Steganalytic methods for the detection of histogram shifting data hiding schemes

Daniel Lerch-Hostalot
Universitat Oberta de Catalunya,
Internet Interdisciplinary Institute (IN3),
Estudis d'Informàtica, Multimèdia i Telecomunicació,
Rambla del Poblenou, 156,
08018 Barcelona, Catalonia, Spain,
Email: dlrech@uoc.edu

David Megías
Universitat Oberta de Catalunya,
Internet Interdisciplinary Institute (IN3),
Estudis d'Informàtica, Multimèdia i Telecomunicació,
Rambla del Poblenou, 156,
08018 Barcelona, Catalonia, Spain,
Email: dmegias@uoc.edu

***Abstract*—In this paper, several steganalytic techniques designed to detect the existence of hidden messages using histogram shifting schemes are presented. Firstly, three techniques to identify specific histogram shifting data hiding schemes, based on detectable visible alterations on the histogram or abnormal statistical distributions, are suggested. Afterwards, a general technique capable of detecting all the analyzed histogram shifting data hiding methods is suggested. This technique is based on the effect of histogram shifting methods on the "volatility" of the histogram of the difference image. The different behavior of volatility whenever new data are hidden makes it possible to identify stego and cover images.**

***Index Terms*—Communication security, steganalysis, steganography.**

I. Introduction

Data hiding [16] is a collection of techniques to embed secret data into digital media such that its existence becomes undetectable by some attacking party. Data hiding can be applied to secret communications, copyright protection, authentication of digital contents and other applications. The most common carriers used for data hiding are images because of their widespread use in the Internet.

To hide data into a cover image, pixel values are changed and image distortion occurs. Usually, the distortion due to data hiding is not reversible and the original image can not be recovered. However, there are techniques that have the ability to restore the original image. These techniques are known as reversible data hiding [14], [5], [8], [11], [3], [7], [9], [6].

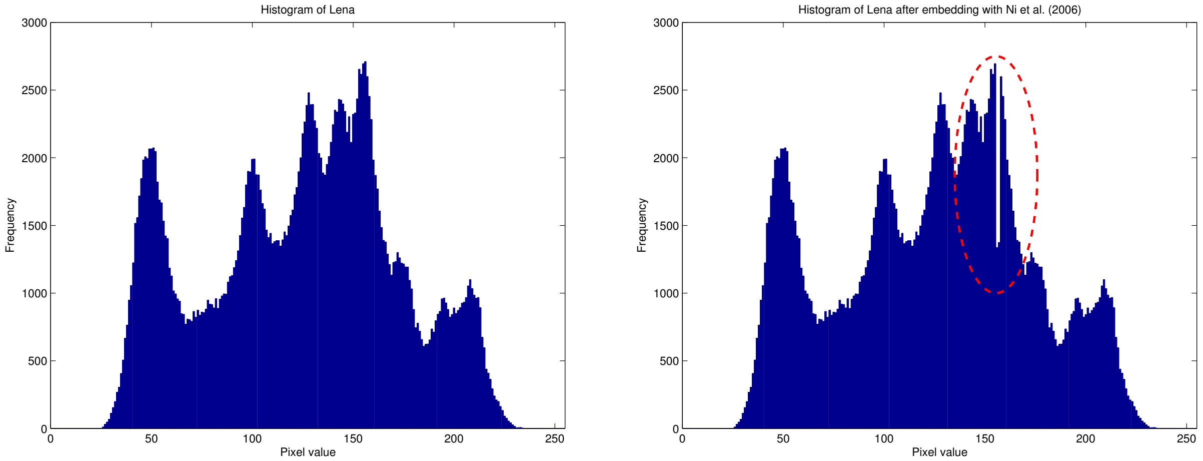
The simplest non-reversible data hiding method consists of modifying the least significant bit (LSB) of some (or all) pixel values, which is often referred to as LSB steganography. In [15], several attacks on LSB steganography are described. Later, in [4], the RS attack is introduced, which can reliably detect messages even for embedding capacities as low as 0.03 bits per pixel (bpp). In general, much work has been devoted to develop steganalytic tools for LSB steganography, LSB matching [12] or JPEG steganography [13], but little attention has been paid to other data hiding strategies, such as the histogram shifting methods analyzed in this paper.

