ITC 2/50

Information Technology and Control
Vol. 50 / No. 2 / 2021
pp. 264-283
DOI 10.5755/j01.itc.50.2.27461

Nested Two-Layer RGB Based Reversible Image Steganography Method

Received 2020/08/07 | Accepted after revision 2020/12/30

http://dx.doi.org/10.5755/j01.itc.50.2.27461

HOW TO CITE: Durdu, A. (2021). Nested Two-Layer RGB Based Reversible Image Steganography Method. *Information Technology and Control,* 50(2), 264-283. https://doi.org/10.5755/j01.itc.50.2.27461

Nested Two-Layer RGB Based Reversible Image Steganography Method

Ali Durdu

Faculty of Political Sciences; Department of Management Information Systems; Social Sciences University of Ankara; Turkey; phone: +90 312 596 44 75; e-mail: ali.durdu@asbu.edu.tr

Corresponding author: ali.durdu@asbu.edu.tr

In this study, a new reversible image steganography method based on Red-Green-Blue (RGB) which hides the colored image into the colored images in two layers nested is proposed. The proposed method hides the 24-bit image to be hidden by hiding two layers of data firstly in the resized version of the cover image with the LSB method, and then hides the resized cover image to the original cover image with the 4-bit method. The proposed method offers a secure communication environment as it hides the hidden image in two layers. When third parties extract data by using the LSB method, they only access the resized version of the cover image. The 4-bit method divides the image to be hidden into 8-bit segments. While the first 4 bits, which are the most important bits of 8-bit data, are hidden directly, 4 bits that can be neglected with less significance are completed by rounding at approximate value through the method function. In this way, since the 8-bit data is reduced to 4-bits, the method performs lossy hiding, but doubles the hiding capacity. Peak signal to noise ratio (PSNR), structural similarity quality criterion (SSIM) and chi-square steganalysis method, which are frequently used in the literature, are used to measure the immunity level of the proposed method. When it is concealed at the same rate with the LSB method and the proposed method, a higher measurement value is obtained in the PSNR image criterion, which is 1.2 dB, SSIM 0.0025, BER 0.0129 and NCC image criterion 0.00027. In additional, it was shown that the proposed method achieved more successful results in chi-square steganalysis and histogram tests compared to the traditional LSB method.

KEYWORDS: data hiding, steganography, two layers, nested, lossy, reversible.

1. Introduction

The security of the data transmitted in the present day is of the utmost importance especially in covid-19 coronavirus pandemic period, when only the technological communication channels are used and communication has become extremely significant. One of the most used techniques for the security of the transmitted data is encryption [15]. Encryption is often used today to secure data as it was in the past. In encryption, the presence of encrypted data is obvious and has an incomprehensible appearance. This makes the encrypted data vulnerable to all threats and attacks by third parties other than communication. Steganography, which is also adapted to today's technological possibilities and was used in the past for the transmission of hidden data without being aware of third parties, does not explicitly expose confidential data [6]. While two people communicate with the data hiding technique, it is very difficult for the third person to notice this communication. Since hidden data is not explicitly displayed, instead it is hidden inside an innocent cover. Thus, third parties other than communication cannot notice communication. The technique that hides data into the least significant bit, LSB (Least Significant Bit), which is one of the data hiding techniques, is frequently used [31].

The methods that follow the statistical traces left by the hiding process to discover and reveal the data hidden by the data hiding techniques are called steganalysis methods [6]. Steganalysis methods which are used to analyze hidden data target the cover medium which is the communication channel. Staganalysis methods that follow the traces of hiding in the data carrier cover environment are designed to prevent malicious use [7].

In steganography, the hidden message is hidden in a carrier medium and transmitted to the other party. On the other hand, after obtaining the carrier's environment, it extracts according to the hiding algorithm. For the actualization extraction process, the hiding algorithm must be known. Steganography methods are classified under four main titles according to the algorithm, hiding environment, security and retrieval features [6]. Steganography is divided into the bit and frequency space according to algorithm methods, image, sound, video and text according to hiding environments, durable and fragile according to security features, and reversible and non-reversible according to removal methods [6]. In the proposed method, bit space as the algorithm type, image as hiding medium and steganography method that does not require a carrier medium as extraction methods are used. The fact that the original cover file is not needed in the extraction method is called reversible and this is very important for the communication not to be noticed. It is also sufficient to transfer a single file to the other party for communication. In non-reversible methods, the original cover file and the stego file should be transmitted to the other party together. This may cause hidden data to be noticed.

Steganography method is used for different purposes besides hiding data and these methods are called watermark [12]. A hidden mark that is not noticed in digital watermarking methods is added to digital multimedia data (image, video, sound and text) and remains hidden for the life of the content by marking it with a mark called watermark [9]. Watermarking methods are used in the content for purposes such as copyright protection, data validation, and data ownership control [9].

In bit space methods, the least important bit is used to hide data [6]. The data to be hidden in bit space methods are converted into two bits and hidden in the carrier environment. When the least significant bit of each byte of data in the carrier medium is changed, there is no change in the carrier image that can be perceived by the human eye. The bit space method is based on the data hiding in the resulting space by making use of neglecting the most insignificant bit. LSB method is the most commonly used method in the bit space method [23].

Another method that hides data by using bit space is the matching method [6]. In the matching method, as in the LSB method, the last bits are not directly changed. Instead, if the least significant bit does not have the same value as the bit to be hidden, the corresponding byte is increased or decreased by 1, and the same value does not change. The matching method was first proposed by Sharp [28]. Sharp [28] uses the key sequence to create random sequences in his proposed method. Sharp [28] encrypts hidden data by using the stego key array and hides it in the carrier medium. Mielikainen [22] develops the method proposed by Sharp [28] and does the hiding process according to the result of the function. According to the method, the carrier image is divided into pairs of pixels. The hidden information is hidden in two-bit groups. The first bit to be hidden is hidden directly to the last bit of the first pixel. The second bit is obtained by the conclusion of the hiding function of the last bits of the pixel pair. Chan [2] proposes a similar method by developing the method proposed by Mielikainen [22]. The method hides data from two consecutive pixels in the image by applying the XOR method on the LSB bit of the first pixel and the previous bit of the second pixel, as in the method proposed by Mielikainen. Tian [34] proposes a new reversible data hiding method by using the matching method. In his proposed method, Tian [34] hides data into the region by doubling the difference between the two pixels of the carrier image. Alatlar [1] develops the method proposed by Tian and hides the 3-bit data into the region by doubling the difference between four pixels. In the method they propose, Chang et al. [3] create the carrier image twice and hide the data in two images by using the module matrix and the direction of change. Lu et al. [18] propose an alternative method called camouflage pixels by developing the method proposed by Chang [3]. Ker [13] uses three pixels to hide two bits of data with 2/3 efficient hiding method. Wu and Tsai [41] propose a new method which hides data by the pixel difference between consecutive pixels. Wang et al. [38] improve the method proposed by Wu and Tsai [41] and hide data by the result of the module function of the difference between the two pixels. Fridrich and Soukal [8] propose a method that offers high data hiding capacity by using the hamming matrix. Kurtuldu and Arıca [16] hide the message data to be hidden in their work, which they call the image squares method, to the pixel group with the sequence closest to the message data to be hidden according to the sequences of the last bits of the block pixels. Doğan [4] proposes a method of data hiding based on the genetic algorithm by using chaotic maps. In another study, Doğan [5] proposes a reversible data hiding method based on the graphic block neighborhood level. Tuncer et al. [37] propose a new method of data hiding for binary images which is inspired by the minefield game.

There are many studies in the literature on watermarking methods. In another study, Tuncer [36] proposes a watermarking method for image authentication. Based on the pixel difference method proposed by Wu and Tsai [41], Prasad and Pal [25] develop a data hiding method for RGB-based images. Thiagarajan et al. [33] propose a new data hiding method based on bit space for RGB images. Hwang et al. [11] hide data by compressing the stego image lossily to reduce the image size. Yang & Wang [42] propose a smart pixel-adjustment block-based data hiding method for color images. Mandal & Das [20] propose a new data hiding method by using adaptive pixel value differencing. In his study, Swain [30] proposes adaptive pixel value differencing steganography by using both vertical and horizontal edges. Sneha et al. proposed an encryption algorithm based on chaos using Walsh-Hadamard transform and chaotic maps to encrypt images [29]. In addition, images were processed on a channel basis and two different chaotic maps called Arnold and Tent maps were used for encryption. Thakur et al. proposed a chaotic-based safe medical image watermarking approach in their study [32]. Their proposed method used non-subsampled contourlet transform (NSCT), redundant discrete wavelet transform (RDWT) and singular value decomposition (SVD) for imperceptibility and robustness. Ramasamy et al. proposed an advanced logistic map (ELM) method using chaotic maps and simple encryption techniques such as block scrambling, modified zigzag transformation for encryption phases, including permutation, diffusion, and key stream generation for secure transfer of images [27]. Tsai et al. proposed a reversible image hiding scheme based on histogram shifting for medical images [35]. Luo et al. They proposed a new reversible watermarking scheme that uses an interpolation technique that can embed large amounts of hidden data into images with imperceptible changes. [19]. In the Liu and Shan studies, Luo et al. They solved the problem of not being the opposite by improving their proposed study and proposed a reversible concealment method [17].

In this study, a new RGB-based reversible steganography method, which hides the colored image into the colored images in two layers, is proposed. The proposed method hides the 24-bit image to be hidden by hiding two layers of data firstly in the resized version of the cover image with the LSB method, and then hides the resized cover image to the original cover image with the 4-bit method. The proposed method offers a secure communication environment as it hides the hidden image in two layers. The novelty of the proposed method is that it provides a secure communication environment as it hides the hidden image in two layers. The proposed method uses the 4-bit hiding method to hide the second layer. Therefore, data extraction from the second layer cannot be done without knowing the 4-bit method. The proposed method provides security in three stages. First, it hides data in a two-layer architecture. Secondly, by making 4-bit obfuscation to the second layer, the target obfuscates and made the decoding process difficult. Thirdly, instead of hiding the grayscale image, it hides the RGB image, making it difficult for third parties to decipher the proposed method. In section 2, the proposed method, in section 3, experimental studies to evaluate the performance of the proposed method and in section 4, the results are given.

2. The Proposed Method

The proposed method hides the 24-bit color image into two layers with two layers. While layer 1 is hidden with LSB method, layer 2 is hidden with 4-bit data hiding. The proposed method provides a safe environment with two layers to the hidden image.

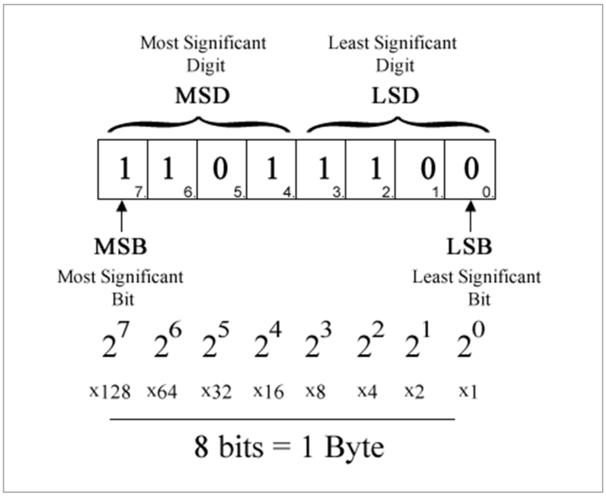
2.1. Least Significant Bit Method

In bit space methods, the least significant bits are used to hide data [6]. The data to be hidden in the LSB method is converted into two bits and hidden in the carrier medium. When the least significant bit of each byte of data in the carrier medium is changed, there is no change in the carrier image that can be perceived by the human eye. The LSB method is based on hiding the data in the area created by making use of neglecting the most insignificant bit. LSB method is the most commonly used method in bit space methods [6].

