Biometric Authentication with Data Privacy

Vireshwar Kumar
Assistant Professor
Computer Science & Engineering
Indian Institute of Technology Delhi

July 6, 2025

Agenda

- Facial Recognition and Authentication
- Challenges with Data Privacy
- Enabling Data Privacy
  - Machine Learning
  - Cryptography

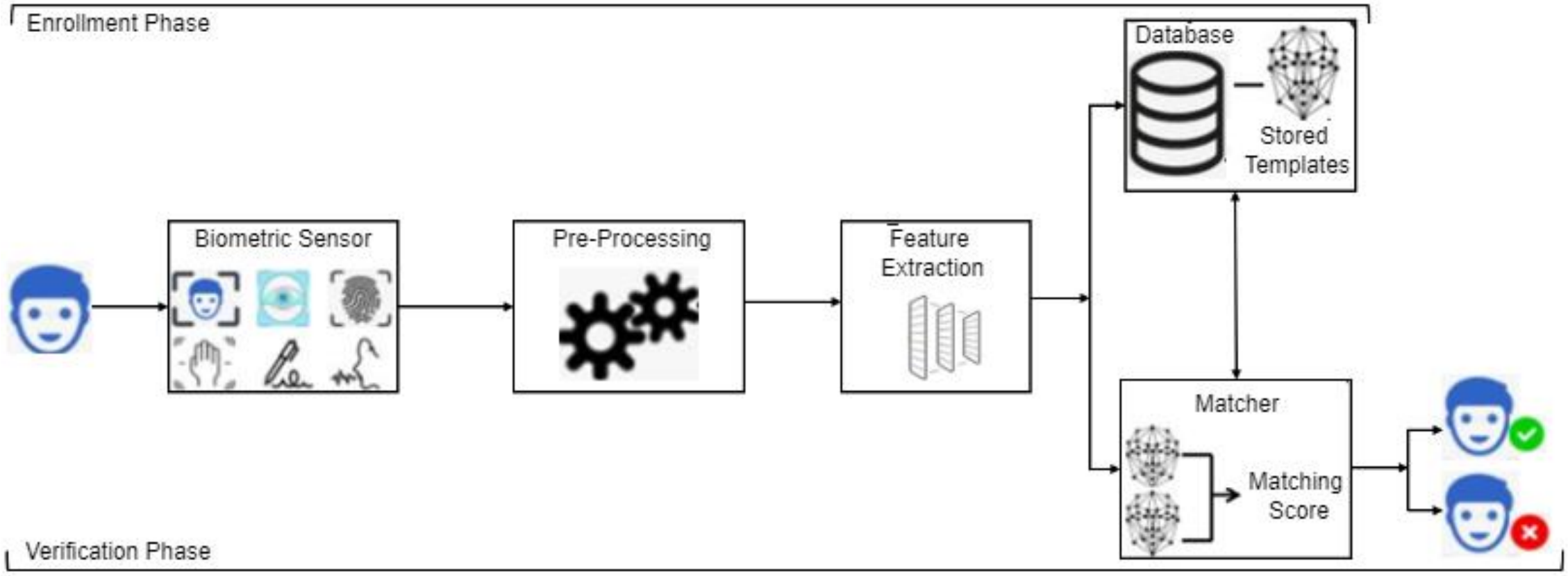
User Authentication

Authentication Type	Example
What I Know (Knowledge-Based)	Password, Passphrase, PIN, Security Question
What I Have (Possession-Based)	Smart Card, USB Token, Mobile Phone
What I Am (Biometric-Based)	Fingerprint, Iris, Face, Voice

