Enhancing Covert Communication Systems through Deep Steganography

Ass.Lec. Haider Akeed Rajab [1]
haider.akeed86@gmail.com

Prof. Methaq Talib Gaata [2]
dr.methaq@uomustansiriyah.edu.iq

Dr.Muhanad Tahrir Younis
mty@uomustansiriyah.edu.iq

Abstract: Deep image steganography has emerged as a promising approach for concealing secret information with in digital images, leveraging the power of deep learning techniques to enhance security. The study explores the integration of deep neural networks to enhance the security and robustness of steganographic methods. Conventional image steganography approaches may have vulnerabilities because of their fixed algorithms, which makes them less flexible in handling different types of image material and more prone to being detected by advanced steganalysis methods. The proposed method aims to advance covert communication systems by utilizing deep learning to achieve imperceptibility and robustness against common structural analysis methods.

This study presents a generic Convolutional Neural Network (CNN) with encoder-decoder architecture for deep image steganography method. It facilitates the seamless concealment and extraction of information. In order to assess the efficacy of the proposed approach, peak signal-to-noise ratio and structural similarity index measurements were used. Experimental results based on an ImageNet dataset show that our approach outperforms the selected related methods in terms of security, robustness and visually imperceptibility. PSNR: 72.79 SSIM: 0.9753 The test results, thus gleaning that the approach we proposed is superior to previous methods.

Keywords: Image steganography, deep learning, CNN, PSNR, SSIM.

[1] M.Sc. Student, Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

[2] Prof., Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

[3] Assist. Prof., Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

1. Introduction

Image steganography is an advanced method used to hide confidential data within digital images, enhancing the security of information exchange [1]. Derived from old clandestine writing techniques [2], this approach has adapted with technological progress and is utilized in domains such as cybersecurity, digital forensics, and covert communication.

There are different types of steganography methods which is based on the data carrier we use fore hiding a message like text, images and audio [3,4]. The fundamental idea of Image Steganography is to covertly change the pixels value in such a way that this pixel difference goes unnoticed while preserving sensitive information, here implementing stego image. Cryptography encrypts data [5] while steganography hides the presence of hidden information, minimizing detectability. Hiding the information in plain images to potentially make it harder for unwanted recipients to spot.

Various techniques and algorithms have been created to aid in image steganography, including simple LSB [6] replacement methods and intricate modifications including frequency domain manipulation [7]. The approaches utilize redundancies in pixel values and undetectable alterations to smoothly incorporate hidden messages, guaranteeing that the stego image closely mirrors the original cover image.

Image Steganography is critical for covert communication and data hiding, which are the best way when traditional encryption mechanisms prove to be futile or unfeasible. This is an old and useful concept of hiding the protected information in many fields to protect confidential data as military communicational, digital copyright protection and many more up-to-date practices like hidden irreversible encrypted message exchange [8]. Image steganography remains an area of study, and innovation is necessary for addressing increasing threats to the confidentiality across communications by exploiting existing as well as new mathematical algorithm.

Image steganography provides heightened security, facilitates data storage, and bolsters resistance against cryptanalysis. It ensures the concealment of information even amidst image processing operations [9]. Nevertheless, the emergence of sophisticated techniques poses a risk of exposing concealed data, prompting its frequent integration with encryption for heightened data safeguarding [10].

Choosing the cover image is crucial for defining the security level of the stego image. Images with higher noise levels and distinct edge areas offer improved data concealing with reduced visibility of alterations compared to smoother images [11].

This paper introduces a novel image steganography technique specifically developed for concealing a secret image within a cover image, resulting in a stego image that closely resembles the cover image. The system utilizes an encoder-decoder architecture in conjunction with convolutional neural networks for training. The subsequent portions of this work are organized as outlined: Section 2 offers a comprehensive summary of relevant literature. Section 3 offers a detailed discussion of the proposed structure. Section 4 explains the method for quantifying loss in the concealment and retrieval procedures. Other measurements utilized to evaluate image steganography, including PSNR and SSIM, are examined in Section 5. Results of the investigation are illustrated and evaluated in Section 6. The conclusion of the investigation is presented in Section 7.

2. Review of the History of Beam-Column Joints

Recently, there has been significant research conducted in the area of image steganography, investigating both conventional and deep learning approaches. These investigations analyze methods, challenges, and emerging trends related to concealing information within images, aiming to enhance secure communication and safeguard data.

