Steganalysis Techniques: A Systematic Review

C. Victoria Priscilla
Associate Professor & Head, PG Department of Computer Science, SDNB Vaishnav College for Women, 'University of Madras', Chennai, India, aprofvictoria@gmail.com

V. HemaMalini
Research Scholar, Research Department of Computer Science, SDNB Vaishnav College for Women, 'University of Madras', Chennai, India, hemaveera123@gmail.com

Abstract

World at present is full of data. Data plays a major role in all aspects in development in any field, future predictions, decision making etc. Securing data is very important not only to avoid breaches but also to shield the confidential messages. There comes the concept of Steganography. Steganography is the art of covering data up under an ordinary text or image or video. When steganography is misused by hiding malware in safe files, there comes the art of detecting steganography called Steganalysis. Some known methods in Steganalysis are Stego-only, Known cover, Known message, Chosen stego and lastly Chosen message attacks. This work presents a survey on recent trends in steganography and use of machine learning algorithms in steganalysis.

Keywords: *Steganography, Steganalysis, Cryptography, Machine learning.*

1 Introduction

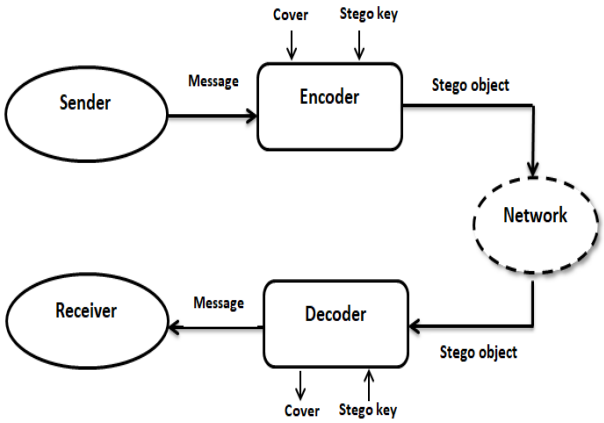
Immense data is produced electronically every second. It is no surprise that protecting the data is very important. Lots of methods evolved in this regard. Steganography is one such method in which other than the sender and the intended recipient, no one could suspect the existence of the message. It is a Greek word meaning "Hidden writing". Steganography was traced long back in history around 440 BC in Greece when people wrote messages on wood and covering them with the cover medium like wax, they passed the message. Invisible inks were used by Romans, whose writings were deciphered using light or heat. Microdots were introduced by Germans. Null ciphers were also used to hide secret messages. In 1499AD from a disguised book named Steganographia, we could find the visibility of the concept (wikipedia, n.d.). Steganography is a partner to Cryptography. While cryptography protects a message, steganography hides the message itself. Though cryptography and steganography sound similar, they are two different concepts with the same goal of protecting the message(Dickson, 2020). In cryptography, the information is transformed to a cipher text using an encryption key. Then the cipher text is transformed back to the initial message using a decryption key by the receiver. The middle men would know that some encryption form has been applied. But in steganography, the existence of the message is concealed. Data is not usually altered in Steganography. But nowadays, data is first encrypted and then concealed for increasing security.(Margie Semilof, 2021). The encoding system of Steganography is its key feature. In the data protection field, Steganography is the flourishing concept.

2 Steganography process

In steganography, use of key is optional but when used, gives more security. There will be a cover file to shield the secret message. The

sender delivers the confidential message enclosing it in a cover file. Together they are loaded to the steganographic encoder. The restricted message is enclosed to the cover file by the encoder function. The stego object, which is the result, looks like the cover file, hiding the message totally. (Choudary, n.d.)

Fig. 1. Steganography Block diagram

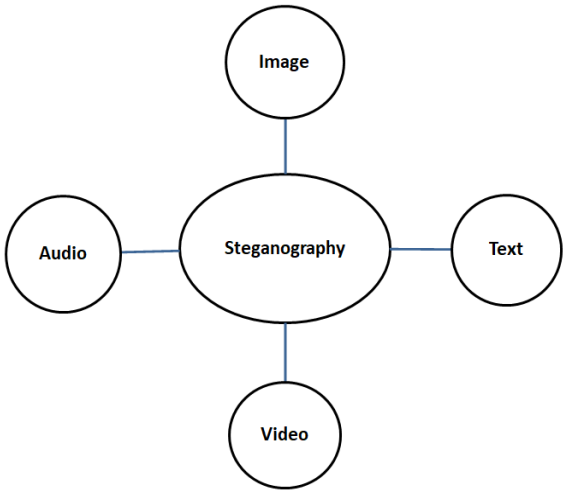


This stego object is passed through the communication channel. In the receiver end, the stego object is passed through the Steganographic decoder to get the cover file and the secret message independently thus delivering the message to the receiver. To make the content more secure nowadays, the message is encrypted using the encryption key. This cipher text is sent through the steganographic encoder.

3 Types of steganography

Depending on the variety of the cover object used for enclosing the secret data, many types of steganography exist like image, text, audio and video steganography.(Dr.Souvik Bhattacharyya, Dr- Indradip Banerjee, 2011)

Fig. 2. Types of Steganography



3.1 Image steganography

The mechanism of enclosing data within an image file is called Image Steganography. The image used for hiding data is known as the cover image and the image we get after steganography is termed the stego image.

Considering the problem of capacity, invisibility and security in image steganography, a novel method called ISGAN was introduced in(Zhang et al., 2019) to hide an image which is grey into an image as color cover in the dispatcher side and in the beneficiary side to get the secret image out. The scholars have given three contributions:

- Firstly, invisibility is improved by hiding secret message in Y- channel of closing image.
- Secondly, by reducing the distribution empirical probability distributions of natural and stego images, the security is strengthened. For this, generative adversarial network is introduced.
- Thirdly, a mixed loss function is constructed for steganography to produce better stego images and give out good secret images.

U-net structure as the base, authors (Duan et al., 2019)gave a vital image steganography procedure. Two networks are included in the trained neural network. They are hiding and extraction network. In the hiding network, the encoder network does the work of encoding secret image under the cover image. The combination is concatenated into 6-channels using U-net based CNN which is modified to accept 256*256 cascaded channels. This is fed to the hiding network. In the extraction network, decoder network is utilized for extracting secret image from stego image. There are 6 Convolutional layers with 3 *3 sized Convolutional Kernels. Using image-to-image translation, steganography and steganalysis modules are added in CycleGAN, a steganographic algorithm is introduced in(Meng et al., 2019) for secure communications in IOT. The generated image quality is guaranteed. The resisting capacity of the stego-image to steganalysis is improved to some extent. This method proved better to the State-of-art method and is named as S-Cycle GAN. The stego-images were very near to the cover images by the facility of Cycle consistency.

