The North African Journal of Scientific Publishing (NAJSP)
مجلة شمال إفريقيا للنشر العلمي (NAJSP)
EISSN: 2959-4820
Volume 1, Issue 4, October-December 2023, Page No: 54-60
Website: https://najsp.com/index.php/home/index
SJIFactor 2023: 3.733 0.63 :2023 (AIF) معامل التأثير العربي ISI 2023: 0.383

Hide Text within Image Watermarks by Employing the Least Significant Bit (LSB) Technique for Enhanced Data Security

Najat Abohamra [1*], Sabriya Alghennai Salheen [2], Abdussalam Ali Ahmed [3]
[1] Computer Department, College of Electronic Technology, Bani Walid, Libya
[2] Department of Communications, College of Electronic Technology, Bani Walid, Libya
[3] Mechanical Engineering Department, Bani Waleed University, Bani Walid, Libya

*Corresponding author: engnajat3@gmail.com

Received: September 25, 2023	Accepted: November 03, 2023	Published: November 08, 2023

Abstract:
The widespread use and rapid development of the Internet have posed a significant challenge to the security of information transmission. To address this challenge, various techniques such as steganography, cryptography, hashing, and access control have been employed for database security. Among these techniques, watermarking has emerged as a highly accurate method for ensuring data security. Watermarking can be applied to various fields, including images, audio, video, and text, with the primary purpose of securing the data.

In the context of image security, different methods have been developed for image watermarking using the Least Significant Bit (LSB) algorithm. This method is based on two parameters, namely, Standard Deviation and Mean. The image watermarking process can be achieved through two approaches, namely, using text for a secret message or using an image for a secret image. Once the information hiding message has been selected, the LSB algorithm is utilized to embed the information on the high result value of these parameters.

Overall, watermarking is a crucial technique for ensuring data security in various fields, and its effectiveness has been demonstrated through its widespread use.

Keywords: Hide Text, Image Watermarking, LSB (Least Significant Bit), Digital Images, Text Embedding, Steganography.

Cite this article as: N. Abohamra, S. A. Salheen, A. A. Ahmed, “Hide Text within Image Watermarks by Employing the Least Significant Bit (LSB) Technique for Enhanced Data Security,” *The North African Journal of Scientific Publishing (NAJSP)*, vol. 1, no. 4, pp. 54–60, October-December 2023.

Publisher’s Note: African Academy of Advanced Studies – AAAS stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

إخفاء النص في WATERMARKS للصور باستخدام تقنية (Least Significant Bit) لتعزيز أمان البيانات

نجاة أبوحمرة [1*]، صبرية الغناي صالحين [2]، عبد السلام علي احمد [3]
[1] قسم الحاسوب وتقنية المعلومات، كلية التقنية الالكترونية، بني وليد، ليبيا
[2] قسم الاتصالات، كلية التقنية الالكترونية، بني وليد، ليبيا
[3] قسم الهندسة الميكانيكية والصناعية، جامعة بني وليد، بني وليد، ليبيا

الملخص

لقد شكل الاستخدام الواسع النطاق والتطور السريع للإنترنت تحديًا كبيرًا لأمن نقل المعلومات. ولمواجهة هذا التحدي، تم استخدام تقنيات مختلفة مثل إخفاء المعلومات والتشفير والتجزئة والتحكم في الوصول لأمن قاعدة البيانات. ومن بين هذه التقنيات، ظهرت watermarking كوسيلة دقيقة للغاية لضمان أمن البيانات. يمكن تطبيق العلامة المائية على مجالات مختلفة، بما في ذلك الصور والصوت والفيديو والنص، بهدف أساسي هو تأمين البيانات. في سياق أمن الصور، تم تطوير طرق مختلفة لوضع العلامات المائية على الصور باستخدام the least significant bit (LSB) algorithm. وتعتمد هذه الطريقة على معلمتين، وهما الانحراف المعياري والمتوسط. يمكن تحقيق عملية وضع العلامة المائية على الصورة من خلال طريقتين، وهما استخدام نص لرسالة سرية أو استخدام صورة لصورة سرية. بمجرد تحديد رسالة إخفاء المعلومات، يتم استخدام خوارزمية LSB لتضمين المعلومات حول قيمة النتيجة العالية لهذه المعلمات. بشكل عام، تعد watermarking تقنية حاسمة لضمان أمن البيانات في مختلف المجالات، وقد تم إثبات فعاليتها من خلال استخدامها على نطاق واسع.

