Literature Survey on Synthetic Biometric Data Generation Using Intelligent Systems

Emanuele Artegiani
emanuele.artegiani@studio.unibo.it
ID: 0001140446

November 2025

Abstract

This literature survey focuses on intelligent systems techniques used to generate **Synthetic Biometric Data**, in particular **Fingerprints**. The concern is to identify success in the implementation of design choices, algorithms, and principles used, the benefits of the application, and the challenges encountered. The study aims to derive insights into current trends and potential advancements in Synthetic Fingerprint generation (SFG).

Index

List of Figures

Chapter 1

Introduction

Biometric recognition systems, which leverage unique physiological and behavioral traits like fingerprints, faces, irises, and voices for identification and verification, are no longer novelties. They are deeply integrated into the fabric of modern security, from unlocking smartphones to securing international borders and processing financial transactions. The efficacy, fairness, and robustness of these systems are critically dependent on the data used to train and test their underlying machine learning algorithms. However, the reliance on real biometric data has created a significant and persistent bottleneck, fraught with logistical, ethical, and technical challenges.

The collection of large-scale, diverse, and representative datasets of real biometric identifiers is notoriously difficult. It is a process that is not only *expensive and time-consuming* but also governed by a complex web of *privacy regulations*, such as the GDPR[6] and HIPAA[7]. The sensitive nature of biometric data—being an immutable and permanently linked part of an individual's identity—makes its collection, storage, and sharing a matter of significant privacy and security risk. Furthermore, even when data is successfully collected, it often suffers from inherent demographic and environmental biases. Datasets may be skewed, over-representing certain populations while under-representing others, which leads to algorithms that exhibit poor and inequitable performance for minority groups. This lack of data diversity also makes it difficult to test the systems' robustness against rare conditions, adversarial attacks, or environmental variations.

In response to this critical data dilemma, the field has increasingly turned to a powerful alternative: synthetic biometric data generation. This approach involves using advanced generative models, such as Generative Adversarial Networks (GANs)[8], Variational Autoencoders (VAEs)[9], and, more recently, diffusion models[10], to create high-fidelity, artificially generated biometric data. This synthetic data is not a simple copy of existing samples; it consists of entirely new, realistic biometric traits that are statistically representative of real data but do not correspond to any real individual.

This paradigm shift offers a transformative solution to the aforementioned challenges. It allows researchers and developers to:

Preserve privacy by training models on data that contains no personally identifiable information (PII).

Mitigate bias by synthetically generating balanced datasets with controlled demographic distributions.

Enhance robustness by creating vast and varied datasets that include specific edge cases, environmental noise, spoofing attempts (e.g., "deepfakes"), and presentation attacks for testing.

Accelerate development by generating virtually limitless amounts of data on demand, bypassing the logistical hurdles of real-world data collection.

As the realism and utility of synthetic data continue to improve, its role is expanding from a simple data augmentation technique to a fundamental enabler of next-generation biometric system development, testing, and certification. This literature survey will provide a comprehensive overview of the state-of-the-art in synthetic biometric data generation. It will be systematically reviewed and analyzed the evolution of generative methodologies, assess the techniques used for SFG, and examined the evaluation metrics used to measure the quality, realism, and utility of the generated data.

The principal architectures and techniques used for generating synthetic fingerprints can be collected into the following categories:

- **Model-Based Architectures (Classical)**: these "bottom-up" methods follow a multi-stage, rule-based process to explicitly model the anatomical structure of a fingerprint. The typical pipeline for a model-based generator involves:

    1. **Singularity and Class Definition**: The process starts by randomly defining the fingerprint class (e.g., Arch, Left Loop, Whorl) and placing the

primary singularities (cores and deltas) in valid anatomical positions.

2. **Orientation Field Generation**: A mathematical model generates a directional "flow map" for the ridges, guided by the positions of the cores and deltas.
3. **Ridge Pattern Generation**: A ridge-valley pattern is created, often using Gabor-like filters that are iteratively applied across the image, following the orientation field. This step also generates minutiae (ridge endings and bifurcations) at random, plausible locations.
4. **Noising and Rendering**: This is a critical final stage that adds realism. The "clean" master print is degraded to simulate real-world acquisition. This includes:
   - Adding random noise, small cuts, and scratches.
   - Simulating skin pores.
   - Modeling skin plasticity and non-linear distortion (to simulate the finger pressing and rolling on a sensor).
   - Adjusting ridge thickness to simulate dry or wet skin.

- **Deep Learning Architectures (Data-Driven)**: These "top-down" methods learn the underlying statistical distribution of real fingerprint images from a large dataset. They generate new samples by sampling from this learned distribution and are known for producing highly realistic and complex textures. The main representatives of this category are as follows:
  - **Generative Adversarial Networks (GANs)**: They are the most widely used deep learning technique for this task. A GAN consists of two competing neural networks: a *Generator* that creates fake images and a *Discriminator* that tries to distinguish the fake images from real ones.
  - **Diffusion Models**: These are a newer class of generative models that have proven to be extremely powerful, often surpassing GANs in image quality and diversity. The main implementation is:
    - **Denoising Diffusion Probabilistic Models (DDPMs)**: These models work by progressively adding "noise" to a real image until it

becomes pure static. They then train a neural network to reverse the process, learning to gradually de-noise the static back into a realistic image.

Finally, we will discuss the key open challenges, ethical considerations, and future research directions that will shape this rapidly advancing field.

Chapter 2

Method

This section details the systematic procedure followed to carry out a comprehensive review of the literature on SFG based on intelligent systems. This methodology intends to follow a systematic review approach, ensuring a comprehensive, unbiased, and reproducible overview of existing research. These processes comprise several key stages, including the definition of objectives and research questions, preparation of the search strategy, selection of relevant studies, assessment of the quality of selected studies, and extraction and synthesis of data from the studies.

The Systematic Literature Review (SLR) methodology adopted here is designed to systematically identify, evaluate, and synthesize the existing literature body on SFG techniques and architectures. This principally aims to understand the design choices, algorithms, and principles behind SFG frameworks and to describe their advantages, challenges, and results.

2.1 Research Objectives and Questions

The primary objective of this literature review is to systematically explore and analyze the methods and utility of SFG in intelligent systems. This involves a detailed examination of the design choices (e.g., GANs, Diffusion Models), algorithms, principles, and frameworks used to create realistic and diverse synthetic fingerprints, as well as an assessment of their benefits and challenges in various application domains such as biometric system evaluation, Presentation Attack Detection (PAD), and bias mitigation.

The main goal of this literature review is to systematically investigate and discuss the applications and technological underpinnings of SFG in intelligent systems. This includes a deeper probing into generative models (e.g., GAN architectures), quality metrics (e.g., NFIQ2), and synthesis frameworks, along with an assessment of their benefits (e.g., privacy, data volume) and challenges (e.g., realism, identity preservation) in critical areas like biometric recognition training and security testing.

To achieve this objective, the following research questions arise:

- How can high quality synthetic fingerprints be obtained?
- What benefits does SFG provide in the creation of intelligent systems?
- What generalization capabilities a system trained solely on synthetic fingerprints can reach?
- Does synthetic generated datasets affect data privacy?

2.2 Search strategy

The search strategy was designed to comprehensively identify relevant studies on SFG intelligent systems. The electronic databases searched are:

- Google Scholar
- IEEE Xplore
- Springer Link
- DBLP

The search was conducted using a combination of correlated words combined to *fingerprint generation* (used also alone):

- Synthetic
- GAN
- VAE

- Diffusion

The search was limited to articles published in English from 2020 to 2025. The inclusion and exclusion criteria applied to the search results are presented in the following section.

2.3 Study selection

The study selection process was conducted in multiple stages to ensure the inclusion of relevant and high-quality studies on SFG.

1. **Initial Screening**: Titles and abstracts of the identified articles from the first phase of the search were reviewed to exclude studies that did not meet the inclusion criteria.

2. **Full-Text Review**: The remaining articles were thoroughly reviewed in full to assess their relevance based on the research questions and the fields of interest identified during the search strategy.

3. **Final Selection**: Articles that provided significant insights into SFG were included in the final review.

2.3.1 Inclusion Criteria

- Peer-reviewed journal articles, conference papers, and reputable academic publications.

- Studies published in the English language in the last 5 years.

- Paper content is pertinent to the research questions.

- Paper content is pertinent to the SFG topic.

- Paper is either openly accessible or accessible through university credentials.

Resources that did not meet these parameters were excluded.

2.4 Quality Assessment Criteria

The following set of quality assessment criteria was applied to the studies that already met the Inclusion Criteria:

- **Relevance**: The study's focus on SFG or its applications in intelligent systems and its alignment with the research questions.
- **Rigor**: The methodological soundness and robustness of the study, including the clarity of the research design, data collection, and analysis methods.
- **Contribution**: The significance of the study's findings to the field of synthetic biometric data generation, including the novelty of the research, the implications of the results, and the contribution to advancing knowledge in the domain.
- **Clarity**: The clarity and coherence of the study's presentation and conclusions, including the logical flow of ideas, the transparency of the methodology, and the articulation of findings.
- **Up-to-date**: The methods and approaches presented in the study are the most recent developments in their category or offer particular contributions or advantages.

2.5 Data extraction

The data extraction process involved systematically recording relevant information from each selected study. The information extracted includes: title, authors, year of publication, and abstract.