The author Baluja [12] introduced a steganographic framework with three networks: preprocessing network, encoder network and decoder network. It was developed to hide images inside other images. The model ensures that the hidden image appears perceptually unchanged from the original visual input. The quality of the dense and reconstructed images is still lower than what most people can accept, even if some significant visual improvement has been achieved on them.

The structure proposed by the authors in [13] combines a CNN with an auto-encoder-like design, known as U-Net. The concealing phase consists of a sequence 4x4 convolutional filters with batch normalization (BN) and leaky ReLU activation. The final image generated by the output layer through a sigmoid activation approach is our stego-image. Despite its numerous benefits, this architecture possesses significant advantages, such as a 24-bit per pixel capacity and good hiding, it lacks the ability to adapt to various input sizes of the image.

An novel and fully automated steganography technique was introduced in a research paper published in [14]. This technique involves concealing one image within another. A deep learning network is designed to automatically extract suitable attributes from both the cover and secret images to enable data integration. This method is highly adaptable and can be applied to images of any kind. The encoder integrates feature maps from various layers of the guest branch with corresponding output feature maps of the host branches until it reaches a depth of k (optimal at k = 7). After the integration process, further convolution and ReLU layers are utilized to generate the blended image, which serves as the final output.

The weakness of this paper is that it used only the grayscale image in the secret image.

The work presented by zhang et. al [15] introduced the ISGAN model, employing generative adversarial networks for invisible steganography. The procedure includes partitioning color cover images into Y, U, and V channels, followed by merging the secret image with the cover image. The secret image must then be extracted by the decoder network. Steganography in this paper is performed in the spatial domain, and steganographic images must be lossless; otherwise, undetectable portions of the secret image will be compromised.

In [11], the authors presented a novel steganography method that allows for concealing a color image within another image of same dimensions without inducing detectable distortion. This method employs an auto-encoding network structure and utilizes deep convolutional neural network training to enable effective hiding and retrieval processes. The approach demonstrates its efficacy across diverse image sources while maintaining satisfactory PSNR and SSIM values. The difficulties in this paper were in testing the method on large images.

A research study in [16] presents a complex convolutional autoencoder architecture consisting of three essential elements: a preprocessing module, an embedding network, and an extraction network. The technique is evaluated on three datasets: CelebA, ImageNet and COCO. The preprocessing module has an input layer and runs through three convolutional layers. The encoding module is composed by two convolutional layers for the embedding process and, a five-layered encoder-decoder where all cascade into three fully connected layer. The extraction network contains 5convolutional layers using Rectified Linear Unit (ReLU) as activation functions. Another issue to be considered is the computational complexity. However, as a weakness of this paper due to the absence of separable dependencies between embedding and extraction networks, it can be concluded that computational complexity is high since in both its single-layered part has compared to Socher's model which only find similarity among parts.

The PSNR ratio in all the related works above is relatively low, making the image somewhat perceptible. The proposed system addresses this issue by achieving a high PSNR value, which enhances the security and imperceptibility of the stego image.

3. Proposed System

For our proposed method, the whole module is divided into three core components: Preparation Module, Embedding and Extraction modules. The preparation phase is responsible for preparing the cover and secret images to be embedded, making it easier to reconstruct the stego image. The embedding module is responsible for enabling the hidden image to be embedded inside cover images which helps in generating stego-images. On the other hand, extraction module focuses on extracting the hidden secret image from steganographic image. The embedder modules develop the stego image by working parallel with preparation and also through the transmission process. Using this stego image, the extraction module will then decode it to retrieve the secret image. Each of the below subsections lists detailed operating information on each module:

A. Preparation network

We first perform initialization on the secret image to remove unnecessary features and lessen the processing load of its embedding network, before proceeding with the secret image processed side by side with cover.

Illustrate the initial network component of a convolutional neural network (CNN) in this series. This network segment prepares the input images (i.e., secret image: input_S1, cover image: input_C) to be embedded into steganographic and called as preprocess network. The first 3 layers are convolutional with different filter sizes (3x3, 4 x 4 and5 x contradictory) applied to secret image independently at the end of network. Different filter sizes are applied to extract different features from the input image, through a large number of convolutional layers which inputs images. The process produces three intermediate feature maps x3, x4 and x5. These feature maps extract different amounts of spatial information from the input image.

