Covert Channel Communication by Betterment Steganography[1]

Amiruzzaman Md[1], Hassan Peyravi[1],
M. Abdullah-Al-Wadud[2], Yoojin Chung[3]
[1]*Department of Computer Science*
Kent State University, Kent, Ohio 44242, USA
{mamiruzz, peyravi}@cs.kent.edu
[2]*Department of Industrial and Management Engineering,*
Hankuk University of Foreign Studies, 89 Wangsan, Mohyun, Cheoin,
Kyonggi, 449-791, South Korea
wadud@hufs.ac.kr
[3]*Department of Computer Engineering,*
Hankuk University of Foreign Studies, 89 Wangsan, Mohyun, Cheoin,
Kyonggi, 449-791, South Korea
chungyj@hufs.ac.kr

Abstract

This paper is presenting a betterment steganographic method for covert channel communication. Two distinct methods are combined to achieve possibly high data hiding capability with high visual quality. The proposed method shifts the last n nonzero AC coefficients from S JPEG block, and changes the magnitude values of the first n nonzero AC coefficients from T JPEG blocks. S and T blocks are determined by the number of nonzero JPEG coefficients in the block. Zero run-length modification method improves the robustness against statistical attack based on magnitude histogram. Magnitude modification method improves the visual quality. This combination complements each other.

Keywords: *Steganography, JPEG image, information hiding.*

1. Introduction

To communicate with each other with the intention of secret communication, covert channel (or steganography) and detection techniques (or steganalysis) are advancing simulteniously. The history of steganography and steganalysis is a history of rat races. Whenever a steganographic method has been proposed, the method is about to be broken soon by new steganalysis methods. Therefore, steganographers[2] try to develop new methods secure fully or partially from the existing steganalysis methods. However, it is not possible all the time to be able to take all security issues into account and solve in one method. From the history of steganography, it is known that steganography is one of the oldest arts or techniques for hiding data to establish a secure covert communication channels. However, it

[1] The original version of this paper at first appeared as "An Improved Steganography Covert Channel," in Communications in Computer and Information Science, vol 59, pp. 176-187, Springer Berlin Heidelberg. (2009)

[2] A group of researcher those who are working for covert channel writings.

is not so long since the ground of digital steganography techniques has been formed. Many innovative steganographic algorithms are available now [4], [5], [6], [7], [8].

The most important goal of steganography is to conceal the existence of a secret message. However, researchers are also having interest to break steganographic schemes. There are many available attacks [3] invented by several researchers. Among them statistical attack [9] is one of the most popular and effective attacks in steganographic world. Another famous attack is 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 histogram to the original histogram. However, keeping the same shape of a magnitude histogram is not easy to achieve as long as the coefficient magnitudes are modified. Note that one branch of steganography methods is inventing schemes to preserve the original histogram perfectly. Least significant bit overwriting methods including OutGuess [4] can preserve the original histogram almost perfect, but 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 of unideal data pattern.

F5 [9] also tries to narrow the gap between original and modified histograms by decrementing nonzero JPEG coefficients towards 0 and applying matrix embedding and permutative straddling. Sallee models the marginal distribution of DCT[3] coefficients in JPEG-compressed images by the generalized Cauchy distribution[4] [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 this method 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.

Preserving the perfect shape of histogram of stego image has been a primary target in the field of steganography. For the first time, one method can preserve the shape of histogram exactly between original and stego images. The main drawback of this method is low embedding capacity with poor image quality. In this paper, a combined approach is introduced to overcome low embedding capacity and poor image quality.

The rest of this paper is organized as follows: In Section 2, coefficient magnitude and run-length histograms are defined. Data hiding method based on the run-length histogram is presented. Section 3 summarizes experimental results. Section 4 concludes the paper.

2. Proposed Approach

As the proposed method works with a combination of two different approaches, two methods have to be discussed one by one: each method to hide data into either S or T JPEG blocks. The S and T blocks are separated on the basis of the number of nonzero AC coefficients. To select the S and T blocks, a threshold value is used. Before further discussion, it is necessary to define S and T JPEG blocks.

2.1. S and T JPEG Blocks

An image can be divided into 8x8 non-overlapping blocks and processed in the frequency domain by transforming using discrete cosine transform (DCT) and quantization block by

[3] Discrete Cosine Transform

[4] Known as χ^2 attack

block. Each block consists of integer values where the leftmost and topmost value is a DC coefficient value, and the other 63 coefficients are AC coefficient values. The DC coefficient plays an important role: it maintains an average luminance value of the block. Hence, the DC coefficient is not used for embedding data due to serious possibility of blocking effects among neighboring blocks.

The S and T blocks are determined by the number of nonzero AC coefficients. The leftmost and topmost AC coefficients close to the DC coefficient are considered to be more important than the rightmost and bottommost AC coefficients far from the DC coefficient. Importance of the coefficients can be measured by the magnitudes of the associated quantization coefficients. In addition, in general, it is believed that low-frequency components are more important than high-frequency components in data compression. The proposed method uses a threshold value to determine S and T JPEG blocks.

