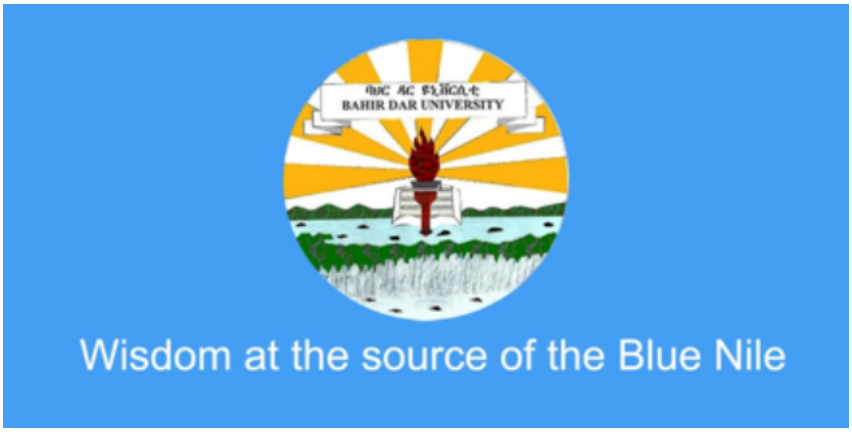
BahirDar Institute of Technology

Faculty of Electrical and Computer Engineering

Thesis Proposal

Master Of Science

Powerful Generative Steganography Using Generative Adversarial Networks



Date of Submission:

November 28, 2019

SUBMITTED BY: Nathan Melaku

ID: BDU/11049

SIGNED: _____

BahirDar Institute of Technology - BahirDar University

School Of Research And Graduate Studies

Faculty Of Electrical And Computer Engineering

THESIS PROPOSAL

Student:

Name Signature Date

The following graduate faculty members certify that this student has successfully presented the necessary written proposal and oral presentation of this proposal for partial fulfillment of the thesis-option requirement for the Degree of Master of Science in Computer Engineering.

Approved:

Advisor:

Name Signature Date

Chair Holder:

Name Signature Date

Faculty Dean:

Name Signature Date

Abstract

Steganographic algorithms are mainly evaluated by their security. Traditional steganographic frameworks used different embedding algorithms to achieve this goal. This means, embedding the secret message directly to a cover image. Nonetheless, with the development of sophisticated machine learning based steganalysis algorithms even the slightest modifications can be detected. This has triggered a lot of researchers to pursue coverless steganography. In my thesis, I will design and implement a generative steganography framework using the state of the art GAN.The main goal is to improve the quality of the generated stego images without compromising the security.

Keywords— Generative Steganography, GAN, Security

Acknowledgment

I would like to thank my family for their relentless support and guidance. I would also like to thank my advisor Dr. Henok Mulugeta for reviewing my research title. I thank my dear friend Kine Tibebu for an insightful discussion about the research matter. Finally and most importantly I thank my dearest and beloved Finot Mebratu, simply speaking what would I do without you.

List of Abbreviations

ACGAN Auxilary Classifier Generative Adversarial Network. 6, 8

BEGAN Boundary Equilibrium Generative Adversarial Networks. 11, 15

DCGAN Deep Convolusional Generative Adversarial Network. 5, 7, 8, 11

DCT discrete cosine transform. 3

DFT discrete Fourier transform. 3

DWT discrete wavelet transform. 3

GAN Generative Adversarial Network. ii, v, 3–11, 20

GPU graphical processing unit. 16

GSK generative steganography with Kerckhoffs' principle. 6

GSS generative steganography by sampling. 7

infoGAN Interpretable representation learning by information maximizing generative adversarial nets. 6, 8, 10

LSB Least Significant Bit. 3

MOS mean opinion score. 12

RGAN Relativistic GAN. 11, 15

SWE steganography with out embedding. v, 5, 6

WGAN Wasserstein Generative Adversarial Network. 5, 8

WGAN-DIV Wasserstein Divergence for GANs. 12, 15

WGAN-GP Improved Training of Wasserstein GANs with gradient penality. 12, 15

Contents

1 Introduction

In the past decades a wide spread use of digital communication and a huge increase in network bandwidth have been observed. The internet has become the primary gateway for media transmission, including audio, video, image, and text. The need for securing this transmission is of prime importance. Many practices which provide this security are proposed and are working in the wild.(Yahya, 2018)

There are two common approaches to provide security in transmission.

