The Invisible Mask

Alex Fefegha
Computational Futures & AI
a.fefeghaetta@arts.ac.uk

ual: creative computing institute

did anyone actually do the homework?

The snowball activity!

TARY

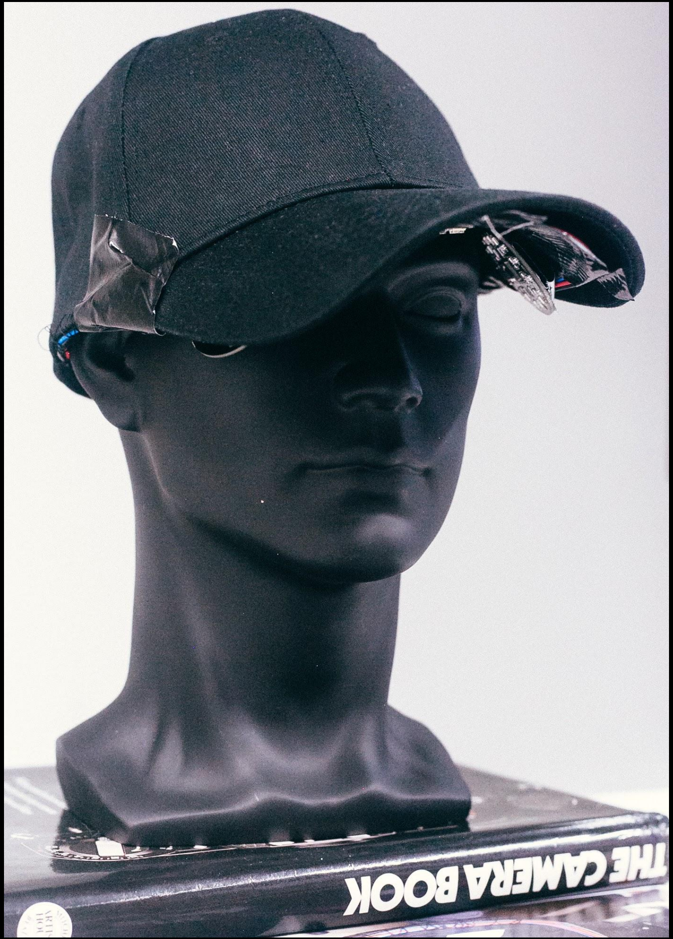
Write one sentence or question—the content depends upon the context—on a piece of paper.

Ball up your paper.

Throw your "snowballs." at *me maybe?*

Pick up the snowball and read the sentence aloud or answer the question.

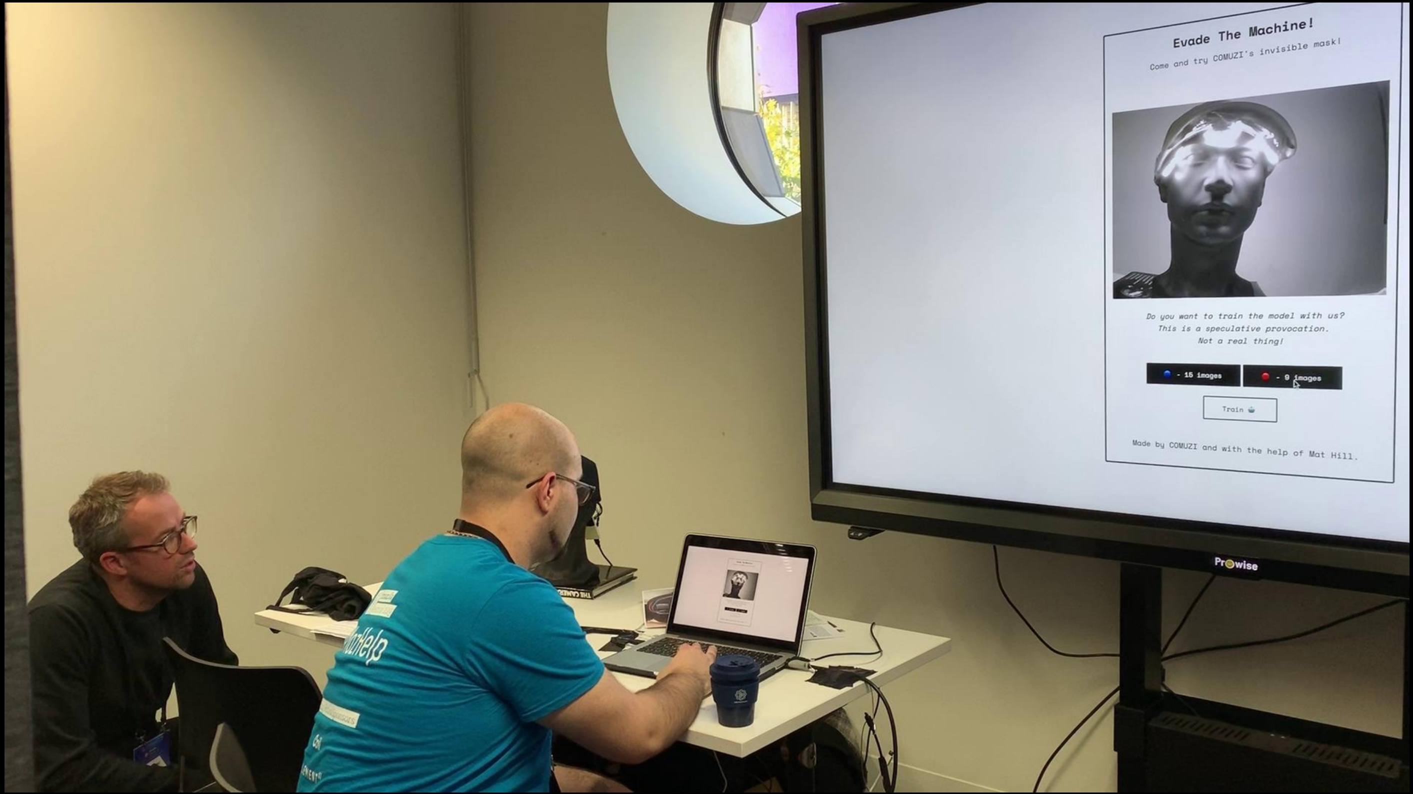
Today we are going to write some code *(might do more)*.

