International Journal of Digital Crime and Forensics
Volume 15 • Issue 1

Latest Trends in Deep Learning Techniques for Image Steganography

Vijay Kumar, Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, India*
Sahil Sharma, Jaypee University of Information Technology, India
https://orcid.org/0000-0002-6694-3365
Chandan Kumar, Amrita Vishwa Vidyapeetham, Amaravati, India
Aditya Kumar Sahu, Amrita Vishwa Vidyapeetham, Amaravati, India
https://orcid.org/0000-0003-4257-0688

ABSTRACT

The development of deep convolutional neural networks has been largely responsible for the significant strides forward made in steganography over the past decade. In the field of image steganography, generative adversarial networks (GAN) are becoming increasingly popular. This study describes current development in image steganographic systems based on deep learning. The authors' goal is to lay out the various works that have been done in image steganography using deep learning techniques and provide some notes on the various methods. This study proposed a result that could open up some new avenues for future research in deep learning based on image steganographic methods. These new avenues could be explored in the future. Moreover, the pros and cons of current methods are laid out with several promising directions to define problems that researchers can work on in future research avenues.

KEYWORDS

Container Image, Cover Image, Deep Learning, Information Hiding, Secret Image, Steganalysis, Steganography

1. INTRODUCTION

Steganography refers to hiding secret information inside some cover, and steganalysis refers to recovering the secret information. Steganography has been around for thousands of years. The word steganography roughly translates to secret writing. Since the first modern human settlements, there has been a demand for private and secure communication channels so that one person can send a message to another so that no one else can know that the message even exists. In the past, most secret messages were military-related; therefore, no one needed to discover the presence of the message. As the danger of discovery was great, they used various extreme methods like writing messages on

DOI: 10.4018/IJDCF.318666
*Corresponding Author

someone's scalp and then waiting for hair to grow up and hide the message, writing the message on silk and then compressing it into a ball covered with wax and writing the messages on wooden tables and covering them with wax.

In more recent history, during world wars, Nazis used microfilm chips the size of a standard typewriter that could hold pages worth of information, drawings, etc. Some used invisible inks, null ciphers, and many other methods.

With the exponential growth of the internet and the world wide web in the last decades, there are a lot of questions and worries about users' privacy. Personal private information of users is being stolen, spread, snooped on, and so on. The demand for steganography is now more than ever. We no longer have to fear tyrant kings and cruel military personnel, but that doesn't solve the problem. Now we have multinational companies recording our every activity over the internet, and there's also the problem of random bad actors trying to get our personal information. With so much private data being created daily, it could negatively affect people's lives if it falls into the wrong hands (Kerry, 2018). There's an urgent need for Information hiding, and researchers are taking notice. Steganography has become one the most popular methods for information hiding because of its simplicity and easy communication through already existing technology and communication channels like IP cameras, smartphones, and social media apps like WeChat, WhatsApp, Telegram, Signal, etc. without any extra cost of additional infrastructures like private key sharing or private communication channels, etc. There have been various works which have not included deep learning in their work, however, have contributed in the field of watermarking and steganography (Hassaballah *et al.*, 2020; Gutub and Al-Ghamdi, 2020; Gutub and Al-Roithy, 2021; Hassan and Gutub, 2021; Al-Roithy and Gutub, 2021; AlKhodaidi and Gutub, 2021; Hameed, Abdel-Aleem and Hassaballah, 2022; Gutub, 2022a, 2022b).

With the rise of deep learning algorithms, steganography has also taken a step forward. Various deep learning algorithms provide a better, more efficient approach to achieving the desired results. But the rise of deep learning has also been counterintuitive to achieving reliable and robust image steganography results since there are just as many deep learning-based steganalysis algorithms. Steganography and steganalysis play a push-and-pull game. Because of the recent improvements in the steganalysis algorithms using deep learning, it is imperative that the steganographic techniques also catch up and provide better robust and reliable results that can avoid steganalysis.

There are basic Image steganography techniques that have been around for some time. Like the Least Significant Bit (LSB) encoding steganography in which the least significant overwritten by the secret message bits or the Masking and Filtering technique in which watermarks are inserted on top of grayscale or RGB Images or the Shift encoding techniques like the Line Shift Coding and Word Shift Coding. A few of these techniques work well under certain circumstances. Hinton and Salakhutdinov (Hinton and Salakhutdinov, 2006) worked on unsupervised pre-training methods proposing optimization of the initial network weight values and then fine-tuning the weights. It is considered the starting point of using deep learning algorithms in steganography. Much research and experimentation took place after that, and various deep-learning algorithms revolutionized the Steganography process. They work exceptionally well than the basic methods as they have certain advantages and problems over the basic techniques, as discussed in the following sections (Hiwe and Nipanikar, 2014).

This paper lays out a comprehensive review of various deep learning algorithms used or could be used in achieving Image Steganography. Different tactical foundations of image steganographic methods are analyzed to rank and review their performances, strengths, and shortcomings.

The contributions of the current work are as follows:

1. To discuss the deep learning-based works in the field of image steganography.
2. To present the comparative analysis of various techniques.
3. To discuss the literature about GANs, Autoencoders, Reinforcement Learning, Attention-based models, and CNNs.
4. To present the future research directions.

The outline of the paper is as follows. The literature review has been presented with the background discussion about the deep learning methods in Section 2. Followed by subsequent subsections discussing the literature about GAN based, autoencoder-based, reinforcement learning-based, attention-based, and convolutional neural networks based image steganography. The future research directions have been presented in Section 3 and the conclusion has been presented in Section 4.

2. LITERATURE REVIEW

2.1 Background

Deep learning algorithms can be subdivided into supervised learning, Unsupervised learning, and Reinforcement learning.

2.1.1. Supervised Learning

The label and characteristic values are passed using the input data in supervised machine learning techniques. The network is trained iteratively by considering the error between the output values and the label values of the network. In supervised learning, regression and classification are the problems that need to be solved. The image classification research field is a researcher's primary experimental ground as it is an essential classification task.

