International Journal of Digital Crime and Forensics
Volume 11 • Issue 1 • January-March 2019

Breaking Steganography:
Slight Modification with Distortion Minimization

Zhenxing Qian, School of Computer Science, Fudan University, Shanghai, China

Zichi Wang, Shanghai Institute for Advanced Communication and Data Science, Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai, China

Xinpeng Zhang, School of Computer Science, Fudan University, Shanghai, China

Guorui Feng, School of Communication and Information Engineering, Shanghai University, Shanghai, China

ABSTRACT

This article describes how to overcome the shortage of steganalysis for small capacity-based embedding. A slight modification method is proposed to break steganography. For a given image, traditional steganalysis methods are first used to achieve a preliminary result. For the "clear" image judged by steganalysis, it is still suspicious because of the incompleteness of steganalysis for small capacity. Thus, slight modifications are made to break the possibility of covert communication. The modifications are made on the locations with minimal distortion to guarantee high quality of the modified image. To this end, a proposed distortion minimization based algorithm using slight modification. Experimental results show that the error rate of secret data extraction is around 50% after implementation, which indicates that the covert communication of steganography is destroyed completely.

KEYWORDS

Distortion Minimizing, Modification, Steganalysis, Steganography

INTRODUCTION

Digital image steganography aims to transmit data secretly by embedding secret data into cover image (Zhang, 2016). Nowadays, the plentiful images transmitted over the social network provide convenience for steganography. How to break steganography is becoming a troublesome issue. Steganalysis attempts to reveal the presence of the embedded data. As shown in Figure 1, however, because of the missing detection error of steganalysis, the images judged as "clear" by steganalysis are still possible carried small amount of secret data. Therefore, some slight modifications should be made to prevent the still possible covert communication. On the other hand, the images judged as "stego" by steganalysis are still possible innocent because of the false alarm error. There are many kind of image processing operations frequently used on the images transmitted over social network, such as denoising, recompression, and beautification. So, the false alarm error may be caused by these

DOI: 10.4018/IJDCF.2019010109

Figure 1. The combat against steganography

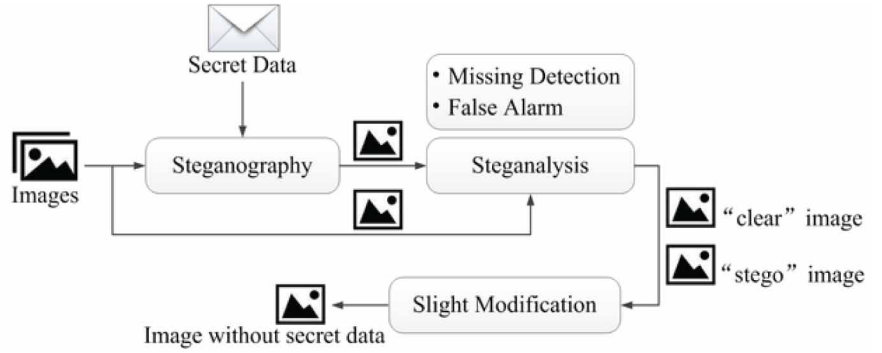


image processing operations instead of steganography. In this case, it is inappropriate to intercepte all the "stego" images. So, these images can also be processed as same as the "clear" image to stop the quite possible covert communication if the evidence is not enough to declare the guilty of the images. In this way, the combat against steganography is victorious, and meanwhile, the innocent images are transmitted over the social network as usual.

In addition, for early steganographic methods which increase the security performance by decreasing the quantity of embedding changes (Frdrich & Soukal, 2006;Zhang & Wang, 2006; Zhang, Zhang & Wang, 2008), current machine learning based steganalytic methods (Kodovsky, Fridrich & Holub, 2012; Fridrich & Kodovsky, 2012; Holub & Fridrich, 2014; Denemark, Sedighi, Holub, Cogranne & Fridrich, 2014; Song, Liu, Yang, Luo & Zhang, 2015) perform excellent detectability. But for modern steganographic methods (Holub & Fridrich, 2013, Li, Wang, Huang & Li, 2014, Sedighi, Fridrich & Cogranne, 2015, Guo, Ni, Su, Tang & Shi, 2015; Wang, Zhang & Yin, 2016) which improve security performance by minimize the additive distortion between a given cover object and its stego version (Filler, Judas & Fridrich, 2011, Filler & Fridrich, 2010), steganalysis becomes powerless to verdict the presence of secret data especially for the case of small capacity. Recently, adaptive steganalysis (Denemark, Boroumand & Fridrich, J. 2016; Yu, Li, Cheng, Zhang, 2016; Tang, Li, Luo & Huang, 2016) improves the detectability observably. In adaptive steganalysis, different weights are assigned to different cover elements in feature extraction. For the elements with high modifying probabilities, larger weights are assigned since these elements contribute more to steganalysis and vice versa. For small capacity, however, these methods still not perform satisfactory detectability. The detection for small capacity is still a to be resolved problem. In other words, the approach to break steganography is still undiscovered.

Actually, to break the covert communication of steganography, steganalysis is not the only choice. For a suspicious image, the possibly existing secret data can be destroyed by modifying the image although it is difficult to judge whether the image is stego or not. In this way, there is no secret data can be transmitted via the modified image. Thus, the threat from steganography is disappeared.