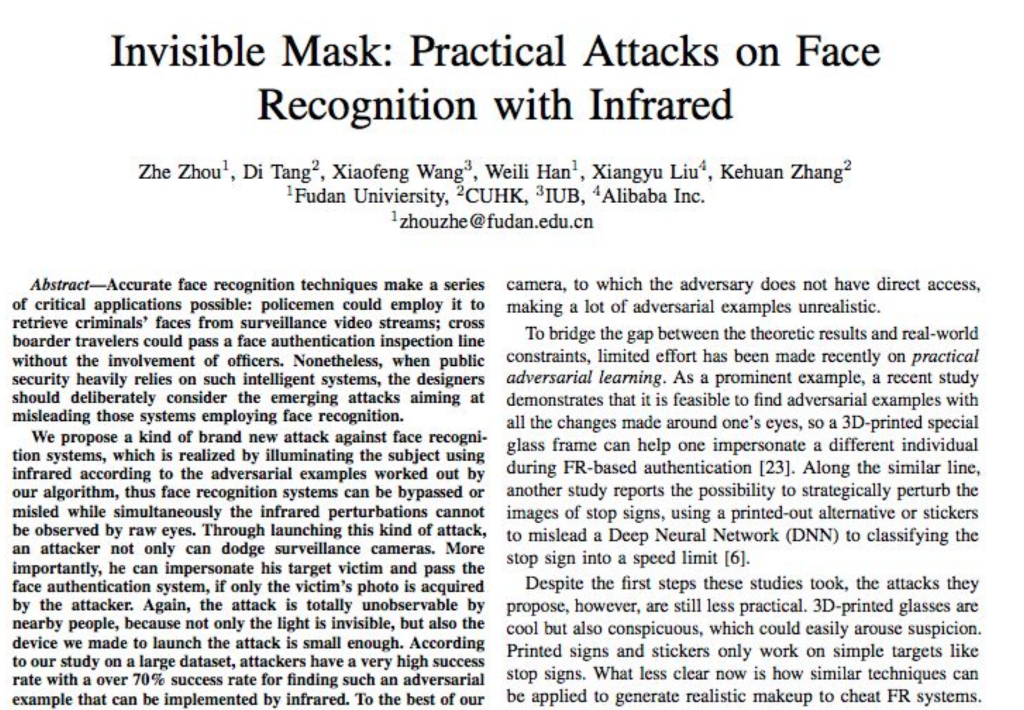


The Invisible Mask

COMUZI

A speculative provocation exploring the attack on human agency and autonomy by facial recognition technologies.


Evade The Machine!
Come and try COMUZI's invisible mask!
Do you want to train the model with us?
This is a speculative provocation.
Not a real thing!
- 15 images
- 9 images
Train
Made by COMUZI and with the help of Mat Hill.
Prowise



Invisible Mask: Practical Attacks on Face Recognition with Infrared

Zhe Zhou[1], Di Tang[2], Xiaofeng Wang[3], Weili Han[1], Xiangyu Liu[4], Kehuan Zhang[2]
[1]Fudan Univiersity, [2]CUHK, [3]IUB, [4]Alibaba Inc.
[1]zhouzhe@fudan.edu.cn

***Abstract*—Accurate face recognition techniques make a series of critical applications possible: policemen could employ it to retrieve criminals' faces from surveillance video streams; cross boarder travelers could pass a face authentication inspection line without the involvement of officers. Nonetheless, when public security heavily relies on such intelligent systems, the designers should deliberately consider the emerging attacks aiming at misleading those systems employing face recognition.**

We propose a kind of brand new attack against face recognition systems, which is realized by illuminating the subject using infrared according to the adversarial examples worked out by our algorithm, thus face recognition systems can be bypassed or misled while simultaneously the infrared perturbations cannot be observed by raw eyes. Through launching this kind of attack, an attacker not only can dodge surveillance cameras. More importantly, he can impersonate his target victim and pass the face authentication system, if only the victim's photo is acquired by the attacker. Again, the attack is totally unobservable by nearby people, because not only the light is invisible, but also the device we made to launch the attack is small enough. According to our study on a large dataset, attackers have a very high success rate with a over 70% success rate for finding such an adversarial example that can be implemented by infrared. To the best of our

camera, to which the adversary does not have direct access, making a lot of adversarial examples unrealistic.

To bridge the gap between the theoretic results and real-world constraints, limited effort has been made recently on *practical adversarial learning*. As a prominent example, a recent study demonstrates that it is feasible to find adversarial examples with all the changes made around one's eyes, so a 3D-printed special glass frame can help one impersonate a different individual during FR-based authentication [23]. Along the similar line, another study reports the possibility to strategically perturb the images of stop signs, using a printed-out alternative or stickers to mislead a Deep Neural Network (DNN) to classifying the stop sign into a speed limit [6].

Despite the first steps these studies took, the attacks they propose, however, are still less practical. 3D-printed glasses are cool but also conspicuous, which could easily arouse suspicion. Printed signs and stickers only work on simple targets like stop signs. What less clear now is how similar techniques can be applied to generate realistic makeup to cheat FR systems.

Invisible Mask: Practical Attacks on Face Recognition with Infrared

Zhou et al (2018)

