An Improvement of Robust and Blind Data Hiding Based on Self Reference in Spatial Domain

JIUN-JIAN LIAW, LIN-HUANG CHANG, YU-SHENG LIAO
Graduate Institute of Networking and Communication Engineering
Chaoyang University of Technology
168 Jifong E. Rd., Wufong Township, Taichung County, 41349
TAIWAN (R.O.C)

Abstract: - According to the recent growth of communication technologies, to protect the transmitting secret data is important. Information hiding schemes have become popular research topic in recent years. In data hiding, the properties of robustness, blindness, and quality are important. In this paper, an improvement of a blind image data hiding method base on self reference in spatial domain is proposed. We replace the original single percentage tolerance with the variable tolerance method and the immovable tolerance method. The experimental results show that the proposed blind technique not only can improve the robustness to withstand compression, but also increase the quality of the stego-image.

Key-Words: - Data hiding; Watermarking; Blindness; Robustness; Image quality; Image processing.

1 Introduction

Since Internet is a public transmission way and it is widely applied in many applications, we can send and receive digital data, such as images, by connected networks. With the recent growth of communication technologies, to conceal data in transmitting message for prevent the illegal copying or protect the secret is very important. Data encryption [1] and information hiding [2] schemes are developed to protect the secret data. Data encryption methods make the secret data into meaningless bits. On the other hand, information hiding techniques hides the message into a meaningful multimedia data. Many techniques for information hiding have been proposed in the literature [3].

Data hiding [4] or watermarking [5][6] are used to hide the secret data (such as the private message or the copyright) into a meaningful host image to distract the attention of the observers. These methods are based on the human visual system which can not recognize tiny difference [7]. In these techniques, the cover-image is used to hide the secret information and the stego-image is the cover- image with the secret data embedded in [8].

The least-significant-bits (LSBs) is the most well-known data hiding scheme which is based on replacing the least bits of pixels in the cover-image with the secret data bits [9]. Some varieties of LSBs are proposed to improve the security and the quality of the stego-image, such as the exhaustive method [10], the dynamic programming strategy scheme [11] and embedding the variable sizes according to the human visual system [12]. However, methods of LSBs are not robust for some processing or attacks (such as low pass filtering, resizing, or lossy compression, etc).

In the specific application, such as the image compression, the stego-image will be compressed and then be transmitted through Internet or other communication. The goal of data compression is to convey the information in a capacity as small as possible. The compressed stego-image saves storage and it can be transmitted faster. On the other hand, data hiding tries to inset additional bits into the original capacity [13]. In fact, the additional bits of data can not improve the compression efficiency. Moreover, the secret information may be broken by compression processing. From the above, a useful data hiding technique should be robust to withstand attack of compression.

Depending on requires of extracting the hided secret data from stego-image, data hiding techniques can be classified into non-blind detection and blind detection. In non-blind detection, extra information for the extraction of the secret data is necessary [14]. On the other hand, blind detection schemes can recover the hided data via stego-image itself [15]. Since to transmit stego-image with extra information is not convenient, blind data hiding techniques are more useful than non-blind method. However, blind data hiding schemes are often less robust than non-blind ones.

From the above mentioned methods, we can see that properties of robustness and blindness are important in data hiding schemes. Moreover, since

the data hiding methods are based on the human visual system, the over-image and the stego-image should be similarity. In other words, the quality of the stego-image is also important.

According to the importance of data hiding, Wang and Pearmain propose a blind image data hiding method [15] (we call it the Wang's method) and this technique reveals robustness image compression attack. The Wang's method is based on relative modulation of pixel value and discrete cosine transform (DCT) coefficient value in spatial domain and frequency domain, respectively. The frequency domain based method reveals extraordinary robustness attacks. But the robustness of spatial domain based method is weak.

In this paper, an improvement of the Wang's method in the spatial domain is proposed. We replace the Wang's percentage tolerance with two types of tolerance (the variable method and the immovable method). The experimental results show that the proposed technique not only can improve the robustness, but also increase the quality of the stego-image.

