An Improved Reversible Data Hiding Scheme Using Extra Space Modulation for Color Palette Image

Munkhbaatar Doyoddorj, Chul Sur, Youngho Park and Kyung-Hyune Rhee

Department of IT Convergence and Application Engineering,
Pukyong National University, Republic of Korea
E-mail: {d_mbtr, kahlil, pyhoya, khrhee}@pknu.ac.kr

Abstract

In this paper, a reversible data hiding scheme for color palette image is proposed. The technique of data embedding is used to hide the secret data into multimedia such as text contents, audio, video, and images. The reversibility of data hiding is an important requirement in some applications such as distance medical treatment and military industrial applications. In recent years, many researchers have proposed reversible techniques that work on grayscale images, but these methods cannot be applied directly to color images, which have increased in popularity and have more redundant space available for embedding the secret data. Moreover, the size of color image can be reduced by sorting the stored palette based format. Some researchers have proposed data hiding techniques for palette based images. While their methods successfully achieve the purpose of secret data delivery, they do not achieve reversibility. In our scheme, we make use of the differences between a center index and its neighboring indexes in each sub-blocks of indexed table by using a palette color replacement. The proposed scheme can enhance the embedding capacity for color palette images and recover the embedded data from the stego image without causing perceptible distortions to the cover image. Moreover, we can embed up to $28K$ *bytes into a* 512×512 *color image, which provides much more embedding capacity than the existing reversible data hiding schemes. The experimental results confirm the effectiveness of our scheme in term of hiding capacity of embedding data and visual quality of stego image.*

Keywords: *Reversible Data Hiding, Color Palette Image, Difference Value, Embedding Capacity*

1. Introduction

Data hiding is referred to as a process to hide secret data into cover media, which plays an important role in information security. Reversibility means that not only secret data but also cover media can be precisely recovered in the decoding stage. Hence, it is applicable to some kind of scenarios such as military remote sensing imaging, diagnostic medical imaging, precious art protection, and online content distribution systems [1, 2, 5, 8, 9, 10].

On the other hand, if some data are embedded into an image, the pixel values of the marked image might be changed. Then, the changes of pixel values are subject to causing degradation to the image. Unless the altered pixels are completely recovered into their original state after the secret data has been extracted, a potential distortion can naturally be occurred. Therefore, reversible data hiding techniques which can recover the hidden data without degrading the visual quality of original image as far as possible are necessary.

However, reversible data hiding introduces certain technical challenges such as increasing the embedding capacity (payload), maintaining the reversible characteristic, and simultaneously decreasing the distortion of the cover image. Consequently, the main goal of our approach is to realize a large embedding capacity while yet maintaining high visual quality of the stego image.

1.1. Related works

In past years, many researchers developed reversible data hiding methods by using different techniques [11, 12, 13, 14]. However, all of these methods were only applied to grayscale images. If these methods are applied to hiding a large data in color images, then the stego images have large distortions. With advances in digital devices, color image has become common in our lives. In order to reduce the size of a color image, a true color image can be represented as a color palette image. The concept of palette based image is to train the significant colors and to use the color's index to represent the image. In this way, just the indices table and palette information need to be kept, and the size of the image will be significantly reduced.

Available reversible data hiding techniques can be divided into spatial domain, transform domain and compressed domain methods. In the spatial domain based methods [15-19], the secret data is usually embedded by pixel values' modification. In the transform domain methods, some reversibility-guaranteed transforms (*e.g.*, integer discrete cosine transform [20, 21], integer wavelet transform [22]) are exploited and the data embedding is reduced to coefficients modulation. In the compressed domain methods, some popular image compression techniques (*e.g.*, vector quantization [23, 24], block truncation coding [5], MPEG coding [25]) are involved.

