https://doi.org/10.46335/IJIES.2025.10.4.2 **e-ISSN: 2456-3463**
Vol. 10, No. 4, 2025, PP. 7-11

International Journal of Innovations in Engineering and Science, www.ijies.net

Securing Data with Steganographic Techniques

Kedar Jawarkar[1], Lalit Patil [2], Riya Patel [3], Farha Naz [4]

[1,2,3,] UG student,[4] Assistant Professor, SVKM Institute of Technology, Dhule, India, 424-001

j.kedar282003@gmail.com

***Received on**: 13 March,2025* ***Revised on**: 16 April,2025* ***Published on**: 18 April,2025*

Abstract *– Image steganography, or data hiding in photographs, is used to conceal private or sensitive information within digital images. The data is embedded into the image's pixels so that the image appears normal to the human eyes. Hidden data can include digital information in text, files, or other multimedia formats. The specific steganography technique used depends on the application's requirements. Some applications may require the hidden data to be completely undetectable, while others may need to conceal a larger, more complex message. This paper examines the modification method for the least significant bit (LSB) in the spatial domain. It analyses and compares different variations of the techniques evaluated through user assessments, focusing on their capacity to hide data and overall efficiency.*

Keywords *Steganography, Cryptography, Encryption, Bits*

INTRODUCTION

With growing privacy concerns, ways to hide information have improved. One such method is steganography, first used in ancient Greece. Unlike cryptography, which protects data by making it unreadable, steganography hides the data. In steganography, a message is hidden within something ordinary, like an image or audio file, so it goes unnoticed. This differs from cryptography, which secures data by encrypting it but can still stand out because the content is still protected without a key. Steganography is good for hiding information, but cryptography is safer because it uses strong encryption to block unauthorized access. This research paper studies steganography, a method commonly used to hide messages.

Encryption keeps a message private by preventing unauthorized access. However, it does not ensure the integrity of the message, so there is no way to know if it has been tampered with while being sent. On the other hand, once a message is encrypted, it cannot be deleted or ignored. In article [1], authors used cryptographic algorithm with different parameters like speed, memory use to develop a combined encryption algorithm that integrates multiple methods to enhance overall security and efficiency. Digital signatures donot guarantee confidentiality since the signed message remains accessible to everyone. However, they are excellent at ensuring the message's integrity, confirming that it has stayed the same. However, digital signatures are not permanent and can be detached or cancelled. Steganography is a method that can protect privacy, but it depends on how it is being used. It keeps the hidden message intact, which makes it challenging to extract without detection. Authors in [2] used steganographic embedding to minimize an additive distortion function, enabling adaptable and efficient embedding schemes without sharing distortion details with the recipient. Steganography is key in cybersecurity, as it stops unwanted access and keeps information safe. It is beneficial in securing communication, safeguarding data, and digital investigations. Steganography hides the message, while encryption protects it without hiding.

Steganography techniques nowadays are used in cybersecurity for purposes like watermarking, copyright protection, detecting intrusions, hiding malware, and secret communication in government and military operations. Authors in [3] analysed steganographic techniques, comparing their effectiveness in balancing secrecy and media file modification for secure authentication. Authors in [4] used steganographic

https://doi.org/10.46335/IJIES.2025.10.4.2 **e-ISSN: 2456-3463**
Vol. 10, No. 4, 2025, PP. 7-11

International Journal of Innovations in Engineering and Science, www.ijies.net

techniques for lossy and lossless (e.g., BMP) image formats, categorized into spatial and transform domains maintaining a balance between imperceptibility, capacity, and robustness. Authors in [5] investigated video steganography by embedding MD5-hashed text into video frames and audio with randomized frame selection for added security. Steganography has evolved with the rise of electronic files. In the literature, text and images are used to hide information. However, digital images were focused more on due to their widespread use and diverse formats. In article [6] DCTR feature set for JPEG steganalysis was introduced to achieve efficient detection with low complexity with potential forensic applications. The security of steganography methods depends on the type of carrier used. The internet's global reach and instant digital information sharing have increased the use of steganography. Government restrictions on cryptosystems have shifted focus to steganography to hide messages so they cannot be read without the correct key, even if the host medium is compromised. Authors in [7] reviewed steganography techniques noting transform domain methods and compression robustness with high capacity but with low security. In article [8], a cost function with high-pass and low-pass filters was proposed to improve security and performance of the HILL stenographic method by optimizing value clustering in textured regions.

