Journal of the Optical Society of Korea
Vol. 12, No. 3, September 2008, pp. 136-146

DOI: 10.3807/JOSK.2008.12.3.136

An Adaptive Steganography of Optical Image using Bit-Planes and Multi-channel Characteristics

Jin-Suk Kang

Dept. of Computer Science and Eng., University of Incheon, 177 Dohwa-dong, Nam-gu, Incheon, 402-749, Korea

Taikyeong T. Jeong*

Dept. of Communication Eng., Myongji University, 38-2 Namdong, Cheoin-gu, Yongin-city, Gyeonggido, 449-728, Korea

(Received June 18, 2008 : revised August 28, 2008 : accepted September 12, 2008)

We proposed an adaptive steganography of an optical image using bit-planes and multichannel characteristics. The experiment's purpose was to compare the most popular methods used in optical steganography and to examine their advantages and disadvantages. In this paper we describe two digital methods: the first uses less significant bits (LSB) to encode hidden data, and in the other all blocks of n×n pixels are coded by using DCT (Digital Cosine Transformation), and two optical methods: double phase encoding and digital hologram watermarking with double binary phase encoding by using IFTA(Iterative Fourier Transform Algorithm) with phase quantization. Therefore, we investigated the complexity on bit plane and data, similarity insert information into bit planes. As a result, the proposed method increased the insertion capacity and improved the optical image quality as compared to fixing threshold and variable length method.

Keywords: Optical Steganography, BPCS(Bit-Plane Complexity Steganography), IFTA(Iterative Fourier Transform Algorithm)

OCIS codes : (100.2000) Digital image processing; (100.2960) Image analysis; (100.2980) Image enhancement; (100.4550) Optical correlators

I. INTRODUCTION

Optical technologies have recently been employed in data security. Compared with traditional computer and electrical systems, optical technologies offer primarily two types of benefits. (1) Optical systems have an inherent capability for parallel processing; that is, rapid transmission of information. (2) Information can be hidden in any of several dimensions, such as phase of spatial frequency; that is, optical systems have excellent capability for encoding information [1, 2, 3, 4].

In several pioneering studies [1, 2, 3], the authors demonstrated different optical verification systems for information security applications based on optical correlations. These systems correlate two functions: one, the lock, is always inside the correlator, and the other, the key, is presented to the system by the user in the verification stage. Mostly, the systems determine whether the input is true or false by detecting the correlation peak, a higher level of security and more sophisticated services than the simple verification offered by the existing systems.

Steganography is a technique used in secret communications for protection of information and also is a type of information hiding technique focused on hiding messages which transmits by inserting secret messages to the cover message so that in contrast to the existing encryption, the existence of the inserted message cannot be determined. Therefore, the most important precondition for steganography is the imperceptibility. Because the imperceptibility at this time is greatly dependent on the amount of secret message information, the modification on cover message is also increased as there is greater insertion capacity. So the imperceptibility of

*Corresponding author: ttjeong@mju.ac.kr having to hide secret messages and the capacity determining the amount of data have very close correlation with each other in steganography [5, 6].

In this paper propose an optical steganography technique of inserting the information adjustably depending on the optical image using bit-plane and multi channel features in order to improve the BPCS (Bit-Plane Complexity Steganography) technique. To make this possible, the weight by channel and the weight by bit-plane are defined to start with. Because the vision of human beings reacts more sensitively to the color tone information for the weight by channel, it is calculated using the correlation relationship on the projection signal of the color. And the weight by bit-plane is calculated using the change of image quality followed by the position of the bit-plane. Therefore, this paper proposes the optical steganography technique of inserting information adjustably to each bit-plane by channel using these weights.

The method proposed is the technique of making each bit-plane of the cover image and the secret image to be inserted into blocks to insert the secret image by measuring complexity and similarity while being able to gain an improved result in optical image quality or capacity over the existing method.

II. OPTICAL STEGANOGRAPHIC METHODS

2.1 Digital methods

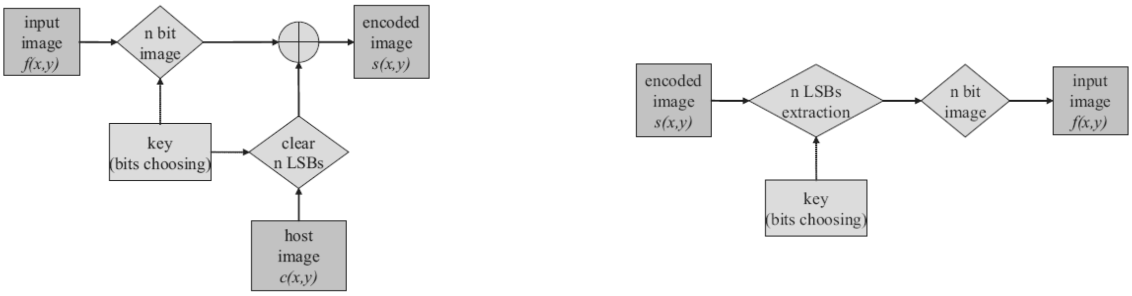
1) Simple LSB method

This first most simple digital method uses less significant bits (LSB) to encode hidden data [9]. The hidden message $f(x,y)$ is divided into one, two or more LSBs of bytes describing each pixel. These bits of host image $c(x,y)$ are replaced with bits from the message (Fig. 1). Thus the hidden image is located in the domain of image and must possess several times less information pixels than the host image. Moreover, using some parts of bytes for hiding data, the color space is smaller and the original host image has to be colored with lesser color levels. If the image should appear normal to the untrained eye the hidden data must not extend above 50% of the image file size (least significant 4 bits).

If the input image is sufficiently smaller, it can be hidden in the host image in a more sophisticated way. Only some pixels can be used for writing such data. The method of choosing these pixels can ensure additional security as it can be treated as a key without which decoding is impossible.

