

Error Concealment for Digital Images Using Data Hiding

Yuxin Liu, Yanda Li

State Key Laboratory of Intelligent Technology and Systems

Department of Automation, Tsinghua University, Beijing, 100084, P. R. China

Email: liuyx@jerry.au.tsinghua.edu.cn

Abstract

A novel strategy for error concealment of digital images is proposed in this paper, which is implemented by adopting the data hiding technique. Different from all the existing data hiding algorithms, the hidden data in our strategy is extracted from the host data, and then is embedded back into the host itself. Such a host signal with redundancy is proved to be robust when transmitted in the error-prone network environment, and the restored hidden data at the decoder can help improve the performance of error concealment of the lost data. Therefore, our new strategy has advanced a new way for solving the problem of error concealment. Meanwhile, it proposes a new application for the data hiding technologies, whose success have been mainly achieved when applied to copyright protection or image authentication. Furthermore, an algorithm as an example is developed based on the functionality of our new strategy, which could demonstrate its flexibility and efficiency.

Keywords: ECDH, data hiding, error concealment, signal estimation and prediction, perceptual analysis

I. Outline of the Novel Strategy

It is well known that digital media (including digital image, video, audio and so on) could experience large changes without causing noticeable perceptual difference, which makes lossy compression possible. Carefully designed lossy compression algorithms could get rid of much redundant data from digital media while maintaining good perceptual effect, just because the ultimate acceptors are human beings' perceptual organs that are not so perfect. Based on the similar motivation comes out a new technique called "data hiding". Data hiding aims at embedding a secondary data (referred to as signature) into an original digital media (referred to as host) with no visible distortions. Usually, a data hiding algorithm should satisfy both the two requirements of robustness and imperceptibility. In another word, the signature hidden in the host could not be perceptually observed and not so easily be got rid of. The key component to design the algorithm is how to manage the trade-off between every two sides of the three factors: imperceptibility of signature, robustness against distortion and noise introduced by signal processing or attacks, and the quantity of hidden data that can be embedded into the host.

There exist several methods to classify all the existing data hiding techniques. First, according to what kind of signature is embedded, they can be divided into two classes: robust data hiding and fragile data hiding. Algorithms of the former class should be robust enough to various kinds of signal deformations such as lossy compression, and to all kinds of malicious attacks such as multi-watermarking as well. While for those algorithms of the latter one, they should show fragility in some specific situation in order to indicate whether the integrity of the original signal has been destroyed. Secondly, there are two kinds of data hiding algorithms according to whether the signature is embedded in the spatial domain or in the frequency domain of the host. Thirdly, with respect to the strategy adopted for hidden data extraction, there are two categories referred to as blind data retrieval and non-blind data retrieval respectively. Here blindness means that the hidden data is restored in the absence of the original host without hidden data embedded.

Great success of data hiding has been achieved when it is applied to copyright protection and image authentication, where the signature data are usually referred to as robust watermark and fragile watermark

respectively. In contrast to digital watermarking, data hiding has some other applications, such as hiding data that could be exploited as reference information or control information, or even hiding another media signal, such as implementation of hiding video-in-video ^{[2][3]}. Such kind of applications, which is usually denoted as augmentation data embedding, however, has achieved less success than digital watermarking does. The reason can be attributed to the great challenges confronted by the technologies that it is required to implement large quantity data embedding while maintaining imperceptibility at the same time. Another reason may be that such kind of application to just embed additional information into a given signal is not so attractive.

In this paper, a new application for data hiding is proposed. Different from all the existing data hiding technologies, the scheme here presented does not embed a secondary media into a given one, but tries to embed the host itself back to the host instead. In particular, such a scheme is applied to error concealment of digital images, i.e., post-processing of images that are transmitted over error prone network.

Numerous methodologies have been advanced in the literature to deal with the problem of digital image transmission in an error-prone network environment. Recently, complete data losses rather than errors on bits are more concerned when transmitting images over a packet-oriented data network ^[12-15]. For example, in ATM networks data are lost badly during the periods of channel congestion. To minimize the impact of such cases, various error concealment techniques have been developed. Generally speaking, there exist two categories of approaches for error concealment: those that are active and those that are passive. In active concealment, error resilient coding techniques are adopted along with retransmission. While in passive concealment, the lost data are restored by post-processing techniques such as the interpolation-type procedures. Thanks to the redundancies that still exist in the coded digital images, it is possible to estimate the missing data from those received at the decoder in an effort to conceal the effect of channel impairments.