2 Review of Wang's Method

In this section, we introduce the Wang's method which is based on the pixel value in spatial domain.

We segment the cover-image into non-overlapping blocks. Each size of block is 3 × 3. In each block, the central pixel value, which is denoted as L_r, is used to embed a bit of secret data. We compute the mean value, which is denoted as L_m, of pixels in the block area except the central pixel.

To embed bit 1, the value of central pixel in the stego-image should be more than or equal to L_m. For this reason, we change the value L_r, if needed, to make sure that L_r is more than or equal to $L_m + \delta$. Similarly, to embed bit 0, the value of central pixel in the stego-image should be less than L_m. For this reason, we change the value L_r, if needed, to make sure that L_r is less than $L_m - \delta$. The value of δ is a tolerance and it is chosen as from 5% to 10% of L_r.

The extraction is processed by a comparison of between L_r and L_m. If L_r is more than or equal to L_m, then the extracted bit is 1, otherwise, the extracted bit is 0.

In the Wang's method, the mean value, L_m, is used to be a base to compare the magnitude with the central pixel value. The tolerance, δ, is also used to be the buffer when the stego-image is compressed or attacked.

It is easy to see that the difference between the cover-image and the stego-image is depending on the value of δ. Since the value of δ is chosen as from 5% to 10% of L_r, obviously, δ is small when L_r is small and δ is big when L_r is big. That is, a small δ makes high quality and weak robustness, but a big δ makes low quality and strong robustness.

3 Proposed Method

The goal of the proposed method is to increase the robustness with small L_r and to enhance the quality with big L_r. In this paper, there are two types of the proposed method. These methods are called variable tolerance and immoveable tolerance and they are summary as follows.

3.1 Variable Tolerance

We divide the range of the pixel value into four sub-ranges which are denoted as r_1, r_2, r_3, and r_4, respectively (see Fig.1).

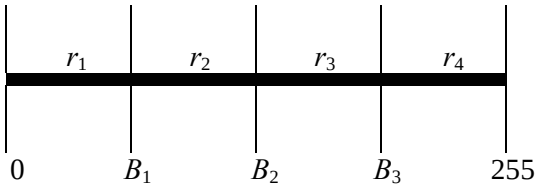


Fig.1. Divided sub-ranges in the pixel value.

When we want to embed a bit into the central pixel of a block, we check the central pixel value (L_r) is in which sub-range, i.e.,

$$L_r \in r_1, \text{ if } 0 \le L_r < B_1, \quad (1)$$

$$L_r \in r_2, \text{ if } B_1 \le L_r < B_2, \quad (2)$$

$$L_r \in r_3, \text{ if } B_2 \le L_r < B_3, \quad (3)$$

and

$$L_r \in r_4, \text{ if } B_3 \le L_r \le 255, \quad (4)$$

where 0, B_1, B_2, B_3, and 255 are boundaries of each sub-range.

In the different sub-range, we define the different percentage, which is denoted as p_i, for computing the tolerance. That is, we set the tolerance value, δ, is the product of L_r and p_i, i.e.,

$$\delta = p_i \times L_r, \text{ if } L_r \in r_i, \quad (5)$$

where i = 1, 2, 3, 4.

3.2 Immovable Tolerance

In the variable tolerance method, we set a small percentage when the central pixel value is big and set a big percentage when the central pixel value is small

to steady the value of tolerance (δ). In the immovable tolerance method, we do not set any ratio to define δ with L_r. Instead, we just set the tolerance value as a constant.

4 Experiments

In our experiments, we embed the same secret data bits which are randomized generated into the cover-images via the Wang's method, the variable tolerance method and the immovable tolerance method, respectively.

