DEEPFAKES IN FACIAL RECOGNITION

Author: Bc. Milan Šalko Supervisor: Ing. Anton Firc 2023

Motivation

How resistant are facial recognition systems to deepfake attacks?

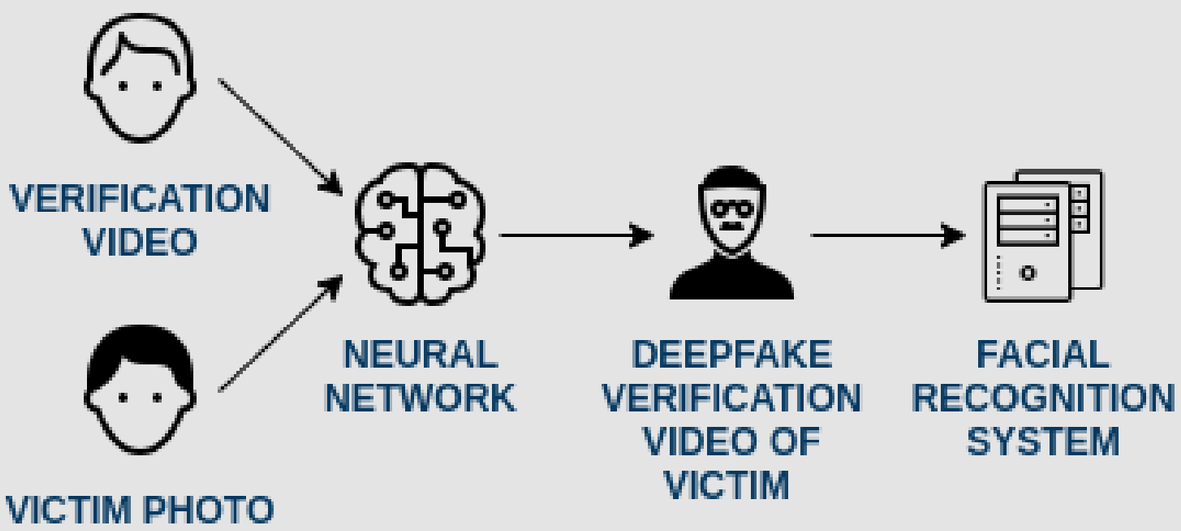
What can be the target of an attack?

Online banking

Know Your Customer

Court evidence

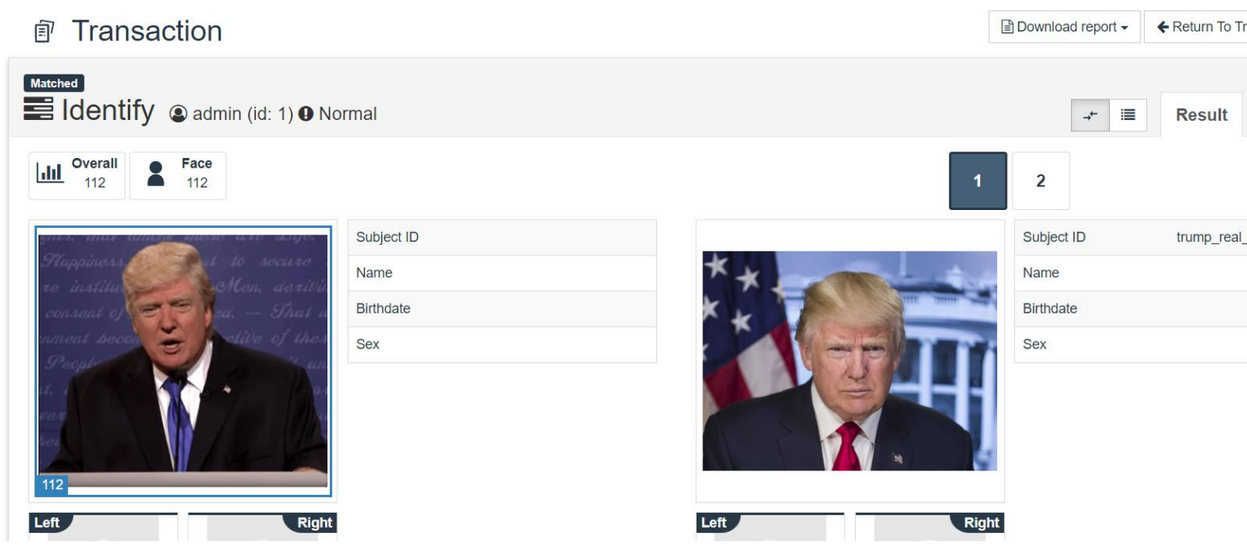
Attack vector



Experiments

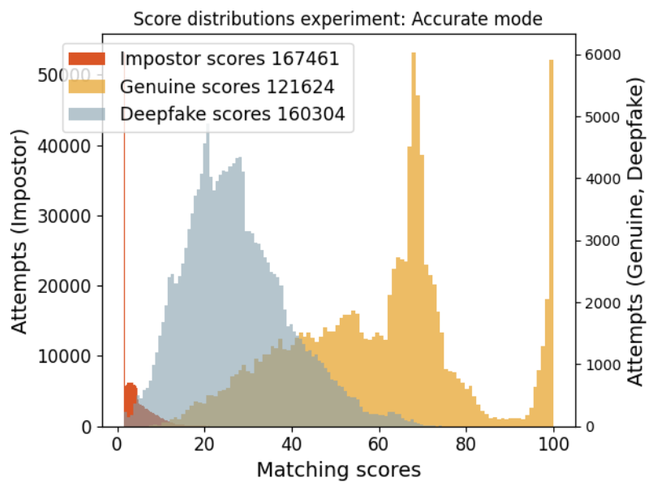
How hard is it to make a quality deepfake ?

Is it possible for an attacker to be identified by the system using deepfake as a victim?

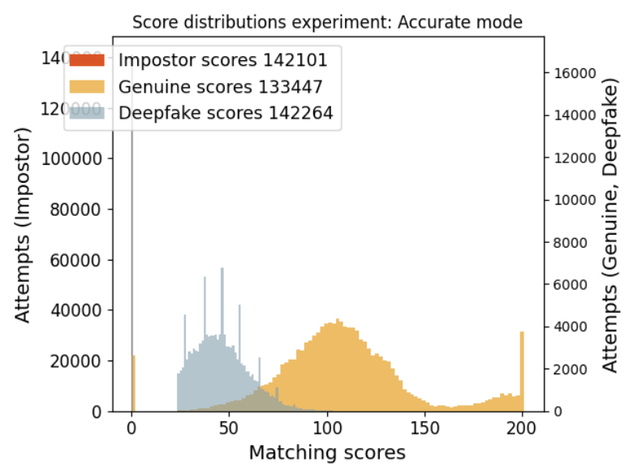


How resistant are facial recognition systems to deepfakes?

Biometry 1



Biometry 2



Excel @FIT 2023

BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF INFORMATION TECHNOLOGY