It is obvious that the more information of the missing data is at hand, the more perfect reconstruction of the missing data can be achieved by passive concealment. Motivated by such a simple principle, a novel strategy can be proposed to implement passive concealment using data hiding techniques. A salient new feature of such a strategy is that it advances a new application for data hiding, and at the same time, it presents the possibility to further improve the performance of error concealment. The outline of such a strategy is illustrated in Figure 1.

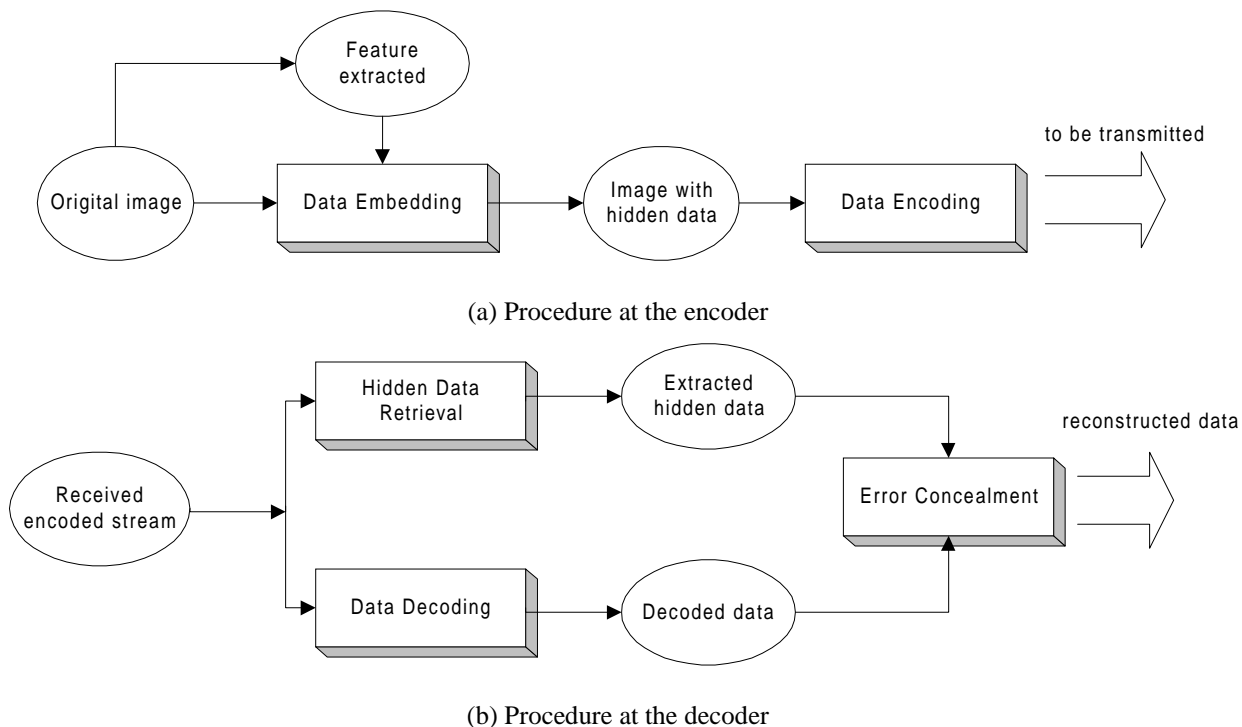


Figure 1. Outline of the proposed strategy for error concealment of digital images using data hiding

In the scheme illustrated in Figure 1, which will be referred as ECDH (error concealment by data hiding) in the later part of this paper, with data hiding techniques adopted, some significant feature information is extracted from a given image signal and embedded back into the image itself. Then, as usual, the host image with the hidden data is coded and transmitted. On decoding, the embedded data are reconstructed and the original host is restored based on the reconstructed hidden data along with some other post processing methods. Since some information of the lost data is hidden within the received packets, it is likely that error concealment could be conducted more successfully under the help of the hidden data. As long as a good blind data hiding algorithm is designed and the hidden data are carefully chosen, it is rational to believe that ECDH holds the potential to further improve the performance of error concealment of digital images transmitted over error-prone data network.

