Swastham Bhavati

Face Biometric Tech Spec

Revision 1.0
June 18, 2023

Milind Deore

Dayananda Sagar College of Engineering
Shavige Malleshwara Hills, 91st Main Rd,
1st Stage, Kumaraswamy Layout,
Bengaluru, Karnataka 560078

https://github.com/Project-Niramaya

Niramaya

Face Biometric - Technical Specification

Niramaya's face biometric is designed for end-user / edge devices like: mobile, smart watches, IOT devices. It's secure, robust, offering better protection than Passwords / PINs, Fingerprints, Iris scans. The solution features quick and easy enrollment / verification right on the edge device without the need of cloud computing. Alongside, we are also developing a cloud based solution for applications that requires scaling. All the applications that require authentication are the potential use cases for Niramaya's biometric solution.

Niramaya provides maximum security against unauthorized attempts to breakin, while ensuring highest verification rates for the user.

Biometric raw data is not retained?

With Niramaya's biometric, it is not necessary to store raw images on the device and never send them to the cloud. The image data is processed immediately by the algorithms and then discarded. The biometric data is stored in a mathematical representation (as 'Embeddings', data structure) that our proprietary algorithms understand; they are stored in a protected area of the app.

Biometric data is encrypted and inaccessible?

The biometric processed / unprocessed data are stored on the device locations that are not accessible to the other apps on the device. For example, Niramaya's Android sample app uses the Android Application Sandbox, which isolates the application data and code execution from other apps, similarly iOS App Sandbox as well. Niramaya also offers a data encryption option whereby all the data is encrypted before writing to the device storage.

Cloud computing is used during the validation process?

Niramaya offers only edge devices specific solutions, this means there is no cloud computing involved or any cloud handshaking is required, neither data nor any validation task talks to the cloud. Users can use the Niramaya solution in the offline mode too, where there is no internet connection present and still they unlock their devices for accessing services.

Niramaya

What does Niramaya's biometric SDK provide?

1. Face biometric library with APIs, it's written in C++ and optimized for ARM and x86.
2. Platform specific sample app including source code.
3. SDK API documentation.
4. Platforms supported: Android, iOS, Linux, OSX.

Face Biometric Features?

1. Enrolment of user face for multiple users on a device.
2. Verification of user face.
3. Strong patented liveness detection to avoid presentation attacks via photo or recorded video.
4. Early anomaly detection.
5. Complete edge solution and no-cloud computing is required.
6. Fast, small neural network models, compact library, and simple to use.
7. Configure security levels to protect on-device data.

Memory requirements by the library?

The core of the library consists of neural network models and C++ code. These models are dynamically loaded onto the device for a specific service, currently only face biometric.

