Simulation of Steganalysis using CNN

Manushree Joshi[1] Mohammad Kaif Khan[2] Shivani Singh[3] Yash Sahni[4]
[1,2,3,4]Department of Computer Science and Engineering
[1,2,3,4]Institute of Technology and Management, Gorakhpur, India

Abstract — Steganography is a technique of data hiding that embeds the secret message inside a digital media for providing a method of invisible communication. Different kinds of digital file formats can be used for steganography of which digital images are the most popular as it is present in a massive number in the internet. There exists a large variety of steganographic techniques, for hiding secret information in image. Several efforts are made to establish ways of detecting whether or not an image contains a steganographic element. Steganalysis is the technique of detecting the presence of steganography that can serve as an effective way to judge the security performance of steganographic techniques. In this paper, we provide an overview of digital image Steganalysis technique for detecting steganographic method and identify the area to look out for the hidden information. These techniques are discussed and analyzed in terms of their ability to detect secret message in an image file. We have also reviewed some researches on steganography. The main aim of this paper is to review the previous work done and available ways, present trends and discuss the challenges that are currently available in the studies. Along with these, the datasets that are commonly used and publicly available, the evaluation metrics considered are also discussed.

Keywords: Combustion Ignition (CI) Engine, Diesel, Mahua Oil Bio-Diesel, Efficiency and Emissions

I. INTRODUCTION

Technology has blitz scaled over the past years which is leading to a wide usage of multimedia for transferring data, especially Internet of Things (IoT). Usually, these transfers take place over insecure network channels. In particular, the internet came across accelerated popularity for exchanging digital media and individuals, private companies, institutions, governments use these multimedia data transfer methods for exchanging data. Though there are number of advantages attached with it, one prominent drawback is the privacy and security of the data. There are numbers of tools available already which are capable of exploiting the privacy, data integrity and security of the data being transmitted which has made the possibility of malicious threats, eavesdropping and other subversive activities. A new research topic, steganography, has gained acceptance in this context to hide the data that is not perceptible to human eyes.

Techniques of information hiding have been available for a long time but recently their importance has been accelerated. The main reason behind this is the increase in the data traffic through the internet and social media networks. Steganography, which is used to hide the information in plain sight, allows the use of wide variety of the secret information forms like image, text, audio, video and files. Cryptography is the popular method used in the field of information hiding, but, steganography has gained popularity in recent times.

Steganography can be defined as the procedure of hiding a secret small multimedia data inside another but much larger multimedia data such as image, text, file or video. Image steganography is a technique to hide an image inside any other image. In image steganography, the cover image is manipulated in such a way that the hidden data is not visible thus making it non-suspicious as in the case of cryptography. Inversely, Steganalysis is used to detect the presence of any secret message covered in the image and to extract the hidden data. Steganalysis is a process of classifying if the image is either a stego image or a normal image. Apart from classifying the image, further investigation is carried out to detect the location and the content of the secret image inside the cover image.

With the availability of massive amounts of data, deep learning (DL) has become the trend and is extensively used for many applications. Deep learning is a useful tool in various applications like image classification, automatic speech recognition, image recognition, natural language processing, recommendation systems, processing of medical images. Though research on steganography is quite recent, it has benefited from DL methods including Convolutional Neural Networks (CNNs) Generative Adversarial Networks (GANs) based methods and their deployment in both steganography and Steganalysis.

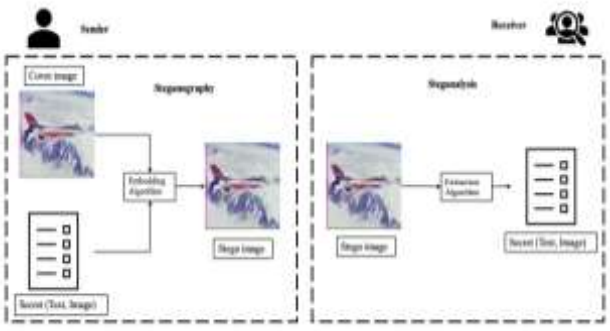

Fig. 1: General working principle of Steganography and Steganalysis.

II. RELATED WORK AND STUDY

A. Paper 1- BOSS: Break Our Steganographic System

Discussion: During the years 2005 and 2007, the data-hiding community supported by the European Network of Excellence in Cryptology (ECRYPT) launched two watermarking challenges, BOWS and BOWS-2 (abbreviations of Break Our Watermarking System). The purpose of participants of both challenges was to break watermarking systems under different scenarios. The purpose of organizers was not only to assess the robustness and the security of different watermarking schemes in the environment similar to real application, but to increase the interest in watermarking and to boost the research progress within the field. Both watermarking contests showed to be popular (BOWS/BOWS2 played more than 300/150 domains and 10/15 participants respectively were ranked), and novel approaches towards breaking watermarking systems were