The development of convolutional neural networks like VGG (Simonyan and Zisserman, 2014) and ResNet (K. He *et al.*, no date) was a direct result of a classification of thousand categories on ImageNet (Russakovsky *et al.*, 2015). Convolutional Neural Networks (CNN) and Deep Belief networks (DBN) are taking hold are popular supervised machine learning techniques. A machine learning technique proposed by (Huang, Zhu and Siew, 2006) is based on feedforward neural networks named Extreme learning machine used for prediction.

2.1.2. Unsupervised Learning

In unsupervised machine learning techniques, it is the machine's job to find common features, correlations, and structures between the input data characteristic values. Various unsupervised learning algorithms focus on how to manage the environment to get better results, like the auto-encoder method (Kingma and Welling, 2013), the deep Boltzmann machine (Montavon and Müller, 2012), and the widely popular generative adversarial networks (GAN) (Goodfellow *et al.*, 2020).

2.1.3. Reinforcement Learning

Another method focuses on maximizing the expected benefits by acting on the environment, known as Reinforcement learning (Mnih *et al.*, 2015). Deep learning has been flexing its muscle in all the following fields with enormous amounts of research work by professionals. Various researchers put forward various ideas to do operations on video files for steganography purposes in the field of video steganography. The field of image steganography (T. He *et al.*, 2019; Wang and Chan, 2018; Barz and Denzler, 2019) showed various methods to operate on images using deep learning. In the semantic understanding field, methods suggested in (Zhuang *et al.*, no date; Qin *et al.*, 2018; Sanh, Wolf and Ruder, 2019) theorize various ways to achieve information hiding in plain sight. These methods are further extended to the object detection research area (Roddick, Kendall and Cipolla, 2018; Jaeger *et al.*, 2020). Image forensics deep learning methods are put forward by (Yu *et al.*, 2017; Cui, McIntosh and Sun, 2018).

Image classification methods in the supervised machine learning field are maturing. They can now be applied for object detection to detect the categories of objects like vehicles, people, leaves, and dogs in digital videos, images, and frames. Image retrieval is another one of the possible functions of supervised machine learning methods. Some of the most commonly used object detection methods based on deep learning are as follows.

Table 1.
Various deep learning-based object detection methods

Year	Citation	Method
2015	(Ren *et al.*, 2015)	Faster R-CNN
2016	(Dai *et al.*, 2016)	Region-based Fully Convolutional Networks R-FCN
2016	(Redmon *et al.*, 2016)	You Only Look Once(YOLO)
2016	(Liu *et al.*, 2016)	Single Shot Multibox Detector(SSD)

2.2 Related Works

2.2.1. Generative Adversarial Networks

Convolutional neural networks can handle object detection tasks better than traditional methods and recognize features more efficiently. Moving onto the unsupervised machine learning techniques, the Generative adversarial network (GAN) is the clear leader of the whole method. The GAN models have the basic principle of a generator and Discriminator. A generator's job is to get the data from a training dataset and generate "natural" data. A generator requires consistent distribution of the original data. The job of a discriminator is to determine whether the provided data is natural, i.e., whether a machine has generated the data. This plays very well into image steganography and image steganalysis approach as the Generator has a similar function. A discriminator can be assumed as an image steganalysis approach. GAN networks are popular in image, language, vision, and video processing. GAN networks can also be used with reinforcement learning.

A solution to the unstable GAN training called Wasserstein GAN (WGAN) (Arjovsky, Chintala and Bottou, 2017) optimizes the GAN. It ensures diverse generated samples, introducing a cross-entropy function to mark the training process. WGAN also uses multi-layered neural networks to complete the training without the need to design a specific network structure. A newer model optimizes the GAN discriminator using a non-saturating and much smoother gradient loss function, known as Least squares GAN (LSGAN) (Mao *et al.*, no date). Another improvement to GAN, known as boundary-seeking GAN, is that discrete outputs can be used to train generators (Hjelm *et al.*, 2017). Another addition to this network was using corresponding output followed by a logarithmic function to get low variance results. This structure is known as Maximum-Likelihood Augmented Discrete GAN (Che *et al.*, 2017). Mode-regularized GAN (Che *et al.*, 2016) acts in the early stages of training to achieve fair data generation and probability quality distribution. It provides a solution to missing a mode problem. (Brock, Donahue and Simonyan, 2018) proposed a method to achieve high-resolution results. More and more research papers focus on reducing the transferring loss between the two transformation targets. The latest image-style transformation research proposed GAN based design (Karras NVIDIA and Laine NVIDIA, no date; Yi *et al.*, no date; Zhu *et al.*, no date; Kim *et al.*, 2017).

The abovementioned deep learning-based approaches of image steganography have been successful on many fronts and attracted much attention from researchers and scholars. However, there are still limitations to these existing methods, as presented in the following table.

The GAN structure completely corresponds to the Image Steganography and Image Steganalysis structure. The generation network in the GAN structure can be considered the Image Steganography part, and the discrimination network coordinates to the Image Steganalysis structure. Researchers have noticed this and have been acting accordingly and applying GAN networks for Image Steganography approaches. GAN makes image Steganography methods more robust and safer. Hidden, hard-to-detect, concealed stego-images are generated.

