IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141165

"ANDROID APPLICATION USING STEGANOGRAPHY TECHNIQUES FOR INFORMATION HIDING"

Prof.Dr. G.G Taware[1], Yogiraj Deshmukh[2], Laxman Bhandarwad[3], Nitesh Jadhav[4]

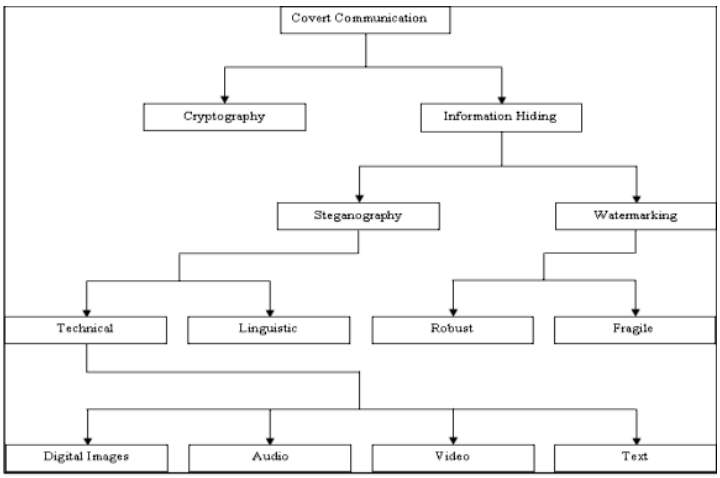
Assistant Professor, Dattakala Group of institutions Faculty Of Engineering, Tal-Daund, Dist-Pune[1]

Scholars, Dattakala Group of institutions Faculty Of Engineering, Tal-Daund, Dist-Pune[2-4]

Abstract: The practice of hiding communication by enclosing data in other data is known as steganography. There are many different carrier file kinds available, but due to their popularity on the Internet, digital photographs are the most popular. From ancient times to the present, the protection of secret information has always been a major concern. The basic goal of steganography is to hide the existence of the message so that an attacker cannot detect it. To incorporate hidden information, any type of cover item, such as text, image, or video, can be used. In this paper, a brief overview of steganography which is one of the main branches of information hiding is explained and covers its primary forms, categorization, and uses.

INTRODUCTION

Data transfer is becoming faster and easier as communication technology advances. As a result, it is simpler for unauthorized users to intercept data transmissions and get access without authorization. Therefore, maintaining the privacy of data while it is in use or being transmitted is a crucial concern. Two important information security methods for preserving data confidentiality are data encryption and data hiding. The hiding of information or resources, as well as protection from disclosure or exposure to unauthorized users or systems, is known as confidentiality. When information or resources are confidential, they are hidden from everyone save the systems or individuals who have been given permission and privileges to access them [3, 6]. When unauthorized users or systems get access to or can view information, confidentiality has been violated: When something is available, it may be accessed when needed, including data and other crucial resources. The ability to obtain and receive information in the desired format and within a fair amount of time without hindrance or interference, in other words, is referred to as availability [6]. Secret communication can be secured in two main ways as shown in figure (2) [11]. Cryptography and Information hiding. They play a significant role in maintaining secrecy. Information is encrypted by cryptography to render it unintelligible, and a cryptographic key regulates access to the encrypted data. Data hiding covers both the existence and the substance of data. No one can argue that information protection is increased by information hiding.