derived during them. This, combined with a thrill associated with organization and participation, inspired us to organize the BOSS (Break Our Steganographic System) challenge. The most important motivation for the contest was to investigate whether content-adaptive steganography improves steganographic security for empirical covers. For the purpose of this contest, a new spatial-domain content-adaptive algorithm called HUGO (Highly Undetectable steGO) was invented. The fact that in adaptive steganography the selection channel (placement of embedding changes) is publicly known, albeit in a probabilistic form, could in theory be exploited by an attacker. Adaptive schemes introduce more embedding changes than non-adaptive schemes because some pixels are almost forbidden from being modified, which causes an adaptive scheme to embed with a larger change rate than a non-adaptive one. On the other hand, the changes are driven to hardtop-model regions; because the change rate is not an appropriate measure of statistical detect ability as it puts the same weight to all pixels. As compared by the state-of-the-art available in mid 2010, HUGO was largely resistant to steganalysis up to 0.4 bits per pixel in 512 × 512 grayscale images. The other incentive for organizing the challenge was a hope to encourage the development of new approaches toward steganalysis, pointing to important deadlocks in steganalysis and hopefully finding solutions to them, finding weaknesses of the proposed steganographic system, and finally raising interest in steganalysis and steganography. While running the contest, we became aware of a similar contest organized within the computer vision community. This paper serves as an introduction to a series of papers describing the attacks on HUGO. Here, we describe the contest, image databases, and the HUGO algorithm to give the papers uniform notation and background.

Conclusion: Break Our Steganographic System (BOSS) is the first scientific challenge conducted to take image steganography from being a research topic to a practical application. The main aim of the competition was to develop a better Steganalysis method that can break the steganographic images created by the HUGO (Highly Undetectable steGO) algorithm. The dataset consists of a training set and testing set along with the HUGO algorithm that can be used to create the steganography images. The training dataset consists of 10,000 grayscale cover images with dimensions 512×512. The testing set consists of 1000 grayscale images with dimensions 512×512. There is an option to download the datasets with steganography images solely for the purpose of steganalysis. Firstly, the raw images are captured using 7 different cameras and they are converted to PGM images.

B. Paper 2- CelebA

Discussion: Predicting face attributes in the wild is challenging due to complex face variations. We propose a novel deep learning framework for attribute prediction in the wild. It cascades two CNN2s, LNet and ANet, which are fine-tuned jointly with attribute tags, but pre-trained differently. LNet is pre-trained by massive general object categories for face localization, while ANet is pre-trained by massive face identities for attribute prediction. This framework not only outperforms the state-of-the-art with a large margin, but also reveals valuable facts on learning face representation.It shows how the performances of face localization (LNet) and attribute prediction (ANet) can be improved by different pre-training strategies. It reveals that although the filters of LNet are fine-tuned only with image-level attribute tags, their response maps over entire images have strong indication of face locations. This fact enables training LNet for face localization with only image-level annotations, but without face bounding boxes or landmarks, which are required by all attribute recognition works. It also demonstrates that the high-level hidden neurons of ANet automatically discover semantic concepts after pre-training with massive face identities, and such concepts are significantly enriched after fine-tuning with attribute tags. Each attribute can be well explained with a sparse linear combination of these concepts.

Conclusion: Large-scale CelebFaces Attributes dataset, also known as CelebA dataset, is a vast dataset with more than 200K images that can be used for face recognition, face detection, face localization and other face-related operations. The dataset consists of images from various sources, locations, background and poses and is best suitable for steganography also. The probability of using a photo/face image as the cover for hiding secret images is very high. Along with the images, there are 40 different annotations available like with/without glasses, emotions, hair styles, other accessories like hat.

C. Paper 3- ImageNet

Discussion: The explosion of image data on the Internet has the potential to foster more sophisticated and robust models and algorithms to index, retrieve, organize and interact with images and multimedia data. But exactly how such data can be harnessed and organized remains a critical problem. We introduce here a new database called “ImageNet”, a large-scale ontology of images built upon the backbone of the WordNet structure. ImageNet aims to populate the majority of the 80,000 synsets of WordNet with an average of 500–1000 clean and full resolution images. This will result in tens of millions of annotated images organized by the semantic hierarchy of WordNet. This paper offers a detailed analysis of ImageNet in its current state: 12 subtrees with 5247 synsets and 3.2 million images in total. We show that ImageNet is much larger in scale and diversity and much more accurate than the current image datasets. Constructing such a large-scale database is a challenging task. We describe the data collection scheme with Amazon Mechanical Turk. Lastly, we illustrate the usefulness of ImageNet through three simple applications in object recognition, image classification and automatic object clustering. We hope that the scale, accuracy, diversity and hierarchical structure of ImageNet can offer unparalleled opportunities to researchers in the computer vision community and beyond.