- **Title**: Synthetic Fingerprint Generation: Bridging the Gap Between Privacy and Security with Variational Auto-Encoders[1]
  - **Authors**: Maiti, Diptadip and Basak, Madhuchhanda and Das, Debashis
  - **Year of publication**: 2024
  - **Abstract**:

Abstract

This study presents a state-of-the-art technique utilizing Variational Autoencoders (VAEs) for synthetic fingerprint generation, aiming to strike a balance between privacy and security in biometric systems. The proposed VAE architecture employs an encoder-decoder network to transform raw fingerprint data into a lower-dimensional latent space, enabling the generation of diverse and realistic synthetic fingerprints. The workflow involves encoding raw data, mapping it to the latent space, and then decoding it to produce detailed synthetic representations. The model's architecture is elucidated, detailing the encoder and decoder components, and their respective parametrizations. The reparameterization trick is employed to address gradient computation challenges during training. The training process involves the minimization of both reconstruction loss and Kullback-Leibler divergence loss, ensuring the generated fingerprints maintain fidelity to the input while adhering to a standard normal distribution in the latent space. The study demonstrates the effectiveness of the proposed VAE through comprehensive results, including reconstruction and KL divergence loss curves. Synthetic fingerprint images are showcased, illustrating the model's ability to faithfully reconstruct input data. Additionally, the model's capability to generate diverse synthetic fingerprints by manipulating latent vectors is highlighted. The generated imaged is checked with NFIQ-2 for checking the quality of the image.

- **Title**: Vikriti-ID: A Novel Approach For Real Looking Fingerprint Data-set Generation[2]
  - **Authors**: Shukla, Rishabh and Sinha, Aditya and Singh, Vansh and Kaur, Harkeerat
  - **Year of publication**: 2024
  - **Abstract**:

Abstract

Fingerprint recognition research faces significant challenges due to the limited availability of extensive and publicly available fingerprint databases. Existing databases lack a sufficient number of identities and fingerprint impressions, which hinders progress in areas such as Fingerprint-based access control. To address this challenge, we present Vikriti-ID, a synthetic fingerprint generator capable of generating unique fingerprints with multiple impressions. Using Vikriti-ID, we generated a large database containing 500000 unique fingerprints, each with 10 associated impressions. We then demonstrate the effectiveness of the database generated by Vikriti-ID by evaluating it for imposter-genuine score distribution and Equal Error Rate (EER) score. Apart from this we also trained a deep network to check the usability of data. We trained the network inspired from [13], on both Vikriti-ID generated data as well as public data. This generated data achieved an EER of 0.16%, AUC of 0.89%. This improvement is possible due to the limitations of existing publicly available data sets, which struggle in numbers or multiple impressions.

- **Title**: DSB-GAN: Generation of deep learning based synthetic biometric data[3]
  - **Authors**: Pankaj Bamoriya and Gourav Siddhad and Harkeerat Kaur and Pritee Khanna and Aparajita Ojha
  - **Year of publication**: 2022
  - **Abstract**:

    Abstract

    Deep learning-based generative networks have brought a significant change in the generation of synthetic biometric data. Synthetic biometric data finds applications in developing biometric systems and testing them on a large amount of data to analyze their performance on extreme load scenarios or run simulation for health care personnel training. Generally, biometric datasets have fewer training samples, due to which deep learning models do not train well. In the proposed DSB-GAN, a generative model based on convolutional autoencoder (CAE) and generative adversarial network (GAN) is used to generate realistic synthetic biometrics for various modalities such as fingerprint, iris, and palmprint. This generated data ensures the availability of data that is not available in general due to various undesired factors like distortion and corruption of data. The model is resource efficient and generates diverse biometric samples as compared to state-of-the-art methods.

- **Title**: PrintsGAN: Synthetic Fingerprint Generator[4]
  - **Authors**: Engelsma, Joshua James and Grosz, Steven and Jain, Anil K.
  - **Year of publication**: 2023
  - **Abstract**:

    Abstract

    A major impediment to researchers working in the area of fingerprint recognition is the lack of publicly available, large-scale, fingerprint datasets. The publicly available datasets that do exist contain very few identities and impressions per finger. This limits research on a number of topics, including e.g., using deep networks to learn fixed length fingerprint embeddings. Therefore, we propose PrintsGAN, a synthetic fingerprint generator capable of generating unique fingerprints along with multiple impressions for a given fingerprint. Using PrintsGAN, we synthesize a database of 525k fingerprints (35K distinct fingers, each with 15 impressions). Next, we show the utility of the PrintsGAN generated dataset by training a deep network to extract a fixed-length embedding from a fingerprint. In particular, an embedding model trained on our synthetic fingerprints and fine-tuned on a small number of publicly available real fingerprints (25K prints from NIST SD 302) obtains a TAR of 87.03% @ FAR=0.01% on the NIST SD4 database (a boost from TAR=73.37% when only trained on NIST SD 302). Prevailing synthetic fingerprint generation methods do not enable such performance gains due to i) lack of realism or ii) inability to generate multiple impressions per finger.

- **Title**: Fingerprint generation and authentication though Adaptive convolution generative adversarial network (ADCGAN)[11]

  - **Authors**: Mustafa, Syed Muhammad Nabeel and Zehra, Syeda Sundus and Baber, Alina and Siddiqui, Maria Andleeb
  - **Year of publication**: 2023
  - **Abstract**:

    Abstract

    Fingerprints are crucial in identification of humans. The uniqueness of finger prints makes it an interesting subject. Fingerprints are termed as a technique used to define, assess, and quantify a person's physical and behavioral property. Deep learning has made its application in all the major fields such as natural language processing, computer vision and speech processing. Deep learning has also found its application in the important subject of fingerprint synthesis and biometric. The ever-growing complexity of fingerprint authentication issues, from cellphone authentication to airport security systems, seems to be best handled by these models. In recent years, deep learning-based models have been used more and more to raise the accuracy of various fingerprint recognition systems. The persuasive capacity of Generative Adversarial Networks (GANs) to generate believable instances can be credibly taken from an existing distribution of samples. GAN exhibits exceptional performance on data generation-based tasks and also encourages study in privacy and security. In this work, using Adaptive Deep Convolution Generative Adversarial Networks (ADCGAN), we develop a model that generates and authenticate the fingerprints. A Socofing dataset was trained on ADGAN model. The model gave 92% accuracy. The conduct of fingerprint research has been made possible due to ADGAN, without restrictions related to the confidential nature of biometric data.

- **Title**: Universal Fingerprint Generation: Controllable Diffusion Model With Multimodal Conditions[5]

  - **Authors**: Grosz, Steven A. and Jain, Anil K.
  - **Year of publication**: 2025

  - **Abstract**:

    Abstract

    The utilization of synthetic data for fingerprint recognition has garnered increased attention due to its potential to alleviate privacy concerns surrounding sensitive biometric data. However, current methods for generating fingerprints have limitations in creating impressions of the same finger with useful intra-class variations. To tackle this challenge, we present GenPrint, a framework to produce fingerprint images of various types while maintaining identity and offering humanly understandable control over different appearance factors, such as fingerprint class, acquisition type, sensor device, and quality level. Unlike previous fingerprint generation approaches, GenPrint is not confined to replicating style characteristics from the training dataset alone: it enables the generation of novel styles from unseen devices without requiring additional fine-tuning. To accomplish these objectives, we developed GenPrint using latent diffusion models with multimodal conditions (text and image) for consistent generation of style and identity. Our experiments leverage a variety of publicly available datasets for training and evaluation. Results demonstrate the benefits of GenPrint in terms of identity preservation, explainable control, and universality of generated images. Importantly, the GenPrint-generated images yield comparable or even superior accuracy to models trained solely on real data and further enhances performance when augmenting the diversity of existing real fingerprint datasets.

- **Title**: DiffFinger: Advancing Synthetic Fingerprint Generation through Denoising Diffusion Probabilistic Models[12]

  - **Authors**: Freddie Grabovski and Lior Yasur and Yaniv Hacmon and Lior Nisimov and Stav Nimrod

  - **Year of publication**: 2024

  - **Abstract**:

    Abstract

This study explores the generation of synthesized fingerprint images using DDPMs. The significant obstacles in collecting real biometric data, such as privacy concerns and the demand for diverse datasets, underscore the imperative for synthetic biometric alternatives that are both realistic and varied. Despite the strides made with Generative Adversarial Networks (GANs) in producing realistic fingerprint images, their limitations prompt us to propose DDPMs as a promising alternative. DDPMs are capable of generating images with increasing clarity and realism while maintaining diversity. Our results reveal that DiffFinger not only competes with authentic training set data in quality but also provides a richer set of biometric data, reflecting true-to-life variability. These findings mark a promising stride in biometric synthesis, showcasing the potential of DDPMs to advance the landscape of fingerprint identification and authentication systems.

Chapter 3

Results

After data selection and extraction are complete, the information acquired can be utilized to address the research questions.

3.1 Q1: How can high quality synthetic fingerprints be obtained?

3.1.1 Variational Auto-Encoders

The two key components of the sophisticated generative model called the VAE are the encoder and the decoder. The encoder is responsible for converting input data, including images, into a lower-dimensional, typically fixed-size latent space. This latent space serves as a condensed representation of the incoming data, capturing its essential features. The encoder additionally produces two vectors for each input: the variance and mean of the latent space distribution. Because these vectors are used to sample points in the latent space, a random element is introduced, making VAEs probabilistic models. The decoder, on the other hand, takes these sampled points from the latent space and utilizes them to create synthetic data that closely resembles the original input.

