International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 79-89, March-2024
https://doi.org/10.47001/IRJIET/2024.803011

A Deep Dive into Deep Learning-Powered Steganography for Enhanced Security: Review

[1]Anfal Shihab Ahmed, [2]Melad Jader Saeed

[1,2]Computer Science Department, University of Mosul, Mosul-Iraq
Authors E-mail: [1]anfal.21csp89@student.uomosul.edu.iq, [2]meladjader@uomosul.edu.iq

***Abstract* - Steganography—the practice of hiding data in digital media—has attracted a lot of interest because of its possible uses in secure communication. This study offers a thorough summary of the most recent developments in steganography, emphasizing the incorporation of deep learning (DL) methods in particular. The review explores several steganographic techniques, classifies them, and assesses the advantages and disadvantages of each. Moreover, it reviews current research projects that use DL to improve security and resilience in steganographic systems. This evaluation finds new trends, problems, and possibilities in the field by examining related studies. The major goal is to advance this field and broaden our understanding of steganography-based secure communication.**

Keywords: Steganography, Digital media, Data hiding, Deep learning.

I. INTRODUCTION

Since the development of information and communication technology (ICT), the Internet has become the primary means for the transmission of sensitive data, including audio, video, and image files [1]. But there are now a lot of issues with accessibility that relate to the dependability and security of this kind of communication. Information security researchers are becoming more and more concerned with the necessity of data communication that protects privacy as well as the legality of information transfer [2].

Protecting data, ensuring data transmission that respects privacy, and preventing data breaches and plagiarism are the main goals of current research. Steganography systems (SS) are one of the many protection strategies that have been quickly developed in response to the ever-evolving threats posed by adversaries and hackers [3]. Historically, safe data transfer has been achieved through the use of encryption techniques; however, worries about unapproved access and modification have prompted research into other approaches. Although digital data are convenient, they can be manipulated and attacked, especially when distributed via unreliable networks like the Internet [4].

Highly secure and privacy-preserving information transfer methods are desperately needed, especially since the Internet and cloud computing play such a crucial part in modern communication. Data transmission over unsecure networks is a common source of information security flaws, making the creation of safe methods to guard against unauthorized access necessary [5]. A lot of research has been done to develop safe and private information exchange, with an emphasis on information masking technologies, in order to overcome these issues. These technologies allow for the secure transmission of sensitive data by enclosing it in digital media such as audio, video, and image files [6].

In example, steganography techniques are frequently used to safely hide textual data within of media, rendering it undetectable to unauthorized users. Cryptography is used in data concealing techniques to make sure that information that is hidden is kept secret unless the right decryption key is present. Although the goal of data concealment procedures is to make buried data undetectable, they might nevertheless be seen by observers without disclosing their contents. In order to keep hidden information out of the hands of unauthorized people, cryptography is essential [7].

Steganography systems' ultimate objective is to improve data security during transmission by hiding sensitive information from prying eyes. Watermarking is a technique used in data concealing that includes subtly altering images in order to incorporate concealed data [8]. Figure (1) shows a classification scheme that describes the different ways in which information can be hidden.

This paper discusses the critical need for extremely private and secure information transfer protocols, especially in light of the Internet's and cloud computing's critical roles in contemporary communication. It draws attention to how vulnerable data transfer over unreliable networks is, highlighting how important it is to come up with safe solutions to prevent unwanted access. Creating private and secure information sharing protocols has been the subject of extensive research, with a focus on information masking technology. These technologies allow for the secure transmission of data by encoding sensitive data into digital files, including audio, video, and image files.

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 79-89, March-2024
https://doi.org/10.47001/IRJIET/2024.803011

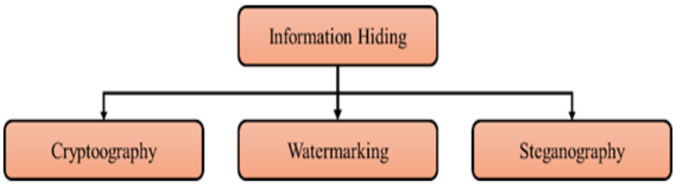

Figure 1: Classification scheme of information hiding

II. STEGANOGRAPHY SYSTEM

Steganography is a technique that allows people with privileged access to communicate covertly by encoding sensitive information into many kinds of digital media carriers, including text, audio, photos, and videos [9]. Figure 2 shows the common block design for steganography. Several terms are frequently used in steganography systems. [10].. The original digital media file—a picture, video, song, text, or other type—that contains the hidden message is referred to as the "cover file." The payload is the message that is supposed to be embedded in the cover file and is considered the secret message. Stego files are ones that are made to closely mimic cover files and carry the secret message that was previously hidden within them. The secret message is extracted from the stego file using the extraction technique, and the hidden message is integrated within the cover file using the embedding process.[11].