Conclusion- ImageNet is also a very large dataset containing images from the WordNet hierarchy with each node containing more than 500 to 1000 images. ImageNet does not have any copyrights to the image and contains only the links or thumbnails to the original image. The dataset consists of images of varying size. Based on the requirement, the number of images, classes they belong to, background and the image size can be selected from the wide range available.

III. PROPOSED MODELLING

A. Traditional-Based Steganography Method

Conventionally, Least Significant Bits (LSB) substitution method is employed to perform image steganography. Images are usually of higher pixel quality, out of which few pixels are used. LSB methods works under the assumption that modifying a few pixel values would not show any visible changes. The secret information is converted into a binary form. The cover image is scanned to determine the least significant bits in the noisy area. The binary bits from the secret image are then substituted in the LSBs of the cover image. As overloading the cover image may lead to visible changes, the presence of the secret information may be leaked; hence, the substitution method has to be performed cautiously.

B. GAN-Based Steganography Methods

General Adversarial Networks are a type of deep CNN. It was introduced by Goodfellow et al. in 2014.In GAN, the generator and discriminator networks are the two networks that compete against each other to generate a perfect image in GAN architecture. The generator model is given the data which generates the output that is a close approximation of the given input image. The discriminator networks discriminate the generated output and classify the images generated as either fake or real. These two networks are trained in such a way that the generator model tries to imitate the input data as close as possible with minimum noise. The discriminator model is trained to effectively find out the fake images. Many variations on GAN have been proposed since it is introduced, making it more powerful and suitable for synthetic image generative tasks.

GANs have a good performance in the image generation field when compared to the traditional and CNN methods. Image steganography can be considered as one such image generation task where two inputs – the cover image and the secret image are given to generate one output – stego image. The existing methods used for image steganography using a GAN architecture can be grouped into five categories - a three network based GAN model, cycle-GAN based architectures, sender-receiver architecture using GAN, coverless model where the cover image is generated randomly instead of being given as input.

Generally, a GAN model consists of two main components: the generator and the discriminator. A new network named, the steganalyzer is introduced in some of the methods in Image steganography. The main functions of these three components of GAN model are as follows-

- A generator model, G, to generate stego images from the cover image and the random message.
- A discriminator model, D, to classify the generated images from the generator as either real or fake.
- A steganalyzer, S, to check is the input image has a confidential secret data or not.

The model we have used in this project is the Convolutional Neural Network model:

C. CNN-Based Steganography Methods

Image steganography using CNN models is mainly inspired from the encoder-decoder architecture. Two inputs – cover image and the secret image are fed as the input to the encoder to generate the stego image and the stego image is given as input to the decoder to output the embedded secret image. The basic principle is the same except different methods have tried different architectures. The way the input cover image and the secret image are concatenated are also different in different approaches while the Variations in the convolutional layer, pooling layer are expected. The number of filters used, strides, filter size, activation function used and loss function vary from method to method. An important point to note here is that the size of the cover image and the secret image has to be same, so every pixel of the secret image is distributed in the cover image.

Convolutional Neural Networks have shown to learn structures that correspond to logical features. These features increase their level of abstraction as we go deeper into the network. Firstly, the ConvNet will have a good idea about the patterns of natural images, and will be able to make decisions on which areas are redundant, and more pixels can be hidden there. By saving space on redundant areas, the amount of hidden information can be increased. The exact way in which the network will hide the information cannot be known to anybody who doesn't have the weights because the architecture and the weights can be randomized, to concatenate the cover image and the secret image, a Separable Convolution with Residual Block (SCR) is used. The embedded image is given as the input to the encoder for constructing the stego image which is fed to the decoder to output the decoded secret image. To obtain this, ELU (Exponential Linear Unit) and Batch normalization are used. A new cost function, called the variance loss is proposed to reduce the effect of noise in the generated container image An encoder-decoder architecture was proposed by Rahim et al. in. This method differs from the others in the way the inputs are given. The encoder part consists of two parallel architectures each for the cover and the secret image. Features from the cover image and the secret images are extracted through the convolutional layer and concatenated. The stego image is constructed with the help of these concatenated features.

The model is composed of three parts: The Preparation Network, Hiding Network (Encoder) and the Reveal Network. The goal of this model is to be able to encode information about the secret image S into the cover image C, generating C_prime that closely resembles C, while still being able to decode information from C_prime to generate the decoded secret image S_prime. This decoded image S_prime should resemble the secret image S as closely as possible. The Preparation Network is responsible for preparing data from the secret image that is to be concatenated with the cover image and later fed to the Hiding Network. The Hiding Network working on it further transforms that input into the encoded cover image C_prime. It is noted here that the loss function for the Reveal Network is different from the loss function for the Preparation and Hiding Networks.

