JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Framework for Image Steganography Using Deep Learning Algorithm

[1]Dr.V.Prasad, [2]G. Mounika, [3]CH. S. N. Balaji, [4]A. Balaji, [5]J. Mithin, [6]B. Amrutha Valli
[1]Associate Professor, [2]Student, [3]Student, [4]Student, [5]Student, [6]Student
[1]Department of Computer Science and Engineering,
[1] GMR Institute of Technology, Rajam, Andhra Pradesh, India.

Abstract : Nowadays, securing information plays a key role while transmitting it to other places. During the transmission, the information might get tampered with by third parties. To avoid tampering with the information, steganography will come into the picture. Image Steganography is defined as the hiding of information such as text, images, videos or audio files inside an image. The primary application of image steganography is encryption, as it adds an extra step for concealing and protecting data. This project describes the hiding of images using deep learning algorithms such as CNN. As inputs, the image that is used for encoding and the hidden image are used. The preparation network receives the secret image as an input, while the cover image is primarily used to conceal the network. The generated cover image, which conceals the secret image, serves to reveal network that generates the concealed secret information. The accuracy is determined by using loss function. This application secures the information using deep learning algorithms, which helps in avoiding cover image tampering.

IndexTerms **- CNN, Cover image, Secret image, Deep Learning, Steganography, Encryption.**

I. INTRODUCTION

The advancement of high-speed networked computers, especially the internet, has facilitated communication. Communication usually happens through insecure networks. Communication is mostly operated through text, video, image, and audio modes. Though there are numerous advantages to it, it lacks privacy and security. Some methods have been introduced to conceal the information and transfer it by providing the utmost security, which are cryptography, steganography, Watermarks. Cryptography means encoding the information in a secret language that is known only to the receiver. Watermarks only enhance the rights of individuals. Steganography has been gaining popularity in recent days. It is defined as the process of concealing secret multimedia within other media. For cryptography, cypher text (information to be hidden) is visible, but in steganography, cypher text is invisible. The aim of this project work concentrates on image steganography, i.e., the secret image which is hidden by using a cover image. Traditional methods for image steganography are Pixel Value Differencing (PVD), Least Significant Bits (LSB) substitution, and Discrete Wavelet Transformation (DWT). This project works on deep learning algorithm, which have more hidden robustness, capacity, and security compared with traditional work. Evaluation metrics used are PSNR and Loss function. CNN encrypts the concealed picture and decrypts the concealed picture from the source images. CNN helps to achieve an optimal solution in image steganography. To explain how the proposed model is implemented See Fig. 1.

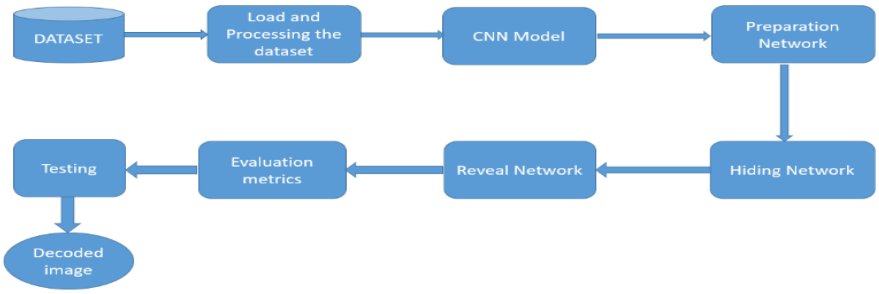


Figure. 1 depicts the design of implementation modules.

II. RELATED WORKS

Subramanian, N.,et al. proposed [1], which is used in image steganography to avoid the visibility of secret images and distortions. [1] is subdivided into three modules (pre-processing module, embedded network, and extraction network). The pre-processing module take out the necessary characteristics from cover and hidden images. The embedded network aids in the

