FRI-ONLINE-1-CCT2-11

ANALYSIS OF THE LEAST SIGNIFICANT BIT SUBSTITUTION ALGORITHM FOR IMAGE STEGANOGRAPHY[27]

Eng. Petar Stoilov, PhD Student
Department of Telecommunications,
University of Ruse "Angel Kanchev"
Phone.: +359 88 79 79 174
E-mail: pstoilov@uni-ruse.bg

Assoc. Prof. Georgi Hristov, PhD
Department of Telecommunications,
University of Ruse "Angel Kanchev"
Phone: +359 82 888 663
E-mail: ghristov@uni-ruse.bg

Assoc. Prof. Plamen Zahariev, PhD
Department of Telecommunications,
University of Ruse "Angel Kanchev"
Phone: +359 82 888 663
E-mail: pzahariev@uni-ruse.bg

Abstract: *Steganography is a science focused on the information protection by hiding the secret data in different types of public media, mainly images and videos. This paper presents an overview of Least Significant Bit (LSB) substitution algorithm. The advantages of Least-Significant-Bit (LSB) steganographic data embedding are that it is simple to understand, easy to implement, and it results in stego-images that contain hidden data, yet appear to be of high visual fidelity The first part of the paper presents a brief analysis on the steganography algorithm. The next part of the paper presents the Least Significant Bit substitution used to hide data on coloured cover images. In the current classical LSB substitution method, the data is hidden in sequence.*

Keywords: *steganography, cryptography, LSB embedding*

INTRODUCTION

The term steganography refers to a technique that aims to hide the communication between two interlocutors. Unlike encryption, which allows you to encrypt a message to make it incomprehensible if you do not have the key to decipher it, steganography aims to keep the very existence of the message away from prying eyes, by hiding it (Kekre et al., 2012).

Cover images with hidden message embedded in them are called stego-images. For hiding data, image quality refers to the quality of the stego-image. One of the most common techniques of hiding a message in image is based on manipulating the least significant bit (LSB) (Petitcolas et al., 1999). It represents replacement of the least significant bit of the cover image with message bits. LSB methods usually achieves high capacity.

Steganography today presents itself as an ideal tool for the creation of secret communication channels, which can be used in sophisticated scenarios of espionage, computer crime and violation of privacy of both public and private subjects. There are many papers and articles, which discuss the techniques for hiding messages (text, image, video, etc.) by specifying the range for pixel values and embedding the required MSB (Most Significant Bit) into the LSB (Least Significant Bit) of the cover image (Kekre et al., 2012).

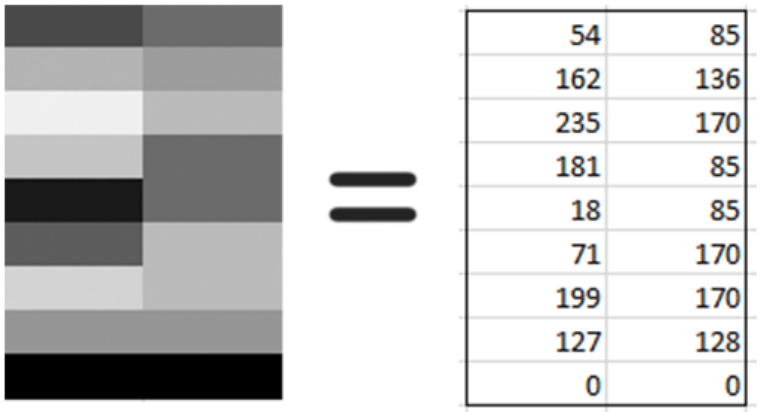
[27] Докладът е представен на заседание на секция 3.2 на 29 октомври 2021 с оригинално заглавие ANALYSIS OF THE LEAST SIGNIFICANT BIT SUBSTITUTION ALGORITHM FOR IMAGE STEGANOGRAPHY