In the LSB method, each bit of hidden data is hidden in the last bit in each byte of the carrier medium. In Figure 1, the internal structure of 1-byte data is shown and there are 8 bits in 1-byte. Each of these 8 bits has a different bit valences. The bits are numbered from 0 to 7 according to their valence. The value of one bit is obtained by multiplying the bit value by the bit number of 2. The 7th bit is called the most significant bit (MSB) because it is the highest-valued bit, and the 0th bit is called the least significant bit (LSB) because it is the lowest-valued bit [24]. In Figure 2, the total of 1-byte data bit value is $1*2^7 + 1*2^6 + 0*2^5 + 1*2^4 + 1*2^3 + 1*2^2 + 0*2^1 + 0*2^0 = 220$. Accordingly, while the bit value of the 7th bit is 128, the bit value of the 0th bit is 0. The bit number is called four bits of 7 to 4, the highest-valued bit group is the most significant digit (MSD), the four bits of 3 to 0 are the least-valued bit group, the least significant digit (LSD). The bit-value sum of the MSD bits is 208 while the bit-value sum of the LSD bits is 12. When the sum of the bit values is considered, the MSD bits are of high importance, while the LSD bits have a negligible low value.

Figure 1

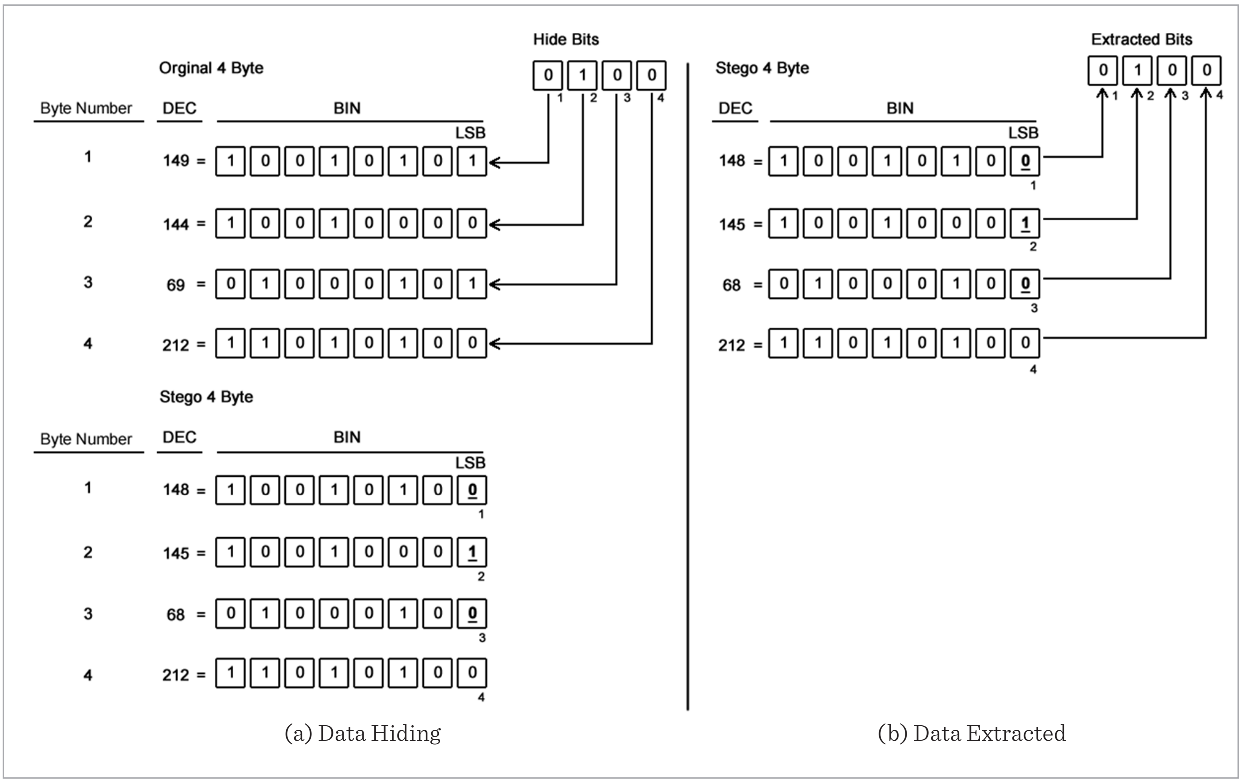
Internal structure of 1-byte data



In Figure 2, hiding 4 bits into 4-byte original data and extracting it from there with the LSB method is shown. Figure 2.a shows the data hiding process with the LSB method. In Figure 2.a, 8 bit binary contents of the original 4-byte data and corresponding decimal number values are given. The decimal number values of the original 4-byte are 149, 144, 69 and 212, respectively. The binary value of the 4-bit data to be hidden in Figure 2.a is 0100_2. The LSB bits which are the last bit of each byte are shown. All bits from the 1st bit to the 4th bit are hidden in the last bits (LSB) of the original bytes respectively. As a result of hiding, stego 4 bytes in Figure 2.a occurs. The LSB bits varying to Stego 4 bytes are underlined. While the last bit of the 1st byte of the original bytes is 1, the result of data hiding becomes 0. While the last bit of the 2nd byte is 0, it is 1; while the last bit of the 3rd byte is 0, the last bits of the 4th and 0th byte are not changed. As a result of hiding data with the LSB method, some bits change while some bits do not. As a result of the hiding, the value of

Figure 2

Hiding and extracting data with LSB method a) Hiding data b) Extracting data



(a) Data Hiding

(b) Data Extracted

the original 1st byte is changed from 149 to 148, the 2nd byte is changed from 144 to 145, the 3rd byte is changed from 69 to 68 and the 4th byte is not changed.

Figure 2.b shows data extraction by using the LSB method. From the last bits of the stego 4 bytes, hidden data is extracted from the 1st byte respectively. Firstly, the last bit of the 1st byte is extracted as 0. Then the last bit of the 2nd byte is extracted as 1, the last bit of the 3rd byte is extracted as 0 and the last bit of the 4th byte is extracted as 0. At the end of the process, 4-bit binary data is extracted as 0100_2. 1/8 of data can be hidden to an image with the LSB method. This is because there are 8 bits in each byte, and only 1 bit of data can be hidden in the last bit of each byte.

2.2. 4-bit Data Hiding Method

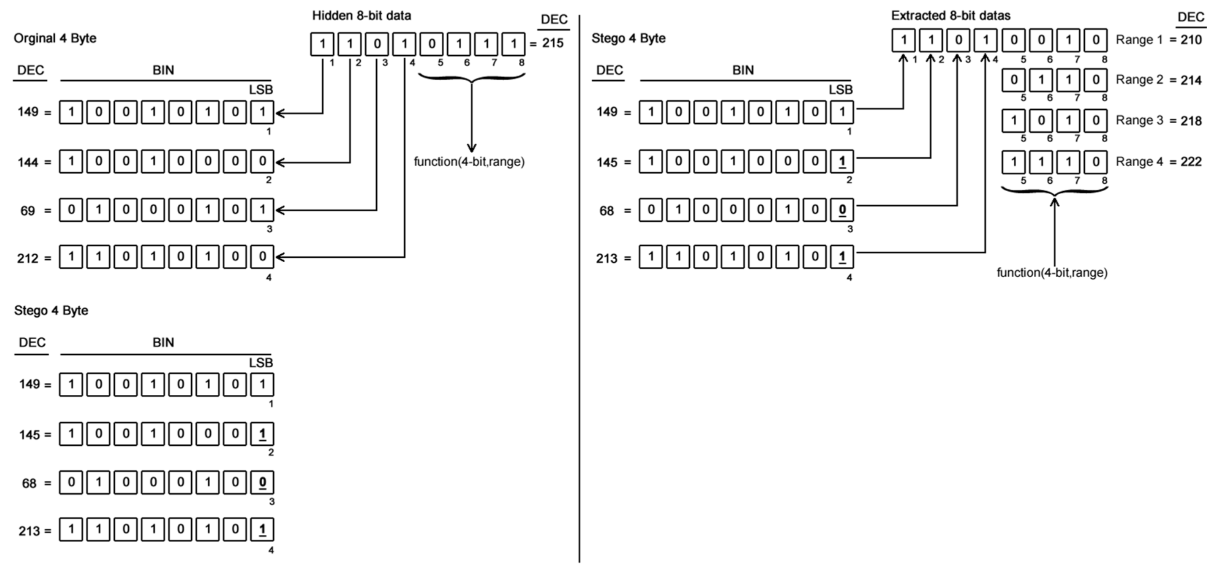
The main motivation for the development of the 4-bit data hiding method is that the small tone changes that occur in the pixels in 24-bit color images with RGB color coding do not create perceptible distortions in the general view of the picture. Small changes in the colored picture to be hidden based on this principle do not cause any change in the image of the picture transmitted to the other person which can be perceived by the human eye. In the hidden image, each pixel contains 3 bytes of information: Red (1-byte), Green (1-byte), Blue (1-byte) channels [14]. Each channel has 8 bits of information. While hiding, the first 4 bits, which are the most important bits of the 8-bit data in each channel, are hidden with the LSB method, while the less important 4 bits that can be neglected are not hidden and are rounded up by the function. In the 4-bit data hiding method, the picture can be hidden inside the picture. The losses resulting from the extraction of the hidden picture are not in a way that can greatly affect the picture obtained. Since 4-bit hiding hides the first 4 bits with the LSB method, 1-byte hides a significant part of the data without loss. In Figure 8, the images hidden and extracted with the suggested method are given. The proposed method hides in the 2nd layer with the 4-bit method. As can be seen in Figure 8, there are no visible changes in the hidden image.

In Figure 3, hiding and extracting 8 bits to 4-byte original data with 4-bit data hiding method is shown. Unlike the LSB method, the 4-bit method hides 8 bits of data in 4 bytes, and accordingly, the 4-bit method can hide twice the data according to the LSB method. Figure 3.a shows the data hiding process with the 4-bit method. In Figure 3.a, the 8-bit binary content of the original 4-byte data and the corresponding decimal number values are given. The binary value of the 8-bit data to be hidden in Figure 3.a is 11010111_2. LSB bits, the last bit of each byte, are shown. MSD bits from 1st to 4th bits are hidden to the last bits (LSB) of the original bytes respectively. LSD bits, which are 4-bit between 5th and 8th bit, are directed to the function. As a result of hiding, stego in Figure 3.a consists of 4 bytes. Stego LSB bits varying in 4 bytes are underlined. As a result of hiding of the first byte from the original bytes, no data change occurred. While the last bit of the 2nd byte is 0, it is 1, the last bit of the 3rd byte is 1, it is 0 and the last bit of the 4th byte is 0, it is 1. There have been 3 bit changes in the 8-bit data hiding process.

