Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 04, April-2023

A Survey on Different Image Steganography Techniques for Securely Transmitting the Data in IOT

Pooja S
Student of B.E
BNM Institute of Technology
Bengaluru

Sarvath Anjum
Student of B.E
BNM Institute of Technology
Bengaluru

Rashmi T V
Assistant Professor
BNM Institute of Technology
Bengaluru

Abstract: **Having information is the wealth of any organization, and in the digital age, when information is being transferred via the internet and digital media, this wealth is greatly enhanced and hence protecting this wealth is a top concern for any organisation. The most popular and effective methods for safe transmission are watermarking, steganography, and cryptography. This survey paper concentrates on the different image steganography techniques present today.**

Keywords: Watermarking, steganography, cryptography.

I. INTRODUCTION

This section includes a brief introduction about steganography and its different types like image, text, audio and video steganography. Steganography, which corresponds to "covered writing" or "hidden writing" comes from the Greek phrases stegos (cover) and grayfia (writing). Steganography is an approach for hiding secret information in a regular, non-confidential file or media for the sake of avoiding detection. As soon as this secret information reaches its final destination, it is extracted.

A. Image Steganography

In simple terms, image steganography as its name indicates hides the secret or confidential information in images. The image chosen for such a purpose is known as the "cover image," and the image produced through steganography is referred as the "stego image." The different terms for image steganography are as follows:

Cover-Image: A special image that can hide information.
Message: The secret data which is to be hided.
Stego image: It is a picture that has a secret message in it.
Stego-key: With the aid of a key, messages can be embedded in cover images and stego-images, or they can be inferred from the pictures themselves.

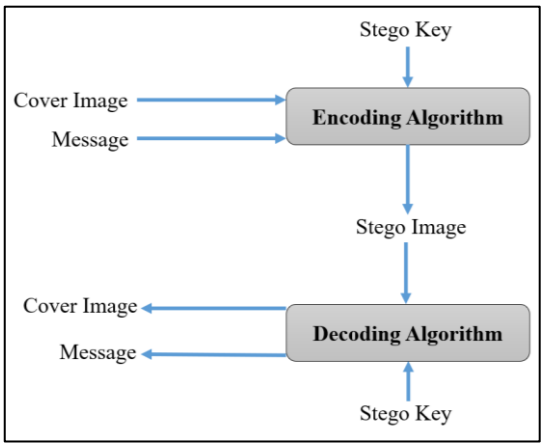

Figure 1: Image Steganography

Figure 1 shows the basic idea of implementing steganography using an image. Encryption and Decryption algorithms are needed for this purpose.

B. Text Steganography

Text steganography is a technique for concealing a secret text message as a covering message within another text or for making a cover message that is related to the original secret message. Text steganography can involve a variety of techniques, including formatting a text, word substitutions, the creation of random letter sequences and the use of context-free grammars to produce legible messages.

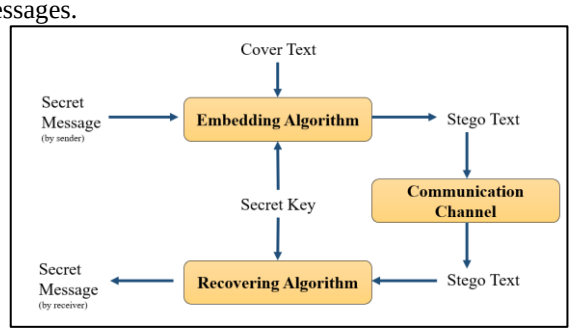

Figure 2: Text Steganography

Figure 2 shows the basic idea of implementing text steganography. Embedding and Recovering algorithms are needed for this purpose.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 04, April-2023

C. Video Steganography

With the help of the technique of video steganography, it is possible to hide any sort of important data or file inside a cover video clip. Because of its size and intricacy, video-based steganography may be more secure to use than other multimedia files.