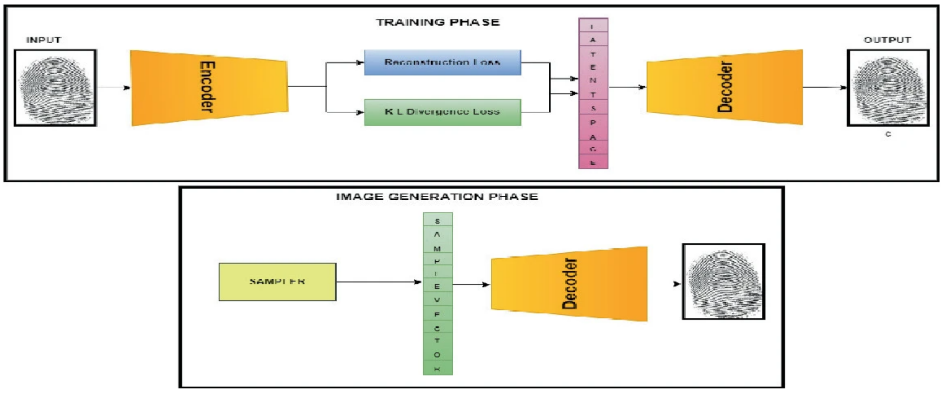


Figure 3.1: Variational auto-encoder-based synthetic fingerprint generation. From [1].

The re-parametrization tirck, which addresses the issue of back-propagating gradients by sampling, represents a significant advancement in the training of VAEs. The encoder network in a VAE generates the mean and log variance of a latent distribution. Instead of directly sampling from this distribution, which is a non-differentiable process, re-parametrization offers a clear stochastic component. To generate a point in the latent space, it takes a sample from a typical normal distribution and adds it to the mean and standard deviation it received from the encoder. By effectively separating the stochastic from the model's parameters, this technique simplifies the computation of gradients during back-propagation.

Reconstruction loss and Kullback-Leibler (KL) divergence loss are the two loss functions used for the VAE's training and testing (a simple graphic representation in Figure 3.1. The discrepancy between the input data and the VAE outputs is measured by the reconstruction loss. The product of the input data's dimensions is used to scale the reconstruction loss.

$$\text{reconstruction\_loss} = \text{MSE}(inputs, outputs) \times \text{input\_shapes} \tag{3.1}$$

where

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \tag{3.2}$$

and denotes the actual or observed value for the i-th data point, the predicted value for the i-th data point, and n is the number of data points. Reconstructing input data accurately and regularizing the latent space distribution are two goals that are combined in KL divergence loss, which penalizes the divergence between the learned latent distribution and a standard normal distribution.

$$\text{kl\_loss} = -0.5 \times \sum \left(1 + \text{z\_log\_var} - \left(z_{mean} - \exp(\text{z\_log\_var})\right)^2\right) \tag{3.3}$$

The final loss value of the VAE is calculated as:

$$\text{vae\_loss} = \text{mean}(B \times \text{reconstruction\_loss} + \text{kl\_loss}) \tag{3.4}$$

The outcomes described in [1] shows that the trade-off between reconstruction accuracy and latent space diversity in VAEs frequently results in generated samples that lack fine features or are fuzzy. The creation of realistic, high-fidelity results is hampered by this intrinsic uncertainty.

3.1.2 Vikriti-ID

Vikriti-ID breaks down the synthesis into multiple phases, each of which focuses on modeling differences between classes, as opposed to immediately mapping random signals to fingerprints using a single GAN. Vikriti-ID creates an intermediate picture using VAE, which serves as the pipeline's starting point. Lastly, it creates a unique ID by simulating the impact of a real fingerprint using the Vikriti-ID GAN. Lastly, several realistic-looking impressions of this generated UniqueID are produced using the Vikriti-ID Impression generator.

The method suggested in [2] creates realistic-looking fingerprints by following a series of stages (Figure 3.2 and Figure 3.3). The following is a summary of the steps:

- VAEs are used for intermediate image generation from a noise matrix MN.

- Generation of a unique fingerprint identity with the proposed Vikriti-ID.

- The last step employs the module of an impression generator (IG) to generate various modules of the unique fingerprint identity.

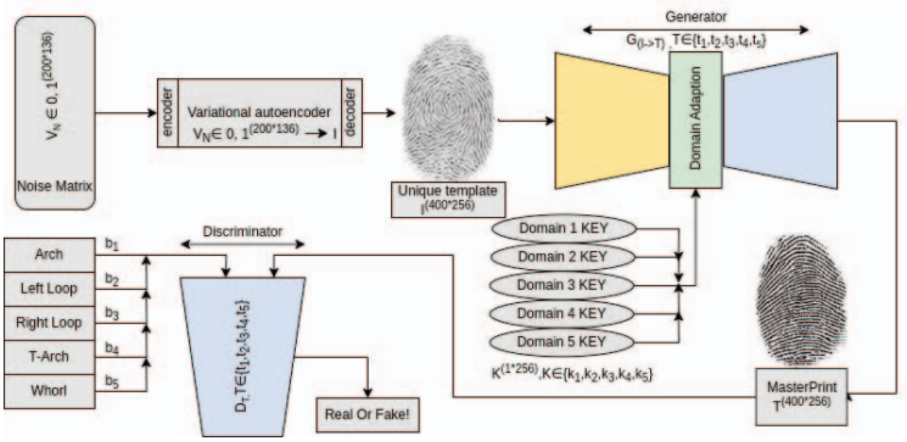


Figure 3.2: Training process of Vikriti-ID (Taking input as an random matrix and generating intermediate image by variational auto-encoder, which passes to generator model to generate unique identity with the help of discriminator). From [2].

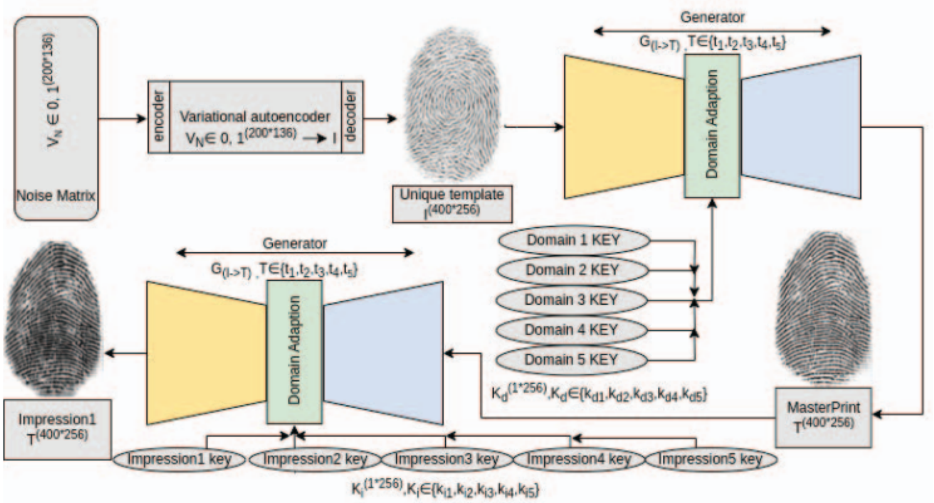


Figure 3.3: Illustration of Vikrit-ID generating impressions from the random noise matrix. From [2].

3.1.3 Deep leaning based Synthetic Biometric GAN (DSB-GAN)

In the DSB-GAN framework[3], a Class Attention Encoder (CAE) is employed to generate augmented biometric data from modalities like fingerprints, palmprints, and irises. The CAE produces biometric samples that mimic original data, which, along with artificial samples from the DSB-GAN generator, is combined with original biometric samples for training. This method enhances the dataset size, improving accuracy in generating synthetic biometric samples, which remain similar yet diverse compared to originals. The DSB-GAN is characterized as lightweight and effectively leverages both original and augmented data for enhanced training outcomes. The flowchart of the proposed method is shown in Figure 3.4