This paper proposes a slight modification method to break steganography. Some slight modifications are made on a suspicious image to break the extracting of secret data. And these modifications are made on the locations with minimal distortion to guarantee high quality of the modified image. Experiment results show that the secret data cannot be extracted from the modified image, and the modified image keeps a high quality comparing with the given image.

PROPOSED METHOD

The framework of the proposed method is shown in Figure 2. For a suspicious image, modern steganalytic methods which is based on feature extraction and classification judgment are employed firstly. After steganalysis, if the image is judged as "clear", something should be done to prevent the still possible covert communication. Otherwise, it can be intercepted to stop the covert communication or also processed as same as the "clear" image.

For the "clear" image, a modifying priority calculation method is employed to get the priority value of each element. The priority value is in inverse proportion to image distortion caused by modifying the element. According to the modification rate, a part of elements with maximal priority values are modified by plus or minus 1 to break the still possible covert communication. In this way, the modifications are gathered in the areas with minimal distortion. Thus, high quality of the modified image is guaranteed, as well as the image's usability. The details are as follows.

Priority Calculation and Location Decision

In modern adaptive steganographic methods, secret data is embedded in whole image via STC (syndrome trellis coding) (Filler, T., Judas, J., & Fridrich, J. 2011). With STC, the additive distortion between cover and stego image is minimized under a user-defined distortion function. As shown in Figure 3, after distortion function calculation, the cover image, distortion function, and secret data are inputed into STC to output the stego image. Denote the stego image as $\mathbf{y} = [\, y_1, y_2, \ldots, y_n \,]$, thus the secret data $\mathbf{m}$ can be extracted in a straightforward manner using Equation (1),

$$\mathbf{m} = \mathbf{H}\mathbf{y} \tag{1}$$

where H is a low-density parity-check matrix determinedd via embedding speed, embedding efficiency and payload. The construction of H is unknown to the attacker, so it is impossible to design targeted attack scheme. Because of the secret data is embedded in whole image, the degree of breaking on secret data is dependent on the amount of modifications instead of locations. Therefore, the modifications

Figure 2. Framework of proposed method

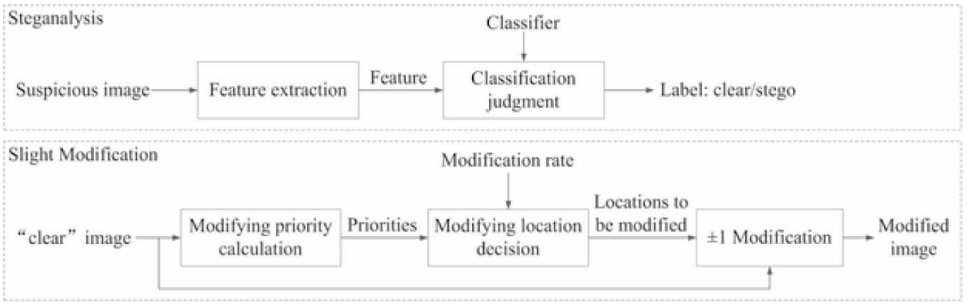
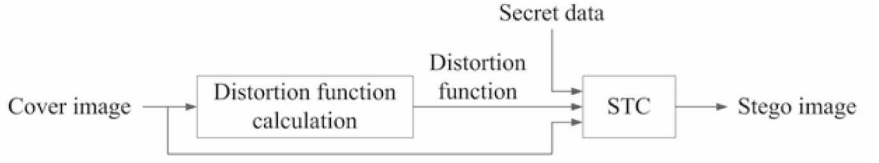


Figure 3. Steganography with STC



can be made on the locations with minimal distortion to guarantee high quality of the modified image, thereby guaranteeing the image's usability. And the degree of breaking on secret data would not be influenced by this selection.

In the framework of STC, the distortion function allots an embedding cost for each cover element. Where the embedding cost quantifies the effect for modifying a cover element, that is to quantify the image distortion caused by modifying the element. So, the embedding cost used in steganography can be employed in the proposed method to calculate the priority value.

For a image contains n elements (pixel for uncompressed image or DCT coefficient for JPEG image), the i-th elements is denoted as x_i, where $i \in \{1, 2, \ldots, n\}$. In modern adaptive steganographic methods, a embedding cost is allocated for each x_i to measure image distortion caused by modifying it. Assume there are w steganographic methods employed to calculate the embedding cost. Denote the embedding cost for x_i calculated by j-th steganographic method as ρ_i^j, where $j \in \{1, 2, \ldots, w\}$. In other words, there are w embedding costs for each element.

The steps to calculate the priority value are as follows.

