Progress

2020019252 김나현

focus on...

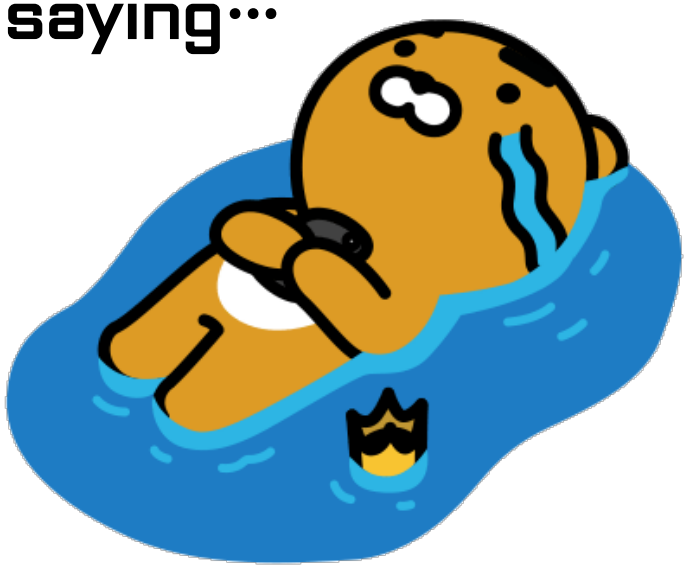
1 Adversarial Attacks

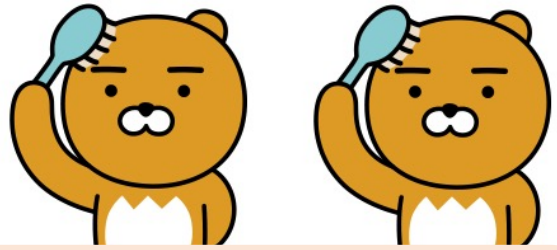
2 Reading papers

1st attempt at reading a paper

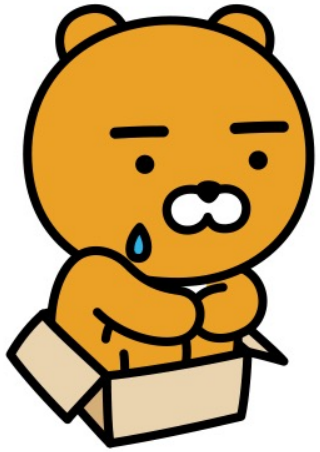
Devil's Whisper: A General Approach
for Physical Adversarial Attacks
against Commercial Black-box Speech Recognition Devices

→ Can't understand what the paper's saying…





Trying to find another paper…



Because I was just wondering
the flow of the paper and how it is organized.

suddenly got a new idea

while watching YouTube !

Copyright detection + Adversarial Attacks

Google Scholar

copyright Adversarial

Articles

About 194,000 results (**0.08** sec)

Any time
Since 2021
Since 2020
Since 2017
Custom range...

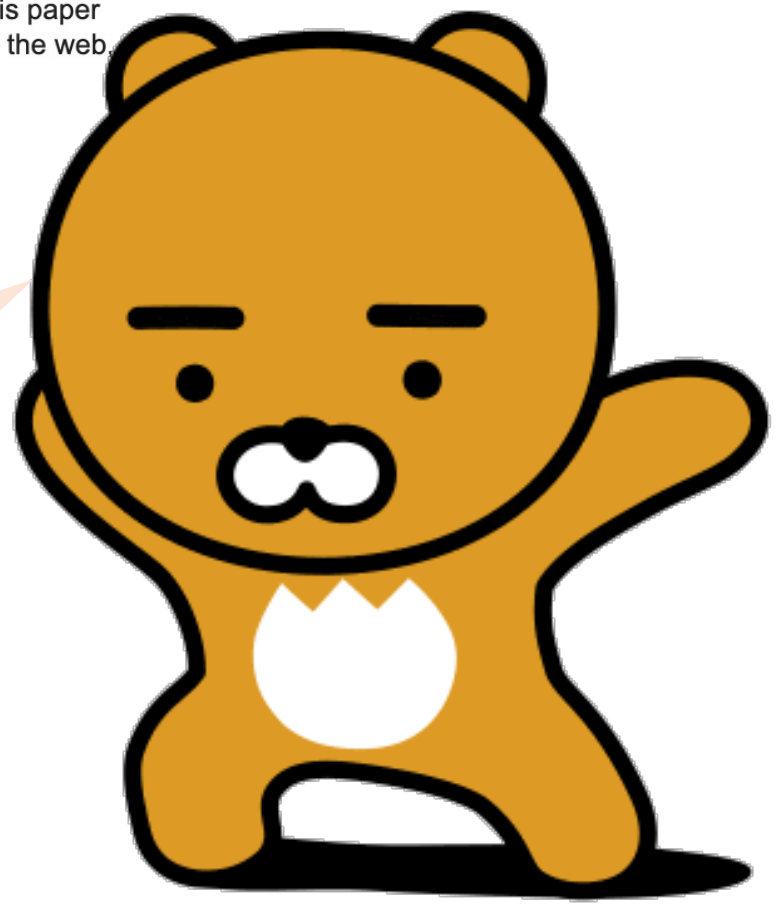
Adversarial attacks on **copyright** detection systems [PDF] mlr.press

P Saadatpanah, A Shafahi… - … Conference on Machine …, 2020 - proceedings.mlr.press

It is well-known that many machine learning models are susceptible to **adversarial** attacks, in which an attacker evades a classifier by making small perturbations to inputs. This paper discusses how industrial **copyright** detection tools, which serve a central role on the web,

☆ Cited by 13 Related articles All 4 versions »

Ah…
There's already one :(



So I decided to read it

Next goals

I'm going to…

- Study ML
- Keep reading papers and get used to it.