VeinGuard: Attention-Driven Autoencoder with GAN-Augmented Features and Random Forest Classification for Robust Fake Finger-Vein Detection

Deepthi M P
Student
MANGALAM college of engineering ettumanoor

Sanitha P S
Assistant professor
FISAT engineering College

Devipriya S Kumar
Assistant professor
MANGALAM college of engineering

Abstract

Finger-vein biometrics is highly secure because the internal and unique vascular patterns are used. However, it is susceptible to advanced presentation attacks. The proposed paper suggests VeinGuard, a hybrid biometric anti-spoofing system which combines unsupervised anomaly detection and supervised classification to deliver effective fake finger vein detection. Attention-based autoencoders are only trained on real finger-vein images in order to be able to learn natural vascular features and identify abnormalities during reconstruction errors analysis. In order to get a better feature diversity and discriminative power, a Generative Adversarial Network (GAN) is used, in which the discriminator is a strong feature extractor, which is trained through adversarial learning. Attributes of autoencoder reconstruction loss, latent embeddings and GAN discriminator loss are combined and categorized with an ensemble of Random Forests. The experimental evidence indicates that VeinGuard is able to perform better in terms of accuracy, ROC-AUC, precision and recall and still enjoys strong generalization against unseen spoofing attacks. The suggested architecture is a scalable and dependable implementation of secure finger-vein biometric.

Keywords— biometrics, GAN, Finger-Vein, image, pattern.

I. INTRODUCTION

A. Background of Finger-Vein Biometrics

Finger-vein biometrics has become a valid and effective physiological authentication modality because it has intrinsic strengths when compared to surface-based characteristics such as fingerprints and facial images. It is a technology that identifies the distinctive vascular patterns under the skin through near-infrared (NIR) imaging; thus, the biometric trait is highly distinctive and hard to observe or replicate externally [1]. The patterns of the finger-vein being internal to the human body, they are safeguarded against wear by the environment, against contamination and casual purchase on the surface. Consequently, there has been an increase in finger-vein recognition systems being used in high-security areas such as banking authentication, access control systems and identity verification systems.

B. Presentation Attack Threats in Finger-Vein Systems

Finger-vein systems are vulnerable even to presentation attacks or spoofing attacks, even though they have the security advantage of being intrinsically secure. Such attacks include providing artificial biometric samples such as printed vein images, synthetic vein patterns, re-execution of infrared captures etc. to spoof the recognition system. Imaging technology and generative models have reduced the cost of attackers to create realistic spoof samples and the threat of biometric integrity increases. Presentation attack detection (PAD) has therefore emerged as an important aspect in achieving credibility and strength of the finger-vein biometric system [2].

C. Limitations of Existing Spoof Detection Methods

Traditional spoof detection methods are based to a large extent on handcrafted features or fully supervised learning models that are trained on labelled genuine and spoof samples. Nonetheless, these approaches have a number of shortcomings. The feature-based methods which are handcrafted do not usually have the ability to generalize to other sensors and types of attacks. Deep learning models that are fully supervised are effective but need a large amount of labelled spoof data [3]. Such reliance on labelled information limits scale and resilience in the process of implementation in real-world settings where new spoofing methods can be developed.

D. Motivation for Hybrid Unsupervised–Supervised Learning

In order to overcome these difficulties, the hybrid unsupervised and supervised learning frameworks as the Auto-encoders and Generative Adversarial Networks (GANs) are able to learn intrinsic representations of natural finger-vein patterns without the need to be supplied with labelled spoof data [5]. These representations can be used to make a good differentiation between abnormal or spoof-like samples when they are used along with supervised classifiers. The hybrid method achieves better generalization, minimizes the use of labelled data of attacks and better detection against new spoofing attacks or attempts.

E. Significance of the Research

The suggested hybrid framework of finger-vein spoof detection is capable of considering real-life security issues. The study will improve the accuracy of the spoof detection, the strength of the learning and the flexibility by exploiting unsupervised feature learning and supervised classification.

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

EXCELLENCE INNOVATIONS
SAMPLE - FOR REFERENCE ONLY

excellenceinnovations.com | Sample - for reference only

II. LITERATURE REVIEW

A. Finger-Vein Recognition Techniques

As per the study of [5], finger-vein biometrics is quickly being identified as a highly secure and effective modality with regard to automated personal identification. Finger-vein recognition makes use of the special vascular configurations that are ingrained underneath the human skin on their fingers. These patterns are captured with the help of near-infrared (NIR) imaging and allow clear visualisation of subcutaneous veins. According to [6], this technology has been widely adopted in applications that require high confidentiality such as healthcare systems, financial transactions, access control, and law enforcement. As per [7], finger-vein recognition has various benefits including contactless acquisition, rapid authentication, contactless acquisition, and better resilience of attack on spoofing. These are the benefits that make it increasingly more preferred to iris, fingerprint and face recognition. The study of [8] explains that early fake finger-vein recognition techniques relied on handcrafted feature extraction methods. These included vein enhancement preprocessing techniques and followed by feature extraction through approaches such as Gabor filters, repeated line tracking, local binary patterns, and maximum curvature analysis. Learning-based and statistical methods were introduced to improve recognition accuracy. Support Vector Machines and k-Nearest Neighbour were used as classifiers and have better discrimination which can be achieved with handcrafted features. While the fake finger-vein recognition techniques have evolved significantly, the challenges related to data security, robustness, and vulnerability still exist.

