11

Surveying Modern Coverless Steganography: Stable Diffusion and Deep Learning Applications in Cybersecurity

Shaurya Chattopadhyay[1], Ayan Ghosh[1], Ayantik Ray[1] and Pabak Indu[1,2,3]*

[1]Department of CSE (AIML) & CSBS, Institute of Engineering and Management, University of Engineering and Management, Kolkata, West Bengal, India
[2]IEM Centre of Excellence for Cloud Computing and IoT, Institute of Engineering and Management, University of Engineering and Management, Kolkata, India
[3]IEM Centre of Excellence for Data Science, Institute of Engineering and Management, University of Engineering and Management, Kolkata, India

Abstract

With the growing threats of cyberattacks in our current digital landscape, the need for more secure ways of communication has never been greater.

To address this growing need, information hiding plays a pivotal role for providing security. Over the past few years, coverless steganography has proven itself as a frontier for hiding information. It uses text, audio, video, and image as a cover media to hide information. Researchers has adopted generative adversarial network, stable diffusion, and various deep learning–based approaches to implement coverless steganography. These new techniques make detection harder by current detection algorithms. This study is drawing a comparative analysis between the proposed solutions dealing with coverless steganography based on various parameters such as robustness, resilience, and embedding capacity.

***Keywords*:** Steganography, stable diffusion, pixel difference algorithm, hybrid techniques, generative adversarial networks (GANs), multimodal steganography, pixel value differencing

**Corresponding author*: pabakindu@yahoo.co.in

Shubham Mahajan, Kamal Upreti and Rashmi Agrawal (eds.) AI-Driven Cyber-Shield: Advances in Security, Cryptography and Blockchain, (275–308) © 2026 Scrivener Publishing LLC

11.1 Introduction

Today, the security of communication is one of the most essential tasks, due to the wide employment of online multimedia data transfer in channels that are not protected [5]. Steganography has nothing in common with cryptography, which involves the encoding of the data to make it unreadable but visible. Instead, steganography is the method of embedding the information into another object, including images, sound files, and videos, which allows the sender and the recipient to communicate in a way that is invisible to observers [9]. Traditional image steganography, although successful in hiding the secret data through the stego-image (SI) carrier, is often at the risk of distortion, which is detectable against different steganalysis techniques, although less complex [3]. Coverless steganography has become one of the new promising techniques in this digital era, and it remains one of the most fascinating areas. This allows secret information to be embedded with no perceptible change in the carrier, which makes it undetectable by conventional steganalysis methods [1, 4]. Basic image steganography is using elements from the image to carry away the information, and often, it causes a distortion and hence becomes vulnerable to the detection [3]. In contrast, coverless steganography is improved by factors whether mapping rules between image features and coverless secret data, or the synthesis of coverless secret data into textures so that the transmitted digital image file can be protected by a method related to image steganography [2].

Latest developments or accomplishments of deep learning (DL)–based steganography with the help of generative adversarial networks (GANs) show better resistance to steganalysis [2, 7]. Nevertheless, there are still some challenges such as the inability of the secret data to be accurately extracted due to the nonreversibility of generators [2]. Besides, the formation and usage of coverless image datasets (CIDs) are obligatory for the operation of these systems, the purpose of which being the capacity and the robustness [8]. Various innovative concepts include coverless steganography, combined with image transformation techniques, to send secret messages through a more secure medium [6]. For example, the application of camouflage pictures and convolutional neural network features can be used as an augmentation that protects against geometric attacks [3], whereas tactics such as secret-to-image reversible transformation technology can be utilized to achieve steganography by increasing hidden capacity and extraction accuracy [9].

The aim of this review will be to introduce and also come up with new ways to improve coverless steganography, emphasizing the robustness, capacity, and security of these methods, which are adaptable for use on different models and datasets [2, 8]. In the broader context of cybersecurity, the scene has an extraordinary amount of change in the recent past. Cybersecurity events have increased their technological finesse and have caused a leap in ransomware attacks, data breaches, and supply chain attacks. Among such cases are the 2017 WannaCry and SolarWinds events. The former is the randomness attack that has benefited from the gape of MS Windows, which has infected data on thousands of systems worldwide, and the latter is the SolarWinds supply chain attack of 2020, where hackers penetrate a major information technology management tool to seize precious data from a number of high-profile organizations.

This ever-evolving need for secure communication methods is brought about by the constant change in cyber threats, including advanced ones such as ransomware and data breaches [19]. Cybercriminals are increasingly making use of artificial intelligence (AI) and machine learning to automate the scale of these attacks, whereas the increased number of IoT devices introduces new points of vulnerability. It is in this line that with the rise of more cyberattacks, the growing demand is toward more robust and adaptable steganographic methods; in this regard, the development of coverless steganography might be seen as a need wherein secretly embedded data could face every challenge in the modern cybersecurity environment, where many threats are being seen, from such huge attacks such as WannaCry and SolarWinds [20].

The list of the biggest cyberattacks in the history is following, which gives us the opportunity to analyze each attack and to take some lessons from it:

1. **Marriott hotel data breach [19]**: In the year 2018, the Marriott hotel brand announced the occurrence of the tricky yet very serious problem on their network. This incident was mainly responsible for leakage of the personal data of as many as 500 million guests of the hotel. The threat has remained undetected in the firm's system for over a couple of years. The same was searched in 2018. A lot of such information as the name of the guests, their place of residence, passport number, etc., was stolen in the event. Almost 339 million visitor records might be affected worldwide, source indirect estimates. Just 2 years after, another way data breach that took the data of almost 5.2 million guests, which had

also been compromised, occurred. In addition to these violations, where the concerned party is operated by the Marriott hotel group, other attacks are also noted.

2. **The 2014 Yahoo attack [19]**: Having been the target of an attack sponsored by the state, Yahoo faced one of the most serious data breaches in the world when the attackers broke its walls of cybersecurity and got hold of 500 million accounts' information in 2014. Data such as names and emails have been stolen and were hacked by the ones who could get into the networks of the company. With respect to the exact course of the attack, no one knows the knowledge of it; however, there are suspicions among some that it may deal with a case when a Yahoo employee was scammed into clicking on some phishing malicious links. The hack took quite long due to the delay of processes as well as the significant amount of data stolen. Thus, the clients faced a much higher likelihood of falling victim to phishing scams and identity theft. Yahoo, after the data theft, decided to tell the clients to change their passwords, and the organization also invalidated the unencrypted security questions. Meanwhile, Yahoo was engaged in the peaceful transition of the transaction of the company with the acquiring company while the law enforcement was also examining and prosecuting the investigation. The consequence of this was $117.5 million, which Verizon Wireless' subsidiary had to shell out because of the lawsuit that claimed they failed to inform their consumers and the necessary authorities after being hit by hackers.
3. **Adobe cyberattack [19]**: Adobe, one of the top industrial giants in the world, released an official statement that a cyberattack in 2013 caused a huge data breach. Emails, credit card information, and encrypted passwords of more than 38 million clients were the objectives of the cloud services provider Adobe breach. On top of the harmless details of the users, the bad actors could silently and quickly access the source code of the Adobe software, such as Photoshop and Acrobat, and even use them for other purposes. As it became evident, the attackers found a way to bypass the system and steal information through the exploitation of the security protocols of Adobe that were weak. It is believed that the assault might have been executed by means of spear

phishing emails, which is a type of attack where the malicious senders try to reach the user with authentic-looking emails. An unnamed officer of Adobe confirmed that the company's first public address pointed to the drawbacks, but in practice, they were worse than initially thought.