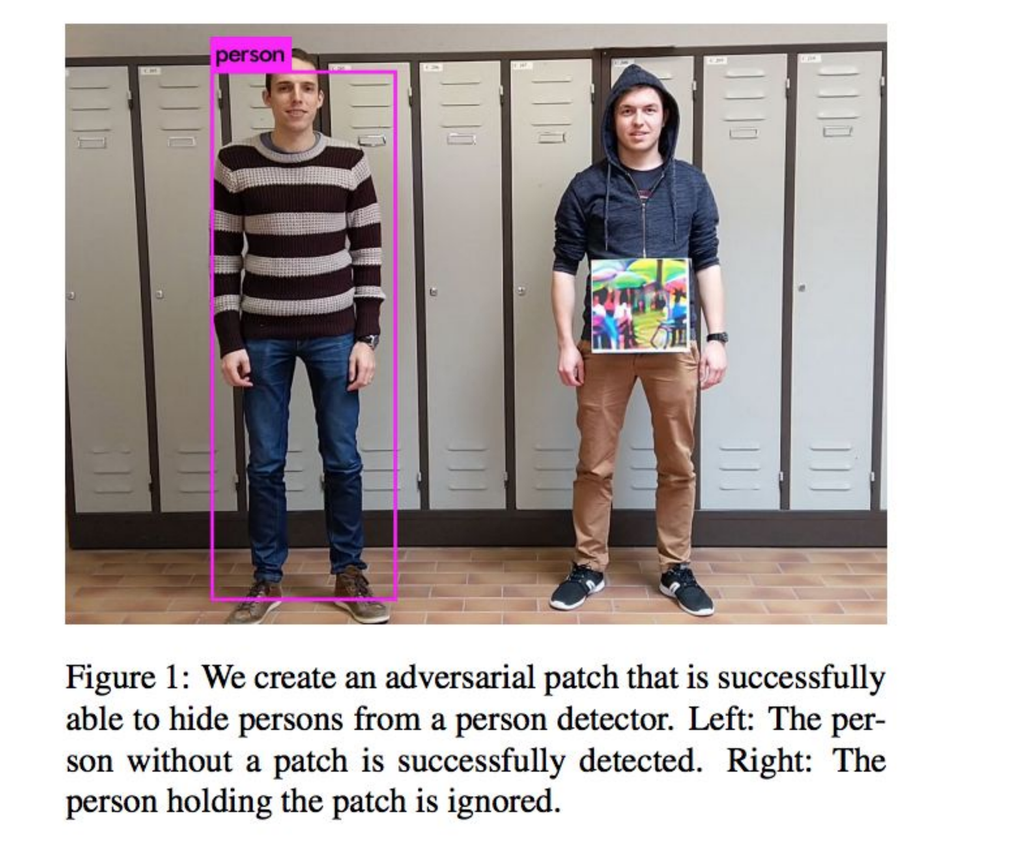
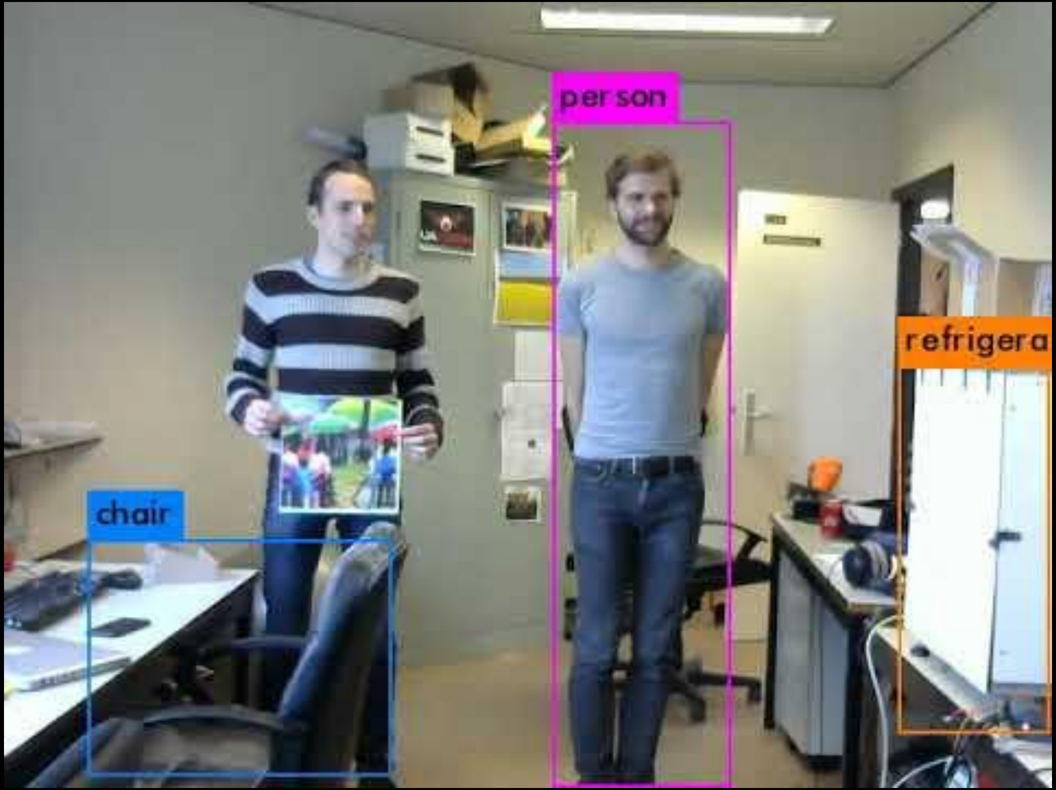
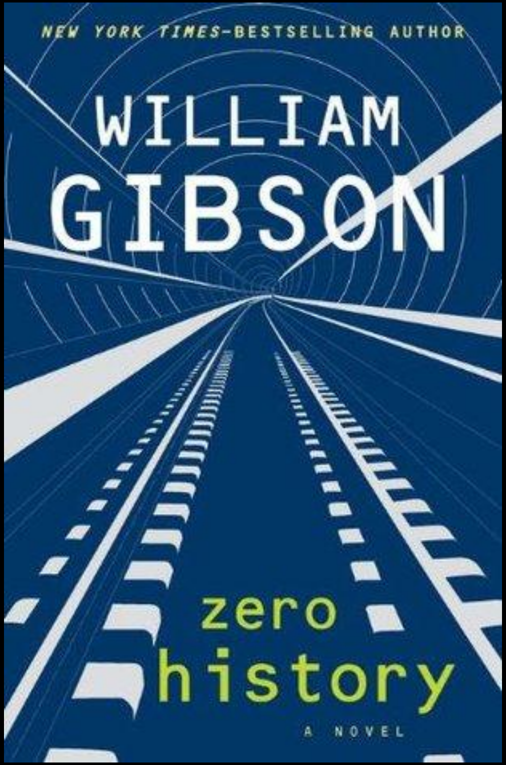


Figure 1: We create an adversarial patch that is successfully able to hide persons from a person detector. Left: The person without a patch is successfully detected. Right: The person holding the patch is ignored.

