Journal of American Science

Websites:
http://www.jofamericanscience.org
http://www.sciencepub.net

Emails:
editor@sciencepub.net
sciencepub@gmail.com

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

LSB BASED IMAGE STEGANOGRAPHY

*****Basawaraja and **Dr. Manoj Kumar

*****Research Scholar, Department of Computer Science, SunRise University, Alwar, Rajasthan (India)
******Associate Professor, Department of Computer Science, SunRise University, Alwar, Rajasthan (India)
Email basu.n.reddy@gmail.com

Abstract: Steganography has recently turn out to be an excellent field of science that is used to shield data from illegal entry. Steganography is described as the skill of communication which involves concealing knowledge in a different medium for instance textual, image, audio, video, or network in order not to provoke any trace; whereas steganalysis is the discipline of destroying the steganographic mechanism to expose the undisclosed communication. The efficiency of a steganography procedure is measured utilizing 3 key criteria, they include payload efficiency, image excellence calculation, and degree of protection. This investigation is concentrated on image steganography which is extremely accepted in the steganography field. The Least Significant Bit (LSB) approach is mainly the effectual method employed to entrench the undisclosed communication. The study, therefore, focused on the Least Significant Bit steganography algorithm thereby increasing its performance by proposing a modified Least Significant Bit steganography called Circular Shift LSB. The study also elucidated the LSB entrenching procedure and presented the assessment outcomes for LSB text steganography for different cover object formats such as .png, .bmp, and .jpeg. This paper has more comprehensive information on different cover image formats, focused on LSB.
[Basawaraja and Kumar, M. **LSB BASED IMAGE STEGANOGRAPHY.** *J Am Sci* 2024;20(7):5-7]. ISSN 1545-1003 (print); ISSN 2375-7264 (online). http://www.jofamericanscience.org 02. doi:10.7537/marsjas200724.02.

Keywords: Steganography, Least Significant Bit, PSNR, MSE, Comparative analysis

Introduction: Data is very much insecure in this internet dominating world now these days. Steganography is technique to hide data in given medium without suspicious of it. So, in this paper one method of data has been discussed in digital images. One image format in which each pixel is represented using 8-bit binary number whose range come from zero to 255. So gray scale image maximum having 256 colors in each pixel. LSB hiding technique uses LSB of 8-bit number representing a pixel. This LSB change due to data hiding causes less change in pixel value which is not detectable through human visual system. For measuring the effectiveness of LSB technique many mathematical parameters can be used like peak signal to noise ratio, mean square error and many others.

Communication is a rudimentary inevitability of all rising zone in the world in recent trends. The proliferation of new networking systems, in particular, the case of data networks requires a specific means of protection mechanisms. Everyone wants their data to be communicated secretly and securely [1]. Data security is a significant topic of concern when sharing facts in an exposed link because cyberspace is not solitary a sole system but a large set of networks around the globe. Network protection is becoming increasingly relevant as the amount of communication shared via Cyberspace intensified daily [2]. Data protection requires storing hidden documents, text, audio, or video files among any other archives that may be used to protect sensitive records. Recent literature works in steganography have the possibility of an anonymous individual remembering hidden knowledge. Owing to new knowledge, information performs a significant function in a wide variety of diverse areas [2, 3]. The steganography method involves masking concealed data into every single pixel's LSB in an image. Built on the LSB procedure, an 8 or 24-bit color image algorithm is established to boost the stego-image accuracy of the color object proficient in generating a hidden concealed object that is fully imperceptible to the human eye [1]. The small, important parts of each pixel can be employed to entrench the hidden communication in the concealment medium. This approach increases adjustment sensitivity but degrades the stego image quality [4].The LSB entrenching procedure implies that images could be concealed in the LSB of the concealment object so that the people's vision won't detect the concealed image in the concealment object [5]. This approach could as well be employed to conceal text in 24-bit or 8-bit or grayscale form. This research was, however, used to embed medical information into color cover file formats such

as .bmp,.png, and .jpeg using a modified LSB steganography technique called Circular Shift LSB steganography algorithm. This paper also presents a comprehensive LSB-built image steganography knowledge in various image forms.

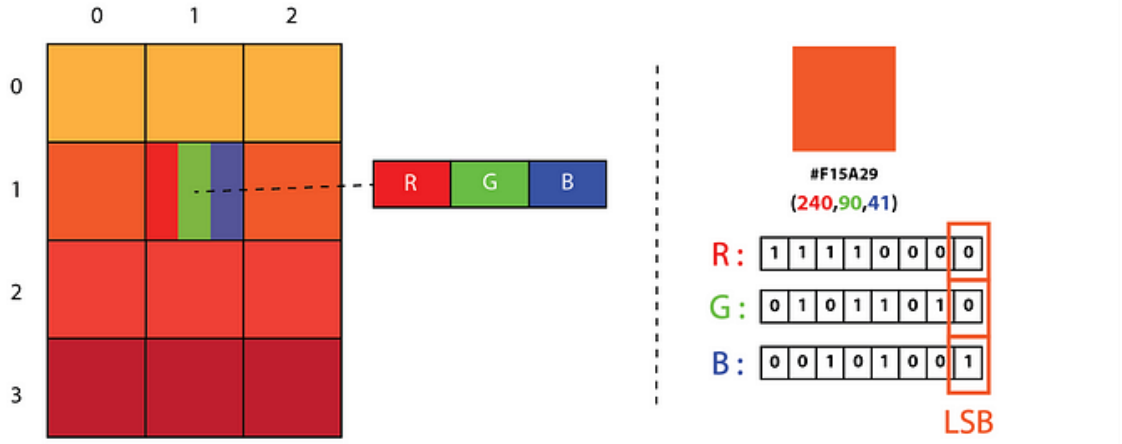
WHAT IS STEGANOGRAPHY?