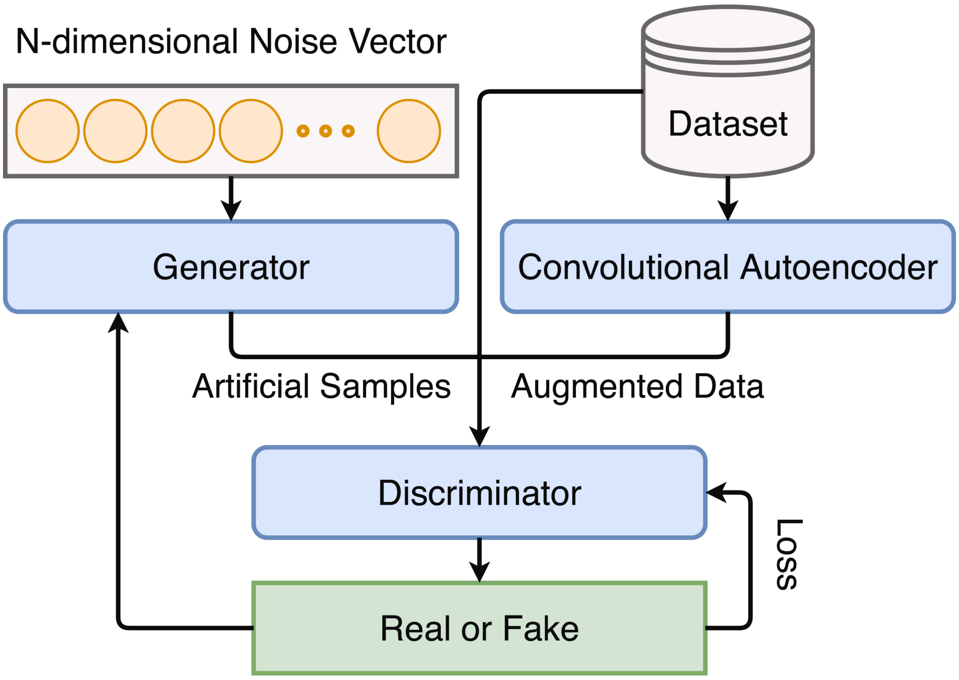
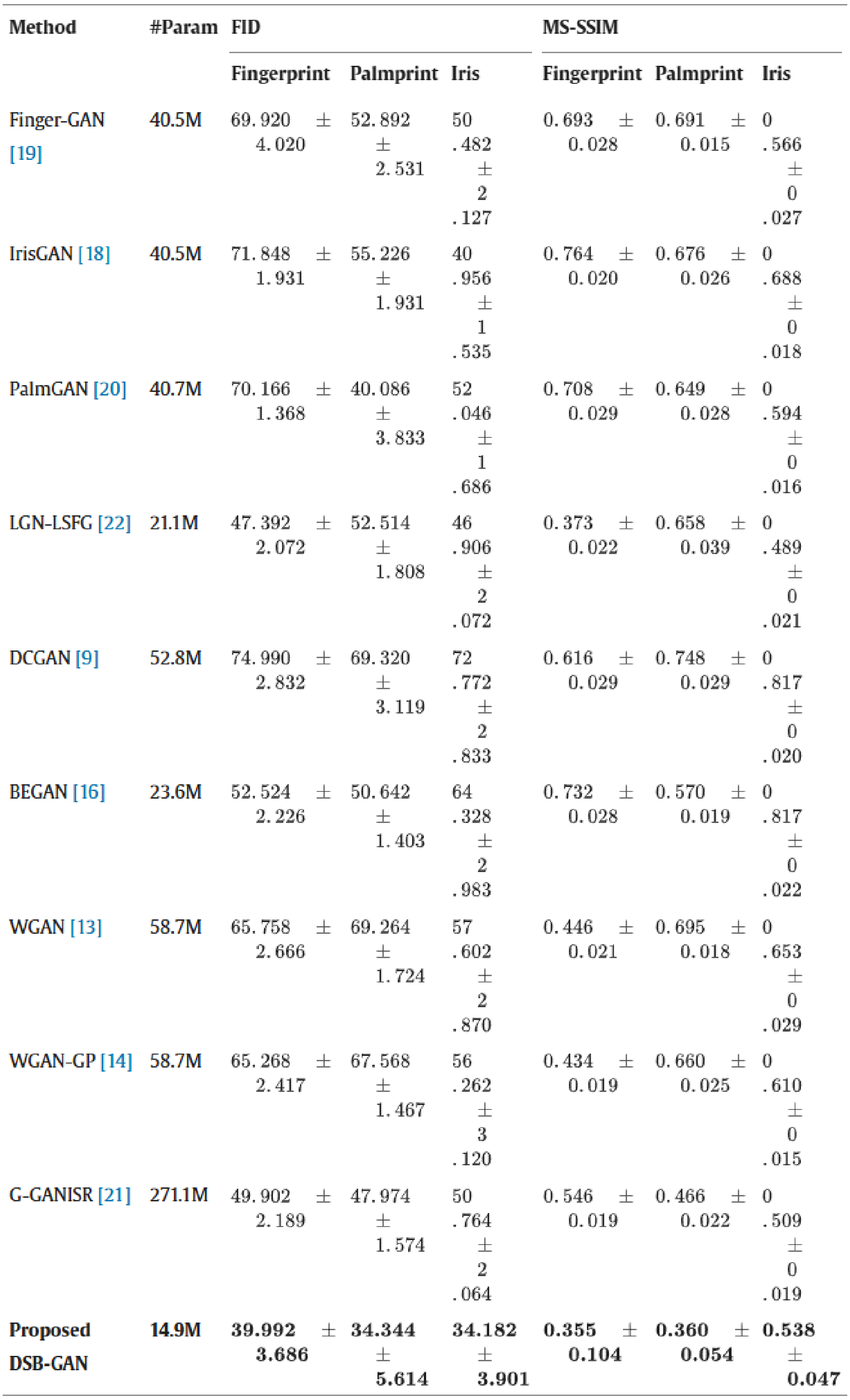


Figure 3.4: DSB-GAN method flowchart. From [3].



Method	#Param	FID			MS-SSIM		
		Fingerprint	Palmprint	Iris	Fingerprint	Palmprint	Iris
Finger-GAN [19]	40.5M	69.920 ± 4.020	52.892 ± 2.531	50.482 ± 2.127	0.693 ± 0.028	0.691 ± 0.015	0.566 ± 0.027
IrisGAN [18]	40.5M	71.848 ± 1.931	55.226 ± 1.931	40.956 ± 1.535	0.764 ± 0.020	0.676 ± 0.026	0.688 ± 0.018
PalmGAN [20]	40.7M	70.166 ± 1.368	40.086 ± 3.833	52.046 ± 1.686	0.708 ± 0.029	0.649 ± 0.028	0.594 ± 0.016
LGN-LSFG [22]	21.1M	47.392 ± 2.072	52.514 ± 1.808	46.906 ± 2.072	0.373 ± 0.022	0.658 ± 0.039	0.489 ± 0.021
DCGAN [9]	52.8M	74.990 ± 2.832	69.320 ± 3.119	72.772 ± 2.833	0.616 ± 0.029	0.748 ± 0.029	0.817 ± 0.020
BEGAN [16]	23.6M	52.524 ± 2.226	50.642 ± 1.403	64.328 ± 2.983	0.732 ± 0.028	0.570 ± 0.019	0.817 ± 0.022
WGAN [13]	58.7M	65.758 ± 2.666	69.264 ± 1.724	57.602 ± 2.870	0.446 ± 0.021	0.695 ± 0.018	0.653 ± 0.029
WGAN-GP [14]	58.7M	65.268 ± 2.417	67.568 ± 1.467	56.262 ± 3.120	0.434 ± 0.019	0.660 ± 0.025	0.610 ± 0.015
G-GANISR [21]	271.1M	49.902 ± 2.189	47.974 ± 1.574	50.764 ± 2.064	0.546 ± 0.019	0.466 ± 0.022	0.509 ± 0.019
Proposed DSB-GAN	**14.9M**	**39.992** ± **3.686**	**34.344** ± **5.614**	**34.182** ± **3.901**	**0.355** ± **0.104**	**0.360** ± **0.054**	**0.538** ± **0.047**

Figure 3.5: DSB-GAN as compared with other GANs in terms of quantitative parameters (at 95% confidence interval). From [3].

Two metrics — the multi-scale structural similarity index (MS-SSIM) and the Fréchet inception distance (FID) — have been used to assess the DSB-GAN's performance. The resulting images' quality is assessed using the FID metric. An improved version of SSIM called MS-SSIM is used to measure perception or structural data at different scales. It falls between 0 and 1, with 1 representing perfect structural similarity. Here, a low FID indicates that the images produced are similar to the original samples, while a low MS-SSIM indicates that the samples produced by DSB-GAN are diverse and highly variable. As we can see in Table 3.5, this approach obtains better performance than other GANs with less parameters.

3.1.4 PrintsGAN

PrintsGAN[4] synthesizes fingerprints through multiple steps. Firstly, a binary Master-Print $I_{ID} \in \{0;1\}^{256\times256}$ is generated using a random noise vector $z_{ID} \in \mathbb{R}^{512}$, where z is drawn from a continuous uniform distribution $U(0,1)$ to create a new fingerprint identity. In Figure 3.6. Next, I_{ID} along with a warping noise vector $z_{distort} \in \mathbb{R}^{16}$ is passed to a non-linear Thin-Plate-Spline (TPS) warping module and cropping GAN $D_W(E_W(I_{ID}))$ to produce a warped Master-Print I_w. Finally, I_w is passed to a renderer $R_D(R_E(I_w))$ along with a texture noise vector $z_{texture} \in \mathbb{R}^{128}$ to impart textural details to the final fingerprint I_r. Thus, by selecting different z_{ID}, it can generate many unique fingerprints. Likewise, by fixing z_{ID}, and selecting different $z_{distort}$ and $z_{texture}$, it can generate different impressions of the same fingerprint. Each of these steps are elaborated upon in the subsections below.

