논문-02-07-2-12

Adaptive Data Hiding based on Turbo Coding in DCT Domain

Jie Yang*, Moon Ho Lee** and Chen Xinhao***

Abstract

This paper develops a novel robust information hiding technique that uses channel codes derived from the error-correcting coder. The message encoded by the turbo encoder is hidden in DCT transform domain of the cover image. The method exploits the sensitivity of human eyes to adaptively embed a visually recognizable message in an image without affecting the perceptual quality of the underlying cover image. Experimental results show that the proposed data hiding technique is robust to cropping operations, lossy JPEG compression, noise interference and secure against known stego attacks. The performance of the proposed scheme with turbo coder is superior to that without turbo coder.

Ⅰ. Introduction

Steganography is an ancient art of conveying message in a secret way such that only the receiver knows the existence of message[1]. The techniques of steganoggraphy are classified into linguistic steganography and technical steganoggraphy[2]. The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, tries to hide message physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguistry. With the development of the Internet technologies, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the Internet rapidly.

Steganography, where the occurrence of communication is concealed, differs from cryptography in which communication is evident but the content of that communication is camouflaged. To be useful, a steganographic system must provide a method to embed data imperceptibly, allow the data to be readily extracted, promote a high information rate or payload, and incorporate a certain amount of resistance to removal[3][4]. Steganography simply takes one piece of information and hides it within another. Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information. The files can then be sent or transported without anyone knowing what really lies inside of them. An image of the space shuttle landing might contain a private letter to your lover. A recording of a short sentence might contain your company's plans for a secret new product. Additionally, steganography can be used to place a hidden "trademark" in images to be placed on Web pages.

Fig. 1(a)illustrates the basic elements of the traditional communication model. The encoder maps a message into a sequence of symbols drawn from some alphabet. The modulator converts a sequence of symbols into a physical signal that can travel over the channel.

* Prof. Jie Yang is on leave from Wuhan University, China

** Institute of Information & Communication, Chonbuk National University, Korea

*** Mr. Xinhao Chen is on leave from South-Central University for Nationalities, China

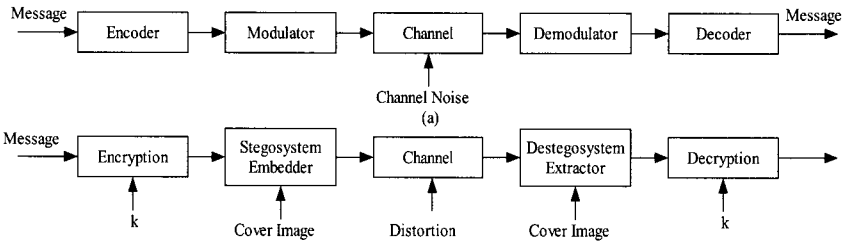

Fig. 1. (a)Standard model of a communication, (b)Steganographic system as communication

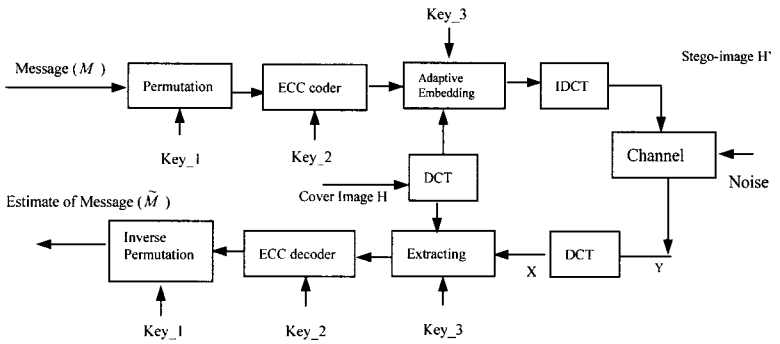

Fig. 2. The block diagram of the proposed steganographic model

In Fig.1 (b), we show one way in which watermarking can be mapped into this framework. A message is embedded in a digital image by the stegosystem encoder, which uses a key or password. The resulting stegoimage is transmitted over a channel to the receiver, where it is processed by the stegosystem decoder using the same key. During transmission the stego image can be monitored by unintended viewers who will notice only the transmission of the innocuous image without discovering the existence of the hidden message. Here, the modulation step is replaced by the step of embedding the encoded message into some media content and the demodulation step is replaced by the step of extracting the (possibly corrupted) watermark signal from the received signal.