These algorithms have been derived considering the widespread information security game of Alice, Bob, and Eve game, i.e., Alice and Bob are communicating with each other by sharing the secret images hidden inside container images, Eve eavesdrops on their conversation and gets the

Table 2.
Various deep learning GAN-based image steganography techniques

Authors	Year	Pros	Cons
(Yuan *et al.*, 2022)	2022	● Multiple loss functions and Wasserstein GAN are used for enhancing stability.	● The dataset scalability has not been tested.
(*Steganography GAN: Cracking Steganography with Cycle Generative Adversarial Networks | DeepAI*, 2020)	2020	● Used Cycle Generative Adversarial Networks (CycleGANs) and Bayesian Optimization to break the Least Significant Bit (LSB) steganography algorithm and compare the use of CycleGANs to that of Convolutional Autoencoders.	● GANs take time to be trained and have higher amount of time complexity from the implementation point of view.
(Goodfellow *et al.*, 2020)	2020	● Image synthesis is achieved using a GAN model for the first time. ● This technique is still widely used for image generation.	● It is complicated to implement image steganography because it isn't very easy to implement because the images are created, and then secret information is embedded into them.
(Volkhonskiy, Nazarov and Burnaev, 2020)	2020	● This method proposed an architecture not only considering the credibility of constructed stego images but also for the credibility of constructed stego images and also providing a defense against the steganalysis algorithms.	● The images constructed using this method are twisted in semantic order drawing the attention of steganalysis and attackers, which is a major drawback considering steganography's steganography's main objective is to avoid attention.
(Ke *et al.*, 2019)	2019	● Embedded messages are created by the generator network instead of encoding secret messages in a cover image.	● It needs a private key to be shared using a secure network restricting the applications of GSK.
(Zhang *et al.*, 2019)	2019	● It achieved 4.4bpp of embedding capacity, about 10 ten folds higher than any other deep learning-based framework. ● The proposed model can work with different different-sized cover images.	● The paper did not compare numerically with other images of steganographic deep learning models. ● The model can only be applied to spatial image steganography.
(Shi *et al.*, 2018)	2018	● It used Wasserian GAN instead of DCGAN, resulting in faster network training. ● It improved the convergence speed to be more secure and fast.	● It follows the same approach as Goodfellow's, i.e., generating images and embedding secret messages, making it complex.
(Hu *et al.*, 2018)	2018	● The first ever proposed model exploiting the GAN mechanism to create stego images without any alterations. Achieved high security.	● The recovery of secret messages from the received stego-image encounters problems. ● The small size of the stego image results in low embedding capacity.
(Yang *et al.*, 2018)	2018	● The proposed model fits the optimal embedding simulator using the TanH activation function. ● The model is faster than ASDL-GAN.	● This model's low embedding capacity can only be applied to spatial domain steganography.
(Tang *et al.*, 2017)	2017	● This model proposed a simultaneous steganographic generator network and steganalysis discriminator network attaining good performance.	● Less secure and low secret message holding capacity. ● The network needs a lot of time and computational power to be pre-trained.

container image and is judging whether the image has any secret information inside of it or not. In this scenario, all three characters are neural networks trying to achieve the best results. Eve is a steganalysis actor as a discriminator, Alice is the Generator, and Bob is the extractor. The Generator,

i.e., Alice generates the stego-container image based on the feedback from the Discriminator, i.e., Eve. The extractor i.e., Bob gets the information on the bits from the container image.

Steganography's specific GAN network structure is also known as Steganographic Generative Adversarial Networks (SGAN) (Volkhonskiy, Nazarov and Burnaev, 2020). In SGAN, another Discriminator is added to do steganalysis based on GAN, known as steganalyzer. The steganalyzer is used to detect and judge whether there's any secret information in the container image. This approach makes the information hiding more secure by reducing the detection rate of the steganalysis.

Compared with the classic methods of image steganography, deep learning-based methods have better performance. Using GANs to generate stego-images directly allows the model to complete the whole process of image steganography in one step. However, training a GAN model can be complicated and carry a set of errors. In case of any errors in training, the information cannot be extracted correctly. The model structure is highly complex for image steganographic models based

Figure 1.
Comparison between steganography, steganalysis, and GAN structures

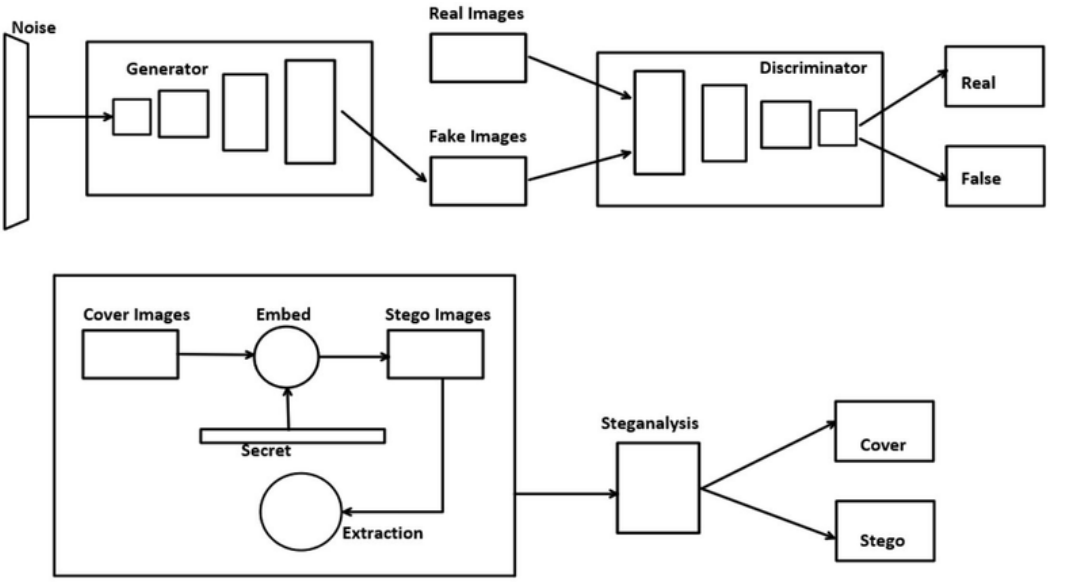
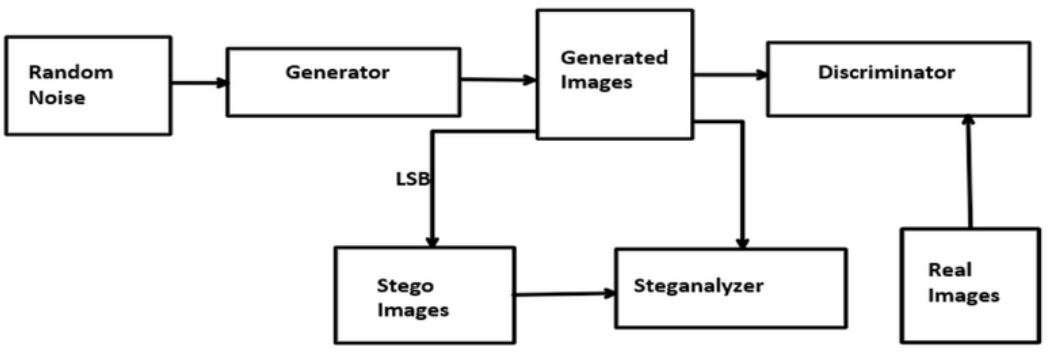