***Definition* 1**

If a JPEG block has less or equal to T_v number of nonzero AC coefficients, then that block is treated as an S block.

***Definition* 2**

Similarly, if the numbers of nonzero AC coefficients are more than the threshold value T_v, then that block is a T JPEG block (see Figure 1).

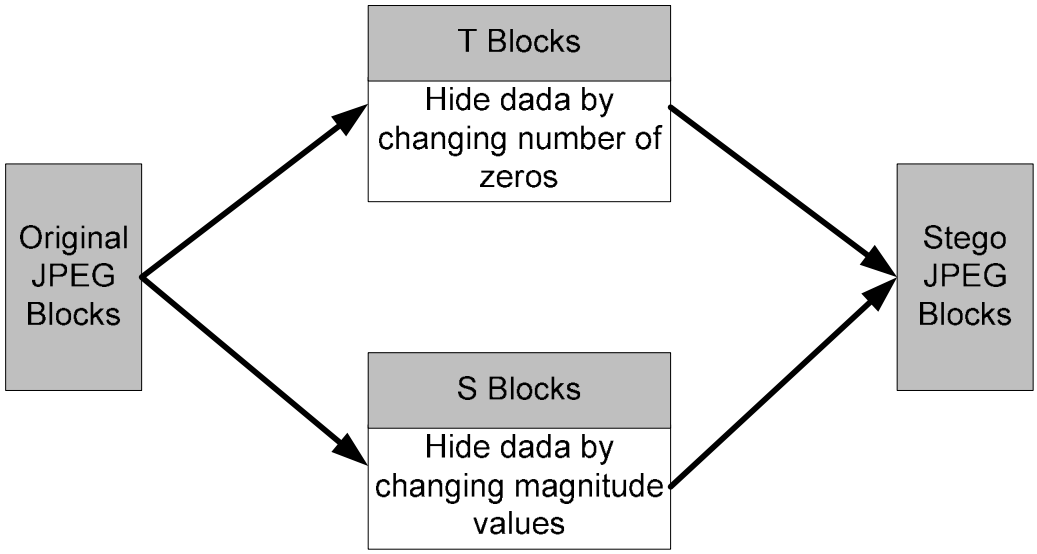


Figure 1: Block diagram of the encoding phase

***Example* 1**

Let the DC coefficient in a block be denoted as DC, the AC coefficients as AC_i, (where, i =1, 2, ⋯, n-1, n), and the threshold value as T_v. In general, $n \leq 63$, where AC_n is the last

nonzero AC coefficient in the block, where an EOB[5] marker follows. Assume that a JPEG block has AC coefficients (i.e., both nonzero and zero)as follows: for example, [16 1 0 0 0 -2 1 0 0 -1 2 EOB]. Then, we denote them as $DC = 16$, $AC_1 = 1$, $AC_2 = 0$, $AC_3 = 0$, $AC_4 = 0$, $AC_5 = -2$, $AC_6 = 1$, $AC_7 = 0$, $AC_8 = 0$, $AC_9 = -1$, $AC_{10} = 2$, and the EOB marker follows. For the efficiency of compression, zero elements after the EOB marker are not considered as regular coefficients.

The nonzero AC coefficients are easily identified. In this example, there are 5: $AC_1 = 1$, $AC_5 = -2$, $AC_6 = 1$, $AC_9 = -1$, and $AC_{10} = 2$. If the threshold value T_v is 3, then the number of nonzero AC coefficients in this toy example is more than T_v, which means that this JPEG block is a T block (see Figure 2).

***Example* 2**

Again, in another toy example with zigzag-scanned JPEG coefficients [32 5 0 0 0 2 EOB], we can denote them as $DC = 32$, $AC_1 = 5$, $AC_2 = 0$, $AC_3 = 0$, $AC_4 = 0$, $AC_5 = 2$, and EOB. The number of nonzero AC coefficients is 2: $AC_1 = 5$ and $AC_5 = 2$. Note that this block is an S block when T_v is 3 (see Figure 3) by the definition of S and T blocks. There is no special meaning in the name of S and T. For the convenience of definition, S and T blocks are used. If the number of nonzero coefficients (except DC value) in a block is larger than T_v, the block is just considered as a T block; otherwise, the block is an S block.

2.2. Shifting Nonzero AC Coefficients

The proposed method allows shifting of nonzero AC coefficients to make either even or odd number of zeros in between two nonzero coefficients in order to hide data. This method has excellent features. Since this method does not change the magnitude of coefficients, the resulting histogram is totally unchanged. Thus, existing statistical attacks cannot find any clue of steganography. This kind of histogram is called magnitude histogram. Existing statistical attack takes the magnitude histogram into consideration.

