Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2013) 21: 548 – 564

doi:10.3906/elk-1108-74

A new digital image steganography algorithm based on visible wavelength

İbrahim COŞKUN[1], Feyzi AKAR[2], Özdemir ÇETİN[3,*]
[1]Department of Electrical and Electronic Technology, Tophane College, Bursa, Turkey
[2]Faculty of Electrical and Electronics Engineering, Naval Academy, Tuzla, İstanbul, 34940, Turkey
[3]Department of Computer Engineering, Faculty of Technology, Sakarya University, Sakarya, Turkey

Received: 24.08.2011 • **Accepted:** 01.11.2011 • **Published Online:** 22.03.2013 • **Printed:** 22.04.2013

Abstract: Stenography is the science that ensures secret communication through multimedia carriers such as image, audio, and video files. The ultimate end of stenography is to hide the secret data in the carrier file so that they are not detected. To that end, stenography applications should have such features as undetectability; robustness; resistance to various images process, sing methods, and compression; and capacity of the hidden data. At the same time, those features distinguish stenography applications from watermarking and cryptography applications. This study is different from other studies in the literature in that the undetectability parameter has been achieved through hiding data in line with the human sight system. In that sense, it has been determined through using the visible light wavelength limits of the pixel-carrying file in which the data are to be hidden. The peak signal-to-noise ratio has been used to evaluate the detectability and quality of the stego-image in which the secret information is embedded as a result of the data embedding process.

Key words: Steganography, data embedding, data hiding, information hiding, visible light wavelength, human vision system

1. Introduction

Acquiring information is easy no matter where you are as a result of the efforts to digitalize the highly increasing information and virtualize the process of reaching information in our contemporary world. In an environment where acquiring information is as easy as that, virtual theft has risen and it has been impossible to protect the privacy of individual lives and to promote the security of interpersonal communication. In that sense, scientists have developed various security methods to promote the security of the privacy of virtual communication (Figure 1). The most popular among them are digital watermarking and stenography, which provide the usage of multimedia files in confidential communication [1].

The most distinguishing factor between stenography and watermarking techniques is that the risk of being subject to attacks in digital watermarking is higher than in stenography, in that digital watermarking is applied to well-known popular media files whereas stenography is applied to unpopular carrier files. That is because the risk of a potential attack is quite low in the stenography method, as the carrier file used is an unknown file [1]. Stenography specifically aims at conveying secret information to authorized people through multimedia files without attracting the attention of unauthorized people [1,3]. Notwithstanding the fact that

*Correspondence: ocetin@sakarya.edu.tr

stenography seems to be a useful/practical application at first sight, it might still be used by ill-intentioned people. For example, it is a well-known fact that terrorist organizations that aim to perform illegal acts share such information as the act plan, its place, and its time on the Internet using those methods [4].

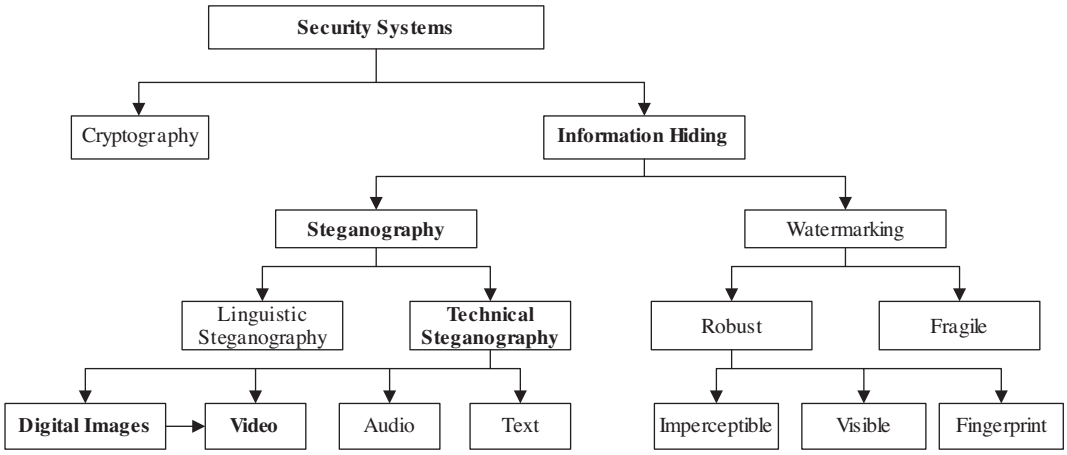


Figure 1. The different embodiment disciplines of information hiding. The arrow indicates an extension and bold font indicates the focus of this study [2].

Stenography applications make intense use of digital images due to the fact that they might be quickly shared through the Internet and provide a high capacity of data storage. Most of the studies in the literature were performed on black and white images because of the complexity of the process. That, however, is no longer valid for the color images currently shared through the Internet. Another important point in that sense is that the data storage capacity of a color image is 3 times more than that of a black and white image [5].

2. Nomenclature

It is important to know some of the terms of stenography for this study to be understood better. "Cover image" refers to the image in which the hidden data are to be embedded. "Stego-image" refers to the image that is to be acquired after the data are embedded in it. Attacks, on the other hand, reflect some image processing techniques and statistical analysis approaches applied to stenography algorithms so as to get hold of the data embedded in a stego-image.

2.1. Related works

Secret communication techniques are applied to image files as well as word files due to their high information storage capacity. The most popular image files shared through the Internet are graphics interchange format (GIF), Joint Photographic Experts Group (JPEG), and portable network graphics (PNG) formats. Images with bitmap (BMP) format are also preferred in that their structural complexity is relatively low in some applications [2].

Image stenography techniques are classified into 2 as the spatial domain and the frequency domain. When the data storage process is carried out in the spatial domain, the hidden data are embedded in the pixel values of the carrier file [6–9]. In the frequency domain method, however, the frequency values of the carrier file are acquired [10–12]. The discrete cosines transform (DCT) or discrete wavelet transform (DWT) transformations are used for that kind of process. Later on, the hidden data are embedded in the parameter values.

2.1.1. Image stenography in the spatial domain

The data hiding process was performed through the modifications made on the pixels of the carrier image in the spatial domain technique that was adopted initially. Potdar et al. [13], who hid data using the spatial domain method, developed a technique resistant to attacks based on image cropping. The researchers underlined resistance as opposed to image crop attacks. They hid data only after dividing the carrier image into subimages. They used the Lagrange interpolating polynomial algorithm to recover the hidden data embedded in the subimages. Given the parameters used for data hiding (such as the number of subimages and threshold values), calculation takes much time.

