QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (9), No (3), Autumn 2024
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Extended Method of Least Significant Bits on Colour Images in Steganography

Alaa Jabbar Qasim
School of Computing, College of Arts and Sciences, University Utara Malaysia, 06010 Sintok, Kedah, Malaysia
alaa_jabbar@ahsgs.uum.edu.my

Roshidi Din
School of Computing, College of Arts and Sciences, University Utara Malaysia, 06010 Sintok, Kedah, Malaysia
roshidi@uum.edu.my

Farah Qasim Ahmed Alyousuf
Department of Information Technology, College of Engineering and Computer Science, Lebanese French University, Erbil, Kurdistan Region, Iraq
frhalyousuf@gmail.com

ARTICLE INFO

Article History:
Received: 15/10/2022
Accepted: 12/6/2023
Published:Autumn2024

Keywords:
LSB, Image Steganography, PSNR, Security Aspect, Data Hiding.

Doi:
10.25212/lfu.qzj.9.3.45

ABSTRACT

The rapid developments in the field of information technology have led to communication between people taking place in the virtual environment. It is of great importance to protect, hide, and secure this information, particularly in the virtual environment. Steganography is the science that ensures secure and confidential transmission of data to the intended recipient. In this field, data is sent by concealing it within various files. This paper focuses on improving the performance of image steganography through a method that involves altering the least significant three bits to hide data in colored images. Experimental studies were conducted using overlay images from standard databases with dimensions of 512 x 512. In these studies, eight-bit data was concealed within a one-pixel area, and the similarity ratios between the cover image and the stego image quality were examined.

1. Introduction

Steganography is derived from the Greek word "Steganos," meaning covert or hidden, and the word "Graphy," which refers to writing or drawing (Alyousuf, Din, Qasim, & Informatics, 2020; Qasim & Alyousuf, 2021; Qasim, Din, Alyousuf, & Informatics, 2020). The objective of steganography is to transmit confidential data to a desired destination without being understood by third parties, using a cover medium (Din, Mahmuddin, Qasim, & Technology, 2019; QASSIM & SUDHAKAR, 2015; Roshidi Din, 2018; Tayel, Shawky, & Hafez, 2012). The media used for storing confidential data include text, pictures, audio, video, or protocol files. Image steganography involves hiding information within an image using various algorithms and studies that have been conducted (Din, Qasim, & Informatics, 2019). The most significant distinction between steganography and cryptography (encryption) is that the presence of the hidden message in steganography is concealed. In other words, only the recipient of the message knows that hidden data is embedded in the cover data, while someone who possesses the cover data cannot realize the existence of the hidden data. In cryptography, it is commonly known that the sent data is confidential, and its contents cannot be understood without the secret key. Understanding the secret data requires significant effort and time. If a third party eavesdropping on two people communicating secretly realizes the confidentiality of the communication (Altaay, Sahib, & Zamani, 2012; Altaay, Zamani, Mazdak, 2012; Alyousuf et al., 2020; Din, Mahmuddin, et al., 2019; Din, Qasim, et al., 2019; Qasim & Alyousuf, 2021; Qasim et al., 2020; QASSIM & SUDHAKAR, 2015; Din, 2018; Tayel et al., 2012; Zaidan, Zaidan, Taqa, & Othman, 2009) the main purpose of steganography will not be achieved. The methods employed in image steganography can be categorized into two main groups: spatial methods and transform methods (A. A. J. Altaay et al., 2012). Spatial methods utilize the least significant bit (LSB) of the image, whereas transform methods convert the image data into frequency domain representations and store the information there. Operations in spatial methods are relatively simple, but they are sensitive to minor changes such as filtering, resizing, and compression. Data hiding techniques used in transform methods exhibit greater resilience to these changes. However, they have a lower data storage capacity compared to spatial methods (Chan & Cheng, 2004). The hash-based LSB algorithm for hiding confidential information in video steganography was proposed by (Liao, Wen, & Zhang, 2011). The LSB method, using 2-3-3 least significant bits substitution, hides data in the pixel values of the blue, green, and red channels of colored cover images (Rasmi.A, 2017). The 8-bit data of the hidden information is stored in a pixel, with the first two bits in red, the next three bits in green, and the last three bits in the blue color channel. In the proposed method, the eight-bit portion of the secret information and three bits of additional information are hidden in the red color channel, three bits in the green color channel, and two bits in the blue color channel. This paper focuses on storing high-capacity data by modifying the three least significant bits in colored images, including Lena, Nature, Peppers, and Baboon cover pictures. Hameed, Abdel-Aleem, and Hassaballah (2023) proposed a secure data hiding approach that combines least-significant-bit manipulation with nature-inspired optimization techniques. The study reported promising results, with the proposed method achieving secure data hiding while minimizing the impact on image quality. This research contributes to the field of steganography and provides valuable insights into enhancing data confidentiality in digital communication (Hameed et al., 2023). The paper is divided into five parts: the introduction, the methodology, the experimental studies and results, and the discussion.