II. Some Discussions on ECDH

1. Robustness Requirements for ECDH

Different from digital watermarking, robustness is not required so strictly in ECDH. Signal deformation imposed on the hidden data in ECDH mainly comes from lossy compression, and the malicious attacks need not be so seriously considered. Thanks to the observation that no matter what coding method is used, many redundancies still exist in compressed digital images, it is most likely to embed in an image relatively large amount of data that can survive deformation caused by lossy compression. Robustness constraint in ECDH can be further loosened. In general, a data hiding algorithm should satisfy the requirement to be robust under various lossy coding methods. But in ECDH, since it is exploited within a specified frame of image encoding, transmission, and decoding procedure, a data hiding technique can be adopted which is designed specifically suitable to a particular image coding method, such as a DCT codec or a DWT codec. Therefore, the overall robustness performance of ECDH can be further improved.

2. Blind Hidden Data Retrieval

Similar to many other applications of data hiding, ECDH needs to conduct data retrieval in the absence of the original host image. Therefore, the success of ECDH largely depends on the development of blind data retrieval techniques. Recently, more and more achievements have been published to deal with blind data retrieval. Obviously it is much more complicated to design blind retrieval algorithms than to do with those non-blind, especially when the hidden data need to be reconstructed rather than just to be identified as in digital watermarking. For signal identification, what is concerned with most is not what the hidden data are, but to identify whether there exists some authorized information embedded. To identify the embedded data, a similarity measure is usually calculated by exploiting signal correlation techniques. In contrary, if the hidden data are to be restored, such as extraction of a second video or image embedded, blind data reconstruction algorithms need to be designed, usually by making use of signal estimation and prediction techniques^[1-3].

3. Passive Concealment or Active Concealment

In general, ECDH can be regarded as a passive concealment scheme, for the hidden data are exploited to help post-process the received image data. However, it is interesting to treat it from another point of view. After an image with hidden data is compressed, the code stream will become more robust than that without data hidden, since in any portion of the data stream, there always exists some information of another portion of the data. The decoding process thus will be less affected by packet loss of the data network. Therefore, data hiding may be combined with image coding and be treated as one procedure, which is much similar to an error resilient coding process. Accordingly, the scheme ECDH can be regarded as an active concealment for image reconstruction after being transmitted in an error-prone environment.

4. Advantages and Disadvantages

It has been pointed out that ECDH can be referred to as an active error concealment method. Compared with any other active concealment schemes, ECDH has some inherent advantages because it adopts the data hiding technique.

For instance, the redundancy information embedded within the host signal is imperceptible, and it does not request any additional heading information that is easily lost. More significantly, as shown in Figure 1, since ECDH is developed under a specified coding procedure, it should not contradict with the existing coding algorithm framework or image transmission standards.

However, similar to any other active schemes for error concealment, ECDH would affect the coding efficiency of the original host signal to some extent, for it should embed additional information within the host and need to maintain the robustness of the signature at well. At this point, the idea of “joint source and channel coding” could be exploited as a reference. By jointly considering the data hiding and the source coding procedures, the optimal coding performance can be achieved under the condition of data embedding at an ideal quality and quantity. On the other hand, the embedded data might degrade the perceptual performance of the host signal. To solve such kind of problems, some techniques such as perceptual analysis need to be utilized.

III. A Simple Example of ECDH

In this section, an example of ECDH is discussed in detail. A schematic of the algorithm is shown in Figure 2. As illustrated in Figure 2, data hiding is conducted in the block-DCT domain, so that it will specifically survive the JPEG lossy compression. Motivated by the methodology of data casting and blind data retrieval introduced in [1][2], we embed the DC coefficient of each 8×8 block into one of its neighboring blocks using multi-dimensional lattice coding method. After the image with hidden data is transmitted over lossy packet network, the extracted DC coefficients are made used of, combined with some post-processing method such as the algorithm presented in [14] that takes advantage of the correlation between transformed blocks, to reconstruct the lost data. On the other hand, in order to execute the perceptual analysis so that the hidden data can be embedded more effectively, an adaptive block classification method based on the so-called Texture Mask Energy (TME) [17] is developed.