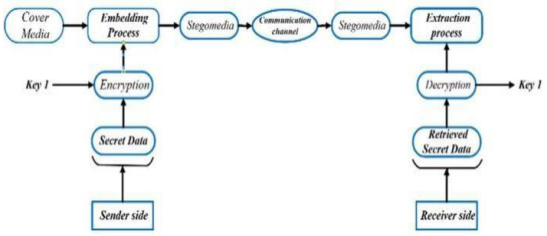

Figure 1. Block Representation of Steganography Techniques

When combined with encryption, steganography adds an extra layer of security by hiding both the message and its existence. This method is beneficial when encryption is prohibited, allowing confidential communication to stay hidden. Various methods exist to alter the pixel values without compromising the overall image. Figure 1 illustrates a block diagram representing various steganography techniques.

One common technique for adding data to an image is the Least Significant Bit (LSB) method. This method adds a part of the hidden message to the less important bit of the image, i.e., the eighth bit, which contains some or all of the bytes in an image. Small parts of the colour components can be used in a colour image, as they are all stored as bytes. Each pixel can store three bits, so an image with 800 by 600 pixels can hold 1,440,000 or 180,000 bytes of information. The binary bits of the message are embedded one by one into the LSB of each colour channel in the selected pixels, replacing the original LSB with the message bit.

Another method, known as bit plane representation, divides each pixel in an image into eight 1-bit fields, with the LSB through the most significant bit (MSB) containing different data levels. Image steganography techniques for data communication using LSB insertion and advanced approaches using GANs and CNNs was reviewed by authors in [9].

This process allows image manipulation by adjusting pixel values in each bit plane. Each field contains essential data, with field 0 for 8-bit data and field 7 for all pixel wavelengths. This method helps analyse image values, assist in image reduction, and determine the magnification needed to count each pixel. In the spiral embedding technique, the hidden data is arranged in a winding pattern within an image to prevent easy decoding and resist visual attacks. It starts by embedding metadata that describes the image's content, aiding in message recovery. The data, including the message and metadata, is serialized and then embedded into the image in a spiral, making it harder to detect or interpret. The altering threshold technique converts the grayscale images into binary images. It replaces each pixel with white if its intensity is higher than a set threshold or black if it is lower, helping to simplify the image for further analysis or processing.

The article is structured as follows: Section 2 provides a detailed overview of the proposed methodology, while Section 3 presents the results of the fault detection and classification, showcasing the algorithm's effectiveness. Finally, conclusions are drawn in Section 4.

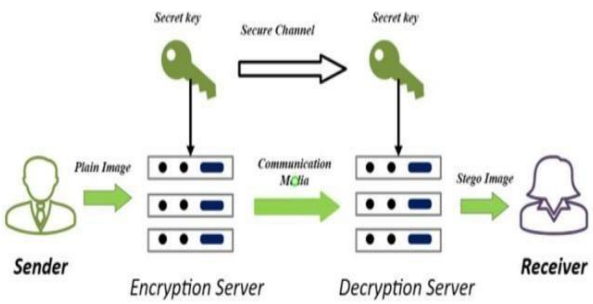

Fig2- Conversion Of plain image into stego image

https://doi.org/10.46335/IJIES.2025.10.4.2 e-ISSN: 2456-3463
Vol. 10, No. 4, 2025, PP. 7-11

PROPOSED METHODOLOGY

The steganography technique consists of several critical steps. Figure 2 illustrates the process of converting pixels into a message.

A. Choosing the Cover Medium

The first step is to select a suitable cover medium. This medium should look ordinary and not attract attention, such as images or audio files, which are altered to hide the secret message while preserving their original appearance or sound. The goal is to ensure the medium remains unnoticed, preventing detection by anyone observing the communication.

B. Encoding the Secret Message

To protect a private message, it is first converted into binary format, where each character or piece of data is represented by a series of bits (using encoding standards like ASCII or Unicode). The message, such as "Hello," is converted into binary and then compressed to reduce size. This makes the message more secure and efficient. After compression, the message is encrypted so it cannot be accessed without the correct decryption key, ensuring privacy and integrity.