Goal of hiding stego message and cheating CNN based steganalyzer is presented in (Tang et al., 2019) with a steganographic scheme and adversarial embedding (ADV-EMB). Keeping in mind the back transmitted gradients from the target CNN steganalyzer, the adversarial embedding adjusts the costs of modifications of image elements. This shows that the inverse sign of gradient and modification direction has high chance of being same. This scheme is capable to overcome highly powerful CNN-based steganalysis and it reduces the performance of steganalyzers. Storage based network steganography is difficult to be detected by the traditional tools. Firstly, the data packets are collected in network traffic. Wireshark tool is used to capture network packets. New features are proposed to detect secret information hidden. Then the records are divided as normal or steganographic packets using machine learning algorithms in(Cho et al., 2018). Random Forest algorithm is found to be better than Naïve Bayes and Support Vector Machines.

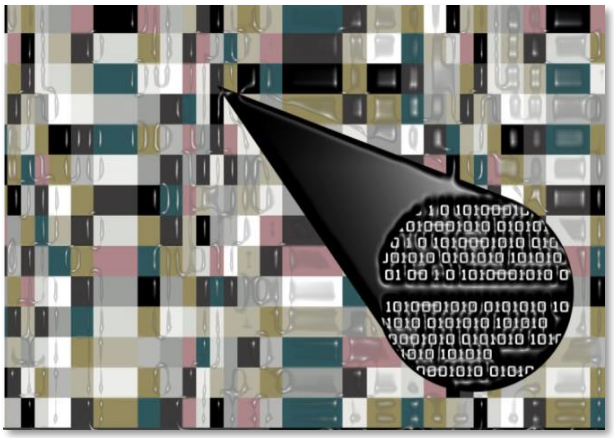
A publicly available cover data is easily accessible to anyone. So a unique cover data could avoid this problem. (Naito & Zhao, 2019)used GAN in this context. Two neural networks are utilized.

- A Generator, which creates virtual images for cover data,
- A Discriminator, which checks the naturalness of the virtual images.

At the gaining end, the generator opens the secret data by decoding the stego image. The Discriminator discards the non-realistic images. It also checks if the sender is a true party or not. The trained generator and the discriminator are split between the sender and the receiver.

Some identity of steganography is left behind in stego files while embedding a message. This is due to some allotted bytes used for the purpose of copyright safety of information. These bytes are extracted as finger prints by (Cao et al., 2019). Three fixed positions are considered. They are File header of the image; Sequential LSBs of the image file data and Random places behind Image file tail. This method is named as Signature method and is proved to be effective. Half tone images are produced using dots of various sizes. A steganographic scheme is proposed for such images by (Lu et al., 2021). Employing the concept of pixel density, authors constructed a PDHistogram. Density blocks are selected to improve visual Quality by density pair selection. A pixel flip strategy is proposed based on PMMTM to increase security against Steganalysis.

Fig. 2. Image Steganography



K-LSB based method for enclosing the image is proposed by (Elharrouss et al., 2020). To know the blocks containing the enclosed image, a region detection process is used. While the process, resolution of the stego image could be spoiled, and this is corrected by the Quality improvement method. PSNR ratio is used to check the image quality. The authors in (F. Chen et al., 2020) proposed a two channel data hiding network, which are used to input the cover image along with confidential image at the same time. There are two networks. They are hiding and extraction networks. The former network is used to conceal the secret image under cover image and form a hybrid image. The latter network is used by the receiver to extract the secret image. Two metrics MSE and SSIM are used to construct the innovative loss function. Special skills like ship connection feature fusion; residual connection reduction of feature dimension and feature extraction

In multi scale level are developed and optimized.(Zhou et al., 2020) constructed a high quality Adversarial image which is used to generate suitable steganography covers. These adversarial images carry secret information in a better way. Before and after steganography, these images get an equivalent classification result which is achieved by a new loss function. “Zero-sum idea of GAN is used to improve security of such images. While embedding confidential data in an image, the likeliness measure of the neighbouring pixels is considered. This is determined using Interval Type-2 Fuzzy logic system taking human perception into account using Rule-based approach. Using the similarity measure defined, the image pixels with greater similarity values are selected. They are used for embedding based on the LSB method. The authors (Ashraf et al., 2020)developed two other methods for comparing with one another. On the selected data sets, everyone of the three techniques are put in and Quality metrics like PSNR, UQI and SSIM are calculated. The proposed method had high payload capacity and proved effective compared to the other steganographic methods.

Deep Learning based high capacity image Steganography is proposed by (Duan, Guo, et al., 2020). The secret image is altered using DCT and ciphered by Elliptic Curve method of Cryptography. This is done to increase the anti-detection property. The SegNet Deep Neural Network is employed. There are two networks namely Hiding and Extraction. The former encloses the enciphered image into the host image and it sends the results to the receiver. The latter then extracts the encrypted image. (Yang et al., 2020) introduced a novel steganography framework with three modules. U-Net based Generator translates cover image to a rooting probability map. During back propagation in adversarial training, while preserving gradient norm, two tanh functions are used without any training before to approximate the optimal embedding simulator. CNN based (XU NET) enhanced steganalyzer with multiple HPF act as a discriminator. General Adversarial Network Tunnel is a network traffic masking method to safeguard the applications from ITC’s (Internet Traffic Classifiers). Here the actual traffic is encapsulated and a duplicate traffic similar to the original is prepared by (Fathi-Kazerooni & Rojas-Cessa, 2020). The original traffic remains safe. A Wasserstein GAN is designed

composing 4 hidden layers of generator and three hidden layers of a critic. Classifiers for example RF and XGboost were used to detect the flow. Accuracy was 0.99 and 0.97 respectively with the classifiers and WGAN which are trained on same data sets and two separate datasets. Aiming to improve the steganographic capacity, FC-DenceNet is utilized by (Duan, Nao, et al., 2020). The first convolution block's input channels and the last convolution block's output channels are reset. After they are concatenated through the hidden network to obtain the stego image, the secret image is enclosed in the bearer image. The object tag category is not used and LogSoftmax() function is deleted.