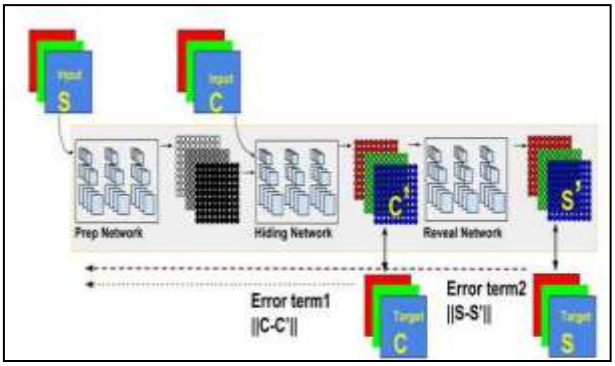

Fig. 2: General working of CNN model.

IV. TECHNIQUES USED

Steganalysis is the technology that tries to defeat steganography by detecting the hidden data and extracting or destroying it. Steganalysis is the procedure of detecting steganography by viewing at variances between bit patterns and unusually high file sizes. It is the art of finding and rendering meaningless covert messages.The main objective of steganalysis is to recognize suspected data streams, determine whether or not they have hidden messages encoded into them, and, if applicable, recover the hidden data.

Steganalysis generally begins with several suspect data streams but uncertainty whether any of these include hidden message. The steganalyst starts by decreasing the group of suspect data streams to a subset of most likely altered data streams. This is generally completed with statistical analysis using advanced statistics techniques.

A. Techniques used

Unusual patterns − Unusual patterns in a stego image are incredulous. For instance, there are some disk analysis services that can filter hidden data in unused division in storage devices.

Filters can also be used to recognize TCP/IP packets that include hidden or invalid information in the packet headers. TCP/IP packets can be used to transport data across the Internet have unutilized or reserved area in the packet headers.

Visual detection − Analyzing repetitive patterns can reveal the recognition of a steganography tool or hidden data. It can be examined these patterns as the method is to analyze the initial cover image with the stego image and detectable differences. This is known as known-carrier attack.

By comparing several images it is possible that patterns appear as signatures to a steganography tool. There are another visual clue to the presence of hidden data is padding or cropping of an image. With some stego tools if an image does not suitable into a fixed size it is cropped or padded with black spaces. There can also be a difference in the file size among the stego-image and the cover image. Another indicator is a large increase or decrease in the number of specific colors, or colors in a palette which enhance incrementally instead of randomly.

B. Tools to detect Steganography

The disabling or elimination of hidden data in images is based on the image processing approach. For instance, with LSB methods of inserting information, simply compressing the image using lossy compression is adequate to disable or delete the hidden message.

There are several available steganographic detection tools including Encase by Guidance Software Inc., ILook Investigator by Electronic Crimes Program, Washington DC, several MD5 hashing service, etc. There is several image steganography tools use least significant bit (LSB) modification to hide data. In low resolution images with 8 bit color, the modification of LSB can generate a noticeable change in the color palette creating it possible to identify hidden content.

C. Challenges

The following are some challenges for consideration in image steganography problems.

Data Availability: Though image steganography is an unsupervised learning and the main goal is image reconstruction, there is no proper benchmark dataset available except BOSSBase. The number of images may be large in the BOSSBase but the images are of grayscale stored available in tiff format. Most of the methods deal with hiding RGB images inside RGB cover images. Finding a suitable dataset can be challenging.

Convergence of GAN Convergence is a major drawback for GAN where the model does not converge irrespective of the parameters chosen. Mode collapse also happens often as the generator and discriminator are inter-dependent. Comparison with other methods Evaluation metrics used by different methods is different and hence comparing the proposed method with the state-of-the-art methods are not easy.

Real-time steganography: Steganography models are trained on a huge amounts of datasets, like in, 45000 training images are used. However, when it comes to the real-time steganography, it gets difficult. The implementation of the trained model for performing the steganography and steganalysis requires transferring the stego image through an untrusted channel to the receiving end. The capability of the trained model in dealing with real time live images which may contain noises, skewing, blurring is not proved. The implementation of the model for real-time steganography is still questionable.

Not only image steganography, but also, video steganography is tried using CNN. Usually, 2D convolutional layers are used for images whereas 3D convolutional layers are used for videos. Temporally connected cover and secret video frames are given as the input to auto encoder network based VStegNET to produce the container video. Each frame of the cover image is concatenated with every frame of the secret video to produce the container video. Identical network architecture is used to reveal the hidden secret video.

After reviewing all the frameworks available, we have grouped the methodologies primarily into three categories, namely, traditional image steganography methods, CNN-based image steganography methods and GAN-based image steganography methods.