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data.

LSB IMAGE STEGANOGRAPHY

LSB Steganography is an image steganography technique in which messages are hidden inside an image by replacing each pixel's least significant bit with the bits of the message to be hidden.

To understand better, let's consider a digital image to be a 2D array of pixels. Each pixel contains values depending on its type and depth. We will consider the most widely used modes — **RGB(3x8-bit pixels, true-color)** and **RGBA(4x8-bit pixels, true-color with transparency mask).** These values range from 0–255, (8-bit values).



Representation of Image as a 2D Array of RGB Pixels

We can convert the message into decimal values and then into binary, by using the ASCII Table. Then, we iterate over the pixel values one by one, after converting them to binary, we replace each least significant bit with that message bits in a sequence.

To decode an encoded image, we simply reverse the process. Collect and store the last bits of each pixel then split them into groups of 8 and convert it back to ASCII characters to get the hidden message.

LSB based Image steganography using MATLAB

Steganography is the method of hiding secret data inside any form of digital media. The main idea behind steganography is to hide the existence of data in any medium like audio, video, image, etc. When we talk about image steganography, the idea is quite simple. Images are made up of pixels which usually refer to the color of that particular pixel. In a grayscale (black and white) image, these pixel values range from **0-255**, 0 being black and 255 being white.

Concept of LSB based data embedding:

LSB stands for Least Significant Bit. The idea behind LSB embedding is that if we change the last bit value of a pixel, there won't be much visible change in the color. For example, 0 is black. Changing the value to 1 won't make much of a difference since it is still black, just a lighter shade.

The encoding is done using the following steps:

1. Convert the image to grayscale
2. Resize the image if needed
3. Convert the message to its binary format
4. Initialize output image same as input image
5. Traverse through each pixel of the image and do the following:
   - Convert the pixel value to binary
   - Get the next bit of the message to be embedded
   - Create a variable **temp**
   - If the message bit and the LSB of the pixel are same, set temp = 0
   - If the message bit and the LSB of the pixel are different, set temp = 1
   - This setting of temp can be done by taking XOR of message bit and the LSB of the pixel
   - Update the pixel of output image to input image pixel value + **temp**
6. Keep updating the output image till all the bits in the message are embedded

7. Finally, write the input as well as the output image to local system.

The dangers of LSB replacement

We have commented that the LSB replacement is insecure, which in steganography means that it is detectable. This is because embedding is done asymmetrically, that is, there is not the same probability of increasing a value as decreasing it.

When we replace the LSB of an even value (an LSB with value 0) for a bit of the message with value 1, the effect is the same as adding one to that value. Similarly, when we replace the LSB of a pixel with an odd value (an LSB with a value of 1) for a bit of the message with a value of 0, the effect is the same as subtracting one from that value. This is an asymmetric operation, in the sense that 1 is never added to an odd value and 1 is never subtracted from an even value.

Conclusion

This study examined modified Least Significant Bit (LSB) steganography for entrenching medical information in different concealment image formats such as .bmp, .png, 6 .jpeg. A comparison between the PSNR and MSE got from this study was compared and the result was also evaluated with previous concealment image formats used by other researchers. The following outcomes were deduced from this study: Firstly, it was illustrated that this modified LSB method called circular shift algorithm performed better than previous researches when compared with them. Secondly, it was deduced that concealment image with .png format is more robust in masking textual information that is it hides textual information better when compared with other image formats because it had the highest PSNR and the lower MSE which are the two metrics used in evaluating the performance of the system.

References:

[1]. Arya, A., & Soni, S. (2018). Performance Evaluation of Secrete Image Steganography Techniques Using the Least Significant Bit (LSB) Method. vol, 6, 160-165.

[2]. Rachael, O., Misra, S., Ahuja, R., Adewumi, A., Ayeni, F., & Mmaskeliunas, R. (2020). Image Steganography and Steganalysis Based on Least Significant Bit (LSB). Lecture Notes in Electrical Engineering, 605 (pp. 1100-1111).

[3]. Abikoye, O.C., Ojo, U.A., Awotunde, J.B., Ogundokun, R.O. (2020). A safe and secured iris template using steganography and cryptography. Multimedia Tools and Applications, 79(31-32), pp. 23483-23506

[4]. Taha M S, et al. "Combination of Steganography and Cryptography: A short Survey", 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019), IOP Conf. Series: Materials Science and Engineering, 518 (2019), DOI:10.1088/1757- 899X/518/5/05200.

[5]. Ogundokun, R.O., Abikoye, O.C., Misra, S., Awotunde, J.B. (2020). Modified Least Significant Bit Technique for Securing Medical Images. Lecture Notes in Business Information Processing 402, pp. 553-565

[6]. Hashim, M., Rahim, M., Shafry, M., & Alwan, A. A. (2018). A Review and Open Issues of Multifarious Image Steganography Techniques in Spatial Do-Main. Journal of Theoretical & Applied Information Technology, 96(4)

[7]. Sharma, M. K., Upadhyaya, A., & Agarwal, S. (2013). Adaptive steganographic algorithm using cryptographic encryption RSA algorithms. Journal of Engineering, Computers & Applied Sciences (JEC&AS) Volume, 2.

[8]. Latika and G. Yogita, "A Review of Steganography Research and Development "International Journal of Advanced Research in Computer Science and Software Engineering, 2015.

[9]. Champakamala and K. Padmini et al., "Least Significant Bit algorithm for image steganography ", International Journal of Advanced Computer Technology (IJACT).

[10]. Patel, F. R., & Cheeran, A. N. (2015). Performance Evaluation of Steganography and AES encryption based on different formats of the Image. Performance .

7/12/2024