PrintVault: Fingerprint Protection by Modifying Templates to Prevent Template Inversion Attacks

Avni Patil

Received May 29, 2025
Accepted September 14, 2025
Electronic access October 31, 2025

Biometric authentication is the new standard for security. The uniqueness of biological data ensures immense integrity within cybersecurity; however, if compromised biometric data can never be reimplemented, unlike passwords, which can be changed. Currently, biometric authentication, specifically with fingerprints, is stored in templates, which are the compact features of the fingerprint. Still, attackers can reconstruct the original fingerprint through a template inversion attack. In this paper, we focus on the prevention of template inversion attacks on fingerprints and propose a novel method through a Generative Adversarial Network (also referred to as GAN). The GAN is trained on a fingerprint dataset of 1000 fingerprint images to add structured noise from a random latent vector. The trained GAN to prevent template inversion attacks in this paper is called PrintVault. The paper proves the principles of obfuscating fingerprint templates to stop template inversion attacks and maintain biometric authentication. We observe the authentication capabilities of PrintVault and the resistance to template inversion attacks. PrintVault introduces a solution to template inversion attacks through its obfuscation with a GAN. Possible applications with biometric authentication and biometric databases provide users with usable, secure fingerprint templates.

Introduction

The Automated Fingerprint Identification System (AFIS) has become widespread as a biometric authentication tool applied at the federal, state, and larger municipal levels. AFIS is a biometric technology that uses digital imaging to store, analyze, and compare fingerprint data to identify individuals, primarily used by law enforcement for criminal investigations and other applications. In like systems, fingerprint features, also referred to as fingerprint templates, are extracted from the fingerprint and stored as reduced-size templates of the characteristic information[1]. During the verification stage, the same characteristic information is extracted from the presented fingerprint and compared to the stored templates. Consequently, fingerprint templates are imperative in fingerprint recognition systems like AFIS to enable secure and accurate identification. Fingerprint authentication strives for security, but has a few key concerns. Biometrics can be misused without consent from the user and are permanently connected to the user; thus, once compromised, all systems that use the biometrics are also compromised.

Template inversion attacks (TIA) on fingerprint recognition systems like AFIS describe an adversary's attempt to reconstruct the original fingerprint from the templates stored in the database. Thus, the adversary can impersonate the user to bypass authentication systems[2]. While recent methods have made progress in preserving authentication accuracy during fingerprint obfuscation, many still face trade-offs between privacy and usability. This work builds on those advancements by further improving the balance between obfuscation strength and recognition performance, as discussed in the Related Works section. However, in this paper, we introduce PrintVault (which is named to reflect its goal of securing fingerprint templates against template inversion attacks), a Fully Connected GAN trained on fingerprint template datasets to perfect the addition of structured noise; thus, effectively preventing template inversion attacks and maintaining authentication accuracy. The GAN, a machine-learning model that creates new data that looks like real data, uses two neural networks–a Generator and a Discriminator. The Generator generates fingerprint images with noise from a latent vector, while the Discriminator tries to distinguish if the generated fingerprint is real. They work in tandem to perfect the GAN algorithm and model. After the model is tuned with the Adam optimization functions and loss functions, the fingerprint images are evaluated using the Structural Similarity Index Metric (SSIM), False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER) to ensure resistance to template inversion attacks and authentication accuracy. The newly generated fingerprint templates must not correlate with the original fingerprint; otherwise, it is susceptible to TIA. In addition, all generated fingerprint templates from the same fingerprint should match with itself to have accurate authentication. The contributions of this paper are concisely as follows:

- Conducted a comprehensive review of biometric security risks, focusing on template inversion attacks and leveraging insights from face template inversion research to address similar threats in fingerprint recognition.

- Designed a Fully Connected GAN (FC-GAN) architecture with carefully chosen layer configurations, activation functions (LeakyReLU/Tanh), and employed the Adam optimizer to generate fingerprint templates that are both obscured and reliably matchable.
- Implemented a preprocessing pipeline including grayscale conversion, resizing, normalization, and binarization to standardize fingerprint images and improve GAN training stability.
- Developed the Generator and Discriminator networks using PyTorch, fine-tuning hyperparameters and training iteratively to maintain a balance between effective template obfuscation and high authentication accuracy.
- Utilized Structural Similarity Index Metric (SSIM), False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER), and fingerprint feature extraction techniques to evaluate that obfuscated templates remain sufficiently dissimilar to originals to prevent inversion while preserving biometric matchability.
- Performed multiple training iterations, investigated failure cases, and refined loss functions and architectural choices to optimize performance and prevent over-transformation that could reduce usability.

