JURNAL TEKNISI **E-ISSN: 2775-0965**
(Jurnal Teknologi Komputer dan Sistem Informasi)
Agustus 2023, Vol 5, No 2, Hlm. 68 – 73
Available online at http://jurnal.goretanpena.com/index.php/teknisi

USING LEAST SIGNIFICANT BIT TECHNIQUE IN STEGANOGRAPHY TO HIDE INFORMATION

Fikri Haikal[1*] , Lailatul Badria[1] , Aurellia Aknesia Hendrawan[1] , Muhammad Raihan Muharram[1], M. Khalil Gibran[1]
[1]Computer Science, Universitas Islam Negeri Sumatera Utara
Email: [1]fikrisajaja@gmail.com

Abstract: In the digital information era, Steganography is a technique and art of hiding digital information and data behind other digital information, so that the real digital information is not visible. This study discusses the application of the Least Significant Bit (LSB) technique in steganography to hide information in image media. The LSB technique allows the insertion of secret messages into images by utilizing the least significant bits of the image pixels, so that the changes that occur are invisible to the human eye and do not arouse suspicion. This study explores the effectiveness of the LSB technique in maintaining data confidentiality, as well as analyzing image quality after information insertion. The results of the study indicate that the LSB technique can be used effectively to hide information without sacrificing the visual quality of the image, making it an attractive solution in the field of data communication security. In addition, this study also discusses the advantages and disadvantages of the LSB technique, as well as the possibility of developing this technique to improve data security in various applications.

Keywords: data security; least significant bit (LSB) technique; steganography.

Abstrak: Di era informasi digital, Steganografi merupakan teknik dan seni menyembunyikan informasi dan data digital di balik informasi digital lainnya, sehingga informasi digital yang sebenarnya tidak terlihat. Penelitian ini membahas penerapan teknik Least Significant Bit (LSB) dalam steganografi untuk menyembunyikan informasi di dalam media gambar. Teknik LSB memungkinkan penyisipan pesan rahasia ke dalam gambar dengan memanfaatkan bit paling signifikan dari piksel gambar, sehingga perubahan yang terjadi tidak terlihat oleh mata manusia dan tidak menimbulkan kecurigaan. Penelitian ini mengeksplorasi efektivitas teknik LSB dalam menjaga kerahasiaan data, serta menganalisis kualitas gambar setelah penyisipan informasi. Hasil penelitian menunjukkan bahwa teknik LSB dapat digunakan secara efektif untuk menyembunyikan informasi tanpa mengorbankan kualitas visual gambar, menjadikannya solusi yang menarik di bidang keamanan komunikasi data. Selain itu, penelitian ini juga membahas kelebihan dan kekurangan teknik LSB, serta kemungkinan pengembangan teknik ini untuk meningkatkan keamanan data di berbagai aplikasi.

Kata Kunci: keamanan data; teknik least significant bit (LSB); steganografi.

JURNAL TEKNISI **E-ISSN: 2775-0965**
(Jurnal Teknologi Komputer dan Sistem Informasi)
Agustus 2023, Vol 5, No 2, Hlm. 68 – 73
Available online at http://jurnal.goretanpena.com/index.php/teknisi

INTRODUCTION

In large computer network systems such as the internet, sending messages via email can be vulnerable to hijacking by unauthorized parties. Two key issues related to message security require attention from users: privacy and information confidentiality. Privacy means that the information in a sent message can only be accessed by authorized recipients. Data security and confidentiality in computer networks are currently crucial and constantly evolving issues, especially with the advancement of the open system concept that allows access to vital areas.

Therefore, data and information protection is essential. Furthermore, copyright issues also require attention, where copyrighted works must be protected from misuse or reappropriation by third parties, which could harm the owner (Lutfi & Rosihan, 2018). One emerging solution to address this issue is steganography, a method of hiding data in digital media to prevent direct detection. One particularly effective approach in steganography is the Bit Plane Complexity Segmentation (BPCS) method, which allows messages to be embedded within visually complex image sections.

Previous studies have extensively explored the use of Least Significant Bit (LSB)-based steganography, but most still employ basic techniques that are less secure against visual and statistical analysis attacks. For example, Sitorus (2015) demonstrated that conventional LSB methods can be easily detected without additional data obfuscation processes. Meanwhile, Apriyansyah et al. (2020) emphasized the importance of improving steganography algorithms to address information security challenges in internet data traffic. This study attempts to address these shortcomings by implementing an enhanced LSB approach to enhance the security of embedding text data into digital images.

