A Lossy Compression Tolerant Data Hiding Method Based on JPEG and VQ

Ren-Junn Hwang, Timothy K. Shih, Chuan-Ho Kao
Department of Computer Science and Information Engineering
Tamkang University
Taipei, Taiwan, R.O.C.
victor@mail.tku.edu.tw, tshih@cs.tku.edu.tw, chk64@ms17.hinet.net

Abstract

A lossy compression tolerant data hiding method is proposed in this paper. The image which hides data is named a stego-image. Most of data hiding methods will lose some hidden data when the stego-image is compressed by lossy compression process. However, there are few people will transmit image without lossy compression in the public internet. By the proposed method, the stego-image can be compressed by lossy compression method to reduce the image size. The receiver extracts complete data correctly from the lossy compressed image. Our hiding technique is based on the Vector Quantization (VQ) and the lossy compression technique of JPEG. The human visual system is difficult to detect there are unusual pixels in the stego-image. Because the proposed method is tolerant of lossy compression, it speeds up the transmission of stego-image and coincides with the transmitting image on the internet.

Keywords: Data Hiding, VQ, JPEG, Image Compression.

1 Introduction

With the proliferation of Internet technology, there are more and more information and data transmitted in it. Sometimes, we don't want to transmit the important information without any protection in the public internet directly. In this information age, the transmission of encrypted texts is not safe enough, because the encrypted texts are meaningless random codes. Transmitting meaningless random codes is directly to note the other people that there is confidence in it. Even if attacker cannot decrypt this cipher text, he can destroy or sequestrate it. Therefore, the pure encryption technology cannot solve the problem of transmitting secret data completely. If user hides the encrypted secret data into meaningful media, it is like to provide a secure channel to transmit confidential information. Other people will think it is a meaningful and its means are independent of the hidden confidential data. Only authorized receivers can extract real secret messages from this meaningful data. Thus, not only the data is difficult to decrypt, but also attackers are difficult to detect the hidden data.

There are some features in the data hiding topic which are very important. The most important feature is imperceptibility. If we want to hide something, we hope the other people would not discern between the original media and the stego-media that have been hidden something in it by us. There is no peculiar in the stego-media. Thus, people will not detect this media has been hidden something in it. The second is the capacity. If people can hide more data in the meaningful media, they will transmit more secret data. It is very conveniently. The third is security. If people find our media hidden something in it, they also cannot extract the data. They only can get some meaningless random code. In specially, the final feature is resistant removal [3][6]. Most of the proposed hiding methods have these features. But their stego-image can not tolerant the lossy compression. If their stego-image compressed by lossy compression, the hidden data will be lost seriously. In other word, the stego-image can not be compressed by lossy compression method to reduce its file size. In this paper, we propose a hidden method that the stego-image compressed by lossy compression process, but we still extract the hidden data correctly from it. In other words, we can reduce the file size of our stego-image by lossy compression [1][19].

In past hiding research, there are two major research categories. One category is use of spatial domain [11][17][23], they change the pixels value directly. The most common and simplest technique is LSB(Least Significant Bit) [15][21][22] data hidden method. People can change the entire least bit in each pixel value to embed their information. The advantage of this method is it provides large capacity. Besides, we usually can embed and extract information easily and quickly. But the robustness of hiding data is bed. The pixels values will be changed when it is processed by filter. Therefore, the stego-image should be transmitted directly without lossy compression. Other people will smell a rat when transmitting no compression image. The other method of spatial domain is based on amplitude modulation. Single hiding bits are multiply embedded by modifying pixel values in the blue channel [12]. The modifications are either additive or subtractive, depending on the value of the bit, and proportional to the luminance [20]. This method has shown to be resistant to both classical attacks, such as filtering, and geometrical attacks. But people can not extract complete data correctly after do the lossy compression process [4][14]. Thus, user can not hide text information in it. If user loses one of the hiding bits, we will misapprehend or not know the hiding contents.