A reversible data hiding method based on histogram shifting was proposed in [11]. This scheme uses the information about peaks and zeros of the histogram of the cover image to perform a partial shift, leaving a gap to hide data. In the Ni *et al.*'s method [11], the embedded secret data cannot be recovered when the knowledge of peak and zero point of histogram are not transmitted to the receiver. In order to overcome the above drawback, Hwang *et al.* [7] proposed a robust reversible data hiding scheme based on the histogram shifting method. This new approach proposes the use of a location map to store the information needed to reverse the process when the minimum point of histogram is non-zero.

Later, in [5], Hong *et al.* presented a scheme which performs a shift of the histogram of prediction errors. This method is based on [11], but has greater capacity. In their paper, Hong *et al.* use the median edge detector (MED) to predict pixel values (as detailed in Section II-C). Since the histogram of prediction errors is sharply centered at zero, we can use the concept of histogram shifting to hide information without determining the peak and zero points, unlike Ni *et al.*'s method. Although the histogram shifting technique is commonly used in reversible data hiding, several methods have recently emerged and are used as non-reversible ones [10].

There is some work on steganalysis applied to histogram shifting methods. Particularly, a few of them perform the detection based on changes in the shape of the histogram. In [14], a technique to attack the method based on shifting the histogram of the difference image of [9] is presented. This technique is based on detecting an unusual shape in the histogram, similar to the attack we present in Section II-A. However, this technique is not applicable to [11]. In [8], a technique to attack the method of [7] is presented. As in the previous case, this technique is based on finding an unusual shape in the histogram but, again, it is not applicable to the histogram shifting method of [11]. In both cases, this irregularity affects seven of the histogram bins. Therefore, it hardly ever occurs in cover (unmarked) images. In [11], the irregularity affects only four bins, making it harder to detect.

This paper presents different steganalytic tools which can be used to detect histogram shifting steganography for Ni *et al.*'s method [11], Mohsenzadeh *et al.*'s method [10] and different histogram shifting of prediction errors techniques, such as that



(a) Histogram of the original Lena image

(b) Histogram of the Lena image marked with [11]

Fig. 1: Histogram comparison

of [5]. In addition, the concept of the "volatility" of a histogram of prediction errors is introduced, and the measurement of this volatility before and after random embedding is shown to be effective to detect all the above histogram shifting data hiding schemes with a significantly high accuracy.

The rest of the paper is organized as follows. Section II proposes four steganalytic techniques. Three of these techniques are specific for particular data hiding schemes, whereas the fourth one is generic and can be applied to any of them. Section III shows the experimental results obtained with the different specific techniques and the generic one. Finally, Section IV draws the conclusions and outlines some guidelines for future research.

II. Proposed Steganalytic Methods

In this section, we present four steganalytic techniques. The first method detects Ni *et al.*'s scheme [11] by finding anomalies in the histogram of pixel intensities. The second steganalytic technique detects Mohsenzadeh *et al.*'s [10] method by searching for an unusual statistical distribution introduced by the embedding algorithm. The third steganalytic technique detects Histogram Shifting of Prediction Errors (HSPE) methods [5] studying the "volatility" of the histogram. Finally, the fourth technique extends the third one to create a generic method which can be applied to detect all of the above.

A. Ni et al.*'s Method*

In 2006, Ni *et al.* [11] presented a reversible data hiding method which consists in shifting the histogram of the image in order to create a gap to hide secret data. Their method uses a simple but effective algorithm:

Procedure 1 (Ni et al.*'s method [11]):*

1) Find the maximum (or peak) of the histogram, which corresponds to a pixel value P, and then find a zero to the right of P, which corresponds to the pixel value Z.
2) Shift the histogram to the right, from the peak to the zero point. To do this, all the pixels of the image with values between $P+1$ and $Z-1$ (included) are increased by 1.
3) To embed the message, it is necessary to scan the entire image looking for all the pixels with value P. These pixels are replaced by $P+1$ to embed '1', or keep the same value (P) to embed '0'.

In Fig.1, we can see the histogram of pixel intensities for the grayscale Lena image with 512×512 pixels [2], before and after data have been hidden with the method described in Procedure 1 [11]. If we compare the original histogram with the histogram of the marked image, there is a visible notch caused by histogram shifting and data hiding, as highlighted in Fig.1(b) with a dashed ellipse.