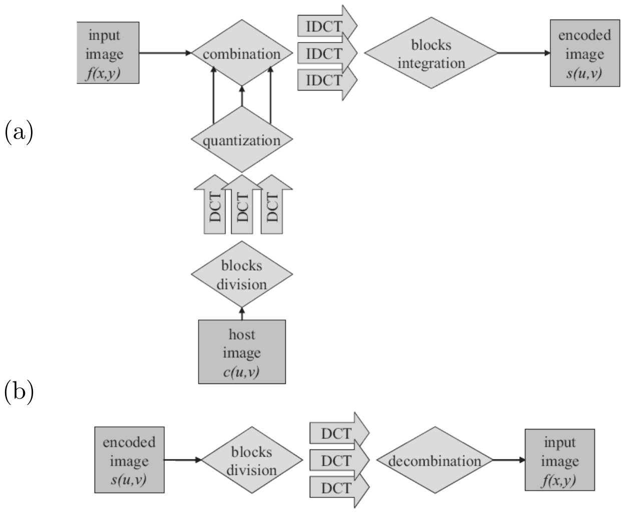
2) DCT based method

This method is closely connected with one of the most popular image formats in the internet – the JPEG standard and its lossy compression algorithm [8]. The decompressed image may not be the same as image before compression and changes in LSBs are expected. Therefore it is unlikely that LSB encoding would work with any lossy algorithm. Consequently a rival and more effective method was developed for work with JPEG compressed images. In this method the whole host image $c(x,y)$ is divided into blocks of $n \times n$ pixels (in basic version n = 8). Each of them is transformed by using DCT(Digital Cosine Transformation). After that we get a block of $n \times n$ transformation coefficients they should be quantized by dividing them by a pre-defined (in JPEG standard) quantization matrix. Next, two of them: c_{ij} and c_{kl} are compared and their values are exchanged or not. If we want to put 0 in such a block and $c_{ij} < c_{kl}$ or if we want to put 1 and $c_{ij} < c_{kl}$ then we exchange the values of these coefficients. Otherwise we do not make any changes. It is also possible to hide information $f(x,y)$ by replacing the LSB of the quantized coefficients with the bit to be hidden in an image as in steganographic tool JSteg [23]. After the completion of this process all blocks should be transformed using inverse DCT obtaining encoded image $s(x,y)$ (Fig. 2). By this method the hidden image is located in the domain of transformation.



(a) (b)

Figure 1. Scheme of LSB method: a) encoding - input image $f(x,y)$ is changed into n bits per pixel of host image in the positions described by a key. n LSB bits in the appropriate pixel of the host image $c(x,y)$ are cleare., Next these two images are combined together into encoded image $s(x,y)$; b) decoding – n LSBs bits are extracted from appropriate pixels of encoded image $s(x,y)$ defined by a key and next folded into the decoded image $f(x,y)$.



(a)

Figure 2. Scheme of DCT method: a) encoding - host image $c(u,\nu)$ is divided into blocks of $n\times n$ pixels transformed by using DCT, next obtained coefficients are quantitized and with such prepared data the input image $f(x,y)$ is combined, after that all these blocks are transformed by using inverse DCT and put together into one encoded image $s(u,\nu)$; b) decoding - encoded image $c(u,\nu)$ is divided into blocks of $n\times n$ pixels transformed by using DCT, next the decoded image $f(x,y)$ is extracted from obtained coefficients.

2.2. Optical Methods

1) Double phase encoding

This method was proposed by [9] and is based on double phase encoding described by [10]. Encoding and decoding process is shown in Figure 3.

The most important part of encoding is using two random phase masks. At the beginning, the input image $f(x,y)$ is multiplied by the first random phase mask $n(u,\nu)$. Finally, it is transformed by using inverse fourier transformation (IFT) and multiplied by a constant α. An image $\Psi(x,y)$ prepared in such a way is added to the host image $c(x,y)$. At the end of the encoding process we obtain encoded image $s(x,y)$. Thanks to using two phase masks in such a way, the encoded image has the features of white noise located in the domain of image and there is no possibility to recover the phase using appropriate algorithms. For decoding the hidden information, the encoded image should be processed in a similar way as during encoding but using the conjugated phase mask in reverse order. After Fourier transformation it is multiplied by conjugated second phase mask $n^*(u,\nu)$ and next, after inverse Fourier transformation it is multiplied by conjugated first phase mask $m^*(x,y)$. At the end of the decoding process we obtain the decoded image $f'(x,y)$ nearly similar to the original input image.

2) Digital hologram with binary phase

This method was developed by [11] and bases on the concepts of [12, 13]. The encoding and decoding process is shown in Fig. 4 First, the input image $f(x,y)$ and the key image $k(x,y)$ should be encoded into pure phase image by using inverse IFTA (Iterative Fourier Transform Algorithm) with phase quantization. Next, this phase version of the input image and conjugated phase version of the key image are multiplied together and then by a constant α and added to the host image $c(u,\nu)$. The best results are achieved in binary phases for both (input and key) images and so the final encoded image $s(u,\nu)$ has the features of a digital hologram. In this method, Fourier transformation of input image is located in the domain of the host image and it can be treated as located in the domain of transformation. To obtain a decoded image $f'(x,y)$ very similar to original input (compound of input, conjugated input and zero order diffraction) the encoded image $s(u,\nu)$ should be multiplied by $2/\alpha$, next transformed by using Fourier transformation and then multiplied by pure phase image from inverse IFTA transformation of key image $k(x,y)$. If an image other than the original key image is used, the decoded image will be totally different from the original input image.