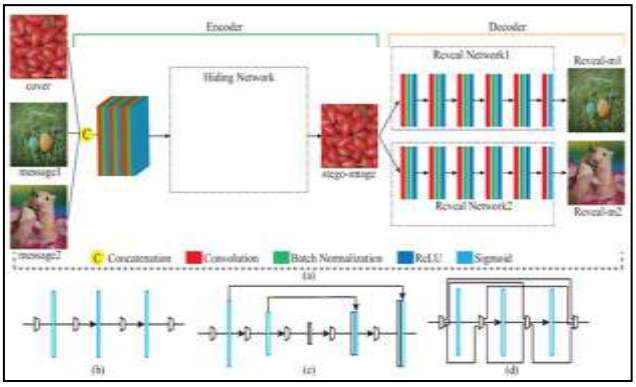

Fig. 3: Figure showing encoder – decoder transformation

The observations made from the results reported by the methods are delineated here. Basically, the hiding capacity, security and robustness factors are taken into account while discussing the observations.

Hiding Capacity: It is generally noted that the hiding capacity of the methods are in the following order. The methods with least hiding capacity are the traditional methods where text is the primary form of secret communication. Following that is the GAN-based methods, where only text message is used as secret. Unlike the traditional and GAN-based methods, the hiding capacity of the CNN-based methods are far better and is almost 1. The size of the secret image is same as the cover image. Even when a gray scale image is used for hiding, the size of the secret and the cover images are equal. In terms of the hiding capacity, CNN-based methods clearly outperform other methods.

Security and Robustness: Security is associated with embedding and robustness is associated with the extraction of the secret image. From our observations, CNN-based methods and GAN-based methods yield higher security. It is worth noting that the extraction of the secret images is prone to loss in information in deep learning methods. However, in traditional methods, the security is less but the robustness is high. PSNR measure is used to correlate the security and the robustness. From 5 and it can be noted that has the highest PSNR value explaining the higher security of the GAN based method. The highest value of PSNR being 64.7, given by the cycle GAN based image steganography method.

From the observations made, CNN-based deep learning methods have the best performance in terms of the hiding capacity (1), PSNR (64.7). The discriminators are trained in a way to overcome any steganalysis attack and has better anti-detection property compared to traditional-based methods.

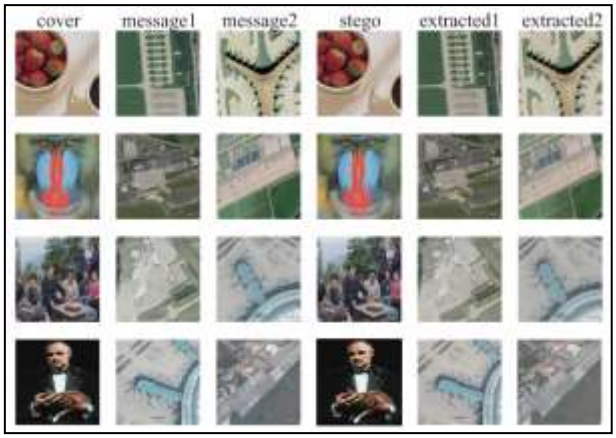

Fig. 4: Output using CNN modeling architecture

V. Discussion and Future Works

CNN-based methods use U-Net/Xu-Net auto encoder-decoder architecture for embedding and extracting. Some methods use the encoder for embedding and decoder for extracting, whereas, some use one auto encoder-decoder for embedding and another for extracting. Though there is some inter dependency, it is not totally linked like GAN methods.

Unbalance in the learning of generator-discriminator can happen where the generator is performing efficiently but the discriminator is struggling. Though the overall efficiency will not be affected, either sender or receiver will be prone to faults. This can be avoided by choosing the parameters carefully and avoiding over fitting during training.

In deep learning methods, the working principle of the image steganography is to extract features from the cover and secret image and concatenate them to produce an end result closer to the cover image. However, where and how the secret image pixels are embedded cannot be understood clearly. Without the counterpart extracting model trained, it may be difficult to crack the steganography image. This increases the security but becomes difficult when the extraction model is not working or crashed.

Some of the major disadvantages are the time taken for training, the computational time during testing and the storage capabilities. The models take two images or one image and a text message converted into bits as input. The features are extracted from both the inputs which increases the computational time in both embedding and extraction. The number of parameters also increases by double at least when compared to a normal architecture which in turn increase the storage space required by the model.

RGB secret images are used by handful methods when others used gray scale images. When converting the gray scale image to RGB image for better understanding, there can be loss of information. Image enhancement techniques are required in addition to understand the secret information properly.

Some of the aspects that can be considered for future works are enumerated below,

The majority of image steganography methods use either text or gray scale image as the secret information and there is a need for more research in hiding image in image and image in video.

Experiments related to optimizing the parameters and decreasing the storage capacities can be further conducted using various datasets.

The era of quantum computing is not far away, more efforts on developing designs on quantum images can be explored.

To benefit from a combination of methods, an ensemble of traditional and deep learning methods can be further studied.

