A Comparative Review of Steganography and Embedding Techniques for Secure Digital Media Communication

Abhishek Sharma
B.Tech Student, Department of CSE, Global Institute of Technology, Jaipur, Rajasthan, India
21egjcs004@gitjaipur.com

Kritika Paliwal
Assistant Professor, Department of CSE, Global Institute of Technology, Jaipur, Rajasthan, India
kritika.paliwal@gitjaipur.com

ABSTRACT: The rapid growth of the internet and digital technologies has transformed the way information is communicated worldwide, increasing the reliance on digital media such as text, images, audio, video, and software for data exchange across public networks. Among these, digital images play a crucial role in various applications including social platforms, e-commerce, online publications, and communication services. However, the open and distributed nature of the Internet makes data vulnerable to unauthorized access, interception, and manipulation by malicious entities. Ensuring secure and reliable communication has therefore become a major concern. Steganography and data embedding techniques have emerged as effective solutions for enhancing digital data security by concealing information within multimedia files, making it difficult for attackers to detect or alter the hidden content. Alongside cryptography, these techniques provide robust protection against unauthorized data breaches. This paper presents a detailed comparative analysis of various steganography and embedding methods used for securing text-based and image-based information. The study highlights the strengths, limitations, and application suitability of each technique, offering insights for future advancements in secure digital communication systems.

KEYWORDS: LSB, DCT, DWT, Embedding, Steganography, Secrete Image, Secrete Text Data.

1. INTRODUCTION

In the today going on technology, for the data exchange the Internet is the most popular and important medium. With advances of the internet and information technology, the digital media has become one of the most popular and best-known data transfer tools. This digital data includes text, images, audio, video and software transferred via the public network [1]. Digital Data are the most widely used modes of communication in very field usually, such as the research, industry, medical, military etc. Significant image transfers take place over an unsecured web network. Therefore, it is necessary to establish adequate security so that the digital picture or digital image prevents from the unauthorized persons to accessing secrete information. Steganography and cryptography are the most popular techniques for data security [2], [3]. Data protection has come to be a heavy digital verbal exchange drawback through the internet or the alternative medium. Cryptography and stenography are the widely used technique for data security. In cryptography data is change one form to another form and in steganography secret data is hidden into cover data [4], [5]. The word Steganography comes from the Greek word "stegos", which meaning "cover" and graphic meaningful writing that designates it as a cover writing [4]. In Image Steganography, data is hidden solely in cover image or picture. Steganography is the science and art of secret communication [6], [7]. Hiding information is important to secure online communication, especially in the military

and commercial areas, and copying and unauthorized access. Correspondence between two gatherings, security offices, any knowledge association, or some other private trade of data must be secure. The main goal of hiding information to pictures is to transfer information safely over the Internet [8], [9]. Steganography is mainly cauterized into four types that are text, image, audio and video steganography. Steganography is widely used for secret communications, feature tagging and copyright protection.

