ISSN (Online):3048-5088

International Journal of Advancement and Innovation in Technology and Research (IJAITR)

Volume 3, Issue 1, (Jan-Jun) 2026

Image Steganography: Password Security Method

Dr. M. Fatima
AIML and CSECS Dept.
Sagar Institute of Research and Technology, Bhopal, India
mfcollege2050@gmail.com

Dr. Kalpana Rai
AIML and CSECS Dept.
Sagar Institute of Research and Technology, Bhopal, India

Dr. Rupali Tabakade
AIML and CSECS Dept.
Sagar Institute of Research and Technology, Bhopal, India

Ajay Yadav
AIML and CSECS Dept.
Sagar Institute of Research and Technology, Bhopal, India

Dhruv Sahu
AIML and CSECS Dept.
Sagar Institute of Research and Technology, Bhopal, India

Avinash Kumar
AIML and CSECS Dept.
Sagar Institute of Research and Technology, Bhopal, India

***Abstract*—Steganography is a powerful technique for embedding hidden information within digital media. This paper focuses on a web-based tool for encoding and decoding hidden text within images using steganography. The primary objective is to provide an intuitive platform for secure communication by concealing sensitive information in the alpha channel of image pixels, ensuring that the modifications are imperceptible to the human eye. The encoding process begins by encrypting the input text with a user-provided password using the AES encryption algorithm. The encrypted text is then embedded into the alpha channel of the image's pixel data, with the length of the text stored in a specific pixel for retrieval during decoding. On the decoding side, the tool extracts the encrypted data from the image, decrypts it with the provided password, and displays the original text. To enhance usability and transparency, the system features a visualization mode that highlights the modified pixels, offering insight into the steganographic process. The paper is implemented using HTML5, JavaScript, and the CryptoJS library for encryption. It features a user-friendly interface for selecting images, entering text, and providing encryption passwords. Additionally, the tool ensures data security by combining encryption with steganography, making it suitable for applications requiring confidential communication or watermarking. This paper demonstrates the integration of cryptographic principles and steganographic techniques, providing a simple yet robust solution for secure data embedding.**

***Index Terms*—Steganography, CryptoJS library, Secure Data Embedding, Watermarking, Encoding Text Within image, decoding Text Within image, Pixels, Text Stored in Image,**

I. Introduction

A. Background

In the digital era, where the transmission of sensitive information is commonplace, data security has become a critical concern. Various techniques have been developed to ensure confidentiality, one of

ISSN (Online):3048-5088
International Journal of Advancement and Innovation in Technology and Research (IJAITR)
Volume 3, Issue 1, (Jan-Jun) 2026

which is steganography. Steganography is the practice of hiding information within a carrier medium, such as text, images, or audio, in a way that conceals the presence of the hidden data [1]. Unlike encryption, which makes the content of a message unreadable, steganography aims to disguise the very existence of the message, adding an additional layer of security [2]. Images are particularly popular carriers for steganographic purposes due to their widespread use and large data capacity [3]. When combined with encryption, steganography can offer a robust method for secure communication, making it suitable for applications such as confidential data sharing, watermarking, and copyright protection [4]. The paper demonstrates the potential of combining encryption and steganography, Steganography process is shown in figure 1.1.

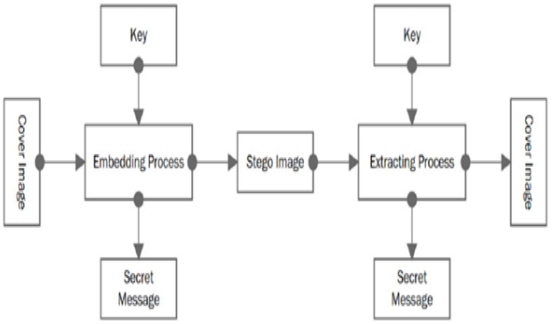

Fig. 1: Process of Image Steganography

II. Literature Review

A. Introduction to Steganography

Steganography, derived from the Greek words ”steganos” (covered) and ”graphein” (writing), has been practiced for centuries. Historically, it was used to conceal messages in physical media, such as writing hidden texts under wax tablets or embedding information in microdots [1]. With the advent of digital technology, steganography has evolved to hide data within digital files, such as images, audio, and video. This digital transformation has greatly expanded its applications and complexity [2]. Digital steganography leverages the characteristics of media files, where minor modifications are generally imperceptible to human senses. For instance, the least significant bit (LSB) of a pixel's color values in an image can be altered to encode information without affecting its visual appearance [3]. When combined with encryption, steganography ensures that even if the hidden data is detected, it remains unintelligible without the decryption key [4].

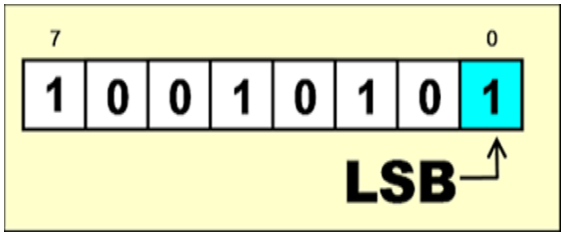

Fig. 2: Least Significant Bit

III. Methodology of Image Steganography

A. Section Overview

This section details the design and implementation of the steganography tool. The methodology focuses on embedding encrypted messages into image files while ensuring usability and security. The paper is implemented using web technologies, including HTML, CSS, JavaScript, and the CryptoJS library for AES encryption.