C. Embedding the Message

Once the message is ready, it is hidden within the cover medium using various techniques. One standard method is LSB insertion, which involves changing the LSB of a pixel in an image or a sample in an audio file. For instance, altering the last bit of a pixel's binary value from 0 to 1 (e.g., from 11011010 to 11011011) allows the message to be hidden without visibly affecting the image or sound. Another method, called Masking and Filtering, hides the message in a way that makes it undetectable to the human senses. In audio files, for example, the message can be embedded in frequencies masked by louder sounds, making it inaudible to listeners. Techniques in the Transform Domain, such as DCT (Discrete Cosine and Transform) and DWT (Discrete Wavelet and Transform), provide a more robust method by embedding messages within the transformed data's coefficients. This process involves converting the original data into a different domain, where the message is hidden in the coefficients. These methods are highly effective because they resist common changes like compression and noise, ensuring the hidden message remains intact even when the cover medium is altered. These techniques allow for efficient and secure data concealment across various media types.

D. Extraction Process

The recipient uses a specific extraction method to retrieve the hidden message from a steganography file, reversing the original embedding process. A Gaussian embedding technique for steganography to minimize the detection error was introduced in article [10]. The article concentrated on payloads in textured regions and reduced embedding in smooth areas. The cover medium, such as an image or audio file, is carefully examined to pinpoint and separate the changed bits or coefficients containing the hidden data. In the LSB insertion method, the receiver examines the LSB of the relevant pixels or audio samples to recover the hidden binary data. In contrast, for transform domain methods, the receiver first applies the reverse transformation to access the modified coefficients and then extracts the concealed data. After extraction, the binary data is converted to its original format, allowing the receiver to read the hidden message. This process ensures that the confidential data is accurately recovered, maintaining its integrity while effectively concealing it within the cover medium. Steganography keeps the message's existence and content secret, making it a valuable tool for maintaining confidentiality and privacy. In article [11] authors analysed cryptographic algorithms and proposed a combining method to optimize security based on speed, memory, throughput, and CPU usage.

RESULTS AND ANALYSIS

In this research article, six systems are used to showcase the online transmission of hidden data.

S1: Selection of cover image to hide data.
S2: Converting the image into double precision type for accurate manipulation.
S3: Breaking down each pixel into its 64-bit components.
S4: Determining the number of replacement bits based on the data size.
S5: Replacing the selected bits with the data bits. S6: Combining the modified pixels to generate the encrypted image.

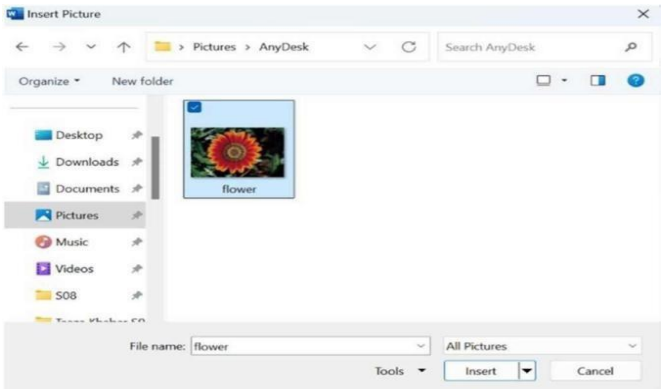

Figure. 3 Selecting cover media

https://doi.org/10.46335/IJIES.2025.10.4.2 **e-ISSN: 2456-3463**
Vol. 10, No. 4, 2025, PP. 7-11

International Journal of Innovations in Engineering and Science, www.ijies.net

Algorithm: Embed Textual Data

Using Pixel Modification

1. Input: Encrypted image imp, decryption password pas.
2. Output: Decrypted secret message message.
3. Initialize message = "", n = 0, m = 0, z = 0.
4. Verify if the decryption password matches the original password.
5. If passwords match:

a. For each character in the secret message:

i. Retrieve the pixel value from (n, m, z).

ii. Convert the value to its corresponding character using dictionary c.

iii. Append the character to message.

iv. Increment n, m, and update z = (z + 1) % 3.

b. Display the decrypted message.