B. Presentation Attack Detection in Biometrics

The study of [9] explains that Presentation Attack Detection (PAD) is also referred to as anti-spoofing and addresses the vulnerability of biometric systems to deliberate attempts aimed at deceiving the sensor during the acquisition process. A presentation attack occurs when an attacker presents a falsified or manipulated biometric sample to a biometric sensor with the intention of masquerading as a legitimate user. These attacks are broadly classified into two types that are physical artefacts and replay attacks. The physical artefacts that imitate genuine biometric traits are commonly known as presentation attack instruments (PAIs) [10]. The replay attacks perform the previously captured biometric data that are reintroduced to the sensor using a suitable display or transmission device. As per [11], to counter these threats, a variety of PAD techniques have been developed across different biometric modalities. These countermeasures aim to distinguish between bona fide biometric samples and attack presentations by analysing structural as well as dynamic cues inherent to genuine traints. PAD has received growing attention as a finger-vein system in the vascular system. The [12] argue that data-driven PAD methods have gained popularity as deep learning models have evolved. Convolutional Neural Networks (CNNs) have evolved to automatically learn discriminative features that are capable of separating genuine samples from PAIs. Liveness detection techniques are simultaneously investigated as an additional defence mechanism. These methods typically analyse temporal or spectral information from near-infrared video sequences to detect physiological responses such as blood flow or subtle motion patterns that are difficult to replicate using artificial artefacts.

C. Deep Learning-Based Spoof Detection Approaches

According to [13], deep learning has significantly advanced PAD by enabling automatic learning of discriminative representations from biometric data, and this technique reduces the dependency on handcrafted features. As compared to traditional texture- or rule-based methods deep learning models can capture complex spatial, spectral, and temporal patterns that differentiate genuine biometric traits from spoofed presentations. Deep learning-based PAD has become a dominant paradigm across modalities such as face, fingerprint, and vascular biometrics. Apart from the conventional CNNs, advanced architectures such as Siamese networks and deep metric learning frameworks have been investigated for PAD. These models aim to learn similarity measures that separate genuine samples from the speeded ones in an embedding space and offer improved discrimination under certain conditions. As per the study of [14], a few temporal deep learning models such as 3D CNNs and recurrent neural networks have been applied to video-based PAD to exploit dynamic cues related to liveness. As per the study of [15], Generative Adversarial Networks (GANs) have been incorporated into PAD research for data augmentation, spoof simulation, and feature enhancement. GAN-based approaches can improve robustness by enriching the training distribution. But these techniques introduce challenges related to training stability and evaluation stability.

D. Autoencoder-Based Anomaly Detection

As per [16], Autoencoder-based anomaly detection has become an effective approach for presentation attack in biometric systems especially when labelled spoof data are limited. Autoencoders are neural networks that are designed to learn compact latent representations of input data by minimising reconstruction error. Spoof samples are treated as anomalies as they often differ structurally or statistically from genuine biometric traits. As per [17], spoof inputs typically result in higher reconstruction errors compared to genuine biometric traits. Spoof units generally result in higher construction errors as compared to genuine samples. Variants such as denoising autoencoders and variational autoencoders have been explored to improve robustness by handling noise and enforcing structured latent spaces.

E. GAN Applications in Biometric Security

Generative Adversarial Networks (GANs) have emerged as a powerful tool in biometric security research due to their ability to model complex data distributions and generate realistic synthetic samples. As per the study by [18], a GAN consists of two competing neural networks which are a generator and a discriminator. This adversarial training paradigm has been widely explored to address important challenge sin biometric systems especially in spoof simulation, data security, and robustness enhancement. According to [19], one of the major applications of GAN is data augmentation, and GAN-generated samples are used to enrich the training datasets as well as enhance the capacity of spoof detection models.

EXCELLENCE IN INNOVATION
SAMPLE - FOR REFERENCE ONLY

F. Research Gaps

Although there has been progress in the finger-vein recognition area, the existing literature is mostly concentrated on identity verification in a benign environment, and major attention has been paid to presentation attack detection. A significant part of PAD methods utilises full supervised deep neural networks that need large labelled spoofing datasets. But these are limited to the case of the finger-vein biometrics and normally result in poor extrapolation to novel attacks. In spite of the studied autoencoders-based anomaly detection as well as GAN-based methods, they are usually implemented alone and lack integrated decision-making processes. A few studies have explored hybrid configurations, which collaboratively utilise unsupervised modelling, generative feature improvement, and perform robust ensemble classification to enhance resilience and flexibility against the changing spoofing attacks.

III. Proposed VeinGuard Framework

A. Overall System Architecture

The suggested VeinGuard framework is developed as a multi-step hybrid biometric anti-spoofing solution that consists of the unsupervised representation learning, generative modeling and supervised classification [20]. There are three main models including an attention-based autoencoder, a Generative Adversarial Network (GAN) and a Random Forest classifier in the design. The images of finger-veins taken in near-infrared are first processed to remove the differences in illumination and improve the vein pattern. The processed images are sent to the autoencoder and the GAN at the same time. The autoencoder is concerned with the inherent structural attributes of the real finger-vein images whereas the GAN data models sophisticated data distribution and the features of discrimination. Lastly, the similarities between the two models are combined into one and used by a Random Forest Classifier to do the last spoof.

B. Hybrid Learning Strategy

The strategy that VeinGuard proposes is a hybrid unsupervised-supervised learning strategy to address weaknesses of purely supervised spoof detection approaches. Attention-based autoencoder is only trained on actual finger-vein samples in an unsupervised way which allows it to learn compact latent codes and reconstruction error patterns exposing anomalies. Simultaneously, the GAN uses supervised learning in its discriminator to differentiate between true and fake samples whereas the generator applies synthetic variations to enhance feature learning [21]. The framework has the ability to improve generalization by trading unsupervised anomaly detection with supervised discrimination in addition to lessening reliance on large labelled spoof data sets.