2. Methodology

Changing the least significant bit (LSB) is one of the commonly used methods in image steganography. In this paper, an eight-bit area of one pixel in the colored cover image is modified using Matlab. Three algorithms, namely LSB332, LSB323, and LSB233, were employed to hide the data. The LSB332 algorithm involves using the last three bits of the red color channel and the green color channel of the pixel in the colored cover image. It also utilizes the last three bits and the last two bits of the blue color channel. Additionally, the information to be hidden in the cover image is encrypted with a user-defined keyword. Therefore, when retrieving the data, the person opening the text should use this keyword.

The parameters used for this study are explained below:

2.1 Hiding capacity:

In the context of image steganography, capacity refers to the amount of data that can be hidden within an image without causing significant changes to its visual appearance. The goal of steganography is to conceal the existence of the hidden data, so it's important to ensure that the modifications made to the image are imperceptible to the human eye.

The capacity of an image in steganography is influenced by several factors, including:

a. Image size: Larger images typically have higher capacity as they contain more pixels to manipulate. Each pixel can potentially carry a piece of hidden information.
b. Color depth: The color depth of an image determines the number of bits used to represent each pixel. A higher color depth allows for more bits to be utilized for hiding data, increasing the capacity.
c. Image complexity: Images with more complex content, such as detailed textures or busy backgrounds, provide better opportunities for hiding data. The variations in pixel values make it easier to embed information without noticeable changes.
d. Steganographic algorithm: The specific technique or algorithm used for embedding data in the image also affects the capacity. Some algorithms are more efficient at hiding data while minimizing visual changes, resulting in higher capacity.
e. Security requirements: The level of security desired for the hidden data can impact the capacity. If strong encryption or error correction is applied to the hidden information, it may reduce the overall capacity as additional bits are required for these purposes.

It's important to note that increasing the capacity often comes at the cost of reducing the robustness of the hidden data against various attacks or potential image modifications. Striking the right balance between capacity and robustness is a crucial consideration in image steganography.

The formula for calculating the capacity (payload) is given by dividing the total number of hidden bits by the product of the width and height of the overlay image.

2.2 PSNR:

PSNR stands for Peak Signal-to-Noise Ratio. It is a widely used metric in image and video processing to measure the quality or fidelity of a reconstructed or compressed image compared to its original, uncompressed version.

PSNR is calculated by measuring the mean squared error (MSE) between the original and reconstructed/compressed images, and then converting it to a logarithmic scale

2.3 SSIM

SSIM, short for Structural Similarity Index Measure, is a commonly used method for evaluating the perceived quality of images or video frames. It takes into account both the structural information and the similarity of pixel intensities between the original and distorted images.

While PSNR primarily focuses on pixel-level differences, SSIM incorporates the understanding of human perception by considering the structural information within the images. It assesses the similarity in terms of luminance, contrast, and structure, which are vital factors for human visual perception.

The calculation of SSIM involves comparing local image windows and computing three similarity components: luminance, contrast, and structural similarity. These components are then combined to generate an overall SSIM index. The SSIM index ranges from 0 to 1, with a value of 1 indicating perfect similarity between the original and distorted images.