In another study, Shirali-Shahreza and Shirali-Shahreza [14] used the Arabic and Persian alphabets to hide the hidden data. These researchers used the spatial-domain stenography method when they used any alphabet as an image for hiding data. While there are only 2 letters in the Latin alphabet in which punctuation is used, which are 'i' and 'j', there are 18 such letters in the Persian alphabet. A secret message is conveyed in 2 ways in that message. Later on, the punctuation marks of those 18 letters are remodified according to those 2 files.

BMP files are commonly preferred in image stenography. However, they do not ensure a transfer as fast as JPEG files to share through the Internet. Nevertheless, it is not possible to perform least significant bits (LSB) techniques on JPEG files due to the complexity of the zip algorithm [15].

2.1.2. Image stenography in the frequency domain

The LSB embedding method marks a thoroughly new period for stenography applications in the real sense of the word. However, LSB techniques are not completely suitable for the human embedding system. In addition, it is more susceptible to attacks when compared to the frequency dimension of data hiding in the spatial domain. The DCT or DWT is used in embedding applications carried out in the frequency dimension. Basically, the identification of a 2-dimensional DCT is given in the formula below.

$$\mathrm{T}pq = \alpha p \alpha q \sum_{\mathrm{m}=0}^{\mathrm{M}-1} \sum_{\mathrm{n}=0}^{\mathrm{N}-1} Fmn \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}$$

$$0 \le p \le M-1$$

$$0 \le q \le N-1$$

$$\alpha p = \begin{cases} 1/\sqrt{M}, & p=0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \qquad \alpha q = \begin{cases} 1/\sqrt{N}, & p=0 \\ \sqrt{2/N}, & 1 \le p \le N-1 \end{cases} \tag{1}$$

M and N represent the dimensions of the entry image. The M and N variables are valued from 0 to M – 1 and 0 to N – 1, respectively.

In the frequency domain, stego-image techniques make use of zipped images as carrier images. The JPEG format, a zipped image format, is zipped according to Eq. (1) with DCT transformation. The image is transformed into 8 × 8 subimage blocks to acquire 64 distinct DCT parameters. As for the data embedding process, the hidden data are embedded in those DCT parameters. Even a single change in only 1 parameter means that the 64 DCT parameters would also change [16].

The JSteg algorithm was the first to use JPEG images for data hiding. This method, which has proven resistant against visual attacks, is not resistant against statistical attacks [17].

Wayner indicated in his study that parameters are created in the form of a curve as a result of the JPEG zip. The JSteg algorithm embeds the hidden data in that curve [18].

In another study, researchers performed an F5 algorithm based on the hiding process [19]. The F5 algorithm performs the embedding process by reducing the actual value of the parameter by 1, as for AC DCT parameters, which are not equal to 0 in value.

In another study using the DWT method, the carrier image and hidden information are decomposed using the DWT [20]. Afterwards, each is divided into 4 $\times$ 4 blocks. The blocks of the hidden information are placed on the blocks of the carrier image to find the best match. Afterwards, error blocks are produced and the parameter of the carrier image that is acquired through the best match is embedded in it.

This study developed a new method of stenography for color images based on the human visual system, which makes it different from other studies in the literature. The technique makes use of the visible light wavelength approach in the determination of pixels suitable for data embedding. During confidential communications, the real aim is to minimize the confidential data detectability so as to prevent the carrier video from being exposed to external attacks. The image quality between the stego-cover and the cover video acquired in the experiments was evaluated according to peak signal-to-noise ratio (PSNR) criteria.

3. Background

3.1. Digital image

The digital image is represented by a serial composed of N lines and M columns. In general, line and column indexes are shown as y, x, or c. Each element of that serial is called a pixel (Figure 2). Basically, pixels are valued as either 0 or 1. Images that are formed through such pixels are called binary images. The '1' and '0' values represent light and dark areas or objects and backgrounds (the environmental background in front of or on which an object is situated), respectively [21]. Digital image files are used in the form of 16 or 24 bits as color images, while gray-level images are used as 8 bits.

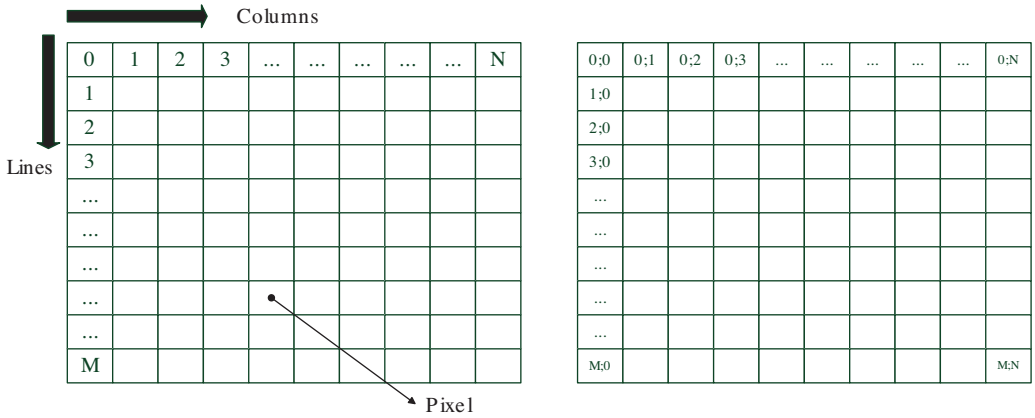


Figure 2. Configuration of a digital image.

As for 24-bit color images, 1 pixel is identified with 3 bytes. As for color, each pixel is composed of 3 main colors, red, green, and blue. That is called the RGB value of a pixel [22]. At the same time, the capacity of an image is based on the color measurement with which it is identified.

For example, a gray-level image of 640 $\times$ 480 pixels is made up of 307,200 pixels. Such an image covers an area of 307,200 bytes in the memory. A color image of the same size, however, covers 3 $\times$ 307,200 bytes.

That means that the data hiding capacity of color images is 3 times more than that of gray-level images.

Color images are classified into 2 categories, as zipped and unzipped. Unzipped images in BMP and GIF format can store much more data than zipped images in JPEG format [23].

