GENERATIVE AI FOR SIGNATURE SPOOFING

By

Haadia Amjad

MSCS-2K21: 00000364346

Supervisor

Dr. Muhammad Imran Malik

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Computer Science (MS CS)

In

School of Electrical Engineering & Computer Science (SEECS) ,

National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(August 2023)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Generative AI for Signature Spoofing " written by Haadia Amjad, (Registration No 00000364346), of SEECS has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Advisor: Dr. Muhammad Imran Malik

Date: 19-Sep-2023

HoD/Associate Dean: _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

Approval

It is certified that the contents and form of the thesis entitled "Generative AI for Signature Spoofing " submitted by Haadia Amjad have been found satisfactory for the requirement of the degree

Advisor : Dr. Muhammad Imran Malik

Signature: _____

Date: 19-Sep-2023

Committee Member 1: Dr. Muhammad Naseer Bajwa

Signature: _____

19-Sep-2023

Committee Member 2: Dr. Junaid Younas

Signature: _____

Date: 19-Sep-2023

Signature: _____

Date: 21-Sep-2023

Dedication

To my loving parents, as without their constant prayers, support and inspiration, this feat would have been impossible.

Certificate of Originality

I hereby declare that this submission titled "Generative AI for Signature Spoofing " is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name:Haadia Amjad

Student Signature: 

Acknowledgments

I am immensely grateful for the unyielding support of my beloved parents, sisters, and friends throughout my life. They have been the driving force behind my relentless pursuit of surpassing my own limitations. The profound impact of my supervisor, Dr Muhammad Imran Malik, during my master's thesis journey, is immeasurable, and his unwavering guidance and tireless efforts have been pivotal to my success.

I cannot overstate the profound influence of my mentors, the luminaries who have shaped my character and abilities - Dr. Momina Moetesum, Dr. Ghulam Ali Mirza, and Dr. Imran Ahmad Siddiqi. They have been instrumental in moulding me into the person I am today.

Lastly, I bow my head in eternal gratitude to Allah (S.W.A), whose divine blessings have graced my life with inexplicable miracles, guiding me through every triumph and challenge.

Haadia Amjad

Contents

List of Figures

List of Tables

Abstract

Biometric data reveals characteristics of human traits that are helpful for identification and verification purposes. A handwritten signature is a type of biometric data that is widely used for online and offline verification purposes. Tasks utilizing this data have been automated for various applications using Machine and Deep learning. Deep learning systems learn to recognise a person's original signature and forged signature to ultimately be able to classify an image as an original or forged signature. To make these systems stronger, more data is needed and better quality data is needed, i.e., the forgeries have to be skilled enough so they are tougher to classify. This made researchers turn to generative techniques to enable forgery generation to increase the amount of data used for verification tasks and also make higher-quality forgeries in the process. Among other generative techniques, Generative adversarial networks (GANs) learn from genuine and forged signatures to generate forged signatures. This technique creates a strong signature verifier which is basically the discriminator model of the GAN. However, work in this area neglects the fact that a forgery can not be too similar or dissimilar to the actual signature because that risks being rejected by real-life verification systems.

Our research focuses on creating a generator that produces such forged samples that achieve a benchmark in spoofing signature verification systems. We use CycleGANs infused with Inception model-like blocks with attention heads and the SigCNN model as a base Discriminator. We train our model with a new paradigm shifting technique. We evaluate the "goodness" of our forgeries by creating a generic evaluation metric that utilizes influential points of the distributions of original samples and forged target samples to determine the closeness of generated forged images to both data domains. Our model successfully surpasses state-of-the-art image generation architectures in spoofing signature verification systems.

Chapter 1

Introduction and Motivation

Biometrics are measurements of the body and computations of human traits. Machine learning techniques commonly employ biometric authentication as a method of access control and identification. It is also used to identify people or groups that have been under observation, serving as a means of surveillance. In order to be made use of, biometric data needs to be collectable for perusal and since it relates to human characteristics, it also needs to be unique and ever-lasting, not subject to change. A behavioural trait utilized in automatic user verification systems within the biometric structures is the signature. Signature is taken as a non-invasive and safer option by a number of users since it is a common part of everyday life [8]. The unique characteristics of an individual's signature can be used for identification or verification purposes.

Signature biometric data is typically captured using a digitizing tablet or other electronic device that records the pressure, speed, and trajectory of the signature. To collect handwritten signatures, research groups conduct focus groups or crowdsourcing events. This data is collected in the form of pairs, genuine and forged signatures [19]. This data is then stored in a digital format and can be used to verify the identity of the signer in the future. Signature biometrics and the collection of handwritten signatures are often used for research by various study groups. Signature biometrics can be easily captured and verified using electronic devices, making them a convenient and accessible form of biometric identification. Other types of biometric verification include both biological and behavioural, with biological encompassing face verification, fingerprint verification, iris and veins etc. While the behavioural set can include keystroke dynamics, gait, sig-

nature, voice etc. In the present day, technology is making use of both biological and behavioural data. The use of deep learning is rapidly increasing in areas where this kind of data can be utilized.

Deep learning methods have the ability to learn high-level features from raw biometric data, such as images or audio recordings. Deep learning usage allows the extraction of relevant information from biometric data, without the need for manual feature engineering. For this reason, it has become wildly popular to use deep learning based verification systems, introducing more accuracy and robustness [41]. Even with these strong verification systems, an attacker may be able to bypass the security check with skilled replications. One of the ways an attacker might bypass a biometric identity verification system is signature spoofing.

Signature spoofing involves creating a valid signature using encryption flaws, potentially leading to fraud. Signature forgery, a crime, includes various types like blind, unskilled trace-overs, and skilled replicas. Precise forgeries might be detected due to advanced verification algorithms analyzing subtle signature details. Such forgeries raise suspicion as they lack the natural variation and imperfections found in genuine signatures. Verification systems use techniques like analyzing stroke features to detect skilled forgeries attempting perfect replication.

Signature verification assesses whether a person's signature is authentic. To use signature biometrics for identification or verification purposes, the signature data is compared against a previously stored signature template. The comparison is typically done using pattern recognition algorithms that analyze the unique features of the signature, such as the shape of the letters, the spacing between the letters, and the overall rhythm and flow of the signature. Signature verification encompasses a number of techniques. First is the descriptive language which draws comparisons between the suspicious and a reference signature using hieroglyphic elements that represent all different kinds of signatures. Secondly, geometrical analysis is a common technique used in signature verification to compare the geometric properties of a signature with a known reference signature. This involves analyzing the shape, size, position, and orientation of various features of the

signature, such as the stroke endpoints, intersections, and inflection points. Thirdly, the analytical method is based on signature delineation and similarities between the components in each variation, making this approach useful in more complex scenarios [4]. This can include removing any noise or distortion from the signature image and to standardize the size and orientation of the image to prepare it for comparison. Then various features of the signature are extracted, such as the curvature. A classification algorithm is applied to determine whether a signature is genuine or forged. Apart from classification models, a generative model can also be used to distinguish between original and forged signatures by identifying underlying patterns and structures of data to reach the goal of generating similar data.

In generative modelling, the underlying distribution of a dataset is learned, and new samples that are comparable to the original data are produced. Generative modelling is probabilistic in nature because it involves modelling the probability distribution of the data and generating new samples from this distribution. In probabilistic modelling, the goal is to estimate the intrinsic probability distribution of the data, based on a set of observed data samples [73]. The probability distribution can then be used to generate new data samples that are similar to the observed data.

One of the most commonly used generative models is the Generative Adversarial Network (GANs). Generative adversarial networks (GANs) are a type of deep neural network that consists of two parts: a generator and a discriminator. The generator is designed to generate new samples of the original data, while the discriminator distinguishes between the original data and the generated data, In this way, they perform mutually adverse roles. The generator loss measures the efficiency of the generator, penalizing it for failing to fool the discriminator. Similarly, discriminator loss is when the discriminator fails to differentiate between the original and false data.

In the field of signature generation, Generative Adversarial Networks (GANs) have been widely explored and have shown promising results. Several papers have proposed GAN-based techniques for signature generation. One such study by Muhammed Mutlu Yapıcı et al. [80] presents the use of CycleGAN architecture for offline handwritten signature

generation with the goal of using it as a data augmentation technique. Chandra Sekhar Vorugunti et al. [104] propose an architecture called OSVGAN for online signature generation. The OSVGAN model consists of a novel variation of Auxiliary Classifier GANs. They switch the latent space to a set of Gaussian distributions. They also propose a Depth Wise Separable Convolution based Neural Network Architecture to classify test signatures. Jiajia Jiang et al. [91] introduce a stroke-aware cycle-consistent GAN architecture for signature verification. The GAN is trained to generate authentic-looking signatures while preserving the stroke-level details and characteristics. By incorporating stroke-level information, this technique enhances the authenticity and fidelity of generated signatures for robust signature verification.

In the above-mentioned research studies, we observe that the focus is on making the discriminator model a strong verifier rather than focusing on strong skilled forgeries. We also observe that the quality of the forgery generated by the model is not considered during evaluation. We introduce a generator-focused generative adversarial network that uses an underlying Inception block concept along with attention heads to produce signature forgeries that can effectively spoof a signature verification system. Additionally, we devise an evaluation metric based on influential data points to quantify the quality of the forgery.

1.1 Problem Statement and Contribution

1.1.1 Problem Statements

- Work on signature data using GANs has been focused towards better discriminators or data augmentation. The need for generator-focused research is created to focus on a better generation of forgeries.
- Since forgeries of a signature can not be too similar or dissimilar to the original sample, the generated images have to be near a certain percentage of closeness to the original image. This fact is not considered while using GANs for forgery generation and hence creates a research gap.
- Research work focusing on generated signatures or data, in general, does not mea-

sure the "goodness" of a forgery which questions the importance or usefulness of the generated data itself. This observation creates space for research towards appropriate evaluation metrics for this area.

1.1.2 Solution Statement and Research Contributions

- Develop a generator-focused generative adversarial network that uses an underlying Inception block concept along with attention heads to produce signature forgeries that can effectively spoof a signature verification system.
- The proposed model will be trained on a paradigm-shifting training theory that thrives to achieve closeness to genuine samples by learning from adversarial samples.
- Develop an evaluation metric based on influential data points to quantify the quality of the forgery.

1.1.3 Limitations

- The evaluation metric cannot be said to work on every type of generated data.
- The system would be assistive in signature verification and not act as one itself.

1.1.4 Thesis Layout

Chapter 2 lays down the foundation for the tools and techniques that have been deployed in this thesis by looking at their history, significance and contributions. The next chapter 3 looks at the research that has been carried out in this domain. The next two sections showcase the methodology that has been followed and the results obtained. Finally, chapter 6 discusses and concludes the thesis, along with the future directions that could be taken.

Chapter 2

Domain Concepts

In order to achieve the research contributions mentioned earlier, a number of technologies would be utilized to achieve a harmonious solution.

2.1 Forgery Creation

Signature spoofing is when a malicious party creates a legitimate signature by taking advantage of an encryption flaw in the setup of the signature verification mechanism. A person who signs in another person's name or modifies a document in order to conduct fraud or deceive others is guilty of the crime of signature forgery [11]. Signature forgeries can be of various types. They can be blind forgeries with no access to the original sign, or they can be trace-overs i.e. unskilled forgery, which is usually a trace over the original and lastly skilled forgeries, which are often replicas of the original and hard to tell apart from. However, if the forgeries are too accurate or near-perfect replicas of the original signature, they may be detected and denied by the verification system. This is because advanced signature verification algorithms can analyze minute details and patterns within a signature to determine its authenticity. When a forgery closely resembles the original signature, it raises suspicion due to the lack of natural variation and the absence of imperfections that are typically present in genuine signatures. The verification system may employ various techniques, such as analyzing the stroke endpoints, intersections, infliction points, and curvature, to detect subtle differences and identify skilled forgeries that aim to replicate the original signature perfectly [92].

2.2 Generative Adversarial Networks (GANs)

Generative Adversarial Networks (GANs) [10] have been used for generating forged signature images. This is typically done by training a GAN to generate images that resemble real signature images. The generator network in the GAN takes a random noise vector as input and generates a fake signature image as output. The discriminator network in the GAN tries to distinguish between real signature images and fake signature images generated by the generator.

