DATA HIDING USING AUDIO STEGANOGRAPHIC TECHNIQUES

[1]Ghule Isha Chetan, [2]Sonawane Dhanashri Hiraman, [3]Sakhala Siddhi Shashikiran,
[4]Khade Tejashree Tukaram, [5]Dahake Ranjana P.

Met Bhujbal Knowledge City
Adgoan, Nashik

Abstract- **Information security is crucial for ensuring secure communications in today's computer-based world. With the widespread use of the internet and multimedia, there is a growing interest in security approaches to protect digital data. Image steganography has gained significant attention as a means to secure and safeguard information. As computer-based communications continue to advance, the need forprotecting digital data extends to audio files as well. Audio steganography involves hiding secret information within audio files, allowing for covert communication andsecure transmission. In our proposed system, we are also implementing a feature that enables users to utilize audio steganography. Users can select an audio file, embed a secret message within it, specify the intended receiver for decryption, and enter a captcha key for authentication. The receiver can then use the provided key to decrypt the hidden message from the audio file, ensuring confidentiality and secure communication.**

Keywords: **image, audio, steganography, captcha, system.**

I.INTRODUCTION

The first recorded use of the term "steganography" was in 1499 by Johannes Tritheism in his treatise on cryptography and steganography called Steganographic. It was disguised asa book on magic. Steganography involves hiding secret messages within something else, such as images, articles, or shopping lists. For instance, invisible ink between visible lines of a private letter can carry hidden messages. Implementations of steganography without a shared secret rely on security through obscurity, while key dependent steganographic schemes follow Kirckhoffs's principle.

Unlike cryptography, which focuses on protecting the contents of a message, steganography conceals the fact that a secret message is being sent and its contents. Digitalsteganography involves concealing information within computer files, often using transport layers like document files, images, programs, or protocols. Media files are particularly suitable for steganographic transmission due to their large size. For example, an innocuous image file can be subtly modified by adjusting the color of specific pixels to represent letters in the alphabet, making it hard to detect without deliberate scrutiny.

Our proposed system aims to provide a scalable approach with potential for future featureexpansion. It offers a user-friendly interface for easy system usage. Users will be able to select an image, add a secret message, specify the receiver for decryption, and enter a captcha key. The receiver can then decrypt the secret message using the provided key.

In the context of data transfer over the internet, steganography plays a crucial role in securely hiding sensitive information within digital cover data. This helps prevent unauthorized access and misuse of valuable information through hacking.

The concept of audio steganography has evolved over time, with the term itself being relatively recent. It involves embedding hidden messages within audio files, making them imperceptible to the human ear. These hidden messages can be encoded within the audio data itself, such as modifying certain frequency components or altering the amplitude of specific samples. Audio files serve as an effective medium for steganographic transmission due to their larger size and complexity compared to text-based data. By utilizing imperceptible modifications to the audio signal, a sender can embed a secret message while maintaining the overall integrity and quality of the audio file.

II.LITERATURE SURVEY

The paper titled "Data Encryption & Decryption Using Steganography" by N. Manohar et al. [1] explores the application of video steganography for secure communication. The study reviews various methods proposed for video steganography and highlights the need for improved security, quality, and compatibility with different formats. The paper introduces new secure steganography methods, including the Secure Base LSB method, Neural Networks, and Fuzzy Logic. The proposed methods are evaluated using metrics such as PSNR (Peak Signal-to-Noise Ratio) and MSE (Mean Squared Error) based on a collected dataset from video streams. The results demonstrate enhanced security, quality, and accuracy compared to other existing methods.

The research paper titled "Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image" by Mehdi Sharifzadeh et al. [2] focuses on digital image steganography and the importance of statistical modeling for achieving better security and hiding data in less detectable regions. The paper addresses the limitations of existing approaches that rely on heuristically defined distortions and non-constrained message models, lacking closed-form expressions for security analysis. The authors develop a statistical framework for image steganography using a multivariate Gaussian model to represent the cover and steganography messages. They propose a novel Gaussian embedding model that maximizes the detection error of optimal detectors within the statistical model. Additionally, the formulation is extended to cost-based steganography, resulting in a universal embedding scheme that improves empirical results compared to current approaches. This methodology provides insights into the image steganography problem and enhances the performance of batch steganography algorithms by assuming a continuous hidden message.

The research paper titled "A Mobile Forensic Investigation into Steganography" by Catrin Burrows et al. [3] explores the use of steganography techniques to conceal data in mobile devices and the forensic investigation tools employed to detect and extract hidden content. With the increasing use of mobile devices in everyday life, they can accumulate significant amounts of information, which may serve as evidence in criminal investigations. The paper investigates various steganography techniques and their artifacts on Android and Apple platforms. Forensic investigation tools are utilized to detect and potentially reveal the concealed data. Additionally, the paper aims to develop guidelines and policies for mobile forensic investigations in relation to steganography.

In the paper titled "Directional Pixogram: A New Approach for Video Steganography" by Mohammed Baziyad et al. [4], a novel approach for video steganography is proposed, leveraging the temporal redundancy inherent in video signals. The video signal is represented as a 3D signal, where rows and columns represent the first and second dimensions, and time represents the third dimension. The proposed Directional Pixogram method optimally exploits the redundancy within a video segment. By utilizing the Discrete Cosine Transform (DCT), highly correlated pixels within the temporal vector are expressed through a few significant DCT coefficients, leaving a large number of insignificant coefficients. Experimental results demonstrate that the Directional Pixogram technique achieves outstanding stego quality while accommodating high hiding capacities.

The paper titled "A Novel Approach to Steganography Using Pixel-Based Algorithm in Image Hiding" by Jawwad A R. Kazi et al. [5] investigates a new algorithm for steganography that aims to hide data within image files to prevent unintentional access by unauthorized individuals. The proposed algorithm involves a cover image file and a message. Each pixel of the cover image is considered for embedding each bit of the secret text, continuing until the last bit of the secret text is embedded. This process hides the data beneath the image, which can then be transmitted to the recipient. The recipient employs a reverse process to retrieve the original text from the image. The paper presents this novel approach to fulfill the objectives of steganography, providing a method for secure data hiding within images.

In the paper titled "Audio Steganography Using Coefficient Comparison in the DCT Domain" by Jain and Trivedi,[6] a novel audio steganography method is introduced. The authors propose hiding secret data within the significant coefficients of the audio signal's Discrete Cosine Transform (DCT). By exploiting the perceptual characteristics of the human auditory system, the authors aim to achieve effective steganography. The performance of the proposed method is evaluated, and analysis is provided based on various metrics.

Santosa and Bao present an audio steganography scheme that involves the wavelet transform and an audio-to-image conversion process[7]. In their paper, the authors describe the transformation of the audio signal into an image representation using the wavelet transform. They then hide secret data within the resulting image. The steps of their approach are discussed, and the performance of the proposed method is analyzed through experimental results and comparisons.

In the paper[8] by Qi, Ye, and Liu, the focus is on audio steganalysis, which aims to detect hidden data in audio signals. The authors propose a steganalysis method specifically designed for detecting multiplicative embedding models in the wavelet domain. They investigate the statistical properties of audio signals and employ wavelet-based analysis to identify traces left by the steganography process. The authors present their findings and discuss the effectiveness of their steganalysis method in detecting multiplicative audio steganography techniques.

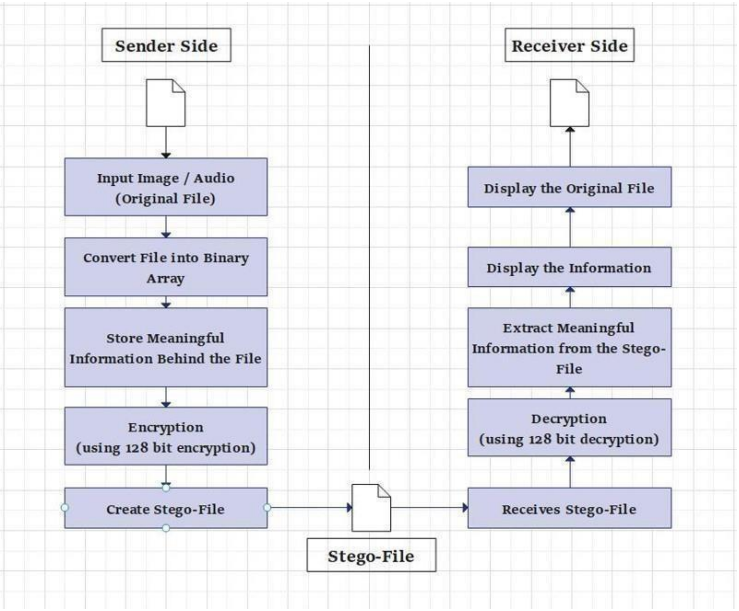
III.PROPOSED WORK

Implementation of data hiding and watermarking in digital images and raw data have wide literature. Data hiding in motion vectors at the encoder replaces the regular pair, due to tampering the motion vectors, to become, where the superscript denotes hiding.The message should survive the lossy compression and can be identically extracted.

Steganography hides the very existence of a message so that if successful it generally attracts no suspicion at all. Using steganography, information can be hidden in carrierssuch as images, audio files, text files, and data transmissions.

SYSTEM ARCITECTURE

Figure 1: System Architecture



METHODOLOGY

Data Encryption Standard (DES): DES stands for Data Encryption Standard. There are certain machines that can be used to crack the DES algorithm. The DES algorithm uses a key of 56-bit size. Using this key, the DES takes a block of 64-bit plain text as input and generates a block of 64-bit cipher text.The DES process has several steps involved in it, where each step is called a round. Depending upon the size of the key being used, the number of rounds varies.

LSB-Steganography: LSB-Steganography is a steganography technique in which we hide messages inside an image by replacing Least significant bit of image with the bits of message to be hidden. By modifying only the first most right bit of an image we can insert our secret message and it also make the picture unnoticeable, but if our message is too large it will start modifying the second right most bit and so on and an attacker can noticethe changes in picture.

LSB-STEGANOGRAPHY:

A. The embedding algorithm at the sender side:

Step (1) : Get the input cover image/audio and secret message.

Step (2) : Convert each character of secret message into its binary form.

Step (3) : Substitute the LSB bit of cover image with binary values of secret message withrespect to the starting point until the end of secret message.

Step (4) : Send a stego-file to the receiver.

B. The extracting algorithm at the receiver side:

Step (1) : Get the input stego file.

Step (2) : Extract each of LSB bit from the stego file until to find out the end bit.Step (3) : Reconstruct the collecting LSB bits from the stego file.

Step (4) : Transform the LSB bits to correspondent characters.Step (5) : Get the original data from stego file.

IV.RESULTS AND DISCUSSION

Audio and image steganography are two popular techniques for hiding secret informationwithin carrier files. An analysis of their performance reveals certain characteristics and considerations.

Audio Steganography:

Audio steganography involves embedding hidden messages within audio files. One advantage of audio steganography is the inconspicuous nature of audio files, which makesthem less likely to attract attention or scrutiny. However, audio files have limited data capacity compared to images due to their smaller size and perceptual limitations. This constraint makes it challenging to hide large amounts of data within audio files without noticeable degradation in audio quality. Robustness is also a concern as audio files are susceptible to lossy compression algorithms and other audio processing techniques, whichmay inadvertently alter or remove the hidden message.

Image Steganography:

Image steganography, on the other hand, offers a higher data capacity compared to audio steganography. Images typically have larger file sizes and more complex data structures, providing ample space for hiding secret information. The robustness of image steganography is generally higher as images can tolerate various transformations, such as resizing, cropping, or minor modifications to the pixel values, without significant loss or corruption of the hidden message. Additionally, image steganography benefits from the abundance of tools and techniques available for image processing and manipulation.[9]

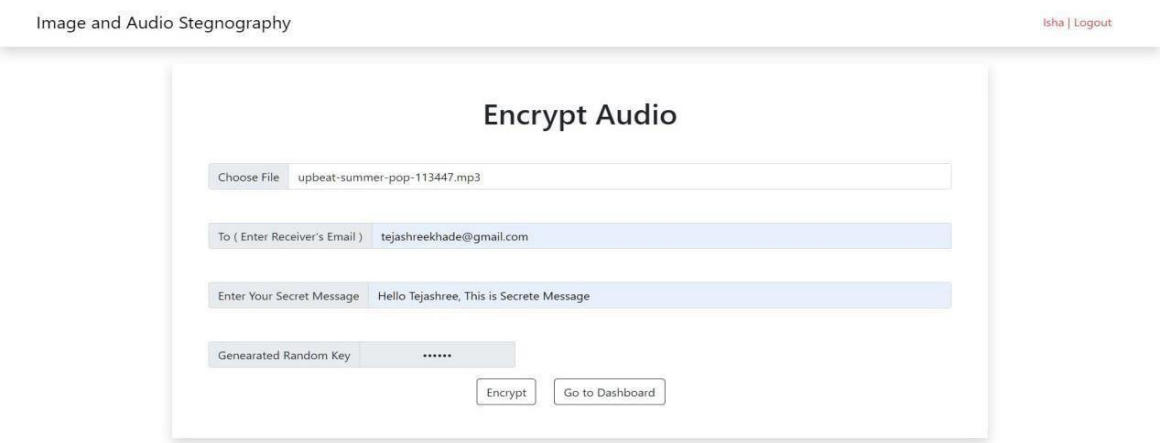


Figure 1: Encrypt Audio
In above figure we show the encryption of audio

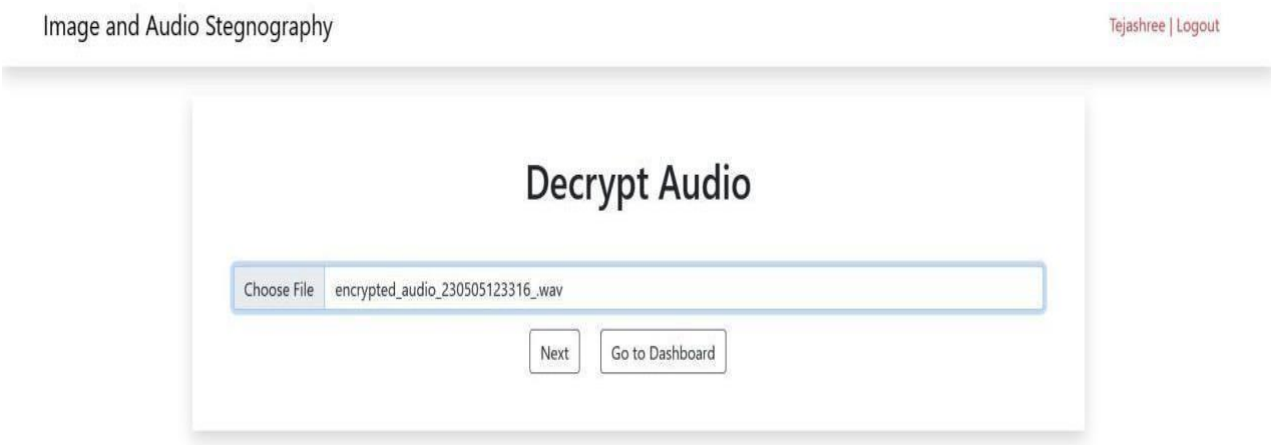


Figure 2: Decrypt Audio
In above figure we show the decryption of audio

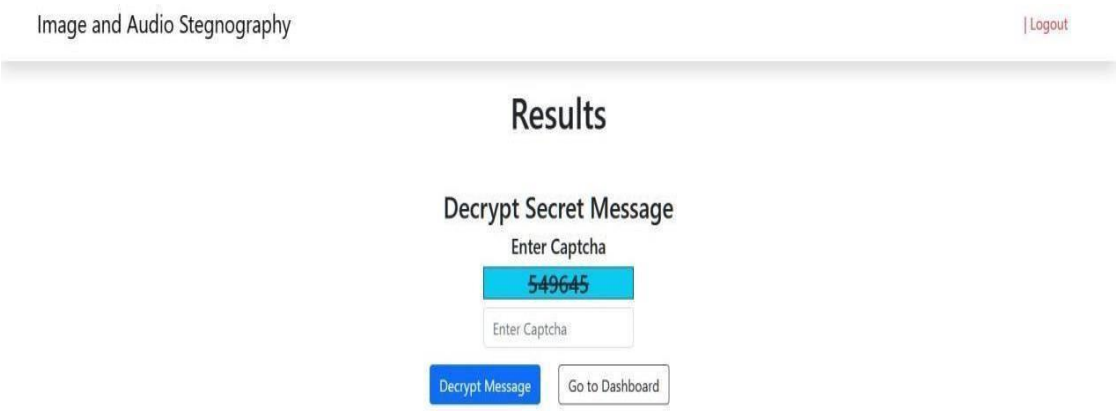


Figure 3: Decrypt secret message
Result of our proposed system

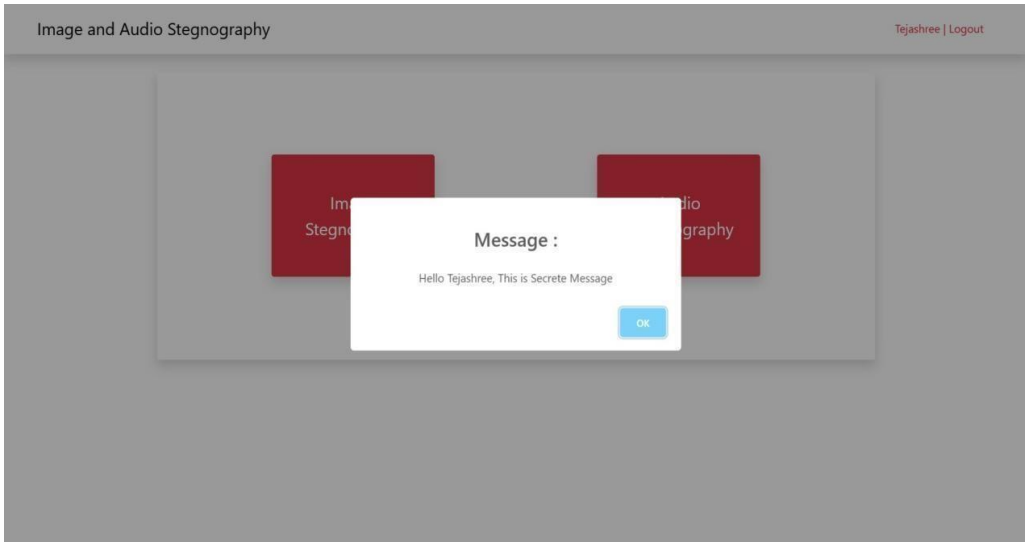


Figure 4: Original Message
Message retrieved

Sr.no	Text file Size	Word Count	Audio size Before Encryption	Audio size after Encryption
1	12kb	1	184kb	0.98MB
2	15kb	180	612kb	3.5MB
3	22.5kb	1472	2.13MB	11.7MB
4	30.8kb	3093	3.05MB	13.1MB
5	40.5kb	4278	5.16MB	15.78MB
6	49.8kb	5225	7.29MB	18.3MB
7	60.6kb	5570	7.50MB	19.5MB
8	72.2kb	6967	11.76MB	22.02MB
9	80.8kb	8022	13.05MB	25.2MB
10	90.8kb	9329	18.12MB	31.07MB

Figure 4: Analysis table of Audio Steganography

V.CONCLUSION

The implementation of the proposed system brings notable advancements to image and audio steganography. The new approach simplifies the implementation process for both image and audio steganography while maintaining a high level of security. Users can now easily embed sensitive information within images and audio files without compromising data integrity or raising suspicion. The efficiency of the new approach ensures that the hidden data remains effectively concealed and difficult for unauthorized parties to detect. With the developed application for testing and evaluation, the effectiveness and performance of the image and audio steganography techniques can be reliably validated. The advancements in image and audio steganography offer enhanced capabilities for covert communication, data protection, and privacy preservation. Overall, this integration provides a powerful toolset for safeguarding sensitive information in a wide range of applications.

VI.FUTURE SCOPE

In the future, image and audio steganography hold significant potential for advancement. We can expect the development of more advanced techniques with increased data capacityand improved robustness against attacks. Multi-media steganography may emerge, combining different media formats for versatile hiding mechanisms.

VII.REFERENCES:

1. N. Manohar; Peetla Vijay Kumar., Data Encryption & Decryption Using Steganography, 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS).
2. Mehdi Sharifzadeh., Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography, IEEE Transactions on Information Forensics and Security PP(99):1-1 DOI:10.1109/TIFS.2019.2929441.
3. Catrin Burrows; Pooneh Bagheri Zadeh, A mobile forensic investigation into steganography, 2016 International Conference On Cyber Security And Protection Of DigitalServices (Cyber Security).
4. Mohammed Baziyad; Tamer Rabie; Ibrahim Kamel, Directional Pixogram: A New Approach for Video Steganography, 2020 Advances in Science and Engineering TechnologyInternational Conferences (ASET).
5. Jawwad A R. Kazi, Gunjan N. Kiratka., A novel approach to Steganography using pixel- based algorithm in image hiding, 2020 International Conference on Computer Communication and Informatics (ICCCI).
6. Jain M.P., Trivedi P.V., Effective Audio Steganography by using Coefficient Comparison in DCT Domain, International Journal of Engineering Research & Technology 2(8) (2013).
7. Santosa R.A., Bao P., Audio-to-Image Wavelet Transform based Audio Steganography, 47th.
8. Qi Y.C., Ye L., Liu C.,\textit {Wavelet domain audio steganalysis for multiplicative embedding model}, International Conference on Wavelet Analysis and Pattern Recognition (2009), 429-432.
9. Ghule Isha Chetan, Sonawane Dhanashri Hiraman,Sakhala Siddhi Shashikiran, Khade Tejashree Tukaram, Dr. Dahake Ranjana,,(REVIEW ON DATA HIDING USING STEGANOGRAPHIC TECHNIQUES),(2023).