Another category of hidden data is based on frequency domain [2][5]. The method will transform pixel value to frequency and employ the feature of frequency to embed data. For example, people often embedded their data on the image based on a JPEG model. First, they will cut the image as 8*8 non-overlapping blocks. Then they use the discrete cosine transformer (DCT) [8] to transform each block. Final, they will use quantization table to scale the DCT coefficients and embed their messages to these coefficients. People often embed their messages into the middle frequency components. Because if people embed their messages into the higher frequency components, their messages are easily be destroyed. In lower frequency, the embed messages will produce the terrible destroy of image quality. In frequency domain, it can resist more attack and raise the robustness [9][11][13]. The common methods are based on discrete cosine transformation or discrete wavelet transformation. The methods of above category have well image quality, but they will lose some embedded data, while the stego-image is compressed by lossy compression methods.

In this paper, we proposed a hiding method based on VQ and JPEG technique [16][18]. The stego-image is generated as the lossy JEPG compression formats. Its file size is small. It is the commonly image lossy compression file type. When we hide data use the proposed method and transmit in the internet, other people will not smell a rat in the file type. The receiver can extract the hidden data correctly from the lossy compression file.

This paper is organized as the following. Section 2 describes the embedding and extracting methods. We show some experiment results in Section 3. Section 4 discusses the experimental result of the proposed hiding method. Finally, we make some conclusions in Section 5.

2 Our Method

This section introduces our hiding method. There are many image compression methods have been proposed to reduce the image bit size but provide good quality. Our method based on two image compression techniques: VQ and JPEG. We hide the embedded data based on the vector quantization codebook. Then, the stego-image can be compressed by JPEG lossy compression to reduce the image file size.

In data hiding method, there are two important data, one is the embedded data and the other is original image. There are two layers to protect the hidden data in our method. In the first layer, we encrypt the hiding data and product one random seed. We rearrange the encryption hiding data bits based on the sequence that was generated by the random seed. In the second layer, we divide the original image by blocks. Each rearranged hidden data bit is corresponding to a block of the original image by left-to-right and top-to-down sequence. We select the codebook based on the hidden data bit. Then we find one codeword from the selected codebook which is the most similar one to the original block and replace the original block. All of the blocks of the original image will be replaced by these methods. We will extract the hidden data correctly based on the proposed extract process. Section 3 shows the experimental results of our proposed method.

Without loss of the generality, this paper assumes the cover image C is an $m \times n$ gray-level image and the gray-level is 256. The image represents as

$$C = \{c_{ij} \mid 0 \leqq i < m, 0 \leqq j < n, c_{ij} \in [0,255]\},$$

The data D, which is embedded in C, represents as

$$D = \{d_i \mid 0 \leqq i < g, d_i \in [0,1]\}$$

The second level of proposed hiding scheme contains two phases: embed data phase and extract data phase. The flow chart of embed data phase is shown in the Figure 1 and the flow chart of extract data phase is shown in the Figure 2. We introduce them in the following paragraphs.

2.1 Embed Data Phase

By this phase, we embed the data D into the cover image C to produce the stego-image. The stego-image is looked like the cover image C by human visual systems. However, the stego-image contains the data D.

[Part 1 Codebook generation]

Step-E1: Divide the cover image C into $(m\times n)/(8\times 8)$ blocks. Each block B_i is an 8×8 pixels block.

Step-E2: Train a 512-codewords codebook W_{512} based on the cover image C by using the VQ-LBG algorithm [7].

Step-E3: Transform the cover image C and its codebook W_{512} of Step-E2 by the DCT function.

Step-E4: Sort the 512-codewords codebook W_{512} by increasing progressively based on the DC value of each codeword.

Step-E5: Divide the 512-codewords codebook into two 256-codewords subcodebooks as the following steps. One is called 0-subcodebook W^0_{256}, another is called 1-subcodebook W^1_{256}.

Step-E5-1: Select the first unselected codeword V_{0i} from W_{512} and mark it as "selected".