Fooling automated surveillance cameras: adversarial patches to attack person detection

Thys et al (2019)


person
refrigera
chair



Zero History

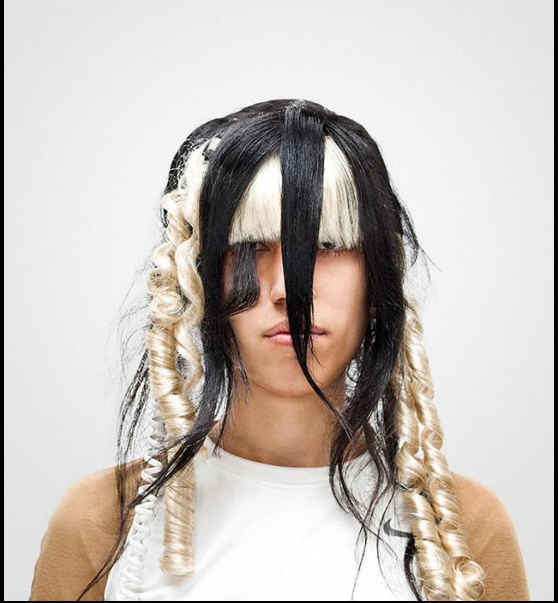
William Gibson (2010)

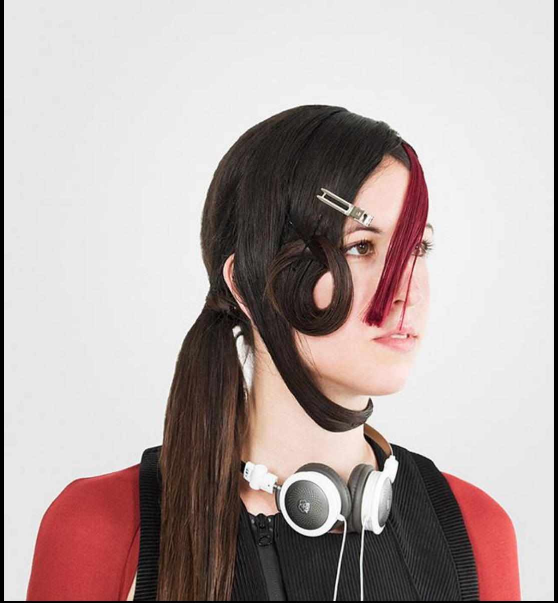
‘They forgot the figure wearing the ugly T-shirt. Forget the head atop it, the legs below, feets, arms, hands. It compels erasure. That which the camera sees, bearing the sigil, it deletes from the recalled image…”

Adversarial machine learning.

A form of hacking focused on fooling machine learning models.

Most examples are focused on image classification.