The abnormal shape in the histogram of the marked image can be detected with some reliability by applying the following observations. Let h_i, h_{i+1}, h_{i+2} and h_{i+3} be four consecutive bins of the histogram, then a peak replacement in h_{i+1} can be detected as follows:

1) $h_{i+1} + h_{i+2}$ is greater that any bin of the histogram,
2) h_{i+1} and h_{i+2} are approximately equal and
3) h_i or h_{i+3} are not much smaller than $h_{i+1} + h_{i+2}$.

The last two conditions require some thresholds as detailed in Section III.

B. Mohsenzadeh et al.*'s Method*

In 2009, Mohsenzadeh *et al.* [10] presented a steganographic method which is able to thwart histogram based steganalysis. Their method uses histogram shifting techniques to hide non-reversible data with the following algorithm.

Procedure 2 (Mohsenzadeh et al.*'s method [10], Alg. 1):*

1) Find the maximum bin (or peak) of the histogram, which corresponds to a pixel value P, and then find the first

zero to the left (Z_l) and the first zero to the right (Z_r) of the peak.

2) Shift the histogram to the right, from $P+1$ to Z_r-1, and do the same to the left from $P-1$ to Z_l+1. To do this, 1 is added to each pixel of the image with value between $P+1$ and Z_r-1 and 1 is subtracted from each pixel between $P-1$ and Z_l+1 .
3) To embed the message, it is necessary to scan the entire image in zigzag order looking for all pixels $I_{\text{zig}}(i)$ with values $P+2$ or $P-2$. To embed '0', set $I_{\text{zig}}(i-1) := P{+}1$ (or $P{-}1$) and, to embed '1', set $I_{\text{zig}}(i{+}1) := P{+}1$ (or $P-1$).

Mohsenzadeh *et al.* [10] present a second algorithm that uses a secret key to randomize the position of the modified pixels. For each selected pixel (with value $P+2$ or $P-2$), the message bit is embedded in one of its eight neighboring pixels, rather than using the neighbors in zigzag order as done in Algorithm 1. This variant is referred to as Algorithm 2.

Procedure 2 (or Algorithm 1 as defined in [10]) produces a significant statistical anomaly, since there is always a $P+1$ (or $P-1$) value next to $P+2$ (or $P-2$). For this reason, we can detect hidden data with this algorithm, counting those occurrences next to all the pixels (in a zigzag traversal of the image). If we consider each pixel of the image as a potential $P+2$ or $P-2$, we can check if this pixel has a $P+1$ or $P-1$ neighbor to its left or right (in zigzag order). If so, we can assume that P is a peak candidate and count this occurrence. Statistically, the maximum number of pixels that satisfy this constraint corresponds to the peak used to embed data. Therefore, if we draw a histogram with the frequency of pairs $(P+2, P+1)$ and $(P-2, P-1)$ counted for each peak candidate P, the highest bin corresponds to the true peak P. This is illustrated in Fig.2 for the Lena image, where the peak P occurs for the value 156. Note that this is not a standard histogram of the pixel intensities. Each pixel value is considered to be $P+2$ (or $P-2$) and, if $P+1$ (or $P-1$) occurs next to the pixel, then we increase the bin of P.

Apart for the highest frequency found for P, there is a detectable anomaly in this histogram since the bins of the values $P+1$, $P-1$, $P+2$ and $P-2$ decrease more than what is statistically expectable. We can also observe this fact in Fig.2. This provides a powerful mechanism for identifying stego images marked with this method, since we only have to verify that, given seven consecutive bins of this histogram: h_j for $j = i, i+1, \ldots, i+6$, the following conditions hold:

1) h_i and h_{i+6} are greater than h_{i+1}, h_{i+2}, h_{i+4} and h_{i+5} and
2) h_{i+3} is the greatest value of the histogram.

This technique, which does not require any threshold, is not applicable to Algorithm 2, due the randomized positions for the modified values $P+1$ and $P-1$.

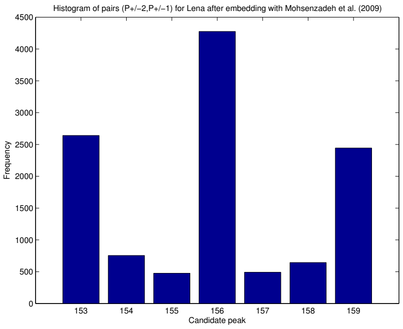


Fig. 2: Frequency of the candidate peaks P for the Lena image marked with [10]

C. Histogram Shifting of Prediction Errors Methods

Histogram Shifting of Prediction Errors (HSPE) methods were presented in [5]. There are many different HSPE data hiding methods and the most popular ones have been selected for the experiments presented in this paper. HSPE schemes obtain a histogram of the differences between the pixels values and a prediction p computed using some prediction equation. This histogram can be used to embed a message using techniques analogous to that of [11].