The purpose of this study is to develop and implement a more secure LSB-based steganography algorithm, emphasizing improvements in the information insertion technique to prevent it from being easily detected by third parties. This study also aims to measure the effectiveness of the proposed method in maintaining the integrity and confidentiality of data embedded in digital images.

The novelty of this research lies in the integration of the LSB method with existing embedding approaches.

METHOD

Least Significant Bit (LSB) steganography is a technique used to hide data within digital media, such as images, without changing its visual appearance (Abdillah et al., 2023) . This process involves three main steps that utilize the least significant bits in the binary representation of pixel color. By modifying these bits, secret information can be embedded without disturbing the overall image, making it difficult for unauthorized persons to detect.

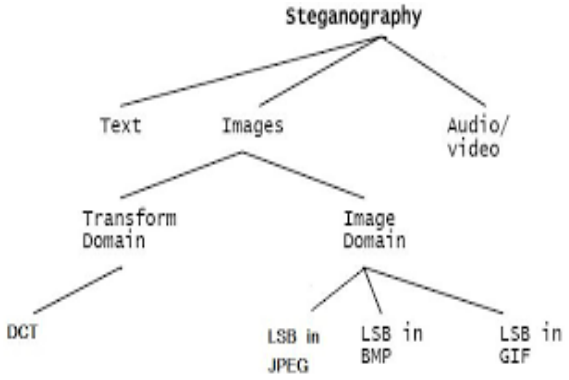

Image 1. Stenografi

Pixel and Bit Selection

The first step in implementing LSB steganography is to select the pixels that will be used to store the data. For example, in a digital image, each pixel consists of three color components: red (R), green (G), and blue (B). Each of these components is represented in binary form. To store the information, the least significant bit of each color component is selected. In the example shown, the bits to be modified are marked with an "X", which means that these bits are the target for data insertion. Replacing the values of these bits can serve to store the binary information that is to be hidden.

Insertion

Once the pixels are selected, the next step is to insert data into the specified bits. The binary value you want to store will replace the

value of the least significant bit (LSB). For example, if the current LSB bit is 0 and the value you want to store is 1, then that bit will be changed to 1. This process is repeated for all data to be stored.

Extraction

The final step is the extraction process, where the hidden data can be retrieved by reading the LSB bits of the same pixel. In this way, users who have access to techniques and algorithms can extract the hidden information in the image.

LSB is the least significant bit in the byte value of an image pixel. Image-based steganography uses LSB to embed secret information into the smallest bit of pixel values in the cover image. The LSB method is often used in steganography techniques because it is easy to implement and less suspicious to the human eye. However, this method has the disadvantage that it is easily detected by steganography detection algorithms.

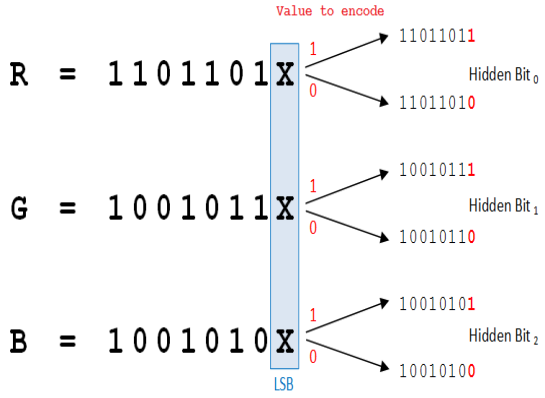

Image 2. Least Significant Bit (LSB) Method

The image above shows the process of data insertion using the Least Significant Bit (LSB) method in color representation in binary format. In this example, there are three color components: red (R), green (G), and blue (B). Each component has 8 bits, and the lowest bit (LSB) of each component will be changed to insert secret information. For example, if the value to be inserted is '1', then the LSB of the red, green, or blue color will be changed to '1', while if the value is '0', the LSB will be changed to '0'. This process allows hidden bits to be inserted without significantly changing the base color.

This process is commonly used in steganography techniques, where information is hidden in an image without damaging its visual appearance. For example, by replacing the LSB of red, green, and blue colors with the desired values, up to three bits of information can be stored in each pixel of the image. When the image is displayed, the changes in the LSB are barely visible to the human eye, so the embedded data can remain secure. Using this method, users can store important or confidential information in digital images in an efficient manner.

RESULTS AND DISCUSSION

The first step is to select an image that will be used as a message container, click the "Select Image" button. Then select the desired image. For the image selection we will use the logo image from UINSU.

