RESEARCH ARTICLE OPEN ACCESS

Analysis and Review on Advancement in Steganography Techniques

Madhuja Saha[1], Nilendu Barman[2], Anirban Bhar[3], Neepa Biswas[4]

[1](B. Tech Student, Department of Information Technology, Narula Institute of Technology, Kolkata, India Email: madhujasaha4@gmail.com)

[2] (B. Tech Student, Department of Information Technology, Narula Institute of Technology, Kolkata, India Email: nilendubarman404@gmail.com)

[3] (Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India Email: anirban.bhar@nit.ac.in)

[4] (Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India Email: neepa.biswas@nit.ac.in)

Abstract:

This research paper explores the world of steganography, a technique that hides sensitive information within seemingly ordinary digital content. Steganography serves a critical purpose in modern information security by allowing confidential data to be transmitted covertly, protecting it from prying eyes. The central problem it addresses is the need to safeguard sensitive information during digital communication. The primary purpose of steganography is to facilitate secure communication by embedding sensitive information within innocuous carriers. In an era of pervasive data breaches and privacy concerns, this study delves into the core problem of ensuring confidential data exchange. Steganography offers a solution by allowing data to be hidden in various digital media, including image, audio, video and text. Our findings underscore the importance of steganography in various real-world applications, such as secure messaging, and even counterterrorism efforts. In conclusion, this research paper serves as a comprehensive resource for understanding steganography's purpose, the challenges it addresses, the design of steganographic methods, and the current state of the field. Steganography has transcended its historical roots to become an indispensable component of modern data protection, offering a secure cloak for information in an increasingly interconnected world.

Keywords — **Steganography, Data hiding, Information hiding, Covert-communications.**

I. INTRODUCTION

The ancient Greeks were the first to adopt a form of steganography, hiding messages by tattooing them on the shaved heads of slaves and then letting their hair grow back over them. Hidden communications were transmitted during the Middle Ages using methods such as invisible inks and microdots.

Computers allowed steganography to make the leap into the digital sphere. The privacy of sensitive data was greatly enhanced by the convenience of digital files. Steganography gained importance with the expansion of the internet and other forms of digital communication. It evolved into a stealthy means of transmitting data without raising eyebrows.

Intelligence agencies, cybercriminals, and activists all employ steganography for clandestine messaging. They can safely share information with one another. Steganography is a method of hiding important information among seemingly unrelated files for use in secure environments. This method

shines in cases where the use of encryption could lead to suspicions.

Finding information that has been steganographically concealed is a complex problem in digital forensics. In order to uncover secret data in multimedia files, sophisticated methods of analysis are required. Research into steganography is crucial for the creation of countermeasures against illegal applications. Steganographic techniques are always being researched by security specialists in an effort to improve detection capabilities.

Digital watermarking uses steganography to make imperceptible modifications to media files that indicate ownership. This is absolutely vital for online copyright security.

When used with encryption, steganography provides an extra layer of protection. A message is twice protected when encrypted and then hidden in a picture.

Steganography is useful for protecting individual privacy. It can be used to conceal metadata in photos, for instance, which might otherwise expose users to privacy risks.

Improvements have been made in both steganography and steganalysis (the study of uncovering secret messages) thanks to AI. Advanced steganographic techniques and enhanced detection capacities are both made possible by employing AI algorithms.

II. LITERATURE REVIEW

Steganography is an intelligent data hiding technique in which the secret data is embedded in a cover media in such a way that the media carrying the secret message are untraceable and unobserved by the intruder or attacker [1]. Steganography is a term that comes from the Greek word steganos, which means "to hide." Even if the message is found, it won't be possible to understand what it says. In the context of the digital world, the goal of both cryptography and steganography is to hold and save the secret message while also protecting it from being hacked or attacked by other individuals [2]. These methods are beneficial whether they are carried out jointly or separately. The combination of the two also produces outstanding results, but it must be done in stages in order to maintain a high level of safety. Text, images, DNA, networks, music, and videos are only some of the several types of data formats that can be hidden via digital steganography today [3]. When one considers the breadth of steganography, one can easily understand that the significance of modern steganography, particularly in relation to the internet, is for the preservation of both confidentiality and authenticity. The resilience of cryptosystems in the internet group has been reduced [1] mostly as a result of the stringent constraints enforced by authorities and the hurdles they have created. Steganography is required since this is the reason why we need it. Steganography ensures that the message that is sent is safe and cannot be retrieved by an intruder from the host medium unless they have the correct key. To the best of our knowledge, among the numerous varieties of digital steganography, picture steganography continues to be the most frequent type of digital steganography medium because of its great ability to disguise the secret data in the cover media with undetectable effects [4].

