HOW TO EVALUATE A FINGERPRINT ALGORITHM - AND ACHIEVE TOP PERFORMANCE

Patrik Lindeberg | COO

2015-06-25

Revision 150623-A

PRECISE™ BIOMETRICS

AGENDA

- BACKGROUND
- PRECISE BIOMETRICS
- FINGERPRINT BIOMETRIC FUNDAMENTALS
- HOW TO EVALUATE AN ALGORITHM
- CONCLUSION

PRECiSE™ BIOMETRICS

BACKGROUND

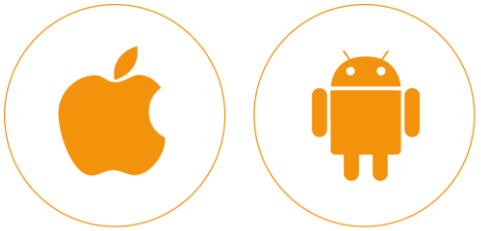
1,400,000,000
SMARTPHONES WITH FINGERPRINT TECHNOLOGY SOLD YEARLY BY **2020**

Source: IHS Technology Research

WHY NOW?

iPhone/iPad
Samsung
Huawei
HTC
Android M

Password replacement



Mobile payment services

PRECiSE™ BIOMETRICS

BACKGROUND

1,400,000,000
SMARTPHONES WITH FINGERPRINT TECHNOLOGY SOLD YEARLY BY **2020**

Source: IHS Technology Research

THE KEY COMPONENTS

Sensor

ACCESS

NO ACCESS

Algorithm

PRECiSE™ BIOMETRICS

BACKGROUND

1,400,000,000

SMARTPHONES WITH FINGERPRINT TECHNOLOGY SOLD YEARLY BY **2020**

Source: IHS Technology Research

TARGET AUDIENCE

Purchase

Product Management

R&D

PRECiSE™ BIOMETRICS

PRECISE BIOMETRICS

1997

Precise Biometrics was founded with a vision to provide fingerprint authentication on mobile devices and smart cards

1999

Filed an innovative patent for fingerprint recognition on small sensors in mobile devices

2001

Project with a leading mobile phone vendor, but the sensor technology was not mature enough and consumer demand was not there

2001 - 2013

- Match on Card
- eID
- Logical Access Solutions
- Physical Access Solutions

2013

Apple introduced fingerprint sensor in iPhone 5S

Signs license agreement with Fingerprint Cards

2014

Signs license agreement with Synaptics

Integrated in the Huawei Mate 7, the first Andriod smart phone with touch fingerprint sensor

Oppo N3 followed shortly after

2015

Precise Biomatch Mobile was integrated in smartphones by Oppo, Coolpad, Newman, LeTV, Gionee and several others

Signs license agreement with Silead

We will continue to drive innovation of convenient and secure access

PRECISE™ BIOMETRICS

PRECISE BIOMETRICS

PARTNERSHIPS

- Smartphone manufacturers

Huawei Ascend Mate 7
- first andriod with touch sensor!

Oppo N3

Oppo R7plus

LeTV max

Newman Button

Coolpad Tiptop Pro

Gionee Elife 8

PRECISE™ BIOMETRICS

PARTNERSHIPS

- Sensor manufacturers

FINGERPRINTS

ilead

Synaptics™

PRECISE™ BIOMETRICS

FROST & SULLIVAN BEST PRACTISE AWARD 2015

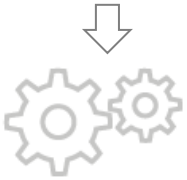
"Precise Biometrics is a leader in fingerprint biometrics for the global mobile device market, and its fingerprint technology, which offers superior convenience and security, is critical for mobile device manufactures to ensure the transition to the new authentication paradigm".