C. Workflow of the VeinGuard Pipeline

The VeinGuard pipeline consists of finger-vein input image preprocessing which is followed by feature extraction (unsupervised) based on the attention-driven autoencoder to retrieve reconstruction errors and latent embeddings. At the same time, the GAN extracts high-level discriminative features of real and synthetic samples. These dissimilar attributes are subsequently fused to make use of a single feature vector. In the last stage, the Random Forest Classifier examines the combined features to conclude whether the sample input is authentic or spoofed [22]. Such a layered workflow makes sure of strong, noise-immune and versatile detection of spoofing.

IV. Attention-Driven Autoencoder for Anomaly Detection

A. Motivation and Design Objectives

The design objectives and motivation of the system serve to provide details and information on the aim of the system design and the motivational tool of the system. The design objectives and motivation of the system are aimed at giving details and information on the objective of the system design and the motivational tool of the system.The rationale behind using an attention-driven autoencoder within the VeinGuard system is the necessity to identify spoofing attacks without paying much attention to labeled attacks examples. In practice, in real-world biometric systems, it is not possible to gather extensive spoofing data because of changing attack methods. Thus, a trained method of anomaly detection based solely on true images of fingers and veins is a viable and scalable solution [23]. The main design requirements of the autoencoder are that they should effectively model the intrinsic structural patterns of true finger-vein images, highlight discriminative vascular areas and generate meaning reconstruction errors with spoofed inputs.

B. Autoencoder Network Architecture

The autoencoder network architecture uses the autoencoder algorithm to reconstruct the original image with minimal error. The model takes the form of an encoder-decoder framework which is trained to learn compact and informative latent codes of finger-vein images. The encoder consists of a sequence of convolutional layers whose channels of features gradually increase. Allowing the hierarchical feature quotient of low-level textures to high-level vascular designs. Activation functions are non-linear and layers of batch normalization are used to stabilize training and enhance governance [24]. The decoder is also a replica of the encoder design in which transposed convolutional layers are employed in recovering the input images in the latent space.

C. Attention Mechanism Integration

An attention mechanism is added to the autoencoder model in order to increase its attention to high-priority areas of the salient veins [25]. The attention module gives the feature maps adaptive weights to enable the network to highlight informative vascular structures and remove background noise. This integration enhances the sensitivity of the model in emerging veins that are hard to counterfeit in spoofed specimens. The attention mechanism provides a great boost to anomaly detection ability by directing the autoencoder to concentrate on areas of discrimination, particularly where illumination, finger placement and sensor noise variants occur.

D. Training Using Genuine Samples Only

The autoencoder given attention is trained in an unsupervised manner using only authentic images of finger-veins. The model is also trained to reduce reconstruction loss between the input and reconstructed images, usually quantified by mean squared error (MSE) [26]. This makes the model very

EXCELLENCE INNOVATIONS
SAMPLE - FOR REFERENCE ONLY

competent in recreating the real samples since it is only exposed to real patterns. By contrast, spoofed or anomalous inputs that are not consistent with what has been learned cause increased reconstruction errors. This type of training removes the reliance on spoof labels and improves flexibility to unknown types of attacks.

E. Reconstruction Error-Based Feature Extraction

The error of reconstruction is important in making a difference between a true and a spoof sample in the VeinGuard model. At every input image, pixel-level and aggregate reconstruction error statistics are determined and they are used as discriminative features in the next stage of classification. Reconstruction error measures combined with latent embeddings and GAN-generated features have a strong influence on the total spoof detection rates and lead to the sound decision in the final classification step.

V. GAN-Augmented Feature Learning Module

A. Rationale for GAN-Based Feature Enhancement

The use of GAN as a part of the VeinGuard system can be explained by the necessity to increase the variety of features and their discriminative capacity when it comes to the detection of spoof. The traditional supervised models tend to perform poorly in generalization when they are trained using small or homogeneous spoof datasets. GANs solve this problem by training on real-world distribution of data and create natural variations of finger-vein patterns. GAN assists the model in learning salient qualities that are sensitive to latent inconsistencies in authentic and spoofed samples, enhancing detection quality with a wider set of realistic samples [27].

B. GAN Architecture (Generator and Discriminator)

The GAN architecture of VeinGuard has two networks such as a generator network and a discriminator network that are competing with each other [28]. The generator is programmed to generate finger-vein-like images by converting layers to enhance spatial details successively. In its turn, the discriminator is a convolutional neural network that is trained to differentiate between actual finger-vein images and generated ones. Additionally, the discriminator acquires rich hierarchical representation, an effective feature extractor.

C. Adversarial Training Strategy

The adversarial training works by an iterative min-max optimization whereby the goal of the generator is to generate realistic samples that could pass through the discriminator whereas the goal of the discriminator is to correctly classify real and synthetic images. This competitive learning approach compels both networks to keep on improving. Real samples are used in capturing finger-vein images during training, whereby the generator gives out an ever more realistic variation [29]. Such dynamic interaction boosts the capability of the discriminator to show subtle deviations that are indicators of attacks of spoofing.