Figure 1 illustrates the diagram of the LSB332 algorithm, where each eight-bit data of the hidden information is embedded in a pixel of the colored cover image (Chan & Cheng, 2004; Cvejic & Seppanen, 2004; Cvejic & Seppänen, 2005; Ker, 2005; Mitra, Roy, Mazumdar, & Saha, 2004; Parthasarathy & Srivatsa, 2005; Raja, Chowdary, Venugopal, & Patnaik, 2005).

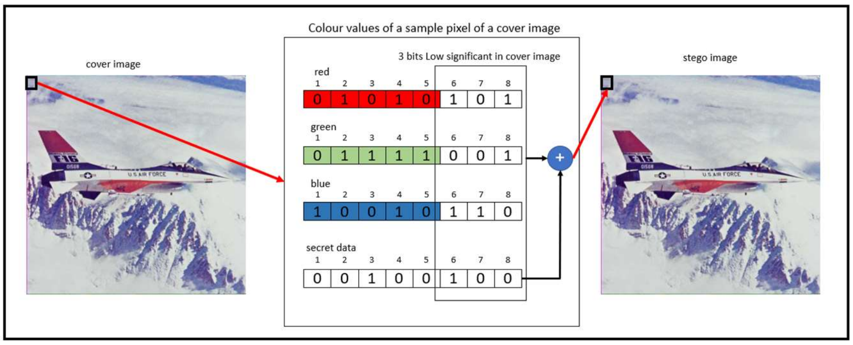

Figure (1): General diagram of 3bit LSB algorithm

The data hiding process in the 3-bit LSB algorithm follows the steps given in the pseudocode below. In the algorithm, steps are presented according to the LSB332 method (Thangadurai & Devi, 2014).

1. A pixel from the colored overlay image is selected, and the information for each color channel of this pixel is extracted and converted into binary format.
2. A one-byte portion of the data to be hidden is obtained, and its ASCII value is converted into binary format.
3. During the data hiding process:
    a. Firstly, the last three least significant bits of the red and green channels are set to zero, and the last two least significant bits of the blue channel are also reset.
    b. The first three most significant bits of the data are concealed within the last three least significant bits of the red color channel.
    c. Bits 4, 5, and 6 of the data to be hidden are embedded within the last three least significant bits of the green color channel.
    d. The 7th and 8th bits of the data are hidden within the last two least significant bits of the blue color channel.
4. The process is repeated starting from the first step until all the data to be hidden has been embedded.

3. Experimental Study

In experimental studies, LSB332, LSB323, and LSB233 methods were carried out, respectively, using 3bit LSB algorithm, and the results are presented. The study used 512 x 512 dimensions color pictures of Lena, Nature, Peppers, and Baboon in standard databases and presented in Figure 2.

Figure (2): Colored cover images used in experimental studies.

To achieve two of the most significant objectives of steganographic methods, which are maintaining the integrity of the cover image and ensuring its secure transmission, certain considerations such as PSNR and SSIM are taken into account in this study. In the evaluation phase of steganography algorithms, the Peak Signal-to-Noise Ratio (PSNR) is used to assess the quality of the stego image, while the Structural Similarity Index (SSIM) is employed to measure the similarity between the cover image and the stego image (ALabaichi, Al-Dabbas, Salih, & engineering, 2020; Alwan, Farhan, Mahdi, & Engineering, 2020; Alyousuf et al., 2020; Eskandari & Engineering, 2013; Taouil, Ameur, & Engineering, 2018). The concept of capacity (payload) is used to indicate the maximum number of bits that can be hidden. Capacity refers to the amount of data that can be concealed in a pixel, measured in bits. The formula for calculating the payload capacity is provided in in (1).

$$Capacity = \frac{total\ bits\ hid}{Width\ x\ Height\ (Overlay\ Image)} \qquad (1)$$

The formula presented calculates the PSNR value, which provides an indication of the success of the developed methods. It allows us to assess the quality and effectiveness of the implemented techniques.

$$PSNR = 10log_{10} \left(\frac{Max^2}{MES}\right) \qquad (2)$$

Meanwhile, the SSIM of the formula is showing the similarity ratio between the cover image and the stego image where is found in (3).

$$SSIM\ (x, y) = \frac{(2u_x\ u_y + c_1)(2\sigma_{xy} + c_2\ )}{(u_x^2 + u_y^2 + c1)(\sigma_x^2 + \sigma_y^2 + c2)} \qquad (3)$$

In the experimental method, 2097152 bits of randomly generated data were used, with 8 bits per pixel, and applied to Lena, Nature, Peppers, and Baboon images. These color pictures, with dimensions of 512 x 512, were hidden using the LSB332, LSB323, and LSB233 methods.