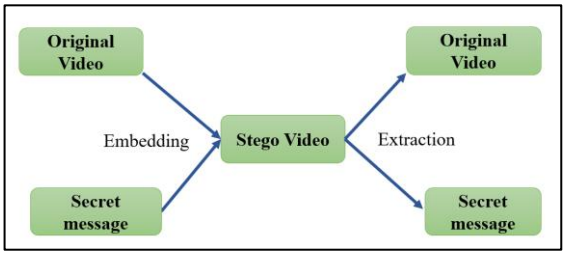

Figure 3: Video Steganography

Figure 3 shows the basic idea of implementing steganography using video file. Embedding and Extraction techniques are involved here.

D. Audio Steganography

A method to concealing information within an audio signal is called audio steganography. Data is altered as it is incorporated into the stream. This change should be rendered unnoticeable to the human perception.

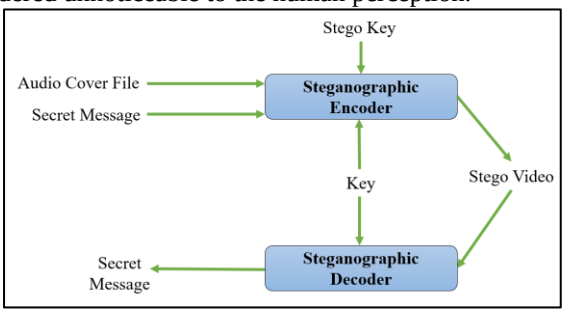

Figure 4: Audio Steganography

Figure 4 shows the basic idea of implementing steganography using an audio file. Steganographic encoder and decoder are involved here.

II. Methodologies used in Image Steganography

There are many Techniques and methodologies existing for implementing steganography using images in order to secretly send the information. This section describes some of the existing approaches for Image Steganography.

A. Executable Steganography for Digital Software Watermarking

Data can be concealed in executable files using a technique called executable steganography [1]. This method can be applied to digital software watermarking, which is the process of adding a distinctive identifier to a piece of software in order to identify the creator or copyright holder. Using the following criteria, it is possible to evaluate the security of image steganography for digital software watermarking.

Robustness: The watermarking method need to be able to resist the assaults like compression, cropping, scaling, or re-sampling and continue to function.

- Imperceptibility: The software application shouldn't function worse because of the watermark, which shouldn't be visible to end users.
- Security: The software program's functionality shouldn't be harmed if the watermark is challenging to remove or change.
- Complexity: The method shouldn't have a substantial impact on the software program's performance.
- Capacity: The method should be able to embed enough data to make the watermark distinctive and challenging to duplicate.

Ultimately, the degree to which the watermarking technique satisfies these criteria will determine how secure executable steganography for digital software watermarking will be.

B. Robust Steganography with Repetitive JPEG Compression

Robust steganography [2] refers to methods that can withstand steganalysis and keep the hidden information secret even when the media is attacked or modified. Repeated JPEG compression, when an image is repeatedly compressed and decompressed using the JPEG compression technique, is a frequent tactic used against steganography. This assault has the potential to reduce the image's quality and introduce artefacts that could make hidden information visible. Features collected from the photos, such as colour histograms, wavelet coefficients, or texture features, etc. are used in the machine learning algorithms. These properties have to be resistant to JPEG compression and able to record the minute alterations brought on by steganography. Overall, a strong dataset of normal and stego images that can be utilised for training and testing, as well as a combination of machine learning algorithms and other methodologies, are needed for an efficient steganalysis for robust steganography with recurrent JPEG compression. Several methods can be employed for steganalysis besides machine learning algorithms, such as statistical analysis of the image's histogram, study of the noise patterns in the image, or investigation of the image's LSB (Least Significant Bit) plane. Overall, a strong dataset of normal and stego images that can be utilised for training and testing, as well as a combination of machine learning algorithms and other methodologies, are needed for an efficient steganalysis for robust steganography with recurrent JPEG compression.

