Nathan Melaku

BahirDar Institute Of Technology

December 4, 2019





Powerful Generative Steganography With Generative Adversarial

Nathan Melaku

Introduction

Literature Review

robiem tatement

bjectives

Viethodolog

Scope

Significance Of The Study

Vork Plan

udget

## Introduction

Powerful Generative Steganography With Generative Adversarial Networks

Literature Review

Nathan Melaku

**Problem Statement** 

roduction

Objectives

terature review

Methodology

Lination

Scope

tilodolo

Significance Of The Study

Study

Work Plan

rk Plan

Budget

uget

References

## Introduction

Steganography

Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

Introduction

Literature Review

Statement

Objectives

Methodology

Scope

ignificance Of

Nork Plan

Budget

References

Hiding Information in plain sight.

## Introduction

Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

Introduction

Literature Review

Statemen

Dbjectives

Methodology

Scope

ignificance O he Study

Nork Plan

udget

References

Steganography

- ► Hiding Information in plain sight.
- simmon's prisoners. (Simmons, 1984)

## GAN

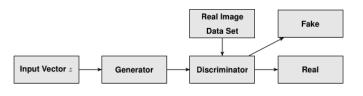


Figure: GAN

$$\begin{split} \min_{G} \max_{D} V(D,G) &= E_{x \ p_{data}(x)}[logD(x)] \\ &+ E_{z \ p_{z}(z)}[log(1-D(G(z)))]. \end{split}$$

Powerful Generative Steganography With Generative Adversarial Networks

## Nathan Melaku

#### Introduction

Literature Review

Statemen

)bjectives

Methodology

#### Scope

Significance Of The Study

Nork Plan

#### udget

Nathan Melaku

Introduction

Literature Review

Stateme

Objectives

Methodology

Scope

Significance O The Study

Nork Plan

Budget

References

## Requirements for steganography

- Imperceptibility
- Robustness
- payload capacity

#### Nathan Melaku

#### Introduction

Literature Review

Stateme

Objective

Methodology

Scope

ignificance The Study

Vork Dlan

Work Plan

udget

References

## Requirements for steganography

- ► Imperceptibility
- Robustness
- payload capacity

#### Nathan Melaku

#### Introduction

Literature Review

Statem

Objective

Methodology

Scope

ignificance Of The Study

Nork Plan

Budget

References

## <□ > <□ > <□ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

Requirements for steganography

ImperceptibilityRobustness

payload capacity

## Literature Review

Powerful Generative Steganography With Generative Adversarial

Nathan Melaku

Introduction

Literature Review

Statement

Djectives

/lethodology

Scope

Significance Of

Vork Plan

udget

deferences

Different approaches to steganography

- cover modification
- cover synthesis: (Fridrich, 2009)

Statement

Scope

Significance O The Study

Vork Plan

Budget

References

## GAN in Steganography.

- ► (Volkhonskiy et al., 2017)
- ► (Shi et al., 2017)
- ► And some more others (Tang et al., 2017),(Hayes & Danezis, 2017)

ntroduction

#### Literature Review

Statement

Objectives

Methodology

Scope

Significance Of The Study

Vork Plan

Budget

References

## GAN in Steganography.

- ► (Volkhonskiy et al., 2017)
- ► (Shi et al., 2017)
- ► And some more others (Tang et al., 2017),(Hayes & Danezis. 2017)

Nathan Melaku

ntroduction

Literature Review

Statement

Objectives

Methodology

Scope

ignificance Of The Study

Vork Plan

Budget

References

## GAN in Steganography.

- ► (Volkhonskiy et al., 2017)
- ► (Shi et al., 2017)
- ► And some more others (Tang et al., 2017),(Hayes & Danezis, 2017)

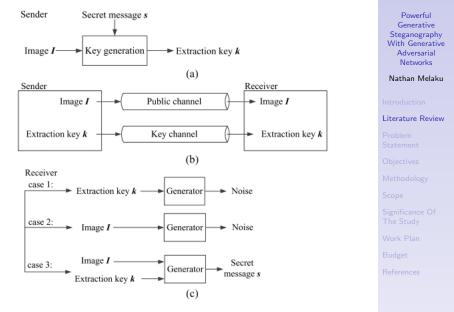


Figure: Proposed System in (Ke et al., 2017)