4. **MOVEit [19]**: In May 2023, a zero-day security hole came to light on a file transfer program that was developed by Progress Software Corporation, the company that created MOVEit. The resulting vulnerability allowed illicit access to the MOVEit servers and the stolen dossier of all the customers. The vulnerability was utilized for many months by various hacker organizations, including a well-known C10p randomness gang. Some healthcare facilities were infected due to the fact that a Clop gang also assaulted some government agencies such as Boots and British Airways. Also, by September, a MOVEit cyberattack has been affecting almost 2000 companies including those companies that have approximately 60 million subscribers (such as airlines). This figure is still on the rise because the personal information of many more people has become exposed. The severity of the data breach, the amount of financial damage caused, and the consequences of the hack on the victims are only some of the multiple things that make this cyberattack one of the most thereby destructive ones ever to happen in history.

Existing problem of cybercrime development is graphically presented by Figure 11.1 where the forecast is depicted for the period from 2018 to 2027. It points out an enormous growth in cybercrimes in this period, which indicated the forms of cybercrimes, such as the use of complex data to commit new crimes, which are relentless and often occur. This upward trajectory is a clear indication of the rise in cybersecurity, which is caused by more factors such as the ubiquitous nature of IoT enabled devices, cybercriminals who are getting access to AI and machine learning that they are using to become more sophisticated, and the fact that infrastructure keeps getting more and more complex. The graph is a picture of the increased danger of cybersecurity attacks targeting the personal user and companies and the necessity to implement security measures and be mindful of security threats in the Internet era [11].

5. **Ukraine power grid attack [19]**: The Ukraine power grid attack has been identified as a cyberattack that was

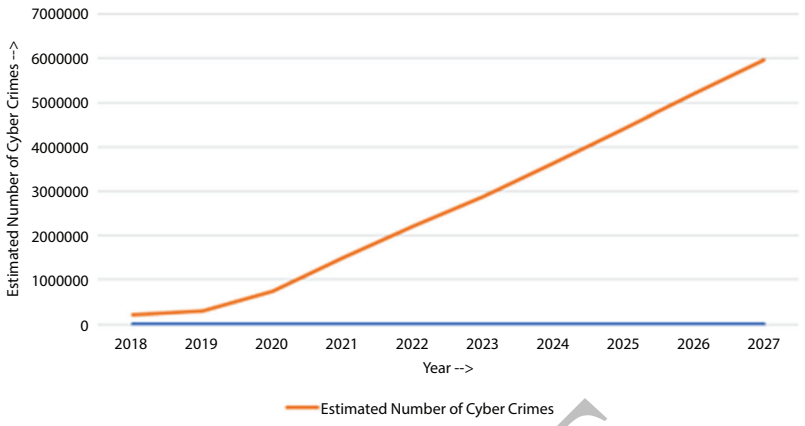

Figure 11.1 Estimated number of cybercrimes (2018–2027) [20].

successfully carried out, resulting in a power outage on a national grid, which is being referred to as the first. The attack was conducted in December 2015 and was focused on the western regions of Ukraine. It not only made customers numbering 230,000 in Ukraine lose the power supply but also was the reason that one-fifth of Kyiv's residents were left without electricity, as the attackers utilized malware to strike the power grid of the capital city. The issue was brought about by an advanced persistent threat group called "Sandworm," who took advantage of BlackEnergy 3 malware to forcibly take over the computer systems of Ukrainian power distribution utilities from a distance.

Since the outbreak of the Russo-Ukrainian War in 2022, there have been plenty of cyberattacks and also physical ones on the national infrastructure of Ukraine. The hack of the nation's Kyyivstar network, which was very recent, is an example of one of such infamous events. This led the network to be down for days and made it impossible for hundreds of thousands of Ukrainians to communicate. The hack is one of the biggest threats ever carried out by a cyber-criminal against an entire group or nation of people.

6. **The PlayStation network attack [19]**: The 2011 PlayStation Network data breach was an incident in which Sony's network was attacked taking advantage of the system vulnerabilities to gain access to around 77 million user accounts

illegally. The leak led to the release of various user names, physical addresses, email addresses, birth dates, and passwords (hashed with the help of cryptographic hash functions), and, in case, even the encrypted credit card data. The incident has also led to the suspension of PlayStation Network and Qriocity services by Sony on April 20, 2011, and the total downtime was around 23 days; hence, millions of users were prevented from accessing online services for PlayStation 3 and PlayStation Portable. Sony took a lot of heat from fans for not informing the incident in time and undertook various steps to secure the network; some measures were having the network rebuilt with better security, working with outside security companies, as well as offering affected users identity theft protection and credit monitoring services. Although many have speculated, no organization has been definitively implicated in the incident that still stands as one of the most significant and impactful data breaches in gaming history.

7. **The NASA cyberattack [19]**: In 1999, the NASA cyberattack was a notable incident in cybersecurity history, a brilliant but a 15-year-old kid named Jonathan James who exploited the gaps in NASA's Marshall Space Flight Center systems to get an unauthorized access. James launched a series of technical and social engineering attacks to open a backdoor, grab login details, and finally steal $1.7 million worth of software, which was used to control the International Space Station's environmental systems. The intrusion forced NASA to idle their computers for 21 days, which resulted in the loss of research and functionalities, and the cleanup of the system and the investigation are estimated to have cost $41,000. James became the first minor in the United States to be found guilty of a cybercrime, underscoring the necessity for strong cybersecurity protocols, even within major government agencies.
8. **The Mellissa virus [19]**: The Melissa virus was a code named March 1999 David L. Smith who launched a Word and Outlook users that virus was a fast-spreading macro. It was a self-replicating program that targeted users of Microsoft Word and Outlook by spreading through email attachments that were infected. The moment the receiver of the message opened the dangerous Word document, the virus would be

triggered, and it would by itself send copy to the first 50 persons in the address book of the victim's Outlook; thus, the result was a huge increase in email traffic; however, some and sometimes even the Ford Market and government email servers would go down, including those of the US Marine Corps and Microsoft. The fact is that Melissa did not damage files or steal information, but still its speed of spreading resulted in the disruption being widespread; consequently, many organizations were forced to shut down their email systems temporarily, and this has led to a loss of hundreds of millions of dollars. The outbreak revealed weaknesses in email security and macro-enabled documents, which, in turn, contributed to upgrading of antivirus software, the filtering of emails, and the raising of user awareness about the risks associated with opening unsolicited attachments.

11.2 Literature Review

Taking a look at some of the different steganography methods by each of the authors, we give a brief rundown of their methods and the differing approaches taken by them and make a comparison at the end.

End-to-end hash generation [1]: The process depicted in Figure 11.2 outlines a flow diagram where input data are processed through a series of interconnected modules for preprocessing, feature extraction, and hashing, ultimately producing a single hash value. This end-to-end hash generation system comprises four key stages: hash sequence creation, image index database construction, secret information embedding, and information recovery.

On the sender's side, the hash-based generation model is first trained. Following this, an image index database is established, linking hash sequences to corresponding images. During the information embedding phase, the secret data are separated into num segments, each of Length 1. For each part, the system searches the image index database to retrieve an image, which has a matching hash sequence to the part's value. These selected images, now referred to as SIs, are then transmitted to the receiver.