In this paper, run-length histogram is introduced to cope with the shifting nonzero AC coefficients by adjusting run-lengths to hide data. If there is no zero coefficient between two consecutive nonzero coefficients, the run-length of zero coefficient is 0 by definition. Similarly, if there are 10 zero coefficient between two consecutive nonzero coefficients, the run-length of zero coefficient is 10 by definition. The run-length histogram shows the number of run-lengths from 0 to 63. In general, this run-length histogram shows an exponentially decaying distribution. However, when a stego image has excessive number of hidden messages, its run-length histogram may be far away from an exponentially decaying distribution.

[5] End-of-Block (EOB)

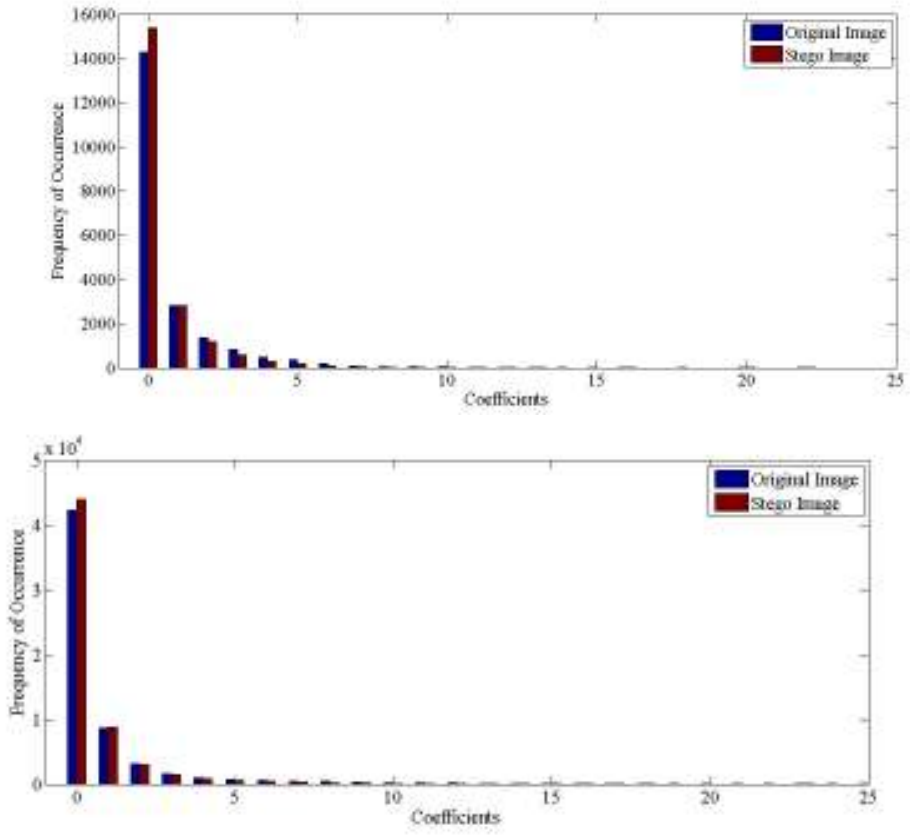


Figure 2: Run-Length histogram of the original Lena image and stogo Lena image (top). Run-Length histogram of the original Baboon image and stogo Baboon image (bottom).

Serious drawback of the coefficient shifting method is its poor image quality. The reason is obvious: Assume that one coefficients is shifted to the left or right by one position, this operation results in change of at least two nonzero AC coefficients. Consider an example with [... 5 0 0 0 6 0 ...] where one more zero coefficient has to be inserted between nonzero coefficients 5 and 6 to make even number of zeros. Then, the changed coefficients have the form [... 5 0 0 0 0 6 0 ...]. Note that the position of 6 is changed to 0 while the position of 0 next to 6 is changed to 6. One is changed from 6 to 0 and the other one from 0 to 6. Subsequent changes may follow due to all nonzero coefficients in the right-hand side of 6. In case of traditional JPEG steganography, the maximum error due to magnitude is, in general, ±1 in a single position. However, the position shifting method causes significant errors at least in two positions.

Thus, inserting or deleting zero coefficients everything in a block is a bad idea. One solution is inserting or deleting T_c number of zero coefficients in between the last nonzero coefficients. Of course, this solution may cause serious image degradation. However, this method is much better than shifting nonzero coefficients everywhere. In general, T_c should be as small as possible such as $T_c = 1$.

