International Journal of Pattern Recognition
and Artificial Intelligence
Vol. 17, No. 6 (2003) 967–981

World Scientific
www.worldscientific.com

SECURE ERROR-FREE STEGANOGRAPHY FOR JPEG IMAGES

YEUAN-KUEN LEE* and LING-HWEI CHEN†

Department of Computer and Information Science,
National Chiao Tung University,
1001 Ta Hsueh Rd., Hsinchu, Taiwan 30050
**yklee@debut.cis.nctu.edu.tw*
†*lhchen@cc.nctu.edu.tw*

The typical model of steganography has led the prisoners' problem, in which two persons attempt to communicate covertly without alerting the warden, that is, only the receiver knows the existence of the message sent by the sender. One available way to achieve this task is to embed the message in an innocuous-looking medium. In this paper, we propose a variation of the Quantization Index Modulation (QIM) for solving the prisoners' problem. We also propose a theorem to show that the error of mean intensity value of an image block caused by JPEG compression is bounded. The proposed method embeds the messages to be conveyed by modifying the mean intensity value, and the resulting stego-image can be stored in the JPEG format with a low quality setting. Besides, a specific pattern caused by using the QIM embedding method is also identified, and this pattern will be removed using the proposed embedding method. Experimental results and the proposed theorem show that the hidden message is error-free against the JPEG distortion under the quality setting as low as 25. Furthermore, the existence of the hidden message is not only visually imperceptible but also statistically undetectable.

Keywords: Information hiding; steganography; steganalysis; covert communication; security.

1. Introduction

Steganography is an ancient art of conveying messages in a secret way so that only the receiver knows the existence of the message.[1,2] The message is hidden in another media such that the transmitted data will be meaningful and innocuous-looking to everyone. Steganalysis is the art of detecting any hidden message on the communication channel. If the existence of the hidden message is revealed, the goal of steganography is defeated.

For all of the steganographic systems, the most important and fundamental requirement is undetectability. The hidden message should not be detected by any other people. Thus, two aspects are usually addressed. First, the embedding process

*Author for correspondence.

should not degrade the media fidelity, that is, the difference between the stego-media and the cover-media should be imperceptible to human perceptual system. Second, the original media, called cover-media, and the media with hidden message, called the stego-media, should appear identical under all possible statistical attacks. Payload and security issues must be involved in the design of a good steganographic system. Note that the blindness is assumed in steganographic model, i.e. the original cover-media are not needed when extracting the hidden message. The blindness is also assumed in the steganalytic process, the original cover-image should not be referred to do any statistical attack.

A great deal of image steganographic techniques were introduced in Ref. 9. Many steganographic tools in the Internet are available for varied image formats.[1,7,14,15,17–19] Paletted-based and JPEG are two most common used formats.

For palette-based images, directly embedding messages in those indices will cause radical color change, since two neighboring colors in the palette may not look the same. Many efforts try to reduce the distortion created in the embedding process. S-Tools[1] reduces the number of colors to about 32 unique colors. Then, message-bits are embedded in the LSB of each RGB channel. The advantage is that the color of each pixel does not change drastically. However, the palette is modified, and colors in the palette form 32 color groups. This specific pattern can be detected automatically and reveals the presence of the hidden message. Machado[14] proposed a steganographic method in which the palette is not modified. For each pixel, the message is embedded by replacing the index of a color with the one of the luminance-closed color. Since two colors with closed luminance may be radically different, the created stego-image may have perceptual distortion. To alleviate this problem, Fridrich[4,5] proposed a new scheme using the parity of palette colors. The closest color with the same parity as the message-bit is used to replace the original color. Since parity bits are randomly distributed, the searched new color never departs from the original one too much.

For JPEG images, Jsteg[19] embeds the hidden message by modulating the rounding choices either up or down in the quantized DCT coefficients. Marvel *et al.*[16] proposed a spread spectrum steganography, called SSIS, in which the technique used is similar to the spread spectrum watermarking.[3] A shortcoming of SSIS is that the stego-images can only be stored in the JPEG format with a very high quality setting. Johnson and Katzenbeisser[13] described an image steganographic system in the DCT domain, which is similar to a technique proposed by Zhao and Koch.[21,22] The message is embedded by modulating the relative size of two specific DCT coefficients with the same quantization value in the middle frequencies. Using this technique, the hidden message can survive JPEG compression with quality setting as low as 50.