C. High Capacity, Transparent and Secure Audio Steganography using Binary Message Size Encoding

When secret messages need to be inserted into audio recordings without affecting their perceptual quality, the Least Significant Bit (LSB) algorithm is frequently utilised [3]. The LSB algorithm, however, has a limited capacity and is susceptible to steganalysis approach detection. This approach is a novel method for improving the LSB algorithm as it involves encoding the length of the secret message in binary format and embedding it in the LSBs of the audio samples prior to embedding the actual secret message.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 04, April-2023

This strategy offers the following benefits:
High capacity: The capacity of the LSB algorithm can be greatly improved by applying binary message size encoding.
Transparency: Binary message size encoding makes sure that the audio file's perceived quality is maintained.
Security: The secret message has an additional degree of security thanks to binary message size encoding.
The following stages are involved in embedding a secret message using binary message size encoding:

- Put the secret message's length in binary format.
- Include the LSBs of the audio samples with the binary message size embedded.
- Include the covert message into the last few LSBs of the audio samples.
- The LSBs of the audio samples can be utilised to determine the binary message size using the key.
- The required secret data can be extracted from the leftover LSBs of the audio samples after the binary message size has been determined.

In conclusion, the LSB technique combined with binary message size encoding can considerably expand the capacity of audio steganography while maintaining security and transparency.

D. Coverless Image Steganography by using Morphed Face Recognition Technique based on Convolutional Neural Networks

The method of concealing information in an image without changing its visual appearance is known as coverless image steganography [4]. Convolutional neural networks (CNNs)-based morphed face recognition can be used for coverless image steganography. A deep learning neural network called a CNN can spot patterns in photos. They are commonly employed in tasks involving picture recognition and categorization. A CNN is trained to recognise faces that have been warped or otherwise manipulated in morphed face recognition. By concealing information within the altered faces, this can be utilised to produce a coverless steganography approach.
The following processes are involved in employing morphing face recognition for steganography:

- Choose a photo to serve as the cover photo. Create a transformed version of the image using a morphing algorithm.
- Employ a pre-trained CNN to identify the image's altered faces.
- Incorporate the confidential information into the morphing faces.
- The final image should be saved as a stego image.

This method can offer a high level of security for concealing information within images because the cover image's visual look is left untouched, making it challenging for a viewer to notice that information is being concealed within the image. However, the strength of the morphing algorithm and the resilience of the CNN utilised for recognition will determine how well the strategy works.

E. IoT related Intelligent Hybrid Optimisation Algorithms

Based on an adaptive embedding procedure, this methodology proposes an image steganography technique which is secured as well [5]. To increase the security of the concealed images, the hidden image is first encrypted using a bit-level image encryption technique. Additionally, an optimization algorithm called Salp Swarm which is based on an adaptive embedding method is used to embed the encrypted data into the cover picture. By providing the smooth and edge blocks with the best parameter values, this procedure effectively embeds the secret data. To improve the stego image clarity, a backpropagation learning algorithm in a hybrid neural network is used. Then, these stego images are sent to the destination by using the IoT's extremely secure protocol. This is run with various secret and cover images to make sure that the stego-picture produced is free from noise or loss of information. The limitation of this approach is that it involves complex calculations and mathematical functions.

F. Evolutionary multi-objective optimisation (EMOsteg)-based image steganography

A high-pass filter bank-based technique for image pre-processing is suggested [6]. The probable sites of the disturbance are created by combining the filter residuals after the cover picture has been pre-processed with a range of directional and non-directional high-pass filters. Under certain embedded capacity limitations, perturbation spots on the cover picture were iteratively explored using the artificial immunity principle to guarantee image quality and resist steganalysis tools. This technique meets the real-time and bandwidth needs of IOT. By minimising imperceptibility and maximising security, EMOsteg formally specifies the multi-objective optimisation problem with embedded capacity as the constraint condition. Because it relies on mobile edge computing, EMOsteg is excellent for hidden communication in IoT environments. The mobile terminal is used to embed the secret according to the perturbation, and the IoT edge server with high computational capacity creates the ideal perturbation as part of the implementation of EMOsteg in the IoT environment. This method's drawback is that it makes use of complicated serialise and perturbation functions.

