Steganography System Using More Lsbs

Veselka T. Stoyanova
National Military University, Faculty of Artillery, AAD and KIS, Shumen, Bulgaria

Abstract

Steganography is the method of hiding message in a cover object for cover communication. The article deals with the steganography system which hides text inside images without losing of data (BMP, PNG, TIFF and GIF). The secret message is hidden in the cover image using Last Significant Bit (LSB) method. Paper presents functionalities of the developing software, using LBS methods. Visual and statistical analysis of LBS method indicate the good results of its application.

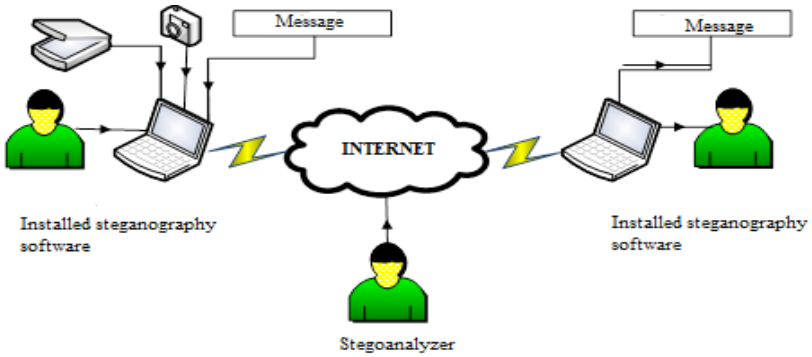
Keywords: steganography, cover image, data hiding, stego image, LSB
JEL classification: L86

Introduction

There are two main methods for hiding confidential information: cryptography and steganography (Johnson et al., 1998, Judge, 2001; Provos et al., 2003). The analysis of the methods of the computer steganography is not a single and complete activity because of the dynamic development of this scientific and applicable field and it is enough complex task (Cox et al., 2008; Arganovskiy et al., 2009; Genne, 2000; Gribunin et al., 2002).

The chart of communication between the sender of the message and the receiver is shown on Figure 1. To achieve the goal the massage, which has to be hidden, is input in the steganography software, installed on the computer of the sender, who chooses an appropriate image for the container and creates a new stego image. It is sent to the addressee by means of Internet (Koduri, 2012). He in turn reads the confidential message, using the same steganography software on his computer.

Figure 1
Chart of Communication



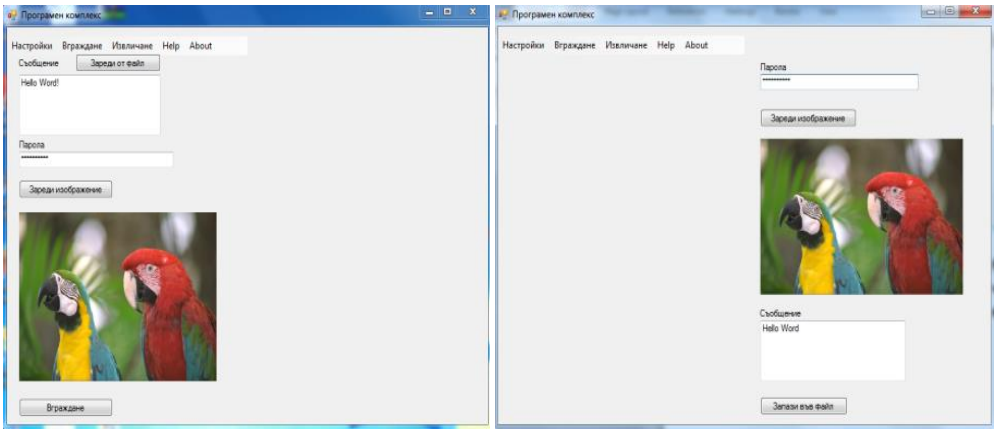
Source: Authors' work

The goal of the paper is to present functionalities of the developing software, using LBS methods, and investigate its effectiveness using visual and statistical analysis.

Methodology

The modified LSB method can be applied with BMP, PNG, GIFF and TIFF image file formats with no restriction in the size. As it has no block for preliminary compression the maximum size of the information which will be embedded in the image is fixed depending on the size of the carrying file minus the header information. The size of the stego file must be identical to that one of the carrying file. The visual presentation of the program system is shown in Figure 2 where in (a) we can see the type of the format and the necessary fields, which must be completed in order for the confidential information to be embedded in a chosen image. In (b) we can see the actions and fields which are used for the information to be extracted from the stego image.