الكلمات المفتاحية: إخفاء النص، تخزين الصور، البت الأقل أهمية (LSB)، الصور الرقمية، تضمين النص.

1. Introduction

Since the advent of the Internet, data security has become one of the most crucial aspects of information technology and communication. Cryptography was developed as a means to ensure the confidentiality of communication, and various techniques have been devised to encrypt and decrypt data in order to keep messages secret.[1] However, there are instances where simply keeping the contents of a message hidden is not enough; it may also be necessary to conceal the very existence of the message. This is where the technique of watermarking images with hidden text comes into play.

Watermarking is a process that involves embedding hidden information within an image to protect its integrity or convey additional data without causing any noticeable visual changes. In the context of hiding text within a watermarking image, the Least Significant Bit (LSB) algorithm is often employed.[2]

In the realm of digital images, an image can be represented as a function of two real variables, such as a (x, y), where "a" denotes the amplitude (e.g., brightness) of the image at a specific coordinate position (x, y). Images can also be seen as a collection of objects, with regions-of-interest referred to as sub-images. The amplitude of an image is typically represented by a real or integer number. [3]

Watermarking an image with hidden text involves modifying the LSB of selected pixels in the image. The LSB is the least significant bit, which carries the least weight in the binary representation of a pixel value. By replacing the LSBs of certain pixels with bits from the text message, the text can be hidden within the image without being readily apparent to the viewer.[4]

This technique finds application in various domains, such as copyright protection, content authentication, and covert communication. By embedding text within a watermarking image using the LSB algorithm, it becomes possible to transmit hidden information in a manner that is difficult to detect, ensuring secure communication.[5]

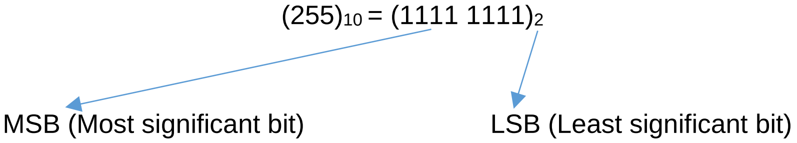
This article aims to explore the process of hiding text within a watermarking image using the LSB algorithm. By focusing on the application of watermarking techniques, specifically targeting the concealment of text, we will delve into the intricacies of this method and discuss its implications in the realm of data security.

2. Theory and concepts

2.1. <u>Bit-Plane Slicing:</u>

Here is an example of bit-plane slicing which allows the understanding of LSB hiding method, assuming the first pixel of a grayscale input image has a value of 255 (which means the pixel is perfectly white).

$$(255)_{10} = (1111\ 1111)_2$$



Changing the MSB will dramatically change the value of the pixel, making it 0 will convert the white pixel to a pure grey level, while changing LSB will not make any noticeable change, in more detailed words: clearing the MSB of the pixel binary value $(0111\ 111)_2$ will change the decimal value from 255 to 127 while clearing the LSB $(1111\ 1110)_2$ will change the value from 255 to 254 which cannot be noticed by the human eye.

For this reason, hiding secret data in LSB was widely spread and used, and for doing this, a process named ‘Bit-Plane Slicing’ was used:

The bit plane slicing is a method to slice the grayscale image to its bit components, an eight-bit gray image will be sliced into 8 binary images, each image represents the matching bit.[6]

Figure 1 shows a diagram of bit plane slicing.

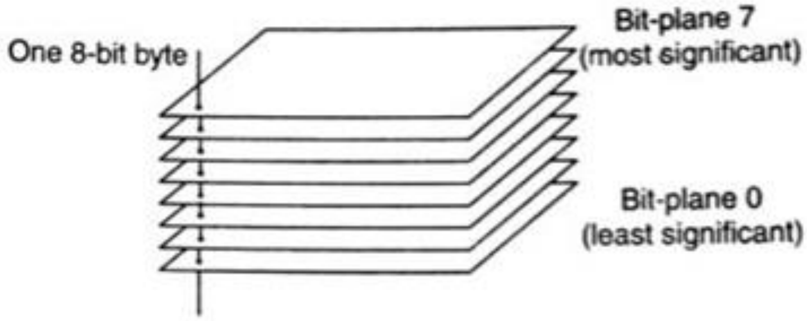


Figure 1 bit plane slicing diagram [6].