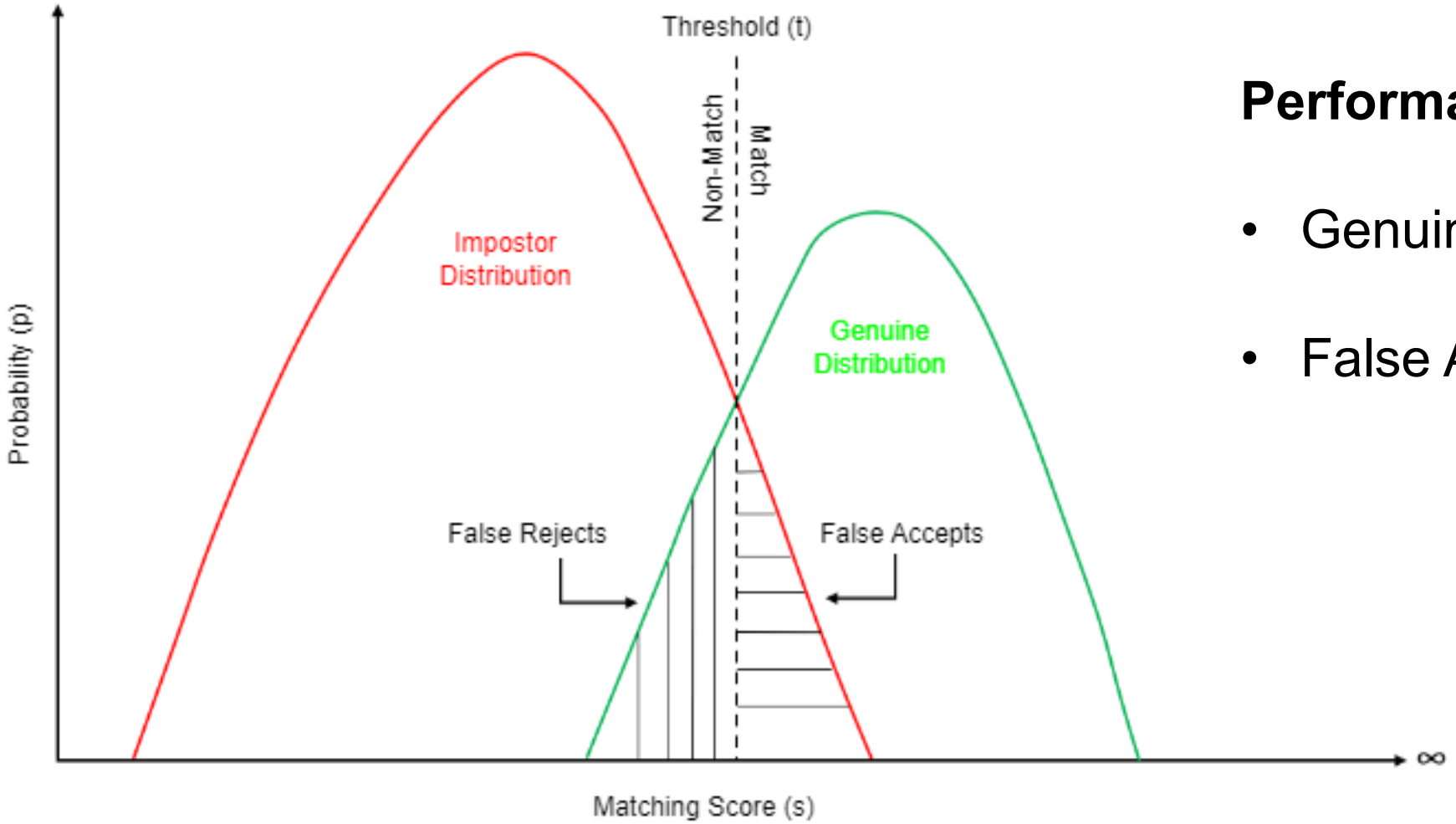
Why Biometrics?

