Steganographic algorithm using the different color components of a 24-bit image

Veselka Stoyanova[1], Ilian Lilov[2]
National Military University, Faculty of Artillery, AAD and KIS, Shumen,Bulgaria[1]
National Military University, Veliko Tarnovo, Bulgaria[2]
veselka_tr@abv.bg

Abstract: *The article deals with the steganography system which hides text inside images without losing data in components of RGB model The secret message is hidden in the cover image using Least Significant Bit (LSB) algorithm. The comparative results for the proposed algorithm are very promising for blue components of image. To evaluate steganography system properties are used the measures like Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PRSN), Mean Squared Error (MSE) and Structural Similarity Index for measuring (SSIM). The aim of the study is to determine whether there is a change in the qualitative characteristics of the stego image, when it is hidden the same information, but in a different color channel, to determine which color channel shows the most invisibility to others and is it advisable to be used in the transmission of confidential information.*

Keywords*: STEGANOGRAPHY, LSB, RGB, IMAGE*

1. Introduction

Development and improvement of information and communication technologies create the establishment of a global digital environment, they offer new opportunities for the restoration of personal, business and institutional communication and interaction, predetermining various limitations.

A matter of ensuring the secure and hidden transmission of information with extremely up-to-date and subject to much research.

Steganography is the art and science of hiding messages inside a digital medium in such a way that only the sender and the receiver, can view the hidden message [7],[8]. However, the *steganographic capacity* is the maximum number of bits that can be embedded in a given cover image with a negligible probability of detection by an adversary[9]. Therefore, the embedding capacity is larger than the steganographic capacity [10]. Steganography modification principle [2] is used to implement the functions of embedding and retrieving data in the cover image, where the pre-existing cover images are changed during the process of embedding. An algorithm is used for insertion into the LSB (Last Significant Bit) for hiding information in image [1], [2], [7]. Through the LSB method is obtained embedding of the message bits in the last significant bits of the color components of individual pixels of the image. It is symmetrical, which means that for embedding and extracting a message, identical operations are performed in the same order. The effect of the algorithm is based on the fact that the secret information is stored in the last significant bits of the pixels of an image, without causing visible differences in its view [1]. It's even a way to transmit information between different groups with dangerous ideas for national security [6]. Steganalysis is used to detect the stego objects and extract the secret messages.

Fig. 1 illustrates some essential factors in Steganography.

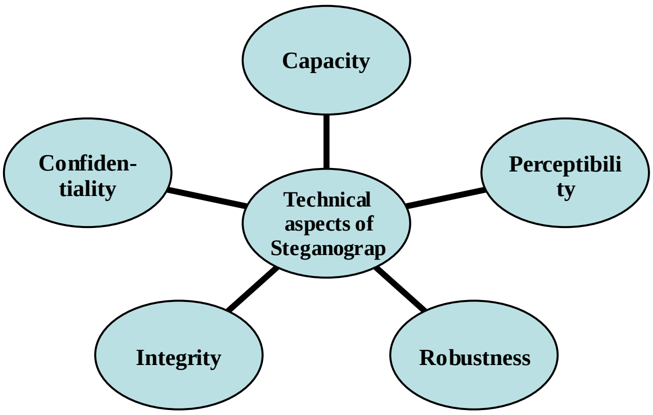


Fig.1 *Some factors that we should consider while evaluating a Steganography algorithm*

2. Steganographic algorithm using the different color

Color images have 3 color channels that can be interpreted in different ways. After preparing the cover image to hide confidential information in it is necessary to select an algorithm by which to perform the hiding. An RGB image has three channels: red, green, and blue. The algorithm allows to manipulate the individual color channels independently, hiding information separately in each of them or realizing combinations of the three possible color channels. This algorithm reduces the maximum capacity of the hidden information in cases where only one of the color channels (red, green or blue) or a combination of two of them is used. Fig. 2 shows a scheme of hiding information in all three color channels.

