दिल्ली प्रौद्योगिकी विश्वविद्यालय

विज्ञानवान् प्रज्ञानवान् भव

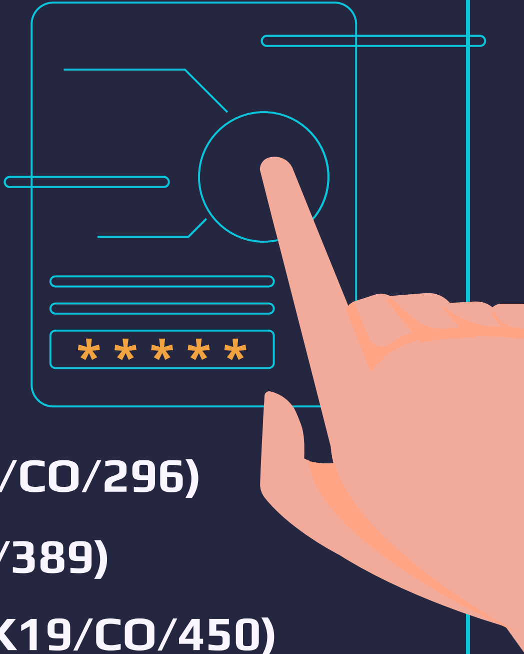
DTU

DELTECH
UNIVERSITY

DELHI TECHNOLOGICAL UNIVERSITY

Information Network and Internet Security

FACE AND VOICE BIOMETRICS



SUBMITTED TO:

INDU SINGH MA'AM

Assistant Professor
Department of Computer Engineering

SUBMITTED BY:

PRIYANKA PATEL (2K19/CO/296)

SRISTI MITRA (2K19/CO/389)

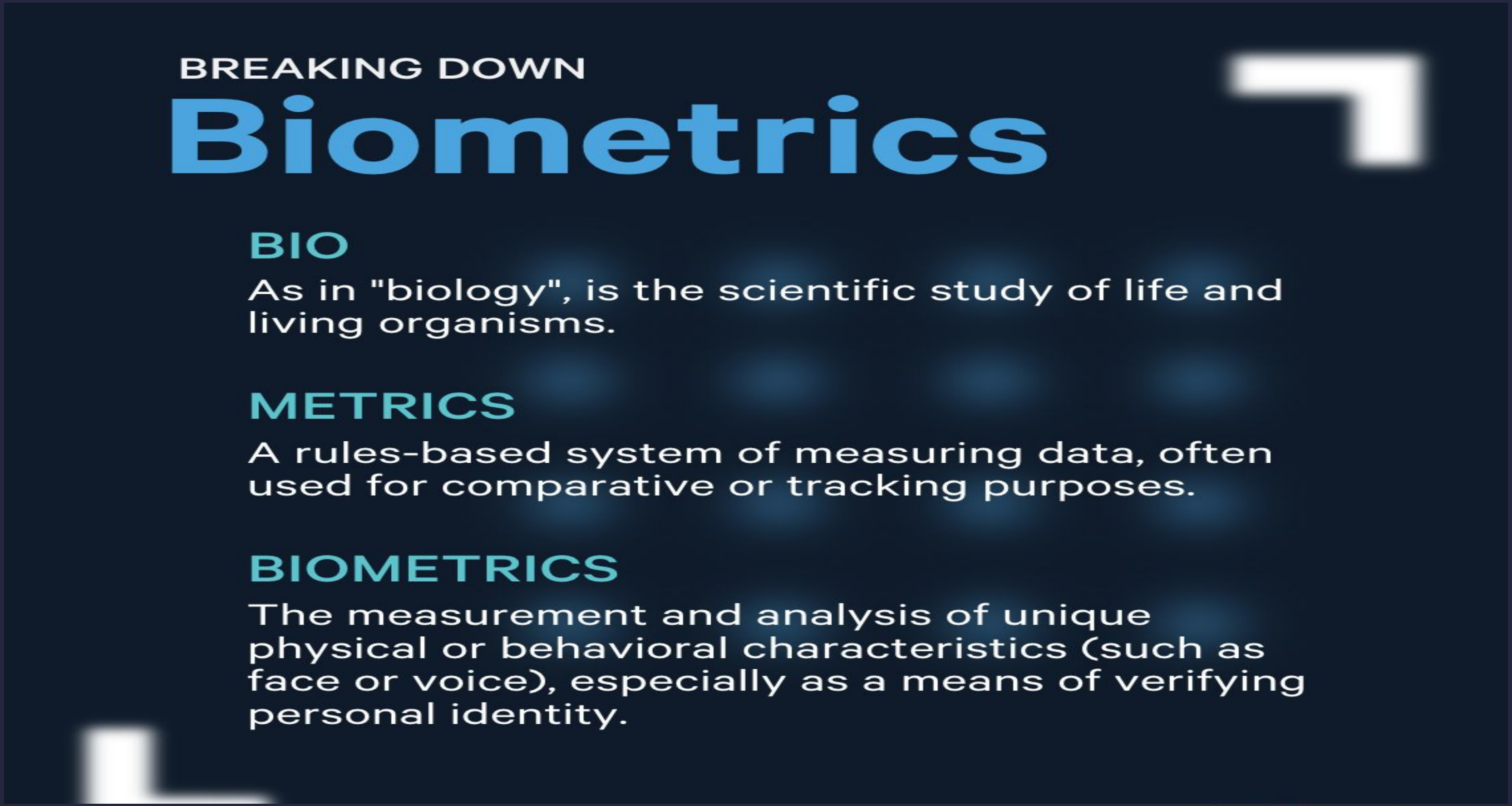
ZISHNENDU SARKER (2K19/CO/450)

