $2i$+1 when embedding a 1, or $2i$+1 changed to $2i$ when embedding a 0. Swappings between $2i$ and $2i$–1 or between $2i$+1 and $2i$+2 never occur. All the three above-mentioned steganalytic approaches use statistical parameters exploring this property in detecting the presence of secret data.

To improve security, we introduce a new embedding method that causes least abnormality in the histogram for resisting the $\chi^2$ test. Also, since both $F_1$ and $F_{-1}$ are used when modifying gray values so that it can withstand RS and GPC steganalyses.

Consider pixels with a gray value $j$, $0 \le j \le 255$, in the host image, among which there are $h_j$ having their LSB different from the corresponding secret bit to be embedded. Modify these pixels by either +1 or –1 instead of simply replacing the LSBs. In this way, as in the simple replacement approach, the resulting LSBs will also be identical to the embedded data. Assume that a total of $x_j$ pixels are modified with –1, and ($h_j$–$x_j$) pixels with +1 in the embedding. The number of newly generated pixels having a gray level $j$ in the stego-image is therefore

$$h'_j = x_{j+1} + \left(h_{j-1} - x_{j-1}\right). \tag{6}$$

At both ends of the gray scale,

$$h'_0 = x_1\,, \tag{7}$$

$$h'_1 = x_2 + h_0\,, \tag{8}$$

$$h'_{254} = h_{255} + \left(h_{253} - x_{253}\right), \tag{9}$$

$$h'_{255} = \left(h_{254} - x_{254}\right). \tag{10}$$

Note that

$$x_0 = 0\,, \tag{11}$$

$$x_{255} = h_{255}\,, \tag{12}$$

$$0 \le x_t \le h_t\,, \qquad t = 1,2,\ldots,254\,. \tag{13}$$

Equations (6)~(10) can be expressed in a matrix form:

$$\mathbf{h}' = \mathbf{M}\mathbf{x} + \mathbf{h}_S\,, \tag{14}$$

where $\mathbf{h}'$ is a column vector $[h'_0, h'_1, \ldots, h'_{255}]^{\mathrm{T}}$, $\mathbf{x} = [x_0, x_1, \ldots, x_{255}]^{\mathrm{T}}$, $\mathbf{h}_S = [0, h_0, h_1, \ldots, h_{254}]^{\mathrm{T}}$ and

$$\mathbf{M} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ -1 & 0 & 1 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & -1 & 0 \end{bmatrix}. \tag{15}$$

For resisting the RS and GPC steganalyses, it is desirable that the numbers of mappings $F_1$ and $F_{-1}$ used in the embedding are equal:

$$\sum_{j=2i} x_j + \sum_{j=2i+1}\left(h_j - x_j\right) = \sum_{j=2i+1} x_j + \sum_{j=2i}\left(h_j - x_j\right)\ . \tag{16}$$

Define an index of histogram abnormality, $d$, as

$$d = \left\|\mathbf{h}'-\mathbf{h}\right\| = \sqrt{\sum_{j=0}^{255}\left(h'_j - h_j\right)^2}\ . \tag{17}$$

Clearly, $d$ is a function of $x_0$, $x_1$, …, and $x_{255}$. The minimum $d$ corresponds to the least histogram abnormality when the conditions (11)~(13) and (16) are satisfied, hence termed the LHA steganography.

To reduce computation complexity, a vector $\mathbf{x}$ corresponding to an approximate minimal $d$ can be found using the following method. Ideally, when $\mathbf{h}' = \mathbf{h}$ the histogram will not change:

$$\mathbf{h}' = \mathbf{M}\mathbf{x} + \mathbf{h}_1 = \mathbf{h}\,. \tag{18}$$

In addition, Eq.(16) should also be satisfied to resist the RS analysis. This results in a system of 257 linear equations with only 256 unknowns:

$$\mathbf{U}\mathbf{x} = \mathbf{v}\,. \tag{19}$$

The sizes of **U** and **v** are 257×256 and 257×1 respectively. An approximate solution to this over-determined problem in the mean square error sense can be found using matrix pseudo-inversion:

$$\hat{\mathbf{x}} = \mathbf{U}^{+}\,\mathbf{v}\,. \tag{20}$$

Let $x_0 = 0$, $x_{255} = h_{255}$ and

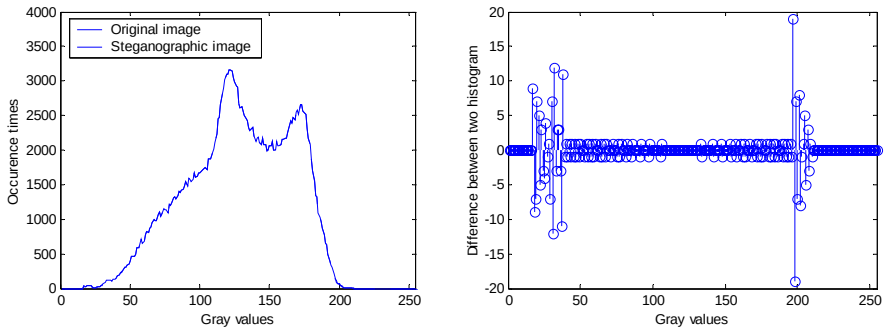
$$x_t = \begin{cases} 0 & \text{if } x_t < 0 \\ h_t & \text{if } x_t > h_t \\ \text{int}(x_t) & \text{otherwise} \end{cases} \qquad t = 1, 2, \ldots, 254\,. \tag{21}$$

In this way, a steganographic scheme **x** is obtained which causes an approximate least histogram abnormality in the mean square error sense.

The above-described LHA algorithm can be summarized as a four-step process:

1. Pseudo-randomly scramble the bit stream to be embedded, and map each bit to one pixel in the host image.
2. Count the number of pixels at gray levels 0~255 which differ in LSBs from the corresponding secret bits to yield a vector **h**.
3. Calculate **x** corresponding to an approximate minimum $d$ from (20) and (21).
4. For each gray level $j$ ($j$ = 0, 1, …, 255), randomly select $x_j$ pixels among $h_j$ pixels, decrease them by 1, and increase the other ($h_j$–$x_j$) pixels by 1.

In this algorithm, although modification to the host pixels may affect the higher bit planes, the induced distortion to the host image is not increased compared to the simple LSB replacement technique. Extraction of the embedded information can still be accomplished by extracting the LSB plane as in the straight LSB method.




(a) (b)

**Fig. 3.** Histograms of the original image Baboon and the stego-image. (a) The two histograms are hardly distinguishable. (b) Difference between the two histograms in a boosted scale.

Fig.3(a) sketches histograms of an original test image Baboon sized 512×512 and the stego-image in which each pixel is used to carry one hidden bit by the proposed method. The two curves are almost identical as the difference due to steganographic embedding is extremely small. Fig.3(b) shows the histogram difference in an expanded scale.

### 3.2 Anti-steganalysis Performance

**Resistance Against $\chi^2$ Test.** With simple LSB replacement, the number of modified pixel is about 50% of the stego-bits, and the number of pixels with a gray value 2*i* becomes roughly the same as that of 2*i*+1. By using the LHA technique, however, the image histogram is preserved so that the signature detectable to the $\chi^2$ test is removed.

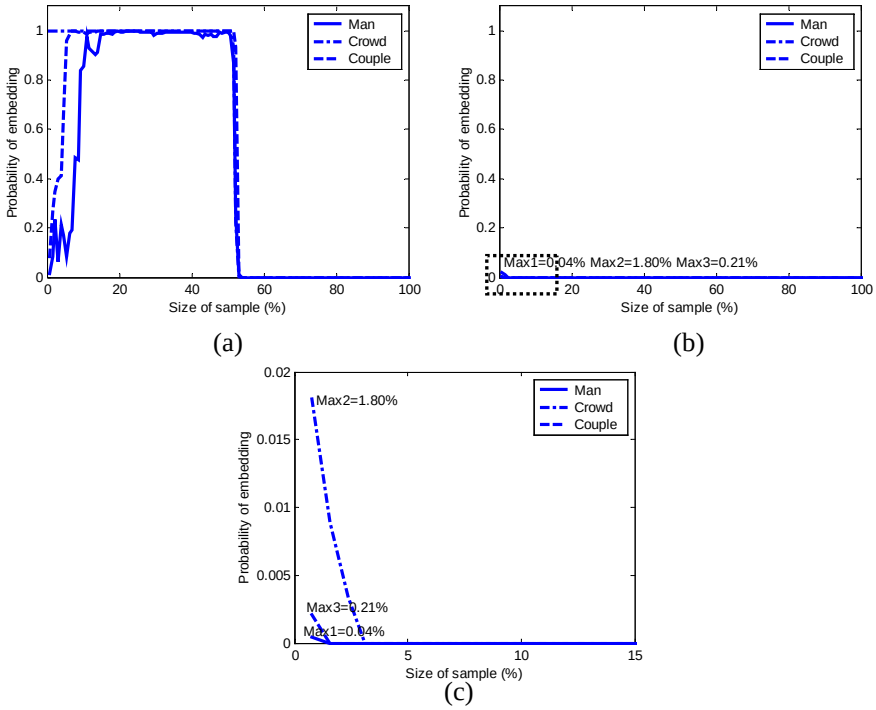



**Fig. 4.** Experimental results of $\chi^2$ test. (a) Simple LSB replacement steganography. (b) LHA approach. (c) Close-up of the bottom-left region in (b).