CV Dazzle

Adam Harvey

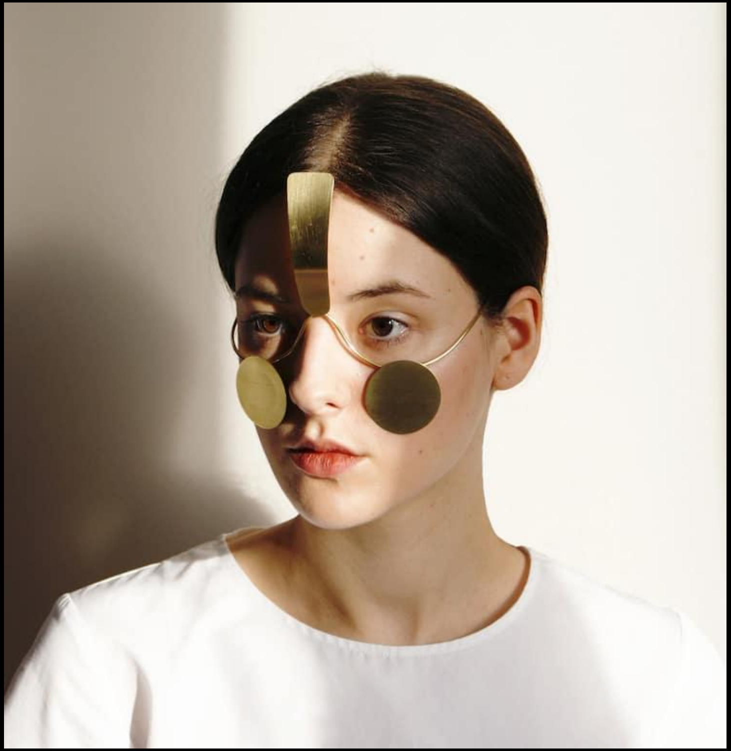
HyperFace™
Prototype

HyperFace™ Type-01 Prototype / Adam Harvey

Rendering by Ece Tankal / Hyphen-Labs

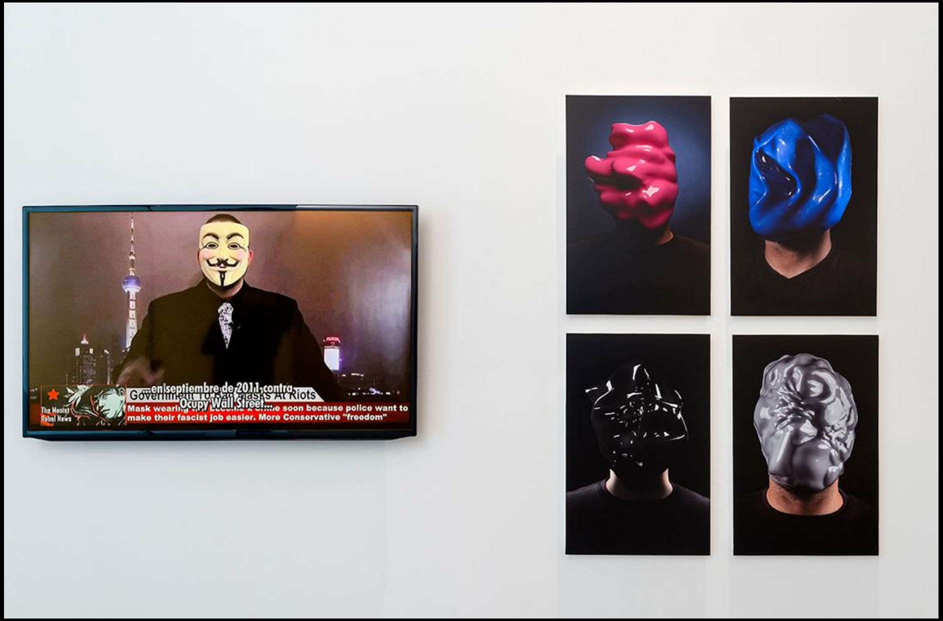
Hyperface

Adam Harvey &
Hyphen-Labs



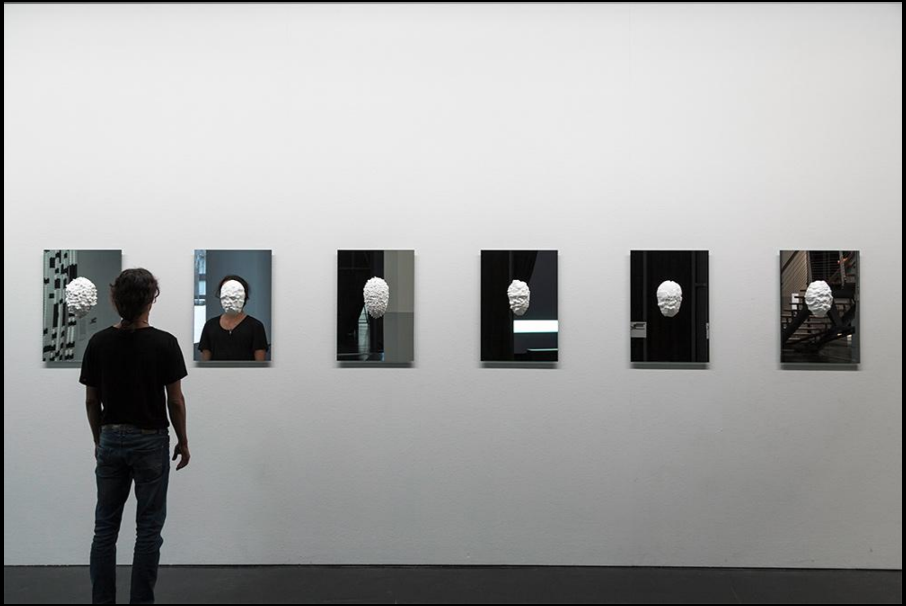
Incognito

Ewa Nowak


...en septiembre de 2011 contra
Government To Ban Masks At Riots
Ocupy Wall Street...
The Maoist Rebel News
Mask wearing will become a crime soon because police want to make their fascist job easier. More Conservative "freedom"

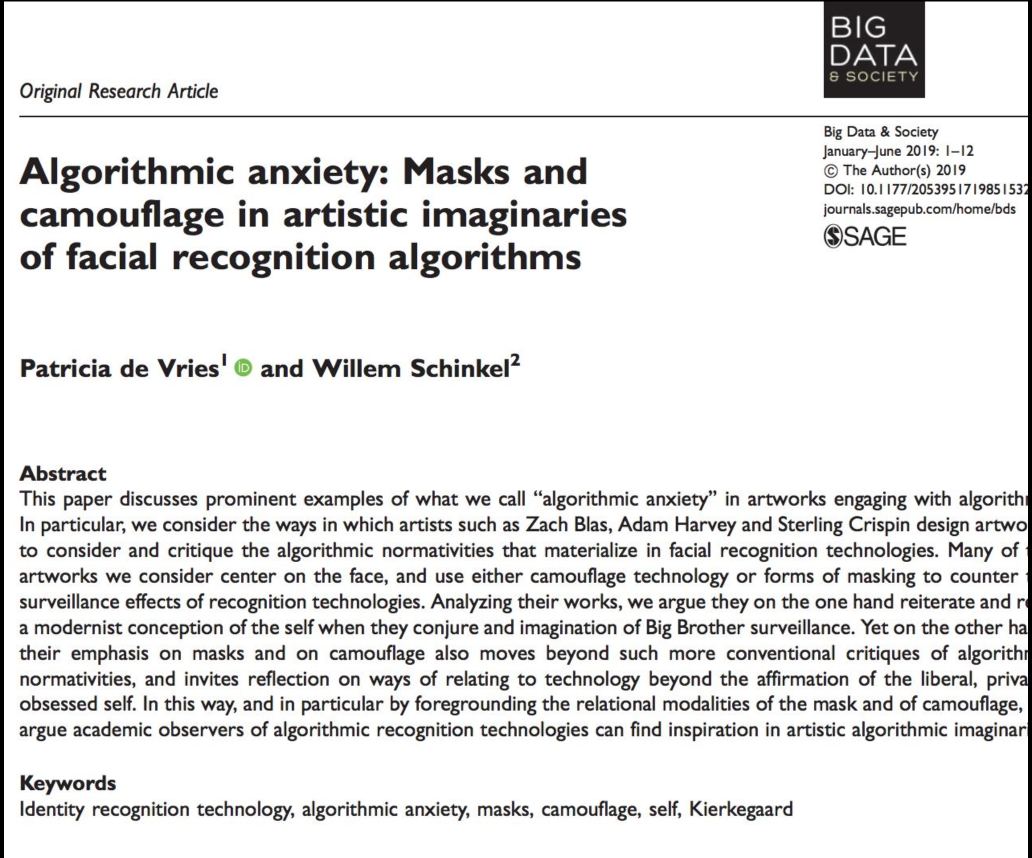
Facial Weaponization Suite

Zach Blas



Data Masks

Sterling
Crispin



Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June 2019: 1–12
© The Author(s) 2019
DOI: 10.1177/2053951719851532
journals.sagepub.com/home/bds
SAGE

Algorithmic anxiety: Masks and camouflage in artistic imaginaries of facial recognition algorithms

Patricia de Vries[1] and Willem Schinkel[2]

Abstract
This paper discusses prominent examples of what we call “algorithmic anxiety” in artworks engaging with algorith
In particular, we consider the ways in which artists such as Zach Blas, Adam Harvey and Sterling Crispin design artwo
to consider and critique the algorithmic normativities that materialize in facial recognition technologies. Many of t
artworks we consider center on the face, and use either camouflage technology or forms of masking to counter t
surveillance effects of recognition technologies. Analyzing their works, we argue they on the one hand reiterate and re
a modernist conception of the self when they conjure and imagination of Big Brother surveillance. Yet on the other ha
their emphasis on masks and on camouflage also moves beyond such more conventional critiques of algorithm
normativities, and invites reflection on ways of relating to technology beyond the affirmation of the liberal, priva
obsessed self. In this way, and in particular by foregrounding the relational modalities of the mask and of camouflage,
argue academic observers of algorithmic recognition technologies can find inspiration in artistic algorithmic imaginar

Keywords
Identity recognition technology, algorithmic anxiety, masks, camouflage, self, Kierkegaard

Algorithmic anxiety: Masks and camouflage in artistic imaginaries of facial recognition algorithms

de Vries and Schinkel (2019)

Let’s explore some code!