Table 1. Comparison of LSB332, LSB323 and LSB233 methods

Image (512 × 512)	Load (bpp)	LSB332		LSB323		LSB 233	
		PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lena	8	39,2707	0,9972	39,1004	0,9965	39,0538	0,9967
Nature	8	39,2639	0,9909	39,1248	0,9892	39,0111	0,9902
Peppers	8	39,1641	0,9967	38,9651	0,9958	38,8469	0,9960
Baboon	8	39,2710	0,9955	39,0900	0,9947	39,0458	0,9953
Average	8	**39,2424**	**0,9951**	**39,0701**	**0,9941**	**38,9894**	**0,9946**

Table 1 presents the results obtained from the experimental studies. In the LSB332 method, the range of PSNR values was between 39.1641 and 39.2710, and the range of SSIM values was between 0.9909 and 0.9972. For the LSB323 method, the range of PSNR values was between 38.9651 and 39.1248, and the range of SSIM values was between 0.9892 and 0.9965. Lastly, for the LSB233 method, the range of PSNR values was between 38.8469 and 39.0538, and the range of SSIM values was between 0.9902 and 0.9967.

Among these methods, the highest PSNR and SSIM values were achieved by the LSB332 method when applied to the Lena image, with values of 39.2707 and 0.9972 respectively. Furthermore, in the average values presented in Table 1, the LSB332 method yielded the best results with a PSNR value of 39.2424 and an SSIM value of 0.9951 when using color pictures with dimensions of 512 x 512.

4. Discussion And Conclusion

In this paper, the method of hiding data using LSB (Least Significant Bit) was applied, which is a commonly used technique in image steganography. The last three least significant bits in each pixel were replaced to conceal the data. The study involved randomly generating a 2097152-bit dataset, which was then hidden in colored cover images using the LSB332, LSB323, and LSB233 methods.

The results of the study showed that using the LSB332 method, which involves changing the last three least significant bits, provided the best performance for hiding 8-bit data in a one-pixel area of colored overlay images. This method allowed for high-capacity data hiding while maintaining a high PSNR (Peak Signal-to-Noise Ratio) value. However, it should be noted that this method may still be detectable by a third party if they suspect the presence of hidden information in the image.

To address this concern, it is suggested to combine the technique of changing the least significant bit with other methods that can offer increased security and efficiency in image steganography. By employing such extended methods, it is possible to enhance the safety and effectiveness of data concealment in images.

References:

1. Ahmed Laskar, S. (2012). High Capacity data hiding using LSB Steganography and Encryption. *International Journal of Database Management Systems, 4*(6), 57-68. doi:10.5121/ijdms.2012.4605

2. ALabaichi, A., Al-Dabbas, M. a. A. A. K., Salih, A. J. I. j. o. e., & engineering, c. (2020). Image steganography using least significant bit and secret map techniques. *10*(1).

3. Altaay, A. A. J., Sahib, S. B., & Zamani, M. (2012). *An introduction to image steganography techniques.* Paper presented at the 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT).

4. Altaay, A. A. J. S., Shahrin Bin Zamani, Mazdak. (2012). *An introduction to image steganography techniques.* Paper presented at the 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT).

5. Alwan, Z. A., Farhan, H. M., Mahdi, S. Q. J. I. J. o. E., & Engineering, C. (2020). Color image steganography in YCbCr space. *10*(1).

6. Alyousuf, F. Q. A., Din, R., Qasim, A. J. J. B. o. E. E., & Informatics. (2020). Analysis review on spatial and transform domain technique in digital steganography. *9*(2), 573-581.