I. As shown in Equation (2), restrict the value range of the embedding cost $\rho^j = [\rho_1^j, \rho_2^j, \ldots, \rho_n^j]$ into [0,1]. Execute this step for all the w steganographic methods respectively. In this way, the embedding costs calculate by the w steganographic methods are restricted in the same value range;

$$\hat{\rho}_i^j = \frac{\rho_i^j - \min\{\rho^j\}}{\max\{\rho^j\} - \min\{\rho^j\}} \tag{2}$$

II. Calculate the average value $\overline{\rho}_i$ of the w new embedding costs $\{\hat{\rho}_i^1, \hat{\rho}_i^2, \ldots, \hat{\rho}_i^w\}$ using Equation (3) to obtain the synthetical measurement of image distortion caused by modifying x_i;

$$\overline{\rho}_i = \frac{1}{w}\sum_{j=1}^{w} \hat{\rho}_i^j \tag{3}$$

III. As shown in Equation (4), calculate the priority value θ_i which is in inverse proportion to image distortion. Where ε is a parameter used to avoid the value of denominator becoming zero. Its value is tiny and set as 10^{-10};

$$\theta_i = \frac{1}{\overline{\rho}_i + \varepsilon} \tag{4}$$

Denote the modification rate as r ($0 < r < 1$). The value of r should large enough to guarantee the possibly existing secret data is destroyed completely. Meanwhile, the value should as small as possible to guarantee high quality of the modified image. More details about the determination of r will be discussed in the next Section. Sort priority value $\{\theta_1, \theta_2, \ldots, \theta_n\}$ in descending order. After sorting, denote the sorted priority value as $\{\theta_1', \theta_2', \ldots, \theta_n'\}$, the image elements corresponding to $\{\theta_1', \theta_2', \ldots, \theta_n'\}$ as $\{x_1', x_2', \ldots, x_n'\}$ respectively. Then the $k = \text{round}(r \times n)$ elements $\{x_1', x_2', \ldots, x_k'\}$ would be modified by plus or minus 1. The embedding manner in modern steganographic methods is ternary embedding. In this embedding manner, the modifications are not only involves

LSB (Least Significant Bit). So, in order to break the secret data completely, the manner of modification in the proposed method is plus or minus 1 instead of modify LSB only.

Estimation Based Modification

After the locations $\{ x_1', x_2', \ldots, x_k' \}$ are decided, these locations would be modified by plus or minus 1. Because of the correlation of natural image, modifications with different polarity make different influence on image. In other words, the influence on image made by +1 and -1 modification is not equivalent. To further improve the quality of modified image, we made a choice on the polarity of modification. The details are as follows.

To determine the polarity of modification, a rule is proposed for both uncompressed image and JPEG image, which is called correlation prior rule. The correlation between image elements is a typical character in natural image (Zhang, X. P. 2011), it is helpful to improve image quality by enhancing correlation (Wang, Z., Bovik, A., Sheikh, H., & Simoncelli, E. 2004). Thus, it is a advisable choice to make the modifications towards the direction to enhance correlation.

For each element x_i, a prediction value $\tilde{x}_i$ is defined to promote the selection of polarity of modification. In a two-dimension image sized $M \times N$, x_i is rewrote as $x_{u,v}$, where $u \in \{1, 2, \ldots, M\}$, $v \in \{1, 2, \ldots, N\}$. For uncompressed image, the prediction value of $x_{u,v}$ is defined in Equation (5), which is the average value of the four neighbourhood pixels. In JPEG image, the inter-block correlation is stronger than intra-block correlation (Wang, Z. C., Yin, Z. Y., & Zhang, X. P., in press). Thus the prediction value is defined in Equation (6), which is the average value of the four coefficients located in the same coordinate of the four neighbourhood DCT blocks. The nonexistent element which is out of the image boundary would be obtained by element symmetric padding. For example, $x_{u+1,v}$ is obtained by copying $x_{u-1,v}$ when it is out of the image boundary, and vice versa.

$$\tilde{x}_{u,v} = \frac{x_{u,v-1} + x_{u,v+1} + x_{u-1,v} + x_{u+1,v}}{4} \tag{5}$$

$$\tilde{x}_{u,v} = \frac{x_{u,v-8} + x_{u,v+8} + x_{u-8,v} + x_{u+8,v}}{4} \tag{6}$$

Finally, the k elements $\{ x_1', x_2', \ldots, x_k' \}$ are modified using Equation (7). Where x_i'' is the element of modified image described in Figure 2. Thus, the locations to be modified are distortion preferentially selected. Note that the overflow of element value is nonexistent in Equation (7).

$$x_i'' = \begin{cases} x_i' + 1 & , \text{ if } i \le k \text{ and } x_i' < \tilde{x}_i' \\ x_i' - 1 & , \text{ if } i \le k \text{ and } x_i' > \tilde{x}_i' \\ x_i' & , \text{ otherwise} \end{cases} \tag{7}$$

In addition, there is another modification manner for JPEG image. That is decompress JPEG image into spatial domain firstly and then modify the pixels. Finally, recompress the image into DCT domain with same quality factor. In this manner, there are some additional and unnecessary work required for the attacker. It would cause the increasing of computational complexity. So we modify the DCT coefficients of JPEG image directly.

EMPIRICAL MODIFICATION RATE DETERMINATION

As mentioned above, the modification rate r should large enough to guarantee the possibly existing secret data is destroyed completely. And meanwhile, the value also should as small as possible to guarantee high quality of the modified image. The details to determine the value of r are as follows.