This paper develops a novel robust information hiding technique that uses channel codes derived from the error-correcting coder. The methodology encompasses derivation of a general theory of steganographic communication, including image processing, information security, the DCT transform and design of an adaptive data-hiding technique. The message encoded by the turbo encoder is hidden in DCT transform domain of the cover image. The proposed method exploits the sensitivity of human eyes to adaptively embed a visually recognizable message in an image without affecting the perceptual quality of the underlying cover image. The simulating Gaussian noises, lossy JPEG compression and cropping are operated to the stego image (We think these independent operations for stego image to be noise.). The error messages extracted with noises are corrected with turbo-decoder. Experimental results show that the proposed scheme can successfully resist the different intensity noises.

Ⅱ. The Proposed Steganographic Model

2. The block diagram of the proposed scheme

Fig. 2 shows the block diagram of the proposed steganographic model. The input messages can be in

any digital form, and are often treated as a bit stream. The embedding messages are pseudo-randomly permuted to form a new binary sequence, the encrypted message. The pseudo-random permutation is can be done using a linear feedback shift register. By setting the state of the shift register by the key_1, a pseudo-random sequence can be generated that is then recoverable by resetting the shift register to its original state. The shift register can be applied in two fashions. The first option is to use the shift register to generate a random sequence of new row and column indices for the two dimensional watermark. This option requires repeated applications of the shift register for both the row and column indices. This is due to the fact that the row and column indices must fall in the range given by the size of the message. Thus, an entirely new set of row indices must be generated for a single column index. The second option is more direct and easier to implement. First, a raster scan of the watermark image is performed to generate a single row vector from the watermark. The elements of this row vector can then be pseudo-randomly permuted into a new row vector via a single execution cycle of the linear shift register. The shift register must only perform one permutation of the indices of the raster scan vector. A new raster scan vector is then generated by assigning the elements from the old raster scan vector to the positions of the new vector, as given by the newly generated indices. The scrambled messages are then constructed by performing the inverse raster scan process on this vector. This second method is implemented in this experiment.

2. Error Control Coding (ECC)

The encrypted messages are then encoded in the ECC coder in order to correct errors that are caused by the modification of the noises of the channel. Any error-control code that is capable of correcting the bit error rate (BER) can be used in our model. We investigated the performance of turbo codes, a recent development in error control [5][6][7], in our system. Turbo codes, also known as parallel concatenated systematic convolutional codes that use two binary convolutional encoders and an interleaver, have been shown [5] to operate very close to Shannon's limit with reasonable decoding complexity. A standard turbo coder scheme that uses rate 1/3 convolutional encoder is shown in Fig.3. The fundamental idea is to encode a message bit using the first encoder to generate 3 bits, consisting of the message bit and 2 parity bits. The message bits are interleaved and used as input to the second encoder, producing an additional set of 2 parity bits. Each code is systematic (the information bits are part of both encoded sequences), we need only to send one copy of the information.

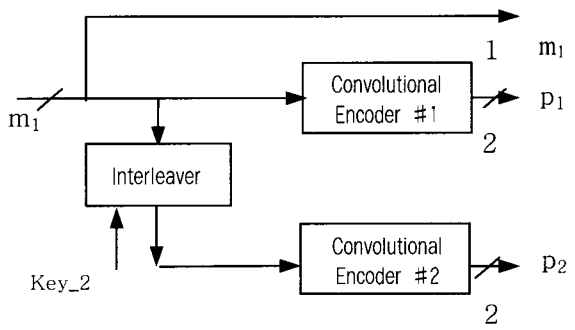

Fig. 3. Turbo Coding Encoder

3. Embedding Process

Embedding technique based on the discrete cosine transform(DCT) and adaptively data-hidden is proposed in this paper. Let $H = \{h(i,j), 0 \le i < M, 0 \le j < N\}$. Where $h(i,j)$ is the intensity of pixel (i,j), be the cover image of size $M \times N$, it is divided into non-overlapping blocks of size 8×8 pixels,. Let B^r represents r-th non-overlapping block of 8×8 pixels of the cover image. Let $D^r = \{d^r(i,j) \mid 0 \le i,j \le 7\}$ represents the 8×8 DCT coefficients corresponding to B^r, $r = 1,2,\ldots, (M \times N)/(8 \times 8)$. The messages are essentially embedded in the middle band of DCT domain, that is D^r, to make a tradeoff between visual degradation and robustness. The location embedded should be decided by the key_3. The selected M middle