D. Discriminator Feature Extraction

The feature finds application in tasks that involve greater complexity than the other methods used earlier. Instead of relying on the ultimate classification outcome of the discriminator, the intermediate feature maps of its hidden layers are removed and used as high-level features. These attributes represent patterns of discrimination which are acquired in the course of adversarial training and which encode inconsistencies which might not be directly apparent in raw images. VeinGuard can tap into a rich feature space by using discriminator-derived embeddings that are complementary to anomaly indicators based on autoencoders.

E. Role of GAN Features in Spoof Detection

The features obtained through GAN are very essential in enhancing the performance of features in spoof detection as they enhance the overall features representation. Combined with reconstruction error indicators and latent embeddings, the features enhance the separation of authentic and spoof samples [30]. This combination helps the ultimate classifier to make more reliable and correct decisions especially in cases of complex or recently unknown spoofing attacks.

VI. Feature Fusion and Random Forest Classification

A. Multi-Source Feature Representation

The VeinGuard system employs a multi-source representation strategy to characterize genuine and spoofed finger-vein patterns comprehensively. Three complementary feature groups are obtained. Firstly, reconstruction-error statistics calculated with respect to attention-driven autoencoder are being computed, which consist of pixel-wise mean squared error (MSE), distributional statistics such as mean and quantiles, and local patch-based reconstruction errors. These characteristics are the measures of any deviation from the learned distribution of actual vein structures, and they are effective indicators of anomalies. Second, small latent embeddings at the autoencoder bottleneck layer are codes of world structural features of finger-vein patterns in the low-dimensional space. Third, intermediate feature layers of the GAN discriminator are obtained at a high level, and they represent discriminative texture, edge, and frequency-domain features related to the spoof artifact. The articulation of anomaly-directed and discriminating attributes allows the model to accommodate the various presentation attack attributes, which have proven to be useful in the recent biometric presentation attack detection (PAD) reports [31] [32].

B. Feature Normalization and Fusion Method

Normalization is done before fusion to facilitate equal contribution of each source of features. The normalization of latent embeddings and discriminator features is based on z-score normalization, whereas the statistics of reconstruction error are normalized through min-max normalization. Further, the effect of extreme outliers, which is typical of reconstruction-error distributions, is reduced by winsorization at the 1st and 99 th percentiles. Because feature scaling is the main parameter to consider when developing a classifier, other normalization techniques such as z-score, min-max, and rank-based

EXCELLENCE IN INNOVATIONS
SAMPLE - FOR REFERENCE ONLY

normalization are also tested, and the one that leads to the highest cross-validated AUC is chosen [33]. The fusion of features is done using the feature-level concatenation, and then there is a dimensionality-reduction phase in which the principal-component-analysis (PCA) or canonical-correlation-analysis (CCA) is used. This projection will decrease redundancy, decrease multicollinearity, improve computational effectiveness, and avoid the loss of discriminative information [34].

C. Random Forest Classifier Design

The final decision model that is used is a Random Forest (RF) classifier because it is resistant to overfitting, it can accommodate heterogeneous features, and it is inherently interpretable. The RF is applied as a forest of 500 decision trees, and the maximum depth and minimum leaf size are optimized using grid search. The weighting of the classes is done to take care of the possible imbalance of the real and fake samples. In order to have more reliable predictions, isotonic regression is used to calibrate predicted probabilities, producing well-correlated estimates of confidence [35]. Nested cross-validation is employed to select hyperparameters as well as estimate performance to reduce bias and maximize generalization.

D. Classification and Decision Strategy

In the process of inference, the RF generates a calibrated probability that depicts the probability of a spoof attack. This likelihood is again added with a normalized autoencoder anomaly score with a simple meta-classifier of logistic regression. The two-step decision strategy allows both discriminative and anomaly-based evidence to be exploited in a complementary with the correction of residual calibration inconsistency. In order to allow trade-offs between false-accept and false-reject, VeinGuard allows configuring operating thresholds to suit various security needs. They include feature-importance analysis and explainability tools based on SHAP, along with monitoring the trends of model behavior and retraining it periodically in line with adaptive PAD system best practices [36] [37].

VII. EXPERIMENTAL SETUP

A. Datasets Description

Experimental analysis uses the PLUSVein-FV3 corpus as the main source of bona fide data, which includes multi-sensor near-infrared finger-vein records of different fingers and subjects and the complementary PLUS-FV3 Spoof subset with the printed and artifact-based presentation attack images obtained by using the collection of PLUSVein [38]. All these sets can be used to perform a closed-set verification experiment and realistic PAD tests with known attack species. The real set can be used to train an autoencoder unsupervised, and the spoof set is used to train a discriminator supervised and evaluate a downstream classifier.

B. Data Preprocessing

Through using edge-based masking of the OpenVein toolkit, raw images are first converted to uniform ROI crops. ROI extraction removes background variability and focuses models on vascular structure. The size of images is reduced to a constant input resolution, and the intensities are normalized per image (zero mean, unit variance). Robust augmentation, including small rotations and contrast jitter, as well as elastic deformations and artificially simulated illumination shifts, is augmented. The scale of augmentation is more relaxed for authentic samples and more drastic for training the GAN module, which rewards a variety of spoofing patterns [36]. Where there are needed sensors, artifacts are removed by outlier removal and histogram equalization before training autoencoders.

C. Training and Testing Protocol

The training adheres to the split design where discontinuous training sets (genuine-only) of the autoencoders are not shared with that of GAN/discriminator or RF training fold to prevent leakage of labels. Precisely, 60% of the subjects are fit to autoencoders, 20% to validation, such as threshold selection and early stopping, and the remaining 20% are the cross-subject testing ones. Spoof specimens are not introduced until the implementation of GAN and RF supervised training and final PAD evaluation. Nested cross-validation is used to tune hyperparameters, and early stopping is used on the loss on validation to select a model [31]. The cross-subject and cross-PAI tests are used to measure robustness to simulate invisible attack species.