Different types of GANs have different specifications, shown in table 2.1. In the vanilla GAN, also known as standard GAN, the generator records the distribution of data and in the meantime, the discriminator seeks to determine the likelihood that the input belongs to a particular class of data. A Conditional Generative Adversarial Network (CGAN) [12] is designed to generate data based on a specific condition or context. In a CGAN, both the generator and discriminator take in additional information as input, which is used to control the generation process. The additional information, or conditioning variable, could be any kind of auxiliary information such as class labels, textual descriptions, or even other images. By conditioning the generator on this additional information, the generator can be trained to generate data that is specific to the input condition. Deep Convolutional GAN (DCGAN) [15] uses convolutional neural networks (CNNs) as building blocks for both the generator and discriminator networks. The generator typically consists of a series of deconvolutional layers that gradually increase the spatial resolution of the generated image, followed by batch normalization and ReLU activation. The output layer usually uses a Tanh activation to generate pixel values between -1 and 1. The discriminator network in DCGAN is a CNN that takes as input either a real or fake image and outputs a probability indicating whether the input is real or fake. The discriminator typically consists of a series of convolutional layers, followed by batch normalization and LeakyReLU activation, and a final dense layer with sigmoid activation that outputs the probability. CycleGAN [26] is designed for image-to-image translation tasks, where the goal is to learn a mapping between two different image domains. StyleGAN [39] generates high-quality synthetic images that are both diverse and highly realistic. Making use of the Generative Adversarial Text Image Synthesis, GANs are able to identify a picture from the dataset that is most com-

parable to the text description and produce images that are comparable to it. Super Resolution Generative Adversarial Network (SRGAN) [21] is designed for the task of single-image super-resolution, which is the process of generating a high-resolution image from a low-resolution image. The generator network takes a low-resolution image as input and generates a high-resolution image as output, while the discriminator network tries to distinguish between real high-resolution images and fake high-resolution images generated by the generator. Wasserstein Generative Adversarial Networks (WGANs) [18] are a variant of GANs designed to improve training stability by using the Wasserstein distance as a measure of generator performance, enabling more robust and effective generation of high-quality data.

2.2.1 CycleGAN

CycleGAN is a groundbreaking deep learning model that has revolutionized the field of image-to-image translation. Introduced by Jun-Yan Zhu et al. [26] in their seminal paper "Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Networks" in 2017, CycleGAN has garnered widespread attention and acclaim for its ability to learn mappings between two distinct image domains without the need for paired training data. The model's core idea lies in the incorporation of cycle consistency, which enforces that the translation from one domain to another and back again should ideally yield the original input image. This ingenious concept enables CycleGAN to achieve impressive results in diverse applications, ranging from artistic style transfer to domain adaptation and image synthesis.

CycleGAN has become a formidable tool in various areas due to its versatility and robustness. One of its common applications lies in style transfer, where it can convert images from one artistic style to another, effectively turning landscapes into the style of a famous painter or transforming real-world scenes into the appearance of a specific artistic genre. Furthermore, CycleGAN has found extensive use in domain adaptation tasks, enabling image translation between different domains, such as transforming satellite images to the style of maps, thus assisting in understanding and interpreting geographical data. Moreover, CycleGAN has been applied in the domain of medical imaging, facilitating the generation of realistic images from different modalities and supporting improved diagnosis and treatment planning. Its ability to perform unpaired

image-to-image translation without requiring matched samples has made CycleGAN an indispensable tool in various domains, empowering researchers and practitioners to explore creative possibilities in image manipulation and synthesis without the burden of paired data [24].

2.3 Attention Head

The attention mechanism has emerged as a powerful concept in deep learning, enhancing the capabilities of neural networks by enabling them to focus on relevant information while processing vast amounts of data. Attention heads were first introduced in the seminal paper "Attention is All You Need" by Vaswani et al. [24] in 2017, which presented the Transformer model. Attention heads facilitate capturing long-range dependencies and relationships between different parts of the input data, allowing the model to selectively attend to specific regions and contextual information, thus significantly improving the performance of various natural language processing tasks. The Transformer's attention mechanism has since become a cornerstone in modern deep learning architectures, being extensively adopted in various domains, including language translation, sentiment analysis, question-answering systems, and text generation.

In recent years, attention heads have been increasingly applied in computer vision tasks [87], witnessing notable success in image recognition, segmentation, and object detection. By introducing self-attention mechanisms, models can effectively process images and detect crucial features regardless of their spatial distance, which has proven beneficial in handling complex and large-scale visual data. Attention heads have also made significant contributions in multi-modal learning, enabling the seamless fusion of information from different sources, such as images and text, leading to a more comprehensive and accurate understanding of cross-modal data. As the attention mechanism continues to evolve and find new applications, its adaptability and efficacy are driving advancements in artificial intelligence and shaping the future of deep learning research.

1. Scaled Dot-Product Attention:

   (a) This attention mechanism is widely used in Transformer models for natural language processing tasks.

   (b) It calculates the attention scores by taking the dot product between the query

and key vectors, scaled by the square root of the dimension of the key vectors.

(c) It is computationally efficient and allows the model to focus on relevant information while attending to long-range dependencies in the input sequence.

2. Multi-Head Attention:

(a) Introduced in the Transformer model, multi-head attention employs multiple sets of attention weights (heads) to learn diverse patterns and dependencies in the input data.

(b) Each head operates independently, capturing different aspects of the data, and the results are concatenated or linearly combined to obtain the final attention representation.

(c) It allows the model to focus on different information at different positions and enables a better representation of learning.

3. Self-Attention (or Intra-Attention):

(a) Self-attention mechanisms are used to model relationships between different elements within the same input sequence.

(b) It enables the model to attend to all positions in the sequence simultaneously, capturing both local and long-range dependencies effectively.

(c) Self-attention is particularly beneficial in natural language processing tasks, where the relationships between words in a sentence are crucial for understanding and translation.

4. Cross-Modal Attention:

(a) Cross-modal attention [71] is employed in multi-modal learning tasks, where information from different modalities, such as images and text, needs to be fused effectively.

(b) It allows the model to attend to relevant regions in one modality based on information from another modality, facilitating a better understanding and representation of cross-modal data.

5. Additive Attention:

(a) Additive attention [14] is an alternative form of attention mechanism that uses a learned alignment vector to calculate attention scores.

(b) It allows the model to learn a more complex relationship between the query and

These are just a few examples of attention mechanisms, and there are many other variants and adaptations used in different deep learning models to suit specific tasks and requirements. Attention mechanisms have become a crucial component in various architectures, enhancing the performance and interpretability of deep learning models across different domains.

GAN Type	Year	Application Areas	Advantages	Disadvantages
CGAN	2014	Image generation, feature extraction, object detection, image classification	Allows control over the type and characteristics of the generated images by conditioning on auxiliary information	Requires labelled data as input and may suffer from mode collapse or convergence issues
DCGAN	2015	Image-to-image translation, text-to-image synthesis, semantic-image-to-photo translation	Improves the stability and quality of GAN training by using convolutional layers, batch normalization, and specific activation functions	May still produce unrealistic or distorted images and lacks control over the output
StyleGAN	2018	Face generation, style transfer, image editing, image inpainting	Enables fine-grained control over the style of the generated images at different levels of detail and introduces noise as a source of variation	May produce artifacts or inconsistencies in some cases and requires large computational resources
SRGAN	2016	Image super-resolution, medical image enhancement, optical character recognition	Produces photo-realistic images with finer textures and details by using a perceptual loss function based on adversarial and content losses	May introduce unwanted artifacts or noise and requires high-quality training data
WGAN	2017	Image generation, image-to-image translation, video prediction, 3D object generation	Solves the problem of mode collapse and provides a meaningful loss function that correlates with the image quality	May require careful tuning of the hyperparameters and clipping of the weights
CycleGAN	2017	Unpaired image-to-image translation, season translation, object transfiguration, style transfer, generating photos from paintings	Enables image translation without paired examples by using a cycle consistency loss to preserve the content of the input image	May not perform well on geometric transformations or complex scenes and may introduce colour inconsistency or distortion

Table 2.1: GAN types, their applications, advantages and disadvantages.

Chapter 3

Literature Review

In this work, we aim to generate forgeries using a modified CycleGAN architecture that succeeds in failing the verification system to assist the ethical generation of forgeries and its research. To achieve this we study adversarial networks and GANs in biometrics, specifically signature generation, and signature verification systems built using learning techniques. We also extensively review datasets to select them for experimentation.

3.1 Adversarial Networks for Signature Generation

Handwritten signature verification is a challenging problem in the field of biometrics and several studies have been conducted to improve its performance. To strengthen verification systems, adversarial networks have been used to generate new forgeries to adversarially attack the system. In the research work of Huan Li et al. [70], a novel adversarial variation network (AVN) model is proposed that actively varies existing data and generates new data to mine effective features for better signature verification performance. The AVN model consists of three modules - extractor, discriminator, and variator - that work together in an adversarial way with a min-max loss function. The authors tested the proposed method on four challenging signature datasets of different languages and compared its performance with previous methods.

In another paper, authors Haoyang Li et al. [69] propose a new method for attacking a handwritten signature verification system using region-restricted adversarial perturbations. The authors begin by noting that many signature verification systems are

vulnerable to adversarial attacks, which can cause the system to misclassify genuine signatures as forgeries. To address this issue, the authors propose a new attack strategy that involves adding adversarial perturbations to specific regions of the signature while leaving other regions unchanged. The proposed method is designed to be a black-box attack meaning that it does not require knowledge of the inner workings of the target signature verification system. The authors evaluate their method on several benchmark datasets and show that it is effective in deceiving the signature verification system. The article concludes by highlighting the potential of the proposed method in improving the robustness of signature verification systems.

3.2 Generative Modeling in Biometrics

Adversarial attacks and defences are a major challenge in generative modelling, particularly in biometrics where the ability to generate realistic synthetic data can be exploited to create convincing forgeries or fool the verification systems. In the biometric domain, various research works show the use of generic modelling, some of which we have discussed in this subsection.

Burlina et al. [37] investigated the use of deep generative models for generating synthetic retinal images to aid in the diagnosis and management of age-related macular degeneration (AMD). The authors trained a deep generative model called the deep convolutional generative adversarial network (DCGAN) on a dataset of high-resolution retinal images. They then evaluated the model's ability to generate realistic synthetic images of AMD. The study found that the DCGAN was able to generate high-quality synthetic images of AMD that closely resembled real-world examples. The authors concluded that the use of deep generative models holds great promise for the generation of high-quality synthetic retinal images for clinical applications.

In recent years, privacy concerns surrounding biometric data have led to the development of privacy-preserving techniques for biometric data. Generative adversarial networks (GANs) can generate synthetic data that preserves the statistical properties of the original data while obscuring personally identifiable information. In the work of

Oleszkiewicz et al. [45], the authors propose a novel privacy-preserving technique called the Siamese Generative Adversarial Privatizer (SGAP) for biometric data. The proposed SGAP model is evaluated on two publicly available datasets, demonstrating its effectiveness in preserving the privacy of biometric data while maintaining the accuracy of the original data. The authors conclude that the proposed SGAP model can potentially be an effective privacy-preserving tool for biometric data.

In the domain of facial recognition, Bessinger et al. [36] proposed a generative model of worldwide facial appearance by training a conditional GAN on a dataset consisting of faces from over 100 countries. The authors used a multi-scale architecture and a novel feature-matching loss to generate high-quality facial images with diverse characteristics. The proposed model was shown to outperform state-of-the-art methods in terms of both quantitative metrics and visual quality. The authors concluded that their approach has the potential to be used in various applications such as virtual try-on and face recognition. Similarly, Tinsley et al. [75] in "This Face Does Not Exist...But It Might Be Yours" presented a method to generate realistic and unique face images using a StyleGAN2 architecture and a facial landmark-based encoding approach. The generated faces were evaluated through a user study and were found to have a high level of realism and uniqueness. The authors also demonstrated the potential for using the generated images for personalized visual content, such as virtual try-on applications.

In their study, Bamoriya et al. [84] propose a deep learning-based approach called DSB-GAN for generating synthetic biometric data. The DSB-GAN model utilizes a deep convolutional GAN architecture to generate realistic and diverse biometric data. The authors evaluate the proposed method on the publicly available FVC2002 and FVC2004 fingerprint databases and demonstrate that the generated synthetic data can be used to improve the performance of fingerprint recognition systems. Their results indicate that the proposed DSB-GAN model can effectively generate high-quality synthetic biometric data and has potential applications in various biometric recognition systems.

