SECURING CLOUD DATA WITH WATERMARKING STRATEGIES IN CLOUD COMPUTING SYSTEM

Amit Kumar[1], Dr. Ravindra Kumar Gupta[2]

[1]M. Tech. Scholar, Department of Computer Science Engineering, RKDFIST, M.P., India
[2] Professor, Department of Computer Science Engineering, RKDFIST, M.P., India

ABSTRACT

In the digital age, the security of sensitive information transmitted over cloud platforms has become increasingly crucial. This research focuses on developing a robust method for embedding confidential data within audio files without introducing noticeable alterations post-insertion. We explore the field of audio steganography as a viable solution for protecting the integrity and confidentiality of information conveyed through voice communications, particularly in insecure environments. Utilizing the Least Significant Bit (LSB) algorithm, our proposed methodology creates a stego audio file that effectively conceals and encrypts secret information. The performance of the technique is evaluated through key metrics, specifically Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE), which serve as indicators of the quality of the stego audio. Experimental results demonstrate high PSNR values and low MSE values, confirming that the embedded audio retains its original quality while facilitating a substantial amount of hidden data. The findings highlight the effectiveness of the LSB technique, especially in scenarios involving audio files with minimal variations in sound quality. This study contributes to the field of cloud data security by presenting a reliable approach for safeguarding sensitive information within audio communications, thereby enhancing data protection measures in cloud environments.

Keyword : - *Cloud computing, data security, watermarking techniques, fragile watermarking, robust watermarking, semi-fragile watermarking, encryption, access control, multi-faceted protection, scalability.*

INTRODUCTION

In Cloud data security is a critical area of concern for organizations and individuals relying on cloud services for data storage and processing. One effective method to address data security issues is through digital watermarking, which adds a layer of protection to safeguard sensitive information from unauthorized access, modification, and duplication. Digital watermarking in the context of cloud security involves embedding invisible, unique markers within data that serve as proof of ownership and authenticity. These markers can only be recognized and verified by authorized users or systems, ensuring that data integrity and provenance are maintained.

In practice, watermarking technology for cloud data security works by embedding an invisible digital signature or identifier into the data before it is uploaded to the cloud. This signature, which remains undetectable to general users, acts as an authentication tool, verifying the data owner’s identity and detecting any unauthorized modifications. If a security breach occurs, such as unauthorized copying or distribution, the watermark allows owners to trace and verify the data source. This feature is particularly useful in protecting sensitive information, intellectual property, and proprietary databases in the cloud, where data ownership is a critical issue

Furthermore, watermarking can be designed to withstand common tampering techniques, providing a robust method for tracking data integrity over time. It is resistant to compression, format changes, and other alterations that data may undergo during cloud processing. Thus, watermarking offers a reliable solution to the problem of ensuring that only authorized individuals can access or manipulate cloud-stored data.

Implementing watermarking for cloud data security can be beneficial across various industries, including finance, healthcare, and legal sectors, where data protection and ownership verification are paramount. By embedding invisible, resilient markers, watermarking not only strengthens data security in the cloud but also fosters trust among cloud service users, enabling them to take full advantage of cloud computing without compromising data confidentiality and integrity. Cloud computing has transformed how individuals and organizations access IT resources, offering a flexible, pay-as-you-go service model that shifts infrastructure management to third-party providers. This model allows users to focus on core operations while accessing scalable, remotely managed hardware and software. However, as cloud reliance grows, so do data security concerns, particularly around unauthorized access and data integrity. To address these challenges, this research proposes a security enhancement technique based on digital watermarking technology, designed to detect unauthorized database access and confirm data ownership.

Digital watermarking is an established method in digital security, often used to safeguard intellectual property by embedding unique, invisible markers within digital content. These markers serve as identifiers, allowing data owners to verify the origin and integrity of their assets. Applied to cloud databases, watermarking offers a layer of protection by embedding ownership information directly into the database, effectively preventing unauthorized copying or tampering.

2. CLOUD COMPUTING

Cloud computing refers to the delivery of computing services over the internet, allowing users to access data storage, applications, networking, and processing power remotely. Instead of managing resources on local servers or personal devices, cloud computing offers access to a shared pool of configurable resources managed by third-party providers. Users can leverage these resources on a pay-as-you-go basis, eliminating the need for upfront investments in hardware and infrastructure. In essence, cloud computing represents a paradigm shift from owning and maintaining computing resources to accessing and utilizing them on demand. It abstracts the underlying infrastructure, enabling users to focus on their applications and business needs without worrying about the complexities of managing hardware, storage, and networking.

