STEGANALYSIS OF LSB GREEDY EMBEDDING ALGORITHM FOR JPEG IMAGES USING COEFFICIENT SYMMETRY

*Bin Li, Fangjun Huang, Jiwu Huang**

Guangdong Key Laboratory of Information Security Technology
Sun Yat-sen University, Guangzhou, China, 510275

ABSTRACT

A recently developed LSB greedy embedding algorithm for JPEG images is capable of resisting the chi-square attack. By carefully studying the quantized DCT (discrete cosine transform) coefficients of the cover and stego images, we find that the embedding algorithm does not preserve the histogram of the DCT coefficients well. In this paper, we define a new chi-square statistic which is used to measure whether the image under scrutiny is like the cover or the stego. Our proposed steganalytic method is based on the symmetry property of the DCT coefficients in JPEG images. It can also be used in the scenario where the cover images are double JPEG compressed. The reliability of this specific steganalytic scheme depends on the embedding rate and it is influenced by the JPEG quality factor. Experimental results show that when the embedding rate exceeds half of the maximal embedding capacity, the steganographic algorithm is detectable with a very low false negative rate, whatever the quality factor is.

Index Terms— Steganalysis, LSB Greedy Embedding, Chi-square Attack

1. INTRODUCTION

Steganography is the technique of embedding secret messages in cover media. By exploring the unusual statistical changes in stego objects, steganalysis aims to discover the presence of the invisible communication. An early steganographic method is the LSB (least significant bit) replacement, which hides messages by modifying the coefficients in spatial domain, such as the gray-scale values of bitmap images or the indices of palette images. It can also be used in transform domain, such as the quantized DCT coefficients of JPEG images. After observing that the frequencies of pairs of values become equal, Westfeld et al. developed the well known χ^2 (chi-square) attack [1] to reveal the existence of LSB replacement when the embedding was sequential. However, it is not effective for the randomly scattered embedding. Its improved versions, including the extended χ^2 attack [2] and the generalized χ^2 at-

tack [3], can compensate this weakness. More powerful specific steganalytic methods, including those in [4, 5, 6, 7], were designed to detect LSB steganography in spatial domain and some could be extended to transform domain. To foil the existing χ^2 attack, Duric et al. designed the LSB greedy embedding algorithm (LSB-GEA) [8] to mimic the chi-square statistic of JPEG coefficients, at a cost of the capacity decreasing by half.

In this paper, we find that although the LSB-GEA preserves the chi-square statistic well, it makes the histogram of the DCT coefficients more undulated and less symmetric. With the help of the coefficient symmetry property in JPEG images, a newly defined chi-square statistic is used to detect the steganographic algorithm. It is also robust to double compressed JPEG images.

The rest of this paper is organized as follows. Section 2 briefly reviews the χ^2 attack and its countermeasure, LSB-GEA. Our steganalytic method is described in Section 3 and followed with experimental results. We summarize our work in Section 4.

2. CHI-SQUARE ATTACK AND LSB GREEDY EMBEDDING ALGORITHM

2.1. Chi-square Statistic and χ^2 Attack

The χ^2 attack developed by Westfeld et al. [1] is a goodness-of-fit measure to analyze the degree of similarity between the observed sample distribution and the theoretically expected distribution of the LSB replaced stego image. As in [8], a conjugate pair is used to describe two coefficients whose binary representation is identical except for their LSBs. Since "0" and "1" are equally distributed in encrypted or compressed message bitstream for embedding, overwriting the LSBs of the cover image makes the coefficients in the same conjugate pair flip into each other, and their occurrences tend to be equalized. In other words, the expected frequency of each coefficient in stego image is close to the arithmetic mean of the two frequencies in a conjugate pair. Let h_i be the histogram of the coefficients and assume that we have a total number of k conjugate pairs. The chi-square statistic with $k-1$ degrees
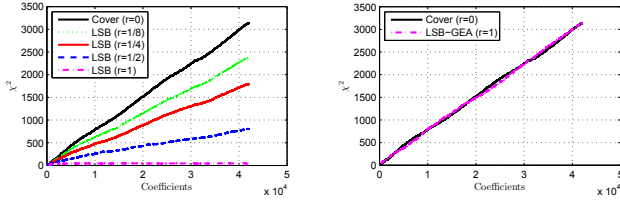
(a) χ^2 computed before and after LSB replacement. The curves from top to bottom correspond to the cover image, the stego images with embedding rate of 1/8, 1/4, 1/2 and 1.

