IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, 2023

SECURE DATA HIDING IN DIGITAL MEDIA USING HYBRID STEGANOGRAPHY TECHNIQUES

[1]Dr.A. Avani,[2]T. Bharath Krishna
[1]Associate Professor, Department of Computer Science and Engineering
Anubose Institute of Technology, New Palvoncha-507115,
Bhadradri Kothagudem-Dist-TG
[2]Department of Computer Science and Engineering
Anubose Institute of Technology, New Palvoncha-507115,
Bhadradri Kothagudem-Dist-TG

ABSTRACT

Cybercrime has become a dangerous threat to all the technical users and layman. Due to lack of skill on using the secured means in the data communication, many users as well as organizations are suffering. Steganography offers an approach to address this issue by providing an efficient method to secure data communication. Steganography is the practice of hiding a message or information within another message or object, with the goal of concealing its existence. It is a form of security through obscurity, where the message is kept secret by not drawing attention to its presence. The motivation behind steganography is to provide a way for people to communicate and share information in a way that is secure, private, and undetectable to anyone who does not have the proper tools and knowledge to uncover the hidden message. However, traditional steganography software can be inefficient and vulnerable to detection. The objective of this project is to overcome the limitations of traditional steganography software by developing an advanced and efficient steganography system. This system aims to address the vulnerabilities and weaknesses of traditional steganography software and provide improved security for data communication. The proposed two-layered approach combines the Least Significant Bit algorithm and Hybrid AES-RSA encryption techniques. The secret message is first encrypted using AES symmetric key and then embedded in the LSB of cover media. This approach ensures that the information is well-hidden within digital content, while encryption provides an additional layer of protection to prevent unauthorized access. Our proposed method *Hybrid AES-RSA Encrypted LSB* achieves an *SSIM* (Structural Similarity Index Measure) index of 0.9999 for images, 0.9773 for videos, and an *RMS* (Root Mean Square) value of 0.000178 for audio files. The achieved accuracy is 97%, which is 13.25% higher than traditional LSB. These metrics demonstrate that the processed images, videos, and audio files closely resemble their originals.

I.INTRODUCTION

In today's interconnected world, where the exchange of information occurs at an unprecedented scale, the need for secure communication has become paramount. While encryption and cryptographic methods provide a robust means to protect the content of messages, they often fail to address the issue of detection. This is where steganography comes into play. Steganography is an ancient art that has seamlessly transitioned into the digital age. It involves concealing sensitive or secret information within innocent-looking digital media such as images, audio recordings, videos, or even text documents, making it virtually undetectable to unintended recipients. In the digital era, steganography has evolved to leverage the vast capacities and complexity of digital media formats. Digital files are composed of binary data, consisting of sequences of 0s and 1s. Steganographic techniques leverage the ability to subtly modify binary data in a way that doesn't noticeably affect the visible characteristics of the carrier media. This is achieved by skillfully manipulating the least significant bits and taking advantage of unused parts of a file. To extract the hidden information, the recipient must possess the knowledge of the steganographic method employed. This typically involves using specialized software or algorithms that reverse the process and reveal the concealed data. The primary aim of this project is to develop a reliable and secure solution for data communication by combining the approaches of encryption and the traditional LSB steganography algorithm. By integrating these two techniques, the project aims to overcome the limitations of traditional steganography software and enhance the security of hidden data.

II.LITERATURE SURVEY

A Secure Video Steganography with Encryption Based on LSB Technique ,The proposed video steganography method aims to hide a secret video stream within a cover video stream by combining cryptography and steganography techniques. The methodology involves several steps to ensure the security and seamless integration of the hidden information. Firstly, symmetric encryption is employed to protect the secret video stream. Each frame of the secret video is converted into 8-bit binary values and encrypted using the XOR operation with a secret key. This encryption process ensures that the hidden data remains confidential and inaccessible to unauthorized parties. Next, sequential encoding is applied to embed the encrypted frames into the cover video stream. The sequential encoding technique follows a predetermined pattern, where each bit of the secret frames is stored in the least significant bit (LSB) of the corresponding cover frames. This process is performed sequentially for each frame of both the secret and cover video streams, ensuring the hidden data is distributed throughout the entire video. The resulting stego video stream is generated by combining the cover frames with the encoded secret frames. Each frame of the stego video contains both the original cover information and the hidden encrypted data, making it visually indistinguishable from the original cover video. The sequential encoding technique guarantees that the hidden information is imperceptible to human observers, as the small changes in the LSBs are generally undetectable. To decode the hidden information, the reverse process is performed. The frames of the stego video are extracted, and sequential decoding is applied.