7. Chan, C.-K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition, 37*(3), 469-474. doi:10.1016/j.patcog.2003.08.007

8. Cvejic, N., & Seppanen, T. (2004). *Increasing robustness of LSB audio steganography using a novel embedding method.* Paper presented at the Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on.

9. Cvejic, N., & Seppänen, T. (2005). Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding. *J. UCS, 11*(1), 56-65.

10. Din, R., Mahmuddin, M., Qasim, A. J. J. I. J. o. E., & Technology. (2019). Review on steganography methods in multi-media domain. *8*(1.7), 288-292.

11. Din, R., Qasim, A. J. J. B. o. E. E., & Informatics. (2019). Steganography analysis techniques applied to audio and image files. *8*(4), 1297–1302.

12. Eskandari, A. R. J. I. J. o. E., & Engineering, C. (2013). A robust steganography method using adjustable parameters. *3*(2), 207.

13. Hameed, M.A., Abdel-Aleem, O.A. & Hassaballah, M. A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques. J Ambient Intell Human Comput 14, 4639–4657 (2023). https://doi.org/10.1007/s12652-022-04366-y

14. Jung, K.-H., & Yoo, K.-Y. (2015). Steganographic method based on interpolation and LSB substitution of digital images. *Multimedia Tools and Applications, 74*(6), 2143-2155.

15. Ker, A. D. (2005). Steganalysis of LSB matching in grayscale images. *IEEE signal processing letters, 12*(6), 441-444.

16. Khudher, I. M. J. E.-E. J. o. E. T. (2021). LSB Steganography Strengthen Footprint Biometric Template. *1*(9), 109.

17. Liao, X., Wen, Q.-y., & Zhang, J. (2011). A steganographic method for digital images with four-pixel differencing and modified LSB substitution. *Journal of Visual Communication and Image Representation, 22*(1), 1-8.

18. Mitra, S., Roy, T., Mazumdar, D., & Saha, A. (2004). *Steganalysis of LSB encoding in uncompressed images by close colour pair analysis.* Paper presented at the IIT Kanpur Hacher's Workshop.

19. Neeta, D., Snehal, K., & Jacobs, D. (2006). *Implementation of LSB steganography and its evaluation for various bits.* Paper presented at the 2006 1st International Conference on Digital Information Management.

20. Parthasarathy, C., & Srivatsa, S. (2005). Increased robustness of LSB audio steganography by reduced distortion LSB coding. *Journal of Theoretical and Applied Information Technology, 7*(1), 080-086.

21. Qasim, A. J., & Alyousuf, F. Q. A. J. Q. Z. S. J. (2021). History of Image Digital Formats Using in Information Technology. *6*(2), 1098-1112.

22. Qasim, A. J., Din, R., Alyousuf, F. Q. A. J. B. o. E. E., & Informatics. (2020). Review on techniques and file formats of image compression. *9*(2), 602–610.

23. QASSIM, A. J., & SUDHAKAR, Y. (2015). Information Security with Image through Reversible Room by using Advanced Encryption Standard and Least Significant Bit Algorithm.

24. Raja, K., Chowdary, C., Venugopal, K., & Patnaik, L. (2005). *A secure image steganography using LSB, DCT and compression techniques on raw images.* Paper presented at the 2005 3rd international conference on intelligent sensing and information processing.

25. Rasmi.A, D. M. M. (2017). HIGH DATA EMBEDDING USING LSB AND PIXEL INTENSITY BASED METHODS. *International Journal of Advanced Research in Computer Science and Software Engineering, 8*(7).

26. Roshidi Din, O. G., Alaa Jabbar Qasim. (2018). Analytical Review on Graphical Formats Used in Image Steganographic Compression. *Indonesian Journal of Electrical Engineering and Computer Science, Vol 12, No 2*, pp. 441~446. doi: 10.11591

27. Satyavathy, G., & Punithavalli, M. (2011). LSB, 3D-DCT and Huffman Encoding based Steganography in Safe Message Routing and Delivery for Structured Peer-to-Peer Systems. *IJCA Special Issue on Artificial Intelligence Techniques*, 1-5.

28. Shamim Ahmed Laskar, K. H. (2012). High Capacity data hiding using LSB Steganography and Encryption. *International Journal of Database Management Systems (IJDMS), 4*(6).