Given a little amount of training data, generative models excel at managing missing or irregular data. When compared to generative models, discriminative models are quick

to anticipate new data which leads to quicker categorization of new data. Ali et al. [83] proposed a hybrid method for keystroke biometric user identification in their recent paper. The proposed method combined the features of keystroke dynamics and physical biometrics to enhance the accuracy and security of user identification. The method was tested on a dataset consisting of 50 users typing the same five phrases three times each. The results showed that the proposed method achieved an accuracy of 99.4%, outperforming other existing methods.

We can look at the study conducted by Ugot et al. [79] which proposed a novel method for generating realistic fingerprint images using GANs. The authors demonstrated that their proposed method can generate high-quality synthetic fingerprints that are visually similar to real-world fingerprints and can be used for biometric verification with accuracy. The authors concluded that their proposed method has the potential to enhance the security of biometric systems by generating synthetic fingerprints for training and testing purposes. In another study, Wang et al. [35] proposed using a GAN for data augmentation in palmprint recognition. They showed that the proposed GAN-based approach significantly improves the performance of palmprint recognition systems, particularly in situations with limited training data. The study highlights the potential of GANs for enhancing the accuracy and robustness of biometric recognition systems and provides an effective solution for addressing the challenge of data scarcity in palmprint recognition. Overall, the study highlights the importance of exploring innovative data augmentation techniques in biometric recognition and the potential of GANs in this domain.

3.3 Signature Verification Systems Based on Machine Learning

Signature verification systems have been using machine learning for a long time. This saves the effort and time of the verification process and enables efficient results. Bibi et al. [52] present a comprehensive review of the state-of-the-art machine-learning techniques used for biometric signature authentication. They outline the different types of signatures and their characteristics, such as static, dynamic, and online signatures. The

authors discuss the challenges faced by the researchers in this area, such as intra-class and inter-class variability, imbalanced data, and spoof attacks. They also highlight the advancements in machine learning techniques, such as deep learning, transfer learning, and ensemble learning, and their applications in signature authentication.

Another focus of extensive research has been machine learning-based offline signature verification systems. In their systematic review, M. Muzaffar Hameed et al. [67] examine the current state-of-the-art in this field. They provide a comprehensive survey of various machine-learning techniques that have been employed for offline signature verification, including artificial neural networks, support vector machines, and deep learning-based methods. The authors analyze and compare the performance of different approaches on various benchmark datasets, highlighting the strengths and limitations of each method. The study by Zheng et al. [50] focused on utilizing RankSVM for offline signature verification. The proposed method achieved state-of-the-art performance on two benchmark datasets - GPDS-160 and GPDS-300. The results obtained by these studies demonstrate the effectiveness of deep learning techniques in handwritten signature verification and their potential to be used in real-world applications.

In their paper, Alghanam et al. [64] propose two models for online handwritten signature verification to enhance prediction accuracy and decrease equal error rate (EER). The first model is based on a neural network backpropagation classifier, which utilizes Hu seven values for preprocessing and Hu moment invariants for feature extraction. Mersa et al. [42] proposed a transfer learning method to extract features from Persian handwriting for offline signature verification. Their approach aimed to enhance the accuracy of signature verification systems by leveraging pre-trained models and adapting them to Persian script.

Some of the biometric techniques used for personal identification include signature identification and verification both. When analysing a person's signature, which is prone to intra- and inter-personal differences in handwriting style, it is possible to consider the signature to represent their own authentication. A detailed, systematic overview of methods for identifying and verifying offline and online signatures is provided in a study

by Kaur and Kumar [101]. Surveys pertaining to the two approaches—writer-dependent and writer-independent approaches—are provided in offline signature verification. Additionally, the collected research on feature extraction and classification methods applied to the process of signature identification and verification has also been included. This paper reports the findings of evaluating several signature identification and verification procedures using many databases that have been introduced in the literature. Chandra [54] proposed a machine learning-based approach for dynamic signature verification.

In recent years, signature verification competitions have been organized to evaluate the performance of different methods. The SVC-onGoing is one such competition, and it has been organized to evaluate the performance of signature verification algorithms on a large-scale dataset. The paper by Ruben Tolosana et al. [99] provides a detailed overview of the competition and its results. Offline and online datasets were evaluated and the results show that the top-performing algorithms achieve a high level of accuracy, and they outperform the state-of-the-art methods by a significant margin. The SVC-onGoing competition has provided a valuable benchmark for evaluating the performance of signature verification algorithms.

3.4 Signature Verification Systems Based on Statistical Modeling

Other than machine learning, signature verification systems also resort to core statistical concepts that evaluate different aspects of the signature verification process. In dynamic signature verification, the time functions of the signature are analyzed in addition to the static appearance of signatures. A study by Yahyatabar and Ghasemi [25] proposed a new method for signature verification using dynamic feature stability (DFS) experiment, which focuses on the most stable signature partitions that are difficult to forge. The authors used the radon transform to transform the rotation effect into a shift effect, which reduced the shift effect in both axes of the image. By implementing the DFS experiment on three Persian datasets, the authors discovered the most significant part of the signature trajectory in signature verification systems. The results showed that the proposed method achieved the least verification error. The authors structured

three separate verification subsystems by the efficacy of SFAs on decision making, which resulted from the DFS experiment. The performance of SFAs was evaluated, and the results showed the minimum error rate by using their usage. The RT technique solved the rotation problem, which is a known obstacle in signature verification systems. The CNN network used in the proposed method can reduce the shift effect through its feature location-independent nature.

In their study, Maergner et al. [31] propose a novel approach for offline signature verification by combining graph edit distance and triplet networks. Graph edit distance is utilized to measure the similarity between signature graphs which are constructed based on the time series data of the signature. Triplet networks are used to learn a feature representation that captures the unique characteristics of genuine signatures. The proposed method achieves promising results on three publicly available datasets demonstrating its effectiveness and potential for practical applications. The combination of graph edit distance and triplet networks provides a robust and accurate solution for offline signature verification which can be further improved with additional data and fine-tuning of the network parameters. Santos et al. [97] introduced a novel online handwritten signature verification technique based on network analysis. Their method focused on analyzing the dynamic characteristics of signatures to enhance the accuracy of verification systems. By employing network analysis, they aimed to capture the unique patterns and behavioural aspects of online signatures for reliable verification.

Manabu Okawa [59] proposed a new online signature verification method that utilizes single-template matching with time-series averaging and gradient boosting. The proposed method aims to capture the temporal dynamics of the signature by averaging a series of samples obtained from a single signature template. Additionally, the gradient boosting classifier is used to improve the accuracy of the verification system. The proposed method was tested on the SigComp 2011 dataset and achieved promising results with an equal error rate of 0.91%. These results demonstrate the effectiveness of the proposed method in online signature verification, which can potentially be used for various real-world applications such as e-commerce and security systems.

3.5 Signature Verification Systems Based on Deep Learning

Over the years, deep learning techniques have been successfully applied to the field of offline signature verification. In their study, Hafemann et al. [16] proposed a novel method for analyzing the features learned by deep convolutional neural networks (DCNNs) in offline signature verification tasks. The proposed method consists of a series of visualization and analysis techniques to gain insight into the important features learned by DCNNs. Experimental results on two publicly available datasets show that the proposed method is effective in understanding the learned features and can be used to improve the performance of the signature verification systems. In the context of handwritten signature verification, D. Tsourounis et al. [34] proposed a new approach based on deep sparse coding architecture. In this study, a novel method was introduced that exploited the capability of deep neural networks to learn relevant representations of handwritten signatures by minimizing a sparse coding objective function. The proposed method was tested on two publicly available datasets, MCYT-75 and GPDS-960, and demonstrated promising performance results, outperforming other state-of-the-art signature verification methods. Another paper by Arenas et al. [46] presented the implementation of a DAG-CNN for offline signature verification. By using this deep learning approach, the network was capable of classifying and authenticating the signatures of 3 users, achieving overall accuracies of 99.4% and 99.3%, respectively. The DAG-CNN allowed the network to learn different characteristics of the signatures and focus on certain sections and details to differentiate genuine from forged signatures.

In their paper, Saffar et al. [32] propose a method for accurate online signature verification that deals with the challenges of lacking sufficient training samples and the need for spatial change invariance. The proposed method builds a one-class classifier for each user based on discriminative features learned by a pre-trained sparse auto-encoder which is applied to represent the training and testing signatures. This approach leads to a self-taught learning method and a independent signature descriptor that models and classifies users' signatures using a one-class classifier. The experimental results indicate significant error reduction and accuracy enhancement on the SVC2004 and SUSIG datasets. In a study, Yilmaz and Ozturk [28] proposed a hybrid

user-independent/dependent offline signature verification technique using a two-channel convolutional neural network (CNN) for feature extraction and verification. The CNN is used to extract features, and the proposed technique achieved an equal error rate (EER) of 4.13% with a 200-dimensional representation. The sensitivity of the model to gray-level and binary images was also investigated, and the authors demonstrated that the availability of gray-level information in train and test data significantly reduced the EER. Thakare and Deshmukh [33] proposed an end-to-end approach for offline signature verification in 2018 which uses a combination of CNNs and Support Vector Machines (SVMs) to extract features and classify signatures. Jahandad et al. [47] proposed using GoogLeNet Inception-v1 and Inception-v3 CNN architectures to verify offline signatures. They demonstrated that the Inception-v3 model outperformed Inception-v1, achieving an accuracy of 99.07%. Calik et al. [38] proposed a large-scale signature recognition system using deep neural networks and feature embedding. They used a large-scale dataset and various deep neural networks to achieve high accuracy, with ResNet-50 outperforming the other models, achieving accuracy of 99.6%. The study by Mohapatra et al. [43] proposed an offline handwritten signature verification system based on a Convolutional Neural Network (CNN) architecture inspired by Inception V1. The proposed model achieved an accuracy of 98.70% on the Brazilian PUC-PR dataset. The proposed method achieved an accuracy of 96.7% on the IUST Persian Signature dataset. Hefny and Moustafa [55] proposed a signature verification method using Legendre Polynomial Coefficients to extract features which were then fed into a deep learning model. They achieved a high accuracy rate of 98.32% on the GPDS-300 dataset. Shariatmadari et al. [48] proposed a patch-based offline signature verification system using a one-class hierarchical deep learning model. Their proposed method achieved a high accuracy rate of 97.29% on the Brazilian PUC-PR dataset. Navid et al. [44] proposed a signature verification method using CNN and achieved an accuracy of 99.8% on the GPDS-300 dataset.

Lopes et al. [93] proposed a deep neural network-based model for offline handwritten signature verification that achieved a high accuracy rate. Jiang et al. [90] introduced the Deep soft-DTW (DsDTW) algorithm for local representation learning in dynamic signature verification which outperformed several state-of-the-art models. Naz et al. [94] fine-tuned a pre-trained deep neural network using transfer learning for signature verification. Hung et al. [89] used deep learning methods for offline handwritten signature

forgery verification. Longjam et al. [102] developed a multi-scripted writer-independent offline signature verification model based on convolutional neural networks. Gupta et al. [88] used transfer learning and data augmentation for signature verification. Tsourounis et al. [100] presented a knowledge transfer-based deep feature learning method for offline signature verification.

Sharma et al. [98] propose an automatic signature recognition system based on a fine-tuned inception V3 transfer learning (TL) model. The model was trained on the largest publicly available synthetic signature dataset and tested against six pre-trained TL convolutional neural network models. The proposed model outperformed all pre-trained models in terms of accuracy, precision, sensitivity, and F1-score, with accuracy reaching 88%. The study conducted by Rasheed and Alkababji [96] also proposes a CNN-based approach for signature verification which analyzes the performance of various feature detectors and descriptors. The CNN architecture was found to be effective in extracting features from input data and robust to changes in signature placement and metrics. The results showed that AGAST, FAST, and BRISK detection achieved the maximum number of detected key points, while STAR, AKAZE, and MSER achieved lesser numbers.