(b) χ^2 computed before and after LSB-GEA fully embedding. The curves are almost overlapped.

Fig. 1. Relation between χ^2 and the amount of coefficients

of freedom for detecting the LSB replacement is defined as

$$\chi^2 = \sum_{i=1}^{k} \frac{(h_{2i} - \frac{h_{2i}+h_{2i+1}}{2})^2}{\frac{h_{2i}+h_{2i+1}}{2}} = \frac{1}{2}\sum_{i=1}^{k} \frac{(h_{2i} - h_{2i+1})^2}{h_{2i} + h_{2i+1}} \quad (1)$$

The probability of embedding is given by

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})} \int_0^{\chi^2} e^{-\frac{t}{2}} t^{\frac{k-1}{2}-1} \mathrm{d}t \quad (2)$$

where Γ is Euler-Gamma function.

2.2. Description of LSB Greedy Embedding Algorithm

In [8], Duric et al. pointed out that the value of χ^2 was related to the amount of coefficients. For cover images, the value of χ^2 increases with the amount of coefficients. However, the LSB replacement lowers the value of χ^2 generally. The more secret message bits to be embedded, the more the slope decreases. The relation between the embedding rate and the value of χ^2 is illustrated in Fig. 1(a). Here the embedding rate r is defined as the ratio of the actual length of an embedded message to the maximal capacity of a cover medium.

In order to preserve the trend of the increasing chi-square statistic along with the amount of coefficients, Duric et al. presented the LSB greedy embedding algorithm. The embedding process for JPEG images consists of the following steps [8]:

1. Denote the N-bit binary message as $M = (m_1, m_2, ..., m_N)$. Get a quantized DCT AC coefficient sequence $B = (b_1, b_2, b_3, b_4, ..., b_{2N-1}, b_{2N})$ from the input JPEG image, where $b_i \neq 0, b_i \neq 1, i \in \{1, 2, ..., N\}$. The order of the coefficients in the sequence may depend on a private key shared between the sender and receiver.

2. Define $x \odot j$ as the operation of replacing the LSB of x by j, where $j \in \{0, 1\}$. For $m_i, i \in \{1, 2, ..., N\}$, a pair of coefficients, denoted as (b_{2i-1}, b_{2i}), are used for embedding one message bit. And the altered coefficients are denoted as (b^*_{2i-1}, b^*_{2i}).

3. If $m_i = 0$, let $b'_{2i-1} = b_{2i-1} \odot 0$, $b'_{2i} = b_{2i} \odot 0$, $b''_{2i-1} = b_{2i-1} \odot 1$ and $b''_{2i} = b_{2i} \odot 1$. If $m_i = 1$, let $b'_{2i-1} = b_{2i-1} \odot 0$, $b'_{2i} = b_{2i} \odot 1$, $b''_{2i-1} = b_{2i-1} \odot 1$ and $b''_{2i} = b_{2i} \odot 0$.

4. Compute the chi-square statistic $\chi^2(B_i)$, $\chi^2(B_i^1)$ and $\chi^2(B_i^2)$ for $B_i = (b_1, b_2, b_3, b_4, ..., b_{2i-1}, b_{2i})$, $B_i^1 = (b^*_1, b^*_2, b^*_3, b^*_4, ..., b'_{2i-1}, b'_{2i})$ and $B_i^2 = (b^*_1, b^*_2, b^*_3, b^*_4, ..., b''_{2i-1}, b''_{2i})$, respectively.

5. If $|\chi^2(B_i) - \chi^2(B_i^1)| < |\chi^2(B_i) - \chi^2(B_i^2)|$, let $b^*_{2i-1} = b'_{2i-1}$ and $b^*_{2i} = b'_{2i}$. Else let $b^*_{2i-1} = b''_{2i-1}$ and $b^*_{2i} = b''_{2i}$.