Figure 2.
The structure of SGAN



on generative adversarial networks, requiring more time to complete embedding and a high need for hardware resources due to more computational needs. To achieve acceptable image steganography results in low-configuration terminals, the embedding efficiency of the model needs to be taken seriously.

Challenges in image steganographic frameworks based on Deep Learning GANs

The results achieved by methods based on GAN architectures can be very impressive, but it is challenging to train a stable GAN network. In the following bullet points, this paper discusses the challenges and issues researchers might face while training GAN architecture-based models.

1) **Unstable Convergence:** The parameters used to train the model are always changing and are never in a stable form fluctuating, diminishing, and never converging over the training period. Convergence is a problem that comes up in theory and practical implementations of the GAN mode. Researchers have proposed several solutions to tackle this problem (Nowozin, Cseke and Tomioka, 2016; Mescheder, Nowozin and Geiger, 2017; Guo *et al.*, 2021).
2) **Mode Collapse:** This occurs when there is insufficient versatility in the samples produced by the GAN model Generator from the real data distribution. Many GAN architecture-based models encounter this problem. Mode collapse can be further subdivided into two subparts.
    a) Some modes present in input data are missing from the generated data.
    b) The Generator learns only a small subset of the original modes.

The major issue behind the mode collapse problem could be an ill-suited objective function. To encounter this problem, various variants of GANs have been proposed, which sometimes focus on either modifying Discriminator's objective (Larsen *et al.*, 2016; Tran, Bui and Cheung, 2018) or modifying the Generator's aim (Guo *et al.*, 2021).

3) **Diminished Gradient:** This problem sometimes occurs during the training of the network. The discriminator network returns acceptable training results, but the generator network learns nothing as it faces gradient vanishing problems. This unbalance between discriminator and generator networks ends up overfitting the model. This overfitted model is highly sensitive to selections of hyperparameters.

2.2.2 Autoencoder Based Steganographic Algorithms

A safe, robust JPEG steganographic system based on an autoencoder with adaptive BCH (Bose-Chaudhuri-Hocquenghem) encoding was proposed by Lu et al. (Lu *et al.*, 2021). Specifically, the autoencoder is initially pretrained to match the transformation connection between the JPEG picture before and after compression, as determined by the compression channel. In addition, the BCH encoding is applied adaptively based on the cover image's content to reduce the error rate of secret message extraction. In order to quickly adjust to new input data while yet maintaining a high level of restoration accuracy, Progonov (Progonov, 2021) suggested using autoencoders, a distinct kind of neural network. This research focused on evaluating the efficacy of shallow denoising autoencoders for spotting stego images created with sophisticated embedding techniques.

Image DisEntanglement Autoencoder for Steganography (IDEAS) steganography without embedding (SWE) approach was presented by Liu et al. (Liu *et al.*, 2022). This method is essentially resistant to standard steganalysis assaults because, rather than immediately embedding the secret information into a carrier picture, information was disguised by changing it into a synthesised image. Separating an image's structure and texture into their own representations allowed to increase synthesis variety by randomising texture representations and improve steganography security by exploiting the stability of structure representation to facilitate secret message extraction. Subramanian et al. (Subramanian *et al.*, 2021) proposed a light-weight yet simple deep convolutional autoencoder architecture to embed a secret image inside a cover image as well as to extract the embedded secret image from the stego-image.

The proposed method has been evaluated using three datasets – COCO (*COCO - Common Objects in Context*, no date), CelebA (*CelebA Dataset*, no date), and ImageNet (Deng *et al.*, 2010).

2.2.3. Reinforcement Learning Based Steganographic Algorithms

Tang et al. (Tang *et al.*, 2021) presented a novel embedding cost learning system called Steganographic Pixel-wise Actions and Rewards with Reinforcement Learning (SPAR-RL). To maximise the benefits from a simulated steganalytic environment, an agent in SPAR-RL used a policy network to break down the embedding process into pixel-wise actions, while the environment used an environment network to award rewards to individual pixels. An adaptive local image steganography (AdaSteg) method was presented by Pan et al. (Pan *et al.*, 2022) to enable image steganography that is both scale- and location-adaptive. The suggested technique increased the security of steganography by adaptively hiding the secret on a local scale, and it also made it possible to conceal several secrets under a single cover. This was accomplished in two distinct phases: the first is the selection of the adaptive patches, while the second is the use of a secret encryption method.

Yang et al. (Yang *et al.*, 2020) proposed Automatic Network Architecture Generation technique for JPEG image Steganalysis based on reinforcement learning (JS-NAG). Unlike the automated neural network creation methods in computer vision, which are based on the strong content signals, steganalysis relies on the weak embedded signals, necessitating a unique architecture. Using Q-learning, the agent was taught to successively choose high-performing blocks to construct networks. A well-designed performance prediction function and an early stop approach were used to decrease the search duration. Ni et al. (Ni *et al.*, 2019) proposed a selective ensemble method in image steganalysis based on deep Q network, which combines reinforcement learning with convolutional neural network and are seldom seen in ensemble pruning. This method improved the generalization performance of the model and reduced the size of ensemble as well.

