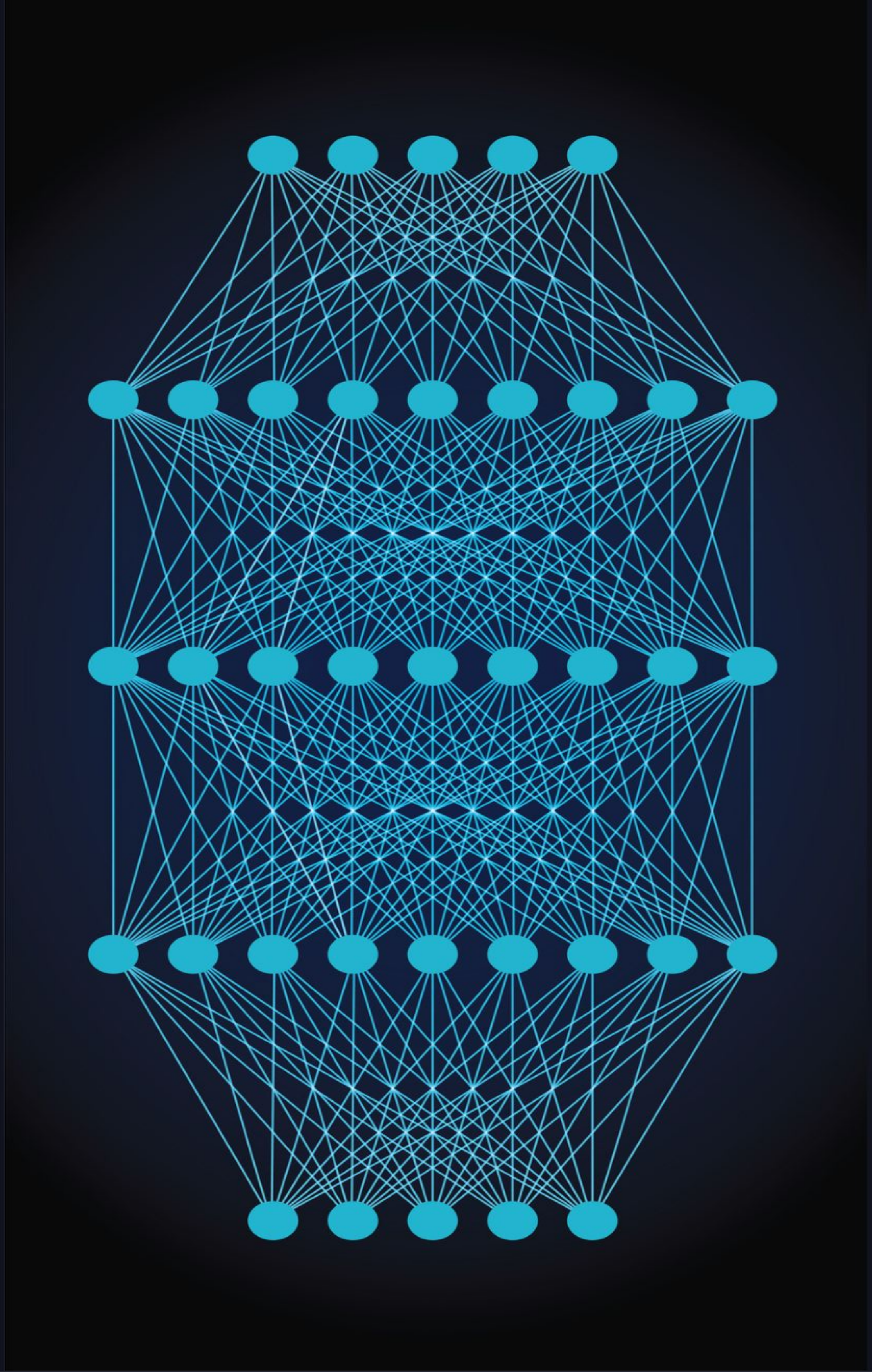


Image Encryption using Convolutional Neural Network

– Satyam Kumar

Motivation: Data Privacy in the Digital Age

1 Ubiquitous Data

The exponential growth of digital content

2 Evolving Threats

Increasingly sophisticated hacking techniques.