6. Repeat Step 3 to 5 until all N message bits are embedded.

The extraction procedure is quite easy. Get $2N$ quantized DCT AC coefficients in the same way as embedding. If the LSBs of (b^*_{2i-1}, b^*_{2i}) are $(0, 0)$ or $(1, 1)$, the retrieved i-th message bit is determined to be "0". Otherwise, it is determined to be "1".

Although the maximum embedding capacity of LSB-GEA is half of the Jsteg [9], it ensure that the chi-square statistic of the altered coefficients will match the original chi-square statistic as best as possible. The chi-square statistics of the cover image and the stego image are compared in Fig. 1(b).

3. PROPOSED STEGANALYTIC METHOD USING COEFFICIENTS SYMMETRY

3.1. Steganalysis of LSB Greedy Embedding Algorithm

LSB-GEA mimics the local chi-square statistic $\chi^2(B_i)$ step by step so that the global chi-square statistic $\chi^2(B)$ is well preserved. However, by carefully observing the histograms of the quantized DCT coefficients shown in Fig. 2, we can find the difference between the cover image and the stego image. For the cover image, the histogram of the DCT AC coefficients resembles a Laplacian distribution, in which the following two characteristic properties hold.

i. The distribution is symmetric around zero.

ii. The frequency of occurrence decreases with the increasing absolute value.

The histogram of the stego image breaks both of these properties. In LSB-GEA, the unbalance of frequency in a conjugate pair is guaranteed, however, in an arbitrary way. As a result, the embedding without consideration of the above properties makes the histogram of the stego image undulated.

Since double compressed JPEG (double-JPEG) images are possible candidates for cover media, we take them into consideration too. Double-JPEG images refer to those images successively being compressed twice into JPEG with different quality factors. The histograms of the DCT coefficients of a double-JPEG image before and after LSB-GEA embedding
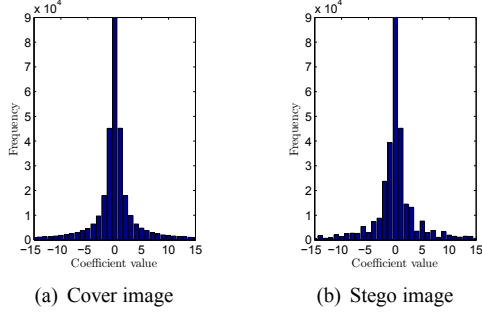
(a) Cover image   (b) Stego image

Fig. 2. Histogram of AC coefficients of a JPEG image before (a) and after (b) LSB-GEA fully embedding
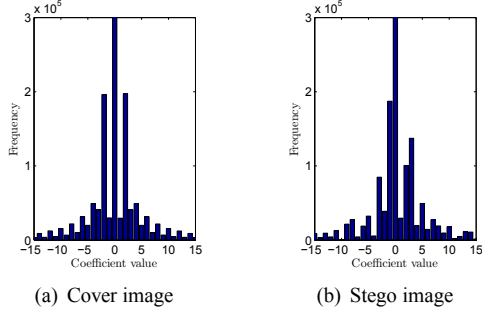

(a) Cover image   (b) Stego image

Fig. 3. Histogram of AC coefficients of a double-JPEG image before (a) and after (b) LSB-GEA fully embedding

are shown in Fig. 3. We can see the histogram of the double-JPEG cover image follows the first property but it is against the second one. Therefore, only the property of symmetry is applied in our proposed steganalytic scheme to detect LSB-GEA.

We define the symmetric pair as the pair of coefficients having the same absolute value but different in signs. Let h_i be the frequency of occurrence of coefficient i in the histogram. In the cover image, h_i and h_{-i} are very close, hence their frequencies are close to the arithmetic mean of their frequencies. We construct the following new chi-square statistic:

$$\hat{\chi}^2 = \sum_{i \in I} \frac{(h_i - \frac{h_i + h_{-i}}{2})^2}{\frac{h_i + h_{-i}}{2}} = \frac{1}{2} \sum_{i \in I} \frac{(h_i - h_{-i})^2}{h_i + h_{-i}} \quad (3)$$

where $I = \{i | i > 0, \frac{h_i + h_{-i}}{2} \geq 5\}$. The value of this statistic is capable of revealing the fact that if the histogram is symmetric. Increasing embedding rate will enlarge the difference between h_i and h_{-i}, hence $\hat{\chi}^2$ grows. In contrary to the chi-square statistic previously defined in (1) which is used to measure how likely the observed coefficient samples are from a stego, we applied the newly defined chi-square statistic to measure how likely the observed coefficient samples are from a cover. Similar to (2), the probability of being a cover