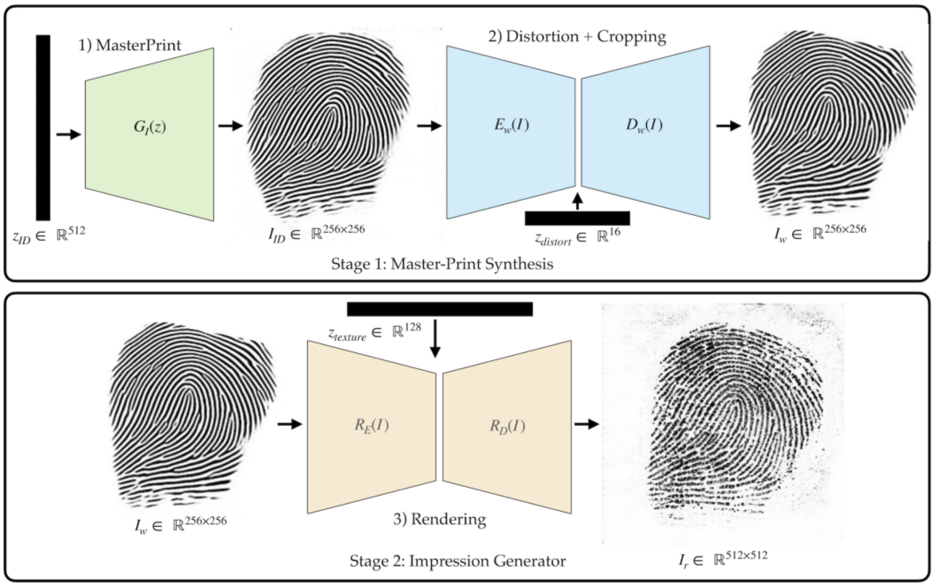

1) MasterPrint
$G_I(z)$
$z_{ID} \in \mathbb{R}^{512}$
$I_{ID} \in \mathbb{R}^{256\times256}$
2) Distortion + Cropping
$E_w(I)$
$D_w(I)$
$z_{distort} \in \mathbb{R}^{16}$
$I_w \in \mathbb{R}^{256\times256}$
Stage 1: Master-Print Synthesis
$z_{texture} \in \mathbb{R}^{128}$
$R_E(I)$
$R_D(I)$
$I_w \in \mathbb{R}^{256\times256}$
3) Rendering
Stage 2: Impression Generator
$I_r \in \mathbb{R}^{512\times512}$

Figure 3.6: Schematic of PrintsGAN. It operates in two stages. In the first stage, a Master-Print, or a new identity is generated. A Master-Print is a binarized friction ridge pattern at 250 ppi. After synthesizing a Master-Print, it is passed to a non-linear warping and cropping module to simulate the effects of pressing the finger against a fingerprint reader platen at different roll, pitch, yaw, and degree of pressure. Finally, this warped and cropped Master-Print is passed to the second stage of the synthesis process where it is rendered with realistic textural details at 500 ppi. By passing different identity noise z_{ID}, distortion noise $z_{distort}$, and texture noise ($z_{texture}$), PrintsGAN is able to generate many fingerprint identities as well as impressions for each identity. In this way, PrintsGAN models both the inter-class and intra-class variance of a large fingerprint database. From [4].

In the first step in the synthesis process the GAN is trained in accordance with the classic adversarial loss:

$$\mathcal{L}_{adv}(G_I, Disc_{ID}) = \mathbb{E}_x\left[logDisc_{ID}(x)\right] \quad + \mathbb{E}_z\left[log(1 - Disc_{ID}(G_I(z)))\right] \tag{1}$$

where x is a binary fingerprint extracted from a real fingerprint.

Given a raw fingerprint I_{raw}, it uses an auto-encoder $R(\cdot)$ to learn a mapping from I_{raw} to a ground-truth binarized fingerprint I_{binary} via an L-2 loss function:

$$\mathcal{L}_{recon} = |R(I_{raw}) - I_{binary}|_2^2. \tag{2}$$

3.1.5 DiffFinger

The DiffFinger model presented in [12] is based on classic DDPM architecture, but to create different fingerprint impressions the authors exploited the capabilities of their DDPM in a unique manner.

The goal of DiffFinger generative process was to produce sets of fingerprints that represent the same identity notwithstanding their differences. To do this, the approach makes use of DDPM's backward diffusion process in a novel way. Initializing an image that is solely noise-based is the first step in the process. This image is then partially denoised up to a certain time step *d*, at which point they pause before moving on to the final reconstruction process. This intermediate image creates a distinct fingerprint identification even though it is still partially veiled by noise. Then the denoising procedure from *t=d* to *t=0* repeated in order to produce several impressions of this identity. Because the DDPM is stochastic, every cycle produces a slightly different image, resulting in variations of the same fingerprint identification.

The advantagies of the proposed DDPM-based approach for fingerprint generation compared to the limitations of GANs can be seen below:

- Overcoming Mode Collapse: Ensuring diverse and realistic fingerprint production is a crucial component of the process. Nevertheless, mode collapse can occur with GANs, causing them to primarily produce samples from particular areas of the distribution of training data. On the other hand, because of their noise-driven training procedure, DDPMs naturally prevent mode collapse.

- Enhancing Realism and Capturing Variability: Creating fingerprints with a high degree of realism and reflecting the inherent diversity of real-world data is another crucial necessity. By iteratively improving noise under the guidance of the learnt data distribution, DDPMs excel in this area. This produces statistically comparable samples that are more realistic, especially when it comes to minute characteristics like ridges. DDPMs are better at modeling these fine-grained characteristics than GANs, which results in the creation of more varied and lifelike fingerprints.

- Potential for Explainability: In machine learning models, explainability is becoming more and more important. DDPMs' intrinsic diffusion process presents a special opportunity to comprehend the model's decision-making. We may learn more about the variables affecting the produced fingerprints by examining the noise prediction and removal processes.

3.1.6 GenPrint

Using weights from the Diffusers library, GenPrint[5] is a multimodal latent diffusion model optimized for fingerprint generation from a pretrained Stable Diffusion model (v1.5). To put it succinctly, this study's contributions are as follows:

- GenPrint is a customizable latent diffusion model that generates a wide variety of realistic-looking synthetic fingerprints by utilizing text and image circumstances.
- Without any further fine-tuning (e.g., zero-shot fingerprint style generation), GenPrint may generate fingerprints of any acquisition type, sensor, fingerprint class, and quality, including fingerprint styles that were not observed during training.
- With language cues that are easy for humans to understand, the generating process is explicable and controllable (in terms of look and identity retention).

Following, the elements that compose the pipeline of GenPrint (visible in Figure 3.7) and that are described carefully in [5]:

- **Control Factors via Text Conditions**: Acquiring a sizable corpus of fingerprint photos and related text descriptions is the first stage in optimizing Stable Diffusion for text to fingerprint synthesis. The low-rank adaptation (LoRA) strategy was adopted for more efficient training.
- **Zero-Shot Style Generation**: Specifically, they embed style embeddings for every training image using a pretrained VGG model that was trained on ImageNet. Cross-attention layers are utilized to inject these style embeddings into the diffusion model. These layers are decoupled from the textual embeddings that regulate the explainable style components, meaning they have their own cross-attention layers.

- **Fingerprint Identity Preservation**: The silhouettes of the ridge flow patterns that give birth to the relative orientation of each finger's minutiae points are the identity discriminative aspects of fingerprints that remain constant across a variety of acquisition and sensor types. With the adjustment of pre-pending a pre-trained ridge extraction module as the initial layers of our identity preserving diffusion model, ID-Net, they propose that ControlNet[13] is a good option for implementing the DDPM model with identity preservation of the fingerprint ridges. The input fingerprint control image is stripped of sensor-dependent and other style elements by these layers, leaving only the ridge pattern silhouette image to direct the spatial preservation of the fingerprint identification.

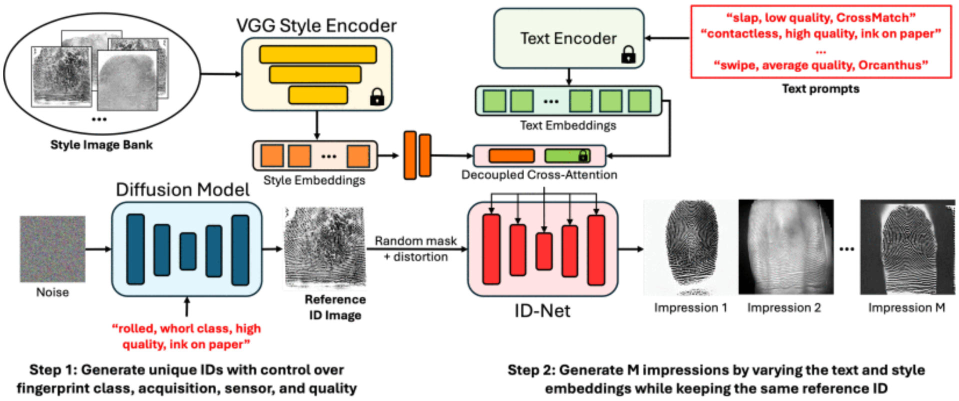

VGG Style Encoder
Text Encoder
"slap, low quality, CrossMatch"
"contactless, high quality, ink on paper"
...
"swipe, average quality, Orcanthus"
Text prompts
Text Embeddings
Style Image Bank
Style Embeddings
Decoupled Cross-Attention
Diffusion Model
Noise
Reference ID Image
Random mask + distortion
ID-Net
Impression 1
Impression 2
Impression M
"rolled, whorl class, high quality, ink on paper"
Step 1: Generate unique IDs with control over fingerprint class, acquisition, sensor, and quality
Step 2: Generate M impressions by varying the text and style embeddings while keeping the same reference ID

Figure 3.7: Overview of the architecture and generation process of GenPrint. GenPrint consists of a two-stage generation process. In the first stage, a reference identity (ID) fingerprint image is generated from a random noise vector and an input text prompt controlling the quality, class, acquisition, and sensor type of the generated fingerprint by a fine-tuned Stable Diffusion model. The second stage then generates M impressions of that reference ID fingerprint via ID-Net, a trained ControlNet model which removes the style characteristics of the input reference ID image and replaces the style with the supplied text prompts and/or style embeddings from M reference style images/prompts. During training, the weights of the VGG Style Encoder, Text Encoder, and the decoupled cross-attention layers of the text embeddings are kept frozen, denoted by the lock symbol in the figure. From [5].