embedding of hidden images in cover images, while the extraction network aids in the revealing of hidden images. The psnr(34.55) is employed to calculate the accuracy of [1], and the hiding capacity metric is high when compared to traditional methods. Steganography suffered from attacks on non-edge pixels. Ray, B., et al. devised a [2] to address this issue. [2] describes convolutional neural networks with deep supervision edge detectors. Initially, the cover image is first processed and transformed into a grayscale edge map using the edge detector model described above. The secret bits that must be hidden are embedded in edge pixels, while some bits are inserted in non-edge constituents. In regards to psnr and payload, [2] outperforms other spatial and edge-based steganography methods. Subramanian, N., et al. investigate the various deep learning techniques used for image steganography. Those are classified into three types: GAN-based methods, traditional methods, and CNN-based methods. [3] provides an overview of steganography methods, datasets, and evaluation metrics, as well as the challenges that methods face and future work to improve hiding capacity and security. According to [3], hiding capacity is lowest for traditional and highest for CNN. GAN is preferred for security, while traditional methods can be used more efficiently for robustness.

The visual quality of data in the embedded container is essential for preventing tampering. [4], which is discussed by Hamid, N., et al. in this paper, plays a significant role to data hiding capacity. An embedding algorithm aids in the incorporation of data into the cover image. The CNN Classifiers then assist in categorising the cover as excellent quality (appropriate for steganography) or poor quality (unsuitable for steganography). When compared to SSIM values and hiding capacity, the accuracy (F1-score) of the two classifiers is 0.926, 0.904. Rustad, S., Andono, & Andono, Syukur, A., P. N. et al. proposed [5] to test the container image bits such that the container image has the least error rate when used for embedding. [5] is applied on medical images and achieves PSNR values of 52.49 to 57.45, where SSIM values found range from 0.9991 to 0.9999. To increase the payload and quality of the steganographic image, Duan, X., Guo, D., and Qin, C. et al. proposed [6]. The secret image is preprocessed with the DCT and encrypted with ECC so that it cannot be recognised by the Human Visual System (HVS). The SegNet network is in charge of implementing steganography. The SSIM values for [6] applied to the ImageNet dataset are found to be greater than 0.96.

[7] is introduced in this paper to resist steganalysis detection and to develop visual quality. [7] is made up of three modules: encoder, decoder, and discriminator. The encoder network generates low-distorted steganographic images, whereas the decoder network generates secret information from steganographic images. The Steganalysis model is used as a discriminator to determine whether a container image contains confidential information. As a result, in [7], Xu'Net and SRNet serve as discriminators. Xu'Net and SRNet have detection accuracy of 98.9% and 99.5%, respectively. Nowadays, the rapid improvement in steganalysis method accuracy poses a significant threat to steganography security. Because GAN-based steganography without embedding results in less payload and hiding capacity,[8] employs the attention method to improve image quality and steganographic capacity. The detection accuracy of steganalysis for the car dataset is given as 99%. Based on the above results, [8] can be used to prevent the tracking of secret information. [9] was proposed by Li, Y., Liu, J., and Zhang, Y.et al. to improve the hiding capacity of stegano images. [9] employs an improved Dense Atrous Spatial Pyramid Pooling module, which aids in image information capacity. It is equipped with an encoder, decoder networks, and a discriminator. [9] was evaluated and compared to the SteganoGAN on three datasets (Div2K, COCO, and Pascal VOC), yielding a consistent accuracy of 99.95%.

Siddiqui, G. F., Iqbal, M. Z., and Khan, M. F. et al. present [10], which proposes embedding more secret information in patient's medical images with improved imperceptibility. [10] categorises grayscale MRI photos into three groups: low, medium, and high intensity.[10] is evaluated using psnr, MSE and SSIM indexes on a set of brain MRI images. Finally, the proposed steganography technique outperforms other similar methods in terms of average PSNR (49.27). [11] proposed by Li, Q., Wang, X., Wang, and Shi, Y. et al. for concealing an encrypted image within a container image of the same size. By transforming encrypted and container images, a convolutional neural network (CNN) generates a encrypted container image. A generative adversarial network (GAN) is used for generating a more practical encrypted image. On LFW image, ImageNet, and PASCAL-VOC12 datasets, the suggested steganography system in [11] outperforms. Almaadeed, Elharrouss, N., O., and Al-Maadeed, S. et al. proposed [12]. To conceal the image, it employs k least bits. A field revelation action is used to determine which sections contain the concealed image in order to decode it, and the encrypted image resolution is improved using a quality enhancement method. The psnr is used for assessing [12]'s effectiveness in hiding one image within another (PSNR). [12] can hide images and extract them with the least amount of distortion and information loss.