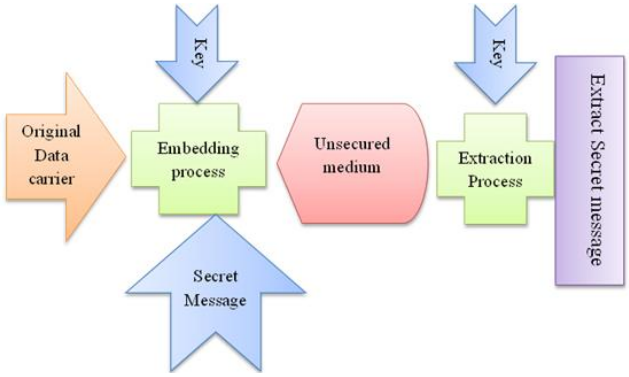

Figure 2: Steganography General Block Diagram

The sender chooses the carrier file and the secret message to start the hiding process in a steganography system. To securely encrypt the message, it is imperative to use the most appropriate and effective steganography algorithm. The sender can deliver the stego file via email, chat, or other modes of communication once the message has been encrypted. When the recipient receives the stego file, they use the extraction process to unlock the encrypted message. This procedure makes sure that private information may be sent between parties in a secure manner and kept hidden from prying eyes[12]. In any effective steganography system, two crucial factors must be considered:

Embedding Payload: This refers to the amount of hidden data concealed within the cover information. The embedding payload is determined by the algorithm's capacity to accommodate the secret message. A higher embedding payload indicates a greater capacity for the secret message. However, embedding efficiency is influenced by various factors such as stego visual quality, security, and resilience against attacks[13].

Embedding Efficiency: A low modification rate and high-quality cover data work together to produce strong embedding efficiency. High embedding efficiency steganography algorithms make it difficult for steganalysis tools to find hidden data and lessen the possibility that attackers have tampered with it. However, after embedding, any changes made to the cover data could draw the notice of attackers. Therefore, the effectiveness of embedding is directly impacted by the security of the steganography system.[14].

A trade-off is there between embedding efficiency and embedding payload in a traditional steganographic method. The video quality that results from expanding a stego file's hidden message capacity usually suffers as a result. As a result, this compromise reduces the embedding process's overall efficacy. It is important to think about both at the same time. The final result is mostly dependent on the user's requirements and the steganography technique selected, which balances embedding efficiency with payload capacity[15].

III. THE USES OF STEGANOGRAPHY

This strategy entails manipulating the image to successfully hide information. It works very well for adding watermarks on photos. This approach makes sure that the data is implanted where it matters most, unlike traditional methods that hide information in dark areas of the image. By applying watermarking techniques, the data is deeply embedded in the picture, providing resilience against possible loss. This technology's versatility and applicability are increased by supporting grayscale and 24-bit images[16].

Watermarking is another application for steganography. Although watermarking is not a steganographic technique per se, information is embedded in watermarks using a variety of steganography techniques. The essential need is still in place: the watermark enhances the original source with new information. The addition of steganography to watermarking makes any changes made to images, sounds, or videos less noticeable to users. This combination of steganography into watermarking can prove advantageous, especially in online business contexts, where minor adjustments are needed.

The transmission of confidential data is one of steganography's other important uses. Even if encryption has its uses, eavesdroppers are a possible danger because they can quickly recognize encrypted communications. However, steganography provides an answer by enabling the covert transmission of personal data without raising listeners' suspicions. Data can flow over this covert communication without being noticed by outside parties. Data can be transferred using steganography on almost any kind of data transport, including emails and online photos [16].

Applications for steganography are numerous and address privacy and data security issues. First of all, it functions as a clandestine means of information transmission, guaranteeing that messages stay unnoticed and untraceable [17]. Furthermore, several data sets can be hidden using steganography inside a single cover source, which makes it difficult to identify important information among less private material [18]. Furthermore, steganography adds an additional layer of camouflage to watermarking techniques, making it harder for users to identify changes made to photos, audio, or video files [19]. Steganography is useful for improving transaction security in e-commerce, especially when combined with other methods like biometric fingerprint scanning and encoding session IDs into fingerprint photos[19].

Steganography also makes covert communications easier, especially when it comes to corporate and national security issues. This has potential uses in protecting confidential data [20]. It is also essential for the safe transportation of sensitive data [21]. Steganography finds further uses outside of these applications, including smart ID creation, picture search engine support, copyright protection, multimedia synchronization, television broadcasting, TCP/IP packet transmission, checksum embedding, and secure data transfer [22].

Steganography has also recently been used in medical imaging systems, where it is crucial to protect patient privacy by separating picture data from delicate captions that include private information. [23][24]

IV. STEGANOGRAPHY TECHNIQUES

Techniques for steganography include a range of approaches to hiding information in a variety of items or media so that it is not readily apparent that it is there. Frequently used methods include picture steganography, which modifies the least important color values in an image file to encode data inside its pixels. Audio steganography hides data within audio recordings by changing specific frequencies or sound waves. Video steganography modifies frames or sequences to hide data from view in video files. Text steganography is the process of encrypting data with words, letters, or punctuation in text files.

By altering the contents of network traffic, such as packets or frames, network steganography conceals data. Data is hidden within transmission methods by the use of fields or flags for encoding, or by developing new protocols specifically designed for steganography. Furthermore, data can be concealed within tangible objects or media, such as invisible ink or microdots, using steganography on physical media. Although there are many uses for these methods, it is important to utilize them responsibly and legally, weighing the advantages and disadvantages before proceeding.