3 User Empowerment

Secure, user-friendly encryption empowers individuals and organizations to protect sensitive information.

Problem Statement

- Conceal a given image inside another image i.e, container
- Retrieve the given image from the combination with high accuracy
- The structural data of the image to be concealed should be preserved
- The generated combination should be similar to the container image

Loss Function: Encoding and Decoding

Decoding Loss

Minimizes the difference between the original and reconstructed images, ensuring accurate recovery.

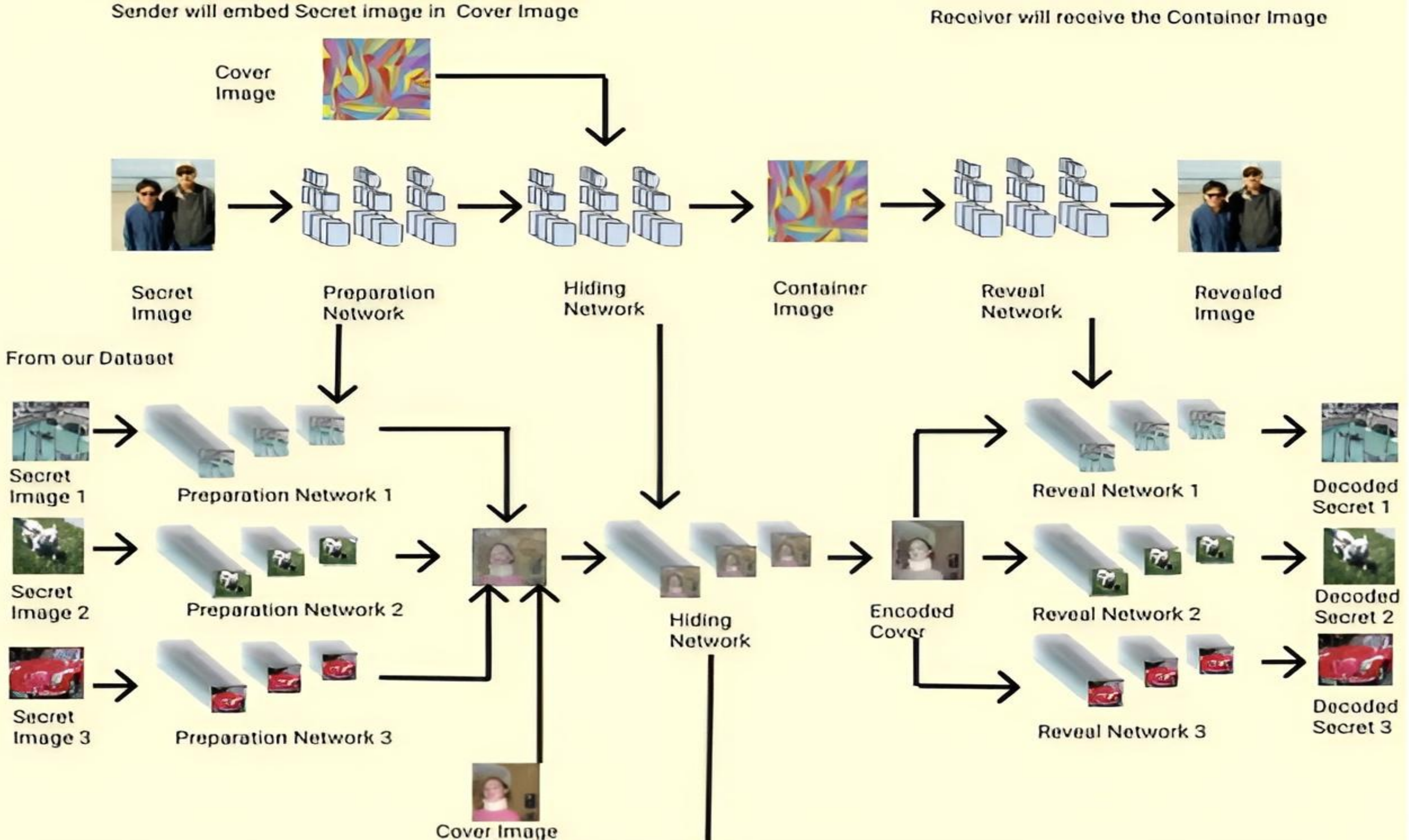
Encoding Loss

Pixel wise mean squared error between container image and encoded output to maintain similarity