B. System Design

The system consists of two main functionalities: encoding and decoding messages. The design process involved the following steps:

1) Encoding Process:

a. **Image Input:** The user selects an image file to serve as the carrier.
b. **Text Input:** The user provides the message to be embedded.
c. **Encryption:** The message is encrypted using the AES algorithm with a user-provided password.

ISSN (Online):3048-5088

International Journal of Advancement and Innovation in Technology and Research (IJAITR)

Volume 3, Issue 1, (Jan-Jun) 2026

d. **Data Embedding:** The encrypted message is embedded into the alpha channel of the image's pixel data. Metadata, such as the length of the message, is stored in the image.
e. **Output Generation:** The modified image is saved as a new file for transmission.

2) Decoding Process:

a. **Image Input:** The user uploads the modified image containing the hidden message.
b. **Data Extraction:** The system retrieves the encrypted message from the image.
c. **Decryption:** The encrypted message is decrypted using the AES algorithm and the user-provided password.
d. **Message Display:** The decrypted message is displayed to the user.

3) Visualization: A visualization mode highlights the modified pixels in red, providing transparency into the embedding process.

IV. Implementation Details

The tool is implemented as a web application with the following components:

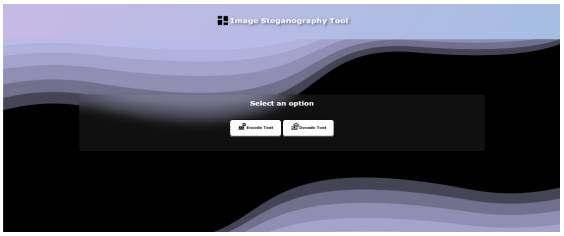

Fig. 3: Home Page

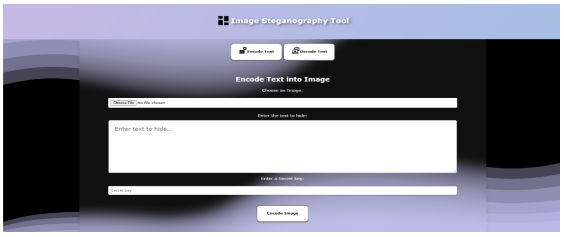

Fig. 4: Encoding Section

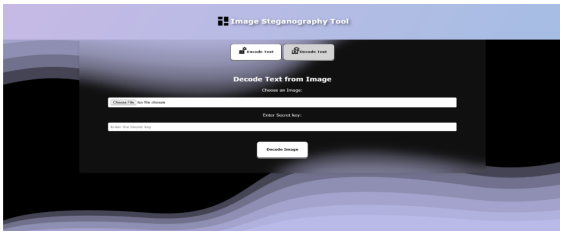

Fig. 5: Decoding Section

Fig. 6: Visualizing changes

A. Security Measures

Password-protected encryption ensures that only authorized users can access hidden data. Visualization mode helps detect unauthorized alterations to the modified image. Figure 3.4 Shows changes in the image after encoding.

V. Conclusion

This paper explored the implementation of a steganography system that embeds and extracts encrypted messages within digital images using the Least Significant Bit (LSB) method. The primary goal was to provide a secure and efficient method for hiding secret data in images, leveraging AES encryption for added security. The paper successfully demonstrated the following:

Message Encoding: The system allows users to embed encrypted text messages into images. The encrypted message is embedded within the image's pixel data, specifically using the alpha channel of pixels and the blue channel to store the message length. Message Decoding: Users can retrieve the hidden message from the encoded image by providing a decryption password. The system then extracts the message from the image, decrypts it using AES, and displays the result to the user. Visualization:

ISSN (Online):3048-5088

International Journal of Advancement and Innovation in Technology and Research (IJAITR)

Volume 3, Issue 1, (Jan-Jun) 2026

The paper also incorporated a visualization feature, highlighting the modified pixels (in red) that were altered during the encoding process. This allows users to visually inspect which parts of the image were changed.

REFERENCES

[1] N. F. Johnson and S. Katzenbeisser, *Information Hiding: Steganography and Watermarking–Attacks and Countermeasures*. Springer, 2000.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[3] M. Hussain *et al.*, "A survey of image steganography techniques," *International Journal of Advanced Science and Technology*, vol. 54, pp. 113–124, 2013.

[4] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press, 2009.

[5] R. Chandramouli and N. Memon, "Analysis of LSB-based image steganography techniques," in *ICASSP 2001. Proceedings (Cat. No. 01CH37221)*, 2001, pp. 1029–1032.

[6] X. Zhang *et al.*, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[7] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An overview of image steganography," in *Proceedings of the Fifth Annual Information Security South Africa Conference*, 2005.