Many steganographic tools introduce a specific pattern in their created stego-images during the embedding process. In Ref. 10, a number of unusual patterns in steganographic tools, such as S-Tools, Jsteg, Hide & Seek,[15] Hide4PGP,[17] and

Mandelsteg[7] are identified. These unusual patterns stand out and expose the possibility of the hidden message. Visual attack and Chi-square attack described in Ref. 20 are used for breaking the steganographic utilities: Stego,[14] Jsteg, Steganos[18] and S-Tools. In Ref. 6, the RS steganalysis is proposed to reliably and accurately detect the LSB steganography.

A new class of information embedding methods, quantization index modulation (QIM), was introduced in Ref. 2. Chen and Wornell showed that QIM is provably good against arbitary bounded and fully informed attacks and provably better rate distortion–robustness tradeoffs than currently popular spread spectrum and LSB modulation methods. Since there exists a specific pattern in these created images, it is dangerous to directly use the QIM technique for covert communication. To treat the above-mentioned problem in this paper, a steganographic model is proposed.

The proposed model uses a variation of QIM embedding method. A specific pattern caused by QIM embedding will be removed using multiple quantizations, called stego-tables in this paper. A theorem will be proposed to show that the error caused by JPEG is bounded on the mean intensity value of image blocks. Therefore, the hidden message embedded in the mean intensity value will be extracted correctly even if the created stego-images are stored in the JPEG format under a low quality setting. Furthermore, using the proposed stego-table generation and a hybrid embedding method, the existence of hidden message is also visually imperceptible.

2. Proposed Image Steganographic Model

In this section, we will describe the proposed secret-key image steganographic model. The main idea behind the proposed method is that the distortion on the mean intensity value of image blocks due to the JPEG compressing/decompressing operation is limited. The secret message embedded in the mean intensity value will be extracted exactly; nevertheless, the stego-image is stored in JPEG format. To avoid producing the specific patterns, a technique using multiple-table look up and a pseudo random number generator (PRNG) is provided.

A table of 256 entries is generated and the content of each entry is a binary symbol that indicates the embedding message. To reach the robustness aim, the neighboring entries are grouped together and contain the same symbol. In the embedding module, the mean intensity of each image block is changed to the closest center of a group with the same symbol as the message-bit. Thus, if the mean intensity value is changed due to JPEG compressing/decompressing operation, it will still be located in the same group, and the embedded message will be extracted correctly.

Figure 1 shows the block diagram of the proposed embedding/extracting method. Both sender and receiver share a secret key before conveying messages. The input message may be in any digital form and be treated as a bit stream. Note that the input message should be compressed and encrypted before embedding. The compression module deals with two problems. First, several content-dependent patterns

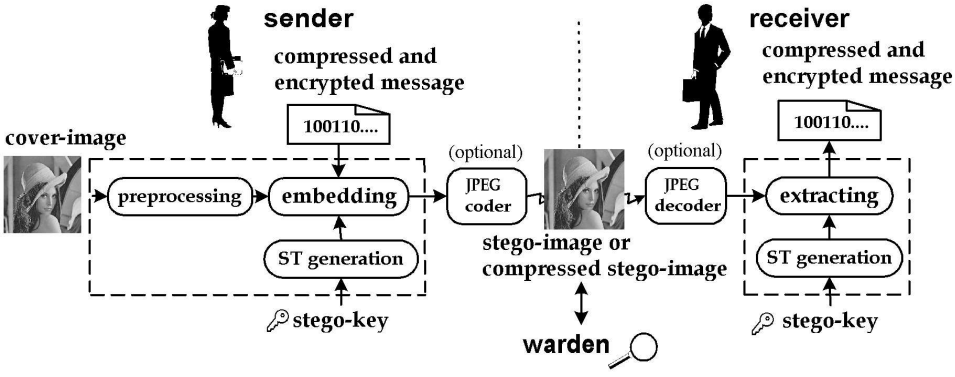


Fig. 1. The block diagram of the proposed embedding/extracting method.

in the original form of a message may reveal the existence of the hidden message. Second, the larger number of message-bits are embedded, the more degradation is introduced. The encryption module also conceals the content-dependent property of a message, but its major purpose is to protect the secret message. A stego-key is used for generating a set of stego-tables, and then these tables are used in both embedding and extracting modules. The preprocessing module is presented to avoid the situation that the mean intensity value of an image block cannot be adjusted while maintaining the image fidelity. During the embedding process, the sender splits the cover-image into 8×8 pixel blocks; each block encodes exactly one compressed and encrypted message-bit. Before the stego-image is transmitted, it may be compressed.

If the receiver possesses the same stego-key, the same stego-tables will be generated. Consequently, the hidden message can be extracted exactly. In the following subsections, we will describe each module in more detail.