MEMBERS CONTRIBUTION

MEMBERS	SLIDE NOs	NUMBER OF SLIDES
PRIYANKA PATEL (2K19/C0/296)	1-3 and 14-20	10 slides
SRISTI MITRA (2K19/CO/389)	9-13 and 23-25	8 slides
ZISHNENDU SARKER (2K19/CO/450)	4-8 and 21-22	7 slides

Table of ContentS

- INTRODUCTION
- BIOMETRIC SYSTEM
- TYPES OF BIOMETRIC SECURITY
- WHAT IS FACE BIOMETRIC
- WORKING OF FACE BIOMETRIC
- VOICE BIOMETRIC
- WORKING OF VOICE BIOMETRIC
- COMPARATIVE STUDY OF FACE AND VOICE BIOMETRICS
- APPLICATIONS OF BIOMETRICS
- ARGUMENTS AND CONTROVERSIES
- CONCLUSION



BREAKING DOWN

Biometrics

BIO

As in "biology", is the scientific study of life and living organisms.

METRICS

A rules-based system of measuring data, often used for comparative or tracking purposes.

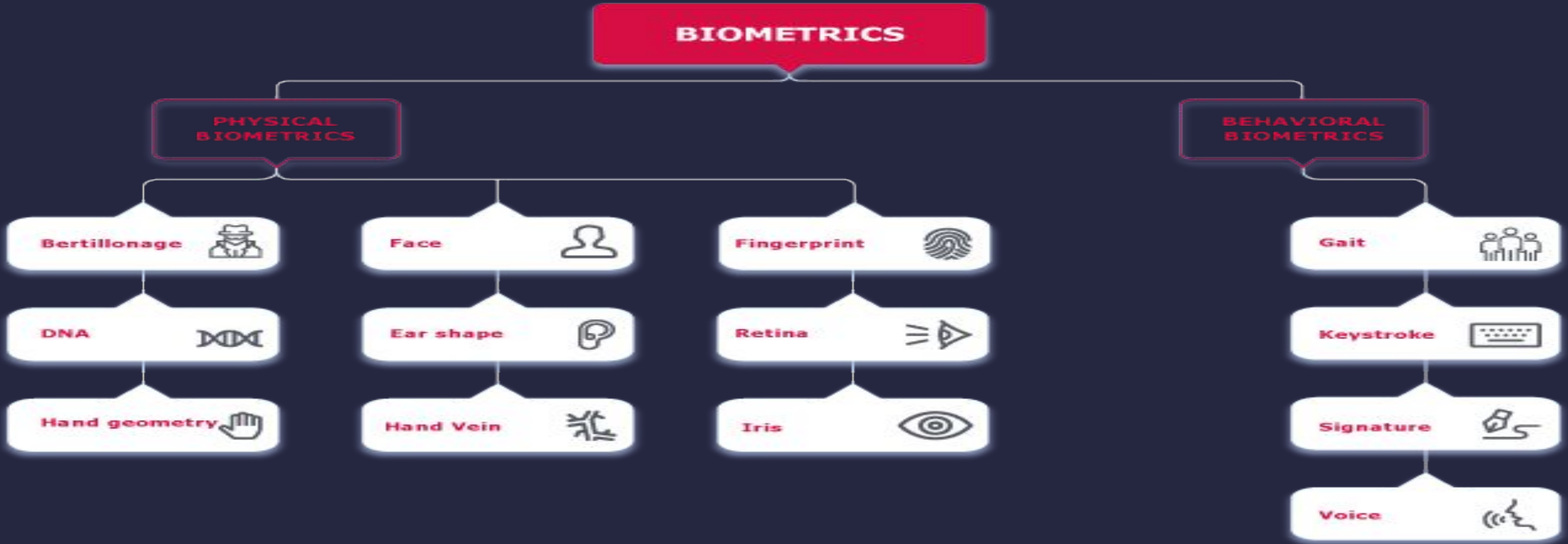
BIOMETRICS

The measurement and analysis of unique physical or behavioral characteristics (such as face or voice), especially as a means of verifying personal identity.

DEFINITIONS & TYPES:-

Biometrics is a technology used to identify, analyze and measure an individual's physical behavioral characteristics.

- ★ Biometrics uses something that we are, rather than something we know
- ★ It measures the unique biological characteristics on an individual.