The alterations of histograms of prediction errors are more difficult to detect than those of pixel intensities, since histograms of prediction errors can be generated from different prediction formulas. However, neighboring pixels are often used for this prediction. For example, Hong et al. [5] use the median edge detector (MED) prediction to calculate the predicted value (p) of a pixel x:

$$p = \begin{cases} \min(b,c), & \text{if } a \geq \max(b,c), \\ \max(b,c), & \text{if } a \leq \min(b,c), \\ b+c-a, & \text{otherwise.} \end{cases}$$

where a, b and c are three neighbors of the pixel x, as shown in Fig.3(a).

a	b
c	x

(a) 2 × 2 adjacent pixels

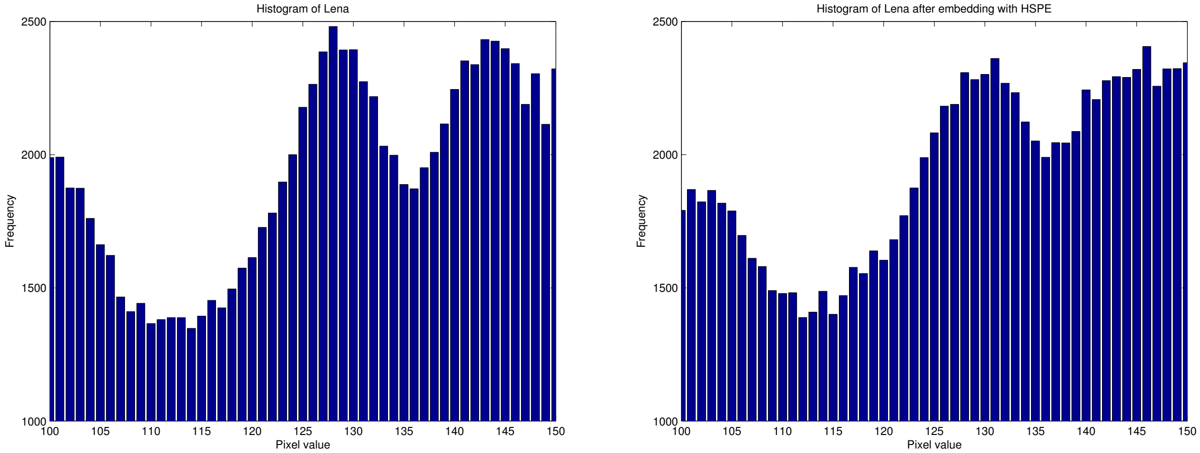
a	b	c
d	x	

(b) 2 × 3 adjacent pixels

Fig. 3: Pixel locations for prediction equations

There are simpler methods such as horizontal prediction: $p = c$, vertical prediction: $p = b$, diagonal prediction: $p = a$ and others even more sophisticated, such as a causal template prediction, like $p = \lfloor (a+b+c+d)/4 \rfloor$, where a, b, c and d are shown in Fig.3(b) with respect to the pixel x to be predicted and $\lfloor y \rfloor$ stands for the largest integer which is lower than or equal to y.

In this case, it is not possible to analyze the histogram of prediction errors directly, since the specific prediction formula will not be known (in general). Thus, It is necessary to take another approach. One of the common traits of HSPE methods is that they modify areas where the pixels are similar. When similar pixels are modified by adding one, these pixels will advance to the next bin of the histogram. As this occurs



(a) Histogram of the original Lena image

(b) Histogram of the Lena image marked with HSPE

Fig. 4: Histogram comparison before and after HSPE embedding

throughout the histogram, after shifting in the difference space, most bins give some of their pixels to their neighbors, producing a less volatile histogram. This situation is illustrated in Fig.4, where it can be seen that the frequencies of the histogram obtained after HSPE embedding are more similar to those of their neighbors. Therefore, the difference of a bin with respect to the preceding and the succeeding ones decreases in Fig.4(b) as compared to the original histogram shown in Fig.4(a). Although the difference from some bins to their neighbors may increase locally, the total difference from all bins to their neighbors decreases globally.