4.1 Spatial Domain Technique

Using spatial domain steganography techniques, information is directly embedded into a picture or video file's pixels. This can be achieved by adjusting the color values of the individual pixels, either by adjusting individual bits or by altering the color value as a whole. [25].

1. **Least Significant Bit Insertion (LSB):** One popular steganographic method for concealing data in digital photos, audio files, and other digital media is insertion. The idea behind Least Significant Bits (LSB) insertion is quite simple: the most significant bits of an image or audio file are left unaltered, while the least significant bits are changed to encode the hidden information. Small modifications to the least significant bits are less likely to be noticed by human observers because they have less bearing on the media's overall visual or aural quality[25].
2. **Binary Pattern Complexity (BPC):** functions as an essential metric for evaluating a steganographic technique's security and effectiveness. It assesses how intricate the binary patterns produced by the algorithm are, which are useful for hiding a message inside a cover object like an audio file or picture. The main goal of steganographic techniques is to minimize any noticeable changes to the message's look or quality by seamlessly embedding it into the cover object. The actual message is encoded as a series of binary numbers that are purposefully inserted using a variety of techniques. [26].
3. **Pixel Value Differencing (PVD):** is a steganographic method for concealing data in digital photos. It works by altering the pixel values so that the secret information is represented by the differences between adjacent pixel values. This method is especially well-liked since it's easy to use and works well at concealing information from view without altering the way the human eye perceives the image[26].

4.2 Transform Domain Based Technique

A variety of approaches are used in transform domain-based steganography to hide sensitive information from view in the transformed domain of digital signals, such as audio, video, and photos. These methods work by applying transformations such as the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), or Wavelet Transform to transform the original signal into a different domain, like the frequency domain. Transform domain-based techniques, in contrast to conventional steganography techniques, integrate the secret message into the signal's transform coefficients rather than changing the original signal directly. This is achieved by altering the coefficients in a manner that stays invisible to human senses, such as introducing minor tweaks to the coefficient values. Discrete Cosine Transform (DCT) steganography is a well-known example of a transform domain-based steganography method that is widely used in picture and video steganography applications.

One common transformation used in picture compression, particularly in the JPEG compression standard, is the Discrete Cosine Transform (DCT). By gently altering the coefficients to fit the secret message, DCT steganography conceals the secret data inside the high-frequency coefficients of the DCT transform. Wavelet Transform steganography is another well-known transform domain-based steganography method. Using a wavelet transform, the image is first converted into the wavelet domain in this manner. The secret message is then encoded into the wavelet coefficients by a variety of techniques, including spread spectrum modulation and quantization index modulation (QIM). Because transform coefficients have a different statistical distribution from the original signal, transform domain-based steganography algorithms have several significant benefits, such as increased security and resistance to statistical analysis. Nevertheless, when compared to spatial domain-based steganography methods, these approaches might require more complex embedding procedures and more computational expenses. [26].

1. **The Discrete Fourier Transform (DFT):** This method uses the discrete Fourier transform, which is by definition discrete, to convert discrete-time signals into discrete frequency characteristics. This procedure creates, from a finite list of evenly spaced samples of a function, a list of coefficients that represent a finite combination of complex sinusoids, arranged by their frequencies. Effectively, the entire original domain of the sampled function—which frequently represented time or position along a line—is transformed into the frequency domain. [27].
2. **The Discrete Cosine Transform (DCT):** In several aspects, this approach resembles the discrete Fourier transform. The symbol or picture is altered using DCT from the spatial area to the repetition space. The numerical adjustments performed to the pixels have the effect of "spreading" the region of the pixel values over a portion of the image[27].
3. **Discrete Wavelet Transform (DWT):** This method is used to convert the image from the spatial area to the recurrence space. During the steganography cycle, DWT determines the high recurrence and low recurrence data of each picture pixel. It is a numerical tool for gradually disassembling images. Non-fixed signal handling is its principal use [27].

4.3 Vector Embedding

An efficient method of vector embedding makes use of MPEG-1 and MPEG-2 codec concepts. Using this technique, audio data is embedded into host video frames at the pixel level. The method adds a motion vector component to the H.264/AVC video coding standard, which acts as a covert carrier and embedding control at the same time. Crucially, the integrated data does not significantly compromise the video sequence's visual or perceptual integrity. This methodology boasts significant embedding capacity and high carrier utilization, enabling fast and effective implementation.[27].

4.4 Spread Spectrum

This method uses concealed information that is dispersed over a large frequency range. The intended low signal-to-noise ratio in each frequency range makes it difficult to identify the presence of information. There would still be enough information in other bands to recover the data even if specific data segments were taken out of a few bands. As such, it is challenging to remove the data fully without jeopardizing the cover as well. This approach is very dependable, especially for military communications[28].

4.5 Statistical Technique

By using this method, a few properties of the cover are changed to install the message. After the cover is divided into sections, one message bit is implanted in each block. The cover block is refreshed just as soon as the message bit size reaches one. [29].

4.6 Distortion Techniques

This technique stores secret data via signal distortion. The encoder performs several modifications on the cover image, and the decoder step uses a secret key to extract the original data from the encrypted data[29].

