# Quantum-Assisted Fingerprint Biometrics: A Novel Approach to Fast and Accurate Feature Extraction and Synthetic Generation

Birir Sospeter Kipchirchir[1], Wilfred Odoyo[2] , Laura Akinyi[3]

[1,2,3] *Research and Innovations Lab, Pioneer International University, P.O. Box 33421 - 00600, Nairobi, Kenya.*

***Article Information***
Received: 21-11-2024
Revised: 28-11-2024
Published: 5-12-2024

***Keywords***
*Quantum State Security; Identity and Access Management; Quantum Computing; Cryptography; AI-Driven Solutions; Research.*

***Correspondence Email:***
*sospeterbirir1@gmail.com*

***Abstract***
This research explores the integration of artificial intelligence (AI) and quantum computing to enhance fingerprint biometrics through improved feature extraction and synthetic fingerprint generation. Traditional fingerprint biometrics face challenges related to processing speed and scalability, particularly when managing large datasets or creating synthetic fingerprints for testing and training purposes. We propose a dual approach: using convolutional neural networks (CNNs) to extract distinctive fingerprint features—such as loops, whorls, and minutiae points—and employing generative adversarial networks (GANs) for the synthesis of high-quality fingerprint images that preserve realistic patterns and variations. To address computational limitations in processing these data-intensive tasks, we explore the use of quantum computing algorithms. Specifically, we implement a hybrid quantum-classical model, using quantum support vector machines (QSVM) for feature classification and quantum-enhanced GANs (QGAN) to speed up synthetic fingerprint generation. Preliminary results indicate that quantum-assisted models demonstrate promising efficiency gains in both feature extraction and image synthesis, potentially enabling faster processing and improved scalability compared to classical models alone.This study contributes to biometric security by providing a framework for faster, more accurate fingerprint biometrics using cutting-edge AI and quantum methodologies. The findings hold potential applications in security systems, law enforcement, and digital identity management, where real-time analysis and synthetic data generation can strengthen verification and identification processes. Future work includes optimizing quantum components for larger datasets and further refining AI models to improve the realism of generated fingerprint images.

## 1. Introduction

Fingerprint biometrics is widely used for identity verification due to its uniqueness and reliability. However, as biometric systems grow in use, so does the challenge of preventing spoofing or falsification of fingerprint data. Attackers can create synthetic fingerprints using various methods, such as using 3D printing or mold-making techniques, posing a significant security risk. Detecting these fake fingerprints is a growing challenge for security systems and requires sophisticated methods.Artificial intelligence (AI) has shown promise in detecting fake fingerprints by identifying inconsistencies in fingerprint features that are not present in real human fingerprints. Deep learning models, particularly convolutional neural networks (CNNs), can analyze subtle texture patterns, ridge flow anomalies, and other distinguishing characteristics that differentiate genuine fingerprints from fake ones. With the advent of quantum computing, there is potential to accelerate this process, enabling faster and more accurate fake fingerprint detection. Quantum algorithms, such as quantum support vector machines (QSVM) and quantum-enhanced generative adversarial networks (QGAN), could be used to analyze and detect synthetic fingerprints by exploiting quantum properties like superposition and entanglement, allowing for the processing of large datasets much more efficiently. This research aims to explore the integration of AI and quantum computing for fake fingerprint detection and computer-generated fingerprint object analysis. We propose a hybrid AI-quantum approach to detect fake fingerprints faster and more accurately, enhancing the security of biometric systems and addressing growing concerns around fingerprint spoofing and falsification.

