Journal of Information Hiding and Multimedia Signal Processing ©2010 ISSN 2073-4212
Ubiquitous International Volume **1**, Number **1**, January **2010**

A Secure Steganography Method based on Genetic Algorithm

Shen Wang, Bian Yang and Xiamu Niu

School of Computer Science and Technology
Harbin Institute of Technology
150080, Harbin, China
shen.wang@ict.hit.edu.cn; bian.yang@ict.hit.edu.cn; xiamu.niu@hit.edu.cn

Received April 2009; revised August 2009

Abstract. With the extensive application of steganography, it is challenged by steganalysis. The most notable steganalysis algorithm is the RS attack which detects the steg-message by the statistic analysis of pixel values. To ensure the security against the RS analysis, we presents a new steganography based on genetic algorithm in this paper. After embedding the secret message in LSB (least significant bit) of the cover image, the pixel values of the steg-image are modified by the genetic algorithm to keep their statistic characters. Thus, the existence of the secret message is hard to be detected by the RS analysis. Meanwhile, better visual quality can be achieved by the proposed algorithm. The experimental results demonstrate the proposed algorithm's effectiveness in resistance to steganalysis with better visual quality.

Keywords: steganography; steganalysis; genetic algorithm; RS algorithm

1. **Introduction.** Steganography is a branch of information hiding. It embeds the secret message in the cover media (e.g. image, audio, video, etc.) to hide the existence of the message. Steganography is often used in secrete communication. In recent years, many successful steganography methods have been proposed. Among all the methods, LSB (least significant bit) replacing method is widely used due to its simplicity and large capacity. The majority of LSB steganography algorithms embed messages in spatial domain, such as BPCS[**?**, **?**], PVD[**?**, **?**]. Some others, such as Jsteg[**?**, **?**], F5[**?**], Outguess[**?**, **?**], embed messages in DCT frequency domain (i.e. JPEG images). In the LSB steganography, secret message is converted into binary string. Then the least significant bit-plane is replaced by the binary string. The LSB embedding achieves good balance between the payload capacity and visual quality. However, the LSB replacing method flips one half of the least-significant bits. Thus the artifacts in the statistics of the image are easy to be detected[**?**].

Steganalysis is the method to reveal the hidden messages, even some doubtful media. The attacks on LSB replacing methods are most based on Chi-square analysis[**?**] and the relationship of pixels or bit–planes[**?**]. In the frequency domain, there are some steganalysis algorithms based on histogram and block effect[**?**]. Among the methods, the RS steganalysis[**?**], proposed by Fridrich, is considered as the most reliable and accurate method to the LSB–replacing steganography. It utilizes the regular and singular groups as the statistics to measure the relationship of pixels. In most nature images, strong correlation exists in adjacent pixels. After the LSB–replacing steganography, the correlation is decreased. Thus, the proportion between the regular and singular groups changes and

the existence of the steganography is detected. Moreover, the secrete message length can be estimated by the amount of regular and singular groups.

To resist to RS analysis, the influence on the correlation of pixels needs to be compensated. The compensation may be achieved by adjusting other bit planes. Nevertheless, the implementation may be computational infeasible. For example, if only two bit planes are modified in a 256×256 gray level image, there are 2^2 possible bit selections for each pixel. For the entire image, there are 2^{524288} times of adjustments. It is not feasible in the practical application. For this reason, optimization algorithms have been employed in information hiding to find the optimal embedding positions. For example, genetic algorithm was been exploited in digital watermarking[**?**, **?**, **?**].

In this paper, a novel stegano algorithm is proposed. The genetic algorithm [**?**] is used to estimate the best adjusting mode. By the adjustment, the artifacts caused by the steganography can be eliminated and the image quality will not be degraded. Experimental results of another RS-resistent method[**?**] are compared with the proposed one, and it is revealed that the proposed algorithm exhibits excellent security and image quality.

The rest of the paper is organized as follows. In Section **??**, the design and implementation of the algorithm are described in detail. The experimental results and discussion are presented in Section **??**. Section **??** concludes briefly our future work.