Then the results of convolutional layers are concatenated, aggregate relevant information from different sizes and form a unified tensor(x). Then feed the concatenated tensor to another convolutional layer as a final process similar like above step then applied stacked patches of flatten on merged features. The operation is repeated one more time, which uses different Conv layers configuration on the input_S1. This is combined with the other back-propagated layer results which are again able to form x1 and this time merge it with input_C (cover image). The last concatenation combines the processed features of both cover as well and secret images to get a complete representation which is finally embedded into Steganography image. Using RELU activation in all the layers. ReLU stands for Rectified Linear Unit; It is a method by which the value of each pixel in feature map shall be tested one after other. The process is to put all negative pixel values equal to zero which means they get replaced.[17]

The primary objective of this preparation network is to improve the compatibility between the cover and secret images. It achieves this by extracting and condensing useful data from the input images, hence reducing the computational burden on the future embedding network.

B. Hiding Network

This part describes one of the main concepts in a CNN which is nothing else than "hiding network". The hiding network embeds the information from secret image into cover image to generate stego-image.

The process starts by passing the input tensor (x) through a few convolutional layers for different filter size (3x3, 4x4 and5 x5). The convolutional layers in this case will be taking out different features from the input data thereby also capturing varying levels of information at a go. The ReLU activation function is used in all the convolutional layers to introduce non-linearity, allowing the network to learn more complex patterns.

After each sequence of convolutional layers, the resulting feature maps (x3,x4,x5) are aggregated by concatenation across channel dimension. Concatenation will combine all of these individual features which are extracted at various filter sizes into a single tensor, thereby boosting the network capacity to represent our input data. The above process is iterated numerous times in order to enhance the network's structure and augment the feature representation. The ultimate merging is fed into an additional convolutional layer to generate the output tensor that represents the stego image.

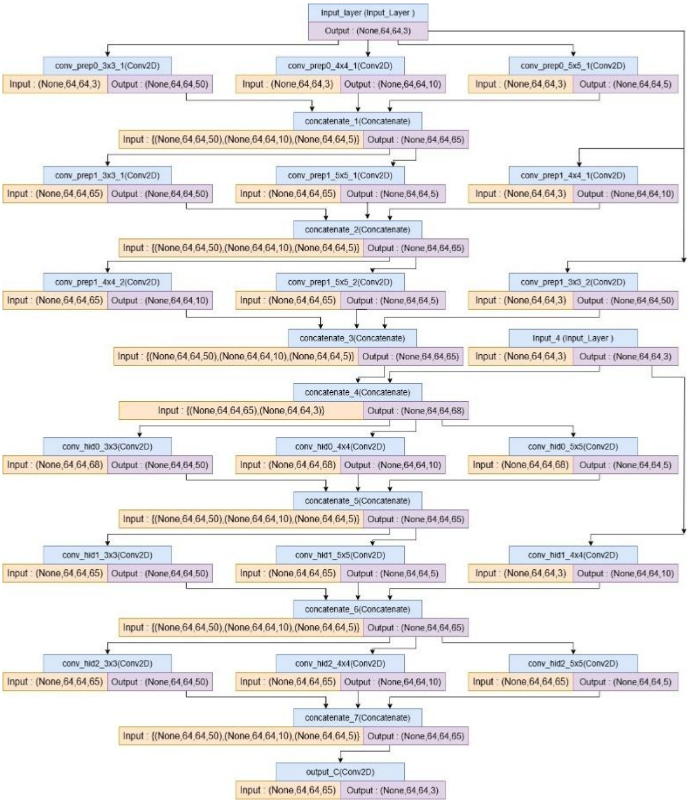


Figure 1: the encoder model.

In summary, this concealment network serves an essential function in incorporating information from the hidden image into the cover image while maintaining the visual integrity of the cover image.

The combined networks, comprising both the preparation and hiding networks, are collectively referred to as the encoder model. Figure 1 illustrates the operational mechanism of the encoder model.

C. Reveal Network

Within the domain of image steganography, a reveal network is essential for exposing hidden information contained within images. These networks are designed to operate with embedding algorithms to detect and interpret concealed data, allowing for the extraction of hidden messages or material from images, while maintaining their visual integrity and ensuring their security.