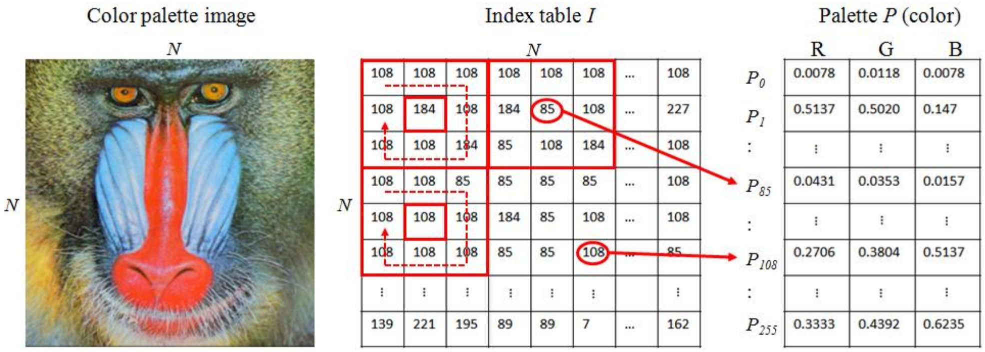
1.2. Our Contributions

In this paper, we propose a reversible data hiding scheme for color palette image, which enhances the embedding capacity without perceptible image distortion. For a color palette image which is composed of a palette and an index table, in our scheme, we divide an index table into a series of non-overlapping blocks consisting of 3×3 indexes. In each block, differences between a center index and its neighboring indexes are calculated, while the center index remains intact. As a reference of the center index, it will be used to restore the neighboring indexes. The extracted difference values of index are applied to two important operations for concealing information, named as extra space extraction and random permutation of indexes in each block. These operations allow the proposed scheme to embed not only large secret data but also provide an unnoticeable way into each block in a single pass period.

The rest of the paper is organized as follows: Section 2 gives an overview of color palette image components. The proposed scheme and its characteristics are described in Section 3. Experimental results and performance comparison are shown in Section 4. Finally, we conclude this paper in Section 5.

2. Color Palette Image Components

Palette based image file formats such as GIF, PNG, TIFF and Microsoft BMP are popular and widely used on the Internet environments. Palette based images have the effect of image compression, which help saving storage space and reducing transmission time [3]. The color palette image is composed of a palette and an index table as shown in Figure 1.



108	108	108	108	108	108	...	108
108	184	108	184	85	108	...	227
108	108	184	85	108	184	...	108
108	108	85	85	85	85	...	108
108	108	108	184	85	108	...	108
108	108	108	85	85	108	...	85
⋮	⋮	⋮	⋮	⋮	⋮		⋮
139	221	195	89	89	7	...	162

	R	G	B
P_0	0.0078	0.0118	0.0078
P_1	0.5137	0.5020	0.147
:	⋮	⋮	⋮
P_{85}	0.0431	0.0353	0.0157
:	⋮	⋮	⋮
P_{108}	0.2706	0.3804	0.5137
:	⋮	⋮	⋮
P_{255}	0.3333	0.4392	0.6235

Figure 1. Color palette image components

Each palette is composed of a list of the selected 256 colors (or 16 colors in a smaller palette) and set of color indices. The actual image color data for each pixel is one index value of the palette. Each pixel's data based on the Red-Green-Blue (RGB) colors which is replaced with an index, that specifies one of the palette colors.

For example, in Figure 1, let image be a color image with size of $N \times N$ pixels, we construct an index table I and a palette P. The index table has same size as large as size of the color palette image, and an every entry corresponds to a pixel. Each pixel displays a value between 0 and 255 which represents a color and corresponds to an index in the palette. The palette is composed of 256 colors. The content of the palette is $P = \{P_0, P_1, \dots, P_{255}\}$. For instance, the index at the entry $I(2,5)$ is 85, which corresponds to the color at P_{85}. Hence, the color of pixel P_{85} displays its RGB as $(0.0431, 0.0353, 0.0157)$.

3. Proposed Reversible Data Hiding Scheme

3.1. Workflow Overview

In the proposed scheme, reversible data hiding and retrieval algorithms are designed by calculating a series of index differences between a center index and its neighboring indexes in each block of the index table, and by utilizing the index differences. In this way, the secret

Table 1. Notations

Notations	Descriptions
I, P	Index table and color palette
n	Number of blocks in an image
p_i^n	i^{th} index value in the n-th block
p_c^n	Center index value in the n-th block
d_i^n	Difference between the i^{th} index and center index values
$d_i^{n^*}$	Modified value of the index difference
pc_i^n	Recovered value of the i^{th} index in the n-th block
s_j	j^{th} bit of secret data
k_j^i	j^{th} bit of i^{th} secret key
k_p	Random permutation key
b_j^i	j^{th} bit of i^{th} index value
τ	Pre-defined threshold value

