SECURED DATA TRANSFER WITH ADVANCED ENCRYPTION DECRYPTION PROCEDURE

[1]Shwetha N, [2]Bhumika M, [3]Harshitha F
[1]Professor, [2,3]Students
Department of CSE
East West Institute of Technology
Bengaluru, India

***Abstract*—The increased use of digital media has prompted substantial concerns regarding its weaknesses in security. Instances of security breaches, such as eavesdropping, camouflage, and manipulation in various forms, have become quite common. Digital steganography specifically focuses on concealing information within digital file formats.**

Steganography refers to a method used to hide information within an everyday file to avoid detection. It involves both encrypting and decrypting processes, where the private data or image meant for transfer is concealed within a cover file, resulting in an encrypted result called a stego object.

Keywords - Video Steganography, Advanced Encrypted Standard(AES), Least Significant Bit(LSB), secret message, cover video, video frames, steganalysis, stego video.

I. INTRODUCTION

In contemporary times, the internet has been a primary conduit for information exchange, encompassing activities like online shopping, rail reservations, money transfers, and payments. However, safeguarding information from unauthorized interception is crucial. Steganography serves as a technique to address this issue by minimizing the risk of interception. The primary objective behind employing steganography is to uphold privacy and prevent unorganized access to information.

While not a novel concept, steganography has been in use for millennia. It enables covert communication between two or more individuals by concealing secret messages within various media covers, such as text, audio, images, or digital video formats. This technique involves embedding the secret message within the media cover using specific algorithms and necessitates sending the stego file itself to the intended recipient.

Certainly, before delving into or applying steganography, several crucial considerations should be thoroughly addressed:

a. Embedding Capacity: The process involves embedding data within a larger file referred to as the cover or carrier file. These carriers usually consist of digital files such as images, audio, video, or text files, preserving their original quality. The embedding capacity denotes the amount of data that could be hidden or inserted into the cover file without compromising its quality. This capacity is evaluated concerning the space of the cover file. When the data size intended for insertion surpasses the cover's capacity, steganography cannot be effectively executed.

b. Undetectability: It's crucial that the process of hiding or embedding data within a carrier file ensures that any secret message or information remains completely imperceptible in the original file to anyone who might access it. If the hidden message is detectable by anyone examining the original file without the knowledge of its presence, then the steganography process is considered unsuccessful or compromised. Maintaining the concealment of the embedded data is essential for the effective of steganography.

c. Robustness: Robustness pertains to the embedding algorithm's ability to preserve the hidden or implanted data even after undergoing procedures like file compression and decompression. A robust steganographic method guarantees that the embedded information stays undisturbed and recoverable despite potential changes or modifications applied to the carrier file.

d. Security: In steganography, Security the primarily focuses on guaranteeing the seamless concealment of concealed data within diverse formats. The primary goal is to hide confidential data in the way that remains undetectable to unauthorized individuals, ensuring that solely the designated sender and recipient possess knowledge of the embedded information. Steganographic security encompasses preventing unorganized access and preserving confidentiality between the communicating parties.

e. Tamper Resistance: This concept emphasizes the ability to withstand intentional manipulation or sabotage of a product or system by individuals who have access to it. For steganography, the strength of the carrier file used to embed a secured data or file is vital; it should be resilient and resistant to being easily deciphered or compromised by unauthorized users. The concealment of a secret message often relies on methods as LSB (Least Significant Bit) and adaptive techniques to enhance tamper resistance. emergencies like accidents or derailments, these systems

II LITERATURE SURVEY

The field of literature review or survey regarding steganography involves concealing text or data within chosen cover files like multimedia files such as audio, images, or videos. The technique of hiding secret messages is a significant method that enables the embedding of confidential information within video or image files using elements within the cover file. One of the primary advantages of using video files to hide data is the enhanced security they provide against hacking attempts. This security advantage stems from the complexity inherent in video files compared to simpler image or audio formats.

Considered researches have been conducted in the field. of image steganography over time .Nevertheless, the increasing volume to data transmitted among the World Wide Web (WWW) and the internet has sparked greater interest in concealing larger amounts of information. This study focuses on introducing methods to hide more extensive data through video steganography. The main objective is to enhance the capacity for concealing significant information, particularly over the internet or WWW. Various methodologies are employed and compared to achieve enhanced results, with a specific focus on comparing parameter value matrices for evaluation purposes..