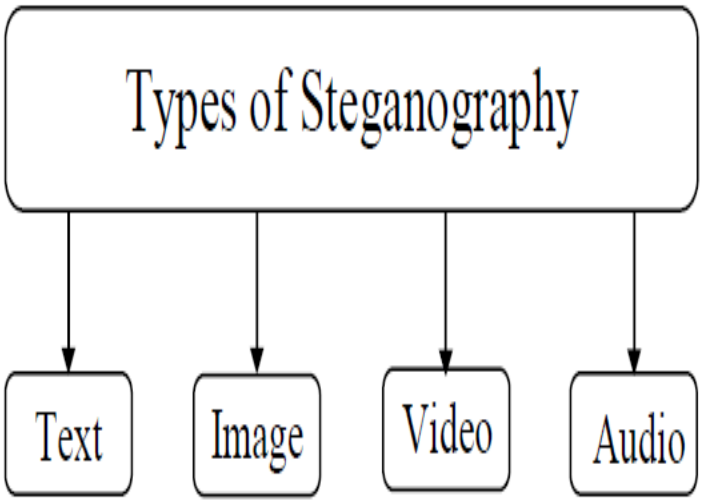

Figure 1: Types of Steganography

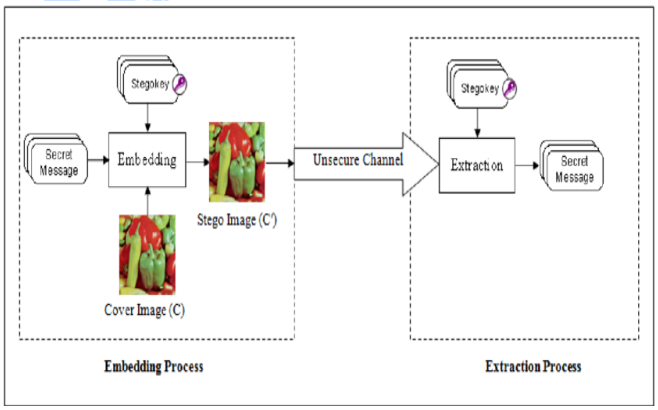

Figure 2: Embedding Process

2. LITERATURE REVIEW

In [10], the authors present the deep learning and transfer learning based ensemble model for leaf diseases using image processing techniques. In [11], various image steganography techniques are reviewed with a focus on improving key performance parameters such as imperceptibility, capacity, and security. The study proposes an adaptive model that selects the most suitable embedding technique to minimize error rates during message insertion. By evaluating multiple models using reverse LSB substitution, the technique ensures the lowest embedding distortion. This adaptive method significantly improves imperceptibility and enhances the overall performance of LSB-based steganography. In [12], a new medical image steganography method based on optimal pixel similarity is presented. Since the human visual system can easily detect distortions in images, maintaining high visual quality is crucial, especially in medical applications. The proposed optimization-based technique increases data hiding capacity while preserving the quality of the medical image. The performance of the method is evaluated using visual quality metrics such as PSNR and MSE, showing better

accuracy and reduced perceptual distortion. In [13], the authors propose a secure grayscale medical image protection technique that embeds sensitive patient information in the form of a 2D barcode using the LSB method. After embedding, the image is encrypted using a Genetic Algorithm to further improve confidentiality. This approach enhances both the security of patient information and the integrity of medical images. In [14], different JPEG steganography techniques are comparatively analyzed. The study considers the three major requirements of steganography capacity, robustness, and imperceptibility and discusses methods recommended by experts for improving data hiding in compressed JPEG images. In [15], the paper presents a data-hiding technique in which both the message bits and the pixel bits of the cover image are randomized. This randomness ensures higher security by producing stego patterns that are difficult for attackers to detect or decode. The approach strengthens confidentiality by minimizing predictable embedding behavior.

Table 1: Comparative Analysis of Different Steganography and Embedding Technique

Ref No.	Technique Used	Description	Advantage
[11]	LSB	In this work proposed a secure image steganography technique in which hide an image in an image using the LSB technique and measure the security of the hiding in the term of MSE and PSNR.	Get low MSE and high PSNR Value.
[12]	optimum pixel similarity	In this discussed the human vision system the quality of image can be noticed and it attracts the attacker attention. So the purpose of this study to increase the hidden data amount and ensure the quality of the setgo image is high quality.	Quality of merit analysis such as PSNR, MSE is better.
[13]	LSB, Genetic Algorithm	Protect digital medical image using pixel based image protection using LSB water marking and AES algorithm.	Difficult to creak. Apply steganography and cryptography together to enhance the security.
[14]	DCT	Discussed a portion of the methods recommended by the specialists.. To apply jpeg steganography, three significant boundaries of image steganography are considered, in particular joining, heartiness and imperceptibility.	Improve the security of the secret data stored in smart device or framework.
[15]	LSB	Used pixel based technique for file security purpose.	the pixel bits of the image are also made unique, making the pattern unintelligible to recognize.

