An Adaptive Codewords Grouping Based Steganography for Index Images

Yung Kuei Chiang and Piyu Tsai

Department of Computer Science and Information Engineering, National United University, Taiwan

No. 1, Lien Da, Kung-Ching Li, Miao-Li 36003, Taiwan

{ykchiang, pytsai}@nuu.edu.tw

Abstract

The practice of hiding secret messages into index-based images generally suffers from problems of image quality degradation and hiding capacity restriction. A steganographic scheme for index-based images using adaptive codeword groupings is proposed in this paper. The proposed scheme grouped the codewords in the codebook into sub-clusters, in terms of their relationship between the codewords for reducing the image distortion. Any size of the sub-cluster was allowed, so as to obtain the hiding capacity substantially, unlike other approaches in which the size of a sub-cluster was restricted to the power of 2.

The proposed scheme was applicable as proven by experimental results. The higher hiding capacity was obviously extended; furthermore, the degradation of the stego-image was less and nearly disregarded. The average performance of the proposed scheme was much better as compared to other methods.

Keywords: index-based image, information hiding, steganography

1. Introduction

Steganography hides secret messages in an ordinary cover material to evade suspicion, as applied in ancient times. The thought of steganography is similar to that of camouflage, as used by many animals to safeguard themselves from being attacked. With the digitalization of data and networking of communication, communication security over the Internet is becoming more and more crucial [1]. The Internet is basically an open channel in which security problems such as modification, interception, as well as others usually occur. Several different approaches have been proposed to make communication secure [2]. The goal of steganography here is to conceal secret messages well enough so that they cannot be heeded by an unauthorized user. Several steganographic schemes have already been presented to cope with the privacy problems [3-11].

The steganography schemes can be generally divided into three categories. In the first category, the schemes concealed a secret message in the spatial domain of the cover image [3-6]. Lee and Chen's scheme [3] modified the least significant bit (LSB) of each pixel in the cover image to inset the secret message. Wang *et* al.'s scheme [4] applied the optimal substitution of LSB. Chung *et al.*'s scheme [5] proposed a singular value decomposition (SVD)-based hiding scheme. Tsai *et al.*'s scheme [6] used the bit plane of each block truncation coding (BTC) block to inlay a secret message.

In the second category, embedding a secret message into a transformed cover image was generally used [7-9]. Some transformation functions such as the discrete cosine transformation (DCT) and the discrete wavelet transformation (DWT) were broadly employed. Chang *et al.*'s approach [7] applied the middle frequency coefficients of the DCT transformed cover image to inset the secret message and modified the quantization table of JPEG to protect the embedded secret message. Kobayashi *et al.*'s approach [8] hid a secret message in the JPEG encoded bit streams. Spaulding *et al.*'s approach [9] applied the embedded zerotree wavelet (EZW) encoded cover image to inset the secret message. The bit-plane complexity segmentation (BPCS) and the visual system were explored to determine the hiding capacity and the stego-image quality.

In the third category, concealing a secret message into the index-based images such as vector quantization (VQ)-based images and color quantization (CQ)-based images was broadly used [10-11]. Jo and Kim's method [10] partitioned the codewords in the codebook into three sub-clusters according to the similarity between the codewords themselves. The higher similarity of members between two special sub-clusters was preserved in order to conceal the watermark information. Fridrich's method [11] searched the closest color parity matching the embedding bit so as to inset the secret message.

The problems of the image quality degradation and the hiding capacity constraint are always unavoidable in the index-based approaches. Besides, there is a tradeoff between capacity and quality; that is, the capacity of hiding secret messages is usually sacrificed in order to keep acceptable stego-image quality, and vice versa. To improve the problems stated above, we shall present a steganographic scheme for index-based images using adaptive codewords grouping in which the hiding capacity increases and acceptable stego-image quality is constant. To accomplish our goal, we divide the codewords in the codebook into different member sub-clusters according to the relationship between the codewords themselves. In particular, the member of a sub-cluster is not restricted to the power of 2. Any size of sub-clusters is permitted. The rest of this paper is organized as follows. In Section 2 the related works are briefly described. The proposed steganographic scheme is introduced in Section 3. Section 4 presents the experimental results of the proposed scheme. In Section 5 the conclusions are stated.

2. An Overview of Related Works

In index-based image hiding, the least significant bit (LSB) modification sought the closest codeword in which the LSB of the corresponding index and the embedding message were the same. Jo and Kim's watermarking declustered all codewords into groups for hiding the watermark information. Fridrich's scheme examined the color parity of the closest color to conceal the secret message.

