Passive Steganalysis Evaluation: Reliabilities of Modern Quantitative Steganalysis Algorithms

N. Prokhozhev, O. Mikhailichenko, A. Sivachev, D. Bashmakov and A. Korobeynikov

Abstract This paper presents initial results from experiments which perform statistically accurate evaluation of the reliability of modern quantitative statistical steganalysis algorithms. The focus here is on the algorithms for detection of simple LSB steganography in grayscale images. The following algorithms were evaluated: RS- analysis, Sample pair analysis, Difference image histogram, Triples analysis, Weighted stego-image. ROC curves were obtained as a result the reliability of image steganalysis algorithms. We also describe some of the questions for a general methodology of evaluation of steganalysis algorithms and potential pitfalls caused by the differences of image resolution.

Keywords Statistical steganalysis · LSB steganography · Regular-singular steganalysis · Difference histogram steganalysis · Triplet steganalysis

N. Prokhozhev · O. Mikhailichenko · A. Sivachev (✉) · D. Bashmakov · A. Korobeynikov
ITMO Univercity, Kronverksky Pr. 49, 197101 Saint Petersburg, Russia
e-mail: avsivachev@corp.ifmo.ru; sivachev239@mail.ru
URL: http://en.ifmo.ru

N. Prokhozhev
e-mail: 144339@corp.ifmo.ru

O. Mikhailichenko
e-mail: 116198@corp.ifmo.ru

D. Bashmakov
e-mail: dabashmakov@corp.ifmo.ru

A. Korobeynikov
e-mail: 105929@niuitmo.ru

A. Abraham et al. (eds.), *Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'16)*, Advances in Intelligent Systems and Computing 451, DOI 10.1007/978-3-319-33816-3_9

1 Introduction

Nowadays steganography is widely used for hide information transferring and hidden messaging. Therefore, while solving problems of the informational security, steganography is being increasingly used by secret agencies, criminal groups and terroristic organizations.

One of the most widespread types of steganography containers is a digital image. Digital images make up a large percentage of the Internet data traffic allows using them as a channel for hidden information transfer with significant throughput and great secrecy.

There is a large number of free software for LSB image steganography. There are two relevant steganography resistance approaches: passive and active.

In the simplest case, the procedure of passive steganography resistance reduces to the problem of binary classification. A tested container should be classified as either original (clear) image or steganogram. It's a main goal quantitative steganalytic algorithms are widely used for. For digital images and LSB steganography, the result of algorithm execution is the estimate of the number of changed pixels in the tested image.

2 Purpose

The main purpose of this paper is the estimation of efficiency of modern steganographic algorithms when resisting LSB steganography with small payload rates. Results illustrate the lower bounds of payload, when the classification accuracy falls dramatically. In the case of such payloads the effective resistance is practically impossible. This lower bound can be used to determine the value of maximal throughput of steganography channel, considering existing abilities of passive resistance.

3 Method of Experiment

The tested image is being selected from a test set. Then LSB bit is being inverted for a fixed number of pixels. In this way, the apply steganography effect is simulated. Payload is measured as a percentage of maximum value for the tested image. Maximum payload of the image is the total amount of pixels in the image. Payload varies in the range of 1−6 %, basing on the stated error of evaluated steganalytic algorithms, roughly estimated at 2 %. Modified image is being tested with steganalytic algorithm. The result of the estimation is a number of pixels affected with steganographic embedding.

The following steganalytic algorithms have been evaluated:

- RS-analysis (RS) [1];
- Sample pair analysis (SP) [2];

- Difference image histogram (DIH) [3];
- Triples analysis (TR) [4];
- Weighted stego-image (WSI) [5].

Test set consists of three grayscale image collections:

- Collection 1–3126 images with resolution from 392 × 550 to 5184 × 3456 [9];
- Collection 2–5214 images with resolution from 1339 × 1357 to 5100 × 4026 [10];
- Collection 3–30682 images with resolution from 700 × 500 to 1300 × 734 [11].

Collections are public and include a great number of images with wide range of characteristics and features.

The pixels' coordinates are pseudo-randomly selected, with uniform distribution.

4 Evaluation Procedure

As noted above, the procedure of passive steganography resistance reduces to the problem of binary classification. Then the classification sets are represented as

$$Y = \{-1, +1\}, \tag{1}$$

and classifier is represented as follows:

$$a(x) = sign[f(x, w) - w_0], \tag{2}$$

where x is a random object, $f(x, w)$ is a classifying function (steganalytic algorithm), w is a parameters vector (the amount of flipped pixels), w_0 is a threshold.

In this case, the steganalytic algorithm acts as a classifier, and the classification procedure is done by comparing result of algorithm execution and some threshold.

The distinction surface is defined as follow:

$$f(x, w) = w_0. \tag{3}$$

The choice of a threshold value w_0 is a difficult task, since it directly affects the probabilities of both true positive and false positive detection. Too small value may result in high probability of both false classifications. In practice, it will result in clear images classified as stego images. Too great value will enlarge the probability of false negative classification.

True positive classification rate (TPR) is defined as follows:

$$TPR(a, X^m) = \frac{\sum_{i=1}^{m}[a(x_i) = +1][y_i = +1]}{\sum_{i=1}^{m}[y_i = +1]}, \tag{4}$$

where

$$X^m = (x_1, \ldots x_m) \tag{5}$$

is a sample, $y_1, \ldots, y_m$ are classification sets of the sample.

False positive classification rate (FPR) is defined as follows:

$$FPR(a, X^m) = \frac{\sum_{i=1}^{m}[a(x_i) = +1][y_i = -1]}{\sum_{i=1}^{m}[y_i = -1]}. \tag{6}$$

The ratio of these two values affects classification quality, and, consequently, the practical efficiency of passive resistance. The ideal classifier has $TPR = 1$ and $FPR = 0$.

