Secure eHealth: A Secure eHealth System to Detect COVID Using Image Steganography

Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed,
Department of Computer Science and Engineering,
Qatar University

Introduction

COVID is a pandemic which has spread to all parts of the world.

Detection of COVID infection is crucial to prevent the spread further. Contactless health care systems are essential which can be implemented with Cloud computing.

Privacy and security of the medical image data transferred through untrusted channels cannot be ensured.

The main aim is to secure the medical details when transferring them from the end device to the cloud and vice versa using image steganography.

The medical lung images are masked under a normal and natural cover images.

Research Questions

1. Can deep learning methods produce secure and robust image steganography without complicated structure?

2. Is it possible to hide a RGB secret image of the same size as the RGB cover image without any distortion?

System Overview
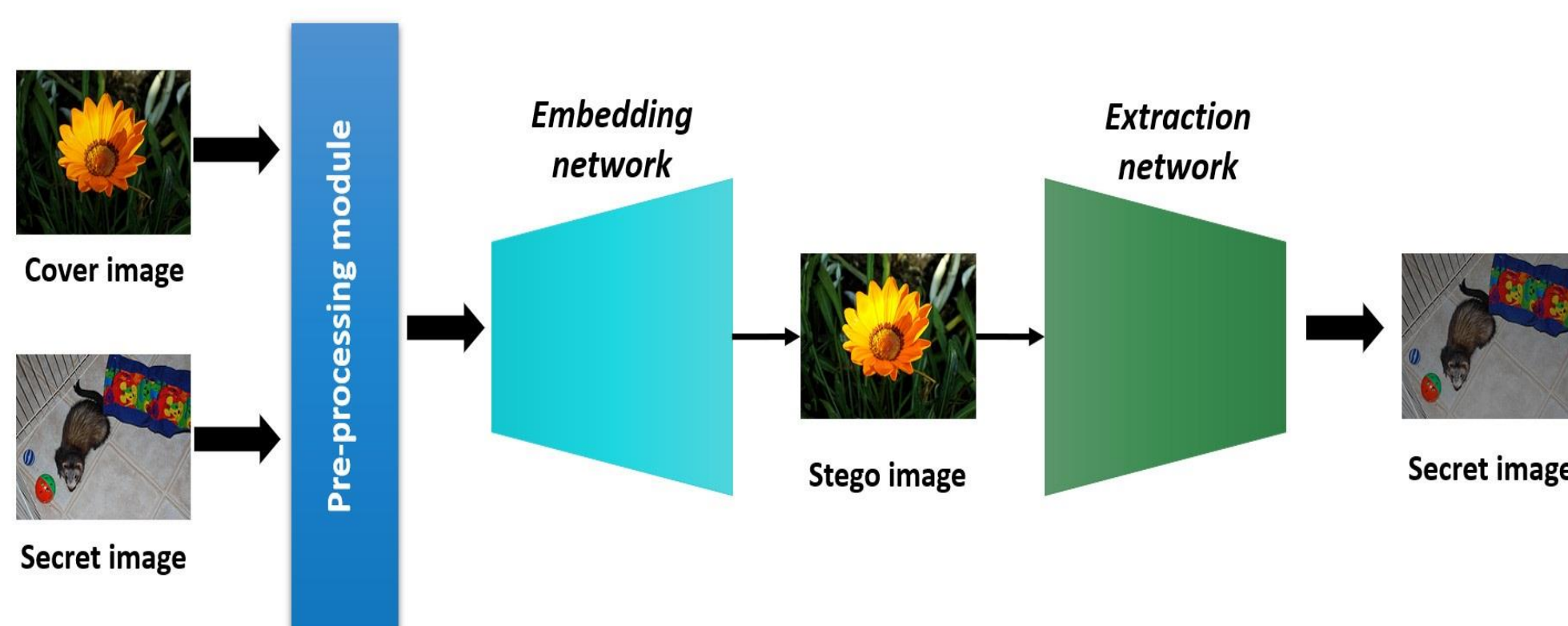
Methodology

Preprocessing Module : Three layers of convolutional layer. Both the original cover image and original secret image are passed concurrently to extract features. A concatenation layer is used to merge the features.

Embedding Network : The merged features are given as input to reconstruct the steganography image with secret image embedded in the cover image. Embedding Network is situated at the end devices side. Pre-processing and the embedding are carried out together.

Extraction Network: The steganography image is used to input to extract the secret image. Extraction network is at the Cloud Server end.