Y. H. Li, C. C. Chang, and Y. Liu et al. proposed [13] an information hiding approach that generates a cluster of transmogrified face images from an arranged small-scale face image dataset. A transmogrified facial image encrypted using a hidden information is sent to the collector to perform morphed face recognition, and two novel Convolutional Neural Network (CNN) frameworks like MFR-Net V1 and MFR-Net V2 are used. The experimental results show that [13] has a higher retrieval capacity, accuracy, and robustness. Al Hussien, M. S., Mohamed, S. S., & Hafez, E. H. et al. proposed [14] for a coverless data hiding concept. Coverless doesn't imply that the secret data will be sent without a container file, nor does it imply that the container file will be neglected. Instead, the secret data will be inserted by producing a container data or an encryption key mapping. [14] employs the OMR and RBML algorithms. The experiment results demonstrated that [14] has very high robustness and security. The data hiding approach proposed by Kamil, S., Abdullah, S. N. H. S., and Bohani, F. A. et al. [15] is based on the flipping approach, which reduces variability and provides less time complexity. The Least Significant Bit algorithm is the maximum commonly used information concealment technique. [15] replaces LSB of the container constituent with the private information bit. Finally, in aspects of variability, visual quality, and time complexity, [15] outperforms Genetic and Bayesian Optimization algorithms as well as the original flip method.

III. METHODOLOGY

Data Collection:

Data collection refers to the method of measuring and gathering information from numerous different data sources. In this paper the data is collected from the Kaggle. This file comprises 100000 images partitioned into 200 classes, each with 500 images

downsized to 64 x 64 colored images. It contains of 50 validation images, 50 test images, and 500 training images in every class. See Fig.2.

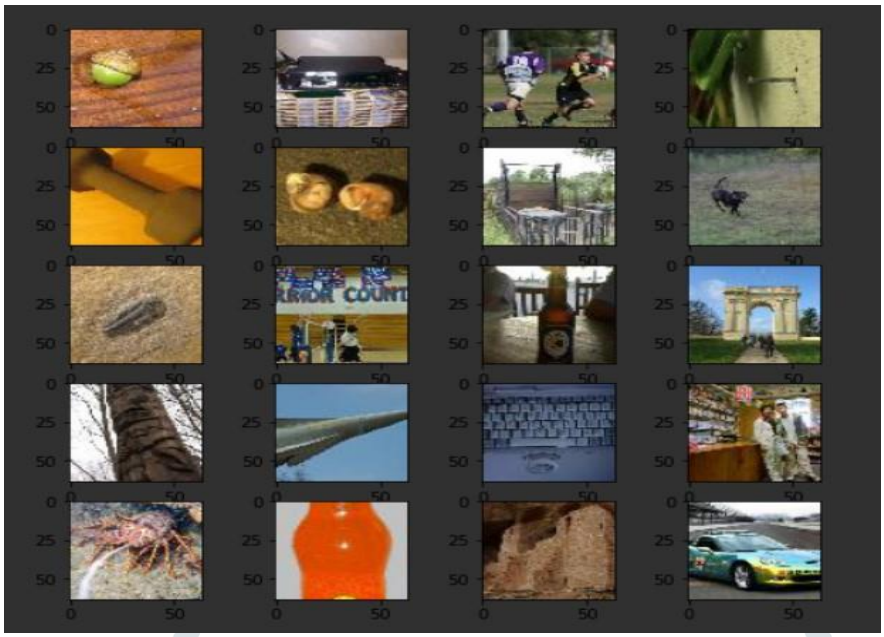


Figure.2. Shows the sample of training images from the ImageNet dataset which is collected from Kaggle.

CNN:

Implementation of CNN in this project is for hiding an image inside another image hence making secrete image effectively invisible to the observer. The neural networks that we have used in our work determines that in the cover image it can hide the information and hence, is a more efficient process than LSB manipulation. A decoder network was also trained to retrieve the hidden information from the container. This process is carried out in such a way that the container image does not change significantly and the changes to the container image are indistinguishable. It can be safely assumed that the intruder does not have accessibility to the original image. Secret image is effectively hidden in all 3 color channels of the container image.