III. INTERACTION DESIGN PRINCIPLES

Steganography is the covert practise of hiding information in plain sight under seemingly unobtrusive cover media in order to protect the information from being discovered by unauthorised parties. By combining the digital world with clandestine communication, this brilliant method ensures that private information can safely travel over the Internet without raising suspicion.

Steganography is based on discreetly modifying the bits and bytes of the cover media, which can be anything from an image to an audio file or even text. These subtle alterations, which are like to digital brushstrokes on a painting, make the concealed data nearly indiscernible from the background noise. It is a modern cypher in which the secret message is integrated into the carrier in such a way as to be undetectable even by the most thorough examination.

Steganography's fascinating uses are just as varied. It has become a crucial component of digital

secrecy, being used for everything from the security of top-secret military intelligence and corporate secrets to the facilitation of clandestine communication for espionage. Steganography has a place even in the worlds of art and culture, allowing creators to leave hidden messages or signatures for other like-minded individuals to discover.

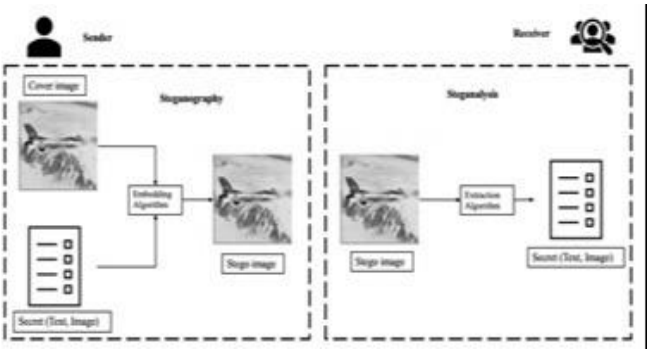

Figure 1: working principle of Steganography [5]

Steganographic methods have advanced in tandem with the rest of the technological world. Steganography has evolved to take use of advances in machine learning and artificial intelligence as encryption techniques have done so. These developments allow steganographic algorithms to make use of the subtleties of cover media, guaranteeing the safety of the hidden data amidst the huge sea of digital content.

However, enormous authority also calls for great accountability. While steganography has many potential benefits, it also presents difficulties for authorities and cybersecurity professionals. This ongoing cat-and-mouse game between those who would conceal information and those who would reveal the hidden realities requires sophisticated tools and procedures to detect these secret messages amidst the immense volume of digital data.

Steganography is a symbol of human creativity and the constant push of digital innovation in a world where information is both currency and weapon. Reminding us that even in the visible spectrum of data, there exist areas of hidden significance, ready to be revealed by those with the expertise and will to do so, it epitomises the fine balance between secrecy and transparency.

There are various types of steganography techniques, each with its own methods of embedding and extracting hidden information. Here are some of the key types of steganography:

- *Image Steganography:* Spatial Domain: Involves directly manipulating the pixel values of an image to hide data. Common techniques include LSB (Least Significant Bit) and LSB matching, where the least significant bits of pixel values are replaced with hidden data.

Transform Domain: Utilizes mathematical transforms like Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) to embed data in the frequency domain of an image.

- *Audio Steganography:* Conceals data within audio files such as WAV or MP3. Techniques include modifying audio samples, phase encoding, and spread spectrum techniques.

Audio steganography can be used for covert communication or watermarking audio content for copyright protection.

- *Video Steganography:* Conceals data within video files. This can be done by modifying frames, altering motion vectors, or embedding data in the temporal and spatial domains of the video stream.

Video steganography is often used for privacy protection or watermarking.

- *Text Steganography:* Embeds hidden information within text documents. Techniques include modifying white spaces, punctuation, or using synonyms to convey hidden messages.

Text steganography is used for covert communication in textual content.

- *Network Steganography:* Involves hiding data within network protocols or traffic. This can include manipulating packet headers, timing, or using covert channels within legitimate network communication.

Network steganography can be used for espionage, data exfiltration, or bypassing network security measures.

- *File Steganography:* Embeds data within various types of files, such as documents, spreadsheets, or executable files. The hidden data may be concealed within the file structure or content.