At the receiver's end, each SI is processed using the same hash generation model to generate a binary hash sequence. These sequences are subsequently combined to reconstruct the original secret information, such as a hidden message or image. The process depicted in Figure 11.2 outlines

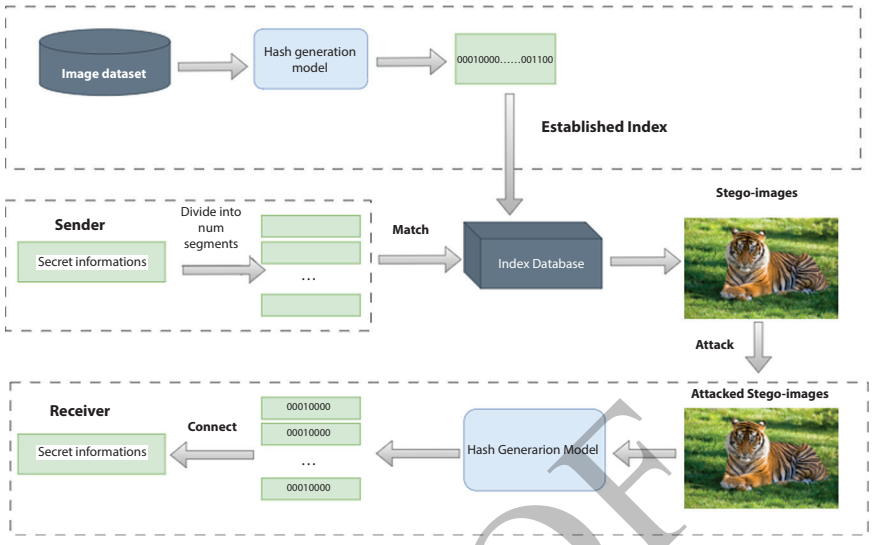

Figure 11.2 The framework of the proposed method for end-to-end hash generation.

a flow diagram where input data are processed through a series of interconnected modules for preprocessing, feature extraction, and hashing, ultimately producing a single hash value. This end-to-end hash generation system comprises four key stages: hash sequence creation, image index database construction, secret information embedding, and information recovery.

On the sender's side, the hash generation model is first trained. Following this, an image index database is established, linking hash sequences to corresponding images. During the information hiding phase, the secret data are divided into num segments, each of Length l. For each segment, the system searches the image index database to retrieve an image whose hash sequence matches the segment's value. These selected images, now referred to as SIs, are then transmitted to the receiver.

At the receiver's end, each SI is processed using the same hash generation model to generate a binary hash sequence. These sequences are subsequently combined to reconstruct the original secret information, such as a hidden message or image.

The image steganography has been transformed with the involvement of various DL techniques, especially the GANs. Various researches have indicated the GANs, which helps in producing the SIs of very high quality without affecting the hidden data [2, 5]. For some instance, the Wasserstein GAN with Gradient Penalty (WGAN-GP) is a well-known option in some

recent literature for its stability during the training and the capacity to generate realistic images [2]. Algorithms such as gradient descent algorithms have been investigated across the country by some researchers to optimize the data extraction processes and to recover the buried information precisely, even when the distortions are present [2]. The employment of camouflage images (CIs) to improve the information transmission invisibly in one of the recent developments [3] in the field of steganography. Now to guarantee the uniform distribution and efficient retrieval—two aspects that are very much essential for the real-world applications—researchers have created some preprocessing processes for image databases [3].

In real-world applications, these techniques are extremely relevant in secure communication networks, e.g., the military or financial institutions, where hidden data transmission are essential. The integration of GANs and steganography based on hashes facilitates inserting confidential information into seemingly harmless images, making it perfectly suited for situations where high confidentiality is needed. But drawbacks include the computational intensity of training GANs and hash models, which requires high resources, possibly restricting deployment to resource-limited devices. Moreover, dependence on big, well-curated image databases for hash matching is a scalability problem because keeping and updating such databases in real-time are costly. Robustness against sophisticated steganalysis tools, which can identify subtle anomalies in SIs, is an area of concern with the need to keep updating the model to avoid detection.

Techniques that make use of interframe similarities in video steganography have been developed to reduce the transfer of auxiliary transfer while increasing the capacity and the security [4].

On minimizing the supplementary information, which has also been addressed in the recent improvements to lower the chance of getting detected by steganalysis algorithms [1, 4], a complete strategy to make confidential and sensitive data, which combines steganographic methods with encryption techniques [1]. The integration of gradient descent algorithms such as GANs, which represent only a significant advancement in the search for effective and safe data concealing strategies [2] for information hiding. DL has been used to increase the concealing capacity and resilience of the traditional approaches such as least significant bit (LSB) replacement, pixel value differencing, discrete cosine transform [5, 6]. Nowadays, scholars have used the datasets such as ImageNet and CelebA to fascinate the efficient training and assessment, showcasing the promise of DL to manage the current obstacles in image steganography [6].

Covert communication through steganography [6]: Figure 11.3 outlines the progressive steps of an advanced steganography approach designed to embed a secret message within cover images. Unlike traditional methods that use an existing image as a carrier for hiding messages, this technique uses a generative network that takes the secret message and a latent input to produce SIs. This approach enhances security by evading common eavesdropping and steganalysis attacks. To address the risk of an attacker illegally obtaining and tampering with the SI during covert communication, an image transformation algorithm is introduced. This algorithm converts the SI into a different style, creating a CI that further protects the stego-content.

To ensure the integrity of the CI, an authentication picture (AuI) is generated by embedding authentication data into the CI. This provides a layer of security through obscurity: even if an unauthorized hacker gains access to the AuI and a secret retrieval tool, they cannot determine whether the SI has been altered without additional contextual information. This is critical because an attacker might still extract confidential messages from the AuI, whether it is authentic or tampered, without realizing the deception.

In practical applications, this advanced steganography method is highly beneficial in fields that require secure secretive communication, such as intelligence operations, secure journalism, or whistleblower communications, in which staying hidden is of utmost importance. Using generative models such as StarGAN to generate SIs and cover images enhances

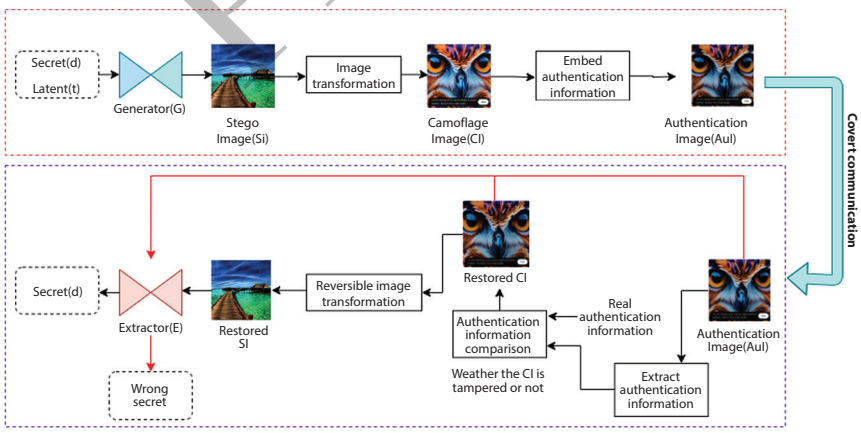

Figure 11.3 Framework of proposed model for covert communication through steganography.

security by making embedded information nearly impossible to differentiate from real images, thereby reducing the chance of being detected by steganalysis software. However, deployment challenges include the substantial computational costs of training and running generative models, perhaps limiting real-time capability on low-power hardware. Additionally, relying on complex algorithms for image modification and authentication increases the risk of error in message retrieval if not properly calibrated, while maintaining the integrity of large systems for generating and verifying AuI can be costly. The efficiency of the method also depends on the attacker lacking knowledge of the specific generative model or contextual information, which might not be guaranteed under sophisticated attacks .In addition, a new technique in paper number 7 is the combination of image selection with StarGAN to get over the restrictions of a traditional steganography through presenting the new cover images, hence the ascension in the capacity of encryption and also in the accuracy of extraction.

