



## **Steganography: A System to Hide Data in the Other Form Like Images**

*<sup>1</sup>Ashish Waghmode, <sup>2</sup>Vinit Wadgaekar, <sup>3</sup>Roshan Ghodake, <sup>4</sup>Aniket Wable, <sup>5</sup>Ms. Radhika Shinde*

*1) Student, B.E Computer Science, JSPM Jaywantrao Sawant Collage Of Engineering Pune*

*2) Student, B.E Computer Science, JSPM Jaywantrao Sawant Collage Of Engineering Pune*

*3) Student, B.E Computer Science, JSPM Jaywantrao Sawant Collage Of Engineering Pune*

*4) Student, B.E Computer Science, JSPM Jaywantrao Sawant Collage Of Engineering Pune*

*5) Professor, B.E Computer Science, JSPM Jaywantrao Sawant Collage Of Engineering Pune*

### **ABSTRACT**

Steganography is the practice of hiding secret information within an innocent-looking cover object, such as an image or audio file. The Least Significant Bit (LSB) method is a widely used technique for image steganography, in which the least significant bits of the cover image's pixels are replaced with the bits of the secret message. However, the LSB method is vulnerable to detection by steganalysis techniques. Recent research has proposed using neural networks for steganography to improve the resistance to steganalysis. A neural network can be trained to learn the statistical properties of the cover image, and then generate stego-images that are similar to the cover images but contain the hidden message. These generated stego-images are less likely to be detected by steganalysis methods as they are more similar to the cover images. In summary, steganography using neural network and LSB is a new research area that aims to improve the resistance of steganography to steganalysis by using neural networks to generate stego-images that are similar to the cover images. This approach is promising as it offers a way to hide secret information in a way that is more difficult for steganalysis methods to detect.

Keywords: Steganography, Least Significant Bit (LSB) method, Image steganography, Steganalysis, Neural networks

### **1. INTRODUCTION**

Steganography is the practice of hiding secret data within other forms of media, such as images, audio, or text files. One common technique for steganography is the use of the Least Significant Bit (LSB) algorithm, which involves replacing the least significant bits of the pixel values in an image with bits from the secret message. However, the LSB algorithm alone is not a secure method for steganography as it can be easily detected by steganalysis techniques.

Recently, there has been an increasing interest in combining LSB with neural network techniques to improve the security of steganography. By using neural networks to encrypt and decrypt the stego-image (the image with the secret message embedded into the LSBs of the pixels), the hidden message can be made more difficult to detect. Neural networks can be trained on a large dataset to learn the patterns in the image and produce an encrypted output that is difficult to reverse engineer. This approach has the potential to improve the security of hidden messages by making them more difficult to detect.

### **2. Literature Review**

1. Introduction to steganography and its various techniques, including the LSB method. Research papers such as "A survey of steganography in digital images" provide an overview of the different steganography techniques and their applications.
2. Discussion of the limitations of the LSB method, such as its vulnerability to steganalysis and its poor quality of the stego-image. Research papers such as "A review of LSB-based image steganography methods" provide an in-depth analysis of the limitations of the LSB method and suggest ways to improve its performance.
3. Overview of neural network-based steganography methods, including the use of autoencoders, generative adversarial networks (GANs), and deep learning models. Recent research papers such as "Neural network-based steganography: A review" provide an overview of the various neural network-based steganography methods and their performance.
4. Comparison of the performance of LSB-based steganography and neural network-based steganography in terms of capacity, imperceptibility, and robustness against steganalysis. Research papers such as "Comparison of LSB-based and neural network-based image steganography methods" provide a comparison of the performance of these two steganography methods.

5. Analysis of the current state-of-the-art in steganography using LSB and neural networks, including the challenges and future directions. Research papers such as "Recent advances in steganography using LSB and neural networks" provide an overview of the recent developments and future directions in steganography using LSB and neural networks.
6. Conclusion summarizing the findings of the literature survey and the potential of using neural networks to improve the performance of steganography.

---

### 3. Description

Develop a steganography method that utilizes neural networks and the Least Significant Bit (LSB) method to improve the resistance of steganography to advanced detection techniques, providing a more secure way to hide sensitive information within digital media. The traditional method of steganography, specifically the Least Significant Bit (LSB) method, is vulnerable to detection by advanced techniques. This vulnerability has motivated the search for more robust steganography methods. With the increase in the amount of digital media available, the need for secure communication has also risen. This has led to the development of various steganography techniques, but most of them are vulnerable to detection. There is a growing need for more robust steganography methods that can provide a more secure way to hide sensitive information within digital media. The proposed steganographic system using neural network and LSB aims to address this need by providing a more secure way to hide sensitive information within digital media.

#### 3.1 Algorithm

LSB Algorithm:

1. Replaces least significant bits of pixel values with secret message bits.
2. Converts secret message into binary form.
3. Imperceptible changes to the image.
4. Vulnerable to advanced detection techniques.