The rest of the paper will delve into the related works, proposed method, experimental results, limitations, comparison with related works, ethical considerations, and finally, the conclusion.

Related Works

Fingerprint recognition and authentication are widely used in the world, but their vulnerability to template inversion attacks means biometric data is at risk. Currently, there are several approaches to mitigate the risks. Our work primarily addresses this template-level vulnerability, but it is important to note that biometric data can also be compromised in transit over networks, on-device via malware, or through sensor spoofing.

Network attacks, such as man-in-the-middle attacks and template interception in transit, have been described in prior work and security standards (e.g., ISO/IEC 24745:2022). In addition, malware running on the host device can exfiltrate data before protection mechanisms are enforced. Such attacks require system-level mitigation, such as secure transmission protocols (TLS), trusted platform modules (TPMs), and secure enclaves for on-device processing. These threats are outside the scope of our work but highlight the importance of layered defense for biometric systems.

Recent work proposes a modality-independent cancelable biometric system. Their framework calculates a distance vector between several randomized transformations of the biometric feature vector. Since only inter-transform distances are retained, the approach eliminates template reconstruction risk, providing strong resistance to inversion attacks. Their framework reports Equal Error Rates (EERs) of as low as 1.5% for face and 1.7% for fingerprint, indicating strong recognition performance despite secure transformation requirements[3]. PrintVault proposes a neural network-based obfuscation approach through a GAN framework. Not only does this ensure revocability through on-demand generation of new obfuscated versions, but it also eliminates the requirement of explicit transformation keys, rendering it less susceptible to key-based compromise. In contrast to many previous schemes, PrintVault is formulated to provide high matching accuracy while providing strong resistance to template inversion, harmonizing both usability and security within a single framework.

Another recent contribution is FaceCloak, a lightweight neural network–based framework that safeguards face templates from inversion attacks. FaceCloak generates renewable binary cloaks by combining a face template with a set of positive and negative disruptors. These disruptors are synthesized using noise, masking, orthogonalization, and GAN-generated synthetic faces. The method optimizes for biometric identity, binarization, and diversity, ensuring that the protected template remains matchable while being difficult to reverse-engineer. FaceCloak achieves irreversibility (0% Success Attack Rate) and strong unlinkability, all while maintaining biometric accuracy (95.7% TMR on LFW using ArcFace)[4]. PrintVault builds on similar principles of using neural-generated noise to obfuscate templates but extends the concept by applying it to fingerprints and ensuring revocability and matching consistency through a GAN-based adversarial training loop.

We propose a novel obfuscation model that directly modifies fingerprint minutiae to distort the template in a way that prevents template inversion attacks, complementing but not replacing encryption techniques such as post-quantum cryptography. While post-quantum cryptographic schemes (e.g., lattice-based encryption) offer strong guarantees for data security during storage and transmission, they still rely on secret key management, which introduces challenges in biometric systems where the template (e.g., a fingerprint) is inherently non-revocable. In contrast, our method adopts a template-level protection approach that does not require keys. By applying learned obfuscation through GAN-generated noise, the fingerprint template becomes non-invertible by design while retaining matching accuracy. This supports principles of cancelable biometrics and biometric template protection without encryption, which are particularly suited for user privacy and revocability in deployments. This approach focuses on maintaining authentication accuracy as the obfuscated fingerprint remains matchable to the original, but ensuring the reconstructed template is unrecognizable, preventing attackers from successfully recovering the original fingerprint. The research

uses a Generative Adversarial Network (GAN) to generate and obscure fingerprint templates in a way that enhances security while preserving usability. By focusing on minutiae-based modifications and implementing machine learning, the proposed method provides a more accurate solution than traditional transformation techniques that often degrade performance. This makes our approach more scalable and resilient in real-world applications, where managing keys or cryptographic methods can be difficult. This approach is designed to offer stronger protection against template inversion attacks while maintaining high recognition accuracy.