Efforts can be directed to form a benchmark dataset containing images from various source cameras, image formats. A compilation of all possible algorithms can also be done to create the steganography images.

Many methods have considered the hiding capacity, security and robustness as the performance measure. However, there are possibilities for man-in-the-middle attacks when the transfer happens through untrusted channels. Tampering of the stego image can also happen during the transfer. These attacks and the performance of the designed algorithm against these attacks can be considered for evaluation along with other metrics.

VI. CONCLUSION

Image steganography is the method used in transmitting secret information by hiding it in plain sight inside a cover image. Deep learning methods are widely used in every field and have been used in the research of steganography. Review of all the related works led to categorizing them into three groups vastly. Most of the traditional based steganography methods use the LSB substitution and some of its variants.

The hiding capacity of the traditional methods are limited as over burdening the cover image by exploiting more pixels for hiding the secret message may led to distortions. Also, the auto encoder-decoder structure with VGG as base, U-Net and Xu-Net are the most prevailing architectures used for CNN-based image steganography methods. More recently, GAN architecture has gained significant attention for their ability to deal with image reconstruction tasks. Image steganography can be considered one such image reconstruction task where the cover image and the secret information is taken as input to reconstruct a steganographic image which is close to the cover image in resemblance.

There is no benchmark image datasets to perform the image steganography while most of them use the ImageNet, CelebA or BOSSBase. Each of the methods have their own evaluation methods and metrics and hence there is no common platform for comparisons. Peak Signal-to-Noise Ratio (PSNR) value comparison shown in table 5 gives an idea on the security performance of the different methods. Traditional methods are less secure as it is only a matter of detection of presence of the secret message. The secret message can be easily extracted as the embedding used a statistical method.

In summary, this paper has elaborated on the techniques used in the recent times for image steganography, the current trends. Along with it, details on the datasets and evaluation metrics are detailed. Challenges faced some discussions on the gaps and the scopes for future direction are also evaluated in this paper. It can be concluded that deep learning has tremendous potential in the image steganography field taking into consideration that all the challenges and gaps are filled.

REFERENCES

[1] Steganography, 2020, [online] Available: https://en.wikipedia.org/wiki/Steganography.
[2] H. Shi, X.-Y. Zhang, S. Wang, G. Fu and J. Tang, "Synchronized detection and recovery of steganographic messages with adversarial learning", Proc. Int. Conf. Comput. Sci, pp. 31-43, 2019.
[3] N. F. Hordri, S. S. Yuhaniz and S. M. Shamsuddin, "Deep learning and its applications: A review", Proc. Conf. Postgraduate Annu. Res. Informat. Seminar, pp. 1-6, 2016.
[4] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen", Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998.
[5] S. Gupta, G. Gujral and N. Aggarwal, "Enhanced least significant bit algorithm for image steganography", Int. J. Comput. Eng. Manage., vol. 15, no. 4, pp. 40-42, 2012.
[6] R. Das and T. Tuithung, "A novel steganography method for image based on Huffman encoding", Proc. 3rd Nat. Conf. Emerg. Trends Appl. Comput. Sci., pp. 14-18, Mar. 2012.
[7] Z. Qu, Z. Cheng, W. Liu and X. Wang, "A novel quantum image steganography algorithm based on exploiting modification direction", Multimedia Tools Appl., vol. 78, no. 7, pp. 7981-8001, Apr. 2019.
[8] S. Wang, J. Sang, X. Song and X. Niu, "Least significant qubit (LSQb) information hiding algorithm for quantum image", Measurement, vol. 73, pp. 352-359, Sep. 2015.
[9] N. Patel and S. Meena, "LSB based image steganography using dynamic key cryptography", Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT), pp. 1-5, Nov. 2016.
[10] O. Elharrouss, N. Almaadeed and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)", Proc. IEEE Int. Conf. Informat. IoT Enabling Technol. (ICIoT), pp. 131-135, Feb. 2020.
[11] M. V. S. Tarun, K. V. Rao, M. N. Mahesh, N. Srikanth and M. Reddy, "Digital video steganography using LSB technique", Red, vol. 100111, Apr. 2020.
[12] S. S. M. Than, "Secure data transmission in video format based on LSB and Huffman coding", Int. J. Image Graph. Signal Process., vol. 12, no. 1, pp. 10, 2020.
[13] M. B. Tuieb, M. Z. Abdullah and N. S. Abdul-Razaq, "An efficiency secured and reversible video steganography approach based on lest significant", J. Cellular Automata, vol. 16, no. 17, Apr. 2020.
[14] R. J. Mstafa, K. M. Elleithy and E. Abdelfattah, "A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC", IEEE Access, vol. 5, pp. 5354-5365, 2017.
[15] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E.-S.-M. El-Rabaie and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography", Proc. 4th IEEE Int. Colloq. Inf. Sci. Technol. (CiSt), pp. 400-404, Oct. 2016.