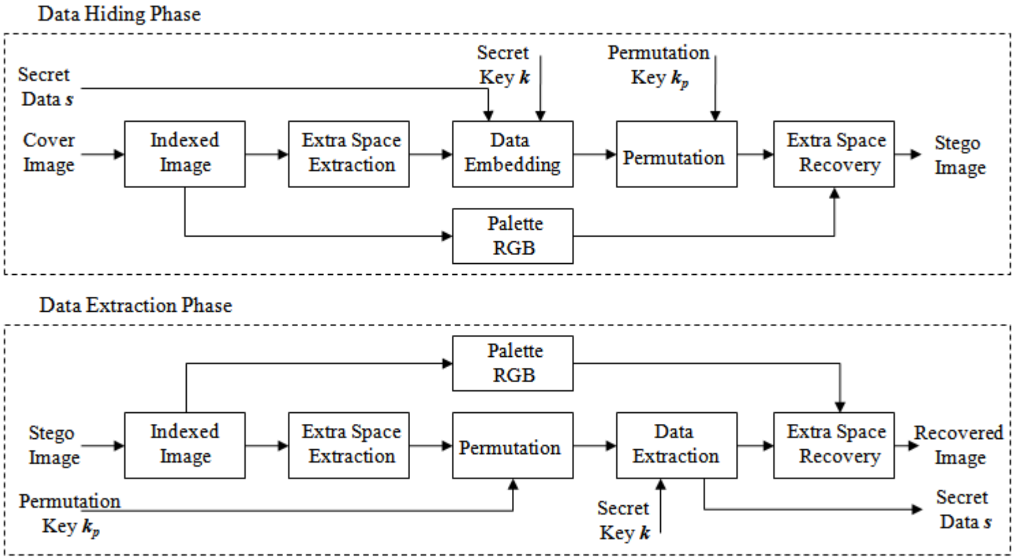


Figure 2. Data hiding and extraction phases of our scheme

data s_j is embedded into the value of index differences of the extracted extra space under the secret key k_j^i. Table 1 gives the notations that will be used in this paper.

Also, the index table $I(N \times N)$ is partitioned into non-overlapped n blocks, and each block has $r(3 \times 3)$ indexes. Then r indexes in each block, $p_1^n, p_2^n, \dots p_8^n$ are obtained as rule of rounding as shown in Figure 1. In each block, we select a center index p_c^n, and create a series of index differences between the center index and its neighboring index values as $d_i^n = p_c^n - p_i^n$, where $1 \le i \le 8$ and $i \ne c$. The center index p_c^n of each block remains unaltered in the data embedding and extraction phases to restore other index values. After these operations, we can embed bits of the secure information s_j into the index table.

Figure 2 shows the reversible data hiding and extraction processes of our scheme, which consist of composing color image components, extra space extraction, random permutation, and data embedding and extraction phases with secret data s_j, secret key k_j^i and random permutation key k_p. We provide the detailed data embedding and extracting processes in the following sections.

3.2. Data Hiding Phase

Before data embedding, we calculate index differences to obtain extra space $d_i^{n^*}$. For this purpose, we set a pre-defined threshold value τ, which is non-negative integer. Then, a difference value d_i^n is modified to $d_i^{n^*}$ as follows:

$$d_i^{n^*} = \begin{cases} d_i^n + 1, & if\ d_i^n > \tau; \\ d_i^n, & if\ (-\tau) \le d_i^n \le \tau; \\ d_i^n - 1, & if\ d_i^n < (-\tau). \end{cases} \tag{1}$$

where $1 \le i \le 8$ and $i \ne c$, and τ is a threshold value. In the experiment, we selected the threshold values as 1, 2, 3…, and evaluated permissible quantity.