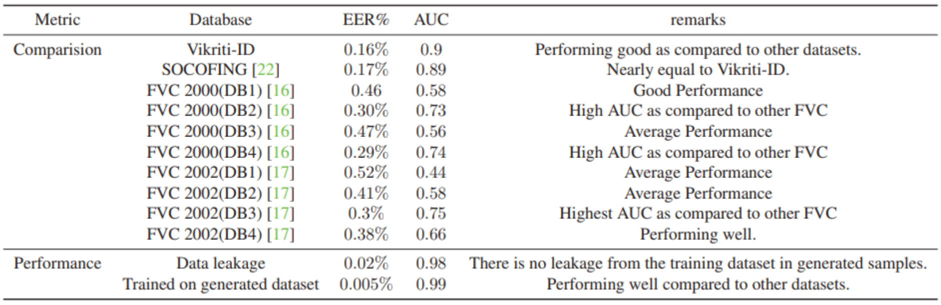
There are two steps in the entire GenPrint generating pipeline. First, a random noise vector is utilized to create entire (i.e., rolled) fingerprint images of different fingerprint classes using the optimized stable diffusion model. While the specific sensor type and fingerprint class patterns can be randomly sampled to increase diversity in the generated dataset, the key component of the text prompt in stage one is that they only include high quality rolled images so that the model has the complete fingerprint ridge pattern to work with in the second stage.

Because the ControlNet component of the ID-Net model would alter the input fingerprint pattern provided as the ControlNet input, it would not result in true non-linear distortions to the output photos. In order to apply realistic distortion grids to the ControlNet image for every generation, they are randomly sampled. By calculating the minute displacements between real fingerprint pairs in the training dataset, these realistic distortion grids are produced. An example distortion grid is sampled and applied to the input reference image during inference. This grid is indexed by the designated fingerprint acquisition type.

3.2 Q2: What benefits does SFG provide in the creation of intelligent systems?

In this section, different data are provided to demonstrate the benefits derived from SFG in the construction of intelligent systems.

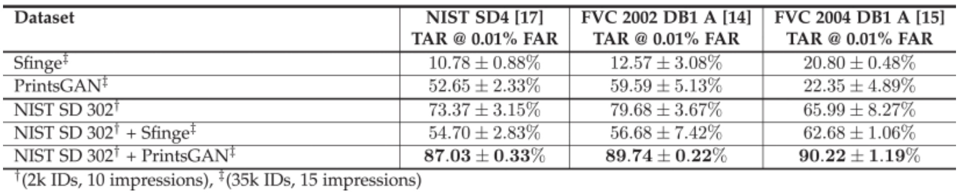
Starting by presenting the performance obtained by the deep network model[2], trained on Vikriti-ID data and publicly available datasets, which achieved an impressive EER, between False Match Rate (FMR) and False Non-Match Rate (FNMR), of 0.16% and AUC of 0.9, as shown in Table 3.8, demonstrating a very good usability. The generated dataset is used for the training of the model and the real one for the fine-tuning.



Metric	Database	EER%	AUC	remarks
Comparision	Vikriti-ID	0.16%	0.9	Performing good as compared to other datasets.
	SOCOFING [22]	0.17%	0.89	Nearly equal to Vikriti-ID.
	FVC 2000(DB1) [16]	0.46	0.58	Good Performance
	FVC 2000(DB2) [16]	0.30%	0.73	High AUC as compared to other FVC
	FVC 2000(DB3) [16]	0.47%	0.56	Average Performance
	FVC 2000(DB4) [16]	0.29%	0.74	High AUC as compared to other FVC
	FVC 2002(DB1) [17]	0.52%	0.44	Average Performance
	FVC 2002(DB2) [17]	0.41%	0.58	Average Performance
	FVC 2002(DB3) [17]	0.3%	0.75	Highest AUC as compared to other FVC
	FVC 2002(DB4) [17]	0.38%	0.66	Performing well.
Performance	Data leakage	0.02%	0.98	There is no leakage from the training dataset in generated samples.
	Trained on generated dataset	0.005%	0.99	Performing well compared to other datasets.

Figure 3.8: Comparison of performance between Vikriti-ID and other publicly available datasets using MCC matcher. From [2].

Another example of authentication accuracy increment achieved pre-training the model on synthetically generated dataset and fine-tining it on real ones can be seen in Table 3.9.



Dataset	NIST SD4 [17] TAR @ 0.01% FAR	FVC 2002 DB1 A [14] TAR @ 0.01% FAR	FVC 2004 DB1 A [15] TAR @ 0.01% FAR
Sfinge[‡]	10.78 ± 0.88%	12.57 ± 3.08%	20.80 ± 0.48%
PrintsGAN[‡]	52.65 ± 2.33%	59.59 ± 5.13%	22.35 ± 4.89%
NIST SD 302[†]	73.37 ± 3.15%	79.68 ± 3.67%	65.99 ± 8.27%
NIST SD 302[†] + Sfinge[‡]	54.70 ± 2.83%	56.68 ± 7.42%	62.68 ± 1.06%
NIST SD 302[†] + PrintsGAN[‡]	**87.03 ± 0.33%**	**89.74 ± 0.22%**	**90.22 ± 1.19%**

[†](2k IDs, 10 impressions), [‡](35k IDs, 15 impressions)

Figure 3.9: Authentication accuracy comparative using different training sets. From [4].

By augmenting training datasets with synthetic fingerprints from PrintsGAN[4], the authentication performance and identification accuracy of deep network models improved significantly. A comparison of a DeepPrint model trained only on NIST SD 302 data against one pretrained on PrintsGAN images (Figure 3.10) showed an increase in closed-set identification accuracy. The model combining NIST SD 302 and PrintsGAN achieved a rank 1 identification rate of 92.05%, up from 85.90% with NIST SD 302 alone. Additionally, using 100k synthetic fingerprints from PrintsGAN for gallery augmentation yielded performance comparable to that of using 100k real fingerprints, confirming the utility of synthetic prints for large-scale fingerprint recognition benchmarking.

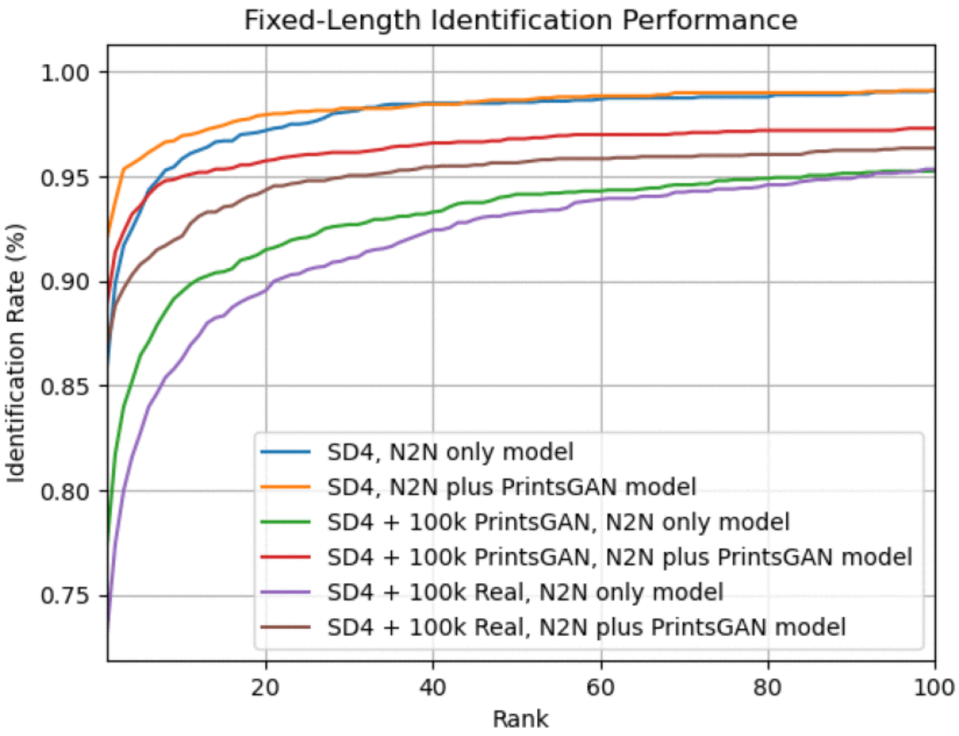


Figure 3.10: Closed-set identification accuracy of DeepPrint models trained on NIST SD 302 (N2N) data only versus. NIST SD 302 (N2N) + PrintsGAN data. The various curves shown are comparing the search performance of these two models on i.) SD4, ii.) SD4 augmented with 100k Real fingerprint images, and iii.) SD4 augmented with 100k PrintsGAN fingerprints. Best viewed in color. From [4].