EXPOSITION

The Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file (Kahn, 1996). This technique can be used for hiding images in 24-bit, 8-bit or gray scale format (Johnson et al., 1998). In this paper, an emphasis is made on the image Steganography that provides a strong focus on the LSB technique. The paper explains the LSB embedding technique and presents the evaluation results for 1,2,3 and 4 Least significant bits. When selecting the message image and embedding it in the cover image, it is necessary to choose the required number of bits to hide the MSB (Most Significant Bit) of the message image behind the LSB (Least Significant Bit) of the cover image. Since the MSB contains the most important information of the image and the LSB contains the least important information of the image, replacing the LSB of the cover image with the MSB of the message image will help form a stego image, which will contain the secret message. In recent times trends are of using digital image files as a cover file to hide another digital file that contains the information. LSB replacement is a common and simple approach to embed information in an image, but it is vulnerable to even slight image manipulation. The method itself can be destroyed easily with simple attacks (Chan et al., 2004).

Hiding the data by taking the cover object as the image is known as image steganography. In digital steganography, images are a widely used cover source, because there is a huge number of bits present in the digital representation of every image. There are lots of ways to hide information inside an image.

Consider an 8-bit grayscale image where each pixel is stored as a byte representing a gray scale value.



54	85
162	136
235	170
181	85
18	85
71	170
199	170
127	128
0	0

Fig. 1. LSB in greyscale images

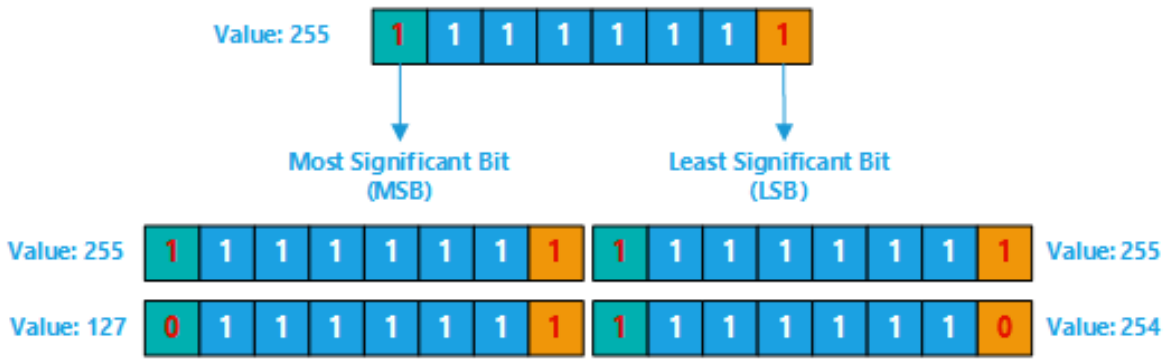


Fig. 2. LSB algorithm

EXPERIMENTAL RESULTS

This section of the paper presents the methodology for the conducted experiments and the results that were obtained. Three gray scaled cover images were used for the experimental evaluation of the presented LSB algorithm:

- building.jpg – with resolution of 960 x 640 pixels;
- dog.jpg – with resolution of 960 x 640 pixels;
- bird.jpg – with resolution of 960 x 707 pixels.

One gray scaled message image - facade.jpg, with resolution of 960 x 640 pixels is used as the original message image. Figure 3 represents the three cover images (building.jpg, dog.jpg and bird.jpg) and the original message image (facade.jpg).

The difference between the LSB is and the MSB is important here. LSB or the least significant bit is the lowest bit in a series of numbers in binary. LSB is located at the far right of the string. For example, in the binary number 01111111, the least significant bit is the far right 1. The most significant bit (MSB) is the bit in a multiple-bit binary number with the largest value. This is usually the bit transmitted first in a sequence or the bit farthest to the left. An example can be seen in Figure 2.