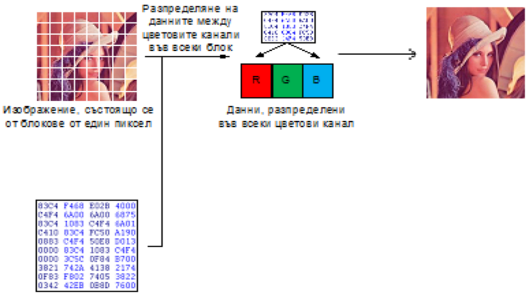
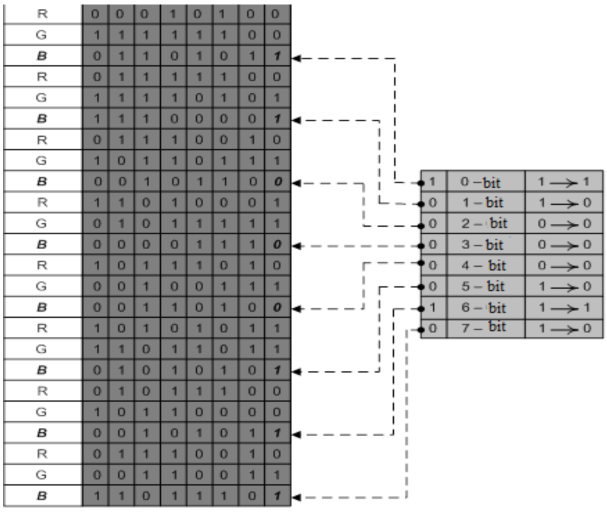


Fig. 2 *Hide information in the three color channels*

If 1 byte of information can be hidden in three pixels when using all three color channels, the same amount of information will be hidden in eight pixels if only one color channel is used. Fig. 3 shows how to hide one byte of information only in the blue color component.



R	0	0	0	1	0	1	0	0
G	1	1	1	1	1	1	0	0
B	0	1	1	0	1	0	1	*1*
R	0	1	1	1	1	1	0	0
G	1	1	1	1	0	1	0	1
B	1	1	1	0	0	0	0	*1*
R	0	1	1	1	0	0	1	0
G	1	0	1	1	0	1	1	1
B	0	0	1	0	1	1	0	*0*
R	1	1	0	1	0	0	0	1
G	0	1	0	1	1	1	1	1
B	0	0	0	0	1	1	1	*0*
R	1	0	1	1	1	0	1	0
G	0	0	1	0	0	1	1	1
B	0	0	1	1	0	1	0	*0*
R	1	0	1	0	1	0	1	1
G	1	1	0	1	1	0	1	1
B	0	1	0	1	0	1	0	*1*
R	0	1	0	1	1	1	0	0
G	1	0	1	1	0	0	0	0
B	0	0	1	0	1	0	1	*1*
R	0	1	1	1	0	0	1	0
G	0	0	1	1	0	0	1	1
B	1	1	0	1	1	1	0	*1*

1	0 – bit	1 → 1
0	1 – bit	1 → 0
0	2 – bit	0 → 0
0	3 – bit	0 → 0
0	4 – bit	0 → 0
0	5 – bit	1 → 0
1	6 – bit	1 → 1
0	7 – bit	1 → 0

Fig. 3 *Scheme for hiding information in the youngest bits of the blue color channel*

If this algorithm is combined with an algorithm that allows more than one lower bit to be used in the color channel of the pixel, such a reduction in the size of the hidden data will not be observed. In this case, the capacity to hidden information in an image will increase proportionally, but this will be at the expense of its quality.

The aim of the study is to determine whether there is a change in the qualitative characteristics of the stego image, when it has hidden the same information, but in a different color channel, to determine which color channel shows the most invisibility to others and it is advisable to be used in the transmission of confidential information.