Title	Authors	Year	Objectives	Advantages	Disadvantages
Image Steganography: A Review of the Recent Advances [1]	Nandhini Subramanian; Omar Elharrouss; Somaya Al-Maadeed; Ahmed Bouridane	2021	The primary goal is to examine current methodologies closely., emphasize ongoing trends, and tackle prevalent challenges within the field of study. Further more, its goal is to explore commonly used publicly available datasets and delve into the evaluation metrics typically considered within this realm of research.	1. The classification of available works in steganography often considers two primary factors: the character of the secret media and the technique employed. Typically, text data along with color or grayscale images serve as secret media for concealing information. Scientists classify these works according to the attributes to the secret media.	An imbalance in the learning process between the generator and discriminator can occur in a generative adversarial network (GAN) setup, where the generator might perform effectively while the discriminator faces challenges. While this imbalance might not significantly impact the overall efficiency of the system, it can create vulnerabilities for either the sender or the receiver participated in the process.
A Review on Text Steganography Techniques [2]	Majeed, M.A.; Sulaiman, R.; Shukur, Z.; Hasan, M.K	2021	1. This paper offers an extensivean examination of the latest research in the field of text steganography. Initially, it furnishes fundamental information regarding text steganography, elucidating its basic procedures. Following this, it delves into an explanation of three distinct classes of text steganography.	1. A model was introduced to enhance both the capacity and security in statistical text steganography by addressing the expense associated with synonym substitution.	A groundbreaking method of coverless text steganography was introduced., leveraging the Markov model and the half frequency crossover principle. This approach adheres closely to the statistical attributes inherent in natural language.
Combination of Steganography and Cryptography: A short Survey [3]	Mustafa Sabah TahaL, Mohd Shafry Mohd Rahim, Sameer Abdulsattar Lafta, Mohammed Mahdi Hashim	2019	The main goal is to perform an extensive review of diverse methodologies that combine steganographic and cryptographic techniques, thereby forming a hybrid system. This review aims to explore how these combined methodologies synergize to enhance data security and confidentiality.	The embedding technique was implemented with the goal of minimizing changes to the length of a particular message. This approach resulted in improved velocity, expanded steganographic capabilities, and enhanced security against both observed and analytical attacks.	The drawn conclusion indicated that methodologies starting with Instances involving cryptography were more frequently noticed than those beginning with steganography...Additionally, these cryptography-oriented methods were found to offer enhanced security while exposing less hidden data.
Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions [4]	Oleg Evsutin; Anna Melman; Roman Meshcheryakov	2020	The primary objective is to pinpoint and elucidate the prevailing issues and challenges within the realms of digital steganography and digital watermarking, contextualized within the current state of this scientific field.	Digital steganography methods are employed to safeguard the confidentiality of information by enabling its discreet transmission within digital objects, especially digital images	Primary drawback associated with spatial methods in digital steganography is their weak robustness The information embedded is extremely vulnerable and at risk of total destruction when the carrier image undergoes various type of image processing or manipulation.

Title	Authors	Year	Objectives	Advantages	Disadvantages
Digital image steganography: A literature survey [5]	Pratap Chandra Mandal, Imon Mukherjee, Goutam Pau , B.N. Chatterji	2022	1. The main challenge in proposing a steganographic technique is to maintain a suitable balance among higher embedding capacity, imperceptiable , and securable that separate it from correlated systems like cryptography and watermarking.	The three main criteria: capacity, imperceptibility, and security, these criteria help us to move in the right direction for enhancing the techniques.	1. The selected parameters for comparison include the technique's advantages, drawbacks, embedding capacity, visual quality, and resistance against statistical attacks or steganalysis.
SteganoGAN: High Capacity Image Steganography with GANs [6]	Kevin A. Zhang, Alfredo Cuesta-Infante,Lei Xu, Kalyan Veeramachaneni	2019	It seems that the sentence provided is incomplete or contains some typographical errors, making it difficult to understand the intended meaning. However, considering the context provided, it seems to be discussing the assessment of a steganographic method's ability to evade detection by conventional steganalysis tools., which are specifically designed to identify whether an image contains hidden information or not.	This scenario replicates a realistic setting where the entity developing the automatic detection model might lack access to the particular STEGANOGAN model being utilized Nonetheless, It's possible that they get to the software utilized for training these models.	By employing a cost function and incorporating handcrafted features, HUGO evaluates the impact of these alterations on the overall image, aiming to ensure those modifications remain imperceptible to human observers effectively hiding the concealed information within the image.
Payload-Independent Direct Cost Learning for Image Steganography [7]	Weixiang Li; Shihang Wu; Bin Li; Weixuan Tang; Xinpeng	2023	This framework directly learns universalexpenses that may be attributed to any payload. PICO-RL incorporates an optimal probability approximation (OPA) module that can calculate the required probability map for embedding simulation directly from a learned cost map for any payload	1.RL training, the learned cost maps of different payloads converge and eventually become similar under the OPA constraint, resulting in payload independence. 2. Experimental results demonstrate that a well-trained PICO-RL model, which acts as a universal cost function, defines costs with superior security performance against steganalysis and has better coding compatibility when encoding with practical steganographic codes.	1. these architectures only learn embedding probabilities rather than costs, and are altered for a specific embedding payload, making it difficult to extend the trained model to serve other payloads.