Step-E5-2 : Find an unselected codeword V_{1i} which is the most similar to V_{0i} in W_{512}. We use a modified Euclidean distance function to evaluate the similarity of two codewords. The modified Euclidean distance function is defined in the following, where we multiple the first eight AC value with the weight values: $\omega_1 = \omega_2 = 128$, $\omega_3 = \omega_4 = 64$, $\omega_5 = \omega_6 = \omega_7 = \omega_8 = 8$ by z-z scan sequence and others AC value with the weight value $\omega_i = 1$, for $i = 9, 10, \ldots, 63$. Besides, the DC value of selected V_{1i} is in the range: [the DC value of V_{0i}-3, the DC value of V_{0i}+3].

$d(V_{0i}, V_{1i}) = \Sigma\, (\omega_j \times (v_{0j} - v_{1j})^2)$, $1 \le j \le 63$ (v_{0j} and v_{1j} is the AC values of V_{0i} and V_{1i})

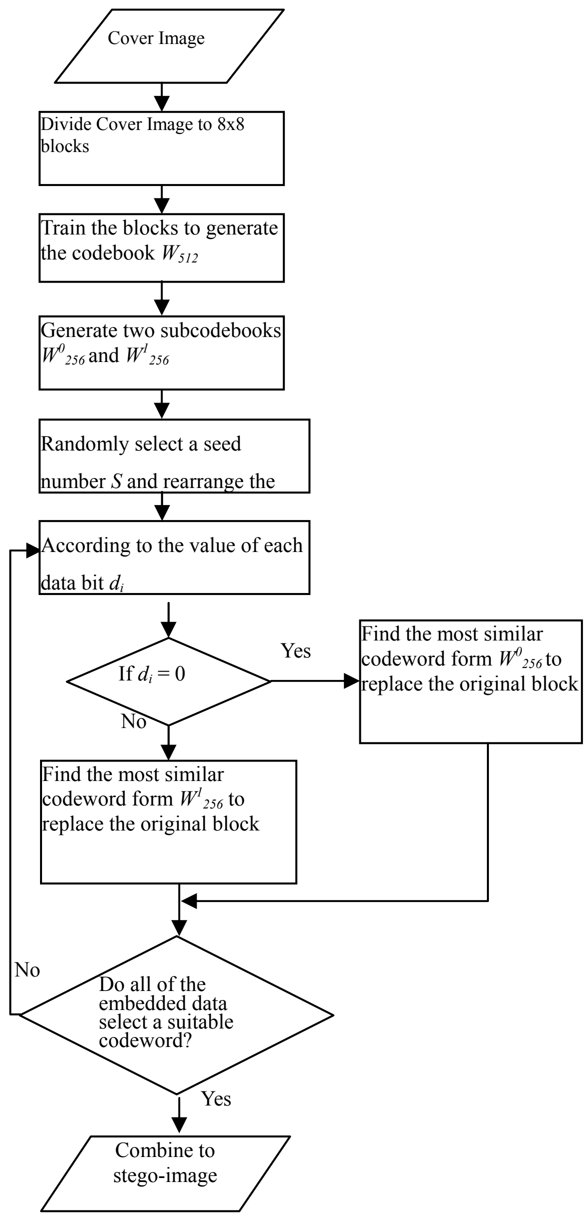


Figure 1 The flow chart of our embed data phase

Step-E5-3 : Put the V_{0i} to W^0_{256} and put the V_{1i} to W^1_{256} sequentially.

[Part 2 Data embedding]

Step-E6 : Randomly select a seed number S.

Step-E7 : Generate g different numbers named $A = \{ a_1, a_2, \ldots, a_g \}$ based on the seed S, where $1 \le a_i \le (m \times n)/(8 \times 8)$ and rearrange the encryption hiding data.

