

Improvement of Steganographic Methods based on the Analysis of Image Color Models

Serhii Buchyk^a, Sergey Tolyupa^a, Yaroslav Symonychenko^b, Anna Symonychenko^a, and Artem Platonenko^c

^a Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., Kyiv, 01033, Ukraine

^b National Aviation University, 1 Lubomir Gyuzar ave., Kyiv, 03058, Ukraine

^c Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine

Abstract

The article examines methods for increasing the stability of a steganographic container to attacks when it is transmitted through the channels of communication. The main characteristics of a fixed container, namely a bitmap image, are defined. The most common color models of the image are analyzed. A method for rounding the values of image elements for modifying the lowest bit in steganographic protection problems is proposed. The results of a study to justify the choice of color scheme are presented as an image of the model in case of increased stability of the steganographic system.

Keywords

Steganographic systems, steganographic container, raster image, color model.

1. Introduction

At the present stage of the development of high-tech technologies, information is the most valuable both from a semantic point of view and from an economic point of view. In modern society, there is an increasing need to create new, more reliable methods of protecting information resources. For the solution, this task should use steganography technology. These methods allow you to hide not only data but also the fact that it is present in information flows when transmitted over a communication channel.

Steganography methods make it possible not only to transmit information covertly but also to successfully solve the problems of noise-proof authentication, protecting information from unauthorized copying, tracking the distribution of information by communication networks, etc. [1].

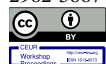
The implementation of steganographic protection methods leads to the creation of special steganographic systems. A steganographic system should be understood as a combination of methods and tools that are used to create a hidden channel for transmitting the information. The steganographic system embeds a message in a container, transmits the filled container to the steganographic channel, and decodes the hidden messages.

2. Task Formulation

One of the main stages of the steganographic system is embedding the message in the container for further transmission via communication channels. Fixed bitmaps (fixed containers) are most often used as containers for hiding and transmitting messages.

Important characteristics of containers for solving steganographic protection problems are raster size, resolution, color depth, and color model. Changing these characteristics affects the structural features of the container. To increase the stability of the steganographic system, it is necessary to strive to change the structural features of the base container as little as possible [2].

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: buchyk@knu.ua (A.1); tolyupa@i.ua (A.2); yaroslavsim@ukr.net (B.3); annasim98@ukr.net (A.4); a.platonenko@kubg.edu.ua (C.5)
ORCID: 0000-0003-0892-3494 (A.1); 0000-0002-1919-9174 (A.2); 0000-0002-9404-6610 (B.3); 0000-0001-5317-3464 (A.4); 0000-0002-2962-5667 (C.5)



© 2021 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

The use of methods of steganographic information protection contributed to the development and application of a new theoretical direction—steganalysis. The purpose of steganalysis is to study qualitative and quantitative assessments of the reliability of the steganographic system, container detection, and text disclosure. The optimal container is determined by a number of indicators based on the differences between the original container and the result container.

Thus, the purpose of this article is to increase the stability of the steganographic container based on the identification of basic characteristics and analysis of color models of the image. Based on the conducted studies, the optimal color model of the image will be determined in the conditions of implementation of steganographic protection processes.

3. Solving the Task

Still, bitmaps are most often used as a fixed container for transmitting a hidden message.

A bitmap image is an image that is a matrix of pixels on a computer monitor, paper, or other devices and materials.

Each pixel of a bitmap image is an object characterized by a specific color, brightness, and possibly transparency. One pixel can only store information about one color, which is associated with it.

Pixels in a bitmap image are arranged in rows and columns.

The more pixels per unit area an image contains the higher its detail. The maximum detail of a bitmap image is set when it is created and cannot be increased. If you zoom in on the image, the level of detail does not increase. Ensuring a smooth transition between the original pixels is due to the addition of new ones, the value of which is calculated based on the values of neighboring pixels of the original image [3].

To describe the placement of pixels, use a system of integer coordinates – pixel numbers with (0,0) in the upper-left corner.

Important characteristics of containers are raster size, resolution, color depth, and color model.

