

OH YEAH DITTO, I CHOOSE YOU.

OH YEAH

百變怪

就決定是你了！



組員：鄭宇兩、羅崧瑋、黃宥睿、王朝立

TWM-AI RED TEAM-05

系統測試畫面

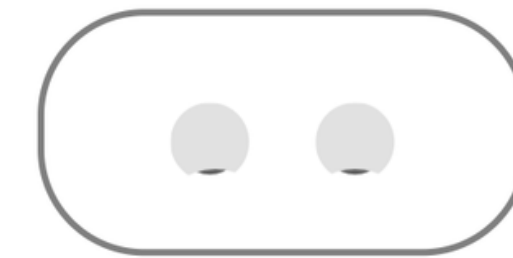
請在框線中向上翻轉您的身分證



在框線內完整拍攝
身分證 反面

在框線內完整拍攝
身分證 正面

請在框線中向左右翻轉您的身分證

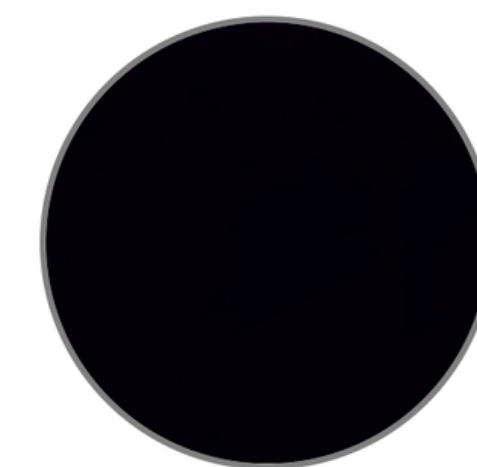


請拉近手機與眼睛的距離

對著鏡頭閉眼
內心默數 2秒 後張開
請移除口罩、帽子或墨鏡等任何遮住臉的物品

換我試試看

Powered by Taiwan Mobile



請完整地將您的臉放在圓框內
請勿遮擋臉部

請移除口罩、帽子或墨鏡等遮住臉的物品



如同過馬路前看來車一樣

看一下左邊
看一下右邊

請保持將臉完整的對準圓框

初步推斷驗證過程

- 不斷進行各別測試
- 詢(打)問(擾)主辦單位



鄭宇兩 <betan050423@gmail.com>

寄給 KevinMHTsai ▾

10月22日 週三 下午2:13 (9 天前) ☆ 😊 ↩ ⋮

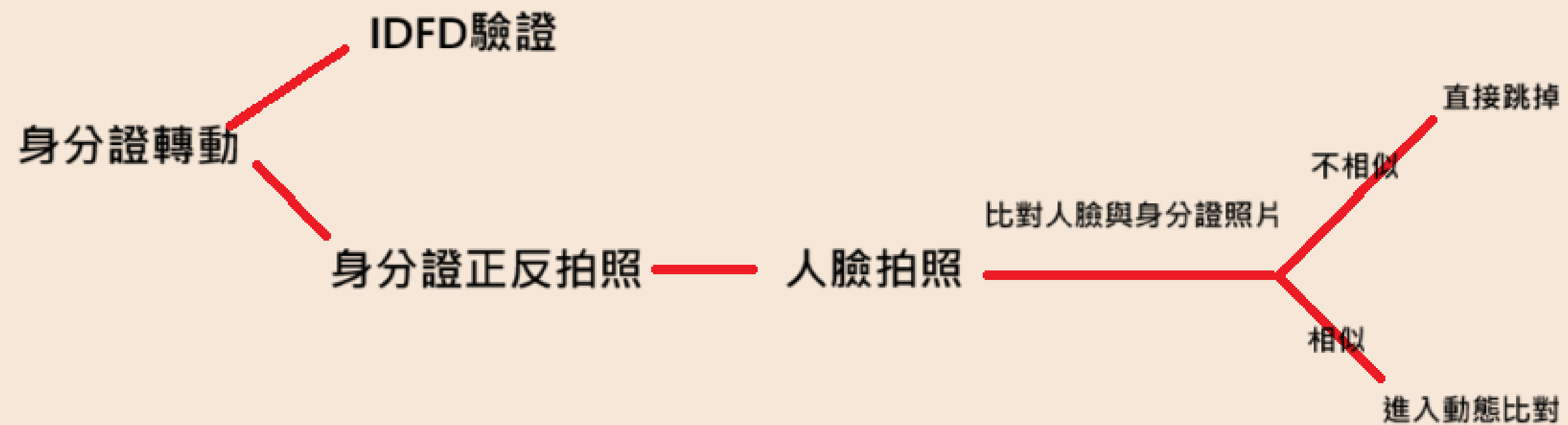
您好，
我們是有報名本次競賽的隊伍「Oh Yeah 百變怪，就決定是你了！」，
我是隊長 鄭宇兩。