3.2. Color theory

The electromagnetic spectrum includes visible light and other forms of electromagnetic energy (X-lights, ultraviolet lights, infrared lights, etc.). Light is identified by "wavelength" and the most suitable unit is the nanometer ($1\ \text{nm} = 10^{-9}\ \text{m}$). The human eye can observe between 350 and 780 nm, which is known as the visible area within the electromagnetic spectrum. The 3 basic elements affecting the perception of color are light source, object, and observer. Color measurement is related to the interaction of those 3 elements and each element has to be signified and identified digitally so that the color can be stated digitally.

Color standards such as RGB and those of the International Commission on Illumination (CIE) have been developed for different applications.

3.2.1. RGB color space

The RGB color domain is one of the most frequently used color domains. The codes of all of the colors in nature are indicated in reference to those 3 basic colors, taking light as the basis. When each color is mixed at a rate of 100%, the outcome is white, whereas the outcome is black when they are mixed at a rate of 0%. As for that domain, since red, blue, and green, which are the main colors, are not indicated, all of the colors change as the definition of those main colors changes. The color system used on the Internet is the RGB color system. That is because it was accepted as a basis first by Polaroid, the first camera to be used in 1953, and then by televisions. Currently, it is used as the standard in cathode ray tube displays, scanners, televisions, and manual cameras [24].

3.2.2. CIE 1931 color space

Light sources are characterized by spectral energy distribution (SED) values and the SED value of a light source signifies the radiative power of the light source at each wavelength ($\text{W cm}^{-2}\ \text{nm}^{-1}$). SED values can be changed by putting gelatin or liquid filters of various colors in front of a light source. Thus, a new system with different SED values can be formed. The color specification that is currently widely used is based on a system specified by the CIE. The standard observer concept, which is the last element of color measurement, was defined as a result of the studies carried out on real test subjects by the CIE in 1931. The primary reference stimuli used in this study were "red" for a 700-nm wavelength, "green" for a 546.1-nm wavelength, and "blue" for a 435.8-nm wavelength. The test subjects were required to "match" the color of the monochromatic test lamp by changing the intensity of those 3 primary sources with the help of a visual colorimeter. As a result of this experimental study, 3 sensitivity curves were discovered, defining the reaction of the human eye to light at different wavelengths, and those curves were defined as "2° Standard Observer" or "CIE 1931 Observer" due to the fact that the test subjects were tested through an observation angle of 2° [25].

It is possible to define x as the curve of "sensitivity to red", y as the curve of "sensitivity to green", and z as the curve of "sensitivity to blue". "λ" arbitrary the letters signifies that those curves change depending on the wavelength.

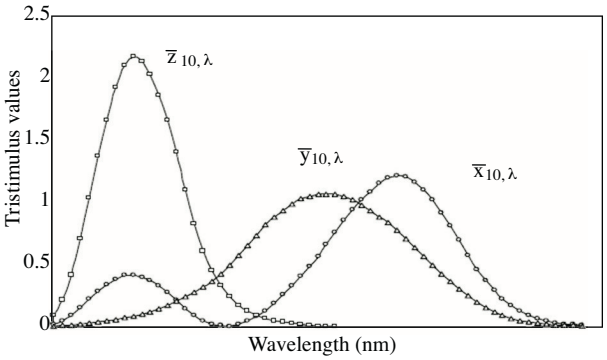


Figure 3. depicts the color match function curve for 10° Standard Observer [25].

3.2.3. Tristimulus values

As for depicting a color digitally, SED values, as for the light source, are multiplied with the percentage reflectance values of an object, and the magnitude of color match functions (color sensitivity values) for Standard Observer (2° or 10°) for each wavelength will be equal to the "digital values" of that color. Those values are defined as the "tristimulus" values of a color and are signified by X, Y, and Z. It is possible to restate the definition above with the equations given below; in that sense, X, Y, and Z are the tristimulus values of that color.

$$X \sum_{0}^{\infty} I(\lambda)\bar{x}(\lambda)d\lambda \tag{2}$$

$$Y \sum_{0}^{\infty} I(\lambda)\bar{y}(\lambda)d\lambda \tag{3}$$

$$Z \sum_{0}^{\infty} I(\lambda)\bar{z}(\lambda)d\lambda \tag{4}$$

As a result, the X-Y-Z values are not related to the observable area in the color spectrum. The chromaticity scheme, however, does not generally have a linear value. That is precipitated by the fact that the value of the unit vector between the 2 radiance values might not have a color value that can be observed with the human eye at all times. Color is defined and labeled as Yxy in that system. Z, the third coordinate, could also be defined, although not necessarily [25].

3.2.4. Color match functions

The XYS color domain is different from other color modes, as it directly takes the measurement of the human eye as its basis and it forms the basis for other color models. First of all, a linear matrix transformation process is carried out so that the RGB values of the pixel can be transformed into the CIE-XYZ format. The X, Y, and Z values are tristimulus values. Tristimulus values specify the amount of the 3 primary colors, R, G, and B, that forms other colors. The formulas used for calculating the X, Y, and Z tristimulus values among the recognized RGB values are given below.

$$\begin{vmatrix} |X| \\ |Y| \\ |Z| \end{vmatrix} = \begin{vmatrix} |XrXgXb| \\ |YrYgYb| \\ |ZrZgZb| \end{vmatrix} \times \begin{vmatrix} |R| \\ |G| \\ |B| \end{vmatrix} \tag{5}$$

Here, the opposite of the matrix is calculated so that the RGB values can be drawn to the other side of the equity.

$$\begin{vmatrix} |R| \\ |G| \\ |B| \end{vmatrix} = \begin{vmatrix} |XrXgXb|(-1) \\ |YrYgYb| \\ |ZrZgZb| \end{vmatrix} \times \begin{vmatrix} |X| \\ |Y| \\ |Z| \end{vmatrix} \tag{6}$$

As for CIE–1931, sRGB is selected from among the parameters given for the different RGB areas and it is placed within the equation. The selection of the sRGB domain is due to the fact that web applications mainly make use of that standard.

$$\begin{vmatrix} |X| \\ |Y| \\ |Z| \end{vmatrix} = \begin{vmatrix} |0.41240.35760.1805| \\ |0.21260.71520.0722| \\ |0.01930.11920.9505| \end{vmatrix} \times \begin{vmatrix} |R| \\ |G| \\ |B| \end{vmatrix} \tag{7}$$

After those processes, Eq. (4) is acquired through linear transformation.

$$\begin{aligned} X &= 0.4124R + 0.3576G + 0.1805B \\ Y &= 0.2126R + 0.7152G + 0.0722B \\ Z &= 0.0193R + 0.1192G + 0.9505B \end{aligned} \tag{8}$$

Of the X, Y, and Z values found, the x, y, and z chromaticity coordinate values were found using Eq. (5).

$$\begin{aligned} x &= \frac{X}{X+Y+Z} \\ y &= \frac{Y}{X+Y+Z} \\ z &= \frac{Z}{X+Y+Z} = 1 - x - y \end{aligned} \tag{9}$$

The x, y, and z values are between 0 and 1.