2.1 The Least Significant Bit (LSB) Modification

The least significant bit (LSB) modification approach modified the LSB of the closest searched index for embedding the secret message into the stego-image. For each block embedding, the closest block from the codebook was first searched and then inspected. If the LSB of the index matched the bit value of the embedding secret message, the index was then unchanged. Otherwise, another new index whose LSB matched the embedding bit value would be searched. As a result, the new index was used to encode the embedding block and the secret message was inset as well. The least distortion of the image was consequently caused.

Each index could only hide one bit of secret message in this approach. The quality of the stego-image was downgraded by the number of the original indices which were modified. This method could also be applied to the palette-based images in which each color index inset one bit of secret message with the least distortion substitution strategy.

2.2 Jo and Kim's Watermarking

Jo and Kim's scheme [10] declustered the codewords in the codebook into three groups (G_{-1}, G_0, and G_1) in accordance with the similarity between the codewords themselves. The group G_{-1} consisted of codewords which were inappropriate for embedding the watermark information. The other two groups contained codewords of which each codeword in one group corresponded to a similar one in the other group; that is, a codeword in group G_0 had a corresponding one similar to it in group G_1. Both groups G_0 and G_1 were able to be considered to represent the bit values 0 and 1 respectively in the watermarking embedding.

For each block embedding, the closest codeword was first searched and then the group to which the codeword belonged was determined. If the searched codeword belonged to the group G_{-1}, this codeword remained unchanged and no watermark information was inset. If the group representation matched the watermark information, the searched codeword was also preserved. Otherwise, another similar codeword in the other corresponding group was instead applied. For example, if the embedding watermark was 0 and the group the closest searched codeword belonged to was G_1, the other codeword with higher similarity in the group G_0 would be chosen. As a result, the closest searched codeword was modified to carry the watermark in terms of the group representation.

However, the hiding capacity in this scheme was tiny because each codeword could only hold, at most, one bit of the watermark information.

2.3 Fridrich's Color Parity Technique

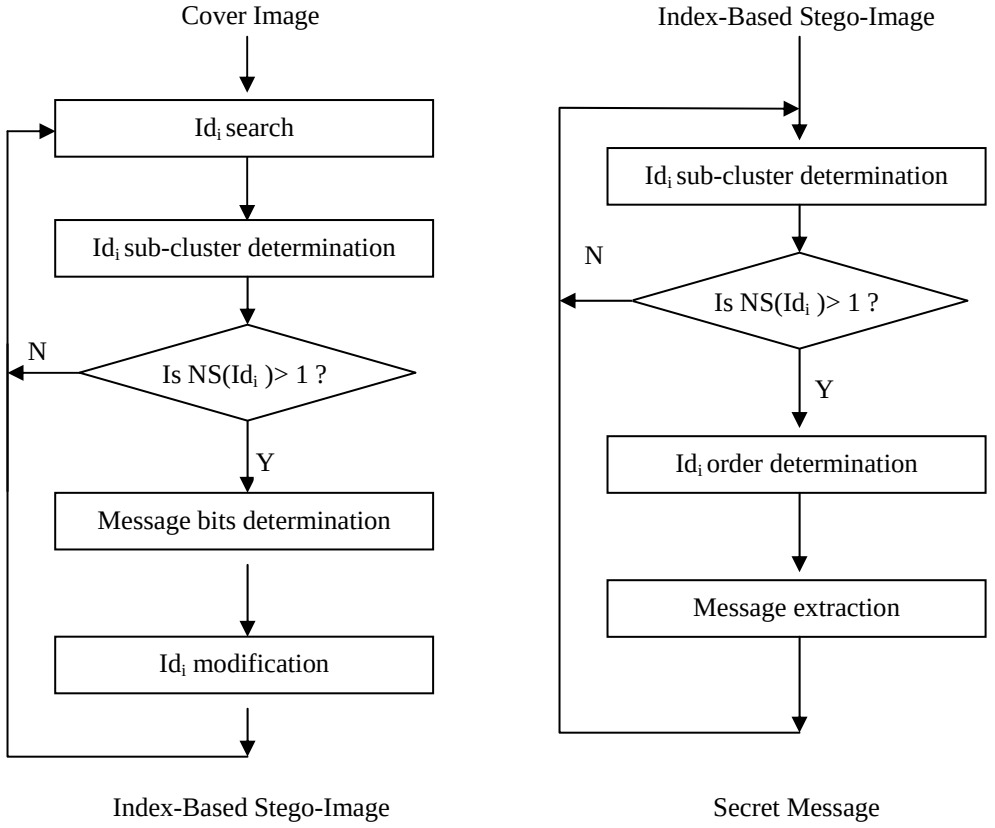
Fridrich's approach [11] searched for the closest color of each pixel so that the parity of searched color matched the desired embedding bit. The parity of each color was the remainder of dividing by 2 the sum of R, G, and B values in palette. If the desired embedding bit matched the color parity of the embedding pixel, the color of the embedding pixel remained unchanged. Otherwise, the next closest color was again searched until the color parity was matched. Once the parity of the new color matching the desired embedding bit was found out, the original index was replaced by this new index, and the secret message was inset.