Last week, we explored Image Classification.

We built our own image classifier tool using ml5.js
+ our webcam!

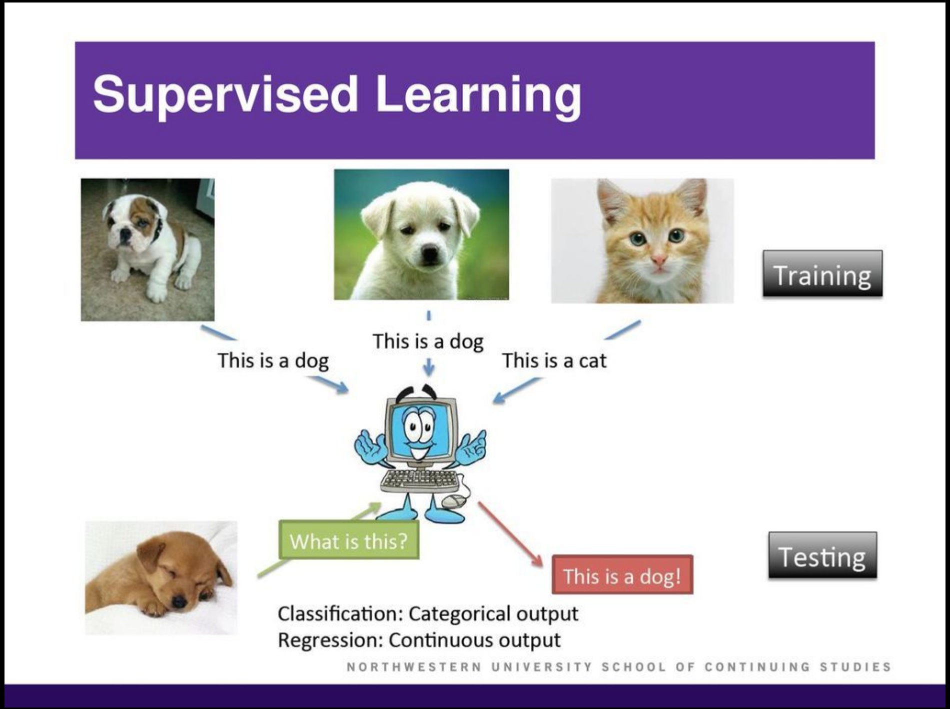
Today we are going to take that one step further.

We are going to learn about feature extraction through transfer learning.

Supervised Learning

Training data is **labeled.**

Source: https://slideplayer.com/slide/12369271/



Supervised Learning

This is a dog

This is a dog

This is a cat

Training

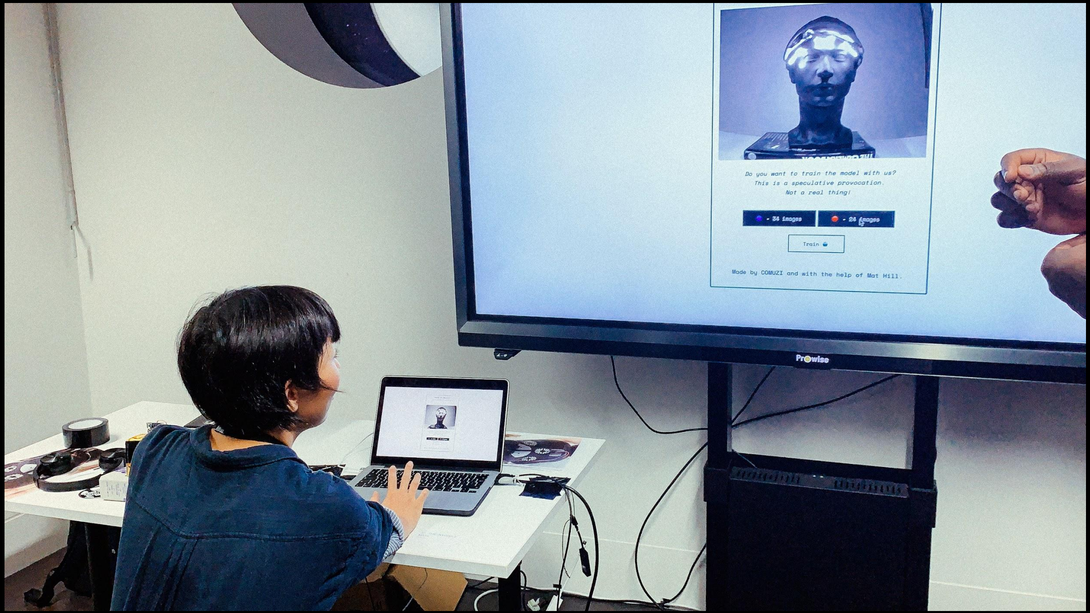
What is this?

This is a dog!