2.1. *Stego-table generation*

Each stego-table contains 256 entries that are indexed from 0 to 255; each entry contains a symbol of "0" or "1". The range of indices, [0, 255], is divided into several intervals. All intervals have the same length, k, except the two boundary intervals. A PRNG is used to generate a sequence of symbols, each of which is "0" or "1". These symbols are assigned to those intervals sequentially, each entry in the same interval will contain the same symbol assigned to the interval. For example, the stego-table generated by the random sequence 0100110001010 with interval length $k = 20$ is shown in Fig. 2.

In the embedding process, each block will embed one message-bit by adjusting the mean intensity value to the center of an interval, to which the original mean intensity value is closest and the symbol of the interval is identical to the message-bit. Following the previous example, let the message-bit be 1 and the mean intensity

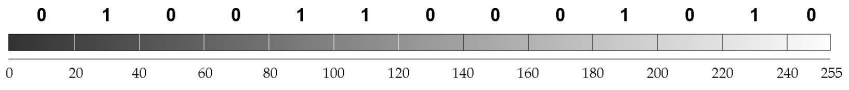


Fig. 2. An example of a generated stego-table ($k = 20$).

value be 15. Since the interval [20, 40) contains symbol "1" and its center is closest to 15, the mean intensity value will be changed to 30. However, if the mean intensity value is 145, the closest center with symbol "1" is 110, the mean value will be changed to 110. This modification may be too large to maintain the image fidelity. This problem is caused due to a number of consecutive 1's or 0's in the stego-table. To treat this problem, we should avoid generating consecutive 1's or 0's. Here, one simple method is provided, each generated symbol "1" is expanded into "10"; "0" is expanded into "01". For example, if the random sequence is 11010001, it will be expanded into 101001100101011. This modification guarantees that each symbol "0" (or "1") always has one neighbor symbol "1" (or "0"), thus the error produced by modifying the block mean intensity value will not exceed 1.5 k.

It is worth mentioning that the length of an interval provides the tolerance to the distortion caused by JPEG compressing/decompressing operation. In general, using a long interval length will produce a low-fidelity stego-image but it allows the stego-image to be compressed under high compression rate, and the hidden message can still be extracted correctly. This is a trade-off between image fidelity and robustness to JPEG distortion.

If only one stego-table is used in the proposed scheme, all of the mean intensity values in the created stego-image will occur at the interval centers. This unusual pattern will reveal the existence of the hidden message and defeat the purpose of steganography. To conceal the pattern, at least k stego-tables are needed when the length of an interval is k. Let ST_i denote the ith stego-table, $i = 0, 1, \ldots, k-1$. The center of the nth interval in ST_i will then be located in $nk + i$, this will make each value in [0, 255] be an interval center in a certain stego-table. After generating all stego-tables, the PRNG continues to generate a new sequence. Every eight consecutive binary symbols in the sequence will be considered as a number, and then a modulo operation (mod k) is applied to the number to obtain a table index which will indicate the currently used stego-table.

2.2. *Preprocessing*

In the embedding module, all of the gray scales of the pixels within a block will be modified such that the mean intensity value of the block will be equal to the closest center of an interval. If there are too many pixels whose gray scales are near the gray scale boundary, i.e. 0 or 255, it will be hard to adjust the mean intensity value while maintaining the image fidelity. For example, the mean value of a block is 195, and half of pixels in this block have gray scale 255, and the desired interval center is 210. Since half of the pixels could not be adjusted, other pixels will be added, 30

on the average. This change may be too large to maintain the image fidelity. Thus, a preprocessing is provided to make all gray scales away from the boundary.

Let $f(x, y)$ represent the original cover-image. The preprocessing procedure will generate a compacted image $f'(x, y)$ whose gray scale at every point (x, y) is in the interval $[k, 255 - k]$. The compaction process is done according to the following equation:

$$f'(x, y) = k + f(x, y) \times \frac{(128 - k)}{128},$$

where k is the interval length. Note that if k is not too large, $f'(x, y)$ will be indistinguishable from $f(x, y)$ by the naked eye.

2.3. *Embedding*

Using the stego-tables and a sequence of table indices, the messages are embedded in the compacted cover-image. The compacted cover-image $f'(x, y)$ is divided into blocks of 8×8 pixels; each block encodes exactly one message-bit in a left-to-right and top-to-bottom order. For reducing the blocking effect in the stego-image, not only the local properties of the current block but also those of neighboring blocks are considered. First, find an interval with the value equal to the message-bit, and the interval should satisfy two conditions: its center is near the mean intensity value and the total distance of the center to the mean intensity values of the neighboring blocks is minimal. Second, embed the hidden message-bit by adjusting every pixel value to make the mean intensity value equal to the center, which is called the destination mean.