This kind of shifting operation results in the change of number of zero AC coefficients while nonzero coefficients are unchanged. If the number of AC coefficients in between nonzero AC coefficients is odd and the message to hide is odd (i.e., 1), this method does not

need to make any change. But if the number of zero coefficients is odd but the message to hide is even (i.e., 0), this method has to make the number of zero coefficients even by either removing or inserting one zero so that the next nonzero AC coefficient shifts from its original position either to the left or right, respectively. There are two more cases to make four possible cases: odd-odd, odd-even, even-odd, and even-even. The other two cases are similar to the previous two cases in nature. The overall four cases are summarized in Subsection 2.3. Note that in case of odd-odd (i.e., odd run-length with odd message to hide) and even-even pairs encoder does not need to insert or delete zeros. However, in any case, zeros are inserted or deleted intentionally to minimize distortion.

In this paper, coefficient shifting method is applied to the T block. For the decoder, odd or even number of zeros indicates the hidden message information. The following block [16 1 0 0 0 -2 1 0 0 -1 2 EOB] is a T block. Embedding of the secret message "01" into this T block changes last two run-lengths like [16 1 0 0 0 -2 1 0 0 -1 0 2 EOB] (see Figure 2). Note that one zero is forcefully inserted in between AC_9 and AC_{10}. Therefore, the position of the last nonzero AC coefficient (i.e., 2) has to be shifted to the right and has a new position AC_{11}.

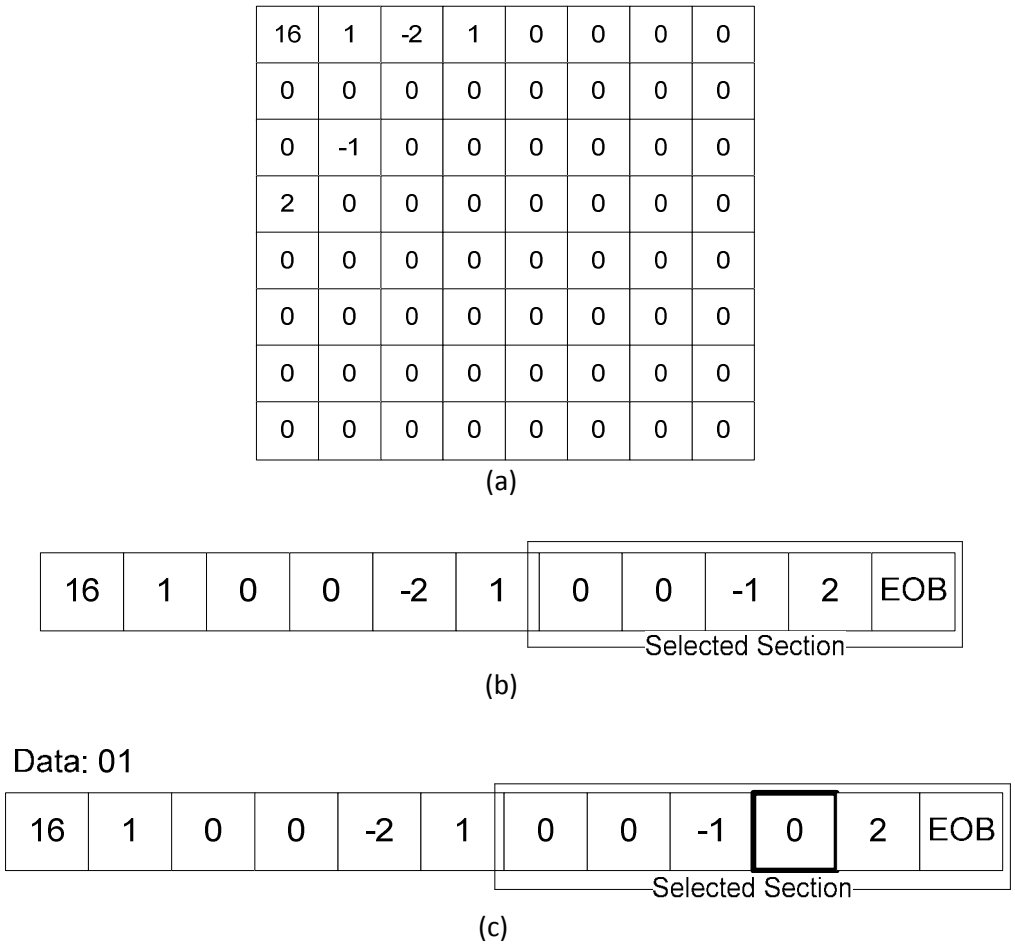


Figure 3: An original T JPEG block (a), the zigzag scanned array of the T block (b), and the changed array after embedding binary data "01" (c).