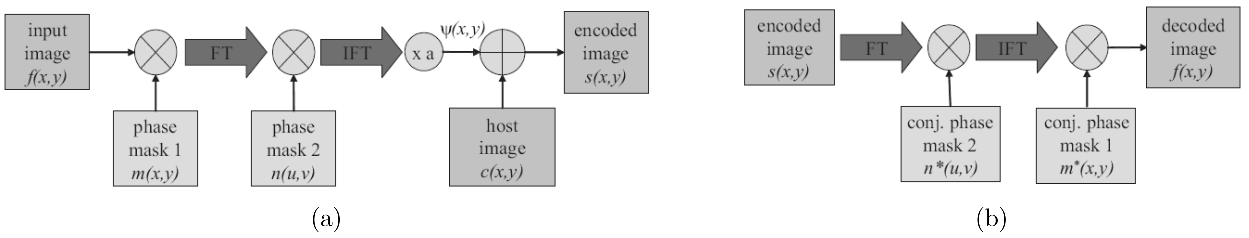
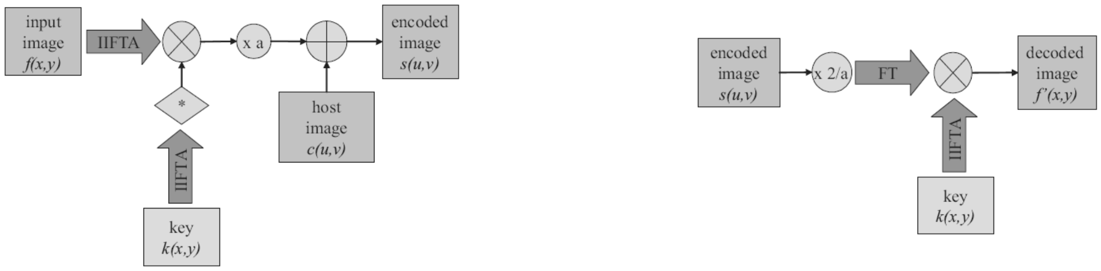


Figure 3. Double phase encoding method scheme: a) encoding - input image $f(x,y)$ is multiplied by first phase mask $m(x,y)$, transformed by using FT and multiplied by second phase mask $n(u,\nu)$, next it is transformed by using IFT, multiplied by a constant α and added to host image $c(x,y)$ obtaining encoded image $s(x,y)$; b) decoding - encoded image $s(x,y)$ is transformed by using FT and multiplied by conjugated second mask $n^*(u,\nu)$, next it is transformed by using IFT and multiplied by conjugated first phase mask $m^*(u,\nu)$ obtaining encoded image $f'(x,y)$ similar to the input image.



(a) (b)

Figure 4. Digital hologram with binary phase method scheme: a) encoding - key image $k(x,y)$ is transformed by IIFTA to obtain pure phase image and subsequently conjugated, next it is multiplied by pure phase image obtained from input image $f(x,y)$ by using IIFTA, then after multiplication by a constant it is added to the host image $c(u,\nu)$ obtaining the encoded image $s(u,\nu)$; b) decoding - encoded image $s(u,\nu)$ is multiplied by $2/\alpha$ and transformed by using FT, next it is multiplied by pure phase image obtained by using IIFTA to the key image $k(x,y)$ obtaining decoded image very similar to the original input image.

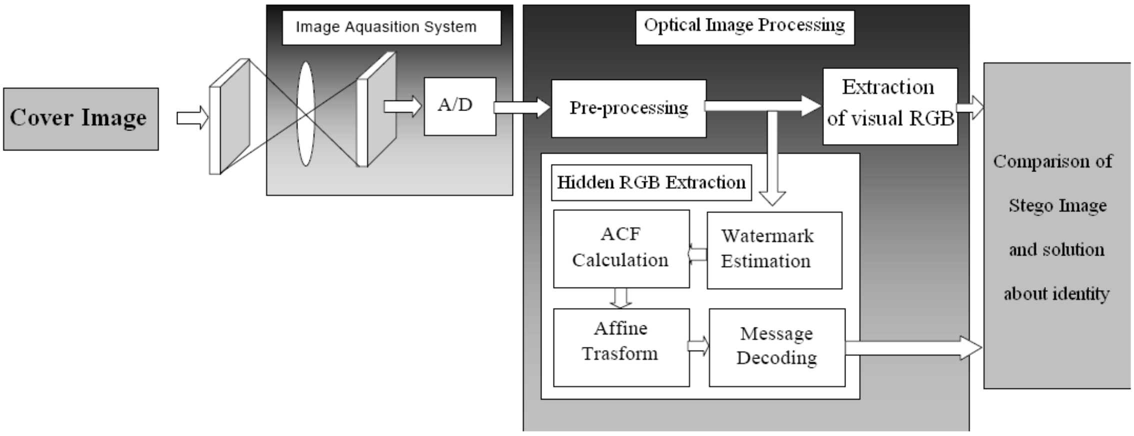


Figure 5. Block Diagram of the optical/digital Steganography

III. THE PROPOSED ALGORITHM

The image acquisition system is to convert the analogue optical image to the digital form that then will be used for the visual and hidden RGB extraction in the following optical image processing system. And each separated R, G and B frames are made into bit-planes and the complexity of each bit-plane is calculated at this time. If the complexity of each bit-plane is calculated, the top 4 bit-planes of highest complexity are selected and at this time, each bit-plane is made into 8×8 blocks and matched in order to measure similarity with inserted secret images. Figure. 5 is the overall structure map of the algorithm proposed in this paper.

In comparison process we should use a metric for the evaluation of watermarking techniques. In Table 1, the set of such metrics is presented. The only rigorously defined metric in Table 1 is PSNR, defined in Eq. 1. The main reason for this fact is that no reliable rigorously defined metric has been proposed that would take the effect of the Human Visual System (HVS) into account. PSNR is provided only to give us a rough approximation of the quality of the watermark. Further levels of evaluation rely strictly on observation under varied conditions, as shown in table 1. Therefore, for strict comparison we used this metric.

$$PSNR = 10\log\left(\frac{(2^k-1)^2}{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij}-B_{ij})^2}\right) \tag{1}$$

Where $M\times N$ stands for the size of compared images, A_{ij} and B_{ij} stands for the value of pixels of image A and B at position (i,j), k stands for the number of bits used for coding gray levels.