The settings of parameters in the variable tolerance method are $B_1 = 54$, $B_2 = 108$, $B_3 = 162$, $p_1 = 0.15$, $p_2 = 0.1$, $p_3 = 0.06$, and $p_4 = 0.04$. The value of δ in the immovable tolerance method is set from 5 to 10. We use the peak signal to noise ration (*PSNR*) to be a measure of the stego-image quality. A larger value of *PSNR* means that the difference between cover-image and stego-image is small. *PSNR* is defined as follows [16]:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}, \tag{6}$$

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C_{xy} - S_{xy})^2, \tag{7}$$

where the image size is $M \times N$ pixels, and C_{xy} and S_{xy} represent the pixel value of the cover-image and the stego-image respectively.

After the stego-images are obtained, we apply JPG compression to each stego-image by PhotoShop CS2 9.0 with high, middle, and low compression qualities. The compression index of the high quality, middle quality, and low quality are set to be 12, 11, and 10, respectively, in PhotoShop.

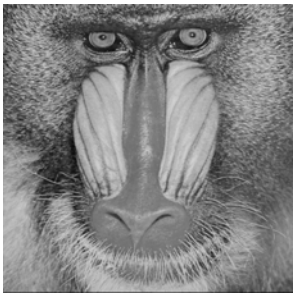
We extract secret data bits from the compressed stego-image and compare with the original data to count the number of error bits.

In our experiments, we use four images, Lena, Man, Baboon, and Peppers (as shown in Fig.2), to be cover-images in our experiments. Each size of the cover-image is 512 by 512 pixels. Since the cover-image is segmented into non-overlapping 3×3 blocks and each block is used to embed 1 bit, the capacity of each cover-image is 28,900 bits.

The experiment results of error bits of high compression quality, middle compress quality, and low compress quality are shown in Table 1, Table 2, and Table 3, respectively. The measured *PSNR* via different methods is also shown in Table 4. Take note of that the tolerance 1-6 are 5-10% of L_r in the Wang's method and 5-10 pixel value in the immovable tolerance method, respectively.

(a) Lena

(b) Man



(c) Baboon

(d) Peppers

Fig.2. Cover-images.

Table 1. Error bits with high compression quality.

Image	Method	Tolerance					
		1	2	3	4	5	6
Fig.2(a)	Wang's	76	28	9	2	0	0
	Immovable	0	0	0	0	0	0
	Variable	0					
Fig.2(b)	Wang's	157	47	29	0	0	0
	Immovable	0	0	0	0	0	0
	Variable	0					
Fig.2(c)	Wang's	62	34	18	12	8	5
	Immovable	0	0	0	0	0	0
	Variable	0					
Fig.2(d)	Wang's	579	488	412	346	306	269
	Immovable	0	0	0	0	0	0
	Variable	0					

Table 2. Error bits with middle compression quality.

Image	Method	Tolerance					
		1	2	3	4	5	6
Fig.2(a)	Wang's	490	302	181	113	64	38
	Immovable	43	5	0	0	0	0
	Variable	3					
Fig.2(b)	Wang's	867	567	416	183	144	89
	Immovable	41	4	0	0	0	0
	Variable	6					
Fig.2(c)	Wang's	267	161	101	66	43	32
	Immovable	27	2	0	0	0	0
	Variable	1					
Fig.2(d)	Wang's	936	762	646	562	510	464

	Immovable	36	3	0	0	0	0
	Variable	2					

Table 3. Error bits with low compression quality.

Image	Method	Tolerance					
		1	2	3	4	5	6
Fig.2(a)	Wang's	1693	1207	873	657	478	360
	Immovable	1168	553	241	99	38	15
	Variable	246					
Fig.2(b)	Wang's	2370	1773	1378	930	762	581
	Immovable	1197	586	262	102	41	15
	Variable	316					
Fig.2(c)	Wang's	937	590	386	273	194	142
	Immovable	836	396	171	66	22	7
	Variable	191					
Fig.2(d)	Wang's	1971	1533	1248	1051	910	818
	Immovable	1058	509	215	82	30	10
	Variable	268					

Table 4. *PSNR* in different methods.