Mo et al. (Mo *et al.*, 2022) suggested a new Decoupled Adversarial Policy (DAP) for targeting the Deep Reinforcement Learning (DRL) method, in which the adversarial agent can decompose the adversarial policy into two distinct sub-policies: 1) the switch policy, which determines whether an attacker should launch the attack, and 2) the lure policy, which determines the action an attacker induces the victim to take. If the adversarial agent samples an injection action from the switch policy, the intruder can access the pre-constructed database in real-time for universal perturbation, deceiving the victim into taking the induced action sampled from the lure policy. To teach the adversarial agent DAP, they used examples in which the two sub-actions of DAP are neither constrained by each other nor by an external restriction, but can alter the attackers' behaviour. Therefore, trajectory clipping, and padding were offered for data trimming, and Decoupled Proximal Policy Optimization (DPPO) was suggested for optimization.

2.2.4. Attention Based Learning Steganographic Algorithms

Wang et al. (2022) proposed a novel scheme that uses the Transformer for feature extraction in steganography. In addition, an image encryption algorithm using recursive permutation is proposed to further enhance the security of secret images.

2.2.5. Convolutional Neural Networks Based Learning Steganographic Algorithms

Yedroudj et al. (2018) suggested a CNN employing a pre-processing filterbank and a Truncation activation function, five convolutional layers with a Batch Normalization coupled with a Scale Layer, as well as the usage of a sufficiently large fully connected section. An expanded database was employed to improve the training of the CNN. This CNN was experimentally assessed against two embedding techniques and its performances were compared with those of three other methods: an Ensemble Classifier with a Rich Model, and two other CNN steganalyzers. Reinel et al. (2021) developed a CNN architecture that included a preprocessing stage employing filter banks to boost steganographic noise, a feature extraction stage employing depthwise and separable convolutional layers, and skip connections. The performance of the WOW, S-UNIWARD, MiPOD, HILL, and HUGO adaptive

steganographic algorithms was tested using the BOSSbase 1.01 and BOWS 2 datasets in conjunction with several experimental settings and adaptive steganographic algorithms.

With two contributions, Xiang et al. (2020) introduced a novel convolutional neural network-based steganalysis technique. By adding more convolutional layers to the lower portion of the model, they presented a novel arrangement of convolutional layers and pooling layers that processes local information more effectively than previous CNN models in steganalysis. By putting the global average pooling layer before the softmax layer rather than utilising it before the fully connected layer, the global average pooling was placed in a better position for steganalysis. Tang et al. (2019) proposed a steganographic technique with an unique operation dubbed adversarial embedding (ADV-EMB), which successfully disguised a stego message and fooled a convolutional neural network (CNN)-based steganalyzer. The proposed method adheres to the standard distortion minimization framework. ADV-EMB specifically modified the costs of picture element alterations based on the gradients back propagated from the target CNN steganalyzer. Therefore, there was a greater likelihood that the direction of the modification was the same as the gradient's sign inversion. Thus, antagonistic stego pictures were created.

3. FUTURE RESEARCH DIRECTIONS

Image steganography based on deep learning approaches offers considerable improvements over traditional image steganographic methods, solving various issues traditional methods face. However, these methods are not foolproof and have several shortcomings that need to be worked. This paper provides an inclusive survey highlighting the pros and cons of existing image steganography algorithms based on deep learning methods. The challenges faced by various techniques are highlighted for the researchers associated with the field of image Steganography using deep learning methods to work on in the future. This paper recognizes the challenges in deep learning image steganographic techniques that researchers can work on in the future and also lists out potential research developments and directions for deep learning methods that could be possible solutions.

- Deep learning methods like the RNN and Bayesian neural networks with theoretical support can be studied. Their approaches can be applied in deep learning steganographic techniques to achieve better results.
- Current deep learning steganographic models can be studied for Clipping and Compression of super-large parameters/size of deep learning steganographic model into a small and concise steganographic analysis framework with acceptable performance.
- Automatic generation of image steganographic deep learning models can be studied to completely exclude the human factors and design this efficient deep learning steganographic result.
- The attempt to solve the linguistic steganography has been made in Yang et al. (2019) and can be extended for this related work.

4. CONCLUSION

This work aims to provide a high-level overview of the various deep learning approaches that are now employed or potentially used for optimal results in the field of image steganography. It's a brief explanation and comparison of some recent deep learning-based Image steganography techniques. Despite the fact that a lot of research has been done in recent years with some very promising outcomes, there is still a long way to go. For example, certain algorithms yield better theoretical results, but their implementation is difficult and results worse than some simpler options. Incorporating new deep learning models into these algorithms is a great way to further fine-tune them. Further, multiple types of deep learning learning models include autoencoder-based, reinforcement learning-based, attention-based, and convolutional neural network-based image steganography has been presented.

REFERENCES

AlKhodaidi, T., & Gutub, A. (2021). Refining image steganography distribution for higher security multimedia counting-based secret-sharing. *Multimedia Tools and Applications*, *80*(1), 1143–1173. doi:10.1007/s11042-020-09720-w

Al-Roithy, B. O., & Gutub, A. (2021). Remodeling randomness prioritization to boost-up security of RGB image encryption. *Multimedia Tools and Applications*, *80*(18), 28521–28581. doi:10.1007/s11042-021-11051-3

Arjovsky, M., Chintala, S., & Bottou, L. (2017). *Wasserstein Generative Adversarial Networks*. Academic Press.