Let B_c denote the current processing block, and B_u, B_l denote the upper and left blocks of B_c. Let m_c, m_u and m_l represent the destination means of B_c, B_u and B_l, respectively. The mean intensity value, denoted by μ, and the standard derivation, denoted by σ, of B_c are computed. Given a message-bit b and a table index i, the stego-table ST_i is searched for the closest interval center, denoted by c_1, with the same value as b. If both m_u and m_l are larger than μ, the second closest interval center, denoted by c_2, is searched under the following condition:
$(c_2 > \mu)$ and $((c_2 - \mu) \leq 3k)$.
If both m_u and m_l are smaller than μ, c_2 is searched under the following condition:
$(c_2 < \mu)$ and $((\mu - c_2) \leq 3k)$.

If c_2 cannot be found, c_1 is assigned as the destination mean of B_c. Otherwise, m_c is assigned by the following expression:

$$m_c = \begin{cases} c_2\,, & \text{if } |c_2 - m_u| + |c_2 - m_l| < |c_1 - m_u| + |c_1 - m_l|\,, \\ c_1\,, & \text{otherwise.} \end{cases}$$

When m_c has been determined, the next step is to adjust the gray scale of every pixel in B_c such that the new mean intensity value will be equal to m_c. There are two simple methods for achieving this task. One is to uniformly change the gray scale of each pixel in B_c, the other is proportional to each gray scale. The

proportional method will make blocking effect unnoticed, but more degradation will be introduced in the edge blocks that are located on the boundary of a large smooth region. Thus a hybrid method is used in the proposed embedding scheme. The uniform method is used in those edge blocks, where their standard derivations are larger than a threshold value T. The other blocks will use the proportional method. To further reduce the blocking effect, a white Gaussian noise with zero-mean and variance s is added to each block. Note that adding the Gaussian noise will not influence the mean intensity value in theory. In other words, the embedded message will not be destroyed by the Gaussian noise adding process. Let $\eta(x, y)$ be the additive Gaussian noise function, and $g(x, y)$ be the created stego-image. Then, $g(x, y)$ can be obtained according to the following expression:

$$g(x,y) = \begin{cases} f'(x,y) + (m_c - \mu) + \eta(x,y)\,, & \text{if } \sigma > T\,, \\ f'(x,y) + \dfrac{n^2(m_c - \mu)f'(x,y)}{\sum_{(x,y)\in B_c} f'(x,y)} + \eta(x,y)\,, & \text{otherwise.} \end{cases}$$

When the sender has finished the embedding process, the created stego-image $g(x, y)$ is either directly sent to the receiver or compressed into a JPEG form and then sent to the receiver. The extracting process done by the receiver will be described in the next subsection.

2.4. *Extracting*

An advantage of the proposed steganographic scheme is that the extracting algorithm is simple and easy to implement. When receiving a stego-image, the receiver uses the same stego-keys to generate the same stego-tables and table indices as those used in the embedding process. The received stego-image will first be decompressed if it is a JPEG compressed form, and then the decompressed form, $g'(x, y)$, is split into 8×8 pixel blocks. For each block, the mean intensity value is computed and then used to find the hidden message from the corresponding stego-table. Given a table index i, the hidden message b can be obtained by the following equation:

$$b = ST_i(\mu')\,,$$

where ST_i is the ith stego-table, μ' is the mean intensity value of the current processing block. Accordingly, the extracted message should be decrypted and decompressed in sequence. Finally, the receiver discovers the hidden information.

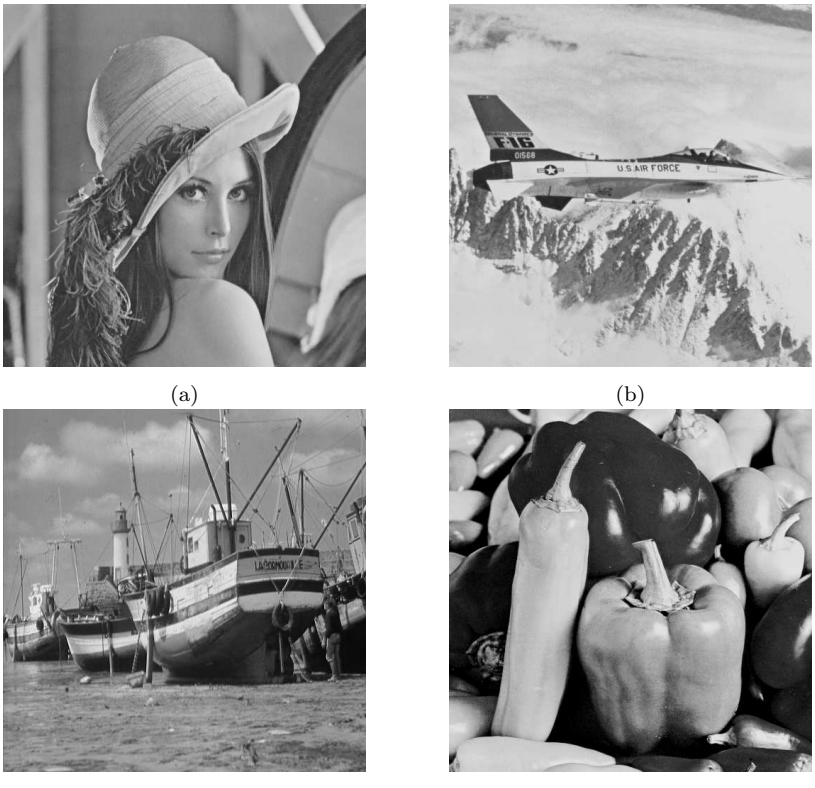
3. Experimental Results and Performance Analysis