- ★ One of the main advantages of biometric authentication is convenience. By using a feature that is a part of us rather than a password or PIN that needs to be remembered, we can access a physical location or an online service without having to wait.



How Biometric System Work:

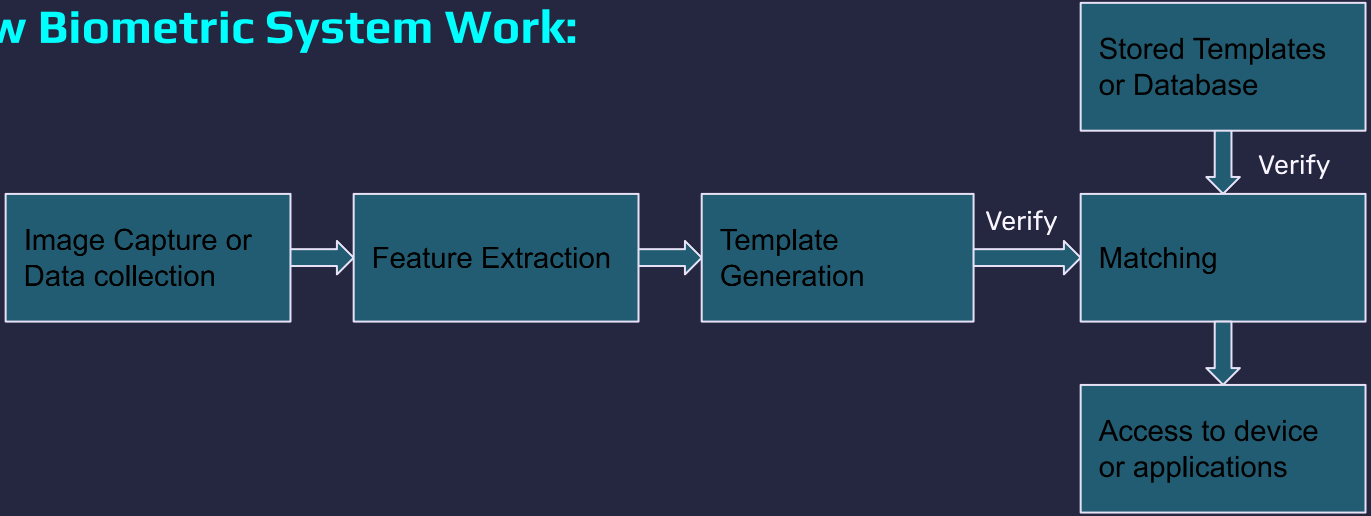


Image Capture or Data collection

Feature Extraction

Template Generation

Verify

Stored Templates or Database

Verify

Matching

Access to device or applications

There are four stages of Biometrics :

1. Image Capture (or collection data)
2. Extraction
3. Comparison
4. Match/Non-match

BIOMETRIC TERMS

Biometric system is a technology which takes an individual's physiological, behavioral or both traits as input, analyzes it and identifies the individual as a genuine or malicious user.

Authentication

It is a one to many process where any biometric identity of the individual will be compared to the whole database.

Verification

Next process is verification and it is a one to one process, the authentication we got from the previous step that is now compared to the biometrics of the visiting person. If the two matches are above **80% (avg)** then it will allow the user to get access.