In the embedding process, each $d_i^{n^*}$ can be represented by 8 bits, $b_7^i, b_6^i, \ldots, b_0^i$, where $b_j^i = \lfloor d_i^{n^*}/2^j \rfloor (mod\ 2)$, and $d_i^{n^*} = \sum \lfloor b_j^i * 2^j \rfloor$, where $j = 0, 1, \ldots, 7$. The secret data s^i is embedded into b_0^i bit of the modified value $d_i^{n^*}$ under the key k_j^i by using a bitwise XOR operation given in equation (2),

$$b_0^i \leftarrow b_0^i \oplus k_j^i \oplus s_j \tag{2}$$

where $1 \le i \le r$, $i \ne c$ and $k_j^i, s_j \in \{0, 1\}$. A secret key k_j^i is generated by pseudo-random generator.

Then, the embedded values $\{d_1^{n^*}, d_2^{n^*}, \ldots, d_8^{n^*}\}$ of the extra space in block are applied to the random permutation. The indexes in the block are calculated using the following permutation operation,

$$P_{k_p}[d_1^{n^*}, d_2^{n^*}, \ldots, d_8^{n^*}]_n = \left[d_{k_{p(1)}}^{n^*}, d_{k_{p(2)}}^{n^*}, \ldots, d_{k_{p(8)}}^{n^*}\right]_n \tag{3}$$

where n is the number of blocks and $k_p \in \{k_1, k_2, \ldots, k_n\}$ is the permutation key.

Finally, we restore the indexes pc_i^n of the index table, by using the difference values between a center index and neighboring permuted indexes as $pc_i^n = p_c^n - d_{k_{p(i)}}^{n^*}$, where $1 \le i \le 8$ and $i \ne c$. The embedded stego image is reconstructed by the index table I and the palette P. Once the secret data is embedded into the image, the components of the stego image can be changed. In general, the difference between the cover image and the stego image should be unnoticeable by the human eyes. Therefore, we can check the histogram distribution of the stego image to identify an alteration of processing as shown in Figure 3.

3.3. Data Extraction Phase

We extract the secret data s and reverse the embedded stego image to the cover image. After constructing the index table I of the stego image, we calculate the difference values $d_{k_{p(i)}}^{n^*} = p_c^n - pc_i^n$. The random permutation is applied to restore an index's positions of the each cover blocks by using the permutation key k_p as follows:

$$P_{k_p}\left[d_{k_{p(1)}}^{n^*}, d_{k_{p(2)}}^{n^*}, \ldots, d_{k_{p(8)}}^{n^*}\right]_n = [d_1^{n^*}, d_2^{n^*}, \ldots, d_8^{n^*}]_n \tag{4}$$

In order to reconstruct the secret data s, the difference values $d_i^{n^*}$ are represented by binary form b_j^i. Then, we perform an extraction of the embedding data by using the bitwise XOR operation between the b_0^i bit of the modified value $d_i^{n^*}$ and secret key k_j^i given in equation (5),

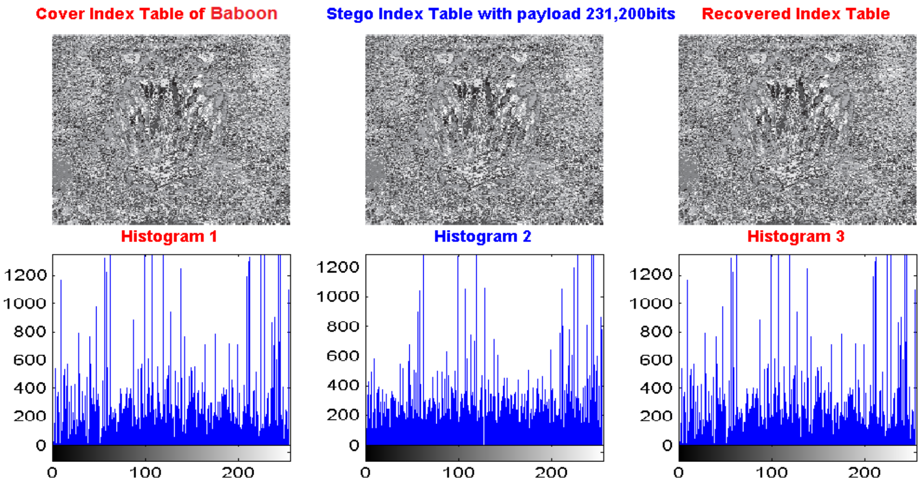


Figure 3. Histogram distributions of the index table

$$s_i = b_0^i \oplus k_j^i \tag{5}$$

where $1 \leq i \leq 8$, $i \neq c$ and $k_j^i, s_j \in \{0, 1\}$.