V. TYPES OF STEGANOGRAPHY

The message and the carrier are two separate components that are used in steganography. The carrier is the medium that holds the message, and the message is the secret information that needs to be kept hidden. Applications for steganography are numerous in the military, diplomatic, and private spheres. Three main factors are frequently taken into account when assessing a steganography approach's effectiveness: the message's size, the challenge of finding the concealed message, and the intricacy of message alteration. In addition, steganography falls into three categories according on its use and approach.[30]:

5.1 Pure Key Stego Systems

This type of steganography removes the need to transmit secret information before transmitting messages because it doesn't require any pre-established data to function. The most popular steganography method is one in which no stego key is shared between the parties involved in communication[31].

5.2 Private Key Stego Systems

With this kind of steganography system, the sender creates a communication channel by enclosing the secret key and the secret message inside the cover. If the secret key is known, the recipient can remove the hidden message from the cover. Similar to sending secret messages, it is impossible to access the data without knowing the secret key[32].

5.3 Public Key Stego Systems

Two keys are used in this third sort of steganography: a public key for sharing the secret message and a confidential key, sometimes referred to as the secret key. While the confidential key is kept safe and is used to encrypt the secret communication, the public key is freely available to all users within the system.[33].

Senders and recipients usually exchange public keys for particular systems and algorithms prior to any transmission occurring. The sender needs the public key of the recipient in order to send a message. The message is subsequently decrypted by the recipient using their private key; if the keys match, the message is sent and received successfully. The source's original intent for the message is still present[34].

VI. DEEP LEARNING (DL)

The application of artificial intelligence (AI) makes it possible to combine several contemporary technologies with the main goal of mimicking human reasoning and sentient behavior. When it comes to solving complicated problems like detection, object recognition, and self-driving, this integration is especially helpful. The two main procedures in machine learning systems (MLS) are usually feature extraction and training[35].

To extract pertinent features from input data, developers create feature extraction procedures. These features are then used to train classifiers in the system. The goal of this procedure is to guarantee the safe exchange of confidential information between senders and recipients. Although MLS is a useful tool for solving complicated issues, it has certain drawbacks[36].

Deep learning (DL) approaches are frequently used in the literature to handle a variety of problems in order to overcome these constraints. It is still difficult to create a suitable feature extractor, though, and calls for programmers with extensive experience and understanding of the particular issue at hand. Furthermore, extending a specific function to other issues poses an additional difficulty.

In response to these issues, DL has developed as a commonly utilized component of ML systems[37]. Figure (3) shows an example of a typical AI architecture, emphasizing how different technologies are integrated to tackle complicated tasks efficiently.

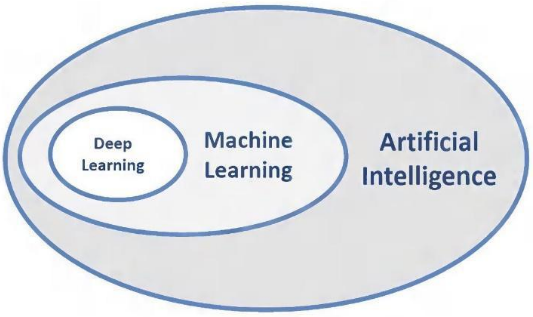

Figure 3: General framework of AI

Encoder-decoder architectures serve as an inspiration for Convolutional Neural Network (CNN)-based image steganography techniques. In order to extract the embedded secret image using these methods, the cover image and the secret image are fed into an encoder to create a stego image, which is subsequently sent through a decoder. Different strategies use different architectures, but the fundamental idea is always the same[38]. These include concatenating input pictures, convolutional layer configurations, pooling layers, number of filters, strides, filter sizes, activation functions, and loss functions. To ensure that every pixel in the secret image is dispersed throughout the cover image, it is imperative that the sizes of the cover and secret images match[39].

On the other hand, Generative Adversarial Networks (GANs) are a sort of deep CNN proposed by Good fellow et al. in 2014, applying game theory to train a generative model for picture generating tasks. The discriminator, which tells actual images from fraudulent ones, and the generator, which approximates images, are the two competing networks in a GAN architecture. The generator seeks to closely replicate input data through adversarial training, whereas the discriminator seeks to successfully detect false images.[40]

There are several GAN-based techniques for image steganography, including coverless models, Alice-Bob-Eve models, sender-receiver models, cycle-GAN architectures, and three-network GAN models.[41] These techniques hide secret images within cover images by utilizing GANs' advantages in image generating jobs. In order to improve steganography detection, several techniques include a Steg analyzer network. In general, GAN-based steganography techniques perform well in creating stego pictures while preserving security[38].

VII. RELATED WORKS

Advances in data hiding techniques, especially in the field of steganography, have attracted a lot of interest from scholars in a variety of fields in recent years. Steganography is a technique that includes hiding sensitive information in seemingly innocent cover media, such photographs. Because of its applications in data security, secure communication, and privacy protection, steganography has gained a lot of attention. Steganographic techniques are being continuously developed and improved by researchers in an effort to strengthen security, increase imperceptibility, and reduce vulnerabilities to possible assaults.