1. Cryptography
2. Steganograpy

Cryptography changes the secret information to be sent known as “plain text”into dis-formed and meaningless data called “cipher text”through reversible mathematical operations. The main purpose of cryptography is to inhibit an unintended recipient from gaining any insight about the message while allowing intended recipients to read the message by reversing the dis-formation with a cryptographic key. Equations 1 and 2 explains this process.

$$c = E_{k_1}\{m\} \tag{1}$$

$$m = D_{k_2}\{c\} \tag{2}$$

Where

- c is the cipher text message
- m is the plain text message
- E_{k_1} is the encryption algorithm under key k_1
- D_{k_2} is the decryption algorithm under key k_2. k_1 and k_2 are not necessarily equal.

Steganography on the other hand approaches the question of security from a different perspective. It is a technique of camouflaging the secret information in a cover media. Thereby preventing any unintended recipient from even recognizing the presence of hidden secret information in the cover media.

Steganography in its classical model was proposed by Simmons in 1984 as the famously known “prisoners’ problem”. (Simmons, 1984) In this problem Alice and Bob

are in prison far apart from each other. And they would like to devise an escape-plan. However, the only form of communication they have is through the warden, who allow the prisoners to exchange message that is completely open to him. So the question is how could Alice and Bob communicate about their escape-plan without the warden getting suspicious. Equations 3 and 4 explains this process.

$$s = Embed\{m, c\} \tag{3}$$

$$m = Extract\{s\} \tag{4}$$

Where

- s is the stego-image, which is the cover image with the embedded message,
- $Embed\{\cdot\}$ is the message embedding algorithm,
- m is the message,
- c is the cover image,
- $Extract\{\cdot\}$ is the message extraction algorithm.

1.1 Requirements Of Steganography

There are mainly three requirements for steganography. (Yahya, 2018) The first requirement is Imperceptibility (indetectability), which measures how difficult it is to recognize the presence of hidden information. This is the most crucial and primary requirement of steganography. (G. Chen, Zhang, Chen, Fu, & Wu, 2012)

Robustness is the other requirement. It measures how well the system resists the elimination of the embedded information in various attacks such as compression, and filtering of the stego-image. (Bahi, Couchot, & Guyeux, 2012)

The third requirement is payload capacity. It represents the maximum amount of data that can be embedded using the steganographic system.

1.2 Traditional Steganography

In traditional steganography, secret message is embedded directly in the pixel values of the cover image. Generally traditional steganographic algorithms can be divided

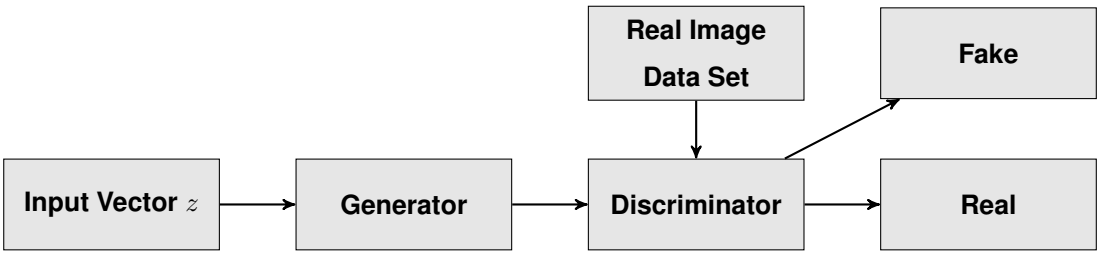


Figure 1: A Generative Adversarial Network

into two: spacial domain hiding and transform domain hiding.(M. M. Liu, Zhang, Liu, Gao, & Zhang, 2018). In spacial domain hiding, the secret information is hidden by replacing the LSB(M. M. Liu et al., 2018) while in transform domain method the cover image data is modified by changing some statistical features to achieve secrete hiding, such as the hidden method in DFT(discrete Fourier transform) domain, DCT (discrete cosine transform) domain, and DWT (discrete wavelet transform) domain.