Image	Method	Tolerance					
		1	2	3	4	5	6
Fig.2(a)	Wang's	39.5	38.4	37.4	36.5	35.6	34.8
	Immovable	40.5	39.6	38.7	37.9	37.2	36.5
	Variable	38.3					
Fig.2(b)	Wang's	38.5	37.7	36.9	36.2	35.5	34.8
	Immovable	38.9	38.3	37.6	36.9	36.3	35.7
	Variable	37.3					
Fig.2(c)	Wang's	33.1	32.7	32.3	31.9	31.5	31.1
	Immovable	33.4	33.1	32.8	32.5	32.2	31.9
	Variable	32.7					
Fig.2(d)	Wang's	38.7	37.7	36.9	36.1	35.3	34.6
	Immovable	39.4	38.8	38.0	37.3	36.7	36.0
	Variable	37.7					

According to the experiment results, we can see that the proposed method reduces more number of error bits than the Wang's method. And the proposed method makes the higher quality of the stego-image than the Wang's method does.

5 Conclusion

In this paper, we proposed an improvement of the Wang's method. The goal of the proposed method is not only to increase the robustness for compression, but also to enhance the quality of the stego-image. There are two types of the proposed method, we call them as the variable tolerance method and the immovable tolerance method. According to the experiment results, both proposed methods make fewer error bits and obtain a higher quality of the stego-image.

References:

[1] H. J. Highland, Data encryption: a non-mathematical approach, Computers & Security, Vol. 16, No. 5, 1997, pp. 369-386.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, Information hiding – a survey, *Proceedings of IEEE*, Vol. 87, No. 7, 1999, pp. 1062-1078.

[3] C.-K. Chan, and L.M. Cheng, Hiding data in images by simple LSB substitution, *Pattern Recognition*, Vol. 37, No. 3, 2004, pp. 469-474.

[4] W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, *IBM Systems Journal*, Vol. 35, No. 3-4, 1996, pp. 313-336.

[5] P.-L. Lin, Robust transparent image watermarking system with spatial mechanisms, *Journal of Systems and Software*, Vol. 50, No. 2, 2000, pp. 107-116.

[6] M. A. Suhail, and M. S. Obaidat, Digital watermarking-based DCT and JPEG model, *IEEE Transactions on Instrumentation and Measurement,* Vol. 52, No. 5, 2003, pp. 1640-1647.

[7] J. Huang, Y. Q. Shi, and Y. Shi, Embedding Image Watermarks in DC Components, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 10, No. 6, 2000, pp. 974- 979.

[8] S.-L. Li, K.-C. Leung, L.M. Cheng, and C.-K. Chan, A novel image-hiding scheme based on block difference, *Pattern Recognition*, Vol. 39, No. 6, 2006, pp. 1168-1176.

[9] S. Walton, Image authentication for a slippery new age, *Dr. Dobb's Journal*, Vol. 20, No. 4, 1995, pp. 18-26.

[10] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, *Pattern Recognition*, Vol. 34, No. 3, 2001, pp. 671-683.

[11] C.-C. Chang, J.-Y. Hsiao, and C.-S. Chan, Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy, *Pattern Recognition*, Vol. 36, No. 7, 2003, pp. 1583-1595.

[12] Y.-K. Lee, and L.-H. Chen, High capacity steganographic model, *IEE Proceedings: Vision, Image and Signal Processing*, Vol. 147, No. 3, 2000, pp. 288-295.

[13] M. Ramkumar, and A. N. Akansu, On the design of data hiding methods robust to lossy compression, *IEEE Transactions on multimedia*, Vol. 6, No. 6, 2004, pp. 947-951.

[14] W.-G. Kim, J. C. Lee, and W. D. Lee, Image watermarking scheme with hidden signatures,

IEEE Proceedings of International Conference on Image Processing, Vol. 2, 1999, pp. 206-210.

[15] Y. Wang, and A. Pearmain, Blind image data hiding based on self reference, *Pattern Recognition Letters*, Vol. 25, No. 15, 2004, pp. 1681-1689.

[16] D.-C. Lou, H.-K Tso, and J.-L. Liu, A copyright protection scheme for digital images using visual cryptography technique, *Computer Standards & Interfaces*, Vol. 29, No.1, 2007, pp. 125-131.