The characteristics studied are represented by formulas (1) and (2), the *PSNR* is based on values obtained for the *MSE*:

$$(1) \qquad MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2,$$

Where m and n are the width and height of the image; $I\ (i, j)$ and $K\ (i, j)$ are relevant pixels with coordinates (i, j) in the original stego-image.

$$(2) \qquad PSNR = 10.\log_{10}\left(\frac{max^2}{MSE}\right) = 10.\log_{10}\left(\frac{max}{\sqrt{MSE}}\right),$$

where *мах* = 255 for 8 bit images[1].

The SSIM index (Structural Similarity Index for measuring) is similar to the MSE and the PSNR, but is designed to improve them both. As an indicator it measures changes in brightness, contrast and structure of an image. In [3], the brightness, contrast, and the value of structural similarity are represented. Average value for the *SSIM* index

$$(3) \qquad SSIM(x,y) = [l(x,y)]^{\alpha} . [c(x,y)]^{\beta} . [s(x,y)]^{\gamma},$$

Where $\alpha > 0$, $\beta > 0$ and $\gamma > 0$ are parameters which determine the relative importance of the three components in the value of the $SSIM(x,y)$. In the article was accepted equal importance of brightness, contrast and value of structural similarity, i.e. $\alpha = \beta = \gamma = 1$ and $C_3 = C_2/2$.

3. Experimental results.

The proposed algorithm can work with BMP, PNG and TIFF file formats of images without size limitations. Since it does not have a block for pre-compression, the maximum amount of information that will be embedded in the image is determined depending on the size of the carrier file minus the information in the header file (service information), while also allocating bytes for the generated code of the password.

By implementing a program system for embedding/ extracting text messages many tests with different size messages and images have been carried out. The studied algorithm is based on the LSB method applied and tested on BMP image formats. Test results of the qualitative characteristics MSE, SNR, PSNR, SSIM and E are analyzed. Visual analysis of the compared images shows lack of visual differences in visual control. Histogram analysis and the results of the qualitative characteristics are obtained by MATLAB.

The amount of the stego-file is the same as that of the carrier file. A stego-key can be typed in the algorithm

We have tested the proposed algorithm for around 20 different cover images of BMP format. Every pixel contains 24 bits (for 8-bit representation) each one as 8 bit components in pixel. In the proposed method, all the three components have been used for data embedding. First, each color component from a pixel is separated and three separate M*N matrix is obtained. The purpose of the study is to determine whether there is a change in the qualitative characteristics of the stego image, when it was hidden the same information, but in a different color component, to determine which of them shows the greatest invisibility to others and it is advisable to be used in the trans. Table 1 presents the results for the studied quality characteristics in hiding 60 kB information. One of the least significant bits is used to hide the information and these settings are combined with the selection of the three color components of the individual pixels of the *Parrots.bmp* image alone or in combination.

Table 1*: Investigated quality characteristics when hiding 60k B text in Latin, using a different combination of color components in the pixels in the image Parrots.bmp use the one LSB*

№	LSB	Color compon ent	MSEavr	SNR	PSNR	E
1.	1bit	RGB	5,05765e-4	64,5345	71.2806	7,6201
2.	1	Red	1,344 e-4	74,2082	80,9543	7.6200
3.	1	Blue	1,3413 e-4	74,3955	81,1416	7.6200
4.	1	Green	3,477e-4	74,2205	80,9666	7.6201
5.	1	RG	7,579 e-5	74,2400	80,9861	7.6200
6.	1	RB	7,587 e-5	74,3261	81,0722	7.6201
7.	1	RG	0.000072	74,3534	81,0995	7.6200
8.	1	BG	0.0004199	64,8525	71,5986	7,6201

Table 1 shows the comparative results with three different color components and RGB combination using the one LSB. The results in Table 1 correspond to those presented in Fig. 4 and fig. 5, from which it can be easily established and concluded that the blue color channel has the best performance in combination with the use of only one low bit.