G. Data Hiding for Security Applications using LSB algorithm

In this technique [7], Data is first concealed within an image, which is then concealed within an audio recording. The Least Significant Bit (LSB) algorithm is used for data hiding in images and picture hiding in audio. Binary values of the data are hidden in various places on the last three bits in order to avoid security threats and give the data maximum security. AIFF or WAV audio files are acceptable choices for the audio recording.
Following are the actions being taken at the sender's end:
• Text, images, or audio files can all contain secret info.
• The carrier or cover could be an image or music.
• Both the carrier and the secret data are converted to binary numbers.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 04, April-2023

• An LSB of carrier can be used to substitute the secret data's binary values.
• The stegno image and sounds are now acquired.
Following are the actions that are being taken on the recipient side:
• The recipient should be aware of the size of the secretly embedded data.
• Stegno image / audio can be used to retrieve the source data.
• The secret data can be successfully recovered by extending the LSB of a stegno image or audio up to the extent of the secret data.
The drawbacks of this strategy include the complexity of using both picture and audio steganography, as well as the requirement that the receiver be aware of the length of the secretly encoded data.

H. 3D Image Steganography using a hybrid approach

This method [8] employs a hybrid algorithm for secure information sharing across numerous applications, including medical, military, and others. Three-dimensional (3D) geometric models are becoming an increasingly important component of mixed media output these days. The outcomes of academic research in the area of PC designs are substantial. A 3D picture is necessary for the proposed 3D image steganography framework as a cover file for secret parallel communication. The two main steganography processes are the implanting and extraction methodologies. The peculiarity of the suggested steganography calculation is that it uses both encoding and encryption to enable the secure transfer of data over a wide variety of applications, including medical, military, and so forth. Without compromising the visual quality or geometrical features of the cover image, up to 256 bits of obscure information can be utilized for creating consecutive or irregular patterns. A substantial fraction of geometrical attacks are defended against by the installed mysterious data. This method has some drawbacks, including 3D image steganography's lower capacity and higher error rate.

III. CONCLUSION

This paper will provide details about the Steganography and its types i.e., Image, Video, Audio and Text Steganography Techniques. It describes the various already existing techniques used in for image steganography.

REFERENCES

[1] J. A. Mullins, J. T. McDonald, W. R. Mahoney and T. R. Andel, "Evaluating Security of Executable Steganography for Digital Software Watermarking," SoutheastCon 2022, 2022, pp. 666-673, doi: 10.1109/SoutheastCon48659.2022.9763988.
[2] J. Feng, Y. Wang, K. Chen, W. Zhang and N. Yu, "An Effective Steganalysis for Robust Steganography with Repetitive JPEG Compression," ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2022, pp. 3084-3088, doi: 10.1109/ICASSP43922.2022.9747061.
[3] M. M. Mahmoud and H. T. Elshoush, "Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio Steganography–An Innovative Approach," in IEEE Access, vol. 10, pp. 29954-29971, 2022, doi:10.1109/ACCESS.2022.3155146.
[4] Li, YH., Chang, CC., Su, GD. et al. Coverless image steganography using morphed face recognition based on convolutional neural network. J Wireless Com Network 2022, 28 (2022), doi: org/10.1186/s13638-022-02107-5
[5] S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana and S. K. Pani, "SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT," in IEEE Access, vol. 9, pp. 87563-87578, 2021, doi: 10.1109/ACCESS.2021.3089357.
[6] X. Ding, Y. Xie, P. Li, M. Cui and J. Chen, "Image Steganography Based on Artificial Immune in Mobile Edge Computing With Internet of Things," in IEEE Access, vol. 8, pp. 136186-136197, 2020, doi: 10.1109/ACCESS.2020.3010513.
[7] G. Ramya, P. P. Janarthanan and D. Mohanapriya, "Steganography Based Data Hiding for Security Applications," 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW), 2018, pp. 131-135, doi: 10.1109/I2C2SW45816.2018.8997153.
[8] A. Ara and D. Gianchandani, "A Hybrid Approach Based 3d Image Steganography Instead of 2d Image for Exchange Information," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018, pp. 244-248, doi: 10.1109/CESYS.2018.8723892.