The network initiates with three Conv2D layers, each utilising distinct filter sizes (3x3, 4x4, and 5x5), all applied to the identical input (reveal_input). The ReLU activation functions are applied to these layers, resulting in output feature maps of varying sizes. The convolutional layers produce an output, which is then combined along the channel axis using the concatenate function, resulting in a single tensor called x.

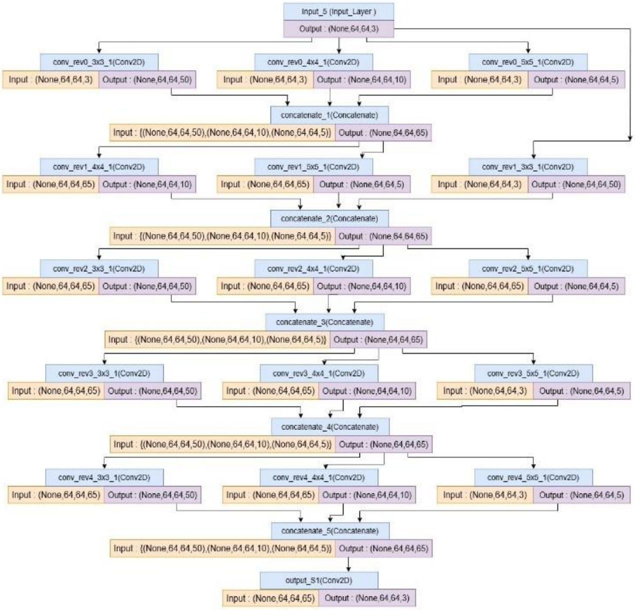


Figure 2: the decoder model.

The above process is iterated numerous times, wherein each iteration incorporates further sets of convolutional layers (x3, x4, x5) and combines their outputs with the preceding x by concatenation. The input for each set of convolutional layers is the output of the preceding concatenation operation. After several iterations, the final concatenated tensor x is passed through another convolutional layers to reduce the number of filters and produce the secret color image (RGB).

This network is called decoder model in proposed system. The figure 2 show how the decoder model work.

4. Loss Function

Conventional methods for hiding image data are evaluated using well-established metrics such as mean squared error (MSE) [18] and peak signal-to-noise ratio (PSNR) [19]. These measurements assess the difference between the original cover image and the steganographic image, as well as the discrepancy between the secret image and the retrieved image.

In another context, the procedure requires the calculation of two separate losses: embedding loss and extraction loss. The process of embedding loss entails a comparison between the original cover image and the stego image produced by the embedding network. Conversely, the extraction loss evaluates the disparity between the initial secret image and the image that the extraction network produces. The cumulative loss encompasses both the embedding and extraction losses.

Let U represent the initial image and U' indicate the reconstituted image, which is created by integrating the hidden image generated by the embedding network. Similarly, the symbol A signifies the hidden image, while A' denotes the secret image that the extraction network has obtained. The loss function should be customised to optimize the learning process for the model. Loss functions are used to evaluate the performance of a model during training epochs by providing feedback through back-propagation. Equation 1 controls the loss function for the embedding network, known as LOSSem, while equation 2 dictates the loss function for the extraction network, known as LOSSex. Equation 3 calculates the total loss, represented as LOSS [20].

$$\mathrm{LOSSem} = |\, U - U' \,| \tag{1}$$

$$\mathrm{LOSSex} = |\, A - A' \,| \tag{2}$$

$$\mathrm{LOSS} = \mathrm{LOSSem} + \alpha * \mathrm{LOSSex} = |\, U - U' \,| + \alpha * |\, A - A' \,| \tag{3}$$

Beta represents the method of evaluating the magnitude of the rebuilding errors. The weights of the error term in the concealing network do not share the weights of the reveal network. However, the weights of the reveal network are shared across all the auto-encoding networks.

5. Quantification of performance

The effectiveness of the suggested model is evaluated using the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index (SSIM) as measurement criteria.

The Peak Signal-to-Noise Ratio (PSNR) is a quantitative measure employed to assess the accuracy of a reconstructed or processed signal in comparison to its initial, original form. It is frequently utilized in areas such as image processing, video compression, and telecommunications.

The computation of Peak Signal-to-Noise Ratio (PSNR) includes the comparison of the original signal I possess both the processed and compressed version K [21]. The Mean Squared Error (MSE)[22] is calculated by taking the average of the squared discrepancies between the pixel values of the two signals as shown in equation 4.

$$MSE = \frac{1}{m.n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I(i,j) - K(i,j))^{2} \quad (4)$$

Let m , n be the dimensions (height, width) for image. Where I (i,j) and K (i,j) denote the pixel values at coordinates (i,j) in the original and processed images, respectively.