During the experiments, two values will be calculated and tracked and they will be used to evaluate the analyzed algorithm:

- PSNR (peak signal-to-noise ratio)
- MSE (mean square error)

All of the evaluation experiments are conducted in MATLAB and the above parameters are calculated based on the original cover image with the stego image as a reference.

```
PSNR=psnr(coverImage, stegoImage);
fprintf('PSNR %0.6f \n', PSNR);

MSE=mse(coverImage - stegoImage);
fprintf('MSE %0.6f \n', MSE);
```

To check the superiority of the stego image, these both parameters are used with the following equations:

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

where I and K correspond to the pixel value of the cover and stego images and

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

where MAX_I^2 corresponds to the maximum pixel value of the cover image.

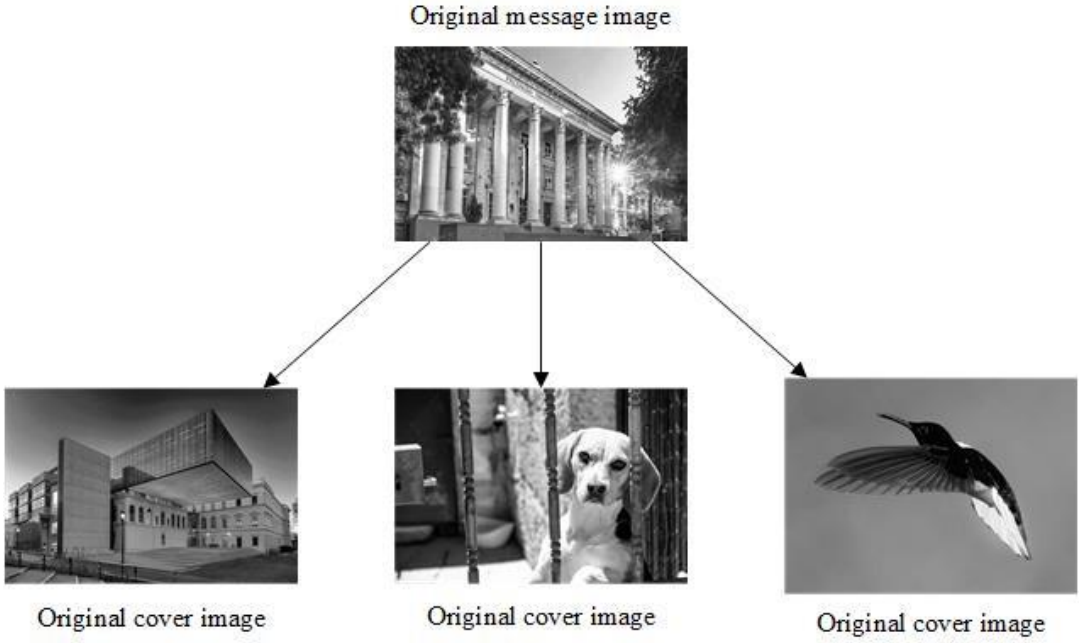


Fig. 3. Original message image and the three original cover images

It is widely known that, the lower the MSE values, the better the quality of the obtained stego image will be. The higher the value of PSNR, the better it is for the reconstruction of the image.