The optical methods have some parameters and therefore before the comparison process we examined those methods in details. The obtained results according to parameter α (the weight) are show in Figure 6. Lines going from top to middle show comparison of encoded and host images whereas lines going from bottom to middle show comparison of decoded and input images.

Table 1. Summary of possible perceptibility assurance Levels

Level of Assurance	Criteria
Low	• Peak Signal-to-Noise Ratio (PSNR) • Slightly perceptible but not annoying
Moderate	• Metric Based on perceptual model • Not perceptible using mass market equipment
Moderate High	• Not perceptible in comparison with original under studio conditions
High	• Survives evaluation by large panel of persons under the strictest of conditions

The lines with '+' marks are for encoded image without any modification when all amplitude and phase information is accessible. The lines with circle marks are only for the amplitude part of encoded image. The lines with diamond marks are for quantized amplitude part of encoded image whose maximal value equals 255. The last lines with '*' marks are for the amplitude park of encoded image, which is quantized and rescaled into range [0,255].

Each method has different advantages and disadvantages. Firstly, the quality of the encoded image is much better for digital methods – in both cases (LSB and DCT) there are no significant changes for the human eye in the host image – the value of PSNR between host and encoded image is around 40. It is totally different from the optical methods, in which such changes are clearly visible and sometimes very strong – the value of PSNR is below 20. Secondly, when there are no distortions the decoded images obtained by digital methods are also much better than for optical ones. But, when the encoded image is changed, in some way, due to technical problems such as noisy transmission, then

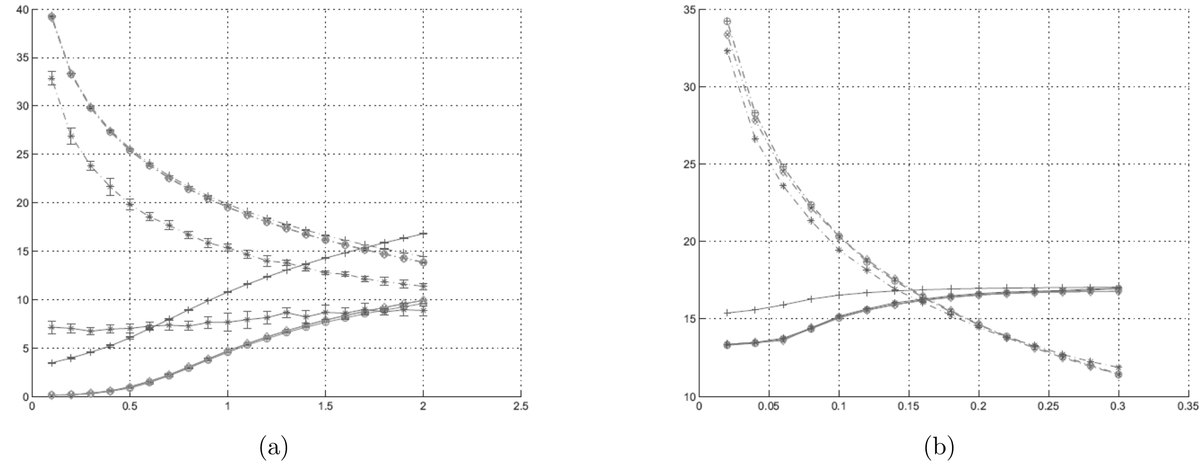


Figure 6. PSNR for encoded in comparison with host (upper lines) and decoded in comparison with input image (lower lines) according to parameter α on x-axe: a) double phase encoding method; b) digital hologram method.

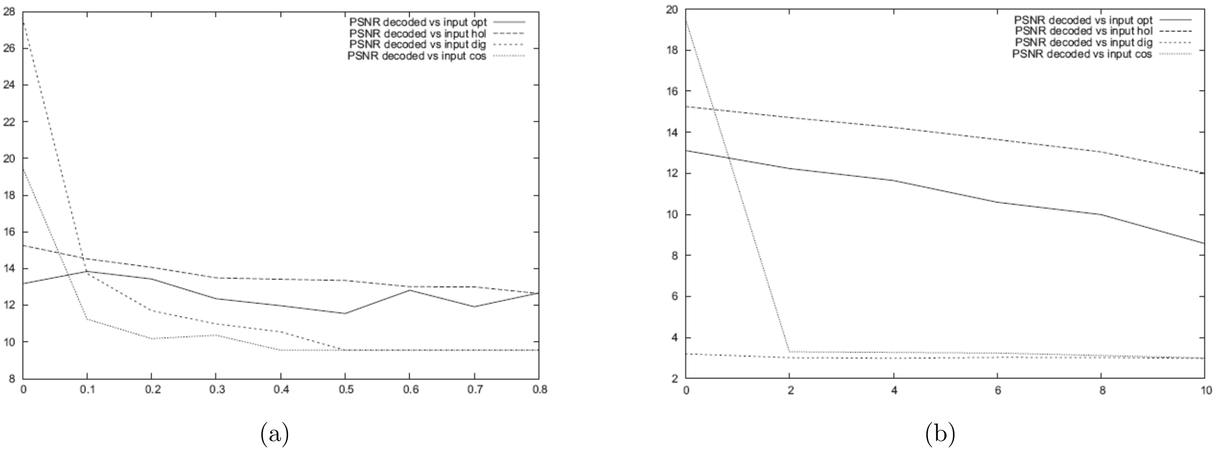


Figure 7. PSNR for encoded images with distortions: a) occlusion (x-axe – the part of occluded image); b) noise (x-axe – variance of Gaussian noise)

optical methods show their effectiveness. As shown on Fig. 7, optical steganography gives better results when the encoded image is occluded or, especially, in case of noise, when digital methods are very deficient.