2.3 Modifying Magnitude Nonzero AC Coefficients

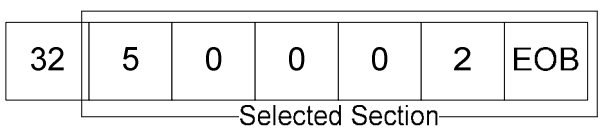
Magnitude changing method is an ugly duckling. Magnitude changing method also has its merits. Thus, this method is applied to the S blocks. The magnitude of the first T_c nonzero coefficients is modified by a very simple rule. When the hidden bit is even (i.e., 0) and the magnitude value of nonzero AC coefficient is odd, then the method reduces or increases the magnitude value by 1 in order to make it even. Similarly, when the method has to hide 1 and the magnitude is even, this method increases or reduces the magnitude by 1 to make it odd. Always the magnitude value 0 was skipped for modification. If zero coefficient is changed from 0 to 1 or -1, decoding becomes wrong. In addition, modification from 1 or -1 to 0 also causes wrong decoding. Thus, magnitude change inwards to 0 is not so good, which has been used traditionally. This method changes a nonzero coefficient to a smaller one by 1 in absolute magnitude. For example, 6 can be changed to 5.

In this paper, magnitude change from 0 outwards is introduced as a baseline method. Outward change increases absolute magnitude by 1. For example, 6 can be changed to 7. It is easy to show that there is not significant difference between inward modification and outward modification. Thus, there is no objection to use outward modification. However, in order to minimize distortion, both inward and outward modification methods are used interchangeably.

In case of odd-even (i.e., odd magnitude with even message to hide) or even-odd pairs, magnitude of coefficients have to be modified. However, in case of odd-odd or even-even pairs, magnitude of coefficients are left unchanged. However, changing all nonzero coefficients gives the hint of data hiding. Thus, in order to fight against statistical attack, not all nonzero coefficients are changed. In this paper, encoder changes T_c number of nonzero coefficients near from the DC coefficient. It is easy to show that magnitude of distortion or magnitude of error after data hiding is almost proportional to the magnitude of the quantization coefficients. It is obvious that most of quantization coefficients are smaller as far as they are closer from the DC coefficient.

32	5	2	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(a)



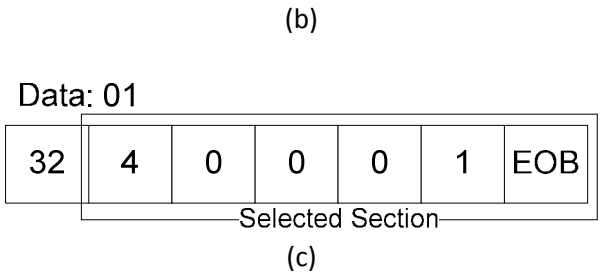


Figure 4: An S JPEG block (a), the zigzag scanned array of the S block (b), and the changed array after embedding binary data "01" (c).

***Example* 3**

An example block [32 5 0 0 0 2 EOB] is an S block (see Figure 4). There are two nonzero AC coefficients: $AC_1 = 5$ and $AC_5 = 2$. After embedding a message string "01" with two bits, the block becomes either like [32 4 0 0 0 1 EOB] or [32 6 0 0 0 3 EOB]. We can choose one of them that produces smaller magnitude of distortion.

2.4. Data Hiding Algorithm

Embedding algorithm of this paper combines two different methods: modification of both magnitude of nonzero coefficients in S blocks and run-length of zero coefficients in T blocks. The algorithm is summarized as follows:

Encoder

1. Separation of S blocks from T blocks by T_v: If a block has less AC coefficients than or equal to T_v, this block is an S block, and otherwise, a T block.

2. Change the magnitude values in the S block from the first Tc nonzero coefficients from the DC coefficient.
   (a) If the message to hide is 0 and the nonzero coefficient magnitude is odd, make it even by either increasing or reducing the magnitude value by 1. Choice is determined by the smaller magnitude of distortion.
   (b) If the message to hide is 1 and the nonzero coefficient magnitude is even, make it odd by either increasing or reducing the magnitude value by 1. Choice is determined by the smaller magnitude of distortion.

3. Change the number of zeros in between the nonzero AC coefficients from the last T_c) run-lengths in the T block.
   (a) If the hidden message is 0 and the number of zeros between two nonzero AC coefficients is odd, then make it even by either adding or deleting additional zeroes. Choice is determined by the smaller magnitude of distortion.
   (b) If the hidden message is 1 and the number of zeros between two nonzero AC coefficients is even, then make it odd by either adding or deleting additional zeroes. Choice is determined by the smaller magnitude of distortion.

Decoder

The decoding algorithm is also simple. Checking magnitudes of run-lengths if they are odd or even and checking a block if it is an S block or a T block are the role of decoder. The decoding algorithm is given bellow.

1. Determine whether a block is an S block or a T block by T_v.

2. In an S block, the magnitude values of first T_c nonzero coefficients from the DC value are checked to see if they are odd or even. The odd magnitude values represent 1 and even numbers represent 0.

3. In a T block, the number of zeros in between last Tc nonzero coefficients are counted. If the number is odd or even, then the hidden message is 1 or 0, respectively.