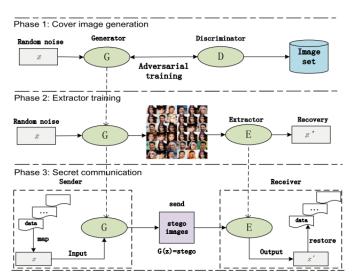


Figure: Proposed System in (Hu et al., 2018)

Nathan Melaku

Introduction

Literature Review

Problem Statemer

Objectives

Methodology

cope

ignificance Of The Study

Vork Plan

Budget

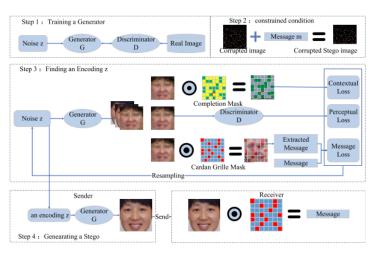


Figure: Proposed System in (Zhang & Yang, 2019)

Nathan Melaku

troduction

Literature Review

roblem tatement

bjectives

Methodolog

cope

Significance Of The Study

Nork Plan

udget

## Problem Statement

Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

Problem Statement

## Observed problems:

- Instability of Training
- Slow convergence
- ► Inadequately realistic image generation

"This is mainly associated to the GAN technique used in the framework."

## Problem Statement

Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

ntroduction

Literature Review

Problem Statement

bjectives

vietnodolo

cope

ignificance Of The Study

Nork Plan

. .

References

Observed problems:

- Instability of Training
- Slow convergence
- ► Inadequately realistic image generation

"This is mainly associated to the GAN technique used in the framework."

# **Objectives**

Design and implement a powerful generative steganographic framework using a most suitable GAN.

Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

Introduction

Literature Review

Statement

Objectives

Methodology

Scope

ignificance Of The Study

Vork Plan

udget

# Objectives

▶ Improve stability of Training and convergence speed.

Generate more realistic image.

Specific objectives:

Maintain state of the art security.

ntroduction

Literature Review

Statement

Objectives

Methodology

Scope

iignificance Of The Study

Nork Plan

Budget

References

## 4□ > 4₫ > 4½ > 4½ > ½ 9 Q C 13

Specific objectives:

Generate more realistic image.

Maintain state of the art security.

▶ Improve stability of Training and convergence speed.

## 13 / 25

ntroduction

Literature Review

Statement

Objectives

Methodology

Scope

lignificance Of The Study

Nork Plan

Budget

References

## Specific objectives:

- Improve stability of Training and convergence speed.
- ► Generate more realistic image.
- Maintain state of the art security.

# Methodology

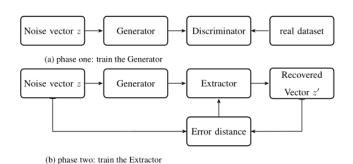


Figure: System Architecture

Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

Introduction

Literature Review

Statement

Objectives

Methodology

cope

ignificance Of

Vork Plan

Budget

#### Nathan Melaku

ntroduction

Literature Review

Problem

Objectives

Methodology

Scope

ignificance Of he Study

Nork Plan

Budget

References

## Choice of GAN:

- ► BEGAN
- ► RGAN
- ► WGAN-DIV
- ► WGAN-GP

ntroduction

Literature Review

Problem Statemen

Objectives

Methodology

Scope

ignificance O

Nork Plan

Budget

References

## Choice of dataset:

- CelebA
- ► LFW
- ► Food101
- ► MNIST

#### Nathan Melaku

ntroduction

Literature Review

Problem Statemen

Objectives

Methodology

Scope

ignificance Of

Nork Plan

Budget

References

# Choice of testing method:

- Visual instpection
- ► Inception score
- ► Visual Turing test
- MOS

#### Nathan Melaku

Introduction

Literature Review

Statement

o bjectives

Methodology

## Scope

Significance Of The Study

Work Plan

Budget

References

## Robustness

- Passive Adversary
- Payload Capacity
- Imperceptibility

# Scope

Powerful Generative Steganography With Generative Adversarial Networks

#### Nathan Melaku

Introduction

Literature Review

Statemer

Objectives

Methodology

## Scope

Significance Of

Nork Plan

udget

- Robustness
- ► Passive Adversary
- ► Payload Capacity
- Imperceptibility

# Scope

- Powerful Generative Steganography With Generative Adversarial Networks
  - Nathan Melaku