PRECISE™ BIOMETRICS

FINGERPRINT BIOMETRIC FUNDAMENTALS

ENROLLMENT

1.
A *fingerprint sensor* is used to produce a *sample*



2.
An *algorithm* extracts the sample's most characteristic features which are used to produce a *template*

3.
The *template* is saved in *secure storage*

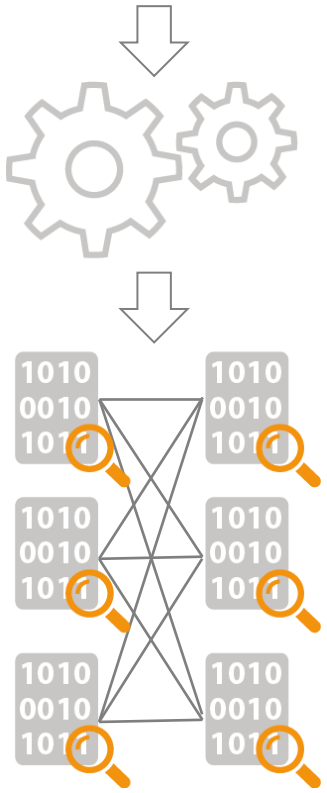
FINGERPRINT BIOMETRIC FUNDAMENTALS

VERIFICATION

FINGERPRINT BIOMETRIC FUNDAMENTALS

PERFORMANCE EVALUATION

1.
Database collection



2.
Mass matching of templates

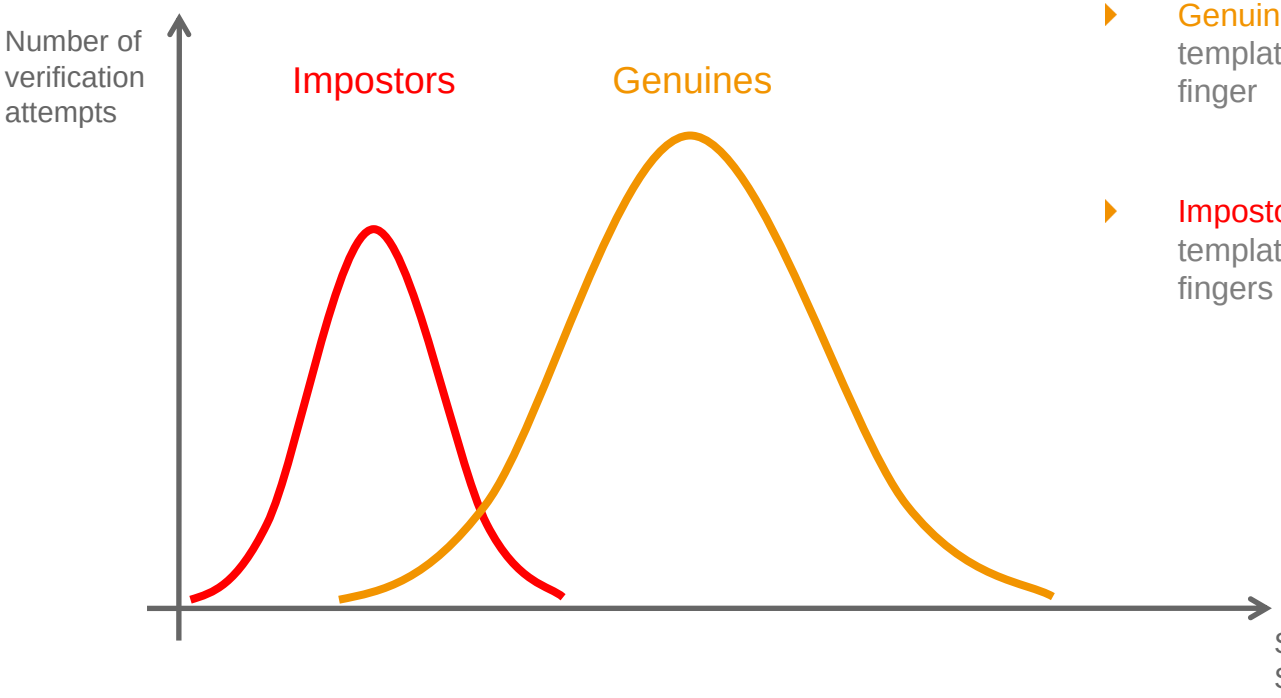