ROC curves illustrate the ratio, for greater clarity [6].

The set of ROC curves for different evaluated algorithms for the same experiment conditions sets makes possible the comparative evaluation of their efficiency.

5 Results

The graph shows ROC curves (Fig. 1) for all evaluated algorithms and the same ROC curves for different payload rates. The same experimental results for distinct image collections are stated in Table 1.

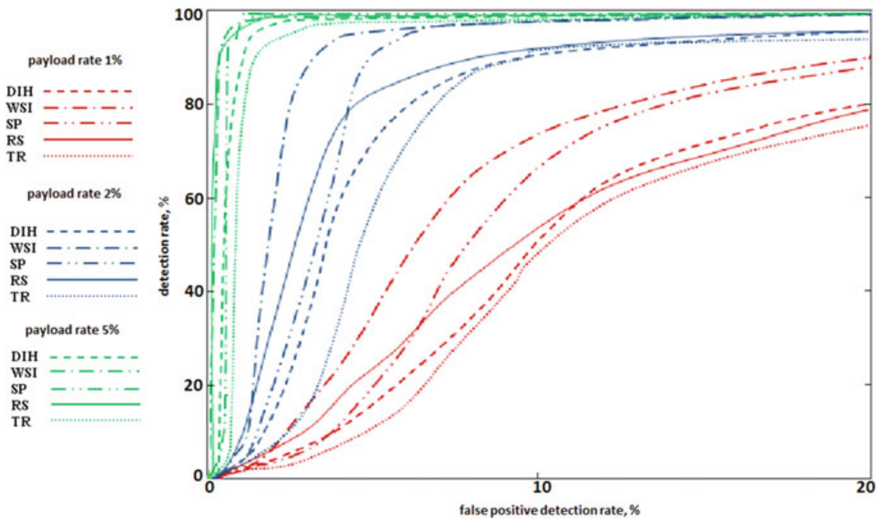

Fig. 1 ROC curves for the evaluated algorithms

Table 1 False positive rate for TPR at 97.5 %

Evaluated algorithm	Collection#	Payload, %				
		1	2	3	4	5
RS-analysis	1	48.1	30.0	7.1	2.1	0.7
	2	3.6	1.5	1.0	0.6	0.3
	3	49.7	32.7	8.3	3.6	1.9
Difference image histogram	1	42.4	33.4	8.0	2.9	1.5
	2	5.8	2.2	1.2	0.8	0.5
	3	44.9	23.5	18.2	7.8	4.6
Sample pair analysis	1	43.9	9.6	2.1	1.1	0.5
	2	5.2	1.8	1.1	0.7	0.3
	3	44.6	12.8	4.8	2.2	1.3
Triples analysis	1	62.7	37.5	8.3	2.7	1.7
	2	4.4	1.9	1.4	1.0	0.7
	3	64.4	36.7	9.4	3.9	1.9
Weighted stego-image	1	36.7	7.1	1.8	0.7	0.5
	2	2.6	0.9	0.5	0.4	0.1
	3	38.3	8.8	2.4	1.1	0.7

6 Findings

Modern quantitative statistical steganalytic algorithms show close accuracy of estimation. Passive steganorgaphy resistance based of them provides comparable classification quality and makes their practical efficiency very similar.

The classification quality falls significantly for steganogram with payload rates, greater than 5 %.

The tested image resolution has significant impact on the classification quality. So, for the images of Collection 2, with resolution as minimum as 1339 × 1357, the false classification rate is almost 10 times less than for Collections 1 and 3, with minimal image resolutions of 392 × 550 and 700 × 500, respectively (see Table 1).

7 Conclusion

Steganalysis based on modern quantitative statistical steganalytic algorithms have an ability to provide effective passive LSB steganography resistance against steganograms with payload value greater than 5 %. Using payload value less than that threshold reduces passive resistance efficiency dramatically. The passive resistance is ineffective against LSB steganography with payload rate less than 1 % for the image with resolutions not exceeding the resolution of modern displays.

The small image with resolution 600 × 400 pixels, used as a stego image with payload rate of 1−2 % is practically undetectable by modern quantitative steganalytic algorithms. In the same time, such payload rate makes possible to embed 5−10 KB of data. Taking into account the possibility of preliminary compression of embedded data and the usage of matrix embedding [7], the evaluated algorithms need further improvements.

References

1. Fridrich, J., Goljan, M., Du, R.: Reliable detection of LSB Steganography in color and grayscale images, State University of New York, Binghamton, NY, USA
2. Lu, P., Luo, X., et. al.: An improved sample pairs method for detection of LSB embedding. In: Proceedings of the 6th Information Hiding Workshop. Springer LNCS, vol. 3200, pp. 116–128 (2004)
3. Zhang, T., Ping, X.: Reliable detection of LSB steganography based on the difference image histogram. In: Proceedings of the IEEE ICSAAP 2003, Part III, pp. 545–548 (2003)
4. Ker, A.D.: A general framework for structural steganalysis of LSB Replacement. In: Proceedings of the Information Hiding, pp. 296–311 (2005)
5. Ye, M., Liu, F., Yang, C., He, X.: Steganalysis based on weighted stego-image for lsb replacement steganography. In: Intelligent Information Hiding and Multimedia Signal Processing IIH-MSP '09, pp. 945–948 (2009)
6. Schaathun, H.G.: Machine learning in image steganalysis. Alesund University College, pp. 164–167 (2012)
7. Kim, Y., Duric, Z., Richards, D.: Modified matrix encoding technique for minimal distortion steganography. In: Proceedings of 8th International Workshop Information Hiding, vol. 4437, pp. 314−327, 10–12 Jul 2006