III.PROBLEM DEFINITION

While encryption is a powerful tool for securing data, it may draw attention from potential attackers due to the nature of encrypted communications. Encrypted messages can act as indicators that sensitive information is being transmitted, potentially making them a target for attackers. Additionally, decryption keys or passwords associated with encryption can be vulnerable to interception or bruteforce attacks. Steganography, on the other hand, provides a way to conceal information within seemingly innocuous carriers, such as images, audio files, or text documents. By embedding the secret data in these carriers, steganography ensures that the existence of the hidden information remains undetectable to unauthorized individuals. This covert communication technique allows sensitive data to be transmitted without raising suspicion or attracting attention. Steganography offers several advantages over traditional encryption methods. It provides an additional layer of security by hiding the data in plain sight, making it difficult for unauthorized users or attackers to even recognize that hidden information is present. As a result, steganography can be an effective method for covert communication, ensuring that sensitive data remains confidential and protected from unauthorized access. But the traditional steganography software has various limitations such as Vulnerability to Detection, Fragility of Hidden Data, Lack of Encryption and performance. This project aims to overcome this by using steganography in conjunction with encryption to provide enhanced security. By combining steganography with encryption, sensitive information can be

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, 2023

both concealed and encrypted, providing a more robust and layered approach to data protection.

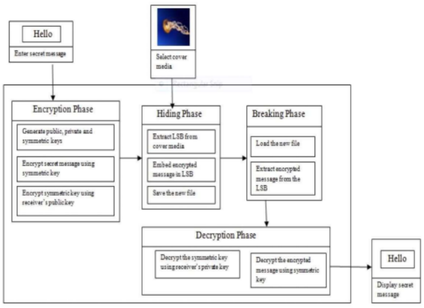
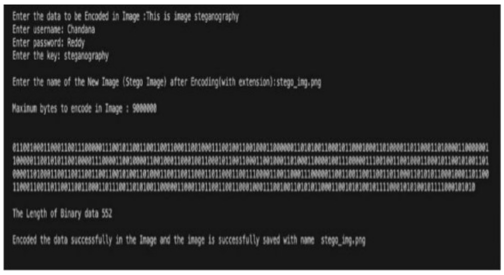
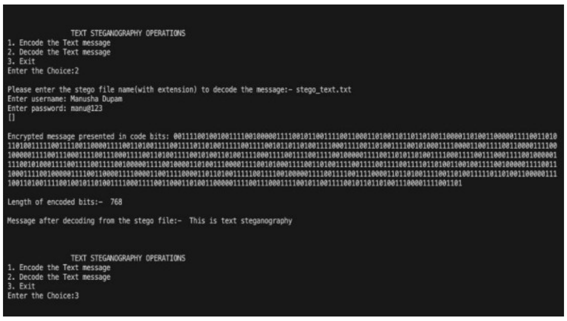


Fig.1 :System Architecture

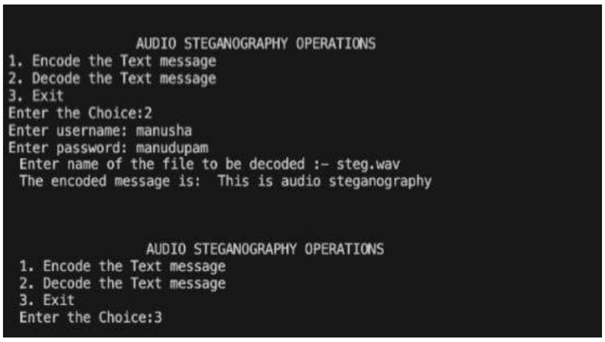
IV.RESULTS



SSIM stands for "Structural Similarity Index." It is a metric used to measure the similarity between two images. The SSIM index compares three aspects of the images being compared: Luminance, Contrast and Structure. For the above two images, the Similarity index is 0.9999984079358767.



Decoding from text file Levenshtein distance, also known as edit distance, is a measure of similarity between two strings. It quantifies the minimum number of single-character edits (insertions, deletions, or substitutions) required to transform one string into another. For the cover text file and generate stego file the levenshtein distance is 0.



Decoding from audio file RMS (Root Mean Square) noise level in audio files measures the average power of the noise present in the audio signal. When comparing audio files for noise levels, you should ensure that the two files are of the same audio format. The noise level in cover file and new stego file is 0.00017853177604225116.