Four gray images sized 512×512, Lena, Man, Lake, and Baboon, shown in Figure 4, are used as cover images to find the suitable modification rate r. The popular adaptive steganographic methods HILL (Li, Wang, Huang & Li, 2014) and SUNIWARD (Holub & Fridrich, 2013) for uncompressed image, JUNIWARD (Holub & Fridrich, 2013) and UED (Guo, Ni & Shi, 2014) for JPEG image are employed to obtain the stego image. The payload is set as 0.05 bpp (bit per pixel) for uncompressed image and 0.05 bpnzac (bit per non-zero AC coefficient) for JPEG image, which is a small payload that steganalysis helplessness.

To calculate the priority value used to select suitable locations for modification, the distortion function of JUNIWARD, UERD (Guo, Ni, Su, Tang & Shi, 2015), and HDS (Wang, Zhang & Yin, 2016) is employed to calculate the distortion value for JPEG image. And the distortion function of HILL, SUNIWARD, and WOW (Holub & Fridrich, 2012) is used to calculate the distortion value for uncompressed image.

Figure 5 shows the relationship between data extracting error and modification rate for four uncompressed image Lena, Man, Lake, and Baboon. For JPEG image, the relationship between data extracting error and modification rate is shown in Figure 6 ~ 8. Where the quality factor QF are set as 50, 70, and 90.

Figure 4. Cover images (a) Lena. (b) Man. (c) Lake. (d) Baboon

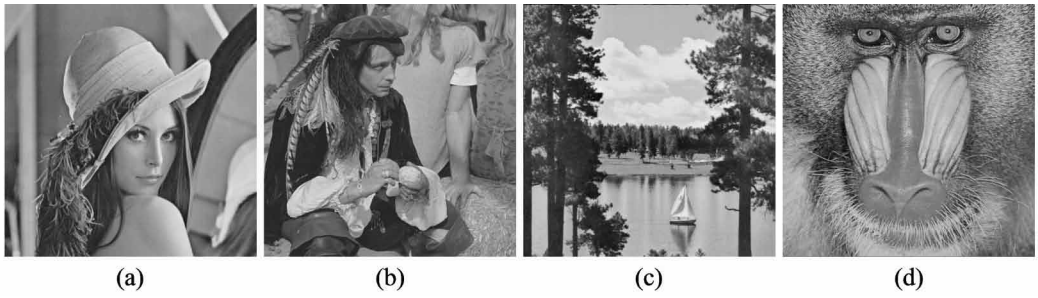
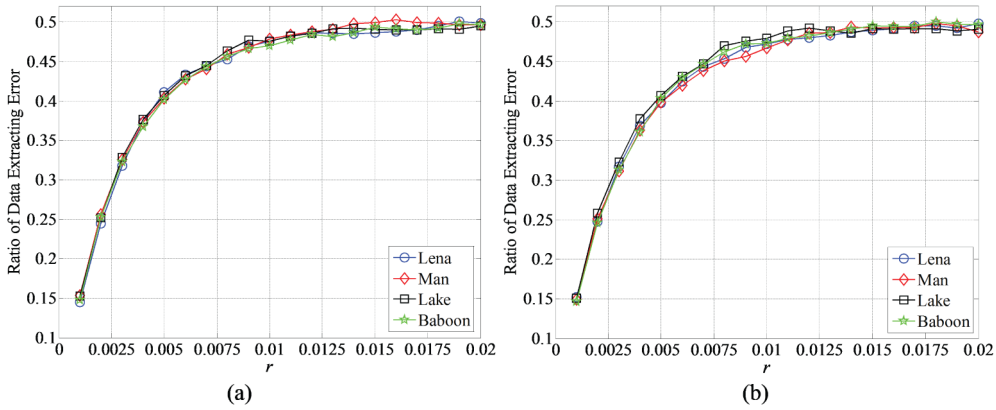


Figure 5. Relationship between data extracting error and modification rate for uncompressed image with payload 0.05 bpp and (a) HILL. (b) SUNIWARD



It can be seen from Figure 5 that the variation between data extracting error and modification rate for uncompressed image performs similar tendency for different images. To guarantee the possibly existing secret data destroyed completely and keep a high quality of the modified image simultaneously. The value of r is determined as 0.01 for uncompressed image where the ratio of data extracting error is larger than 45% for all images.

For JPEG image, it can be concluded from Figure 6 ~ 8 that data extracting error is in inverse proportion to quality factor with same ratio of modifications. In other words, the necessary amount of modifications is in proportion to quality factor. In our opinion, the reason of this observation is related to the mechanism of JPEG compression. As we know, the quantization step is in inverse proportion of QF. For a given image, a small QF means larger quantization step and less non-zero AC coefficients. Thus, for a same payload (bit per non-zero AC coefficient) in DCT domain, a small QF means less capacity (bit). Therefore, for a small QF, a few amount of modifications made in DCT domain can cause completely destroy of secret data. Conversely, for a big QF, more amount of modifications is necessary.