Barz, B., & Denzler, J. (2019). Hierarchy-Based Image Embeddings for Semantic Image Retrieval. *2019 IEEE Winter Conference on Applications of Computer Vision (WACV)*, 638–647. doi:10.1109/WACV.2019.00073

BrockA.DonahueJ.SimonyanK. (2018). *Large Scale GAN Training for High Fidelity Natural Image Synthesis.* Available at: https://arxiv.org/abs/1809.11096

CelebA Dataset. (n.d.). Available at: http://mmlab.ie.cuhk.edu.hk/projects/CelebA.html

CheT. (2016). *Mode Regularized Generative Adversarial Networks*. Available at: https://arxiv.org/abs/1612.02136

CheT. (2017). *Maximum-Likelihood Augmented Discrete Generative Adversarial Networks*. Available at: https://arxiv.org/abs/1702.07983

COCO - Common Objects in Context. (n.d.). Available at: https://cocodataset.org/#home

Cui, Q., McIntosh, S., & Sun, H. (2018). Identifying materials of photographic images and photorealistic computer generated graphics based on deep CNNs. *Computers*, *Materials and Continua*, *55*(2), 229–241. doi:10.3970/cmc.2018.01693

Dai, J. (n.d.). *R-FCN: Object Detection via Region-based Fully Convolutional Networks*. Available at: https://github.com/daijifeng001/r-fcn

Deng, J. (2010). *ImageNet: A large-scale hierarchical image database*. doi:10.1109/CVPR.2009.5206848

Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography. (n.d.). Available at: https://www.researchgate.net/publication/344311992_Enhancing_Medical_Data_Security_via_Combining_Elliptic_Curve_Cryptography_and_Image_Steganography

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2020). Generative adversarial networks. *Communications of the ACM*, *63*(11), 139–144. doi:10.1145/3422622

Guo, X. (2021). Relaxed Wasserstein with applications to GANS. *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 3325–3329. doi:10.1109/ICASSP39728.2021.9414454

Gutub and Adnan. (n.d.a). *Enhancing Cryptography of Grayscale Images via Resilience Randomization Flexibility*. 10.4018/IJISP.307071

Gutub and Adnan. (n.d.b). *Watermarking Images via Counting-Based Secret Sharing for Lightweight Semi-Complete Authentication*. 10.4018/IJISP.2022010118

Gutub, A. (2022a). Boosting image watermarking authenticity spreading secrecy from counting-based secret-sharing. *CAAI Transactions on Intelligence Technology*, cit2.12093. Advance online publication. doi:10.1049/cit2.12093

Gutub, A. (2022b). Dynamic smart random preference for higher medical image confidentiality. *Journal of Engineering Research*. .10.36909/jer.17853

Gutub, A., & Al-Ghamdi, M. (2020). Hiding shares by multimedia image steganography for optimized counting-based secret sharing. *Multimedia Tools and Applications*, *79*(11–12), 7951–7985. doi:10.1007/s11042-019-08427-x

Gutub, A., & Al-Roithy, B. O. (2021). Varying PRNG to improve image cryptography implementation. *Journal of Engineering Research*, *9*(3A), 153–183. doi:10.36909/jer.v9i3A.10111

Hameed, M. A., Abdel-Aleem, O. A., & Hassaballah, M. (2022). A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques. *Journal of Ambient Intelligence and Humanized Computing*, *1*, 1–19. doi:10.1007/s12652-022-04366-y

Hassaballah, M. (2020). A color image steganography method based on ADPVD and HOG techniques. Digital Media Steganography: Principles, Algorithms, and Advances. doi:10.1016/B978-0-12-819438-6.00010-4

Hassan, F. S., & Gutub, A. (2021). Efficient Image Reversible Data Hiding Technique Based on Interpolation Optimization. *Arabian Journal for Science and Engineering*, *46*(9), 8441–8456. doi:10.1007/s13369-021-05529-3

He, K. (n.d.). *Deep Residual Learning for Image Recognition*. Available at: https://image-net.org/challenges/LSVRC/2015/

He, T. (n.d.). *Bag of Tricks for Image Classification with Convolutional Neural Networks*. Available at: https://github.com/dmlc/gluon-cv

Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the Dimensionality of Data with Neural Networks. *Science*, *313*(5786), 504–507. doi:10.1126/science.1127647 PMID:16873662

Hiwe, M. S., & Nipanikar, P. S. I. (2014). An Analysis of Image Steganography Methods. *International Journal of Engineering Research & Technology (Ahmedabad)*, *3*(2). Advance online publication. doi:10.17577/IJERTV3IS21289

HjelmR. D. (2017) Boundary-Seeking Generative Adversarial Networks. Available at: https://arxiv.org/abs/1702.08431

Hu, D., Wang, L., Jiang, W., Zheng, S., & Li, B. (2018). A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 38303–38314. doi:10.1109/ACCESS.2018.2852771

Huang, G., Zhu, Q.-Y., & Siew, C.-K. (2006). Extreme learning machine: Theory and applications. *Neurocomputing*, *70*(1–3), 489–501. doi:10.1016/j.neucom.2005.12.126

Image Steganography to Facilitate Online Students Account System. (n.d.). Available at: https://www.researchgate.net/publication/338177613_Image_Steganography_to_Facilitate_Online_Students_Account_System?channel=doi&linkId=5e04fc4b4585159aa49d3476&showFulltext=true

Jaeger, P. F. (2020). *Retina U-Net: Embarrassingly Simple Exploitation of Segmentation Supervision for Medical Object Detection, Machine Learning Research*. Available at: https://github.com/pfjaeger/medicaldetectiontoolkit

Karras, T., & Laine, S. (n.d.). *A Style-Based Generator Architecture for Generative Adversarial Networks Timo Aila NVIDIA*. Available at: https://github.com/NVlabs/stylegan

Ke, Y., Zhang, M., Liu, J., Su, T., & Yang, X. (2019). Generative steganography with Kerckhoffs' principle. *Multimedia Tools and Applications*, *78*(10), 13805–13818. doi:10.1007/s11042-018-6640-y

Kerry, C. F. (2018). *Why protecting privacy is a losing game today—and how to change the game*. Available at: https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/

Kim, T. (2017). *Learning to Discover Cross-Domain Relations with Generative Adversarial Networks*. Academic Press.