Results Interpretation :

ISSN 2347–3657

Volume 11, Issue 4, 2023

Accuracy	Text	Image	Audio	Video
Traditional LSB	90%-95%	80%-85%	70%-75%	75%-80%
AES-RSA encrypted hybrid LSB	95%-99%	96%-99%	90%-95%	90%-95%

Fig.2:Result of Simulations

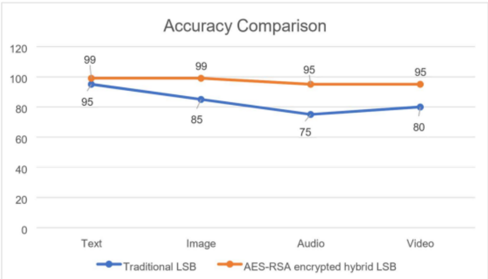


Fig.3:Accuracy Comparison

The figure 3 and table 4 compares the accuracy percentages achieved by traditional LSB and our proposed methodology. For Text data, the AES-RSA encrypted hybrid LSB method achieves an accuracy improvement of 5% to 9% compared to Traditional LSB. Similarly, for Image data, the improvement is even more significant, with hybrid approach showing an accuracy boost of 16% to 19% over Traditional LSB. The Audio data also benefits from the hybrid approach, as it outperforms Traditional LSB with an accuracy gain of 15% to 20%. There is a substantial difference of 10% to 15% in accuracy between the two techniques for Video data. The increase in accuracy for the AES-RSA encrypted hybrid LSB technique can be attributed to the use of encryption and a hybrid approach. In Traditional LSB data hiding, information is embedded directly into the least significant bits of the pixel values, which can be vulnerable to detection and extraction by unauthorized users. It is a basic and straightforward technique, but it may not provide robust security. On the other hand, the AES-RSA encrypted hybrid LSB technique employs both encryption and LSB data hiding. AES and RSA are wellknown encryption algorithms that provide strong security for the data being hidden. The use of encryption ensures that the hidden data remains confidential and secure, making it harder for unauthorized users to detect or extract the hidden information. In conclusion, AESRSA encrypted hybrid LSB proves to be a superior choice for data hiding, offering notably higher accuracy across various digital media types.

Comparison Between Traditional LSB and AES-RSA Encrypted Hybrid LSB :

In Traditional LSB data hiding, information is embedded directly into the least significant bits of the pixel values, which can be vulnerable to detection and extraction by unauthorized users. On the other hand, the AES-RSA encrypted hybrid LSB technique employs both

ISSN 2347–3657

Volume 11, Issue 4, 2023

encryption and LSB data hiding. AES and RSA are wellknown encryption algorithms that provide strong security for the data being hidden.

V.CONCLUSION

Steganography is a powerful tool to secure data hiding and can be applied in various contexts. This project highlights the importance of steganography in ensuring the confidentiality and integrity of sensitive data. By embedding secret information within innocuous-looking digital media such as images, audio files, or videos, it is possible to conceal the existence of hidden data from unauthorized individuals. This technique can be particularly useful in scenarios where encryption alone may draw unwanted attention or suspicion. This project is a success over making a fusion of old tradition of steganography with new technologies to create a safe and secure tool to hide sensitive information under an innocent looking cover file to increase the security of confidential messages across a network. The scope of this project is to include all significant current security efforts and the old tradition of handling confidential messages to create a tool that may allow users to secure their confidential messages.

VI.FUTURE SCOPE

This project currently deals only with hiding text data in other multimedia formats such as image, audio and video. There is also a limit on the data that can be hidden in the cover media depending on its size. The future work on this project is to hide all formats of secret messages in the cover media and increase the amount of data that can hidden in the media using compression.

VII.REFERENCES

[1]E. Abdelfattah, R. J. Mstafa, and K. M. Elleithy, "A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC," IEEE Access, vol. 5, pp. 5354-5365, 2017.

[2]G. Fu, H. Shi, S. Wang, X.-Y. Zhang, and J. Tang, "Synchronized detection and recovery of steganographic messages with adversarial learning," Proc. Int. Conf. Comput. Sci, pp. 31-43, 2019.

[3]G. Gujral, S. Gupta, and N. Aggarwal, "Enhanced least significant bit algorithm for image steganography," Proc. Int. J. Comput. Eng. Manage., vol. 15, no. 4, pp. 40-42, 2012.

[4]I. Aljazaery, and M. Aziz, "Combination of hiding and encryption for data security," hj,hk., vol. 10, no. 15, pp. 10-20, 2020.

[5] Khare, P., Singh, J. and Tiwari, "Digital Image Steganography", Journal of Engineering and Studies , Vol. II, Issue III, pp. 101-104, 2011.

[6]K. Ibrahim Mohammad Abuzanouneh and M. Hadwan 'Multi-Stage Protection using Pixel Selection Technique for Enhancing Steganography', International Journal of Communication Networks and Information Security (IJCNIS), 2021

[7]Laskar, S.A. and Hemachandran, "An Analysis of Steganography and Steganalysis Techniques", Assam University Journal of Science and Technology, Vol.9, No.II, pp.83- 103, 2012.

[8]M. H. Abd, "Dynamic Data Replication for Higher Availability and Security," Journal of Computer and Mathematics Sciences, pp. 31-42, 2021. N. F. Hordri, S. S. Yuhaniz, and S. M. Shamsuddin, "Deep learning and its applications: A review," Proc. Conf.