Figure 6. Relationship between data extracting error and modification rate for QF = 50 with payload 0.05 bpnzac and (a) JUNIWARD. (b) UED

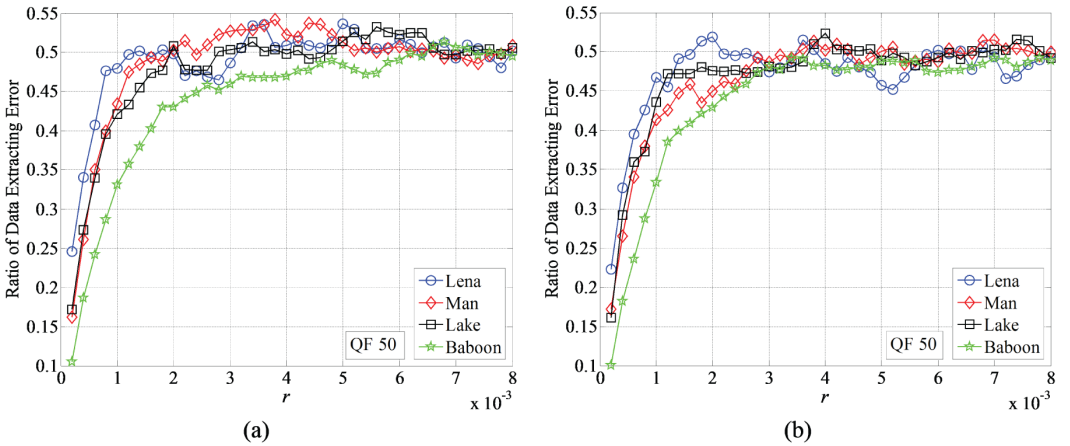


Figure 7. Relationship between data extracting error and modification rate for QF = 70 with payload 0.05 bpnzac and (a) JUNIWARD. (b) UED

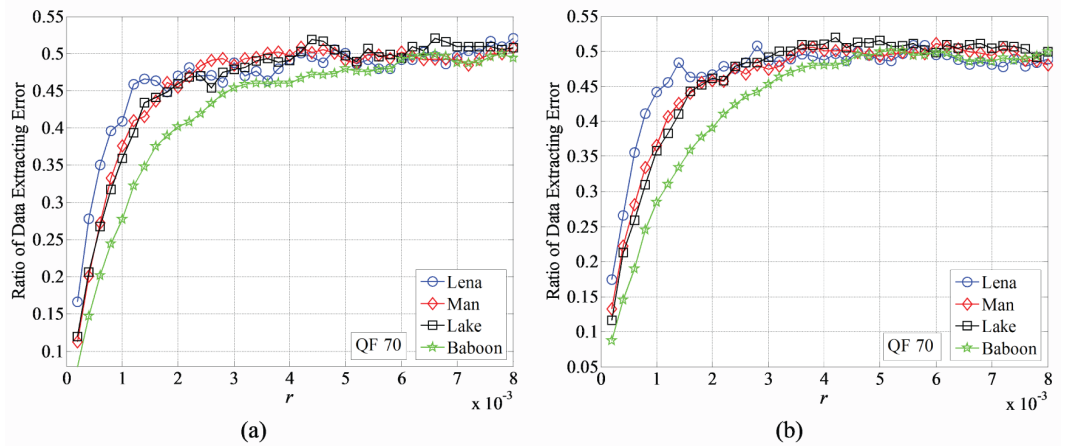
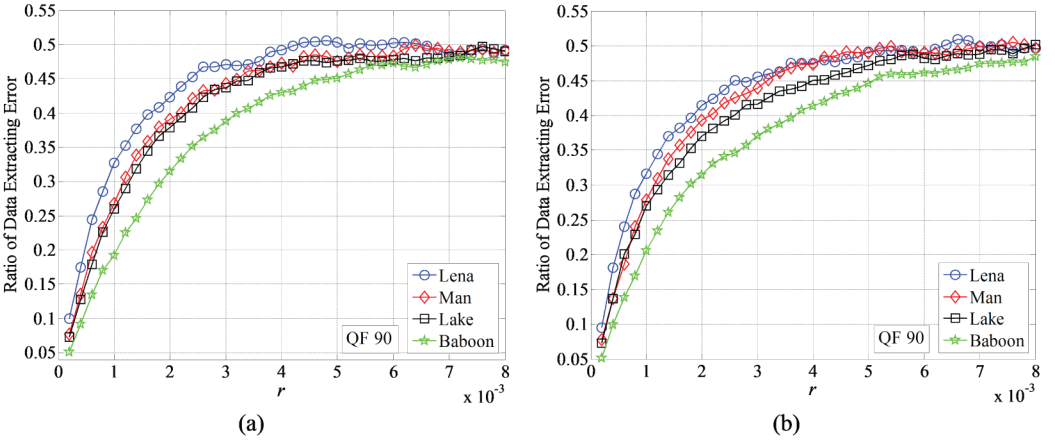


Figure 8. Relationship between data extracting error and modification rate for *QF* = 90 with payload 0.05 bpnzac and (a) JUNIWARD. (b) UED



Specifically, for the cases of $QF = 50$, 70, and 90, the suitable value of r can be determined as 0.0025, 0.004, and 0.0055 respectively following the same criterion with uncompressed image. For other scale factors, the value of r can be calculated for JPEG image using Equation (8), which is obtained using linear fit,

$$r = \max\left\{\frac{75 \cdot QF - 1250}{10^6} \quad , \quad 0.0025\right\} \tag{8}$$

where $1 \le QF \le 100$. It can be calculated that the range of r is $0.0025 \le r \le 0.00625$. The maximal value 0.00625 for JPEG image is smaller than 0.01 for uncompressed image. This phenomenon also verified the above analysis for JPEG image.