As a result of this operation, we obtain the hidden secure data s_j, and then the b_0^i bit value is restored without any degradation by using equation (2). Afterward, the represented value $d_i^{n^*}$ from binary form is modified to the difference value d_i^n, according to the following equation,

$$d_i^n = \begin{cases} d_i^{n^*} - 1, \ \ if \ d_i^{n^*} > \tau + 1; \\ d_i^{n^*}, \ \ if \ (-\tau) + 1 \leq d_i^{n^*} \leq \tau + 1; \\ d_i^{n^*} + 1, \ \ if \ d_i^{n^*} < (-\tau) + 1. \end{cases} \tag{6}$$

where $1 \leq i \leq r$ and $i \neq c$, and τ is threshold value.

The indexes of recovered index table are obtained by calculating a difference between the center index and its neighbor indexes as $p_i^n = p_c^n - d_i^n$, where $1 \leq i \leq 8$, $i \neq c$. Finally, the cover image is reconstructed by the index table I and the palette P.

4. Experimental Results

In this section, we describe our experiments and discuss the results. The simulation was carried out using Matlab version R2008a. In order to evaluate the performance of our scheme, we considered eight commonly used color images with the size of 512×512 as shown in Figure 4.

Embedding quality is an important factor for reversible data hiding since one can hide more data with less computation and with a reasonably good perceptual quality. It is measured by Peak-Signal-to-Noise-Ratio ($PSNR$). Typically, it is acceptable if the $PSNR$ in lossy image is between 30 dB and 50 dB, where higher is better performance. We chose the secure data as Figure 4(k), which is divided into several payload parts: 30 percent of whole payload is 69,360 bits, 60 percent of whole payload is 138,720 bits, 100 percent of whole payload is 231,200 bits, and so on.

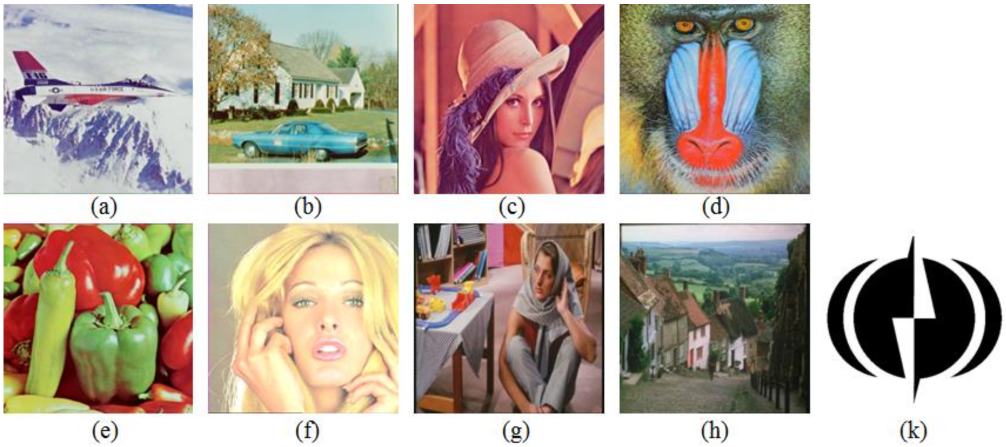


Figure 4. Test color images (512x512). (a) Airplane, (b) House, (c) Lena, (d) Baboon, (e) Pepper, (f) Tiffany, (g) Barbara, (h) Goldhill and (k) Secret data s (binary image 231,200bits)

Table 2. Visual quality and permissible quantity of test images depend on payload sizes