Step-E8 : Construct the stego-image C' based on W^0_{256}, W^1_{256}, cover image C and embedded data D. C' is the stego-image that look like C and embedded the data D. According to the value of

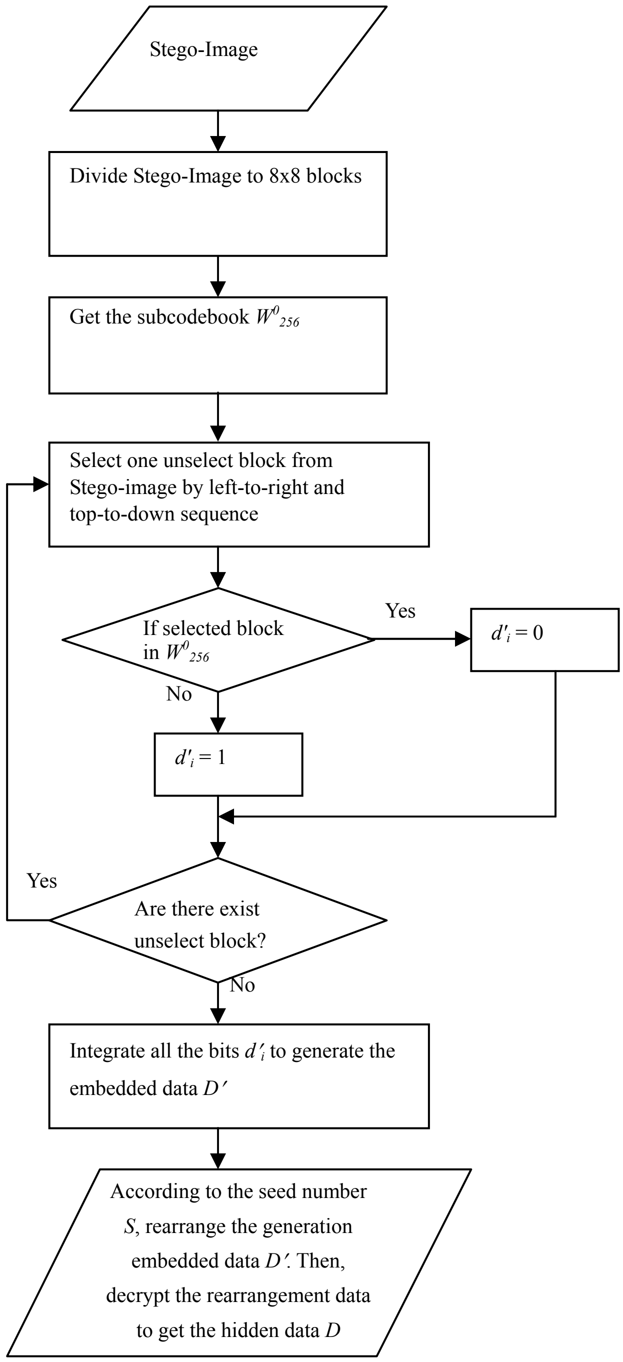


Figure 2 The flow chart of our extract data phase

Table 1 The experiment result (1)The first row is the compression ratio of cover image and stego-image.(The JPEG quality is 50) (2)The second row is the PSNR value of JPEG decompression of cover image and decompression of stego-image (3)The third row is the PSNR value of VQ decompression of cover image and decompression of stego-image (4)The forth row is the PSNR value of JPEG and VQ decompression of cover image and decompression of stego-image

	Lena	F16	Goldhill	Pepper	Toys
Compression ratio	17.8：1	16.24：1	13.91：1	12.60：1	16.97：1
The PSNR value of JPEG of cover image and stego-image	29.21	27.24	27.68	28.67	27.79
The PSNR value of VQ of cover image and stego-image	29.4	27.76	28.38	29.32	27.90
The PSNR value of JPEG and VQ of cover image and stego-image	30.41	28.92	30.03	30.12	29.18

each data bit d_i, generate the block $B'a_i$ of C' based on the Ba_i of C as follows: If the embedded data d_i = 0, then we select the codeword in the W^0_{256} as the $B'a_i$ by modified Euclidean distance, which is the most similar to the block Ba_i of the cover image; if the embedded data d_i = 1, then we select the codeword in the W^1_{256} as the $B'a_i$ by modified Euclidean distance, which is the most similar to the block Ba_i of the cover image.

Step-E9：Organize each $B'a_i$ $(i=1, 2,..., g)$ to construct the stego-image C'.

2.2 Extract data Phase

Assume the stego-images $C' = \{ c'_{ij} \mid 0 \leqq i < m , 0 \leqq j < n , c'_{ij} \in [0,255] \}$. The receiver extracts the embedded data from C' as the following steps.