The Peak Signal-to-Noise Ratio (PSNR) is then logarithmically processed using the square of the maximum possible pixel value (MAX^2), by dividing it with MSE, and scaling this rescaled version with a factor of 10 [23]. Equation 5 definition of PSNR formula.

$$PSNR = 10 \,.\, log_{10}(\frac{MAX^{2}}{MSE}) \quad (5)$$

Where MAX is the highest achievable pixel value, such as 255 for 8-bit grayscale images. PSNR is commonly represented in decibels (dB), serving as a metric for signal accuracy. Higher Peak Signal-to-Noise Ratio (PSNR) levels are indicative of superior quality, whereas lower values imply increased distortion or loss of information during the process of processing or compression.

The SSIM, standing for Structural Similarity Index [24] , is a clear image quality assessment metric measuring similarity between two images in terms of luminance, contrast and structure. This decision is based on the computation over mean, variance and correlation of pixel data with some carefully calculated constants there to ensure precision. The SSIM formula takes into account the local patterns of pixel intensities in both the original (x) and manipulated(y) images. The equation 6 representing the Structural Similarity Index (SSIM) [25].

SSIM(x,y)= ((2μxμy+C1)(2σxy+C2))/((μ_x^2 +μ_y^2+C1)(σ_x^2 +σ_y^2+C2)) (6)

Here, μx and μy are the means of x and y, σx and σy are the standard deviations, σxy is the covariance, and C1 and C2 are constants to avoid instability issues. Higher SSIM values indicate greater similarity between the images [26].

6. Result and discussion

Our objective is to present our experimental discoveries obtained through the analysis of a dataset that includes ImageNet and compare these results with many similar image steganography algorithms.

In the experiment, the dataset that was used was ImageNet and the cover image and secret image were resized to 32x32; the number of epochs was 35; the batch size was 32; and the number of images was 500 in each epoch. The results were as follows: The average PSNR for the cover image and decoded cover is 72.7943 dB and the average PSNR for the secret image and decoded secret is 69.7537 dB . The average SSIM for cover image and decoded cover is 0.97538 and the average SSIM for secret image and decoded secret is 0.92778. When the size of the cover and secret image changed to 64x64, other results showed that the PSNR for the cover image was 72.4855 dB and the PSNR for the secret image was 67.9996 dB . The SSIM for the cover image is 0.9431 and the SSIM for the secret image is 0.8573. But when the image size was as follows: 128 x 128, the average PSNR for the cover image and decoded cover was 73.6797 dB and the average PSNR for the secret image and decoded secret was 69.9525 dB . The average SSIM for cover image and decoded cover is 0.9480 and the average SSIM for secret image and decoded secret is 0.8570 . The final experiment was carried out using identical data parameters, with both cover and secret images sized at 256x256 pixels. And the result was : PSNR for cover image = 73.6342 dB and PSNR for secret image = 69.7512 dB . The SSIM for the cover image is 0.94477 and the SSIM for the secret image is 0.80442 . We found that when the number of images is less than 200 in each epoch, the PSNR for cover is 72.96340 and the PSNR for secret is 69.7512, which means the number of images when equal to 500 is best.

Table 1: PSNR and SSIM values for different runs of the proposed algorithm on ImageNet dataset.

Size	Cover-Stego		Secret-Revealed	
	PSNR	SSIM	PSNR	SSIM
32 X 32	72.794	0.9753	69.753	0.9277
64 x 64	72.485	0.9431	67.999	0.8573
128 x 128	73.679	0.9480	69.952	0.8570
256 x 256	73.634	0.9447	69.751	0.8044

The achieved results, as shown in table 1, indicate that the best values for PSNR and SSIM were reported with an image size of 128 x 128.

The figure 3 show us the loss validation for proposed model cross 35 epoch and figure 4 show sample result of the proposed algorithm on ImageNet dataset.