[16] Arya and S. Soni, "Performance evaluation of secrete image steganography techniques using least significant bit (LSB) method", Int. J. Comput. Sci. Trends Technol., vol. 6, no. 2, pp. 160-165, 2018.
[17] G. Swain, "Very high capacity image steganography technique using quotient value differencing and LSB substitution", Arabian J. Sci. Eng., vol. 44, no. 4, pp. 2995-3004, Apr. 2019.
[18] Qiu, X. Chen, X. Sun, S. Wang and W. Guo, "Coverless image steganography method based on feature selection", J. Inf. Hiding Privacy Protection, vol. 1, no. 2, pp. 49, 2019.
[19] R. D. Rashid and T. F. Majeed, "Edge based image steganography: Problems and solution", Proc. Int. Conf. Commun. Signal Process. Appl. (ICCSPA), pp. 1-5, Mar. 2019.
[20] X. Liao, J. Yin, S. Guo, X. Li and A. K. Sangaiah, "Medical JPEG image steganography based on preserving inter-block dependencies", Comput. Electr. Eng., vol. 67, pp. 320-329, Apr. 2018.
[21] W. Lu, Y. Xue, Y. Yeung, H. Liu, J. Huang and Y. Shi, "Secure halftone image steganography based on pixel density transition", IEEE Trans. Dependable Secure Comput., Aug. 2019.
[22] Y. Zhang, C. Qin, W. Zhang, F. Liu and X. Luo, "On the fault-tolerant performance for a class of robust image steganography", Signal Process., vol. 146, pp. 99-111, May 2018.
[23] P. Wu, Y. Yang and X. Li, "Image-into-image steganography using deep convolutional network", *Proc. Pacific Rim Conf. Multimedia*, pp. 792-802, 2018.
[24] P. Wu, Y. Yang and X. Li, "StegNet: Mega image steganography capacity with deep convolutional network", *Future Internet*, vol. 10, no. 6, pp. 54, Jun. 2018.
[25] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang and C. Qin, "Reversible image steganography scheme based on a U-Net structure", *IEEE Access*, vol. 7, pp. 9314-9323, 2019.
[26] T. P. Van, T. H. Dinh and T. M. Thanh, "Simultaneous convolutional neural network for highly efficient image steganography", *Proc. 19th Int. Symp. Commun. Inf. Technol. (ISCIT)*, pp. 410-415, Sep. 2019.
[27] R. Rahim and S. Nadeem, "End-to-end trained CNN encoder-decoder networks for image steganography", *Proc. Eur. Conf. Comput. Vis. (ECCV)*, pp. 1-6, 2018.
[28] Z. Wang, N. Gao, X. Wang, J. Xiang and G. Liu, "STNet: A style transformation network for deep image steganography", *Proc. Int. Conf. Neural Inf. Process*, pp. 3-14, 2019.
[29] K. Yang, K. Chen, W. Zhang and N. Yu, "Provably secure generative steganography based on autoregressive model", *Proc. Int. Workshop Digit. Watermarking*, pp. 55-68, 2018.
[30] S. Baluja, "Hiding images in plain sight: Deep steganography", *Proc. Adv. Neural Inf. Process. Syst.*, pp. 2069-2079, 2017.
[31] R. Zhang, S. Dong and J. Liu, "Invisible steganography via generative adversarial networks", *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8559-8575, Apr. 2019.
[32] S. Islam, A. Nigam, A. Mishra and S. Kumar, "VStegNET: Video steganography network using spatio-temporal features and micro-bottleneck", *Proc. BMVC*, pp. 274, Sep. 2019.
[33] Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, et al., "Generative adversarial nets", *Proc. Adv. Neural Inf. Process. Syst.*, pp. 2672-2680, 2014.
[34] D. Volkhonskiy, B. Borisenko and E. Burnaev, "Generative adversarial networks for image steganography", *Proc. ICRL Conf.*, 2016.
[35] D. Volkhonskiy, I. Nazarov and E. Burnaev, "Steganographic generative adversarial networks", *Proc. 12th Int. Conf. Mach. Vis. (ICMV)*, vol. 11433, 2020.
[36] D. J. Im, C. D. Kim, H. Jiang and R. Memisevic, "Generating images with recurrent adversarial networks" in arXiv:1602.05110, 2016, [online] Available: http://arxiv.org/abs/1602.05110.
[37] H. Shi, J. Dong, W. Wang, Y. Qian and X. Zhang, "SSGAN: Secure steganography based on generative adversarial networks", *Proc. Pacific Rim Conf. Multimedia*, pp. 534-544, 2017.
[38] J. Hayes and G. Danezis, "Generating steganographic images via adversarial training", *Proc. Adv. Neural Inf. Process. Syst.*, pp. 1954-1963, 2017.
[39] J. Yang, K. Liu, X. Kang, E. K. Wong and Y.-Q. Shi, "Spatial image steganography based on generative adversarial network" in arXiv:1804.07939, 2018, [online] Available: http://arxiv.org/abs/1804.07939.
[40] J. Yang, D. Ruan, J. Huang, X. Kang and Y.-Q. Shi, "An embedding cost learning framework using GAN", *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 839-851, 2020.
[41] W. Tang, S. Tan, B. Li and J. Huang, "Automatic steganographic distortion learning using a generative adversarial network", *IEEE Signal Process. Lett.*, vol. 24, no. 10, pp. 1547-1551, Oct. 2017.
[42] H. Naito and Q. Zhao, "A new steganography method based on generative adversarial networks", *Proc. IEEE 10th Int. Conf. Awareness Sci. Technol. (iCAST)*, pp. 1-6, Oct. 2019.
[43] K. Zhang, A. Cuesta-Infante and K. Veeramachaneni, "SteganoGAN: Pushing the limits of image steganography" in arXiv:1901.03892, Jan. 2019, [online] Available: https://arxiv.org/abs/1901.03892.
[44] J. Zhu, R. Kaplan, J. Johnson and L. Fei-Fei, "Hidden: Hiding data with deep networks", *Proc. Eur. Conf. Comput. Vis. (ECCV)*, pp. 657-672, 2018.
[45] Y. Ke, M. Zhang, J. Liu, T. Su and X. Yang, "Generative steganography with Kerckhoffs' principle based on generative adversarial networks" in arXiv:1711.04916, 2017, [online] Available: http://arxiv.org/abs/1711.04916.
[46] J.-Y. Zhu, T. Park, P. Isola and A. A. Efros, "Unpaired image-to-image translation using cycle-consistent adversarial networks", *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, pp. 2223-2232, Oct. 2017.
[47] P. G. Kuppusamy, K. C. Ramya, S. Sheebha Rani, M. Sivaram and V. Dhasarathan, "A novel approach based on modified cycle generative adversarial networks for