QUALITY OF MODIFIED IMAGE

In this section, the criterion employed to evaluate the image quality is *PSNR* (Peak Signal to Noise Ratio) and a universal quality index *SSIM* (Wang & Bovik, 2002). The two criterions is designed for uncompressed image. For JPEG image, it would be decompressed into spatial domain firstly. While *PSNR* simply indicates the energy of distortion caused by modification, *SSIM* combines correlation loss, luminance distortion and contrast distortion (Zhang, X. P. 2012). Higher *PSNR* or *SSIM* means better quality. The range of *PSNR* and *SSIM* are $0 < PSNR \le +\infty$ and $0 \le SSIM \le 1$ respectively.

The quality of modified uncompressed image is shown in Table 1, and quality of modified JPEG image is shown in Table 2. Where "Rand" means the locations to be modified are selected randomly.

Table 1 ~ 2 indicate that the image keeps a excellent quality after modified using the proposed method, and the image quality is improved observably when the locations to be modified are distortion preferentially selected. Numerically, for JPEG image with $QF = 50$, the *PSNR* for Lena can be improved by 15.3dB and *SSIM* for Lena can be improved by 10.605% . For $QF = 70$, the *PSNR* for Baboon can be improved by 15.9dB and *SSIM* for Lena can be improved by 10.211%.

To demonstrate the improvement of the proposed method compared with "Rand" manner adequately, 1000 images are randomly selected from image dataset BOSSbass ver. 1.01 (Bas, P., Filler, T., & Pevný, T. 2011) and compressed into JPEG image with quality factor $QF = 50$, 70 and 90. The comparison of image quality is shown in Figure 9.

Table 1. Image quality of four uncompressed images with $r = 0.01$

		Lena	Man	Lake	Baboon
PSNR (dB)	Proposed	68.1	68.1	68.1	68.1
	Rand	68.1	68.1	68.1	68.1
SSIM	Proposed	0.99999	0.99999	0.99999	0.99999
	Rand	0.99974	0.99973	0.99982	0.99997

Table 2. Image quality of four JPEG images

			Lena	Man	Lake	Baboon
$QF = 50$ $r = 0.0025$	*PSNR* (dB)	Proposed	53.0	52.7	52.9	53.7
		Rand	37.7	37.6	37.6	37.6
	SSIM	Proposed	0.99981	0.99975	0.99986	0.99991
		Rand	0.89376	0.93583	0.91605	0.97441
$QF = 70$ $r = 0.004$	*PSNR* (dB)	Proposed	55.2	55.1	55.4	55.8
		Rand	39.9	40.2	39.9	39.9
	SSIM	Proposed	0.99988	0.99988	0.99993	0.99995
		Rand	0.89777	0.94327	0.92796	0.98102
$QF = 90$ $r = 0.0055$	*PSNR* (dB)	Proposed	64.1	64	64.5	64.7
		Rand	48.2	48.2	48.3	48.1
	SSIM	Proposed	0.99998	0.99998	0.99999	0.99999
		Rand	0.97271	0.98411	0.98367	0.99704

From Figure 9 we can see that the average quality of the 1000 images is also improved for all cases via distortion preferentially selecte the modifying locations, and the average quality keeps on a high level. For example, average quality index *SSIM* of the images modified using the proposed method is always extraordinarily close to 1, which means tiny distortion in the modified image. For *PSNR*, the improvement is more than 10dB for all cases compared with "Rand" manner. These observations further demonstrate the effectiveness of the proposed method.

There is another approach to break steganography except the proposed method and the "Rand" manner. That is use the current steganography method to embed messages again. The comparison between the proposed method with current steganographic method to break steganography tested on four JPEG images with *SSIM* is shown in Table 3. Where "CSM" means the four JPEG images are embedded by UED with a necessary payload to break steganography completely.

It can be seen from Table 3 that the "CSM" manner is not performed well with the proposed method. In addition, the "CSM" manner would be impracticable due to the lack of the knowledge of the steganographic method employed for embedding.

CONCLUSION

This paper proposes a slight modification method to break steganography by making some slight modifications on the suspicious image filtrated by steganalysis. The quantity of the modifications made on the suspicious image is large enough to completely destroy the possibly existing secret

Figure 9. Average image quality of 1000 JPEG images with different quality metrics. (a) *PSNR*. (b) *SSIM*