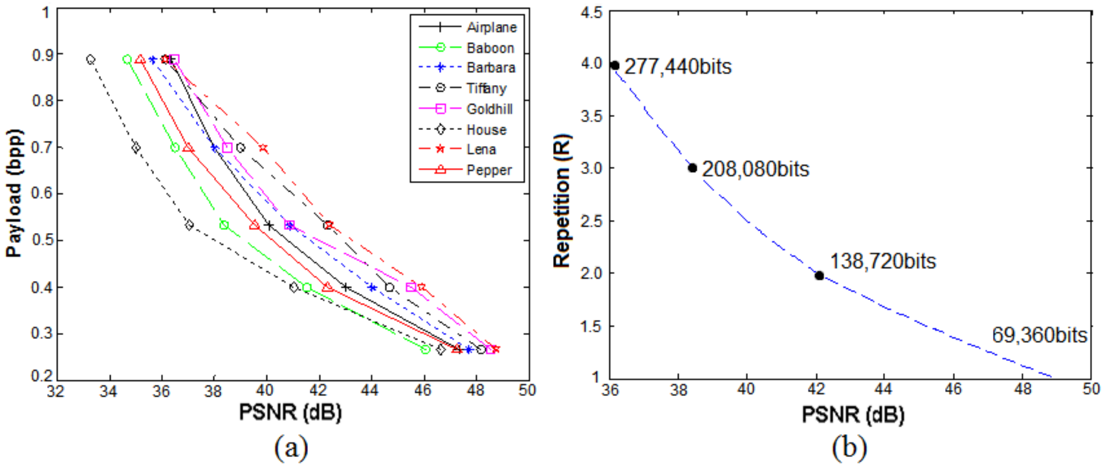
	Payload (30%)		Payload (60%)		Payload (100%)	
Test Images	PSNR(dB)	PQC(bpp)	PSNR(dB)	PQC(bpp)	PSNR(dB)	PQC(bpp)
Airplane	47.27		42.53		36.41	
Baboon	47.11		41.84		37.59	
Barbara	47.59	0.267bpp	43.25	0.533bpp	37.73	0.889bpp
Tiffany	48.38		44.65		38.34	
Goldhill	48.31	69,360bits	44.69	138,720bits	39.19	231,200bits
House	46.54		42.24		36.65	
Lena	48.49		44.15		38.29	
Pepper	48.23		43.56		37.63	

The permissible quantity of concealing (PQC) is the proportion of the maximum quantity of concealment to the size of image. The PQC can be found by the formula $PQC = Q/(N \times N)$, where Q is the total quantity of payload.

We present the results of $PSNR$ and PQC for all test images in Table 2 according to payload size. From these comparisons, we can conclude that our scheme has achieved the high $PSNR$ with a quite large embedding capacity. The results of $PSNR$ values of stego images are higher than 46 dB with a payload 0.267 bpp, so that our scheme can be observed low image degradation. Furthermore, we can embed 231,200 bits payload ($\approx 28K\ bytes$), for an image of 512×512 size.

Figure 5(a) shows the results of $PSNR$ where single-pass embedding is applied to each test images, respectively. The $PSNR$ values are depending on the size of payload, we varied the payload size from 69,360 bits (0.267 bpp) to 231,200 bits (0.889 bpp). According to the decrement of payload sizes, the qualities of stego images are up to 46.49 dB.

However, R, the number of repetition of multi-pass embedding is directly affected to increase the embedding capacity as shown in Figure 5(b). In case of $R = 2$, the $PSNR$ value around 42 dB while we can embed $69{,}360 \times 2 = 138{,}720$ bits into in size of 512×512 color images. This is much more capacity than the existing reversible data hiding schemes for color palette image.



(a) (b)

Figure 5. The performance of permissible quantity of (a) single-pass embedding and (b) multi-pass embedding

Table 3. A compared results with previous data hiding schemes

	PSNR (dB)	PQC (bpp)	Payload (bits)
Lena (512×512)			
Scheme [4]	40.49	0.015	4,096
Scheme [7]	48.20	0.021	5,460
Scheme [6]	43.52	0.200	52,445
Proposed	48.49	0.301	69,360
Airplane (512×512)			
Scheme [4]	40.26	0.015	4,096
Scheme [7]	48.30	0.062	16,171
Scheme [6]	44.49	0.251	65,920
Proposed	47.27	0.301	69,360
Baboon (512×512)			
Scheme [4]	35.95	0.015	4,096
Scheme [7]	48.20	0.021	5,421
Scheme [6]	36.39	0.106	27,948
Proposed	48.61	0.301	69,360