If passwords do not match, display an error message

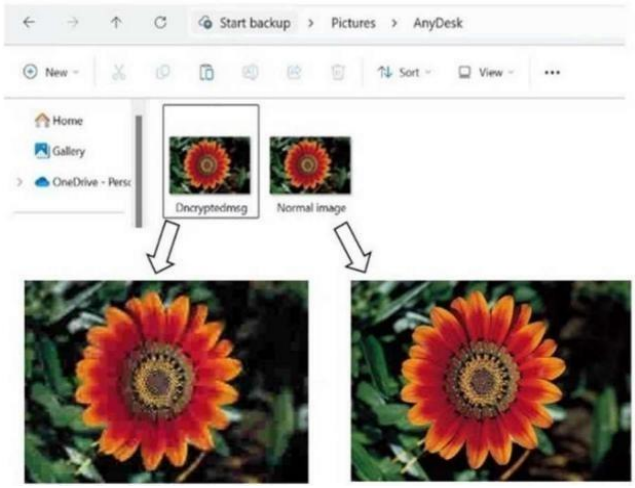

Figure. 4 Final decrypted image

The steps taken to perform image steganography were as follows:

- Selection of the Cover Image to carry the secret message.
- Setting up of Python Environment to run the steganography program.
- Executing the steganography program for the chosen cover image.
- Assigning a security key and the secret message into the program.
- Executing the program to embed the secret message into the image pixels.
- Generation of the Encrypted Image containing the embedded secret message.

```
Enter secert message:Hello
Enter password:1234
Enter passcode for Decryption:1234
Decryption message: Hello
```

Lacks inherent mechanisms to verify the integrity of the hidden data.	Ensures integrity through hash functions and digital signatures.
Ideal for covert communication and watermarking.	Suitable for protecting sensitive data in communication, storage, and transactions.

The image on the left represents the original, unaltered "Normal Image," showcasing its clear and vibrant details. On the other hand, the image on the right, labeled as the "Decrypted Image," exhibits modifications caused during the encryption and decryption process. While the overall structure remains recognizable, subtle differences may emerge, reflecting the impact of steganographic encoding and decoding procedures. This comparison highlights the transition of data security processes where the integrity and confidentiality of information are preserved without drastically altering its visual appearance. The juxtaposition demonstrates how steganography ensures data protection while maintaining accessibility in its decrypted state.

Table 1. Advantages of steganography over

Steganography	Cryptography
Hides the existence of data within a medium (e.g., images, audio).	Secures the content of data by converting it into an unreadable format.
Data remains hidden; medium appears unchanged.	Encrypted data is visibly scrambled and unreadable.
Concealment: Ensures that the existence of data is undetectable	Protection: Ensures that the data cannot be understood without decryption.
Vulnerable if detection methods identify the hidden data.	Stronger security through robust encryption algorithms like AES, RSA.
Limited by the capacity of the carrier medium.	Ensures integrity through hash functions and digital signatures.

CONCLUSION

Steganography is increasingly utilized in computer systems, highlighting the need for enhanced robustness. The effectiveness of existing methods varies, making

establishing standardized evaluation frameworks essential for consistent assessment and comparison. A robust steganography system needs to have the following:

- Maintaining the quality of the cover medium,
- Safe transmission of hidden data,
- Ability to handle large amounts of data without interference, and
- Resilience against potential attacks

This paper presented a dual steganography-cryptography technique designed to transmit various text data securely. The proposed method is straightforward, versatile, and suitable for various applications. The robustness of the system is validated through both experimental and theoretical analysis.

REFERENCES

[1] *Research on Various Cryptography Techniques ,Y Alemami, MA Mohamed, S Atiewi - International Journal of Recent Technology and …, 2019*

[2] *Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes, T Filler, J Judas, J Fridrich - IEEE Transactions on Information Forensics and …, 2011*

[3] *Steganography Techniques a Review, J Kour, D Verma - International Journal of Emerging Research in …, 2014*

[4] *Image Steganography Techniques: An Overview, N Hamid, A Yahya, RB Ahmad, OM Al-Qershi - International Journal of Computer …, 2012*

[5] *A Video Steganography Approach with Randomization Algorithm Using Image and Audio Steganography, G Kale, A Joshi, I Shukla, A Bhosale - … Conference on Emerging Smart Computing and …, 2024*