Testing

Classification: Categorical output
Regression: Continuous output

NORTHWESTERN UNIVERSITY SCHOOL OF CONTINUING STUDIES



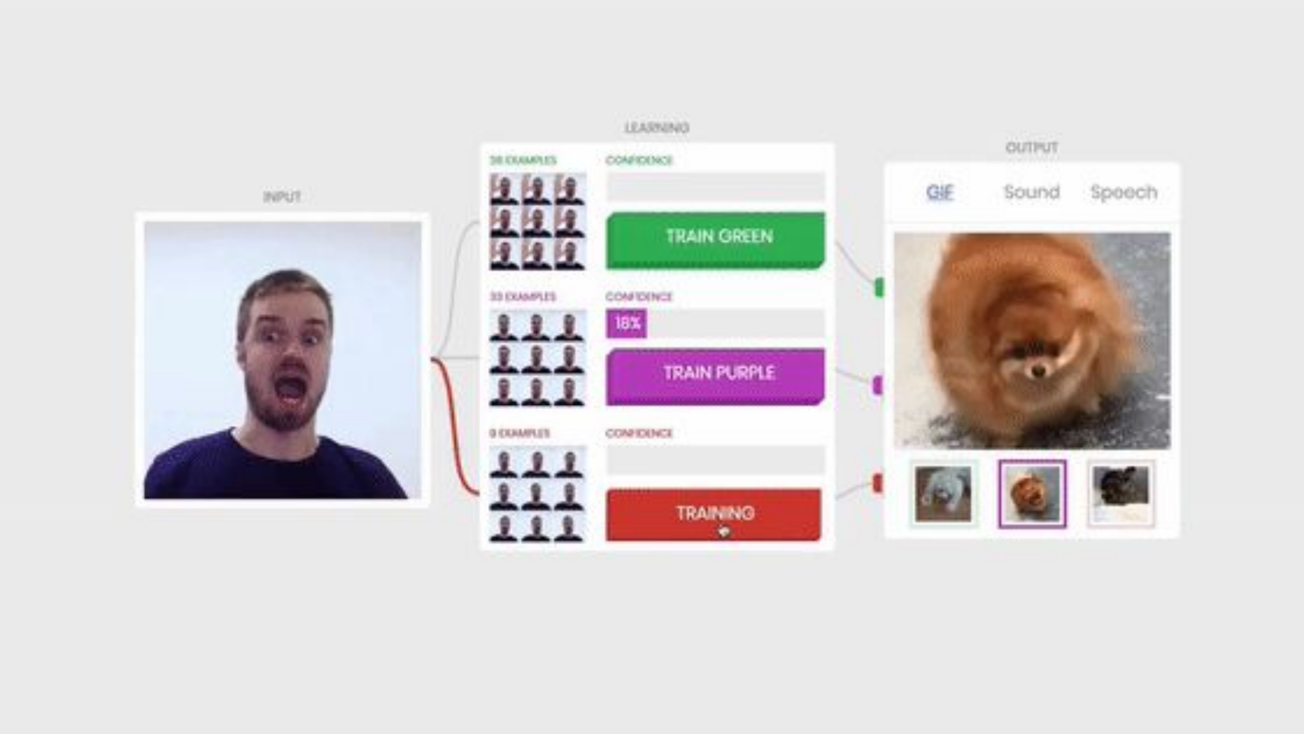
Do you want to train the model with us?
This is a speculative provocation.
Not a real thing!

Made by COMUZI and with the help of Mat Hill.

https://sassy-end.glitch.me/

Transfer Learning.

Using a already existing model and add more data on top of it!

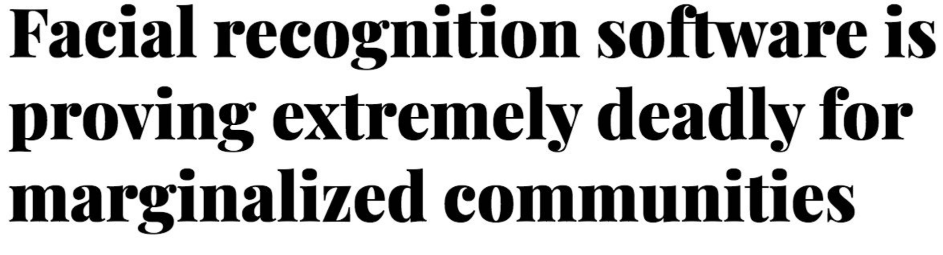


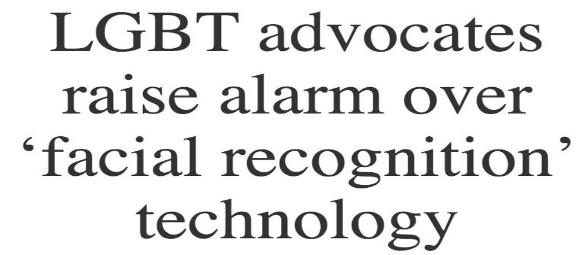
https://teachablemachine.withgoogle.com/

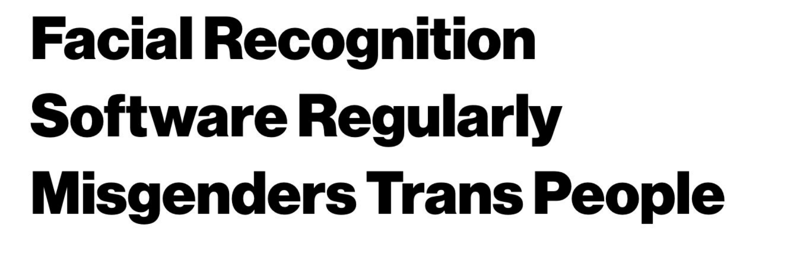
Break

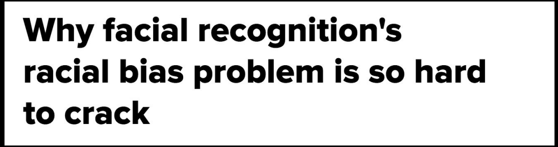
Homework or class work.

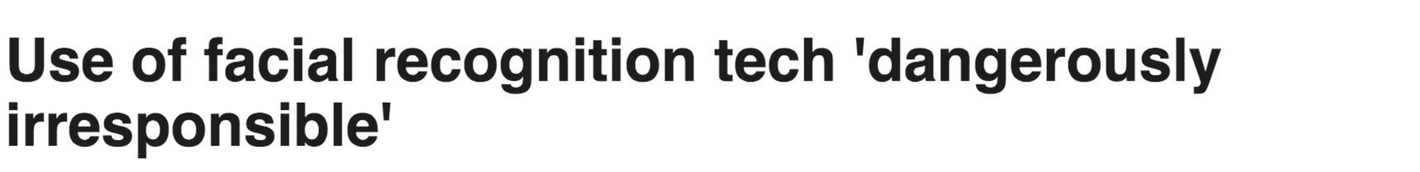
Make a guide for someone from a marginalized group on how to use a invisible mask.