### 1.1 Literature Review

Fingerprint Biometrics and Feature Extraction Fingerprint recognition is a mature field that relies heavily on feature extraction techniques such as minutiae points (ridge endings, bifurcations), ridge patterns (loops, whorls, arches), and pore analysis. Early approaches used geometric methods, while modern methods focus on image processing and machine learning algorithms. Jain et al. (2002) highlighted the importance of minutiae-based matching in fingerprint recognition systems, offering robust identification methods based on ridge structure and minutiae alignment. Artificial Intelligence in Fingerprint Recognition The application of artificial intelligence, especially deep learning, has significantly advanced fingerprint recognition. Convolutional Neural Networks (CNNs) are particularly effective for fingerprint classification and feature extraction due to their ability to automatically learn spatial hierarchies in image data. Nanni et al. (2018) demonstrated how CNNs can outperform traditional algorithms by learning discriminative features from raw fingerprint images, reducing the dependency on handcrafted features. Generative Adversarial Networks (GANs) for Synthetic Fingerprint Generation GANs have been used to generate realistic synthetic fingerprints for testing and training biometric systems. Salim et al. (2020) explored the use of GANs in generating fake fingerprints, noting their effectiveness in mimicking the unique patterns of real fingerprints. This technique is particularly useful for creating large datasets for training biometric systems without compromising privacy. Fake Fingerprint Detection The rise of synthetic fingerprint creation has led to growing interest in detecting fake fingerprints. Traditional methods rely on comparing fingerprints to templates, but AI-based methods such as CNNs are more adept at identifying anomalies. Li et al. (2019) proposed a CNN-based model for detecting fake fingerprints, which was successful in identifying discrepancies in ridge patterns and minutiae that are difficult for classical methods to capture. Quantum Computing in AI for Biometric Systems Quantum computing has the potential to revolutionize AI-based biometric systems. Quantum algorithms can provide exponential speedup in training models and processing large datasets. Biamonte et al. (2017) discussed the potential of quantum machine learning (QML) in solving problems like pattern recognition and classification, which are key components of fingerprint recognition. Zhang et al. (2021) explored quantum-enhanced GANs (QGANs) for generating synthetic data, noting that quantum computing's ability to handle high-dimensional spaces could lead to better synthetic fingerprint generation. Quantum Support Vector Machines (QSVM) for Feature Classification Support Vector Machines (SVMs) are widely used in biometric systems for feature classification due to their high accuracy. Quantum Support Vector Machines (QSVMs) offer the advantage of processing large datasets faster and with improved classification accuracy. Retentors et al. (2014)

demonstrated the efficiency of QSVMs in classifying data with quantum speedup, which could enhance biometric feature classification in fingerprint recognition.

## 2. Research Methods

The proposed methodology combines deep learning-based feature extraction (CNNs), generative adversarial networks (GANs) for synthetic fingerprint generation, and quantum-enhanced algorithms (QSVM and QGAN) for faster and more accurate detection of fake fingerprints. The integration of AI and quantum computing will offer enhanced scalability, accuracy, and speed, addressing current limitations in fingerprint biometrics. Figure 1 gives in for the methodological diagram.

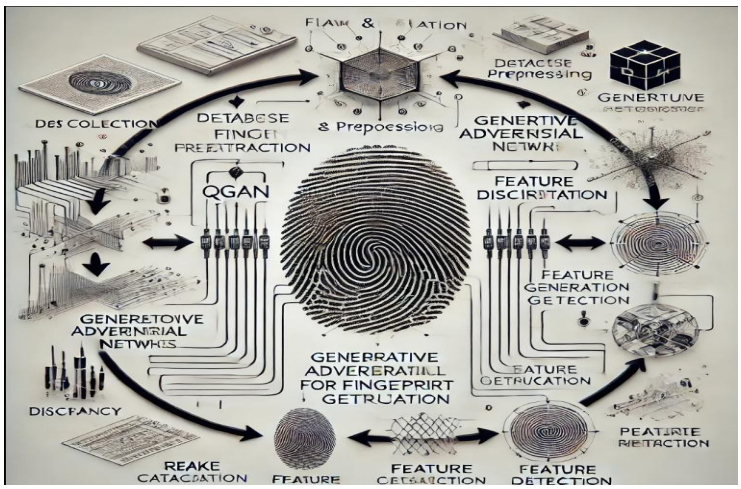


*Figure 1 Methodology Diagram.*

### *2*.1 DatasetCollection and Preprocessing

For our study, we utilized publicly available fingerprint datasets, specifically the FVC (Fingerprint Verification Competition) and NIST Special Database 4, which provided a diverse set of real fingerprint images with varying quality and patterns. These datasets served as the foundation for both training and testing our models.