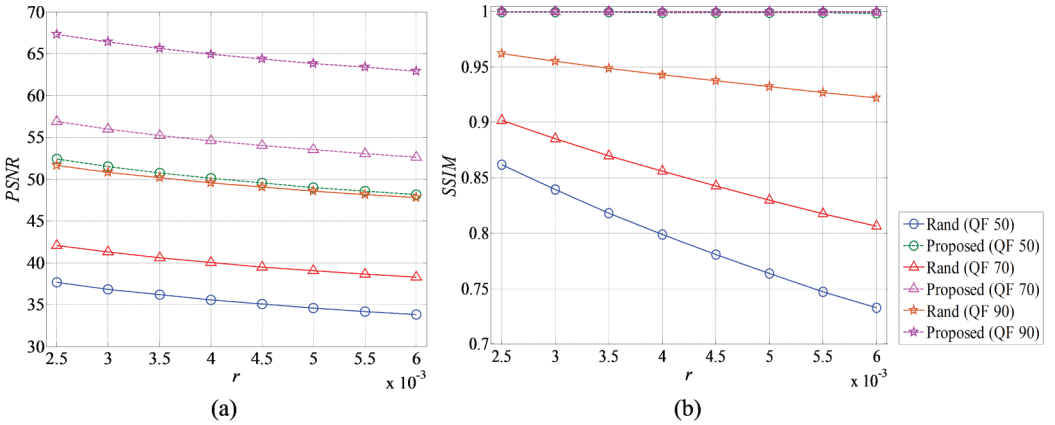


Table 3. Image quality comparison of proposed method and current steganographic method with *SSIM*

		Lena	Man	Lake	Baboon
$QF = 50$	Proposed	0.99981	0.99975	0.99986	0.99991
	CSM	0.99971	0.99948	0.99946	0.99966
$QF = 70$	Proposed	0.99988	0.99988	0.99993	0.99995
	CSM	0.99983	0.99968	0.99960	0.99985
$QF = 90$	Proposed	0.99998	0.99998	0.99999	0.99999
	CSM	0.99996	0.99992	0.99992	0.99997

data. Meanwhile, these modifications are made on the locations with minimal distortion. So the high quality of the modified image is guaranteed. Experiment results show that the covert communication of steganography is destroyed completely after the proposed method is implemented. For further study, it is significant to determine the modification rate by theoretical derivation instead of experiment observation.

ACKNOWLEDGMENT

This work was supported by the Natural Science Foundation of China (U1636206, U1736213, U1536108, 61572308, 61373151, 61525203, and 61502009), the Shanghai Dawn Scholar Plan (14SG36) and the Shanghai Excellent Academic Leader Plan (16XD1401200).

REFERENCES

Bas, P., Filler, T., & Pevný, T. (2011). Break Our Steganographic System: The Ins and Outs of Organizing BOSS. In *Proc. 13th International Conference on Information Hiding,* Prague, Czech Republic (pp. 59-70).. doi:10.1007/978-3-642-24178-9_5

Denemark, T., Sedighi, V., Holub, V., Cogranne, R., & Fridrich, J. (2014). Selection-Channel-Aware Rich Model for Steganalysis of Digital Images. In *Proc. 2014 IEEE International Workshop on Information Forensics and Security,* Atlanta, GA (pp. 48-53). doi:10.1109/WIFS.2014.7084302

Denemark, T. D., Boroumand, M., & Fridrich, J. (2016). Steganalysis Features for Content Adaptive JPEG Steganography. *IEEE Transactions on Information Forensics and Security*, *11*(8), 1736–1746. doi:10.1109/TIFS.2016.2555281

Filler, T., & Fridrich, J. (2010). Gibbs Construction in Steganography. *IEEE Transactions on Information Forensics and Security*, *5*(4), 705–720. doi:10.1109/TIFS.2010.2077629

Filler, T., Judas, J., & Fridrich, J. (2011). Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes. *IEEE Transactions on Information Forensics and Security*, *6*(3), 920–935. doi:10.1109/TIFS.2011.2134094

Frdrich, J., & Soukal, D. (2006). Matrix Embedding for Large Payloads. in Proc. International Society for Optics and Photonics (pp. 60721W-60721W-12). San Jose, CA, Feb. 2006.

Fridrich, J., & Kodovsky, J. (2012). Rich Models for Steganalysis of Digital Images. *IEEE Transactions on Information Forensics and Security*, *7*(3), 868–882. doi:10.1109/TIFS.2012.2190402

Guo, L. J., Ni, J. Q., & Shi, Y. Q. (2014). Uniform Embedding for Efficient JPEG Steganography. *IEEE Transactions on Information Forensics and Security*, *9*(5), 814–825. doi:10.1109/TIFS.2014.2312817

Guo, L. J., Ni, J. Q., Su, W. K., Tang, C. P., & Shi, Y. Q. (2015). Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited. IEEE Trans. *Information Forensics and Security*, *10*(12), 2669–2680. doi:10.1109/TIFS.2015.2473815

Holub, V., & Fridrich, J. (2012). Designing Steganographic Distortion Using Directional Filters. In *Proc. IEEE International Workshop on Information Forensics and Security,* Binghamton, NY (pp. 234-239).