The following algorithm is implemented in pseudo code with comments. The actual implementation was written in Visual C++. This code works for bitmap images (or any image that has lossless compression). Compression ruins the watermarking for obvious reasons; it destroys the small changes that the algorithm makes to each pixel.

The actual loading and writing of image data is library and platform specific and is beyond the scope of the paper. This code is only for the encoding portion of the data, to decode, these steps must be taken in reverse order.

```
integer height, width;
2DArray imgbuffer = LoadImage(“imagefile”, &height, &width);
// load data of our image into matrix
string txtbuffer = LoadText(“textfile”);
//load the data to be hidden
stringofbits binarydata;
// the number of bits will be 8 * length(txtbuffer)
integer index;
integer x, y;
integer Red, Green, Blue;
for[index = 0; index < length(txtbuffer); index++]
binarydata += GBDFA (txtbuffer[index]);
// get the binary data from the ascii character
end for
index = 0;
// now iterate through each pixel of data encoding 3 bits
// into every image by changing the least significant bit
// of each color value
for[x = 0; x < width; x++]
for[y = 0; y < height; y++]
    GetRGB(&Red, &Green, &Blue, imagebuffer[x][y]);
// get the current values
// encode the bit of the data into the color
    EncodeBitIntoCol or (binarydata[i++], Red);
// fails if index doesn't exist
    if i == length(binarydata)
            breakout of loop;
EncodeBitIntoColor(binarydata[i++],Green);
    if i == length(binarydata)
            breakout of loop;
EncodeBitIntoColor(binarydata[i++],Blue);
    if i == length(binarydata)
            breakout of loop;
SetRGB(Red,Green,Blue,imagebuffer[x][y]);
// write new colors to the pixel data
end for
end for
SaveImage(“imagefile”); //save the new image
```

This code reads two files from the disk: the document that needs to be hidden and the optical image that will serve as the hiding place. The document that was read from the disk is then converted into the 8 bit binary equivalents each character's ASCII value. For example: the letter A is found in the document; that is 97 ASCII which is 01100001 binary. Once all of the characters in the document are converted to binary, the image's color values are read into a matrix that corresponds to each pixel in the image. The algorithm modifies the least significant bit of each pixel containing red, green and blue values. Each pixel in the image matrix is modified until all of the document data is hidden.

For example:

Pixel 0,0 contains the color values 255,255,255 which are 11111111, 11111111, 11111111 in binary (a very bright white).

The data we are encoding is the first three bits of the capital letter A: 011.

The encoding would make the values change in this order
11111111 becomes 1111111**0**
11111111 stays as 1111111**1**
11111111 stays as 1111111**1**

And the resulting color triple is 254,255,255 which is a shade of white that has an indiscernible difference compared to the previous color. What this means is that the optical steganography Image will look nearly identical to the original image. Once all this data is encoded into the image data in memory it is written back to disk with the hidden data.

This algorithm does not add a tag to show the reverse steganography algorithm where to stop and start. This would be necessary so that junk data is not extracted from the file. This algorithm does not verify the size of the document data and the image data. The max character data that can be stored in the image is:

((Length * Width * 3)/8) - (SIF).

Where Length and Width are in number of Pixels and SIF is the length in characters of the signature files appended to the data that needs to be hidden. If this is not checked errors can and will occur in the encoding and decoding of data. The things mentioned here were not implemented for one of two reasons. The first reason being the fact that some of the image saving and rewriting is far too operating system/library dependent to be included in the pseudo-code; meaning it would be cumbersome and unnecessary to include this code. Secondly some of the code was excluded because it was not the core part of the algorithm and the actual implementation of the code left out could easily be implemented in a variety of ways.

① Compress, encrypt and then hide data. This adds two layers of protection. The file name could provide the decryption key. While this method may not be perfect, it provides an additional layer of obscurity.
② Use the last two bits of every color value, resulting in greater image distortion but also a greater amount of data stored in the image. This would allow 6 bits to be stored per pixel instead of three.

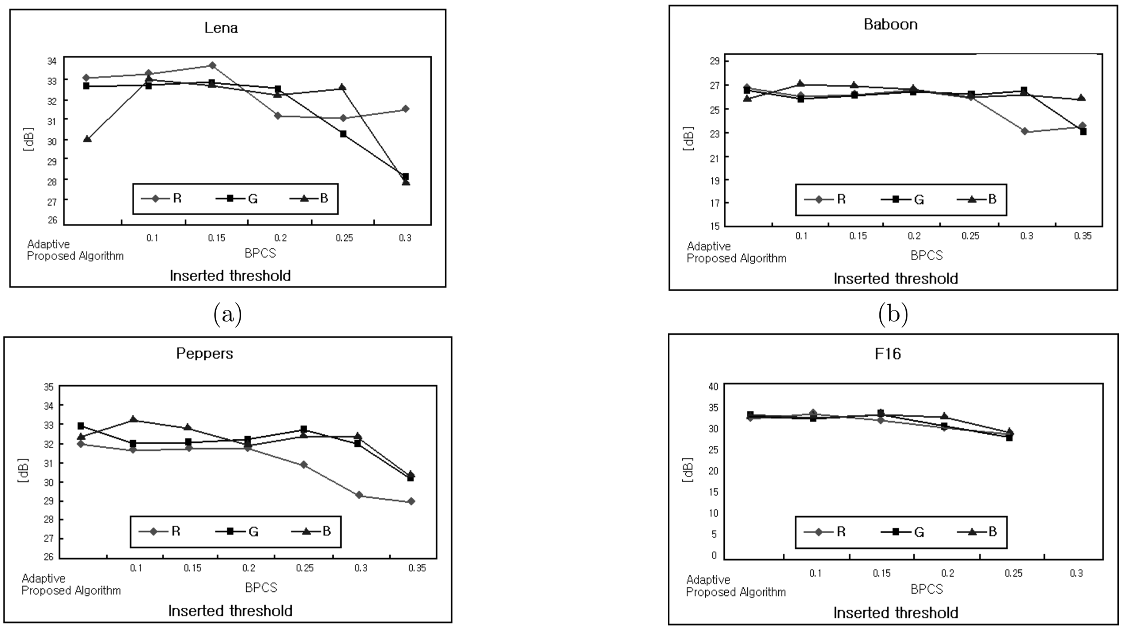
When implementing the signature information make it variable so that someone cannot randomly look through images for hidden data. Only the persons that watermarked the image would have a clue where the image data stopped and started.