Preparation Network:

This network equips the hidden image with additional beneficial features that can be encoded, such as edges. It contains 50 filters of (3X3, 4X4,5X5) patches there are total 6 layers of this kind. Each preparation network is built with two layers arranged on top of each other. Each layer is built with three independent Conv2D layers. The three Conv2D layers possess 50, 10, and 5 channels, respectively, with kernel sizes consists of 3, 4, and 5 for each layer. Along each of the two axes, the stride length remains unchanged at one. To keep the output image in the same dimensions, appropriate padding is allocated to each Conv2D layer. After each Conv2d layer, a Relu activation is applied.

Hiding Network:

This network will take the output of the preparation network and will then create a Container Image. It is a CNN with 5 convolutional layers that have 50 filters of (3X3, 4X4, 5X5) patches. This layer consists of total of 15 convolutional layers in this network. The concealing network is a three-layer aggregation. Each of these layers is made up of three individual Conv2D layers. Conv2D layers in the hidden network possess an identical basic structure to the Conv2Dlevels in the Preparation Network.

Reveal Network:

Reveal Network Converts the Container image in to original image this network is used for decoding. Which has 5 convolutional layers that have 50 filters of (3X3, 4X4, 5X5) patches. This layer consists of total of 15 convolutional layers in this network. It has a similar basic design to the hidden network, having three levels of Conv2Dlayers that are proportionate in shape.

ReLU activation function :

The above function was primarily used to test the network with various learning rates. Most CNN networks use it de facto. ReLU is a variational or piecewise linear function that, if positive, returns the input immediately; otherwise, it returns zero. This is the most commonly employed activation function in deep learning, especially in Deep Neural Networks and Multilayer Perceptrons. It is simple, but more effective than its predecessors, likely sigmoid or tanh.
Mathematically, it's also written as - y(x)=maximum (0, x)

Graphically, it is pictured below, see Fig.3.

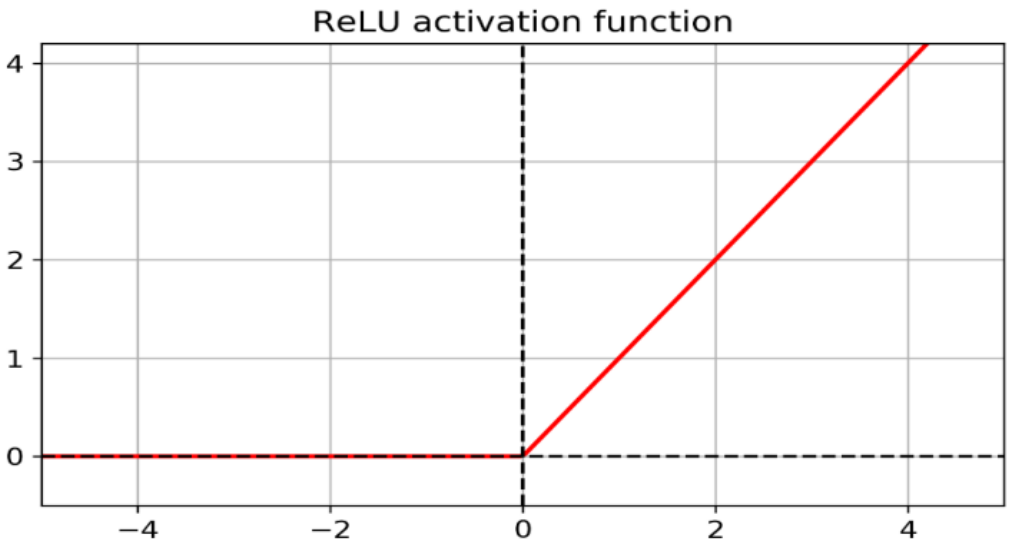


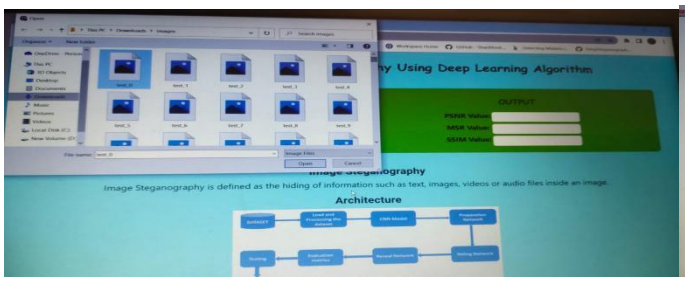
Figure. 3 illustrates a graphical view of the ReLU activation function.