3.
Matching scores

A	A	300
A	B	20
A	C	15
A	D	40
A	E	25

Statistical conclusion

..to be continued

FINGERPRINT BIOMETRIC FUNDAMENTALS

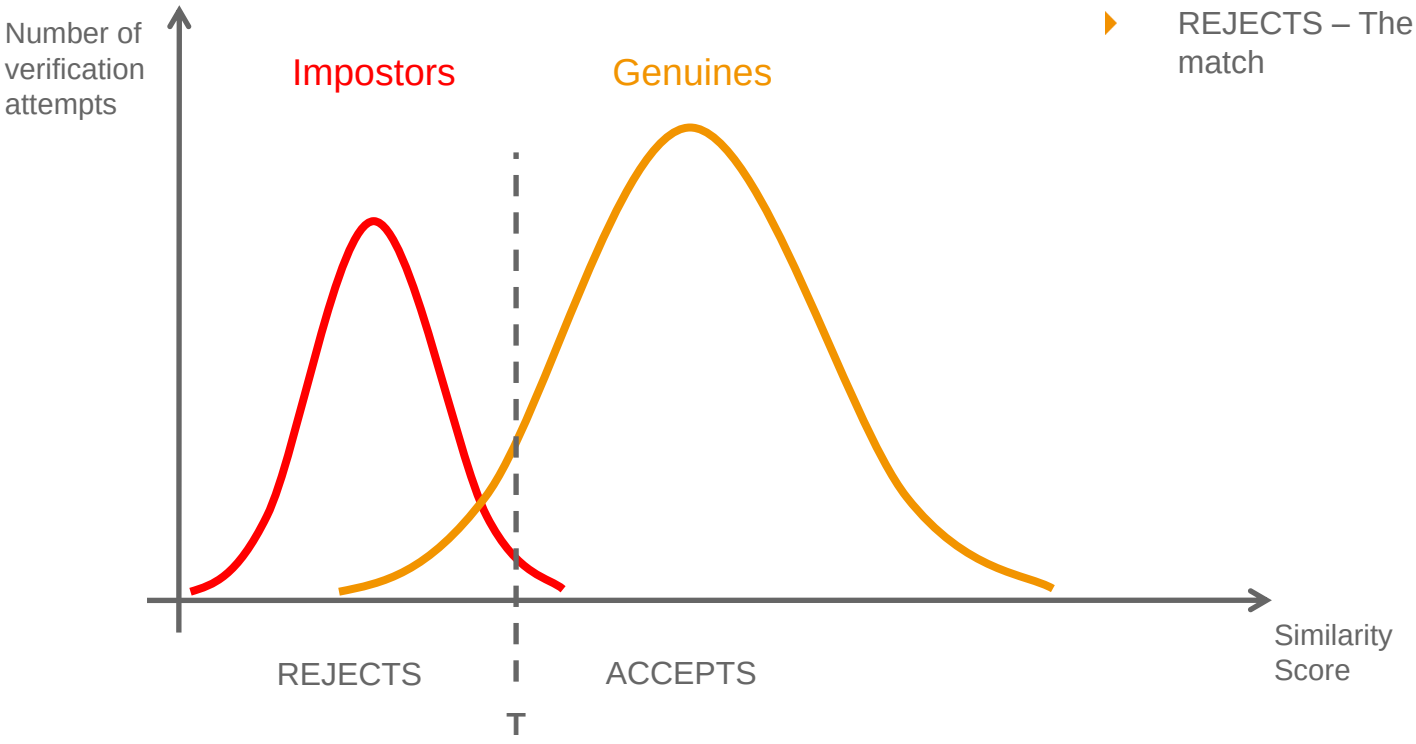


- Genuines – matches where both templates are extracted from the same finger
- Impostors – matches where the two templates are extracted from different fingers

PRECiSE™ BIOMETRICS

FINGERPRINT BIOMETRIC FUNDAMENTALS

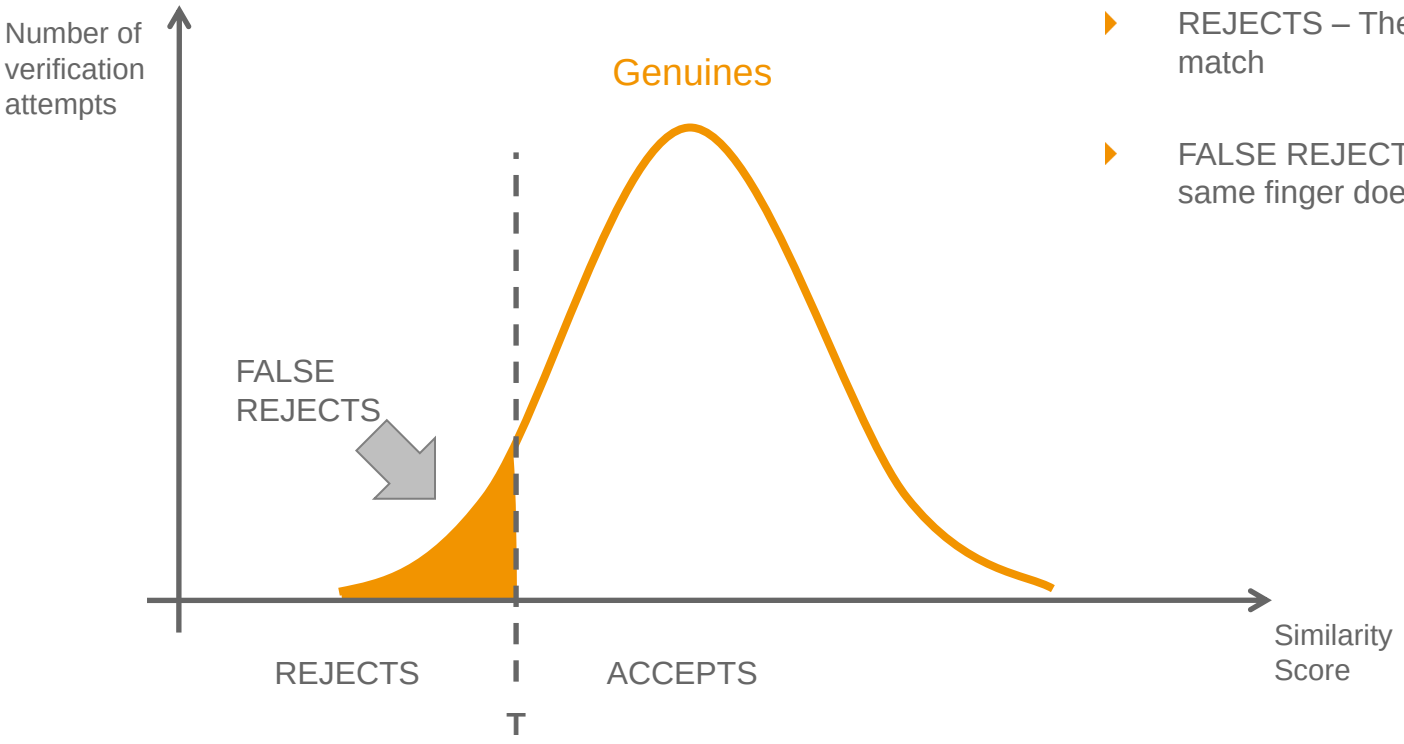
- ACCEPTS – Positive match, the two templates match
- REJECTS – The two templates do not match