image steganography", *Scalable Comput. Pract. Exper.*, vol. 21, no. 1, pp. 63-72, Mar. 2020.
[48] C. Chu, A. Zhmoginov and M. Sandler, "CycleGAN a master of steganography" in arXiv:1712.02950, 2017, [online] Available: http://arxiv.org/abs/1712.02950.
[49] H. Porav, V. Musat and P. Newman, "Reducing steganography in cycle-consistency GANs", *Proc. CVPR Workshops*, pp. 78-82, 2019.
[50] R. Meng, Q. Cui, Z. Zhou, Z. Fu and X. Sun, "A steganography algorithm based on CycleGAN for covert communication in the Internet of Things", *IEEE Access*, vol. 7, pp. 90574-90584, 2019.
[51] Odena, C. Olah and J. Shlens, "Conditional image synthesis with auxiliary classifier GANs", *Proc. Int. Conf. Mach. Learn.*, pp. 2642-2651, 2017.
[52] Z. Zhang, G. Fu, J. Liu and W. Fu, "Generative information hiding method based on adversarial networks", *Proc. Int. Conf. Comput. Eng. Netw*, pp. 261-270, 2018.
[53] M.-M. Liu, M.-Q. Zhang, J. Liu, Y.-N. Zhang and Y. Ke, "Coverless information hiding based on generative adversarial networks" in arXiv:1712.06951, 2017, [online] Available: http://arxiv.org/abs/1712.06951.
[54] X. Duan, H. Song, C. Qin and M. K. Khan, "Coverless steganography for digital images based on a generative model", *Comput. Mater. Continua*, vol. 55, no. 3, pp. 483-493, Jul. 2018.
[55] M. Arjovsky, S. Chintala and L. Bottou, "Wasserstein GAN" in arXiv:1701.07875, 2017, [online] Available: http://arxiv.org/abs/1701.07875.
[56] C. Li, Y. Jiang and M. Cheslyar, "Embedding image through generated intermediate medium using deep convolutional generative adversarial network", *Comput. Mater. Continua*, vol. 56, no. 2, pp. 313-324, 2018.
[57] Z. Wang, N. Gao, X. Wang, X. Qu and L. Li, "SSteGAN: Self-learning steganography based on generative adversarial networks", *Proc. Int. Conf. Neural Inf. Process*, pp. 253-264, 2018.
[58] P. Bas, T. Filler and T. Pevný, "'Break our steganographic system': The ins and outs of organizing BOSS" in Information Hiding, Berlin, Germany:Springer, pp. 59-70, 2011.
[59] T. Pevný, T. Filler and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography" in Information Hiding, Berlin, Germany:Springer, pp. 161-177, 2010.
[60] Z. Liu, P. Luo, X. Wang and X. Tang, "Deep learning face attributes in the wild", *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, pp. 3730-3738, Dec. 2015.

