최소 왜곡을 위한 새로운 스테가노그래피 방법

A New Steganographic Method with Minimum Distortion

롱구이 장, 아미루자만, 김 형 중*
(Rongyue Zhang, Amiruzzaman Md. and Hyoung Joong Kim*)

Abstract: In this paper a new steganographic method is presented with minimum distortion. This paper focused on DCT rounding error and optimized that in a very easy way, resulting stego image has less distortion than other existing methods. The proposed method compared with F5 steganography algorithm, and the proposed method achieved better performance. This paper considered the DCT rounding error for lower distortion with possibly higher embedding capacity.

Keywords: Steganography, JPEG image, coefficient, rounding error, distortions.

I. Introduction

As more and more data hiding techniques are developed and improved, Steganalysis techniques are also advanced. As the Steganalysis advances, the steganography becomes more complicated. Least significant bit (LSB) modification method is considered as a pioneer work of steganography. LSB modification and LSB matching have two different application areas. LSB modification is popular for uncompressed domain, while LSB matching is popular for compressed domain. It is found that detection processes of these techniques are also different. Nowadays, steganographic techniques are getting more secure against statistical attacks and undetectable by other different attacks. Many innovative steganographic algorithms are developed within last decade. Among them, [4], [5], [6], [7], [8] are most popular. However, many researchers are also having interest to break steganographic schemes. There are several steganalysis methods invented within last decade [3], [9]. Among them statistical attack [9] is one of the most popular and effective attacks in steganographic world. Another famous attack are the calibrated statistics attack [1], [2].

Data hiding methods have to be designed to make them secure from statistical attack because this attack is relatively easy to combat. Simple solution against this attack is keeping the same or similar stego image histogram to the original image histogram. However, keeping the same shape of a magnitude histogram is not easy to achieve as long as the coefficient magnitudes are altered.

Note that one branch of past history of steganography was inventing methods to preserve the original histogram perfectly. LSB overwriting methods including OutGuess [4] can preserve the original histogram almost perfect (in fact, not absolutely perfect). This method modifies half of the nonzero coefficients and corrects the distorted histogram by adjusting with the rest of unused coefficients. In general, perfect preservation is not possible because data pattern is not ideal, but random.

The most popular and revoultionary method is F5 by Westfeld [9]. F5 method [9] also tries to narrow the gap between original and modified histograms by decrementing nonzero JPEG coefficients to 0 and applying matrix embedding and permutative straddling.

Sallee models the marginal distribution of DCT coefficients in JPEG-compressed images by the generalized Cauchy distribution [5]. Thus, the embedded message is adapted to the generalized Cauchy distribution using arithmetic coding. Arithmetic coding transforms unevenly distributed bit streams into shorter, uniform ones. This procedure is known as MB1. One weak point of the MB1 is that block artifact increases with growing size of the payload. MB2 has presented a method to overcome this weakness [6]. The MB2 embeds message in the same way as MB1 does, but its embedding capacity is only half of that of MB1. The other half of the nonzero DCT coefficients is reserved for de-blocking purpose. For the first time, in [10], mentioned about the distortion by rounding operation in JPEG image processing. In their paper they gave a detail description of rounding errors. They also proposed an embedding technique by LSB modification with a modified matrix embedding. In this proposed method a instead of matrix a group to coefficient is used. The main advantage of the proposed method is variable length of group, easy to implement and easy to control the hiding capacity.

The rest of this paper is organized as follows: In Section 2, the proposed method. Section 3 summarizes experimental results. Section 4 is discussion and, Section 5 concludes the paper.

II. Proposed Method

At first this method collected all nonzero AC coefficients in a one-dimensional array, another array used to keep all the information of rounding error. Before rounding the AC coefficients during DCT operation, that value used to calculate rounding error. DCT AC coefficients without rounding is denoted by r_i, where $i = 1, 2, 3 \ldots n$ (Eqn. 1), after rounding the same AC coefficient is also considered and denoted by r'_i, where $i = 1, 2, 3 \ldots n$ (Eqn. 2) and the rounding error calculated by subtracting without rounding the AC coefficient value from after rounding the AC coefficient value. The rounding error is denoted by e_i, where $i = 1, 2, 3 \ldots n$ (see Eqn. 3) and saved that value in rounding error record array (see Eqn. 3)

$$r_i = AC\ coefficients\ (before\ rounding) \quad (1)$$

$$r'_i = AC\ coefficients\ (after\ rounding) \quad (2)$$

$$e_i = r'_i - r_i \quad (3)$$

Later, the rounding error record array used to choose AC coefficient for modification with minimum distortion. As a result, the modified image after data hiding has less distortion.