Image resolution. The resolution of a bitmap image is measured in pixels per inch (ppi). Image clarity depends on how many pixels are calculated per inch to reproduce graphic information, the more pixels, the sharper the image.

And the resolution of images printed on paper or other media is measured in dots per inch (dpi), since the smallest fraction of such an image is the printed dot on a piece of paper. So, the monitor screen is capable of displaying 72 (and possibly 96) pixels one inch vertically and horizontally, while the print image should contain 100–300 ppi.

Two digital images with a resolution of 72 and 300 ppi. The physical size of these images is one inch (2.54 cm) vertically and horizontally. If print these images on paper, with the same physical dimensions, the quality of the printed image will be different.

The image will have the best clarity of 300 ppi and the worst at 72 ppi.

When playing these images on the monitor screen there will be a noticeable increase in size images with 300 ppi (at 100% zoom). The increase will occur due to the fact that the monitor displays only 72 pixels per inch. That is, each part of the 300 ppi image will be increased to a size of one inch relative to the monitor screen.

Size of the image bitmap. The raster is a matrix of $N \times M$ pixels, where N and M are the pixel dimensions of the raster.

The size of the bitmap image is set as two integers that define the dimensions' images in horizontal and vertical pixels, such as 640×480 (width—640 pixels, height—480 pixels). As a result of the image, it consists of 307,200 pixels. The higher the resolution and size of the image, the higher the image detail.

Image color depth. One of the important characteristics of a bitmap image there is color depth. According to psychophysiological by studying, the human eye has the ability to distinguish 350,000 colors.

A different number of bits can be allocated to encode the pixel color. This determines the number of colors that can be displayed on the screen simultaneously. The longer the length of the binary code colors, the more colors you can use when playing a graphic object.

Color depth is the number of bits used to encode a single pixel. The color depth of a bitmap image is measured in bits per pixel (bpp).

Classify images by depth colors in this way [4]:

- Binary images (bitwise) have 1 bit per pixel.
- Grayscale-grayscale or other colors (1 byte per pixel).
- Color images. Two bytes (16 bpp) allow you to define 65,536 different colors (High Color mode). If for encoding colors 3 bytes (24 bpp) are used, and 16.7 million colors can be displayed (True Color mode).

Computer graphics systems also use a greater color depth is 32/48 bpp, etc.

To store and represent a bitmap image, a bitmap is used, where on each pixel is allocated 1 bit of information. Allocating a single byte (8 bits) allows you to encode 256 different color shades. High Color mode is designed to represent the shades of “real-life,” that is, it is most conveniently perceived by the human eye.

32-bit color is a valid 24-bit color with an additional 8-bit channel that is either filled with zeros or is an alpha channel that specifies image transparency for each pixel. For example, to display the effect of semi-transparent windows, menus, and shadows [5].

The reason for using the alpha channel is the desire to optimize the work with video memory, which in most modern computers, it has a 32-bit addressing and a 32-bit data bus.

Color models of the bitmap image. Most shades are formed by mixing primary colors. The method of dividing a color shade into components is called a color model. There are many different types of color models. To solve this problem, we will consider the following color models: RGB, HSV, and HLS [6].

RGB. In this color model, the pixel color is it is formed by mixing three main components of RGB model colors.

Color synthesis is formed by encoding gradations of the three constituent channels (Red, Green, and Blue). By mixing three base colors in different proportions, you can get all variety of shades.

This model is presented as a three-dimensional coordinate system.

Each coordinate (channel) reflects the contribution of a component in the resulting color that ranges from zero to the maximum value. Inside the resulting cube are all colors forming a color space (Fig. 1).

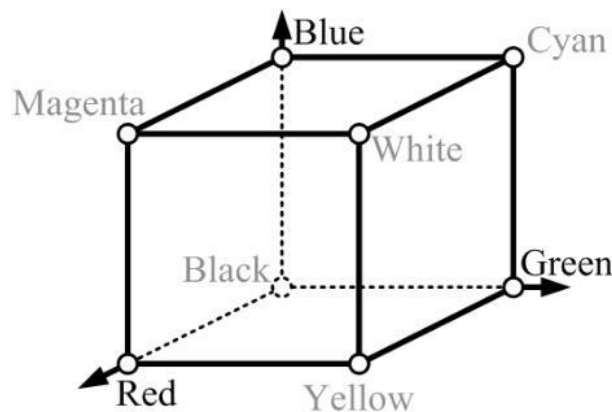


Figure 1: RGB color space

The number of gradations of each channel depends on the RGB bit value. Usually, a 24-bit model is used, in which 8 bits are allocated for each channel, and therefore the number of gradations is from 0 to 255 (Fig. 2).