Ruiz et al. [61] developed an off-line signature verification method using compositional synthetic generation of signatures and Siamese Neural Networks. This method generates synthetic signatures by dividing an original signature into several components and recombining them to form new signatures. Espinosa-Leal et al. [65] utilized Extreme Learning Machines (ELM) for signature verification and demonstrated that the ELM model outperformed traditional machine learning algorithms. Bonde et al. [53] proposed an offline signature verification method using Convolutional Neural Network (CNN) which showed significant improvement over the traditional methods. Similarly, Ebrahim Parcham [72] and colleagues developed a novel Capsule Neural Network (CapsNet) based model named CBCapsNet for writer-independent offline signature verification. The proposed model can capture local and global features of a signature image by employing convolutional layers and capsule networks. On the other hand, R. Tolosana [77] and colleagues proposed DeepSign, an online signature verification model based on a deep neural network. The model can perform signature verification in real-time by taking advantage of the speed and accuracy of deep learning models. In addition, Yi-

wen Zhou [81] and colleagues proposed an improved combined feature-based method for handwritten signature verification.

In recent years, air signature recognition has gained attention due to its advantages over traditional signature recognition methods. In research, Behera et al. [27] propose a deep convolutional neural network-based sequential model for air signature recognition. The proposed model comprises three modules, namely signature segmentation, feature extraction, and classification. The signature segmentation module is used to isolate the signature from the background. The feature extraction module uses a deep CNN to extract features from the segmented signature, and the classification module is used to classify the signature. The proposed model was tested on a dataset of air signatures and achieved recognition accuracy of 94.9%, demonstrating its effectiveness for air signature recognition. In another study, Malik et al. [57] proposed a deep learning-based approach for in-air signature verification.

Online signature verification (OSV) has become a popular technique in various applications such as medical, e-commerce, and m-commerce to legally bind the user. However, high-speed systems demand faster writer verification with limited information, low training and storage costs. Vorugunti et al. [62] propose a DeepFuseOSV framework that combines a hybrid architecture of depth-wise separable convolution neural network (DWSCNN) and long short-term memory (LSTM) network for online signature verification (OSV). The proposed framework also uses a feature fusion technique that fuses traditional statistical-based features with deep representations from a convolutional auto-encoder. Alajrami et al. [51] proposed a deep learning-based model for signature verification. Similarly, Jivesh Poddar et al. [60] proposed an offline signature recognition and forgery detection method using deep learning. Moreover, Kao and Wen [56] proposed an offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach. Hanmandlu et al. [29] proposed a deep learning-based offline signature verification system in 2018, which employs a combination of Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to learn signature features and classify genuine and forged signatures.

Biometric signature verification is also an important topic in the field of document analysis and recognition. In recent years, recurrent neural networks (RNNs) have emerged as a powerful tool for modelling sequential data in capturing the temporal dynamics of online signature data, making them an attractive option for signature verification. In their paper, Tolosana et al. [23] propose a novel approach for signature verification using RNNs which can capture the temporal dynamics of the signature. The proposed method is evaluated on the SigComp2011 dataset and achieves state-of-the-art performance. The results show that RNNs are a promising approach for signature verification and can outperform traditional methods such as support vector machines and hidden Markov models. The authors suggest that the use of RNNs in signature verification could lead to new opportunities for developing more accurate and efficient signature verification systems.

Lai et al. [20] proposed a novel method for online signature verification that combined RNNs and Length-Normalized Path Signature Descriptors (LNPSDs). The proposed method achieved a high accuracy rate of 97.5% on the GPDS dataset and outperformed previous state-of-the-art methods. The results indicate the effectiveness of combining RNNs and LNPSDs in online signature verification, demonstrating the potential of this approach for practical applications. Nathwani [58] proposed an online signature verification system using Bidirectional Recurrent Neural Network (BRNN), which achieved high accuracy in real-time signature verification. C. Li et al. [40] presented a stroke-based recurrent neural network (RNN) model for writer-independent online signature verification, which takes into account the temporal evolution of signature strokes. The model was evaluated on the GPDS-300 dataset, and achieved an accuracy of 94.29%, outperforming several state-of-the-art methods. The authors also tested the model on a cross-domain signature dataset and demonstrated its effectiveness in writer-independent scenarios.

Rajib Ghosh [66] presented a Recurrent Neural Network (RNN) based model that can handle varying-length signature inputs and produce reliable verification results. The model utilizes a stacked RNN architecture that can extract temporal information and learn complex signature features from the input image. Singh and Viriri [63] proposed an online signature verification method using deep descriptors. Lai and Jin [30] pro-

posed a Recurrent Adaptation Network (RAN) model for online signature verification in 2019, which uses a sequence-to-sequence structure to learn the temporal information of signatures.

These studies demonstrate the effectiveness of deep learning-based methods in signature verification. However, there is still room for improvement in terms of accuracy, robustness, and generalization. Future research could focus on developing more sophisticated deep learning models and exploring new types of data augmentation techniques to further enhance the performance of signature verification systems

3.6 Generative Adversarial Networks for Signature Spoofing

Signature spoofing aims to fail verification systems in their task of classifying genuine and forged signatures by passing high-quality skilled forgeries that get mistaken for original signatures. Some work has been done to achieve this task using GANs.

Zhang et al. [17] proposed a multi-phase system for offline signature verification using deep convolutional generative adversarial networks (DCGANs). The authors extracted local and global features from signature images using a pre-trained convolutional neural network (CNN) and used a DCGAN to generate multiple plausible variants of the signature. They combined the extracted features from the original signature image with the features extracted from the generated variants and used them for signature verification with an SVM classifier. The authors evaluated the proposed system on two publicly available signature datasets and achieved state-of-the-art performance with an equal error rate (EER) of 2.25% and 3.06% respectively. The proposed system generates diverse signature variants and improves the performance of signature verification systems, demonstrating the effectiveness of the proposed multi-phase system in offline signature verification using DCGANs and multi-phase feature extraction.

Traditional methods of image recognition face challenges such as feature selection, lack

of standardization, and low accuracy. A study by Wang and Jia [49] proposes a special network called SIGAN (Signature Identification GAN) based on the idea of dual learning. The trained discriminator of SIGAN is used to determine the authenticity of test handwritten signatures with the loss value of the trained discriminator serving as the identification threshold. The experimental dataset used in this study consists of five hard pen-type signatures including both genuine and deliberate imitations. The experimental results show that the average accuracy of the SIGAN-based signature identification model is 91.2%, which is 3.6% higher than that of traditional image classification methods. This study shows the effectiveness of the proposed approach in enhancing signature verification performance and highlights the potential for GAN-based methods in improving the accuracy of biometric identification.

Online Signature Verification (OSV) is an important task in the field of biometrics, which is challenging due to data scarcity and intra-writer variations. In their research work, Vorugunti et al. [104] propose a novel OSV framework that addresses these challenges using two methods. Firstly, to address the issue of data scarcity, they generate writer-specific synthetic signatures using Auxiliary Classifier GAN (AC-GAN), trained with a maximum of 40 signature samples per user. Secondly, to achieve a one-shot OSV with reduced parameters, they propose a Depth wise Separable Convolution-based Neural Network. The authors evaluate their proposed framework on two widely used datasets, SVC and MOBISIG, and demonstrate its state-of-the-art performance in almost all categories of experimentation. The proposed framework shows competence for real-time deployment in limited data applications. This work is the first attempt to generate virtually unlimited synthetic signature samples per user from a maximum of 40 signatures per user based on a modified version of AC-GAN. The authors' future work will focus on enhancing the generative skills of GANs and filling the missing and noisy parts of the signatures.

Jiajia Jiang et al. [91] presented a novel signature verification approach using a stroke-aware cycle-consistent generative adversarial network (SACGAN). This method synthesizes fake signatures with different styles and variations to augment the training data and improve the system's generalization performance. The proposed SACGAN model is stroke-aware, meaning that it generates fake signatures with similar strokes and

structures as genuine ones. Experiments conducted on benchmark datasets, including GPDS-960 and CEDAR-Signature, show that the proposed method outperforms state-of-the-art approaches in terms of accuracy, robustness, and forgery detection. Similarly, Yapıcı et al. [80] proposed a deep learning-based data augmentation method to generate synthetic signatures for improving the offline handwritten signature verification system. The proposed method uses a GAN-based data augmentation approach to create additional synthetic samples that are diverse, realistic, and representative of the signature dataset. Experimental results show that the proposed method improves the verification performance of the system, demonstrating the effectiveness of GAN-based data augmentation in improving signature verification accuracy.

Since GANs have gained immense popularity in the field of computer vision for their ability to generate realistic images, Fazle Rabbi et al. [95] investigated the application of conditional GANs for generating fake images of handwritten signatures. They implemented a GAN model that can generate fake signatures by taking in a condition vector tailored by humans. The results showed that the proposed model is effective in generating realistic fake signatures. Jordan Bird [85] explored how robots and generative approaches can be used for adversarial attacks on signature verification systems. They trained a convolutional neural network for signature verification and then used two robots to forge signatures to test the system's security. The results showed that the robots and conditional GAN were able to fool the system to a significant extent, but fine-tuning the model and transfer learning with robotic and generative data reduced the attack success rate to below the model threshold. These findings indicate that while GANs and robots can be used for adversarial attacks on signature verification systems, there is still scope for improving the model's robustness and security against such attacks.

3.7 Signature Dataset

There are many datasets that are used for signature verification. These datasets contain a certain number of original signatures and a certain number of forgeries of the same user, as shown in table 3.1. The total images in the dataset then amount to the number of users into the sum of original and forged signatures. For the purpose of our research,

we have considered only English-based signatures and datasets that had no or so little portion of synthetic images that it can be ignored.

The CEDAR Signature dataset [6] consists of 2640 signatures comprising 24 genuine signatures and 24 forged signatures. It involves a total of 55 individuals with each person providing 48 signatures. The dataset was created in the year 2007 and is primarily used for handwritten signature verification tasks.

The s ICDAR 2021, SVC2021, [78] contains a total of 2856 signatures. Among these 8 signatures are genuine while 16 signatures are forged for each of the 119 individuals who participated in the data collection. It was released in the year 2021 and serves as a valuable resource for research and development in the field of signature verification.

SUSIG [7] is another notable dataset specifically designed for signature analysis. It consists of 3000 genuine signatures and 2000 forged signatures. The dataset involves 100 individuals, each with multiple sets of forged signatures. SUSIG was created in 2009 and has been widely used for evaluating signature verification systems and studying forgery detection techniques.

The MCYT-100 [103] dataset comprises a total of 2250 signatures, including 15 genuine signatures and 15 forged signatures. It involves 75 individuals, with each person providing 30 signatures. The dataset was created in 2003 and has since served as a benchmark for evaluating signature recognition algorithms and systems.

DeepSignDB [76] is a large-scale signature dataset containing 62244 signatures. It involves 1526 users, making it a diverse and extensive resource for signature analysis and verification tasks. DeepSignDB was introduced in 2021 and has contributed significantly to the advancement of research in the field of signature recognition and verification.

The GPDS 960 [5] dataset encompasses a total of 47574 signatures. Out of these, 24 signatures are genuine, while 30 signatures are forged. The dataset involves 960 individuals, with each person contributing 54 signatures. GPDS 960 was created in 2015 and

has been widely used for benchmarking and evaluating signature verification algorithms and systems.

After observing that the CEDAR signature dataset is more widely used than others, we decided to select it for our work as well. This decision was also based on the availability of limited computation resources.

Name	**Quantity**	**Other Specifications**	**Year**
CEDAR Signature	1320 = 24 (org) + 24 (forg)	55 individuals, 48 sigs each	2007
ICDAR 2021 (SVC2021)	2856 = 8 (org) + 16 (forg)	119 individuals	2021
SUSIG	3000 (org) + 2000 (forg)	100 individuals, multiple sets of forgeries	2009
MCYT - 100	2250 = 15 (org) + 15 (forg)	75 individuals, 30 sigs each.	2003
DeepSignDB	62244	1526 users	2021
GPDS 960	47574 = 24 (org) + 30 (forg)	960 individuals, 54 sigs each.	2015

Table 3.1: Signature Datasets

Chapter 4

Design and Methodology

The literature described in 3 demonstrated the effectiveness of CycleGAN for image translation and generation. Thus we aimed to modify the base architecture of Cyclegan to generate forgeries that emphasize underlying human biometric traits with attention mechanisms.

The walkthrough of this chapter is as follows. The first half of the section describes the dataset, as well as the preprocessing that would be required. The remaining section discusses the modelling that was carried out, along with relevant figures to ensure a deeper understanding of the context.