T = Threshold score that defines security level

PRECiSE™ BIOMETRICS

FINGERPRINT BIOMETRIC FUNDAMENTALS

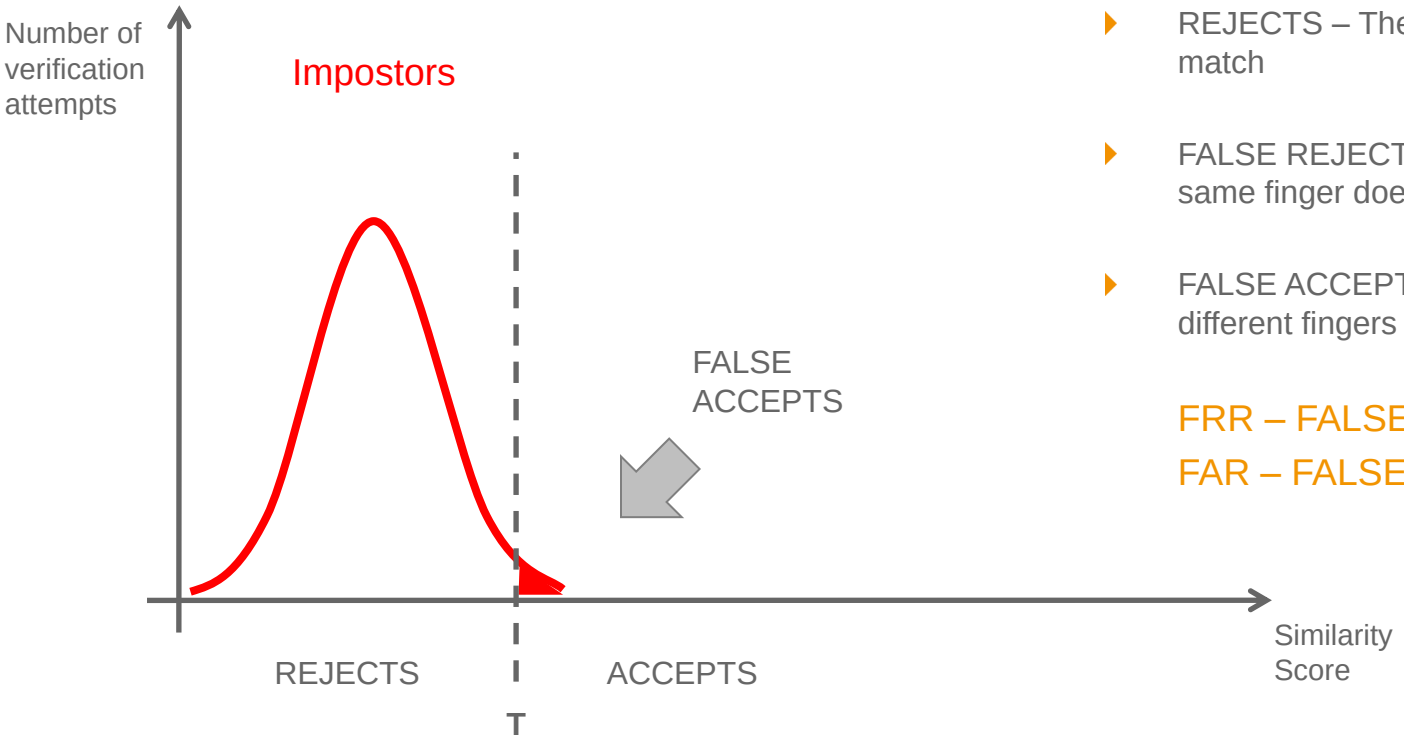


- ACCEPTS – Positive match, the two templates match
- REJECTS – The two templates does not match
- FALSE REJECTS – Two templates from the same finger does not match

T = Threshold score that defines security level

PRECiSE™ BIOMETRICS

FINGERPRINT BIOMETRIC FUNDAMENTALS



- ACCEPTS – Positive match, the two templates match
- REJECTS – The two templates does not match
- FALSE REJECTS – Two templates from the same finger does not match
- FALSE ACCEPTS – Two templates from different fingers match