We can measure the volatility V of the histogram comparing the value of each bin h_i with its neighbors h_{i-1} and h_{i+1} as follows:

$$V = \sum_{i=1}^{254} \left| \frac{h_{i-1} + h_i + h_{i+1}}{3} - h_i \right| ,$$

which yields:

$$V = \sum_{i=1}^{254} \left| \frac{h_{i-1} - 2h_i + h_{i+1}}{3} \right| . \qquad (1)$$

Expression 1 is presented for clarity, but the following normalized expression has been used in the implementation of the methods:

$$V = \sum_{i=1}^{254} \frac{\max(\widetilde{h}_i, h_i) - \min(\widetilde{h}_i, h_i)}{\max(\widetilde{h}_i, h_i)}, \qquad (2)$$

where $\widetilde{h}_i = (h_{i-1} + h_i + h_{i+1})/3$. If $h_{i-1} = h_i = h_{i+1}$, the i-th bin is not included in the computation of V (since it contributes with 0 to the overall volatility).

The experiments show that the volatility of the image histogram of pixel intensities is significantly reduced when a message is embedded into a cover image. However, when it is embedded into a stego image, the volatility is reduced to a smaller extent. This behavior provides a detection mechanism: the volatility of the test image can be compared with the volatility after embedding a new message into it. If this process significantly reduces the volatility, the image is cover, otherwise it is stego. The new message is embedded by choosing a random binary mask with the same dimensions of the test image and adding it to the pixels values. This means that, on average, 50% of the pixel values are increased by 1, whereas the other 50% remains unchanged.

D. Generic Steganalytic Method

The detection technique presented in the previous section is useful because it exploits some common characteristics of different data hiding systems. However, it does not detect the methods introduced by Ni *et al.* [11] or Mohsenzadeh *et al.* [10]. The reason for this is that these schemes affect only a reduced group of values of the frequencies of the histogram, whereas some other frequencies are only shifted. Thus, it becomes necessary to use a different histogram for which most bins are affected by the different data hiding methods introduced above. We have found that a histogram of differences is suitable for this purpose if the following prediction equation is used:

$$p = \left\lfloor \frac{a + b + c}{3} \right\rfloor , \qquad (3)$$

where a, b and c are as shown in Fig.3(a). Once all such predictions are computed, a histogram based on the value of the differences $|x - p|$ is obtained.

When analyzing this histogram of differences, volatility goes the opposite way as compared to the histogram of pixel intensities. When embedding data, the volatility of the histogram of differences increases instead of decreasing. However, after embedding a new message into a stego image, the volatility remains almost unchanged.

Now, the method proceeds as described in the previous section. Firstly, the volatility of the histogram of differences, with the prediction of Expression 3, is calculated as per Expression 2. Then, a new message is embedded (using a random binary mask as described in the previous section) into the image and, finally, the volatility is computed again. If the volatility increases significantly after embedding, then the image is declared cover, otherwise it is detected as stego.

III. Experimental results

In this section, we present the experimental results obtained with all the proposed algorithms. In these experiments, the National Resource Conservation System (NRCS) [1] database of 1371 images has been used. These images have been embedded with the different methods described above. More precisely, a testing set consisting of 2742 images, half of them stego and half of them cover have been used for each of the experiments detailed below (except for the mixed experiments of Section III-D which have more specific settings).

For the generic algorithm, we have used a threshold of 15%. This means that an image is considered stego if its volatility increases less than 15% when embedding a new message, otherwise it is considered cover. The results of the experiments show that this threshold is appropriate.

A. Ni et al.*'s Method*

As detailed in Section II-A, this specific detection technique requires two thresholds. The first threshold is to verify that h_{i+1} and h_{i+2} have a similar value. We have used a maximum difference of 10%. The second threshold is to verify that h_i or h_{i+3} are not much smaller than $h_{i+1} + h_{i+2}$. A maximum difference of 30% has been used for this condition. The experiments show that these thresholds are appropriate.

TABLE I: Experimental results for Ni *et al.*'s method [11]

Results	Specific	Generic
Successful	85.19%	85.22%
Positive	40.29%	44.93%
Negative	44.89%	40.29%
False positive	5.10%	9.70%
False negative	9.70%	5.06%

The results are shown in Table I. The row "Successful" refers to the percentage of correctly identified images (either as cover or stego), the row "Positive" reports the percentage of the correctly identified stego images (the maximum is 50%), "Negative" reports the number of correctly identified cover (unmarked) images (again, the maximum is 50%), "False positive" reports the percentage of cover images incorrectly identified as stego and, finally, "False negative" is the percentage of stego images which are not correctly detected by the technique. Note that the number of positives plus false negatives equals 50%. Analogously, the number of negatives plus false positives also equals 50% of the total number of images.

It can be observed that both the specific and the generic methods correctly identify more than 85% of the images. The specific scheme has a higher percentage of false negatives, whereas the generic one has a higher ratio of false positives.

B. Mohsenzadeh et al.*'s Method*

For For Mohsenzadeh *et al.*'s method with Algorithm 1, the specific algorithm described in Section II-B does not need any threshold, just analyzes the shape of the histogram as shown in Fig.2.

TABLE II: Experimental results for Mohsenzadeh *et al.*'s method [10] – Algorithms 1 and 2

Results	Algorithm 1		Algorithm 2
	Specific	Generic	Generic
Successful	90.99%	81.65%	90.18%
Positive	42.19%	41.35%	49.89%
Negative	48.79%	40.29%	40.29%
False positive	1.23%	9.70%	9.70%
False negative	7.76%	8.64%	0.10%

The results shown in Table II for Algorithm 1 indicate higher scores for the specific algorithm, but the generic method also yields remarkable results. For Mohsenzadeh *et al.*'s method with Algorithm 2, only the generic algorithm has been applied, since the exact position of the neighboring pixels used to embed data is protected by means of a secret key and cannot be used by a specific attack. The results, which are shown in the same table, indicate a large ratio of success using the generic algorithm. In addition, in this case, the reliability of the detection of positives is remarkable, with a 49.89% of success for a maximum of 50%.

C. HSPE Methods

For detecting HSPE methods, the specific algorithm presented in Section II-C has been used with a threshold of 15%. This means that an image is considered stego if its volatility decreases less than 15% when embedding a new message, otherwise it is considered cover. The experiments show that this threshold is appropriate.

Table III shows the results for HSPE steganography with five different prediction equations: horizontal, vertical, diagonal, causal and MED. As horizontal prediction is concerned, both the specific and the generic methods obtain similar success ratios, with somewhat better results for the generic one. The same goes to the results for diagonal prediction errors, with an almost identical performance for both methods and a small difference in favor of the generic one. For vertical prediction errors, it can bee seen that the success ratios are, again, similar with both methods, but this time the results are slightly better for the specific one.

As causal prediction is concerned, the results of Table III show that the specific method is particularly unsuitable for this embedding technique using the same thresholds as for the other HSPE methods. By modifying the threshold of the specific method slightly, success ratios of above 80% can be obtained, but this also increases the number of false positives. Finally, when MED prediction errors are used, the results are analogous to those obtained with causal prediction errors. Again, the successful identification ratio with the specific

TABLE III: Experimental results for HSPE data hiding

Results	Horizontal		Vertical		Diagonal		Causal		MED	
	Specific	Generic	Specific	Generic	Specific	Generic	Specific	Generic	Specific	Generic
Successful	86.94%	87.16%	88.84%	87.19%	87.52%	88.65%	61.19%	86.10%	63.78%	85.88%
Positive	43.47%	46.86%	45.36%	46.90%	44.05%	48.35%	17.72%	45.80%	20.31%	45.58%
Negative	43.47%	40.29%	43.47%	40.29%	43.47%	40.29%	43.47%	40.29%	43.47%	40.29%
False positive	6.52%	9.70%	6.52%	9.70%	6.52%	9.70%	6.52%	9.70%	6.52%	9.70%
False negative	6.52%	3.13%	4.63%	3.09%	5.94%	1.64%	32.27%	4.19%	29.68%	4.41%

technique could be improved over 80% by modifying the thresholds at the price of increasing the false positive ratio.

D. Mixed Experiments

In this section, an experiment was performed with 1000 cover and 1000 stego images. The set of stego images contains a mixture of all the presented methods in equal parts. *I.e.*, the 1000 stego images are marked using Ni *et al.*'s method, Mohsenzadeh *et al.*'s Algorithms 1 and 2, and HSPE with horizontal, vertical, diagonal, causal and MED predictions. Hence, eight different embedding methods are used and 125 images are embedded with each method.