It is observed that during rounding some value which is bigger than 1 but smaller than 2 is became 2 (after rounding), similarly some value

* Hyoung Joong Kim (Corresponding Author)
논문접수 : 2008. 08. 12., 채택확정 : 2008. x. xx.
롱구이 장, 아미루자만, 김 형 중 : 고려대학교 정보보호대학원
(ryue.zh@gmail.com, amir@korea.ac.kr, khj-@korea.ac.kr)
※본 연구는 ITRC(Information Technology Research Center)와 MIC(Ministry of Information and Communication, Korea)의 지원을 받아 연구되었음.

which is bigger than 2 but smaller than 3 is also became 2. Such as if any DCT AC coefficient value is 1.6 (before rounding) then after rounding this value will be 2, and if any DCT AC coefficient value is 2.3 (before rounding) then after rounding this value also will be 2.

In general, all other data hiding methods modified all the coefficients either by adding 1 or subtracting 1, did not consider about the distortion. The existing method did not consider about rounding error, and resulting stego image has higher distortion than the proposed method.

During the coefficient modification the proposed method was always careful about Eqn. 4, and using r''_i (where $i = 1, 2, 3 \ldots n$) value calculated e'_i (where $i = 1, 2, 3 \ldots n$) value

$$r''_i = \begin{cases} r'_i + 1 \text{ if } e_i < 0 \text{ and } r_i \neq \\ r'_i - 1 \text{ if } e_i \geq 0 \text{ and } r_i \neq \\ 2 \text{ if } r_i = -1 \\ -2 \text{ 1 if } r_i = -1 \end{cases} \quad (4)$$

Using e'_i where $i = 1, 2, 3 \ldots n$ (see Eqn. 5) and e_i where $i = 1, 2, 3 \ldots n$ (see Eqn. 3) the proposed method calculated the modification distortion (see Eqn. 6). The intension of the proposed method was to keep the distortion value as smaller as possible.

$$e'_i = r''_i - r_i \quad (5)$$

$$distortion = ||e'_i| - |e_i|| \quad (6)$$

Example as the proposed method is keeping all the information about rounding error. Thus during modification this method try to keep least error and resulting stego image has lest distortion. Such as if one AC coefficient value is 1.63 (before rounding), this value will move to 2 after rounding. Thus the rounding error for this particular AC coefficient is (2 – 1.63 = 0.37), as this AC coefficient is a even number (i.e., after rounding), to make this number odd there is two choices, either adding by 1 or subtracting by 1 (e.g., 2 +1 = 3 (odd), again 2 -1 = 1 (odd)). If any method will add by 1 then the distance with the original value will be (|3 – 1.63| = 1.37), now if any method will subtract by 1 then the distance between the original value and modified value will be (|1 – 1.63| = 0.63). This proposed method always took the smaller distance and hide data.

This method embeds the hidden message in a smarter way, at first collects all the nonzero AC coefficients in a single array. This method finds the sum of a group of elements. The group of element is determined by α (where, α = 1, 2, 3 … *n*). From α, all LSB bits was counted and made a sum, if the sum was odd and this method has to hide 0 then only one element was changed in order to make the sum even. Similarly, when the sum was even and this method has to hide 1 then only one element was changed in order to make the sum odd. The embedding capacity and number of element in a group is controlled by using Eqn. 7. The element for modification was made by following the distortion table.

$$capacity = \left\lfloor \frac{1}{\alpha} \right\rfloor \quad (7)$$

III. Experimental Results and Comparisons

The proposed method tested over 1173 gray scale image and successfully obtained better results. The proposed method and F5 method compared with two different image quality factor (QF).