Step-D1：Generate the set A based on the seed S as Step-E7.

Step-D2：Divide the stego-image into 8×8 pixels blocks.

Step-D3：Extract each data bit d_i from its correspondence block Ba_i in stego-image by comparing the block Ba_i with all the codewords in the 0 sub-codebook. If we find one codeword in the W^0_{256} which is same the block Ba_i, the embedded value $d'_i = 0$; otherwise the embedded value $d'_i = 1$.

Step-D4：Integrate all the bits d'_i extracted by Step-D3 to generate the embedded data D'.

Step-D5：According to the seed number S, rearrange the generation embedded data D'. Then, decrypt the rearrangement data to get the hidden data D.

3 Experiment

This section shows some experimental results of the proposed method. We use the C language to write the VQ and JPEG lossy compression. In our experiment, we randomly select 4096 bits to be the embedded data. We select Lena, F16, Goldhill, Pepper and Toys, as the cover images. They are gray-level 512×512 pixels images. The JPEG compression quality is 50 and the codebook size is 512 codewords.

It is difficult to estimate the quality of an image by human visual system. It is also not objectivity by the sense of quality of image from some people. The sense of an image will be influenced by different screen and VGA card setting. Up to now, there is no optimal measurement to estimate the quality of an image. PSNP (Peak Signal to Noise Ratio) value is an objectivity measurement, which is used to estimate the difference between two images. PSNR is a measure of the peak error. It is derived from the comparison of two pixels comprised of valued matrices — by the order of the number of pixels in a row-to-column. We use PSNR to estimate the difference between cover-image and stego-image. The mathematical formulae for the PSNR are:

$$\mathrm{MSE} = \left(\frac{1}{m \times n}\right)\sum_{i=0}^{i<n}\sum_{j=0}^{j<m}(c'_{ij} - c_{ij})^2 \text{,}$$

$$\mathrm{PSNR} = 10 \log_{10} \frac{255^2}{\mathrm{MSE}} \mathrm{dB} \text{.}$$

c_{ij} and c'_{ij} denote the pixel values of C and C' image and MSE is mean-square error. The results of our experiment are shown in Table 1. The first row is the compression ratio of cover image and stego-image. The compression ratio are larger than 12. The second row of table is the PSNR value of JPEG decompression of cover image and decompression of stego-image. The third row of Table 1 is the PSNR value of VQ decompression of cover image and decompression of stego-image. The fourth row of Table 1 is the PSNR value of JPEG and VQ decompression of cover image and decompression of stego-image. The third and fourth row values are very similar. So the hiding scheme did not destroy the image too much. Obviously, there are good compression feature in our proposed method. The most important is we can extract all of the hiding data correctly after these lossy compressions.

It is clear that our method provides good transparent and high capacity. In other word, people hiding important data based our method is not easily to be detected when transmitted the stego-image in the public internet. Furthermore, the stego-image of our method can be compressed by the lossy JPEG to reduce the file size which speeds up the transmitting time. The proposed method is a secure and convenience method.

4 Discussion

Hiding information is a hot topic. There are many research results have been proposed. People often estimate their method by security, PSNR value and capacity. This section not only shows that our method is an efficient method, but also shows the characteristic of our method. Users can rely on this experimental result to find the best setting value of their environment. Thus, users exactly decide what their want according to their need. In other words, users use the proposed method adequately.

In security aspect, user applies the cryptography technique to protect the hiding information first. Then, he embeds the cipher text by our method and transmits it. Thus, if other people extract the data, they don't know what in it. Besides, we use one random seed S to recombine the hiding location. If other people don't get the seed, they can not recover the correct data. So, the proposed method combines with two additional security technology layers to protect the hiding data.

Compression ratio and image quality are two important features in our proposed data hiding method. But if we want to get a larger compression ratio of image, the image quality will be bad. User decides whether to increase the compression ratio to speed up transmitting or to maintain the image quality. In our experiment, we select the JPEG compression quality is 50 and the codebook is 512 codewords. People can alter the value of JPEG compression quality or codebook size to change the compression ratio or image quality. Of course using the better VQ training technique, we can get the better image quality.

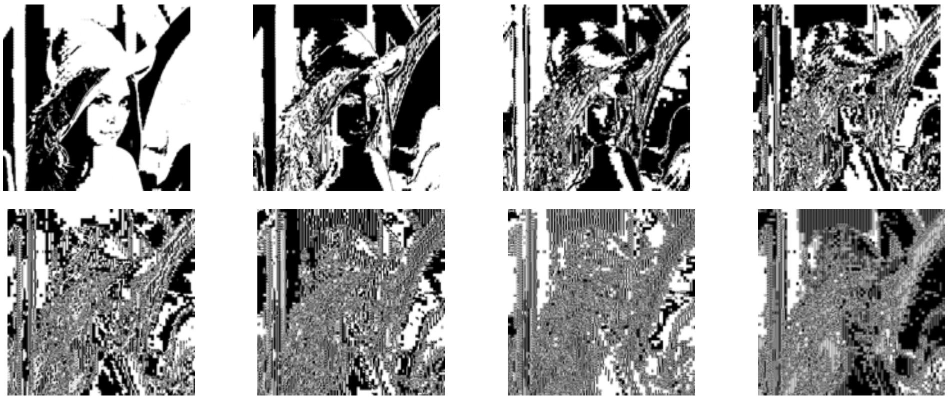
Our embedded process includes the JPEG lossy compression technique. We can extract the embedded data completely from the lossy compressed stego-image. Thus, we can let the stego-image to be small size. People use our proposed method can reduce the transmitting time and process a large number secret data conveniently. The most important thing is there are few people transmit no compression image in the internet. Our method generates a JPEG lossy compression type of stego-image. It is fit the transmission of real internet nowadays.

How to find the two similar blocks is a very important issue in our method. It will influence the PSNR of stego-image and cover-image. The traditional method to evaluate the similarity is the Euclidean distance equation. It can be defined as: $d(V_i, V'_i) = \Sigma (v_j - v'_j)^2$, where v_j and v'_j are two components of these two blocks. In our method, we modify the Euclidean distance equation as value of $d(V_i, V'_i) = \Sigma\, \omega_i\, (v_j - v'_j)^2$. The front of the AC coefficients by z-z scan in DCT transformation are multiplied by weights because of they are more influential. The modified function helps us to find the more similar blocks. Thus, we get a better PSNR value of the image.

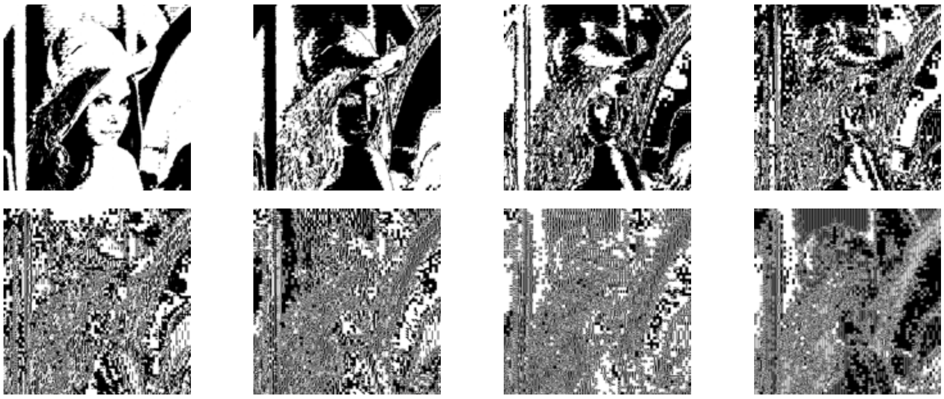
One normal image's bit-planes will have normal spread. If we use LSB or spatial domain technique to embedded data, it will destroy this spread. The attacker can easily detect that the stego-image is unmoral. The bit-planes of a stego-image that is generated by our method are shown Figure 3(b). By the experiment results of Figure 3, it is clear that the bit-planes of the stego-image are similar to the bit-planes of cover image with JPEG and VQ lossy compression. The attack is hard to detect the stego-image which is generated by our method.