Due to the drawback of the payload capacity, a novel deep convolutional neural network is introduced by(Duan, Wang, et al., 2020)with steganography volume of 1 byte/pixel. A pyramid pool module is added to the enclosing and excluding network based on up-sampling and down sampling structure with all important previous features. This ensured huge-capacity embedding and the visual effect of the image. During the process of training, this also minimized the loss function of the framework. STNet is a Style Transfer method where the content is enclosed in style images and art images are created by (Z. Wang, Gao, et al., 2019). This help in resisting steganalysis tools. The arbitrary size of the stego images produced is 0.06bit/pixel. Being an Unsupervised end-to-end training model, STNet is the style transfer based first steganographic method. As the stego images are art images, they are hard to be detected. Style- transfer is done by Adaptive Instance Normalization. Arbitrary bits of unrevealed messages can be embedded. The regular singular method in steganography has been revisited and re-energized and brought via neutralization to modern generation by (Chang, 2020). Adversarial learning is introduced to get back the regularity of natural images after the discrimination done. GAN are trained for prediction of bit planes to carry the information which is hidden. Guidance on embedding data and recovering image is provided by a synthetic image formed.

To encipher the secret message in Steganography, a cover medium or cover image is used. This cover image is removed by steganalysis algorithms and secret messages are read. To solve this problem, coverless image steganography method is used by (Saad et al., 2021) which is highly robust. It is gleaned from Optical Mark Recognition and RBML i.e.. Rule Based Machine Learning. The advantages of this method are:

- No secret information to be shared
- No requirement of database
- Image need not be searched in database so it is time saving
- Embedding capacity is very high robust. So can resist attacks
- No expensive or special tools used in OMR
- Highly secure

SPAR-RL is the new cost learning framework introduced by(Tang et al., 2021).There is an iterative interaction amidst the agent and the surrounding. The agent uses the policy network to breakdown the process inside into pixel-wise actions. The environment utilizes its network for pixel-wise assignment of rewards to the agent.

The main inputs in the work are:

- The agents learn the embedded policy to maximize rewards.
- The embedded policy reduces the image level into pixel-wise actions.
- Pixel-wise reward function helps agent to know about the embedding policy.

The security and stability performance proved good when compared to the other cost methods.

Table 1. Image Steganography Techniques

Title & Publication	Data set	Techniques/ Algorithms/ Architecture	Advantages	Disadvantages/ future work
(Zhang et al., 2019)	PASCAL-Voc12, IMAGENET	ISGAN	Grey scale image concealed in color cover image	Some image loss caused by transmission during training
(Naito & Zhao, 2019)	CelebA	DCGAN	A generator to produce cover images and a discriminator to filter out unnatural images are used.	Discriminator should be trained with a new loss function to keep track with the generator.
(Cao et al., 2019)	500 images (Google website)	Stego tools (Message smuggler, Image hide, Invisible secrets)	fingerprint extraction done for fixed embedding in 3 ways	Stego tools which embed message in arbitrary position cannot be applied
(F. Chen et al., 2020)	Pascal-VOC, NWPU-RESISC45, AID dataset	TDHN(Two Channel Deep Hiding Network)	Two channels one for hiding and the other for extracting secret message are used.	GAN to be included to minimize data driven dependence.
(Duan, Guo, et al., 2020)	ImageNet	SegNet Deep Neural Network	Both encryption and enclosing data are done.	-
(Yang et al., 2020)	BOSSBase, SZUBase	U-Net, UT-GAN, XU-NET	Three module frameworks are proposed.	GAN based method in Steganography in JPEG domain can be applied.
(Duan, Wang, et al., 2020)	ImageNet	StegoPNet, Pyramid pooling module	Large capacity embedding and good visual effect	Attention mechanism may be introduced to conceal secret information during training.

(Chang, 2020)	BossBase, USC-SIPI	U-Net, CNN	Images are converted to 8-bit grey scale. They are again converted to 256*256 pixels.	Deep neural Network can be involved in invertible steganography.
(Saad et al., 2021)	Bubble sheet template prepared.	Optical Mark Recognition , Rule Based Machine Learning	Time saving, robust, secure, high embedding capacity.	-
(Tang et al., 2021)	SZUBase BOSSBase	SPAR-Reinforcement Learning	More secure and stable.	Other forms of reward functions should be investigated;

3.2 Audio steganography

When the secret data is hidden within a cover audio, it is termed as Audio Steganography.

Multiple steganography detecting methods, based on Bayesian network code elements, are proposed in low bit rate to flattened speech by (Yang et al., 2019). Code element perspective is considered in developing this method, as there exist the spatio-temporal correlations between them. Using Dirichlet distribution prior for learning network parameters and Bayesian inference based implementations Steganalysis is taken forward. For digital audio, a new steganography method based on adversarial attacks, initial costs are iteratively updated by (J. Wu et al., 2020). There are two steps involved. Firstly, training the CNN based series of steganalyzers iteratively and secondly, stegos are generated according to the already trained steganalytic network. An audio steganographic framework is proposed by (L. Chen et al., 2021)which learns automatically to create steganographic cover audio for inserting messages. The framework has three components. They are the generator, the discriminator and the steganalyzer. Here the stego audio is created by implanting confidential message into steganographic cover audio. Perception quality is high. Traditional LSBM algorithm is applied to embed untold message to steganographic cover audio.

Table 2. Audio Steganography Techniques

Title & publication	**Data set**	**Techniques/ Algorithms**	**Advantage**
(Yang et al., 2019)	700 speech segments from nternet.	Bayesian network code element, Dirichlet distribution	Low bit rate compressed speech

(J. Wu et al., 2020)	TIMIT (40000 samples; 16-bit)	Iterative adversarial examples.	Initial costs are iteratively updated.
(L. Chen et al., 2021)	TIMIT corpus, UME corpus	LSB algorithm, Deep learning methods(Lin-Net, Chen-net)	Perception quality is high

3.3 Text Steganography

Text Steganography is the process of covering secret information within a text.