In case of QF = 50, it is found that F5 algorithm has higher Steganalysis error probability than the proposed method. With 5% data hiding capacity F5 algorithm has 23.085 Steganalysis error probability, while the proposed method has 44.8041 (for the best situation the error probability is 50%). With 10% data hiding capacity and with QF = 50, F5 algorithm has 4.5997 Steganalysis error probability, while the proposed method has 33.0494. With 15% data hiding capacity and with QF = 50, F5 algorithm has 2.0443 Steganalysis error probability, while the proposed method has 18.9949. Again, with 20% data hiding capacity and with QF = 50, F5 algorithm has 0.5111 Steganalysis error probability; while the proposed method has 4.4293 (see Table 1).

Similarly, with 5% data hiding capacity and QF = 75, F5 algorithm has 18.3986 Steganalysis error probability, while the proposed method has 44.9744. With 10% data hiding capacity and with QF = 75, F5 algorithm has 2.1995 Steganalysis error probability, while the proposed method has 33.3049. With 15% data hiding capacity and with QF = 50 F5 algorithm has 0.6814 Steganalysis error probability, while the proposed method has 17.4617. Again, with 20% data hiding capacity and with QF = 50 F5 algorithm has 0.2555 Steganalysis error probability; while the proposed method has 3.8330 (see Table 1).

Table 1. The caption comes before the table.

Steganalysis by Error Probability					
		5%	10%	15%	20%
QF 50	F5	23.0835	4.5997	2.0443	0.5111
	[1]MDE	44.8041	33.0494	18.9949	4.4293
QF 75	F5	18.3986	2.1295	0.6814	0.2555
	MDE	44.9744	33.3049	17.4617	3.8330

[1]The proposed method is named by minimum distortion embedding (MDE)

The proposed method and F5, was tested with support vector machine to detect Steganalysis probability, the following comparison are prepared after getting the Steganalysis detection result (see Fig 1 and Fig 2).

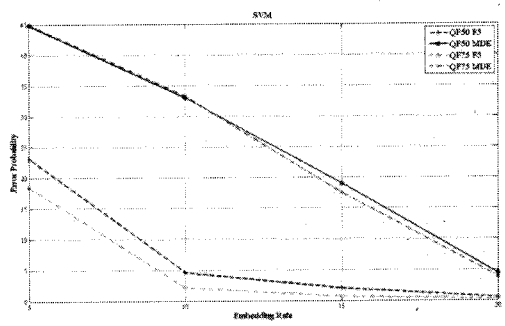


Fig 1. Steganalysis comparison by support vector machine (SVM) of the proposed method with F5 algorithm

During the performance testing, the error probability and embedding rate was considered with QF = 50, and QF = 75. With both QF, the proposed method has achieved better performance than F5 and proposed method (see Fig 1).

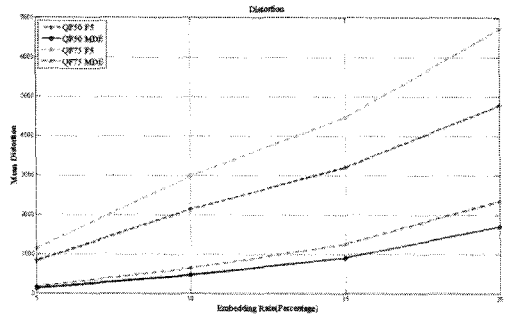


Fig 2. Distortion comparison by Mean distortion (MD) Vs Embedding rate (ER) of the proposed method with F5 algorithm

During the performance testing, the mean distortion and embedding rate was considered with QF = 50, and QF = 75. With both QF, the proposed method has achieved better performance than F5 and proposed method (see Fig 2).

IV. Conclusions

The proposed method has better resistance against Steganalysis. In case of steganography attacks are more important than capacity, while this method has better hiding capacity also. The main advantage of this proposed method is freedom of modifying any coefficients. Resulting better quality of stego image and higher resistance against attacks.

Acknowledgement

This work was in part supported by Information Technology Research Center (ITRC), by the Ministry of Information and Communication, Korea.

References

[1] J. Fridrich, M. Goljan, H. Hogea, "Attacking the OutGuess," *Proc. of the ACM Workshop on Multimedia and Security*, pp. 967-982, 2002.

[2] J. Fridrich, M. Goljan, H. Hogea, "Steganalysis of JPEG image: Breaking the F5 algorithm," *In Lecture Notes in Computer Science*, vol. 2578, pp. 310-323, 2003.

[3] J. Fridrich, "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes," *In Lecture Notes in Computer Science*, vol. 3200, pp. 67-81, 2004.