IV. RESULTS AND DISCUSSION

The proposed model accepts both the container image and the concealed image as input and attempts to embed the concealed image within the cover image. The generated container is an onsite image, first as the output, then as the encoded container image, which is decoded into the container and hidden image. The decoded hidden data is considered the second output. Figure 4: In this case, PSNR, MSE, and SSIM values are used as evaluation metrics to verify the accuracy of the encoded container image and the data protection of the proposed model.

Figure 4 displays the cover image, secret image, encoded cover image (concealed secret image) and decoded secret image.

The proposed model secures higher PSNR values compared with references taken and also achieves lower MSE values which indicate the good quality of the stego image. This model attained a PSNR value of 73.01db, SSIM value of 0.9540, and MSE value of 0.6241. The comparison is done in table 1.



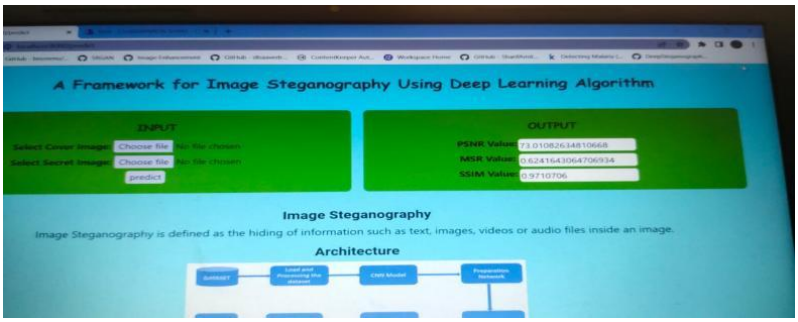


Figure.5, Figure.6, Figure.7. represent the working of research model with graphical user interface.

1. PSNR (Peak Signal to Noise Ratio)

It's also interpreted as the ratio of the container's maximum performance representation to the embedded image. As a result, the PSNR value represents the embedded image's performance. The strength of the embedded image is good if the PSNR value is high; otherwise, the strength of the embedded image is poor.

2. SSIM (Structure Similarity Index Measure)

It's a metric for calculating the correlation between two images. In this model, SSIM computes the commonality between the original container and the encoded container image. The SSIM result ranges from -1 to 1, with 1 indicating perfect similarity and 0 indicating no similarity. As a result, the proposed model's SSIM value is nearly equal to one, indicating perfect resemblance.

3. MSE (Mean Squared Error)

It is a metric used to determine the appropriateness of an encoded image. The sum of the squared absolute errors between the container and the encoded container image is used to calculate it. A low mse value indicates that the error is small, which results in more accurate images.

A graph compares PSNR values with the proposed model and related models. Figure 4: According to the graph, the proposed model has a high PSNR value, indicating that the researched model produces a safe and high-quality stego image.
Table 1 shows comparison in evaluation metrics of different models.

MODEL	**PSNR (dB)**	**SSIM**
[1]	34.55	-
[2]	48.91	-
PROPOSED MODEL	73.01	0.9540
[6]	48.183	0.9693
[10]	49.27	-
[11]	42.3	0.987
[12]	33.85	-