We have tested the proposed embedding scheme on a great deal of gray-scale images. In this section, we will present a number of experimental results and analyze the undetectability and the bit error rate (BER) of the embedded message. In our experiments, the standard derivation of Gaussian noise is set to be 2.5, and the

standard derivation threshold is specified as 25. First, four general cover-images and their corresponding created stego-images are shown and a histogram comparison between using one stego-table and using three stego-tables is presented. Then, a series of JPEG compressing/decompressing operations are used to estimate BERs of the embedded message. In addition, a theorem about the distortion caused by JPEG operation is presented to show that the proposed method is error-free against JPEG distortion under a low quality setting.

3.1. *Undetectability*

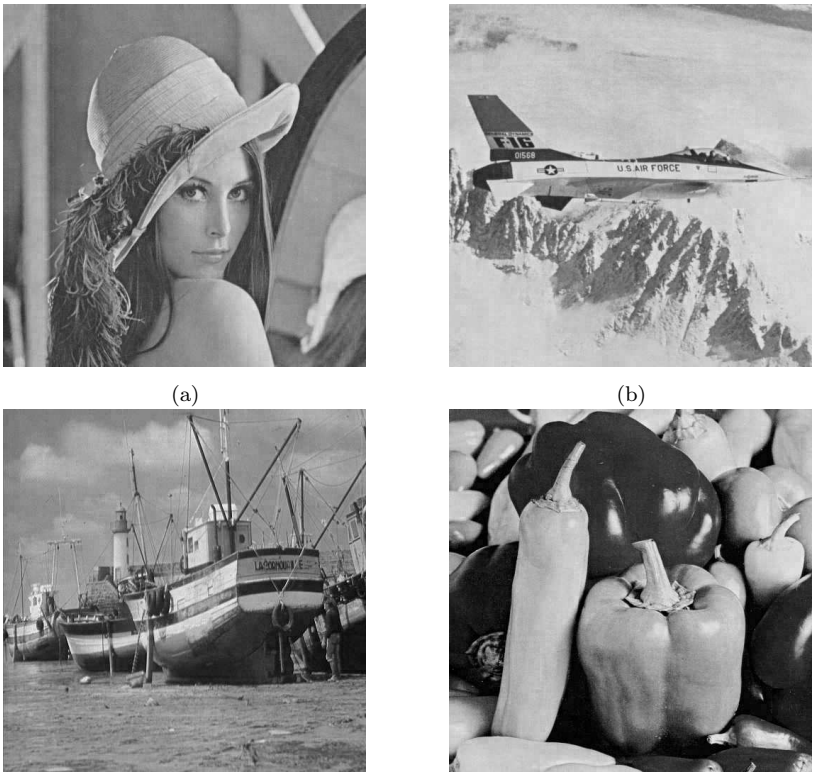
Figure 3 shows four original gray-scale cover-images, entitled Lena, F16, Fishingboat, Peppers, respectively. The size of these cover-images is 512×512, thus there are a total of 4096 message-bits embedded in each image. The payload of the proposed model is 0.015625 bits per pixel (bpp). The resulting stego-images are shown in Fig. 4. These cover-images and stego-images are nearly indistinguishable by the naked eyes.



(a) (b)

(c) (d)

Fig. 3. Four original cover-images. (a) Lena. (b) F16. (c) Fishingboat. (d) Peppers.