CIS novel coverless steganography method based on image selection and StarGAN [7]: Figure 11.4 depicts the flowchart of the proposed CIS novel method, which combines image selection and StarGAN for steganography. The process starts with selecting an initial image to serve as the base for embedding secret data. If the secret information is extensive, it is segmented into *N* parts, each divided into two portions: A and B, following a consistent methodology. Because the secret data's length may not divide

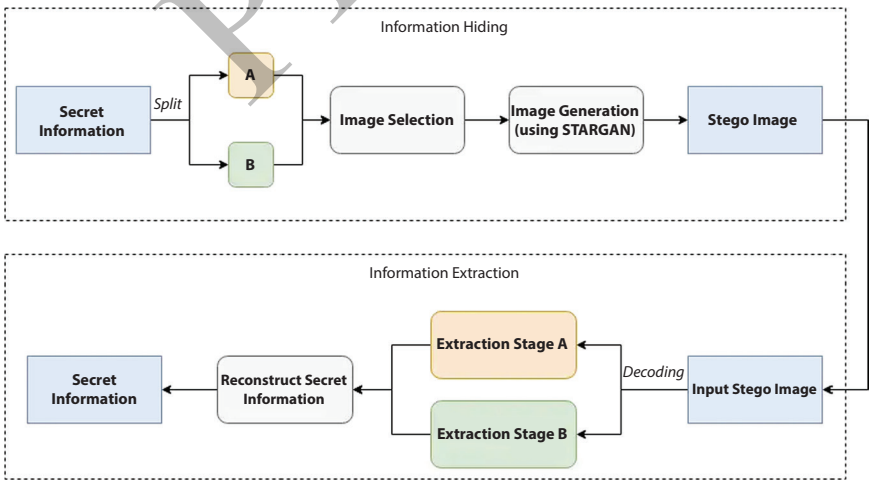

Figure 11.4 Flowchart of the proposed CIS novel coverless steganography method based on image selection and StarGAN.

evenly, the final image's embedding capacity may be reduced compared to earlier ones.

To increase the algorithm's adaptability, auxiliary information is embedded into a randomly chosen image from the database using the LSB technique or another steganography approach. As a result, the secret information is encoded across a series of coverless steganography images, plus one extra image holding the auxiliary data.

The receiver processes these images sequentially, first extracting essential details from the additional image and then retrieving the secret data from the others. Each segment shares the same embedding and extraction process. For demonstration, the segment "101111101111111110101011" is used as sample secret information in the detailed explanation that follows. In the A embedding phase, an appropriate image is selected to conceal Section A using the standard CIS method *via* image selection. In the B embedding phase, the image from A is processed by StarGAN to create an SI representing Section B.

The effectiveness of coverless steganography in the field of evading the conventional detection techniques has been emphasized. It does this by generating the SIs directly from secret data, thus omitting the need for the cover image [6, 9]. The secret information may be performed with huge capacity and accuracy by using the flow-based models such as Glow for reversible changes between latent vectors and pictures [9]. Reduction of noticeable alterations in cover images is achieved nationally by steganographic techniques, which use ML to optimize the distortion functions [9]. In real-life applications, the CIS algorithm paired with StarGAN has great promise for secure data transfer in use cases such as covert communications or intellectual property protection, as it does not require a classic cover image, minimizing detectability by steganalysis algorithms. The drawback of deployment is that StarGAN is computationally expensive, requiring a lot of processing power and time, and thus less ideal for real-time use or resource-constrained environments. The use of large, varied image databases to make efficient image selection and mapping possible in the method also brings scalability problems along with it, as curating and managing such a database may prove to be resource-heavy. Also, the security of the auxiliary image, which holds essential metadata, is a weakness, as its breach might render the entire data extraction procedure useless.

The emphasis has been placed on the effectiveness for CIDs made using high-dimensional feature extraction and unsupervised clustering methods [8]. The development of novel mapping and inverse mapping for the purpose of data extraction procedures has increased the steganography process's overall efficiency [2, 8].

Below is the comparison table, which encompasses the main features of nine works on coverless steganography. The pros of each paper, such as high accuracy, robustness, and efficiency, are set against the cons—the security risks, dataset dependence, and complexity. Generalizability, long-term security, and scalability are gaps in current knowledge underlined in the table. This gives the screenshot of the strengths and weaknesses for different steganographic approaches and areas, which need further research in this brief overview.

End-to-end image steganography using deep convolutional autoencoders [10]: This introduces a streamlined DL approach for concealing a secret image within a cover image through a unique autoencoder–decoder framework. In contrast to conventional steganographic methods that depend on statistical alterations (such as LSB substitution), this approach retrieves and combines essential characteristics from both images through a preprocessing module, minimizing redundancy and improving efficiency. It utilizes an embedding network to create an SI that closely resembles the original cover and an extraction network to recover the concealed image with minimal degradation. A tailored loss function maintains a balance between embedding and extraction precision. In real-world situations, this approach is particularly suitable for secure data transfer in domains such as digital rights protection and secret communications, because it attains high imperceptibility and strength, rendering SIs almost as indistinguishable from cover images as possible to human perceivers and steganalysis software. Its support for full-color RGB images with a hiding capacity of 1 increases its practicality for real-world applications involving considerable amounts of data hiding. However, challenges are posed by the extensive computational resources needed for training and deploying the autoencoder–decoder model, which may restrict its application to resource-limited settings such as mobile phones. Moreover, the performance of the method is greatly based on the quality and diversity of training data such as COCO, CelebA, and ImageNet, presenting scalability concerns in areas with limited exposure to such data. Overfitting risk to dataset specifics might also diminish generalizability, requiring constant retraining of the model to sustain resistance to changing steganalysis.

Assessed on datasets such as COCO, CelebA, and ImageNet, the model demonstrates excellent imperceptibility, robustness, and a hiding capacity of 1—substantially surpassing both classic and alternative DL approaches regarding peak signal-to-noise ratio (PSNR) and computational efficiency, even when secret content consists of full-color (RGB) images.

Secure medical image communication using fragile data hiding based on discrete wavelet transform and A_5 lattice vector quantization [11]: This research introduces a delicate watermarking technique aimed at safely embedding sensitive patient metadata, authentication codes, and images into medical images for telemedicine purposes, utilizing integer-to-integer discrete wavelet transform (IIDWT) and A_5 lattice vector quantization (LVQ). The technique allows for substantial data embedding while maintaining image quality, reaching PSNR values exceeding 53.88 dB and efficient detection of tampering *via* message authentication codes (MACs). It functions by converting medical images into subbands and incorporating data into wavelet coefficients through lattice-based quantization, guaranteeing resilience and invisibility without needing the original image for retrieval. In real-world applications, this technique is extremely useful in telemedicine and healthcare networks, where patient data transmission, including medical images and metadata, must be secure for remote diagnosis and patient confidentiality. The high values of PSNR ensure that data embedded do not affect image quality, which makes the system suitable for clinical applications, while the tamper detection feature through MAC increases confidence in data integrity. Besides, IIDWT and A_5 LVQ computational complexities can inhibit real-time processing on limited resources of medical devices, especially under rural or mobile healthcare environments. Its use of gray-scale images restricts its application to color medical imaging modalities such as magnetic resonance imaging (MRI) or ultrasound, calling for further adaptation for easier adoption. Moreover, the possible shortcomings of parameter exposure could be used against it if not secured adequately, and without clinical validation, regulatory approval may be extended for general utilization across healthcare infrastructures. Although providing 50% greater embedding capacity than similar techniques, drawbacks involve computational complexity, dependence on gray-scale images, and possible weaknesses in parameter exposure. The research enhances the transmission of secure medical data and suggests future avenues including color image extension, dynamic parameter adjustments, and clinical validation.

DL-based parameterization of diffeomorphic image registration for cardiac image segmentation [12]: This research presents an innovative DL framework that merges convolutional neural networks with diffeomorphic deformable image registration to attain precise and topology-preserving segmentation of cardiac structures from both two-dimensional (2D) and three-dimensional (3D) MRI scans. By forecasting radial and rotational deformation parameters, this approach allows for accurate manipulation

of segmentations, greatly enhancing metrics such as the Dice score and Hausdorff distance in comparison to leading-edge methods. Evaluated on three varied datasets (ACDC, Sunnybrook, and LA), it showed excellent segmentation precision, computational efficiency, and reliable volume estimation, indicating its appropriateness for clinical workflows. In real-world situations, this approach is most relevant in clinical applications for the automatic analysis of cardiac MRI with real-time accurate segmentation of cardiac anatomy, which can aid cardiologists in diagnosis and treatment planning for cardiac diseases with limited manual input. Its computational efficiency makes it a candidate to be embedded in imaging equipment found in hospitals, to reduce the time of diagnosis and improve patient outcomes. However, its use is constrained due to its susceptibility to dataset variations, which might limit generalizability across different patient populations or imaging situations, e.g., those threatened by motion artifacts. The demand for quality, annotated datasets, such as ACDC, Sunnybrook, and LA used in training, raises scalability concerns due to the resource requirements of acquiring and supporting such datasets. Also, the performance of the method may be compromised in complicated situations with large motion or anatomical variations, necessitating fine-tuning of parameters and possibly restricting its reliability in dynamic clinical settings. Although the approach demonstrates solid performance and stability, its ability to generalize could be constrained by variations in the dataset and sensitivity to parameters, particularly in intricate or motion-influenced scenarios. However, it represents an important progress in automated, real-time cardiac MRI assessment with limited human involvement.