IV. EXPERIMENTATION AND EVALUATION ANALYSIS

In this paper, the change of image quality and the insertion capacity have been tested using a permanent threshold of BPCS and adjustment threshold by bit-plane depending on the proposed channel. Also, the insertion capacity and image quality of the cover image were measured and tested using a similarity measurement in which the complexity of the optical image bit-plane and value of average absolute error have been used. For the experiment, the standard color images of 512 × 512 (786,432 byte) have been used and inserted information was tested with text and various images.

4.1 Estimation of image quality using insertion threshold value by each complexity of BPCS

Fig. 8 is the comparison of each channel after inserting same capacity using the proposed adjustment threshold and insertion threshold for each complexity of BPCS. In the proposed adjustment threshold method, the blue channel had relatively low PSNR compared to other channels. For the BPCS method, the PSNR of each channel was higher than the proposed method as the result of inserting to the block with complexity of 0.2 or less. However, we could see that the PSNR of each channel goes down rapidly in case of inserting information into 0.2 or greater. But for the optical image, the image cannot be judged only with PSNR by each channel. Furthermore, Figure 9 is Lena Stego image which is the result of Figure 8(a). Figures 9(b), (g) is the case of information being inserted at sections with complexity of



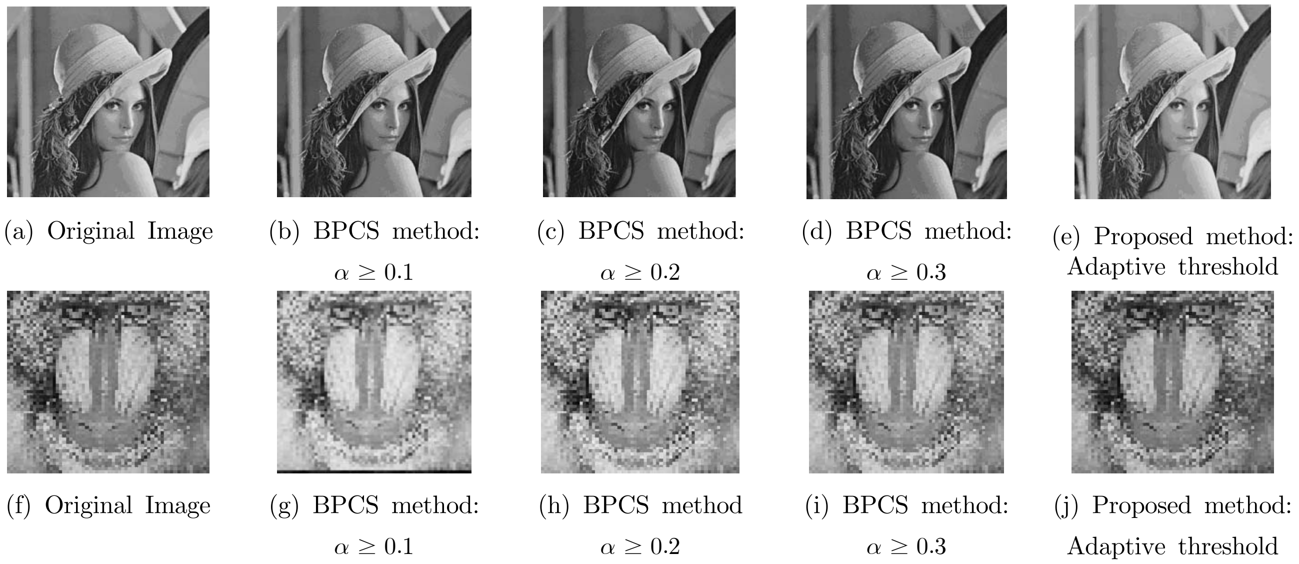
(a)

(b)

(c)

(d)

Figure 8. Comparison of image Quality by Channels Applying Proposed Adjustment Threshold Value and Permanent Threshold Value of BPCS. (a) Extract from Lena threshold value Insertion(350,000bytes); (b) Extract from Baboon threshold value Insertion(470,000bytes); (c) Extract from Peppers threshold value Insertion (370,000bytes); (d) Extract from F16 threshold value Insertion(350,000bytes).