Figure 2
Program System with (a) Embedding and Coding of the Message, (b) Extracting and Deciphering of the Secret Message in the Image



(a) (b)

Source: Author's work

As a result of the system work we get a stego image containing the confidential information which can be sent to the receiver via non protected channel without arousing any interest in the information in any spying party. The digital color images are stored in files with 24-bit format and used RGB (Red, Green, Blue) color model (Cox et al., 2008). This is precondition for a big informational excess which can be used for the purposes of the steganography.

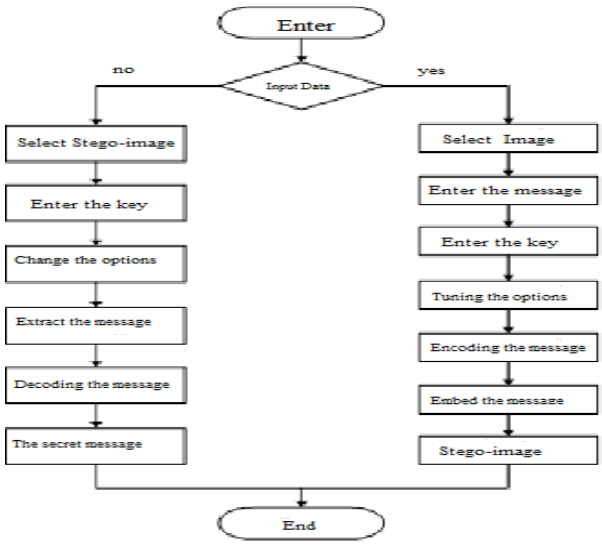
For realizing of the functions for embedding and extraction of data in the covering image we have chosen the principle of steganography by modification (Cole, 2003) in which the covering images exist preliminary and when embedded they change. We use a method inserting the least significant bit (LSB) which is often used and an easy way for hiding information in an image (Cole, 2003; Tasheva, 2011). We make embedding of the message bits in the least significant bits of the color components of particular pixels from the image. The algorithm is symmetrical, i.e. when embedding and extracting message identical operations are executed in the same order. The essence of the algorithm is based on the fact that the secret information is written in the least significant bits of the pixels of one image with no visible differences in its look.

In Figure 3 we have a block scheme of an executed algorithm in which we have a verification if there is data input or no. With the help of a conditional block we

check what operation will be executed then we go to embed or extract the confidential information.

When entering one and the same key in the party which transfers and the party which receives the message by generating a sequence of random positions of the pixels in the image the sequence is identical in the both images and in this way embedded message can be restored correctly. When entering a wrong password from the recipient we have different sequences and the read bits will not be from the hidden message.

Figure 3
Block Scheme of the Program System



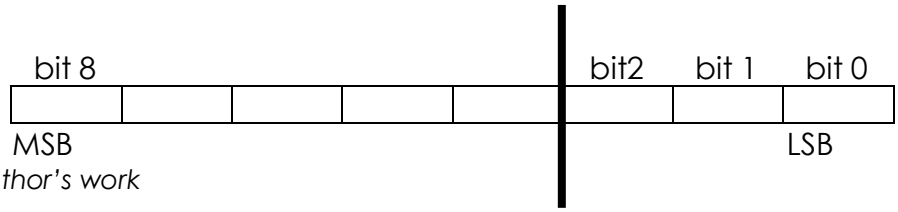
Source: Authors' work

In the concrete realization the method consists of several main steps:

1. Embedding a confidential message:
   - Enter the text which must be hidden;
   - Choose the image which must be hidden;
   - Create a key (password);
   - Choose the settings-choose number of bits;
   - Embed the message;
   - Save the stego image.
2. Extracting the confidential message:
   - Load the stego file;
   - In order to extract information the user must input a key;
   - The extraction of information is executed;
   - After completing the information the message is stored in a file.

The proposed image steganography system allows 1 byte information to be hidden in 1 pixel if there are used three of LSB of the bytes in the color channel of the pixel (Figure 4).