Methods

In this paper, we consider a threat model as described in Sec. 3.1 and use the proposed GAN method (dubbed PrintVault) described in Sec. 3.3. Before the training and in the pre-processing stage, we use multiple techniques to prepare the fingerprint templates.

Threat Model

In this work, the threat model assumes an adversary gains access to stored fingerprint templates within a biometric authentication system and attempts to reconstruct the original fingerprint image through a template inversion attack. Specifically, we assume the attacker employs a gradient-based optimization or image synthesis approach, where the goal is to generate a fingerprint image that, when passed through the same feature extractor as the system, closely matches the stored template. These inversion methods were used in prior face and fingerprint reconstruction attacks, where attackers optimize or train generative models to produce an image with a feature vector similar to the one in the database[5]. The model assumes a black-box scenario, where the attacker does not have access to internal system parameters but can observe outputs or similarity scores. To evaluate inversion risk experimentally, we use the Structural Similarity Index (SSIM) between the original fingerprint and its GAN-obfuscated version as a proxy, based on the assumption that higher visual similarity correlates with greater reconstructability[6]. While this does not constitute an active inversion attack, it captures the underlying principle: that successful inversion typically yields a fingerprint visually or structurally close to the original. Future work will incorporate adversarial reconstruction models to more rigorously test PrintVault's resilience against targeted inversion threats.

Pre-Processing

The fingerprint templates need to be pre-processed to prevent reconstruction techniques. Real-world data has problems such as irrelevant data, noisy data, and missing values[8]. The fingerprint dataset was collected from all four databases within dataset_FVC2000, which had problems with noisy and unclean data, likely due to imperfect skin condition or other environmental factors. To increase consistency for the model, we pre-processed the data with binarization, normalization, and resizing. Additionally, to introduce variability and prevent the model from memorizing patterns, we introduce data augmentation.

Fig. 1 Fingerprint Template dataset[7]

Fig. 2 Fingerprint pre-processing steps.

We applied a set of data augmentation techniques as part of the fingerprint pre-processing. Each input image was randomly rotated within a $\pm$15-degree range to simulate orientation variability commonly encountered in real-world fingerprint captures. We also adjusted image brightness by up to $\pm$20% to account for sensor lighting differences. To further enhance spatial diversity, random width and height shifts of up to 10% of the image dimensions were applied. These augmentations were applied probabilistically to each image during training, ensuring that the model encountered a wider range of fingerprint variations and structural distortions. This approach helps prevent overfitting and encourages the model to focus on essential invariant features. The pre-processing steps exclude greyscale conversion as the dataset is already in greyscale. Then, binarization converts the template into a black-and-white image. A pixel must meet

a certain threshold of darkness to be converted to a black pixel. After extensive hypertuning, a threshold of 0.5 provided the best results. Normalization then forces each pixel value to fix a range between [0, 1] by dividing by 255. Finally, resizing the images to a standard size of 128x128. To ensure model compatibility, the images are resized to 128x128 to maintain an input size that is a power of 2. GANs are designed for input sizes that are powers of 2 (e.g., 64, 128, 256). Reducing the image size from 160×160 to 128×128 significantly cuts down the number of pixels (from 25,600 to 16,384), reducing memory usage, training time, and GPU load. According to a 2016 study, resizing down to 128x128 is sufficient for valid conclusions. After pre-processing, the images were more consistent[9].

Training GAN

PrintVault utilizes a GAN-based architecture to obfuscate fingerprint templates by introducing structured noise while preserving key biometric features. GANs are well-suited for this task due to their ability to learn complex, high-dimensional transformations in an unsupervised setting. In PrintVault, the Generator creates fingerprint variations that are both realistic and untraceable, serving as a form of biometric camouflage. The architecture used is a Fully Connected GAN (FC-GAN), in which all layers are densely connected[10].

To improve training stability and gradient flow, PrintVault adopts the Wasserstein GAN with Gradient Penalty (WGAN-GP) framework. Instead of a standard Discriminator, WGAN-GP trains a Discriminator that assigns a continuous score indicating the realness of fingerprint images, without applying a Sigmoid activation[10]. The Generator is trained to maximize this score, encouraging the production of realistic samples. The gradient penalty enforces the Lipschitz constraint, ensuring smooth gradients and preventing training instabilities common in traditional GANs. This allows PrintVault to reliably generate obfuscated fingerprints that remain matchable for authentication while strongly resisting inversion attacks.