Figure 3.b shows the data extraction process with the 4-bit method. From the last bits of Stego 4 bytes, hidden data is extracted from the 1st byte respectively. Firstly, the last bit of the 1st byte is extracted as 1. Then the last bit of the 2nd byte is extracted as 1, the last bit of the 3rd byte is extracted as 0 and the last bit of the 4th byte is extracted as 1. At the end of the process, the MSD bits 1101_2 of the hidden 8-bit are extracted. The remaining 4-bit LSD bits are extracted via the function. According to the range value, the function returns 4-bit data. Accordingly, 4-bit data is returned when the range value 1 is 0010_2, 2 is 0110_2, 3 is 1010_2 and 4 is 1110_2. LSD bits are less important in 4-bit data hiding which is completed by the function with approximate value. According to four different range values, the secret data has 215 decimal values, and the data that extracted has a value of 210 when the range value is 1, 214 when it is 2, 218 when it is 3, and 222 when it is 4. In all range values, values close to hidden data are obtained. The closest value is 214 with 1 difference when the range value is 2. The image hidden by the method suggested in Figure 8 has been removed with four different range values. The images extracted in Figure 8 were analyzed with image criteria and the results are given in Table 1. When the results were examined, more successful results were obtained than the image criteria when the range value was 2. In general, it gives the most successful result when the range value is 2 in the subtraction process in all images. This is be-

Figure 3

Hiding and extracting data with 4-bit data hiding method a) Hiding data b) Extracting data



(a) Data Hiding

(b) Data Extracted

cause range value is the middle value of 2, and because it is the middle value, the byte value extracted in the 4-bit suppression function contains the value closest to the original byte value.

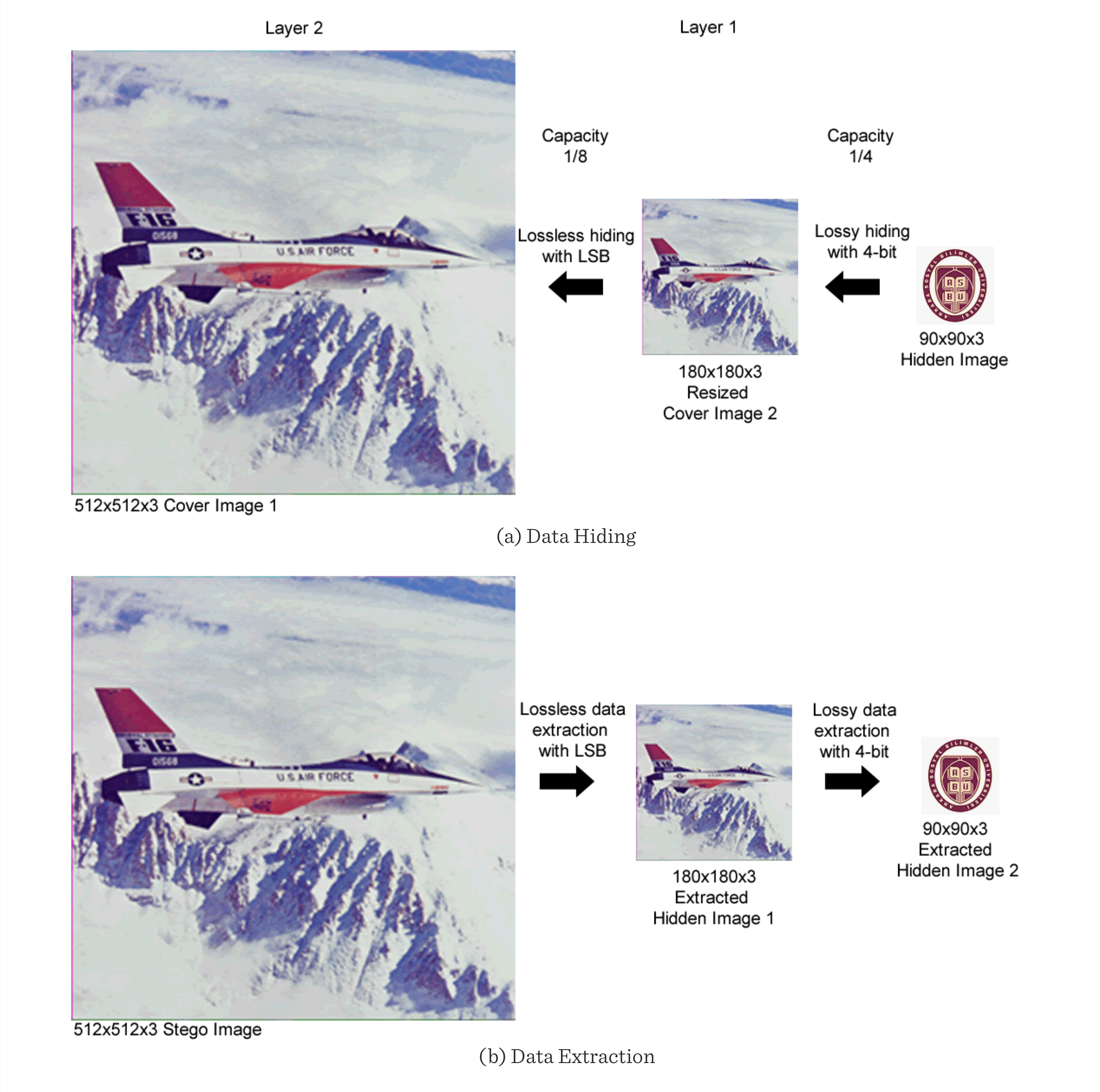
2.3. Hiding and Extracting Data with the Proposed Method

The proposed method hides the 24-bit color0020image into the 24-bit color image with nested two layers. The two layers provide a safe environment for the hidden image.

The 90x90x3 hidden image is hidden into the 512x512x3 size Lena image of the method suggested in Figure 4 and extracted from it. The proposed method hides the hidden image in two layers. In Figure 4.a, firstly, the hidden image in 90x90x3 size is hidden in resized cover image 2 (Layer 1) which is 0.35 resized version of the original cover image by 4-bit hiding meth-

Figure 4

Hiding and extracting data with the proposed method a) Hiding data b) Extracting data


Layer 2
Layer 1
Capacity 1/8
Capacity 1/4
Lossless hiding with LSB
Lossy hiding with 4-bit
90x90x3 Hidden Image
180x180x3 Resized Cover Image 2
512x512x3 Cover Image 1
Lossless data extraction with LSB
Lossy data extraction with 4-bit
180x180x3 Extracted Hidden Image 1
90x90x3 Extracted Hidden Image 2
512x512x3 Stego Image

(a) Data Hiding

(b) Data Extraction

od. In the LSB method, the image $\frac{512}{\sqrt{8}}\times\frac{512}{\sqrt{8}}$ = 180x180, in the proportion of 1/8 and in the size of $\frac{1}{\sqrt{8}}$ = 35%, can be hidden in the 512x512 image. In the figures in the article, square images are preferred in order to understand the method easily. At this stage, the 4-bit hiding method provides 1/4 capacity capabilities. $\frac{180}{\sqrt{4}}\times\frac{180}{\sqrt{4}}$ = 90x90, size can be hidden according to the size of the cover image in the 1st layer. Secondly, cover image 2 in the 1st layer of 180x180x3 size, which has a hidden image in it, is hidden in cover image 1 (Layer 2) with the size of 512x512x3. Lossless hiding is done with the LSB method to the 2nd layer. The reason for doing lossless hiding at this stage is that the information in the 1st layer should be completely extracted. Loss hiding in layer 2 causes meaningful bits (MSD) in layer 1 to disappear.

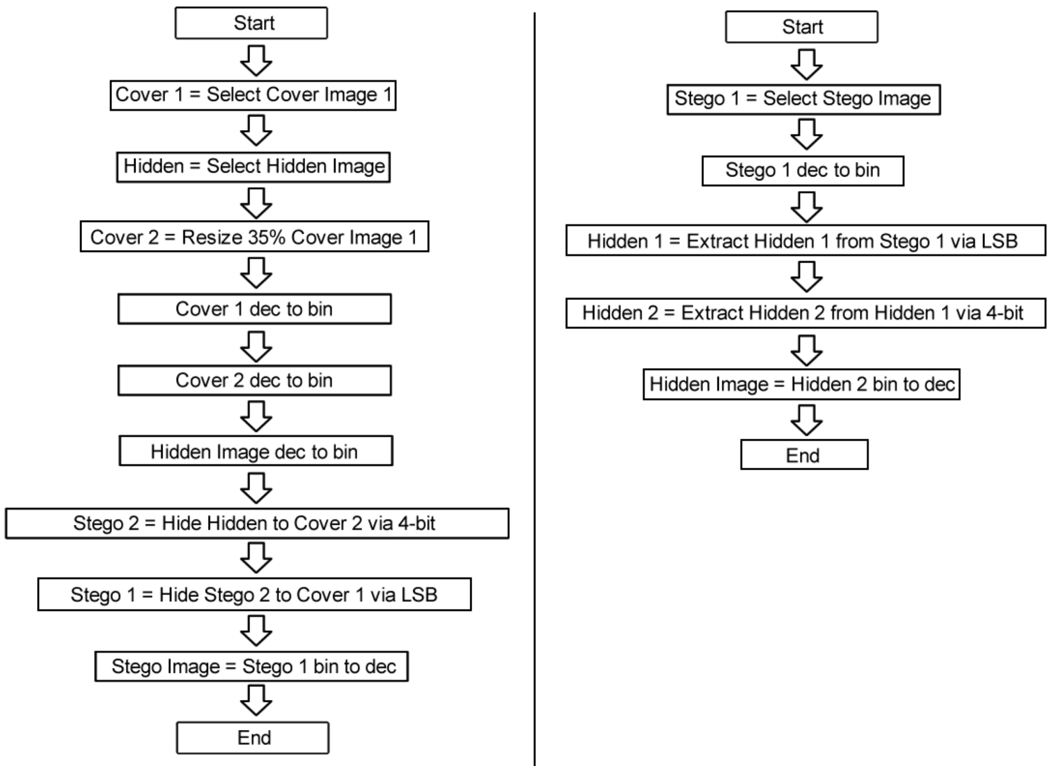
With the 4-bit lossy hiding method, only MSD bits are hidden, and LSD bits are completed by the function at approximate value. When 4-bit hiding is done in the 2nd layer, the hidden image inside the 1st layer causes the MSD bits to be lost. With the LSB method, 1/8 capacity is obtained.

Data extraction was performed with the method suggested in Figure 4.b. There are two images hidden inside each other in 512x512x3 stego image. In the extraction process, first, the lossless data is extracted from the 2nd layer, 512x512x3 stego image by using the LSB method and 180x80x3 1st hidden image (Layer 2) is obtained. Secondly, the lossy 90x90x3 2st hidden image is extracted from the 2nd layer by 4-bit method. Thus, the real hidden image is extracted. Third parties who listen to the communication between the two parties can access the image in layer 2 instead of the hidden image when they extract data by using the LSB method to decipher the communication. Thus, it is more difficult to reach the true hidden image.