The x = y = z = (1/3) point is white, theoretically. Moving away from this point, the saturation of the colors will increase.

4. Proposed data embedding algorithm

Until recently, most of the stenography techniques used were developed without considering the human visual system (HVS), which is the most important measurement and evaluation system that can distinguish the detectability of hidden information. However, lately new stenography algorithms have been developed, or are still being developed, whose detectability based on HVS is much lower than before due to masking/adaptive stenography techniques. This study has also developed a new HVS-based data embedding algorithm [1,26]. In

Figure 4, the process steps of the proposed algorithm are illustrated as a block diagram, where it can be seen that the hidden data are embedded within the cover file through embedding and encoding algorithms. The hidden data are recovered according to the embedding and encoding algorithms used by the receiver party and the sender party.

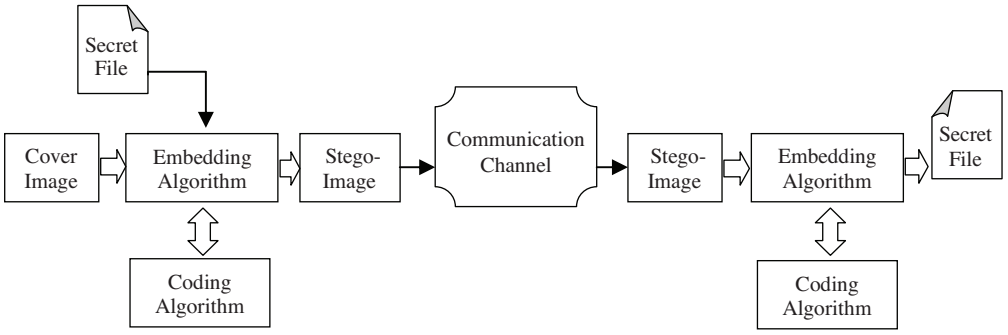


Figure 4. General block diagram for the proposed algorithms.

4.1. Wav-Steg

This paper suggests the use of a new approach comprising a HVS-based observable light wavelength, which is suitable for hiding data within a carrier video. That approach, which is known as wavelength, is different from other studies in that it makes use of observable light wavelength information owned by each pixel in the energy spectrum for specifying the pixels in which data might be embedded in a carrier image. The distance between the repetitive parts of a wave pattern of the observable light wavelength can be defined and is inversely proportional to the frequency. As can be seen in the energy spectrum in Figure 5, waves outside of the observable light range (such as ultraviolet lights, infrared lights, etc.) cannot be detected by the HVS.

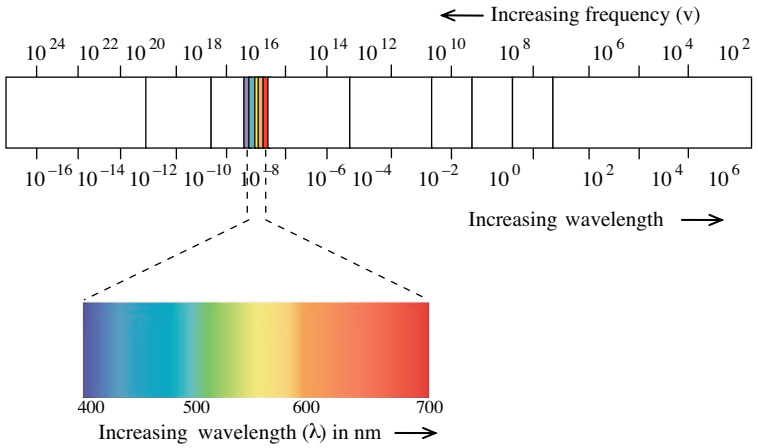


Figure 5. Observable light area in energy spectrum [27].

In the wavelength approach, data embedding can be performed in 2 steps. As for the first step, pixels with colors have values close to the limit wavelength values (380–700 nm) of the observable light range in the cover image. Calculation of the wavelength value from the RGB values of each pixel consists of a 3-step process.

1. RGB values of a pixel are transformed into the CIE-XYZ format using Eqs. (1), (2), (3), and (4).

2. Of the X, Y, and Z values found, the x, y, and z chromaticity coordinate values are found using Eq. (5).

3. At the last step, the equivalents of the x, y, and z values of each wavelength are calculated using Algorithm 1 with a range of 5 nm.

Algorithm 1.

```
NM_TO_XYZ converts a light wavelength to CIE xyz chromaticities.
!      x = X / ( X + Y + Z ), y = Y / ( X + Y + Z ), z = Z / ( X + Y + Z )
Input, real W, the wavelength of the pure light signal, in nanometers.
Input wavelengths outside this range will result in X = Y = Z = 0.
Output, real X, Y, Z
implicit none
integer, parameter :: ndat = 81
real, save, dimension ( ndat ) :: ldat = (/ &)
..
..
real w
  real x
  real, save, dimension ( ndat ) :: xdat = (/ &)
..
..
real y
  real, save, dimension ( ndat ) :: ydat = (/ &)
..
..
real z
 real, save, dimension ( ndat ) :: zdat = (/ &)
..
..
if ( w >= 380.0E+00 .and. w <= 780.0E+00 ) then
    call interp ( ndat, w, ldat, x, xdat )
    call interp ( ndat, w, ldat, y, ydat )
    call interp ( ndat, w, ldat, z, zdat )
  else
    x = 0.0E+00
    y = 0.0E+00
    z = 0.0E+00
  end if
  return
end
```

The RGB value of each pixel is transformed into wavelength using the method suggested. The lists of color codes used in the suggested method are available on the Internet, as well. An example of such lists is given in Table 1.

Table 1. The defined colors' wavelength range.