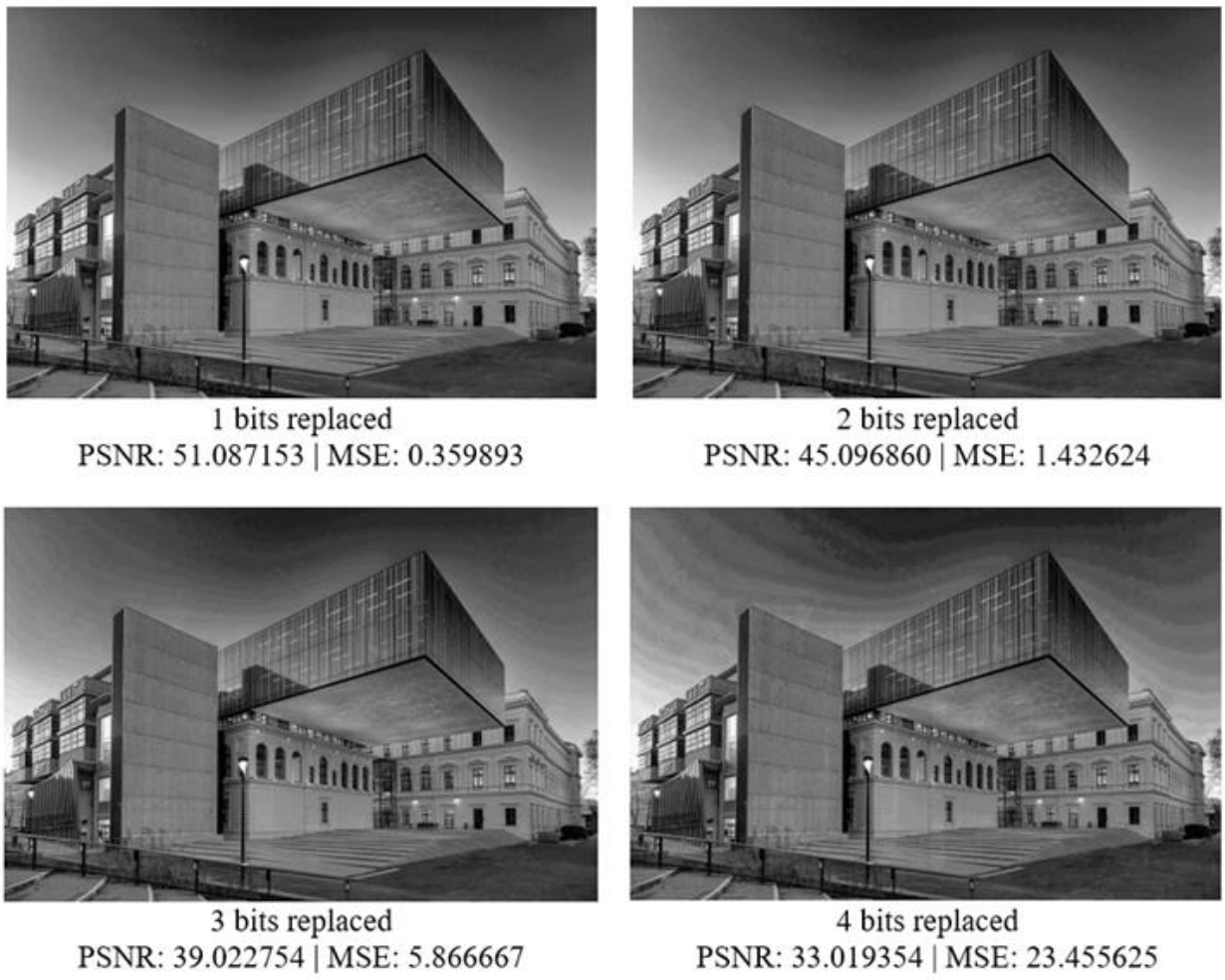


Fig. 4. Replacement of 1, 2, 3 and 4 bits in building.jpg

In Figure 4, the cover image used is building.jpg with 960 x 640 pixels in size and the message image, fasade.jpg, is with 960 x 640 pixels in size. Even though the differences between these images is not noticeable in the scenarios with 1- and 2-bits replacement, its MSE values vary, which is evident in Table 1. Bigger differences, which are also more noticeable for the human eye, are the results when 3 and 4 bits are replaced. In these scenarios, the MSE also increases drastically, while the quality decreases.