2. **The Proposed Algorithm.**

2.1. **RS analysis.** In RS steganalysis, 3 kinds of block flipping are defined. They are positive flipping F_1, negative flipping F_{-1} and 0 flipping F_0. F_1 is the transformation relationship between $2i$ and $2i+1$, (i.e. $0-1, 2-3, \ldots, 254-255$), which is same as LSB. F_{-1} is the transformation relationship between $2i-1$ and $2i$, i.e. $-1-0, 1-2, \ldots, 255-256$. The relationship between the two flipping is written as:

$$F_{-1} = F_1(x+1) - 1 \tag{1}$$

Similarly, define F_0 as the identity permutation

$$F_0(x) = x \tag{2}$$

F_0, F_1 and $F_{-1}$are called flipping functions. The flipped group is resulted from applying flipping functions on pixels of image block. It is denoted as:

$$F(G) = (F_{M(1)}(x_1), F_{M(2)}(x_2), \ldots, F_{M(n)}(x_n)) \tag{3}$$

$M = M(1), M(2), \ldots, M(n)$ is called a flipping mask, where $M(i)$ are 1, 0, or -1. G is regular if $f(F(G)) > f(G)$, G is singular if $f(F(G)) < f(G)$.

The RS analysis includes following steps. Firstly, the image is divided into non-overlapping blocks and each one is re-arranged into a vector $G = (x_1, x_2, \ldots, x_n)$ in the Zigzag scan order. The correlations of pixels can be determined by discrimination function:

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n-1} |x_i - x_{i+1}| \tag{4}$$

Where x is the pixel value and n is the number of pixels. The value of f represents the spatial correlation between the adjacent pixels. A small f means the strong correlation. After all the $f(G)$ are obtained, apply non-negative flipping (i.e. $M(1), M(2), \ldots, M(n) =$ 0 or 1) and non-positive flipping (i.e. $M(1), M(2), \ldots, M(n) = 0$ or -1) on each block. Then use Eq. **??** to calculate $f(F(G))$ in each block. The relative number of regular blocks after positive flipping is denoted as R_m, and that of singular blocks is denoted as

S_m. In the same way, R_{-m} and S_{-m} are defined as the relative number of regular and singular blocks after the negative flipping.

It is pointed out by Fridrich that in nature images, the numbers of aforementioned blocks hold the following relationships:

$$R_m \approx R_{-m}, S_m \approx S_{-m} \quad and \quad R_m > S_m, R_{-m} > S_{-m}$$

The difference between R_m and R_{-m} increases with the length of the embedded message. The same trend exists in the difference between S_m and S_{-m}.

2.2. **Our genetic based approach.** Based on the above discussions, we adjust the pixel values to make $R_m \approx S_m, R_{-m} \approx S_{-m}$. As the changes of the bits in higher planes will degrade the visual effect of the steg-image, only the second and third lowest bit-planes are modified. For example, B is the original value of an image block. If only the second lowest bit-plane is modified, the change between the original block and modified block can be considered as an adjustment matrix like A_1 or A_2. The modified image blocks are $B_1^{'} = B + A_1$ and $B_2^{'} = B + A_2$. Here, we will use one example to illustrate this process. For the original block B, $f(B) = 99$ and $f(F_-(B)) = 120$, where F_- is the non-positive flipping. For the modified block $B_1^{'}$, $f(F_-(B_1^{'})) = 90$, if F is non-positive flipping. For another modified block $B_2^{'}$, $f(F_-(B_2^{'})) = 150$. In summary, the type (regular or singular) of the block can be changed by a proper adjustment. Hence, the RS analysis cannot detect the existence of the steg-message.

$$B = \begin{bmatrix} 107 & 109 & 107 & 105 & 104 & 102 & 102 & 104 \\ 107 & 106 & 105 & 104 & 105 & 103 & 105 & 102 \\ 107 & 105 & 107 & 105 & 102 & 103 & 104 & 103 \\ 107 & 107 & 105 & 106 & 104 & 103 & 103 & 104 \\ 107 & 109 & 107 & 104 & 104 & 102 & 103 & 102 \\ 104 & 107 & 106 & 103 & 103 & 104 & 102 & 100 \\ 110 & 109 & 109 & 105 & 105 & 105 & 105 & 102 \\ 109 & 109 & 109 & 106 & 104 & 105 & 105 & 104 \end{bmatrix}$$

$$A_1 = \begin{bmatrix} 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 \\ 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 0 & 0 & 2 & 0 & 2 \\ 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 \\ 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 & 2 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 2 & 2 & 2 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 \\ 2 & 2 & 0 & 2 & 2 & 0 & 0 & 2 \end{bmatrix}$$

In this paper, we adopt genetic algorithm to search for a best adjustment matrix. Genetic algorithm is a general optimization algorithm. It transforms an optimization or search problem as the process of chromosome evolution. When the best individual is selected after several generations, the optimum or sub-optimum solution is found. The

three most important operations of genetic algorithm are reproduction, crossover and mutation. The adaptive values affect the copy operation. In general, the individuals with larger fitness values have higher possibilities to be selected to breed the next generation. Figure **??** shows the proposed genetic based algorithm in detail.