band coefficients on each DCT domain are recorded in zig-zag scanning order, where M is the numbers of middle band coefficient and should be p times. And then, the M coefficients are divided into non-overlapping blocks of size $1 \times p$. Let $E_t^r = \{e^r(k) \mid 1 \le k \le p\}$ be the blocks of size $1 \times p$, t=1,2,..., M/p. The bit is inserted in the following Step:

1. Sort the DCT domain pixels in block E_r^t in an ascending order based on their intensity values.
2. Compute the average q_{mean}^r, the minimum $q_{\min}^r$and the maximum $q_{\max}^r$of the intensities of the DCT domain pixels in E_r^t. That is

$$q_{mean}^r = \frac{1}{p}\sum_{k=1}^{p} e^r(k) \tag{1}$$

$$q_{\min}^r = \min(e^r(k), \mid 1 \le k \le p) \tag{2}$$

$$q_{\max}^r = \max(e^r(k), \mid 1 \le k \le p) \tag{3}$$

3. Classify each DCT domain pixel in E_t^r into one of two categories, based on whether its intensity value is above or below the mean of the block:

$$e^r(k) \in Z_H \text{ if } e^r(k) > q_{mean} \tag{4}$$

$$e^r(k) \in Z_L \text{ if } e^r(k) \le q_{mean} \tag{5}$$

where Z_H and Z_L are the high and low intensity classes, respectively.

4. Compute the means, m_L and m_H, for the two classes, Z_H and Z_L
5. Define the contrast value of block E_t^r as

$$C_E = \max(C_{\min}, \alpha(q_{\max} - q_{\min})) \tag{6}$$

where α is a constant and $C_{\min}$ is a constant which defines the minimal value a DCT domain pixel's intensity can be modified.

6. Given the value of coded message b_w is -1 or 1, modify the DCT domain coefficients in E_t^r according to:

if b_w=1, for k=1,2,...,p.

$$e_{new}^r(k) = \begin{cases} q_{\max}, & if \quad e^r(k) > m_H \\ q_{mean}, & if \quad m_L \le e^r(k) < q_{mean} \\ e^r(k) + \delta, & if \quad otherwise \end{cases} \tag{7}$$

if b_w=-1, for k=1,2,...,p.

$$e_{new}^r(k) = \begin{cases} q_{\min} & , if \quad e^r(k) < m_L \\ q_{mean} & , if \quad q_{mean} \le e^r(k) < m_H \\ e^r(k) - \delta, & if \quad otherwise \end{cases} \tag{8}$$

where $e_{new}^r(k)$ is the new intensity value for the coefficient in DCT domain which had original intensity value $e^r(k)$ and δ is a random value between 0 and C_E. When the sender has finished the embedding process, the created stego-image are H' are then sent to the receiver. The extracting process done by the receiver will be described in the next subsection.

4. Extracting Process

When the receiver receives a stego-image, the same stego-keys are used to extract the hidden messages from the stego-image X. The extraction of a message is similar to the embedding process while in a reverse order. In the proposed algorithm, the extraction of a message must refer to the cover image. First, the stego-image is divided into non-overlapping blocks of size 8×8 pixels. Let p^r represents r-th non-overlapping block of 8×8 pixels of the stego-image X. Let $O^r = \{o^r(i,j) \mid 0 \le i,j \le 7\}$ represents the 8×8 DCT coefficients corresponding to p^r, r=1,2,..., $(M \times N)/(8 \times 8)$. Select M middle band coefficients on each DCT domain with stego-key_3 are recorded in zig-zag scanning order, where M should be p times. And then, the M coefficients are divided into non-overlapping blocks of size $1 \times p$. Let $F_r^t = \{f^r(k) \mid 0 \le i,j \le 7\}$be the blocks of size $1 \times p$,