The goals, approaches, findings, advantages, and disadvantages of a number of significant steganography-related studies are compiled in Table (2). These works add to the changing field of data hiding technologies by examining deep learning-based methods and facial image steganography techniques. Whether it's increasing imperceptibility, strengthening security and robustness, or creating new encryption techniques, every research project aims to solve a particular problem. By these initiatives, scientists hope to improve steganographic techniques' efficacy and dependability for a range of uses, from secure communication to photo sharing that protects privacy and beyond.

Table 2: Related works analysis

Researchers	Objectives	Method	Results	Strength Points	Limitations
(Chaumont, 2019) [43]	Advance data hiding techniques, improve imperceptibility, enhance security against attacks	Develop DL-based methods for feature extraction, classification, and embedding in JPEG images and other media types	Achieve improved security and data hiding capacity, increase embedding ratio	Reliability across different image types, successful management of training and testing stages	Vulnerable to hacker attacks, inability to significantly increase imperceptibility
(Tao et al., 2023) [44]	Develop AI-assisted steganography model with high embedding ratio and compatibility between training and testing modes	Train embedded images with AI-assisted classifier, achieve 70% embedding ratio in training, 30% in testing	Successful embedding of secret data with limited embedding data, increased security	Efficient training and testing mode management, compatibility between stages	Limited embedding capacity, potential for improvement in security and robustness
(Bashir & Selwal, 2021) [45]	Enhance security and robustness of DL-based steganography	Develop DL algorithms for encoding and decoding in steganography, improve security and robustness	Enable learning of reversible steganography, distribution of data according to NN algorithm	Potential for reversible steganography learning, application of NN algorithm	Need for improvement in security and robustness, susceptibility to attacks
(Tang et al., 2017) [46]	Introduce three models for steganography with encoding and decoding networks, with enhanced models focusing on security and robustness	Basic model hides grayscale secret image in color channel B of cover image; Enhanced models add steganalysis and attack networks for improved security	Enhanced models are more secure and robust; Basic model hides secret image effectively	Use of less perceptible blue color channel enhances imperceptibility	Basic model lacks additional security features of enhanced models

(Naito & Zhao, 2019) [47]	Develop sender-receiver model using generator and discriminator in GAN architecture	Generator creates stego images, discriminator distinguishes true sender from third parties	Efficient sender-receiver communication, consistent results with shared generator and discriminator	Prevents wasting time on third party stego images	Susceptible to adversarial attacks targeting GAN architecture
(Zhu et al., 2018) [48]	Propose HIDDeN method using GAN with encoder, decoder, discriminator, and noise layer	Encoder encodes cover image and secret message into noised image; Decoder decodes secret message; Discriminator assesses image authenticity	High level of security with GAN-based approach	Encoder and decoder facilitate secure communication	Vulnerable to attacks targeting GAN architecture
(Ke et al., 2019) [49]	Introduce Generative Steganography with Kerckhoffs' Principle (GSK)	Generate new stego image with secret message instead of modifying cover image; Use discriminator with extraction key for decoding	Ensures secure transmission with extraction key requirement	Publicly available generator facilitates communication	Dependency on extraction key may hinder usability
(Meng et al., 2019) [50]	Implement CycleGAN for steganography and steganalysis in covert communication	Convert RGB cover image to grayscale, embed secret message in luma field; Introduce denoiser for noise reduction	Integration of steganography and steganalysis for enhanced security	Effective noise reduction improves data extraction	Complexity of model may impact performance
(Hayes & Danezis, 2017) [51]	Propose adversarial learning method with Alice, Bob, and Eve components	Alice creates steganographic images, Bob recovers secret message, Eve assesses probability of stego image	Active eavesdropping by Eve enhances security	Adversarial training improves model robustness	Complexity of model may increase computational requirements
(Wang et al., 2018) [52]	Introduce Self-supervised Steganographic GAN (SSteGAN) with Alice, Bob, Dev, and Eve components	Alice generates stego images, Bob decodes secret message, Eve classifies stego images, Dev competes against Alice	Self-supervised learning enhances model security	Use of input noise diversifies generated images	Increased computational complexity may impact performance
(Ali et al., 2022) [53]	Explore obfuscation techniques for privacy-preserving photo sharing	Investigate mosaicing, blurring, and P3 encryption for image obfuscation	Enhanced privacy in photo sharing; Improved security against unauthorized access	Increased privacy protection; Higher security for shared photos	Potential loss of image quality; Complexity of encryption methods
(Abbood et al., 2018) [54]	Develop cloaking methods to prevent unauthorized access to hidden information	Introduce complex algorithms and random methods for information hiding	Enhanced security against attackers; Robust protection of hidden data	Increased difficulty for attackers to access hidden information	Complexity of method may hinder usability; Potential impact on image quality
(Subramanian et	Classify deep	Categorize	Comprehensive	Provides insights	Complexity of