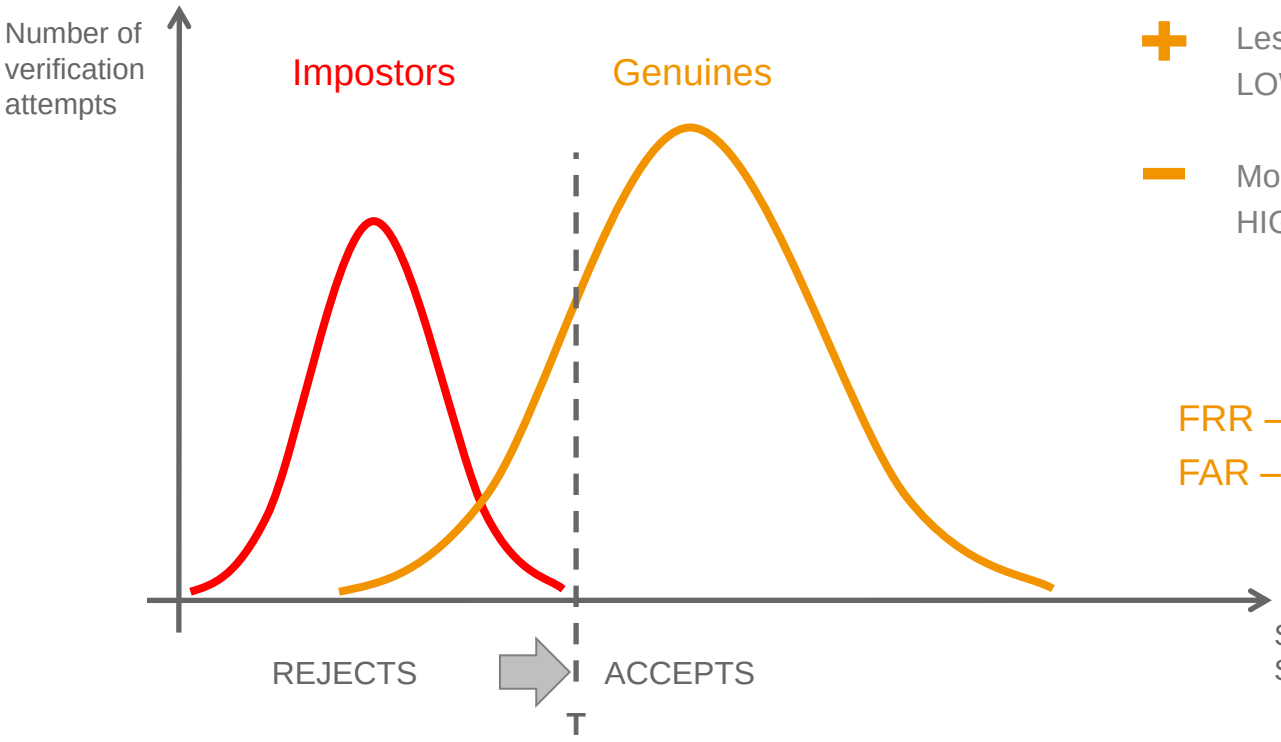
FRR – FALSE REJECT RATE

FAR – FALSE ACCEPT RATE

T = Threshold score that defines security level

PRECISE™ BIOMETRICS

FINGERPRINT BIOMETRIC FUNDAMENTALS



SECURITY LEVEL INCREASED

\+ Less impostors will be accepted; LOW FAR

– More genuines will be rejected; HIGH FRR

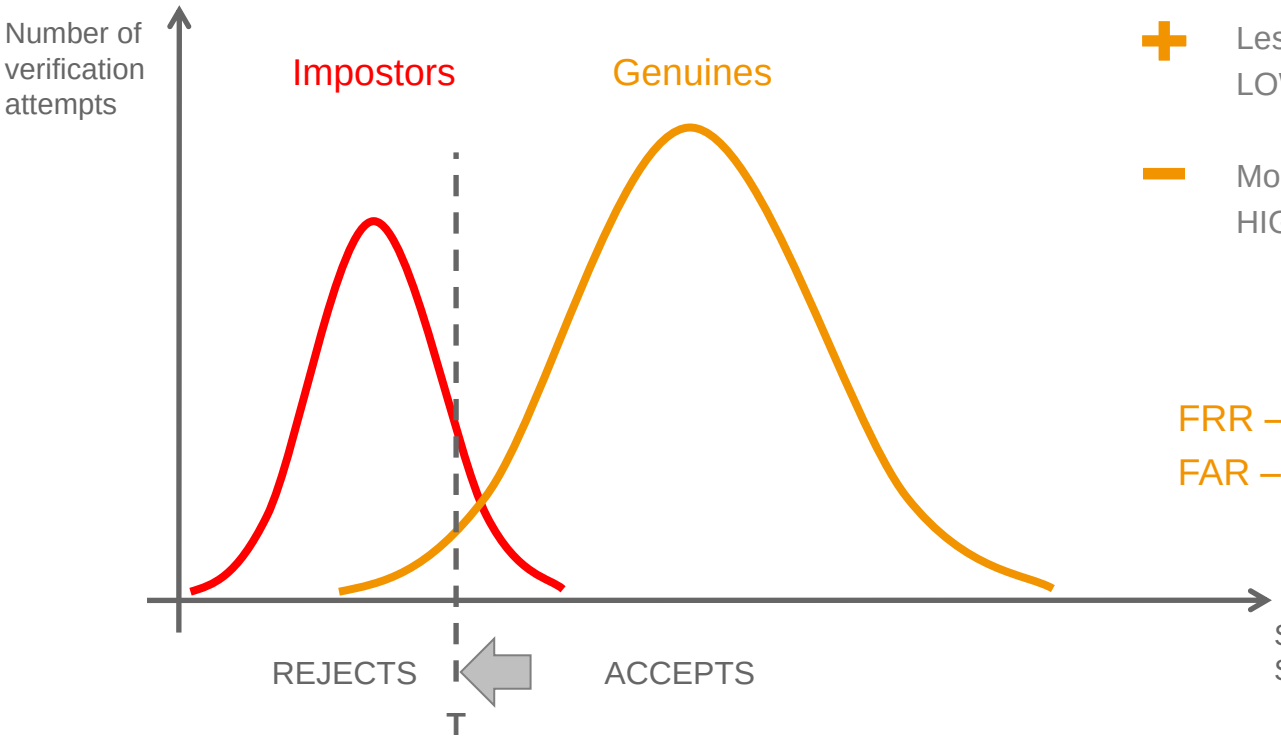
FRR – FALSE REJECT RATE

FAR – FALSE ACCEPT RATE

T = Threshold score that defines security level

PRECiSE™ BIOMETRICS

FINGERPRINT BIOMETRIC FUNDAMENTALS



SECURITY LEVEL DECREASED

\+ Less genuines will be rejected; LOW FRR

− More impostors will be accepted; HIGH FAR

FRR – FALSE REJECT RATE

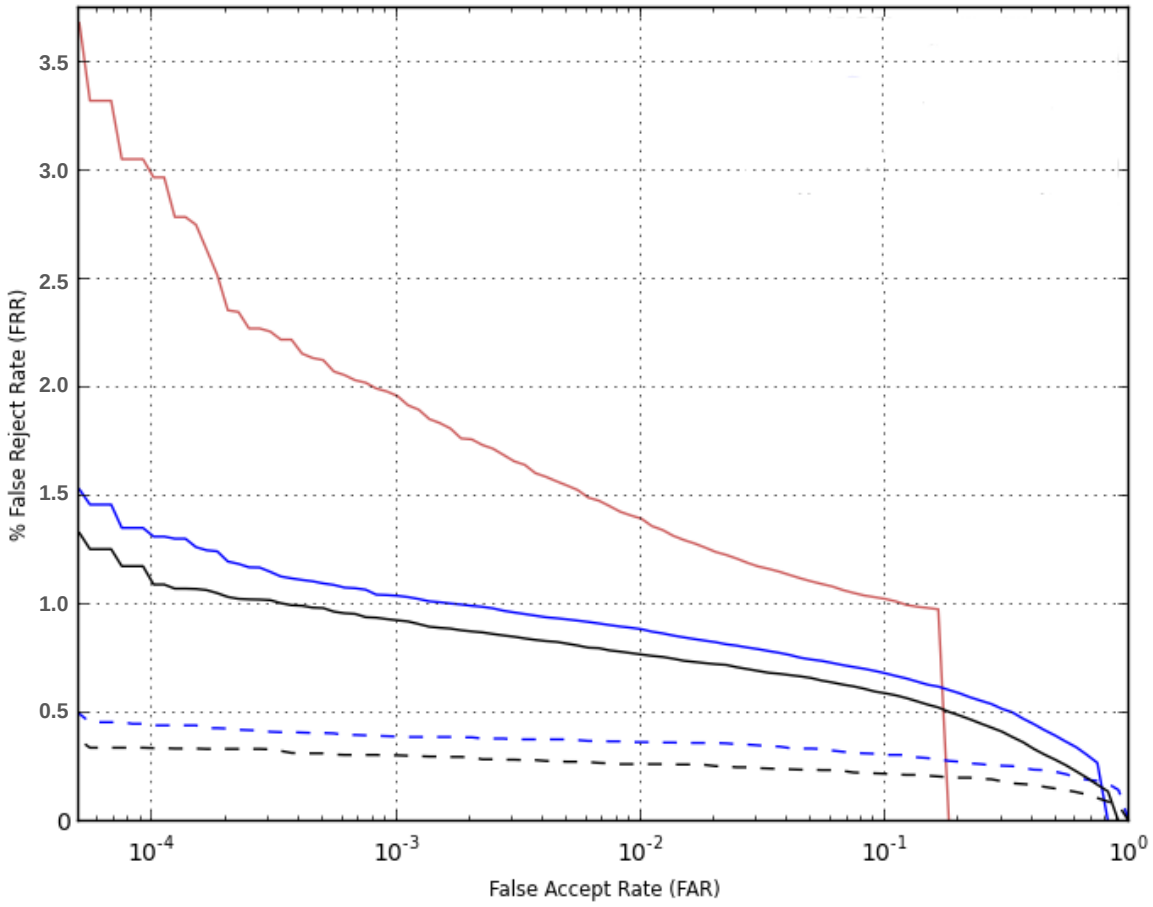
FAR – FALSE ACCEPT RATE

T = Threshold score that defines security level

PRECiSE™ BIOMETRICS

FINGERPRINT BIOMETRIC FUNDAMENTALS

DET (DETECTION ERROR TRADE-OFF) CURVE



FRR – FALSE REJECT RATE

FAR – FALSE ACCEPT RATE

PRECiSE™ BIOMETRICS

FINGERPRINT BIOMETRIC FUNDAMENTALS

CHALLENGES WITH SMALL SENSORS

- Less unique features to extract

- Poor overlap between enrolled and verification templates

- Sensitive to rotation by 90º

PRECiSE™ BIOMETRICS

FINGERPRINT BIOMETRIC FUNDAMENTALS

THE SOLUTION

- Multiple templates that together represents the complete fingerprint
- Assures good overlap between enrolled and verification templates
- Additional templates can be added through dynamic template update

- Recommended to enroll additional rotated images to improve performance for the rotated use cases

PRECiSE™ BIOMETRICS

HOW TO EVALUATE AN ALGORITHM

?