Flow charts of the two-layer data hiding method proposed in Figure 5 are given. According to the data hiding flow chart of the data hiding method proposed in Figure 5.a, Cover Image 1 (Layer 2) and hidden image

Figure 5

Flow charts of the proposed method a) data hiding b) data extraction


Start
Cover 1 = Select Cover Image 1
Hidden = Select Hidden Image
Cover 2 = Resize 35% Cover Image 1
Cover 1 dec to bin
Cover 2 dec to bin
Hidden Image dec to bin
Stego 2 = Hide Hidden to Cover 2 via 4-bit
Stego 1 = Hide Stego 2 to Cover 1 via LSB
Stego Image = Stego 1 bin to dec
End
Start
Stego 1 = Select Stego Image
Stego 1 dec to bin
Hidden 1 = Extract Hidden 1 from Stego 1 via LSB
Hidden 2 = Extract Hidden 2 from Hidden 1 via 4-bit
Hidden Image = Hidden 2 bin to dec
End

(a) Data Hiding

(b) Data Extraction

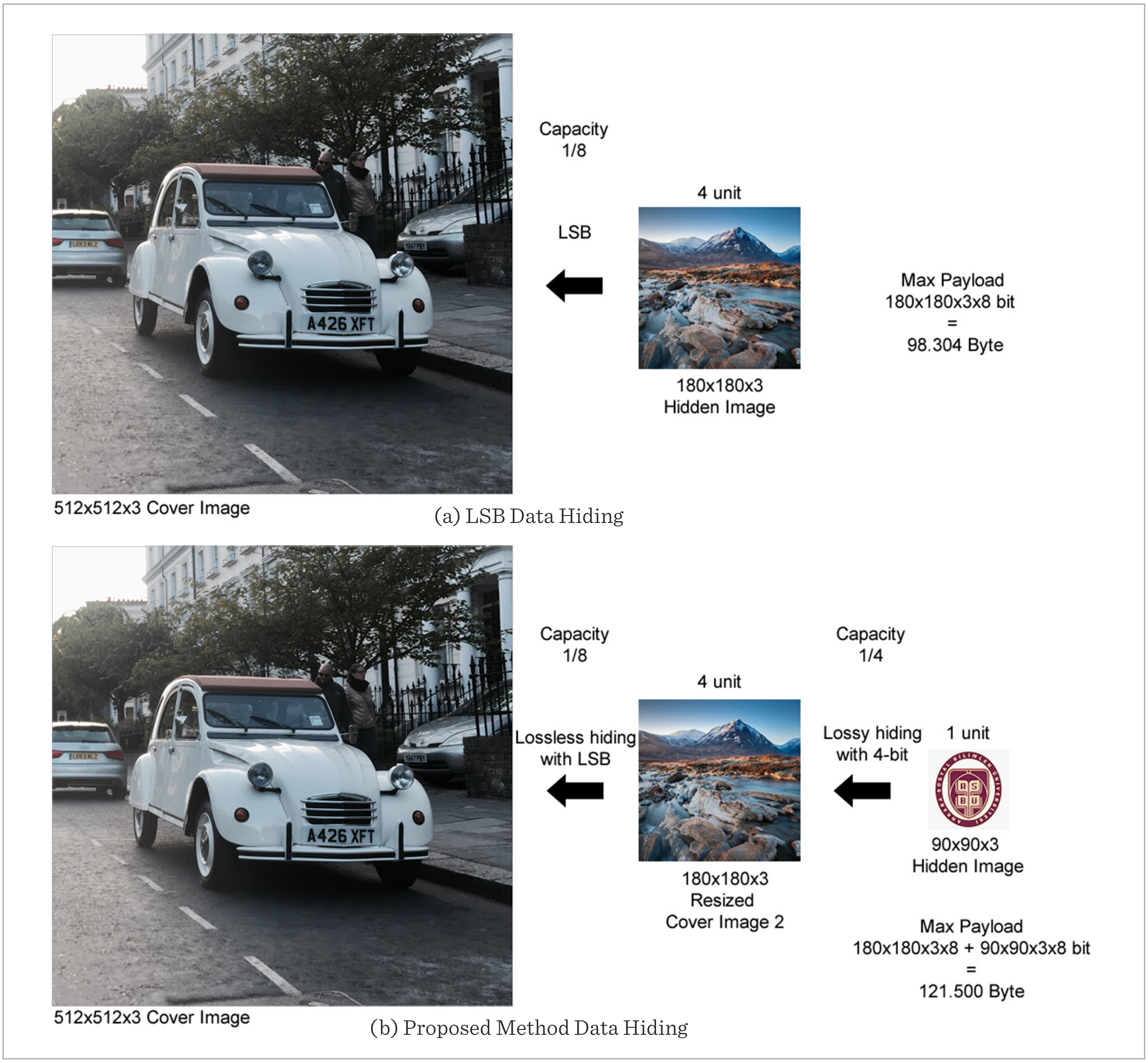
are selected first. Later Cover Image 1 is reduced by 35% to obtain Cover Image 2 (Layer 1). Then, it is converted from Cover 1, Cover 2 and Hidden decimal number system to binary number system respectively. The hidden image is hidden in the Cover 2 image via 4-bit. The image of Stego 2 formed as a result of the 1st hiding is hidden in the Cover 1 image. The resulting Stego 1 image is converted from the binary number system to the decimal number system and a nested hidden Stego Image is obtained due to this conversion.

In the method proposed in Figure 5.b, the flow diagram of data extraction from stego image is given. First, Stego Image 1 is selected and converted from decimal number to binary number. Then, by using LSB method, Stego Image 1 (Layer 2) hidden image is extracted and Hidden 1 (Layer 1) is obtained. Hidden 2 as lossy, is extracted from the Hidden 1 image with 4-bit method. Since Hidden 2 is extracted as binary, Hidden Image is obtained by converting it to decimal number system.

Data hiding capacities are visualized with LSB and the recommended method and are given in Figure 6. A 24-bit colored Cover image with dimensions of 512x512x3 in Figure 6.a can be hidden by LSB method with 24 images ($\frac{512}{\sqrt{8}}$x$\frac{512}{\sqrt{8}}$x3=180x180x3), at $\frac{1}{8}$ ratio $\frac{1}{\sqrt{8}}$ = 35%.

Figure 6

Comparison of data hiding capacities with LSB and the proposed method



(a) LSB Data Hiding

(b) Proposed Method Data Hiding

Accordingly, 180*180*3*8 = 777.600 bits = 97.200 bytes of data can be hidden with the LSB method. With the proposed method, 180x180x3 images can be hidden to the 1st layer (Cover image) with the LSB method, and 90x90x3 images at the rate of ¼ to the 2nd layer (Resized Cover image) with the 4-bit method. Accordingly, 90*90*3*8 = 194.400 bits = 24.300 bytes of data can be hidden in a 24-bit image of 180x180x3 dimensions with the 4-bit method. As a result, 121.500 bytes of data in total can be hidden with the proposed method. The proposed method hides an extra 24.300 bytes of data in addition to the LSB method. According to the numerical data, 4 units of data can be hidden with the LSB method, while 5 units of data can be hidden with the proposed method. According to this result, the proposed method hides 25% more data than the LSB method. However, in order to strengthen the security, the proposed method hides the cover image inside the cover and this reduces the hiding area that can be used. In this respect, a 24-bit image of 512x512x3 size and a 24-bit secret image of 90x90x3 size can be safely hidden with the recommended method.

The maximum computational complexity in terms of Big O representation of the algorithm of the proposed method is given in Equation 1.

$$\text{Computation complexity} = O(25+31\times n+11+46\times n+9) = O(77\times n+45) = O(77n) \quad (1)$$

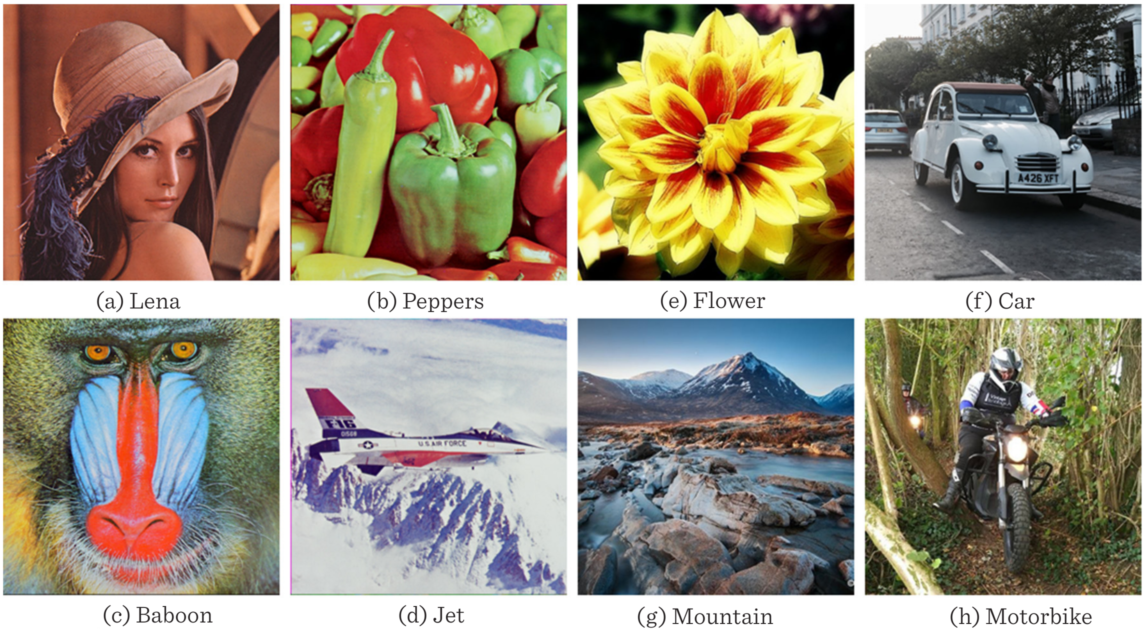
The algorithm of the proposed method. Computational complexity is calculated as 77n+45. In Big O notation, since constant numbers are ignored, when the constant 45 is ignored, the computational complexity is found to be 77n. Considering the computational complexity, it is seen that the proposed method has low computational complexity and high performance as an algorithm.

3. Experimental Studies

In order to measure the performance of data hiding methods, image criteria and steganalysis methods are used. Lena, Pepper, Baboon, Jet, Flower, Car, Mountain and Motorbike carrier images, which are frequently used in the 24-bit color literature in 512 x 512 x 3 dimensions in Figure 7, are used to test the performance of the proposed hiding method. To test the perceptibility of the proposed method, six image quality index, which are frequently used in the literature, were used. These are MSE (Mean Square Error) [10],

Figure 7

512x512x3 Original Test Images a) Lena b) Peppers c) Baboon d) Jet e) Flower f) Car g) Mountain h) Motorbike



PSNR (Peak Signal to Noise Ratio) [10], SSIM (Structural Similarity) [10] [40], UQI (Universal Quality Index) [39], Bit Error Rate (BER) [26], Normalized Cross Correlation (NCC) [42] were used. In addition, histogram and chi-square steganalysis methods are used to measure the resistance of the proposed method to steganalysis algorithms.