TABLE IV: Experimental results for different mixed histogram shifting data hiding methods

Results	Generic
Successful	86.05%
Positive	46.15%
Negative	39.90%
False positive	10.10%
False negative	3.85%

As shown in Table IV, the generic algorithm for a mixture of histogram shifting data hiding schemes yields a successful classification ratio of above 86%.

IV. Conclusions

In this paper, we have shown that histogram shifting-based data hiding schemes cause alterations in the image histogram and that these alterations can be detected. We have introduced a technique, based on the analysis of the histogram's volatility, which can be applied to several data hiding methods. The experimental results show that the analysis of the histogram's volatility can be used to detect relevant changes in the histogram, and that the analysis of the histogram of differences provides remarkable results, being able to identify between 80% and 90% of the test images correctly as cover or stego.

As future work, it would be advisable to study the use of other histograms to estimate volatility, as well as exploring the applicability of this steganalytic technique to other data hiding schemes.

Acknowledgments

This work was partly funded by the Spanish Government through projects TSI2007-65406-C03-03 E-AEGIS, TIN2011-27076-C03-02 CO-PRIVACY and CONSOLIDER INGENIO 2010 CSD2007-0004 ARES.

References

[1] "National Resource Conservation System (NRCS) Photo Gallery," accessed on May 30, 2012. [Online]. Available: http://photogallery.nrcs.usda.gov

[2] "Standard test images," accessed on May 30, 2012. [Online]. Available: http://www.ece.rice.edu/~wakin/images/

[3] C.-C. Chang, W.-L. Tai, and C.-C. Lin, "A reversible data hiding scheme based on side match vector quantization," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 16, no. 10, pp. 1301–1308, oct. 2006.

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

[5] W. Hong, T.-S. Chen, and C.-W. Shiu, "Reversible data hiding based on histogram shifting of prediction errors," in *Intelligent Information Technology Application Workshops, 2008. IITAW '08. International Symposium on*, dec. 2008, pp. 292–295.

[6] C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," United States Patent N.: 6,278,791 B1, 2001, accessed on May 30, 2012. [Online]. Available: http://www.freepatentsonline.com/6278791.html

[7] J. Hwang, J. Kim, and J. Choi, "A reversible watermarking based on histogram shifting," in *Digital Watermarking*, ser. Lecture Notes in Computer Science, Y. Shi and B. Jeon, Eds. Springer Berlin / Heidelberg, 2006, vol. 4283, pp. 348–361.

[8] W.-C. Kuo and Y.-H. Lin, "On the security of reversible data hiding based-on histogram shift," in *Proceedings of the 2008 3rd International Conference on Innovative Computing Information and Control*, ser. ICICIC '08. Washington, DC, USA: IEEE Computer Society, 2008, p. 174.

[9] S.-K. Lee, Y.-H. Suh, and Y.-S. Ho, "Lossless data hiding based on histogram modification of difference images," in *Proceedings of the 5th Pacific Rim conference on Advances in Multimedia Information Processing - Volume Part III*, ser. PCM'04. Berlin, Heidelberg: Springer-Verlag, 2004, pp. 340–347.

[10] Y. Mohsenzadeh, J. Mohajeri, and S. Ghaemmaghami, "Histogram shift steganography: A technique to thwart histogram based steganalysis," in *Proceedings of the 2009 Second International Workshop on Computer Science and Engineering - Volume 02*, ser. IWCSE '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 166–170.

[11] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 16, no. 3, pp. 354–362, mar. 2006.

[12] T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 215–224, june 2010.

[13] T. Pevný and J. Fridrich, "Merging Markov and DCT features for multi-class JPEG steganalysis," in *Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, CA, January 29–February 1*, E. Delp and P. Wong, Eds., vol. 6505, January 2007, pp. 03–14.

[14] C. T. H. Thom, H. V. Canh, and T. N. Tien, "Steganalysis for reversible data hiding," *International Journal of Database Theory and Application*, vol. 3, no. 2, pp. 21–30, jun. 2010.

[15] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Information Hiding*, ser. Lecture Notes in Computer Science, A. Pfitzmann, Ed. Springer Berlin / Heidelberg, 2000, vol. 1768, pp. 61–76.

[16] W. Zeng, "Digital watermarking and data hiding: technologies and applications (invited talk)," in *Proc. International Conference on Information Systems, Analysis and Synthesis*, vol. 3, 1998, pp. 223–229.