The main weekness of traditional steganographic framework defined in equations 3 and 4 is it involves the modification of an existing cover image. Therefore, it is inevitable to leave slight trace of modification. This opens a door for very successful steganalysis. To provide a solution to this a different type of steganography that is based on cover sythesis has been proposed and is still a hot research issue.(Hu, Wang, Jiang, Zheng, & Li, 2018)

1.3 GAN (Generative Adversarial Network)

GANs are first introduced in (Goodfellow et al., 2014) in 2014. In a GAN a generative model is trained with an adversary, namely the discriminator which is trained on a real image data set to discriminate any counterfeit image that are not from the real data distribution. This competition drives both parties to improve their technique until the generated images are not distinguishable from the real ones. Figure 1 show the over all model of a GAN. The paper (Goodfellow et al., 2014) further shows that when both the generator and the discriminator are multilayer perceptron it is possible to train the entire system using backpropagation.

Starting from their conception GANs are being widely used in computer vision, natural language processing, image synthesis, and now in steganography. (Zhang & Yang, 2019)

2 Literature Review

(Fridrich, 2009) was the first one to investigate the idea of cover synthesis. (Fridrich, 2009) He proposed an image hashing method for achieving secret embedding. First selecting an appropriate image for the secret and sending it, then the receiver will calculate the image hash to reveal the secret information. However, this is not practical because of low secret embedding capacity. (Otori & Kuriyama, 2007) proposed a method of synthesizing texture images for embedding secret data by using smart techniques of generating repetitive texture patterns through feature learning of a sample image. They used a sample texture and some color points generated using the secret message and used this to construct dense texture images. Then this was improved to have more capacity by (K.-C. Wu & Wang, 2014).

Even though there were this improvements in the area of cover synthesis steganography, the main leap was not achieved until the discovery of GANs in (Goodfellow et al., 2014). After the discovery of GANs, *et.al.* (Volkhonskiy, Nazarov, Borisenko, & Burnaev, 2017) proposed a model for generating image containers using DCGAN. They used DCGAN to generate cover images that are more secure in hiding the secret information. This approach is found to be more secure than the traditional steganographic models. (Shi, Dong, Wang, Qian, & Zhang, 2017) used this concept and improved the GAN performance by using different type of GAN called WGAN.(Arjovsky, Chintala, & Bottou, 2017) This greatly improved the convergence speed, training stability and image quality. This and some other papers proposed similar improvements and variations of cover synthesis algorithms.(Tang, Tan, Li, & Huang, 2017)(Hayes & Danezis, 2017)

As noted in (Zhang & Yang, 2019) this previous papers still rely on cover modification after the cover synthesis phase. This is a poor utilization of GANs. Since GANs are powerful generators they are powerful samplers. Therefore, exploiting this feature will result in better frameworks with no modification. In the following subsection I will explain three papers that have achieved steganography without embedding (SWE) .(Zhang & Yang, 2019)(Hu et al., 2018)(Ke, Zhang, Liu, Su, & Yang, 2017)

2.1 SWE

(Ke et al., 2017) first proposed a generative steganography called GSK. In GSK, the secret messages are generated by a cover image using a generator rather than embedded into the cover, thus resulting in no modifications in the cover. The GSK framework consists of two GANs called the Message GAN and the Cover GAN. The message GAN is used to control the output by using feature codes. Feature codes are attributes in the samples of the dataset that are independent and give meaning to the generated images. Examples given are skin color, "fat or thin", *etc.* Using this feature code and a noise vector the message GAN will generate not only realistic images but also images that conform to this feature set. The message GAN was implemented with infoGANs (X. Chen et al., 2016). The cover GAN has the main functionality of making the cover image a necessary input to determine the generation of secret message according to Kerckhoff's principle.(Kerckhoffs, 1883) The cover GAN is composed of three neural networks that are structured based on adversarial neural symmetric cryptography(Abadi & Andersen, 2016), in which Alice and Bob both neural networks are trained to minimize what Eve a third neural network learns about the communication by eavesdropping. Despite this remarkable design one of the main pitfall of this framework is its low capacity. Since the secret hiding space is the feature code of the image it imposes a small capacity. The other main pitfall is the quality of the generated images.