The next experiment is designed to compare the permissible quantity of our scheme with those of the other reversible data hiding schemes [4, 6, 7]. Table 3 shows the results of our experiment. In [4], secret data is hidden in each block of quantized discrete cosine transformation (DCT) coefficients on a JPEG image. Two successive zero coefficients of the medium-frequency components in each block are used for secret data to be embedded. Overall, the proposed scheme is superior to scheme [4]. Our scheme can offer a higher hiding capacity than scheme [6]. Since there is large variation in the gray-levels of most adjacent pixels in "Baboon", the amount of extra data is so largely required to be recorded by scheme [6] that there is not enough space to hide the secret data. Although the scheme [7] provides a better stego image quality, its hiding capacity is much smaller than that of our scheme.

5. Conclusion

We proposed a reversible data hiding scheme for color palette image. Our scheme not only improves the visual quality but also provides larger payload capacity than other related schemes. Specifically, the proposed scheme is able to embed about $5K$ bytes through $28K$ bytes into a 512×512 color image while guaranteeing the $PSNR$ of the stego image versus the cover image to be above $46\ dB$. This implies that the proposed scheme can offer high embedding quality and low image degradation. It is expected that our reversible data hiding technique will be deployed for a wide range of applications, such as secure medical image data system, law enforcement, image authentication and covert secure communication, and so on.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Grant No. 2011-0012849).

References

[1] C. C. Chang and T. D. Kieu, “A reversible data hiding scheme using complementary embedding strategy”, Information Sciences, vol. 180, no. 16, **(2010)**, pp. 3045-3058.

[2] C. C.Chang, P. Y. Pai, C. M. Yeh and Y. K. Chan, “A high payload frequency-based reversible image hiding method”, Information Sciences, vol. 180, no. 11, **(2010)**, pp. 2286-2298.

[3] M. Y. Wu and J. H. Lee, “A reversible data hiding method for palette-based images with capacity optimization”, International Conference on Image Processing, Computer Vision and Pattern Recognition, vol. 02, **(2008)**, pp. 95-100.

[4] C. C. Chang, C. C. Lin, C. S. Tseng and W. L. Tai, “Reversible hiding in DCT-based compressed images”, Information Sciences, vol. 177, no. 13, **(2007)**, pp. 2768-2786.

[5] C. C. Chang, C. Y. Lin and Y. H. Fan, “Lossless data hiding for color images based on block truncation coding”, Pattern Recognition, vol. 41, **(2008)**, pp. 2347-2357.

[6] J. Tian, “Reversible data embedding using a difference expansion”, IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, **(2003)**, pp. 890-896.

[7] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, “Reversible data hiding”, IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, **(2006)**, pp. 354-362.

[8] C. C. Chang and T. C. Lu, “Lossless information hiding scheme based on neighboring correlation”, International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 2, no. 1, **(2009)**, pp. 49-56.

[9] D. Bhattacharyya, A. Roy, P. Roy and T. -H. Kim, “Receiver compatible data hiding in color image”, International Journal of Advanced Science and Technology, vol. 6, **(2009)**, pp. 15-24.

[10] B. Surekha and G. N. Swamy, “A spatial domain public image watermarking”, International Journal of Security and Its Applications, vol. 5, no. 1, **(2011)**, pp. 1-12.

[11] A. M. Alattar, “Reversible watermark using the difference expansion of a generalized integer transform”, IEEE Transactions on Image Processing, vol. 13, no. 8, **(2004),** pp. 1147–1156.

[12] A. Ker, “Steganalysis of LSB matching in grayscale images”, IEEE Signal Processing Letters, vol. 12, no. 6, **(2005)**, pp. 441–444.

[13] X. Wang, T. Yao and C. T. Li, “A palette-based image steganographic method using color quantization”, In: Proceedings of IEEE International Conference on Image Processing, vol. 2, **(2005)** September, pp. 1090–1093.

[14] M. Y. Wu, Y. K. Ho and J. H. Lee, “An iterative method of palette-based image steganography”, Pattern Recognition Letters, vol. 25, **(2004)**, pp. 301–309.