4.1 Dataset and Preprocessing

4.1.1 The Dataset

As mentioned in the previous section, we have worked with CEDAR handwritten signature dataset. This decision was made due to the popular use of the dataset and our limited GPU resources for this research. CEDAR handwritten signature dataset comprises a total of 2640 images where the total number of genuine signatures is 1320 and the same number of skilled forgeries. For usage, the dataset is treated according to the number of users which is 55. This means that during training or evaluation, the genuine or forged signatures of each individual user is considered against themselves and not as a whole.

4.1.2 Data Preprocessing

Our preprocessing component takes inspiration from the work of Akhundjanov and Starovoitov [82]. In their work, they have specifically designed a preprocessing pipeline for the CEDAR signature dataset which we have translated into our work as shown in figure 4.1. We achieve the preprocessing pipeline by using Python libraries Numpy, Sklearn, Natsort, Scipy, Glob and CV2. The preprocessing component consists of 6 steps:

Stage 1: Digitize the Pixels Per Inch (PPI)

By determining the PPI, the resolution of the signature image is standardized, allowing for consistent analysis and comparison across different signatures. This digitization process ensures that signatures with varying image qualities and resolutions can be handled uniformly, laying the foundation for subsequent pre-processing steps.

Stage 2: Convert original PPI to grayscale signature image

To facilitate further analysis and processing, the original PPI of the handwritten signature image is converted into a grayscale representation. This conversion eliminates colour information while retaining the essential features of the signature. By converting to grayscale, the subsequent pre-processing techniques can be applied more effectively, enabling enhanced recognition accuracy and reducing the impact of colour variations on the final result.

Stage 3: Convert signature into Band interleaved by pixel (BIP)

TThe BIP format reorganizes the signature data by interleaving the pixels, allowing for efficient data manipulation and processing. This format simplifies subsequent analysis steps, such as segmentation and feature extraction, enabling improved recognition performance. By transforming the signature into BIP, the paper demonstrates the advantages of optimized data organization in the pre-processing stage.

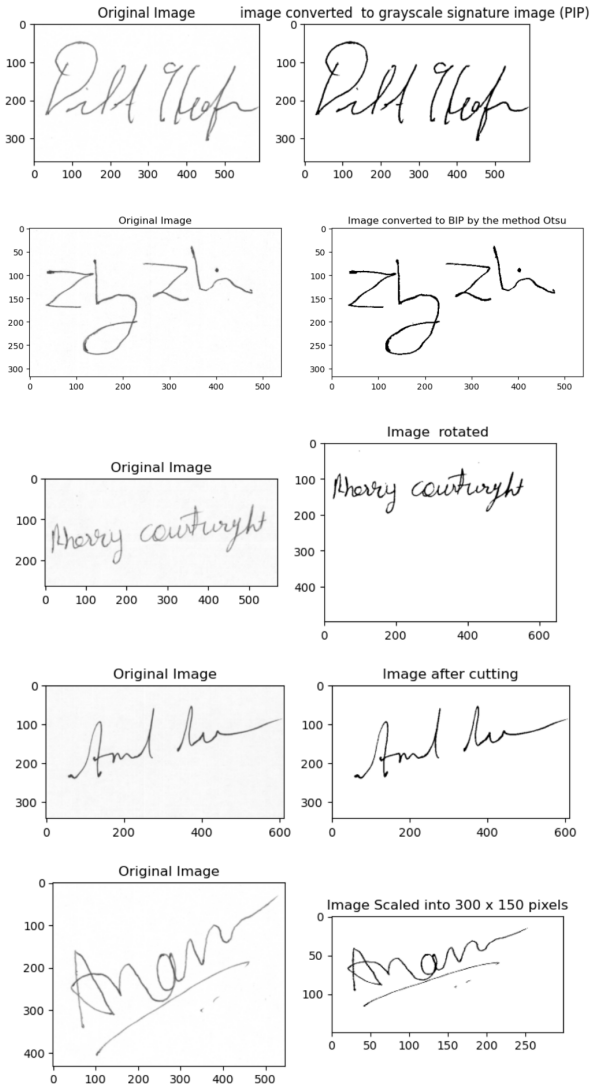

Figure 4.1: Plot of steps from our preprocessing component. 1) Grayscaling and PIP conversion 2) BIP and Otsu binarization 3) Image Rotation (straightening with PCA) 4) Binarization 5x5 cutting 5) Scaling

Stage 4: Cut out a rectangle over BIP (Otsu binarization 5x5 over BIP)

In order to isolate the signature from the background and improve segmentation accuracy, a rectangle is cut out over the Band interleaved by pixel (BIP) representation. The Otsu binarization technique [3] with a 5x5 kernel is employed to determine the optimal threshold for binarizing the signature. By applying Otsu binarization, the signature is separated from the background, creating a binary representation that facilitates subsequent processing steps, such as feature extraction and recognition algorithms. This step effectively removes unwanted information and noise, further enhancing the quality of the pre-processed signature image.

Stage 5: PCA method for rotation

By applying PCA, the signature is analyzed in terms of its principal components, enabling the detection and correction of rotation. This technique ensures that the signatures are aligned properly, contributing to more accurate recognition results.

Stage 6: Scale to 300x150 px

This scaling process ensures uniformity across different signatures and enables compatibility with recognition algorithms. By resizing the signatures to a consistent dimension, potential variations in size and aspect ratio are minimized, thereby enhancing the overall accuracy and reliability of the signature recognition system.

The new representation of signatures has proven to be well-suited for processing, especially considering our limited GPU capacity. Through effective preprocessing, the model can now extract highly influential points and efficiently handle the data within a feasible time frame. This optimization significantly elevates the overall performance and capability of the system.

4.2 Generator

Our architecture is based on CycleGAN architecture, as shown in figure 4.2. One of the primary advantages of CycleGAN is its ability to perform unsupervised image translation, meaning it can learn to convert images from one domain to another without the

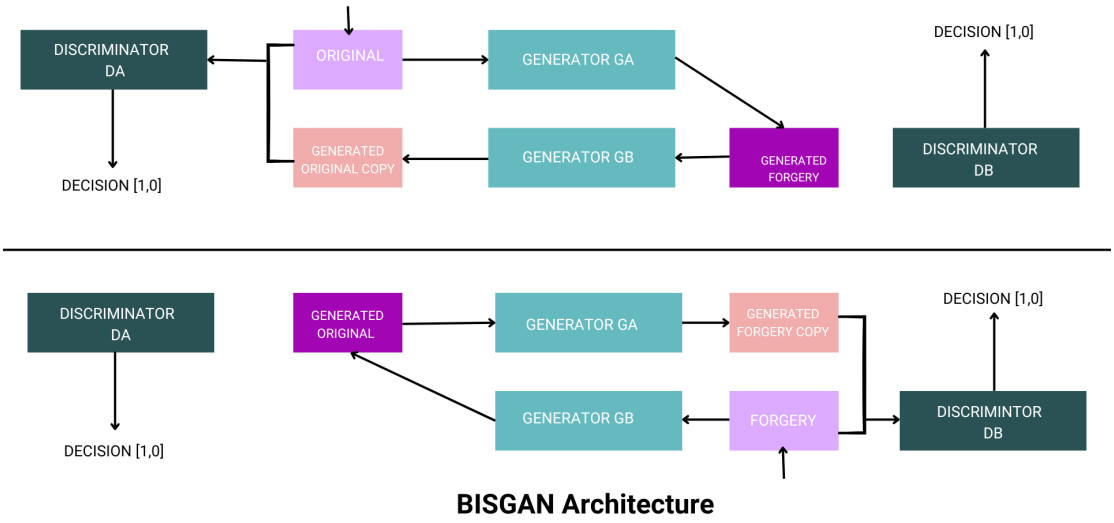

Figure 4.2: Architecture of BISGAN

need for paired training data. This flexibility makes CycleGAN particularly valuable when paired datasets are scarce or difficult to obtain. This ability of CycleGAN makes it suitable for our work. Moreover, CycleGAN can handle non-parallel data, allowing it to learn mappings between domains with distinct characteristics. The inherent cyclic consistency of CycleGAN enables the preservation of content and structure during image translation, resulting in realistic and coherent output. Each CycleGAN model consists of two generators: one for translating images from domain A to domain B and another for the reverse translation from domain B to domain A. These domains become the genuine and forged signatures in our case.

Both our generators have the same architecture as is usually the case with CycleGAN architectures. In BISGAN, the generators are infused with inception blocks after each convolution followed by an attention head, as shown in figure 4.3. The ResNet base of the generator layers of 64 7x7 filters, 128 3x3 filters, 256 3x3 filters, 512 3x3 filters, Six (6) transformer layers of 512 3x3 filters, which are followed by the layer blocks from before the transformer in reverse order. After each of these convolution layers an inception block with filters 1x1, 5x5, 3x3 and 3x3 max pool. After the inception block, an attention layer is placed which is followed by concatenation that is embedded in ResNet architecture.

We use inception blocks because they enable multi-scale feature extraction by performing convolutions of different filter sizes in parallel, allowing the model to capture fine-grained

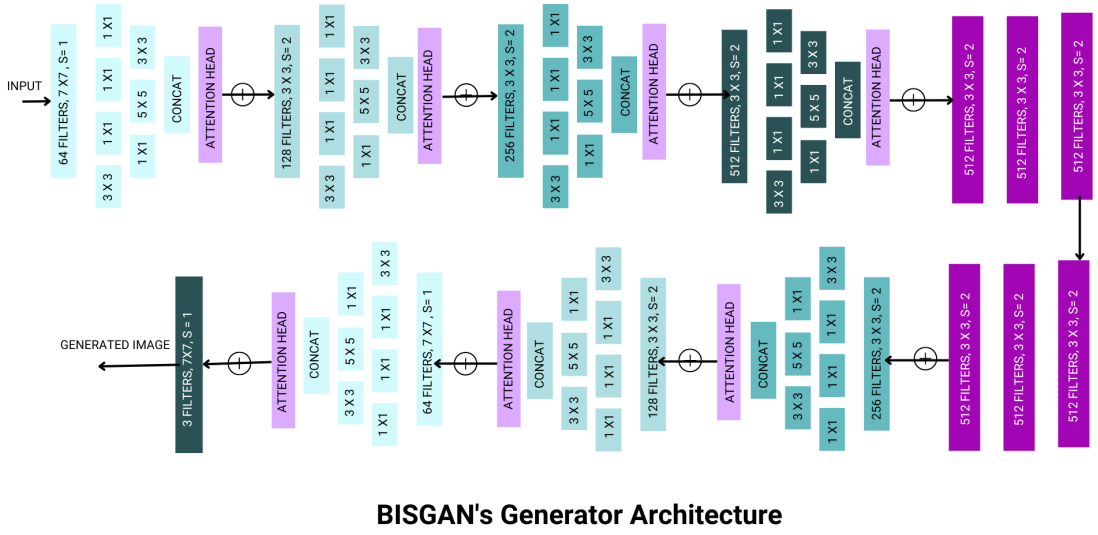

Figure 4.3: Generator architecture of BISGAN

and high-level abstract features simultaneously. Inception blocks are stacked to increase network depth, enabling the learning of hierarchical representations and capturing complex relationships within the data, leading to improved performance in various tasks. Attention layers allow the model to focus on the most relevant parts of the input data by assigning different attention weights to spatial locations or feature channels. Due to the above reasons, we have utilized both techniques in our architecture to achieve our intended goal.

4.3 Discriminator

Our discriminator is inspired by the work done by Jiang et al [91]. In their work, they introduced SigCNN for signature verification using Spatial Pyramid Pooling. We alter this architecture with inception blocks similar to our generator architecture and use this architecture for both of the discriminators in our model, as shown in figure 4.4. We use convolution layers of 64 7x7 filters, 128 3x3 filters, 256 3x3 filters. Each layer is followed by an inception block. Additionally, each inception block is followed by a max pool layer and a convolution layer that it had before the inception block. At the end of the model, we pass through a Spatial Pyramid Pooling layer followed by two parallel 512 Fully connected layers that are then concatenated for end result.