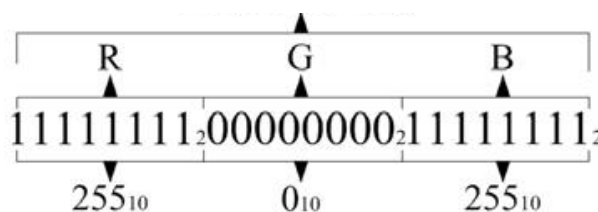


Figure 2: 24-bit RGB color synthesis model

In the RGB model, the center point with coordinates (0,0,0) is black. The maximum values of the components (255,255,255) correspond to white. Red (255,0,0), green (0,0,255), and blue (0,0,255). The RGB color model is designed to display images in electronic systems such as television, computers, photography, etc. [7].

HSV. HSV is a model that describes the color space, which is based on three color characteristics: Hue, Saturation, and Value or Brightness. The color space of the HSV model has a conical reflection (Fig. 3).

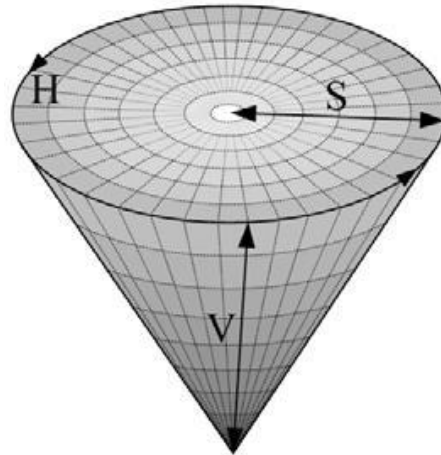


Figure 3: HSV color space

A closer look at the color space:

- Color tone (spectral color) is characterized by the H position on the color wheel and it is determined by the angle value from 0 to 360°.
- Saturation (S) is a parameter that determines the purity of the color. Saturation changes in the range from 0 to 100%. On the border of the color code, the circles are arranged as saturated as possible colors (saturation value - 100%). Color as the S decreases, it lightens. If the value is S-0%, any color turns white.
- Brightness or value (B or V) is a color parameter that characterizes illumination. Brightness varies from 0 to 100%. A reduction in color brightness is achieved by adding black (color dimming).

The HSV color model is used by computer artists when creating images in image editors.

After creating the image, it must be converted to an RGB or CMYK model.

The model is converted to RGB to display the image on the monitor screen, and in CMYK to get a printed image.

HLS. HLS is a color model in which the color coordinates are: Hue-color tone, Lightness, and Saturation.

In HLS, the color space is represented as a double cone (Fig. 4), in which L (Lightness) is deposited along the vertical axis, and the other two parameters are set in the same way as in the previous models.

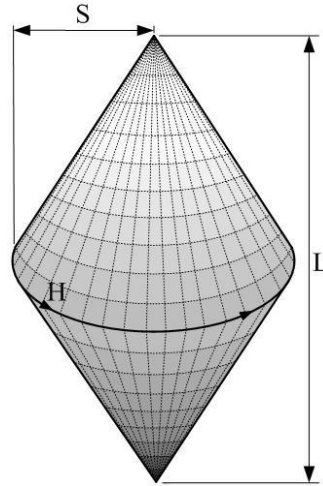


Figure 4: HLS color space

The brightness parameter varies from 0 to 100%. The 0% value corresponds to the vertex of the lower cone and sets the black color.

The white color of the maximum light intensity is set by the vertex of the upper cone and corresponds to the value of 100%.

The most intense color tones correspond to the bases of cones with $L = 50\%$.