In order to measure the distortions in the cover images, the mean square error (MSE) given in Equation 2 and the peak signal noise ratio (PSNR) quality criteria given in Equation 3 are used. In Equation 2, m and n represent line and column information of images; O represents original cover image; S represents the stego image. After the MSE value is calculated, the next step is PSNR calculation. PSNR is an image criterion that measures the similarity ratio between the cover image and the stego image. In Equation 3, MAX is the maximum value that a pixel can take and it is usually 255. SSIM quality criteria are given in Equation 4. In SSIM quality criterion, quality index is calculated by taking into consideration the similarities between X and Y vector. In Equation 4, X represents the original carrier image and Y represents the data hidden image. In order to show the sizes of the hidden data, the unit of bits per pixel (bpp) given in Equation 5 is used. The number of bits per pixel in Equation 5 is calculated by the ratio of the number of bits used in the hiding process in the image to the total number of bits in the image. Equation of UQI image criterion, which makes quality analysis between two images, is given in Equation 6. In Equation 7, the definition equation of NCC image criterion analyzing the original image and the stego image is given.

$$MSE=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[O(i,j)-S(i,j)]^2 \tag{2}$$

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{3}$$

$$SSIM(x,y)=\frac{(2\mu x\mu y+C1)(2\sigma xy+C2)}{(\mu 2x+\mu 2y+C1)(\sigma 2x+\sigma 2y+C2)} \tag{4}$$

$$Bpp = \frac{\text{Number of Hidden Bit}}{\text{Total Number of Bits}} \tag{5}$$

$$UQI = \frac{4\sigma_{xy}\overline{xy}}{\left(\sigma_x^2+\sigma_y^2\right)\left[(\overline{x})^2+(\overline{y})^2\right]} \tag{6}$$

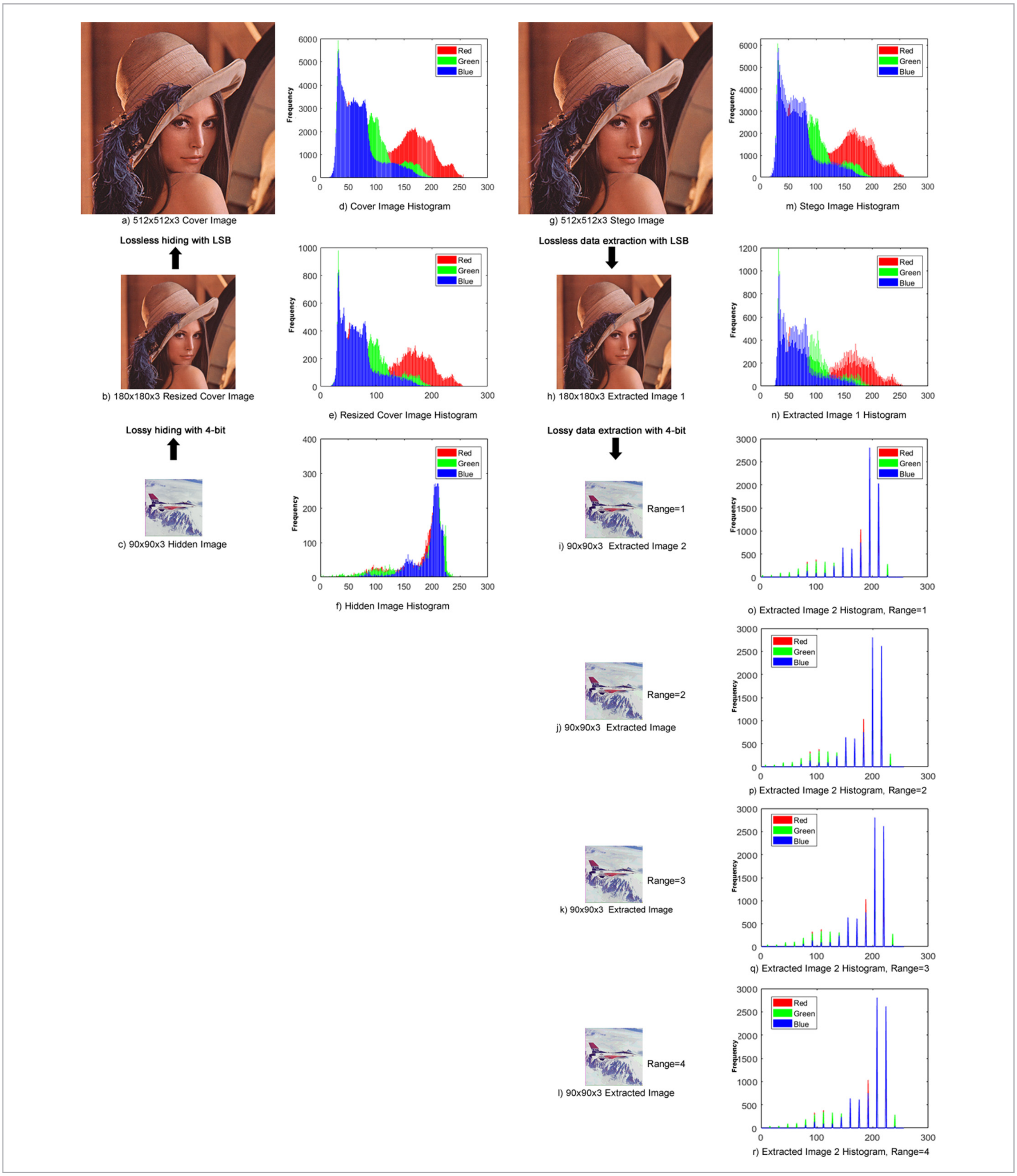
$$NCC = \sum_{i=1}^{m}\sum_{i=1}^{n}\frac{\left(A_{ij}\times B_{yj}\right)}{A_{ij}^2} \tag{7}$$

90x90x3 size Jet hidden image in Figure 8.c is hidden in the original Lena cover image of 512x512x3 size in Figure 8.a by the proposed hiding method. In the proposed data hiding process, it is first converted to the size of 180x180x3 in Figure 8.b by resizing the cover image in Figure 8.a by 35.15%. Then, the hidden image in Figure 8.c is first hidden to the resized cover image in Figure 8.b lossily by 4-bit hiding method. Afterwards, the image of Figure 8.c and the hidden image of Figure 8.b are hidden in the cover image in Figure 8.a without any loss by LSB method. As a result of hiding, stego Lena image is given in Figure 8.g. As a result of data extraction with the proposed method, 180x180x3 size extracted image 1, which is recovered by LSB method, is given in Figure 8.h. The extracted image is the same as the original cover image. In this way, the 1st security layer is created. If the hiding process is discovered by third parties, only the image in Figure 8.h is obtained in the extraction operation with the frequently used LSB method. To extract the hidden image, the hidden image should be extracted from the image in Figure 8.h by knowing the correct hiding algorithm. Thus, the 2nd security layer is created in this way. In Figure 8.i, j, k and 1, the original hidden images in the size of 90x90x3 are given which are extracted from the extracted image 1 in Figure 8.h lossily with the values of range 1, 2, 3 and 4, respectively. Depending on the range values, extraction operations are performed with different bit interval values. The four images recovered in Figure 8.i, j, k, and l do not show any visible differences, except for image distortion caused by loss of data hiding. All extracted images have the same appearance as the original hidden image.

The RGB histograms of original and stego images are given in Figure 8.d and m. When two histograms are examined, it is seen that data hiding does not make a noticeable change in the cover image. Histograms of the resized cover image and extracted image 1 are given in Figure 8.e and n. When the two histograms are examined, there is no difference in the histograms of the image hidden and the image extracted. In Figure 8.f and Figure 8.o, p, q, and r, 90x90x3 hidden Jet image and histograms of the lossy extracted images from 1 with the values of range 1, 2, 3 and 4, respectively, are given. When the histograms are examined, since the hiding process is hidden with 4-bit loss, the his-

Figure 8

Hiding data with the proposed method and extracting data with different range values and RGB Histograms a) 512x512x3 Cover Image b) 180x180x3 Resized Cover Image c) 90x90x3 Hidden Image d) Cover Image Histogram e) Resized Cover Image Histogram f) Hidden Image Histogram g) 512x512x3 Stego Image h) 180x180x3 Extracted Image 1 i) 90x90x3 Extracted Image 2, Range = 1 j) Extracted Image 2, Range = 2 k) Extracted Image 2, Range = 3 l) Extracted Image 2, Range = 4 m) Stego Image Histogram n) Extracted Image 1 Histogram o) Extracted Image 2 Histogram, Range = 1 p) Extracted Image 2 Histogram, Range = 2 q) Extracted Image 2 Histogram, Range = 3 r) Extracted Image 2 Histogram, Range = 4



a) 512x512x3 Cover Image

d) Cover Image Histogram

g) 512x512x3 Stego Image

m) Stego Image Histogram

b) 180x180x3 Resized Cover Image

e) Resized Cover Image Histogram

h) 180x180x3 Extracted Image 1

n) Extracted Image 1 Histogram

c) 90x90x3 Hidden Image

f) Hidden Image Histogram

i) 90x90x3 Extracted Image 2

o) Extracted Image 2 Histogram, Range=1

j) 90x90x3 Extracted Image

p) Extracted Image 2 Histogram, Range=2

k) 90x90x3 Extracted Image

q) Extracted Image 2 Histogram, Range=3

l) 90x90x3 Extracted Image

r) Extracted Image 2 Histogram, Range=4

tograms of the extracted images have similarities and differences with the histogram of the hidden image. Histograms in all range values also have minor differences. Although histograms perform the same movements as the histogram of the hidden image, the frequency ranges are sparse as there is lossy hiding. The results show that the original hidden image is hidden by 2 layers of security and the hidden image is successfully obtained as a result of the extraction process.

Image quality index results of the proposed method and the previous study [6] to compare the original, stego Lena images in Figure 8 and extracted images with different range values with the original image are given in Table 1. In the proposed method, 0.49 MSE, 51.19 dB PSNR, 0.99914 SSIM, 1 UQI, 0.0617 BER and 0.0012 NCC values were obtained in the original and stego Lena images in Figures 8.a and g, while in the previous study [6] 51.06 dB PSNR and 0.996 SSIM values were obtained. In Figure 8.b and h, 17.81 MSE, 35.62 dB PSNR ve 0.97577 SSIM, 0.99 UQI, 0.2128 BER, 0.0043 NCC values are obtained in the resized original and hidden stego Lena images hidden in as the 1st security layer. Since this layer was not found in the previous study, there is no data. The security layer hides the hidden image as a secret. According to MSE, PSNR, SSIM, UQI, BER and NCC values, the security layer is successfully hidden. In Figure 8.c and i, the original hidden image Jet image security layer in the size of 90x90x3 is hidden in Figure 8.b, and the values between the range value 1 and the hidden Jet image extracted, 43.57 MSE, 31.73 dB PSNR, 0.93182 SSIM, 0.99 UQI, 0.2501 BER, 0.0051 NCC, between the image extracted and range value 2, 22.91 MSE, 34.52 dB PSNR, 0.93218 SSIM, 0.99 UQI, 0.2501 BER, 0.0051 NCC, between the image extracted and range value 3, 34.26 MSE, 32.78 dB PSNR, 0.93198 SSIM, 0.99 UQI, 0.2472 BER, 0.0050 NCC, and between the image extracted and range value 4, 77.60 MSE, 29.23 dB PSNR, 0.93126 SSIM, 0.99 UQI, 0.2488 BER, 0.0051 NCC are obtained. According to MSE, PSNR, SSIM, UQI, BER and NCC results, the most successful range value is 2. The proposed method has safely hidden and extracted the hidden image.

The graphics showing the PSNR values according to the data capacity with the method suggested to the test images and LSB method are given in Figure 9. In the tests, data was hidden at rates between 0 - 1bpp for all images. In Figure 9, when data is hidden in Lena, Peppers, Baboon, Jet, Flower, Car, Mountain and Motorbike images at the rate of 1bpp, it is 51.14 dB, 51.12 dB, 51.14 dB, 51.14 dB, 51.12 dB, 51.13 dB, 51.14 dB and 51.13 dB, respectively, with the LSB method. While obtaining the PSNR value, 52.16 dB, 52.17 dB, 52.16 dB, 52.15 dB, 52.19 dB, 52.15 dB, 52.16 dB and 52.17 dB PSNR values are obtained in the proposed method. Results are close to each other in all images. The proposed method is slightly more successful than the LSB method. The proposed method first hides data to the first layer with the 4-bit method, then the first layer is hidden to the second layer with the LSB method. Since data is hidden to the last layer with the LSB method, PSNR values are close to the LSB method, but the proposed method gives more successful results. When 1 bpp data is hidden in the Lena image, 52.16 dB PSNR value is obtained in the proposed method, and 51.14 dB PSNR in the LSB method. The proposed method achieves 1.02 dB higher PNSR value than the LSB method.