Holub, V., & Fridrich, J. (2013). Digital Image Steganography Using Universal Distortion. In *Proc. the first ACM workshop on Information Hiding and Multimedia Security,* New York, NY (pp. 59-68). doi:10.1145/2482513.2482514

Holub, V., & Fridrich, J. (2014). Low Complexity Features for JPEG Steganalysis Using Undecimated DCT. *IEEE Transactions on Information Forensics and Security*, *10*(2), 219–228. doi:10.1109/TIFS.2014.2364918

Kodovsky, J., Fridrich, J., & Holub, V. (2012). Ensemble Classifiers for Steganalysis of Digital Media. *IEEE Transactions on Information Forensics and Security*, *7*(2), 432–444. doi:10.1109/TIFS.2011.2175919

Li, B., Wang, M., Huang, J. W., & Li, X. (2014). A New Cost Function for Spatial Image Steganography. In *Proc. IEEE International Conference on Image Processing*, Paris, France (pp. 4206-4210). doi:10.1109/ICIP.2014.7025854

Sedighi, V., Fridrich, J., & Cogranne, R. (2015). Content-Adaptive Pentary Steganography Using the Multivariate Generalized Gaussian Cover Model. In Proc. International Society for Optics and Photonics, San Francisco, CA.

Song, X. F., Liu, F. L., Yang, C. F., Luo, X. Y., & Zhang, Y. (2015). Steganalysis of Adaptive JPEG Steganography Using 2D Gabor Filters. In *Proc. the 3rd ACM Workshop on Information Hiding and Multimedia Security,* New York, NY (pp. 15-23). doi:10.1145/2756601.2756608

Tang, W., Li, H., Luo, W., & Huang, J. W. (2016). Adaptive steganalysis based on embedding probabilities of pixels. *IEEE Transactions on Information Forensics and Security*, *11*(4), 734–745.

Wang, Z., & Bovik, A. (2002). A Universal Image Quality Index. *IEEE Signal Processing Letters*, *9*(3), 81–84. doi:10.1109/97.995823

Wang, Z., Bovik, A., Sheikh, H., & Simoncelli, E. (2004). Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE Transactions on Image Processing*, *13*(4), 600–612. doi:10.1109/TIP.2003.819861 PMID:15376593

Wang, Z. C., Yin, Z. Y., & Zhang, X. P. (in press). Distortion Function for JPEG Steganography Based on Image-Texture and Correlation in DCT Domain. *IETE Technical Review*.

Wang, Z. C., Zhang, X. P., & Yin, Z. X. (2016). Hybrid distortion function for JPEG steganography. *Journal of Electronic Imaging*, *25*(5). doi:10.1117/1.JEI.25.5.050501

Yu, J., Li, F. Y., Cheng, H., & Zhang, X. P. (2016). Spatial steganalysis using contrast of residuals. *IEEE Signal Processing Letters*, *23*(7), 989–992. doi:10.1109/LSP.2016.2575100

Zhang, W. M., Zhang, X. P., & Wang, S. Z. (2008). Maximizing Steganographic Embedding Efficiency by Combining Hamming Codes and Wet Paper Codes. In *Proc. 10th International Workshop on Information Hiding,* Santa Barbara, CA (pp. 60-71). doi:10.1007/978-3-540-88961-8_5

Zhang, X. P. (2011). Reversible Data Hiding in Encrypted Image. *IEEE Signal Processing Letters*, *18*(4), 255–258. doi:10.1109/LSP.2011.2114651

Zhang, X. P. (2012). Separable Reversible Data Hiding in Encrypted Image. *IEEE Transactions on Information Forensics and Security*, *7*(2), 826–832. doi:10.1109/TIFS.2011.2176120

Zhang, X. P. (2016). Behavior Steganography in Social Network. In *Proc. the 12th International Conference on Intelligent Information Hiding and Multimedia Signal Processing,* Kaohsiung, Taiwan (pp. 21-23).

Zhang, X. P., & Wang, S. Z. (2006). Efficient Steganographic Embedding by Exploiting Modification Direction. *IEEE Communications Letters*, *10*(11), 781–783. doi:10.1109/LCOMM.2006.060863

Zhenxing Qian received both the B.S. and the Ph.D. degrees from University of Science and Technology of China (USTC), in 2003 and 2007, respectively. He is currently a professor with the School of Computer Science, Fudan University, China. His research interests include data hiding and multimedia security. He has published over 80 papers on these topics.

Zichi Wang received the BS degree in electronics and information engineering from Shanghai University, China, in 2014, and the MS degree in signal and information processing from the same university in 2017. He is currently pursuing the PhD degree at Shanghai University, China. His research interests include steganography, steganalysis and reversible data hiding. He has published about 10 papers in these areas.

Xinpeng Zhang received the BS degree in computational mathematics from Jilin University, China, in 1995, and the ME and PhD degrees in communication and information system from Shanghai Univer-sity, China, in 2001 and 2004, respectively. Since 2004, he has been with the faculty of the School of Communication and Information Engineering, Shanghai Univer-sity, where he is currently a professor. His research interests include information hiding, image processing, and digital forensics. He has published over 200 papers in these areas.

Guorui Feng received the B.S. and M.S. degrees in computational mathematics from Jilin University, Changchun, China, in 1998 and 2001, respectively. He received the Ph.D. degree in electronic engineering from Shanghai Jiaotong University, Shanghai, China, in 2005. From 2006 to 2006, he was an Assistant Professor at East China Normal University, Shanghai. In 2007, he was a Research Fellow with Nanyang Technological University, Singapore. He is currently with the School of Communication and Information Engineering, Shanghai University, Shanghai. His current research interests include image processing, image analysis, and computational intelligence.