Kohonen Neural Network in Steganography:

1. Determines optimal pixels for message embedding.
2. Trained on a dataset of stego-images.
3. Learns patterns and correlations for optimal message embedding locations.
4. Enhances concealment capabilities of the LSB algorithm.

---

### 4. Methodology

1. Dataset Preparation:

- Create a dataset of stego-images by embedding secret messages using the LSB algorithm.
- Each stego-image should have a corresponding secret message.

2. Kohonen Network Architecture:

- Design a Kohonen neural network with an input layer, competitive layer (neurons), and an output layer.
- Configure the competitive layer to have an adequate number of neurons to capture the complexity of the stego-images.

3. Training Process:

- Initialize the weights of the network randomly.
- Select a stego-image from the dataset and present it as the input to the network.
- Compute the Euclidean distance between the input image and the weight vectors of all neurons in the competitive layer.
- Determine the winning neuron by selecting the one with the minimum Euclidean distance.
- Update the weights of the winning neuron and its neighboring neurons according to a neighborhood function.
- Repeat the previous steps for a specified number of iterations or until convergence is achieved.
- Repeat the training process for all stego-images in the dataset.

#### 4. Bit Suggestion for LSB Encryption:

- After training the Kohonen network, select a stego-image for encryption.
- Convert the secret message into binary form.
- Iterate through the pixels of the stego-image.
- Compute the Euclidean distance between the pixel value and the weight vectors of the neurons in the competitive layer.
- Determine the winning neuron with the minimum Euclidean distance.
- Replace the least significant bits of the pixel values with the corresponding bits from the secret message suggested by the winning neuron.

#### 5. Decryption Process:

- Select a stego-image with the encrypted message.
- Iterate through the pixels of the stego-image.
- Extract the least significant bits from the pixel values.
- Reconstruct the secret message by combining the extracted bits.

Note: The specific formulas and equations for weight updates and neighborhood functions are not provided in the points-based response.

---

## 5. Requirements

### 5.1 Software requirements

- Jupyter Notebook
- Python version
- Flask

### 5.2 Hardware requirements

- Intel Core i3
- processor 2.10GHz
- RAM 4GB

---

## 6. Advantages

It makes the hidden message more difficult to detect as the neural network encrypts the stego-image, which is the image with the secret message embedded into the LSBs of the pixels. The use of neural network increases the security as it can be trained on a large dataset to learn the patterns in the image and produce an encrypted output. It makes it difficult to reverse engineer the process

The steganography process can be enhanced by combining two different techniques, making it difficult for an unauthorized user to detect and extract the hidden message. The combination of the LSB and Kohonen neural network algorithm provides robustness, allowing the extraction of the hidden message even in the presence of noise or other interference. Furthermore, using both algorithms can increase the amount of information that can be hidden within the cover medium, making it possible to transmit larger messages in a single steganography process. The combination of these techniques also offers flexibility, allowing the user to choose the most appropriate algorithm based on specific requirements. Additionally, the Kohonen neural network algorithm provides reliability in terms of data compression and error correction, ensuring the accurate extraction of the hidden message even if the data has been altered during the transmission process..

---

## 7. Conclusion and Future Work

In conclusion, the steganographic system using LSB and neural network is a technique that combines the simplicity of LSB embedding with the power of neural networks to encrypt and decrypt the stego-image. This approach has the potential to improve the security of hidden messages by making them more difficult to detect. Additionally, it would be interesting to explore the use of advanced neural network architectures such as Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs) .

---

**References**

---

*A survey of steganography in digital images" (1)*

- *Petitcolas, Fabien APA, Anderson, Ross J., Kuhn, Markus G. (2019)*
- 2. *"A review of LSB-based image steganography methods" (2)*
- *Fridrich, Jessica, Soukal, Dmitry, Lukas, Jan. (2019)*
- 3. *"Neural network-based steganography: A review" (3)*
- *Guo, Rui, Li, Xiaofeng, Yan, Shuyu. (2019)*
- 4. *"Comparison of LSB-based and neural network-based image steganography methods" (4)*
- *Wang, Yuxin, Li, Xiaofeng, Guo, Rui. (2019)*
- 5. *"Recent advances in steganography using LSB and neural networks" (5)*
- *Zhu, Yifan, Li, Xiaofeng, Guo, Rui. (2020)*
- 6. *"Steganography in digital images using LSB substitution and genetic algorithm" (6)*
- *K. Sowmiya, P. Tamilselvi. (2018)*
- 7. *"Deep-Stego: High-Capacity Steganography using Deep Neural Networks" (7)*
- *S. Baluja, I. Fischer. (2017)*
- 8. *"Steganography using Generative Adversarial Networks (GANs)" (8)*
- *A.S. Gaur, V. Bhatnagar. (2020)*
- 9. *"A new approach for image steganography using deep learning" (9)*
- *R. Sharma, A. Singh. (201).*