Authorization

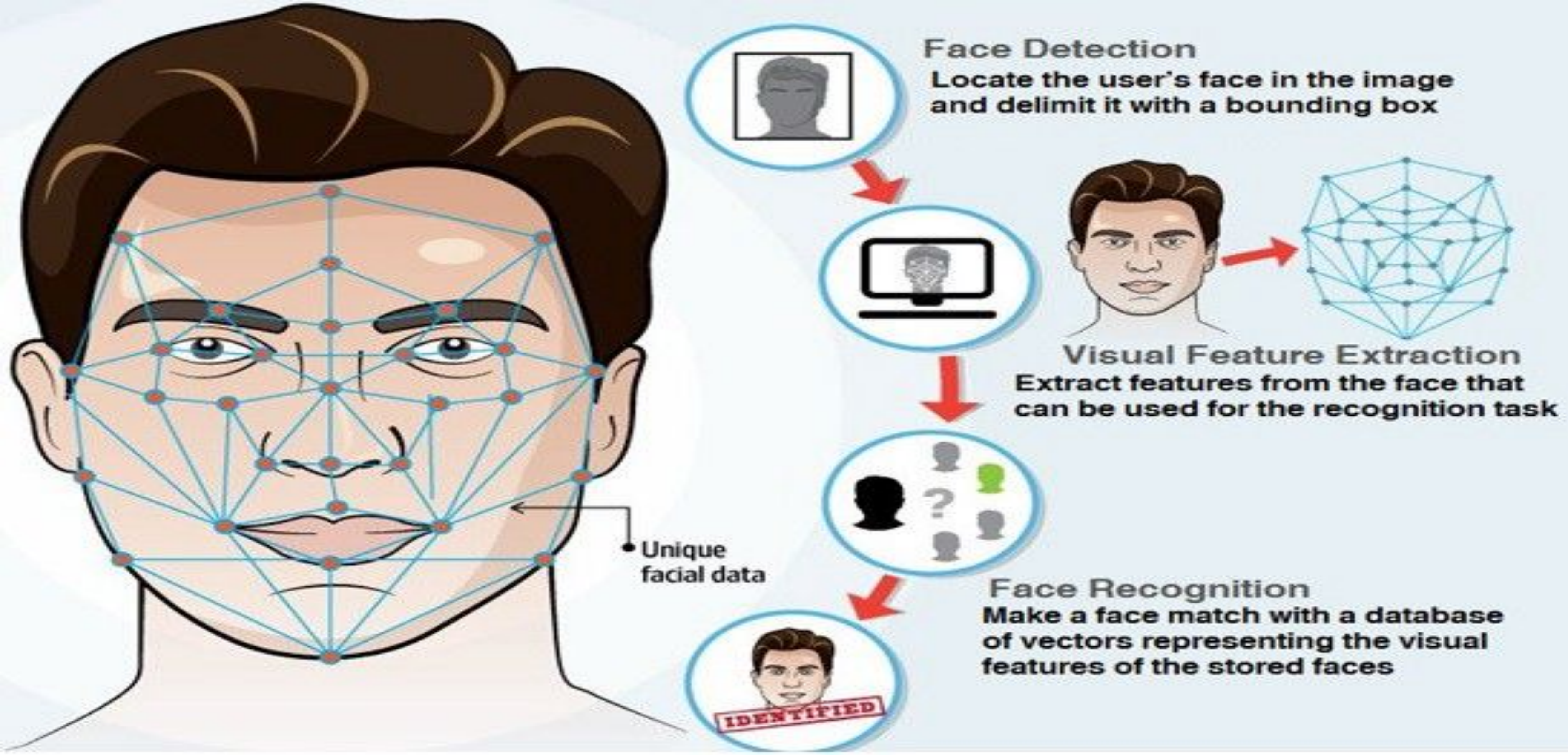
Here in next step, the person will only be granted with the access to a certain aspect that he is allowed to. If he tries to access more than that then he do not get the permission to do it.

FACE BIOMETRICS

Facial recognition is a biometric tool as with other commonly used biometric technologies, where it recognizes or authenticates a person based on specific aspects of their physiology.

- ★ Facial recognition can identify human faces in images or videos, determine if the face in two images belongs to the same person, or search for a face among a large collection of existing images.
- ★ A face analyzer is software that identifies or confirms a person's identity using their face.
- ★ Biometric security systems use facial recognition to uniquely identify individuals during user onboarding or logins as well as strengthen user authentication activity.
- ★ Mobile and personal devices also commonly use face analyzer technology for device security.
- ★ It works by identifying and measuring facial features in an images.