Architecture of the Proposed Model
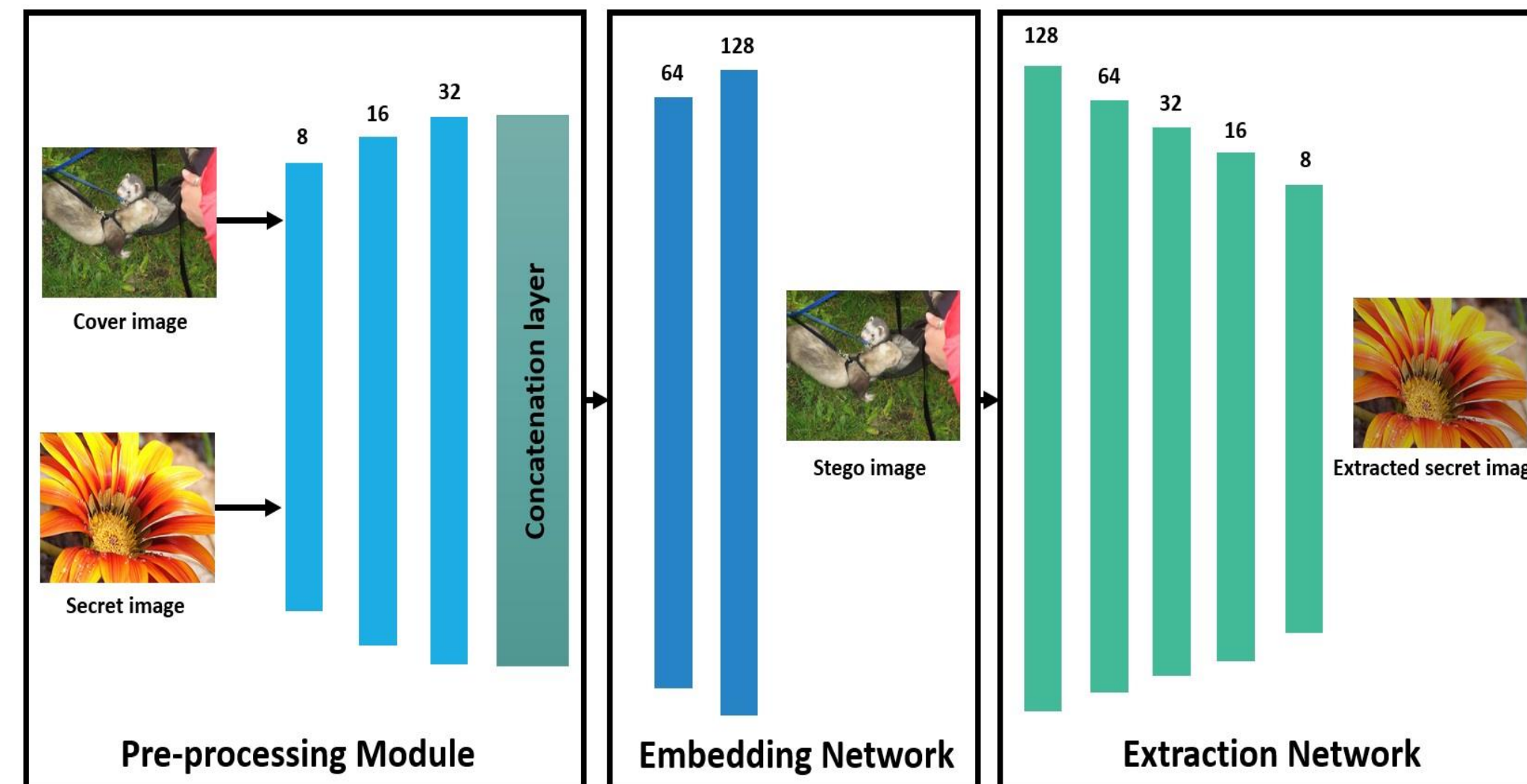
Tiny Imagenet – Sample Images
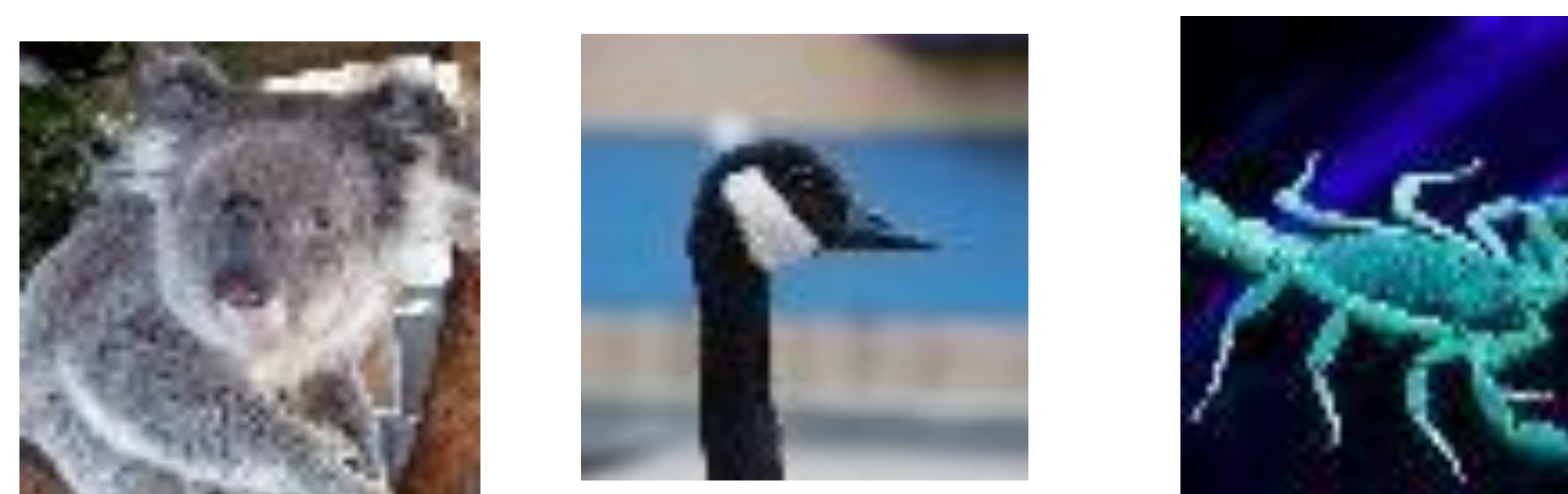
Evaluation Metrics