Sending messages through social media has taken increasing popularity with the advent of smart phones and high speed mobile data. During the transfer of text messages through social media or SMS, end to end safety is very much necessary. To accomplish this, (Taleby Ahvanooey et al., 2018) proposed AITSteg, a novel text Steganography method. A trusted scenario is considered while evaluating AITSteg technique. The parity of Chinese characters' stroke number is analyzed by (K. Wang & Gao, 2019). A binary digit can be expressed by employing the parity and a binary digit string is expressed by its combination. Space mapping concept is exploited. By using the secret binary digit string produced from a secret, a binary search tree is initialized depending on the text from internet and corresponding text is searched by exploiting space mapping concept. Hiding secret messages into ebooks with Electronic PUBlication (EPUB) format is taken as study by (D. C. Wu & Su, 2020). By using the lexographical orders of the selectors and CSS rule declarations, embedding messages into CSS file if e book is done. To increase the capacity of data embedding in CSS file, artificial fake rules are created. For a self-generative cover text, NLP based Markov chain model is proposed by (Gurunath et al., 2021). Between two RNN models .e RNN- Stega and RNN- Generated Lyrics, embedding rate, capacity and many other attributes are contradicted LSTM Neural Network is followed by the RNN model.

Table 3. Text Steganography techniques

Title & publication	Data set	Techniques/ Algorithms	Advantage
(Taleby Ahvanooey et al., 2018)	Social media messages	AITSteg	High embedding capacity, invisible and secure.
(K. Wang & Gao, 2019)	Chinese characters from Internet	Coverless method based on PCCSN feature	High enclosing rate and good concealment.
(D. C. Wu & Su, 2020)	40 CSS files from ebooks in EPUB format	Lexographical orders of selectors, CSS rules	Feasible and robust

(Gurunath et al., 2021)	Twitter posts, news, movie reviews and lyrics	NLP based Markov chain model	High volume and high rate of messages.

3.4 Video steganography

Video cover hiding the confidential data is termed as Video Steganography.

A novel video steganography in H.265 or HEVC is put forward by (J. Wang et al., 2019). Assumed from Intra prediction mode (IPM), Probability distribution 4*4 IPMs is analyzed and then combining with the Coding unit and Prediction Unit. Cover selection rule data is proposed. This improves the Stego Video stream's security performance. To execute the steganography on HEVC video streams, coding example used is matrix coding. This algorithm is easy to implement and maintains video quality and security performance. An outlook to video steganography depending on LSB algorithm and corner point concept is given by (Mstafa et al., 2020). Within the cover video frames, firstly SHI-TOMASHI algorithm is applied to detect the cover points. Then the confidential data is hidden inside the known corner points using 4-LSBs algorithm. Encrypting confidential data is also done using Arnold's cat map method to increase safety. Enclosing data into carrier video might cause errors. This error should be limited. To do that, efficient embedding mapping rule is utilized by (Zhao et al., 2021). The embedding error is analyzed by changing the transfer block decision and partitioning parameters of CB, PB and TB. This helped to enclose unrevealed message and update corresponding residuals.

Combining game theory model's strategy adaptation and cover model's content adaptation, a hybrid model satisfying Kerkhoffs principle is proposed by (K. Niu et al., 2019). Improving the distortion function is done in consonance with H.264 video coding characteristics in UNIWARD algorithm. This function is then used to find out the enclosing probability of every single position in the cover and generate bias function in game theory model. The embedding chance of cover location and the distortion cost function within the developed UNIWARD algorithms generate the new distortion function. This helps to embed information in DCT co-efficient block of H.264 residual. A new concept of Pixogram is introduced by (Rabie & Baziyad, 2019). Pixogram converts individual frames highly uncorrelated spatial areas into correlated temporal segments. This is done in a video segment by using the temporal correlation between same scenes' frames. This maximizes the redundant area for hiding transform domain.

Table 4. Video Steganography techniques

Title & publication	Data set	Techniques/ Algorithms	Advantage
(J. Wang et al., 2019)	Video databases containing traffic, park, party race etc containing 23 YUV sequences	High efficient video coding based on IPM	Good video quality, easy implementation. Cover choosing rule can be combined to other HEVC IPM Steganography.
(Mstafa et al., 2020)	15 video sequences from	LSB, Shi-Tomasi	Secure from salt and pepper,

	YUV video sequences dataset	algorithm and Arnold's cat map	speckle and Gaussian noise attacks.
(Zhao et al., 2021)	Video sequences of resolution 416*240 to 1920*1080	Transfer block decision for H.265 and HEVC	Good visual quality, large enclosing capacity and less bit rate increase.
(K. Niu et al., 2019)	7-segment QCIF format and 4-segment CIF format	UNIWARD, bias function in Game theory model	Good invisibility, highly secure.
(Rabie & Baziyad, 2019)	Gravity.avi, Chappie.avi, train.avi	Pixogram	Increased payload capacity

4 Machine learning in Steganalysis

Now we know that messages are concealed using Steganography. Those messages are detected by means of Steganalysis (Paladion, 2005). This Steganalysis not only detects the hidden message but also sometimes destroys it. Nowadays Steganalysis is performed mostly using Convolutional Neural Networks. Let us take a look on some of the recent works on Steganalysis.

Feature representations are automatically learnt from the text and complex dependencies are captured using Convolutional Neural Network by (Wen et al., 2019). The syntax and semantic feature of words are extracted using the word embedding layer. Next, the sentence features are learnt using different sized rectangular convolution kernels. Long texts are detected using the decision strategy. Accuracy, FNR, Precision and F1 score are employed to calculate the errors. Deep convolutional neural network built for Steganography detectors has some constraints which were corrected by a deep residual architecture by (Boroumand et al., 2019). SRNet that minimizes externally enforced elements to supply accuracy in state of art detection for JPEG Steganography and spatial domain. Noise residuals are computed in the front part of the detector. To prevent stego signal suppression, pooling has been disabled. Selection channel boosts the present performance. SRNet reduces the use of heuristic design elements and has probabilistic effect of fixing in the form of selection channel. Steganalysis is finding the hidden information in Steganography and destroying it. Depending upon the different covers used in Steganography, Steganalysis methods are improved by (Z. Wang, Li, et al., 2019) to capture the changes. In the method, many images from target users are collected and supervised learning algorithm like k-means are employed to improve the performance of trained classifier. This is done with the help of pseudo labels from images. The accuracy is found to be very good when stego images percentage is between 00.3 and 0.7.