How does facial recognition work?



Face Detection

Locate the user's face in the image and delimit it with a bounding box

Visual Feature Extraction

Extract features from the face that can be used for the recognition task

Face Recognition

Make a face match with a database of vectors representing the visual features of the stored faces

Benefits

- Efficient security
- Improved accuracy
- Easier integration

Use Case

- Fraud detection
- Cyber security
- Airport and border control
- Banking
- Healthcare

ACCURACY ANALYSIS OF FACE BIOMETRICS

★ *Verification algorithms used to match subjects to clear reference images (like a passport photo or mugshot) can achieve accuracy scores as high as 99.97% on standard assessments like NIST's Facial Recognition Vendor Test (FRVT).*

★ *"In real world deployments, accuracy rates tend to be far lower. For example, the FRVT found that the error rate for one leading algorithm climbed from 0.1% when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured "in the wild," where the subject may not be looking directly at the camera or may be obscured by objects or shadows.*

★ *NIST's 2017 Face in Video Evaluation (FIVE) tested algorithms and the test found that when using footage of passengers entering through boarding gates—a relatively controlled setting—the best algorithm had an accuracy rate of 94.4%.*

This level of accuracy takes face biometrics from being a useful convenience for a limited range of applications to opening up new practical applications for face biometrics.

Spoofing Attacks on face Biometrics

Photo attacks

A photo attack consists of displaying a photograph of the attacked identity to the sensor of the face recognition system.

Video attacks

An attacker could play a video of the legitimate user in any device that reproduces video and then presents it to the sensor/camera.

3D Mask Attacks

in this type of attack, the attacker builds a 3D reconstruction of the face and presents it to the sensor/camera.