To find the optimal color model for implementing steganographic protection, we will compare images based on the Pearson correlation coefficient indicator, determined by the formula:

$$r_{xy} = \frac{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{S_x^2} \sqrt{S_y^2}}, \quad (1)$$

where \bar{x} , \bar{y} are the average values of the sample x and y ; S is the standard deviation.

A 24-bit image was used to study the color models of the image. The image was saved in BMP format since it is the most optimal format when performing a steganographic conversion [8]. Three color models were used, namely: RGB, HSV, HLS.

The information was hidden by modifying the lowest bit of the image element. For performing the study, filling in the form was performed each component of all three color models. The degree of modification of the container was from 10 up to 100%.

A graphical display of coefficient values correlations is shown in Fig. 5. As can be seen, the best component for hiding data in an RGB model is the blue component.

The correlation coefficient of the blue component remains the highest at different degrees of container modification. Thus, the blue component is more resistant to steganographic conversion compared to other components, red and green.

The Saturation (S) component is more resistant to steganographic conversion when used in the HSV color model (Fig. 6). Since it has the highest correlation coefficient in all cases, compared to components H and V. Thus, the use of component S is more optimal for this color model.

When studying the HLS color model, the S component is optimal for hiding data. The value of the correlation coefficient, when using this component, has the highest value and is 0.99999994, which is more acceptable for increasing the stability of the steganographic system, compared to other components of this model (Fig. 7).

After examining all three bitmap color models, it should be noted that the HLS model, namely the S component, is more stable, since it has the highest correlation coefficient at different degrees of filling, compared to other color models.

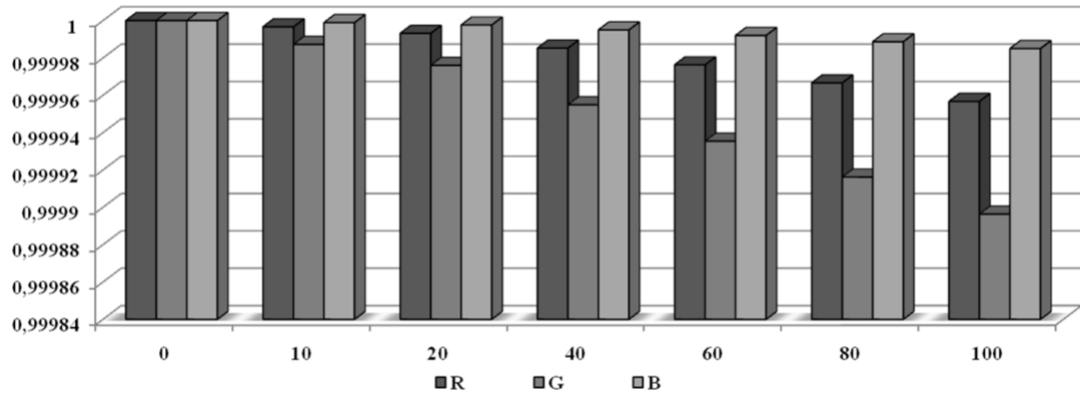


Figure 5: Values of the correlation coefficients of the RGB color model depending on the degree of filling