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141165

LITERATURE SURVEY

Data and information are hidden in [21] in digital image format since the internet is the primary market for it. Many different ways have been created for data hiding, some of which are simple while others are a little more laborious. Each technique has its advantages, applications, and restrictions. The primary objective of this essay is to provide an overview of steganography, along with information about its demand, benefits, and methodologies. This study also makes an effort to determine which steganography approaches are more beneficial and what are required of them. It also illustrates which applications will be more compatible with each steganography methodology The improved LSB method for 24-bit color images is shown in [23] to be superior to the LSB technique for 8-bit color images. Before comparing their results, the peak signal-to-noise ratio (PSNR), mean squared error (MSE), and histogram analysis are calculated for the LSB approach for both 8- bit and 24-bit color images. The improved LSB method for 24-bit color images is then discussed. The hidden image's MSB was integrated into the cover image's LSB using the LSB algorithm. Two approaches are provided for the 24-bit color image. Firstly, 2 MSB of the secret image are used in place of the final 2 LSB of each plane (red, green, and blue) of the cover image. In the second technique, the first MSB of the secret picture is substituted for the last LSB of each red plane, followed by the following two MSBs of the secret image for each green plane, and the next three MSBs of the secret image for each blue plane. This indicates that a total of 6 bits of a secret image can be hidden in a 24-bit color image. According to experimental findings, in the case of a 24- bit stego-image, the original cover image cannot be visually distinguished The LSB substitution approach is described in as the most straightforward method for hiding data within a picture. The LSB replacement method overwrites the low-order bit (LSB) of each byte in a cover picture using the binary representation of hidden data. In the existing method, there used the cover image of 256*256 and split the image into four parts then they are using LSB substitution and pixel indicator in a zigzag manner. They achieved a stego image with PSNR of greater than 50 DB and also the MSE value of the existing method is low. In the proposed method, we are going to flip the image into 8 parts. By using pixel indicator and LSB substitution method we are trying to achieve the Stego-image having greater than 60 DB PSNR value and lower MSE value. A simple LSB substitution-based data hiding method is proposed in. The picture quality of the stego - image can be considerably enhanced with minimal additional computing cost by using an optimum pixel adjustment technique to the stego image created by the straightforward LSB substitution method.

METHODOLOGY

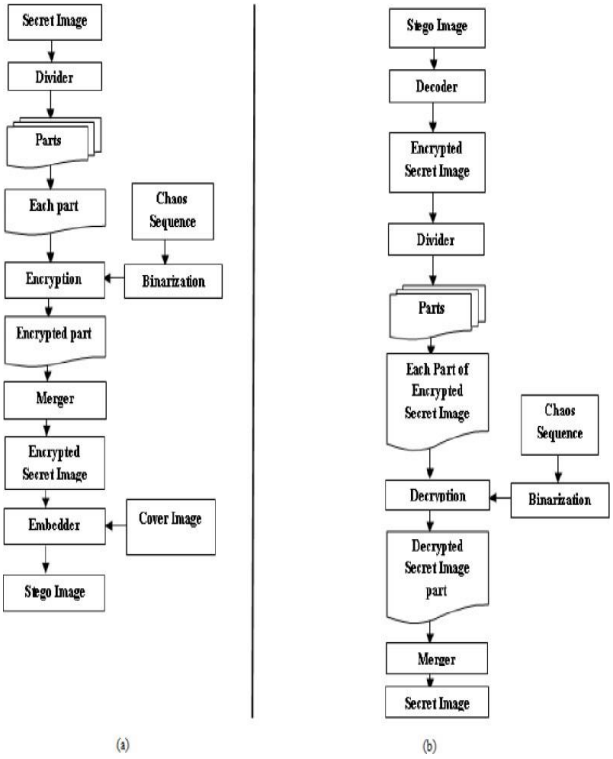
The methodology of steganography involves a systematic process of concealing secret information within a cover medium such as an image, audio, video, or text file in such a way that the existence of the hidden data remains undetectable. The process typically begins with the **selection of a suitable cover medium** that has enough redundant or less significant data portions where information can be embedded without noticeable distortion. Next, the **secret message**—which may be text, image, or any digital data—is **converted into a binary format** to facilitate embedding. A **key or algorithm** is then used to determine the positions within the cover medium where the secret bits will be hidden. One of the most commonly used techniques for image steganography is the **Least Significant Bit (LSB) substitution**, where the least significant bits of the pixel values are replaced with bits of the secret message. After embedding, the **stego object** (the medium containing the hidden data) is generated and trans After embedding, the **stego object** (the medium containing the hidden data) is generated and transmitted to the receiver. At the receiver's end, the hidden information is **extracted using the same key and algorithm**, ensuring that only authorized parties can retrieve the secret message. To maintain the integrity and security of the hidden data, **encryption** may also be applied before embedding. The methodology thus ensures **confidentiality, imperceptibility, and robustness**, making steganography an effective technique for secure communication and data protection.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