(a) Original Image
(b) BPCS method: $\alpha \geq 0.1$
(c) BPCS method: $\alpha \geq 0.2$
(d) BPCS method: $\alpha \geq 0.3$
(e) Proposed method: Adaptive threshold
(f) Original Image
(g) BPCS method: $\alpha \geq 0.1$
(h) BPCS method $\alpha \geq 0.2$
(i) BPCS method: $\alpha \geq 0.3$
(j) Proposed method: Adaptive threshold

Figure 9. Stego Image Applying Permanent Threshold Value by Each Complexity of BPCS and Proposed Adjustment Threshold Value

Table 2. Comparison of image Quality after Inserting the Same Amount of Information

Experimentation Image	Capacity(Byte)	Channel	BPCS method		Proposed method	
			PSNR([dB])	RMS	PSNR([dB])	RMS
Baboon	400,000 (50.86%)	R	27.93	10.23	28.90	9.15
		G	28.33	9.77	31.83	6.53
		B	32.37	6.14	31.98	6.42
Lena	358,279 (45.56%)	R	32.47	6.07	33.39	5.46
		G	29.52	8.52	33.16	5.60
		B	28.58	9.50	32.51	6.04
Girl	270,499 (34.40%)	R	33.89	5.15	36.20	3.95
		G	35.39	4.34	39.87	2.59
		B	35.78	4.15	38.74	2.95
Pepper	386,422 (49.14%)	R	28.48	9.61	29.28	8.71
		G	29.20	8.84	32.48	6.01
		B	29.47	8.57	32.45	6.04
F16	316,108 (40.20%)	R	31.59	6.72	34.73	4.68
		G	31.30	6.94	34.90	4.59
		B	35.14	4.46	35.45	4.31
Tiffany	313,591 (39.88%)	R	31.9	6.48	36.99	3.61
		G	37.53	10.72	33.10	5.64
		B	29.73	8.32	33.67	5.28
Sailboat	395,892 (50.34%)	R	28.62	9.46	28.43	9.66
		G	26.86	11.57	30.92	7.25
		B	27.94	10.22	32.61	5.97
Average	348,684 (44%)	R	30.70	7.67	32.56	6.46
		G	29.73	8.67	33.75	5.46
		B	31.29	7.34	33.92	5.29

0.1 or greater and figures 9(c), (h) is the case of information being inserted at sections with complexity of 0.2 or greater.

As the result, the degradation of image quality has occurred relatively more frequently at flat areas of face and shoulders than the proposed adjustment method of figures 9(e), (j). Also, Figure 9(d) is the result of using an insertion threshold of 0.2 or greater. As the result, the degradation of image quality has occurred relatively more frequently at the border section around the pupils of eyes than the proposed adjustment of Figure 9(e). As the result of the experiment, we could see it also had influence on the channel in which information is inserted due to characteristics of the color. This shows that while the PSNR of the blue channel was relatively low in the proposed adjustment method, it is hard to recognize the difference of image quality degradation for the blue channel. Therefore, we could see that human eyesight had lower sensitivity for the blue channel than for the red or green channel.

4.2 Image inserted and estimation of image quality

Table 2 has inserted the same capacity for each cover image using the conventional BPCS method and the proposed technique. About 44% on the average has been inserted to the cover image of the experimental result. The green channel has improved the image quality by average of about 4[dB] in the method using an adjustment threshold by channel compared to the BPCS method.

As the result, red and blue channels have improved the image quality by an average of about 2[dB], 3[dB] and the as the result of the experiment, the method proposed in this paper doesn't show much change of image quality even if the capacity of the secret message becomes greater in contrast to the existing method using permanent threshold or adjustment method using

Table 3. Comparison of insertion capacity on same image quality (about 34[dB]) on the average

Experimentation Image	Capacity(Byte)	Channel	BPCS method		Capacity (Byte)	Channel	Proposed method	
			PSNR([dB])	RMS			PSNR([dB])	RMS
Lena	301,354 (38.32%)	R	35.77	4.15	358,279 (45.56%)	R	33.39	5.46
		G	32.64	5.95		G	33.16	5.60
		B	31.40	6.86		B	32.51	6.04
Pepper	325,000 (41.33%)	R	31.44	6.83	360,000 (45.78%)	R	32.16	6.29
		G	33.68	5.28		G	32.90	5.77
		B	34.58	4.76		B	34.08	5.04
Girl	225,178 (28.63%)	R	36.11	3.99	284,714 (36.20%)	R	35.65	4.21
		G	36.61	3.77		G	37.08	3.57
		B	36.13	3.98		B	35.17	4.45
Sailboat on lake	340,000 (43.23%)	R	32.60	5.98	360,500 (45.84%)	R	32.12	6.32
		G	32.98	5.72		G	32.20	6.26
		B	33.75	5.23		B	35.42	4.32
F16	277,786 (35.32%)	R	33.26	5.54	331,000 (42.09%)	R	32.58	5.99
		G	32.26	6.22		G	32.93	5.75
		B	33.81	5.20		B	33.57	5.35
Tiffany	260,746 (33.16%)	R	36.31	3.90	320,000 (40.69%)	R	35.65	4.21
		G	31.34	6.91		G	32.06	6.36
		B	32.72	5.90		B	33.38	5.46
Baboon	352,000 (44.76%)	R	32.44	6.09	360,000 (45.78%)	R	32.02	6.39
		G	32.40	6.11		G	31.83	6.53
		B	34.73	4.68		B	36.98	3.61
Couple	210,882 (26.82%)	R	35.51	4.27	261,418 (33.24%)	R	35.65	4.21
		G	35.95	4.07		G	37.08	3.57
		B	35.84	4.12		B	35.17	4.45
Average	286,618 (36.45%)		33.93	5.23	329,480 (41.90%)		33.95	5.22

variable threshold.

We confirmed that while permanent bit-plane is used or the actual image quality of the image creates serious image quality degradation, as the capacity of secret data being inserted, becomes greater in the existing spatial bit-plane insertion method. The reason is the blocks between the cover image and secret image are inserted a 1:1 ratio, at a most similar location in the method proposed in this paper. By measuring similarity of each block and the existing algorithm method, we cannot find much degradation of image quality and rather had less serious degradation of image quality, as the similarity of cover image bit-plane is greater and the image is more secret in general.