5 Conclusion

This paper proposes a hiding method which tolerates lossy compression. The stego-image can be compressed by lossy compression process without affect the hidden data. Our approach is based on the VQ and JPEG technique lossy compression process. It provides large compression ratio. When receiver receives the stego-image, he decompresses the stego-image and extracts all of the embedded data correctly from it. This hiding technique reduces the image size and raises the rate of embedded size. When people transmit the lossy compressed stego-images, it is more efficient than transmit the no compressed stego-image. It is more practical than the other hiding methods.



(a) The bit-planes of the cover image with JPEG and VQ lossy compression



(b) The bit-planes of the stego-image which is embedded secret data by our method
Figure 3 The bit-planes of our experiment results (from MSB→LSB)

References

[1] Bender, W., Gruhl D., Morimoto, N., and Lu, A., "Techniques for data hiding", IBM System Journal, 35(3&4), 1996, pp. 313-336.

[2] Chang, C. C., Chen, T. S., and Chung, L. Z., "A Steganographic Method Based upon JPEG and Quantization Table Modification", Information Sciences, Vol. 141, 2002, pp. 123-138.

[3] Chen, L. H., and Chang, H. M., "Two New Methods for Visible Digital Watermarking," In the Proceedings of the Ninth National Conference of Information Security, 1999, pp. 23-26.

[4] Chen, T. S., Chang, C. C., and Hwang, M. S., "A Virtual Image Cryptosystem Based upon Vector Quantization," IEEE Transactions on Image Processing, Vol. 7, No. 10, Oct. 1998, pp. 1485-1488.

[5] Chung, K. L., Shen, C. H., and Chang, L. C., "A novel SVD- and VQ-based image hiding scheme", Pattern Recognition Letters, Vol. 22, 2001, pp.1051-1058.

[6] Cox, I. J., Kilian, J., Leighton, T., and Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, Vol. 6, No. 12, 1997, pp. 1673-1687.

[7] Gersho, A., and Gray, R. M., "Vector Quantization Signal and Compression", Kluwer Academic Publisher, Boston Hardbound Nov. 1991.

[8] Gray, R. M., and Neuhoff, D. L., "Quantization", IEEE Trans. Information Theory, Vol. 44, No. 6, 1998, pp. 2325-2383.

[9] Hsu, C. T. and Wu, J. L., "Hidden Digital Watermarks in images", IEEE Transactions on Image Processing, Vol. 8, No 1, Jan. 1999, pp.58-68.

[10] Hsu, C. T., and Wu, J. L., "DCT-Based Watermarking for Video", IEEE Transactions on Consumer Electronics, Vol. 44, No. 1, 1998, pp. 206-215.

[11] Hwang, R. J., Shih, T. K., Kao, C. H., and Chang, T. M., "Lossy Compression Tolerant Steganography", Lecture Notes in Computer Science, Vol. 2105, Jan. 2001, pp. 427-435.

[12] Kutter, M., Jordan, F., and Bossen, F., "Digital Signature of Color Image using Amplitude Modulation", J. Electron. Imaging 7 (2), April 1998, pp. 326-332.

[13] Langelaar, G. C., and Lagendijk, R. L., "Optimal Differential Energy Watermarking of DCT Encoded Images and Video," IEEE Transactions on Image Processing, Vol. 10, No. 1, Jan. 2001, pp. 148-158.

[14] Langelaar, G. C., Lagendijk, R. L., and Biemond, J., "Removing Spatial Spread Spectrum Watermarks by Non-linear Filtering," In 9th European Signal

Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 1998, pp. 2281-2284.

[15] Lee, Y. K. and Chen, L. H., "An Adaptive Image Steganographic Model Based on Minimum-Error Replacement", Proceedings of the Ninth National Conference on Information Security, May. 14-15, Taichung, Taiwan, 1999, pp. 8-15.