Another numerical example will be shown in Figure 2, let’s take a 3×3, 3-bit image as shown below. We know that the pixel values for 3-bit can take values between 0 to 7.

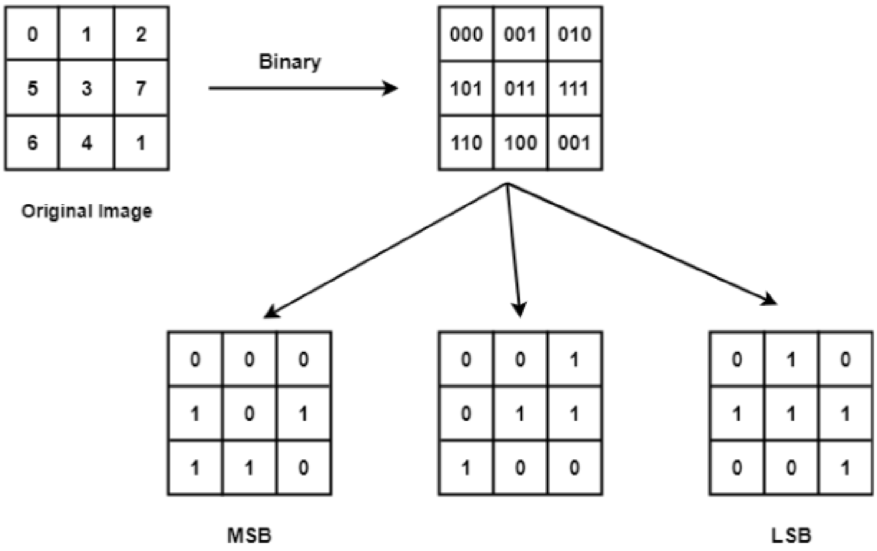


Figure 2 An example of bit plane slicing

2.2. The LSB algorithm

is currently being utilized for the purpose of steganography in digital images. This approach involves the insertion of data into the least significant bits of an image, which is a straightforward yet effective technique for embedding information. The process involves directly inserting the bits of data into the LSB of the cover image in a specific sequence.[7]

Digital images are commonly used as cover images, and they can be categorized into two types: 24-bit images and 8-bit images. In 24-bit images, up to three bits of data can be inserted into each pixel, while in 8-bit images, only one bit of data can be hidden in each pixel. The resulting image, in which the secret message is embedded, is referred to as the stego-image.

The LSB technique operates by replacing the least significant bit of each pixel with the data that is to be hidden. This replacement does not have a significant or noticeable effect on the cover image, and third-party users will not be able to detect any information embedded within it. However, there may be a minor and unnoticeable change in the intensity level of the original and stego images, but it is impossible to detect any change in the image with the naked eye.

Some approaches depend on some filters, researchers in [8] used a Laplacian filter to embed a watermark into the bit positions. Some other researchers tend to use machine learning methods to solve this task, as the researchers did in [9], by integrating artificial neural networks with the LSB method.

2.3. Research hiding/recovery pseudo code:

For this research, the steps of hiding a text in an image are:

1- Text will be converted into bits (each letter turns into 8 bits in ASCII code) meaning the phrase “Good Morning!” for example will be converted into 13*8=104 bits.
2- These bits will be hidden in the LSB image after slicing the image to its bit planes, starting from the pixel (1,1) and going on line by line.
3- To solve the recovery problem, and to ensure that the receiving side will get the exact length of text, the number of letters will be also sent in the watermarked image, exactly in the last pixel of it. Another solution is possible, when retrieving data from the watermarked image, every 8 bits will be converted into a letter, and the conversion will stop when reaching a set of zeros (end of coding).
4- For recovering the hidden data, depending on the method used to define the number of letters, each 8 bits will be set together and then converted by ASCII code to a letter of a character.