- Convenience
- Reliability
- Security

Typical Biometric Authentication



Performance Evaluation



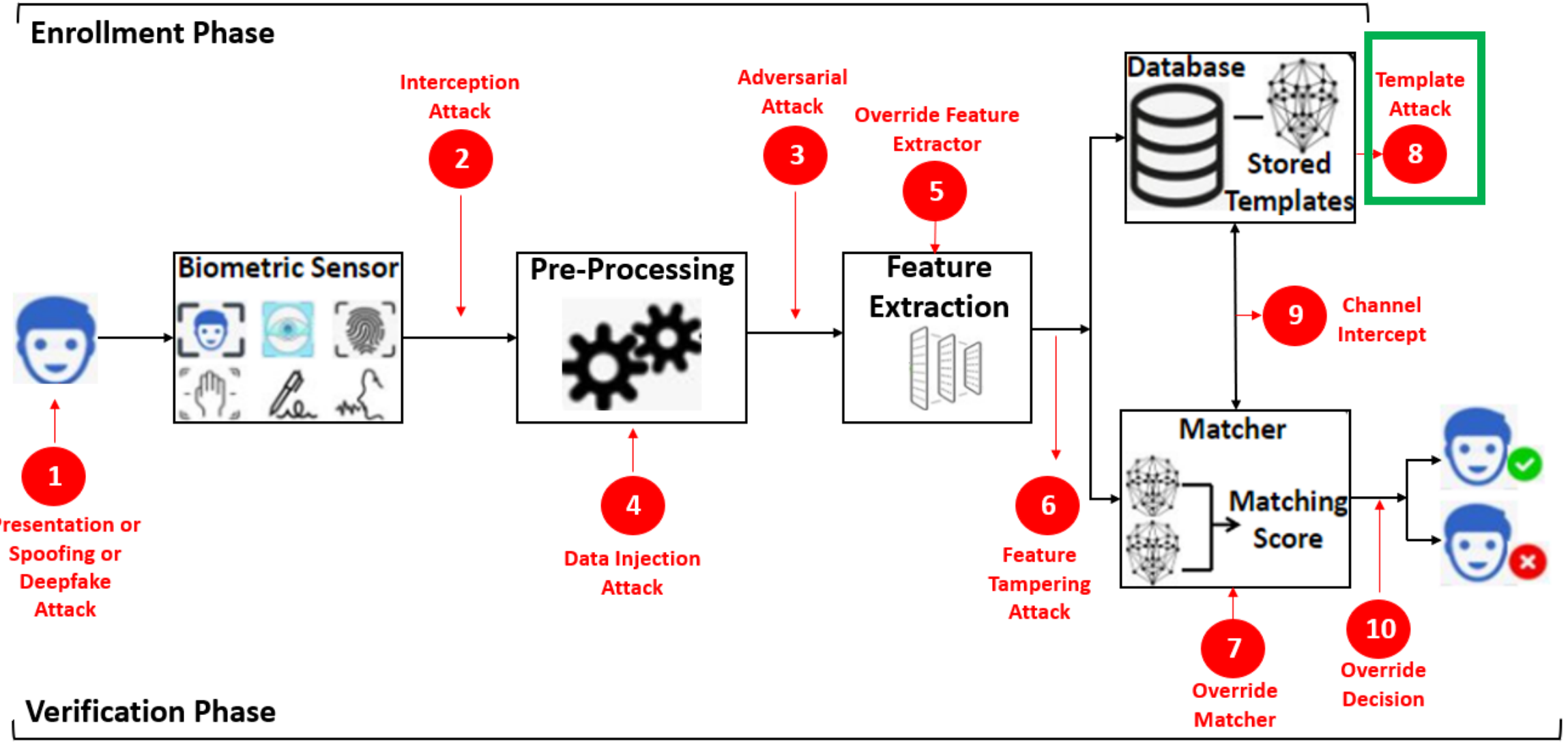
Performance Metrics

- Genuine Accept Rate (GAR)
- False Accept Rate (FAR)

Critical Concerns

- Easy to capture
- Non-revocable

Attack Surfaces



Implications of Template Attack

- Inversion: Reconstruct the biometric data (face image) from the template

- Impersonation: Alter attacker’s biometric traits to match victim’s template

Demo of Reconstruction Attack

- Requires GPU support.