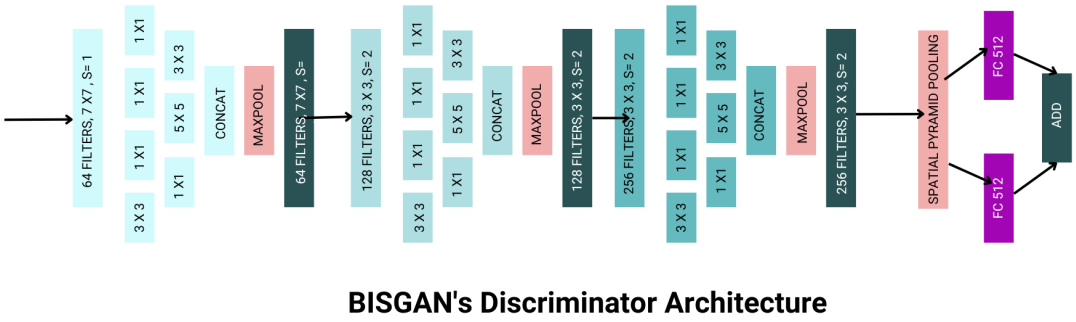

Figure 4.4: Discriminator architecture of BISGAN

4.4 Training Paradigm Shift

During training, CycleGAN enforces the generators to produce images that can be translated back to the original domain without significant information loss. This constraint is implemented through the cycle consistency loss, which calculates the difference between the original input image and the image obtained by translating it to the target domain and then back to the original domain. The generators optimize this loss to ensure that the translations are consistent and coherent. Through an adversarial training process and the cycle-consistency constraint, the generators in CycleGAN learn to capture the underlying mappings between two domains and generate high-quality images in both directions.

As discussed earlier in this work, generated forgeries should not be too similar or dissimilar to the genuine signature as a verification system would identify it. When a generator learns from the latent space of an image in a domain, it learns the significant data points and aims to replicate them. Thus, a forged signature would contain the strong feature or features of the original signature. If we learned from forged images instead of genuine signatures, the model would learn from the most commonly focused strong features replicated in forgeries and generate an image closer to the genuine signature, as represented in 4.5. Applying this theory to our CycleGAN-based would imply making the forged dataset domain A so that the focus is aimed in that direction. We test our theory by training our model the traditional way and with our paradigm-shifting theory as well. We compare and present the results of both in the evaluation section of this paper.

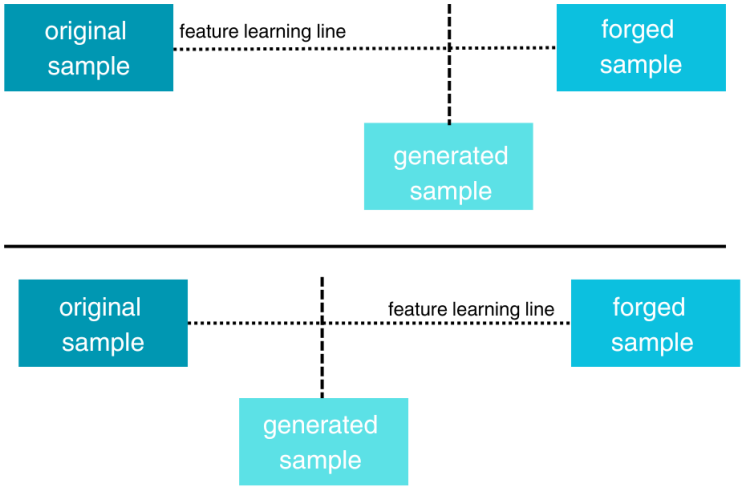

Figure 4.5: Abstract representation of achievement of new training technique.

Figure 4.6: WandB platform visualizations during training (epoch 200).

4.5 Visualization

To view our results and see real-time progress with learning, we use the Weight and Bases (wandb) platform. We create a dashboard where the image generation steps are visualized along with heat maps for identity loss, images generated by generator B using fake domain A images and vice versa, as shown in figure 4.6.

4.6 Computational Resources

During the creation and experimentation of this architecture, we had limited resources. Hence, we trained all GANs in turns of three with 200 epochs each. Each cycle would resume from the hyperparameters of the last checkpoint extracted from checkpoints. We

also used a total of three machines when we needed to run other GANs in the same time frame. These machines had the following GPUs: NVIDIA GeForce GTX 1650 4GB, NVIDIA GTX 1050ti 4GB and NVIDIA GTX 1060 3GB.

Chapter 5

Results

It is important to note that the success of our work can not be measured with traditional measures as the goal of our generated images is to fail the verification systems. Hence, the performance of the systems would be bad, indicating that the system is unable to correctly identify the generated forgeries as forgeries, which is the goal. We perfect other experiments to quantify the success of our model. Additionally, we propose an evaluation technique that helps present the quality of the forgery generated and can be used to define the quality of other domains of image generation.

5.1 Spoofing Verification Systems

Signature spoofing attempts at making a verification system unable to identify the forged signatures. As that is the goal of our model, the verification systems should perform poorly. We quantify this by analyzing the percentage of forged images that the verification system labels as genuine signatures. We brand this percentage as our success rate.

For this experiment, we train three deep-learning models on the CEDAR signature dataset to act as our verification systems. It is important to note that this dataset is small for learning and may impact results. Regardless, we stick with this dataset because the BISGAN model is trained on this dataset. Our verification systems are VGG-16 [13], AlexNet [9] , and CapsNet [22] models. Oot of these three, AlexNet performs the best during traditional training and testing that can be seen in table 5.1.

Next, we generate ten (10) forgeries from the BISGAN model. Additionally, we train

Verification Model	ACC	Precision
VGG-16	0.933	0.917
AlexNet	0.982	0.947
CapsNet	0.887	0.813

Table 5.1: Performance of Verification Models on CEDAR Signature Dataset

seven (7) other image generation models on the CEDAR signature dataset and generate 10 forgeries from each of these. Two (2) of them are based on techniques other than GANs to generate images, namely, RSAEG (perturbation-based) and the Diffusion model [68]. Two (2) of them are GAN techniques that have not been used for signature generation, namely, MaskGIT [86] and DCGAN. Three (3) of them are the latest GAN techniques used to generate signatures; CycleGAN, OSVGAN and Stroke-cCycleGAN. We pass the generated images of all the above architectures one by one as input to the three (3) verification systems that we have trained. We extract the success rate of all these architectures including our own, as shown in 5.2.

Model/Technique	VGG-16	AlexNet	CapsNet
RSAEG	60%	60%	80%
Diffusion Model	30%	20%	30%
CycleGAN	40%	50%	50%
OSVGAN	40%	40%	50%
Stroke-cCycleGAN	70%	70%	80%
MaskGIT	30%	20%	40%
DCGAN	20%	30%	50%
CEDAR	0%	0%	0%
BISGAN	**90%**	**80%**	**90%**
BISGAN (paradigm shift)	**90%**	**90%**	**100%**

Table 5.2: Results of different techniques on signature verification systems. The percentage determines how successful the technique is in fooling the verification system. Example: if a technique has obtained 60% success, it means that 6 out of 10 images given to the system were incorrectly identified as original signatures when in truth they were forgeries.

We observe that our BISGAN with paradigm shift training performs the best in our goal

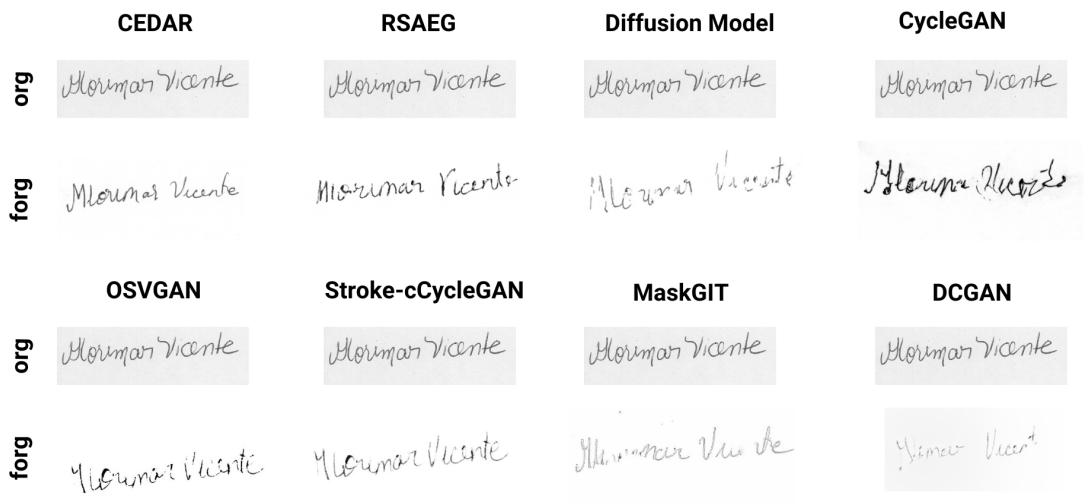

Figure 5.1: Comparison of generated forgeries of models.

Model/Technique	VGG-16	AlexNet	CapsNet
ICDAR 2021 Multi-script	80%	70%	90%
MCYT-100	90%	90%	100%

Table 5.3: Results of successful spoofing attempts using forgeries generated by BISGAN for ICDAR 2021 Multi-script dataset and BISGAN trained on MCYT-100 using the paradigm-shift technique.

of signature spoofing followed closely by our normally trained BISGAN. The second and third successful techniques are Stroke-cCycleGAN and RSAEG respectively.

To establish the generalizability of our model, we train BISGAN on another dataset and assess the success rate. We use the Roman script subscript from ICDAR 2021 Multi-script Dataset on Roman and Devanagari [74]. The Dataset contains 3,929 Roman signatures from 80 writers. We use BISGAN model to generate 10 images on this dataset and assess the success rate of these generated forgeries on our selected verification system models, that we train on this same dataset. We achieve benchmark results in successful spoofing attempts. Additionally, we train the BISGAN model in the paradigm-shift technique using the MCYT-100 dataset. We generate ten (10) forged images and pass them to our three verification models, after training them on the same dataset. The generated forgeries surpass the detection of the verification models. The results are shown in table 5.3.

Figure 5.2: Forgeries generated by BISGAN compared with original samples.

5.2 Generated Quality Metric (GQM)

Our work utilizes the theory that a forged signature cannot be too similar or dissimilar to a genuine signature. However, the data characteristics of a forgery should be similar to a genuine signature if it is to spoof a verification system. This answers the question of how good the generated forgery actually is. We propose the Generate Quality Metric (GQM), a metric that utilizes the data distributions of the input domain and leverages influential points of the dataset to compute the closeness of the generated image which quantifies the goodness of the generated image.

Considering influential data points converts the similarity function into a metric for goodness as it matches the important features in the data with the generated sample. GANs use the concept of latent space to learn about the input data domain. This primary concept has inspired our use of data distributions for a quality measure as well. We find the influential points over the distribution of both, the original and forged sample data using Mahalanobis distances [1]. P. C. Mahalanobis first introduced the Mahalanobis distance as the separation between a point P and a distribution D. It takes into account the covariance structure of the data to aid in locating significant deviations from the predicted distribution. Next, we compare the influential point vectors of both the original and forged samples with the influential points of the generated forged image using Cook's distance [2]. The scaled change in fitted values is known as Cook's distance. It measures how much removing a specific data point alters the model's estimates which is helpful as a distance measure in our case. Ultimately, we highlight which sample, original or forged, is the generated image closer to, strictly in terms of influential factors.

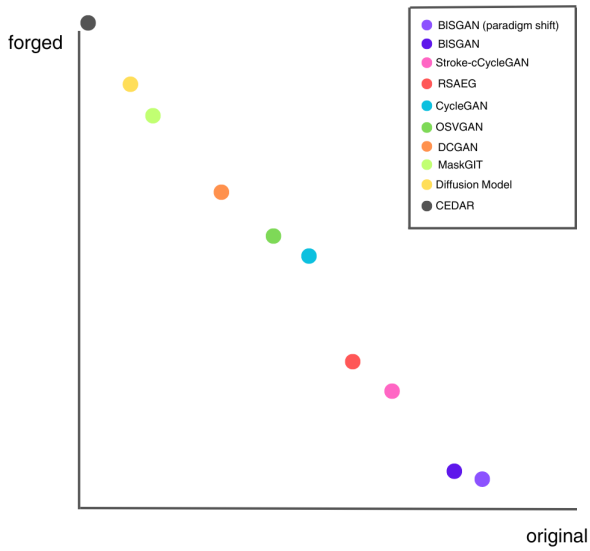

Figure 5.3: Mapping of GQM evaluation of generated samples of different architectures.

Mahalanobis distance is defined as:

$$d_M(\vec{x}, Q) = \sqrt{(\vec{x} - \vec{\mu})^T S^{-1} (\vec{x} - \vec{\mu})} \tag{5.2.1}$$

And Cook's distance is defined as:

$$D_i = \frac{r_i^2}{p \cdot MSE} \cdot \frac{h_{ii}}{(1 - h_{ii})^2}, \tag{5.2.2}$$

After constructing this metric, we evaluate the generated forgeries from the same architectures we used in our signature spoofing experiment. We randomly pick a generated forgery from the set of ten (10) generated by each architecture and one from the test forgery images of the CEDAR dataset. GQM shows BISGAN to be closest to the original, followed closely by RSAEG and then later Stroke-cCycleGAN. We map our results as shown in the figure.

5.3 Other Evaluations

As mentioned earlier in this section, traditional evaluation metrics are not useful in our case as the purpose of our model is to fail verification models. Regardless, we include the Equal Error Rate (EER) of our discriminator and compare it to the EER rate of OSVGAN in this section for a full presentation of our research. For most signature

Model/Technique	ERR
OSVGAN	2.55
BISGAN	**6.79**
BISGAN (paradigm shift)	**13.66**

Table 5.4: Traditional performance measure scores of our discriminator against the evaluation of other models as presented in their respective papers.

generation GANs, the EER rate is not presented in their research. We observe that BISGAN's discriminator on paradigm shift training performs worst as shown in table 5.4.

Chapter 6

Discussion and Conclusion

The results obtained from our ethical spoofing attempt could be better understood by looking at the significance of the major components of the methodology.

6.1 Discussion

Understanding the purpose of generated images is very important to any generative AI research. In our work, understanding that signature is a biometric trait and how to replicate it to a certain threshold played an important role. We centre our work around the concept of influential points of the input data distribution while both, creating our GAN architecture and devising our evaluation metric. RSAEG proves to be an efficient technique to achieve signature spoofing. However, it is not based on GANs hence BISGAN proves to be more powerful. Given more powerful systems to handle large amounts of data, BISGAN's training can be improved and hence its performance.

6.2 Summary and Conclusions

Signature verification encompasses various techniques, including descriptive language, geometrical analysis, and the analytical method. These methods utilize pattern recognition algorithms to compare and analyze unique features of signatures for authentication purposes. In addition to classification models, generative models are also used to differentiate between original and forged signatures by identifying underlying patterns and structures.

We identify a need for generator-focused research in signature data using GANs, as well as the importance of considering the percentage of similarity between original, forged, and generated samples. The lack of appropriate evaluation metrics for generated data also poses a research gap in this area.

Our research utilizes CycleGANs with Inception model-like blocks and attention heads, as well as the SigCNN model as a base Discriminator, to develop generators for signature forgery generation. The architecture of the generators is detailed, showcasing the combination of convolution layers, inception blocks, attention layers, and concatenation within a ResNet framework

The theory that generated forgeries should possess strong features of the original signature is explored in our work and the research presents results comparing traditional training methods with a paradigm-shifting approach. We also construct a quality metric that considers the influential data points and the use of Mahalanobis distances and Cook's distance as goodness measures for generated samples. We find that the BISGAN with paradigm shift training performs the best in achieving the goal of signature spoofing, followed closely by the normally trained BISGAN.

6.3 Future Work

For future research work, the transition of GQM to different domains and GAN architectures can be evaluated. Although we believe that GQM can be generalized for many different GAN architectures since the concept of latent space is common among all, it is important to test it for different domains. We have constructed BISGAN solely for signature datasets but it could be experimented with in other domains of image translation but probably not image style transfer.

This work encourages the usage of GANs in ethical spoofing research. As generative AI reaches a stage of uncontrollable use, such research can help protect future systems

using biometric data. Innovation in generative AI research towards evaluation holds significance in terms of control and verification of data.

Bibliography

[1] Mahalanobis P.C. "On the generalized distance in statistics." In: *Proceedings of the National Institute of Sciences of India* 2.1 (1936), pp. 49–55.

[2] Cook R. Dennis. "Detection of influential observation in linear regression." In: *Technometrics* 19.1 (1977), pp. 15–18.

[3] Nobuyuki Otsu. "A threshold selection method from gray-level histograms". In: *IEEE transactions on systems, man, and cybernetics* 9.1 (1979), pp. 62–66.

[4] Peter Olver, Guillermo Sapiro, and Allen Tannenbaum. *Differential invariant signatures and flows in computer vision: a symmetry group approach*. Springer, 1994.

[5] JF Vargas et al. "Off-line handwritten signature GPDS-960 corpus". In: *Ninth International Conference on Document Analysis and Recognition (ICDAR 2007)*. Vol. 2. IEEE. 2007, pp. 764–768.

[6] H Srinivasan, Sargur N Srihari, and Mathew J Beal. "Machine learning for signature verification". In: *2008 19th International Conference on Pattern Recognition*. 2008, pp. 1–4.

[7] Alisher Kholmatov and Berrin Yanikoglu. "SUSIG: an on-line signature database, associated protocols and benchmark results". In: *Pattern Analysis and Applications* 12 (2009), pp. 227–236.

[8] Saroj Kumar Panigrahy et al. "On the privacy protection of biometric traits: palmprint, face, and signature". In: *Contemporary Computing: Second International Conference, IC3 2009, Noida, India, August 17-19, 2009. Proceedings 2*. Springer. 2009, pp. 182–193.

[9] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. "Imagenet classification with deep convolutional neural networks". In: *Advances in neural information processing systems (NIPS)*. 2012, pp. 1097–1105.

[10] Ian Goodfellow et al. "Generative adversarial nets". In: *Advances in neural information processing systems* 27 (2014), pp. 2672–2680.

[11] Christoph Günther. "A survey of spoofing and counter-measures". In: *NAVIGATION: Journal of the Institute of Navigation* 61.3 (2014), pp. 159–177.

[12] Mehdi Mirza and Simon Osindero. "Conditional generative adversarial nets". In: *Proceedings of the 3rd International Conference on Learning Representations (ICLR)*. 2014.

[13] Karen Simonyan and Andrew Zisserman. "Very deep convolutional networks for large-scale image recognition". In: *Proceedings of the international conference on learning representations (ICLR)*. 2014.

[14] Bahdanau Dzmitry. Cho Kyunghyun. Bengio Yoshua. "Neural machine translation by jointly learning to align and translate". In: *Proceedings of the 3rd International Conference on Learning Representations (ICLR)* (2014).

[15] Alec Radford, Luke Metz, and Soumith Chintala. "Unsupervised representation learning with deep convolutional generative adversarial networks". In: *arXiv preprint arXiv:1511.06434* (2015).

[16] Luiz G Hafemann, Robert Sabourin, and Luiz S Oliveira. "Analyzing features learned for offline signature verification using deep CNNs". In: *2016 23rd international conference on pattern recognition (ICPR)*. IEEE. 2016, pp. 2989–2994.

[17] Zehua Zhang, Xiangqian Liu, and Yan Cui. "Multi-phase offline signature verification system using deep convolutional generative adversarial networks". In: *2016 9th international Symposium on Computational Intelligence and Design (ISCID)*. Vol. 2. IEEE. 2016, pp. 103–107.

[18] Martin Arjovsky, Soumith Chintala, and L'eon Bottou. "Wasserstein generative adversarial networks". In: *International conference on machine learning*. 2017, pp. 214–223.

[19] Luiz G Hafemann, Robert Sabourin, and Luiz S Oliveira. "Offline handwritten signature verification—literature review". In: *2017 seventh international conference on image processing theory, tools and applications (IPTA)*. IEEE. 2017, pp. 1–8.

[20] Songxuan Lai, Lianwen Jin, and Weixin Yang. "Online signature verification using recurrent neural network and length-normalized path signature descriptor". In: *2017 14th IAPR international conference on document analysis and recognition (ICDAR)*. Vol. 1. IEEE. 2017, pp. 400–405.

[21] Christian Ledig et al. "Photo-realistic single image super-resolution using a generative adversarial network". In: *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2017, pp. 4681–4690.

[22] Sara Sabour, Nicholas Frosst, and Geoffrey E Hinton. "Dynamic routing between capsules". In: *Advances in neural information processing systems (NIPS)*. 2017, pp. 3856–3866.

[23] Ruben Tolosana et al. "Biometric signature verification using recurrent neural networks". In: *2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR)*. Vol. 1. IEEE. 2017, pp. 652–657.

[24] Ashish Vaswani et al. "Attention is all you need". In: *Advances in Neural Information Processing Systems* 30 (2017), pp. 5998–6008.

[25] Mohammad E Yahyatabar and Jamal Ghasemi. "Online signature verification using double-stage feature extraction modelled by dynamic feature stability experiment". In: *IET Biometrics* 6.6 (2017), pp. 393–401.

[26] Jun-Yan Zhu et al. "Unpaired image-to-image translation using cycle-consistent adversarial networks". In: *Proceedings of the IEEE international conference on computer vision*. 2017, pp. 2223–2232.

[27] Santosh Kumar Behera et al. "Air signature recognition using deep convolutional neural network-based sequential model". In: *2018 24th International Conference on Pattern Recognition (ICPR)*. IEEE. 2018, pp. 3525–3530.

[28] Mustafa Berkay Yilmaz and Kagan Ozturk. "Hybrid user-independent and user-dependent offline signature verification with a two-channel CNN". In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*. 2018, pp. 526–534.

[29] Madasu Hanmandlu, A Bhanu Sronothara, and Shantaram Vasikarla. "Deep learning based offline signature verification". In: *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE. 2018, pp. 732–737.

[30] Songxuan Lai and Lianwen Jin. "Recurrent adaptation networks for online signature verification". In: *IEEE Transactions on information forensics and security* 14.6 (2018), pp. 1624–1637.

[31] Paul Maergner et al. "Offline signature verification by combining graph edit distance and triplet networks". In: *Structural, Syntactic, and Statistical Pattern Recognition: Joint IAPR International Workshop, S+ SSPR 2018, Beijing, China, August 17–19, 2018, Proceedings 9*. Springer. 2018, pp. 470–480.

[32] Mohammad Hajizadeh Saffar et al. "Online signature verification using deep representation: a new descriptor". In: *arXiv preprint arXiv:1806.09986* (2018).

[33] Bhushan S Thakare and Hemant R Deshmukh. "A Novel End-To-End Approach For Offline Signature Verification System". In: *2018 3rd International Conference for Convergence in Technology (I2CT)*. IEEE. 2018, pp. 1–7.

[34] Dimitros Tsourounis et al. "Handwritten signature verification via deep sparse coding architecture". In: *2018 IEEE 13th image, video, and multidimensional signal processing workshop (IVMSP)*. IEEE. 2018, pp. 1–5.

[35] Gengxing Wang et al. "Generative adversarial network (GAN) based data augmentation for palmprint recognition". In: *2018 Digital Image Computing: Techniques and Applications (DICTA)*. IEEE. 2018, pp. 1–7.

[36] Zachary Bessinger and Nathan Jacobs. "A generative model of worldwide facial appearance". In: *2019 IEEE Winter Conference on Applications of Computer Vision (WACV)*. IEEE. 2019, pp. 1569–1578.

[37] Philippe M Burlina et al. "Assessment of deep generative models for high-resolution synthetic retinal image generation of age-related macular degeneration". In: *JAMA ophthalmology* 137.3 (2019), pp. 258–264.

[38] Nurullah Calik et al. "Large-scale offline signature recognition via deep neural networks and feature embedding". In: *Neurocomputing* 359 (2019), pp. 1–14.

[39] Tero Karras, Samuli Laine, and Timo Aila. "A style-based generator architecture for generative adversarial networks". In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (2019), pp. 4401–4410.

[40] Chuang Li et al. "A stroke-based RNN for writer-independent online signature verification". In: *2019 international conference on document analysis and recognition (ICDAR)*. IEEE. 2019, pp. 526–532.

[41] Alberto Botana López. "Deep learning in biometrics: a survey". In: *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal* 8.4 (2019), pp. 19–32.

[42] Omid Mersa et al. "Learning representations from persian handwriting for offline signature verification, a deep transfer learning approach". In: *2019 4th International Conference on Pattern Recognition and Image Analysis (IPRIA)*. IEEE. 2019, pp. 268–273.