3. Simulation and result

In this section, we present the simulation setup and discuss the results obtained from the simulation of hiding a text or a phrase in an image.

3.1. Simulation Setup

The simulation framework was implemented using MATLAB's built-in image processing systems toolbox. The text message to be hidden and recovered using LSB method.

3.2. Results

The first experiments were done on a well-known image in MATLAB, which is ‘cameraman.tif’, the hidden message varied by type and length for each experiment.

The simulation process will be done in two main phases:

- Hiding phase: we start by reading the source image and writing the text that wanted to be hidden separately, then converting the text to ASCII code to become binary bits, an additional step is sending a number representing the length of message bits to the last pixel of the image, after that comes the main step of the research which is hiding these binary bits in the LSB of each pixel of the image starting from the pixel (1,1) and going on till the end of the message bits, last step is saving the watermarked image in a new file.
- Recovery phase: this phase starts by reading the watermarked image which includes the hidden message, the next step is getting the length of the message bits (from the last pixel of the image), then start to get the LSB of every pixel until it reaches the exact length, the last step is converting these bits back by ASCII to reconstruct the message letters and symbols.

Experiment one:

Hiding the word ‘Hello!’ in the image ‘cameraman.tif’. Figure 3 shows the original image and the image after hiding data in its LSB, and as it was expected, there is no way to read the word in a watermarked image, but to ensure that the word already exists.

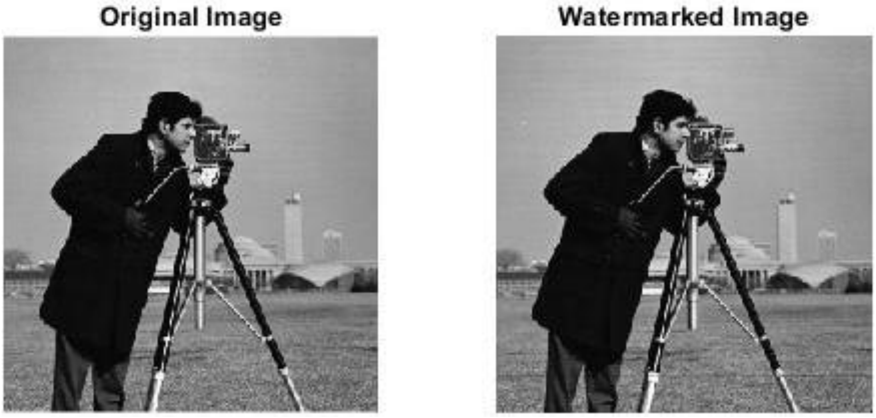


Figure 3 Original image and watermarked image – experiment one

For more details, Figure 4 will show the result of subtracting the two images (the result is a binary image consisting of zeros except the positions that contain bits of the word we hid before).

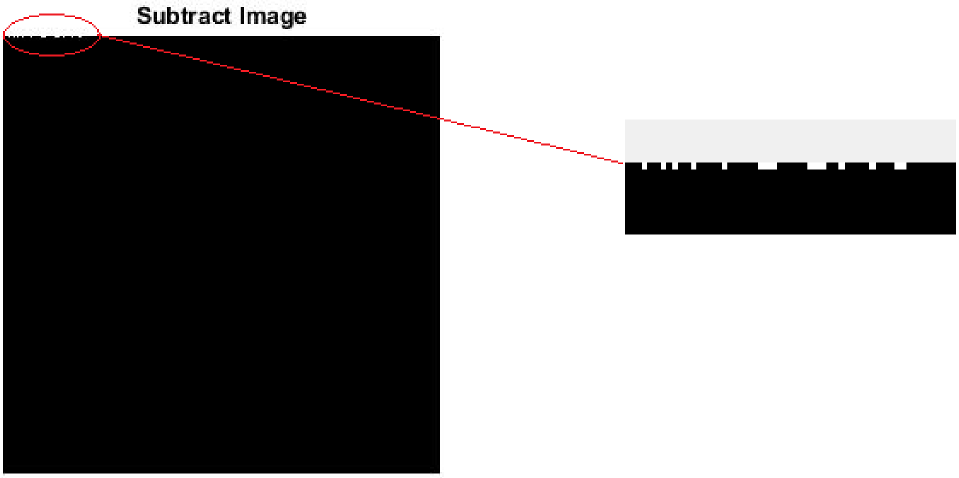


Figure 4 Hidden data in the image – experiment one.