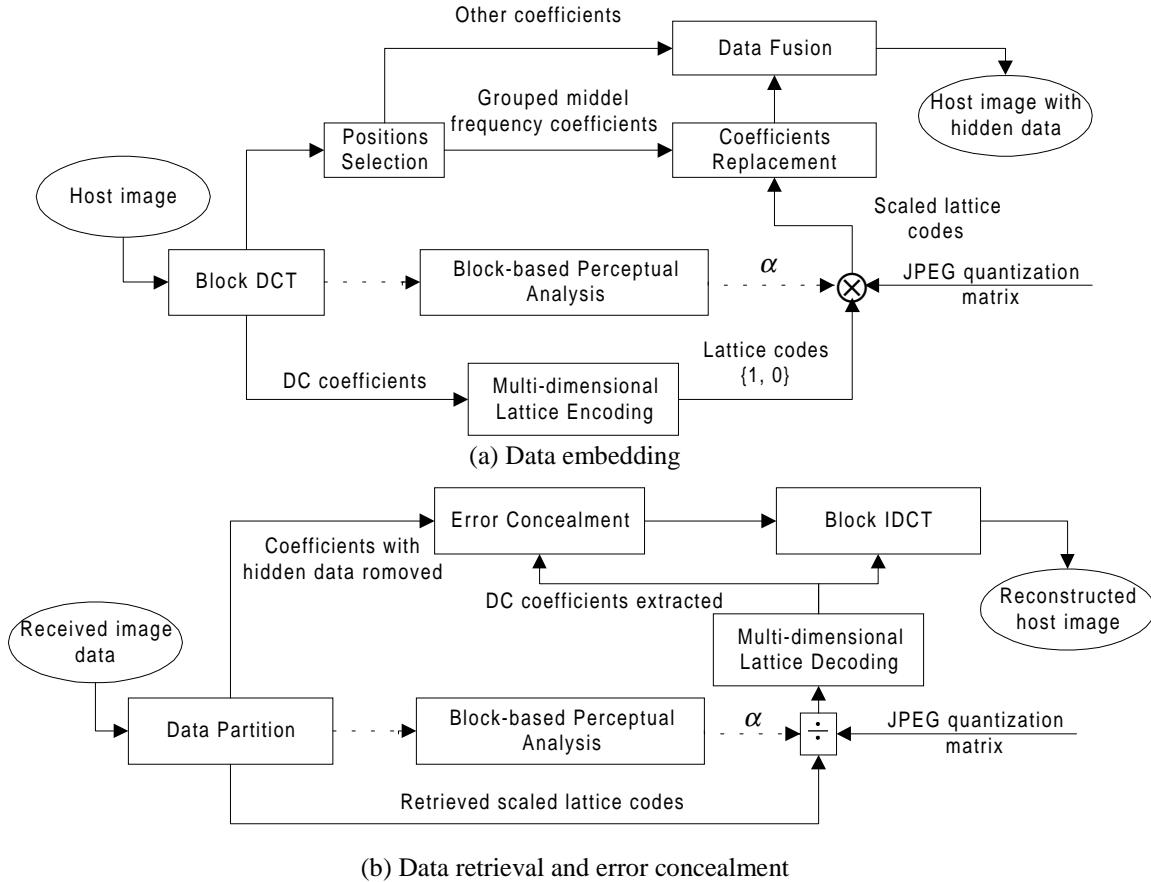


Figure 2 Outline of the algorithm as an example of ECDH

The DC coefficients are chosen as the signature in the above algorithm based on the following considerations: (1) Since data hiding is executed in the DCT domain, DC coefficients are easily obtained; (2) The DC of one block is the most significant coefficient that represents the overall information and contains the major energy of the block. The algorithm here presented is just an example, which mainly aims at demonstrating the feasibility and efficiency of the ECDH strategy. This algorithm could be naturally generalized so as to suit image coding methods other than DCT-based codec. For example, an algorithm can be advanced where the procedure of data hiding is conducted in the wavelet domain, so that it may survive the DWT based lossy compression in the context of JPEG 2000. Further more, techniques can be easily developed under the framework of ECDH to be applied to error concealment of other digital media data such as encoded video streams.

IV. Experimental Results

As shown in Figure 3, the algorithm discussed is applied to the 512×512 gray-level Lena image.