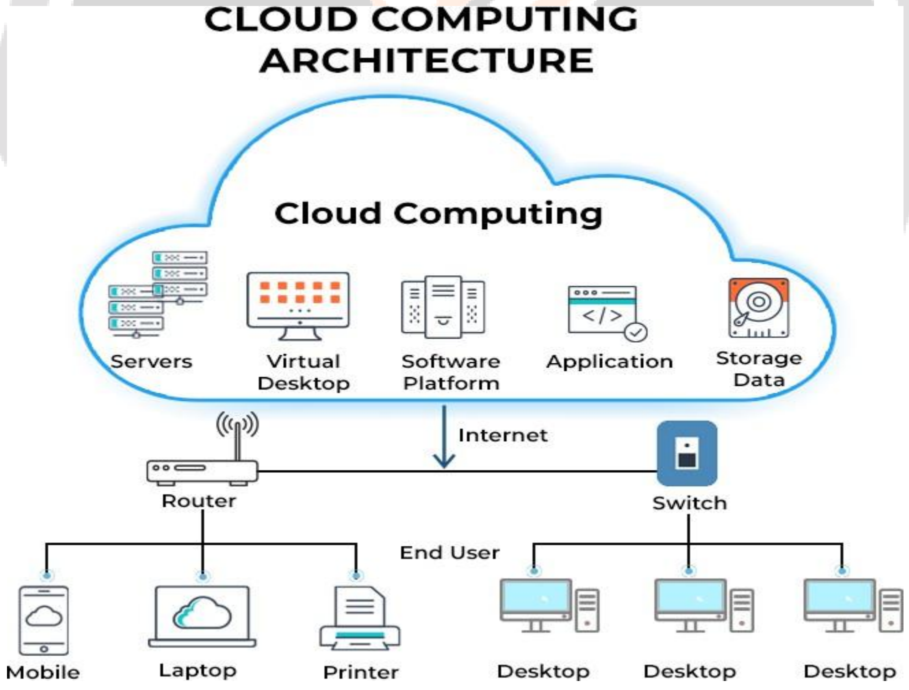


Fig -1 Shows cloud computing

3. METHODOLOGY

The creation of digital records in their kind of style has attracted a specific curiosity as of researchers to form positive their safety. System like encoding and watermarking are already utilize throughout this regard. Though, the requirement for new procedure and new algorithms to counter constantly-changing malicious makes an effort to the integrity of digital data has been converted into a necessity in today's digital time. Steganography, that literary implies that "covered writing" has drawn further thought among the previous few years. Its main goal is to cover the actual fact that a communication is taking place between 2 components.

The sender embeds secret information into a digital cover file using a key, creating a stego file in such a way that an observer cannot detect the presence of the hidden information. On the receiving end, the recipient processes the stego file to extract the concealed information. An example of audio steganography can be illustrated with a digital audio signal serving as the cover file. A practical application of this technique would involve covert communication using a seemingly innocuous audio signal, such as conversations from phone calls or video chats. Various factors can influence the effectiveness and quality of audio steganographic methods. The importance and so the impact of each feature depend on the applying and so the transmission atmosphere. The most vital properties include robustness to noise and to signal manipulation, safety and hiding ability of embedded data. Robustness requirement is tightly related to the applying and is that the most difficult to satisfy during a steganographic system. in addition, there's a trade-off between robustness and hiding-capacity. Generally, they hardly exist within a similar steganographic system.

The proposed method employs various techniques, including thresholding, Discrete Cosine Transform (DCT), and Least Significant Bit (LSB) manipulation. This approach operates efficiently while optimizing storage capacity and enhancing the security level. Additionally, it improves the quality of the steganographic images.

The new plan has been planned for the security of secret data and parties also. The most goal of this technique is to develop an efficient security system for the protection of confidential information during the transformation method. The fundamental plan of this technique is to analyze the image, secure the secret file also because the cover files with strong algorithmic rule. The system consist of 2 main phases encoding and decoding numerous stages of encoding are; image acquisition, preprocessing, enhancement, read and convert audio file, applying compression using DWT transform, Embedding audio in image using LSB technique, Stego image is retrieved. In preprocessing stage, if image contain any form of noise, smoothing are applied to remove noise. Afterwards, in enhancement part, the visual look of the image is improved using histogram equalization. Proceeding towards audio file, scan and compression is performed using DWT (discrete wave transforms). Currently encode the audio file using AES (advance coding algorithm), it's the strongest algorithmic rule for coding yet. When encoding audio file is embedded in image using LSB (least significant bit) technique and Stego image is retrieved. Currently decoding part, embedded image is retrieved. Secret information is recovered. Decode the audio file; convert the audio file from hexadecimal to decimal number. Retrieve the first audio file