Equation 1: Generator Loss

$$L_G = -\mathbb{E}_{z\sim p_z(z)}[\log D(G(z))]$$

$G(z)$ is passed into the Discriminator, which assigns a real-valued score $D(G(z))$ indicating how realistic the generated fingerprint is. The Generator aims to maximize this score, encouraging the creation of outputs that the Discriminator evaluates as increasingly real. The Generator loss function is minimized during training using backpropagation and gradient descent. Unlike traditional GANs, this approach avoids vanishing gradients by providing meaningful feedback to the Generator even when its outputs are initially poor, resulting in more stable and effective training[10].

The Discriminator, which does not classify inputs as real or fake, but instead assigns a real-valued score that reflects how realistic an image is. Unlike standard GANs, the output does not pass through a Sigmoid activation, and the Discriminator does not output a probability. Instead, the Discriminator directly evaluates the realism of the input fingerprint image, helping the model learn a more meaningful representation of data similarity. The input 128×128 grayscale image is processed through four convolutional layers to extract hierarchical features, and the final output is a scalar score.

The Discriminator loss in WGAN-GPs:

$$L_D = \mathbb{E}_{\tilde{x}\sim P_g}[D(\tilde{x})] - \mathbb{E}_{x\sim P_r}[D(x)] + \lambda \cdot \mathbb{E}_{\hat{x}\sim P_{\hat{x}}}[(\|\nabla_{\hat{x}} D(\hat{x})\|_2 - 1)^2]$$

This loss formulation improves stability and prevents overfitting by ensuring smoother gradients and consistent feedback throughout training. The Discriminator trains to maximize the difference between the average scores for real and generated images while maintaining a bounded gradient norm[11]. This encourages the Generator to produce increasingly realistic fingerprint templates that maintain authentication accuracy while resisting inversion attacks.

To reproduce the proposed methodology, the following experimental setup was used. The model was trained for 100 epochs with a batch size of 128 and a learning rate of 0.0002. We employed the Adam optimizer with β_1 set to 0.5 and β_2 to 0.999 for stable convergence. The Generator received a 100-dimensional latent noise vector sampled from a standard normal distribution, $\mathcal{N}(0,1)$, as input. LeakyReLU with $\alpha = 0.2$ was used as the activation function for all hidden layers, while the Generator's output layer used a Tanh activation to produce normalized outputs. The Discriminator employed a Sigmoid activation function in its final layer to output probability scores distinguishing real from fake fingerprints.

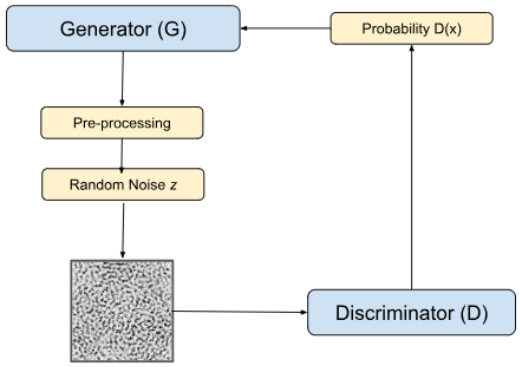

Fig. 3 Overview of GAN Architecture of the PrintVault.

Results

Dataset and Evaluation Metric

The dataset used in this study is dataset FVC2000[7], which consists of 1000 fingerprint templates. The dataset was split such that 80 percent (800 images) were used for training the GAN, including both the Generator and Discriminator networks, and 20 percent (200 images) were kept unseen during training and were used exclusively for testing and evaluation. Noise augmentation was applied only within training, and all transformations were carried out after the dataset was split. This ensures that no augmented or obfuscated version of a test image was ever seen by the model during training, which prevents data leakage and guarantees a fair evaluation of the model's generalization.

Each template is a 160x160-pixel grayscale image that captures detailed fingerprint features. The dataset allows for variability in fingerprint impressions. Despite its high quality, the dataset may contain noise and inconsistencies, which require pre-processing steps like grayscale conversion, binarization, normalization, and resizing to 128x128 pixels. This dataset is widely used in biometric research, providing a reliable and standardized foundation for testing fingerprint recognition models.