Low-dose CT image synthesis for domain adaptation imaging using a GAN with noise encoding transfer learning [13]: This research introduces GAN-NETL, a DL system that uses GANs with noise encoding and transfer learning to generate authentic low-dose computed tomography (LDCT) images from normal-dose computed tomography (NDCT) scans across various scanners and noise levels. By distinguishing between content and noise characteristics, the model facilitates domain adaptation, which leads to better LDCT image production and improved efficacy of denoising methods. The model, which is trained on both public and private datasets, demonstrates enhanced image quality and structural integrity in comparison to current style transfer techniques, evidenced by metrics such as FID and SSIM. The elements of the architecture—content-noise separation, a preprocessing module, and custom loss functions—are assessed through ablation studies, verifying their contribution to generating clinically valuable LDCT images. In real-world applications, GAN-NETL is extremely

relevant in medical imaging, especially in radiology, where minimizing radiation dose through LDCT is essential for patient safety while ensuring diagnostic quality. Having the capability to generalize across scanners and noise levels makes it useful in hospitals having varied imaging equipment, possibly allowing LDCT imaging protocols to become standardized. Nonetheless, limitations are the model's dependence on paired NDCT-LDCT data, which cannot always be readily available, and hence scalability will be limited in resource-constrained environments. Computational overhead of GAN-NETL may discourage real-time applicability on generic clinical hardware, and extensive clinical verification may slow down regulatory clearance and application to everyday use. Moreover, heterogeneity of scanner-specific noise patterns may necessitate ongoing retraining to sustain performance with new equipment. Although the model demonstrates potential for decreasing radiation exposure and enhancing diagnostic quality, its dependence on paired data and requirement for extensive clinical validation are significant constraints. The framework enhances synthesis of medical images and domain adaptation, with possibilities for real-time incorporation in clinical procedures.

Toward generated image provenance analysis *via* conceptual-similar-guided-SLIP retrieval [14]: This research introduces compressed sensing (CS) SLIP, an innovative multimodal image retrieval system aimed at tracking the origin of AI-generated images by detecting possible reproduction from training datasets. By integrating visual attributes with textual direction, the approach uses self-supervised, contrastive, and conceptually similar-guided learning to obtain detailed representations. It utilizes CLIP and SLIP features for the initial search, improved by a re-ranking phase focused on cross-modal similarity. Evaluated on a carefully selected Danbooru2017 dataset, the framework greatly surpasses current methods in recognizing visually and semantically comparable source images, supporting copyright protection and authenticity validation. In real-world applications, CS-SLIP is extremely useful in digital forensics, content filtering, and intellectual property rights, especially when searching for the origins of AI-generated images on hosting user-generated content platforms, i.e., social networks or art platforms. Its capacity to trace generated images back to training datasets increases accountability and transparency in AI content generation, facilitating legal and ethical compliance. There are, however, challenges such as scalability constraints by the computational complexity of multimodal retrieval and re-ranking that could impede real-time deployment on large-scale platforms. Incomplete or low-quality textual captions within datasets can lower retrieval precision, and

the generalizability of the model across different datasets or domains is still limited, necessitating additional adaptation for extensive use. Furthermore, dependence on certain datasets such as Danbooru2017 does not necessarily respond to the intricacies of real-world image sources and thus requires constant dataset expansion and tuning. Despite ongoing issues with scalability, caption accuracy, and generalizability, the approach presents a hopeful avenue for digital content forensics and prospective studies in extensive and cross-domain provenance analysis.

SpineParseNet: **spine parsing for volumetric MR image by a two-stage segmentation framework with semantic image representation [15]**: This research presents SpineParseNet, a DL model aimed at precise, efficient, and interpretable multiclass segmentation of vertebrae and intervertebral discs (IVDs) from volumetric MRI scans. Integrating a 3D graph convolutional segmentation network with a 2D residual UNet, the architecture seizes spatial correlations among spinal components through semantic image representation and innovative region pooling/unpooling modules. SpineParseNet, trained on data from 215 subjects, attained impressive Dice scores (~87.5%) and surpassed baseline models in terms of accuracy, memory efficiency, and interpretability. The two-phase design harmonizes accuracy and resource consumption, rendering it appropriate for clinical application. In clinical use, SpineParseNet can prove highly beneficial in the clinic for computer-assisted evaluation of spinal MRI for facilitating precise segmentation of IVDs and vertebrae to support diagnosis and surgery planning for conditions such as disc herniation or spinal stenosis. Its memory efficiency and interpretability make it perfect to assist in integration with hospital imaging systems, which may speed up workflows and reduce radiologists' workload. Nonetheless, its deployment is compromised by its poor performance with unusual or incomplete spinal structures, potentially limiting precision in patients with unusual anatomies or very severe pathologies. Its basis on a training set of only 215 subjects might limit generalizability, requiring more extensive and varied sets to guarantee robustness for diverse populations. Moreover, implementing the model within current systems may necessitate substantial infrastructure upgrades and validation to ensure regulatory compliance, causing scalability and cost-related difficulties.

Although it excels generally, the model encounters challenges with rare or incomplete structures and might have difficulty with unfamiliar anatomical variations. However, it provides a solid basis for spinal assessment and surgical strategy, with possibilities for future improvements *via* expanded datasets, diverse inputs, and clinical incorporation.

Learning the regularization in dynamic contrast-enhanced MR image reconstruction for functional imaging of kidneys [16]: This research presents a neural network–based reconstruction technique tailored for individual patients, utilizing deep image prior (DIP) to improve the quality of undersampled dynamic contrast-enhanced (DCE) MRI kidney images, with the goal of maintaining temporal dynamics essential for precise functional evaluation. The approach uses a low-dimensional input that mirrors physiological contrast phases and integrates it with a dual-module neural network, thereby avoiding the necessity for extensive training datasets while proficiently minimizing artifacts and preserving clear temporal features. Evaluated on children's datasets, the method surpassed conventional CS techniques, demonstrating improved retention of dynamic contrast enhancement and a higher correlation with quantitative biomarkers ($R^2 \approx 0.94$). In real-life situations, this technique is very relevant in clinical practice, more so for pediatric nephrology, where high-quality noninvasive DCE-MRI imaging is important in evaluating kidney function without subjecting small children to high doses of radiation and contrast media. Reconstructability of high-quality images from reduced sampling leads to shortening of scan times, enhancing patient comfort and throughput in clinical radiology settings. Nonetheless, shortcomings are the heavy computational loads and increased reconstruction times, which might preclude real-time use in resource-limited clinical settings. The tuning dependency of the method might make standardization across varied populations or imaging modalities problematic and that limited large-scale validation outside pediatric data might slow broader use. Further, the computer hardware needed for the double-module neural network is not always available in smaller hospitals, and investment in equipment or cloud services may be necessary. Despite the longer reconstruction times and high computational demands, the approach provides a strong framework that can adjust to different acquisition circumstances and establishes a foundation for enhanced noninvasive renal imaging and wider dynamic MRI uses.