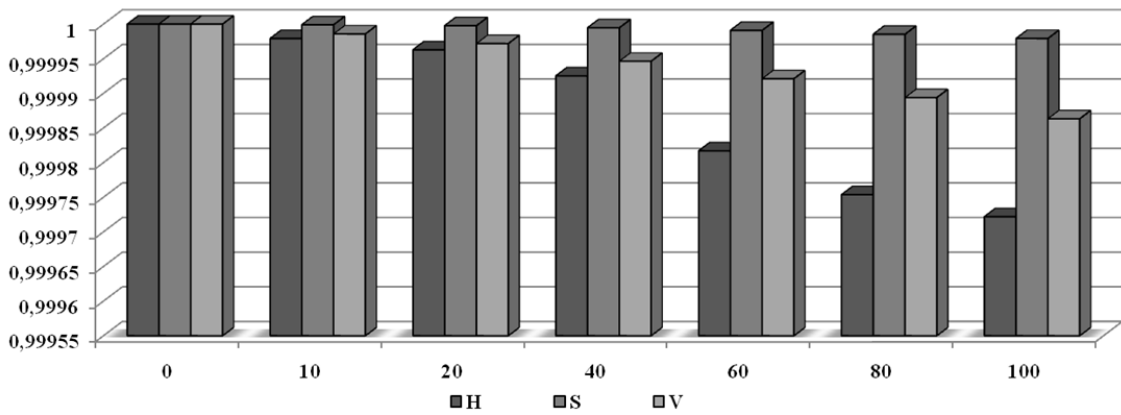


Figure 6: Values of the correlation coefficients of the HSV color model depending on the degree of filling

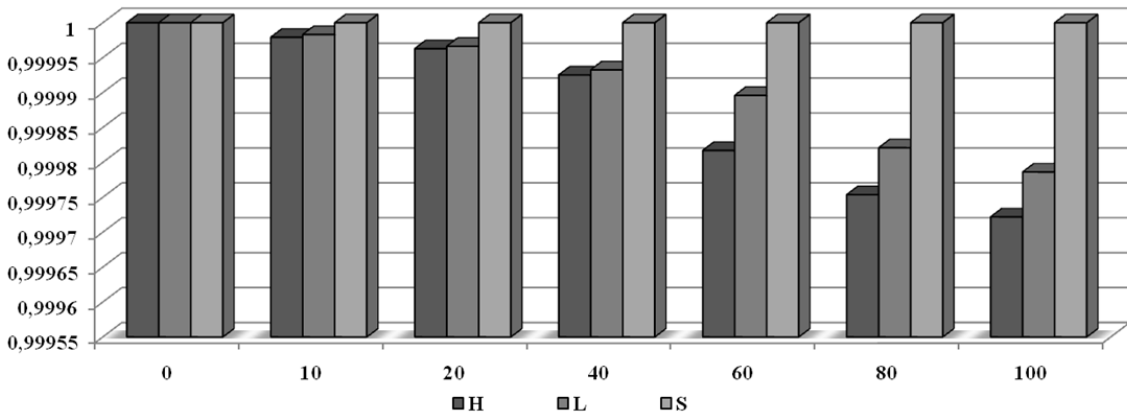


Figure 7: Values of correlation coefficients of the HLS color model depending on the degree of filling

As a consequence, the use of this component increases the stability of the steganographic system to steganalysis and the reliability of steganographic message transmission by the communication channel. The saturation component of the HSV color model has less resistance steganographic conversion since it has less value of the correlation coefficient.

The blue component of the RGB model is less stable than the saturation component. The use of the component somewhat reduces the resistance of the steganographic system to steganalysis. But using this model is also appropriate when hiding a small message.

Thus, to increase the stability of the steganographic system, the model should be used HLS. When using the HLS model, the value is elements components are expressed in terms of a decimal fraction. It is shown in Table 1.

Table 1.

Values of saturation component elements

		146	147	148
S =	10	61.93	61.93	61.93
	11	61.81	61.81	61.81
	12	61.74	61.74	61.74
	13	61.52	61.52	61.52

When hiding data each value of the elements of the corresponding component is converted to a binary format to modify the lower bit with the message bit, but the conversion to binary format occurs only in the integer part of the number because there is no fractional part in binary format.

In the case of using a binary system, each bit can take the values 0 or 1. So, alternating the lowest bit of binary values numerical sequence with sequential growth occurs alternately 0, 1, 0, 1, 0, 1, 0, 1, ... Binary representation of values of saturation components in the HLS model and numerical sequence are shown in this calculations:

$$\begin{aligned}
 61.93 &\rightarrow 0011 \ 1101_2 \quad 10_{10} = 1010_2 & (2) \\
 61.81 &\rightarrow 0011 \ 1101_2 \quad 11_{10} = 1011_2 \\
 61.74 &\rightarrow 0011 \ 1101_2 \quad 12_{10} = 1100_2 \\
 61.52 &\rightarrow 0011 \ 1101_2 \quad 13_{10} = 1101_2
 \end{aligned}$$