According to (Zhang & Yang, 2019) the term "generative steganography"was first introduced in (M. M. Liu et al., 2018).They used ACGAN which have an input of class label in addition to the noise vector of a standard GAN. The main idea of the method in (M. M. Liu et al., 2018) is that the class label of GANs is replaced with the secret information as a driver to generate hidden image directly, and then extract the secret information from the hidden image through the discriminator.

(Hu et al., 2018) proposed an image SWE method based on deep convolutional generative adversarial networks. They map the secret information into a noise vector and use the trained generator neural network model to generate the carrier image based on the noise vector. No modification or embedding operations are required during the process of image generation, and the information contained in the image can be extracted successfully by another neural network, called the extractor, after training. This framework has an advantage of high capacity with relative capacity of 9.16e-3 and re-

markable recovery accuracy that could reach even up to 98%.However it greatly suffers from generated image quality. The authors reported that due to poor image quality some images did not escape detection by staganalysis tools. According to the paper one the main drawback of this framework is the usage of DCGANs.

Recently (Zhang & Yang, 2019) proposed data-driven information hiding scheme called "generative steganography by sampling" (GSS). This method uses semantic image inpainting. The message is written in advance to an uncorrupted region that needs to be retained in the corrupted image. Then, the corrupted image with the secret message is fed into a Generator trained by a GAN for semantic completion. They treated generative steganography as constrained image inpainting problem. Instead of generating a whole image they started from a corrupted image and used a GAN for image completion. Before this corrupted image is fed to the generator the secret message is inserted in the uncorrupted regions of the corrupted image using Cardan grille. They have achieved good relative capacity that could be up to 1.10e-2. However just like the above mentioned papers they suffer from poor image quality. They used DCGAN for the generator and they have admitted that the use of a more powerful generator will enhance the quality of the generated images. The other main contribution of this paper is the introduction of a new security criterion motivated by ϵ-security of (Cachin, 1998). They used the Jenson-Shanon divergence which is the loss metric of DCGAN to measure the steganographic security. However if the two probability distributions whose divergence is being measured are so far apart that there is no overlap between the two the Jenson-Shanon divergence is constant which is a fatal problem for gradient based learning, since it would make the gradient zero at this point. Though this problem is noted in the paper, they choose Jenson-Shanon because they used DCGAN for the generator.

3 Statement Of Problem

Generative Steganography has better defense against steganalysis tools. The main reason behind this strength is synthesis of cover images and the lack of modification. Despite this useful advantage, Generative steganography is at its infancy. The main drawbacks are instability of training, slow convergence speed, and inadequately realistic image generation. This is mainly associated to the GAN technique used in the framework. As shown in section 2 the GAN technique mostly used is DCGAN, and to lesser extent ACGAN, infoGAN and WGAN. This problem is explicitly mentioned in (Hu et al., 2018), (Zhang & Yang, 2019), and (Ke et al., 2017). However, GANs have been improved through the past five years. And there are more than 30 variants available at this time. This calls for a better generative steganography framework using a powerful GAN.

4 Objectives

The research have the following general objective:

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

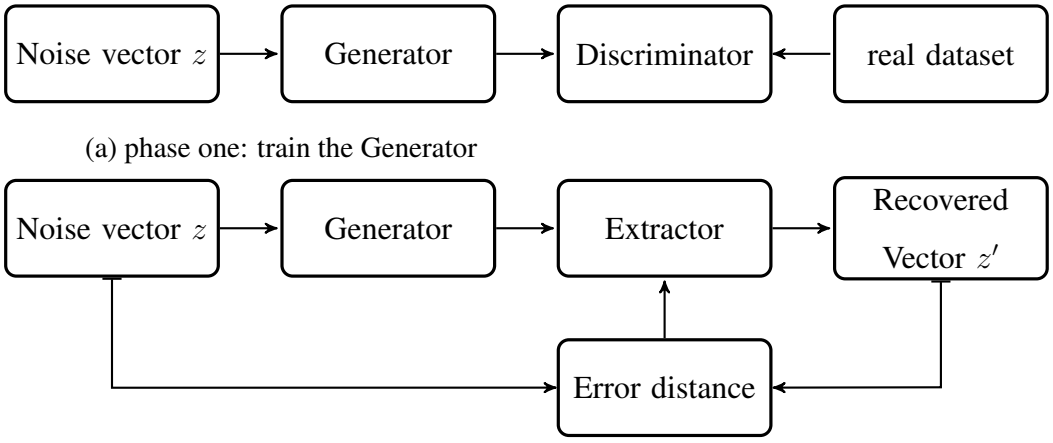
In Order to achieve the above mentioned goal the following specific goals must be mate.

1. Improve the convergence speed and stability of training.
2. Generate more realistic images.
3. Maintain state of the art security.

5 Methodology

To address the problem mentioned in section 3, I'll be using the system architecture proposed in (Hu et al., 2018) with some modifications. This architecture is shown in Figure 2. I choose this system because it is more reliable architecture when it comes to recovery of message compared to (Zhang & Yang, 2019). This error of recovery can be further improved by adding some form of error recovery code like Reed-Solomon. If time permits I will also try to address this issue. However it is optional.

In addition to this I took into consideration, how much of an improvement could the change of GAN would have on the final result. This eliminates the system proposed in (Ke et al., 2017). The choice of infoGAN in (Ke et al., 2017) is crucial for overall working of the system.



(a) phase one: train the Generator

(b) phase two: train the Extractor

Figure 2: System architecture of the proposed research. Figure 2a Shows the training of the generator, and 2b shows the training of the extractor.

As depicted in Figure 2a before the communication between Alice and Bob starts Alice will train a generator. This generator is a GAN, which will try to generate the most realistic images it can come up with. After the generator is trained to its convergence. Alice will train the extractor by using the generator's output, and the error between recovered noise vector z' from the output of extractor and the initial noise vector z. This second phase is shown in Figure 2b. When this is done Alice will have both a generator and an extractor that act as encoder and decoder respectively. The extractor will be sent to Bob and steganographic communication can start between Alice and Bob.

According to (Cachin, 1998), if the relative entropy between probability distribution of cover image and probability distribution of stego image is less than ε the system is considered to be ε-secure. (Zhang & Yang, 2019) extended this method to generative steganography as follows.

Definition 5.1. ε-secure generative steganography: If the generated images have sufficiently similar probability distribution as that of the real dataset, the system is considered to be secure. This relation is shown in equation 5.

$$\mathcal{D}(P_{generated}, P_{real}) \leq \varepsilon \tag{5}$$

If $\varepsilon = 0$ then the system is said to be perfectly secure.

(Zhang & Yang, 2019) used the Jensen-Shannon divergence (D_{JS}) as the function $\mathcal{D}(\cdot)$. However, in my method I will not use DCGAN. So the usage of D_{JS} will not be feasible. Therefore I will have to come up with another metric to calculate this divergence, and this would be selected based on the choice of GAN.

The next important question that must be answered in my research is the choice of GAN. For this I am going to consider the following parameters.

1. Stability,
2. Convergence speed,
3. Quality of generated image
4. And most importantly how the divergence between the probability distributions is measured in the proposed GAN.

I am going to implement the proposed architecture with different GANs and test for the above mentioned parameters. Even though more research is going to be conducted in the coming months, the following GANs must be tested since they have good performance in terms of the above mentioned parameters.

- BEGAN (Berthelot, Schumm, & Metz, 2017)
- RGAN (Jolicoeur-Martineau, 2018)
- WGAN-DIV (J. Wu, Huang, Thoma, Acharya, & Van Gool, 2018)

- WGAN-GP (Gulrajani, Ahmed, Arjovsky, Dumoulin, & Courville, 2017)

In any machine learning research selecting the dataset for training is crucial. In my research I will consider the following point to guide me in the selection process.