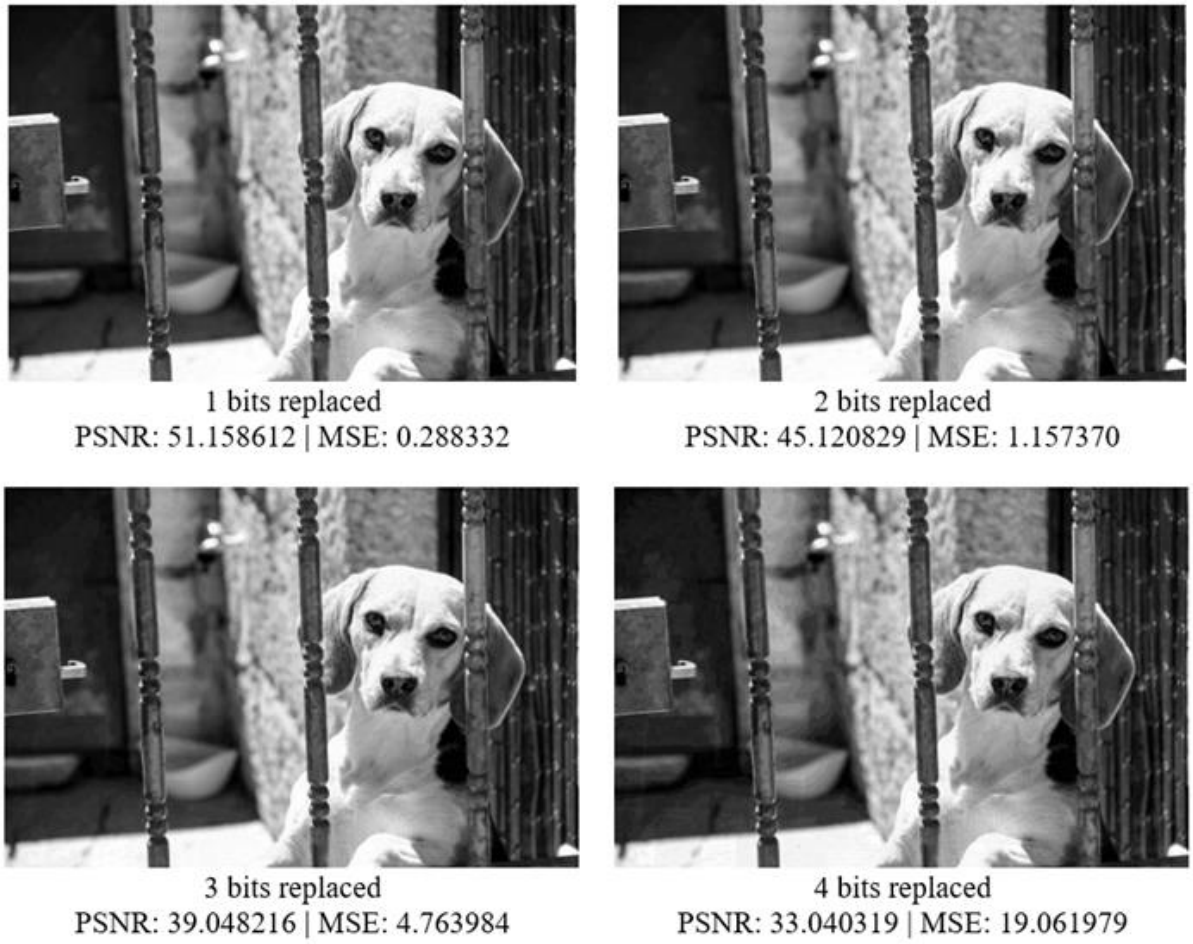


Fig. 5. Replacement of 1, 2, 3 and 4 bits in dog.jpg

In Figure 5 the cover image used is dog.jpg with 960 x 640 pixels in size and the message image, fasade.jpg, is with 960 x 640 pixels in size. Even though the differences between these images is not noticeable in almost all scenarios with bits replacements, the MSE values vary, which is also evident in Table 1. In these experiments the differences are not that noticeable for the human eye.