Because Fridrich's embedding method was based on the color parity of each pixel, and the color parity was gained roughly by (R+G+B) mod 2, the PSNR of the cover image was down conspicuously when the number of the embedding secret bits was up.

3. The Proposed Scheme

The proposed steganography based on the codewords grouping in which any size of sub-clusters is allowed will be introduced in this section. The

codewords grouping will first be described. The embedding and extracting procedures will then be stated. An overview of the proposed scheme is shown in Figure 1. The considerations of hiding capacity and image quality will also be discussed.



(a) The embedding procedure (b) The extracting procedure

Figure 1 An overview of the proposed scheme

3.1 The Codewords Grouping

A codebook contains a set of codewords, which is generally applied in the index-based image encoding/decoding. The codewords grouping partitions the codewords into distinct member sub-clusters in order to hide secret messages. The number of sub-cluster members intrinsically determines the hiding capacity. In the encoding procedure, an image is first divided equally into blocks with n×n pixels. For each block encoding, the closest one among the codewords in the codebook is sought in terms of a similarity measure (e.g. squared Euclidean distance, MSE) to represent the block. The index of the closest searched codeword in the codebook is instead used to substitute for the original block in the encoded image for reducing the storage space.

Each codeword in the codebook actually stands for a set of training vectors, which is generated by a specific algorithm. Any modification of the closest searched index may thus cause a large amount of image distortion. The relationship between codewords is therefore utilized to alleviate the image distortion caused by index modification. The squared Euclidean distance between codewords is applied to indicate the relationship. A smaller distance illustrates a stronger relationship. A larger distance on the contrary indicates a weaker relationship.

The proposed codewords grouping approach splits the codewords into various member sub-clusters according to the relationship between codewords. A set of predefined distance thresholds is used to determine members of a sub-cluster. The codewords with stronger relationships are grouped into a sub-cluster in which the

distance of members is less than the predefined threshold. In an extreme case, a codeword may be solely grouped into a sub-cluster if the relationship between the codeword itself and others is greater than all thresholds; namely, this sub-cluster contains only a member of the codeword itself.

The hiding capacity is determined by the number of sub-cluster members in this proposed approach; that is, the more sub-cluster members there are, the higher the hiding capacity will be. Therefore, the sub-clusters with more members will be first grouped to increase the hiding capacity. The sub-clusters with fewer members will then be grouped. Finally, the residual codewords with weaker relationship between others will be individually grouped into a sub-cluster with only a single member.

For a concrete example, consider a codebook with 256 codewords is grouped into 4-member, 3-member, 2-member, and 1-member sub-clusters according to predefined thresholds. For each codeword, the squared Euclidean distances between the codeword itself and other codewords are computed and sorted. The sorted distances indicate the relationship between the codeword itself and the other codewords. After the distances for each codeword are calculated and sorted, the sub-cluster grouping can be performed. Initially, the sub-clusters with 4 members are grouped. For each codeword, the distances of its three higher relationship codewords are summed together. Among the summed distances, the least summed distance is compared to the predefined threshold TH4 each time. If it is less than TH4, these codewords with the least summed distance are grouped together as a 4-member sub-cluster. Otherwise, the 4-member sub-cluster grouping terminates.

Actually, it is possible for a codeword keeping a higher relationship with many codewords. Therefore, a measure ought to be taken to prevent a codeword from appearing in two or more sub-clusters; that is, once any of the codewords with the next least summed distance have already been grouped into another sub-cluster, the summed distances for each remaining codewords will be calculated repeatedly. Eventually, the most similar codewords are capable of being grouped into the same sub-cluster together.