Now we analyze the most recent SFG present in the literature, GenPrint[5]. The authors used a pre-trained AFR-Net[14] fingerprint recognition model to calculate authentic and impostor score distributions for both the test split of NIST SD302 and the dataset generated by GenPrint. The results are displayed in Figure 3.11, which illustrates how the score distributions of the generated and real datasets are identical. Since NIST SD302 includes several of the various acquisition types (rolling, slap, and contactless) that GenPrint is taught to do, we selected it for this comparison. The overlap in the distributions when compared to the actual fingerprint dataset shows how realistic GenPrint-generated photos are. The real and synthetic datasets' identification performance is likewise quite similar, confirming the identity retention of later synthetic photographs of the same finger that provide high genuine and low impostor similarities.

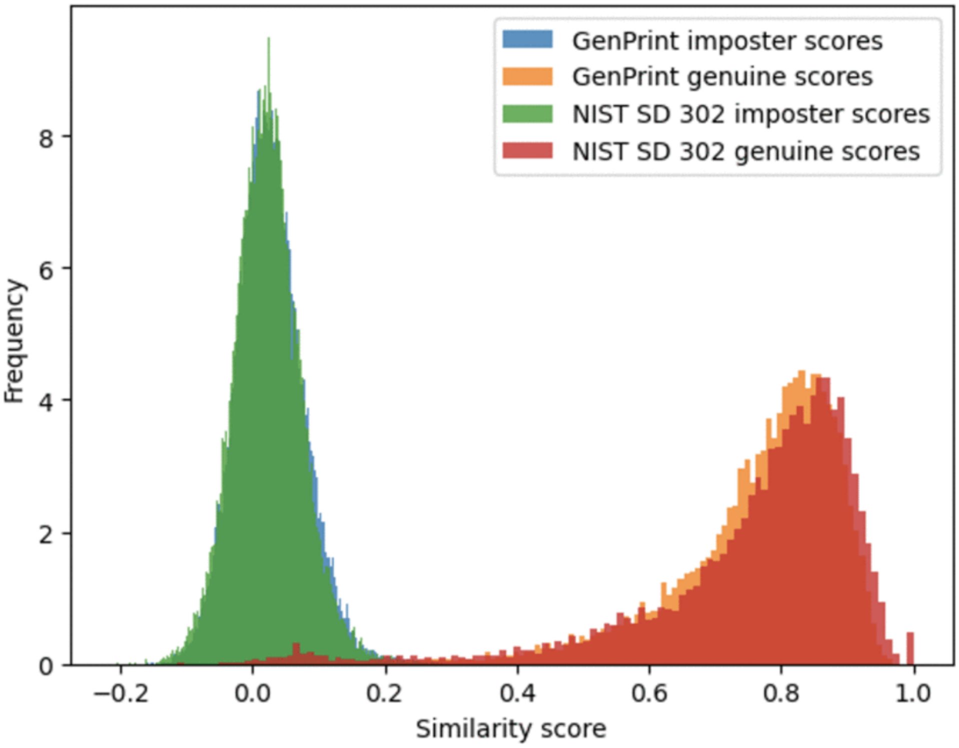
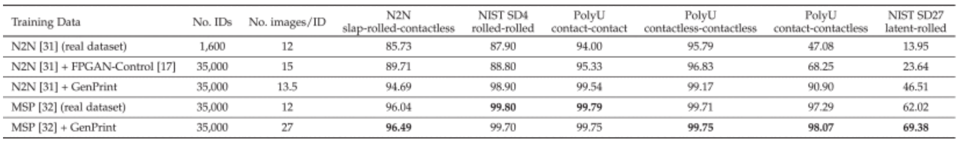


Figure 3.11: AFR-Net similarity score distributions for NIST SD302 real dataset and similar GenPrint dataset. From [5].

GenPrint is trained to accommodate via text prompts, including control over the fingerprint class, acquisition, sensor, and quality level, providing a high control degree over fingerprint generation.

Moreover, the ability of synthetic fingerprint generators to train fingerprint recognition models is one of the most crucial standards for their quality. The authors assess GenPrint's usefulness both when training only on artificially created images and when adding synthetic data to a collection of real fingerprints. As baselines, they compare with a number of earlier synthetic fingerprint generators, such as SFinGe, PrintsGAN, and FPGAN-Control. In Table 3.12 are presented the accuracy scores obtained by ResNet50[15] with True Acceptance Rate (TAR) and False Acceptance Rate (FAR) set to 0.1%, trained on dataset augmented using different generators. Figure 3.13 displays the outcome of adding GenPrint impressions to MSP[16]. The graphs demonstrate that GenPrint does, in fact, greatly enhance performance by increasing the diversity of the pre-existing fingerprint photos as the number of identities rises. This gain is especially noticeable when the test datasets include sensor characteristics (such contactless and latent fingerprints) that GenPrint can synthesize but were not present in the original MSP dataset.



Training Data	No. IDs	No. images/ID	N2N slap-rolled-contactless	NIST SD4 rolled-rolled	PolyU contact-contact	PolyU contactless-contactless	PolyU contact-contactless	NIST SD27 latent-rolled
N2N [31] (real dataset)	1,600	12	85.73	87.90	94.00	95.79	47.08	13.95
N2N [31] + FPGAN-Control [17]	35,000	15	89.71	88.80	95.33	96.83	68.25	23.64
N2N [31] + GenPrint	35,000	13.5	94.69	98.90	99.54	99.17	90.90	46.51
MSP [32] (real dataset)	35,000	12	96.04	**99.80**	**99.79**	99.71	97.29	62.02
MSP [32] + GenPrint	35,000	27	**96.49**	99.70	99.75	**99.75**	**98.07**	**69.38**

Figure 3.12: Authentication Accuracy (TAR At FAR=0.1%) of ResNet50 trained on a combination of real and synthetic data from FPGAN-Control and the proposed GenPrint evaluated on six different test scenarios. From [5].

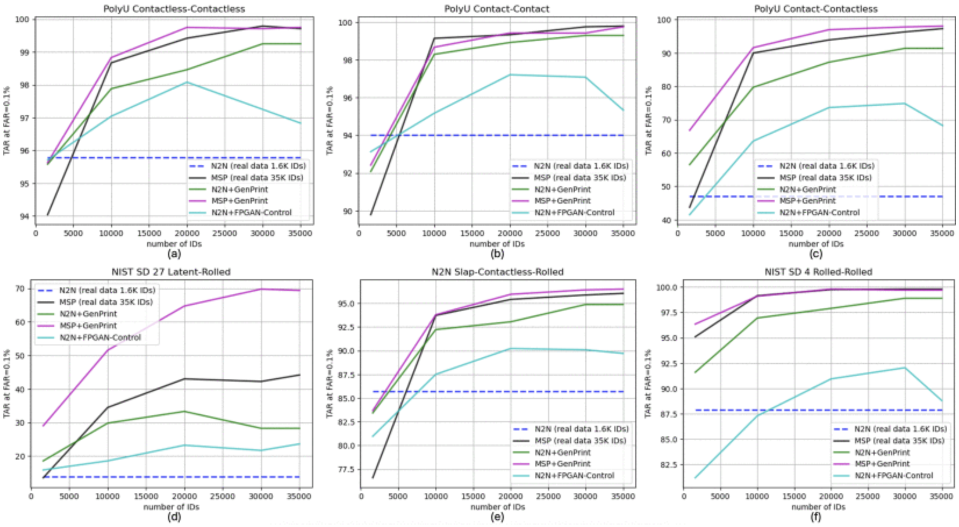


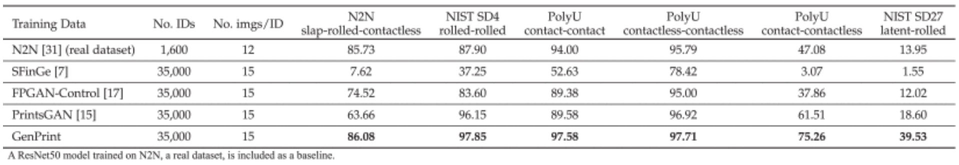
Figure 3.13: Authentication accuracy (TAR at FAR=0.1%) of ResNet50 trained on a combination of real and synthetic data from FPGAN-Control and the proposed GenPrint evaluated on six different test scenarios. From [5].

3.3 Q3: What generalization capabilities a system trained solely on synthetic fingerprints can reach?

In this section only information coming from [5] are riported and analyzed, because in this paper are reported data relative to other approaches of SFG.

In Table 3.14 are presented the authentication accuracy obtained by the same deep neural network trained on different synthetic dataset made up using various generators. It can be noted that GenPrint allows the model to obtain the best performance in the batch, even better than the ones obtained using a real dataset.

It is evident from Figure 3.15 that the recognition model trained on GenPrint images outperforms all baseline synthetic methods and, as the number of synthetic identities increases, even outperforms training on the actual N2N fingerprint dataset.



Training Data	No. IDs	No. imgs/ID	N2N slap-rolled-contactless	NIST SD4 rolled-rolled	PolyU contact-contact	PolyU contactless-contactless	PolyU contact-contactless	NIST SD27 latent-rolled
N2N [31] (real dataset)	1,600	12	85.73	87.90	94.00	95.79	47.08	13.95
SFinGe [7]	35,000	15	7.62	37.25	52.63	78.42	3.07	1.55
FPGAN-Control [17]	35,000	15	74.52	83.60	89.38	95.00	37.86	12.02
PrintsGAN [15]	35,000	15	63.66	96.15	89.58	96.92	61.51	18.60
GenPrint	35,000	15	**86.08**	**97.85**	**97.58**	**97.71**	**75.26**	**39.53**

A ResNet50 model trained on N2N, a real dataset, is included as a baseline.