PRECiSE™
BIOMETRICS

HOW TO EVALUATE AN ALGORITHM

HOW TO COMPARE FINGERPRINT SYSTEMS

FRR 1% @ FAR 1 / 50,000 =

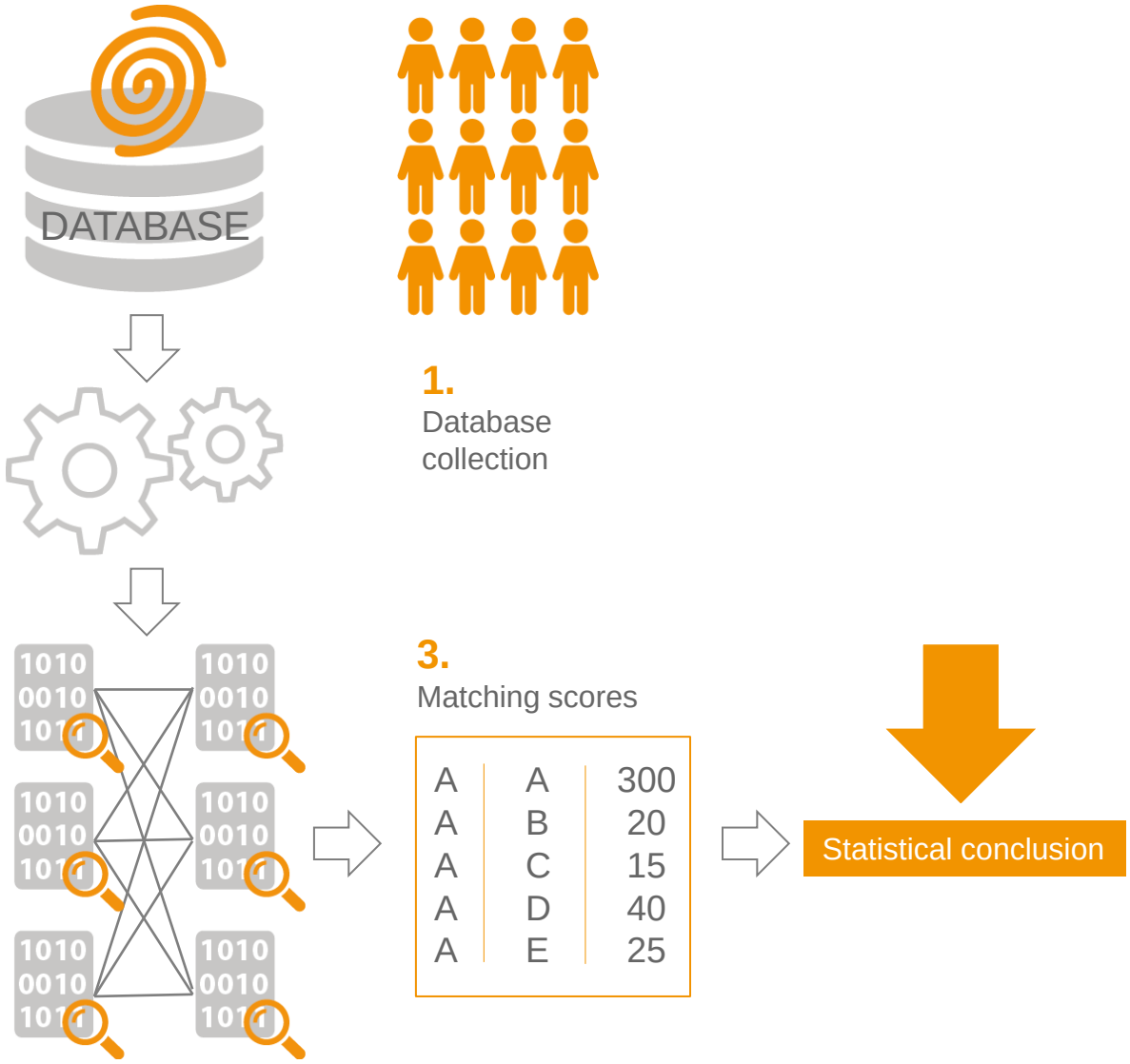
1 out of 50,000 impostor attempts is (falsely) considered a match and1% of the genuine attempts will fail (be falsely considered nonmatches)

What does this really tell you?

PRECISE™ BIOMETRICS

HOW TO EVALUATE AN ALGORITHM

PERFORMANCE EVALUATION



HOW TO EVALUATE AN ALGORITHM

THE IMPORTANCE OF A RELEVANT FINGERPRINT DATABASE

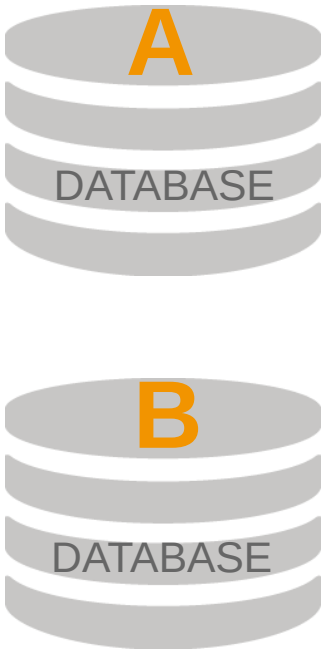
CRITICAL DATABASE PROPERTIES

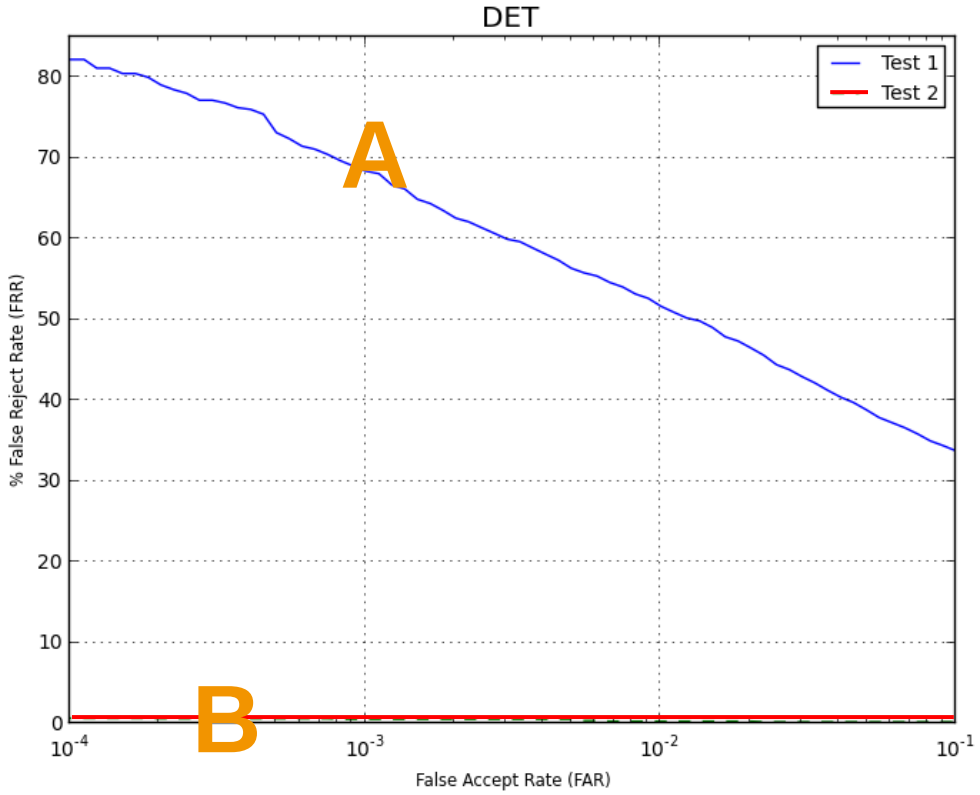
- Size & quality of sensor
- Scenarios – ergonomy, environment
- Volunteers – men/women, young/old, cooperative/non cooperative
- Instruction level – user guidence