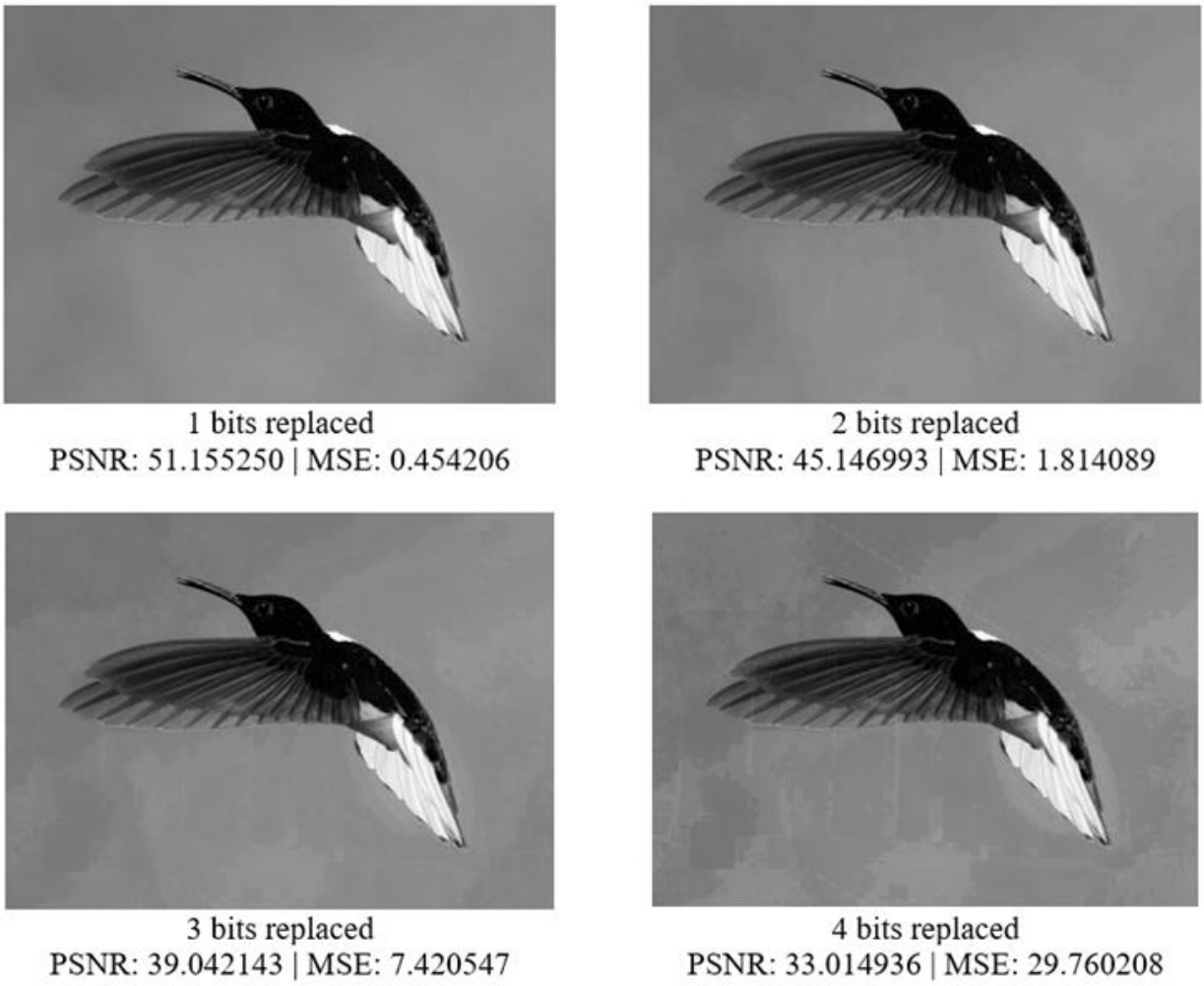


Fig. 6. Replacement of 1, 2, 3 and 4 bits in bird.jpg

In Figure 6 the cover image used is bird.jpg with 960 x 707 pixels in size, while the message image, fasade.jpg, is with 960 x 640 pixels in size. Here the difference can be seen at the 2 bits replacement scenario, although the MSE values are closer to the ones from the other experiments. In the 4 bits replacement scenario, a part of the message image can be seen. Replacement of bits, such as the 4, 3, 2 and 1 bit is smaller, as compared to replacing bits like 6 and 7, since in the latter case the message is visible in the stego image itself.