Although the coded section of the image was declared, still the data are not readable, a conversion to characters using ASCII coding is needed.

However, the series of data is:

“01001000 01100101 01101100 01101100 01101111 00100001”

Counting stopped here because the other pixels are all zeros, means nothing else is hidden.

The last step is converting these bits into letters using ASCII: “72 101 108 108 111 33” means “Hello!”. Which is the correct hidden word?

Experiment two - Hiding the words ‘TOP Secret !!’ in the image ‘cameraman.tif’:

Hiding the words ‘TOP Secret !!’ in the image ‘cameraman.tif’. Figure 5 shows the original image and the image after hiding data in its LSB, and as it was expected, there is no way to read the word in watermarked image, but to ensure that the word already exists.

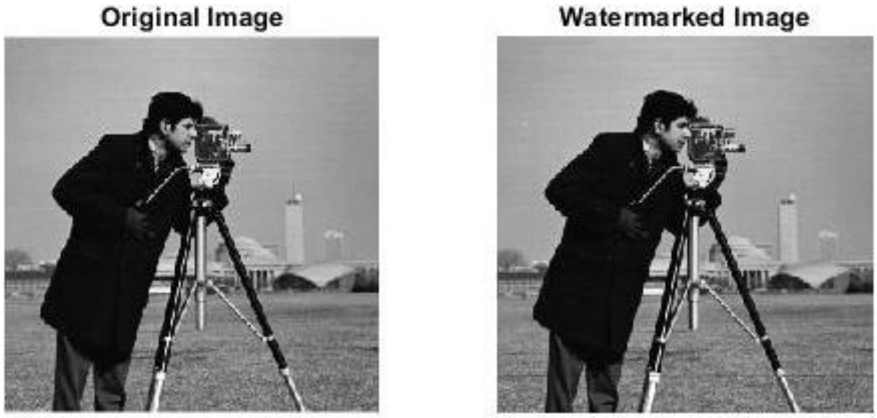


Figure 5 Original image and watermarked image – experiment two.

For more details, Figure 6 will show the result of subtracting the two images (the result is a binary image consisting of zeros except the positions that contain bits of the words we hide before).

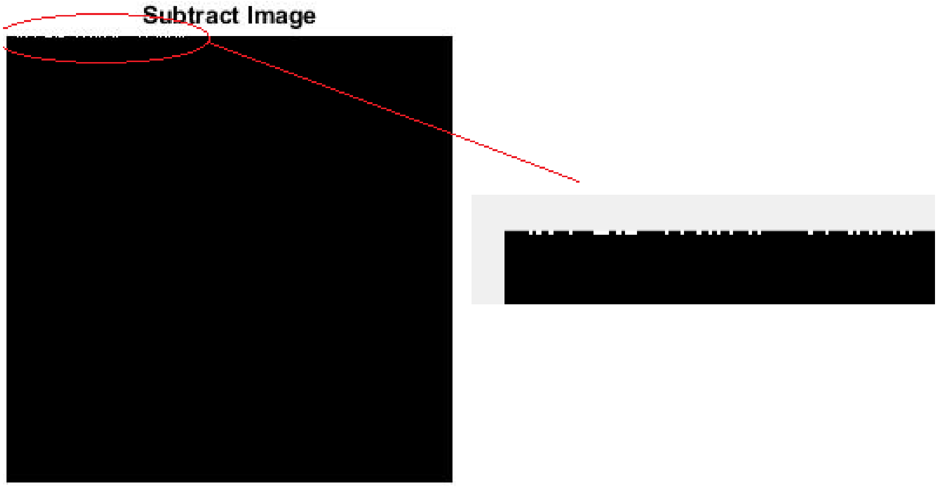


Figure 6 Hidden data in the image – experiment two.

After doing the same steps as experiment one, getting all bits and grouping them eight by eight, then converting it by ASCII, the final result is "TOP Secret!". Which is the correct hidden phrase?