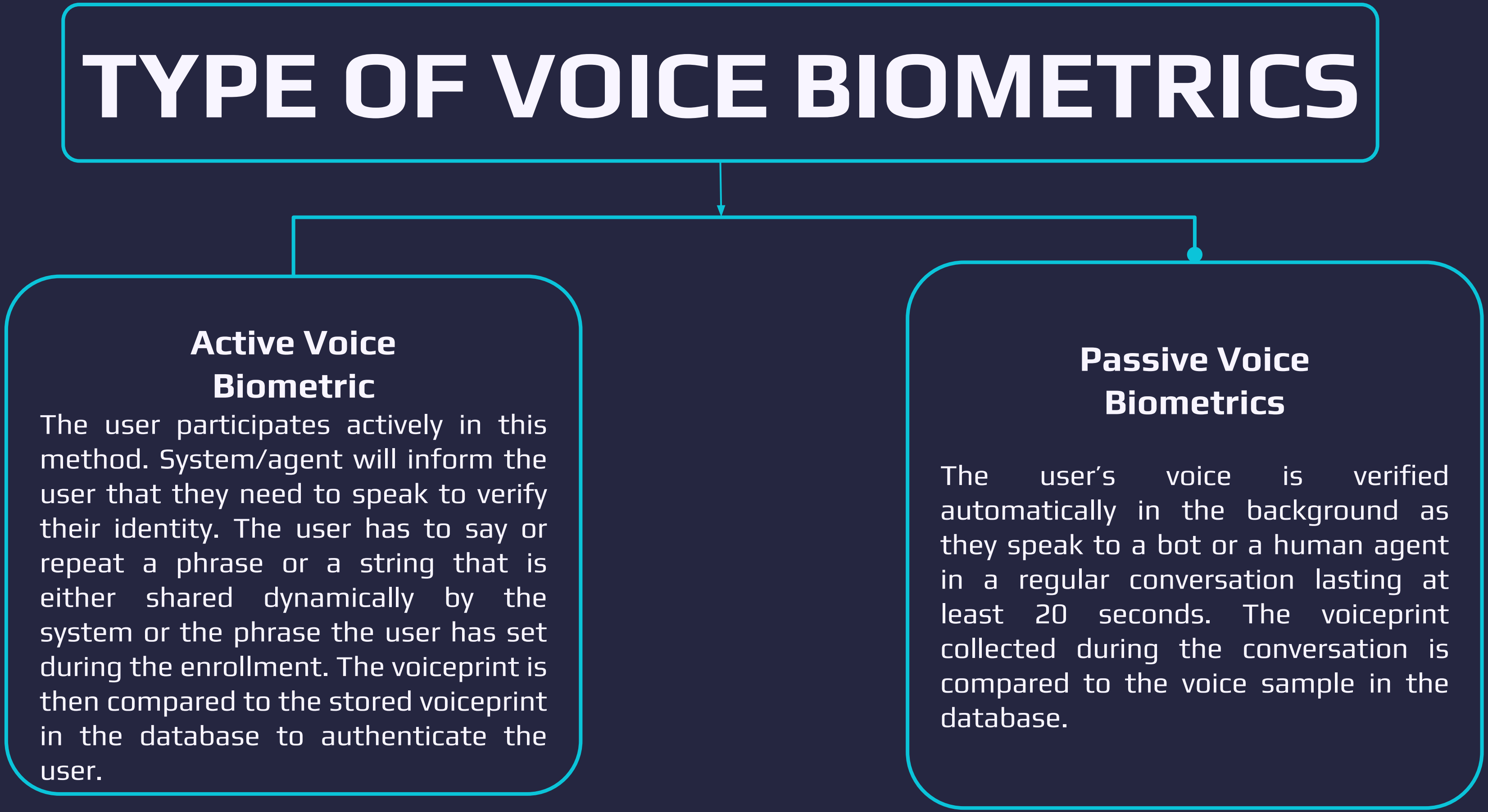
VOICE BIOMETRICS

Voice biometrics is the science of using a person's voice as a uniquely identifying biological characteristic in order to authenticate them.

★ It also referred to as voice verification or speaker recognition, voice biometrics enables fast, frictionless and highly secure access for a range of use cases from call center, mobile and online applications to chatbots, IoT devices and physical access.

★ In the case of the human voice, this wave is produced when the air goes from the lungs through the vocal folds (vocal cords), causing their vibration.

★ Each human voice is unique because of the individual form and size of the vocal organs and the manner in which they are used. For example, women and children usually have smaller larynxes and shorter vocal cords – that is why their voices are often higher.