- Dong, Xingbo, et al. "Reconstruct face from features based on genetic algorithm using GAN generator as a distribution constraint." Computers & Security 125 (2023): 103026. https://dl.acm.org/doi/10.1016/j.cose.2022.103026

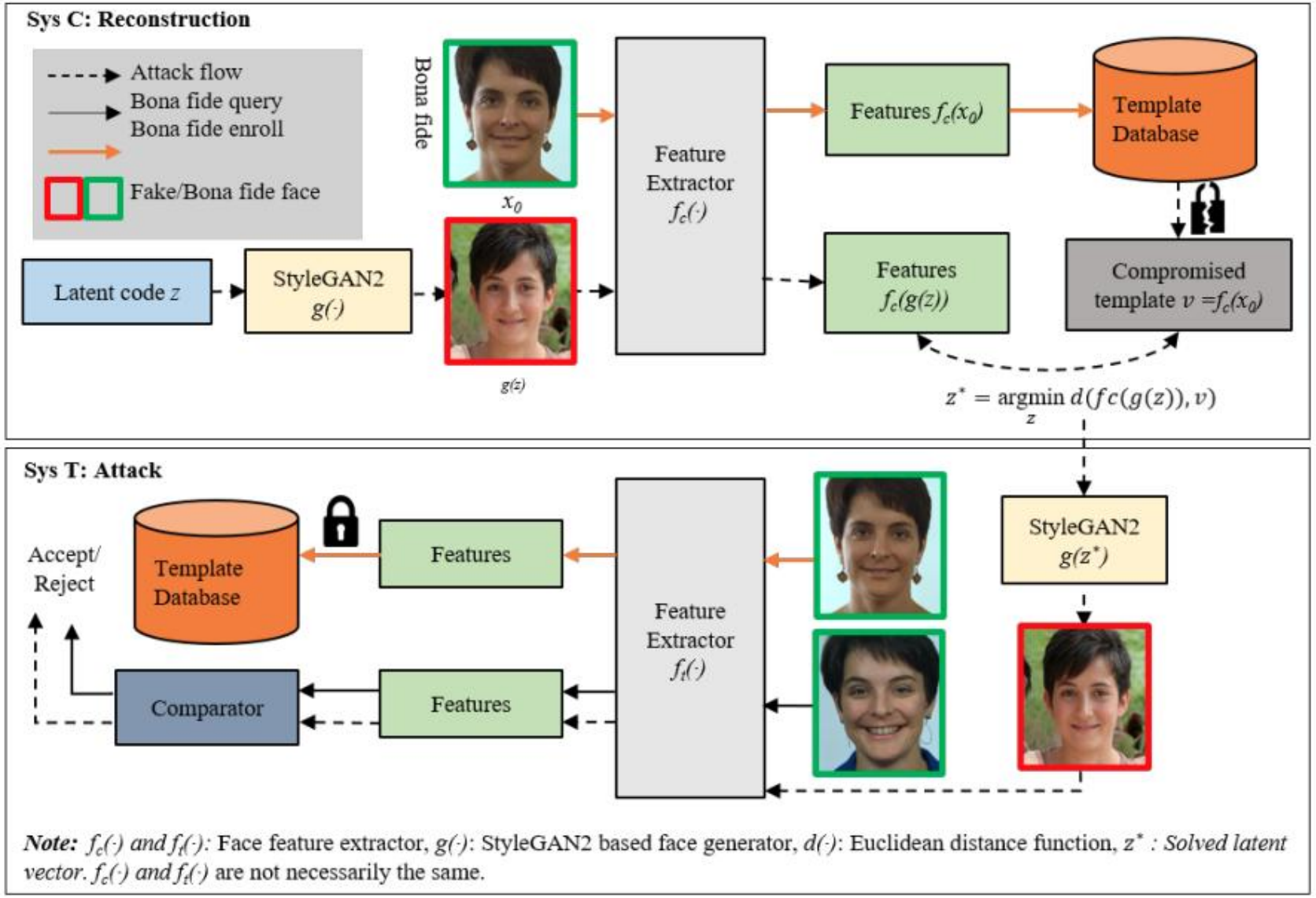
- Github Link: https://github.com/xingbod/FromDeepFeatures2HQFace