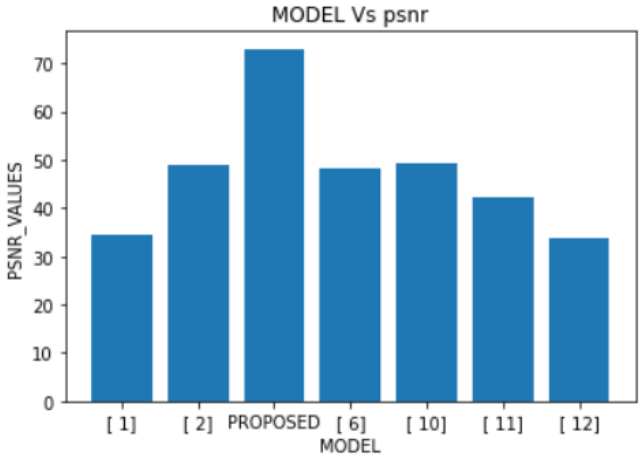


Figure.4. Shows comparison of proposed model and existing models in terms of PSNR values

V. CONCLUSION

Steganography is a strategy for concealing secret information in another medium and transmitting it. There are various methods for concealing data. In which this model employs deep learning techniques. The suggested framework employs a neural network of convolutions to conceal an encrypted image within another background image. When compared to other works, the proposed model has higher psnr & ssim values, indicating that the stego image is of high quality. This model has also demonstrated increased security and robustness.

VI. FUTURE SCOPE

The proposed algorithm, which only focuses on security, quality, and robustness, can be applied to other secret multimedia in the future, such as audio. To ensure that the suggested algorithm is resistant to real-world attacks, additional evaluation metrics can be used to compute its performance.

VII. REFERENCES

[1] Subramanian, N., Cheheb, I., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). End-to-end image steganography using deep convolutional autoencoders. IEEE Access, 9, 135585-135593.
[2] Ray, B., Mukhopadhyay, S., Hossain, S., Ghosal, S. K., & Sarkar, R. (2021). Image steganography using deep learning based edge detection. Multimedia Tools and Applications, 80(24), 33475-33503.
[3] Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. IEEE access, 9, 23409-23423.
[4] Hamid, N., Sumait, B. S., Bakri, B. I., & Al-Qershi, O. (2021). Enhancing visual quality of spatial image steganography using SqueezeNet deep learning network. Multimedia Tools and Applications, 80(28), 36093-36109.
[5] Rustad, S., Syukur, A., & Andono, P. N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. Journal of King Saud University-Computer and Information Sciences, 34(6), 3559-3568.
[6] 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.
[7] Zhangjie, F., Wang, F., & Xu, C. (2020). The secure steganography for hiding images via GAN. EURASIP Journal on Image and Video Processing, 2020(1).
[8] Yu, C., Hu, D., Zheng, S., Jiang, W., Li, M., & Zhao, Z. Q. (2021). An improved steganography without embedding based on attention GAN. Peer-to-Peer Networking and Applications, 14(3), 1446-1457.
[9] Li, Y., Liu, J., Liu, X., Wang, X., Gao, X., & Zhang, Y. (2021). HCISNet: Higher-capacity invisible image steganographic network. IET Image Processing, 15(13), 3332-3346.
[10] Siddiqui, G. F., Iqbal, M. Z., Saleem, K., Saeed, Z., Ahmed, A., Hameed, I. A., & Khan, M. F. (2020). A dynamic three-bit image steganography algorithm for medical and e-healthcare systems. IEEE Access, 8, 181893-181903.
[11] Li, Q., Wang, X., Wang, X., Ma, B., Wang, C., Xian, Y., & Shi, Y. (2020). A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks. IEEE Access, 8, 168166-168176.
[12] Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. (2020, February). An image steganography approach based on k-least significant bits (k-LSB). In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 131-135). IEEE.
[13] Li, Y. H., Chang, C. C., Su, G. D., Yang, K. L., Aslam, M. S., & Liu, Y. (2022). Coverless image steganography using morphed face recognition based on convolutional neural network. EURASIP Journal on Wireless Communications and Networking, 2022(1), 1-21.
[14] Al Hussien, S. S., Mohamed, M. S., & Hafez, E. H. (2021). Coverless image steganography based on optical mark recognition and machine learning. IEEE Access, 9, 16522-16531.
[15] Kamil, S., Abdullah, S. N. H. S., Hasan, M. K., & Bohani, F. A. (2021). Enhanced Flipping Technique to Reduce Variability in Image Steganography. IEEE Access, 9, 168981-168998.