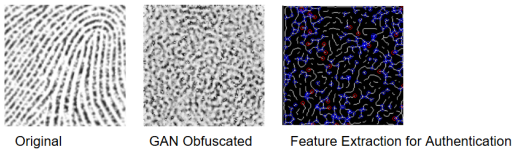

Fig. 4 Transformation of the fingerprint template: original, obfuscated, and features for authentication.

To evaluate the effectiveness of the proposed PrintVault method, we measured the Structural Similarity Index Metric (SSIM) between the generated obfuscated fingerprints and their corresponding original templates, as well as the consistency between multiple obfuscated versions of the same fingerprint. A low SSIM score between the obfuscated and original fingerprints indicates that the obfuscation effectively disrupts recognizable features, thereby providing strong resistance to template inversion attacks. Our experiments show an average SSIM of 0.0321 between the original fingerprints and the GAN-obfuscated outputs, which is significantly below the NIST-recommended threshold of 0.05[12]. This threshold is based on large-scale analyses by NIST using standardized fingerprint matchers, where similarity scores distinguish genuine pairs from impostor pairs. The low similarity score achieved demonstrates that PrintVault successfully transforms fingerprint templates into unrecognizable forms, substantially reducing the risk of successful template inversion attacks.

Secondly, we evaluated the metric that compares the matchability between two different GAN-generated obfuscated versions of the same original fingerprint to each other. A high matchability score here suggests that the GAN is producing stable and consistent obfuscated templates, which are still usable for authentication, even after obfuscation. Through feature extraction, two GAN-obfuscated fingerprints can be authenticated by identifying consistent and distinguishing patterns that remain preserved despite the visual alterations introduced by the obfuscation process. While the GAN modifies the fingerprint to prevent template inversion, it retains the underlying structural features, such as ridge flow, minutiae distribution, and overall topology, that are critical for matching. These features are extracted by the fingerprint recognition system, allowing it to compare and match the obfuscated template against enrolled data with high accuracy, thereby enabling secure and reliable authentication. In Figure 4, the blue circles identify the bifurcation points and the red circles classify the termination points. These features are necessary for authentication. The authentication accuracy between two different GAN-obfuscated fingerprints is 0.9406, which exceeds the expected standard of 0.70[12].

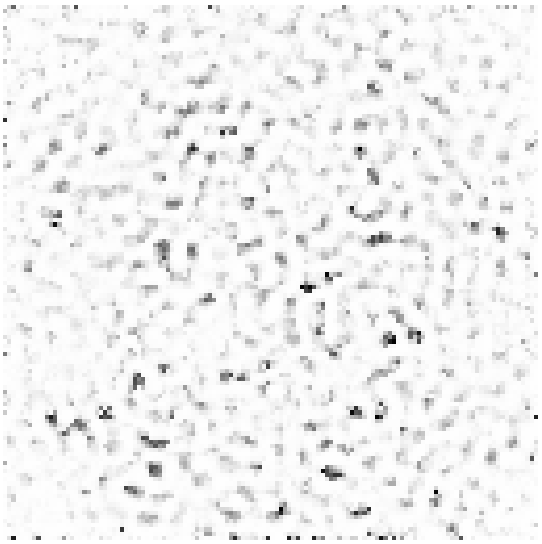

Fig. 5 Example of a GAN obfuscated fingerprint image with matching accuracy of 0.0317.

Figure 5 shows a fingerprint that was obfuscated by the GAN but ultimately could not be matched. As demonstrated in this example, some failures can be attributed to the GAN's lack of output consistency, particularly due to its sensitivity to variations in the latent input vector z. Because the generator is trained unconditionally using random noise, there is no guarantee that multiple runs using the same fingerprint will produce similar obfuscated outputs. This is especially problematic near the model's decision boundaries, where small changes in z can lead to significantly different outputs. To address this limitation, a Conditional GAN (cGAN) can be used, incorporating a fixed fingerprint embedding as a condition to guide the generation process and improve consistency. Additionally, incorporating a feature-matching loss can encourage the generator to produce

more stable outputs by minimizing differences in intermediate discriminator features. Further improvements could include data augmentation and the use of fingerprint class labels during training to reduce mode collapse and enhance generation stability.