1. Availability of the dataset.
2. Usage of the dataset in previous researches.
3. Feature richness and diversity

Based on this celebA (Z. Liu, Luo, Wang, & Tang, 2015) dataset has no competitor. It has 202,599 face images, with more than 40 binary attributes. In addition it has been used in (Zhang & Yang, 2019), (Hu et al., 2018) and (Ke et al., 2017). This dataset is available at `http://mmlab.ie.cuhk.edu.hk/projects/CelebA.html`. Some other datasets that are previously used in similar research include MNIST (Yann LeCun, n.d.), Food101 (Bossard, Guillaumin, & Van Gool, 2014), and LFW (Huang, Ramesh, Berg, & Learned-Miller, 2007). All of them are available freely.

Another important method that needs to be devised is a testing method for comparison. Testing for convergence speed and stability is straight forward. It can be interpreted from the error loss vs training epoch graph. However, measuring for image quality is somewhat a difficult challenge. In most papers (Jolicoeur-Martineau, 2019), (Arjovsky et al., 2017), (Gulrajani et al., 2017) visual inspection of image fidelity is used. (Y. Li, Xiao, & Ouyang, 2018) used inception score to measure the quality and diversity of the generated images. There are some other testing methods for image quality that might assist in this research. This include visual turing test (Geman, Geman, Hallonquist, & Younes, 2015) and MOS (mean opinion score) (Streijl, Winkler, & Hands, 2016). I will research more in to this methods and select meaningful methods for comparison.

6 Scope

This section clearly specifies what this research will focus on. The scope of this research is shown as follows.

- This research does not focus on robustness of generative steganographic frameworks. Robustness in this scenario is defined in section 1.1. Improving or analyzing robustness is outside of the scope of this research.
- In the classic paper (Simmons, 1984) the warden acts as an active adversary. He can change or modify the contents of the message to trick Alice and Bob. However in all of generative steganographic frameworks proposed till now passive adversary is assumed. (Hu et al., 2018), (Zhang & Yang, 2019), (Ke et al., 2017). This research will also assume passive adversary. In order to address the problem with active adversary, steganographic frameworks complemented with cryptographic frameworks would provide a good solution. Nonetheless, this would be an area for further study.
- Increasing payload capacity of generative steganography is outside the scope of this research. However payload capacity of the proposed framework in this research must be comparable with state of the art frameworks.
- Out of the three requirements of steganography shown in section 1.1 this research focus on Improving the first one, namely **Imperceptibility**.