KingmaD. P.WellingM. (2013). *Auto-Encoding Variational Bayes*. Available at: https://arxiv.org/abs/1312.6114

Larsen, A. B. L. (2016). Autoencoding beyond pixels using a learned similarity metric. *ICML*, *4*, 2341–2349.

Liu, W. (2016). *SSD*. Single Shot MultiBox Detector. doi:10.1007/978-3-319-46448-0_2

Liu, X. (2022). *Image Disentanglement Autoencoder for Steganography Without Embedding*. doi:10.1109/CVPR52688.2022.00234

Lu, W., Zhang, J., Zhao, X., Zhang, W., & Huang, J. (2021). Secure Robust JPEG Steganography Based on AutoEncoder with Adaptive BCH Encoding. *IEEE Transactions on Circuits and Systems for Video Technology*, *31*(7), 2909–2922. doi:10.1109/TCSVT.2020.3027843

Mao, X. (n.d.). *Least Squares Generative Adversarial Networks*. Academic Press.

Mescheder, L., Nowozin, S., & Geiger, A. (2017). Adversarial Variational Bayes: Unifying Variational Autoencoders and Generative Adversarial Networks. *PMLR*, 2391–2400. Available at: https://proceedings.mlr.press/v70/mescheder17a.html

Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., Graves, A., Riedmiller, M., Fidjeland, A. K., Ostrovski, G., Petersen, S., Beattie, C., Sadik, A., Antonoglou, I., King, H., Kumaran, D., Wierstra, D., Legg, S., & Hassabis, D. (2015). Human-level control through deep reinforcement learning. *Nature*, *518*(7540), 529–533. doi:10.1038/nature14236 PMID:25719670

Mo, K. (2022). Attacking Deep Reinforcement Learning with Decoupled Adversarial Policy. *IEEE Transactions on Dependable and Secure Computing*. Advance online publication. doi:10.1109/TDSC.2022.3143566

Montavon, G., & Müller, K.-R. (2012). *Deep Boltzmann Machines and the Centering Trick*. doi:10.1007/978-3-642-35289-8_33

Ni, D., Feng, G., Shen, L., & Zhang, X. (2019). Selective Ensemble Classification of Image Steganalysis Via Deep Q Network. *IEEE Signal Processing Letters*, *26*(7), 1065–1069. doi:10.1109/LSP.2019.2913018

Nowozin, S., Cseke, B., & Tomioka, R. (2016). f-GAN: Training Generative Neural Samplers using Variational Divergence Minimization. Advances in Neural Information Processing Systems, 29. doi:10.1016/0022-4405(75)90045-X

Pan, W., Yin, Y., Wang, X., Jing, Y., & Song, M. (2022). Seek-and-Hide: Adversarial Steganography via Deep Reinforcement Learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *44*(11), 7871–7884. doi:10.1109/TPAMI.2021.3114555 PMID:34550880

Progonov, D. (2021). Performance Analysis of Stego Images Detection Using Shallow Denoising Autoencoders. *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology, PIC S and T 2021 - Proceedings*, 179–182. doi:10.1109/PICST54195.2021.9772180

Qin, Y. (2018). *Autofocus Layer for Semantic Segmentation*. doi:10.1007/978-3-030-00931-1_69

Redmon, J. (n.d.). *You Only Look Once: Unified, Real-Time Object Detection*. Available at: https://pjreddie.com/yolo/

Reinel, T. S., Brayan, A.-A. H., Alejandro, B.-O. M., Alejandro, M.-R., Daniel, A.-G., Alejandro, A.-G. J., Buenaventura, B.-J. A., Simon, O.-A., Gustavo, I., & Raul, R.-P. (2021). GBRAS-Net: A Convolutional Neural Network Architecture for Spatial Image Steganalysis. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 14340–14350. doi:10.1109/ACCESS.2021.3052494

Ren, S. (n.d.). *Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks*. Available at: https://github.com/

RoddickT.KendallA.CipollaR. (2018). *Orthographic Feature Transform for Monocular 3D Object Detection*. Available at: https://arxiv.org/abs/1811.08188

Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., Huang, Z., Karpathy, A., Khosla, A., Bernstein, M., Berg, A. C., & Fei-Fei, L. (2015). ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision*, *115*(3), 211–252. doi:10.1007/s11263-015-0816-y

Sanh, V., Wolf, T., & Ruder, S. (2019). A Hierarchical Multi-Task Approach for Learning Embeddings from Semantic Tasks. *Proceedings of the AAAI Conference on Artificial Intelligence*, *33*(1), 6949–6956. doi:10.1609/aaai.v33i01.33016949

Shi, H. (2018). *SSGAN*. Secure Steganography Based on Generative Adversarial Networks. doi:10.1007/978-3-319-77380-3_51

SimonyanK.ZissermanA. (2014). *Very Deep Convolutional Networks for Large-Scale Image Recognition.* Available at: https://arxiv.org/abs/1409.1556

Steganography GAN: Cracking Steganography with Cycle Generative Adversarial Networks | DeepAI. (n.d.). Available at: https://deepai.org/publication/steganography-gan-cracking-steganography-with-cycle-generative-adversarial-networks

Subramanian, N., Cheheb, I., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). End-to-End Image Steganography Using Deep Convolutional Autoencoders. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 135585–135593. doi:10.1109/ACCESS.2021.3113953

Tang, W., Li, B., Barni, M., Li, J., & Huang, J. (2021). An automatic cost learning framework for image steganography using deep reinforcement learning. *IEEE Transactions on Information Forensics and Security*, *16*, 952–967. doi:10.1109/TIFS.2020.3025438

Tang, W., Li, B., Tan, S., Barni, M., & Huang, J. (2019). CNN-Based Adversarial Embedding for Image Steganography. *IEEE Transactions on Information Forensics and Security*, *14*(8), 2074–2087. doi:10.1109/TIFS.2019.2891237

Tang, W., Tan, S., Li, B., & Huang, J. (2017). Automatic Steganographic Distortion Learning Using a Generative Adversarial Network. *IEEE Signal Processing Letters*, *24*(10), 1547–1551. doi:10.1109/LSP.2017.2745572

Tran, N.-T., Bui, T.-A., & Cheung, N.-M. (2018). Dist-GAN: An Improved GAN using Distance Constraints. Academic Press.