Table 1. Mean of $\hat{p}_s$ of 1338 single compressed JPEG images

r	QF=75	QF=80	QF=85	QF=90	QF=95
r=0	0.16	0.14	0.11	0.08	0.05
r=0.1	0.24	0.21	0.18	0.13	0.08
r=0.2	0.40	0.37	0.34	0.29	0.19
r=0.3	0.66	0.63	0.62	0.59	0.51
r=0.4	0.88	0.88	0.88	0.90	0.89
r=0.5	0.99	0.99	0.99	0.99	0.99
r=0.6	1.00	1.00	1.00	1.00	1.00
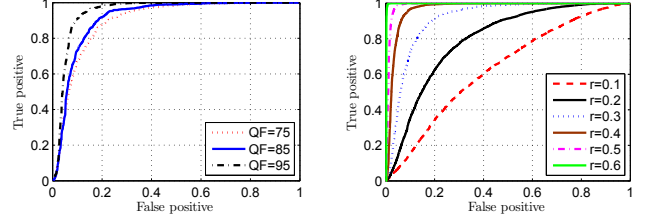
(a) ROC curves for images under a specific QF with embedding rate of 0.3

(b) ROC curves for images under a variety of QFs with embedding rate varying from 0.1 to 0.6

Fig. 4. ROC curves for single compressed JPEG images

image is given by

$$\hat{p}_c = 1 - \frac{1}{2^{\frac{k-1}{2}} \Gamma(\frac{k-1}{2})} \int_0^{\hat{\chi}^2} e^{-\frac{t}{2}} t^{\frac{k-1}{2}-1} dt \quad (4)$$

where $k = |I|$, the amount of symmetric pairs we use. Thus, the probability of being a stego image is given by

$$\hat{p}_s = 1 - \hat{p}_c \quad (5)$$

3.2. Experimental Results

In our experiment, 1338 TIFF images from UCID [10] are compressed with different quality factors (QFs) ranging from 75 to 95 to obtain the single compressed JPEG cover images. We observe that the QF has impact on the performance of our method. Table 1 displays the mean of $\hat{p}_s$ of images with different embedding rates r under different QFs. With the same QF, $\hat{p}_s$ monotonically increases with the embedding rate. Ideally, the $\hat{p}_s$ of cover (r=0) should be close to 0. However, the cover images under a lower QF tend to have larger $\hat{p}_s$, indicating that they are less symmetric in the sense of our chi-square test. Therefore, given a false positive rate, we can predefine a threshold value Th ($0 \leq Th \leq 1$) for each QF. The threshold value for a specific QF can be determined by computing the $\hat{p}_s$ of a large number of cover images. If the $\hat{p}_s$ of a testing image is larger than the Th, we consider it as a stego. For example, we experimentally compute Th=0.057 for QF=95 and Th=0.240 for QF=75 given a false positive rate of 20%. In this case, the false negative rate is 1% and 12.9% for QF=95 and QF=75 when the embedding rate is 0.3. If we change the

Table 2. Mean of $\hat{p}_s$ of 1338 double-JPEG images

r	QF=75	QF=80	QF=85	QF=90	QF=95
r=0	0.18	0.19	0.19	0.23	0.22
r=0.1	0.39	0.49	0.58	0.59	0.39
r=0.2	0.58	0.64	0.74	0.79	0.68
r=0.3	0.78	0.83	0.88	0.92	0.91
r=0.4	0.93	0.95	0.97	0.98	0.99
r=0.5	0.99	0.99	1.00	1.00	1.00
r=0.6	1.00	1.00	1.00	1.00	1.00
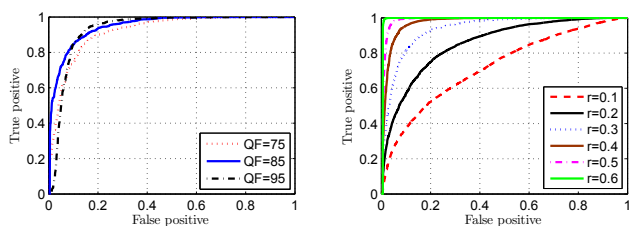
(a) ROC curves for images under a specific QF with embedding rate of 0.3