Results of the $\chi^2$ test on 3 stego-images (Man, Crowd, and Couple) using the LSB replacement and the LHA approach, respectively, are shown in Fig.4. The images are divided into top-left and bottom-right halves by the diagonal. Data were embedded into the top-left halves. The $\chi^2$ analysis started from the top-left corner, and the images were scanned in a zigzag fashion until the entire image was covered. Curves representing the *p* value as a function of pixel number covered in the test are shown in Fig.4(a). Because the top-left sections of the LSB plane were replaced with stego-data, the *p*-value was very close to 1. Fluctuation near the vertical axis is due to small sample sizes. The *p*-value dropped to nearly 0 as soon as the covered area exceeded 50%. As such, the length of stego-data and the embedded region can be estimated quite reliably. The results for the LHA method is given in Fig.4(b) where the *p*-value is always near 0. Fig.4(c) is a close-up view of the dotted box in 4(b). It is therefore verified that the LHA technique can effectively resist the $\chi^2$ test.

**Resistance Against the RS Analysis.** With the simple LSB replacement technique, only the mapping $F_1$ is applied to the LSBs that differ from the secret bits to be hidden. Changes of smoothness are different when $F_1$ and $F_{-1}$, respectively, are applied to part of the pixels in a stego-image so that $R_{-M} - S_{-M} > R_M - S_M$. When the test is carried out on a clean image, on the other hand, one has $R_M \approx R_{-M} > S_M \approx S_{-M}$.

With the LHA approach, on the other hand, both $F_1$ and $F_{-1}$ are applied. Therefore, changes of smoothness are very close when applying $F_1$ and $F_{-1}$, respectively, to the stego-image so that $R_M \approx R_{-M} > S_M \approx S_{-M}$ as in a clean image. In other words, the RS test can no longer distinguish a stego-image from a clean one.

Fig.5 shows the RS analysis results for a stego-image Baboon. When LSB replacement is used, the larger the payload, the greater is the difference between $(R_{-M} - S_{-M})$ and $(R_M - S_M)$. With LHA, however, $R_M \approx R_{-M} > S_M \approx S_{-M}$ always holds irrespective of the increasing payload. Fig.6 shows $R_{-M}$–$R_M$ from 100 stego-images using the straight LSB method and LHA techniques respectively, and from 100 *clean* images. Clearly, RS analysis is effective for the straight LSB method, but invalid for LHA.

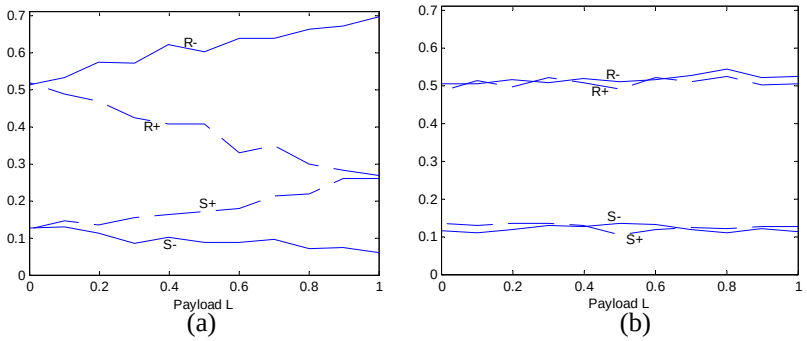



**Fig. 5.** RS analysis of the stego-image Baboon. (a) Using the simple LSB replacement technique. (b) Using the LHA technique.

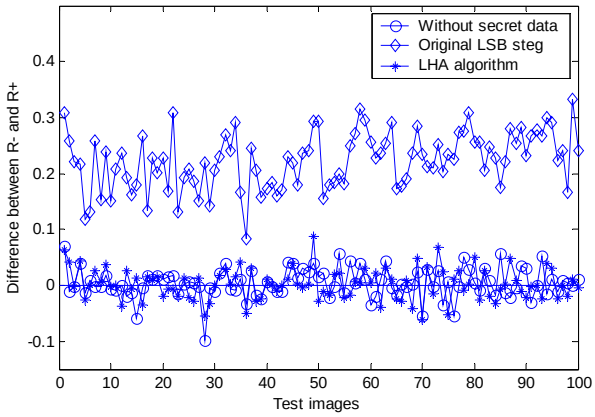



**Fig. 6.** Values of $R_{-M}$–$R_M$ calculated from 100 stego-images by using the LSB-replacement method and the LHA techniques, and from the same 100 images without secret data.