Principles of modern steganography and steganalysis [17]: This document offers a fundamental summary of contemporary digital steganography and steganalysis, detailing essential ideas, system elements, and security frameworks. It examines how steganography conceals secret messages within multimedia content (such as pictures or audio) so that they go unnoticed, whereas steganalysis seeks to uncover this concealed information. Two main design approaches are examined: altering natural materials with slight modifications and creating covers from the ground up. The section highlights adversary types (passive vs. active), criteria

for assessing detectability and robustness, and the compromises between capacity, stealth, and resilience. It emphasizes the significance of cover domain choice, theoretical modeling, and the influence of Kerckhoffs' principle in secure design. In real-world situations, contemporary steganography is very much usable in applications involving hidden communication, including national security, intelligence gathering, and secure data transfer in financial or journalistic industries where embedding sensitive information in multimedia can go unnoticed by opponents. Its use of embedding messages in commonly accepted formats such as images or audio makes it well-suited for digital media, and steganalysis aids forensic work in uncovering illegal communications. Nonetheless, challenges are the inability to find equilibrium between high embedding capacity and low detectability, because boosting capacity tends to reduce stealth. Practicality is hampered by the computational overhead of sophisticated steganographic algorithms, which might not be viable for real-time operation on limited-resource devices. Furthermore, steganalysis effectiveness against advanced steganographic techniques is reliant on access to sophisticated detection tools, which are not always available universally, and the absence of empirical testing in varied real-world situations restricts instant deployment. The dynamic nature of steganalysis techniques also creates the burden of a constant struggle, necessitating incessant updating of steganographic techniques to ensure security. Although the conversation is primarily theoretical, it highlights constraints such as idealized premises, absence of empirical proof, and difficulties in practical implementation, paving the way for upcoming studies on secure, resilient, and pragmatic steganographic systems.

Image camouflage by reversible image transformation [18]: This research presents a reversible image transformation method that allows for the secure concealment of a secret image within a visually akin target image, producing a CI from which the original can be flawlessly retrieved. Utilizing shift-based color alterations, tile rotation, and uneven clustering of image sections based on standard deviation (SD), the technique minimizes the amount of auxiliary data while improving visual quality. Experiments demonstrate notable enhancements in image similarity (increased SSIM, reduced RMSE) and effective lossless recovery of hidden images. The method also accommodates multiround alterations, allowing for the hiding of several images, although this is presently restricted by the embedding capability of reversible data hiding methods. In real-world situations, this invertible image transformation technique is extremely useful in safe image sharing, for example, in digital watermarking, copyright

Table 11.1 Comparison between some existing solutions.

Ref. no.	Embedding capacity (bpp)	Resilience	Methodology
[1]	3.05e−5 (8 bits ≈ 1 byte in 512 × 512 gray-scale image, 256 KB total)	High robustness for geometric (rotation, cropping: 83.9%–96.2%) and nongeometric attacks (JPEG: 98.2%, noise: high accuracy)	CNN (DenseNet-161 with spatial/channel attention)
[2]	0.3125 (1280 bits ≈ 0.16 KB in 64 × 64 gray-scale image, 4 KB total)	Strong for nongeometric attacks (JPEG, noise: >90%), weak for rotation (53.83%–67.19%) and large filtering (66.52%–82.19%)	GAN (WGAN-GP, DCGAN, SAGAN, BEGAN with gradient descent)
[3]	6.10e−5 (16 bits ≈ 2 bytes in 512 × 512 gray-scale image, 256 KB total)	Excellent for geometric attacks (rotation: 92%–100%, cropping: 84%–100%), moderate for noise (46%–85%)	CNN (DenseNet121 with k-means++ clustering)
[4]	2.20e−3 (9 bits ≈ 1.125 bytes in 64 × 64 frame, 4 KB total)	Strong for geometric (rotation: 97.7%, cropping: 98%–100%) and video attacks (frame deletion: 95.3%–96.9%), weaker for high-intensity noise (65.2%)	Non–deep learning (interframe similarity)
[5]	6.87e−5 (18 bits ≈ 2.25 bytes in 512 × 512 gray-scale image, 256 KB total)	Varies; GAN-based (CycleGAN, PSNR = 64.7) robust for image attacks, traditional methods reliable but less secure	Traditional, CNN (U-Net, VGG), GAN (DCGAN, WGAN, CycleGAN)

(*Continued*)

Table 11.1 Comparison between some existing solutions. (*Continued*)

Ref. no.	Embedding capacity (bpp)	Resilience	Methodology
[6]	1.56e−2 (1024 bits ≈ 0.125 KB in 256 × 256 gray-scale image, 64 KB total)	Lossless restoration (PSNR = Inf), resists tampering, not tested for specific attacks (e.g., noise, rotation)	GAN (StyleGAN2 with reversible transformation)
[7]	5.04e−4 (33 bits ≈ 4.125 bytes in 256 × 256 gray-scale image, 64 KB total)	Feature extraction robust (96.89%–100% for rotation, noise, filtering), network extraction weak (5.50%–41.00%)	GAN (StarGAN) with SIFT-based selection
[8]	~0.000061 bpp (16 bits/image for 512 × 512 images)	High: robust to image processing attacks (e.g., JPEG, noise, rotation), with 100% SAR for JPEG Q = 50, 90, and stable performance across datasets due to large intercluster distances	Deep learning (CNN-based): uses DCMH-CNN for deep hash extraction and k-means clustering for CID construction
[9]	4 bpp (practical, up to 16.2 bpp theoretical)	Moderate: SE-S2IRT is robust to intensity change, contrast enhancement, and sterilization (up to 1.00 accuracy), but weaker against JPEG, rotation, and strong noise (0.61–0.86 accuracy)	Deep learning (flow-based): uses Glow model for reversible S2IRT and SE-S2IRT schemes
[10]	24 bpp (100% payload for RGB secret image)	Low: high imperceptibility (PSNR ~34.55 dB), but no robustness testing against image attacks (e.g., JPEG, noise), limiting real-world applicability	Deep learning (autoencoder): uses lightweight convolutional autoencoder with preprocessing module

(*Continued*)

Table 11.1 Comparison between some existing solutions. (*Continued*)

Ref. no.	Embedding capacity (bpp)	Resilience	Methodology
[11]	0.77 bpp (>20 KB in 512 × 512 gray-scale image)	Low: fragile by design for tamper detection, not robust to attacks (e.g., JPEG, noise), but ensures integrity *via* MAC verification	Deep learning (wavelet-based): uses IIDWT and A_5 lattice vector quantization for fragile data hiding
[12]	Not applicable (captures radial and rotational transformation components for cardiac MRI segmentation)	High: robust to pathological variability, achieving Dice 0.92–0.98 and HD 0.35–3.25 mm across datasets, with reliable performance ($R(0.75) \approx 1.0$)	Deep learning (CNN-based): uses UNet-style CNN for diffeomorphic registration with radial/rotational parameterization
[13]	Not applicable (captures content and noise features for LDCT synthesis)	High: robust to domain shifts *via* two-stage transfer learning, achieving SSIM 0.9955, RMSE 0.0026, and FID 2.05 across datasets	GAN: uses GAN-NETL with noise encoding and transfer learning
[14]	Not applicable (captures visual and semantic features for cross-modal retrieval)	Moderate: handles lack of ground truth and stylistic variations (mAP 0.72, R@10 0.90), but limited by dataset specificity and computational cost	Stable diffusion + deep learning: uses stable diffusion for image generation and CS-SLIP for cross-modal retrieval
[15]	Not applicable (segmentation task)	Moderate; robust to interclass similarity and intraclass variation *via* GCNs, but limited by single-center dataset and poor T9–T11 performance	Deep learning: two-stage framework with 3D graph convolutional segmentation network (GCSN) and 2D residual UNet (ResUNet) (no GANs or stable diffusion)

(*Continued*)

Table 11.1 Comparison between some existing solutions. (*Continued*)