(b) ROC curves for images under a variety of QFs with embedding rate varying from 0.1 to 0.6

Fig. 5. ROC curves for double compressed JPEG images

Th, an ROC (receiver operating characteristic) curve can be derived. Figure 4(a) shows the ROC curves for QF=75, 85 and 95 when r=0.3. If we set a global threshold value without considering the QF, the detection result is still acceptable, as it is demonstrated in Fig. 4(b). In this case, the QFs of the cover images are randomly selected from 75 to 95, and the corresponding stego images are generated with different embedding rate. When the embedding rate exceeds 0.5, no matter what the QF is, the false negative rate is extremely low.

We also select double-JPEG images as cover and the results are illustrated in Table 2 and Fig. 5. The double-JPEG cover images are initially compressed with a first QF uniformly selected from 50 to 100 and then re-compressed with a second QF of 75 to 95 respectively. Although the coefficients of the double-JPEG cover images with a higher second QF are less symmetric, due to the fact that the first QFs are smaller in most of the cases, we can derive a similar detection reliability as the case of the single compressed JPEG images.

4. CONCLUSIONS

In this paper, we take a close look on the LSB greedy embedding algorithm. The LSB-GEA may be applied in spatial domain without noticing major difference in histogram. But for JPEG images, it is not a good choice. Considering the symmetry property of DCT coefficients, we define a new chi-square statistic, based on which a simple steganalytic method is presented to attack the LSB-GEA. The extracted feature is monotonically changed with the embedding rate. We also

consider the case of double-JPEG images. Experimental results show that the method is effective for the single as well as the double compressed JPEG images especially when the embedding rate exceeds 0.5. Moreover, the symmetry feature may also be hopeful to be incorporated into the universal JPEG steganalytic scheme, such as [11], to enhance its performance. It will be involved in our future work.

5. REFERENCES

[1] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in Proc. of *3rd International Workshop on Information Hiding*, LNCS 1768, pp. 61–76, Springer-Verlag, 2000.

[2] N. Provos and P. Honeyman, "Defending against statistical steganalysis," in *10th USENIX Security Symposium*, Washington, DC, USA, Auguest 2001.

[3] A. Westfeld, "Detecting low embedding rates," in Proc. of *5th International Workshop on Information Hiding*, LNCS 2578, pp. 324–339, Springer-Verlag, 2003.

[4] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, 2001.

[5] S. Dumitrescu, Xiaolin Wu, and Zhe Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Tran. on Signal Processing*, vol. 51, no. 7, pp. 1995–2007, 2003.

[6] T. Zhang and X. Ping, "Reliable detection of LSB steganography based on the difference image histogram," in Proc. of *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, vol. 3, pp. 545–548, 2003.

[7] K. Sullivan, O. Dabeer, U. Madhow, B.S. Manjunath, and S. Chandrasekaran, "LLRT based detection of LSB hiding," in Proc. of *IEEE Int. Conf. on Image Processing*, vol. 1, pp. 497–500, 2003.

[8] Z. Duric, D. Richards, and Y. Kim, "Minimizing the statistical impact of LSB steganography," in Proc. of *Second Int. Conf. on Image Analysis and Recognition*, LNCS 3656, pp. 1175–1183, Springer-Verlag, 2005.

[9] D. Upham, "Jsteg v4," Software available at http://www.nic.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz.

[10] G. Schaefer and M. Stich, "UCID – An uncompressed colour image database", in Proc. of *SPIE, Storage and Retrieval Methods and Applications for Multimedia*, pp. 472–480, San Jose, USA, 2004.

[11] J. Fridrich, "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes," in Proc. of *6th International Workshop on Information Hiding*, LNCS 3200, pp. 67–81, Springer-Verlag, 2004.