File steganography can be used to hide sensitive information within seemingly harmless files.

IV. ADVANCED STEGANOGRAPHIC ALGORITHMS

A. Genetic Algorithm-based Steganography:

Steganography that relies on evolutionary algorithms, such those found in Genetic Algorithms (GA), is a method used to covertly conceal information within other forms of digital material. Genetic algorithms are search heuristics that take their cue from the process of natural evolution, while steganography seeks to hide the fact that secret information ever exists. Using GAs in steganography entails seeing information concealment as an optimisation issue, the solution to which is to find the most imperceptible manner to embed data into a cover material.

The process of GA-based steganography is described in detail below.

Produce a seed set of potential solutions. When discussing steganography, these options stand for various strategies for concealing information inside the medium of concealment. To determine how successfully secret information may be concealed in a given cover medium, a fitness function must be defined. This metric evaluates how well a stego-object hides its contents and how accurately it can retrieve them.

The second step is selection, which involves using the fitness function to rank each solution in the population.

Using a population's fitness as a criterion, select the best possible solutions (people). Better data concealment solutions will be chosen.

Third, Recombination (Crossover): Produce offspring by crossing children of selected solutions. When two or more solutions are crossed over, their best parts are combined to form a new solution. Mutate some of the answers randomly to keep the population's genetic makeup diverse.

Fourth, using the fitness function, rate the success of the progeny.

Choose members of the next generation from the pool of parents and offspring. The strongest individuals can thrive and pass on their genes in this way.

Examine the presence of a termination condition. Limits on time, fitness, or the number of generations can all be used to force the algorithm to stop running.

After the evolutionary algorithm finishes, the optimal solution (the one with the maximum fitness) is the stego-object carrying the secret information, and this information can be extracted in last step.

B. Deep Learning Approaches in Steganography:

A message, file, image, or video can be steganographed if it is embedded in another file, image, or video in such a way that it is impossible to identify or decipher without the knowledge of the intended receiver. In recent years, steganography has benefited from the use of deep learning techniques, resulting in the creation of more advanced and efficient methods for concealing data within digital media. Some examples of the use of deep learning in steganography are as follows:

1. *Generative Adversarial Networks (GANs):*

Both the generator and discriminator neural networks of a GAN are trained at the same time. GANs can be used to create convincing cover pictures and steganographic images for use in steganography. The discriminator attempts to tell the difference between authentic and steganographic images, while the generator generates the latter. In order to make more convincing and undetected steganographic information, training GANs is essential.

2. *Convolutional Neural Networks (CNNs):*

Due to its capacity to capture spatial patterns, CNNs have found widespread use for image-related tasks. CNNs can be used to analyse cover and stego images for hidden features. In order to aid in the detection and extraction of hidden information, CNNs can be trained on a large dataset of cover and stego pictures.

3. *Attention Mechanisms:*

The network can zero in on a specific subset of the input data thanks to attention mechanisms in deep learning models. To selectively conceal data in different parts of an image, steganography makes advantage of attention mechanisms. Steganographic algorithms can better hide information while reducing visual artefacts if they focus on the right sections of the cover image.

4. Recurrent Neural Networks (RNNs):

Since RNNs perform well with sequential data, they can be used in steganography to secretly encode sequential data inside of a picture or a video. RNNs generate coherent, undetectable steganographic material by processing the data sequentially.

5. Autoencoders:

Autoencoders are neural networks that may be taught to compress the input data into a representation and then decode that representation back into the original data. Autoencoders are useful in steganography because of their ability to conceal data in the latent space. Information can be steganographically embedded by altering the latent space representation, and then decoded to reveal the embedded information.

6. Adversarial Training:

Adversarial training, which is used in GANs, can also be used in steganography. Training a steganographic encoder and a detector at the same time in an adversarial fashion improves both systems' abilities to hide and uncover information. Strong steganographic methods are developed as a result of this adversarial process.

To improve the safety and efficacy of steganographically concealed communication, researchers are always looking into novel deep learning architectures and methodology. While these methods can be quite effective, they also present some serious ethical considerations and have the potential to be abused, which is why there has to be careful study and development in this area.

One of the main benefits of steganography based on GAs is their flexibility in accommodating a wide variety of cover media and hidden information.

Due to their ability to solve nonlinear and complex optimisation issues, GAs are well-suited for use in steganography across media types.

Optimisations made by GAs during the embedding phase render the concealed information invisible to both human eyes and statistical methods of analysis.