3. CONCLUSION

In this, many important stenography techniques have been introduced and analyzed to become familiar with the different stenography algorithms that used for the image that has been transferred to the network. According to the survey of recent research, it has been said

that security is the main concern in the transmission of images. The security issue is expanding quickly with devices created for hacking image information. Numerous analysts have proposed answers for the security issue; however have not had the option to get total security on the unstable organization. Stenography sends privileged insights through apparently innocuous covers to hide the presence of a secret. Hide advanced data, images and their subordinates is progressively utilized and applied. In this give an overview and comparative analysis of different stenography techniques for image, data or information hiding.

REFERENCES

[1] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," in Proc. 2021 6th IEEE International Conference on Communication and Electronics Systems (ICCES), pp. 1153–1157, 2021.

[2] N. Tiwari, D. Goyal and N. Hemrajani, "A hybrid method for image watermarking," International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), vol. 6, no. 6, pp. 894–898, 2017.

[3] G. K. Soni, H. Arora and B. Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm," in Artificial Intelligence: Advances and Applications 2019 – Algorithms for Intelligent Systems, Springer, 2020, pp. 83–90, 2020.

[4] G. Sharma, N. Hemrajani, S. Sharma, A. Upadhyay, Y. Bhardwaj and A. Kumar, "Data management framework for IoT edge-cloud architecture for resource-constrained IoT application," Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, no. 4, pp. 1093–1103, 2022.

[5] A. Maheshwari, R. Ajmera and D. K. Dharamdasani, "Unmasking Embedded Text: A Deep Dive into Scene Image Analysis," in Proc. 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), pp. 1403–1408, 2023.

[6] V. Singh, M. Choubisa and G. K. Soni, "Enhanced Image Steganography Technique for Hiding Multiple Images in an Image Using LSB Technique," TEST Engineering & Management, vol. 83, pp. 30561–30565, May–Jun. 2020.

[7] M. K. Ramaiya, D. Goyal and N. Hemrajani, "Improved Image Steganographic System by using Multiple Encryption and DWT," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 6, issue 8, pp. 1–7, 2017.

[8] A. Upadhyay, R. Misra, S. K. Henge and Y. Bhardwaj, "Protection of Digital Image and Text Information Security Using LSB and Crossover Techniques," in Computational Vision and Bio-Inspired Computing, Advances in Intelligent Systems and Computing, vol. 1439, pp. 601–608, 2023.

[9] P. Jha, K. K. Sharma, B. Jain and V. Sharma, "Digital Image Encryption Using AES Algorithm," EIJO Journal of Engineering, Technology and Innovative Research (EIJO–JETIR), vol. 4, issue 2, pp. 1–6, 2019.

[10] P. Jha, D. Dembla and W. Dubey, "Implementation of Transfer Learning Based Ensemble Model using Image Processing for Detection of Potato and Bell Pepper Leaf Diseases," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, pp. 69–80, 2024.

[11] S. Rustad, D. R. I. M. Setiadi, A. Syukur and P. N. Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility," Journal of King Saud University – Computer and Information Sciences, pp. 1–10, 2021.

[12] S. Karakus and E. Avci, "A new image steganography method with optimum pixel similarity for data hiding in medical images," Medical Hypotheses, vol. 139, pp. 1–8, 2020.

[13] G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique," in Smart Systems and IoT: Innovations in Computing, pp. 483–492, 2020.

[14] D. Watni and S. Chawla, "A Comparative Evaluation of Jpeg Steganography," in Proc. 2019 5th IEEE International Conference on Signal Processing, Computing and Control (ISPCC), pp. 36–40, 2019.

[15] A. G. Benedict, "Improved File Security System Using Multiple Image Steganography," in Proc. IEEE International Conference on Data Science and Communication (IconDSC), pp. 1–5, 2019.