# Advancing Biometric Authentication: A Framework for Template Reconstruction Attack Detection

**Y. Teja**

Department of Computer Science and Engineering, SRM University-AP, Amaravati, Andhra Pradesh, India

**Koutharapu Babinadh**

Department of Computer Science and Engineering, SRM University-AP, Amaravati, Andhra Pradesh, India

**Venkata Satya Koushik Devarabhotla**

Department of Computer Science and Engineering, SRM University-AP, Amaravati, Andhra Pradesh, India

**Nithin Sai Manchikalapudi**

Department of Computer Science and Engineering, SRM University-AP, Amaravati, Andhra Pradesh, India

**Dilip Kumar Vallabhadas**

Department of Computer Science and Engineering, Centre for Interdisciplinary Research, SRM University-AP, Amaravati, Andhra Pradesh, India

## Abstract:

Although fingerprint biometrics are broadly used in authentication systems, they are facing a serious problem: in case the templates are stolen or compromised, the original fingerprint patterns can be restored. Such reconstruction attacks allow adversaries to create synthetic fingerprints to bypass authentication or gain access to large-scale systems. Complementary to most traditional cancelable biometric approaches aiming at template protection, we tackle for the first time the practical problem of detecting such reconstruction attempts before causing misuse. We propose a hybrid dynamic projection-based detection framework identifying inconsistencies between genuine fingerprint embeddings and synthetically reconstructed templates. Based on a ResNet-50 backbone trained with metric learning, our system extracts robust 512-D embeddings and projects them dynamically with a hybrid projection to produce protected templates. The reconstructed samples show measurable deviations in projection consistency, score distribution, and correlation structure, allowing our system to reliably detect attacks while minimally influencing normal authentication accuracy. Based on expensive experiments using the CASIA-FingerprintV5 dataset and extensive simulated attack scenarios, we explain that the proposed approach provides strong attack detection performance at improved high recognition.

## Keywords:

Fingerprint biometrics, template reconstruction attack, biometric security, cancelable biometrics, dynamic random projection, deep learning, ResNet-50, attack detection, biometric forensics.