29. Taouil, Y., Ameur, E. B. J. I. J. o. E., & Engineering, C. (2018). Steganographic Scheme Based on Message-Cover matching. *8*(5).

30. Tayel, M., Shawky, H., & Hafez, A. E.-D. S. (2012). *A new chaos steganography algorithm for hiding multimedia data.* Paper presented at the Advanced Communication Technology (ICACT), 2012 14th International Conference on.

31. Thangadurai, K., & Devi, G. S. (2014). *An analysis of LSB based image steganography techniques.* Paper presented at the Computer Communication and Informatics (ICCCI), 2014 International Conference on.

32. Zaidan, B., Zaidan, A., Taqa, A., & Othman, F. (2009). Stego-Image Vs Stego-Analysis System. *International Journal of Computer and Electrical Engineering, 1*(5), 572.

پەرەپێدانی شێوازێک بۆ شاردنەوەی داتاکان بە شێوازی کەمترین بیت گرنگ لە وێنە ڕەنگاوڕەنگەکاندا

پوختە:

پێشکەوتنە خێراکان لە بواری تەکنەلۆژیای زانیاریدا وایکردووە پەیوەندی نێوان مرۆڤەکان لە ژینگەی مەجازیدا هەبێت. گرنگە ئەم زانیاریانە بپارێزرێن و بیانشارنەوە و پارێزراو بن، بەتایبەتی لە ژینگەی مەجازیدا زانستی ستیگانۆگرافی گرنگییەکی زۆر بەرزی هەیە، بەو پێیەی ئەو زانستەیە کە دەستەبەر دەکات لە گواستنەوەی داتاکان بە سەلامەتی و نهێنی بۆ لایەنی بەرامبەر. لەم لقەی زانستەدا ئەو زانیاریانەی کە دەبێ بۆ لایەنی بەرامبەر بنێردرێت بە دەمامککردنی داتاکان بۆ گواستنەوەیەکی پارێزراو دەگوازرێنەوە. لە توێژینەوەکەماندا، شێوازی گۆڕینی سێ بیتی کۆتایی کەمترین گرنگ بەکارهاتووە بۆ دەمامککردنی داتاکان لە وێنە ڕەنگاوڕەنگەکاندا. لە قۆناغی تاقیکاریی توێژینەوەکەدا وێنەی ستاندارد بە قەبارەی 512 512 x بەکارهێنراوە، هەروەها لە توێژینەوەکەدا داتای هەشت بیتی

له ناوچەی یەک پێکسڵدا شاراوەتەوە، هەروەها ڕێژەی لێکچوون لە نێوان وێنەی بەرگ و کوالێتی... وێنەی stego پشکنینیان بۆ دەکرێت بۆ دڵنیابوون لە جیاوازی نێوان وێنەی بەرگ و وێنەی شاراوەی زانیارییەکان

تطوير طريقة إخفاء البيانات بطريقة البت الأقل أهمية في الصور الملونة

الملخص:

أدت التطورات السريعة في مجال تكنولوجيا المعلومات إلى جعل التواصل بين الناس في البيئة الافتراضية. من الأهمية لحماية هذه المعلومات وإخفائها وتأمينها، في البيئة الافتراضية خاصة يحظى علم إخفاء المعلومات بأهمية عالية جدا حيث هو العلم الذي يضمن نقل البيانات بشكل آمن وسري إلى الطرف الآخر. في هذا الفرع من العلم، يتم إرسال البيانات المراد إرسالها إلى الطرف الآخر عن طريق إخفاء البيانات للحصول على نقل امن. في ورقتنا البحثية هذه، تم استخدام طريقة تغيير البنات الثلاثة الأخيرة الأقل أهمية لإخفاء البيانات في الصور الملونة. في المرحلة التجريبية للبحث، تم استخدام الصور القياسية بحجم 512 × 512. في الدراسة أيضا، يتم إخفاء بيانات ثمانية بت في منطقة بكسل واحد، ويتم فحص نسب التشابه بين صورة الغلاف وجودة صورة stego للتأكد من الفرق بين صورة الغلاف وصورة المخفي فيها المعلومات.