After 4-member sub-clusters are completely grouped, the sub-clusters with 3 members for the remaining codewords are next grouped. The 3-member sub-cluster grouping is similar to the way that the 4-member sub-clusters grouping except that the threshold TH3 is used. In the same way, the sub-clusters with 2 members are accordingly grouped. Finally, each remaining codeword is grouped individually into a sub-cluster with a single member of itself. As a result, all codewords in this codebook are declustered into different member sub-clusters.

3.2 The Embedding Procedure

The embedding procedure is to embed the secret message into the cover image. The codewords in the codebook have already been grouped into varied member sub-clusters. In the encoding procedure, each encoding block in the cover image seeks the closest codeword to stand for itself. Once the closest codewords is sought, the sub-cluster to which the codeword belongs is identified. The number of members in this sub-cluster $NS(Id_i)$ is also determined, where Id_i is the index of the closest codeword searched to represent the encoding block. If the number of sub-cluster members is greater than one; namely $NS(Id_i) > 1$, the embedding procedure is then performed as well. Otherwise, the encoding block is not suitable for hiding any secret message.

Actually, the number of sub-cluster members implies the size of the secret message can be inset. A 4-member sub-cluster indicates that a 2-bit secret message can be hidden. Thus, a 2-member sub-cluster indicates that only one bit can be used. However, a single 3-member sub-cluster is not used to hide any message. Instead, the combination of two 3-member sub-clusters together is used. According to the product rule, there will be nine applications; that is, at least 3 bits hiding capacity can be applied to hide secret messages with the combination of two 3-member sub-clusters.

In the embedding procedure, the index of the closest searched codeword may be modified. The modification for both 4-member and 2-member sub-clusters is quite simple, it is determined by the secret message to be embedded and the order of the searched index in the sub-cluster which the searched index itself belongs to. The index whose order in the sub-cluster matches the embedded secret message is consequently adopted to substitute for the closest searched index. In other words, the new index is used to encode the encoding block. As a result, the encoding block is modified to embed the secret message.

As an example, consider the 4-member sub-cluster shown in Table 1 demonstrating the proposed embedding strategy. In Table 1, the sub-cluster is comprised of four members, which are ordered as 0, 1, 2, and 3, respectively. The indices of these four members in the codebook are 103, 134, 112, and 98, respectively. In the block encoding, suppose the index of the closest searched codeword is 103, and the number of the identified sub-cluster members is 4. A sub-cluster with four members shows that it is capable of hiding a 2-bit secret message. Assume that the 2-bit secret message to be embedded is valued at 3 (11 in binary) ;thus, an index value of 98, as ordered 3 in the sub-cluster, is applied to encode this block. The index 98 is used to replace the closest searched index 103.

Table 1 The index and the order of a 4-member sub-cluster

Sub-cluster order	0	1	2	3
Codeword index	103	134	112	98

A variant of the index modification is used for sub-clusters with three members. In the block encoding, when a 3-member sub-cluster to which the closest searched index belongs is first recognized, the index modification will be postponed until the next one with three members comes out. As soon as two sub-clusters with three members are accumulated, the index modification is performed immediately. As stated above, the join of two 3-member sub-clusters together indicates that it is able to hide a 3-bit secret message.

An example shown in Tables 2 and 3 illustrates the embedding strategy for combining two 3-member sub-clusters. In Table 2, each sub-cluster with three members is ordered from 0 to 2 in the same way. The indices of three members in the sub-cluster *A* are 80, 70 and 95, respectively. On the other hand, the indices of these three in the sub-cluster *B* are 140, 120 and 135, respectively. The mappings of the combinations from two 3-member sub-clusters onto the 3-bit values are listed in Table 3. In the block encoding, suppose the index of the closest searched codeword in sub-cluster *A* is 80, and the index of the closest searched codeword in sub-cluster *B* is 120. Assume that the 3-bit secret message to be embedded is valued at 5 (101 in binary). According to the mappings shown in Table 3, the value 101 in binary is mapped from member order 1 in the sub-cluster *A* together with member order 2 in the sub-cluster *B*. The index of member order 1 in sub-cluster *A* is 70, and the index of member order 2 in sub-cluster *B* is 135, respectively. As a result, the index 70 is used to replace the closest searched index 80 in the first encoding block; on the other hand, the index 135 is thus used to replace the index 120 in the second encoding block.