al., 2021) [55]	learning techniques for image steganography into three categories	methods as traditional, CNN-based, and GAN-based	overview of deep learning methods in steganography	into different approaches for image steganography	GAN-based methods; Limited explanation of traditional methods
(Kumar, 2017) [56]	Introduce a facial image steganography technique for secure message encoding	Develop CodeFace architecture for encrypting and decrypting hidden messages	High robustness in decrypting hidden messages; Secure message encryption	Conceals messages within facial images effectively	Potential degradation of image quality; Complexity of encryption and decryption
(Lin & Li, 2021) [57]	Present a cancellable face recognition scheme based on face image encryption	Employ FO Lorenz chaotic system for generating user-specific keys	Enhanced security with user-specific encryption keys	Protection against unauthorized face recognition	Impact on recognition accuracy; Complexity of encryption process
(Lawnik et al., 2022) [58]	Investigate chaotic image encryption algorithms for text encryption	Encode text message into image and apply specific image encryption algorithm	Secure text encryption using chaotic image encryption methods	Enhanced security for text encryption using image encryption	Potential impact on image quality; Complexity of encryption process
(Waykole & Sharma, 2022) [4]	Develop a method for hiding data within images for enhanced security	Use color images and digital bit modification methods for data hiding	Improved security with data hiding within images; Enhanced signal-to-noise ratio	Conceals data within images effectively	Potential impact on image quality; Complexity of encryption process

The review of relevant studies emphasizes how steganography approaches have evolved, especially with the use of DL methods. Progress in adversarial learning, generative steganography, and privacy-preserving obfuscation approaches are noteworthy contributions. To improve security and imperceptibility in steganography, researchers have looked into cutting-edge techniques including generative adversarial networks (GANs), self-supervised learning, and adversarial networks. Even though these techniques appear promising, further research is still needed to address issues including their complexity, vulnerability to attacks, and possible influence on image quality.

VIII. CONCLUSIONS

In conclusion, there are encouraging opportunities for development in the realm of steganography with the incorporation of deep learning (DL) techniques. Recent research has shown that DL-based strategies can be used to more effectively, robustly, and securely conceal information through digital media. Nonetheless, issues like complexity, scalability, and adversarial threats continue to exist, suggesting areas that need more research and development. To successfully solve these issues, future research efforts might concentrate on creating DL-based steganography models that are more reliable and effective. Steganography can develop into an essential method for enabling safe communication across numerous applications and domains by utilising DL's strengths. All things considered, adding DL to steganography has a great deal of promise to improve data security and privacy in the digital age. To fully realize this potential and reap the benefits of DL-powered steganography in protecting sensitive data during transmission, research and development activities must continue.

ACKNOWLEDGEMENT

The authors would like to thank University of Mosul for Support.

REFERENCES

[1] M. Ahmid and O. Kazar, “A Comprehensive Review of the Internet of Things Security,” *J. Appl. Secur. Res.*, vol. 18, no. 3, pp. 289–305, 2023, doi: 10.1080/19361610.2021.1962677.

[2] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014, doi: https://doi.org/10.1016/j.jcss.2014.02.005.

[3] A. M. Fadhil, H. N. Jalo, and O. F. Mohammad, “Improved Security of a Deep Learning-Based Steganography System with Imperceptibility Preservation,” *Int. J. Electr. Comput. Eng. Syst.*, vol. 14, no. 1, pp. 73–81, 2023, doi: 10.32985/ijeces.14.1.8.

[4] S. Waykole and A. Sharma, “Reversible Secured Data Hiding using Binary Encryption and Digital Bit Modification Scheme,” *Transdiscipl. J. Eng. Sci.*, vol. 13, pp. 101–118, 2022, doi: 10.22545/2022/00181.

[5] J. Zhou, X. Dong, Z. Cao, and A. Vasilakos, “Secure

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 79-89, March-2024
https://doi.org/10.47001/IRJIET/2024.803011

and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, pp. 1299–1314, Jun. 2015, doi: 10.1109/TIFS.2015.2407326.

[6] J. Domingo-Ferrer, O. Farràs, J. González, and D. Sánchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges," *Comput. Commun.*, vol. 140–141, pp. 38–60, May 2019, doi: 10.1016/j.comcom.2019.04.011.

[7] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, 1998, doi: 10.1109/49.668971.

[8] J. Mishra, "Video Steganography Techniques," *Int. Res. J. Eng. Technol.*, no. June, pp. 4694–4699, 2020.

[9] A. A., T. A., A.-H. Seddik, and S. M., "New Image Steganography Method using Zero Order Hold Zooming," *Int. J. Comput. Appl.*, vol. 133, no. 9, pp. 27–31, 2016, doi: 10.5120/ijca2016908016.

[10] M. A. Alsarayreh, M. A. Alia, and K. A. Maria, "A novel image steganographic system based on exact matching algorithm and key-dependent data technique," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 5, pp. 1212–1224, 2017.

[11] R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in DCT domain based on hamming and BCH codes," *37th IEEE Sarnoff Symp. Sarnoff 2016*, no. May, pp. 208–213, 2017, doi: 10.1109/SARNOF.2016.7846757.

[12] G. Rao, "Steganography Encryption Using Data," *Int. J. Comput. Electron. Asp. Eng.*, vol. 2, no. 3, pp. 57–60, 2021.

[13] R. J. M. and K. M. Elleithy, "Efficient and Robust Video Steganography Algorithms for Secure," no. April, 2017.