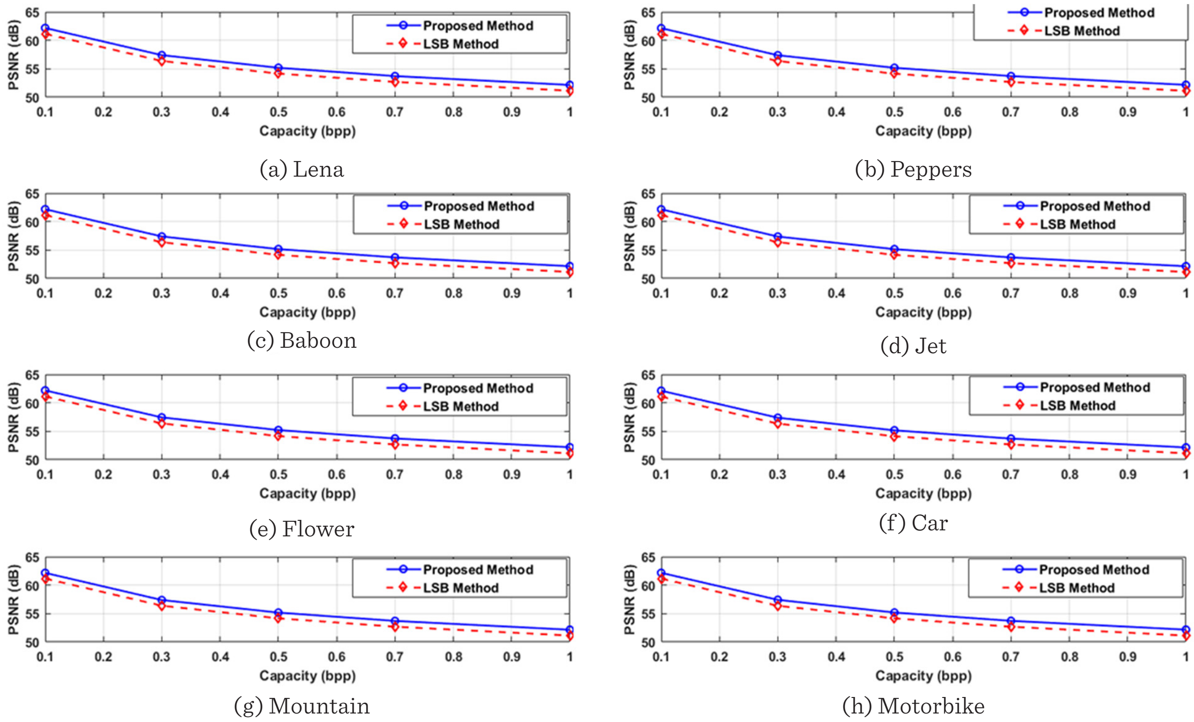
Table 1

Image quality index values of original, stego Lena images and extracted images that are extracted according to the range value

Image	Previous Study [6]		Proposed Method					
	PSNR	SSIM	MSE	PSNR	SSIM	UQI	BER	NCC
512x512x3 Orginal 1.Cover & Stego Lena	51.06	0.996	0.49	51.19	0.99914	1	0.0617	0.0012
180x180x3 Resized 2.Cover & Extracted 1. Hidden	-	-	17 .81	35.62	0.97577	0.99	0.2128	0.0043
90x90x3 Hidden & Extracted 2.Hidden, Range=1	15.38	0.889	43.57	31.73	0.93182	0.99	0.2501	0.0051
90x90x3 Hidden & Extracted 2.Hidden, Range=2	19.00	0.938	22.91	34.52	0.93218	0.99	0.2518	0.0051
90x90x3 Hidden & Extracted 2.Hidden, Range=3	22.95	0.948	34.26	32.78	0.93198	0.99	0.2472	0.0050
90x90x3 Hidden & Extracted 2.Hidden, Range=4	21.90	0.938	77.60	29.23	0.93126	0.99	0.2488	0.0051

Figure 9

PSNR values of previous study [6] and LSB method proposed according to hidden data capacity a) Lena b) Peppers c) Baboon d) Jet e) Flower f) Car g) Mountain h) Motorbike



(a) Lena

(b) Peppers

(c) Baboon

(d) Jet

(e) Flower

(f) Car

(g) Mountain

(h) Motorbike

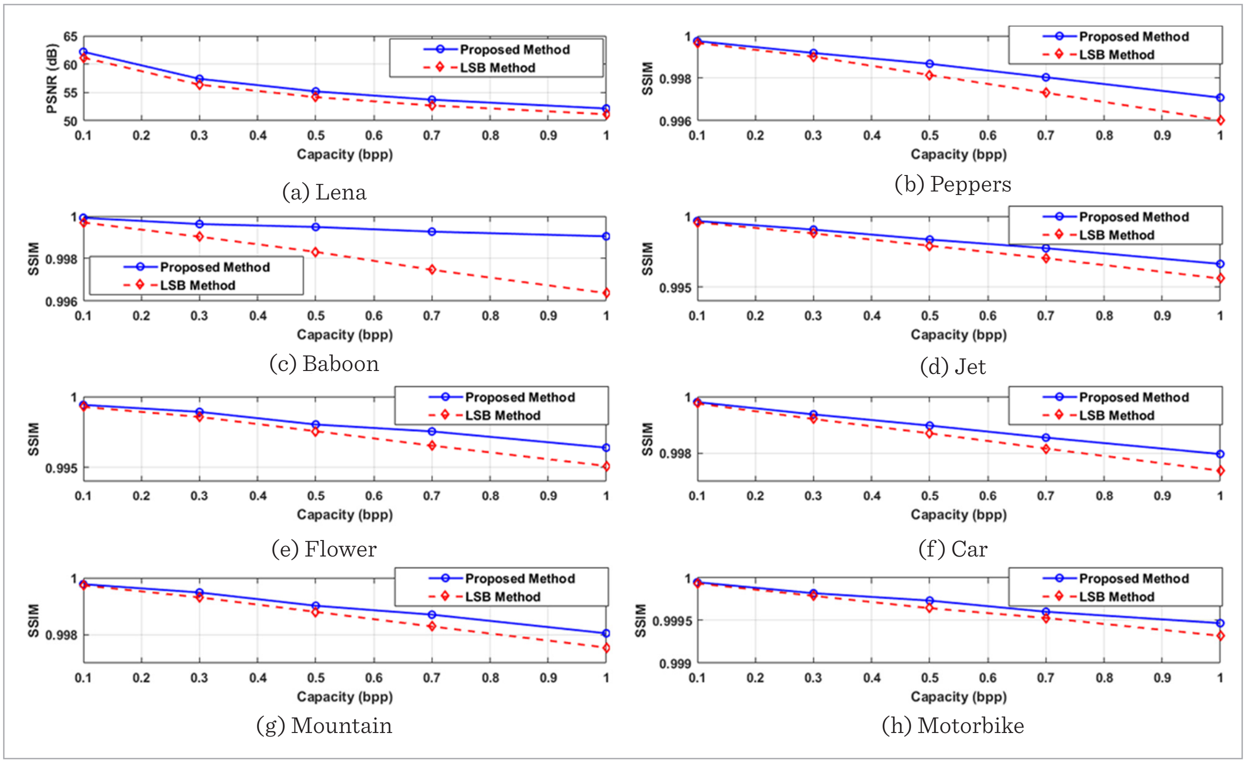
The graphics showing the SSIM values according to the data capacity with the method recommended for the test images and the LSB method are given in Figure 10. In Figure 10, when 1bpp data is hidden in Lena, Peppers, Baboon, Jet, Flower, Car, Mountain and Motorbike images, the LSB method provides values of 0.9963, 0.9960, 0.9963, 0.9955, 0.9950, 0.9973, 0.9975, 0.9993, respectively, and 0.9971 in the proposed method. SSIM values of 0.9970, 0.9990, 0.9966, 0.9963, 0.9979, 0.9980, 0.9994 are obtained. According to the SSIM values in Figure 10, the recommended method has obtained more successful results than the LSB method. According to the SSIM value, the proposed method increased by 0.0008 in the Lena image.

Chi-square steganalysis graphics of stego images, which are formed by hiding 1 bpp data to the original test images with the LSB method and the proposed method, are given in Figure 11. When the graphs in Figure 11 are examined, the original test images in Lena, Peppers and Flower images and the chi-square steganalysis values of LSB and data hidden images with the proposed method are at close levels. As a result of the original Baboon image, the results of the original, recommended and LSB methods differ from 50%. While the chi-square steganalysis values obtained by hiding 1bpp data in the result of the original Jet and Car images are very close to the results of the original Jet and Car images, the results of the LSB method are up to 38% in the Jet image and 23% in the Car image. As a result, the hiding method suggested in the test images could not be detected by the chi-square steganalysis test and produces very close values to the results of the original images.

Data hiding performances of the proposed method and LSB method were compared. The values of MSE, PSNR, SSIM, UQI, BER and NCC image criteria for Lena, Peppers, Baboon, Jet, Flower, Car, Mountain and Motorbike test images with the proposed method and LSB method are given in Table 2. Results are given for 5 different rates of payload as 0.1, 0.3, 0.5, 0.7

Figure 10

SSIM values of previous study [6] and LSB method proposed according to hidden data capacity a) Lena b) Peppers c) Baboon d) Jet e) Flower f) Car g) Mountain h) Motorbike



(a) Lena

(b) Peppers

(c) Baboon

(d) Jet

(e) Flower

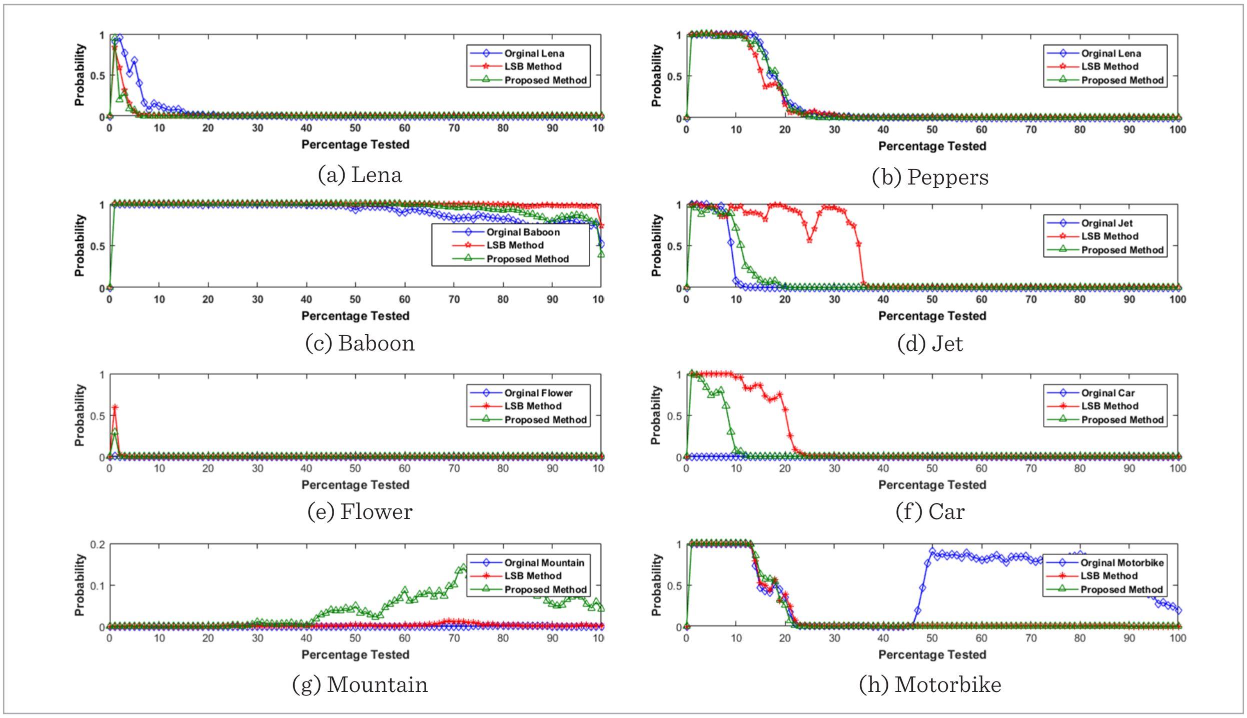
(f) Car

(g) Mountain

(h) Motorbike

Figure 11

Chi-square steganalysis graphs of original, recommended and data-hidden test images with LSB methods a) Lena b) Peppers c) Baboon d) Jet e) Flower f) Car g) Mountain h) Motorbike