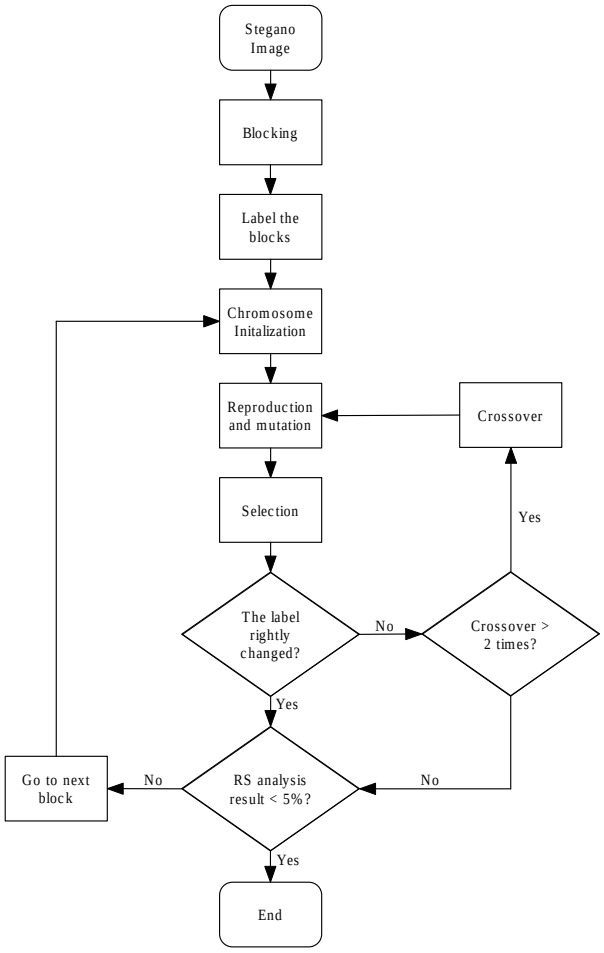

FIGURE 1. Procedure of proposed algorithm

After embedding the secret message in cover image by LSB. The adjustment is proceeded as follows:

Firstly, the steg-image is divided into 8×8 blocks. Secondly, the blocks are classified and labeled by follow steps:

1. For a block B, apply the non-positive flipping F_- and the non-negative flipping F_+ on the block. The flipping mask $M+$ and $M-$ are generated randomly. The result is B'_+ and B'_-.
2. calculate $f(B'_+)$, $f(B'_-)$ and $f(B)$.
3. do step 1 and 2 5000 times. Define four variables to categorize the blocks by comparison of $f(B'_+)$, $f(B'_-)$ and $f(B)$.
   - P_{+R}, the count of the occurrence when the block is regular under the non-negative flipping.
   - P_{+S}, the count of the occurrence when the block is singular under the non-negative flipping.
   - P_{-R}, the count of the occurrence when the block is regular under the non-positive flipping.

- P_{-S}, the count of the occurrence when the block is singular under the non-positive flipping.

4. compare P_{+R} to P_{+S} and P_{-R} to P_{-S}, and the labels of the block are determined:
   - $R+$, if $P_{+R}/P_{+S} > 1.8$.
   - $S+$, if $P_{+S}/P_{+R} > 1.8$.
   - $R-$, if $P_{-R}/P_{-S} > 1.8$.
   - $S-$, if $P_{-S}/P_{-R} > 1.8$.
5. at last, the blocks are categorized into 4 groups $R+R-$, $R+S-$, $S+R-$, $S+S-$. The blocks, which are not included in the 4 categories, are not processed in follow steps.

Compared with the original image, the amounts of $R+R-$ and $S+R-$ blocks are increased in the steg-images. This phenomenon can be detected by the RS analysis. The target of our algorithm is to decrease the amount of $R-$ blocks. We use genetic method to adjust them in follow steps:

1. Initialization. From the first pixel, select every 3 adjacent pixels in the block as the initial chromosomes C(shown in Figure **??**).