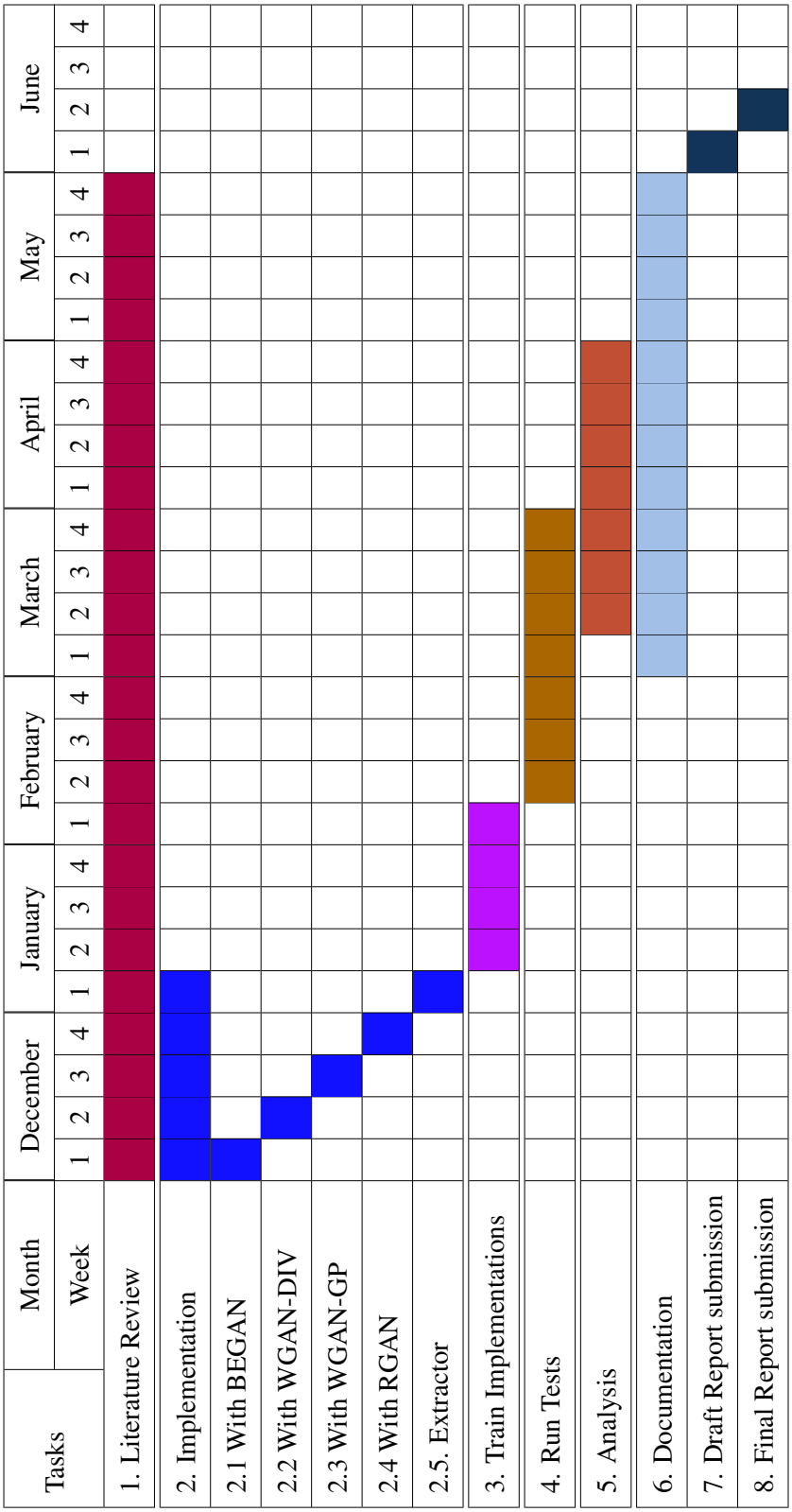
7 Significance Of The Study

Generative steganography from its conception has evolved a lot. Most recent studies focus on devising a novel plan rather than improving on previously proposed frameworks. However this research does not propose a novel framework to address the issues raised in the field. It aims at improving a previously proposed framework by utilizing recent advancements in the underlining technology, namely GAN.

This research will have a good influence in the field by addressing one of the main drawback of generative steganography that is a core concept of the field of steganography by itself, which is imperceptibility. This concept is described in 1.1. In short it describes the quality of steganography at hiding information in plain sight.

8 Work plan

Table 1: Work plan of the proposed research



9 Budget

The only budget requirement for this research is the cost of training machine. Since this research is being conducted in the field of deep learning, It requires the use of very high performance computers with GPUs. If the university have such computer in the lab, I will ask for permission to use it. However if I could not get my hand on such a machine at this university, I will use a cloud service. There are many cloud providers for machine learning research computers. Some of them are AWS E2 of amazon, and Google cloud which have fair price range. In total I will be spending less than 20,000 birr. If I could find a sponsor I will be glad to accept. Nevertheless, In the worst case scenario I will cover the cost by my self.

References

Abadi, M., & Andersen, D. G. (2016). Learning to protect communications with adversarial neural cryptography. *arXiv preprint arXiv:1610.06918*.

Arjovsky, M., Chintala, S., & Bottou, L. (2017). Wasserstein generative adversarial networks. In *International conference on machine learning* (pp. 214–223).

Bahi, J. M., Couchot, J.-F., & Guyeux, C. (2012). Steganography: a class of secure and robust algorithms. *The Computer Journal*, *55*(6), 653–666.

Berthelot, D., Schumm, T., & Metz, L. (2017). Began: Boundary equilibrium generative adversarial networks. *arXiv preprint arXiv:1703.10717*.