The evaluation results demonstrate that the fingerprint recognition system performs exceptionally well in distinguishing between genuine and impostor fingerprints. The False Acceptance Rate (FAR) is very low at 0.20%, indicating that the system rarely incorrectly accepts unauthorized users, which reflects strong security. Meanwhile, the False Rejection Rate (FRR) is at 0.51%, showing that legitimate users are almost never rejected, ensuring excellent usability. The Equal Error Rate (EER), where FAR and FRR are equal, is also 0.13%, highlighting an ideal balance between security and user convenience. Overall, these metrics suggest the system achieves near-perfect accuracy on the evaluated dataset, effectively preventing false matches without sacrificing genuine user access.

The balance between security and usability is crucial in biometric systems. If an obfuscation method is too aggressive, it may destroy essential features needed for authentication. The proposed method successfully prevents template inversion attacks while ensuring fingerprint authentication remains reliable. Compared to prior techniques (e.g., feature transformations, fuzzy vaults), this approach achieves stronger security without significantly compromising biometric recognition accuracy.

Discussion

Limitations

The effectiveness of the GAN-based obfuscation method has been validated using the FVC2000 dataset; however, its generalizability to other fingerprint datasets or real-world biometric systems remains untested. A key concern is the potential for overfitting, where the neural network may perform well on this specific dataset but fail to generalize to new data[13]. Additionally, training GAN models is highly computationally intensive, requiring significant processing power and memory, which may limit scalability for large-scale deployment[14]. While the method effectively prevents template inversion attacks, adversaries may develop countermeasures such as adversarial training or more advanced reconstruction techniques to bypass obfuscation[15]. Lastly, PrintVault is trained on 128×128 fingerprints, meaning real-world applications may require additional preprocessing and resizing for compatibility with varying fingerprint resolutions[16]. While GANs are known to be vulnerable to adversarial attacks, PrintVault mitigates these risks through architectural design. The system functions as a template obfuscator rather than a classifier, meaning adversarial gradients cannot be easily leveraged to influence outcomes. It produces stochastic, revocable outputs, which limits the effectiveness of frequency-domain and gradient-based attacks like FGSM or PGD due to the lack of consistent spectral patterns and deterministic behavior[17]. Furthermore, since the GAN operates separately from the matcher, common adversarial paths are disrupted[18]. Future work may explore integrating adversarial training to further strengthen security under attack conditions. Regarding standard fingerprint quality measures like NFIQ2, PrintVault's obfuscated fingerprints may show a reduced raw image quality score due to the added noise and transformation; however, this does not translate into decreased authentication performance. This is because the obfuscation specifically targets the irreversibility of the templates rather than degrading key features used by matchers. Thus, while NFIQ2 may indicate a lower quality by traditional imaging standards, the functional quality in terms of successful matching remains high, demonstrating that PrintVault effectively preserves the usability of fingerprints for authentication despite altered quality metrics.

Comparison

PrintVault offers several advantages over traditional fingerprint template protection techniques, such as cancelable biometrics, fuzzy vault schemes, and biohashing. Cancelable biometrics rely on applying non-invertible transformations to the biometric template, which provides security but often degrades matching accuracy and lacks flexibility for different use cases. Fuzzy vault schemes combine biometric features with cryptographic keys, but they are vulnerable to record multiplicity attacks and suffer from high computational overhead. Biohashing introduces randomness through user-specific keys, but it is no longer considered secure if the key or transformation function is exposed.

In contrast, PrintVault uses a GAN-based approach to learn a transformation function that introduces structured, stochastic noise into fingerprint templates. This not only obscures the original biometric data effectively by resisting inversion, but also preserves matching consistency, since multiple outputs for the same fingerprint are still similar enough to authenticate successfully. The results suggest that PrintVault balances security (irreversibility) and usability (authentication accuracy) better than many existing schemes, especially those that require deterministic transformations or manual key management.