Table 2 The index and the order of two 3-member sub-clusters

Sub-cluster order	0	1	2
Codeword index in sub-cluster *A*	80	70	95
Codeword index in sub-cluster *B*	140	120	135

Table 3 The mappings of the combinations from two 3-member sub-clusters to the 3-bit values

Order in sub-cluster *A*	Order in sub-cluster *B*	Value in binary
0	0	000 (0)
0	1	001 (1)
0	2	010 (2)
1	0	011 (3)
1	1	100 (4)
1	2	101 (5)
2	0	110 (6)
2	1	111 (7)
2	2	Unused

3.3 The Extracting Procedure

The hidden secret messages from a stego-image are extracted in the extracting procedure. The codewords are also grouped into different member sub-clusters. As the block decoding is performed, the extraction of hidden secret messages can be incorporated.

In the decoding procedure, the indices of the stego-image are decoded to rebuild the original cover image. Meanwhile, the sub-cluster to which each decoding index belongs is also identified. If the members of the identified sub-cluster are less than two, no secret message is embedded. Otherwise, a portion of the secret message is hidden in the current decoding index. The order of the decoding index in both of the 4-member and 2-member sub-clusters is exactly the embedded message. For instance, the current decoding index in the 4-member sub-cluster is 98, whose relative members in the sub-cluster are shown in Table 1. The number of the sub-cluster members and the order of the decoding index are 4 and 3, respectively. As a result, a 2-bit secret message valued at 3 (11 in binary) is extracted.

However, some effort is needed to extract the secret message embedded in an index which belongs to a 3-member sub-cluster. When the first 3-member sub-cluster to which the closest searched index belongs is identified, the secret message extracting will be postponed until the next one with three members comes upon. As soon as two sub-clusters with three members are accumulated, the secret message extracting is performed immediately. For example, suppose the decoding indices in the first and the second 3-member sub-cluster are 70 and 135, respectively, whose relative members in both sub-clusters are shown in Table 2. The orders of both decoding indices are 1 and 2, respectively. The mapping from member order 1 in sub-cluster *A* together with member order 2 in sub-cluster *B* onto the value in binary is 101, as shown in Table 3. As a result, a 3-bit secret message valued at

5 (101 in binary) is extracted.

3.4 Quality and Capacity Considerations

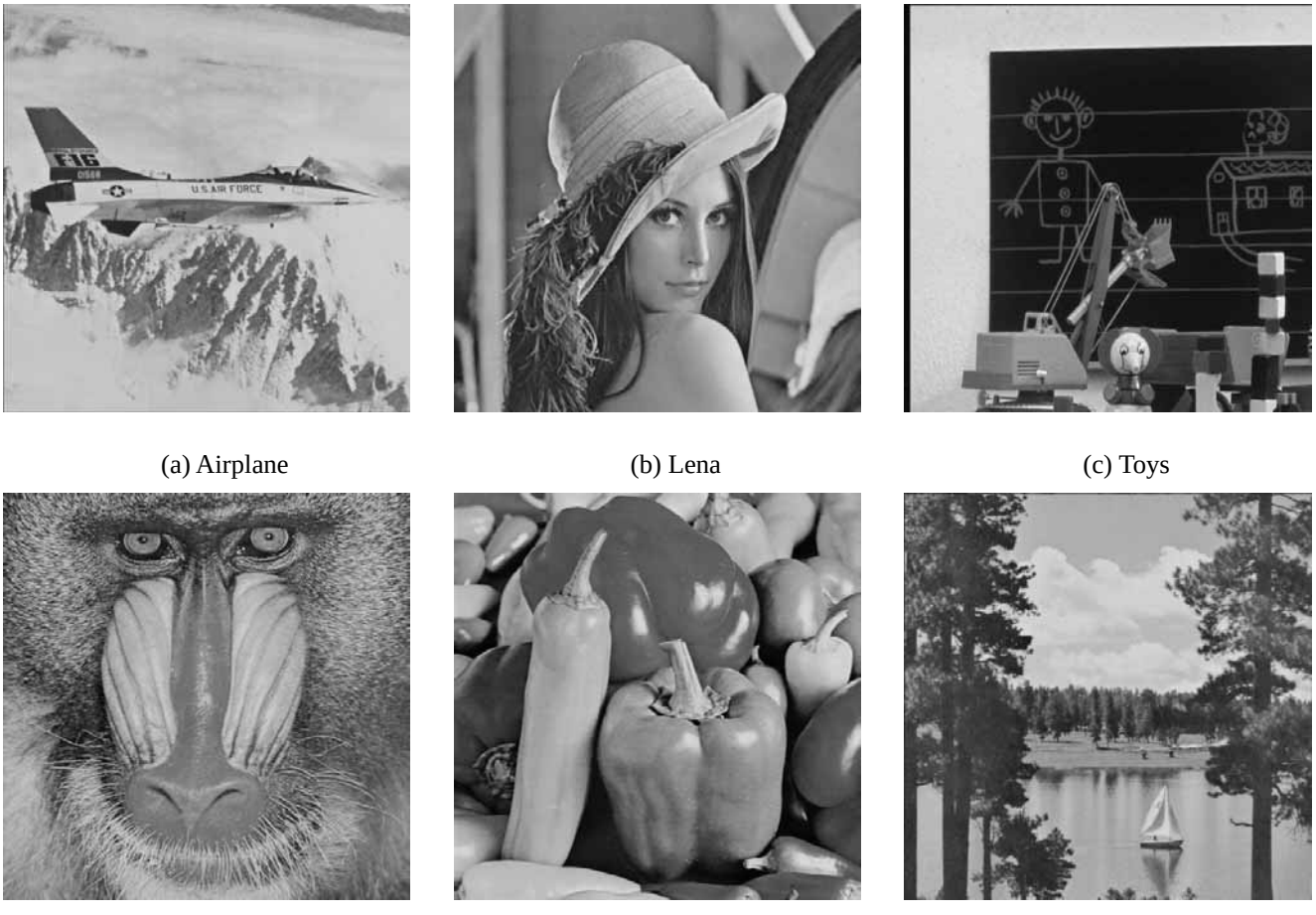
There is a tradeoff between the hiding capacity of a cover image and the image quality of a stego-image in the image-hiding schemes. In order to enlarge the hiding capacity of the cover image and preserve the high quality of the stego-image, we present a scheme using adaptive codewords grouping according to the relationship between the codewords.