TYPE OF VOICE BIOMETRICS

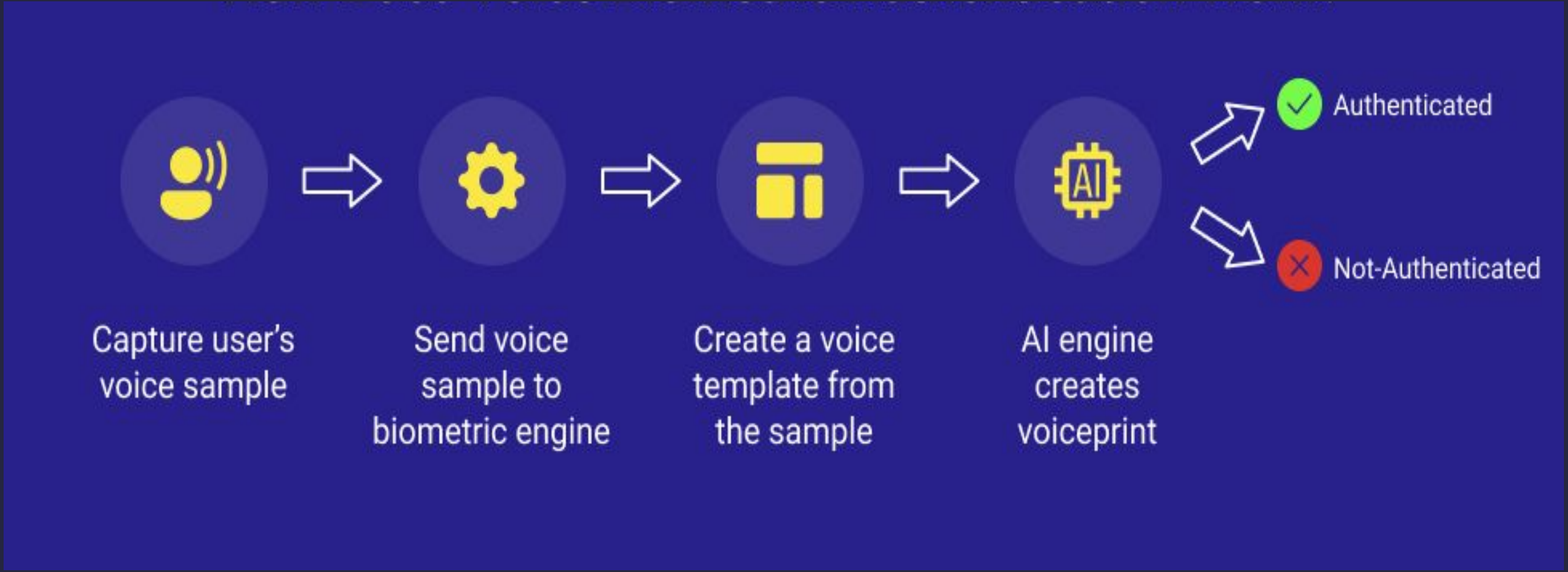
Active Voice Biometric

The user participates actively in this method. System/agent will inform the user that they need to speak to verify their identity. The user has to say or repeat a phrase or a string that is either shared dynamically by the system or the phrase the user has set during the enrollment. The voiceprint is then compared to the stored voiceprint in the database to authenticate the user.

Passive Voice Biometrics

The user’s voice is verified automatically in the background as they speak to a bot or a human agent in a regular conversation lasting at least 20 seconds. The voiceprint collected during the conversation is compared to the voice sample in the database.

How does voice recognition work?



Capture user’s voice sample

Send voice sample to biometric engine

Create a voice template from the sample

AI engine creates voiceprint

Benefits

★ Low operational Cost

★ Enhanced User Experience

★ Increased Accuracy

★ Easy to Implement

Use Case

★ Contact Center

★ Fraud Detection

★ Financial Services

★ Digital Signatures

★ Workforce Management

ADVANTAGES OF VOICE BIOMETRICS

Enhance the customer experience with fast, frictionless authentication

Improve security and minimize breaches due to compromised passwords, phishing, etc.

Reduce threats by identifying known fraudsters

Free agents from time spent verifying users and resetting passwords

Instantly identify users and personalize the interaction

Use as part of a two-factor authentication process to increase security without adding effort