[14] R. J. Mstafa and K. M. Elleithy, "A DCT-based robust video steganographic method using BCH error correcting codes," *2016 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2016*, no. October 2017, 2016, doi: 10.1109/LISAT.2016.7494111.

[15] O. Ahmed and W. Abdullah, "A Review of Intrusion Detection Systems," *Acad. J. Nawroz Univ.*, vol. 6, no. 3, pp. 106–111, 2017, doi: 10.25007/ajnu.v6n3a91.

[16] M. Reddy and K. B. Raja, "Wavelet based Secure Steganography with Scrambled Payload," *Int. J. Innov. Technol. Explor. Eng.*, no. 2, pp. 2278–3075, 2012.

[17] R. Doshi, P. Jain, and L. Gupta, "Steganography and its Applications in Security," *Int. J. Mod. Eng. Res.*, vol. 2, no. 6, pp. 4634–4638, 2012.

[18] S. C.P, S. T, and U. G, "A Study of Various Steganographic Techniques Used for Information Hiding," *Int. J. Comput. Sci. Eng. Surv.*, vol. 4, no. 6, pp. 9–25, 2013, doi: 10.5121/ijcses.2013.4602.

[19] J. Ashok, Y. RAJU, S. Munishankaraiah, and K. Srinivas, "Steganography: an Overview," *Int. J. Eng. Sci. Technol.*, vol. 2, no. 10, pp. 5985–5992, 2010.

[20] K. Koptyra and M. R. Ogiela, "Distributed steganography in PDF files - Secrets hidden in modified pages," *Entropy*, vol. 22, no. 6, 2020, doi: 10.3390/E22060600.

[21] K. D. Abel, S. Misra, A. Agrawal, R. Maskeliunas, and R. Damasevicius, "Data Security Using Cryptography and Steganography Technique on the Cloud," *Lect. Notes Electr. Eng.*, vol. 834, no. 6, pp. 475–481, 2022, doi: 10.1007/978-981-16-8484-5_46.

[22] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: an overview," *Int. J. Comput. Sci. Secur.*, vol. 6, no. 3, pp. 168–187, 2012.

[23] A. Kumar and K. Pooja, "SteKumar, A., & Pooja, K. (2010). Steganography- A Data Hiding Technique. International Journal of Computer Applications, 9(7), 19–23. https://doi.org/10.5120/1398-1887ganography- A Data Hiding Technique," *Int. J. Comput. Appl.*, vol. 9, no. 7, pp. 19–23, 2010.

[24] H. Kaur and J. Rani, "A Survey on different techniques of steganography," *MATEC Web Conf.*, vol. 57, 2016, doi: 10.1051/matecconf/20165702003.

[25] S. Narang and A. Shrivastava, "Various Steganographic Approaches : A Review," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 3, no. Viii, pp. 444–447, 2015.

[26] A. Arya and S. Soni, "Performance Evaluation of Secrete Image Steganography Techniques Using Least Significant Bit (LSB) Method," *Int. J. Comput. Sci. Trends Technol.*, vol. 6, no. 2, pp. 160–165, 2018.

[27] Al-Jaber.S.M, "Council for Innovative Research," *J. Adv. Chem.*, vol. 10, no. 1, pp. 2146–2161, 2015.

[28] V. Surabhy, P. N. P, and T. Mahalekshmi, "Real Time Approach for Secure Text Transmission Using Video Cryptography," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 9, no. 3, pp. 120–125, 2020.

[29] S. Mangasuli and A. Nelli, "A Framework for Efficient and Secure Information Transform by using LSB and Diffie Hellman Algorithm," *Int. J. Eng. Res. Technol.*, vol. 7, no. 08, pp. 1–5, 2019.

[30] T. A. Al-Asadi, "A Novel Method for Image Steganography Based on Texture Features," *Eur. Acad. Res.*, vol. II, no. 1, pp. 193–203, 2014.

[31] Z. K. AL-Ani, A. A. Zaidan, B. B. Zaidan, and H. O. Alanazi, "Overview: Main Fundamentals for Steganography," *J. Comput.*, vol. 2, no. June 2014, pp. 158–165, 2010.

[32] J. Madison, S. D. Dickman, C. Forensics, and T. Paper, "An Overview of Steganography An Overview of Steganography," *IOSR J. Comput. Eng.*, vol. 11, no. July, pp. 15–19, 2007.

[33] S. H. Abdullah, "Steganography Methods and some application (The hidden Secret data in Image)," 2009.

[34] R. K. \Chawla, "Comparative Study on different Steganographic Techniques," *Int. J. Sci. Res. Manag.*, vol. 5, no. 06, pp. 5410–5414, 2017, doi: 10.18535/ijsrm/v5i6.08.

[35] D. K. Dake, G. K. Bada, and A. E. Dadzie, "Internet of Things (Iot) Applications in Education: Benefits

and Implementation Challenges in Ghanaian Tertiary Institutions," *J. Inf. Technol. Educ. Res.*, vol. 22, no. August, pp. 311–338, 2023, doi: 10.28945/5183.