Threat Model

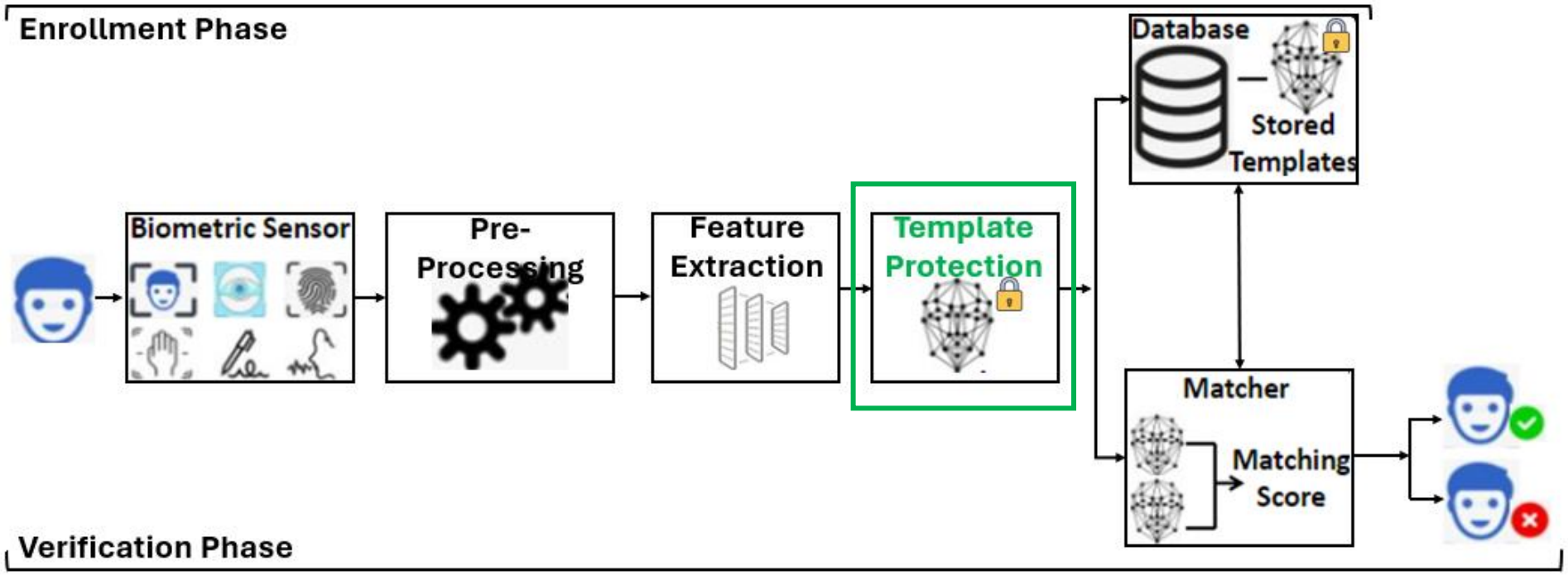
- Goal
  - Generate the original face image of the victim

- Knowledge
  - Blackbox

Reconstruction: Generative Adversarial Network



Biometric Template Protection



Requirements:

- Security
- Performance
- Revocability or Renewability
- Diversity or Unlinkability

Potential Template Protection Methodology

Machine Learning

Cryptography

Potential Ideas

- Hashing
- Encryption

User-Specific Random Projection

- Idea
  - Each user has a secret key (like a password)
  - Key generates a unique random transformation matrix

- Implication
  - Without the user's specific key, the original biometric cannot be recovered

- Google Colab Code prepared by Sainath
  - https://colab.research.google.com/drive/1ZupFesT-0DWR5At2LqfoXQmOWl1yT1WL?usp=sharing

Homomorphic Encryption

- Key Generation
- Encryption
- Evaluation
- Decryption

Thank you!

Vireshwar Kumar

viresh@cse.iitd.ac.in

http://www.cse.iitd.ac.in/~viresh/