D. Evaluation Metrics

Classical classification metrics (AUC, EER, precision, recall, F1) are used to report the performance, PAD-specific metrics that are standardized by ISO (APCER, BPCER and ACER) are used to quantify attack and bona-fide error rates in defined scenarios (ISO/IEC 30107-3; LivDet benchmarks). It is claimed that calibration and operating-point selection can be used to facilitate application-level tradeoffs between false-accept and false-reject results [39].

E. Implementation Details

The autoencoder and GAN blocks are trained in PyTorch using Adam (β_1=0.9, β_2=0.999), 1e-4 and 2e-4 (respectively) initial learning rate and batch normalization in the encoder/decoder blocks. Nested folds are used to optimize the hyperparameters of the RF classifier, which has 500 trees, class weighting, and isotonic probability calibration. Training uses the concept of early stopping, mixed-precision arithmetic where available, and model checkpoints in order to achieve reproducibility. Experiment metadata is logged with source code and trained checkpoints in order to support replication and retraining regularly as novel PAI species appear [31] [36].

VIII. RESULTS AND DISCUSSION

A. Result

The quantitative and qualitative results reveal the efficiency of the suggested VeinGuard system in anomaly recognition at the stage of detection and supervised classification.

EXCELLENCE INNOVATIONS
SAMPLE - FOR REFERENCE ONLY

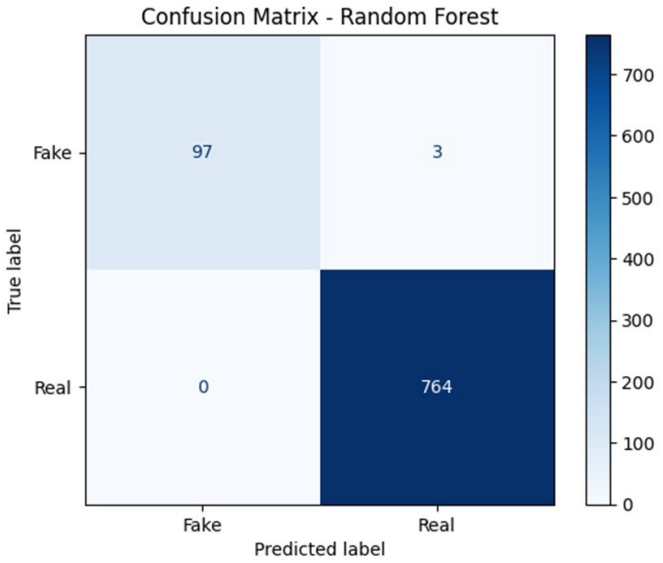

Figure 8.1.1: Random Forest classification performance.

The confusion matrix generated by the Random Forest classifier suggests a very sound discrimination of actual and fake finger vein samples. Among the test set used, 97 spoof samples were successfully identified as spoof, 3 spoof samples were incorrectly identified as genuine, and 764 genuine samples were identified correctly. This is associated with a total accuracy of 99.65, a precision of 1.00, a recall of 0.97, a specificity of 1.00, and an F1-score of around 0.985. False positives are not present, which underscores the capacity of the system to ensure an extremely low false-accept rate, which is a critical requirement of biometric presentation attack detection (PAD) systems [36].

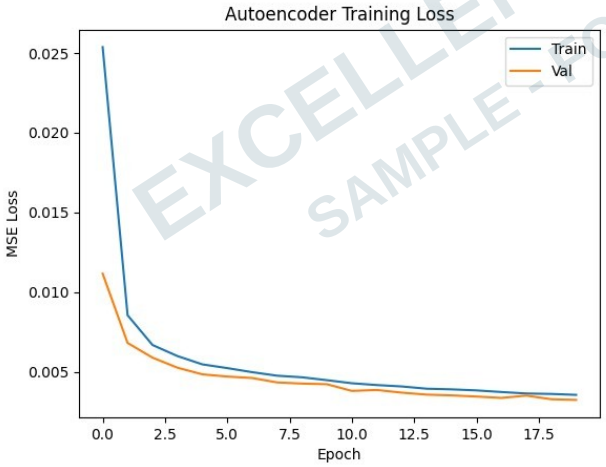

Figure 8.1.2: Autoencoder training behaviour.

The autoencoder training and the validation loss curve indicate a quick convergence of the autoencoders during the initial few epochs and then a slow stabilization. The two curves decline steadily and are highly parallel throughout training, and they ultimately come to a final mean squared error (MSE) of 0.003-0.004. The absence of a divergence between training and validation losses is a sign of stable learning and little overfitting, which proves that the attention-driven autoencoder successfully draws intrinsic patterns of real finger-vein structures [31] [32].

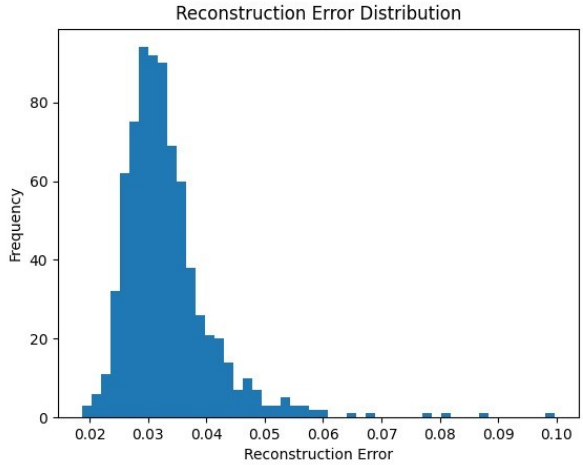

Figure 8.1.3: Reconstruction error distribution.