Introduction

Literature Review

Statemen

Objectives

Methodology

## Scope

Significance Of

Nork Plan

Budget

References

Robustness

- ► Passive Adversary
- ► Payload Capacity
- Imperceptibility

# Scope

Powerful Generative Steganography With Generative Adversarial Networks

#### Nathan Melaku

Introduction

Literature Review

Stateme

Objectives

Methodology

### Scope

Significance Of

Nork Plan

udget

References

Robustness

- ► Passive Adversary
- ► Payload Capacity
- ► Imperceptibility

# Significance Of The Study

The main problem in generative steganography

**Imperceptibility** 

Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

Introduction

Literature Review

Problem Statement

Objectives

1ethodology

Scope

Significance Of The Study

Nork Plan

udget

References

## Work Plan

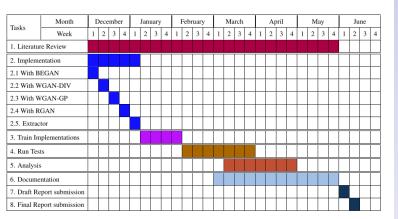


Figure: Proposed work plan

Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

roduction

Literature Review

roblem tatement

bjectives

vietnodoi

cope

ignificance Of he Studv

Work Plan

References

# Budget

## Main cost of the project:

- ► Powerful GPU for training.
  - From the university
  - ► Amazon EC2
  - ► Google Cloud

Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

Introduction

Literature Review

Problem Statemen

Objectives

/lethodology

Scope

ignificance Of

Vork Plan

Budget

## Reference I

Fridrich, J. (2009). Steganography in digital media: principles, algorithms, and applications. Cambridge University Press.

Hayes, J., & Danezis, G. (2017). Generating steganographic images via adversarial training. In Advances in neural information processing systems (pp. 1954–1963).

Hu, D., Wang, L., Jiang, W., Zheng, S., & Li, B. (2018). A novel image steganography method via deep convolutional generative adversarial networks. *IEEE Access*, 6, 38303–38314. doi: 10.1109/ACCESS.2018.2852771

Ke, Y., Zhang, M.-q., Liu, J., Su, T.-t., & Yang, X.-y. (2017). Generative Steganography with Kerckhoffs' Principle based on Generative Adversarial Networks. arXiv preprint arXiv:1711.04916, 1–5. Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

troduction

Literature Review

statement

Jecuves

vietnodolo

cope

Significance Of The Study

Vork Plan

. . .

References

Shi, H., Dong, J., Wang, W., Qian, Y., & Zhang, X. (2017). Ssgan: secure steganography based on generative adversarial networks. In Pacific rim conference on multimedia (pp. 534-544).

Simmons, G. J. (1984). The prisoners' problem and the subliminal channel. In Advances in cryptology (pp. 51–67).

Tang, W., Tan, S., Li, B., & Huang, J. (2017). Automatic steganographic distortion learning using a generative adversarial network. IEEE Signal Processing Letters, *24*(10), 1547–1551.

Volkhonskiy, D., Nazarov, I., Borisenko, B., & Burnaev, E. (2017). Steganographic generative adversarial networks. arXiv preprint arXiv:1703.05502.

## Reference III

Zhang, M., & Yang, X. (2019). Generative Steganography by Sampling.  $IEEE\ Access,\ 7,\ 118586-118597.$  doi: 10.1109/ACCESS.2019.2920313

Powerful Generative Steganography With Generative Adversarial Networks

Nathan Melaku

Introduction

Literature Review

roblem tatement

biectives

Methodology

Scope

gnificance Of le Study

ork Plan

ıdget

## Nathan Melaku

Introduction

Literature Review

Statemen

Objectives

Methodology

Scope

Significance Of

/ork Plan

ıdget

References

THANK YOU