3. Experiment and Discussions

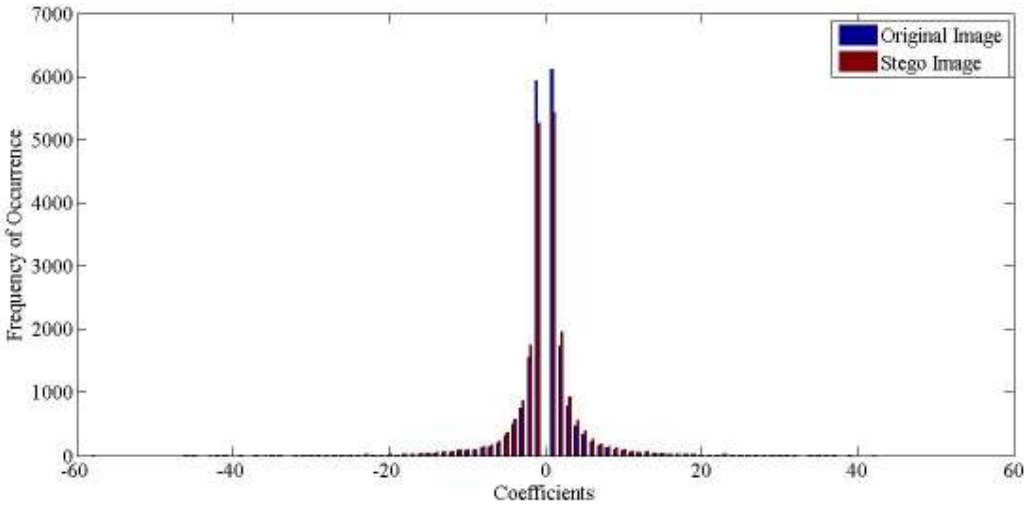
Implementing the proposed method is simple and easy. For the encoder and decoder, the proposed method was tested on four images. Performance of the data hiding methods is compared with different threshold values. The sample images are 512x512 in size and, therefore, have 4,096 8x8 DCT blocks. With different threshold values, various numbers of S and T blocks are obtained to hide data. The threshold values are used to control the capacity as well as image quality (i.e., PSNR). In case of higher capacity with T_v = 4 and T_c = 4, different images achieve different hiding capacity due to different number of S and T blocks. Lena image allows 8,658 bits to be hidden with 34.05 dB, and Barbara image 10,284 bits with 27.87 dB. Again, with the same threshold value, Gold-hill and Baboon images achieve data embedding capacity with 11,667 bits and 12,131 bits with 35.47 dB and 26.69 dB, respectively (see Table 1). After changing the threshold values as T_v = 4, and T_c = 3, the proposed method achieves different hiding capacity. Lena image embeds 6,575 bits with 36.05 dB, and Barbara image 7,466 bits with 29.83 dB. Since Baboon image has many nonzero AC coefficients due to its rich high-frequency components, the hiding capacity is significantly higher than other images. Note that with T_v = 4, and T_c = 3, the embedding capacity of Baboon image is 8,162 bits with 28.29 dB of visual quality.

Table 1: Performance over Hiding Capacity, Measured by different T_v and T_c value

		PSNR	Capacity	in S	in T
		[dB]	[bits]	[bits]	[bits]
Lena	T_v = 4, T_c = 4	34.06	8,658	6,099	2,559
	T_v = 4, T_c = 3	36.05	6,558	4,066	2,509
	T_v = 4, T_c = 2	38.49	4,560	2,527	2,033
	T_v = 3, T_c = 3	35.95	6,467	1,791	4,676
	T_v = 3, T_c = 2	38.49	4,119	1,781	2,338
	T_v = 2, T_c = 2	38.49	4,679	3,734	945
Barbara	T_v = 4, T_c = 4	27.88	10,284	1,776	8,508
	T_v = 4, T_c = 3	29.8329	7,466	1,774	5,692

	$T_v = 4, T_c = 2$	33.28	4,615	1,767	2,848
	$T_v = 3, T_c = 3$	29.73	7,283	1,109	6,174
	$T_v = 3, T_c = 2$	33.28	4,200	1,103	3,097
	$T_v = 2, T_c = 2$	33.28	3,914	542	3,372
Gold-hill	$T_v = 4, T_c = 4$	35.48	11,667	2,373	9,294
	$T_v = 4, T_c = 3$	36.88	8,552	2,356	6,196
	$T_v = 4, T_c = 2$	39.14	5,471	2,353	3,108
	$T_v = 3, T_c = 3$	36.71	8,010	876	7,134
	$T_v = 3, T_c = 2$	39.14	4,461	874	3,587
	$T_v = 2, T_c = 2$	39.14	4,121	327	3,794
Baboon	$T_v = 4, T_c = 4$	26.69	12,131	275	11,856
	$T_v = 4, T_c = 3$	28.29	8,162	258	7,904
	$T_v = 4, T_c = 2$	31.21	4,222	270	3,952
	$T_v = 3, T_c = 3$	28.35	8,144	100	8,044
	$T_v = 3, T_c = 2$	31.21	4,128	96	4,032
	$T_v = 2, T_c = 2$	31.21	4,088	24	4,064

