Crypson

An end-to-end deep learning encryption framework

Andreas Karatzas

April 16, 2024

Advanced Computer Security

Electrical, Computer and Biomedical Engineering

Crypson

Introduction

What is **Crypson**

1. An end-to-end deep learning encryption framework.
2. **Encoder:** ❶ Conditional Generative Adversarial Network with ❷ Variational Auto-Encoder and ❸ Deep Time Step Generator.
3. **Decoder:** ❹ Classifier.
4. EMNIST dataset.
5. Classification accuracy of 90.77%.

Motivation

Conventional encryption and **Quantum** computing

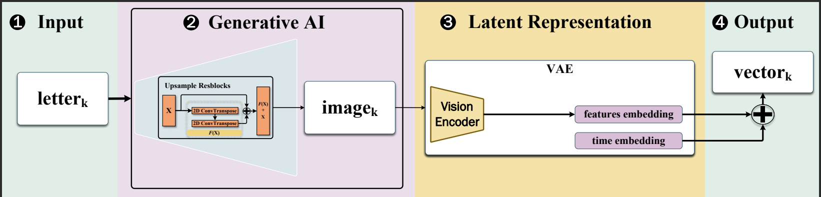
Basic neural network properties:

1. **Non-linear** relationships.
2. **Scalability**.
3. **Efficiency**.

Methodology

Encoder

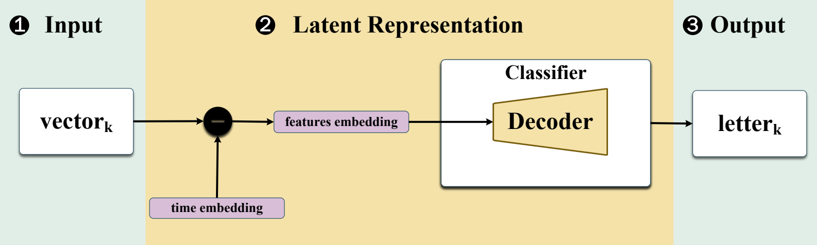
① Sequence of words. ② Tokenize words into letters l_k, $k \in 0, N$. ③ For each letter, input random noise in cGAN. ④ Generating letter (encryption key). ⑤ Invoke VAE to compress pixel features. ⑥ Sum with a time embedding. ⑦ Send encrypted vector k.



Methodology

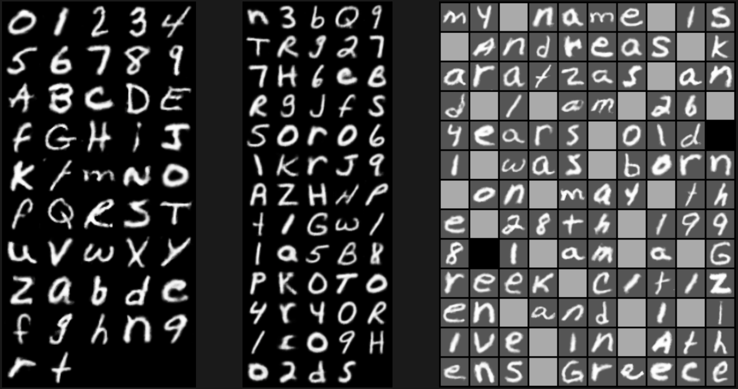
Decoder

❶ Receive encrypted vector *k*. ❷ Subtract time embedding. ❸ Invoke classifier to decrypt message.



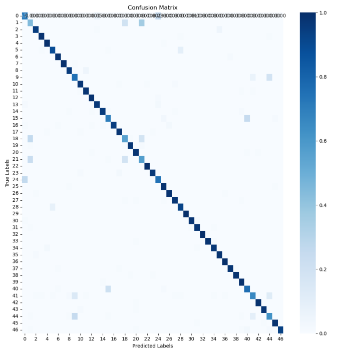
Results

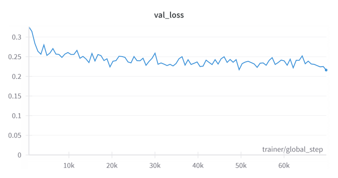
Generated and **Reconstructed** samples

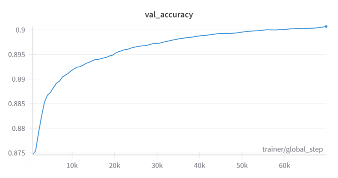


Results

Classifier







Implementation & Demo

GitHub Repo

Conclusion & Questions

Summary

❶ Capitalize on AI to address security challenges in end-to-end encryption. ❷ Peer-to-peer ❸ conditional Generative Adversarial Network (cGAN) ❹ Variational Auto-Encoder (VAE) ❺ classifier to decode. ❻ The framework is evaluated on the EMNIST dataset and achieves a classification accuracy of 90.77%, rendering it:

1. **Secure:** Time embedding to mask the latent space.
2. **Scalable:** VAE to compress the images into a latent space.
3. **Efficient:** Classifier to predict the class.