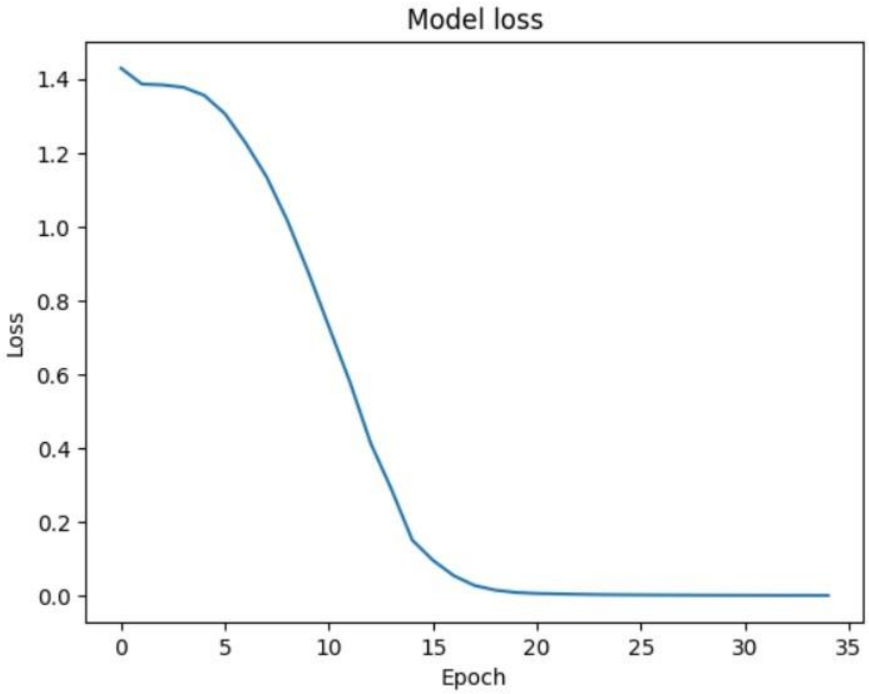
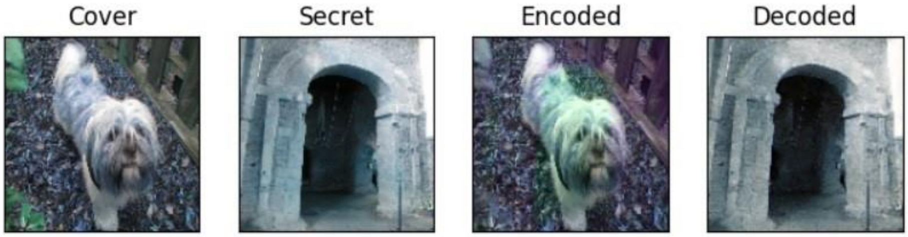


Figure 3: Loss function.



(A) (B) (C) (D)

Figure 4: (A) represent the cover image, (B) represent the secret image, (C) represent the Stego image, (D)represent the extract secret image.

The outcomes obtained using various techniques and deep learning algorithms were assessed in this section. as displayed in Table 2.

Table 2: Outcome derived from a deep learning approach.

Paper	Cover image size	Secret image size	Technique	Dataset	PSNR(dB)	SSIM
[11]	32 x 32 x 3	32 x 32 x 3	Auto-Encoder	ImageNet	34.88	0.9825
Proposed	32 x 32 x 3	32 x 32 x 3	Encoder-decoder	ImageNet	**72.79**	0.9753
[27]	144 x 144 x 3	144 x 144 x 3	ISN(GAN)	ImageNet	38.05	0.954
Proposed	144 x 144 x 3	144 x 144 x 3	Encoder-decoder	ImageNet	**69.33**	0.9033
[11]	128 x 128 x 3	128 x 128 x 3	Auto-Encoder	ImageNet	36.00	0.9692
Proposed	128 x 128 x 3	128 x 128 x 3	Encoder-decoder	ImageNet	**73.67**	0.9480
[15]	256 x 256 x 3	256 x 256 x 1	ISGAN	ImageNet	34.89	0.9681
[11]	256 x 256 x 3	256 x 256 x 3	Auto-Encoder	ImageNet	35.22	0.9554
[16]	256 x 256 x 3	256 x 256 x 3	Encoder-decoder	ImageNet	34.55	---
Proposed	256 x 256 x 3	256 x 256 x 3	Encoder-decoder	ImageNet	**73.63**	0.9447

The reported data vividly illustrate the remarkable efficacy of the suggested architecture, especially in terms of enhanced security, resilience, invisibility, and information concealment capabilities.