Trustworthy image security via involving binary and chaotic gravitational searching within PRNG selections | Request PDF. (n.d.). Available at: https://www.researchgate.net/publication/351591611_Trustworthy_image_security_via_involving_binary_and_chaotic_gravitational_searching_within_PRNG_selections

Volkhonskiy, D., Nazarov, I., & Burnaev, E. (2020). Steganographic generative adversarial networks. *Twelfth International Conference on Machine Vision (ICMV 2019)*, 97. doi:10.1117/12.2559429

WangQ.ChanA. B. (2018). *CNN+CNN: Convolutional Decoders for Image Captioning*. Available at: https://arxiv.org/abs/1805.09019

Wang, Z. (2022). Deep Image Steganography Using Transformer and Recursive Permutation. *Entropy 2022, 24*(7), 878. 10.3390/e24070878

Xiang, Z., Sang, J., Zhang, Q., Cai, B., Xia, X., & Wu, W. (2020). A New Convolutional Neural Network-Based Steganalysis Method for Content-Adaptive Image Steganography in the Spatial Domain. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 47013–47020. doi:10.1109/ACCESS.2020.2978110

YangJ. (2018). *Spatial Image Steganography Based on Generative Adversarial Network*. Available at: https://arxiv.org/abs/1804.07939

Yang, J. (2020). Reinforcement Learning Aided Network Architecture Generation for JPEG Image Steganalysis. *IH and MMSec 2020 - Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*, *20*, 23–32. doi:10.1145/3369412.3395060

Yang, Z. L., Guo, X.-Q., Chen, Z.-M., Huang, Y.-F., & Zhang, Y.-J. (2019). RNN-Stega: Linguistic Steganography Based on Recurrent Neural Networks. *IEEE Transactions on Information Forensics and Security*, *14*(5), 1280–1295. doi:10.1109/TIFS.2018.2871746

Yedroudj, M., Comby, F., & Chaumont, M. (2018). Yedroudj-Net: An Efficient CNN for Spatial Steganalysis. *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2092–2096. doi:10.1109/ICASSP.2018.8461438

Yi, Z. (n.d.). *DualGAN: Unsupervised Dual Learning for Image-to-Image Translation*. Academic Press.

Yu, J. (2017). *A Multi-purpose Image Counter-anti-forensic Method Using Convolutional Neural Networks*. doi:10.1007/978-3-319-53465-7_1

Yuan, C., Wang, H., He, P., Luo, J., & Li, B. (2022). GAN-based image steganography for enhancing security via adversarial attack and pixel-wise deep fusion. *Multimedia Tools and Applications*, *81*(5), 6681–6701. doi:10.1007/s11042-021-11778-z

ZhangK. A. (2019). *SteganoGAN: High Capacity Image Steganography with GANs*. Available at: https://arxiv.org/abs/1901.03892

Zhu, J.-Y. (n.d.). *Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Networks Monet Photos*. Available at: https://github.com/junyanz/CycleGAN

Zhuang, J. (n.d.). *ShelfNet for Fast Semantic Segmentation*. Available at: https://github.com/

Vijay Kumar is Associate Professor in Information Technology, Dr. B.R. Ambedkar NIT Jalandhar. He received his Ph.D. degree from NIT Kuruksherta. Previously, he received M.Tech. and B.Tech. degrees from GJUS&T, Hisar and M.M. Engineering College, Mullana, respectively. He has more than 3 years of teaching and research experience in the National Institute of Technology, Hamirpur. He has 4 years of teaching and research experience in the Thapar Institute of Engineering & Technology, Patiala. Prior, he has 8 years of teaching experience in various reputed institutes. He completed 2 DST SERB sponsored research projects. Presently, he is working on 1 CSIR sponsored research project. He has published more than 100 research papers in International Journals/Conferences. He has many book chapters in international repute publishers. He has supervised many Ph.D. and M.Tech. thesis on Metaheuristics, Image Mining, and Data Clustering. He has been listed among World's Top 2% Scientists (2021 and 2022). He is the reviewer of several reputed SCI journals. He is member of ACM, CSI, International Association of Engineers, International Association of Computer Science and Information Technology, Singapore. His current research area is Soft Computing, Data Mining, Deep Learning, Steganography, and Pattern Recognition.

Sahil Sharma is currently working as Assistant Professor (Senior Grade) in the Department of Computer Science & Information Technology at Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh. He has more than 5 years of teaching and research experience. He has completed his Ph.D. thesis with title "Metaheuristic Approaches for Occlusion Invariant 3D Face Recognition Technique" in Computer Science & Engineering Department from Thapar Institute of Engineering and Technology, Patiala, Punjab. He obtained his M.E. with thesis title "Predicting Employability from User Personality using Ensemble Modelling" in Computer Science Information Security from Thapar University, Patiala, Punjab. He has obtained his B.Tech. in Computer Science & Engineering from Punjab Technical University, Jalandhar, Punjab. He has also qualified NTA UGCNET June 2019 (98.901 Percentile) and GATE CS 2013 (96.7193 Percentile). He has around 9 SCI/SCIE research publications and few conference publications.

Chandan Kumar received the Ph.D. degree in Computer Science from NIT Jamshedpur, India, in 2018. He is currently the Assistant Professor of School of Computing, Amrita Vishwa Vidyapeetham, Amaravati Campus, Andhra Pradesh, India. His research interest includes machine learning, deep learning, data science, software engineering and bibliometrics analysis.