3D steganalysis is used to check the hidden information from 3D objects by (Li & Bors, 2020). The distinction between stego objects and cover objects is not done previously which is called cover source mismatch. Steganalyzers face great challenge in differentiating them. Pearson correlation co-efficient and mutual information criterions are the methods used in feature selection. These features are selected from whole lot which is very effective in distinguishing covering items and stego items in the given set of objects. The robustness of the features is taken in to consideration. RRFS algorithm is proposed whose two versions are discussed. The 1st uses PCC and 2nd uses MIC. The Robustness of the features is evaluated by

the algorithm. Three different data hiding methods are considered. A new CNN network structure is designed, where deduction accuracy of special domain steganography is improved by (Zhang et al., 2020). In the pre-processing layer, convolution kernels are optimized by using 3X3 Kernels. Separable convolutions are used. This helps to:

- Apply Channel correlation of residuals.
- Image substance compression.
- Signal -To-Noise ratio increased

Spatial pyramid pooling is used to enhance the ability of representation. Data augmentation is used to raise performance of network.

A novel steganalysis method is introduced to detect all steganography types with Q factor between 99 and 100. Rounding errors when decompressing JPEG image, exhibits Gaussian distribution with 1/12 as variance which increased on steganographic embedding on DCT co efficient. This helps in accurate detection. The approach from(Butora& Fridrich, 2020)is named as "reverse JPEG Compatibility attack". The attack is examined based on statistical signal detection using reasoning under simple assumptions. Machine learning tools provide best detection practice. The method proves good with a variety of JPEG compressions on diverse datasets of color and grey scale images and with five steganographic schemes. Importance of data security is explained in terms of steganography and steganalysis by (Jung, 2019). Categories of steganography based on the cover media used and divisions of steganalysis like visual, statistical, structural and learning are discussed. The authors also reviewed on the frameworks like Tensor flow, Keras, Scikit learn which are used to develop machine learning algorithms. Finally the process of machine learning for steganalysis is briefly unfolded.

As the existing CNN based steganalysis algorithms combine the output of separately trained networks with same architecture, a popular CNN model including ensemble classification strategy is presented by (Su & Zhao, 2019). The method can be employed in boosting detection accuracy in spatial and JPEG steganography by some steganalysis based on CNN with the given architecture. An optimized novel voting fusion structure is also proposed. This method upgrades the execution of CNN based steganalysis. Space to train well designed base learners is also constructed. Based on deep Q network, a selective collective process in image steganalysis is given by (Ni et al., 2019). This method combines reinforcement learning with CNN and they are not seen in collective pruning. Deep Q Network is an ensemble optimization method. Feature extraction methods such as GFR, SRM and maxSRMd2 are employed. When images are intentionally resized by nearest-neighbour interpolation, performance of CNN is disturbed. To solve this, a pre-processing is proposed for intentional image down sampling by (Kato et al., 2020). In both resized original and steganographic images, additional steganographic signals are embedded. These signals get embedded in same pixels of resized images. So the special frequency differences are apparent. This helps CNN to learn features. As the vast existing deep learning based steganalysis resulted in huge cost and storage, the authors (Tan et al., 2021)proposed a Channel pruning drawn deep residual network architecture, where the network structure is shrinked. This is done by combining two network pruning schemes with a hybrid criterion in a data-driven manner. The network resulted seemed to be in a slim and bottleneck like structure.

GBRAS-net is a novel CNN architecture from (Reinel et al., 2021). The Softmax activation function is applied towards the end here. The pre-processing step uses filter banks to increase steganographic noise. The feature extraction step uses depth-wise separable convolutional layers. To improve the traditional text

steganalysis methods, a hybrid method combining BI-LSTM Recurrent Neural Network and CNN is proposed by (Y. Niu et al., 2019). Long term semantic information of texts is captured by BI-LSTM and local connections between words are extracted by Asymmetric CNN. The method is designed to handle different steganographic algorithms very effectively. Semantic feature space which is high dimensional is visualized. Data is obtained from Twitter, IMDB and Gutenberg.

Table 5. Steganalysis Techniques and Datasets

Title & Publication	Data set	Techniques/ Algorithms/ Architecture	Advantages	Disadvantages/ future work
(Wen et al., 2019)	COCO, Gutenberg	Simple CNN architecture is designed using the principle of Occam's Razor	Decision strategy is proposed to increase long text performance	Advanced frame like RNN and Attention Mechanism can be used to design new steganalysis architecture.
(Boroumand et al., 2019)	BOSSBase BOWS2	SRNet, spatial-domain embedding methods such as WOW, HILL, MiPOD, S-UNIWARD	Reducing the use of heuristic design elements, Using selection channel for JPEG domain	Inner workings of steganographic techniques should be monitored
(Z. Wang, Li, et al., 2019)	BOSSbase ver.1.01, UCID	*k*-means, SUNIWARD and WOW(for steganography) SRM and PSRM (feature extraction)	Even a very smaller set of suspected images, the method works well	Should recognize steganography users and then conduct a Performance comparison.
(Li & Bors, 2020)	AIM@SHAPE, FOCUS K3D, Shape retrieval contest 2007	RRFS algorithm using PCC and MIC	Use of three varying data hiding methods	Limited transformation sets are used.
(Zhang et al., 2020)	BOSSBase v1.01 BOWS2	S-UNIWARD, WOW and HILL CNN network-Zhu-Net, Spatial Pyramid Pooling	Number of parameters is reduced by better convolution kernels; Residual is used in pre-processing layer; mapping to fixed dimensions are done by SPP-module.	To measure how the development in the network shape impacts on the working of the steganographic Analyzer.
(Butora & Fridrich, 2020)	BOSSbase 1.01 BOWS2,	Detectors : e-SRNet, e-GFR, e-Hist Embedding	Training the detector in one embedding algorithm makes it applicable in other	For spatial domain embedding, decompressed JPEGs should not

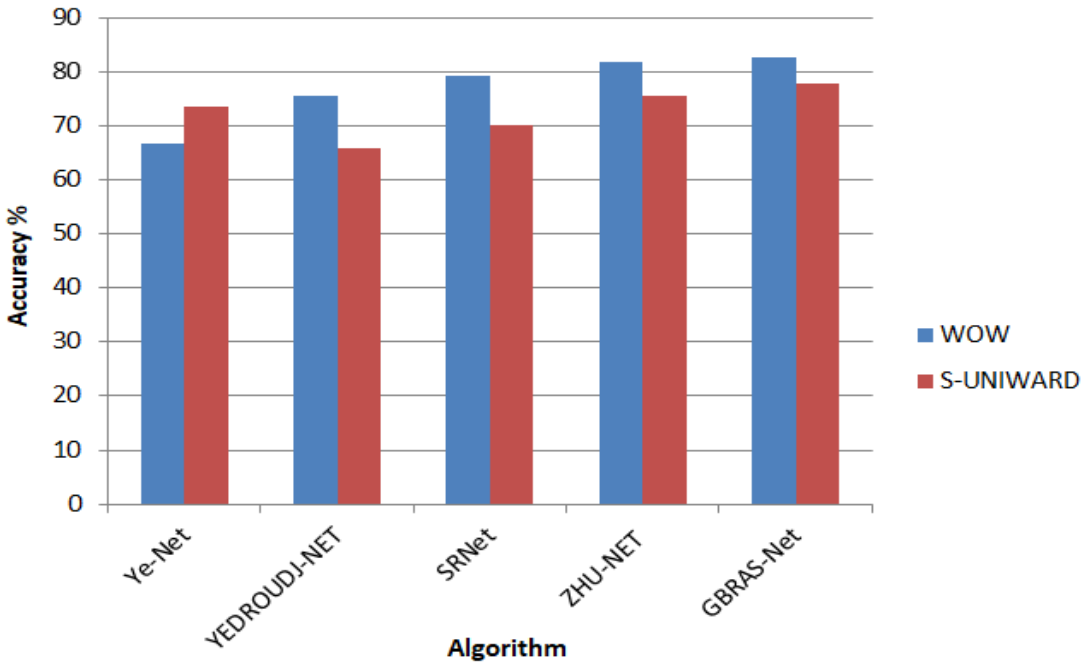
		algorithms: nsF5, J-UNIWARD, Jsteg	embedding algorithms.	be used.
(Y. Niu et al., 2019)	Twitter, IMDB, Gutenberg	R-BILSTM-C combining Bi-LSTM and CNN	Both the long term text semantic information and local features are captured to improve efficiency.	-
(Su & Zhao, 2019)	BOSSBase	CAECS S-UNIWARD J-UNIWARD	One model is trained to produce a group. Detection accuracy is boosted in both spatial and JPEG steganography.	New ways to create subspaces to be exploited.
(Ni et al., 2019)	BOSSbase 1.01	Ensemble optimization method ground on Deep Q Network. S-UNIWARD J-UNIWARD	Automatically the machine can find two goals to meet the goal state at the same time.	-
(Kato et al., 2020)	BOSSbase 1.01	CNN based SRNet, Xu-Net	Less training time for the pre-processing layer	More practical way should be devised, which yields Comparable effectiveness.
(Tan et al., 2021)	BOSSbase 1.01 BOWS2, ImageNet, ALASKA	Deep Residual Network CALPA-NET	achieve good detection execution with a less % of the model size and a minimum proportion of working cost.	To develop self-adaptive deep learning steganalyzers without introducing parameters.
(Reinel et al., 2021)	BOSSBase BOWS2	CNN architechture-GBRAS-Net WOW, MiPOD, S-UNIWARD, HILL HUGO	Huge capacity to find adaptive steganography in spatial domain.	New techniques to be incorporated and techniques to improve pre-processing stage should be worked on.

Accuracy percentage of various CNN architectures in Steganalysis is found to be increasing from the previous one to the other (Refer Table 6).

Table 6. Percentage of Accuracy in various CNN architectures using BOSSbase 1.01 data and BOWS 2 for training (Reinel et al., 2021)

Algorithm	Payload	WOW	S-UNIWARD
Ye-Net	0.2bpp	73.6	65.1
YEDROUDJ-NET		75.7	65.9
SRNet		79.4	70.1
ZHU-NET with ReLU and Optimized kernels		82.0	75.7
GBRAS-Net		82.7	77.9

Fig. 4. Accuracy percentage of various Algorithms



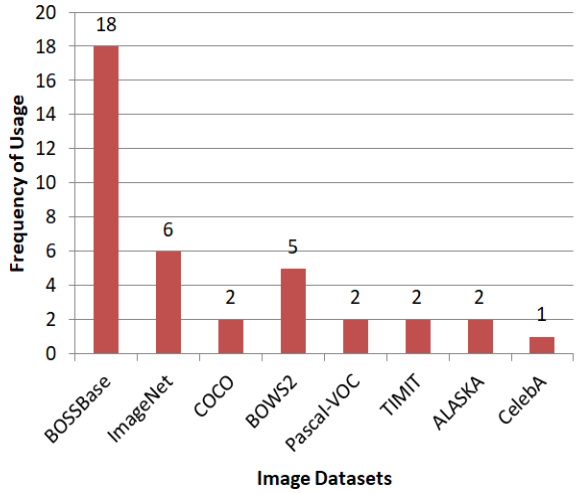
5 Dataset for Steganography and Steganalysis

It could be noted that the BOSSBase 1.01 and BOWS2 are the popular datasets used in image Steganography and Steganalysis. Some articles use other image sets like CelebA, ALASKA, COCO and ImageNet. The usage frequency of the popular datasets in the reviewed articles is given in the table below.

Table 7. Usage frequency of Datasets in Steganography and Steganalysis

Dataset	References	Usage frequency
BOSSbase 1.01	(Boroumand et al., 2019) (Z. Wang, Li, et al., 2019) (Zhang et al., 2020) (Butora & Fridrich, 2020) (Su & Zhao, 2019) (Ni et al., 2019) (Kato et al., 2020) (Tan et al., 2021) (Reinel et al., 2021) (Tang et al., 2021) (Tang et al., 2019) (Lu et al., 2021) (Chang, 2020) (Zhou et al., 2020) (Xu et al., 2016) (You et al., 2021) (Yedroudj et al., 2018) (Ye et al., 2017)	18
ImageNet	(Tan et al., 2021) (Duan et al., 2019) (Duan, Guo, et al., 2020) (Duan, Wang, et al., 2020) (Duan, Nao, et al., 2020) (Zhang et al., 2019)	6
COCO	(Wen et al., 2019) (Z. Wang, Gao, et al., 2019)	2
BOWS2	(Tan et al., 2021) (Reinel et al., 2021) (Butora & Fridrich, 2020) (Zhang et al., 2020) (Ye et al., 2017)	5
Pascal-VOC	(F. Chen et al., 2020) (Zhang et al., 2019)	2
TIMIT	(L. Chen et al., 2021) (J. Wu et al., 2020)	2
CelebA	(Naito & Zhao, 2019)	1
ALASKA	(Tang et al., 2021) (Tan et al., 2021)	2

Fig. 5. Frequency of dataset Usage in literature



6 Conclusion

The study reveals the different types of Steganography and the popular Machine Learning algorithms and also the Deep learning techniques applied in Steganalysis. This review has also discussed on the Datasets, the techniques used and the advantages and disadvantages of some of the recent articles. Traditionally LSB technique was applied in Steganography. In recent trend as Machine learning and Deep learning have taken their path, CNN and GAN are mostly applied in many experiments in analyzing Steganography.

References

Ashraf, Z., Roy, M. L., Muhuri, P. K., & Lohani, Q. M. D. (2020). Interval type-2 fuzzy logic system based similarity evaluation for image steganography. Heliyon, 6(5), e03771. https://doi.org/10.1016/j.heliyon.2020.e03771

Boroumand, M., Chen, M., & Fridrich, J. (2019). Deep residual network for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 14(5), 1181–1193. https://doi.org/10.1109/TIFS.2018.2871749

Butora, J., & Fridrich, J. (2020). Reverse JPEG Compatibility Attack. IEEE Transactions on Information Forensics and Security, 15(c), 1444–1454. https://doi.org/10.1109/TIFS.2019.2940904

Cao, P., He, X., Zhao, X., & Zhang, J. (2019). Approaches to obtaining fingerprints of steganography tools which embed message in fixed positions. Forensic Science International: Reports, 1(July), 100019. https://doi.org/10.1016/j.fsir.2019.100019

Chang, C. C. (2020). Adversarial Learning for Invertible Steganography. IEEE Access, 8, 198425–198435. https://doi.org/10.1109/ACCESS.2020.3034936

Chen, F., Xing, Q., & Liu, F. (2020). Technology of Hiding and Protecting the Secret Image Based on Two-Channel Deep Hiding Network. IEEE Access, 8, 21966–21979. https://doi.org/10.1109/ACCESS.2020.2969524

Chen, L., Wang, R., Yan, D., & Wang, J. (2021). Learning to Generate Steganographic Cover for Audio Steganography Using GAN. IEEE Access, 9, 88098–88107. https://doi.org/10.1109/ACCESS.2021.3090445

Cho, D. X., Thuong, D. T. H., & Dung, N. K. (2018). A Method of Detecting Storage Based Network Steganography Using Machine Learning. Procedia Computer Science, 154, 543–548. https://doi.org/10.1016/j.procs.2019.06.086

Choudary, A. (n.d.). Steganography Tutorial – A Complete Guide For Beginners. Edureka. https://www.edureka.co/blog/steganography-tutorial

Dickson, B. (2020). What is steganography? A complete guide to the ancient art of concealing messages. https://portswigger.net/daily-swig/what-is-steganography-a-complete-guide-to-the-ancient-art-of-concealing-messages

Dr.Souvik Bhattacharyya, Dr- Indradip Banerjee, P. . G. S. (2011). Data Hiding Through Multi Level Steganography and SSCE. 2.

Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A New High Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network. IEEE Access, 8, 25777–25788. https://doi.org/10.1109/ACCESS.2020.2971528

Duan, X., Jia, K., Li, B., Guo, D., Zhang, E., & Qin, C. (2019). Reversible image steganography scheme based on a U-net structure. IEEE Access, 7, 9314–9323. https://doi.org/10.1109/ACCESS.2019.2891247

Duan, X., Nao, L., Mengxiao, G., Yue, D., Xie, Z., Ma, Y., & Qin, C. (2020). High-capacity image steganography based on improved FC-Densenet. IEEE Access, 8, 170174–170182. https://doi.org/10.1109/ACCESS.2020.3024193

Duan, X., Wang, W., Liu, N., Yue, D., Xie, Z., & Qin, C. (2020). StegoPNet: Image steganography with generalization ability based on pyramid pooling module. IEEE Access, 8, 195253–195262. https://doi.org/10.1109/ACCESS.2020.3033895

Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. (2020). An image steganography approach based on k-least significant bits (k-LSB). 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020, February, 131–135. https://doi.org/10.1109/ICIoT48696.2020.9089566

Fathi-Kazerooni, S., & Rojas-Cessa, R. (2020). GAN Tunnel: Network Traffic Steganography by Using GANs to Counter Internet Traffic Classifiers. IEEE Access, 8, 125345–125359. https://doi.org/10.1109/ACCESS.2020.3007577

Gurunath, R., Alahmadi, A. H., Samanta, D., Khan, M. Z., & Alahmadi, A. (2021). A Novel Approach for Linguistic Steganography Evaluation Based on Artificial Neural Networks. IEEE Access, 9, 120869–120879. https://doi.org/10.1109/ACCESS.2021.3108183

Jung, K. H. (2019). A study on machine learning for steganalysis. ACM International Conference Proceeding Series, 12–15. https://doi.org/10.1145/3310986.3311000

Kato, H., Osuge, K., Haruta, S., & Sasase, I. (2020). A preprocessing by using multiple steganography for intentional image downsampling on CNN-based steganalysis. IEEE Access, 8, 195578–195593. https://doi.org/10.1109/ACCESS.2020.3033814

Li, Z., & Bors, A. G. (2020). Selection of Robust and Relevant Features for 3-D

Steganalysis. IEEE Transactions on Cybernetics, 50(5), 1989–2001. https://doi.org/10.1109/TCYB.2018.2883082

Lu, W., Xue, Y., Yeung, Y., Liu, H., Huang, J., & Shi, Y. Q. (2021). Secure Halftone Image Steganography Based on Pixel Density Transition. IEEE Transactions on Dependable and Secure Computing, 18(3), 1137–1149. https://doi.org/10.1109/TDSC.2019.2933621

Margie Semilof, C. C. (2021). What is steganography? https://www.techtarget.com/searchsecurity/definition/steganography

Meng, R., Cui, Q., Zhou, Z., Fu, Z., & Sun, X. (2019). A Steganography Algorithm Based on CycleGAN for Covert Communication in the Internet of Things. IEEE Access, 7, 90574–90584. https://doi.org/10.1109/ACCESS.2019.2920956

Mstafa, R. J., Younis, Y. M., Hussein, H. I., & Atto, M. (2020). A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector. IEEE Access, 8, 161825–161837. https://doi.org/10.1109/ACCESS.2020.3021356

Naito, H., & Zhao, Q. (2019). A New Steganography Method Based on Generative Adversarial Networks. 2019 IEEE 10th International Conference on Awareness Science and Technology, ICAST 2019 - Proceedings, 1–6. https://doi.org/10.1109/ICAwST.2019.8923579

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. https://doi.org/10.1109/LSP.2019.2913018

Niu, K., Li, J., Yang, X., Zhang, S., & Wang, B. (2019). Hybrid Adaptive Video Steganography Scheme under Game Model. IEEE Access, 7, 61523–61533. https://doi.org/10.1109/ACCESS.2019.2902464

Niu, Y., Wen, J., Zhong, P., & Xue, Y. (2019). A Hybrid R-BILSTM-C Neural Network Based Text Steganalysis. IEEE Signal Processing Letters, 26(12), 1907–1911. https://doi.org/10.1109/LSP.2019.2953953

Paladion. (2005). Steganalysis.