Image 3. Initial image before insertion

The results of selecting the image file will appear as in the image below.

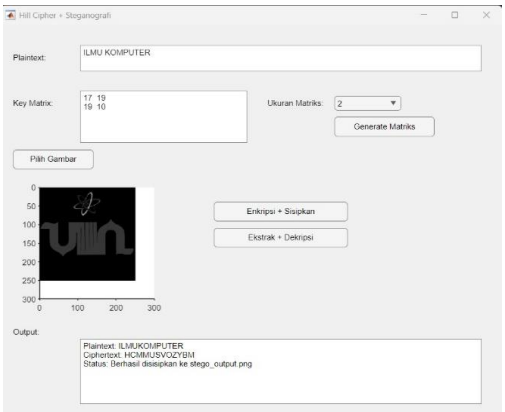

Image 4. View after inserting the image

JURNAL TEKNISI **E-ISSN: 2775-0965**
(Jurnal Teknologi Komputer dan Sistem Informasi)
Agustus 2023, Vol 5, No 2, Hlm. 68 – 73
Available online at http://jurnal.goretanpena.com/index.php/teknisi

The next step is to input the message and key. After we insert the image file, we will continue by entering the message and key. By clicking plaintext type the desired message and click the text box key enter the key for the secret message. From this result we can see in figure 4 below .

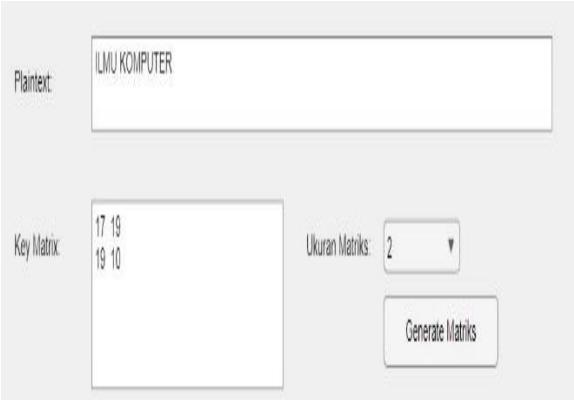

Image 5. Message and key input process

For the next process, press the extract + description button, then the process of inserting the file from the secret message into the image will be carried out. as follows:

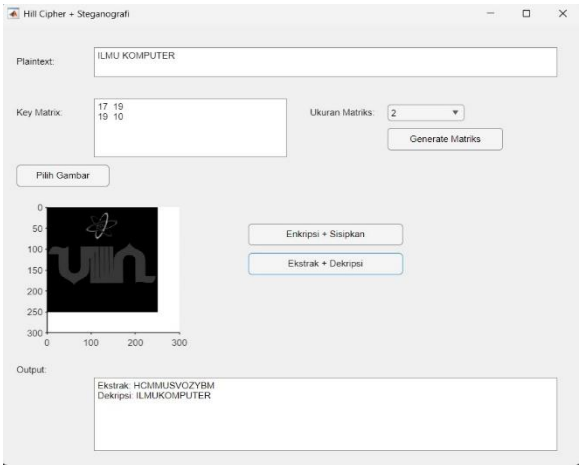

Image 6. Process of Inserting Secret Messages into Images

After the description process is carried out, we can finally find out the secret message that was sent .

In the right image, the image has not been inserted, and in the left image, the image has been inserted.

The image above has been inserted with a secret message. It is more beneficial for us because for most other steganography there will be a very striking difference in the histogram of the image before and after the message insertion. With this difference, it is more difficult for third parties to know that there is a secret message hidden in the image.

This research successfully implemented a steganography technique using the Least Significant Bit (LSB) algorithm to embed secret messages into digital images. The process begins with selecting an image to serve as the message container, which in this study used the UINSU logo. After selecting the image, the process continues with inputting the secret message and encryption key through a designed application interface. Message embedding is performed by replacing the least significant bits of each color component (R, G, B) in the image pixels with bits from the secret message. This process is carried out without significantly altering the image's visual appearance.

The results demonstrate that the message can be embedded intact into the image without any visible deterioration in visual quality. A comparison of the images before and after embedding shows a very slight difference in the histogram, making it difficult for third parties to detect without specialized equipment. This demonstrates the effectiveness of the LSB method in maintaining information confidentiality while enhancing data communication security. During the extraction stage, the previously embedded secret message was successfully retrieved intact and accurately, without any changes to its content.