$$MSE = \frac{\sum_{R,C}[Image_1(r,c) - Image_2(r,c)]^2}{R * C}$$

$$PSNR = 10 LOG_{10}(\frac{M^2}{MSE})$$

Results

Result of the Proposed Method

Method	Embedding Network		Extraction Network	
	MSE	PSNR	MSE	PSNR
Proposed Method	77.18	29.30	44.85	27.90

Comparison Results with Traditional Steganography Methods

Method	Image Size	Airplane	Baboon	Lena	Peppers
[1]	512x512	37	37	37	37
[2]	512x512	32.74	32.41	33.16	32.41
[3]	512x512	-	-	32.09	-
[4]	512x512	32.774	32.448	32.49	32.725
Proposed Method	64x64	32.15	29.76	29.49	29.14

Image result of the Proposed Method on ImageNet dataset

(a) Cover image (b) Secret image (c) Stego image (d) Extracted Secret image

Image result of the Proposed Method on real time lung X-ray images

(a) Cover image (b) Secret image (c) Stegano image (d) Extracted Secret image
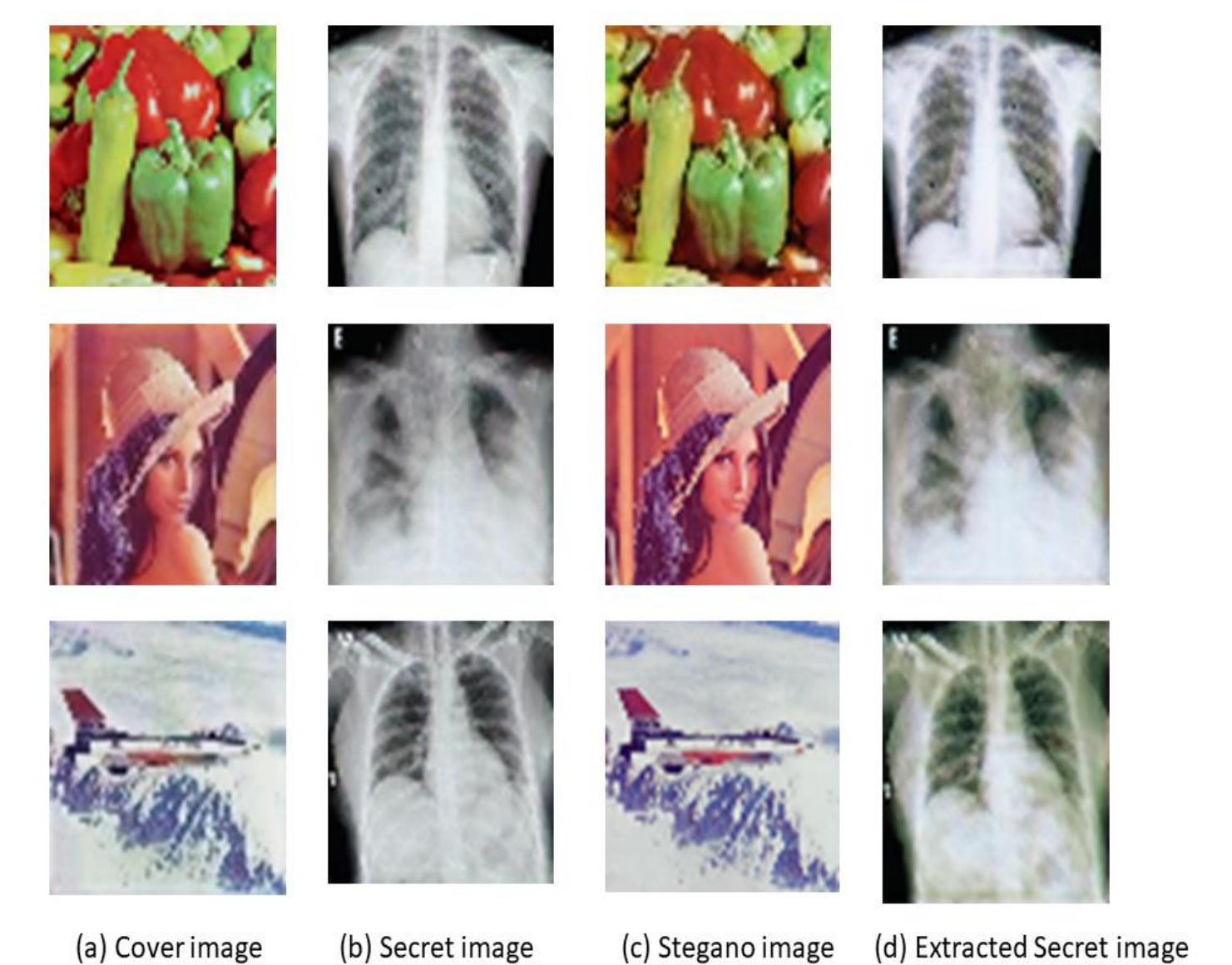
Discussion

It can be clearly seen that the generated steganography image obtained using the proposed deep learning model is similar to the cover image without any noise and higher invisibility.

Generated steganography images have higher invisibility, higher security and robustness compared to the traditional LSB methods.

Higher security and robustness is obtained even when the cover image is plain (black/white) and the secret image is full of information.

Privacy and security of the medical records of the patients is ensured through image steganography.

Acknowledgment

Contact

Nandhini Subramanian
Email:ns1808900@student.qu.edu.qa