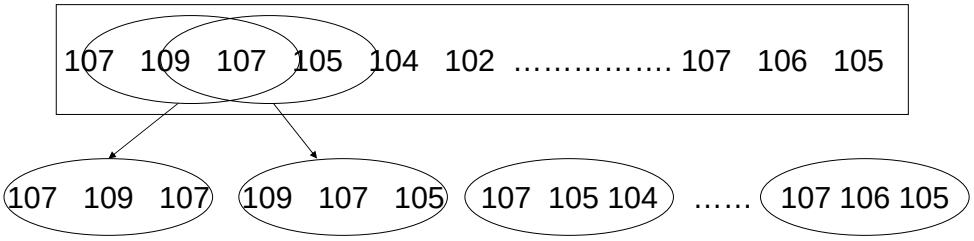

FIGURE 2. choosing chromosomes

2. Reproduction and Mutation. Flip the second lowest bits in the chromosomes randomly, the several second generation chromosomes C_i are generated.
3. Selection. Select the best chromosome, which maximize the fitness function (Equation **??**), to replace its corresponding initial chromosome.

$$Fitness = \alpha(e_1 + e_2) + PSNR \qquad \alpha \ldots \text{weight} \tag{5}$$

   e_1 is the probability of $f(F_-(C_i)) < f(C_i)$ and e_2 is the probability of $f(F_+(C_i)) > f(C_i)$. PSNR is the peak signal-to-noise ratio of the chromosome. α is the weight decided empirically. The factor α is used to control the weights of the visual quality of the steg-image and the secrecy of the embedded message. For a given α, higher e_1 and e_2 demonstrate a higher security of the stego algorithm. Therefore, we aim at maximizing the value of fitness function. In this step, e_1 and e_2 must be larger than threshold T, which is an decided by the user. The minimum of T is 50%.
4. Calculate P_{-R} and P_{-S} of the adjusted image block. If $P_{-S} > P_{-R}$, the block is successfully adjusted.
5. Crossover. Shift the chromosomes one pixel, goto step 2. If crossover has been applied two times, stop the cycle.

After a block is adjusted, calculate R_m ,R_{-m}, S_m and S_{-m} of the image. If the difference between R_m and R_{-m} is more than 5%, or the the difference between S_m and S_{-m} is more than 5%, adjust the next block.

In our algorithm, the blocks are labeled before the adjustment. Thus, the computational complexity is reduced. The usage of the genetic method avoids the exhausting searching and the algorithm is easy to be implemented.

3. **Experimental Results and Discussion.** Two 256×256 gray–level images are used as cover images as shown in Figure **??**. The embedding capacity is 90%.

(a) Lena (b) Lake

FIGURE 3. Cover image

Firstly, RS steganalysis is applied on the the two cover images (Lena, Lake) and the results are shown in Table **??**. The results on the steg-images are shown in Table **??**. In the cover images, $R_m \approx R_{-m}$ and $S_m \approx S_{-m}$. In Table **??**, it is found that the value of $|R_m - R_{-m}|$ and $|S_m - S_{-m}|$ increases with the embedding capacity. So the adjustment becomes more difficult.

TABLE 1. RS steganalysis result of cover images

Cover image	$\|R_m - R_{-m}\|$	$\|S_m - S_{-m}\|$
Lena	0.0078	0.0088
Lake	0.0020	0.0010

TABLE 2. RS steganalysis result of steg-images

Cover image	$\|R_m - R_{-m}\|$	$\|S_m - S_{-m}\|$
Lena 30%	0.097	0.090
Lena 60%	0.161	0.140
Lena 90%	0.291	0.263
Lake 30%	0.088	0.064
Lake 60%	0.178	0.153
Lake 90%	0.252	0.220

The result of RS steganalysis and PSNR with different genetic parameters are shown in Table **??**. The data illustrate the relationship between security and image quality. As the T increases from 0.5 to 0.88. The PSNR decreases about 1dB. The steganography is more undetectable with a larger T, degradations of the visual quality of the steg-images are observed. In all conditions, the $|R_m - R_{-m}|$ and $|S_m - S_{-m}|$ is less than 5%, when the RS analysis is not reliable.