This is also confirmed in the reconstruction error histogram, which confirms the ability of the autoencoder to detect anomalies. True samples have a small distribution with a value of minimum reconstruction errors (about 0.025-0.035), whereas spoof samples spread in the direction of much higher values up to and including 0.10. In spite of the minimal overlap in the tails of the distributions, the general distance implies that reconstruction error is a useful discriminative feature in the detection of presentation attacks.

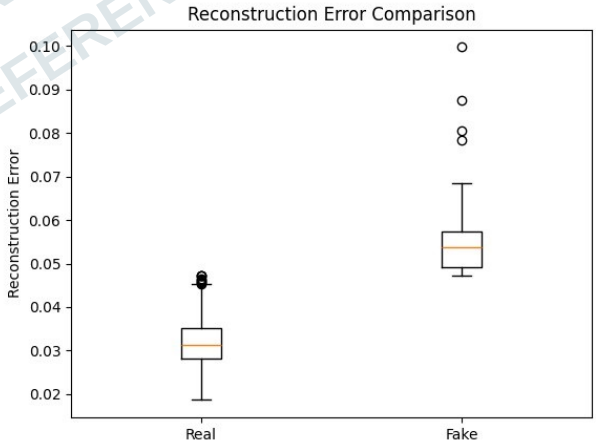

Figure 8.1.4: Reconstruction error comparison.

This observation is also supported by the boxplot comparison, which shows that the median reconstruction errors of fake samples (0.055) are higher than those of genuine samples (0.032), and that the variance and several large error outliers in the spoof class are also high. This phenomenon can be viewed as the failure of the autoencoder that is only trained on actual data to correctly recreate spoof artifacts, which usually have an unnatural texture or structural anomalies [31].

B. Discussion

The experimental outcomes validate that the unsupervised anomaly detection with supervised ensemble learning produces high PAD results, as the recent developments in the research on biometric security do [36] [37]. The autoencoder based on

EXCELLENCE INNOVATIONS
SAMPLE - FOR REFERENCE ONLY

attention captures the true finger-vein manifold as the reconstruction error is low, and it converges consistently, whereas the spoof samples generate high error rates as a result of deviations in structure and material artifacts.

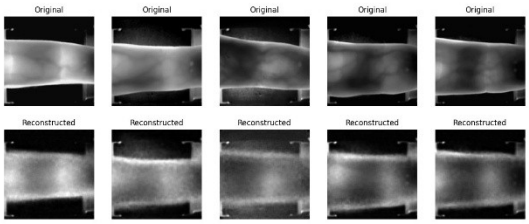

Figure 8.2.4: Original and Reconstructed Images

Nevertheless, the error of reconstruction alone cannot be sufficient to ideal separation, as shown by the similarity of the tails of distributions and the existence of individual outliers. This drawback is properly documented in the anomaly-based PAD methods and leads to the addition of auxiliary discriminative features [32]. The GAN discriminator also provides high-frequency and texture-sensitive features, and the Random Forest is efficient in combining these heterogeneous features, solving ambiguous cases, and achieving near-perfect performance.

The fact that there were no false-positives in the confusion matrix is especially worth noting, as the greatest security threat of any biometric system is the false acceptance of spoof samples (ISO/IEC 30107-3). However, the low count of false negatives indicates that even highly advanced or high-quality spoof attacks can still partly replicate real patterns. This observation is consistent with the previous research highlighting the necessity of cross-dataset and cross-PAI analysis in order to guarantee the extrapolation of results outside of controlled laboratory settings [33] [37].

In general, the findings show that VeinGuard has a positive ratio between sensitivity and robustness, and uses anomaly-related information to generalize and supervised learning to be precise.

IX. Conclusion and Recommendation

A. Conclusion

This paper introduced VeinGuard, which is a finger-vein PAD framework that combines the attention-based autoencoder, GAN-enhanced feature learning, and Random Forest classification. The test outcomes reveal that the autoencoder can learn true vein features, with different reconstruction error patterns on spoof samples, and the feature fusion and ensemble classification provide an overall accuracy of 99.65 percent and almost no false acceptance. The results of this study confirm the power of the hybridization between the unsupervised and the supervised learning models in strong biometric spoof detection, as modern research in PAD studies indicates.

B. Recommendation

To work and deploy in the future, it is suggested that:

1. Conduct leave-one-PAI-out and cross-dataset tests to assess resilience to unidentified spoofing techniques.
2. Test and evaluate more sensors and conditions of acquisition to better generalize to the real world.
3. In order to maintain long-term performance, include drift monitoring and adaptive retraining with explainability tools.
4. Research threshold optimization mechanisms, specific to particular security applications, by considering a trade-off between convenience and risk [36] [37].