[36] H. Westermann and H. Westermann, "Using Artificial Intelligence to Increase Access to Justice," no. March, 2023.

[37] M. M. Taye, "Understanding of Machine Learning with Deep Learning :," *Comput. MDPI*, vol. 12, no. 91, pp. 1–26, 2023.

[38] Y. Qian, J. Dong, W. Wang, and T. Tan, *Learning and transferring representations for image steganalysis using convolutional neural network*. 2016. doi: 10.1109/ICIP.2016.7532860.

[39] M. M. Taye, "Theoretical Understanding of Convolutional Neural Network: Concepts, Architectures, Applications, Future Directions," *Computation*, vol. 11, no. 3, 2023, doi: 10.3390/computation11030052.

[40] H. Sharma, "A Chronological Survey of Theoretical Advancements in Generative Adversarial Networks for Computer Vision," 2023, [Online]. Available: http://arxiv.org/abs/2311.00995

[41] G. Xu, H. Wu, and Y. Q. Shi, "Structural Design of Convolutional Neural Networks for Steganalysis," *IEEE Signal Process. Lett.*, vol. 23, p. 1, May 2016, doi: 10.1109/LSP.2016.2548421.

[42] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[43] M. Chaumont, *Deep Learning in steganography and steganalysis from 2015 to 2018 To cite this version : HAL Id : lirmm-02087729 Deep Learning in steganog- raphy and steganalysis from*. 2019.

[44] F. Tao, C. Cao, H. Li, B. Zou, L. Wang, and J. Sun, "Adversarial Attack for Deep Steganography Based on Surrogate Training and Knowledge Diffusion," *Appl. Sci.*, vol. 13, no. 11, 2023, doi: 10.3390/app13116588.

[45] B. Bashir and A. Selwal, "Towards Deep Learning-Based Image Steganalysis: Practices and Open Research Issues," *SSRN Electron. J.*, no. January, 2021, doi: 10.2139/ssrn.3883330.

[46] W. Tang, S. Tan, B. Li, and J. Huang, "Automatic Steganographic Distortion Learning Using a Generative Adversarial Network," *IEEE Signal Process. Lett.*, vol. 24, no. 10, pp. 1547–1551, 2017, doi: 10.1109/LSP.2017.2745572.

[47] H. Naito and Q. Zhao, *A New Steganography Method Based on Generative Adversarial Networks*. 2019. doi: 10.1109/ICAwST.2019.8923579.

[48] J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "HiDDeN: Hiding data with deep networks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11219 LNCS, pp. 682–697, 2018, doi: 10.1007/978-3-030-01267-0_40.

[49] Y. Ke, M. qing Zhang, J. Liu, T. ting Su, and X. yuan Yang, "Generative steganography with Kerckhoffs' principle," *Multimed. Tools Appl.*, vol. 78, no. 10, pp. 13805–13818, 2019, doi: 10.1007/s11042-018-6640-y.

[50] R. Meng, Q. Cui, Z. Zhou, Z. Fu, and X. Sun, "A Steganography Algorithm Based on CycleGAN for Covert Communication in the Internet of Things," *IEEE Access*, vol. 7, no. c, pp. 90574–90584, 2019, doi: 10.1109/ACCESS.2019.2920956.

[51] J. Hayes and G. Danezis, "Generating steganographic images via adversarial training," *Adv. Neural Inf. Process. Syst.*, vol. 2017-Decem, pp. 1955–1964, 2017.

[52] Z. Wang, N. Gao, X. Wang, X. Qu, and L. Li, "SSteGAN: Self-learning Steganography Based on Generative Adversarial Networks: 25th International Conference, ICONIP 2018, Siem Reap, Cambodia, December 13–16, 2018, Proceedings, Part II," 2018, pp. 253–264. doi: 10.1007/978-3-030-04179-3_22.

[53] S. S. Ali, J. H. Al'Ameri, and T. Abbas, "Face Detection Using Haar Cascade Algorithm," *Proc. - CSCTIT 2022 5th Coll. Sci. Int. Conf. Recent Trends Inf. Technol.*, no. Aece, pp. 198–201, 2022, doi: 10.1109/CSCTIT56299.2022.10145680.

[54] E. A. Abbood, R. M. Neamah, and S. Abdulkadhm, "Text in image hiding using developed LSB and random method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 4, pp. 2091–2097, 2018, doi: 10.11591/ijece.v8i4.pp2091-2097.

[55] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[56] S. S. Kumar, "A New Approach of Image Steganography Technique for Information Hiding using Nearest Filling Technique," no. January 2016, pp. 14–17, 2017.

[57] R. Lin and S. Li, "An Image Encryption Scheme Based on Lorenz Hyperchaotic System and RSA Algorithm," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/5586959.

[58] M. Lawnik, L. Moysis, and C. Volos, "Chaos-Based Cryptography: Text Encryption Using Image Algorithms," *Electronics*, vol. 11, no. 19, 2022, doi: 10.3390/electronics11193156.

Citation of this Article:

Anfal Shihab Ahmed, Melad Jader Saeed, "A Deep Dive into Deep Learning-Powered Steganography for Enhanced Security: Review" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 8, Issue 3, pp 79-89, March 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.803011

****