In the codewords grouping, the relationship between the codewords is mainly applied to reduce the image distortion. Besides, a set of distance thresholds is used for deciding the members of a sub-cluster. In general, the larger the threshold is, the more sub-clusters with large size there will be. On the contrary, the smaller the threshold is, the more sub-clusters with small size there will be. A large sub-cluster size generally offers a high hiding capacity. Therefore, the more sub-clusters with large size there are, the more hiding capacity there will be.

The larger threshold can however lead the stego-image towards degradation. A set of thresholds properly predefined is thus becoming critical. As long as a set of thresholds is appropriately selected, a part of secret messages can be embedded and the quality of the stego-image would be accepted. The tradeoff as described above can be solved approximately by the proposed grouping scheme.

4. Experimental Results

To evaluate the performance of the proposed steganography, a vector quantization (VQ) encoder was simulated. Six gray-level images with 512×512 pixels taken as cover images shown in Figure 2, “Airplane,” “Lena,” “Toys,” “Baboon,” “Peppers,” and “Sailboat” were simulated by the VQ encoder. The codebook with 256 16-dimension codewords used in this simulation was generated by LBG algorithm [12] in which five training images “Airplane,” “Barbara,” “Boat,” “Lena,” and “Toys” were employed. Three binary images “NUU,” “IEEE,” and “CCU” of 128×128 bits were used as secret messages and shown in Figure 3.



(a) Airplane (b) Lena (c) Toys

(d) Baboon (e) Peppers (f) Sailboat

Figure 2 The cover images of 512×512 pixels

(a) NUU (b) IEEE (c) CCU

Figure 3 The secret messages of 128×128 bits

The relationship between codewords in the codebook is first explored. The codewords were partitioned into different member sub-clusters with different thresholds. The grouped results shown in the first and the second column in Table 4 correspond to grouping thresholds of 4-member, 3-member and 2-member with Euclidean distances of 2000, 1500, 1000 and 3000, 2000, 1500, respectively. The residual codewords are grouped into single member sub-clusters individually. In Table 4, the number of 4-member sub-clusters in the second column is more than that of 4-member sub-clusters in the first column. Also, the sum of grouped sub-clusters in the second column is larger than that of grouped sub-clusters in the first column. In general, the larger number of groups implies the higher capacity to hide a secret message.

To evaluate the capacity of cover images, both the relationship of codewords and the characteristics of images are explored. The hiding capacities of each cover image were shown in Tables 5 and 6 according to the grouping results shown in the first and the second column of Table 4, respectively. The capacity is computed in terms of the number of blocks, which belongs to 4-member, 3-member, or 2-member sub-clusters. By comparing the capacities in Tables 5 and 6, it is clearly seen that the capacities in Table 6 are larger than those in Table 5. This is because the larger grouping thresholds were used in Table 6. In Tables 5 and 6, the hiding capacities provided by the same grouping threshold are different for each cover image. This is because the characteristics of the cover images are different though the sizes are the same. From Tables 5 and 6, it can be seen that the adaptive hiding capacity can be achieved by using different grouping thresholds.