After hiding data by the proposed method, small changes are observed in the magnitude histogram of the stego image compared with original image. Two graphs of histogram for original image and the difference between original and stego images are shown in Figures 5 and 6. It is observed that the difference is almost negligible, and, hence, the stego image is relatively secure due to its capability to keep almost the same as original original histogram. Histogram of the original image compressed by JPEG has a Cauchy-like distribution as shown in Figures 5 and 6. Difference between two histograms is almost equal to the number of total nonzero coefficients changed in the T blocks. By adjusting the threshold values T_v and T_c, histogram of the difference can be controlled. Note that the differences between magnitude histograms depend on images. However, most differences are occurred at 1 and -1.



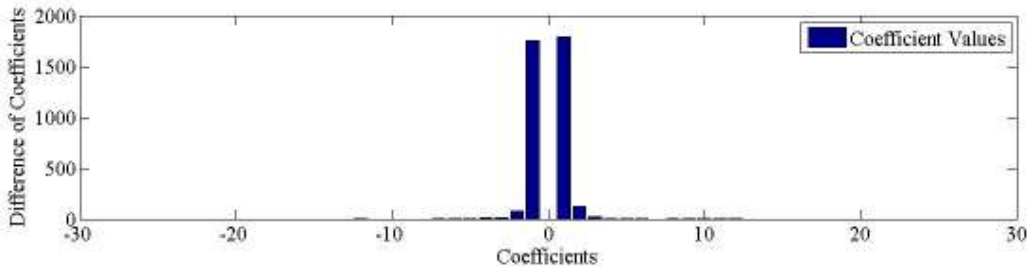


Figure 5: Histogram of the original Lena image (top) and that of the difference between original and stego images (bottom) with $T_v = 4$, and $T_c = 4$.

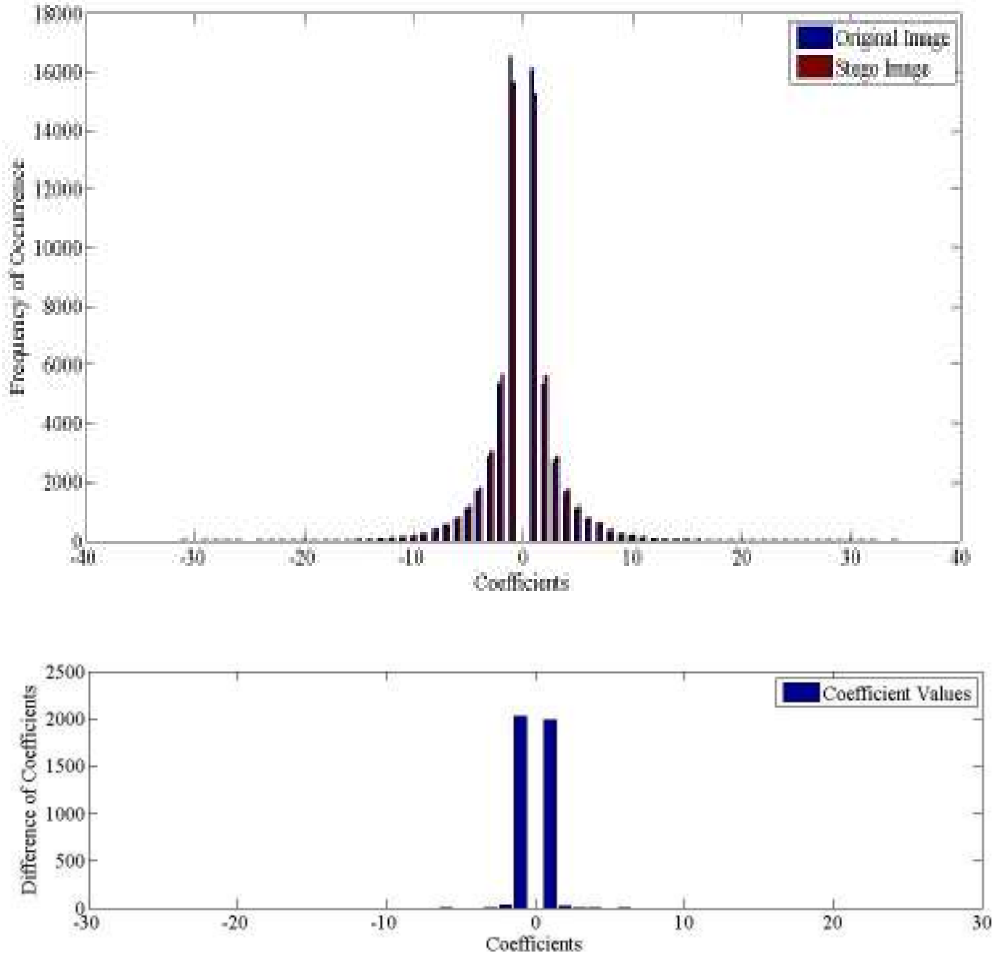


Figure 6: Histogram of the original Baboon image (top) and that of the difference between original and stego images (bottom) with $T_v = 4$ and $T_c = 4$

.