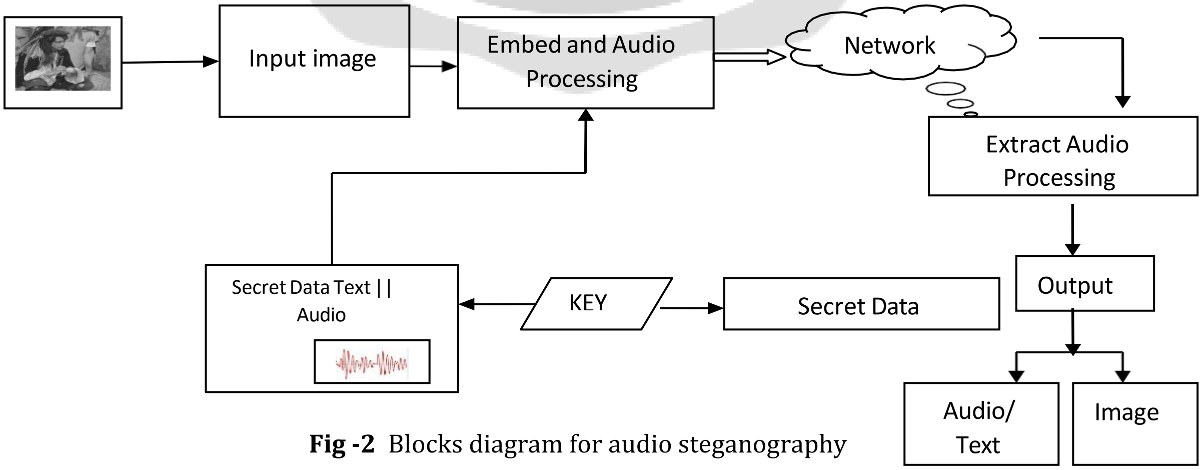


Fig -2 Blocks diagram for audio steganography

The propose solution is analyzed on the idea of PSNR (peak signal to noise ratio) and MSE (mean sq. error) frequency. Whereas PSNR is used to measure the image quality of original and Stego image. Generally, high value of PSNR indicates that Stego image is of higher quality. MSE may be a risk performs that represents average sq. error between the first image and Stego image.

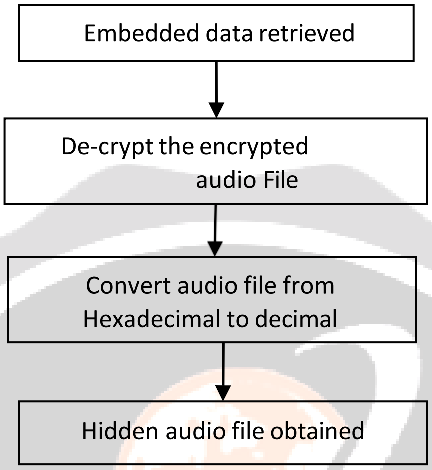

Embedded data retrieved
De-crypt the encrypted audio File
Convert audio file from Hexadecimal to decimal
Hidden audio file obtained

Fig -3 Decryption process

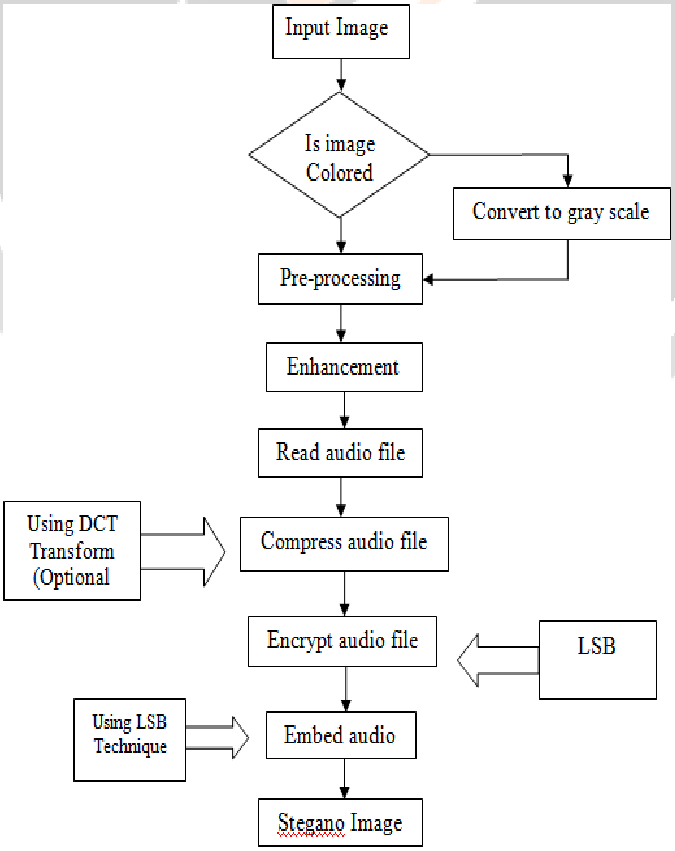
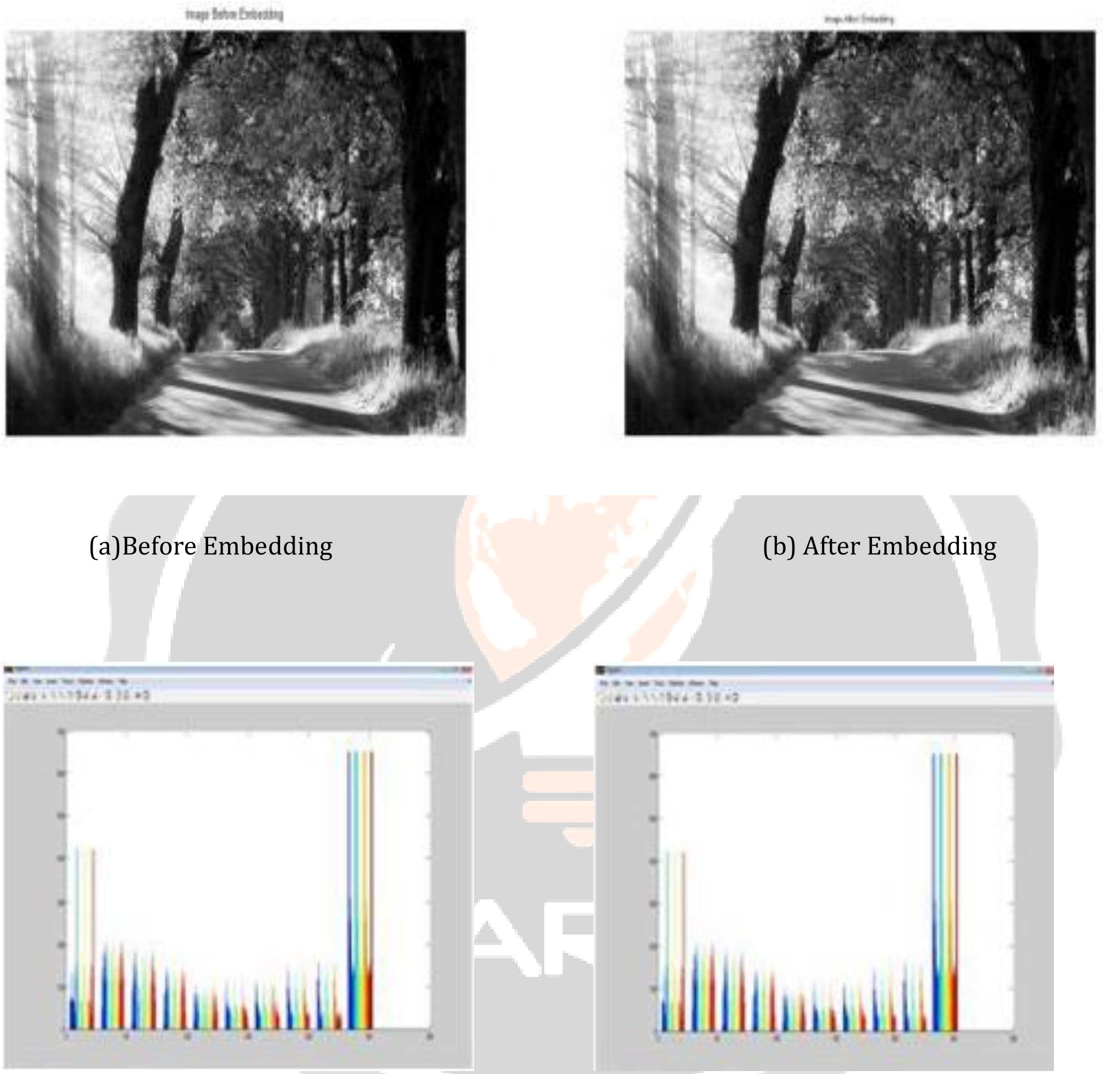


Fig -4 Flow chart of proposes solution.

3.1 RESULTS AND DISCUSSION

The simple LSB technique is applied on the images below. Single bit of each byte is manipulated using LSB and the change is too minor that it can’t be seen by naked eye. After implementation Original-images, Embedded- images along with their histograms are shown respectively.



(a)Before Embedding

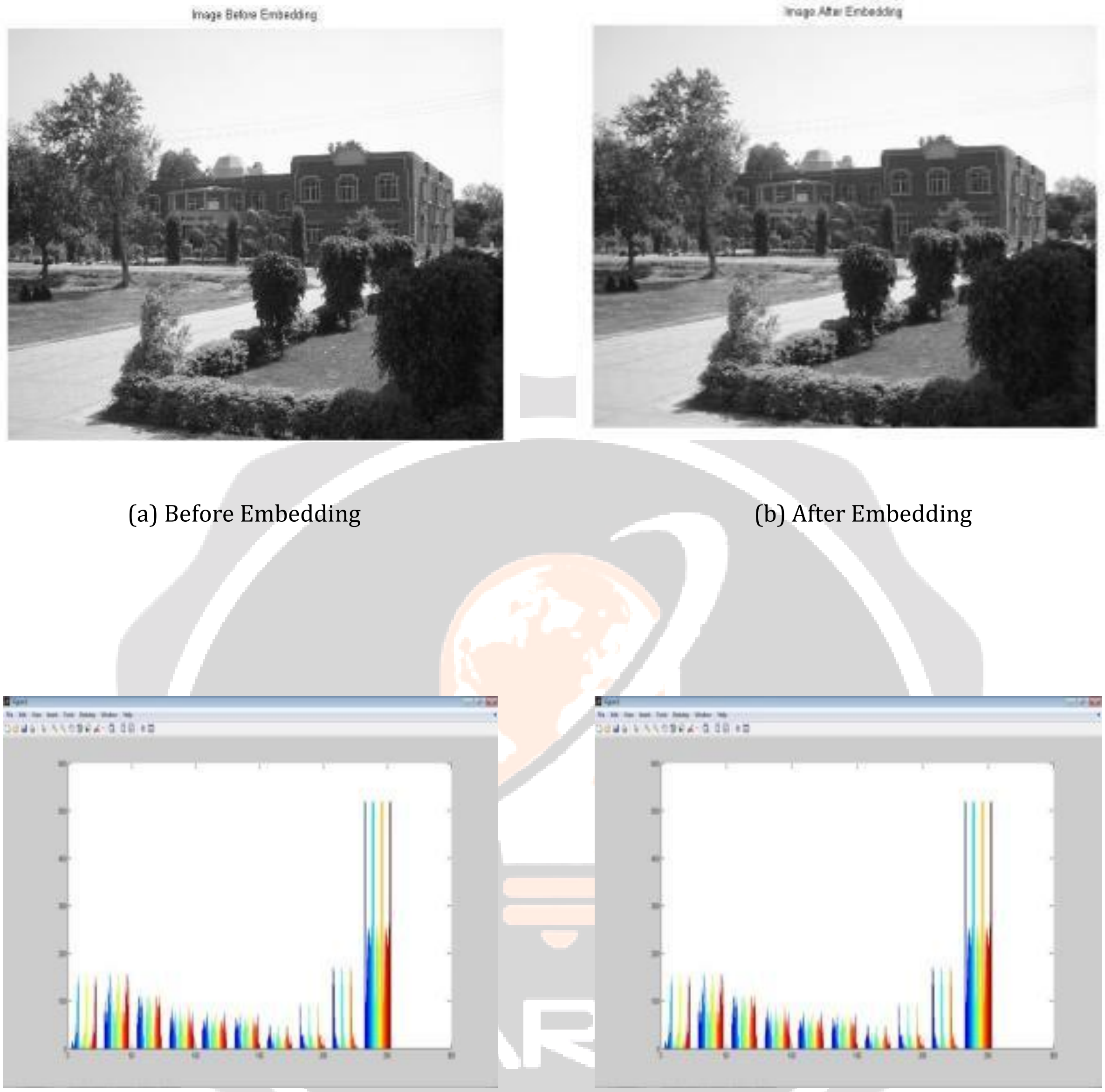
(b) After Embedding

(c) Histogram Original Image

(d) Embedded Image

Fig -5 Landscape.jpeg

Figure 5 illustrates the Landscape.jpeg image. In this figure, part (a) displays the original image, while part (b) presents the output image after the embedding process. Part (c) depicts the histogram of the original image, and part (d) shows the histogram of the embedded image.



(a) Before Embedding

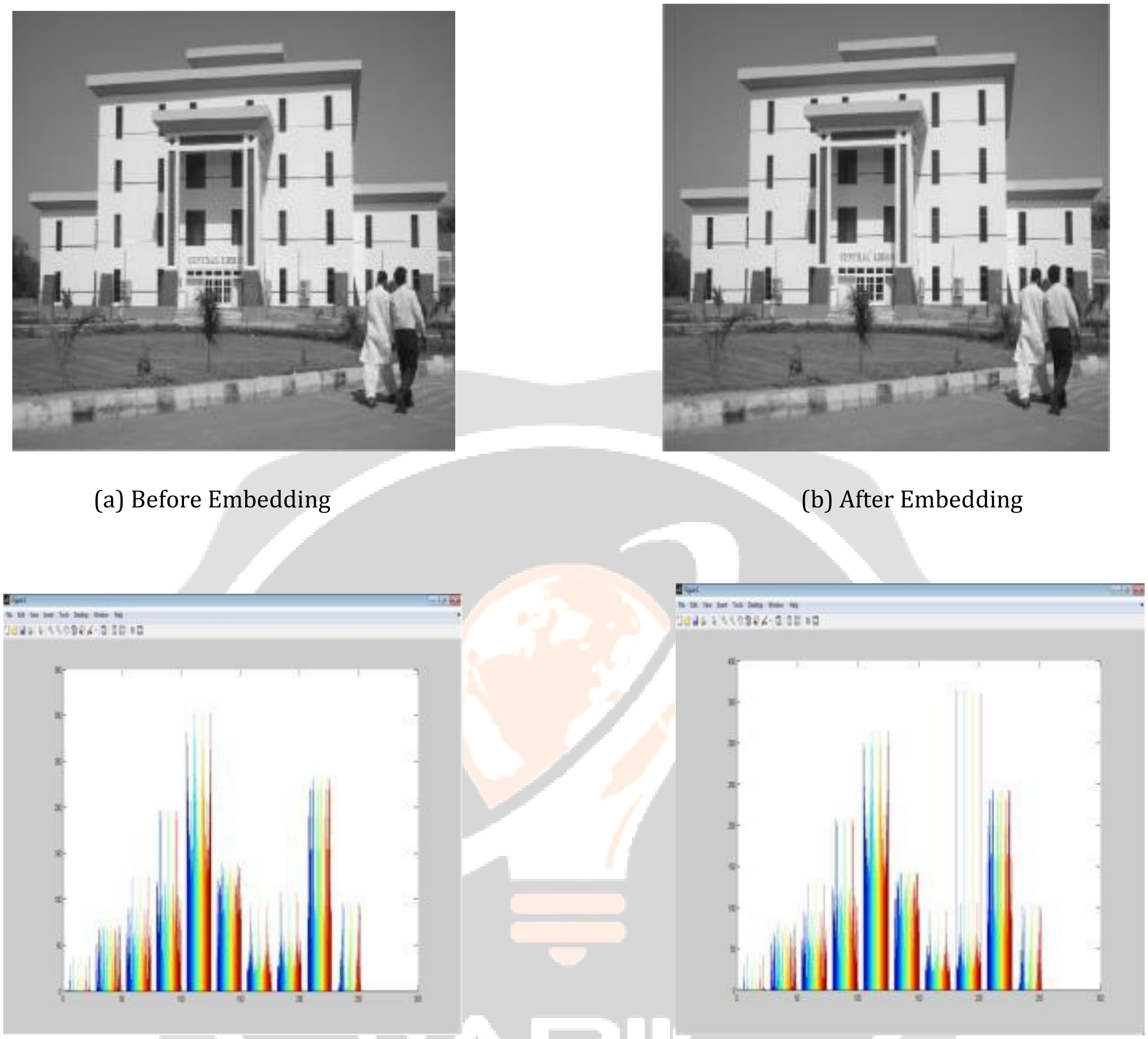
(b) After Embedding

(c) Histogram Original Image

(d) Histogram Embedded Image

Fig- 6 Institute.jpeg

Figure 6 presents the institute.jpeg image. In this illustration, part (a) displays the original image, while part (b) shows the output image following the embedding process. Part (c) provides the histogram of the original image, and part (d) depicts the histogram of the embedded image.



(a) Before Embedding

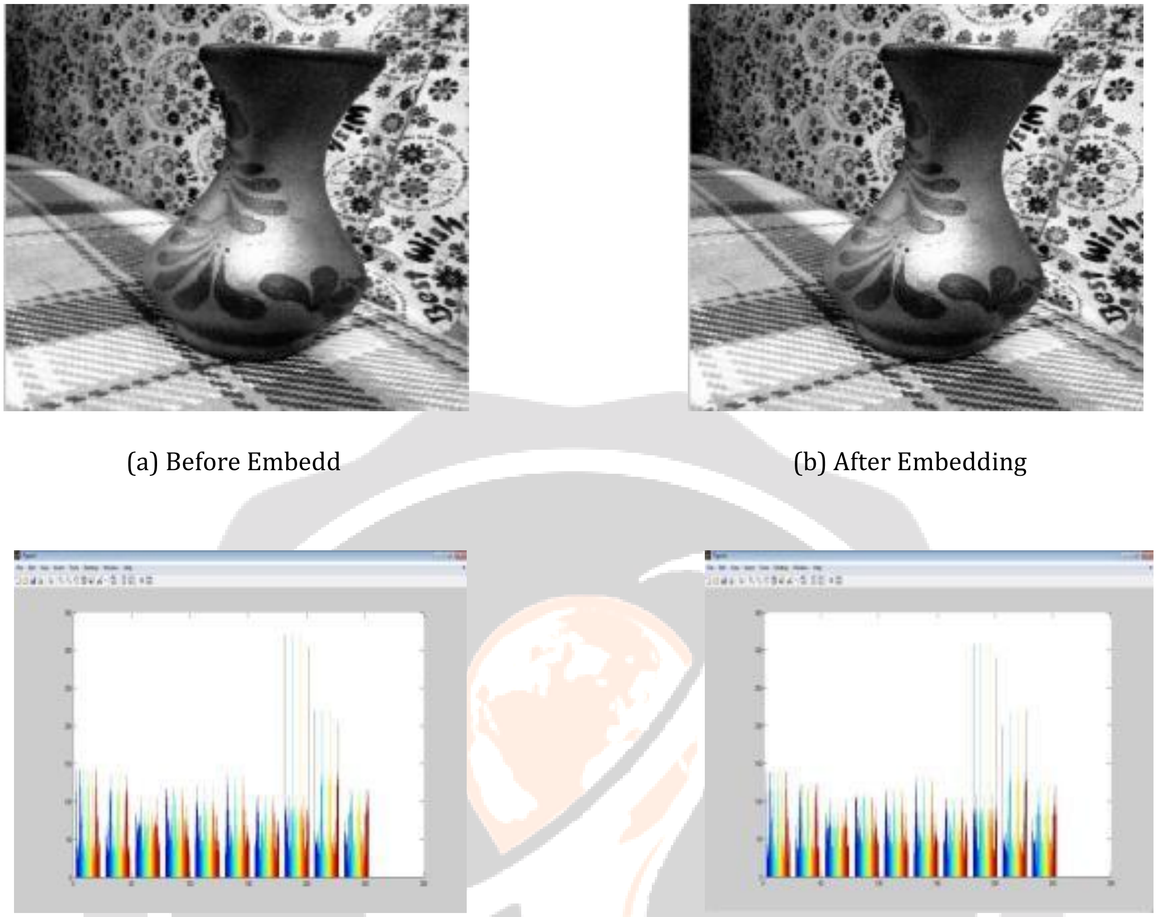
(b) After Embedding

(c) Histogram Original Image

(d)Histogram Embedded Image

Fig- 7 Library.jpeg

Figure 7 illustrates the library.jpeg image. In this figure, part (a) presents the original image, while part (b) depicts the output image obtained after the embedding process. Part (c) shows the histogram of the original image, and part (d) displays the histogram of the embedded image.



(a) Before Embedd

(b) After Embedding

(c) Histogram Original Image

(d) Histogram Embedded Image

Fig- 8 Jaar.bmp

Figure 8 presents the Jaar.bmp image. In this figure, part (a) displays the original image, while part (b) illustrates the output image resulting from the embedding process. Part (c) features the histogram of the original image, and part (d) showcases the histogram of the embedded image.

4. CONCLUSIONS

This paper primary aim of this research is to devise a method for securely embedding information within audio files without causing any perceptible changes post- insertion. Given the increasing importance of digital data security, various innovative techniques have been explored in recent studies. Audio steganography, in particular, focuses on safeguarding and preserving the integrity of sensitive information concealed within voice communications, especially during transmission over insecure channels. This thesis presents advanced techniques and methodologies for digital audio steganography tailored for cloud data security. The proposed approach effectively generates a stego audio file that incorporates and encrypts secret information using the Least Significant Bit (LSB) algorithm. The efficiency of this method is rigorously assessed through several metrics, with Peak Signal-to- Noise Ratio (PSNR) and Mean Squared Error (MSE) identified as the most reliable parameters for evaluating the quality of the stego audio. Experimental findings reveal that the PSNR values are notably high while MSE values are correspondingly low, indicating minimal alterations to the embedded audio. A higher PSNR value signifies that the embedded audio remains largely unaltered, enabling a significant volume of hidden information to be integrated seamlessly. The results confirm that the LSB technique is highly effective and particularly advantageous for embedding information in audio files, especially those with low color variation or monochrome characteristics.

6. REFERENCES

[1] S.K. Sahoo, Mohammed Arif, P. Das,“Improving Cloud Data Security With Watermarking In Cloud Computing”, 2023 IJCRT, Volume 11, Issue 5 May 2023, ISSN: 2320-2882.

[2] Neha Khajanchi, Prof. Vishakha Nagrale,” To Apply Watermarking Technique in Cloud Computing To Enhance Cloud Data Security”, Volume 4, Issue 7, July 2019 IJSDR.

[3] Amrit Anil; Vinod Kumar Shukla; Ved Prakash Mishra, “Enhancing Data Security Using Digital Watermarking”, ISBN:978-1-7281-4098-8,2020,IEEE, DOI: 10.1109/ICIEM48762.2020.9160090.

[4] Alaa Abdulsalam Alarood, “Improve The Efficiency For Embedding In Lsb Method Based Digital Image Watermarking”, August 2022. Vol.100. No 15, ISSN: 1992-8645, Journal of Theoretical and Applied Information Technology.

[5] Shakun Gupta , Harsimran Singh, "To Propose A Novel Technique for Watermarking In Cloud Computing", IJEDR - INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, Vol.3, Issue 2, page no.504-509, May2015,Available:https://rjwave.org/IJEDR/papers/IJEDR1502094.pdf.

[6] Padmini Devi B; Deepak S; Abimanyu N K; Harish Kumar S, “Review On Prevention of Data Leakage in Cloud Server by Utilizing Watermarking and Double Encryption Techniques”, ISSN: 2469-5556, 2023, IEEE, DOI: 10.1109/ICACCS57279.2023.10112767.

[7] Nagaram Ramesh, B. Nagaveni, P. Satyavathi, “An Efficient Technique to provide Security for Data Owners Cloud Computing”, ISSN: 2278-0181, Vol. 1 Issue 5, July – 2012, International Journal of Engineering Research & Technology (IJERT).

[8] Sarvesh Kumar, Surendra Kumar, Nikhil Ranjan, Shivam Tiwari, T. Rajesh Kumar, Dinesh Goyal, Gajanand Sharma, Varsha Arya, Marjan Kuchaki Rafsanjani, “Digital Watermarking-Based Cryptosystem for Cloud Resource Provisioning”, International Journal of Cloud Applications and Computing (IJCAC) 12(1), DOI: 10.4018/IJCAC.311033.

[9] Ching-Chun Chang; Chang-Tsun Li; Yun-Qing Shi, “Privacy-Aware Reversible Watermarking in Cloud Computing Environments”,IEEE Access (Volume:6), ISSN:2169-3536,2018,DOI: 10.1109/ACCESS.2018.2880904.

[10] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu, “Data Security and Privacy in Cloud Computing” Volume 10, Issue 7, July 2014, International Journal of Distributed Sensor Networks, DOI: https://doi.org/10.1155/2014/190903.

[11] Riya Naik; Manisha Naik Gaonkar, “Data Leakage Detection in cloud using Watermarking Technique”, ISBN:978-1-5386-8260-9, 2019, IEEE, DOI: 10.1109/ICCCI.2019.8821894.

[12] Ashwani Kumar, “A cloud-based buyer-seller watermarking protocol (CB-BSWP) using semi- trusted

third party for copy deterrence and privacy preserving", Volume 81, pages 21417–21448, (2022), Springer.

[13] Swati Singh & Sarita Soni, "Security of Data with 3DES & Watermarking Algorithm", Volume: 4 Issue: 1, ISSN: 2454-4248, 2018, International Journal on Future Revolution in Computer Science & Communication Engineering

[14] Samarth.K.N, Poornapragna.M.S, Sambhav Kumar.P.Jain, Nagarathna, "A Novel Technique Of Hiding An Audio Message In An Image", International Conference on Electronics and Communication Engineering, 28th April-2013, Bengaluru, ISBN: 978- 93-83060-04-7.

[15] Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade , "Image Steganography using Karhunen-Loève Transform and Least Bit Substitution", International Journal of Computer Applications ,Volume 79 – No9, October 2013, (0975– 8887).

[16] K.Sakthisudan, P.Prabhu and P.thangaraj, "Secure Audio Steganography for hiding Secret Information", International Conference on recent trends in Computational methods, Communication and Controls (ICON3C 2012).

[17] Pritam Kumari, Chetna Kumar, Preeyanshi and jaya Bhushan, " Data Security Using Image steganography And Weighing Its Techniques", International Journal Of Scientific & Technology Research, Volume 2,Issue 11,November 2013. ISSN 2277-8616

[18] Budda Lavanya, Yangala, Srinivasa Rao, " Data Hiding In Audio By Using Image Steganography Technique," International Journal Of Emerging Trends & Technology In Computer Science, Volume. 2, Issue 6, Nov-Dec 2013. ISSN: 2278-6856.