Ref. no.	Embedding capacity (bpp)	Resilience	Methodology
[16]	Not applicable (reconstruction task)	Moderate; robust to undersampling artifacts and generalizable without ground truth, but sensitive to phase clustering noise and small dataset	Deep learning: deep image prior (DIP) with fully convolutional and fully connected networks (no GANs or stable diffusion)
[17]	1% of cover size (0.01 bpp)	High; resistant to statistical steganalysis for low-capacity methods, but algorithm-dependent	Non–deep learning: general steganographic framework (e.g., LSB, transform-domain embedding) (no GANs, stable diffusion, or deep learning)
[18]	~0.6–0.7 bpp (accessorial information for 4 × 4 tiles)	Moderate; vulnerable to strong steganalysis, but secure against unauthorized access with AES encryption	Non–deep learning: reversible image transformation with mean-shift and k-means clustering (no GANs, stable diffusion, or deep learning)

protection, or secret visual communication in journalism or military missions, where hiding sensitive images inside visually identical covers provides security as well as lossless recovery. The excellent SSIM and minimum RMSE guarantee the camouflage picture looks natural, minimizing suspicion while transmitting. However, it poses challenges such as limited embedding capacity, limiting the number of images that can be embedded, especially for multiround changes. The effectiveness of the method is limited to images with comparable SD distributions, not allowing wide-ranging use on various or highly textured images. Extension of the technique to colored images or complicated transformations needs further extension, and computational expense of tiling rotation and clustering

Table 11.2 Strengths and limitations of some existing solutions.

Ref. no.	Paper name	Pros	Cons
[1]	A Robust Coverless Image Steganography Based on an End-to-End Hash Generation Model	1. Uses an innovative end-to-end CNN model to generate hash sequences efficiently and directly 2. Boosts robustness with attention mechanisms and adversarial training against various image attacks	1. Struggles with limited capacity as hash sequence variety drops with longer secret messages 2. Requires significant computational power due to complex CNN and attention mechanisms, slowing real-time use
[2]	A Robust Coverless Steganography Based on Generative Adversarial Networks and Gradient Descent Approximation	1. Offers a clever way to extract secret data using gradient descent with GANs, avoiding extra networks 2. Achieves high capacity and payload, hiding lots of data in images with great accuracy	1. Extraction can get stuck in local optima with some datasets, reducing reliability across all cases 2. Depends heavily on choosing the right initial noise values, which can cut capacity in half
[3]	A Robust Coverless Steganography Scheme Using Camouflage Image	1. Boosts robustness by using camouflage images and CNN features to resist various image attacks effectively 2. Offers flexible capacity settings, allowing users to adjust hiding ability without relying on strict mapping rules	1. Requires both sender and receiver to maintain a shared image database, increasing setup complexity significantly 2. Depends on clustering quality, where uneven results can weaken retrieval accuracy and overall performance

(*Continued*)

Table 11.2 Strengths and limitations of some existing solutions. (*Continued*)

Ref. no.	Paper name	Pros	Cons
[4]	A Robust Coverless Video Steganography Based on the Similarity of Inter-Frames	1. Enhances security by eliminating auxiliary information transmission, using a shared SCVD and mapping table instead 2. Achieves near-theoretical maximum effective capacity while resisting both image and video-specific attacks effectively	1. Relies on a large, shared video database, which could complicate setup and scalability for users 2. Robustness may drop with higher values, as distinguishing video differences becomes harder after attacks
[5]	Image Steganography: A Review of the Recent Advances	1. The paper provides a comprehensive review of image steganography, covering traditional, CNN-based, and GAN-based methods in detail 2. It includes valuable insights into datasets, evaluation metrics, and future research directions, aiding researchers effectively	1. The lack of a standardized benchmark dataset beyond BOSSBase limits consistent method comparison across studies 2. The paper highlights convergence issues in GAN-based methods, which may affect their practical reliability and performance

(*Continued*)

Table 11.2 Strengths and limitations of some existing solutions. (*Continued*)

Ref. no.	Paper name	Pros	Cons
[6]	Joint Coverless Steganography and Image Transformation for Covert Communication of Secret Messages	1. The proposed method enhances security by combining coverless steganography with image transformation, resisting eavesdropping and steganalysis effectively 2. It achieves high-quality stego-images with a PSNR of 31.78 and 100% secret message extraction accuracy, surpassing many existing methods	1. The complexity of integrating generative networks and image transformation may increase computational overhead, limiting real-time application feasibility 2. Dependence on specific datasets such as FFHQ and Bedrooms restricts generalizability, potentially reducing effectiveness across diverse image types
[7]	Novel Coverless Steganography Method Based on Image Selection and Star GAN	1. The method significantly increases hidden capacity to 33 bits using StarGAN, surpassing traditional CIS limits of 18 bits 2. It enhances security and robustness by generating high-quality stego-images resistant to statistical and deep learning steganalysis	1. The reliance on the CelebA database limits applicability to face images, reducing flexibility for other image types 2. Feature extraction accuracy drops to 95% with 20 attributes, indicating potential challenges with complex multiattribute scenarios

(*Continued*)

Table 11.2 Strengths and limitations of some existing solutions. (*Continued*)

Ref. no.	Paper name	Pros	Cons
[8]	Robust Coverless Image Steganography Based on Neglected Coverless Image Dataset Construction	1. The method enhances capacity by mapping high-dimensional deep hashes to low-dimensional secret messages efficiently 2. It improves robustness using unsupervised clustering, ensuring large feature domain distances for better resistance to attacks	1. Constructing a large coverless image dataset requires significant computational resources, potentially limiting practical scalability 2. The method's effectiveness relies heavily on the original dataset size, restricting capacity in smaller datasets
[9]	Secret-to-Image Reversible Transformation For Generative Steganography	1. The S2IRT scheme achieves high hiding capacity, up to 4 bpp, with near-perfect extraction accuracy 2. SE-S2IRT enhances robustness against common image attacks, maintaining reliable secret message recovery	1. The Glow model's reliance on small training datasets limits the quality of generated images 2. Both schemes exhibit reduced robustness to strong attacks such as JPEG compression and rotation
[10]	End-to-End Image Steganography Using Deep Convolutional Autoencoders	1. High hiding capacity with RGB image support 2. Lightweight and efficient end-to-end architecture	1. Fixed image size limits flexibility 2. Lacks robustness evaluation against compression or attacks

(*Continued*)

Table 11.2 Strengths and limitations of some existing solutions. (*Continued*)

Ref. no.	Paper name	Pros	Cons
[11]	Secure Medical Image Communication Using Fragile Data Hiding Based on Discrete Wavelet Transform and A_5 Lattice Vector Quantization	1. High embedding capacity with excellent image quality (PSNR > 53.88 dB) 2. Enables tamper detection and secure metadata embedding without requiring the original image	1. Computationally intensive due to complex lattice operations 2. Limited to gray-scale images; adaptation to color and real-world distortions is needed
[12]	Deep Learning Based Parameterization of Diffeomorphic Image Registration for Cardiac Image Segmentation	1. Achieves high segmentation accuracy with topology preservation and minimal computation time (~0.03 s) 2. Generalizable to both 2D and 3D cardiac MRI data, enhancing clinical utility	1. Relies on specific datasets, limiting generalizability to other imaging protocols 2. Sensitive to parameter tuning and image artifacts such as motion, requiring expert handling
[13]	Low-Dose CT Image Synthesis for Domain Adaptation Imaging Using a Generative Adversarial Network With Noise Encoding Transfer Learning	1. Effectively synthesizes high-fidelity LDCT images with controllable noise styles across different domains 2. Enhances downstream denoising performance and supports generalization using transfer learning and noise modeling	1. Depends on paired datasets, limiting use in scenarios where such data are unavailable 2. Generalizability may be affected by scanner variability and untested real-world clinical conditions

(*Continued*)

Table 11.2 Strengths and limitations of some existing solutions. (*Continued*)

