



# DEEPPFAKE DEFENSE

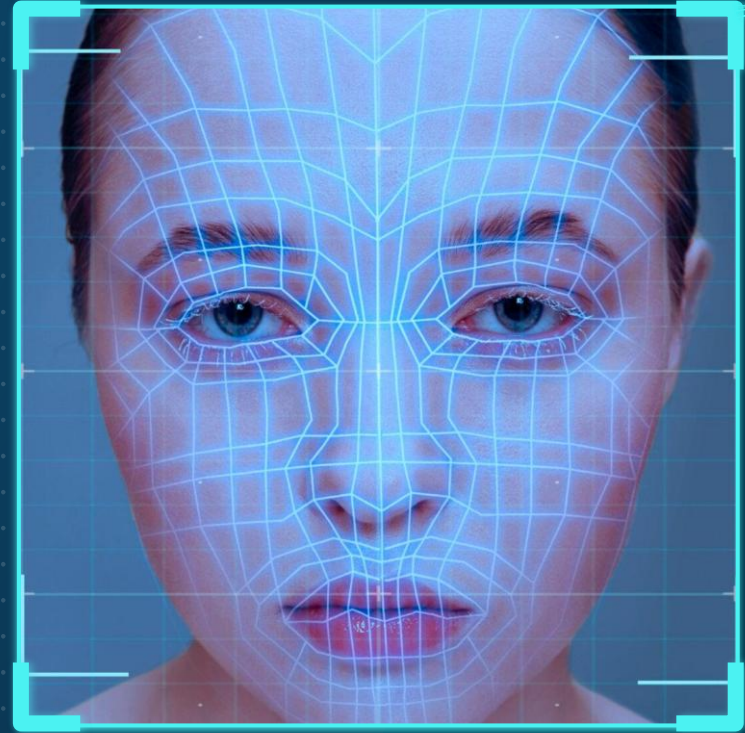
---

METHODS TO PREVENT DEEPPFAKE

# WHAT IS DEEPPFAKE?

---

A deepfake is a fake image, video, or audio created using artificial intelligence (AI) and machine learning.



# TYPES OF DEEPPFAKE



## VIDEO

Someone's face or voice is digitally altered to make it appear as if they are saying or doing something they never actually did



## IMAGE

A digitally manipulated image where a person's face has been replaced with another person's likeness



## AUDIO

A piece of artificially generated audio that uses artificial intelligence to convincingly mimic a specific person's voice



# SOCIETY CONCERNS

---

Misinformation and Fake News  
Privacy Violation  
Cyber Crime and Frauds  
Security

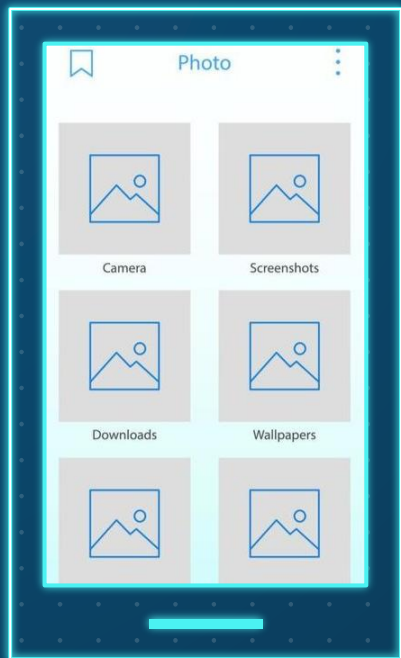


## TECHNIQUES USED TO COLLECT DATASET

---

- Fetching Media URL
- Web Scrapping
- Using Private and Reverse Engineered API's





# PERSONAL DATA

---

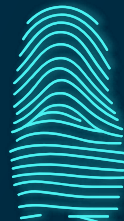
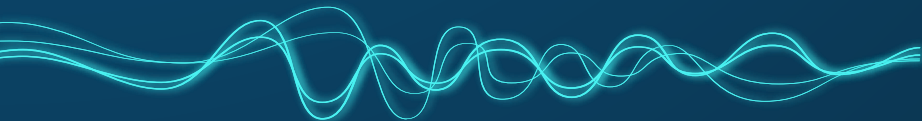
Sometimes Hackers may access your data (like Videos, images, voice recordings etc..) for the dataset.