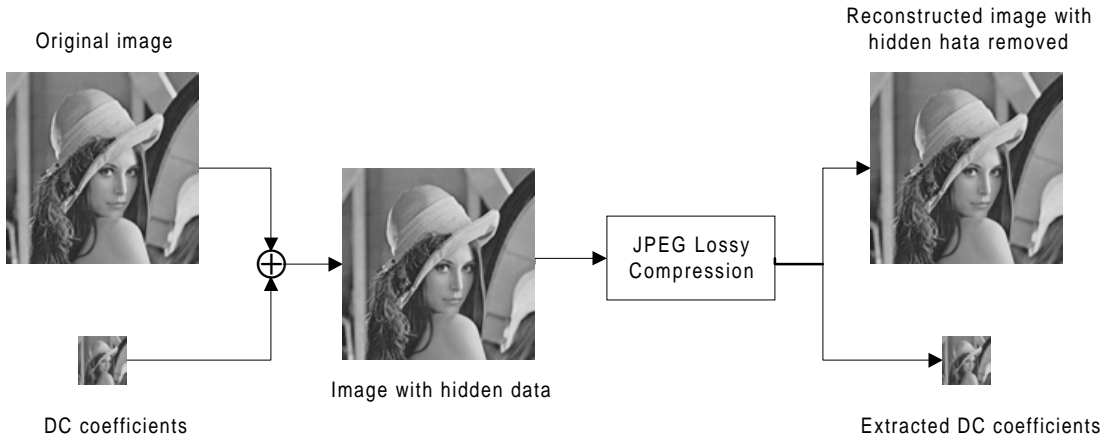


Figure 3. Data embedding and extraction applied to Lena

To implement error concealment, random block loss is simulated. For simplicity, 10% of the $64 \times 64 = 4096$ blocks of Lena are lost randomly through all the experiments to be conducted. As is presented in [14], an $N \times N$ block Z can be represented as an $N^2 \times 1$ vector, say P_Z , with each element representing the corresponding gray value of the block. At the decoder, those successfully received blocks at the decoder are used to reconstruct the lost or damaged blocks by exploiting linear interpolation:

$$\hat{P}_Z = \tilde{P}_Z + w_T \bar{P}_T + w_B \bar{P}_B + w_L \bar{P}_L + w_R \bar{P}_R \quad (1)$$

where \tilde{P}_Z is the vector of correctly received values of the block to be reconstructed, with zeros in the positions of those lost pixels. \bar{P}_X ($X=T, B, L, \text{ or } R$) denotes the vector containing the complemented set of gray values from adjacent block X . By minimizing the squared difference between pixels across block boundaries, referred to as the total squared edge error ε^2 , the optimal weights can be calculated, and the lost block can be reconstructed in a way to satisfy the smooth connection with its four neighbors. In our scheme, after the DC coefficient of one lost block is extracted, it can be exploited to reconstruct the lost data in two ways. The first is that the lost block is simply reconstructed by just executing the reverse DCT with the extracted DC and all other AC coefficients zero-valued. Second, the reconstructed block by the first way is referred to as the term \tilde{P}_Z in Eq.(1), and then the reconstruction is implemented with the above discussed algorithm that makes use of linear interpolation. Compared with the case that \tilde{P}_Z has to be set to zero if no hidden data can be exploited, the reconstruction performance should be improved definitely. The experimental results of above two methods are listed in the 2nd and 3rd columns of Table 1. The peak signal-to-noise ratio (PSNR) is exploited to evaluate the objective visual quality of a processed image compared with the original image, which is calculated as follows:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (2)$$

where MSE denotes the mean squared error.

For further comparison, another two groups of experiments are conducted. The third experiment adopts data hiding but does not make use of the extracted DC coefficients at the decoder for the error concealment by linear interpolation, while the fourth never considers the data hiding procedure. Therefore, the \tilde{P}_Z s in Eq.(1) for these two groups of experiments are both zero-valued. The experimental results are also listed in Table 1, as shown in the 4th column and the 5th column respectively. Since the visual quality of the host image should be affected by data hiding, the performance in the 5th column is definitely better than that in the 4th column. However, with JPEG lossy compression executed, the performance degradation caused by data hiding is not so obvious and can even be ignored, as is presented in Table 1. It can also be observed from Table 1 that by adopting data hiding (as shown in the 3rd column), the performance of image reconstruction could gain 0.3dB or so exceeding that in the 5th column in which the data hiding are never executed. Even by just restoring the lost block with IDCT based on the DC values (as shown in the 2nd column), the performance of reconstruction is also good enough. Furthermore, compared with linear interpolation, reconstruction by simple IDCT has much less calculation complexity.