V. DISCUSSION AND CONCLUSION

In this paper, the adjustment threshold has been calculated on optical images using characteristics of bit-plane and multi-channels while applying this to propose an optical steganography method. The existing BPCS method had applied permanent threshold regardless of the channel and bit-plane. As the result, it is hard to find the optimum insertion threshold value depending on the amount of information to be inserted. Also, as a result of using same permanent threshold value for color channels, we could see the difference in degradation of image quality on optical stego image in which the information is inserted.

Therefore, the proposed research is to solve the problem of the permanent insertion threshold value applied to optical images, improve image quality and to increase the information inserting capacity.

To solve this problem, the adjustment threshold values have been applied for each channel by considering the characteristics of RGB channels and bit-planes of the optical image. While the existing optical steganography method uses permanent threshold value or inserts secret messages, there is greater degradation of image quality as the capacity of secret message.

In this experiment, the image quality and insertion capacity have been tested by applying the BPCS method and the proposed method to images such as Baboon and Lena, etc of 24 bits. The average of about 44% the capacity of the cover image has been inserted in order to evaluate the image quality by channel. As the result, the proposed method has improved the image quality by about 2~4[dB] on the average. Also, the insertion capacity has been evaluated when the image quality of stego image was about 34[dB] on the average. As the result, about 36.5% of the cover image has been inserted in the BPCS method and about 41.9% on the average has been inserted in the proposed method. Therefore, the proposed method has increased the amount of insertion by about 5.5% on the average above that of the BPCS method.

ACKNOWLEDGMENT

This Work was supported by the 2 Stage Brain Korea 21 Project in 2008. This research was supported by the Korea Science and Eng. Foundation(KOSEF) grant funded by the Korea gov. (MOST) (No.R01-2007-000-20599-0) and (No.M20809005636-08130900-63610). The circuit was designed at IC Design Center.

REFERENCES

[1] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Optical Engineering*, vol. 33, pp. 1752-1756, 1994.

[2] B. Javidi, G. S. Zhang, and J. Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," *Optical Engineering*, vol. 35, pp. 2506-2512, 1996.

[3] B. Javidi and E. Ahouzi, "Optical security system with Fourier plane encoding," *Optical Engineering*, vol. 37, pp. 6247-6255, 1998.

[4] R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," *Optical Engineering*, vol. 35, pp. 2464-2469, 1996.

[5] N. F. Johnson, Z. Duric, and S. Jajodia, "Information Hiding- Steganography and Watermarking Attacks and Countermeasures," *Kluwer Academic Publishers*, pp. 18-44, 2001.

[6] M. Niimi, H. Noda, and E. Kawaguchi, "Steganography Based on Region Segmentation with a Complexity Measure," S*ystems and Computers in Japan*, vol. 30, issue. 3, pp. 1132-1140, 1999.

[7] H. Wang and S. Wang, "Cyber warfare: Steganography vs steganalysis," *Communications of the ACM*, vol. 47, no. 10, 2004.

[8] G. K. Wallace, "The jpeg still picture compression standard," *Communications of the ACM*, vol. 34, issue. 4, pp. 30-44, 1991.

[9] K. Sherif and J. Bahram, "Information hiding technique with double phase encoding," *Appl. Opt.*, vol. 41, no. 26, pp. 5462-5470, 2002.

[10] R. Philippe and J. Bahram, "Optical image encryption using input plane and Fourier plane random encoding," *Proceeding of SPIE*, Vol. 2565, pp. 767-769, 1995.

[11] T. Nomura and B. Javidi, "Information security using digital holography," *Opt. Lett.*, vol. 25, no. 1, pp. 28-30, 2000.

[12] X. Zhou, L. Chen, and J. Shao, "Investigation of digital hologram watermarking with double binary phase encoding," *Optical Engineering*, vol. 44, 2005.

[13] R. W. Gerchberg and W. O. Saxton, "A practical algorithm for the determination of phase from image and diffraction plane pictures," *Optik*, vol. 35, pp. 237-246, 1972.

[14] E. Kawaguchi and R.. Taniguchi, "Complexity of binary pictures and image thresholding - An application of DF-Expression to the thresholding problem", *Proceedings of 8th International Conference on Pattern Recognition*,

vol. 2, pp. 1221-1225, 1986.

[15] E. Kawaguchi and R.. Taniguchi, "The DF-Expression as an image thresholding strategy", *IEEE Transactions on Systems*, Man and Cybernetics, vol. 19, no. 5, pp. 1321-1328, 1989.

[16] E. Kawaguchi and R.. Taniguchi, "Depth-First Coding for multi-valued figures using bit-plane decomposition", *IEEE Transactions on Communications*, vol. 43, no. 5, pp. 1961-1995.

[17] J. Fridrich, "A New Steganographic Method for Palette Based Images," *Proceeding of the IS&T PICS conference*, pp. 285-289, 1988.

[18] L. M. Marvel, C. G. Boncelet, Jr., and C. T. Retter, "Spread Spectrum Image Steganography," *IEEE Transactions on Image Processing*, vol. 8, no. 8, pp. 1075-1083, 1999.

[19] M. Niimi, H. Noda, and E. Kawaguchi, "An Image Embedding in Image Complexity based Region Segmentation Method," *Proceeding of International Conference on Image Processing*, vol. 3, pp. 77-77, 1977.

[20] N. F. Johnson, Z. Duric, and S. Jajodia, "Information Hiding Steganography and Watermarking Attacks and Countermeasures," *Kluwer Academic Publishers*, pp.18-44, 2001.

[21] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic systems," *Lecture Notes in Computer Science*, vol. 1768, Springer-Verlag, pp. 61-75, 2000.

[22] Sin-Joo Lee, Jae-Min Bae, and Sung-Hwan Jung, "High Capacity Image Steganography using Complexity Measure," *Proceeding of East-Asia Language Processing and Internet Information Technology*, pp. 349-352, 2002.

[23] http://funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz.