IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 10, May 2023

Image, Audio and Video Steganography

Dr. Murthy S V N[1], Gagana J P Reddy[2], Sharanya R[3], Shirisha S[4], Yashawini S[5]
Associate Professor, Department of CSE[1]
Engineering Students, Department of CSE[2,3,4,5]
SJC Institute of Technology Chikkaballapura, India

Abstract: *Steganography is defined as concealing a message inside another data format in a way that makes it undetectable, without committing plagiarism. Steganography is an advanced security technique which allows sensitive information to be concealed and transmitted without detection, making it difficult for an eavesdropper to detect the fundamental principle of steganography is ensuring that hidden message remains undetectable for the casual observer. The primary objective is to prevent unintended individuals from detecting the presence of the concealed message. It is essential that individuals who are not intended to receive the message are not even aware that a hidden message exists. Sometimes, images can hold concealed information that is not immediately evident to the casual observer. Although an image may appear ordinary at first sight, those with specialized knowledge can detect additional details. The objective of steganography is to enable secretive communication, and we have developed a methodology that involves creating a framework for hiding data that is ideal for steganography purposes. This technique is used to hide messages in images, audio, and video files. The data can be encrypted for security purposes, making it difficult for unauthorized users to access the hidden content. The data can also be compressed, making it possible to embed larger amounts of information without compromising the quality of the file. Steganography is covert method of interacting a text undetected in a embedded medium. Researchers have conducted significant work in data hiding methods for digital media, and experimentation in this field is still ongoing. Initially, the primary focus of steganography analysis was on the least significant bit embedding in bitmap and GIF images. This method was later expanded to include JPEG, audio, and video files, which are the most commonly used image formats. As time passed, numerous data hiding techniques and algorithms were created to further develop the field of steganography. This method of data hiding is more secure than other methods as it is more difficult to detect. It works by replacing the least significant bits in the file with data that is to be hidden, while preserving the overall look of the file. This makes it difficult to detect, as any changes to the file will be minor and difficult to spot. Audio and video steganography have gained widespread usage and acceptance among numerous users, and have become increasingly popular in recent times. The proposed system aims to enhance its robustness and security by utilizing audio and video steganography techniques, as outlined in this paper. Steganography is a technique used to conceal a confidential message within an image or audio file. It allows users to securely send and receive data without anyone else knowing that the data is there. By using audio and video steganography, users can be sure that their data is safe and secure, while also allowing them to send and receive large amounts of data without anyone being able to detect it.*

Keywords: Steganography

I. INTRODUCTION

Steganography commonly employs digital images as cover objects, owing to their widespread usage. Different applications require steganography algorithms that are tailored to specific file formats. As such, the algorithms used for concealing information in images, audio, and video files may vary. An image comprises a set of pixels or bytes, which can be manipulated to embed data in a manner that is not easily detectable, each with different levels of brightness or color intensity. In steganography, images with 8-bit and 24-bit per pixel file formats are commonly used to conceal data. These file formats enable the manipulation of individual pixels, allowing for the subtle modification of the image's appearance to embed a hidden message. but they have a limited color palette of only 256 possible colors. This

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 10, May 2023

constraint can pose a challenge during encoding. For 8-bit images, a grayscale color palette is typically used, such as the one found in (GIF), Steganography is often performed using 24-bit images because they offer a high degree of flexibility. The reason behind this is the vast array of colors available (more than 16 million), which goes beyond the limits of the Human Visual System (HVS). It makes it more challenging to detect a gradual change in color resulting from the encoding of a secret message in the image. In contrast, steganography using 8-bit images may be more easily detected since they have a smaller range of available colors.As a result, it is much harder to detect a secret message encoded within a 24-bit image.

Concealing confidential information within audio data is a complex process in the field of steganography. The primary reason behind this is the remarkable capacity of the Human Auditory System (HAS) to perceive a vast range of audio signals. For instance, The Human Auditory System (HAS) is renowned for its sensitivity, as it can detect power ranges that exceed one million to one and frequency ranges that exceed one thousand to one. These capabilities pose a significant challenge to anyone attempting to insert or extract information from the original audio data format without detection. without being detected. However, the only vulnerability of the HAS lies in distinguishing sounds, which can be exploited to encode secret messages in audio without arousing suspicion.- The conventional approach to audio steganography involves using block ciphers such as AES or Data Encryption Standard (DES) to ensure the security of the covert message, which is considered a standard security measure. However, encrypting long secret messages using block cipher may cause the encrypted message to become too lengthy to embed into the audio file, resulting in distortion of the original audio. To overcome this problem, it is advisable to use stream cipher for message encryption before embedding it into the audio file. Stream cipher offers variable length encryption, unlike block cipher which provides fixed length encryption, and is also faster. The primary goal of encrypting the message is to maintain its confidentiality and ensure that only authorized individuals with the secret key can retrieve the hidden message from the audio file.

Video steganography refers to the process of concealing confidential information in video files by embedding additional data into them. This technique involves generating an intermediate signal by combining the hidden message data with the content signal data. The intermediate signal is then utilized to encode the content data, which embeds the additional data, such as copy control data that prohibits unauthorized copying, and pseudo-random key data that maintains the encoding's confidentiality. Moreover, regulation data may be embedded in the content signal to facilitate the identification of the supplementary data in the embedded content signal. The encoding process is designed to withstand content degradation resulting from scaling, resampling, or other factors. Even in such situations, the supplementary data can still be retrieved from the degraded content.

II. LITERATURE SURVEY

[1] Novel Image Steganography Methodvia DCGANS

Title: Novel Image Steganography Methodvia DCGANS

Authors: Liang Wang et.al

Published: July 4, 2018

Description: In 2018, Liang Wang presented a new technique for image steganography which employed stego images generated by Deep Convolutional Generative Adversarial Networks, using secret information as input. This approach diverges from traditional methods of embedding secret information, as it establishes a functional connection between the secret information and stego images using CNNs. Wang also introduced a CNN model which was successful in extracting secret information from stego images. By utilizing this method, the imperceptibility of secret information was greatly improved, making it highly resilient against steganalysis and forensics algorithms.

Remarks: Our application of DCGANS in image steganography has revealed certain drawbacks associated with the model. For instance, the parameters of the DCGANS can oscillate, destabilize and fail to converge. However, these limitations can be overcome by developing more advanced neural networks with greater capabilities. Although our method does not achieve perfect recovery accuracy, this issue can be addressed by incorporating error-correction codes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 10, May 2023

[2] Mega Image Steganography Capacity with Deep Convolutional Network
Title: Mega Image Steganography Capacity with Deep Convolutional Network
Authors: Pin Wu et.al
Published: June 15, 2018 in Future Internet
Description: In 2018, Pin Wu proposed a novel approach based on deep learning for image steganography. Through their research, they demonstrated that conventional image steganography methods generally lack a sufficient payload capacity.
Remarks: The Steg Net approach, as proposed, establishes a complete mapping from the cover image and hidden image to the embedded image, and subsequently to the decoded image, creating an end-to-end process. This technique has exhibited superior performance in comparison to traditional methods, while still maintaining a high level of robustness.

[3] Hiding Data with Deep Networks
Title: Hiding Data with Deep Networks
Authors: Jiren Zhu et.al
Published: In European Conference on 26 July 2018
Description: Jiren Zhu presented a new framework in 2018 for concealing data in images that employs neural networks in an end-to-end training process. The approach offers greater flexibility by adjusting parameters or noise layers during training, which allows for a better trade-off between capacity, secrecy, and robustness to different types of noise. This technique demonstrated improved quantitative and qualitative performance compared to conventional data hiding methods. Additionally, the HIDDEN framework stands out as the first end-to-end method for robust watermarking utilizing neural networks.
Remarks: End-to-end techniques, such as Hidden, offer a fundamental advantage in robust data hiding by enabling the incorporation of new distortions directly into the training process, without the need for designing specialized algorithms. This allows the system to adapt to new types of distortions and maintain robustness, without requiring the creation of entirely new methods to handle each one.

[4] CNN-based Steganalys is has proven effective in detecting steganography.
Title: Convolutional Neural Network Steganalysis's Application to Steganography
Authors: Mehdi Sharif Zadeh et.al
Published: December 1, 2017 IEEE Visual Communications and Image Processing
Description: In 2017, Mehdi Sharif Zadeh put forward a spatial image steganography technique that surpasses the current cutting-edge algorithms in terms of specific payloads (0-0.62 bits per pixel).
The method involves computing pixel costs using a trained steganalysis convolutional neural network. An intriguing area for future research would be to explore more intricate embedding patterns than simply modifying the image pixel by pixel. This approach could aid in measuring embedding distortions and in compensating for classification.
Remarks: Research has demonstrated that this technique exhibits superior detection performance in identifying adaptive steganography utilizing the Discrete Cosine Transform (DCT) compared to the previous leading JPEG steganalysis method..

[5] Can Machine Learn Steganography?
Title: Can Machine Learn Steganography?
Authors: Han-Zhou Wu et.al
Published: June 16, 2016
Description: In 2016, Han-Zhou Wu published a paper focused on detecting covert communication through steganography. Researchers have recently made strides in steganalysis by leveraging deep convolutional neural networks (CNNs), which has achieved impressive detection rates. This suggests that deep neural network-based steganalysis has the potential to offer the best detection performance in the future. Given that artificial neural networks (ANNs) are capable of approximating highly complex functions from observations, it may also be possible to use ANNs for steganography.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 10, May 2023

Remarks: The development of steganography with artificial neural networks (ANNs) is worth paying attention to. If steganography using neural networks is extensively studied and produces excellent results, it could lead to a war between neural networks for steganography and steganalysis.

[6] Steganalysis of DCT-Embedding Based Adaptive Steganography and YASS
Title: Steganalysis of DCT-Embedding Based Adaptive Steganography and YASS
Authors: Qing Zhong Liu et.al
Published: September 29, 2011 at Association for Computing Machinery New York.
DescriptionIn 2017, Qing Zhong Liu proposed an improved approach to detect adaptive steganography in the DCT domain, relied on neighboring joint density. This represents a significant advancement over earlier DCT-embedding techniques. The authors proposed a unique approach to detect steganography in YASS. The approach involves comparing the joint density of neighboring blocks for all possible host blocks that could have been used for data embedding with the neighboring blocks that were not utilized for embedding.
Remarks: The technique utilizes support vector machine and logistic regression classifiers.

[7] Advanced Steganography for Hiding Data and Image using Audio-Video
Title: Advanced Steganography for Hiding Data and Image using Audio-Video
Authors: Ms. Madhuri R. Shende et.al
Published: IJRITCC January 2016
Description: Ms. Madhuri R. Shende et.al at 2016 in their paper proposed, Various techniques have been proposed for embedding information in different media types such as text, image, audio/video signals, and IP datagrams. However, these techniques have certain limitations. For instance, the stego media generated by existing multimedia steganography methods are vulnerable to attacks such as media formatting and compression. To address this issue, researchers are continuously exploring new and robust steganographic techniques. In this regard, they have proposed a framework that employs an audio-video approach to produce better stego files. This approach enhances data security by utilizing data hiding with the aid of computer forensic techniques. Furthermore, the method ensures error-free data recovery at the receiver end, making it a highly secure and reliable technique for information security.

[8] An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection
Title: An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection
Authors: Marwa M. Emam et.al
Published: IJACSA 2016
Description: Marwa M. Emam at 2016 proposed A novel steganographic method has been proposed, which offers high embedding capacity and PSNR (Peak Signal-to-Noise Ratio). This method also employs a Pseudo Random Number Generator (PRNG) to enhance the system's security.
Remarks: Empirical findings indicate that our proposed method is a highly effective steganographic approach that successfully fulfills the goals of a steganographic system.

[9] Image Steganography With LSB
Title: Image Steganography With LSB
Authors: Rahul Joshi et.al
Published: IJARCET January 1, 2013
Description: Rahul Joshi at 2013 in their paper proposed a method, The LSB method is a straightforward approach that is easy to implement. However, it has some notable drawbacks. For instance, a significant disadvantage of the LSB method is that a malicious user can manipulate the LSB of all image pixels, compromising the hidden data's security.
Remarks: Modifying the image quality even slightly, such as with a range of +1 at each pixel position, can lead to the destruction of the hidden message. Moreover, the LSB method is not immune to noise and compression techniques, making it vulnerable to potential attacks or information loss.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 10, May 2023

[10] Automatic Detection of Steganography

Title: Automatic Detection of Steganography

Authors: George Berg et.al

Published: IAAI 2006

Description: In 2006, George Berg and his colleagues conducted a study that demonstrated the effectiveness of machine learning and data mining (ML/DM) in developing automatic steganography attacks. The researchers employed both content-based (GIF) and compression-based (JPEG) image formats, and used a canvas representation to depict the media formats. They then proceeded to identify all the characteristics that were suitable for steganographic embedding, they were able to select a set of features such as value occurrence probabilities, unconditional and conditional entropies to improve the accuracy of the automatic steganography attacks. The results showed that ML/DM techniques were effective in distinguishing stego-files from clean ones.

Remarks: Machine learning and data mining techniques can be utilized to improve steganalysis methods. As steganography continues to advance, it is critical to have effective methods for detecting hidden messages, and ML/DM techniques offer a promising approach to achieve this.

III. PROPOSED SYSTEM

Proposed system allows both the sender and receiver to access the application in a two-way security method. The text is basically encrypted in the hits of an image or frames of audio/video being played. First, both user and receiver will open the application with a secret key which is known only to them. After activating the application with the secret key, the sender is able to encrypt a text file into image, audio or video. After encryption, an automatic OTP/code is generated and the encrypted image/audio/video along with the OTP/code is sent directly/automatically to a mail suggested by either sender or receiver. Now, the receiver downloads the encrypted image/audio/video and will have to provide the OTP/code generated. If he/she fails to do so, the hidden message cannot be decrypted and will not be received by the receiver. This automatic generation of encrypted image/audio/video to the mail suggested results in efficient usage of the application and also faster decryption of the confidential information so that threats from hackers, viruses can be avoided easily.

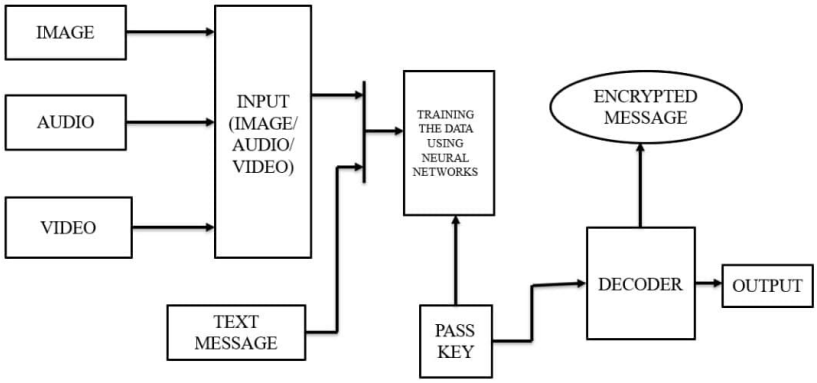

Figure 1 : Proposed Architecture

IV. METHODOLOGY

In essence, a methodology comprises a set of rules, procedures, techniques, practices, processes, and methods. In the realm of project management, methodologies are typically strict and specific, and consist of a sequence of steps and activities that correspond to each phase of a project's life cycle.User needs to run the application.Image Steganography with LSB Algorithm is done for image embedding process and message extraction.Audio Steganography with LSB Algorithm is done for encoding and decoding audio.Video Steganography with LSB Algorithm is done for encoding and decoding video.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 10, May 2023

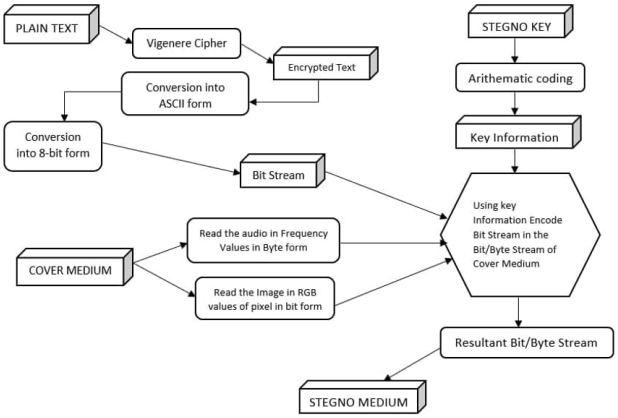

Figure 2 : Encoding

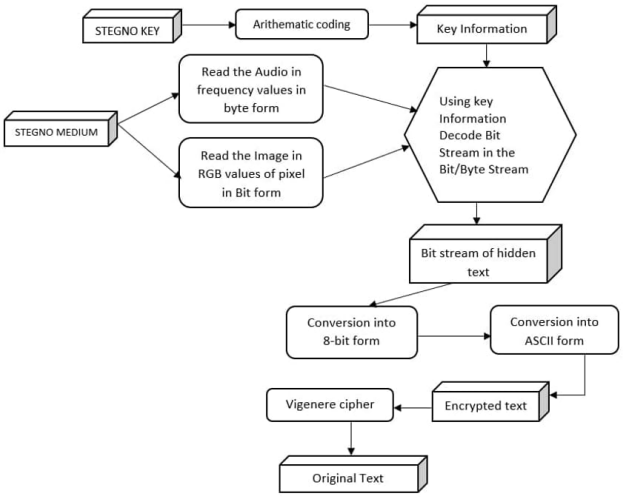

Figure 3 : Decoding

V. CONCLUSION AND SCOPE

Steganography refers to the technique of concealing the existence of information or communication in a manner that remains undetected.

This technique involves encoding confidential information in such a way that it remains hidden. Over the years, there has been a growing interest in using images as a cover for steganographic communication, and there are numerous tools available for image-based steganography. However, the detection of covert communications that use images has become an important issue.

This explores the fundamentals of steganography and steganalysis. Although there are few techniques developed in this field, steganography can be thought of as a modulation technique. Steganography is an important tool for communication that allows information to be hidden within digital media. While there are limitations to this technique, it remains an effective way of transmitting information in a covert manner. This algorithm is simple and has a negligible effect on the carrier image after embedding the text, making it difficult to detect tpresence of hidden messages.

The algorithm can be modified in several ways to enhance security and versatility. The PNG file format is primarily used as the carrier cover image, and the LSB algorithm can be easily changed to improve security.

A secret image/audio/video itself could be embedded in an image/audio/video or vice versa, the combination of any of the above provides higher levels of security can be implemented to ensure the protection of transmitted information. Larger sizes and run times of videos and audios could be used for encryption and decryption.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 10, May 2023

The same application could be subjected to machine learning where it could take a huge number of text, image, audio and video data to be trained and tested so that the sender could have a variety of options to choose from the above data to be encrypted and will be followed the same by the receiver.It could be used in In digital watermarking, it is crucial to maintain control over data ownership and integrity as it travels through various communication channels.It is observed that there exists a tradeoff between the properties of perceptibility, embedding capacity, and robustness in steganography. To improve steganography, new techniques must maintain high levels of all three properties. Some potential avenues for future research in steganography include investigating the potential of wavelet transforms to increase both embedding capacity and robustness. Additionally, utilizing Hamming or Matrix coding could help mitigate the impact of steganography and improve the PSNR. Another area of interest involves combining cryptography techniques like RSA, AES, and hash functions with steganography to enhance overall security..

REFERENCES

[1] Mehdi Sharif Zadeh,ChiragAgarwal,MohammedAloraini,DanSchonfeld,"ConvolutionalNeural Network Steganalysis's Application to Steganography", Volume 8, No. 9, November-December2017InternationalJournal of Advanced Research in Computer Science.

[2] Han-ZhouWu,Hong-Xia Wangand Yun-QingShi, "Can a Machine Learn Steganography?-Implementing LSB Substitution and Matrix Coding Steganography with Feed-Forward Neural Networks" in Proceedings of the2001 workshop on Multimedia and security:new challenges.

[3] Qingzhong Liu, "Steganalys is of DCT-Embedding Based Adaptive Steganography and YASS" ,IRENat. Conv. Rec, vol. 4, no. 142-163,

[4] Ms. Madhuri R. Shende, Prof. Amit Welekar, "Advanced Steganography for hiding data andimage using Audio and Video" in EURASIP journal on Information Security, vol. 2014, no. 1,pp.1-13, 2016.

[5] Liang Wang, Donghui Hu, Wenjie Jiang and Shuli Zheng, "Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks" in IEEE, vol.6, 4 July 2018.

[6] Pin Wu, Yang Yang and Xiaoqiang Li, "Mega Image Steganography Capacity with Deep Convolutional Network", in Future Internet, 15 June 2018.

[7] Jiren Zhu, Russell Kaplan, Justin Johnson and Li Fei-Fei, "HiDDeN: Hiding Data with Deep Networks", European Conference, 26 July 2016.

[8] Marwa M. Emam, Abdelmgeid A. Aly and Fatma A. Omara, "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection", International Journal of Advanced Computer Science and Applications, vol. 7, no. 3, 2016.

[9] Rahul Joshi, Lokesh Gagnani and Salony Pandey, "Image Steganography with LSB", International Journal of Advanced Research in Computer Engineering and Technology", volume 2, Issue 1, January 2013.

[10] George Berg, Ian Davidson, Ming-Yuan Duan and Goutam Paul, "Searching for Hidden Message: Automatic Detection of Steganography", American Association for Artificial Intelligence, 2006