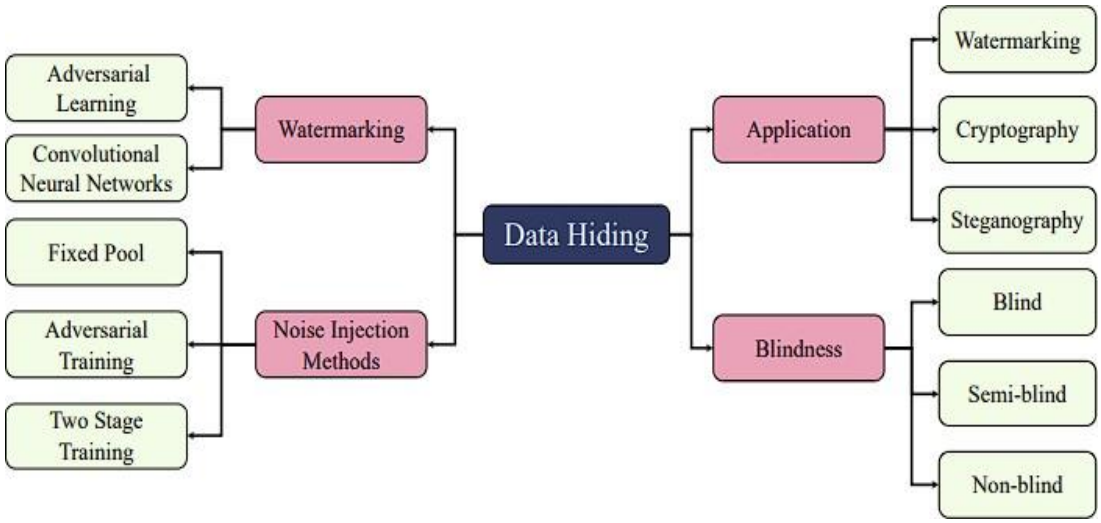
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141165



SYSTEM ARCHITECTURE



CONCLUSION

This survey has provided an extensive overview of current deep learning techniques for data hiding, encompassing watermarking and steganography methods. Through analysis of network architecture and model performance, the survey has demonstrated how digital watermarking and steganography share a common goal of embedding information in digital media, and how both can benefit from deep learning techniques. Additionally, the survey explored future research directions and highlighted the potential for this field to revolutionize the protection of digital IP and communication security in Responsible AI software industries. As deep learning techniques continue to advance, they are expected to surpass traditional algorithms in all types of media, ultimately enhancing the accountability and safety of AI. This promising field holds great potential and is expected to have a significant impact on digital security.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141165

REFERENCES

[1] A. Herrigel, S. Voloshynovskiy, and Z. Hrytskiv, "An optical/digital identification/verification system based on digital watermarking technology," Proceedings of SPIE - The International Society for Optical Engineering, 03 2000.

[2] S. Bhattacharya, "Survey on digital watermarking- a digital forensics & security application," International Journal of Advanced Research in Computer Science and Software Engineering ISSN number:2277-128X, vol. 4, p. 11, 11 2014.

[3] R. Lu, G. Zhang, L. Kou, L. Zhang, C. Liu, Q. Da, and J. Sun, "A new digital watermarking method for data integrity protection in the perception layer of iot," Security and Communication Networks, vol. 2017, p. 12, 10 2017.

[4] A. Ferdowsi and W. Saad, "Deep learning-based dynamic watermarking for secure signal authentication in the internet of things," in 2018 IEEE International Conference on Communications (ICC). IEEE, 2018, pp. 1–6.

[5] G. Hua, J. Huang, Y. Q. Shi, J. Goh, and V. L. Thing, "Twenty years of digital audio watermarking—a comprehensive review," Signal processing, vol. 128, pp. 222–242, 2016.

[6] A. Jadhav and M. Kolhekar, "Digital watermarking in video for copyright protection," in Proceedings - International Conference on Electronic Systems, Signal Processing, and Computing Technologies, ICESC 2014. Nagpur, India: IEEE, 01 2014, pp. 140–144.

[7] S. Abdelnabi and M. Fritz, "Adversarial watermarking transformer: Towards tracing text provenance with data hiding," in 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021, pp. 121–140.

[8] S. P. Mohanty, A. Sengupta, P. Guturu, and E. Kougianos, "Everything you want to know about watermarking: From paper marks to hardware protection: From paper marks to hardware protection." IEEE Consumer Electronics Magazine, vol. 6, pp. 83–91, 2017