References

[1] Zayed, H. L., Hamid, H. M. A., Kamal, Y. M., & Zekry, A. H. A. (2023). A comprehensive survey on finger vein biometric. *Journal of Advances in Information Technology*, *14*(2), 2-8.doi: 10.12720/jait.14.2.212-223. https://www.researchgate.net/profile/Hossam-Labib-Zayed/publication/369437121_A_Comprehensive_Survey_on_Finger_Vein_Biometric/links/642498aba1b72772e43628e9/A-Comprehensive-Survey-on-Finger-Vein-Biometric.pdf

[2] Mandalapu, H., PN, A. R., Ramachandra, R., Rao, K. S., Mitra, P., Prasanna, S. M., & Busch, C. (2021). Audio-visual biometric recognition and presentation attack detection: A comprehensive survey. *IEEE access*, *9*, 37431-37455.https://doi.org/10.1109/access.2021.3063031

[3] Syed, L., Alsaeedi, A., Alhuri, L. A., & Aljohani, H. R. (2023). Hybrid weakly supervised learning with deep learning technique for detection of fake news from cyber propaganda. *Array*, *19*, 100309.https://doi.org/10.1016/j.array.2023.100309

[4] Maiti, D., Basak, M., & Das, D. (2024). Fingerprint Bio-metric: Confronting Challenges, Embracing Evolution, and Extending Utility-A Review. *Journal of Engineering Research and Sciences*, *3*(9), 26-60.https://dx.doi.org/10.55708/js0309003

[5] Al-Khafaji, R., & Al-Tamimi, M. (2022). Vein biometric recognition methods and systems: A review. *Advances in Science and Technology Research Journal*, *16*(1), 36-46. https://doi.org/10.12913/22998624/144495

[6] Zhou, L. (2023). Finger Vein Recognition Technology: Principles, Applications, and Future Prospects. *International Journal of Biology and Life Sciences*, *3*(2), 45-48. https://pdfs.semanticscholar.org/a7b5/3a6d112271fc0660efbf4c4c761d134fe562.pdf

[7] Zayed, H. L., Hamid, H. M. A., Kamal, Y. M., & Zekry, A. H. A. (2023). A comprehensive survey on finger vein biometric. *Journal of Advances in Information Technology*, *14*(2), 2-8. Doi: 10.12720/jait.14.2.212-223

[8] Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). Enhancing Finger Vein Recognition with Image Preprocessing Techniques and Deep Learning Models. *IEEE Access*. DOI: 10.1109/ACCESS.2024.3498601

[9] Vorderleitner, A., & Uhl, A. (2025, March). Finger Vein Spoof GANs: Issues in Presentation Attack Detector Training. In *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing* (pp. 751-758). hps://doi.org/10.1145/3672608.3707714

[10] Baran, A., & Bartuzi-Trokielewicz, E. (2025). Face the Challenge—Generalization of Presentation Attack Detection. *Sensors*, *25*(18), 5792. https://doi.org/10.3390/s25185792

[11] Sharma, D., & Selwal, A. (2023). A survey on face presentation attack detection mechanisms: hitherto and future perspectives. *Multimedia Systems*, *29*(3), 1527-1577. https://doi.org/10.1007/s00530-023-01070-5

[12] Pooshideh, M., Beheshti, A., Qi, Y., Farhood, H., Simpson, M., Gatland, N., & Soltany, M. (2024). Presentation attack detection: a systematic literature review. *ACM Computing Surveys*, *57*(1), 1-32. hps://doi.org/10.1145/3687264

[13] Kaur, M., Verma, A., & Kaur, P. J. (2024). Deep learning-based finger vein recognition and security: A review. *Applied Data Science and Smart Systems*, 34-42. https://dx.doi.org/10.1201/9781003471059-5

[14] Sánchez-Caballero, A., Fuentes-Jiménez, D., & Losada-Gutiérrez, C. (2023). Real-time human action recognition using raw depth video-based recurrent neural networks. *Multimedia Tools and Applications*, *82*(11), 16213-16235. https://doi.org/10.1007/s11042-022-14075-5

EXCELLENCE IN INNOVATIONS SAMPLE - FOR REFERENCE ONLY

[15] Alhoraibi, L., Alghazzawi, D., & Alhebshi, R. (2024). Generative adversarial network-based data augmentation for enhancing wireless physical layer authentication. *Sensors*, *24*(2), 641. https://doi.org/10.3390/s24020641

[16] Saranya, K., & Valarmathi, A. (2025). A multilayer deep autoencoder approach for cross layer IoT attack detection using deep learning algorithms. *Scientific Reports*, *15*(1), 10246. https://doi.org/10.1038/s41598-025-93473-9

[17] Wone, A., Di Manno, J., Charrier, C., & Rosenberger, C. (2025). Fingerprint Spoof Generation Using Style Transfer. *IEEE Transactions on Biometrics, Behavior, and Identity Science*. https://hal.science/hal-04964484/document

[18] You, A., Kim, J. K., Ryu, I. H., & Yoo, T. K. (2022). Application of generative adversarial networks (GAN) for ophthalmology image domains: a survey. *Eye and Vision*, *9*(1), 6. https://doi.org/10.1186/s40662-022-00277-3

[19] Qin, H., Xi, H., Li, Y., El-Yacoubi, M. A., Wang, J., & Gao, X. (2023). Adversarial learning-based data augmentation for palm-v

[20] Kim, S. G., Kim, J. S., & Park, K. R. (2025). FGFNet: Fourier Gated Feature-Fusion Network with Fractal Dimension Estimation for Robust Palm-Vein Spoof Detection. *Fractal and Fractional*, *9*(8), 478.https://doi.org/10.3390/fractalfract9080478

[21] Jain, S., Seth, G., Paruthi, A., Soni, U., & Kumar, G. (2022). Synthetic data augmentation for surface defect detection and classification using deep learning. *Journal of Intelligent Manufacturing*, *33*(4), 1007-1020.https://doi.org/10.1007/s10845-020-01710-x