$t=1,2,\ldots,M/p$. Calculate the sum of coefficients, $S_f^r(t)$ and $S_e^r(t)$, of F_t^r and E_t^r, respectively. The bit value b_w' is determined by comparing $S_f^t(t)$ and $S_e^r(t)$.

$$b_w' = \begin{cases} 1 & if \quad S_f^r(t) > S_e^r(t) \\ 0 & otherwise \end{cases} \tag{9}$$

The extracted message bit values, b_w's, and corresponding parity checks are then decoded via an iterative turbo decoder with key_2, as show in Fig.4. The decoder has a soft-input/soft-output decoder for each of the encoders along with a deinterleaver. These decoders take turns operating on the received data, forming and exchanging estimates of the message bit. At last decoded message are inversely permuted to get the reconstructed messages with key_1.

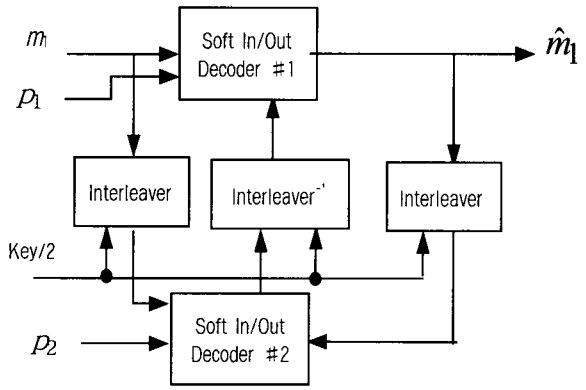

Fig. 4. Turbo Coding Decoder

Ⅲ. The System Security

In steganographic system security is related to the prevention of detection of any hidden communication by a hostile party [8]. We assume that the embedding technique and the cover image are both available a known to the public, i.e., we consider the case of known stego attack [8]. According to [9] a stego system is called ε -secure if

$$D(P_c \| P_s) = \sum P_c \log \frac{P_c}{P_s} \le \varepsilon \tag{10}$$

where P_C represents the distribution of the cover object, P_S represents the distribution of the stego object and $D(P_C \mid P_S)$ represents the relative entropy between the two probability distribution. For a perfectly secure system we must have $D(P_C \mid P_S)=0$. Furthermore, if an observer examines the difference (residual) between the two images, the resulting signal looks like white noise that has Gaussian distribution in both spatial and transform domains. Since the Gaussian noise has the highest uncertainty of all distributions for a given variance [10]. By examining the residual signal it is very difficult to assert whether this signal resulted from covert communication or due to some random transmission noise. Even if an observer suspects that some covert communication is taking place, it is not possible to extract any useful information by observing the difference signal.

Ⅳ. Experimental Results

In the simulation, to evaluate performances of our proposed data hidden algorithms, we take the popular image "Lena" as the cover image (cover image size 512×512, Fig.5) and set hiding data to be a stream of 64×128 bits. The stego-image and the extracted message

(a) (b)

Fig. 5. (a)The cover image (b)The hiding message

(a) (b)

Fig. 6. (a)The sego-image (b)The Extracted message

are shown in Fig. 6. The turbo code encoder using rate 1/3 convolutional encoders in the experiment. We also set $p=4$, $M=24$, The M middle band coefficients on each DCT domain with key_3 are recorded in zig-zag scanning order, and then, these coefficients are divided into non-overlapping blocks of size 1×4. Let $F_t^r=\{f^r(k)\,|\,1\le k\le 4\}$ be the blocks of size 1×4, $t=1,2,\ldots,M/4$, $r=1,2,\ldots,(M\times N)/64$. Calculate the sum of coefficients, $S_f^r(t)$ and $S_e^r(t)$, of F_t^r and E_t^r, respectively. The bit value b_w^i is determined by the equation(9). To test and verify the robustness of our algorithm, the sego-image is attacked by JPEG compression, cropping and Gaussian noise, as shown in Table 1 to Table 3 and Fig.7 to Fig.9. The similarity measurement "NC" between the original message M and the extracted message $\tilde{M}$ is defined as:

$$NC=\frac{\sum_i\sum_j m(i,j)\tilde{m}(i,j)}{\sum_i\sum_j[m(i,j)]^2} \tag{11}$$

JPEG is the important standard for still image compression, so we compress the stego-image at various levels of quality factors and show the corresponding correlation of the retrieved message. The results show

