Stego-eHealth: An eHealth System for Secured Transfer of Medical Images Using Image Steganography.

Nandhini Subramanian[1], Jayakanth Kunhoth[1], Somaya Al-Maadeed[1], Ahmed Bouridane[2]
[1]Department of Computer Science and Engineering, Qatar University
[2]Department of Computer and Information Sciences, Northumbria University, United Kingdom

Faculty and PostDoc, ICT

Introduction

COVID pandemic which has spread to all parts of the world has necessitated the need for virtual and online health care systems to avoid contacts and hence the spread of the virus.

The transfer of sensitive medical information including the chest and lung X-ray happens through untrusted channels making it prone to many possible attacks.

This paper aims to secure the medical data of the patients using image steganography when transferring through untrusted channels.

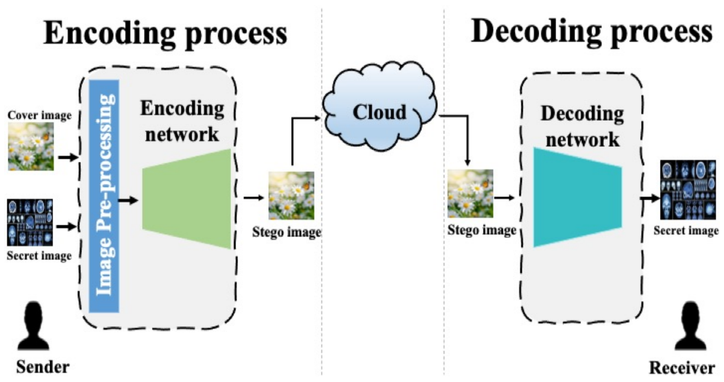
At the sending end, the medical images are embedded in a normal natural scene image and at the receiving end the embedded medical image is extracted for easy access.

Research Questions

1. Is it possible to develop an end-to-end image steganography using deep learning method? Can a simple, light-weight produce secure, robust and imperceptible stego image?

2. Is it possible to embed a 3-channel secret image inside a 3-channel cover image of the same size without image distortion?

System Overview



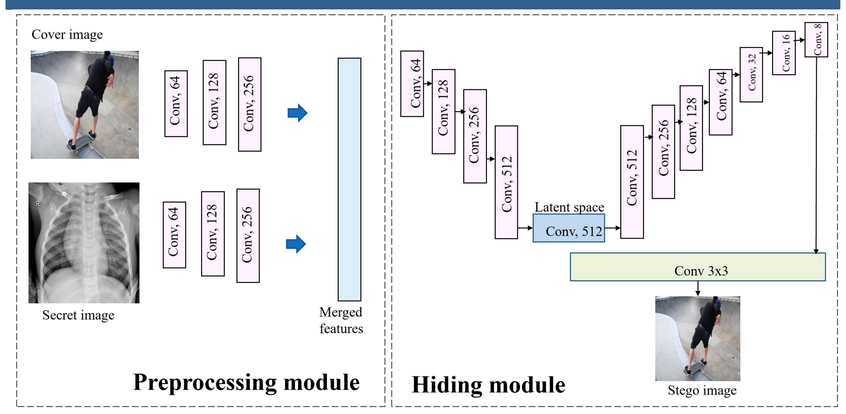
Methodology

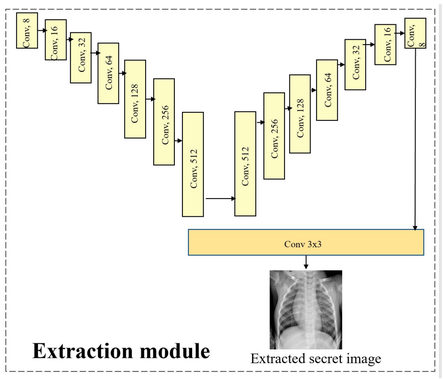
Preprocessing Module : Features from the cover image and the secret image are extracted by passing it concurrently through three convolutional layers in the preprocessing module.

Embedding Network : The merged features from the preprocessing module is used to output the stego image which is similar in resemblance to the cover image by the embedding network

Extraction Network: The stego image is given as the input to the extraction network to extract the ingrained secret image. A customized loss which is the combination of the embedding loss, and the extraction loss is used. The training and testing of the proposed model is performed on the COCO and the Kaggle Chest Xray dataset.