**Resistance against the GPC Analysis.** Because the mapping $F_{-1}$ is also used, both $N_O$ and $N_E$ are increased due to data embedding, and distribution of $R$ remains centered around $R$=1 as shown in Fig.7, where the solid and dashed lines represent the distributions of $R$ of the original and the stego-images generated with the LHA approach, respectively. Therefore, it is impossible to distinguish a stego-image from a clean image based on the parameter $R$.

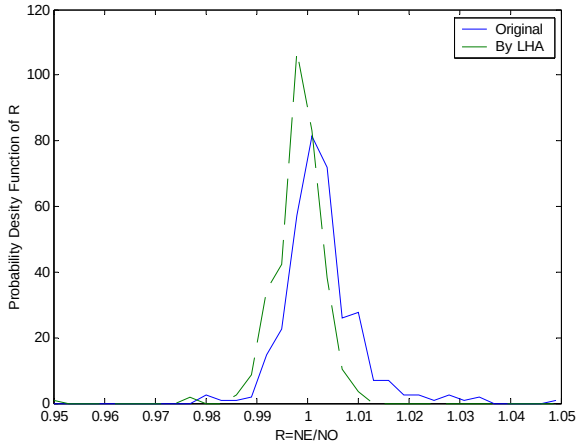



**Fig. 7.** Distributions of $R$ of original images and that of LHA based stego-images.

### 3.3 Application of LHA to Transform Domain Embedding

Digital images are often stored in the JPEG format as quantized DCT coefficients. In this case, secret data can also be embedded to the LSB of quantized coefficients. But images in the JPEG format have a property that the coefficient's occurrence frequency decreases with increasing magnitude, and the data insertion must not change this feature. To hide data in JPEG images, F5 has been proposed [11], which is developed from its predecessors F3 and F4 using a *matrix encoding* technique.

In F3, nonzero coefficients are used, whose magnitudes are decremented by 1 when the LSB does not match. This is for keeping the above-mentioned features and preventing the occurrence frequencies of $2i$ and $2i$+1 from being close to each other, a signature detectable by $\chi^2$ test. However, since the magnitude decrements generate 0s from the original +1 or –1, the receiver is unable to distinguish a steganographic 0 from an original 0, and the data-hider must repeatedly embed the affected bits when zeros are produced. Thus, F3 produces more even coefficients than odd ones resulting in an abnormal histogram, therefore becomes vulnerable to steganalysis.

F4 overcomes the above drawback by making both even negative and odd positive coefficients represent a stego-one, and odd negative and even positive represent a stego-zero. F5 is a combination of F4 and matrix encoding, which embeds $m$ bits into $2^m$–1 coefficients using less than one LSB alteration to reduce distortion due to data embedding. But F5 causes a decrease of image energy because of the magnitude decrement, or shrinkage of histogram. This may provide a clue for steganalysis [10].

By using the LHA approach, a coefficient equal to $j$ is changed to either $j$+1 or $j$–1 when it differs from a corresponding hidden bit, where both even negative and odd positive coefficients are also used to represent a stego-one, and odd negative and even positive with a stego-zero. There are two exceptions: a coefficient originally equal to –1 may be changed to –2 or 1, and an original +1 may be changed to –1 or +2. So, the magnitude and shape of the coefficient histogram is preserved when the LHA technique is used, and any steganalytic algorithm that explores abnormality in histogram can be defeated. Fig.8 shows the histograms of original quantized DCT coefficients and stego-coefficients of a compressed image Baboon with a quality factor 70. A secret bit was embedded into the (3,3) coefficient in every 8-by-8 block using F5 and LHA, respectively. It is clear that the LHA method keeps the histogram of transform coefficients unchanged whereas F5 causes detectable modifications.