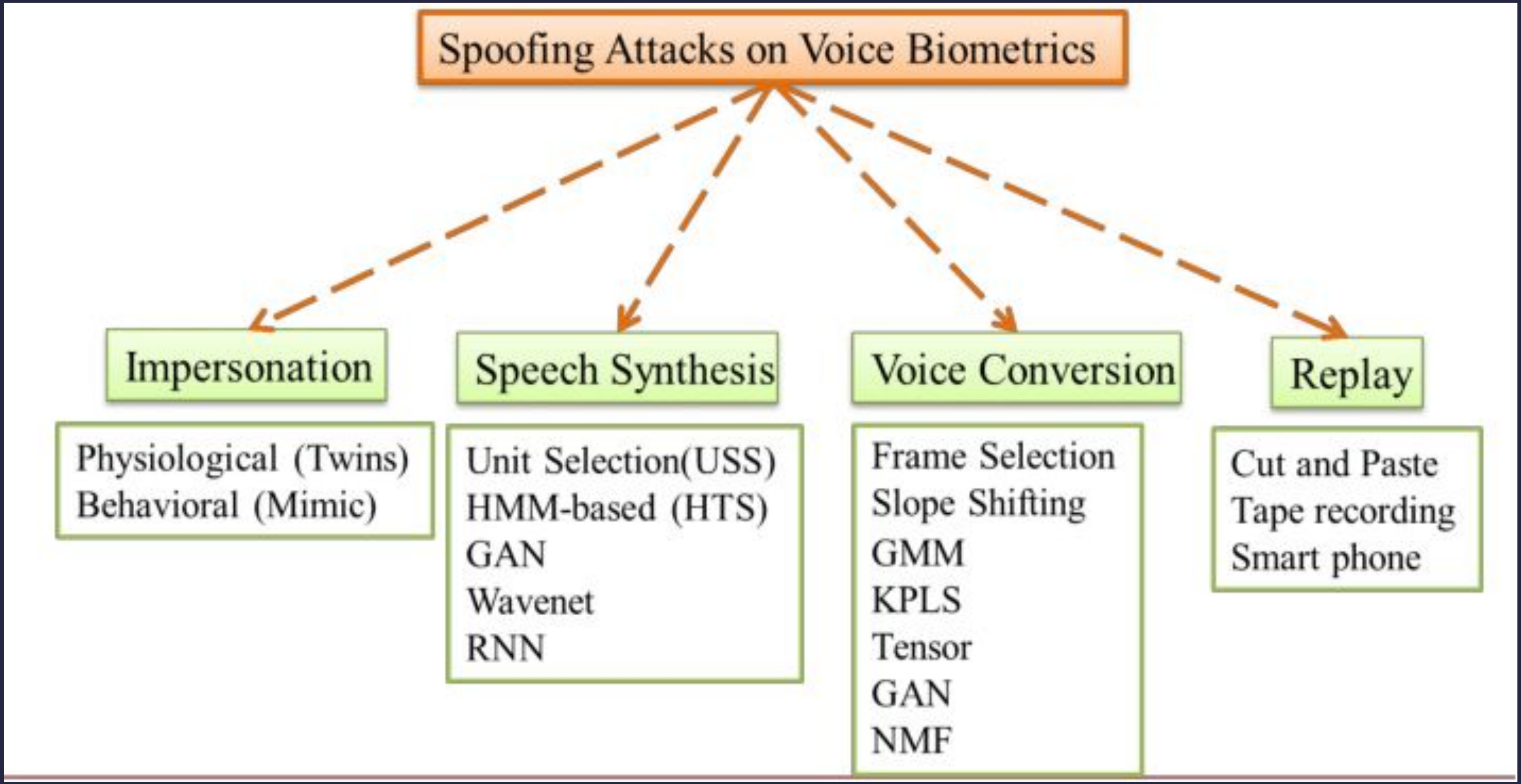
ACCURACY ANALYSIS OF VOICE BIOMETRICS

- *“Carrying out this test was extremely challenging from a technical standpoint. For example, audio used for a task that involved identifying people in a telephone conversation had extremely loud background noise and line noise and was difficult to hear even for human beings.*

- *“However, despite the harsh circumstances, NEC’s voice recognition system was able to uphold an accuracy rate of approximately 95%. As the baseline system accuracy rate set by NIST was at approximately 89%, the error rate was recorded at lower than half than that of the baseline system. As you can see, we were able to demonstrate an exceptionally high level of technological ability.*

- *“Although we are unable to publicise the results ranking due to the strong academic disposition of NIST’s voice recognition evaluation, this evaluation proved to be another good opportunity for us to show that our voice recognition is at a level worthy to compete globally.”*

This level of accuracy takes voice biometrics from being a useful convenience for a limited range of applications to opening up new practical applications for voice biometrics.



Spoofing Attacks on Voice Biometrics

Impersonation

- Physiological (Twins)
- Behavioral (Mimic)

Speech Synthesis

- Unit Selection(USS)
- HMM-based (HTS)
- GAN
- Wavenet
- RNN

Voice Conversion

- Frame Selection
- Slope Shifting
- GMM
- KPLS
- Tensor
- GAN
- NMF

Replay

- Cut and Paste
- Tape recording
- Smart phone

Controversies

There are vocal arguments against biometric technology with the biggest being its threat to an individual's privacy. Some countries in the world are trying to ban the some biometric recognition because your data can be collected and stored without your permission.

Also, there is evidence that many facial recognition algorithms produce far more false positives on non white faces.

SIMILARITIES BETWEEN FACE AND VOICE BIOMETRICS

★ Low false accept and false reject rates.

★ Rapid verification of biometrics.

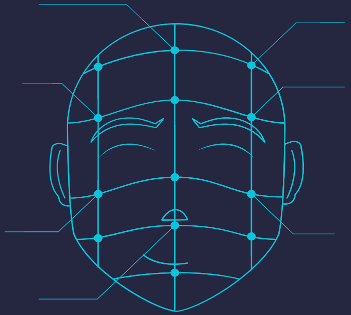
★ Long term stability of both the biometrics system is at medium level.

★ Security level for both the system is at low level because more secure and reliable biometrics systems are presented now a days in order to keep one's system secure from cryptanalyst or being forged.

★ Potential circumvention for both systems are at high level.

DIFFERENCES BETWEEN FACE AND VOICE BIOMETRICS

BIOMETRIC MODALITY/CHARACTERISTICS	FACE BIOMETRICS	VOICE BIOMETRICS
Accuracy	High (about 95%)	Medium (about 91%)
Cost	Low	Medium
Size of template	Large	Small
User Acceptance	Medium	High
Collectibility	High	Medium
Error Incidences	Lighting, age, glasses, hair	Noise, cold, weather



Since it adds extra layers of security that manual pass codes would not, voice and face authentication is a wonderful technique to confirm a user's identity. Voice and face authentication reduces customer and corporate dissatisfaction associated with time-consuming login procedures.

—Conclusion

THANK YOU

ANY QUESTIONS?