
# Generator Adversarial Network (GAN)
# Enhancing Medical Vision, Exploiting Cyber Vulnerabilities

A Thesis Submitted in Partial Fulfillment for the Requirement of the
**Degree of BS** in Mathematics

By

**Ms. Rahila and Alina**

Supervised By

**Dr. Haider Ali**

**DEPARTMENT OF MATHEMATICS**
**UNIVERSITY OF PESHAWAR**
**December 2025**

## CERTIFICATE

We hereby declare that this thesis neither as an entire nor a segment of it has been copied out from any source. It is furthermore articulated that we have built up this proposition on the preface of my possess endeavors made beneath the genuine course of my supervisor. Not a part of the work displayed on this thesis has been submitted in help of some other degree or capability in any other University or Institute of learning, if observed we would stand stand mindful.

Signature:_____

Signature:_____

Name: Rahila and Alina

# Acknowledgement

This thesis would not have seen the light of the day without the expressible support and help of many individuals .

First of all, we are very thankfull to Almighty **Allah**, who gave us the strength and courage to carry out this fabulous work. Moreover he kept us motivated and healthy throughout this research.

We also would like to thank our respectable supervisor **Dr.Haider Ali** who supported me throughout this research, gave us his precious time, encouraged me whenever we were disappointed and helped us whenever we got stuck, and also Dr.Imran Khan who helped us in our thesis writing.

we were greatly helped by all the teachers at the department and we are equally thankful to them.

We express our deep gratitude to all those who, one way or the other, helped and supported our work.

**Rahila and Alina**

## 0.1 List of Abbreviation

The following abbreviations are used in this thesis:

- GAN : Generative Adversarial Network
- WGAN : Wasserstein Generative Adversarial Network
- DEF : Discriminator Ensemble Function.
- CD : Calibrated Discriminator.
- Langevin : Dynamics for Generator Sampling (MCMC).
- MH : Multi-Head, Sampling Acceptance Rate.
- MHLoss : Multi-Hinge Loss ,Function for Fine-Tuning.
- MCMC : Markvo Chain Monte Carlo (statistical technique)
- MHERGAN : Multi-Resolution Hierarchical Embedded Recurrent Generator Adversarial Network

# Abstract

This thesis explores the recent advancements in **Generative Adversarial Networks (GANs)**, which have become increasingly valuable in artificial intelligence applications, particularly in medical imaging, computer vision, and cybersecurity domains. These fields often face the challenge of limited data availability, as seen in drug discovery, target recognition, and malicious traffic detection, where collecting large-scale datasets is costly or impractical.

To address this issue, the study proposes a novel framework that combines GANs with Markov Chain Monte Carlo (MCMC) sampling and ensemble learning techniques. This integration aims to mitigate the bias and noise typically introduced by synthetic data, thereby improving data quality and model robustness. Additionally, the method incorporates an innovative loss function (MHLoss) and a reparameterized GAN ensemble, which collectively enhance training stability and accelerate model convergence.

The resulting algorithm, termed MhERGAN, demonstrates strong performance in classification tasks under small-sample conditions. Experimental results confirm that the proposed approach significantly improves model adaptability and generalization, offering a promising solution for data-scarce machine learning scenarios.

# Contents

# Chapter 1

# Introduction

In this chapter, we discuss **Generative Adversarial Networks (GANs)**—a class of deep learning models introduced by **Ian Goodfellow** in 2014—which have gained significant attention in recent years for their powerful generative capabilities.

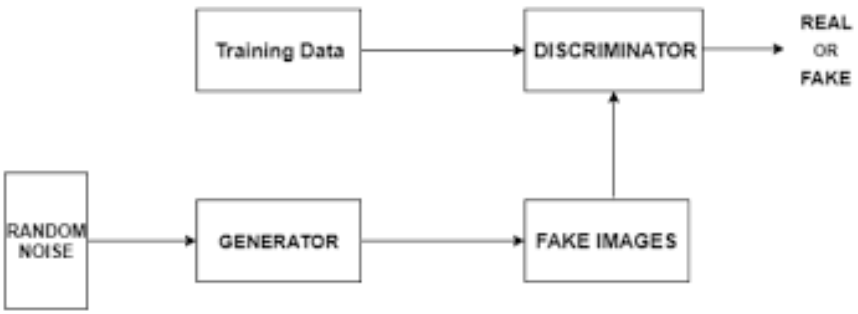
### 1.0.1 Generative Adversarial Network (GAN)

A GAN is a type of deep learning architecture comprised of two neural networks, a Generator and a Discriminator, that are trained in an adversarial manner.

1. The Generator learns to create synthetic data samples (e.g., images, text, audio) that resemble the real data.

2. The Discriminator learns to distinguish between real data samples and the fake data generated by the Generator.

Through this competitive process, both networks improve over time. The Generator becomes better at producing realistic fake data, while the Discriminator becomes better at identifying it. The ultimate goal is for the Generator to produce synthetic data that is indistinguishable from real data.



## 1.1 Background and Motivation

In many real-world scenarios—such as drug discovery, medical diagnostics, and cybersecurity—machine learning models face a critical challenge: the lack of sufficient labeled data. Traditional models typically require large datasets to perform well, making them unsuitable for domains where data is scarce, expensive, or sensitive.

Few-shot learning addresses this issue by enabling models to learn effectively from a limited number of samples. However, existing few-shot approaches often suffer from bias and instability, particularly when using data augmentation or fine-tuning with unrelated datasets.

To tackle these problems, this research proposes a novel framework that integrates GAN, MCMC sampling, and ensemble learning to generate high-quality synthetic data while maintaining model stability and accuracy. This combined approach helps bridge the gap between data scarcity and high-performing, generalizable models [1].

## 1.2 Research Problem

Despite the progress in few-shot learning, several key challenges remain:

1.Data Scarcity: Traditional machine learning models struggle with performance when only a few labeled samples are available.

2.Bias in data Augmentation: Synthetic data generated through common augmentation techniques often introduces noise and bias.

3.Dependency on related datasets: Model-based approaches like fine-tuning and metric learning typically require access to similar or related datasets, which may not always be available.

4.Instability in training: Few-shot learning models often suffer from unstable training and poor convergence, especially when working with small datasets.

This research aims to address these problems by developing a framework that combines generative modeling and optimization techniques to improve both the quality of synthetic data and the stability of model training.

## 1.3 Objectives

The main objectives of this research are:

1.We reviewed to few-shot learning performance in data-scarce environments.

2.We also reviewed that to reduce bias in synthetic data using a reparameterized

GAN ensemble with MCMC sampling.

3.We also seen to enhance model fine-tuning stability and convergence using the MHLoss strategy.

4.To develop a unified framework (MhERGAN) that integrates data augmentation and model optimization for better classification accuracy on small datasets [3].

## 1.4 Contributions

This research makes the following key contributions:

1.Proposes a novel reparameterized GAN ensemble to reduce bias in few-shot data generation.

2.Introduces MCMC sampling to correct the generator's distribution for more realistic synthetic data.

3.Applies discriminator ensemble learning to improve stability and reduce variance.

4.Enhances fine-tuning with a multi-head loss (MHLoss) strategy for faster convergence and better accuracy.

5.Develops the MhERGAN framework, which effectively improves classification performance in small-sample scenarios [7].

### 1.4.1 Few-Shot Learning Approaches

The thesis identifies three primary perspectives in few-shot learning:

1.Data-based methods: These approaches enhance the dataset to address the small-sample problem.

.Sample-level methods expand the quantity of data.

.Feature-level methods reduce the required sample size through feature selection and optimization.

2.Model-based methods: These methods tackle few-shot learning by designing models that can learn effectively from limited data.

.Model fine-tuning leverages knowledge from related domains.

.Metric learning learns suitable metrics for small-sample data.

3.Optimization algorithm-based methods: These methods modify the hypothesis

search approach to improve the probability of finding the optimal hypothesis.

.Meta-learning is a widely recognized optimization algorithm for few-shot learning. It trains a meta-learner across multiple tasks to enable the model to quickly learn new tasks.

We reviewed from this project that data-based methods may introduce noise or bias, while model-based and optimization algorithm-based methods often require related datasets. To address these issues, We are review from this research that the proposes a framework that combines data-based and model-based approaches [18].

### 1.4.2 Data Augmentation Techniques

, data augmentation is a critical component in tackling the challenges of few-shot learning, where the scarcity of data can hinder the performance of machine learning models. The authors identify two main categories within data augmentation:

.Sample-level methods: These techniques aim to increase the quantity of data.

.Feature-level methods: These techniques aim to reduce the required sample size by focusing on feature selection and optimization.

A significant challenge with data augmentation, as highlighted in the paper, is the potential introduction of noise or bias into the dataset. To mitigate this, the paper proposes a novel approach that integrates GANs with advanced optimization techniques. The authors' method employs MCMC sampling to correct the distribution learned by the generator and uses ensemble methods to constrain discriminator learning, effectively addressing the limitations of traditional data augmentation in few-shot learning scenarios [20].

### 1.4.3 Optimization Techniques in Few-Shot Learning

The project that we reviewed identifies optimization algorithm-based methods as a key perspective in few-shot learning. These methods aim to improve the probability of finding the optimal hypothesis by modifying the hypothesis search approach. Meta-learning is highlighted as a widely recognized optimization algorithm for few-shot learning. The core idea of meta-learning is to train a meta-learner across multiple tasks, enabling the model to quickly learn new tasks [12].

### 1.4.4 Summary of Gaps in Existing Research

we have to see from this work that we are represent in our thesis, identifies the following gaps in existing research:

.Data-based methods for few-shot learning, while intuitive, may introduce noise or bias into the dataset.

.Model-based methods and optimization algorithm-based methods often require additional related datasets, which may not always be available.

.Classical GANs suffer from issues such as biased distributions in both the generator and discriminator when dealing with few-shot data [4].

## 1.5 Literature Review

Few-shot learning is a challenging area in machine learning, particularly relevant to domains where data collection is difficult, such as drug discovery, medical health records, and malicious traffic detection (Altae-Tran et al., 2017; Fei et al., 2024; Wang et al., 2022). Traditional machine learning models heavily rely on large amounts of data, but their effectiveness is limited in scenarios with scarce data. Researchers have explored various strategies to address this issue, including data-based, model-based, and optimization algorithm-based approaches.

Data-based methods enhance datasets through sample-level and feature-level techniques (Liu et al., 2024). Sample-level methods increase the quantity of data, while feature-level methods reduce the required sample size through feature selection and optimization (Wei et al., 2024). However, a significant challenge with data-based methods is the potential introduction of noise or bias.

Model-based methods tackle the few-shot learning problem by designing models that can effectively learn from limited data. These methods include model fine-tuning and metric learning. Model fine-tuning leverages knowledge from related domains to improve few-shot learning performance, while metric learning aims to learn suitable metrics for small-sample data to uncover valuable information (Dong et al., 2024; Luo et al., 2024). However, these methods often require additional related datasets.

Optimization algorithm-based methods, particularly meta-learning, modify the hypothesis search approach to improve the likelihood of finding the optimal hypothesis. Meta-learning trains a meta-learner across multiple tasks to enable the model to quickly learn new tasks (Duan et al., 2024).

GAN have emerged as a powerful tool in machine learning for learning data distributions and generating new data (Goodfellow et al., 2020). A GAN comprises two neural networks: a generator and a discriminator. The generator learns to produce new data samples, while the discriminator distinguishes between real and generated samples. Through adversarial training, GANs can generate synthetic data that closely resembles real data. However, GANs can suffer from issues such as unstable training, slow convergence, and mode collapse. Wasserstein GANs (WGANs) were introduced to address some of these problems by improving distance metrics and adding weight constraints (Arjovsky et al., 2017).

This project addresses the limitations of both data-based and model-based approaches in few-shot learning. It proposes a novel framework that combines GAN-based data augmentation with model fine-tuning to extract more accurate information from limited samples [14].
We have seen about GAN intro , background , objective, review etc . Now let's proceed.

In next chapter we are discuss mathematical framework of this project

# Chapter 2

# Methodology

In this chapter, we examine the mathematical principles behind GANs. This includes an explanation of how GANs are structured, how they learn through adversarial training, and the key equations that define their behavior. Understanding these mathematical foundations is essential for analyzing how GANs generate data and how their performance can be improved.

## 2.1 Mathematical framework

Here is the mathematical framework used in this project:

We reviewed a reparameterization GAN method into few-shot learning. This approach uses MCMC sampling to correct the distribution learned by the generator, and ensemble methods to constrain discriminator learning and correct its learned distribution. The key elements of this framework are as follows:

### 2.1.1 Ensemble Discriminator:

.The ensemble discriminator is defined as:

$$D(x) = Com(D_1(x), D_2(x), ..., D_T(x)). \tag{2.1}$$

Where $(D_t(x))$represents each sub-discriminator, and the objective is to minimize the overall

### 2.1.2 Calibrated Discriminator

The calibrated discriminator is obtained by:

$$D_{cal} = cal(D). \tag{2.2}$$

Where $D_{cal}$ is the calibrated discriminator, and *cal* represents the calibration method. This calibration aims to make the discriminator's implicit distribution closer to the true distribution [6].

### 2.1.3 Generator Bias Correction with MCMC Sampling

The sample update method using the Langevin approach is given by:

$$z' = z_k - \frac{\tau}{2}\nabla_z \log(D_{cal}^{-1}(x_k) - 1) + \frac{\tau}{2}\nabla_z \log p_0(z_k) + \sqrt{\tau} \cdot \epsilon. \tag{2.3}$$

where:

- $z_k$ is the sample at the $k$-th state.
- $z'$ is the proposal sample.
- $\tau$ is the step size.
- $\epsilon$ is random noise.

The acceptance rate for the Metropolis-Hastings (MH) sampling is:

$$\alpha_{REP}(x', x_k) = \min\left(1, \frac{p_0(z')q(z|z')}{p_0(z_k)q(z|z_k)} \cdot \frac{D_{cal}^{-1}(x_k) - 1}{D_{cal}^{-1}(x') - 1}\right). \tag{2.4}$$

. where:

- $p_0$ denotes the prior distribution in latent space.
- $q$ denotes the proposal distribution.

## 2.2 Generative Adversarial Networks (GANs)

We have review GAN are employed as a key component in addressing the challenges of few-shot learning. GANs, introduced by Goodfellow et al. (2020), are a class of deep learning frameworks that learn data distributions and generate new data through a process of adversarial learning.

A GAN comprises two primary neural networks:

Generator (G): The generator network learns the underlying data distribution and generates synthetic data samples.

Discriminator (D): The discriminator network evaluates whether a given data sample is real (from the original dataset) or fake (generated by the generator).

The generator and discriminator are trained in an adversarial manner. The generator aims to produce synthetic data that is increasingly realistic, thereby "fooling" the discriminator. Simultaneously, the discriminator aims to improve its ability to accurately distinguish between real and fake data. This competitive process drives both networks to improve their performance, ultimately enabling the generator to generate data that closely resembles the real data distribution [8].

The mathematical formulation of the GAN objective function, as follows:

$$min_G max_D V(G,D) = E_{x\sim p_x}[\log D(x)] + E_{z\sim p_z}[\log(1 - D(G(z)))] = \int p_x \log D(x) dx. \tag{2.5}$$

Where:

$D(x)$ represents the probability that the discriminator classifies a real sample $(x)$ as real.

$D(G(z))$ represents the probability that the discriminator classifies a generated sample $(G(z))$ as real.

This adversarial dynamic enables GANs to effectively learn complex data distributions and generate new samples that exhibit characteristics similar to the training data.

## 2.3 Wasserstein GAN (WGAN)

Wasserstein GAN (WGAN):

The thesis explains that the original GAN model has several issues, including inadequate distance metrics for model training, slow convergence, and mode collapse. To address these problems, the Wasserstein GAN (WGAN) was introduced. WGAN improves upon the original GAN in three main ways:

.Removing the sigmoid layer.

.Replacing the Jensen-Shannon (JS) divergence with the Wasserstein distance.

.Adding weight smoothness constraints.

These modifications enable WGAN to provide more stable training and better performance compared to the original GAN [19].

## 2.4 Markov Chain Monte Carlo (MCMC) Sampling

The thesis utilizes Markov Chain Monte Carlo (MCMC) sampling to address the issue of generator bias in few-shot learning scenarios. MCMC methods are a class of algorithms used to sample from probability distributions based on constructing a Markov chain that has the desired distribution as its equilibrium distribution.

In this context, the authors employ MCMC sampling to correct the distribution learned by the generator network. The distribution learned by the discriminator is used as the target distribution for this correction, leveraging the fact that the discriminator's learned distribution is typically more accurate than the generator's, especially in few-shot settings.

To improve the efficiency and performance of the Markov chain construction, conditional proposal sampling is achieved by mapping the Markov chain to a latent space. The sample update method using the Langevin approach, a specific MCMC algorithm, is employed [11].

The sample update with the Langevin approach is given by:

$$z' = z_k - \frac{\tau}{2}\nabla_z \log(D_{cal}^{-1}(x_k) - 1) + \frac{\tau}{2}\nabla_z \log p_0(z_k) + \sqrt{\tau} \cdot \epsilon. \tag{2.6}$$

Where:

$(z_k)$ is the sample at the $k - th$ state.

$(z')$ is the proposal sample obtained through the Langevin method. $(\tau)$ is the step size.

$(\epsilon)$ is random noise.

The Metropolis-Hastings (MH) algorithm is then used to determine whether to accept the proposed sample (x'). The acceptance rate for the MH sampling is calculated as:

$$\alpha_{REP}(x', x_k) = \min\left(1, \frac{p_0(z')q(z|z')}{p_0(z_k)q(z|z_k)} \cdot \frac{D_{cal}^{-1}(x_k) - 1}{D_{cal}^{-1}(x') - 1}\right). \tag{2.7}$$

Where:

$(p_0)$ denotes the prior distribution in latent space.

$(q)$ denotes the proposal distribution.

Through this process, MCMC sampling enables the generation of a corrected dataset that better represents the true data distribution, ultimately improving the performance of few-shot learning models.

## 2.5 Ensemble Learning Methods

The thesis uses ensemble learning methods to address the issue of biased distributions learned by the discriminator in few-shot learning scenarios. Ensemble learning is employed to improve the discriminator's stability and reduce model bias.

Specifically, the authors apply the Bagging ensemble strategy to the discriminator. Bagging is a common ensemble method that can reduce variance and errors caused by sample fluctuations. By applying Bagging to the discriminator, the authors aim to correct its learned distribution, making it more robust and less susceptible to the noise inherent in small datasets [2].

The ensemble discriminator is defined as:

$$D(x) = Com(D_1(x), D_2(x), ..., D_T(x)). \tag{2.8}$$

Where:

$(D_t(x))$ represents each sub-discriminator.

The objective is to minimize the overall loss sum of all sub-discriminators.

## 2.6 Multi-Head Loss (MHLoss) Strategy

To enhance the stability of model fine-tuning on few-shot data, the paper introduces the Multi-Head Loss (MHLoss) strategy. This approach aims to accelerate model convergence by minimizing the overall loss across multiple models.

Specifically, for a given pre-trained classifier, multiple fine-tuning iterations yield several classification models. The MHLoss strategy then combines the outputs of these multiple models to obtain the final classification model. The loss function for fine-tuning classification models using MHLoss is defined as:

$$L_{MH} = \frac{1}{H}\sum_{h=1}^{H} L_h = -\frac{1}{H}\sum_{h=1}^{H} E_{x\sim p_x}[y \log(\theta_h^T x)] + \gamma |w_h|_2^2. \tag{2.9}$$

Where:

$(H)$ is the number of classifier heads.

$(\theta_h)$ represents the parameters of the $h-th$ classifier head.

$(\gamma)$ is a regularization parameter.

By minimizing the overall loss across these multiple models, MHLoss accelerates model convergence and improves fine-tuning stability.

## 2.7 Proposed Methodology

This thesis introduces a novel approach to enhance few-shot learning by integrating GAN-based data augmentation with model fine-tuning. The core idea is to address the limitations of traditional data augmentation and model-based methods when dealing with small sample sizes. The proposed methodology involves two key components [17]:

**Reparameterization GAN Ensemble:**

To mitigate the distribution bias in both the generator and discriminator, the authors propose a reparameterization of the GAN framework. This involves:

.An ensemble strategy is applied to the discriminator to improve its accuracy and reduce bias.

.MCMC sampling is employed to correct the distribution learned by the generator, bringing it closer to the true data distribution.

**Few-shot Data Model Fine-tuning:**

To enhance the stability and convergence speed of model fine-tuning, the paper incorporates increased iteration rounds and a Multi-Head Loss (MHLoss) fine-tuning strategy. This includes:

.Increasing iteration rounds to improve fine-tuning stability.

.Employing MHLoss to accelerate model convergence by minimizing the overall loss across multiple classification models generated during fine-tuning.

In summary, the proposed methodology combines GAN-based data augmentation with MCMC sampling and ensemble discriminative strategies, along with MHLoss for fine-tuning, to enhance few-shot learning [25].

### 2.7.1 Discriminator Bias Correction

The paper acknowledges that when dealing with small sample sizes, the distribution learned by the discriminator can often exhibit bias. To mitigate this issue, the authors propose applying an ensemble strategy to the discriminator. By using an ensemble of discriminators, the model's bias is reduced, and the discriminator's stability is improved.

The ensemble discriminator is defined as:

$$D(x) = Com(D_1(x), D_2(x), ..., D_T(x)). \tag{2.10}$$

Where:

$(D_t(x))$ represents each sub-discriminator.

.The objective is to minimize the overall loss sum of all sub-discriminators.

.Essentially, this approach combines the decisions of multiple discriminators to arrive at a more accurate and robust assessment of whether a sample is real or generated.

### 2.7.2 Fine-Tuning Strategy with MHLoss and Iterative Training

To enhance the stability of model fine-tuning on few-shot data, the paper employs two key strategies:

Increased Iteration Rounds: The authors suggest increasing the number of fine-tuning epochs to improve model stability [5].

**MHLoss:**

To accelerate model convergence, the Multi-Head Loss (MHLoss) strategy is utilized. MHLoss minimizes the overall loss across multiple models, effectively speeding up the convergence process and improving fine-tuning stability [13].

**By combining increased iteration rounds with the MHLoss fine-tuning strategy**

the thesis aims to achieve both enhanced fine-tuning stability and accelerated convergence, leading to improved classification performance on small-sample datasets.

## 2.8 Experimental Design

In this study, the authors designed experiments to evaluate the effectiveness of their proposed approach, MhERGAN, in enhancing few-shot learning. The experimental design can be summarized as follows:

**1.Dataset:**

The CIFAR-10 image dataset was used to validate the effectiveness of the reparameterized GAN ensemble method. A small-sample dataset was created by randomly sampling 5000 images from the original CIFAR-10 dataset.

**2.Implementation Details:**

.DCGAN was used as the base Generative Adversarial Network architecture.

.The ensemble strategy employed Bagging, with 5 sub-discriminators.

.Softmax was used to combine the outputs of the sub-discriminators.

**3.Evaluation Metrics:**

The Inception Score (IS) was used to measure the realism of the generated data. Additionally, the accuracy, precision, and F1 score were used to evaluate the performance of the MhERGAN algorithm in few-shot learning tasks [22].

**4.Comparative Analysis:**

The performance of the MhERGAN algorithm was compared against the hGAN algorithm under 2-way 30-shot and 2-way 2m-shot evaluation methods.

### 2.8.1 Dataset Description

The paper utilizes the CIFAR-10 image dataset to validate the effectiveness of the reparameterized GAN ensemble method. The CIFAR-10 dataset is a well-known dataset in computer vision, consisting of 60,000 32x32 color images in 10 classes, with 6,000 images per class. For the purpose of evaluating few-shot learning performance, the authors created a small-sample dataset by randomly sampling 5,000 images from the original CIFAR-10 dataset. This small-sample dataset was then used to train and test the proposed MhERGAN algorithm.

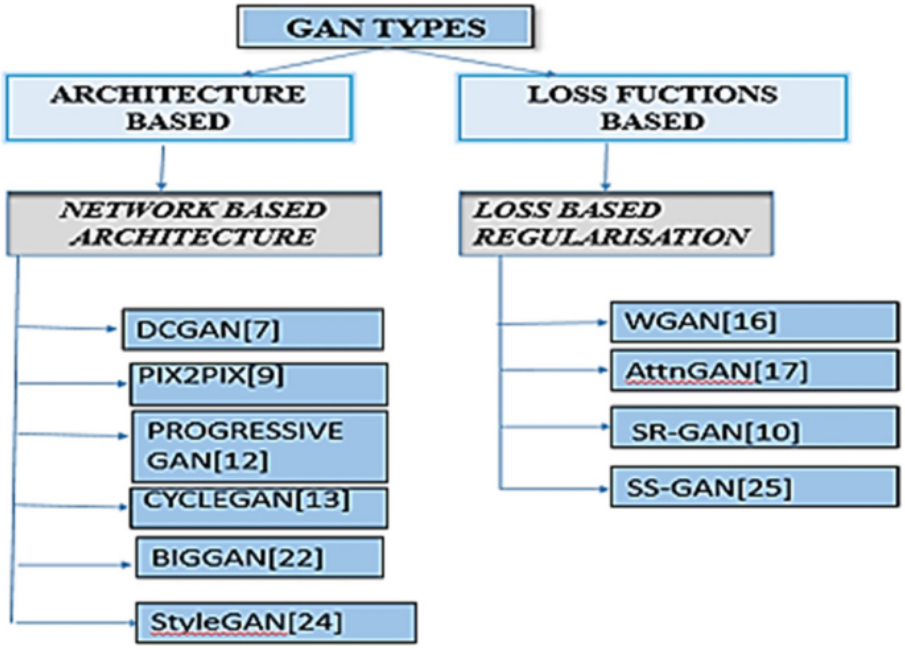
### 2.8.2 GAN Architecture and Settings

**.GAN Architecture:**

The paper adopts the DCGAN (Deep Convolutional Generative Adversarial Network) architecture as the base Generative Adversarial Network.

**.Ensemble Strategy:**

The ensemble strategy used for the discriminator is Bagging, with the number of sub-discriminators set to 5.




**.Combination Strategy:**

The outputs of the sub-discriminators are combined using Softmax.

### 2.8.3 Implementation of Ensemble and MCMC

**Ensemble Implementation:**

An ensemble strategy is applied to the discriminator to improve its stability and reduce bias.

.The Bagging ensemble method is used.

.The number of sub-discriminators in the ensemble is set to 5.

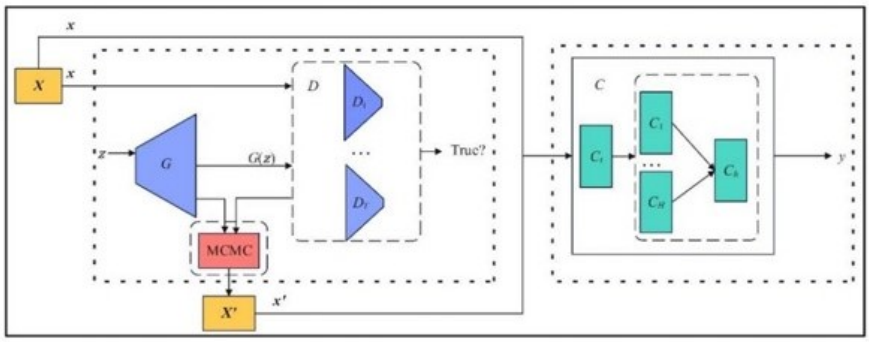
.The outputs of the sub-discriminators are combined using the softmax function.

.The objective of the ensemble discriminator is to minimize the overall loss of all sub-discriminators.

**MCMC Implementation:**

.MCMC sampling is employed to correct the bias in the generator's learned distribution.

.The distribution learned by the discriminator is used as the target distribution for the MCMC sampling.




.To improve the efficiency of Markov chain construction, conditional proposal sampling is performed in the latent space.

.The Langevin method is used to obtain the Markov chain in the latent space.

.The Metropolis-Hastings (MH) sampling method is used to determine whether to accept proposal samples.

.The acceptance rate for the MH sampling is calculated using a specific formula that involves the prior distribution in the latent space and the inverse of the calibrated discriminator's output.

.A relevant dataset is constructed using samples from the latter part of the Markov chain, and the implicit distribution of this dataset represents the corrected distribution of the generator [21].

Now we know more about GAN, that is, mathematical framework , architecture and many other things about GAN
We proceed in next chapter and discuss results ,comparison ,conclusion of GANs.

# Chapter 3

# Results and Analysis

In this chapter, we present and analyze the experimental results of the proposed GANs framework.

## 3.1 Performance of Reparameterized GAN Ensemble

In the reparameterized GAN ensemble experiment, the authors found that both MCMC sampling and the discriminative model ensemble strategy enhance the realism of the generated data. Notably, the ensemble strategy had a more significant impact on improving data realism. Combining both MCMC sampling and the discriminative model ensemble strategies resulted in the greatest improvement in data realism [24].

## 3.2 Comparison with Baseline Models (hGAN, SMOTE, ROS)

Here's a comparison of the MhERGAN model with the baseline models (hGAN, SMOTE, ROS) based on the information in the thesis:

**Comparison with hGAN:**

.MhERGAN outperforms hGAN on most datasets under the 2-way 30-shot evaluation method, demonstrating the effectiveness of MhERGAN.

.Even when MhERGAN's performance is slightly lower on some datasets, the decrease is minimal, indicating the algorithm's robustness and stability across varying sample sizes [16].

**Comparison with SMOTE and ROS:**

.Under the 2-way 30-shot evaluation, MhERGAN has higher average values for accuracy, precision, and F1 score compared to SMOTE.

.Results from 2-way 2m-shot evaluation are consistent with the 2-way 30-shot results, with MhERGAN outperforming both ROS and SMOTE on most datasets.

In summary, the MhERGAN algorithm demonstrates superior or comparable performance to the baseline models across different evaluation metrics and datasets, highlighting its effectiveness in few-shot learning scenarios.

## 3.3 Analysis under 2-Way 30-Shot and 2m-Shot Settings

**2-way 30-shot setting:**

The MhERGAN algorithm outperformed the hGAN algorithm on most datasets, demonstrating its effectiveness. This result highlights the advantages of the GAN bias correction and fine-tuning stability improvement strategies, particularly for small-sample data. While performance on two datasets showed a slight decline, the decrease was minimal, suggesting that even in cases where the MhERGAN algorithm does not improve performance, it does not cause significant degradation. This indicates the algorithm's robustness and stability, even when sample sizes vary [23].

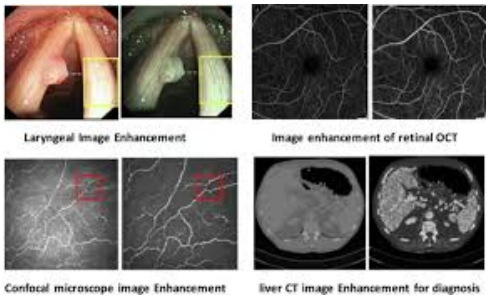
**2-way 2m-shot setting:**

The experimental results under 2-way 2m-shot are basically consistent with the 2-way 30-shot results. Under both evaluation methods, the MhERGAN algorithm outperforms the ROS and SMOTE algorithms on most datasets.

## 3.4 Discussion on Robustness and Generalization

We reviewed emphasizes the robustness and generalization capabilities of the MhERGAN algorithm in the context of few-shot learning. The authors highlight that the MhERGAN algorithm maintains stable performance across varying sample sizes, demonstrating its robustness. Even in scenarios where the algorithm does not lead to improved performance, it avoids significant performance degradation, further attesting to its stability.

Moreover, the MhERGAN algorithm exhibits good generalization performance. The experimental results demonstrate that MhERGAN outperforms the ROS and SMOTE



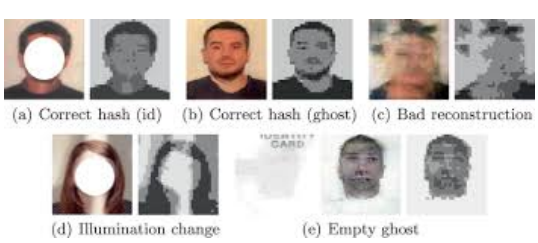

algorithms on most datasets under both 2-way 30-shot and 2-way 2m-shot evaluation methods. This consistency in performance across different evaluation settings indicates that MhERGAN can generalize well to unseen data.

## 3.5 Conclusion

This research significantly impacts the field of artificial intelligence by presenting a novel framework that addresses key limitations in data-scarce environments, pushing the boundaries of few-shot learning to be more effective and adaptable across various applications. By integrating GAN-based data augmentation with MCMC sampling and ensemble discriminative strategies, the proposed framework minimizes biases that typically hinder synthetic datasets, ensuring that generated data aligns closely with real-world distributions. This combination of generative models and fine-tuned discriminative approaches, further optimized through MHLoss and extended training iterations, creates a stable and rapid convergence, enhancing model robustness and accuracy. This advancement is transformative for the Al field, as it reduces dependency on extensive datasets while enabling high-performance models in complex, data-limited scenarios. The value of this framework is especially pronounced in critical fields such as drug discovery, defense, and cybersecurity, where data acquisition is often costly, restricted, or inherently limited due to confidentiality concerns. By achieving reliable results with minimal data, the MhERGAN algorithm empowers Al systems to perform accurately and adapt swiftly, ultimately expanding the scope of practical AI deployment in sensitive, high-impact domains. Through this integrated approach, the paper not only advances the technical frontier of few-shot learning but also demonstrates Al's potential to operate effectively in real-world, data-scarce environments, setting a foundation for more accessible and scalable Al applications in diverse fields where traditional data-heavy methods are impractical. This work, therefore, underscores a paradigm shift, proving that high-performing, generalizable Al systems are achievable even in settings with significant data constraints, thereby supporting broader and more innovative Al applications across industries [10].

### 3.5.1 Summary of Findings

Here's a summary of the key findings:





.The reparameterized GAN ensemble model enhances the realism of generated data by integrating MCMC sampling and discriminative model ensemble strategies.

.The MhERGAN algorithm demonstrates effectiveness in few-shot learning, outperforming the hGAN algorithm on most datasets.

.MhERGAN shows higher average values for accuracy, precision, and F1 score compared to the SMOTE algorithm in 2-way 30-shot evaluation.

.MhERGAN consistently outperforms ROS and SMOTE algorithms on most datasets in both 2-way 30-shot and 2-way 2m-shot evaluations.

.The GAN bias correction and fine-tuning stability improvement strategies are effective for small-sample data scenarios.

.MhERGAN exhibits robustness and stability across varying sample sizes.

### 3.5.2 Contributions to the Field

.Addresses the critical limitations of traditional machine learning models that require large datasets, particularly in fields with limited data availability, such as drug discovery, target recognition, and malicious traffic detection.

.Proposes a novel strategy that leverages GAN and advanced optimization techniques to improve model performance with limited data.

.Addresses the noise and bias issues introduced by data augmentation methods, contrasting them with model-based approaches that rely heavily on related datasets.

.Combines Markov Chain Monte Carlo (MCMC) sampling and discriminative model ensemble strategies within a GAN framework. This approach adjusts generative and discriminative distributions to simulate a broader range of relevant data.

.Employs MHLoss and a reparameterized GAN ensemble to enhance stability and accelerate convergence, leading to improved classification performance on small-sample images and structured datasets.

.Develops the MhERGAN algorithm, which is highly effective for few-shot learning, offering a practical solution that bridges data scarcity with high-performing model adaptability and generalization.

.Reduces dependency on extensive datasets while enabling high-performance models in complex, data-limited scenarios.

.Offers a solution for critical fields such as drug discovery, defense, and cybersecurity, where data acquisition is often costly, restricted, or inherently limited due to confidentiality concerns.

.Empowers AI systems to perform accurately and adapt swiftly with minimal data, expanding the scope of practical AI deployment in sensitive, high-impact domains.

.Demonstrates AI's potential to operate effectively in real-world, data-scarce environments, setting a foundation for more accessible and scalable AI applications in diverse fields where traditional data-heavy methods are impractical.

.Proves that high-performing, generalizable AI systems are achievable even in settings with significant data constraints [15].

### 3.5.3 Limitations

**Dependency on GANs:**

The approach relies on the performance of GAN, which can be notoriously difficult to train and optimize. GANs are known to suffer from issues like instability, mode collapse, and sensitivity to hyperparameter tuning.

**Computational Complexity:**

The integration of MCMC sampling and ensemble methods increases the computational cost of the model. MCMC sampling, in particular, can be computationally intensive, especially for high-dimensional data.

**Dataset Limitations:**

The experiments primarily use the CIFAR-10 dataset, which consists of relatively small and simple images. The effectiveness of the proposed method on more complex, high-resolution images or other data modalities (e.g., text, audio) is not thoroughly explored.

**Hyperparameter Sensitivity:**

The paper mentions the use of specific settings for the GAN architecture (DCGAN), ensemble strategy (Bagging with 5 sub-discriminators), and other parameters. However, it does not provide an extensive analysis of the sensitivity of the model's performance to these hyperparameters. The optimal values of these parameters may vary for different datasets and tasks.

**Limited Comparison with Other Few-Shot Learning Methods:**

While the paper compares the proposed MhERGAN algorithm with hGAN, SMOTE, and ROS, it does not include comparisons with other state-of-the-art few-shot learning methods. A more comprehensive comparison would provide a better understanding of the relative strengths and weaknesses of MhERGAN.

**Lack of Theoretical Analysis:**

While the paper provides empirical results to demonstrate the effectiveness of the proposed method, it lacks a strong theoretical analysis. A more rigorous theoretical foundation would help to better understand the properties of the MhERGAN algorithm and provide insights into its potential limitations.

### 3.5.4 Future Research Directions

Based on the limitations and conclusions presented in the paper, here are some potential future research directions:

**Explore More Stable GAN Architectures:**

Investigate the use of more advanced and stable GAN architectures, such as those based on Wasserstein GANs (WGANs) or other improved training techniques, to mitigate issues like instability and mode collapse.

**Reduce Computational Complexity:**

Develop methods to reduce the computational cost associated with MCMC sampling and ensemble methods. This could involve exploring more efficient sampling techniques or approximation methods.

**Evaluate on More Complex Datasets:**

Assess the performance of the proposed method on more complex and diverse datasets, including high-resolution images, text, and audio data, to validate its generalizability.

**Analyze Hyperparameter Sensitivity:**

Conduct a thorough analysis of the sensitivity of the model's performance to different hyperparameter settings to provide practical guidance for applying the method to new problems.

**Compare with More Few-Shot Learning Methods:**

Perform a more comprehensive comparison with other state-of-the-art few-shot learning methods to better understand the relative strengths and weaknesses of the proposed approach.

**Develop Theoretical Analysis:**

Develop a more rigorous theoretical foundation for the proposed method to provide insights into its properties and limitations [9].

**Apply to Real-World Applications:**

Explore the application of the proposed method to specific real-world problems, such as drug discovery, medical image analysis, and other areas where data is limited.

# Bibliography


[1] Han Altae-Tran, Bharath Ramsundar, Aneesh S Pappu, and Vijay Pande. Low data drug discovery with one-shot learning. *ACS central science*, 3(4):283–293, 2017.

[2] Martin Arjovsky, Soumith Chintala, and Léon Bottou. Wasserstein generative adversarial networks. In *International conference on machine learning*, pages 214–223. PMLR, 2017.

[3] Yiru Cang, Yihao Zhong, Rongwei Ji, Yingbin Liang, Yiming Lei, and Jinyin Wang. Leveraging deep learning techniques for enhanced analysis of medical textual data. In *2024 IEEE 2nd International Conference on Sensors, Electronics and Computer Engineering (ICSECE)*, pages 1259–1263. IEEE, 2024.

[4] Yuxin Dong, Shuo Wang, Hongye Zheng, Jiajing Chen, Zhenhong Zhang, and Chihang Wang. Advanced rag models with graph structures: Optimizing complex knowledge reasoning and text generation. In *2024 5th International Symposium on Computer Engineering and Intelligent Communications (ISCEIC)*, pages 626–630. IEEE, 2024.

[5] Shiyu Duan, Ziyi Wang, Shixiao Wang, Mengmeng Chen, and Runsheng Zhang. Emotion-aware interaction design in intelligent user interface using multi-modal deep learning. In *2024 5th International Symposium on Computer Engineering and Intelligent Communications (ISCEIC)*, pages 110–114. IEEE, 2024.