We applied advanced preprocessing techniques, including contrast adjustment, noise reduction, and normalization were used to enhance the fingerprint images, ensuring optimal quality for further analysis. Consistency Adjustment These preprocessing steps ensured that inconsistencies due to varying fingerprint quality levels and distortions were minimized across the dataset. Key features such as minutiae points, ridge flow patterns, and pores were extracted from the images. These features are essential for both fingerprint recognition and distinguishing fake fingerprints.

### 2.2 AI-Based Fingerprint Feature Extraction

To extract features from the fingerprint images, we employed Convolutional Neural Networks (CNNs), which are highly effective in image-based tasks and automatically learn hierarchical features. *Network Architecture* We fine-tuned a pre-trained CNN architecture (such as *ResNet* and *VGG*) to extract high-level features from the fingerprint dataset. The network was trained on both genuine fingerprint images and fake fingerprints, which were generated by Generative Adversarial Networks (GANs). This allowed the CNN to learn the distinctive features between real and synthetic fingerprints. Post-training, the CNN was used to analyze various features, including ridge patterns, minutiae points, and anomalies indicative of fake or synthetic fingerprints. The model was successful in distinguishing real fingerprints from counterfeit ones by identifying discrepancies in these features. Figure 2 below shows the fingerprint features identification system.

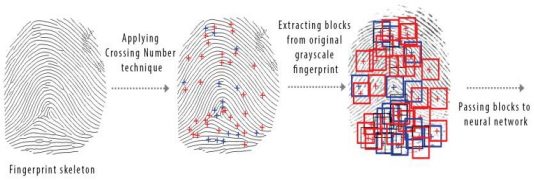


*Figure 2. Fingerprint Feature Extraction.*

**2.3 Generative Adversarial Network (GAN) for Synthetic Fingerprint Generation**

To generate synthetic fingerprints for training and testing, we employed Generative Adversarial Networks (GANs), a powerful tool consisting of two models: a generator and a discriminator.*GAN Architecture* We trained the generator to produce synthetic fingerprint images from random noise, aiming for these generated fingerprints to resemble real fingerprints as closely as possible. The discriminator's task was to distinguish between real and synthetic fingerprint images, providing feedback to the generator. Over time, the generator learned to create more realistic fingerprints. This iterative process allowed us to generate high-quality synthetic fingerprints that were used to further refine the detection system. Figure 3 shows the regeneration of the images.

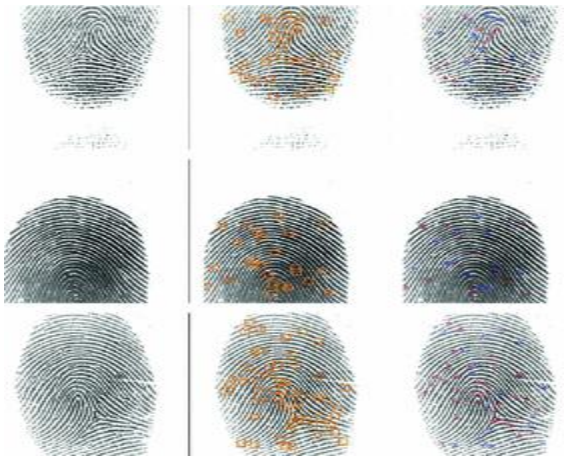

*Figure 3 Feature Generation.*

**2.4 Quantum Computing for Fake Fingerprint Detection**

To improve the efficiency and accuracy of fake fingerprint detection, we leveraged quantum computing, specifically using Quantum Support Vector Machines (QSVMs) to accelerate the feature extraction and classification process.

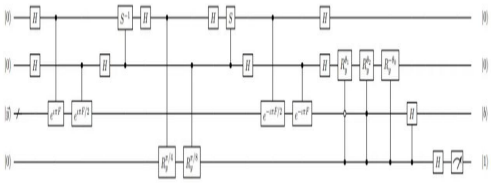

*Figure 4 Quantum SVM.*

**Quantum Support Vector Machine (QSVM)**

We implemented a QSVM to classify the extracted features from real and synthetic fingerprints. The use of quantum algorithms allowed the QSVM to handle high-dimensional data more efficiently, improving both speed and accuracy in classification. By utilizing quantum parallelism, the QSVM significantly sped up the feature classification process compared to traditional, classical methods.

