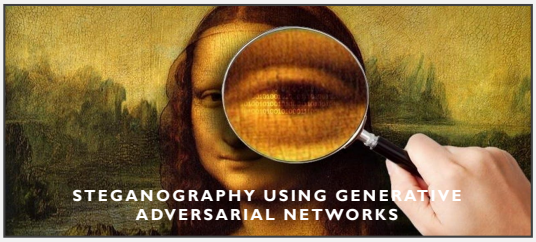


CS 512-COMPUTER VISION

Presented by:

Sahil Bhaware	A20552865
Aniket Chougule	A20552758

1

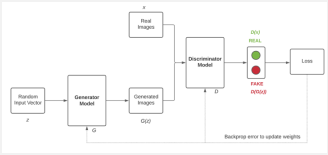
WHAT IS STEGANOGRAPHY?

Steganography is the art and science of concealing information within another medium, such as an image, audio, or video file, in a way that makes the hidden content undetectable to unintended observers, thereby ensuring covert communication

2

WHAT IS GAN

Generative Adversarial Network (GAN)



- **Two-Part Model**: Generator and discriminator compete.
- **Generator**: Makes realistic fake data.
- **Discriminator**: Detects fake data.
- **Training**: Networks improve by competition.
- **Uses**: Image generation, style transfer, medical imaging.

3

THE NEED FOR GAN-BASED STEGANOGRAPHY

ISSUES WITH TRADITIONAL TECHNIQUES

1. Detectability
2. Quality Loss
3. Limited Scalability

HUGO | LSB Matching | WOW | S-UNIWARD

DEVELOPMENT OF STEGANALYSIS

Histogram analysis | LSB Analysis | statistical anomaly detection

4

ADVANTAGES OF GAN-BASED STEGANOGRAPHY OVER EMBEDDING

Higher Capacity

GANs can hide more data without compromising image quality.

Automatic Generation

Ideal for large-scale or dynamic implementations.

Undetectability

GANs generate realistic images, making hidden data less detectable.

5

PROJECT INSPIRATION

'A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks'

- published in 2018 by IEEE
- DONGHUI HU, LIANG WANG, WENJIE JIANG, SHULI ZHENG, AND BIN LI

6

DATASET

Dataset Used: CelebA Dataset

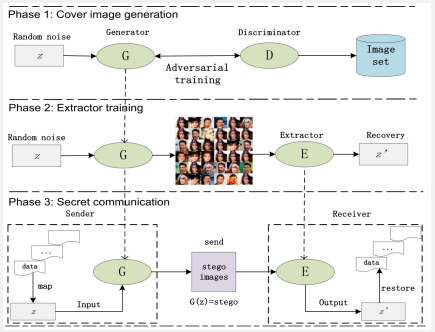
- contains over 200,000 celebrity images
- 10,000 unique identities
- 40 attribute labels (e.g., age, gender, facial features

Preprocessing:

- Image Resizing
- Normalization
- Data Shuffling

7

IMPLEMENTATION PROPOSED IN THE PAPER



8

OUR IMPLEMENTATION

PHASE 1: DATASET AND PREPROCESSING
Selects and prepares the dataset, resizing and normalizing images for uniformity and efficient loading.

PHASE 2: BUILDING DCGAN MODEL
Constructs the generator and discriminator models, setting up for adversarial image generation and classification.

PHASE 3: DCGAN TRAINING
Trains both models in an adversarial loop, optimizing the generator to produce realistic images.

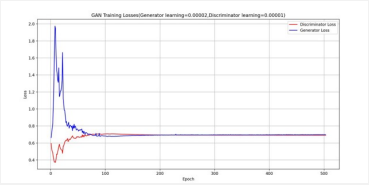
PHASE 4: EXTRACTOR MODEL
Develops a model to decode hidden messages by retrieving encoded noise vectors from stego images.

PHASE 5: SECRET MESSAGE HIDING (SENDER SIDE)
Uses the generator to embed binary messages in images, creating stego images for secure data transfer.

PHASE 6: SECRET MESSAGE EXTRACTION (RECEIVER SIDE)
Decodes the hidden message from stego images, reconstructing the original data accurately for the receiver.

9

EVALUATION



To summarize,

- **Initial High Loss**: Both generator and discriminator start with high losses.
- **Rapid Decrease in Discriminator Loss**:Discriminator quickly learns to differentiate real from fake.
- **Stabilization of Losses**: Losses settle around 0.6, indicating balance.
- **Learning Rates Impact**: Gradual convergence due to small learning rates.
- **Adversarial Training Dynamics**: Generator and discriminator reach a balanced state.

10

CHALLENGES FACED

- Resource and Memory Constraints
- Long and Computationally Intensive Training
- Complexity in Model Convergence and Stability
- Hyperparameter Tuning and Optimization
- Data Preprocessing and Augmentation Needs
- Evaluating and Interpreting Model Performance

11

FUTURE SCOPE AND ENHANCEMENTS

GAN with Advanced Architectures
Try WGAN, PG-GAN, or StyleGAN for improved realism.

Conditional GANs
Add controls for specific features (e.g., color, style).

12