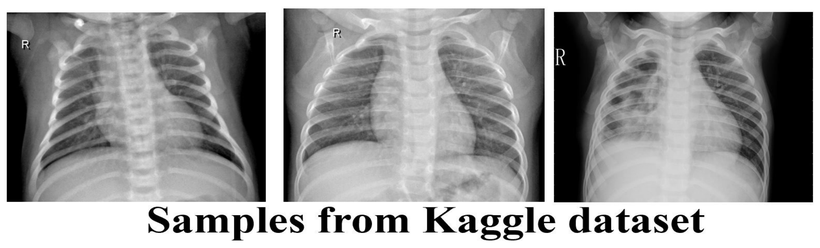
Architecture of the Model





Datasets

Samples from COCO dataset



Samples from Kaggle dataset

Results

Result of the Proposed Method

Method	Embedding Network		Extraction Network	
	MSE	PSNR	MSE	PSNR
Proposed Method	40.15	32.16	44.64	31.96

Comparison of PSNR Among the proposed and traditional methods

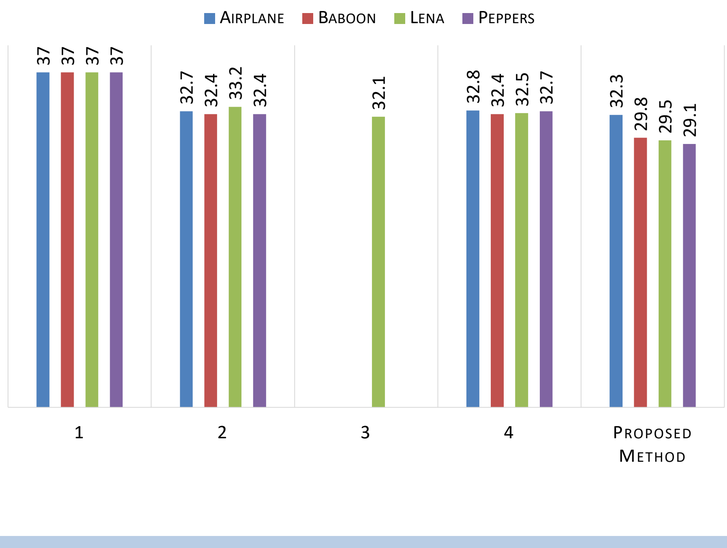
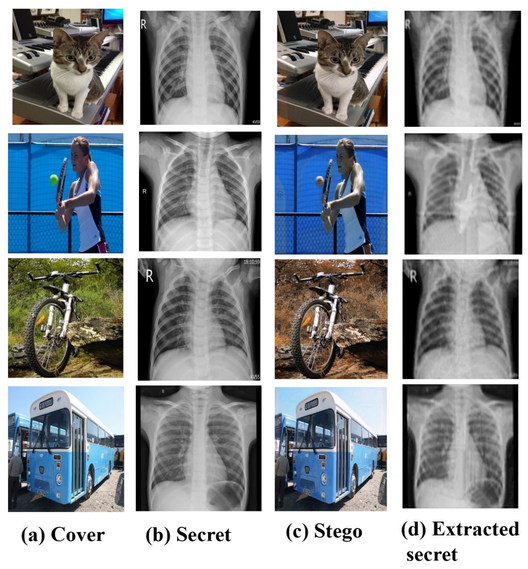
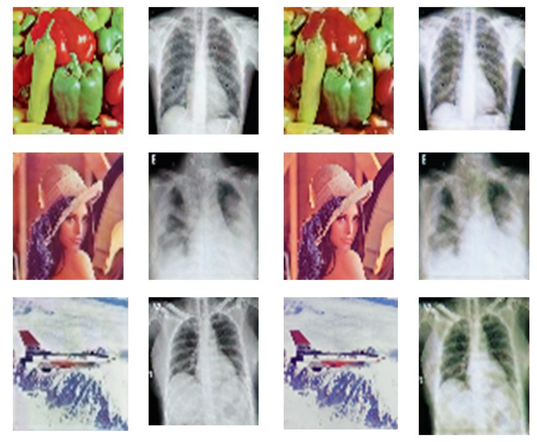


Image result of the Proposed Method on COCO and Kaggle dataset



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

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

The image results produced by the method shows higher imperceptibility.

The hiding capacity of the proposed method is 100% since both the cover and the stego images are of the same size.

PSNR value of the proposed method shows higher security and robustness compared to the traditional LSB methods.

A simple and light-weight architecture is proposed without any compromise on the performance of the method.

Sensitive data is secured and the privacy is preserved while transferring them through untrusted channel.

Acknowledgment

This work was made possible by NPRP11S-0113-180276 from the Qatar National Research Fund (a member of Qatar Foundation). The findings achieved herein are solely the responsibility of the author.

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.