Title	Authors	Year	Objectives	Advantages	Disadvantages
DKiS: Decay weight invertible image steganography with private key . [8]	Hang Yang, Yitian Xu, Xuhua Liu	2023	a novel private key-based image steganography technique. This approach ensures the security of hidden information, requiring a corresponding private key for access, irrespective of the public knowledge of the steganography method. We present experimental evidence demonstrating our method's effectiveness, showcasing its real-world applicability.	1. By employing complex neural networks, it has become possible to embed larger amounts of data with improved security measures. 2. These deep learning models can learn optimal ways to conceal data within images, making detection by thirdparty observers or automated systems significantly more challenging.	Image steganography continues to evolve, facing the challenge of maintaining confidentiality amidst widespread popularity. The known methods of steganography can be compromised by unauthorized parties, making it unsuitable for high-security contexts.
FIXED NEURAL NETWORK STEGANOGRAPHY: TRAIN THE IMAGES, NOT THE NETWORK [9]	Varsha Kishore, Xiangyu Chen, Yan Wang, Boyi Li, Kilian Q Weinberger	2022	An innovative steganographic steps leverages the sensitivity of neural networks to minute alterations. Our approach, known as Fixed Neural Network Steganography (FNNS), demonstrates substantially reduced error rates compared to previous state-of-the-art methods. It reliably achieves a 0% error rate when concealing up to 3 bits per pixel (bpp) of confidential information within images.	1. Use similar encoder-decoder architectures to hide and recover structured images instead of random bits. These methods assume the secured data is an image, which allows them to learn image priors that aid in hiding the hidden image. Researchers have also investigated from invertible networks for concealing images within other images.	1. Instead of targeting a single prediction bit (e.g. the classification of an image), the sender manipulates thousands or even millions of output bits simultaneously. For intended recipient (Bob) can use the same decoder network and recover the hidden message.
An Automatic Cost Learning Framework for Image Steganography Using Deep Reinforcement Learning [10]	Weixuan Tang, Bin Li, Mauro Barni, Jin Li, Jiwu Huang	2020	1. In SPAR-RL, an agent utilizes a policy network which decomposes The embedding process involves pixel-wise actions and focuses on maximizing the overall rewards within a simulated steganalytic environment. while the environment employs an environment network for pixel-wise reward assignment.	A sampling process is utilized to mimic the message embedding process of an ideal embedding simulator. Experimental results demonstrate that the proposed framework achieves state-of-the-art security performance against various modern steganalyzers, and outperforms existing cost learning frameworks with regard to learning stability and efficiency.	1. However, these methods still have limitations that hinder the complete exploitation of their capabilities., including using a function-approximated neural-network-based embedding simulator and a coarse-grained optimization objective without explicitly using pixel-wise information

III . CONCLUSION

In summary, Steganography serves as a technique employed to covertly embed confidential information or messages within various media files, acting as covers during transmission from a sender to a receiver.. Due to its complexity, learning steganography is not straightforward. Hence, Both sender and receiver need to have a thorough understanding of steganographic techniques. across various formats and under diverse conditions. This knowledge is crucial for effectively utilizing this method of communication.

For successful communication using steganography, both involved parties—the sender incorporating the information, and receiver retrieving it—extracting it—should possess knowledge and proficiency in diverse steganographic methods applicable to different data formats and scenarios. This comprehensive understanding ensures the successful transmission and extraction of concealed information while navigating through various formats and potential environmental conditions.

REFERENCES

[1] Almuhammadi S and Al-Shaaby A 2017 A survey on recent approaches combining cryptography and steganography Computer Science Information Technology (CS IT).

[2] Hashim M, Rahim M, Shafry M and Alwan A A 2018 A review and open issues of multifarious image steganography techniques in spatial domain Journal of Theoretical & Applied Information Technology.

[3] Seth D, Ramanathan L and Pandey A 2010 Security enhancement: Combining cryptography and steganography International Journal of Computer Applications

[4] Laskar S A and Hemachandran K 2012 Combining JPEG steganography and substitution encryption for secure data communication Computer Science\& Information Technology (CS\& IT).

[5] Lyubashevsky V, Micciancio D 2018 Asymptotically Efficient Lattice-Based Digital Signatures Journal of Cryptology.

[6] Morkel T 2012 Image steganography applications for secure communication Doctoral dissertation, University of Pretoria.

[7] Al-Husainy M A F and Uliyan D M 2018 Image Steganography Technique Based on Extracted Chains from the Secret Key Journal of Engineering and Applied Sciences.

[8] Hussain M, Wahab A W A, Idris Y I B, Ho A T and Jung K H 2018 Image steganography in spatial domain: A survey Signal Processing: Image Communication.

[9] Dhamija A and Dhaka V 2015, October A novel cryptographic and steganographic approach for secure.

[10] cloud data migration In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on (pp. 346-351) IEEE.

[11] Patil S S and Goud S 2016 Enhanced Multi Level Secret Data Hiding In An International Conference.

[12] Hingmire A, Ojha S, Jain C, Thombare K 2016 Image steganography using adaptive b45 algorithm combined with pre-processing by twofish encryption International Educational Scientific Research Journa.

[13] Yassein M B, Aljawarneh S, Qawasmeh E, Mardini W and Khamayseh Y 2017, August Comprehensive study of symmetric key and asymmetric key encryption algorithms. In Engineering and Technology (ICET), 2017 International Conference on (pp. 1-7) IEEE.