[6] *Low-Complexity Features for JPEG Steganalysis Using Undecimated DCT, V Holub, J Fridrich - IEEE Transactions on Information forensics and …, 2014*

[7] *Image Steganography Techniques: An Overview, N Hamid, A Yahya, RB Ahmad, OM Al-Qershi - International Journal of Computer …, 2012*

[8] *A new cost function for spatial image steganography B Li, M Wang, J Huang, X Li - 2014 IEEE International conference on image …, 2014*

[9] *Exploring the Effectiveness of Steganography Techniques: A Comparative Analysis, S Hegde, P Sunag, RP Varun - 2023 3rd International Conference on Smart Data …, 2023*

[10] *Quantized Gaussian Embedding Steganography, M Sharifzadeh, M Aloraini, D Schonfeld - ICASSP 2019-2019 IEEE International …, 2019*

[11] *Research on Various Cryptography Techniques, Y Alemami, MA Mohamed, S Atiewi - International Journal of Recent Technology and …, 2019*

[12] *Ge, Huayong, Mingsheng Huang, and Qian Wang. "Steganography and steganalysis based on digital image." In 2011 4th international congress on image and signal processing, vol. 1, pp. 252-255. IEEE, 2011.*

[13] *Saxena, Aditya, and Ganga Maheshwari. "Digital image steganography." In 2021 International Conference on Simulation, Automation & Smart Manufacturing (SASM),*
a. pp. 1-5. IEEE, 2021.

[14] *Singh, Juhi, and Mukesh Singla. "A Novel Method of high- Capacity Steganography Technique in Double Precision Images." In 2021 International Conference on Computational Performance Evaluation (ComPE), pp.*
a. 780-784. IEEE, 2021.
b. Niimi, Michiharu, Hideki Noda, Eiji Kawaguchi, and Richard O. Eason. "High capacity and secure digital steganography to palette-based images." In Proceedings. International conference on image processing, vol. 2, pp. II-. IEEE, 2002.
c. Steganalysis, High Capacity Despite Better, and Andreas Westfeld. "F5—A steganographic algorithm." In Information Hiding: 4th International Workshop, IH 2001, Pittsburgh, PA, USA, April 25-27, 2001.Proceedings, vol. 2137, p. 289. Springer, 2001.

[15] *Fridrich, Jessica. Steganography in digital media: principles, algorithms, and applications. Cambridge university press, 2009.*

[16] *Qin, Jiaohua, Yuanjing Luo, Xuyu Xiang, Yun Tan, and Huajun Huang. "Coverless image steganography: a survey." IEEE access 7 (2019): 171372-171394.*

[17] *Holub, Vojtěch, and Jessica Fridrich. "Low-complexity features for JPEG steganalysis using undecimated DCT." IEEE Transactions on Information forensics and security 10, no. 2 (2014): 219-228.*

[18] *Song, Xiaofeng, Fenlin Liu, Chunfang Yang, Xiangyang Luo, and Yi Zhang. "Steganalysis of adaptive JPEG steganography using 2D Gabor filters." In Proceedings of the 3rd ACM workshop on information hiding and multimedia security, pp. 15-23. 2015.*

[19] *Sharifzadeh, Mehdi, Mohammed Aloraini, and Dan Schonfeld. "Quantized Gaussian embedding steganography." In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2637-2641. IEEE, 2019.*

[20] *Filler, Tomáš, Jan Judas, and Jessica Fridrich. "Minimizing additive distortion in steganography using syndrome-trellis codes." IEEE Transactions on Information Forensics and Security 6, no. 3 (2011): 920935.*

[21] *Li, Bin, Ming Wang, Jiwu Huang, and Xiaolong Li. "A new cost function for spatial image steganography." In 2014 IEEE International conference on image processing (ICIP),pp. 4206-4210. IEEE, 2014.*

[22] *Holub, Vojtěch, Jessica Fridrich, and Tomáš Denemark. "Universal distortion function for steganography in an arbitrary domain." EURASIP Journal on Information Security 2014 (2014): 1-13.*

[23] *Baluja, Shumeet. "Hiding images within images." IEEE transactions on pattern analysis and machine intelligence 42, no. 7 (2019): 1685-1697.*

.