[4] N. Provos, "Defending against statistical steganalysis," *Proc. of the 10th USENIX Security Symposium*, pp. 323-335, 2001.

[5] P. Sallee, "Model-based steganography," *In Lecture Notes in Computer Science*, vol. 2939, pp. 154-167, 2004.

[6] P. Sallee, "Model-based methods for steganography and steganalysis," *In International Journal of Image and Graphics*, vol. 5, no. 1, pp. 167-190, 2005.

[7] K. Solanki, A. Sarkar, B. S. Manjunath, "YASS: Yet another steganographic scheme that resists blind steganalysis," *Proc. of the 9th International Workshop on Information Hiding*, Saint Malo, Brittany, France, pp.16-31, 2007.

[8] A. Westfeld, A. Pfitzmann, "Attacks on steganographic systems," *In Lecture Notes in Computer Science*, vol. 1768, pp. 61-75, 2000

[9] A. Westfeld, "F5: A steganographic algorithm: High capacity despite better steganalysis," *In Lecture Notes in Computer Science*, vol. 2137, pp. 289-302, 2001.

[10] Y. Kim, Z. Duric, D. Richards, "Modified Matrix Embedding Technique for Minimal Distortion Steganography," *Proc. of the Information Hiding (IH), Lecture Notes on Computer Science*, Vol. 4437, pp. 314-327, 2007.

Appendix

Suppose, a group is containing seven AC coefficients (see Fig 3). While LSB sum of these seven elements is 4 (even). If this method has to hide 1 then one element needs to modify (see Fig 3).

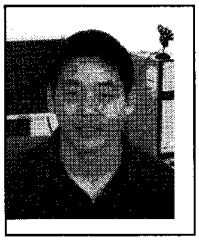
2	5	-2	-1	3	1	2	...
0	1	0	1	1	1	0	...

Fig 3. A selected group of AC coefficients and with their corresponding LSB values (here seven nonzero AC coefficients are in one group).

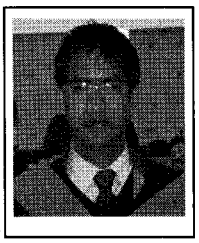
Now, suppose the last AC coefficient value was 1.63 (before rounding), this value will move to 2 after rounding. Thus the rounding error for this particular AC coefficient is (2 – 1.63 = 0.37), as this AC coefficient is a even number (i.e., after rounding), to make this number odd there is two choices, either adding by 1 or subtracting by 1 (e.g., 2 +1 = 3 (odd), again 2 -1 = 1 (odd)). If any method will add by 1 then the distance with the original value will be (|3 – 1.63| = 1.37), now if this method will subtract by 1 then the distance between the original value and modified value will be (|1 – 1.63| = 0.63). Now, in order to hide 1 and make the LSB sum odd, this method changes last 2 to 1. Note that there was another 2 which is making higher distortion (see Fig 4).

2	5	-2	-1	3	1	1	...
0	1	0	1	1	1	1	...

Fig 4. A selected group of AC coefficients and with their corresponding LSB values, last nonzero values LSB has been modified according to less distortion.



Rongyue Zhang received his B.S, M.S, and Ph.D degrees from Sun Yat- Sen University, Guangzhou, China (PRC), in 1997, 2004, and in 2007, respectively. He is a Postdoctoral Fel-low with the Graduate School of Information Management and Security, Korea University, Korea (ROK) since March 2008. His current research interests include Watermarking, Data Hiding and Multimedia Security.



Amiruzzaman Md. received his B.S degree in Computer Science and M.S. degree in Computer Science and Engineering from National University, Bangladesh in 2002 and Sejong University, Korea (ROK) in 2008 respectively. Now he is a PhD student in the Graduate School of Information Management and Security, Korea University, Korea (ROK). His research interests Steganography, Watermarking, and Information Theory.

Hyoung Joong Kim received his B.S degree in Electrical Engineering from Seoul National University, Korea (ROK) in 1978. He also received M.S, and PhD in Control and Instrumentation Engineering from Seoul National University, Korea (ROK) in 1986, and in 1989 respectively. Currently he is a full professor in the Graduate School of Information Management and Security, Korea University, Korea (ROK). His research interests Multimedia Computing, Multimedia Security, Semantic Analysis, and e-Learning applications.