DS 7406 Machine Learning Systems
Joseph Choi (nmf8dm)
Karolina Naranjo-Velasco(kn3cs)
September 21, 2022
Project proposal

Introduction

The applications of deep learning systems in healthcare - image processing- involve technological and ethical challenges to protect patient data (Abdullah et al., 2021). Some techniques such as generative adversarial networks (GANs) and GMEI-GANs have been used to generate meaningful encrypted images for data hiding techniques, such as the reversible hiding technique (RDH), seeking to promote security and privacy in machine learning systems (Huang et al., 2022).

The use of autoencoders for data encryption is computationally expensive. For this reason, new frameworks have been developed for lossy image encryption and decryption using a simple surface-encryption neural network maintained by a low-power mobile ARM processor in real-time (Gupta, 2020).

In addition, batch image encryption has been used for schemes with a stacked self-encryption (SAE) network - parallel computing - leading to a significant reduction in runtime complexity (Hu et al., 2017). Therefore, we proposed a neural-network based encoding scheme to protect highly sensitive data, i.e., medical record of the patient.

Research Problem

- How can we transfer data over the network more 1) efficiently and 2) securely?

Data

- NIH ChestXRay data set [6]:
  100,000 de-identified images of chest x-rays of 32,717 unique patients for eight disease labels (in 256 x 256 resolution)

Methods

- Deep Neural Network is known for a “black-box” model [ref]. We suggest to apply deep representative network based methods to encode medical images ($R^{256x256}$) into a latent vector (R^{15}) [ref-ref]. Unlike mathematical based encoding algorithms, it is nearly impossible to decipher latent vector representation of the medical image without the correct neural network based decoder, thus we could achieve a more **secure** method to protect the medical images. Thus, we believe we can achieve **efficiency** with the latent representation as transferring and storing 15 real numbers are much more efficient than 256 x 256 real numbers.

Timeline

1) Data manipulation and design of the architecture
2) Experiments
3) Deliverable 1: the written report
4) Deliverable 2: presentation

References

Abdullah, T. A., Zahid, M. S. M., & Ali, W. (2021). A review of interpretable ml in healthcare: Taxonomy, applications, challenges, and future directions. *Symmetry*, *13*(12), 2439.

Castelvecchi, D. (2016). Can we open the black box of AI? *Nature* **538**, 20-23.

Huang, Q. X., Yap, W. L., Chiu, M. Y., & Sun, H. M. (2022). Privacy-Preserving Deep Learning With Learnable Image Encryption on Medical Images. *IEEE Access*, *10*, 66345-66355.

Tsai, C. S., Wu, H. C., Li, Y. W., & Ying, J. J. C. (2021). Applying GMEI-GAN to Generate Meaningful Encrypted Images in Reversible Data Hiding Techniques. *Symmetry*, *13*(12), 2438.

Gupta, C. (2020). Shallow Encoder Deep Decoder (SEDD) Networks for Image Encryption and Decryption. *arXiv preprint arXiv:2001.03017*.

Wang, M. et al., (2017). ChestX-ray8: hospital-scale chest x-ray database and benchmarks on weakly-supervised classification and localization of common thorax diseases. *CVPR 2017.*