Table 1. Comparison of visual quality of reconstructed images obtained by different procedures (PSNR in dB, $\alpha = 3.6$, with 10% blocks randomly lost)

JPEG Compression Quality	Data Hiding for Error Concealment			Error concealment with no data hiding
	Reconstruction by conducting the IDCT	Reconstruction with DC regarded as \tilde{P}_Z	Reconstruction without exploiting the DC	
90%	32.52	33.28	32.94	32.97
85%	32.36	33.09	32.76	32.78
80%	32.23	32.91	32.62	32.64
75%	32.11	32.79	32.50	32.51

Reference

- [1] J. J. Chae, and B.S. Manjunath, "A Technique for Image Data Hiding and Reconstruction without Host Image", SPIE EI'99, Security and Watermarking of Multimedia Contents, Vol. 3657, pp. 386~396, San Jose, California, Jan., 1999.
- [2] Debargha Mukherjee, Jong Jin Chae, Sanjit K. Mitra, and B.S.Manjunath, "A Source and Channel Coding Framework for Vector Based Data Hiding in Video", submitted to IEEE Trans. on C&S for Video Tech.
- [3] M. D. Swanson, B. Zhu, A. H. Tewfik, "Data Hiding for Video-in-Video", Proceedings of International Conference on Image Processing, Vol. 2, pp. 676~679, 1997.
- [4] I. J. Cox, J. Killian, T. Leighton, and T. Shamoan, "Secure Spread Spectrum watermarking for Multimedia", IEEE Trans. on Image Processing, Vol. 6, No. 12, pp. 1673~1687, Dec. 1997.
- [5] Deepa Kundur, Dimitrios Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication", Proceedings of the IEEE, vol. 87, No. 7, Jul. 1999, pp. 1167~1180.
- [6] Mitchell D. Swanson, Mei Kobayashi, and A. H. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies", Proceedings of IEEE, Vol. 86, No. 6, Jun. 1998, pp. 1064~1087.
- [7] Houg-Jyh Wang, Po-Chyi Su, and C. -C. Jay Kuo, "Wavelet Based Blind Watermark Retrieval Technique", SPIE Phonics East-Symposium on Voice, Video, and Data Communications, Boston, MA, November 2-5, 1998.
- [8] Po-Chyi Su, Houg-Jyh Mike Wang, and C. -C. Jay Kuo, "Blind Digital Watermarking for Cartoon and Map Images", SPIE Phonics West-Electrical Imaging (EI 99), San Jose, CA, January 25-29, 1999.
- [9] Min Wu, and Bede Liu, "Watermarking for Image Authentication", <http://www.ee.princeton.edu/~minwu/>.
- [10] Mi Wu, Hong Heather Yu, and Alex Gelman, "Multi-level Data Hiding for Digital Image and Video", SPIE Photonics East'99, Boston, 1999.
- [11] Chiou-Ting Hsu, and Ja-Ling Wu, "Hidden Digital Watermarks in Images", IEEE Tran. On Image Processing, Vol. 8, No. 1, January, 1999.
- [12] Paul Salama, Ness Shroff, and Edward J. Delp, "Error Concealment in Embedded Zerotree Wavelet Codecs", Proceedings of the International Workshop on Very Low Bit Rate Video Coding, Urbana, Illinois, pp. 200~203, October 8-9, 1998.
- [13] J. J. Chae, and B. S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients", Proceedings of SPIE EI'98, Storage and Retrieval for Image and Video Database VI, Vol. 3312, pp. 308~317, San Jose, 1998.
- [14] Sheila S. Hemami, and Teresa H.-Y Meng, "Transform Coded Image Reconstruction Exploiting Interblock Correlation", IEEE Trans. on Image Processing, Vol. 4, No. 7, Jul. 1995, pp. 1023~1027.
- [15] Paul Salama, Ness B. Shroff, and Edward J. Delp, "Error Concealment in Encoded Video Streams", submitted to IEEE Journal on Selected Areas in Communications.
- [16] J. H. Conway, N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*, Springer-Verlag, 1988.
- [17] Soon Hie Tan, Khee K. Pang, and King N. Ngan, "Classified Perceptual Coding with Adaptive Quantization", IEEE Trans. on Circuits & Systems for Video Tech., Vol. 6, No. 4, Aug. 1996, pp. 375~388.