(a) Lena

(b) Peppers

(c) Baboon

(d) Jet

(e) Flower

(f) Car

(g) Mountain

(h) Motorbike

Table 2

Analysis values of the image criteria of the LSB method and proposed with Original and Stego test images

		Proposed Method						LSB Method					
Image	bpp	MSE	PSNR	SSIM	UQI	BER	NCC	MSE	PSNR	SSIM	UQI	BER	NCC
Lena	**0.1**	0.039	62.17	0.9997	0.999	0.0049	0.0001	0.049	61.14	0.9997	1	0.0062	0.00012
	0.3	0.118	57.39	0.9992	0.999	0.0147	0.0003	0.149	56.37	0.9990	1	0.0187	0.00038
	0.5	0.197	55.18	0.9986	0.999	0.0246	0.0005	0.249	54.15	0.9983	0.999	0.0312	0.00064
	0.7	0.276	53.71	0.9981	0.999	0.0345	0.00071	0.349	52.69	0.9974	0.999	0.0437	0.00090
	1.0	0.395	52.16	0.9971	0.999	0.0494	0.00101	0.499	51.14	0.9963	0.999	0.0623	0.00128
Peppers	**0.1**	0.039	62.14	0.9997	0.999	0.0049	0.0001	0.050	61.13	0.9996	1	0.0062	0.00012
	0.3	0.118	57.38	0.9991	0.999	0.0148	0.0003	0.150	56.36	0.9990	1	0.0187	0.00038
	0.5	0.197	55.17	0.9986	0.999	0.0246	0.0005	0.250	54.14	0.9981	0.998	0.0313	0.00064
	0.7	0.276	53.71	0.9980	0.998	0.0345	0.00071	0.350	52.68	0.9973	0.995	0.0438	0.00090
	1.0	0.393	52.17	0.9970	0.995	0.0492	0.00101	0.501	51.12	0.9960	0.993	0.0626	0.00129
Baboon	**0.1**	0.039	62.17	0.9999	0.999	0.0049	0.0001	0.049	61.14	0.9997	1	0.0062	0.00012
	0.3	0.118	57.38	0.9996	0.999	0.0148	0.0003	0.149	56.37	0.9990	1	0.0187	0.00038
	0.5	0.197	55.16	0.9994	0.999	0.0247	0.00051	0.249	54.15	0.9983	0.999	0.0312	0.00064
	0.7	0.276	53.70	0.9992	0.999	0.0346	0.00071	0.349	52.69	0.9974	0.999	0.0437	0.00090
	1.0	0.395	52.16	0.9990	0.999	0.0494	0.00101	0.499	51.14	0.9963	0.999	0.0623	0.00128
Jet	**0.1**	0.039	62.15	0.9996	1	0.0049	0.0001	0.050	61.13	0.9995	1	0.0062	0.00012
	0.3	0.119	57.37	0.9990	1	0.0148	0.0003	0.149	56.38	0.9987	1	0.0186	0.00038
	0.5	0.198	55.15	0.9983	1	0.0247	0.00051	0.249	54.15	0.9979	0.999	0.0312	0.00064
	0.7	0.277	53.70	0.9977	1	0.0346	0.00071	0.349	52.69	0.9970	0.999	0.0437	0.00090
	1.0	0.396	52.15	0.9966	1	0.0495	0.00102	0.499	51.14	0.9955	0.999	0.0624	0.00128
Flower	**0.1**	0.039	62.18	0.9994	0.990	0.0049	0.0001	0.050	61.11	0.9992	0.990	0.0062	0.00013
	0.3	0.117	57.43	0.9989	0.989	0.0146	0.0003	0.149	56.38	0.9985	0.987	0.0187	0.00038
	0.5	0.195	55.21	0.9980	0.978	0.0244	0.0005	0.249	54.15	0.9975	0.976	0.0312	0.00064
	0.7	0.275	53.73	0.9975	0.977	0.0343	0.0007	0.350	52.68	0.9965	0.966	0.0438	0.00090
	1.0	0.392	52.19	0.9963	0.964	0.0490	0.00101	0.501	51.12	0.9950	0.956	0.0626	0.00129
Car	**0.1**	0.039	62.12	0.9998	0.999	0.0049	0.0001	0.050	61.09	0.9997	1	0.0063	0.00013
	0.3	0.118	57.38	0.9993	0.998	0.0148	0.0003	0.150	56.34	0.9992	0.997	0.0188	0.00038
	0.5	0.197	55.16	0.9989	0.997	0.0247	0.00051	0.251	54.13	0.9987	0.997	0.0313	0.00064
	0.7	0.276	53.71	0.9985	0.997	0.0345	0.00071	0.351	52.67	0.9981	0.995	0.0439	0.00090
	1.0	0.395	52.15	0.9979	0.996	0.0494	0.00102	0.501	51.13	0.9973	0.994	0.0626	0.00129
Mountain	**0.1**	0.039	62.15	0.9997	1	0.0049	0.0001	0.049	61.16	0.9997	1.000	0.0062	0.00012
	0.3	0.118	57.38	0.9994	1	0.0148	0.0003	0.149	56.38	0.9993	0.999	0.0186	0.00038
	0.5	0.197	55.17	0.9990	0.999	0.0246	0.0005	0.249	54.16	0.9988	0.999	0.0311	0.00064
	0.7	0.276	53.71	0.9987	0.999	0.0345	0.00071	0.349	52.69	0.9982	0.999	0.0436	0.00090
	1.0	0.395	52.16	0.9980	0.999	0.0493	0.00101	0.499	51.14	0.9975	0.999	0.0624	0.00128
Motorbike	**0.1**	0.039	62.16	0.9999	1	0.0049	0.0001	0.049	61.15	0.9999	1	0.0062	0.00012
	0.3	0.117	57.41	0.9998	0.999	0.0147	0.0003	0.149	56.37	0.9997	1	0.0187	0.00038
	0.5	0.196	55.19	0.9997	0.999	0.0245	0.0005	0.249	54.15	0.9996	1	0.0312	0.00064
	0.7	0.275	53.72	0.9996	0.999	0.0344	0.00071	0.349	52.69	0.9995	1	0.0437	0.00090
	1.0	0.393	52.17	0.9994	1	0.0492	0.00101	0.500	51.13	0.9993	1	0.0625	0.00129

and 1.0 bpp for all images. In Table 2, when data is hidden in Lena image at a rate of 1bpp, 0.499 MSE, 51.14 PSNR, 0.9963 SSIM, 0.999 UQI, 0.0623 BER, 0.00128 NCC values are obtained with the LSB method, respectively, while in the proposed method 0.395 MSE, 52.16 dB PSNR, 0.9971 SSIM, 0.999 UQI, 0.0494 An NCC value of BER, 0.00101 is obtained. In Table 2, when data is hidden at the rate of 1bpp in the Motorbike image, 0.499 MSE, 51.14 PSNR, 0.9975 SSIM, 0.999 UQI, 0.0624 BER, 0.00128 NCC values are obtained with the LSB method, respectively, while the recommended method is 0.395 MSE, 52.16 PSNR, 0.9980 SSIM, 0.999 UQI, 0.0493 BER. An NCC value of 0.00101 is obtained. The method suggested in all image criteria gave more successful results.

The proposed method has been compared with other data hiding studies in the literature. PSNR values for Lena, Baboon and Jet test images with the proposed method and Tsai [35], Luo [19] and Liu [17] methods in the literature are given in Table 3. Accordingly, for the 0.3, 05 and 1.0 bpp payload in the Lena image, respectively Tsai [35] 45.04, 40.14, 31.05 dB, Luo [19] 48.67, 43.22, 33.21 dB, Liu [17] 50.91, 47.58, 37.89 dB PSNR values, respectively, the proposed method achieves PSNR values of 57.39, 55.18 and 52.16 dB. Similarly, for the Jet image 0.3, 05 and 1.0 bpp payload, respectively, Tsai [35] 46.89, 41.46, 32.13 dB, Luo [19] 49.28, 44.24, 34.12 dB, Liu [17] 52.10, 49.76, 40.13 dB PSNR values, respectively, the proposed method achieves PSNR values of 57.37, 55.15 and 52.15 dB. In the Baboon image, for 0.3, 05 and 1.0 bpp payload, Tsai [35] cannot hide data for 46.89 dB, 0.5 and 1.0 bpp, respectively, Luo [19] cannot hide data for 37.89, 31.12 dB, 1.0 bpp, Liu [17] 41.76, 34.41 dB. While, cannot hide data for 1.0 bpp, the proposed method achieves PSNR values of 57.38, 55.16 and 52.15 dB. According to the results, the proposed method achieves higher PSNR values at all payloads compared to other methods.

Since the limit of the proposed method hides data in two layers to increase security, its data hiding capacity is lower than the LSB method. The proposed method lossy hides the hidden image to the second layer. The purpose here is to increase the capacity and make less data changes in the cover image. The use of the proposed method is a threat to the validity of the method if the hidden image contains sensitive information, especially if it is not suitable for lossy transmission in images containing small text.

The proposed method may work for grayscale images. In the grayscale images, data can be concealed from there without any change in the dimensions given in the article. There is no situation to change the results. The proposed method is designed to be used both in 24-bit RGB color images and 8-bit grayscale images.

Consequently, according to all these experimental results, the proposed method manages to hide data with high reliability by making minimal changes in the cover image. The proposed method obtains higher PSNR and SSIM values compared to the previous study [6] and LSB method. The proposed method obtained values close to the results of the original images in all test images in the chi-square steganalysis attack and successfully passed through the chi-square attacks. In addition, the proposed method hides two layers of data. Accordingly, third parties trying to extract data with the standard LSB method will only get the original resized image from the image, where the data is hidden. Thus, accessing the original hidden

Table 3

Comparison of PSNR values of the proposed method with studies in the literature

PSNR (dB)												
Image	Tsai [35]			Luo [19]			Liu [17]			Proposed Method		
bpp	0.3	0.5	1.0	0.3	0.5	1.0	0.3	0.5	1.0	0.3	0.5	1.0
Lena	45.04	40.14	31.05	48.67	43.22	33.21	50.91	47.58	37.89	**57.39**	**55.18**	**52.16**
Baboon	34.87	-	-	37.89	31.12	-	41.76	34.41	-	**57.38**	**55.16**	**52.16**
Jet	46.89	41.46	32.13	49.28	44.24	34.12	52.10	49.76	40.13	**57.37**	**55.15**	**52.15**

image becomes two times more difficult. In order to extract the real hidden image, they need to know the 4-bit hiding algorithm. According to all these results, it is seen that the proposed method can hide data securely. The proposed method has its advantages and disadvantages.