Rabie, T., & Baziyad, M. (2019). The Pixogram: Addressing High Payload Demands for Video Steganography. IEEE Access, 7, 21948–21962. https://doi.org/10.1109/ACCESS.2019.2898838

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, 9, 14340–14350. https://doi.org/10.1109/ACCESS.2021.3052494

Saad, A. H. S., Mohamed, M. S., & Hafez, E. H. (2021). Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning. IEEE Access, 9, 16522–16531. https://doi.org/10.1109/ACCESS.2021.3050737

Su, A., & Zhao, X. (2019). Boosting Image Steganalysis under Universal Deep Learning Architecture Incorporating Ensemble Classification Strategy. IEEE Signal Processing Letters, 26(12), 1852–1856. https://doi.org/10.1109/LSP.2019.2950081

Taleby Ahvanooey, M., Li, Q., Hou, J., Dana Mazraeh, H., & Zhang, J. (2018). AITSteg: An innovative text steganography technique for hidden transmission of text message via social media. IEEE Access, 6, 65981–65995. https://doi.org/10.1109/ACCESS.2018.2866063

Tan, S., Wu, W., Shao, Z., Li, Q., Li, B., & Huang, J. (2021). CALPA-NET: Channel-Pruning-Assisted Deep Residual Network for Steganalysis of Digital Images. IEEE Transactions on Information Forensics and Security, 16(c), 131–146. https://doi.org/10.1109/TIFS.2020.3005304

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. https://doi.org/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. https://doi.org/10.1109/TIFS.2019.2891237

Wang, J., Jia, X., Kang, X., & Shi, Y. Q. (2019). A Cover Selection HEVC Video Steganography Based on Intra Prediction Mode. IEEE Access, 7, 119393–119402. https://doi.org/10.1109/ACCESS.2019.2936614

Wang, K., & Gao, Q. (2019). A Coverless Plain Text Steganography Based on Character Features. IEEE Access, 7, 95665–95676. https://doi.org/10.1109/ACCESS.2019.2929123

Wang, Z., Gao, N., Wang, X., Xiang, J., & Liu, G. (2019). STNet: A Style Transformation Network for Deep Image Steganography. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 11954 LNCS. Springer International Publishing. https://doi.org/10.1007/978-3-030-36711-4_1

Wang, Z., Li, S., & Zhang, X. (2019). Towards Improved Steganalysis: When Cover Selection is Used in Steganography. IEEE Access, 7, 168914–168921. https://doi.org/10.1109/ACCESS.2019.2955113

Wen, J., Zhou, X., Zhong, P., & Xue, Y. (2019). Convolutional neural network based text steganalysis. IEEE Signal Processing Letters, 26(3), 460–464. https://doi.org/10.1109/LSP.2019.2895286

wikipedia. (n.d.). Steganography-wikipedia.

Wu, D. C., & Su, H. Y. (2020). Steganography via E-Books with the EPUB format by rearrangements of the contents of the CSS Files. IEEE Access, 8, 20459–20472. https://doi.org/10.1109/ACCESS.2020.2966889

Wu, J., Chen, B., Luo, W., & Fang, Y. (2020). Audio Steganography Based on Iterative Adversarial Attacks against Convolutional

Neural Networks. IEEE Transactions on Information Forensics and Security, 15(XX), 2282–2294. https://doi.org/10.1109/TIFS.2019.2963764

Xu, G., Wu, H. Z., & Shi, Y. Q. (2016). Structural design of convolutional neural networks for steganalysis. IEEE Signal Processing Letters, 23(5), 708–712. https://doi.org/10.1109/LSP.2016.2548421

Yang, J., Liu, P., & Li, S. (2019). A common method for detecting multiple steganographies in low-bit-rate compressed speech based on bayesian inference. IEEE Access, 7, 128313–128324. https://doi.org/10.1109/ACCESS.2019.2939629

Yang, J., Ruan, D., Huang, J., Kang, X., & Shi, Y. Q. (2020). An Embedding Cost Learning Framework Using GAN. IEEE Transactions on Information Forensics and Security, 15, 839–851. https://doi.org/10.1109/TIFS.2019.2922229

Ye, J., Ni, J., & Yi, Y. (2017). Deep Learning Hierarchical Representations for Image Steganalysis. IEEE Transactions on Information Forensics and Security, 12(11), 2545–2557. https://doi.org/10.1109/TIFS.2017.2710946

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, 2018-April(1), 2092–2096. https://doi.org/10.1109/ICASSP.2018.8461438

You, W., Zhang, H., & Zhao, X. (2021). A Siamese CNN for Image Steganalysis. IEEE Transactions on Information Forensics and Security, 16, 291–306. https://doi.org/10.1109/TIFS.2020.3013204

Zhang, R., Dong, S., & Liu, J. (2019). Invisible steganography via generative adversarial networks. Multimedia Tools and Applications, 78(7), 8559–8575. https://doi.org/10.1007/s11042-018-6951-z

Zhang, R., Zhu, F., Liu, J., & Liu, G. (2020). Depth-Wise Separable Convolutions and Multi-Level Pooling for an Efficient Spatial CNN-Based Steganalysis. IEEE Transactions on Information Forensics and Security, 15, 1138–1150. https://doi.org/10.1109/TIFS.2019.2936913

Zhao, H., Liu, Y., Wang, Y., Liu, S., & Feng, C. (2021). A Video Steganography Method Based on Transform Block Decision for H.265/HEVC. IEEE Access, 9, 55506–55521. https://doi.org/10.1109/ACCESS.2021.3059654

Zhou, L., Feng, G., Shen, L., & Zhang, X. (2020). On Security Enhancement of Steganography via Generative Adversarial Image. IEEE Signal Processing Letters, 27(c), 166–170. https://doi.org/10.1109/LSP.2019.2963180