TABLE 3. RS steganalysis parameters with variable weights

Cover image	T	$\|R_m - R_{-m}\|$	$\|S_m - S_{-m}\|$	PSNR
Lena	0.88	2.79	2.03	41.7
	0.5	3.69	3.32	42.6
Lake	0.88	3.29	2.76	40.3
	0.5	3.70	3.01	40.7

In [**?**], Marcal presents an RS resistant method by using reversible histogram transform, where secrete images are hidden in the cover image after the histogram transform. The

results of our algorithm and the one in [**?**] are compared in Table **??**. As can be seen form Table 1, the proposed algorithm outperforms the one in [14]

TABLE 4. RS steganalysis parameters for image without message embedding

Cover image	$\lvert R_m - R_{-m}\rvert$	$\lvert S_m - S_{-m}\rvert$
Lena	2.79	2.03
Paper[**?**]	3.39	2.35
Lake	3.29	2.76
Paper[**?**]	4.97	3.59

Figure **??** shows the image with secret messages. Because the visual quality of the images is well preserved by our algorithm, no visible artifact is introduced by the adjustment.

(a) Lena

(b) Lake

FIGURE 4. Stego image

4. **Conclusions.** A secure stegano algorithm based on the genetic method is proposed in this paper. Benefited from the effective optimization, a good balance between the security and the image quality is achieved. Our future work will focus on improving the efficiency of the proposed algorithm.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (Project Number: 60703011, 60832010, 60671064), the Chinese national 863 Program (Project Number: 2007AA01Z458), and The Research Fund for the Doctoral Program of Higher Education(RFDP: 20070213047).

REFERENCES

[1] Steganography software for windows, http://members.tripod.com/steganography/stego/software.html.
[2] S. C. Chu, H. C. Huang, Y. Shi, S. Y. Wu, and C. S. Shieh, Genetic watermarking for zerotree-based applications. *Circuits, Systems, and Signal Processing*, vol. 27, no. 2, pp. 171-182, 2008.
[3] J. Fridrich, M. Goljan, and R. Du, Detecting lsb steganography in color, and gray-scale images, *IEEE MultiMedia*, pp. 22–28, 2001.
[4] J. Fridrich, M. Goljan, and D. Hogea. Attacking the outguess, *Proc. of ACM Workshop Multimedia and Security*, 2002.
[5] J. Fridrich, M. Goljan, and D. Hogea, Steganalysis of jpeg images: Breaking the f5 algorithm, *Proc. of ACM Workshop on Multimedia and Security 2002*, 2002.
[6] D. E. Goldberg, *The genetic algorithms in search, optimization and machine learning*, Addison-Wesley, 1989.
[7] C. T. Hsu, J. Wu, and L. Hidden, Digital watermarks in images, *IEEE Trans. Image Processing*, pp. 58-68, 1999.
[8] H. C. Huang, C. M. Chu, and J. S. Pan, The optimized copyright protection system with genetic watermarking, *Soft Computing*, vol. 13, no. 4, pp. 333–343, 2009.
[9] H. C. Huang, J. S. Pan, Y. H. Huang, F. H. Wang, and K. C. Huang, Progressive watermarking techniques using genetic algorithms, *Circuits, Systems, and Signal Processing*, vol. 26, no. 5, pp. 671–687, 2007.

[10] E. Kawaguchi and R. O. Eason, Principle and application of bpcs-steganography, *Proc. of SPIE:Multimedia Systems and Applications*, pp. 464–472, 1998.

[11] A. R. S. Marcal and P. R. Pereira, A steganographic method for digital images robust to rs steganalysis, *Lecture Notes in Computer Science*, pp. 1192–1199, 2005.

[12] N. Provos, Steganography detection with stegdetect, http://www.outguess.org/detection.php.

[13] A. Westfeld, F5-a steganographic algorithm, *Proc. of the 4th International Workshop on Information Hiding, Lecture Notes in Computer Science,2137.Springer-Verlag*, pp. 289–302, 2001.

[14] A. Westfeld and A. Pfitzmann, Attacks on steganographic systems, *Proc. of Information Hiding-Third International Workshop*, 1999.

[15] A. Westfeld and A. Pfitzmann, Attacks on steganographic systems, *Lecture Notes in Computer Science*, pp. 61–76, 1999.

[16] D. C. Wu and W. H. Tsai, A steganographic method for images by pixel-value differencing, *Pattern Recognition Letters*, pp. 1613–1626, 2003.

[17] X. Zhang and S. Z. Wang, Statistical analysis against spatial bpcs steganography, *Computer-Aided Design & Computer Graphics*, pp. 395–406, 2003.

[18] X. Zhang and S. Z. Wang, Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security, *Pattern Recognition Letters*, pp. 331–339, 2004.