Ethical Considerations

The use of biometric data inherently raises concerns regarding privacy, security, and ethical considerations. Fingerprint data, once compromised, cannot be changed like a password, making secure collection, storage, and protection critical. Proper consent from users and adherence to strict data protection regulations, such as GDPR and BIPA, are necessary to ensure ethical use. Although the proposed method strengthens fingerprint security by preventing template inversion attacks, there is a risk that

similar obfuscation techniques could be misused by malicious actors to bypass legitimate authentication systems. Furthermore, if the training dataset lacks diversity, the GAN model may introduce unintended biases, leading to disparities in recognition accuracy across different demographic groups. This could result in unequal access to secure authentication and further ethical concerns about fairness and inclusivity in biometric security systems. Addressing these challenges requires careful oversight, regular audits, and improvements in dataset representativeness to ensure fairness and effectiveness.

Conclusion

This research presents a novel GAN-based obfuscation technique to protect fingerprint templates from template inversion attacks while preserving authentication accuracy. By transforming fingerprint data into an unrecognizable yet matchable format, the method enhances biometric security without significantly compromising performance. Experimental results demonstrate that the obfuscated templates resist reconstruction while maintaining reliable authentication with remarkable resistance of about 3 percent. However, challenges such as dataset bias and potential misuse must be addressed to ensure ethical implementation. Future work will focus on improving generalization across diverse datasets, further strengthening security measures, and testing using active template inversion attacks. PrintVault represents a step forward in safeguarding biometric data in an increasingly digital world.

Acknowledgments

I would like to thank my advisor, Kristen Preston, for the valuable insight provided to me.

References

1 M. Kenneth, *Automated Fingerprint Identification System (AFIS*.

2 S. Hatef and S. Marcel, *Template Inversion Attack against Face Recognition Systems Using 3D Face Reconstruction*, https://openaccess.thecvf.com/content/ICCV2023/papers/Shahreza_Template_Inversion_Attack_against_Fa.

3 R. Sp, T. Thomas and S. Emmanuel, *Cancelable biometric template generation using random feature vector transformations*, https://doi.org/10.48550/arXiv.2503.15648)., arXiv.org (2025), (available at.

4 S. Banerjee, A. Jain, C. Hegde and N. Memon, *Facecloak: Learning to protect face templates*, https://doi.org/10.48550/arXiv.2504.06131)., arXiv.org (2025), (available at.

5 K. Wijewardena, S. Grosz, K. Cao and A. Jain, *Fingerprint template invertibility: Minutiae vs*, https://arxiv.org/abs/2205.03809)., deep templates. arXiv.org (2022), (available at.

6 *Image quality assessment: From error visibility to structural similarity —*, https://ieeexplore.ieee.org/document/1284395/)., available at.

7 D. Maltoni, *FVC2000*.

8 M. Kiran, *A Review: Data Pre-Processing and Data Augmentation Techniques*, https://doi.org/10.1016/j.gltp.2022.04.020, Sciencedirect,.

9 B. Sukarna, *FCC-GAN: A Fully Connected and Convolutional Net Architecture for GANs*, https://doi.org/10.48550/arXiv.1905.02417.

10 D. Mishkin, N. Sergievskiy and J. Matas, *Systematic evaluation of CNN advances on the ImageNet*, https://arxiv.org/abs/1606.02228)., arXiv.org (2016), (available at.

11 I. Gulrajani, F. Ahmed, M. Arjovsky, V. Dumoulin and A. Courville, *Improved training of Wasserstein Gans*, https://arxiv.org/abs/1704.00028)., arXiv.org (2017), (available at.

12 T. Elham, *NFIQ 2 NIST Fingerprint Image Quality*, https://doi.org/10.6028/nist.ir.8382.

13 G. J, *Generative Adversarial Networks*.

14 C. Antonia, *Generative Adversarial Networks: An Overview*, https://doi.org/10.1109/msp.2017.2765202, ieeexplore.ieee.org/abstract/document/8253599,.

15 A. Anish, *Synthesizing Robust Adversarial Examples*, https://doi.org/10.48550/arXiv.1707.07397.

16 J. Anil and K. Nandakumar, *Biometric Template Security*, https://doi.org/10.1155/2008/579416.

17 H. Li and R. Ramachandra, *Deep learning based Fingerprint Presentation Attack Detection: A Comprehensive Survey*, https://arxiv.org/abs/2305.17522)., arXiv.org (2023), (available at.

18 D. Yin, R. Lopes, J. Shlens, E. Cubuk and J. Gilmer, *A Fourier perspective on model robustness in computer vision*, https://arxiv.org/abs/1906.08988)., arXiv.org (2020), (available at.