PRECISE™ BIOMETRICS

HOW TO EVALUATE AN ALGORITHM

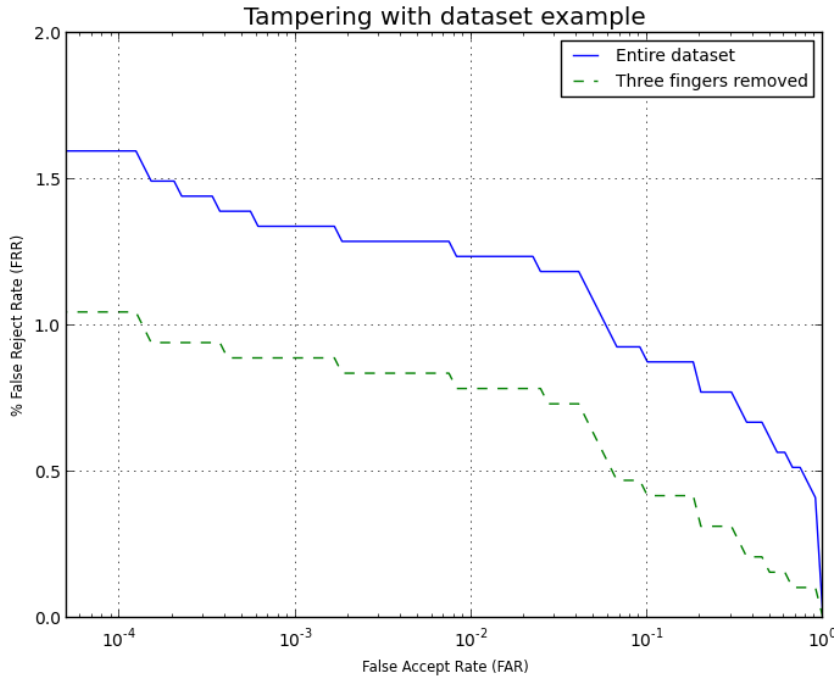
SAME ALGORITHM PERFORMANCE RESULTS FROM TWO DATABASES MAY BE TOTALLY DIFFERENT!





HOW TO EVALUATE AN ALGORITHM

THE IMPORTANCE OF A RELEVANT FINGERPRINT DATABASE



TAMPERING WITH DATABASE

- Removal of templates from only a few fingers may strongly improve results
- Database with only limited tampering may show strongly biased results!

PRECISE™ BIOMETRICS

HOW TO EVALUATE AN ALGORITHM

DATABASE SIZE RECOMMENDATION

- Minimum 100 persons
- Minimum 6 fingers / person
- Minimum 36 enrollment samples from each finger
- Minimum 10 verification samples from each finger

These minimum recommendations would give a total of
100 x 6 x (36 + 10) = 27,600 images
of which 100 x 6 x 10 = 6,000 are dedicated for verification.

Normally this data would allow for :
• 100 x 6 x (100 – 1) x 6 = 356,400 impostor matches.
• 100 x 6 x 10 = 6,000 genuine matches.

At a FAR-level of 1/50,000, only 356,400 / 50,000 = 7 matches would be the base to statistically justify your measurements.

PRECISE™ BIOMETRICS

CONCLUSION

- USE RELEVANT SENSOR
- USE RELEVANT SCENARIOS
- USE RELEVANT TARGET GROUP BASE
- USE LARGE ENOUGH DATABASE
- USE SAME DATABASE WHEN COMPARING DIFFERENT ALGORITHMS

PRECISE™ BIOMETRICS

CONCLUSION

If you follow these guidelines you have established

the base to achieve top performance!

PRECiSE™
BIOMETRICS

THANK YOU!

MORE INFORMATION
Understanding Biometric Performance Evaluation (White Paper)

TOOLS
Precise Performance Evaluation Suite

FOLLOW US
Right Touch – Precise Biometrics Newsletter
LinkedIn
Twitter

Patrik Lindeberg | COO
info@precisebiometrics.com

White Paper

Right Touch Newsletter

Presentation (News section)

www.precisebiometrics.com

LinkedIn
twitter

PRECISE™ BIOMETRICS