Ref. no.	Paper name	Pros	Cons
[14]	Toward Generated Image Provenance Analysis *via* Conceptual-Similar-Guided-SLIP Retrieval	1. Effectively combines visual and textual features for accurate provenance detection of AI-generated images 2. Outperforms existing retrieval methods using innovative conceptual-similar guidance and cross-modal re-ranking	1. High computational and storage demands limit scalability on large datasets 2. Accuracy depends on the quality of automatically generated captions, which may not always be reliable
[15]	SpineParseNet: Spine Parsing for Volumetric MR Image by a Two-Stage Segmentation Framework With Semantic Image Representation	1. High segmentation accuracy and efficient memory usage, suitable for real-time clinical use 2. Graph-based modeling improves discrimination between anatomically similar spinal structures	1. Limited generalization for underrepresented or incomplete structures in the dataset 2. Performance may degrade on atypical anatomies or images with poor quality or resolution
[16]	Learning the Regularization in DCE-MR Image Reconstruction for Functional Imaging of Kidneys	1. Preserves crucial temporal dynamics in DCE-MRI without needing large training datasets 2. Achieves superior artifact suppression and quantitative accuracy compared to traditional CS methods	1. High computational cost with long reconstruction times (~5 h per dataset) 2. Limited generalizability validation due to small, pediatric-only cohort

(*Continued*)

Table 11.2 Strengths and limitations of some existing solutions. (*Continued*)

Ref. no.	Paper name	Pros	Cons
[17]	Principles of Modern Steganography and Steganalysis	1. Provides a thorough conceptual foundation for both steganography and steganalysis with clear system models and metrics 2. Highlights the critical balance between capacity, security, and robustness in covert communication design	1. Lacks empirical validation and real-world implementation insights. 2. Assumes ideal conditions that may not hold in practical or adversarial environments
[18]	Image Camouflage by Reversible Image Transformation	1. Enables lossless recovery of secret images with high visual quality in the camouflage output 2. Reduces auxiliary data through nonuniform SD-based clustering, supporting efficient reversible embedding	1. Performance declines when secret and target images have dissimilar SD distributions 2. Limited multiround transformation capacity due to RDH constraints and increased auxiliary data

may prevent real-time usage on resource-limited devices. Furthermore, robustness against sophisticated steganalysis software continues to be an issue, calling for ongoing improvement to ensure security. Although efficient for images exhibiting similar SD distributions, difficulties persist in managing texture variability, embedding capacity, and adapting to color images or more intricate transformations. The Table 11.1 shows the comparison between the working principle some existing solutions and Table 11.2 describes the strengths and limitations of those solutions.

11.3 Conclusion

The study explores a variety of steganographic methods that leverage AI and DL to enhance the security and the reliability of covert communication. With the advent of image generation capabilities using stable diffusion, it becomes possible to embed the data, which are sensitive and confidential inside AI-generated carrier images and videos in a way such that it must be visually indistinguishable from natural content, thereby evading detection and enhancing data security. To offer the secrecy of data, such approaches also show potential for data compression, serving dual roles in an efficient and secure information handling.

Through a complete survey, the paper highlights how coverless steganography method utilization techniques, such as GANs, hash generation models, image transformation and multimodal embedding, improve the robustness and adaptability of data hiding techniques. These methods outperform traditional approaches by resisting steganalysis and surviving attacks such as compression, noise addition, and geometric transformations. However, limitations still persist, particularly regarding dataset dependency, computational cost, and the vulnerability to strong image manipulations.

As cyber threats grow increasingly sophisticated with examples such as WannaCry, SolarWinds, and MOVEit, the need for resilient steganographic solutions is urgent. Coverless steganography, by generating various media from secret itself rather than modifying the existing carriers, offers a novel and secure alternative for future digital communication.

To unlock its full capacity, future efforts should prioritize improving scalability, adaptability to diverse datasets, and real-time efficiency. As research progresses, coverless steganography has the potential to emerge as a key component in cybersecurity, offering secure, undetectable, and high-capacity communication in an ever-more interconnected digital landscape.

AI disclosure statement: The author confirms that no artificial intelligence (AI)-generated content or AI-assisted writing tools were used in the preparation of this chapter (including summaries and the abstract). All text, analysis, and conclusions are the result of the author's original work.

References

1. Meng, L., *et al.*, A robust coverless image steganography based on an end-to-end hash generation model. *IEEE Trans. Circuits Syst. Video Technol.*, 33, 7, 3542–3558, 2022.
2. Peng, F., Chen, G., Long, M., A robust coverless steganography based on generative adversarial networks and gradient descent approximation. *IEEE Trans. Circuits Syst. Video Technol.*, 32, 9, 5817–5829, 2022.
3. Liu, Q., Xiang, X., Qin, J., Tan, Y., Zhang, Q., A robust coverless steganography scheme using camouflage image. *IEEE Trans. Circuits Syst. Video Technol.*, 32, 6, 4038–4051, 2021.
4. Meng, L., *et al.*, A Robust Coverless Video Steganography Based on the Similarity of Inter-Frames. *IEEE Trans. Multimedia*, 2023.
5. Subramanian, N., *et al.*, Image steganography: A review of the recent advances. *IEEE Access*, 9, 23409–23423, 2021.
6. Wen, W., Huang, H., Qi, S., Zhang, Y., Fang, Y., Joint Coverless Steganography and Image Transformation for Covert Communication of Secret Messages. *IEEE Trans. Network Sci. Eng.*, 2024.
7. Chen, X., *et al.*, Novel coverless steganography method based on image selection and StarGAN. *IEEE Trans. Network Sci. Eng.*, 9, 1, 219–230, 2020.
8. Zou, L., *et al.*, Robust coverless image steganography based on neglected coverless image dataset construction. *IEEE Trans. Multimedia*, 25, 5552–5564, 2022.
9. Zhou, Z., *et al.*, Secret-to-image reversible transformation for generative steganography. *IEEE Trans. Dependable Secure Comput.*, 20, 5, 4118–4134, 2022.
10. Subramanian, N., *et al.*, End-to-end image steganography using deep convolutional autoencoders. *IEEE Access*, 9, 135585–1355935, 2021.
11. Akhtarkavan, E., Majidi, B., Mandegari, A., Secure Medical Image Communication Using Fragile Data Hiding Based on Discrete Wavelet Transform and A&xxx2085; Lattice Vector Quantization. *IEEE Access*, 11, 9701–97155, 2023.
12. Sheikhjafari, A., *et al.*, Deep learning based parameterization of diffeomorphic image registration for cardiac image segmentation. *IEEE Trans. Nanobiosci.*, 22, 4, 800–807, 2023.
13. Li, M., *et al.*, Low-dose CT image synthesis for domain adaptation imaging using a generative adversarial network with noise encoding transfer learning. *IEEE Trans. Med. Imaging*, 42, 9, 2616–2630, 2023.
14. Xia, X., *et al.*, Towards generated image provenance analysis *via* conceptual-similar-guided-slip retrieval. *IEEE Signal Process Lett.*, 2024.
15. Pang, S., *et al.*, SpineParseNet: spine parsing for volumetric MR image by a two-stage segmentation framework with semantic image representation. *IEEE Trans. Med. Imaging*, 40, 1, 262–273, 2020.

16. Koçanaoğulları, A., *et al.*, Learning the regularization in dce-mr image reconstruction for functional imaging of kidneys. *IEEE Access*, 10, 4102–41115, 2021.
17. Böhme, R., Principles of modern steganography and steganalysis, in: *Advanced Statistical Steganalysis*, pp. 11–77, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.
18. Hou, D., Zhang, W., Yu, N., Image camouflage by reversible image transformation. *J. Visual Commun. Image Represent.*, 40, 225–2365, 2016.
19. https://em360tech.com/top-10/top-10-most-notorious-cyber-attacks-history (accessed on 25th July, 2024).
20. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/ (accessed on 25th July, 2024).