4. Conclusion

In this study, we proposed a method for hiding text within digital images using the Least Significant Bit (LSB) technique. Our research aimed to address the need for an efficient and secure text hiding technique in image watermarking, catering to the requirements of copyright protection, authentication, and covert communication.

Through extensive experimentation and evaluation, we have demonstrated the effectiveness of our approach. The proposed LSB-based text hiding method achieves imperceptible embedding while maintaining a high level of resistance against various attacks and image processing operations. Our method has shown robustness against common attacks and has proven its viability in the presence of compression algorithms.

The significance of our research lies in its potential applications in digital watermarking and related fields. The ability to hide textual information within images opens up opportunities for enhanced copyright protection, secure authentication, and covert communication. By leveraging the LSB technique, we have provided a practical solution that balances imperceptibility and robustness, addressing the limitations of existing methods.

While our research has achieved promising results, there are avenues for further exploration. Future work could focus on optimizing the embedding capacity without compromising visual quality, investigating different steganographic techniques for text hiding, or exploring the integration of our method with other watermarking schemes.

In conclusion, our proposed method for hiding text in image watermarking using LSB has demonstrated its effectiveness in achieving imperceptible embedding and robustness against attacks. This research contributes to the field by providing a practical and secure approach for concealing textual information within digital images. As digital media continues to evolve, our method holds promise for applications in copyright protection, authentication, and covert communication, safeguarding the integrity and authenticity of digital content.

The advantage of LSB technique lies in its simple structure and ease of implementation. LSB method also allows high embedding capacity. The LSB technique uses an encryption key and thus it is more secure. Hiding secret data using the Steganography method lowers the chances of secret data being detected. LSB technique for digital image Steganography works smoothly for 8 bits and 24 bits BMP, GIF and PNG image formats. Using these encoding and decoding algorithms, one can retrieve the secret message exactly as the original data without altering the cover image.

5. References

[1] Begum, Mahbuba & Uddin, Mohammad Shorif. (2020). Digital Image Watermarking Techniques: A Review. Information. 11. 110. 10.3390/info11020110.

[2] Begum, M., & Uddin, M. S. (2020). Digital image watermarking techniques: a review. Information, 11(2), 110.

[3] Faheem, Z.B.; Ishaq, A.; Rustam, F.; de la Torre Díez, I.; Gavilanes, D.; Vergara, M.M.; Ashraf, I. Image Watermarking Using Least Significant Bit and Canny Edge Detection. Sensors 2023, 23, 1210. https://doi.org/10.3390/s23031210

[4] Kumar, A. (2020). A Review on Implementation of Digital Image Watermarking Techniques Using LSB and DWT. In: Tuba, M., Akashe, S., Joshi, A. (eds) Information and Communication Technology for Sustainable Development. Advances in Intelligent Systems and Computing, vol 933. Springer, Singapore.

[5] Abdul, Nada & Mustafa, Nada. (2022). An Improved Method for Hiding Text in Image Using Header Image. Wasit Journal of Computer and Mathematics Science. 1. 10.31185/wjcm.79.

[6] Nyeem, Hussain. (2017). Reversible data hiding with image bit-plane slicing. 1-6. 10.1109/ICCITECHN.2017.8281763.

[7] Faheem, Zaid & Ali, Mubashir & Arslan, Farrukh & Ali, Jehad & Masud, Mehedi & Mohammad, Shorf. (2022). Image Watermarking Scheme Using LSB and Image Gradient. Applied Sciences. 12. 4202. 10.3390/app12094202.

[8] Imran, Naveed & Hameed, S & Hafeez, Z & Faheem, Zaid & Waseem, Muhammad & Latif, U & Amin, Muhammad. (2021). Image Watermarking Approach Using LSB and Laplacian Filter. Journal of Physics: Conference Series. 2129. 012015. 10.1088/1742-6596/2129/1/012015.

[9] Farah Deeba, She Kun, Fayaz Ali Dharejo & Hira Memon (2020) Digital image watermarking based on ANN and least significant bit, Information Security Journal: A Global Perspective, 29:1, 30-39, DOI: 10.1080/19393555.2020.1717684