Wavelength	R color intensity	G color intensity	B color intensity
Violet: 380–420	97–130	0–30	97–175
Red: 680–700	161–200	0–30	0–50

According to Table 1, it is possible to assert that a pixel with (100,0,105) RGB value has an acceptable wavelength value. Therefore, pixels with wavelength values close to the limit values of observable light (400 or 700 nm) are specified for embedding data using the developed algorithm. By changing the limit values in Table 1, the security/capacity parameters can also be changed. However, it is important to remember that the security and hidden information capacity parameters are opposite of each other. Increasing security would

mean reducing the capacity and vice versa. As an example, the framework in Figure 6 could be analyzed, where the pixels suitable for embedding data according to the given criteria are marked with an X. The wavelength values of those pixels are 680–700 nm for red and 380–420 nm for violet.

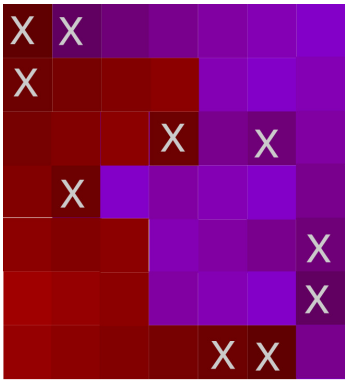


Figure 6. An exemplary framework composed of the violet and red wavelengths.

As for the second step, each pixel specified for embedding data is checked to see whether it remains at the initial wavelength value or close to it after the data are embedded in it. If a pixel remains within an acceptable color wavelength, or in other words if there is no significant change in the original value of the pixel after the data are embedded, that pixel is suitable for embedding data. Otherwise, it is not possible to use a pixel for embedding data. The starting point of this method is based on the understanding that ultraviolet and infrared light waves cannot be detected by the HVS. As a result, it could be asserted that it is harder for the HVS to detect slight changes in colors with wavelengths close to ultraviolet and infrared lights when compared to the changes in other colors.

Figure 7a displays an exemplary image composed of 4 pixels with a 380-nm wavelength value. If data are embedded in pixel 2 and its value remains within the range of 380 nm and 420 nm even after this process, it is suitable for embedding data (Figure 7b). However, if the pixel has a value of 430 nm after the data are embedded, it turns out that the data should not be embedded in that pixel (Figure 7c). There is a difference between the first pixel value and the last pixel value that can be observed by the HVS.

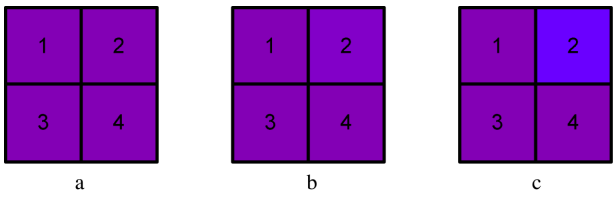


Figure 7. Exemplary blocks of 4 pixels with violet wavelength values: a) an exemplary block with 4 pixels, all of which have a 400-nm wavelength; b) an exemplary block whose pixel 2 has a 405-nm wavelength; c) an exemplary block whose pixel 2 has a 430-nm wavelength.

Given a standard digital image of 640 $\times$ 480 used for fast sharing on the Internet, the number of pixels forming the image turns out to be 307,200. Among nearly 300,000 pixels, it would be hard for the HVS to detect the change that pixel 2 in Figure 7a underwent in Figure 7b. However, such a change, as given in Figure 7c, is more likely to be detected by the HVS. The flow diagram of the Wav-Steg will be as is shown in Figure 8.

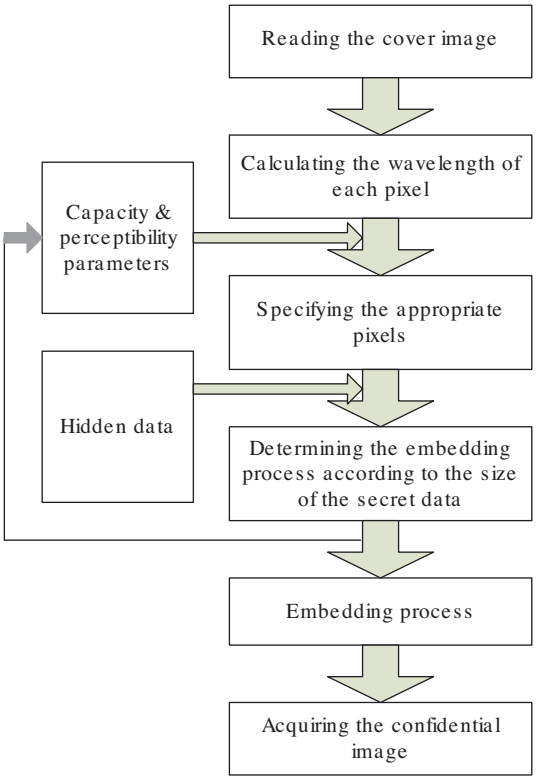


Figure 8. Flow diagram of the Wav-Steg.

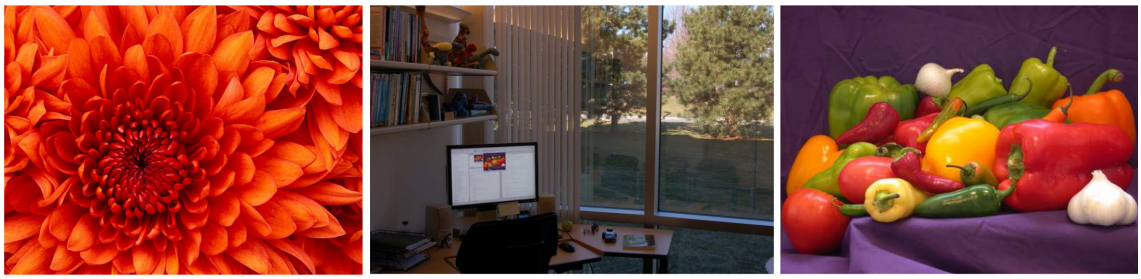
According to the flow diagram in Figure 8, the data hiding process begins with the resolution of the cover image to its pixels. That process helps to read the RGB values of the cover image in terms of its pixels. The algorithm begins to operate by calculating the RGB values acquired and the wavelength values of the pixels. The algorithm, operating according to the criteria produced in Table 1, determines the pixels suitable for embedding data. After the suitable pixels are determined, the software calculates the maximum confidential data capacity that could be embedded to relate it to the user. For the embedding process, the capacity of the selected hidden data should not exceed the maximum hidden data capacity; otherwise, it would not be possible to complete the data embedding process. ASCII codes of the hidden data are embedded in the pixels of the cover image specified for data hiding according to the encoding method. The duration of the data hiding depends on the size of the hidden data. After the embedded file is hidden in the cover image, the stego-image is saved in a directory and the application ends with the presentation of the statistical data of the embedding process to the user.

In other words, the main principle of the wavelength approach is that the pixel in which the hidden data are embedded should remain close to its original value after the data are embedded. That would make it possible to embed data independently in each pixel forming the image. In that sense, the complexity of the algorithm will increase and this, in turn, will guarantee increased communication security.

5. Experimental results

In this section, the experimental results obtained from 3 different images for the Wav-Steg is presented. During the experimental work, 'flower.bmp', 'home.bmp', and 'veggies.bmp' images were used at 768 $\times$ 102, 600 $\times$ 903, and 384 $\times$ 512 pixels, respectively. To evaluate the stego-image quality during the experimental work,

not only were statistical metrics used, but perceptual metrics such as mean structural similarity (M-SSIM), universal image quality index (UQI), and the PSNR human visual system-modified (PSNR-HVS-M) were also used.



a b c

Figure 9. The 3 original test images: a) flower, b) home, c) veggies.

The PSNR is a statistical metric that indicates the similarity between 2 images. It specifies to what extent a modified image is identical to the original one. A high PSNR value means that the visual quality is high. It is a requisite to calculate the mean squared error (MSE) to find the PSNR value between 2 images [28]. Eq. (3) or Eq. (4) can be used for calculating the MSE value.

$$\mathrm{MSE} = \frac{1}{\mathrm{mn}} \sum_{\mathrm{i}=0}^{\mathrm{m}-1} \sum_{\mathrm{j}=0}^{\mathrm{n}-1} \|\mathrm{O}\,(\mathrm{i,j}) - \mathrm{C}\,(\mathrm{i,j})\|^{2} \tag{10}$$

$$\mathrm{MSE} = \frac{\sum_{\mathrm{M,N}} [\mathrm{O}\,(\mathrm{i,j}) - \mathrm{C}\,(\mathrm{i,j})]^{2}}{\mathrm{M} \times \mathrm{N}} \tag{11}$$

O and C are compared to each other as the original and the data-embedded images, whereas the m and n values signify the line and column values of the images, respectively. After the MSE value is calculated, the next step is to find the PSNR using Eq. (5) [28].

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}^{2}}{\mathrm{MSE}}\right) \tag{12}$$

In that context, the MAX value refers to the number of bits for each pixel in an image.

5.1. Performance analysis of the Wav-Steg

In experimental studies, the performance analysis of the algorithm was carried out for 3 different images whose specifications were presented above. The graphic in Figure 10 is formed according to the wavelength value (WaV), hidden data capacity, and the parameters of the total bits damaged. The WaV parameter is important in the sense that it directly influences the perceptibility of the hidden data in the carrier image. Five different WaV values were employed to form 5 security levels in the study. When the WaV parameter value is high, the hidden data capacity will be reduced while the security level is increased. The fact that the number of damaged bits and the hidden data capacity decrease as the WaV increases can also be deduced from Figure 10. On the other hand, the security level of the system increases.

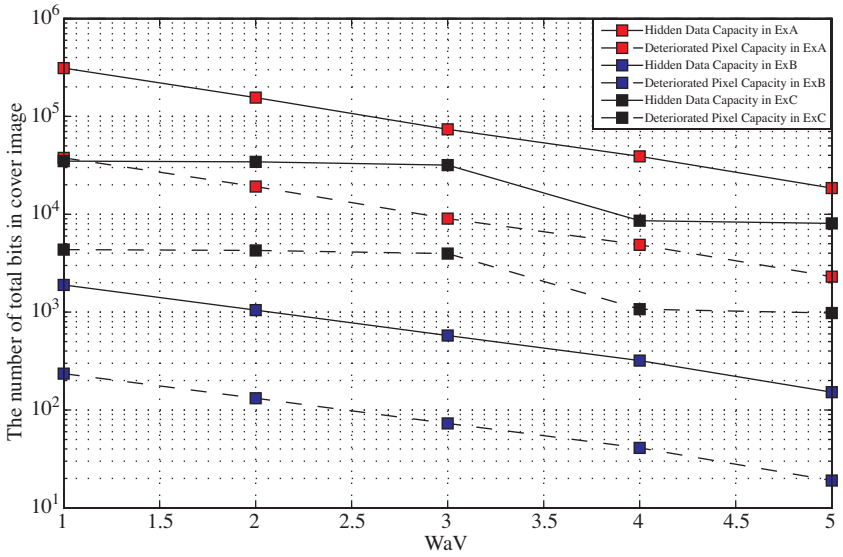


Figure 10. Performance analysis of the Wav-Steg using the WaV parameter.

5.2. Visual quality analysis of the Wav-Steg

The algorithm developed was applied to the images whose specifications were presented above and the PSNR values were found in order to analyze the quality of those images. For image processing studies, the PSNR value is accepted as 30 to 50 dB in the literature [29].

The statistical metric results are produced in Figures 11 and 12. The PSNR values are formed according to the different security levels in Figures 11 and 12. While the PSNR value is 48.8406 dB at its lowest security level for 'flower.bmp', it turns out to be 70.2827 dB at its highest security level for 'home.bmp'. Those results reveal that the PSNR values of the suggested stenography activity are quite satisfactory. Moreover, the PSNR-HVS-M values indicate better results than the PSNR metric in Figure 12.

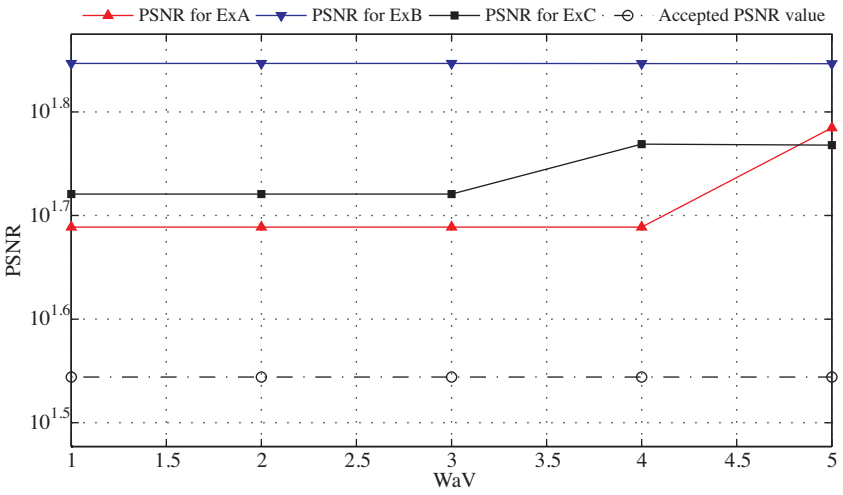


Figure 11. PSNR analysis of the Wav-Steg.