Bossard, L., Guillaumin, M., & Van Gool, L. (2014). Food-101 – mining discriminative components with random forests. In *European conference on computer vision.*

Cachin, C. (1998). An information-theoretic model for steganography. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1525*, 306–318. doi: 10.1007/3-540-49380-8_21

Chen, G., Zhang, M., Chen, J., Fu, D., & Wu, Y. (2012). Capacity and security for imperfect batch steganography. *Możliwości i bezpieczeństwo niedoskonałej steganografii pakietowej*, *88*(7), 324–327.

Chen, X., Duan, Y., Houthooft, R., Schulman, J., Sutskever, I., & Abbeel, P. (2016). Infogan: Interpretable representation learning by information maximizing generative adversarial nets. In *Advances in neural information processing systems* (pp. 2172–2180).

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

Geman, D., Geman, S., Hallonquist, N., & Younes, L. (2015). Visual turing test for computer vision systems. *Proceedings of the National Academy of Sciences*, *112*(12), 3618–3623.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... Bengio, Y. (2014). Generative adversarial nets. In *Advances in neural information processing systems* (pp. 2672–2680).

Gulrajani, I., Ahmed, F., Arjovsky, M., Dumoulin, V., & Courville, A. C. (2017). Improved training of wasserstein gans. In *Advances in neural information pro-*

cessing systems (pp. 5767–5777).

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

Huang, G. B., Ramesh, M., Berg, T., & Learned-Miller, E. (2007, October). *Labeled faces in the wild: A database for studying face recognition in unconstrained environments* (Tech. Rep. No. 07-49). University of Massachusetts, Amherst.

Jolicoeur-Martineau, A. (2018). The relativistic discriminator: a key element missing from standard gan. *arXiv preprint arXiv:1807.00734*.

Jolicoeur-Martineau, A. (2019). The relativistic discriminator: A key element missing from standard GaN. *7th International Conference on Learning Representations, ICLR 2019*.

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.

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des sciences militaires*, *9*, 161-191.

Li, C., Zhu, J., Welling, M., & Zhang, B. (2018). Graphical generative adversarial networks. *Advances in Neural Information Processing Systems*, *2018-Decem*(January), 6069–6080.

Li, Y., Xiao, N., & Ouyang, W. (2018). Improved boundary equilibrium generative adversarial networks. *IEEE Access*, *6*, 11342–11348. doi: 10.1109/ACCESS.2018.2804278

Liu, M. M., Zhang, M. Q., Liu, J., Gao, P. X., & Zhang, Y. N. (2018). Coverless Information Hiding Based on Generative Adversarial Networks. *Yingyong Kexue Xuebao/Journal of Applied Sciences*, *36*(2), 371–382. doi: 10.3969/j.issn.0255-8297.2018.02.015

Liu, Z., Luo, P., Wang, X., & Tang, X. (2015, December). Deep learning face attributes in the wild. In *Proceedings of international conference on computer vision (iccv).*

Otori, H., & Kuriyama, S. (2007). Data-embeddable texture synthesis. In *International*

symposium on smart graphics (pp. 146–157).

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).

Streijl, R. C., Winkler, S., & Hands, D. S. (2016). Mean opinion score (mos) revisited: methods and applications, limitations and alternatives. *Multimedia Systems*, *22*(2), 213–227.

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*.

Wu, J., Huang, Z., Thoma, J., Acharya, D., & Van Gool, L. (2018). Wasserstein divergence for gans. In *Proceedings of the european conference on computer vision (eccv)* (pp. 653–668).

Wu, K.-C., & Wang, C.-M. (2014). Steganography using reversible texture synthesis. *IEEE Transactions on Image Processing*, *24*(1), 130–139.

Yahya, A. (2018). Steganography techniques for digital images. *Steganography Techniques for Digital Images*, 1–122. doi: 10.1007/978-3-319-78597-4

Yann LeCun, C. J. B., Corinna Cortes. (n.d.). *The mnist database of handwritten digits.* Retrieved November 28, 2019, from `http://yann.lecun.com/exdb/mnist/`

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