4. Conclusions

The proposed method provides significantly higher embedding capacity with slightly worse

image quality in comparison with a method of shifting nonzero coefficients only. In terms of security issue, this method is less weaker than traditional methods that modify magnitude of coefficients, but still can produce almost the same magnitude histogram and less distortion in visual quality. For the future work, optimization can be used to improve performance and security level. Many variations are possible in combination of two methods.

Acknowledgements

The authors would like to thank the reviewers for their valuable comments and suggestions, which have improved the paper. This work was supported by Hankuk University of Foreign Studies Research Fund of 2009.

References

[1]. J. Fridrich, M. Goljan, H. Hogea. Attacking the Out-Guess. Proceedings 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. 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. Lecture Notes in Computer Science, vol. 3200, pp. 67-81, (2004).

[4]. N. Provos. Defending against statistical steganalysis. Proceedings of the 10th USENIX Security Symposium, pp. 323-335, (2001).

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

[6]. P. Sallee. Model-based methods for steganography and steganalysis. 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. Proceedings of the 9th International Workshop on Information Hiding, Saint Malo, Brit-tany, France, pp.16-31, (2007)

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

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

Author

Md Amiruzzaman *received his B.S. degree in computer science from National University of Bangladesh in 2005. He received his M.S. in computer science and engineering from the Sejong University, Korea in 2008. At present he is a PhD candidate at Kent State University, USA. His research interest includes covert channel, IP covert channel, steganography, image processing, image*

analysis, network packet analysis, networks and systems security.

Hassan Peyravi *Dr. Peyravi received his M.S. and Ph.D. degrees in Computer Science from University of Oklahoma in 1980 and 1985, respectively. He joined joined the faculty of Computer Science at Kent State University in 1985. From 1987 to 1989, he became a Member of Technical Staff at AT&T Bell Laboratories in New Jersey. During this period, he conducted research in network architecture, adaptive routing algorithms for ISDN network controllers, and frame relay. Dr. Peyravi has been awarded research grants from NASA Space Communication Division to design, study and evaluate the performance of multiple access control (MAC) protocols for the Mars Regional Network. He has been awarded by CAIDA (Cooperative Association for Internet Data Analysis) to establish an Internet Engineering and Teaching Laboratory at Kent State University and to study traffic management, network management and routing protocols for IP routers. He has been awarded by the Internet2 Technology Evaluation Center (ITEC) to study QoS provisioning and traffic management for the next generation of IP networks. Dr. Peyravi has participated in the review process of numerous transactions papers and journal articles for the major computer and communication societies including IEEE, ACM, Elsevier, The Society for Modeling and Simulation International, and The International Society for Optical Engineering. He has also participated in the review process of several NSF panels and a few academic review boards. Dr. Peyravi has served as a member of the executive committee for the Internet2 Technology Evaluation Center (ITEC-Ohio), and a member of the program committees for several international conferences including International Conference on Parallel Processing (ICPP), Wireless Networks and Mobile Computing, QoS over Next Generation Data Networks, and the International Society for Optical Engineering. Dr. Peyravi's research encompasses multiple access protocols, traffic management and congestion control, optical switching and transmissions, interconnection networks, systems modeling and performance evaluation.*

Yoojin Chung *(Department of Computer Engineering, Hankuk University of Foreign Studies, San 89, Mohyeon, Yongin, Korea) She received the B.E., the M.S. and the Ph.D. degrees in Computer Science and Engineering from Seoul National University, Seoul, Korea, in 1989, 1991 and 1997, respectively. She has been with the Department of Computer Engineering, Hankuk University of Foreign Studies since 2001, where she is currently a professor and a graduate head of the department. She was a department chair during 2005 and 2006 and a visiting professor at the University of California, Irvine from 2007 to 2008. Her research interests include embedded systems, computer security, algorithms, information retrieval, and bioinformatics.*

M. Abdullah-Al-Wadud *received his B.S. degree in computer science and M.S. in computer science and engineering from the University of Dhaka, Bangladesh in 2003 and 2004, respectively. He received his PhD in Computer Engineering from Kyung Hee University, South Korea in 2009. He has been*

with the Department of Industrial and Management Engineering, Hankuk Uniersity of Foreign Studies, as a lecturer since 2009. He also served in Daffodil International University, Bangladesh and East West University, Bangladesh as a lecturer in department of Computer Science and Engineering in 2003-2004 and 2004-2005, respectively. His research interest includes image enhancement, medical image processing, pattern recognition, and security mechanisms in multimedia and sensor networks.