(a) (b) (c) (d)

Fig.7 The message retrieved from the stego-image "Lena" after JPEG compression with different compression ratio. (a)JPEG Compression ratio=17.71 (NC=0.8633) (b) JPEG compression ratio=18.18 (NC=0.8053) (c)JPEG compression ratio=19.69 (NC=0.7862) (d) JPEG compression ratio=23.69 (NC=0.7862)

(a) (b)

Fig. 8. The message retrieved from the stego-image "Lena" after cropping. (a)Remaining ratio=62.87% (NC=0.8279) (b)Remaining ratio=72.31% (NC=0.8624

Fig. 9. The message retrieved from the stego-image "Lena" under Gaussian noise with different noise (a)Gaussian noise, β =20% (NC=1.0000) (b)Gaussian noise, β =30% (NC=0.9194) (c)Gaussian noise, β =40% (NC=0.8018) (d)Gaussian noise, β =50% (NC=0.7462)

that our algorithms can achieve good correlation at the higher compression ratio, see Fig.10. To measure the difference between original and extracted message, we use peak signal (original message) to noise (the difference of original and extracted message) ratio. It is defined as

$$PSNR = 20\log 10(b/rms) \tag{12}$$

Table 1. The NC value and Bit Error Rate (BER) under JPEG lossy compression with different compression ratio

	JPEG compression with different compression ratio				
Compression ratio	8.2100	9.7000	11.2300	14.5000	17.7100
NC	0.9998	0.9812	0.9490	0.9148	0.8633
BER(Bit err rate)	0.0002	0.0656	0.0766	0.1855	0.3866

Table 2. The NC value and Bit Error Rate (BER) under Gaussian noise with different noise intensity

	Gaussian noise with different noise intensity				
β value (Gaussian noise)	10%	20%	30%	40%	50%
PSNR(dB)	22.4436	20.7059	19.3280	18.2354	17.3537
NC	1.0000	1.0000	0.9194	0.8018	0.7462
BER(Bit err rate)	0	0	0.0962	0.1941	0.2451

Table 3. The NC value and Bit Error Rate (BER) with remaining ratios after cropping

	Remaining ratios after cropping				
Remaining ratios	95.70%	87.89%	72.31%	68.87%	58.59%
PSNR(dB)	19.0671	15.3946	11.5654	10.5816	9.9653
NC	1.0000	0.9710	0.8714	0.8261	0.8053
BER(Bit err rate)	0	0.0300	0.1292	0.1727	0.2455

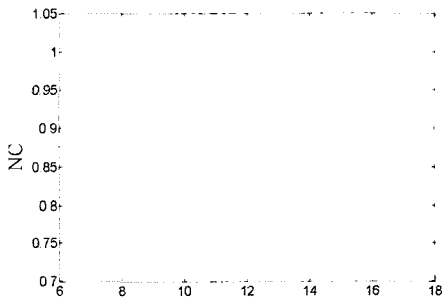

Fig. 10. A comparison of normalized cross correlation values for variant JPEG compression.

where b is the largest possible value of the signal, (typically 255 or 1), here $b=1$, and rms is the root mean square difference between two images.

We add simulating noises in Gaussian noise to stego-image, H'.

$$X = H' + \beta * N \tag{13}$$

Where N is Gaussian noise signal, its amplitude ranges are 0~1. We increase noise intensity parameter β from 10%~50%, so the stego-images with different intensity noises can be gotten. We estimate the mean