Figure 4
Bits of RGB Model of Image

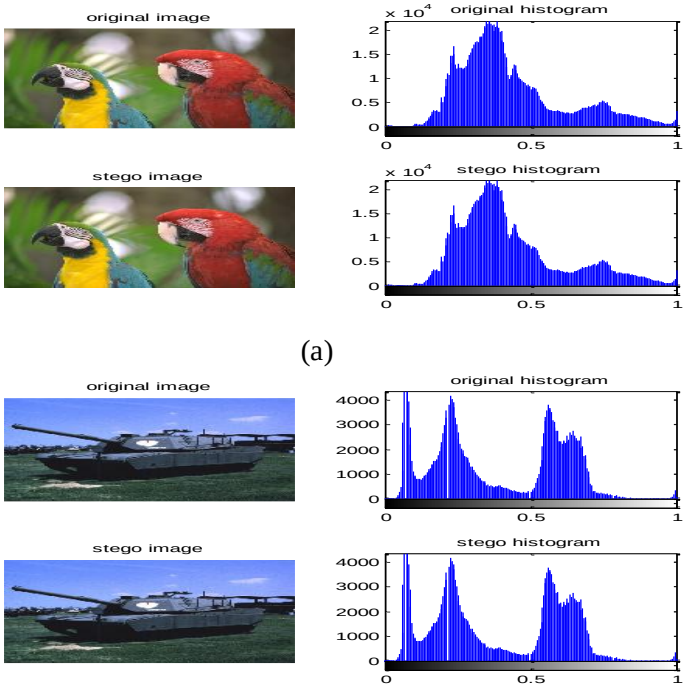


Source: Author's work

Discussion

Important characteristics which are defined in the course of the program work are: length of message, the pixels for reading and saving, the reading and saving of the concrete bits.

Figure 5
Histogram of Original Image and Stego Image Dependence of (a) SNR and PSNR and (b) MSEav. for parrots.bmp, Mage for Values of 170 to 240 kB (a) parrots.bmp, (b) amf10.bmp



Source: Author's work

The statistical characteristics of the stego image remain the same as those of the original image which can be seen from figure 5 where there are a histogram of the original image and a histogram of the stego image and there is no difference in (a) and (b).

Results

The statistical characteristics with which we check the same in the studied couples images are Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PRSN), Mean

Squared Error (MSE) and Structural Similarity Index for measuring (SSIM). They are calculated with the help of integral features of the programming environment Matlab 2014a version. In the same environment are received and histograms of the images. 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.

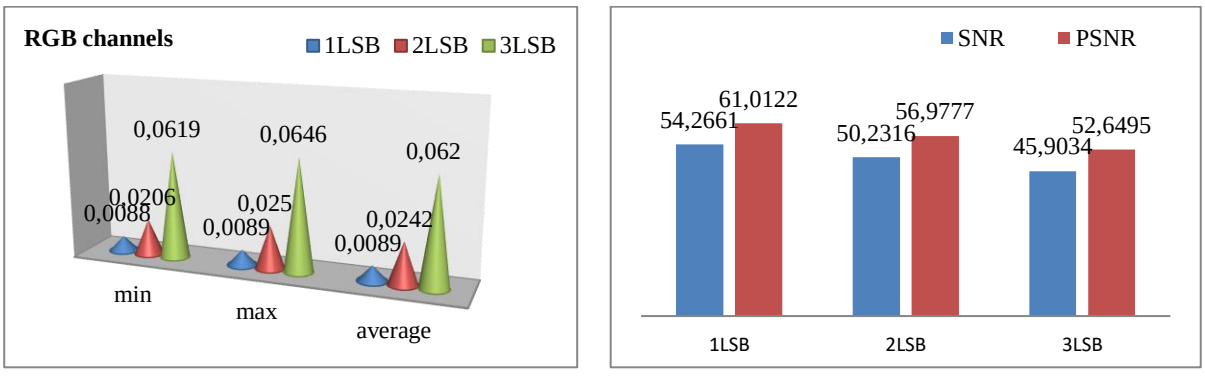
Table 1
Qualitative Characteristics of *parrot.bmp* Image with Hidden 60 kB Information in Deferent LSB

Number of LSB whit hide information	MSE_{aver}	SNR	PSNR	SSIM	Entropy
1	0,0089	54,2661	61,0122	0,998	7,6208
2	0,0242	50,2316	56,9777	0,998	7,6208
3	0,0620	45,9034	52,6495	0,998	7,6210

Note: The average MSEav. was obtained as the average of the minimum and maximum MSE.
Source: Author's work

Table 1 presents the results of the qualitative characteristics of embedded text files in English with a size of 60 kB and cover digital image *parrot.bmp* is used in different LSBs.