References

1. Qiu, A., Chen, X., Sun, X., Wang, S., Guo, W.: Coverless image steganography method based on feature selection. Journal of Information Hiding and Privacy Protection 1(2), 49 (2019).
2. Swain, G.: Very high capacity image steganography technique using quotient value differencing and lsb substitution. Arabian Journal for Science and Engineering 44 (06 2018). https://doi.org/10.1007/s13369-018-3372-2
3. Patel, N., Meena, S.: Lsb based image steganography using dynamic key cryptography. In: 2016 International Conference on Emerging Trends in Communication Technologies (ETCT). pp. 1{5. IEEE (2016).
4. Elharrouss, O., Almaadeed, N., Al-Maadeed, S.: An image steganography approach based on k-least signi_cant bits (k-lsb). In: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). pp. 131{135 (2020).
5. Xintao, D., Jia, K., Li, B., Guo, D., Zhang, E., Qin, C.: Reversible image steganography scheme based on a u-net structure. IEEE Access PP, 1{1 (01 2019). https://doi.org/10.1109/ACCESS.2019.2891247
6. Ali, M.A., Jaoua, A., Al-Maadeed, S.A.: A novel conceptual machine learning method using random conceptual decomposition. In: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). pp. 18{22 (2020).
7. Baluja, S.: Hiding images in plain sight: Deep steganography. In: Advances in Neural Information Processing Systems. pp. 2069{2079 (2017).
8. 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," in IEEE Access, vol. 7, pp. 90574-90584, 2019, doi: 10.1109/ACCESS.2019.2920956.