Because statistical metrics are inadequate for evaluating perceptual quality, several perceptual measures such as the UQI [30,31], M-SSIM [32], and PSNR-HVS-M [33] have been improved. In this paper, these measures

were used to evaluate the Wav-Steg. The UQI is measured as a quality result (Q) that ranges between [–1 and 1] and the M–SSIM is measured as a quality result (Q) that ranges between [0 and 1]. According to the given ranges, the best Q value is 1 for both of them. Examining the original and the test images, the M–SSIM and UQI are obtained as in Figures 13 and 14. The results indicate that the Wav-Steg provides very high perceptual invisibility.

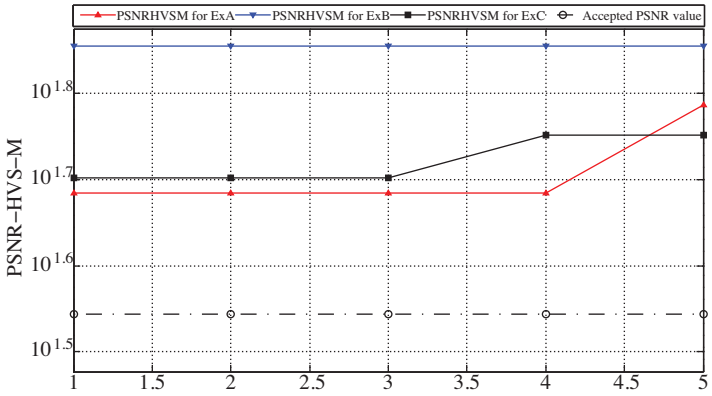


Figure 12. PSNR-HVS-M analysis of the Wav-Steg.

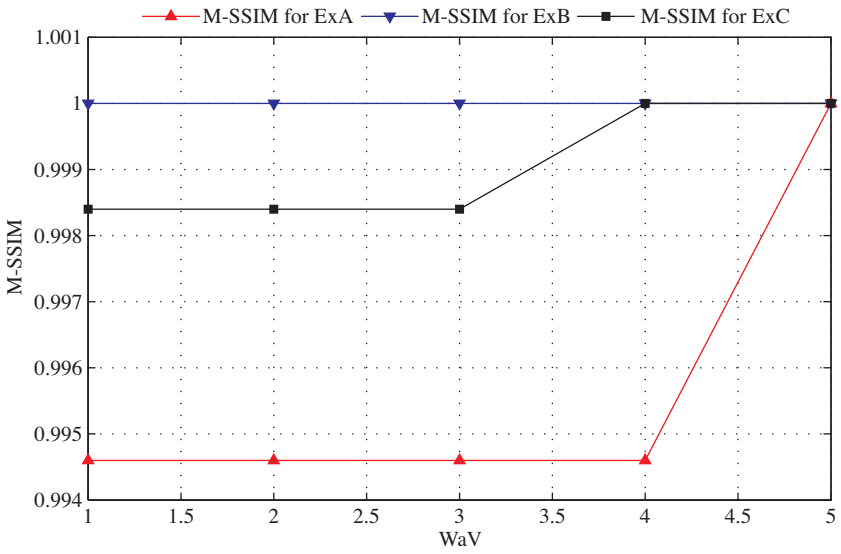


Figure 13. M-SSIM analysis of the Wav-Steg.

5.3. Steganalysis of the Wav-Steg

In this part of the paper, the Wav-Steg is studied using a well-known steganalysis method, the Stegdetect (OutGuess steganography detection) tool. As is known, steganographic methods cover and transmit hidden data within a carrier [34]. In a steganographic method, if the hidden data can be realized by an attacker, then the steganographic method fails. These types of attacks are known as detection attacks [35].

The robustness of the Wav-Steg is also checked using the Stegdetect tool. The result of the Stegdetect test gives a list that has 2 possible results, that the hidden data are found or not found. The results of the 2 stego-images are shown in Table 2, where it can be seen that the Wav-Steg method is quite successful.

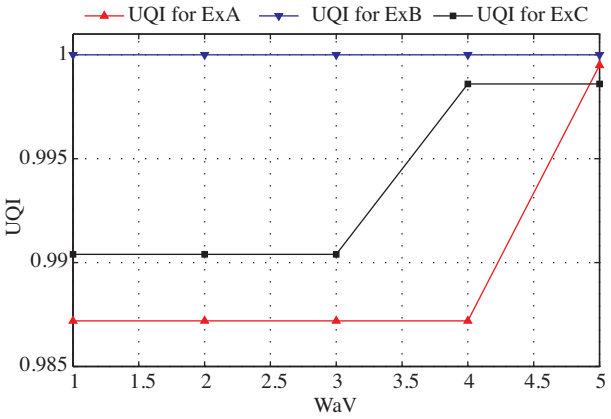


Figure 14. UQI analysis of the Wav-Steg.

Table 2. Stegdetect steganalysis of the Wav-Steg.

Stego-image	Stegdetect result
Flower	Negative
Home	Negative
Veggies	Negative

6. Conclusion

This study aimed to design a new data embedding algorithm for color images using the sensitivity of the HVS in the color spectrum. The most distinguishing quality of the suggested method is that it develops an algorithm according to the sensitivity of the HVS.

The high statistical quality of the Wav-Steg method, not only in terms of the PSNR but also the UQI and M–SSIM, is applicable to digital images.

The most critical phase of the study was the determining of the WaV parameter appropriately. When the security level of the WaV parameter is 5, the hidden data capacity will be extremely low. In that sense, users are presented with the flexibility of using alternatives according to the security of the communication. The color combination of the carrier image is of the utmost importance in that suggested method. As the algorithm needs the limit values of violet and red to embed the data, the hidden data capacity will increase considerably if the carrier image consists of those color combinations.

The experimental results of the Wav-Steg clearly show that the visual differences between the original and the corresponding stego-images' hidden data cannot be detected by the HVS. As a last word, neither visual nor statistical comparison enables the perception of the steganographic application being realized.

Acknowledgment

This study is a part of a research project that is supported by the Sakarya University Commission for Scientific Research Projects.