Balanced Optimization

The model is trained using a loss function that tries to minimize both the decoding and encoding loss and is controlled by a scale factor

Architecture


Sender will embed Secret image in Cover Image
Receiver will receive the Container Image
Cover Image
Secret Image
Preparation Network
Hiding Network
Container Image
Reveal Network
Revealed Image
From our Dataset
Secret Image 1
Preparation Network 1
Secret Image 2
Preparation Network 2
Secret Image 3
Preparation Network 3
Cover Image
Hiding Network
Encoded Cover
Reveal Network 1
Reveal Network 2
Reveal Network 3
Decoded Secret 1
Decoded Secret 2
Decoded Secret 3

Training

1

Loading and preprocessing

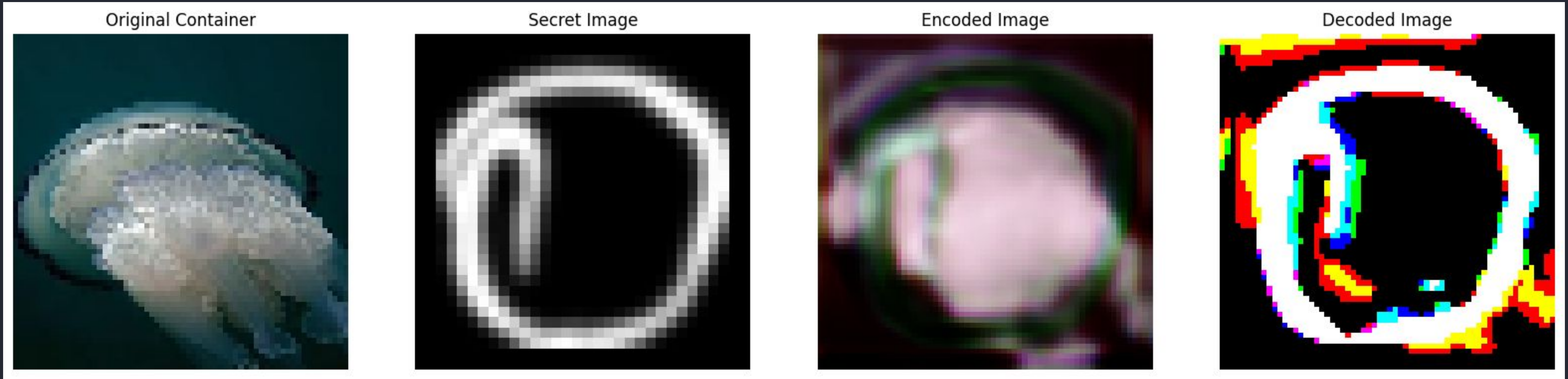
2

Pairing up images randomly and making batches

3

Training the model for 2000 iterations with custom loss function

Results



Original Container

Secret Image

Encoded Image

Decoded Image

Demonstration

Phase 2

Robustness

Enhancing the model's resilience against adversarial attacks and noise to ensure reliable encryption.

Efficiency

Optimizing the model's computational and memory requirements for real-time, resource-constrained applications.

Generalization

Expanding the model's capabilities to handle diverse image types and resolutions.

Interpretability

Improving the model's transparency and explainability to build user trust and confidence.

Learnings

References

- IMAGE STEGANOGRAPHY USING CNN Shourya Chambial, Dhruv Sood
- Tensorflow documentation
- Lab assignments on image processing
- Tkinter documentation