Table 1. Experiment results

LSB	BITS	PSNR	MSE
Fig. 4 (building.jpg)	1 bit	51.144668	0.361281
	2 bits	45.134409	1.443294
	3 bits	39.142881	5.761094
	4 bits	33.065260	23.378021
Fig. 5 (dog.jpg)	1 bit	51.245234	0.342359
	2 bits	45.076423	1.420303
	3 bits	39.083159	5.861858
	4 bits	32.286958	29.223857
Fig. 6 (bird.jpg)	1 bit	51.110155	0.367655
	2 bits	45.071904	1.469648
	3 bits	39.013029	5.911250
	4 bits	32.983376	24.093750

CONCLUSION

After comparing the different stego-images obtained from the implementation of the LSB substitution technique, several conclusions can be formulated. As seen from Table 1, the MSE (Mean Squared Error) values for Figure 4, Figure 5 and Figure 6 with the 4 bits substitution are dramatically higher in comparison to the MSE values when 3 bits are replaced. The value of the MSE drastically jumps from a single digit to a double digit. Example can be given in Figure 4 - 5.761094 to 23.378021, which illustrates that there is a high rate of mean squared error. In this case the stego image and the original cover image show major differences in terms of their pixel values. Similar conclusions are also drawn in the experiments of other authors (Chan et al., 2004).

In the presented experiments, the secret messages are embedded in the cover files directly. The least significant bits (LSB) are replaced with bits from the secret message/image. Noticing the slight difference is not easy. Therefore, this method exploits the natural weakness of the Human Visual System (HVS) therein, as described by Chan et al., 2004.

This method can be used for grayscale images and color images by changing some the 8 bits of the image data for the grayscale image, so that the alteration of the image is not perceptible for the human eye. Advantages of the LSB technique are that the original image degradation is not easy to detect and the hiding capacity is larger, which means that more information can be stored in an image object. Disadvantage of this LSB technique is that the robustness is low, therefore the hidden information can be destroyed by attacks.

Converting an image from a format like JPEG to BMP or PNG and back could destroy the hidden information stored with the LSB algorithm. Altering the LSB will only cause minor changes in the color or the grayscale values and this is why it is usually not noticeable by the human eye (Johnson et al., 1998). The LSB technique is an easy and simple method for hiding data, but stego-images can draw suspicion or be easily detected from statistical analysis (Fridrich et al., 2000).

ACKNOWLEDGMENTS

This paper is supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Ministry of Education and Science of Bulgaria.

The work presented in this paper is completed as partial fulfilment of Project 2021 – FEEA-03 “Design, FPGA implementation and investigation of digital communication devices”, financed under the Scientific and Research Fund of the University of Ruse “Angel Kanchev”.

REFERENCES

Kahn, D. (1996). *The Codebreakers - the Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, New York.

Chan, C.K., & Cheng, L.M. (2004). *Hiding data in images by simple LSB substitution*. Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong.

Johnson N., & Jajodia, S. (1998). *Exploring steganography: seeing the unseen*, IEEE Computer, pp. 26-34, Feb 1998.

Fridrich, J., Du, R., & Meng, L. (2000). *Steganalysis of LSB Encoding in Color Images*. IEEE International Conference on Multimedia and Expo., pp. 1279–1282.

Petitcolas, F., Anderson, R., & Kuhn, M. (1999). *Information Hiding – A Survey*, Proceedings of the IEEE, Vol. 87. July 1999.

Kekre, H. B., Mishra, D., Khanna, R., Khanna, S., & Hussaini, A. (2012). *Comparison between the basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB’s Method for Images*, International Journal of Computer Applications, ISSN 0975-8887, Volume 45, No.1, pp. 33-38, May 2012