[6] Shiyu Duan, Runsheng Zhang, Mengmeng Chen, Ziyi Wang, and Shixiao Wang. Efficient and aesthetic ui design with a deep learning-based interface generation tree algorithm. *arXiv preprint arXiv:2410.17586*, 2024.

[7] Xinghui Fei, Sheng Chai, Weijie He, Lu Dai, Ruilin Xu, and Lianjin Cai. A systematic study on the privacy protection mechanism of natural language processing in medical health records. In *2024 IEEE 2nd International Conference on Sensors, Electronics and Computer Engineering (ICSECE)*, pages 1819–1824. IEEE, 2024.

[8] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial networks. *Communications of the ACM*, 63(11):139–144, 2020.

[9] Yufeng Li, Xu Yan, Mingxuan Xiao, Weimin Wang, and Fei Zhang. Investigation of creating accessibility linked data based on publicly available accessibility datasets. In *Proceedings of the 2023 13th International Conference on Communication and Network Security*, pages 77–81, 2023.

[10] Bingyao Liu, Iris Li, Jianhua Yao, Yuan Chen, Guanming Huang, and Jiajing Wang. Unveiling the potential of graph neural networks in sme credit risk assessment. In *2024 5th International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI)*, pages 562–566. IEEE, 2024.

[11] Shaobo Liu, Guiran Liu, Binrong Zhu, Yuanshuai Luo, Linxiao Wu, and Rui Wang. Balancing innovation and privacy: Data security strategies in natural language processing applications. In *2024 5th International Conference on Machine Learning and Computer Application (ICMLCA)*, pages 609–613. IEEE, 2024.

[12] Wenyi Liu, Rui Wang, Yuanshuai Luo, Jianjun Wei, Zihao Zhao, and Junming Huang. A recommendation model utilizing separation embedding and self-attention for feature mining. In *2024 3rd International Conference on Cloud Computing, Big Data Application and Software Engineering (CBASE)*, pages 295–299. IEEE, 2024.

[13] Jiahang Lu, Haruya Kyutoku, Keisuke Doman, Takahiro Komamizu, Yasutomo Kawanishi, Takatsugu Hirayama, and Ichiro Ide. A study on intra-modal constraint loss toward cross-modal recipe retrieval. *IEICE Technical Report; IEICE Tech. Rep.*, 2021.

[14] Yuanshuai Luo, Rui Wang, Yaxin Liang, Ankai Liang, and Wenyi Liu. Metric learning for tag recommendation: Tackling data sparsity and cold start issues. In *2024 5th International Symposium on Computer Engineering and Intelligent Communications (ISCEIC)*, pages 99–103. IEEE, 2024.

[15] J Ross Quinlan et al. Bagging, boosting, and c4. 5. In *Aaai/Iaai, vol. 1*, pages 725–730. Citeseer, 1996.

[16] Mengfang Sun, Wenying Sun, Ying Sun, Shaobo Liu, Mohan Jiang, and Zhen Xu. Applying hybrid graph neural networks to strengthen credit risk analysis. In *2024 3rd International Conference on Cloud Computing, Big Data Application and Software Engineering (CBASE)*, pages 373–377. IEEE, 2024.

[17] Chihang Wang, Yuxin Dong, Zhenhong Zhang, Ruotong Wang, Shuo Wang, and Jiajing Chen. Automated genre-aware article scoring and feedback using large language models. *arXiv preprint arXiv:2410.14165*, 2024.

[18] Zihao Wang, Kar Wai Fok, and Vrizlynn LL Thing. Machine learning for encrypted malicious traffic detection: Approaches, datasets and comparative study. *Computers & Security*, 113:102542, 2022.

[19] Jianjun Wei, Yue Liu, Xin Huang, Xin Zhang, Wenyi Liu, and Xu Yan. Self-supervised graph neural networks for enhanced feature extraction in heterogeneous information networks. In *2024 5th International Conference on Machine Learning and Computer Application (ICMLCA)*, pages 272–276. IEEE, 2024.

[20] Yijing Wei, Ke Xu, Jianhua Yao, Mengfang Sun, and Ying Sun. Financial risk analysis using integrated data and transformer-based deep learning. *Journal of Computer Science and Software Applications*, 4(7):1–8, 2024.

[21] Zhizhong Wu, Jiajing Chen, Lianghao Tan, Hao Gong, Yuru Zhou, and Ge Shi. A lightweight gan-based image fusion algorithm for visible and infrared images. In *2024 4th International Conference on Computer Science and Blockchain (CCSB)*, pages 466–470. IEEE, 2024.

[22] Ke Xu, You Wu, Haohao Xia, Ningjing Sang, and Bingxing Wang. Graph neural networks in financial markets: Modeling volatility and assessing value-at-risk. *Journal of Computer Technology and Software*, 1(2), 2022.

[23] Zhen Xu, Jingming Pan, Siyuan Han, Hongju Ouyang, Yuan Chen, and Mohan Jiang. Predicting liquidity coverage ratio with gated recurrent units: A deep learning model for risk management. In *2024 5th International Conference on Machine Learning and Computer Application (ICMLCA)*, pages 108–112. IEEE, 2024.

[24] Xu Yan, Weimin Wang, Mingxuan Xiao, Yufeng Li, and Min Gao. Survival prediction across diverse cancer types using neural networks. In *Proceedings of the 2024 7th International Conference on Machine Vision and Applications*, pages 134–138, 2024.

[25] Yun Zi, Xiaohan Cheng, Taiyuan Mei, Qi Wang, Zijun Gao, and Haowei Yang. Research on intelligent system of medical image recognition and disease diagnosis based on big data. In *2024 IEEE 2nd International Conference on Image Processing and Computer Applications (ICIPCA)*, pages 825–830. IEEE, 2024.