Another advantage of this method is its simplicity of implementation and its ability to securely store confidential data without arousing visual suspicion. However, as stated in several previous studies, the LSB method also has weaknesses, namely its vulnerability to steganalysis attacks if not combined with additional security techniques. Nevertheless, this study demonstrated that for small-scale message insertion needs, LSB can perform optimally and efficiently.

CONCLUSION

Based on the analysis results, it is known that the steganography application that has been produced from the implementation of the LSB (Least Significant Bit) algorithm can be used very well to hide secret messages into an image in such a way that other people do not realize there is something in the message because the difference between the original image and the image that is inserted with the secret message is very thin. In the extraction process, the message or information inserted in the test image file in this steganography application can be obtained back in full or in other words the message inserted before the insertion process and after the extraction process is the same without any changes.

BIBLIOGRAPHY

Abdillah, MO, Pane, OA, & Lubis, FRA (2023). Implementation of Steganography Information Asset Security Using the Least Significant Bit (LSB) Method. Journal of Science and Technology (JSIT) , 3 (1), 40–46. https://doi.org/10.47233/jsit.v3i1.482

Anwar, N. (2018). Design of Hidden Message Steganography with Least Significant Bit Insertion (LSB) Method Based on Matlab. Journal of Algorithms, Logic and Computation , 1 (1), 25–30. https://doi.org/10.30813/j-alu.v1i1.1107

Apriyansyah, Unik, M., & Mukhtar, H. (2020). Implementation of Text Message Security System with Steganography Technique Using Least Significant Bit (LSB) Method. Journal of Computer Science and Information Technology , 1 (1), 8–12.

Laksono, AW, Suhada, S., & Zakaria, A. (2024). Implementation of the Least Significant Bit (LSB) Method in Steganography Techniques on Digital Images Using Matlab . 4 (1).

Miftakhul Fahmi, G., Isnaini, KN, & Suhartono, D. (2023). Implementation of Steganography on Digital Image With Modified Vigenere Cipher Algorithm and Least Significant Bit (LSB) Method. Jurnal Teknik Informatika (Jutif) , 4 (2), 333–344. https://doi.org/10.52436/1.jutif.2023.4.2.340

Satria, W., & Antares, J. (2022). Steganography Method Least Significant Bit (LSB) And End Of File (EoF) On Digital Data Security. Journal of Information Technology , 6 (2), 252–257.

Supardi, S., Alkodri, AA, & Isnanto, B. (2021). Steganography Technique for Hiding Secret Text Messages in Digital Images Using the Least Significant Bit Method. Jurnal Sisfotek Global , 11 (1), 70. https://doi.org/10.38101/sisfotek.v11i1.351

Tabe, H. T., & Materechera, E. K. (2024). Academic writing technique: the influence of stenography on students' academic performance in higher education. *Cogent Education*, *11*(1), 2306883.

Matted, S., Shankar, G., & Jain, B. B. (2021). Enhanced image security using stenography and cryptography. In *Computer Networks and Inventive Communication Technologies: Proceedings of Third ICCNCT 2020* (pp. 1171-1182). Singapore: Springer Nature Singapore.

Permana, F. R., Fauzi, A. R., & Setiyanto, R. F. (2023). Image Steganography Dengan Menggunakan Metode Lsb Pada Python. *Jurnal Tiple A Pendidikan Teknologi Informasi dan Teknologi Informasi*, *2*(1), 1-7.

Syaima'Fadel, A., Saputra, R. D., Fatma, Y., & Putra, R. N. (2024). Analisis keamanan steganografi teks dengan metode lsb (least significant bit) pada citra digital. *Jurnal CoSciTech (Computer Science and Information Technology)*, *5*(1), 36-41.

Abdillah, M. O., Pane, O. A., & Lubis, F. R. A. (2023). Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB). *Jurnal Sains Dan Teknologi (JSIT) Vol*, *3*(01).

Jurnal, J. T. I. K. (2022). Teknik Steganography untuk Menyisipkan Pesan pada Sebuah Citra Menggunakan Metode Least Significant Bit (LSB). *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, *6*, 3.

Sembiring, M. A. (2024). Analisis Faktor Prediksi Diagnosa Tingkat Serangan Jantung Menggunakan Metode Regression. *Jurnal Teknisi*, *4*(1), 16-22.

Sembiring, F. W. (2024). Mengukur Tingkat Akurasi 6 Model Regresi Dalam Machine Learning Untuk Estimasi Penyakit Diabetes. *JURNAL TEKNISI*, *4*(1), 23-27.