Difficulties and Things to Think About:

There is typically a compromise between how much information may be buried and how well the stego-object mimics the original cover media. Generally speaking, these elements need to be balanced by GAs.

When working with huge, high-dimensional media files, GAs can be very computationally intensive.

The strength of the algorithm's protection is determined by its complexity, the amount of randomness it introduces, and its ability to withstand attacks from steganography.

It is important to be familiar with both genetic algorithms and digital media types before attempting to use GA-based steganography. New approaches and enhancements to GA-based steganography are constantly being investigated by researchers and applied by professionals in order to boost security and efficiency.

C. Cryptographic Techniques in Steganography:

Steganography is the process of hiding information in another file or communication so that it cannot be easily discovered or decoded. Combining steganography with cryptographic methods strengthens the confidentiality of transmitted data. Some examples of cryptographic procedures that can be used in steganography are shown below.

1. Encryption:

If you want to conceal a message in an image or some other media, you need encrypt it first. Even if the secret message is uncovered, an unauthorised reader would still need the decryption key.

2. Digital Signatures:

Make sure the secret message is genuine and intact. A digital signature verifies the authenticity of the sender and guarantees that the encrypted message has not been tampered with in transit.

3. Public Key Infrastructure (PKI):

Transmitting and receiving keys are safely exchanged. With PKI, you may safely trade encryption keys, guaranteeing that only the receiver you specify can read your secret communication.

4. Hash Functions:

Check that the secret message is still intact in the stego-object (picture, for example). The stego-object can be represented by a fixed-size hash value generated by a hash algorithm. A different hash value indicates that the stego-object has been tampered with.

5. Symmetric and Asymmetric Encryption:

Make available a variety of essential administration and security settings. Asymmetric encryption employs a set of public and private keys, while symmetric encryption use a single key for both encryption and decryption. Asymmetric encryption helps with the safe transfer of symmetric keys.

6. One-Time Pads:

Keep the secret message's location completely under wraps. Message-length random keys are used to create one-time pads. When used with the XOR technique, they provide a secure code that cannot be cracked. The difficulty, however, lies in doing so in a safe and reliable manner.

7. Steganographic Algorithms:

Use a cover media (photo, song) to conceal the encrypted message. Algorithms used in steganography decide where and how the secret message data will be concealed within the cover medium. The Least Significant Bit (LSB) substitution and spread spectrum methods are just two examples.

8. Visual Cryptography:

Break apart the secret message into parts that, taken separately, reveal nothing. In visual cryptography, an image is divided into shares, and the secret message is deciphered by stacking the shares. These stocks and bonds do not reveal the secret message on their own.

9. Watermarking:

Include details about the cover media in the secret message. Copyright data is just one example of what might be embedded into a cover using watermarking techniques. While not technically steganography, it does entail secretly transmitting data via digital multimedia.

10. Key Management Protocols:

Take charge of the cryptographic keys. To safely trade encryption keys between sender and recipient, protocols such as Diffie-Hellman key exchange and RSA key exchange are utilised.

Combining steganography with cryptographic methods strengthens the secrecy of transmitted data and makes it more difficult to intercept, decode, or tamper with hidden signals.

V. CONCLUSION

Integration of AI, Q.C., and blockchain technology into the future of sophisticated steganography techniques has promising prospects. However, it raises concerns about privacy and safety. Finding a happy medium between protecting users' anonymity and blocking malevolent actors will be a major challenge.

In order to keep one step ahead of detection methods, researchers and practitioners in this sector will need to maintain a constant state of vigilance. To advance the field and keep the playing field equal between those who hide information and those who want to reveal it, collaboration between experts in steganography and steganalysis will be important.

REFERENCES

[1] Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing, 335, 299-326.

[2] Hussain, Mehdi, et al. "Image steganography in spatial domain: A survey." Signal Processing: Image Communication 65 (2018): 46-66.

[3] Taha, Mustafa Sabah, et al. "Information Hiding: A Tools for Securing Biometric Information." Technology Reports of Kansai University 62.04 (2020): 1383-1394.

[4] Saini, Ravi, Kamaldeep Joshi, and Rainu Nandal. "An Adapted Approach of Image Steganography Using Pixel Mutation and Bit Augmentation." Smart Computing Techniques and Applications. Springer, Singapore, 2021. 217-224.

[5] Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. IEEE access, 9, 23409-23423.