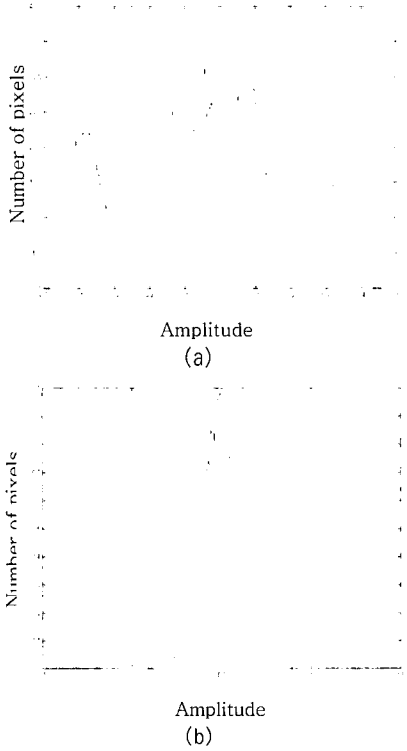

Fig.11. Histogram of stego and cover images, ":"denotes Ps, "-"denotes Pc (a)Spatial domain (b)Transform domain

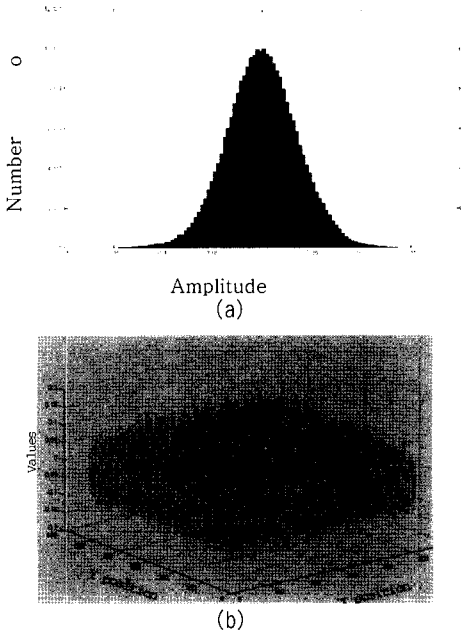

Fig.12 The histogram and spatial domain distribution of the residual image (a)Histogram of residual image (b)Spatial domain distribution of residual image

and the variance of the DCT coefficients of the stego and cover image. Their means of the coefficient distribution is the same, equal to 0.5029. The value of the variance for the stego image is 0.1712, while the value of the variance for the cover image is 0.1677. Fig.11 shows the distribution of the cover and stego images in the transform domain. Their distributions look similar. The pdf of the cover signal is close to follow a Gaussian distribution[10][11]. This distribution is determined by its mean and variance. Therefore, when we take their difference and divide the result by their product the ratio $P_C/P_S \approx 1$, which means the two distributions are close and $D(P_C \mid P_S) \approx 0$. Fig.12 shows the spatial distribution of the difference between the cover and stego image and a histogram of it. It is obvious that the residual signals follow a Gaussian distribution. Even if an observer suspects that some covert communication is taking place, it is not possible to extract any useful information by observing the difference signal. Hence the system is secure. Fig.13 shows the comparison of bit error rate with turbo coder and no turbo coder, here the line with star represents no coder and the line with round represents coder.

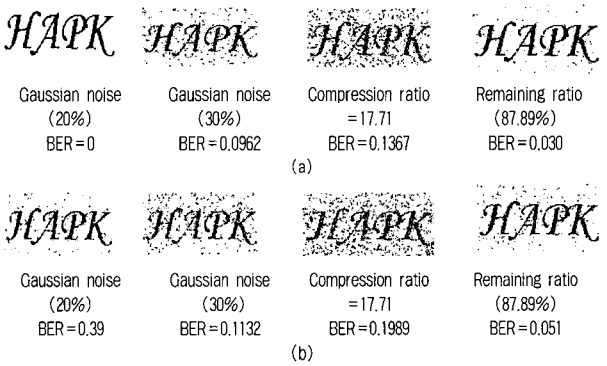

Fig. 13. The comparison of BER with turbo coder and no turbo coder. (a)BER with turbo coder (b)BER without turbo coder

V. Conclusion

This paper develops a novel robust information hiding technique that uses channel codes derived from the

error-correcting coder. The messages encoded by the turbo encoder are hidden in DCT transform domain of the cover image. Comparing with [12], NC values in Fig.10 are larger than those of [12], (see fig.9 in [12]), with the same compression ratio. Another advantage is that the proposed method is robust to Gaussian noise. The reason is that Turbo coder is used in the scheme. Some error messages extracted from the distorted image are corrected.