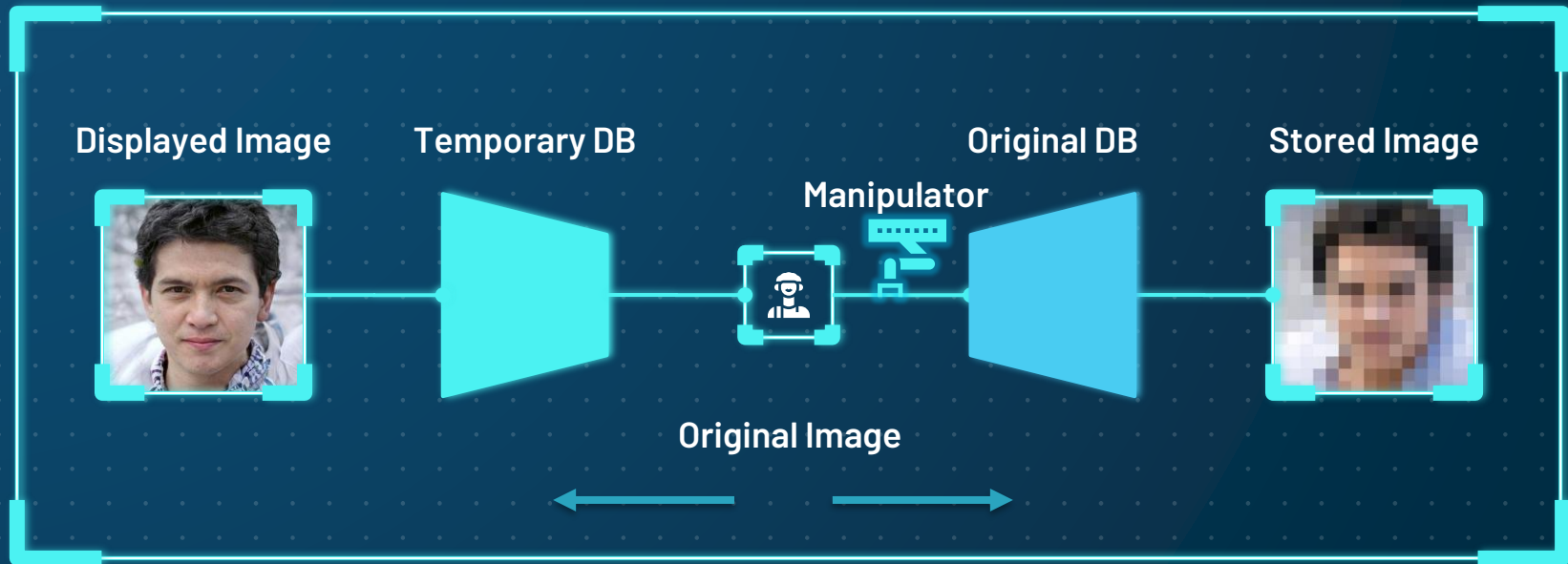
# TECHNIQUES TO PREVENT DEEPFAKE

THERE ARE 3 WAYS TO PREVENT FROM DEEPFAKE –

- Preventing Screenshots
- Preventing Screen Recording
- Server-Side Processing
- Adding Dead Pixels



# SERVER-SIDE PROCESSING





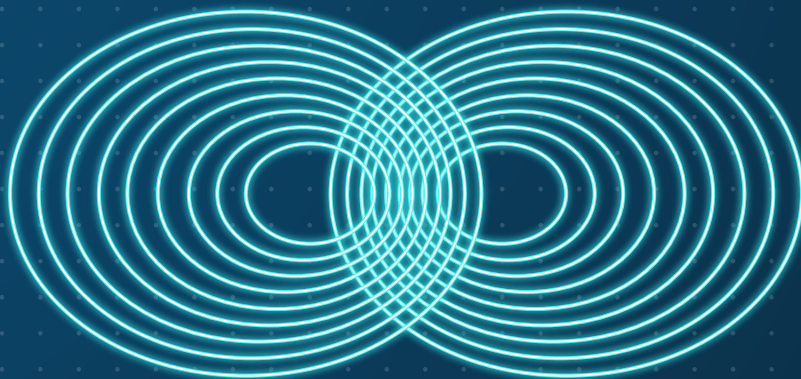
# ADDING DEAD PIXELS

“CAT”



Original Image

OUR MACHINE



“CCAATT”



Image with Dead Pixels




# FUTURE SCOPE

---

- It can be integrated to Social Media Platforms
- Decreases Cyber Crimes
- Decreases Social Anxiety

# CONCERNS

---

- It have access for what user uploads
  - Takes more time to upload an media into platforms
- 
- 