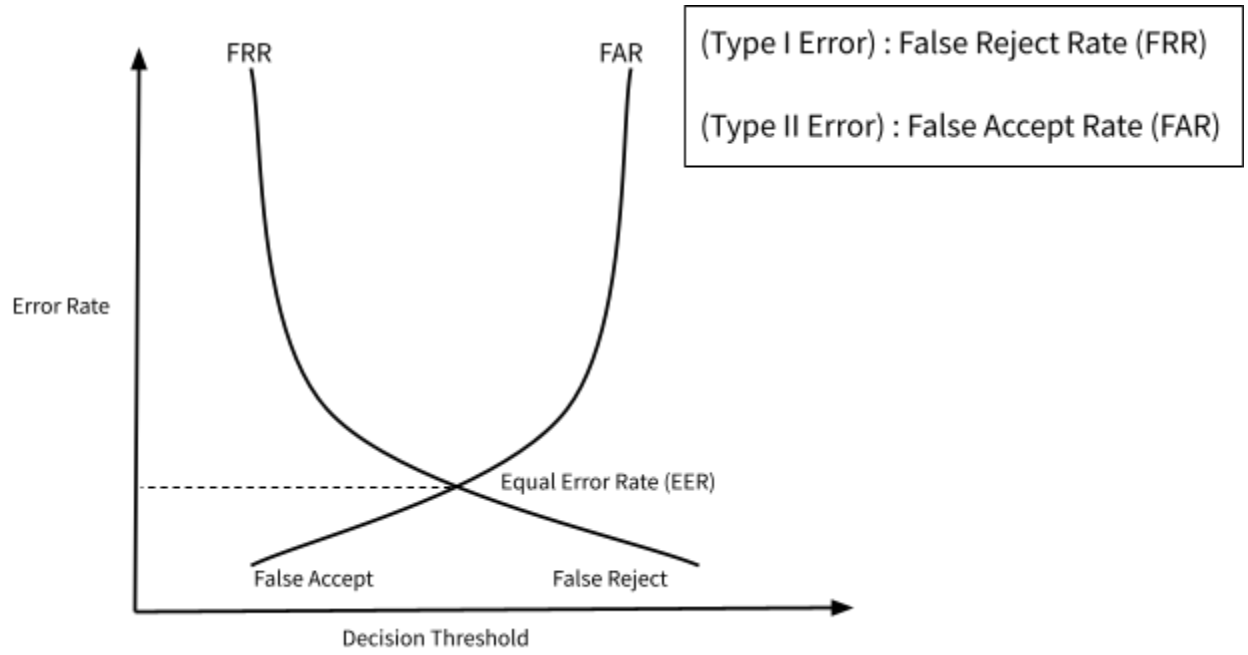
Overall size for all neural network models for face biometric : **4.1 MB**
Neural network utilize tensorflow lite library (size) : **3.7 MB**
OpenCV for image processing (size) : **6 MB**
Overall size of C++ library : **744 KB**

Biometric accuracy and performance analysis?

True measure of any biometric system is its accuracy to validate. There are constant focus and steps to improve the valuation algorithms by Niramaya.

Two factors that characterized any biometric system accuracy - The False Accept Rate (FAR) and the False Reject Rate (FRR). FAR is when an impostor is pretending to be the real enrolled user and trying to break into the system with his/her biometric, this is an attack scenario. On the other hand FRR is when the real users fail to authenticate themselves.

The below diagram suggests a biometric system with an operating point where the trade-off between FAR and FRR is minimum. In other words, it's a trade-off between security and convenience to use the system. Higher security is achieved by using tighter matching thresholds, making it more difficult for impostors to break the system. Greater convenience is obtained by using a looser threshold, making it easier for enrolled users to successfully authenticate under a wider range of conditions.



Therefore it is essential for a biometric system to have the best of both FAR and FRR.

Face validation details for our algorithms are detailed below:

Model Size (MB)	LWF (%)	Val@0.003(%)	Inference@MSM8976 cpu (ms)
1.4	99.40	98.40	260

Our face validation algorithm is not certified by external agencies as yet, the efforts are in progress.

Validation data size is 13,000 images with 1680 different face identities.

The Detection Error Tradeoff (DET) for face validation is : FRR at 1/13,000 FAR is approximately 0.6% (Detection Rate 99.4%)

Neural network inference speeds?

All our neural networks are designed for mobile and hence the tiny model structure is considered without compromising the accuracy. Except for face validation, all other models consume inference time in the range of 3 to 12ms.

To speed up the inference time, multi-threading is utilized as most of the smartphones have multiple cores on them.

Currently, all the processing is done on CPU, hardware acceleration like DSP or mobile GPUs are underway. For ARM based processors, NEON and VFPv3 are enabled.

Library overview?

Library is written in C++ utilizing Android NDK and JNI interface is also provided for Java Application. Similarly for iOS C++ APIs are provided.

Video capture requirements?

Modern day smartphones have all the required hardware for Niramaya's face biometric to run seamlessly on them. But at a high level a front camera with video resolution of 680x480 or higher is required.

To avoid motion blur and better validation results, a camera with 30FPS or higher would be required.