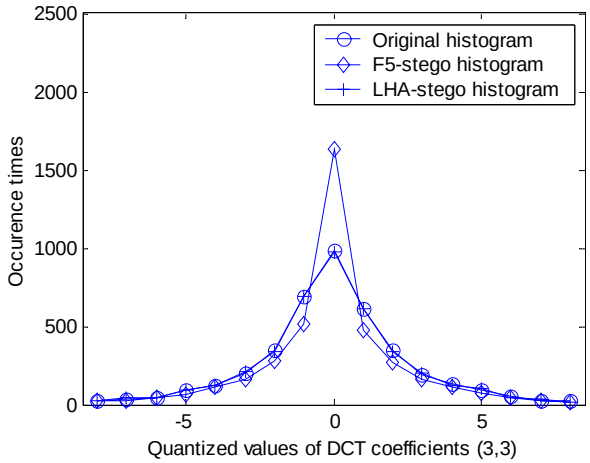



**Fig. 8.** Histograms of original quantized and stego-DCT coefficients with F5 and LHA.

## 4 Conclusion

In addition to the $\chi^2$ test and RS analysis, the presence of secret message based on LSB replacement can also be revealed by viewing the image as a 3D landscape and counting the numbers of crossings, $N_0$ and $N_1$, through two interleaved families of gray-level planes, $\mathbf{P}_O$ and $\mathbf{P}_E$. These two families may be referred to as odd and even gray-level planes. With an increasing amount of embedded information, $N_E$ rises whereas $N_O$ keeps unchanged. This leads to a new steganalytic method as named the GPC analysis in this paper.

All the three steganalytical methods make use of the asymmetry inherent in the procedure of conventional LSB embedding as only the mapping $F_1$ is used. In order to resist this type of attacks, a more balanced scheme is introduced in which both $F_1$ and $F_{-1}$ are used to preserve the image histogram so that some abnormal features are effectively avoided. Although modifications are no longer confined to the least significant bit plane, the new method does not introduce any additional visual distortion to the cover image. Extraction of the embedded data can still be accomplished by simply

extracting the LSBs of the stego-image. The proposed approach is also applicable to the LSB modification of transform domain coefficients, and a detectable signature of histogram shrinkage introduced by techniques such as F5 is avoided.

## Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 60072030) and Key Disciplinary Development Program of Shanghai (2001-44).

## References

1. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information Hiding — A Survey," *Proc. IEEE*, **87**, 1999: pp.1062 –1078.
2. J. Fridrich, and M. Goljan, "Practical Steganalysis of Digital Images — State of the Art," *Proceedings of SPIE*, Vol. **4675**, San Jose, USA, Jan. 2002, pp. 1–13.
3. H. Wang, and S. Wang, "Cyber Warfare — Steganography vs. Steganalysis," *Communication of the ACM* (in press).
4. A. Westfeld, and A. Pfitzmann, "Attacks on Steganographic Systems," *Lecture Notes in Computer Science*, vol.**1768**, 1999: pp.61–76.
5. N. Provos, and P. Honeyman, "Detecting Steganographic Content on the Internet," *CITI Technical Report 01–11*, 2001.
6. J. Fridrich, et al., "Detecting LSB Steganography in Color and Gray-Scale Images," *Magazine of IEEE Multimedia, Special Issue on Security*, Oct-Dec, 2001: pp. 22–28.
7. J. Fridrich, R. Du, and M. Long, "Steganalysis of LSB Encoding in Color Images," in *2000 IEEE Int. Conf. on Multimedia and Expo*, vol.**3**, 2000: pp.1279–1282.
8. J. Fridrich, M. Goljan, and R. Du, "Steganalysis Based on JPEG Compatibility," *Proceedings of SPIE*, Vol. **4518**, 2001: pp. 275-280.
9. J. Fridrich, M. Goljan, and D. Hogea, "Attacking the OutGuess," in *Proc. of the ACM Workshop on Multimedia and Security 2002*, Juan-les-Pins, France, December 6, 2002.
10. J. Fridrich, et al., "Steganalysis of JPEG Image: Breaking the F5 Algorithm," in *5th International Workshop on Information Hiding*, Noordwijkerhout, Netherlands, Oct. 2002.
11. A. Westfeld, "F5 — A Steganographic Algorithm," *Lecture Notes in Computer Science*, vol.**2137**, 2001: pp.289–302.
12. S. Lyu, and H. Farid, "Detecting Hidden Message Using Higher-Order Statistics and Support Vector Machines," in *5th International Workshop on Information Hiding*, Noordwijkerhout, The Netherlands, 7–9 October 2002.
13. J. Ettinger, "Steganalysis and Game Equilibria," *Lecture Notes in Computer Science*, vol.**1525**, 1998: pp.319–328.
14. N. Provos, "Defending against Statistical Steganalysis," in *10th USENIX Security Symposium*, Washington, DC, 2001.
15. S. Wang, X. Zhang, and K. Zhang, "Steganographic Technique Capable of Withstanding RQP Analysis," *Journal of Shanghai University*, **6**, 2002: pp. 273–277.