[43] Ramesh Kumar Mohapatra, Kumar Shaswat, and Subham Kedia. "Offline handwritten signature verification using CNN inspired by inception V1 architecture". In: *2019 Fifth International Conference on Image Information Processing (ICIIP)*. IEEE. 2019, pp. 263–267.

[44] Shayekh Mohiuddin Ahmed Navid et al. "Signature verification using convolutional neural network". In: *2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON)*. IEEE. 2019, pp. 35–39.

[45] Witold Oleszkiewicz et al. "Siamese generative adversarial privatizer for biometric data". In: *Computer Vision–ACCV 2018: 14th Asian Conference on Computer Vision, Perth, Australia, December 2–6, 2018, Revised Selected Papers, Part V 14*. Springer. 2019, pp. 482–497.

[46] Javier O Pinzón-Arenas, Robinson Jiménez-Moreno, and César G Pachón-Suescún. "Offline signature verification using DAG-CNN." In: *International Journal of Electrical & Computer Engineering (2088-8708)* 9.4 (2019).

[47] Suriani Mohd Sam et al. "Offline signature verification using deep learning convolutional neural network (CNN) architectures GoogLeNet inception-v1 and inception-v3". In: *Procedia Computer Science* 161 (2019), pp. 475–483.

[48] Sima Shariatmadari, Sima Emadi, and Younes Akbari. "Patch-based offline signature verification using one-class hierarchical deep learning". In: *International Journal on Document Analysis and Recognition (IJDAR)* 22.4 (2019), pp. 375–385.

[49] Siyue Wang and Shijie Jia. "Signature handwriting identification based on generative adversarial networks". In: *Journal of Physics: Conference Series*. Vol. 1187. 4. IOP Publishing. 2019, p. 042047.

[50] Yan Zheng et al. "Ranksvm for offline signature verification". In: *2019 International Conference on Document Analysis and Recognition (ICDAR)*. IEEE. 2019, pp. 928–933.

[51] Eman Alajrami et al. "Handwritten signature verification using deep learning". In: (2020).

[52] Kiran Bibi, Saeeda Naz, and Arshia Rehman. "Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities". In: *Multimedia Tools and Applications* 79.1-2 (2020), pp. 289–340.

[53] SV Bonde, Pradeep Narwade, and Rajendra Sawant. "Offline signature verification using convolutional neural network". In: *2020 6th International Conference on Signal Processing and Communication (ICSC)*. IEEE. 2020, pp. 119–127.

[54] Subhash Chandra. "Verification of dynamic signature using machine learning approach". In: *Neural Computing and Applications* 32.15 (2020), pp. 11875–11895.

[55] Amr Hefny and Mohamed Moustafa. "Online signature verification using deep learning and feature representation using Legendre polynomial coefficients". In: *The International Conference on Advanced Machine Learning Technologies and Applications (AMLTA2019) 4*. Springer. 2020, pp. 689–697.

[56] Hsin-Hsiung Kao and Che-Yen Wen. "An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach". In: *Applied Sciences* 10.11 (2020), p. 3716.

[57] Jameel Malik et al. "DeepAirSig: End-to-end deep learning based in-air signature verification". In: *IEEE Access* 8 (2020), pp. 195832–195843.

[58] Chirag Nathwani. “Online signature verification using bidirectional recurrent neural network”. In: *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE. 2020, pp. 1076–1078.

[59] Manabu Okawa. “Online signature verification using single-template matching with time-series averaging and gradient boosting”. In: *Pattern Recognition* 102 (2020), p. 107227.

[60] Jivesh Poddar, Vinanti Parikh, and Santosh Kumar Bharti. “Offline signature recognition and forgery detection using deep learning”. In: *Procedia Computer Science* 170 (2020), pp. 610–617.

[61] Victoria Ruiz et al. “Off-line handwritten signature verification using compositional synthetic generation of signatures and Siamese Neural Networks”. In: *Neurocomputing* 374 (2020), pp. 30–41.

[62] Chandra Sekhar Vorugunti et al. “DeepFuseOSV: online signature verification using hybrid feature fusion and depthwise separable convolution neural network architecture”. In: *IET Biometrics* 9.6 (2020), pp. 259–268.

[63] Abigail Singh and Serestina Viriri. “Online signature verification using deep descriptors”. In: *2020 Conference on information communications technology and society (ICTAS)*. IEEE. 2020, pp. 1–6.

[64] Orieb AbuAlghanam, Layla Albdour, and Omar Adwan. “Multimodal biometric fusion online handwritten signature verification using neural network and support vector machine”. In: *transactions* 7.8 (2021).

[65] Leonardo Espinosa-Leal et al. “Extreme learning machines for signature verification”. In: *Proceedings of ELM2019 9*. Springer. 2021, pp. 31–40.

[66] Rajib Ghosh. “A Recurrent Neural Network based deep learning model for offline signature verification and recognition system”. In: *Expert Systems with Applications* 168 (2021), p. 114249.

[67] M Muzaffar Hameed et al. “Machine learning-based offline signature verification systems: A systematic review”. In: *Signal Processing: Image Communication* 93 (2021), p. 116139.

[68] Jonathan Ho et al. “Denoising diffusion probabilistic models”. In: *arXiv preprint arXiv:2006.11239* (2021).

[69] Haoyang Li et al. “Black-box attack against handwritten signature verification with region-restricted adversarial perturbations”. In: *Pattern Recognition* 111 (2021), p. 107689.

[70] Huan Li, Ping Wei, and Ping Hu. “AVN: An adversarial variation network model for handwritten signature verification”. In: *IEEE Transactions on Multimedia* 24 (2021), pp. 594–608.

[71] Cai Siqi. Li Peiwen. Su Enze. Xie Longhan. “Auditory Attention Detection via Cross-Modal Attention”. In: *Frontiers in Neuroscience* 15 (2021), p. 652058. DOI: 10.3389/fnins.2021.652058.

[72] Ebrahim Parcham, Mahdi Ilbeygi, and Mohammad Amini. “CBCapsNet: A novel writer-independent offline signature verification model using a CNN-based architecture and capsule neural networks”. In: *Expert Systems with Applications* 185 (2021), p. 115649.

[73] Lars Ruthotto and Eldad Haber. “An introduction to deep generative modeling”. In: *GAMM-Mitteilungen* 44.2 (2021), e202100008.

[74] Obaidullah Sk et al. *Multi-script handwritten signature (Roman Devanagari)*. 2021. DOI: 10.21227/bgmm-t264. URL: https://dx.doi.org/10.21227/bgmm-t264.

[75] Patrick Tinsley, Adam Czajka, and Patrick Flynn. “This face does not exist... but it might be yours! identity leakage in generative models”. In: *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*. 2021, pp. 1320–1328.

[76] Ruben Tolosana et al. “DeepSign: Deep On-Line Signature Verification”. In: *IEEE Transactions on Biometrics, Behavior, and Identity Science* 3.2 (2021), pp. 275–289.

[77] Ruben Tolosana et al. “DeepSign: Deep on-line signature verification”. In: *IEEE Transactions on Biometrics, Behavior, and Identity Science* 3.2 (2021), pp. 229–239.

[78] Ruben Tolosana et al. “SVC-onGoing: Signature Verification Competition”. In: *2021 International Conference on Document Analysis and Recognition (ICDAR)*. 2021, pp. 1–6.

[79] Ogban-Asuquo Ugot, Chika Yinka-Banjo, and Sanjay Misra. "Biometric fingerprint generation using generative adversarial networks". In: *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities*. Springer, 2021, pp. 51–83.

[80] Muhammed Mutlu Yapıcı, Adem Tekerek, and Nurettin Topaloğlu. "Deep learning-based data augmentation method and signature verification system for offline handwritten signature". In: *Pattern Analysis and Applications* 24 (2021), pp. 165–179.

[81] Yiwen Zhou et al. "Handwritten signature verification method based on improved combined features". In: *Applied Sciences* 11.13 (2021), p. 5867.

[82] U Yu Akhundjanov and VV Starovoitov. "Pre-processing of handwritten signature images for following recognition". In: *«System analysis and applied information science»* 2 (2022), pp. 4–9.

[83] Md L Ali, Kutub Thakur, and Muath A Obaidat. "A hybrid method for keystroke biometric user identification". In: *Electronics* 11.17 (2022), p. 2782.

[84] Pankaj Bamoriya et al. "DSB-GAN: Generation of deep learning based synthetic biometric data". In: *Displays* 74 (2022), p. 102267.

[85] Jordan J Bird. "Robotic and Generative Adversarial Attacks in Offline Writer-independent Signature Verification". In: *arXiv preprint arXiv:2204.07246* (2022).

[86] Huiwen Chang et al. "MaskGIT: Masked Generative Image Transformer". In: *CVPR 2022*. May 2022. URL: 1.

[87] Meng-Hao Guo et al. "Attention mechanisms in computer vision: A survey". In: *Computational Visual Media* 8.3 (2022), pp. 331–368. DOI: 10.1007/s41095-022-0271-y.

[88] Yash Gupta et al. "Handwritten Signature Verification Using Transfer Learning and Data Augmentation". In: *Proceedings of International Conference on Intelligent Cyber-Physical Systems: ICPS 2021*. Springer. 2022, pp. 233–245.

[89] Phan Duy Hung et al. "Offline handwritten signature forgery verification using deep learning methods". In: *Smart Trends in Computing and Communications: Proceedings of SmartCom 2022*. Springer, 2022, pp. 75–84.

[90] Jiajia Jiang et al. “Dsdtw: Local representation learning with deep soft-dtw for dynamic signature verification”. In: *IEEE Transactions on Information Forensics and Security* 17 (2022), pp. 2198–2212.

[91] Jiajia Jiang et al. “Forgery-free signature verification with stroke-aware cycle-consistent generative adversarial network”. In: *Neurocomputing* 507 (2022), pp. 345–357.

[92] Pavlos Kipouras. “THE EVOLUTION OF THE SIMULATED SIGNATURE BY THE FORGER”. In: *International Journal of Law in Changing World* 1 (2022).

[93] José AP Lopes et al. “Offline handwritten signature verification using deep neural networks”. In: *Energies* 15.20 (2022), p. 7611.

[94] Saeeda Naz, Kiran Bibi, and Riaz Ahmad. “DeepSignature: fine-tuned transfer learning based signature verification system”. In: *Multimedia Tools and Applications* 81.26 (2022), pp. 38113–38122.

[95] Md Fazle Rabby, Md Abdullah Al Momin, and Xiali Hei. “Handwritten Signature Spoofing With Conditional Generative Adversarial Nets”. In: *Security, Data Analytics, and Energy-Aware Solutions in the IoT*. IGI Global, 2022, pp. 98–110.

[96] Ali Fathel Rasheed and Ahmed M Alkababji. “A Novel Method for Signature Verification Using Deep Learning”. In: *Webology* 19.1 (2022), pp. 1561–1572.

[97] Yan Antonino Costa Santos, Leandro Chaves Rêgo, and Raydonal Ospina. “Online handwritten signature verification via network analysis”. In: *Physica A: Statistical Mechanics and its Applications* 600 (2022), p. 127582.

[98] Neha Sharma et al. “Offline signature verification using deep neural network with application to computer vision”. In: *Journal of Electronic Imaging* 31.4 (2022), pp. 041210–041210.

[99] Ruben Tolosana et al. “SVC-onGoing: Signature verification competition”. In: *Pattern Recognition* 127 (2022), p. 108609.

[100] Dimitrios Tsourounis et al. “From text to signatures: Knowledge transfer for efficient deep feature learning in offline signature verification”. In: *Expert Systems with Applications* 189 (2022), p. 116136.

[101] Harmandeep Kaur and Munish Kumar. “Signature identification and verification techniques: state-of-the-art work”. In: *Journal of Ambient Intelligence and Humanized Computing* 14.2 (2023), pp. 1027–1045.

[102] Teressa Longjam, Dakshina Ranjan Kisku, and Phalguni Gupta. “Multi-scripted Writer Independent Off-line Signature Verification using Convolutional Neural Network”. In: *Multimedia Tools and Applications* 82.4 (2023), pp. 5839–5856.

[103] Biometrics and Data Pattern Analytics - BiDA Lab. *MCYT-Signature-100*. http://atvs.ii.uam.es/atvs/mcyt100s.html.

[104] Chandra Sekhar Vorugunti Sai Sasikanth Indukuri et al. “OSVGAN: Generative Adversarial Networks for Data Scarce Online Signature Verification”. In: ().