Figure 3.14: Authentication Accuracy (TAR At FAR=0.1%) of ResNet50 Trained on Synthetic Data from various fingerprint generators including the proposed GenPrint. From [5].

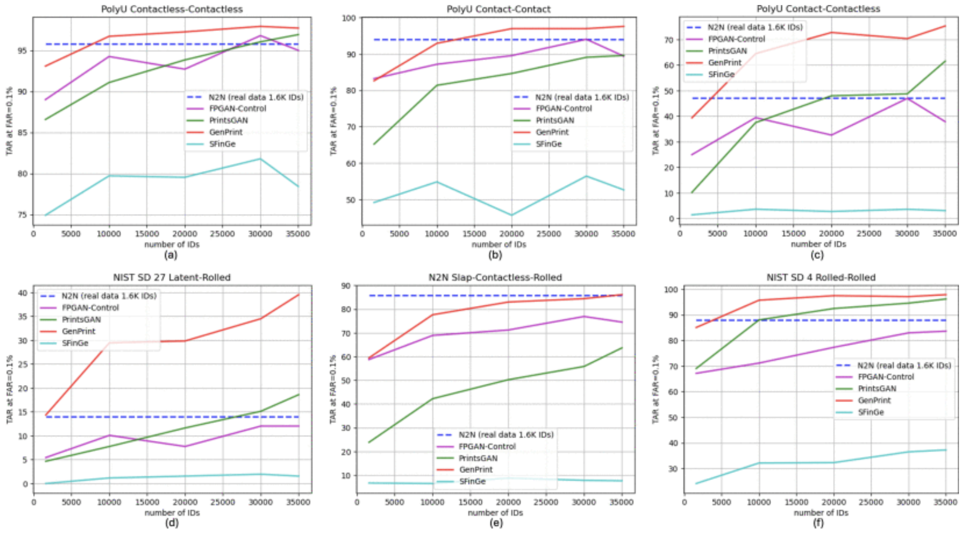


Figure 3.15: Authentication accuracy (TAR at FAR=0.1%) of ResNet50 trained on synthetic data from various fingerprint generation methods including the proposed GenPrint. From [5].

3.4 Q4: Does synthetic generated datasets affect data privacy?

Avoid leakage of data is a key factor when generating synthetic fingerprint because generated samples have to be statistically distinct from real samples, ensuring that the use of synthetic data preserves the privacy of real identities.

In the paper of Vikriti-ID[2] and of GenPrint[5] some measurement of identity leakage are described. The authors of Vikriti-ID calculated match scores between 1000 training fingerprint samples, randomly selected between 50000 samples, and 1000 unique IDs of actual generated database, in order to reduce time and computation load. As reported in Figure 3.8, they got an EER of 0.01%, indicating that the model can preserve the original IDs.

Using a pre-trained AFR-Net fingerprint recognition model, the authors of GenPrint generated 35000 distinct synthetic fingerprint identities and calculated similarity scores to each of the 37351 real training finger IDs in their training dataset in order to gauge the possible identity leaking of their model. Only 10 (0.03%) of these 35000 fake identities got a similarity score with any training identity higher than 0.231, which is the true match criterion calculated on FVC 2002 DB1A at FAR=0.01%. Moreover, the maximum similarity score attained was only 0.297, just marginally above the barrier, even among those 10 similarity values that were above the threshold.

Also for PrintsGAN[4] was made a similar analysis and it was found that only 0.04% of the database has some minimal degree of information leakage.

Chapter 4

Conclusions

Advanced deep learning models are essential for quality: Modern deep learning architectures are the most effective way to create realistic, high-quality synthetic fingerprints. GANs (e.g. PrintsGAN, DSB-GAN) and particularly more recent DDPMs (e.g. GenPrint, DiffFinger) are demonstrated to be more successful than VAEs. In particular, diffusion models effectively overcome typical GAN drawbacks like mode collapse and yield incredibly realistic outcomes.

Novelty and controllability are achievable: The more sophisticated models, like GenPrint, provide substantial, comprehensible control over the generation process. This enables text prompts to be used to provide characteristics such as fingerprint class, quality, and sensor type. A significant benefit is that these models can even produce unique fingerprint patterns that were not observed during training (a process known as "zero-shot style generation").

System performance is significantly improved by synthetic data: As a data augmentation tool, SFG offers enormous advantages. The review demonstrates that pre-training models on synthetic data and fine-tuning them on actual data, or adding synthetic samples to real datasets, results in significant and quantifiable gains in identification performance and authentication accuracy.

Synthetic data enhances model robustness: SFG enables intelligent systems to be trained on a greater range of data than is frequently accessible in real-world datasets by creating large and varied datasets. This enhances the robustness and generalization capabilities of the system, especially when it comes to managing various sensor kinds, acquisition techniques (such contactless and latent), and quality levels.

Synthetic generation effectively preserves privacy: The review finds that the best techniques are successful in protecting privacy, which is a major motivator for SFG. Analyses present in the paper taken into account reveal very little to no identity leakage. The privacy and security issues connected with gathering and utilizing actual biometric data are reduced since the generated fingerprints are statistically different from the genuine identities in the training data.

In conclusion, SFG has demonstrated great potencial when enployed for training intelligent systems for different tasks related to fingerprint, solving data scarsity and variability needings. SFG techniques and their continuous evolution hold promise for practical applications and future research advancements.

Bibliography

[1] Diptadip Maiti, Madhuchhanda Basak, and Debashis Das. Synthetic fingerprint generation: Bridging the gap between privacy and security with variational auto-encoders. In Jagdish Chand Bansal, Samarjeet Borah, Shahid Hussain, and Said Salhi, editors, *Computing and Machine Learning*, pages 221–235, Singapore, 2024. Springer Nature Singapore. ISBN 978-981-97-7571-2. URL https://link.springer.com/chapter/10.1007/978-981-97-7571-2_18.

[2] Rishabh Shukla, Aditya Sinha, Vansh Singh, and Harkeerat Kaur. Vikriti-id: A novel approach for real looking fingerprint data-set generation. In *2024 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, pages 6383–6391, 2024. doi: 10.1109/WACV57701.2024.00627. URL https://ieeexplore.ieee.org/document/10484524.

[3] Pankaj Bamoriya, Gourav Siddhad, Harkeerat Kaur, Pritee Khanna, and Aparajita Ojha. Dsb-gan: Generation of deep learning based synthetic biometric data. *Displays*, 74:102267, 2022. ISSN 0141-9382. doi: https://doi.org/10.1016/j.displa.2022.102267. URL https://www.sciencedirect.com/science/article/pii/S0141938222000865.

[4] Joshua James Engelsma, Steven Grosz, and Anil K. Jain. Printsgan: Synthetic fingerprint generator. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(5):6111–6124, 2023. doi: 10.1109/TPAMI.2022.3204591. URL https://ieeexplore.ieee.org/abstract/document/9893541.

[5] Steven A. Grosz and Anil K. Jain. Universal fingerprint generation: Con-

trollable diffusion model with multimodal conditions. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 47(2):1028–1041, 2025. doi: 10.1109/TPAMI.2024.3486179. URL `https://ieeexplore.ieee.org/abstract/document/10734169`.

[6] European Union. Gdpr. URL `https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng`.

[7] U.S. Department of Health and Human Services. Hipaa. URL `https://www.hhs.gov/hipaa/index.html`.

[8] Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial networks, 2014. URL `https://arxiv.org/abs/1406.2661`.

[9] Diederik P. Kingma and Max Welling. An introduction to variational autoencoders. *Foundations and Trends® in Machine Learning*, 12(4):307–392, 2019. ISSN 1935-8245. doi: 10.1561/2200000056. URL `http://dx.doi.org/10.1561/2200000056`.

[10] Jonathan Ho, Ajay Jain, and Pieter Abbeel. Denoising diffusion probabilistic models, 2020. URL `https://arxiv.org/abs/2006.11239`.

[11] Syed Muhammad Nabeel Mustafa, Syeda Sundus Zehra, Alina Baber, and Maria Andleeb Siddiqui. Fingerprint generation and authentication though adaptive convolution generative adversarial network (adcgan). In *2023 7th International Multi-Topic ICT Conference (IMTIC)*, pages 1–5, 2023. doi: 10.1109/IMTIC58887.2023.10178664. URL `https://ieeexplore.ieee.org/document/10178664`.

[12] Freddie Grabovski, Lior Yasur, Yaniv Hacmon, Lior Nisimov, and Stav Nimrod. Difffinger: Advancing synthetic fingerprint generation through denoising diffusion probabilistic models, 2024. URL `https://arxiv.org/abs/2405.04538`.

[13] Lvmin Zhang, Anyi Rao, and Maneesh Agrawala. Adding conditional control to text-to-image diffusion models, 2023. URL https://arxiv.org/abs/2302.05543.

[14] Steven A. Grosz and Anil K. Jain. Afr-net: Attention-driven fingerprint recognition network, 2022. URL https://arxiv.org/abs/2211.13897.

[15] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition, 2015. URL https://arxiv.org/abs/1512.03385.

[16] Soweon Yoon and Anil K. Jain. Longitudinal study of fingerprint recognition. *Proceedings of the National Academy of Sciences*, 112(28):8555–8560, 2015. doi: 10.1073/pnas.1410272112. URL https://www.pnas.org/doi/abs/10.1073/pnas.1410272112.