7. Conclusions

In this paper, we introduced a deep steganography method tailored for color images, employing an encoder-decoder architecture. By integrating PSNR and SSIM metrics into our evaluation framework, we not only ensured high embedding capacity but also prioritized perceptual quality and imperceptibility. Through extensive experimentation and evaluation on ImageNet dataset, our method exhibited superior performance compared to existing techniques, achieving a balance between hiding capacity and perceptual fidelity. The results demonstrate its potential for secure and covert communication applications, emphasizing the importance of maintaining both integrity and confidentiality in data transmission.

While our method has shown promise, future research can further advance deep steganography for color images. One avenue is to explore advanced neural network architectures and optimization techniques to enhance embedding capacity while minimizing perceptual distortion, as quantified by PSNR and SSIM metrics. Additionally, investigating the impact of different embedding strategies and payload sizes on system performance under real-world conditions would provide valuable insights. Addressing the challenge of steganalysis resistance by integrating adversarial training or other defense mechanisms could bolster security and stealthiest. Furthermore, extending the applicability of our method to other multimedia formats, such as videos, and exploring its potential for content protection in 3D models would broaden its utility. Overall, continued research in this direction holds promise for advancing deep steganography and bolstering its efficacy in practical applications requiring secure information hiding.

8. References

[1] ALRikabi, H. and H.T. Hazim, Enhanced data security of communication system using combined encryption and steganography. iJIM, 2021. 15(16): p. 145.

[2] Kumar, V., et al., Latest trends in deep learning techniques for image steganography. International Journal of Digital Crime and Forensics (IJDCF), 2023. 15(1): p. 1-14.

[3] Sattar, I.A. and M.T. Gaata. Image steganography technique based on adaptive random key generator with suitable cover selection. in 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT). 2017. IEEE.

[4] Kumar, M., S. Kumar, and H. Nagar, Comparative Analysis of Different Steganography Technique for image or Data Security. International Journal of Advanced Science & Technology (IJAST), 2020. 29(4).

[5] Shareef, F.R., A novel crypto technique based ciphertext shifting. Egyptian Informatics Journal, 2020. 21(2): p. 83-90.

[6] Rachael, O., et al. Image steganography and steganalysis based on least significant bit (LSB). in Proceedings of ICETIT 2019: Emerging Trends in Information Technology. 2020. Springer.

[7] Singhal, D., et al., CNN-based multiple manipulation detector using frequency domain features of image residuals. ACM Transactions on Intelligent Systems and Technology (TIST), 2020. 11(4): p. 1-26.

[8] Mandal, P.C., et al., Digital image steganography: A literature survey. Information sciences, 2022.

[9] Subramanian, N., et al., Image steganography: A review of the recent advances. IEEE access, 2021. 9: p. 23409-23423.

[10] Mehdi, S.A. and z.l. ali, Image Encryption Algorithm Based on a Novel Six-Dimensional Hyper- Chaotic System. Al-Mustansiriyah Journal of Science, 2020. 31(1): p. 54-63.

[11] Kich, I., Y.T. El Bachir Ameur, and A. Benhfid, Image steganography by deep CNN auto-encoder networks. International Journal, 2020. 9(4).

[12] Baluja, S., Hiding images in plain sight: Deep steganography. Advances in neural information processing systems, 2017. 30.

[13] Duan, X., et al., Reversible image steganography scheme based on a U-Net structure. IEEE Access, 2019. 7: p. 9314-9323.

[14] Rahim, R. and S. Nadeem. End-to-end trained cnn encoder-decoder networks for image steganography. in Proceedings of the European conference on computer vision (ECCV) workshops. 2018.

[15] Zhang, R., S. Dong, and J. Liu, Invisible steganography via generative adversarial networks. Multimedia tools and applications, 2019. 78: p. 8559-8575.

[16] Subramanian, N., et al., End-to-end image steganography using deep convolutional autoencoders. IEEE Access, 2021. 9: p. 135585-135593.

[17] Khassaf, N.M. and S.H. Shaker, Image Retrieval based Convolutional Neural Network. Al-Mustansiriyah Journal of Science, 2020. 31(4): p. 43-54.

[18] Hodson, T.O., T.M. Over, and S.S. Foks, Mean squared error, deconstructed. Journal of Advances in Modeling Earth Systems, 2021. 13(12): p. e2021MS002681.