Both capacity and quality of the stego-image are concerned to evaluate the performance of the steganographic scheme. The quality of the stego-image by the proposed steganography is measured by the peak signal-noise ratio (PSNR). The experimental results are shown in Figure 4 and Table 7 in which the first column grouping result shown in Table 4 is used. From Table 7, it is noted that the average stego-image quality measured by PSNR is near the VQ encoded image quality. In other words, the distortion is less while the secret message is hidden. From Figure 4, it is difficult to distinguish the difference between the original images and stego-images by the human eye. Therefore, the proposed steganography provides good stego-image quality. The secret images from stego-images “Airplane,” “Lena,” “Peppers,” and “Sailboat” are completely extracted and shown in Figure 3. On the other hand, the extracted secret images from stego-images “Toys,” and “Baboon,” are uncompleted because of the limitation of the hiding capacity.

The quality and hiding capacity among LSB, Jo and Kim’s, Fridrich’s and the proposed methods are compared. The secret images “NUU” of 128×128 bits are embedded in the test images. The compared results are shown in Table 8. From Table 8, it is seen that the average stego-image quality and hiding capacity of the proposed method are better than those of LSB and Fridrich’s methods. In comparison with Jo and Kim’s method, higher capacity is obviously obtained and less distortion is caused by the proposed method. Also, it is noted that the images “Toys” and “Baboon” do not provide enough capacity to hide the secret image in Jo and Kim and proposed methods. This is because of the consideration of the quality. If the higher capacity is required, the adaptive grouping threshold is adopted in the proposed method, but it is not in Jo and Kim’s method. From Table 8, it is shown that the proposed method not only provides adaptive hiding capacity but also keeps good image quality.

Table 4 The number of different member sub-clusters with different thresholds

Thresholds	Sub-clusters			Sub-clusters		
	4-member TH=2000	3-member TH=1500	2-member TH=1000	4-member TH=3000	3-member TH=2000	2-member TH=1500
Numbers	16	5	25	40	3	25

Table 5 The number of different member sub-cluster codewords and total capacity using the results of the first column in Table 4

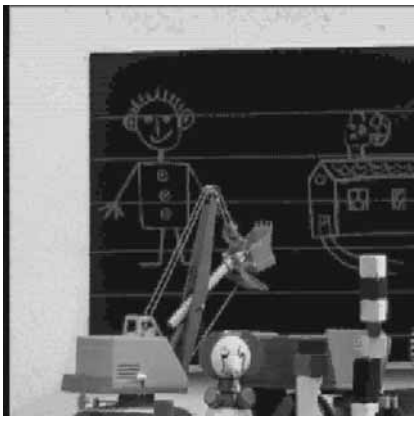
Numbers / Images	Sub-clusters			Total Capacity
	4-member	3-member	2-member	
Airplane	8955	744	3304	22330
Lena	7423	2633	2947	21741
Toys	4620	611	1863	12018
Baboon	3398	1718	2856	12229
Peppers	6878	7999	2519	20772
Sailboat	3825	4169	2964	16866

Table 6 The number of different member sub-cluster blocks and total capacity using the results of the second column in Table 4

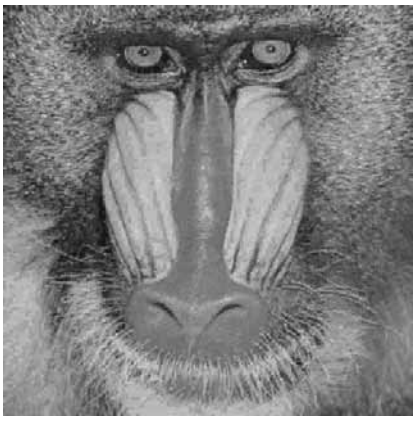
Numbers / Images	Sub-clusters			Total Capacity
	4-membeer	3-member	2-member	
Airplane	9784	255	3425	23374
Lena	9763	849	3232	24030
Toys	5331	161	2007	12909
Baboon	5404	518	3351	14936
Peppers	9438	453	2679	23055
Sailboat	9008	453	3073	21767