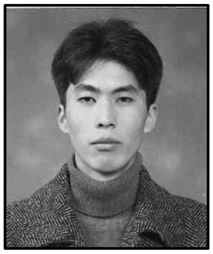
[15] C. C. Chang and T. C. Lu, “A difference expansion oriented data hiding scheme for restoring the original host images”, The Journal of Systems and Software, vol. 79, no. 12, **(2006)**, pp. 1754–66.

[16] C. C. Lee, H. C. Wu, C. S. Tsai and Y. P. Chu, “Adaptive lossless steganographic scheme with centralized difference expansion”, Pattern Recognition, vol. 41, no. 6, **(2008)**, pp. 2097–106.

[17] C. C. Lin and N. L. Hsueh, “A lossless data hiding scheme based on three-pixel block differences”, Pattern Recognition, vol. 41, no. 4, **(2008)**, pp. 1415–25.
[18] J. Y. Hsiao, K. F. Chan and J. M. Chang, “Block-based reversible data embedding”, Signal Processing, vol. 89, no. 4, **(2009)**, pp. 556–69.
[19] K. S. Kim, M. J. Lee, H. Y. Lee and H. K. Lee, “Reversible data hiding exploiting spatial correlation between sub-sampled images,” Pattern Recognition, vol. 42, no. 11, **(2009)**, pp. 3083–96.
[20] B. Yang, M. Schmucker, W. Funk, C. Brush and S. Sun, “Integer DCT-based reversible watermarking for images using companding technique”, Proceedings of SPIE, Security, Steganography and Watermarking of Multimedia Contents, vol. 5306, **(2004)**, pp. 405–15.
[21] B. Yang, M. Schmucker, X. Niu, C. Busch and S. H. Sun, “Integer-DCT-based reversible image watermarking by adaptive coefficient modification”, Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents, vol. 568, **(2005)**, pp. 218–29.
[22] G. Xuan, Y. Q. Shi, Q. Yao, Z. Ni, C. Yang and J. Gao, “Lossless data hiding using histogram shifting method based on integer wavelets”, International Workshop on Digital Watermarking, Lecture Notes in Computer Science, vol. 4283, **(2006)**, pp. 323–32.
[23] Z. M. Lu, J. X. Wang and B. B. Liu, “An improved lossless data hiding scheme based on image VQ-index residual value coding”, Journal of Systems and Software, vol. 82, no. 6, **(2009)**, pp. 1016–24.
[24] J. X. Wang and Z. M. Lu, “A path optional lossless data hiding scheme based on VQ index table joint neighboring coding”, Information Sciences, vol. 179, no. 19, **(2009)**, pp. 3332–48.
[25] B. G. Mobasseri and D. Cinalli, “Lossless watermarking of compressed media using reversibly decodable packets”, Signal Processing, vol. 86, no. 5, **(2006)**, pp. 951–61.

Authors

Munkhbaatar Doyoddorj received his B.S. degree in Department of Electronic Engineering from National University of Mongolia in 2003, the M.S. degree in Department of Information Security from Pukyong National University, Republic of Korea in 2010, and is currently pursuing the Ph.D. degree in Department of Information Security, Pukyong National University. His research interests are related with multimedia security, image forensics and watermarking security.



Chul Sur received his M.S. and Ph.D. degrees in Department of Computer Science from Pukyong National University, Republic of Korea in 2004 and 2010, respectively. He worked as a post doctor course researcher in the Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan. His research interests are related with applied cryptography, network security, and secure e-commerce.

Youngho Park received his M.S. and Ph.D. degrees in Department of Computer Science and Information Security from Pukyong National University, Republic of Korea in 2002 and 2006, respectively. He worked as a post doctor course researcher in Department of IT Convergence and Application Engineering, Pukyong National University. His research interests are related with information security, applied cryptography and network security; secure ad hoc network, authentication, key management, and identity-based cryptosystem.

Kyung-Hyune Rhee received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Daejeon Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Daejeon Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide, the University of Tokyo, the University of California, Irvine and Kyushu University. He has served as a Chairman of Division of Information and Communication Technology, Colombo Plan Staff College for Technician Education in Manila, the Philippines. He is currently a professor in the Department of IT Convergence and Application Engineering, Pukyong National University, Republic of Korea. His research interests center on key management and its applications, mobile communication security and security evaluation of cryptographic algorithms.