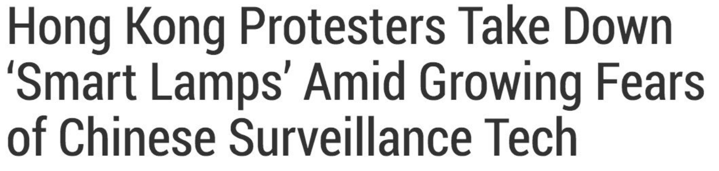

Facial recognition software is proving extremely deadly for marginalized communities

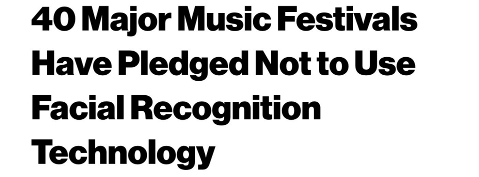

LGBT advocates raise alarm over ‘facial recognition’ technology


Facial Recognition Software Regularly Misgenders Trans People


Why facial recognition's racial bias problem is so hard to crack

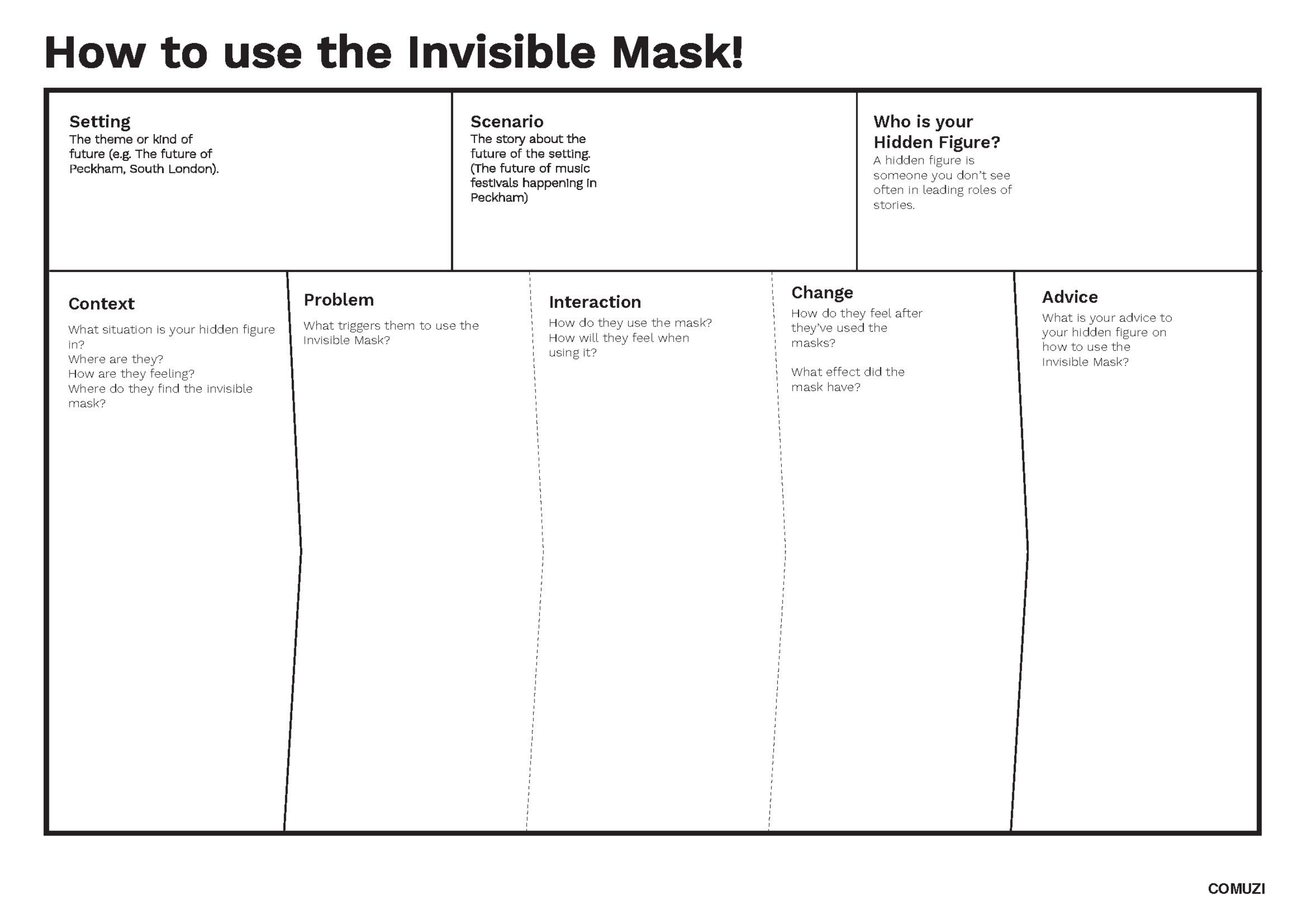

Use of facial recognition tech 'dangerously irresponsible'


Hong Kong Protesters Take Down ‘Smart Lamps’ Amid Growing Fears of Chinese Surveillance Tech


40 Major Music Festivals Have Pledged Not to Use Facial Recognition Technology

Worldbuilding is the process of constructing an imaginary world, sometimes associated with a whole fictional universe.

The resulting world may be called a constructed world.



How to use the Invisible Mask!

Setting
The theme or kind of future (e.g. The future of Peckham, South London).

Scenario
The story about the future of the setting. (The future of music festivals happening in Peckham)

Who is your Hidden Figure?
A hidden figure is someone you don't see often in leading roles of stories.

Context
What situation is your hidden figure in?
Where are they?
How are they feeling?
Where do they find the invisible mask?

Problem
What triggers them to use the Invisible Mask?

Interaction
How do they use the mask?
How will they feel when using it?

Change
How do they feel after they've used the masks?

What effect did the mask have?

Advice
What is your advice to your hidden figure on how to use the Invisible Mask?

COMUZI

Class done.
You are free!

ual: creative computing institute