(a) Airplane+NUU

(b) Lena+IEEE



(c) Toys+CCU



(d) Baboon+NUU

(e) Peppers+IEEE

(f) Sailboat+CCU

Figure 4 The stego-images

Table 7 The quality of stego-images by VQ encoder and the proposed method

PSNR / Images	VQ	Proposed		
		NUU	IEEE	CCU
Airplane	29.7869	29.0525	28.9981	29.0208
Lena	30.9054	30.0574	29.9817	29.9946
Toys	28.8157	28.1791	28.0585	28.0536
Baboon	23.8179	23.5912	23.5692	23.5679
Peppers	30.1613	29.2802	29.1976	29.2001
Sailboat	27.9992	27.1923	27.1140	27.1122
Average	28.5811	27.8921	27.8199	27.8249

Table 8 The image quality and hiding capacity of gray-level stego-image by LSB, Jo and Kim's, Fridrich's and the proposed method

Methods / Covers	LSB		Jo and Kim		Fridrich		Proposed	
	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity
Airplane	28.5719	16384	29.3741	11136	28.4774	16384	29.0525	22330
Lena	29.6533	16384	30.3243	12622	29.5414	16384	30.0574	21741
Toys	27.2966	16384	28.5343	7023	24.4115	16384	28.1791	12018
Baboon	23.3151	16384	23.6790	7919	23.2871	16384	23.5912	12229
Peppers	28.8572	16384	29.5855	12263	27.4891	16384	29.2802	20772
Sailboat	27.0710	16384	27.6318	10493	27.0206	16384	27.1923	16866
Average	27.4609	16384	28.1892	10243	26.7046	16384	27.8921	17659

5. Conclusions

The proposed scheme partitioned the codewords into sub-clusters in accordance with the relationship. With the strong relationship between the codewords in a sub-cluster, the index modification of the closest searched block for insetting a secret message wouldn't lead to image distortion. Any size of sub-clusters was permitted so as to evidently increase the hiding capacity, unlike other methods in which the size of a sub-cluster was limited to the power of 2. The goal of adaptive steganography was achieved as shown by experimental results. The higher hiding capacity was substantially enlarged; moreover, the degradation of the stego-image was less and nearly disregarded.

The average performance of the proposed scheme was much better as compared to other methods. In comparison with Jo and Kim's method, the proposed scheme provided more than twice the hiding capacity and preserved approximate image quality. The average stego-image quality and hiding capacity of the proposed approach were better than those of LSB and Fridrich's methods.

An acceptable result between the image quality of the stego-image and the hiding capacity of the cover image was also capable of achieving by merely fixing the distance thresholds.

6. References

[1] Q. Cheng and T. S. Huang, "An Adaptive Approach to Transform-Domain Information Hiding and Optimum Detection Structure," *IEEE Transactions on Multimedia*, 3(3), 273-284(2001).

[2] D. Artz, "Digital Steganography: Hiding Data within Data," *IEEE Internet Computing*, 5(3), 75-80(2001).

[3] Y. K. Lee and L. H. Chen, "High Capacity Image Steganographic Model," *Proceedings of IEE* International *Conference on Vision, Image and Signal Processing*, 147(3), 288-294(2000).

[4] R. Z. Wang, C. F. Lin and J. C. Lin, "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," *Pattern Recognition*, 34(3), 671-683(2001).

[5] K. L. Chung, C. H. Shen and L. C. Chang, "A Novel SVD- and VQ-based Image Hiding Scheme," Pattern Recognition *Letters*, 22(9), 1051-1058(2001).

[6] P. Tsai, Y. C. Hu and C. C. Chang, "An Image Hiding Technique Using Block Truncation Coding," Proceedings *of Pacific Rim Workshop on Digital Steganography*, Kitakyushu, Japan, July, 54-64(2002).

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

[8] H. Kobayashi, Y. Noguchi and H. Kiya, "A Method of Embedding Binary Data into JPEG Bitstreams," *IEICE* Transactions, J83-D2(6), 1469-1476(2000).

[9] J. Spaulding, H. Noda, M. N. Shirazi and E. Kawaguchi, "BPCS Steganography Using EZW Lossy Compressed Images," *Pattern Recognition Letters*, 23(13), 1579-1587(2002).

[10] M. Jo and H. D. Kim, "A Digital Image Watermarking Scheme Based on Vector Quantization," *IEICE Transactions on Information and Systems*, E85-D(6), 1054-1056(2002).

[11] J. Fridrich, "A New Steganographic Method for Palette-Based Images," *Proceedings of the IS&T PICS Conference*, Savannah, Georgia, April, 285-289(1998).

[12] Y. Linde, A. Buzo and R. M. Gray, "An Algorithm for Vector Quantizer Design," *IEEE Transactions on Communications*, 28, 84-95(1980).