[22] Vajrobol, V., Saxena, G. J., Pundir, A., Singh, S., B. Gupta, B., Gaurav, A., & Rahaman, M. (2025). Identify spoofing attacks in Internet of Things (IoT) environments using machine learning algorithms. *Journal of High Speed Networks*, *31*(1), 61-70.https://doi.org/10.1177/09266801241295886

[23] Sreekumar A, Kumar, S., & Sreemol R. (2023). A Secure Finger vein Recognition System using WS-Progressive GAN and C4 Classifier. *International Journal of Biometrics*, *1*(1), 1–1. https://doi.org/10.1504/ijbm.2024.10053719

[24] Alkhouly, A. A., Mohammed, A., & Hefny, H. A. (2021). Improving the Performance of Deep Neural Networks Using Two Proposed Activation Functions. *IEEE Access*, *9*, 82249–82271. https://doi.org/10.1109/access.2021.3085855

[25] Sadiq, T., & Omlin, C. W. (2025). Sensing in Smart Cities: A Multimoda Machine Learning Perspective. *Smart Cities*, *9*(1), 3.https://doi.org/10.3390/smartcities9010003

[26] Duan, R., Chen, Z., Zhang, H., Wang, X., Meng, W., & Sun, G. (2023). Dual residual denoising autoencoder with channel attention mechanism for modulation of signals. *Sensors*, *23*(2), 1023.https://doi.org/10.3390/s23021023

[27] Habeeb, D., Alhassani, A. H., Abdullah, L. N., Der, C. S., & Alasadi, L. K. Q. (2024). Advancements and Challenges: A Comprehensive Review of GAN-based Models for the Mitigation of Small Dataset and Texture Sticking Issues in Fake License Plate Recognition. *Engineering, Technology & Applied Science Research*, *14*(6), 18401-18408.https://doi.org/10.48084/etasr.8870

[28] Mathew, A., & Amudha, P. (2024). Improved Finger Vein Recognition Using Generative Adversarial Network and Transfer Learning. *Journal of Nanoelectronics and Optoelectronics*, *19*(10), 1042-1052.https://doi.org/10.1166/jno.2024.3643

[29] Kim, S. G., Hong, J. S., Kim, J. S., & Park, K. R. (2024). Estimation of fractal dimension and detection of fake finger-vein images for finger-vein recognition. *Fractal and Fractional*, *8*(11), 646.https://doi.org/10.3390/fractalfract8110646

[30] Li, F., Chen, Y., Liu, H., Zhao, Z., Yao, Y., & Liao, X. (2024). Vocoder detection of spoofing speech based on GAN fingerprints and domain generalization. *ACM Transactions on Multimedia Computing, Communications and Applications*, *20*(6), 1-20.https://doi.org/10.1145/3630751

[31] Givnan, S., Chalmers, C., Fergus, P., Ortega-Martorell, S., & Whalley, T. (2022). Anomaly Detection Using Autoencoder Reconstruction upon Industrial Motors. Sensors, 22(9), 3166. https://doi.org/10.3390/s22093166

[32] Chen, L., Guo, T., Li, L., Jiang, H., Luo, W., & Li, Z. (2023). A Finger Vein Liveness Detection System Based on Multi-Scale Spatial-Temporal Map and Light-ViT Model. Sensors, 23(24), 9637. https://doi.org/10.3390/s23249637

[33] Demircioğlu, A. (2024). The effect of feature normalization methods in radiomics. Insights into Imaging, 15(1). https://doi.org/10.1186/s13244-023-01575-7

[34] Du, Y., Huang, Y., Wan, G., & He, P. (2022). Deep Learning-Based Cyber–Physical Feature Fusion for Anomaly Detection in Industrial Control Systems. Mathematics, 10(22), 4373. https://doi.org/10.3390/math10224373

[35] Guehairia, O., Ouamane, A., Dornaika, F., & Taleb-Ahmed, A. (2020). Feature fusion via Deep Random Forest for facial age estimation. Neural Networks, 130, 238–252. https://doi.org/10.1016/j.neunet.2020.07.006

[36] Gomez-Alanis, A., Gonzalez-Lopez, J. A., & Peinado, A. M. (2022). GANBA: Generative Adversarial Network for Biometric Anti-Spoofing. Applied Sciences, 12(3), 1454. https://doi.org/10.3390/app12031454

[37] Kim, S. G., Choi, J., Hong, J. S., & Park, K. R. (2022). Spoof detection based on score fusion using ensemble networks robust against adversarial attacks of fake finger-vein images. Journal of King Saud University - Computer and Information Sciences, 34(10), 9343–9362. https://doi.org/10.1016/j.jksuci.2022.09.012

[38] Hsia, C.-H., Ke, L.-Y., & Chen, S.-T. (2023). Improved Lightweight Convolutional Neural Network for Finger Vein Recognition System. Bioengineering, 10(8), 919. https://doi.org/10.3390/bioengineering10080919

[39] Das, P., McGrath, J., Fang, Z., Boyd, A., Jang, G., Mohammadi, A., Purnapatra, S., Yambay, D., Marcel, S., Trokielewicz, M., Maciejewicz, P., Bowyer, K., Czajka, A., Schuckers, S., Tapia, J., Gonzalez, S., Fang, M., Damer, N., Boutros, F., … Ross, A. (2020). Iris Liveness Detection Competition (LivDet-Iris) -- The 2020 Edition (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2009.00749

EXCELLENCE INNOVATIONS
SAMPLE FOR REFERENCE ONLY