[16] Linde, Y., Buzo, A., Gray, R.M., "An Algorithm for Vector Quantizer design", IEEE Trans. Comm., Vol. 28, No. 1, 1988, pp. 84-95.

[17] Liu, J.C. and Chen, S.Y., "Fast two-layer image watermarking without resorting to original image and watermark ", Proc. of joint Conference of International computer Symposium, 2000, pp. 231-238, Taiwan, Republic of China.

[18] Pennebaker, W. B. and Mitchell, J. L., JPEG: Still Image Data Compression Standard. New York: Van Nostrand Reinhold, 1993.

[19] Pfitzmann, B., "Information Hiding Terminology," Information Hiding (Anderson, R. et.), Lecture Notes in Computer Science, Vol. 1174, Springer, 1996, pp. 347-350.

[20] Swanson, M. D., Xu, B., and Tewfik, A. H., "Robust Data Hiding for Images," In 7th Digital Signal Processing Workshop (DSP96), IEEE, Loen, Norway, 1996, pp. 37-40.

[21] Thien, C. C. and Lin, J. C., "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function", Pattern Recognition, Vol.36, 2003, pp.2875-2881.

[22] Wu, D. C. and Tai, W. S., "A Steganographic Method for Images by Pixel-Value Differencing", Pattern Recognition Letters, vol. 24, 2003, pp. 1613-1626.

[23] Yu, P. T., Tsai, H. H., and Kin, J. S., "Digital watermarking based on neural networks for color images", Signal Processing, Vol. 81, 2001, pp. 663-671.

Biographies

Ren-Junn Hwang was born in, Nantou , Taiwan, Republic of China, on April 15, 1964. He received the B. S. in Applied Mathematics in 1986 from Chung Cheng Institute of Technology, Taoyuan, Taiwan. He received his M. S. degree in Computer Science in 1992 and Ph. D. in Computer Science in 1998 from National Chung Cheng University, Chiayi, Taiwan. From 1998 to 2000, he worked as an associate professor of the Department of Computer Science and Information Engineering at Chung Cheng Institute of Technology, Taoyuan, Taiwan. Since August 2000, he has worked as an associated professor of the Department of Computer Science and Information Engineering at TamKang University, Taipei, Taiwan. Dr. Hwang is a member of IEEE and the Phi Tau Phi Society of the Republic of China. His research interests include network security, computer cryptography, computer security, information hiding, steganography.

Timothy K. Shih is a Professor of the Department of Computer Science and Information Engineering at Tamkang University, Taiwan, R.O.C. He is a senior member of IEEE and a member of ACM. His current research interests include Multimedia Computing and Networking, Distance Learning, and Content-Based Multimedia Information Retrieval. He was a faculty of the Computer Engineering Department at Tamkang University in 1986. In 1993 and 1994, he was a part time faculty of the Computer Engineering Department at Santa Clara University. He was also a visiting professor at the University of Aizu, Japan in summer 1999, a visiting researcher at the Academia Sinica, Taiwan in summer 2001, and an adjunct faculty member of Xidian University, China. Dr. Shih received his BS and MS degrees in Computer Engineering from Tamkang University and California State University, Chico, in 1983 and 1985, respectively. He also received his Ph.D. in Computer Engineering from Santa Clara University in 1993. Dr. Shih has edited many books and published over 300 papers and book chapters, as well as participated in many international academic activities, including the organization of many international conferences and special issues of international journals. He is the founder and co-editor-in-chief of the International

Journal of Distance Education Technologies, published by Idea Group Publishing, USA. Dr. Shih has received many research awards, including Tamkang University research awards, NSC research awards (National Science Council of Taiwan), and IIAS research award of Germany. He also received many funded research grants from both domestic and international agencies. Dr. Shih has been invited frequently to give keynote speeches, tutorials, panels, and talks at international conferences and overseas research organizations.

Chuan-Ho Kao received the B.S. degree from the Department of Computer Science and Information Engineering at Tamkang University, Taiwan, R.O.C., in 2000. He is a Ph.D. student in the Department of Computer Science and Information Engineering at Tamkang University. His research interests include information hiding and content based retrieval.