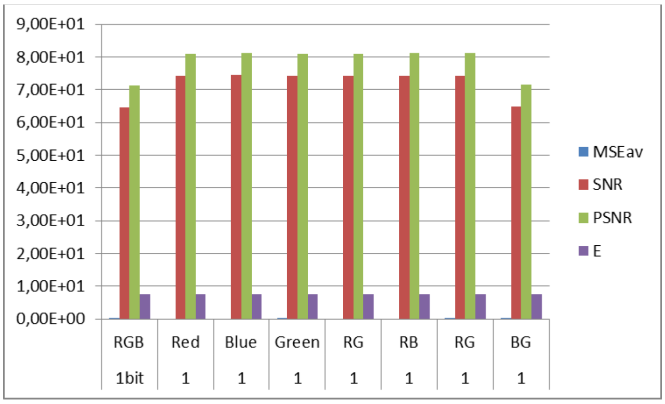
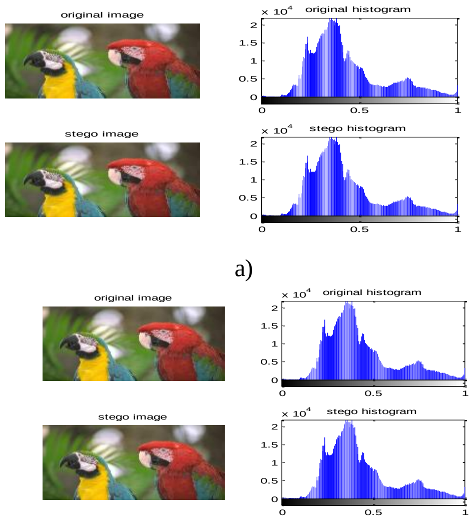


fig.4 *Diagram of quality characteristics for evaluation of the hiding of 60kB text in Latin, in different color channels in Parrots.bmp*



a)

b)

fig.5 *Presentation of original and stego image of Parrot.bmp and their histograms, with embedded a) 40kB and b) 60kB information*

Table 2 shows the comparative results with three different color components and RGB combination use the two LSB.

***Table 2:** Investigated quality characteristics when hiding 60k B text in Latin, using a different combination of color components in the pixels in the image Parrots.bmp use the two LSB*

№	LSB	Color component	MSEavr	SNR	PSNR	E
1.	2	RGB	0.0004786	64,1356	70,8817	7.6201
2.	2	Red	3,3002 e-4	70,9295	77,6756	7.6200
3.	2	Blue	4,2566 e-4	70,7788	77,5249	7.6201
4.	2	Green	3,0825e-4	71,1253	77,8714	7.6200
5.	2	RG	1,756 e-4	70,8061	77,5522	7.6200
6.	2	RB	1,756 e-4	70,8809	77,6270	7.6200
7.	2	RG	0.0001801	70,8915	77,6377	7,6200
8.	2	BG	4,884 e-4	64,6990	71,4451	7.6201

Fig. 6 presented PSNR between cover image and stego-image, and corresponding to the results in Table 2.

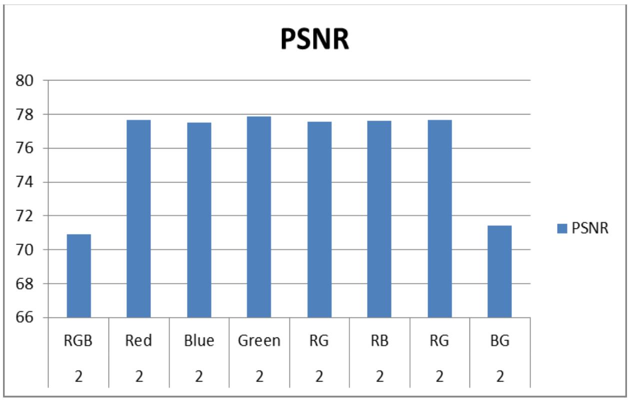


fig.6 Diagram of PSNR for evaluation of the hiding of 60kB text in Latin, in different color channels in Parrots.bmp use the two LSB

From above experimental results, it is apparent that each stego-image is almost analogous to corresponding cover image and shows better imperceptibility. That is deterioration of the quality of images due to the embedding of the secret messages cannot be distinguished.