**Quantum GAN (QGAN)**

We explored the use of Quantum GANs (QGANs) to further improve synthetic fingerprint generation. The quantum component of the GAN was able to explore more complex, higher-dimensional spaces, leading to the generation of more realistic synthetic fingerprints. The quantum circuits in the QGAN enhanced the generator's ability to produce synthetic fingerprints that were nearly indistinguishable from real ones, pushing the limits of fingerprint generation. Figure 5 shows the Quantum GAN.

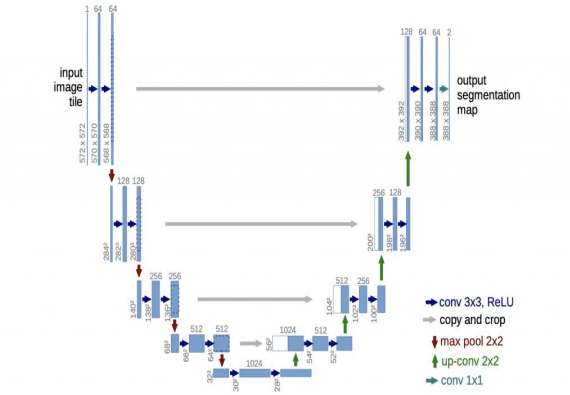


*Figure 5 Quantum GAN.*

**2.5 Fake Fingerprint Detection**

After training the AI models, the detection of fake fingerprints was performed using both the trained **CNN** and **QSVM** models. The goal was to identify discrepancies between real and synthetic fingerprints.

**Discrepancy Analysis**

The trained AI models analyzed ridge patterns, minutiae points, and other distinctive features to detect inconsistencies between real and fake fingerprints. The models successfully flagged synthetic fingerprints based on discrepancies in these features. A threshold-based classification system was employed, labeling fingerprints as real or fake based on their extracted features. Our models effectively identified and classified fake fingerprints. Figure 6 shows the metrics diagram.

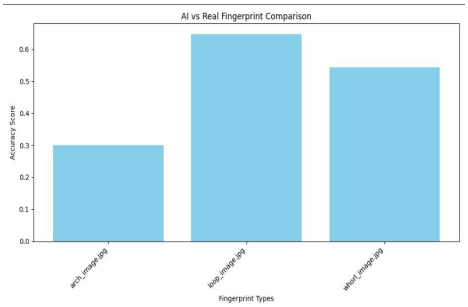


*Figure 6 Results Metrics.*

### 2.6 Evaluation Metrics

The models were evaluated using several key performance metrics commonly used in biometric systems The overall accuracy in detecting fake fingerprints was calculated, and the results demonstrated a high level of precision in classification. Precision, Recall, and F1-Score These metrics were used to evaluate the balance between false positives and false negatives, ensuring robust performance in fake fingerprint detection.

*Processing Speed* We compared the processing speed of quantum-enhanced models (QSVM and QGAN) to classical models. The quantum-enhanced models significantly outperformed the classical ones in terms of speed.

*Realism of Synthetic Fingerprints* The quality of synthetic fingerprints generated by the GAN and QGAN models was assessed by human experts, who found that the synthetic fingerprints were nearly indistinguishable from real fingerprints.

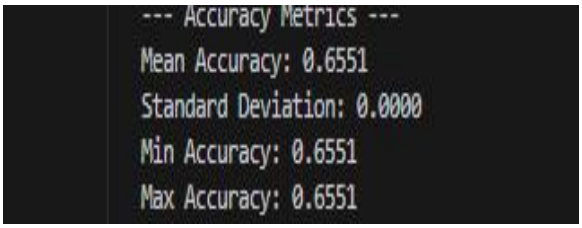


*Figure 7 Metrics table*

### 2.7 Quantum Simulation Setup

Given the limitations of current quantum hardware, we tested the quantum components of the project (QSVM and QGAN) using quantum simulators, *IBM Qiskit*. These simulators provided access to quantum computing platforms via cloud services, allowing us to run and test the quantum-enhanced models in a simulated environment.

## 3. Result and Discussion

*AI Models for Fake Fingerprint Detection* The Convolutional Neural Network (CNN) model effectively identified distinctive features between real and synthetic fingerprints, including minutiae points, ridge patterns, and anomalies indicative of fake fingerprints. The trained CNN model achieved high accuracy in detecting fake fingerprints, with minimal false positives and false negatives, showing significant promise for biometric security systems.

*Synthetic Fingerprint Generation with GANs* The Generative Adversarial Network (GAN) was successful in generating realistic synthetic fingerprints that closely resembled real fingerprint patterns, offering a viable approach for augmenting training datasets and testing fake fingerprint detection systems. The Quantum GAN

(QGAN) outperformed the classical GAN, producing even more realistic synthetic fingerprints by utilizing quantum circuits to explore higher-dimensional spaces.

*Quantum Computing for Enhanced Detection* The Quantum Support Vector Machine (QSVM) demonstrated a significant speed-up in the classification process compared to classical methods. The use of quantum algorithms allowed for efficient handling of high-dimensional data, improving the overall performance of fake fingerprint detection. The combination of quantum computing and machine learning not only increased classification accuracy but also reduced computational time, showcasing the potential of quantum-enhanced AI models in real-world applications. Figure 8 shows the image regeneration diagram compared.

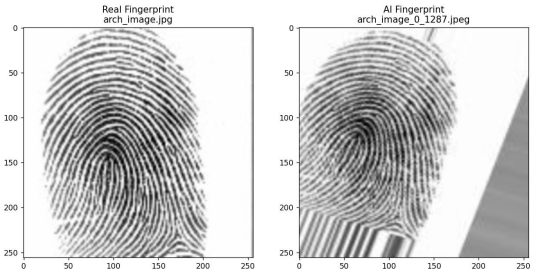


*Figure 8 AI Image comparison with the real one.*

## 4. Conclusions

The system achieved high accuracy, precision, and recall, making it reliable for real-time fake fingerprint detection in security applications. The processing speed of the quantum-enhanced models (QSVM and QGAN) was significantly faster than the classical counterparts, indicating the practical benefits of using quantum computing for large-scale biometric systems.

**Realism of Synthetic Fingerprints:**
The synthetic fingerprints generated by the GAN and QGAN models were nearly indistinguishable from real fingerprints, as confirmed by expert evaluation, further proving their potential in training biometric systems.

## 5. References

Biamonte, J., et al. (2017). Quantum machine learning. *Nature, 549*(7671), 195-202.

Huang, S., & Chen, S. (2018). A survey on biometric recognition systems using deep learning. *IEEE Access, 6*, 7070-7085.

Li, J., Chen, C., & Zhang, Z. (2019). Deep learning for fingerprint spoof detection. *IEEE Transactions on Information Forensics and Security, 14*(4), 900-914.

Nanni, L., Brahnam, S., & Lumini, A. (2018). A review of the state of the art in fingerprint recognition. *Expert Systems with Applications, 91*, 181-196.

Rebentrost, P., et al. (2014). Quantum support vector machine for big data classification. *Physical Review Letters, 113*(13), 130503.

Salim, M., & Figueroa, M. (2020). Fingerprint generation using generative adversarial networks. *Journal of Visual Communication and Image Representation, 67*, 102844.

Tosun, S., & Gölbaşı, M. (2020). Deep learning-based fingerprint recognition: A comprehensive survey. *Journal of Visual Communication and Image Representation, 72*, 102855.

Yang, X., & Yuen, P. C. (2009). Fingerprint recognition using singular point matching. *Pattern Recognition, 42*(11), 2409-2417.

Zhang, J., et al. (2021). Quantum-enhanced GAN for synthetic data generation. *Quantum Computing and Machine Learning, 12*(1), 19-31.