[19] Suriyan, K., et al., Performance analysis of peak signal-to-noise ratio and multipath source routing using different denoising method. Bulletin of Electrical Engineering and Informatics, 2022. 11(1): p. 286-292.

[20] Nissar, A. and A.H. Mir, Classification of steganalysis techniques: A study. Digital Signal Processing, 2010. 20(6): p. 1758-1770.

[21] Keleş, O., et al. On the Computation of PSNR for a Set of Images or Video. in 2021 Picture Coding Symposium (PCS). 2021. IEEE.

[22] Chicco, D., M.J. Warrens, and G. Jurman, The coefficient of determination R-squared is more informative than SMAPE, MAE, MAPE, MSE and RMSE in regression analysis evaluation. PeerJ Computer Science, 2021. 7: p. e623.

[23] Hussien, M.k., Encryption of Stereo Images after Compression by Advanced Encryption Standard (AES). Al-Mustansiriyah Journal of Science, 2018. 28(2): p. 156 - 161.

[24] Setiadi, D.R.I.M., PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimedia Tools and Applications, 2021. 80(6): p. 8423-8444.

[25] Nilsson, J. and T. Akenine-Möller, Understanding ssim. arXiv preprint arXiv:2006.13846, 2020.

[26] Tang, Y., F. Ren, and W. Pedrycz, Fuzzy C-means clustering through SSIM and patch for image segmentation. Applied Soft Computing, 2020. 87: p. 105928.

[27] Lu, S.-P., et al. Large-capacity image steganography based on invertible neural networks. in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2021.

تعزيز أنظمة الاتصالات السرية من خلال إخفاء المعلومات العميقة

م . م . حيدر عقيد رجب [1]
haider.aqeed@gmail.com

أ.د. ميثاق طالب كاطع[2]
dr.methaq@uomustansiriyah.edu.iq

أ. م . د. مهند تحرير يونس[3]
mty@uomustansiriyah.edu.iq

المستخلص: لقد برز إخفاء الصورة العميقة كنهج واعد لإخفاء المعلومات السرية باستخدام الصور الرقمية، والاستفادة من قوة تقنيات التعلم العميق لتعزيز الأمن. تستكشف الدراسة تكامل الشبكات العصبية العميقة لتعزيز أمان ومتانة أساليب إخفاء المعلومات. قد تحتوي أساليب إخفاء المعلومات التقليدية على نقاط ضعف بسبب خوارزمياتها الثابتة، مما يجعلها أقل مرونة في التعامل مع أنواع مختلفة من مواد الصور وأكثر عرضة للاكتشاف بواسطة طرق تحليل إخفاء المعلومات المتقدمة. تهدف الطريقة المقترحة إلى تطوير أنظمة الاتصالات السرية من خلال استخدام التعلم العميق لتحقيق عدم الإدراك والقوة مقابل طرق التحليل الهيكلي الشائعة. تقدم هذه الدراسة شبكة عصبية تلافيفية عامة (CNN) مع بنية التشفير وفك التشفير لطريقة إخفاء الصور العميقة. فهو يسهل إخفاء المعلومات واستخراجها بسلاسة. من أجل تقييم فعالية النهج المقترح، تم استخدام قياسات نسبة الإشارة إلى الضوضاء ومؤشر التشابه الهيكلي. تظهر النتائج التجريبية المستندة إلى مجموعة بيانات ImageNet أن النهج الذي نتبعه يتفوق على الطرق المختارة ذات الصلة من حيث الأمان والقوة وعدم القدرة على الرؤية بصريًا. :72.79PSNR :0.9753SSIM نتائج الاختبار، وبالتالي نستنتج أن النهج الذي اقترحناه يتفوق على الطرق السابقة.

الكلمات المفتاحية: إخفاء الصور، التعلم العميق، الشبكة العصبية الملتفة، ذروة نسبة الإشارة إلى الضوضاء، قياس مؤشر التشابه الهيكلي.

[1] طالب ماجستير؛ قسم علوم الحاسبات – كلية العلوم - الجامعة المستنصرية - بغداد - العراق
[2] استاذ دكتور؛ قسم علوم الحاسبات – كلية العلوم - الجامعة المستنصرية - بغداد - العراق
[3] استاذ مساعد دكتور؛ قسم علوم الحاسبات – كلية العلوم - الجامعة المستنصرية - بغداد - العراق