Steganalysis intends to find the secret information that carries some stego-information by attacking the security of the used steganography algorithm[9]. Best images to hide information in them are Bitmap 24 bit images since they are considered as the largest and highest quality image file types. When an image has a high image quality and capacity, the information can be easily hidden[11].

4. Conclusion

Data hiding is a challenging and most important task in the field of information security.

The results from the research can be summarized in the following conclusions about the characteristics of the studied steganography algorithm:

It is noticed that the blue color channel has the best qualities compared to the other two (red and green) when using the one LSB, although the difference is only one in the indicator, it is with about 0.2% better values. But when we use the two LSB it is noticed that the green color channel has the best qualities compared to the other two (red and blue).

The research was carried out using different dimensions of the hidden data. It should be noted that files larger than 60 kB can hardly be hidden in just one color components.

It could be recommended when using the algorithm with different color channels, which is applied mainly to blue color, examining the best characteristics of the stego image.

Moreover, proposed method extracts the hidden secret message efficiently without using the range tables

5. References

1. Stoyanova,V. and Zh.Tasheva, *Research of the characteristics of a steganography algorithm based on LSB method of embedding information in images*, Machines. Technologies. Materials.Vol. 9 (2015), Issue 7, pg(s) 65-68,. https://stumejournals.com/journals/mtm/2015/7/65
2. Cole, E., „*Hiding in Plain Sight: Steganography and the Art of Covert Communication*", Wiley Publishing, Inc., Indianapolis, Indiana, (2003)
3. Wang Z., A .C .Bovik, H. R. Sheikh, and E. P. Simoncelli. "*Image quality assessment: From error measurement to structural similarity*," IEEE Trans.ImageProcessing,vol.13, Jan.(2004)
4. Tasheva, Zh., and A. Tasheva. "Combining cryptography and steganography in software system for hiding confidential information." Journal Science Education Innovation, Association Scientific and Applied Research Vol. 1, 2013, pp. 84-92 (2013)
5. Димитров, Д., *Използване на полюсни модели за формиране на базисни функции*, Сборник научни трудове, Шуменски университет, т 2, с.394 – 397, Шумен, 2009, ISBN:978-954-577- 549-6.
6. Atanasov, A., *Бежанската вълна от Сирия – заплаха за националната сигурност,* II International Scientific Conference ConfSec18, Borovec, Year 2, ISSUE 1(3) ISSN 2603-2945 (print), ISSN 2603-2953 (online)
7. H. Abdulrahman, M. Chaumont, Ph. Montesinos, B.Magnierhttps, Color Image Steganalysis Based On Steerable Gaussian Filters Bank, IH&MMSec: *Information Hiding and Multimedia Security*, Vigo, Spain. pp.109-114, Jun (2016), ff10.1145/2909827.2930799fm //hal.archives-ouvertes.fr/hal-01374101/document
8. G. Kumar and A. Rana, "*Data hiding techniques in digital multimedia*," International Journal of Engineering Science Invention Research and Development, vol. 1, pp. 333–337, 2015.
9. A. Soria-Lorente and S. Berres, A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information, volume 2017, https://doi.org/10.1155/2017/5397082
10. S. Sachdeva, A. Sharma, and V. Gill, "*Colour image steganography using modified JPEG quantization technique*," International Journal of Latest Research in Science and Technology, vol. 1, pp. 1–5, 2012.

11. A. Nejahi, F.Z. Boroujeni, *The Improvement of Steganography Function Based on the Least Significant Bit in RGB Color*, American Journal of Software Engineering and Applications, Volume 5, Issue 3-1, May (2016).