Figure 6
The Average MSEav. was is Visualized in the Graph of Figure 6a, SNR and PSRN (fig.6b).



(a) (b)

Source: Author's work

Table 2
The Results of Hiding Different Secret Information in Two or Three LSB in the Image (Parrots.bmp, 1536x1024)

№	Size of the hidden message	LSBs	MSE			SNR	PSNR	SSIM	E
			MSE_{min}	MSE_{max}	MSE_{av}				
1.	2 kB	2	$6{,}8622e^{-4}$	$8{,}3775e^{-4}$	$7{,}6198e^{-4}$	65,0517	71,7978	1	7.6201
2.	20 kB	2	0,0076	0,0081	0,00785	55,0173	61,7635	1	7,6203
3.	50 kB	2	0,0187	0,0205	0,0196	51,0205	57,7666	0,998	7,6207
4.	2 kB	3	0,0015	0,0020	0,00175	58,9473	65,6934	1	7,6201
5.	20 kB	3	0,0217	0,0220	0,02185	50,5248	57,2710	1	7,6204
6.	50 kB	3	0,0536	0,0557	0,05465	46,5805	53,3267	0,998	7,6209

Source: Author's work

Conclusion

The proposed image steganography method is based on modified LSB method. Steganography use in the spatial domain reaches best results concerning the histograms of the stego images, which restricts the possibility for them to yield to the modern stegoanalysis. By increasing the size of the embedding data the statistical characteristics of the images deteriorate, although, the visual quality of the images processed with steganography system remains excellent.

References

1. Arganovskiy, A. V., Balakin, A. V., Gribunin, V. G., Sapozhnikov, S. A. (2009, Steganografiya, tsifrovyye vodyanyye znaki i steganoanaliz (Steganography, digital watermarks and steganoanalysis), Vuzovskaya kniga, Moscow.
2. Cole, E. (2003), Hiding in Plain Sight: Steganography and the Art of Covert Communication, Wiley Publishing, Inc., Indianapolis, Indiana.
3. Cox, I. J., Miller, M. L., Bloom, J.A., Kalker, T., Fridrich, J. (2008), Digital watermarking and steganography. Second Edition, Elsevier Inc., Burlington, MA, USA.
4. Genne, O. V. (2000), "The Main Provisions of Steganography", Journal "Information Security. Confident", Vol. 3, pp. 20-25.
5. Gribunin, V. G., Okov, I. N., Turintsev, I. V. (2002), Tsifrovaya steganografiya (Digital steganography), Solon-Press, Moscow.
6. Johnson, N. F., Jajodia, S. (1998), "Exploring steganography: Seeing the unseen", Computer, Vol. 31, No. 2, pp. 26-34.
7. Judge, J. C. (2001), Steganography: Past, present, future, Lawrence Livermore National Lab., CA, USA.
8. Koduri, N. (2012), Information Security through Image Steganography using Least Significant Bit Algorithm, Master's Thesis, Information Security and Computer Forensics, University of East London.
9. Provos, N., Honeyman, P. (2003), "Hide and seek: An introduction to steganography", IEEE Security & Privacy, Vol. 99, No. 3, pp. 32-44.
10. Tasheva, A. (2011), "Izsledvane kharakteristikite na steganografski algoritŭm pri razlichni stepeni na zashtita" (Investigation of the characteristics of a steganographic algorithm at different degrees of protection), Sbornik s dokladi „VII Natsionalna student·ska nauchno-tekhnicheska konferentsiya 2011", Tekhnicheski universitet – Sofiya, str. 157-162.

About the author

Veselka Stoyanova, Ph.D., is an Assistant Professor at Department of Computer Systems and Technologies, Faculty of Artillery, Air Defense and KIS, National Military University of Bulgaria. She received PhD in Information and communication Systems at Faculty of Artillery, AAD and KIS, Shumen with the dissertation thesis "Improve opportunities for hiding information in communication and information systems using Steganography methods". She participated in Erasmus-Preparatory-Visit-Program in Lomza, Poland. Her main research interests are computer graphic, e-learning, programming, information and communication technology. Veselka Stoyanova published several scientific papers in international and national journals and participated in many scientific international conferences and projects. The author can be contacted at **veselka_tr@abv.bg.**