The scheme utilizes the sensitivity of human visual system to adaptively modify the contents of a set of blocks of DCT domain. The pixel intensities in a block are changed adaptively depending on the contrast of the block, without introducing any distortion and affecting the perceptual quality of the underlying cover image. Experimental results show that the proposed data hiding technique is robust to cropping operations, JPEG compression, Gaussian noise, and secure against known stego attacks by showing that both the perceptual quality in the spatial domain and the statistical properties in embedding transform domain of the cover and the stego images are both similar. Furthermore, the effect of embedding the data into the image is equivalent to an additive Gaussian noise. Hence, no evidence of cover communication can be claimed. The hidden information cannot be extracted unless one has access to the keys.

References

[1] David Kahn, "The Codebreakers: the comprehensive history of secret communication from ancient time to the Internet," Scribner 1996.

[2] F.L. Bauer, "Decrypted secrets: methods and maxims of cryptology," Berlin, Heidelberg, Germany, Springer-Verlag, 1997.

[3] I.J.Cox, J.Kilian, T.Leighton and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, pp.243-246, Sep. 1996.

[4] B.Pfitzmann, "Trials of traced traitors," Workshop on Information Hiding, Cambridge, Springer-Verlag, Berlin, pp.49-64, 1996.

[5] C.Berrou, A. Glavirux and P. Thitimajshima, "Near shannon limit error-correcting coding and decoding: Turbo-codes," Proceedings of the 1993 International Conference on Communication (ICC'93), pp. 1064-1070, 1993.

[6] C.Berrou and A. Glavirux, "Near optimum error correcting coding and decoding: Turbo-codes," IEEE Transactions on Communications vol. 44, pp.1261-1271, Oct. 1996.

[7] Soonyoung Kim, Jinsu Chang and Moon Ho Lee, "Simple iterative decoding stop criterion for wireless packet transmission," Electronics Letters, Vol.36, pp.2026-2027, Nov. 2000.

[8] S.Katzenbeisser and F.A.Petitcolas, "Information hiding techniques for steganography and digital watermarking," Artech House, Boston, MA, 2000.

[9] C.Cachin, "An information theoretic model for steganography," Information Hiding: Second International Workshop, Lecture notes in Computer Science, Spring-Verlag, Germany, pp.306-318, 1998.

[10] T.M. Cover and J.A.Thomas, Elements of Information Theory, John Wiley, New York, 1991.

[11] F. Alturki and R. Mersereau, "Secure blind image steganographic technique using discrete fourier transformation,", 2001 International Conference on Image Processing, Vol. 2, pp. 542 -545, Oct. 2001.

[12] Chang Hsing Lee and Yeuan Kuen Lee, "An adaptive digital image watermarking technique for copyright protection," IEEE Transactions on Consumer Electronics, Vol.45, pp.1005-1015, Nov. 1999.

저 자 소 개

楊傑(Yang Jie)

- 1978年 9月~1982年 8月 : 西安電子科技大學信息工程係 學士
- 1985年 9月~1988年 3月 : 武漢交通科技大學計算機及自動化係 碩士
- 1996年 9月~1999年 6月 : 上海交通大學 電子信息學院 博士
- 1999年 10月~2001年 9月 : 武漢理工大學 信息學院 敎授
- 2001年 12月~現在 : KISTEP 招請 在韓國全北大學 情報通信研究所 研究員
- Interesting areas : Information hiding, cryptography and multimedia communication
- Email : jieyang116@hotmail.com

李門浩(Moon Ho Lee)

- 1983年~1990年 : 全南大電氣工學科, 日本東京大學 情報通信工學科 博士
- 1980年~現在 : 全北大學校 情報通信工學科 敎授
- Interesting areas : Information hiding, Channel coding for Mobile communication, Image Processing
- Email : moonho@chonbuk.ac.kr

陳心浩(Xinhao Chen)

- 1990年 9月~1993年 8月 : 中南民族大學 電子與資訊學院 學士
- 2001年 8月~2002年 8月 : 韓國全北大學校 情報通信研究所 研究員
- Interesting areas : Signal processing, Spread Spectrum communication
- Email : xinhaochen@msn.com