References

[1] Ö. Çetin, A Data Embedding Algorithm Design for Video Applications Using a New Steganography Approach, PhD, Sakarya University, Sakarya, Turkey, 2008.

[2] A. Cheddad, J. Condell, K. Curran, P. McKevitt, "Digital image steganography: survey and analysis of current methods", Signal Processing, Vol. 90, pp. 727–752, 2010.

[3] O. Çetin, A.T. Özcerit, "İGS tabanl yeni bir video–s rörtme yöntemi", Proceedings of the 3rd Information Security and Cryptology Conference with International Participation, pp. 84–88, 2008 (article in Turkish).

[4] B.T. McBride, G.L. Peterson, S.C. Gustafson, "A new blind method for detecting novel steganography", Digital Investigation, Vol. 2, pp. 50–70, 2005.

[5] J.J. Chae, D. Mukherjee, B.S. Manjunath, "Color image embedding using multidimensional lattice structures", Proceedings of the IEEE International Conference on Image Processing, Vol. 1, pp. 460–464, 1998.

[6] C.K. Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, Vol. 37, pp. 469–474, 2004.

[7] C.C. Chang, J.Y. Hsiao, C.S. Chan, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy", Pattern Recognition, Vol. 36, pp. 1583–1595, 2003.

[8] C.C. Thien, J.C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function", Pattern Recognition, Vol. 36, pp. 2875–2881, 2003.

[9] R.Z. Wang, C.F. Lin, J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition, Vol. 34, pp. 671–683, 2001.

[10] C.C. Chang, T.S. Chen, L.Z. Chung, "A steganographic method based upon JPEG and quantization table modification", Information Sciences, Vol. 141, pp. 123–138, 2002.

[11] M. Iwata, K. Miyake, A. Shiozaki, "Digital steganography utilizing features of JPEG images", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E87-A, pp. 929–936, 2004.

[12] H. Noda, J. Spaulding, M.N. Shirazi, E. Kawaguchi, "Application of bit-plane decomposition steganography to JPEG2000 encoded images", IEEE Signal Processing Letters, Vol. 9, pp. 410–413, 2002.

[13] V.M. Potdar, S. Han, E. Chang, "Fingerprinted secret sharing steganography for robustness against image cropping attacks", Proceedings of the 3rd IEEE International Conference on Industrial Informatics, pp. 717–724, 2005.

[14] M.H. Shirali-Shahreza, M. Shirali-Shahreza, "A new approach to Persian/Arabic text steganography", 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse, pp. 310–315, 2006.

[15] J. Fridrich, M. Goljan, D. Hogeg, "Steganalysis of JPEG images: breaking the F5 algorithm", Revised Papers from the 5th International Workshop on Information Hiding, pp. 310–323, 2002.

[16] A.M. Fard, M. Akbarzadeh-T, F. Varasteh-A, "A new genetic algorithm approach for secure JPEG steganography", Proceedings of the IEEE International Conference on Engineering of Intelligent Systems, pp. 1–6, 2006.

[17] N. Provos, P. Honeyman, "Hide and seek: an introduction to steganography", IEEE Security and Privacy, Vol. 1, pp. 32–44, 2003.

[18] P. Wayner, Disappearing Cryptography, 2nd ed., Burlington, MA, USA, Morgan Kaufmann Publishers, 2002.

[19] A. Westfeld, "F5—A steganographic algorithm: high capacity despite better steganalysis", Proceedings of the 4th International Workshop on Information Hiding, Vol. 2137, pp. 289–302, 2001.

[20] A.A. Abdelwahab, L.A. Hassan, "A discrete wavelet transform based technique for image data hiding", Proceedings of the 25th National Radio Science Conference, pp. 1–9, 2008.

[21] Ş. Sağıroğlu, M. Tunçkanat, Güvenli İnternet Haberleşmesi İçin Bir Yazılım: Türksteg, Kayseri, Turkey, Erciyes University, 2002 (in Turkish).

[22] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An overview of image steganography", Proceedings of the 5th Annual Information Security South Africa Conference.

[23] M.D. Hassan, Comparison for Steganalysis Approaches, MSc, Gazi University, Ankara, Turkey, 2008.

[24] Wikipedia, RGB Renk Uzayı, at http://tr.wikipedia.org/wiki/RGB_renk_uzay%C4%B1 (last accessed 10 January 2013; in Turkish).

[25] E. Öner, Tekstil Endüstrisinde Renk Ölçümü, Marmara University, Paper No: 672, İstanbul, 2001 (in Turkish).

[26] O. Cetin, A.T. Ozcerit, "A new steganography algorithm based on color histograms for data embedding into raw video streams", Computers & Security, Vol. 28, pp. 670–682, 2009.

[27] Wikipedia, EM spectrum.svg, at http://en.wikipedia.org/wiki/File:EM_spectrum.svg (last accessed 10 January 2013).

[28] M. Rabbani, P.W. Jones, Digital Image Compression Techniques, Vol. TT7, Washington, SPIE Optical Engineering Press, 1991.

[29] A.N. Netravali, B.G. Haskell, Digital Pictures: Representation, Compression, and Standards, 2nd ed., New York, Plenum Press, 1995.

[30] Z. Wang, A.C. Bovik, "A universal image quality index", IEEE Signal Processing Letters, Vol. 9, pp. 81–84, 2002.

[31] Y. Yalman, F. Akar, I. Erturk, "An image interpolation based reversible data hiding method using R-weighted coding", 13th IEEE International Conference on Computational Science and Engineering, pp. 346–350, 2010.

[32] Z. Wang, A.C. Bovik, H.D. Sheikh, E.P. Simoncelli, "Image quality assessment: from error visibility to structural similarity", IEEE Transactions on Image Processing, Vol. 13, pp. 600–612, 2004.

[33] K. Egiazarian, J. Astola, N. Ponomarenko, V. Lukin, F. Battisti, M. Carli, "New full-reference quality metrics based on HVS", Proceedings of the 2nd International Workshop on Video Processing and Quality Metrics, 2006.

[34] C.Y. Lin, C.C. Chang, Y.Z. Wang, "Reversible steganographic method with high payload for JPEG images", IEICE Transactions on Information and Systems, Vol. E91.D, pp. 836–845, 2008.

[35] J. Fridrich, R. Du, M. Long, "Steganalysis of LSB encoding in color images, IEEE International Conference on Multimedia and Expo, Vol. 3, pp. 1279–1282, 2000.