Advantages:

1. The proposed method hides 24-bit color image to 24-bit color image. The method provides two layers of secure data hiding. This feature makes it difficult to reach the hidden image of the proposed method and increased its security.
2. The rate of indestructibility against the proposed Chi-square steganalysis methods is high and the results are more successful.
3. The proposed method can recover the image it hides from the previous study [6] with higher quality and low loss.

Disadvantages:

1. The proposed method hides the hidden image with loss to make less changes to the cover image.
2. Since it hides data in two layers, the data hiding capacity is lower than the LSB method.

4. Conclusions

In this study, a new two-layer and reversible data hiding method is proposed, which hides the 24-bit color image in a 24-bit color image. The proposed method has obtained more successful imperceptibility values than traditional LSB methods and the previous study [6]. According to the tests performed, when the LSB method and the proposed method are hidden at the same rate, the PSNR image criterion, which is 1.2 dB, SSIM 0.0025, BER 0.0129 and NCC image criterion, has a higher measurement value of 0.00027. According to the tests carried out, the proposed method obtains more successful PSNR and SSIM values compared to the previous study [6] and LSB. The proposed method hides the hidden image to the resized version of the cover image with the LSB method by hiding two layers of data, and then hides the resized cover image to the original cover image with the 4-bit method. It has increased security by hiding the hidden image in two intertwined cover images. When third parties extract data by using the LSB method, they can only access the resized version of the cover image. Also, since the proposed data hiding method is reversible, it does not need the original image in the extraction process.

References

1. Alattar, A. M. Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform. IEEE Transactions on Image Processing, 2004, 13(8), 1147-1156. https://doi.org/10.1109/TIP.2004.828418
2. Chan, C. On Using LSB Matching Function for Data Hiding in Pixels. Fundamenta Informaticae, 2009, 96(1-2), 49-59. https://doi.org/10.3233/FI-2009-166
3. Chang, C. C., Chou, Y. C., Kieu, T. Information Hiding in Dual Images with Reversibility. 3rd International Conference on Multimedia and Ubiquitous Engineering China, June 4-6, 2009. https://doi.org/10.1109/MUE.2009.35
4. Doğan, S. A New Data Hiding Method Based on Chaos Embedded Genetic Algorithm for Color Image. Artificial Intelligence Review, 2016, 46(1), 129-143. https://doi.org/10.1007/s10462-016-9459-9
5. Doğan, S. A Reversible Data Hiding Scheme Based on Graph Neighbourhood Degree. Journal of Experimental & Theoretical Artificial Intelligence, 2017, 29(4), 741-753. https://doi.org/10.1080/0952813X.2016.1259264
6. Durdu, A. A High Capacity Reversible Steganography Method Based on Lsb Mapping Area for Hiding Lossy Images into Images. Phd Thesis, Sakarya University, Sakarya, Turkey, 2016.
7. Durdu, A. Analysis of Steganographed Audio Files with the Guide of Artificial Neural Networks. Master Thesis Sakarya University, Sakarya, Türkiye, 2010.
8. Fridrich, J., Soukal, D. Matrix Embedding for Large Payloads. IEEE Transactions on Information Forensics and Security, 2006, 1(3), 390-395. https://doi.org/10.1109/TIFS.2006.879281
9. Hernández, J. R., Amado, M., Pérez-González, F. DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure. IEEE Transactions of Image Processing, 2000, 9(1), 55-68. https://doi.org/10.1109/83.817598
10. Hore, A., Ziou, D. Image Quality Metrics: PSNR vs. SSIM. 20th International Conference on Pattern Recognition, Istanbul, Turkey, August 23-26, 2010, 2366-2369. https://doi.org/10.1109/ICPR.2010.579

11. Hwang, R. J., Shih, T. K., Kao, C. H. A Lossy Compression Tolerant Data Hiding Method Based on JPEG and VQ. Journal of Internet Technology, 2004, 5(3), 171-178.

12. Kazan, S., Vural, C. Sayısal Görüntü Damgalama Yöntemlerinin Jpeg Sıkıştırmasına Karşı Dayanıklılığının Karşılaştırılması. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 2016, 2(1).

13. Ker, A. D. Quantitative Evaluation of Pairs and RS Steganalysis. Proceedings of SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, 2004, 89-97. https://doi.org/10.1117/12.526720

14. Kısa, M. Grafik Tasarım Ve Baskı Ortamında Kullanılan Görsellerin Rgb Renk Uzayından Cmyk Renk Uzayına Dönüşümü Esnasında Oluşan Renk Ve Ton Kayıplarının Önlenmesi, Humanities Sciences, 2019, 14(2), 25-31.

15. Kodaz, H., Botsalı, F. M. Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması. Selçuk Teknik Dergisi, 2010, 9(1), 10-23.

16. Kurtuldu, O., Arica, N. A New Steganography Method Using Image Layers. 23rd International Symposium on Computer and Information Sciences, Istanbul, Turkey, October 27-29, 2008. https://doi.org/10.1109/ISCIS.2008.4717893

17. Liu, Z., L., Shan, G. An Improved Reversible Data Hiding Scheme Using Layered Embedding. Multimedia Tools and Applications, 2019, 78, 16311-16328. https://doi.org/10.1007/s11042-018-6958-5

18. Lu, T., Tseng, C., Wu, J. Dual Imaging-Based Reversible Hiding Technique Using LSB Matching. Signal Processing, 2015, 108, 77-89. https://doi.org/10.1016/j.sigpro.2014.08.022

19. Luo, L, Chen, Z, Chen, M, Zeng, X, Xiong, Z., Reversible Image Watermarking Using Interpolation Technique. IEEE Transactions on Information Forensics and Security, 2010, 5(1), 187-193. https://doi.org/10.1109/TIFS.2009.2035975

20. Mandal, J. K., Das, D. Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow. In2nd International Conference on Computer Science, Engineering and Applications, Delhi, India, 2012. https://doi.org/10.5121/csit.2012.2211

21. Memon, F., Unar, M., A., Memon, S. Image Quality Assessment for Performance Evaluation of Focus Measure Operators. Mehran University Research Journal of Engineering and Technology, 2015, 34(4), 379-386.

22. Mielikainen, J. LSB Matching Revisited. IEEE Signal Processing Letters, 2006, 13(5), 285-287. https://doi.org/10.1109/LSP.2006.870357

23. Özbilgin, F., Durmuş, F., Karagöl, S. Encrypting Written Text and Hiding It with LSB Method. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 2018, 6(3), 676-685.

24. Öztürk, E., Mesut, Andaç, Ş., Mesut, A. LSB Ekleme Yönteminde Bilgi Gizleme İçin Tek Renk Kanal Kullanımının Güvenliğe Etkileri, 4. Ağ ve Bilgi Güvenliği Sempozyumu, Ankara, 2011.

25. Prasad, S., Pal, A. K. An RGB colour Image Steganography Scheme Using Overlapping Block-Based Pixel-Value Differencing. Royal Society Open Science, 2017, 4(4), 161066. https://doi.org/10.1098/rsos.161066

26. Proakis, J. G., Salehi, M. Digital Communications, McGraw-Hill Education, 2007.

27. Ramasamy, P., Ranganathan, V., Kadry, S., Damaševičius, R., Blažauskas, T. An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic-Tent Map. Entropy, 2019, 21, 656. https://doi.org/10.3390/e21070656

28. Sharp T. An Implementation of Key-Based Digital Signal Steganography. In: Moskowitz, I. S. (Ed.) Information Hiding, Lecture Notes in Computer Science, 2137, Springer, Berlin-Heidelberg, 2001, 13-26. https://doi.org/10.1007/3-540-45496-9_2

29. Sneha, P. S., Sankar, S., Kumar, A. S. A Chaotic Colour Image Encryption Scheme Combining Walsh-Hadamard Transform and Arnold-Tent Maps. Journal of Ambient Intelligence and Human Computing, 2020, 11, 1289-1308. https://doi.org/10.1007/s12652-019-01385-0

30. Swain, G. Adaptive Pixel Value Differencing Steganography Using Both Vertical and Horizontal Edges. Multimedia Tools and Applications, 2016, 75(21), 13541-13556. https://doi.org/10.1007/s11042-015-2937-2

31. Şahin, A. The New Methods Used in Image Steganography and Their Reliability. Phd Thesis, Trakya University, Trakya, Türkiye, 2007.

32. Thakur, S., Singh, A. K., Ghrera, S. P. Chaotic Based Secure Watermarking Approach for Medical Images. Multimedia Tools and Applications, 2020, 79(7-8), 4263-4276. https://doi.org/10.1007/s11042-018-6691-0

33. Thiagarajan, C., Aarthi, M. N., Valli, M. R. A., Anitha, M. R., Ruthira, M. A. A Novel Algorithm for RGB Image Steganography. International Journal of Computer Science and Mobile Computing, 2016, 5(4), 261-270.

34. Tian, J. Reversible Data Embedding Using a Difference Expansion. IEEE Transactions on Circuits and Systems, 2003, 13(8), 890-896. https://doi.org/10.1109/TCSVT.2003.815962

35. Tsai, P, Hu, Y. C, Yeh, H., L. Reversible Image Hiding Scheme Using Predictive Coding and Histogram Shifting. Signal Processing, 2009, 89(6), 1129-1143. https://doi.org/10.1016/j.sigpro.2008.12.017

36. Tuncer, T. A Probabilistic Image Authentication Method Based on Chaos. Multimedia Tools and Applications, 2018, 77(16), 21463-21480. https://doi.org/10.1007/s11042-017-5569-x

37. Tuncer, T., Avcı, D., Avcı, E. İkili Imgeler Için Mayın Tarlası Oyunu Tabanlı Yeni Bir Veri Gizleme Algoritması. Journal of the Faculty of Engineering and Architecture of Gazi University, 2016, 31(4), 951-959. https://doi.org/10.17341/gazimmfd.278450

38. Wang, C. M., Wu, N. I., Tsai, C. Y., Hwang, M. S. A High Quality Steganographic Method with Pixel-Value Differencing and Modulus Function. Journal of Systems and Software, 2008, 81(1), 150-158. https://doi.org/10.1016/j.jss.2007.01.049

39. Wang, Z., Bovik, A. C. A Universal Image Quality Index. IEEE Signal Processing Letters, 2002, 9(3), 81-84. https://doi.org/10.1109/TIP.2003.819861

40. Wang, Z., Bovik, A. C., Sheikh, H. R., Simoncelli, E. P. Image Quality Assessment: From Error Visibility to Structural Similarity. IEEE Transactions on Image Processing, 2004, 13(4), 600-612. https://doi.org/10.1109/TIP.2003.819861

41. Wu, D., Tsai, W. A Steganographic Method for Images by Pixel-Value Differencing. Pattern Recognition Letters, 2003, 24(9-10), 1613-1626. https://doi.org/10.1016/S0167-8655(02)00402-6

42. Yang, C. Y., Wang, W. F. Block-Based Colour Image Steganography Using Smart Pixel-Adjustment. Advances in Intelligent Systems and Computing, 2015, 329, 145-154. https://doi.org/10.1007/978-3-319-12286-1_15