(a) (b)

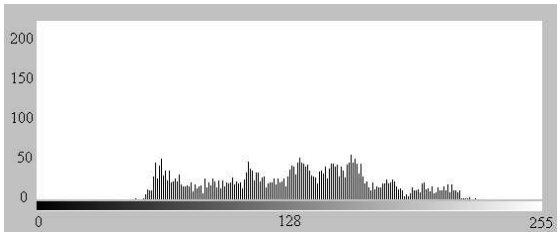
(c) (d)

Fig. 4. Four stego-images resulting from applying the proposed hybrid method ($k = 3$, $s = 2.5, T = 25$) in Fig. 4. (a) Lena stego-image. (b) F16 stego-image. (c) Fishingboat stego-image. (d) Peppers stego-image.

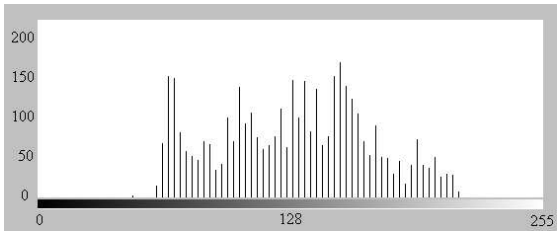
As mentioned in Sec. 2.1, if only one stego-table is used in the proposed model, all mean intensity values in each stego-image will be the interval centers. One example of the specific characteristic is presented in Fig. 5. The histogram of the mean intensity values for Lena cover-image is shown in Fig. 5(a). In the embedding processing, if only one stego-table is used and the interval length is chosen to be 3, this will make all block mean intensity values in the resulting stego-image are at equal space of 3 [see Fig. 5(b)]. This unusual pattern can be detected automatically using a simple detection procedure. It reveals the existence of the hidden message and defeats the purpose of steganography. Fortunately, if three stego-tables are used [see Fig. 5(c)], the specific pattern will disappear. Thus, using multiple stego-tables will meet the requirement of undetectability.

3.2. *The BER of embedded message*

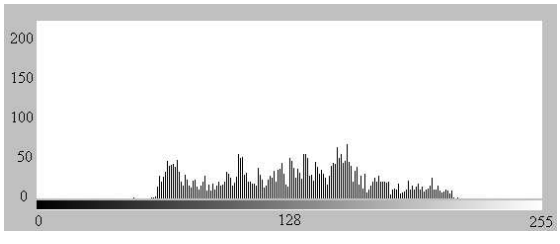
A series of JPEG compressing/decompressing operations were performed on the stego-images shown in the previous subsection to corroborate the effectiveness of



(a)



(b)



(c)

Fig. 5. The histograms of mean intensity values of image blocks ($k = 3$). (a) Cover-image Lena. (b) Stego-image using only one stego-table. (c) Stego-image using three stego-tables.

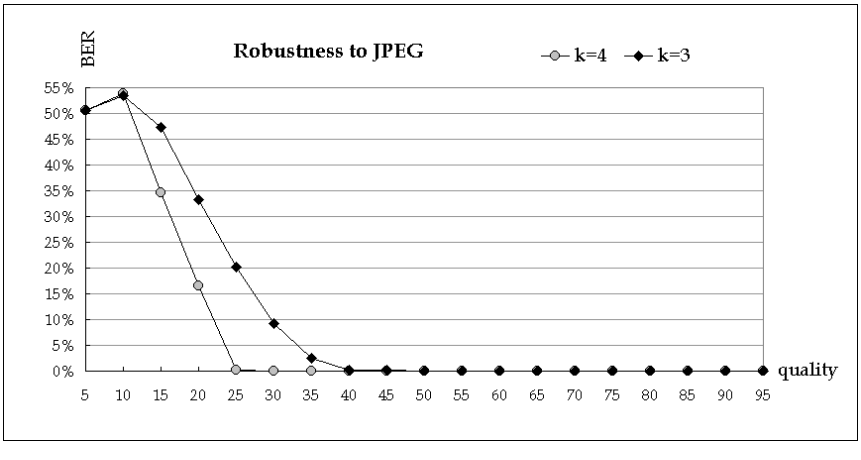


Fig. 6. Average BER with various user-specified JPEG quality setting.

the proposed model. We evaluated the average BER for various JPEG quality setting. The experimental results concerning the BER of using different interval lengths are presented in Fig. 6. From the figure, we can see that when the interval length is 4 and JPEG quality setting is higher than 25, the BER is 0%. This result is theoretically true and will be proved later. And it is also promising, since JPEG quality setting is usually taken higher than 25.

In the free IJG JPEG software,[11] the user-specified quality setting, QS_{user}, is converted to a percentage scaling factor and the quantization table Q is set as follows.

$$Q_{i,j} = \text{round}\left[\frac{SQ_{i,j} \times SF}{100}\right], \tag{1}$$

where $Q_{i,j}$ is the (i,j)th entry on Q and

$$SF = \begin{cases} 5000/QS_{\text{user}}\,, & \text{if } \ QS_{\text{user}} \leq 50\,, \\ 200 - 2 \times QS_{\text{user}}\,, & \text{otherwise.} \end{cases}$$

Note that SF is the percentage scaling factor and SQ is the sample quantization table given in JPEG Spec.[8] Based on these descriptions, the above-mentioned experimental results for JPEG compression can be expected since the block mean error due to JPEG compression can be deduced by the following theorem.

Theorem 1. *After applying the JPEG compression, the error of mean intensity value, denoted by δ, for the reconstructed image block satisfies the condition:*

$$|\delta| \leq \frac{1}{16} Q_{0,0}\,,$$

where $Q_{0,0}$ is the DC component of the percentage-scaled quantization table in the JPEG compression.

The proof of Theorem 1 is stated in detail in the Appendix. Note that $SQ_{0,0} = 16$ in the given sample quantization table ($QS_{\text{user}} = 50$). From Theorem 1, if the block mean error is restricted within 2, $Q_{0,0}$ could not exceed 32. Thus, according to Eq. (1), QS_{user} should be set higher than 25. This implies that if the length of the interval k in the stego-table is chosen to be 4 in the proposed embedding scheme, the hidden message survives the JPEG distortion under the user-specified quality setting $QS_{\text{user}} \geq 25$, that is, BER = 0%. The present theorem successfully explains those experimental results shown in Fig. 6.

4. Conclusion

In this paper, we have proposed a secure steganographic scheme for JPEG images. By using the proposed embedding method, the mean intensity value can be adjusted while maintaining the image fidelity and reducing the blocking effect. To escape the attention of the warden, k (interval length) stego-tables and a PRNG are used to avoid an unusual pattern appearing in the stego-image. From the experimental

results, we conclude that the secret message is error-free against JPEG distortion under a quality setting as low as 25.

Acknowledgment

This research was supported in part by the National Science Council, R.O.C. under contract NSC 90-2213-E-009-163.

Appendix

Proof of Theorem 1. In the JPEG encoding process, each image block is first transformed via the normalized 2D DCT. Let $f_{m,n}$ be the gray values of the pixel (m,n) in an image block. After applying DCT to $f_{m,n}$, we obtain the transform coefficient $F_{u,v}$ as follows:

$$F_{u,v} = c_u c_v \frac{2}{\sqrt{MN}} \sum_{m=0}^{N-1} \sum_{n=0}^{M-1} f_{m,n} \cos\left[\frac{(2m+1)u\pi}{2M}\right] \cos\left[\frac{(2n+1)v\pi}{2N}\right],$$
$$u = 0, 1, \ldots, M-1, \qquad v = 0, 1, \ldots, N-1,$$

where

$$c_u, c_v = \begin{cases} \dfrac{1}{\sqrt{2}} & u, v = 0, \\ 1, & u, v \neq 0. \end{cases}$$

Since the block size is 8×8, i.e. $N = M = 8$, the DC coefficient, denoted by $F_{0,0}$, is given by

$$F_{0,0} = \frac{1}{8} \sum_{m=0}^{7} \sum_{n=0}^{7} f_{m,n}$$
$$= 8\mu,$$

where μ is the mean intensity value of the image block. After applying DCT, the quantization through a quantization table $Q_{u,v}$, is conducted and the quantized coefficient $\hat{F}_{u,v}$ is obtained by

$$\hat{F}_{u,v} = \text{round}\left[\frac{F_{u,v}}{Q_{u,v}}\right]$$
$$= \frac{F_{u,v}}{Q_{u,v}} + \varepsilon,$$

where ε is the rounding error, and $-0.5 < \varepsilon \leq 0.5$. Then, all quantized coefficients will be entropy-coded.

In the JPEG decoding process, the reconstructed block can be obtained by applying entropy-decoding, inverse quantization, and inverse DCT. In the inverse

quantization step, the quantized DCT coefficients will be multiplied by $Q_{u,v}$. Let $F'_{u,v}$ be the reconstructed DCT coefficient, then

$$\begin{aligned} F'_{u,v} &= \hat{F}_{u,v}\, Q_{u,v} \\ &= \left(\frac{F_{u,v}}{Q_{u,v}} + \varepsilon \right) Q_{u,v} \\ &= F_{u,v} + \varepsilon\, Q_{u,v}\,. \end{aligned}$$

Since $F'_{0,0}$ is eight times the mean intensity value of the reconstructed block, the mean intensity value of a reconstructed block, denoted by μ', is obtained as follows:

$$\begin{aligned} \mu' &= \frac{1}{8}\, F'_{0,0} \\ &= \frac{1}{8}\, F_{0,0} + \frac{\varepsilon}{8}\, Q_{0,0} \\ &= \mu + \frac{\varepsilon}{8}\, Q_{0,0}\,. \end{aligned}$$

Let δ denote the error of mean intensity value, i.e. $(\mu' - \mu)$. Since $-0.5 < \varepsilon \leq 0.5$, we obtain

$$-\frac{1}{16}\, Q_{0,0} < \delta \leq \frac{1}{16}\, Q_{0,0}\,.$$

So,

$$|\, \delta \,| \leq \frac{1}{16}\, Q_{0,0}\,.$$

The proof has been done.

References

1. A. Brown, "S-Tool V4," ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tools4.zip.
2. B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Th.* **47**, 4 (2001) 1423–1443.
3. I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Imag. Process.* **6**, 12 (1997) 1673–1687.
4. J. Fridrich, "A new steganographic method for palette-based images," *Proc. IS&T PICS*, Savannah, Georgia, 25–28 April 1999, pp. 285–289.
5. J. Fridrich and R. Du, "Secure steganographic methods for palette-based images," *Proc. 3rd Int. Workshop on Information Hiding*, Dresden, Germany, 29 September–1 October 1999, pp. 47–60.
6. J. Fridrich, M. Goljan and R. Du, "Detecting LSB steganography in color and gray images," *Mag. IEEE Multimedia* (*Special Issue on Security*), October–November 2001, pp. 22–28.
7. H. Hastur, "Mandelsteg," ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/.
8. ISO/IEC JTC1 10918-1, *Information Technology — Digital Compression and Coding of Continuous-tone Still Images*: *Requirement and Guidelines*, 1994.

9. N. F. Johnson and S. Jajodia, "Steganography: seeing the unseen," *IEEE Comput.* **31**, 2 (1998) 26–34.
10. N. F. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," *Proc. 2nd Int. Workshop on Information Hiding*, Portland, Oregon, USA, 14–17 April 1998, pp. 273–289.
11. "JPEG image compression FAQ," http://www.faqs.org/faqs/jpeg.faq/.
12. D. Kahn, *The Codebreakers — The Compressive History of Secret Communication from Ancient Times to the Internet*, Scribner, NY, 1996.
13. S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, London, 2000.
14. R. Machado, "Stego," http://www.stego.com.
15. C. Maroney, "Hide & Seek," http://www.rugeley.demon.co.uk/security/hdsk50.zip.
16. L. M. Marvel Jr., C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," *IEEE Trans. Imag. Process.* **8**, 8 (1999) 1075–1083.
17. H. Repp, "Hide4PGP," http://www.rugeley.demon.co.uk/security/hide4pgp.zip.
18. STEGANOS company, "Steganos," http://www.steganos.com.
19. D. Upham, "Jsteg," ftp://ftp.funet.fi/pub/crypt/steganography.
20. A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-Tools — and some lessons learned," *Proc. 3rd Int. Workshop on Information Hiding*, Dresden, Germany, 29 September–1 October 1999, pp. 61–76.
21. J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection," *Proc. Int. Conf. Intellectual Property Rights for Information, Knowledge and New Techniques*, 1995, pp. 242–251.
22. J. Zhao and E. Koch, "Towards robust and hidden image copyright labeling," *Proc. IEEE Workshop on Nonlinear Signal and Image Proceedings*, 1995, pp. 452–455.

Yeuan-Kuen Lee received his B.S., M.S. and Ph.D. degrees in computer and information science from the National Chiao-Tung University, Hsinchu, Taiwan, in 1989, 1991 and 2002, respectively. From 1993 to 1995, he was a Lecturer at the Aletheia University, Taipei, Taiwan. He is currently an Assistant Professor in the Department of Computer Science and Information Engineering at Ming Chuan University, Taoyuan, Taiwan.

His research interests are in the areas of image and signal processing, digital steganography and computer security.

Ling-Hwei Chen received the B.S. degree in mathematics and the M.S. degree in applied mathematics from the National Tsing Hua University, Hsinchu, Taiwan in 1975 and 1977, respectively, and the Ph.D. in computer engineering from National Chiao Tung University, Hsinchu, Taiwan in 1987.

From August 1977 to April 1979, she worked as a research assistant in the Chung-Shan Institute of Science and Technology, Taoyan, Taiwan, after which she worked as a research associate in the Electronic Research and Service Organization, Industry Technology Research Institute, Hsinchu, Taiwan. From March 1981 to August 1983, she worked as an engineer in the Institute of Information Industry, Taipei, Taiwan and is now a Professor at the Department of Computer and Information Science at the National Chiao Tung University.

Her current research interests include image processing, pattern recognition, document processing, image compression and image cryptography.