Using the method will be more reliable rounding the value of image elements in HLS models to the next integer part of the value this element is used to change the lowest bit. For comparative analysis of methods, will modify the lowest bit of the image element when using the whole part. To do this, convert each value of the component elements to binary form. After that let's change the lowest bit of the binary value and reverse it to a decimal view. Change the low bit and reverse transformation and sum of absolute difference values each corresponding element are shown in this calculations:

$$\begin{aligned}
 0011 \ 1100_2 &\rightarrow 60_{10} \quad 61.93_{10} - 60_{10} = |1.93_{10}| & (3) \\
 0011 \ 1100_2 &\rightarrow 60_{10} \quad 61.81_{10} - 60_{10} = |1.81_{10}| \\
 0011 \ 1100_2 &\rightarrow 60_{10} \quad 61.74_{10} - 60_{10} = |1.74_{10}| \\
 0011 \ 1100_2 &\rightarrow 60_{10} \quad 61.52_{10} - 60_{10} = |1.52_{10}|
 \end{aligned}$$

Calculate the sum of absolute difference values each of the corresponding elements before and after steganographic conversion. It is: $1,93 + 1,81 + 1,74 + 1,52 = 7$.

Let's perform a similar transformation using the method of rounding element value a component of a bitmap image component for changes to the junior bit. We will round the elements to the next integer part.

So to change the lowest bit of the number 61.93 round-up its value to 62. Then we have $62_{10} = 0011 \ 1110_2$. After that, we get decimal values of elements with modified lower bits. Thus, the sum of absolute values of element differences: $0,07 + 0,19 + 0,26 + 0,48 = 1$. The rounding of elements and sum of absolute values of the differences of each corresponding element is shown in this calculations:

$$\begin{aligned}
61.93_{10} \square 62_{10} & \quad 61.93_{10} - 62_{10} = |0.07_{10}| \\
61.81_{10} \square 62_{10} & \quad 61.81_{10} - 62_{10} = |0.19_{10}| \\
61.74_{10} \square 62_{10} & \quad 61.74_{10} - 62_{10} = |0.26_{10}| \\
61.52_{10} \square 62_{10} & \quad 61.52_{10} - 62_{10} = |0.48_{10}|
\end{aligned}
\tag{4}$$

So, using the first method, we changed the values of image elements by seven units, and the sum of differences in the values of elements after the value of the component elements was 1. Using the rounding method reduces the difference between the values of the original image elements and the resulting image, in this case, seven times.

4. Conclusions

Thus, after conducting research on bitmap images and comparative analysis it should be noted that to increase the reliability of the steganographic system, it is optimal to embed the message in the saturation component (S) of the model HLS, and the embedding process itself should be performed using the rounding method for element values. The use of rounding allows you to reduce image distortion (container) after steganographic conversion and increase the resistance of the steganographic system to attacks.

5. References

- [1] V. Serdyuk, Information security of automated systems of enterprises, Accountant and computer 1 (2007).
- [2] V. Gribunin, I. Okov, I. Turintsev, Digital steganography, Solon-Press, 2002.
- [3] V. Porev, Computer graphics: textbook. The allowance, BWH-Petrburg, 2004.
- [4] O. Yudin, Y. Symonychenko, A. Symonychenko, The Method of Detection of Hidden Information in a Digital Image Using Steganographic Methods of Analysis, in: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 262-266, doi: 10.1109/ATIT49449.2019.9030479.
- [5] W.-Y. Chen, Public-key image steganography using discrete cosine transform and quadtree partition vector quantization coding, Optical Engineering 42 (10) (2003) 2886-2892.
- [6] O. Yudin, et al., Efficiency Assessment of the Steganographic Coding Method with Indirect Integration of Critical Information, in: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 36-40, doi: 10.1109/ATIT49449.2019.9030473.
- [7] D. Vatolin, et al., Methods of data compression. The device of archivers, compression of images and video, DIALOG-MEPHI, 2002.
- [8] G. F. Konakhovich, A. Yu. Puzyrenko, Computer steganography. Theory and practice, MK-Press, 2006.