我們隊伍在測試的過程中，
有幾點問題是有關貴單位那邊提供的測試系統想確認一下：

1. 有關「加分項目：文件篡改（Fake Document Attack）」的部分，主要指的部分就是**IDFD是否通過**的部分嗎？還是說是有另外的內容需要實作的。
2. 關於換臉測試通過的評判標準，是否主要就為驗證結束後的 **驗證結果** 以及 **PAD是否通過** 的這兩部分去進行評斷。例如驗證結果%數越高，就代表本次測試最終判讀的可信度就是越高之類的(或是相反)
3. 關於測試結束後的最下方資訊，是否都是固定的內容，並且也不會是本次比賽需要去修改的內容、或是著重的地方嗎？(例如最下方的姓名都是陳筱玲，出生年月之類的都是固定的)
4. 關於本次挑戰內容是否就是單純的去對人臉辨別的系統進行攻擊，而完全不需要再去對測試環境進行另外的攻擊之類的。
5. 是否能夠根據測試的UUID來去回去查詢當時測試所驗證的資料
6. 有關挑戰內容 **Deepfake技術、攻擊活體偵測**，其中的**Deepfake技術**指的是**PAD是否通過**，而**攻擊活體偵測**指的則是最後的驗證結果的部分嗎？兩個部分是獨立去判讀的，還是彼此會去綜合考量的呢？
7. 有關建議可以提及的 **防禦手段及後續建議進行強化說明** 部分，我們是否是只需要去提出概念來說明這部分就好，又或是我們是需要去修改整個驗證系統來讓他能夠去成功阻擋假冒攻擊呢？如果是需要去實作出來這部分的話，請問能否麻煩主辦方協助提供測試系統的原始代碼或是相關的驗證邏輯呢？

不好意思我們的疑問可能會比較多，
還需麻煩您協助解答了，
感謝協助

HOW 2 BYPASS



HOW 2 BYPASS

- 文件篡改 (Fake Document Attack)
 - IDFD 身分證驗證
- Deepfake技術
 - 人證比對
- 攻擊活體偵測
 - PAD 動態識別

驗證結果	
人證比對	100%
TID	InnoServe
UUID	3ffe4e41-a
IDFD是否通過	True
PAD是否通過	True

身分證浮水印

活體辨識

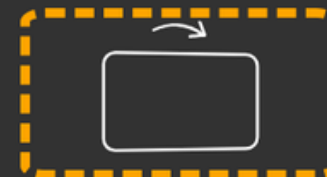
HOW 2 BYPASS

- IDFD

請在框線中向上翻轉您的身分證



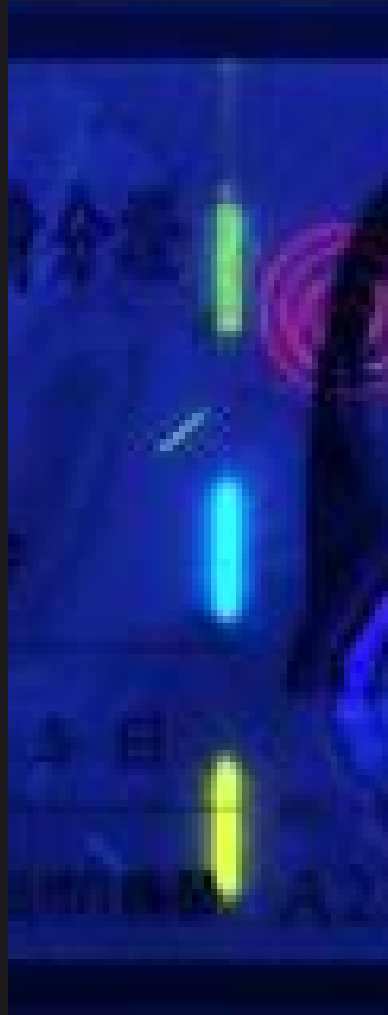
請在框線中向左右翻轉您的身分證



BYPASS ID



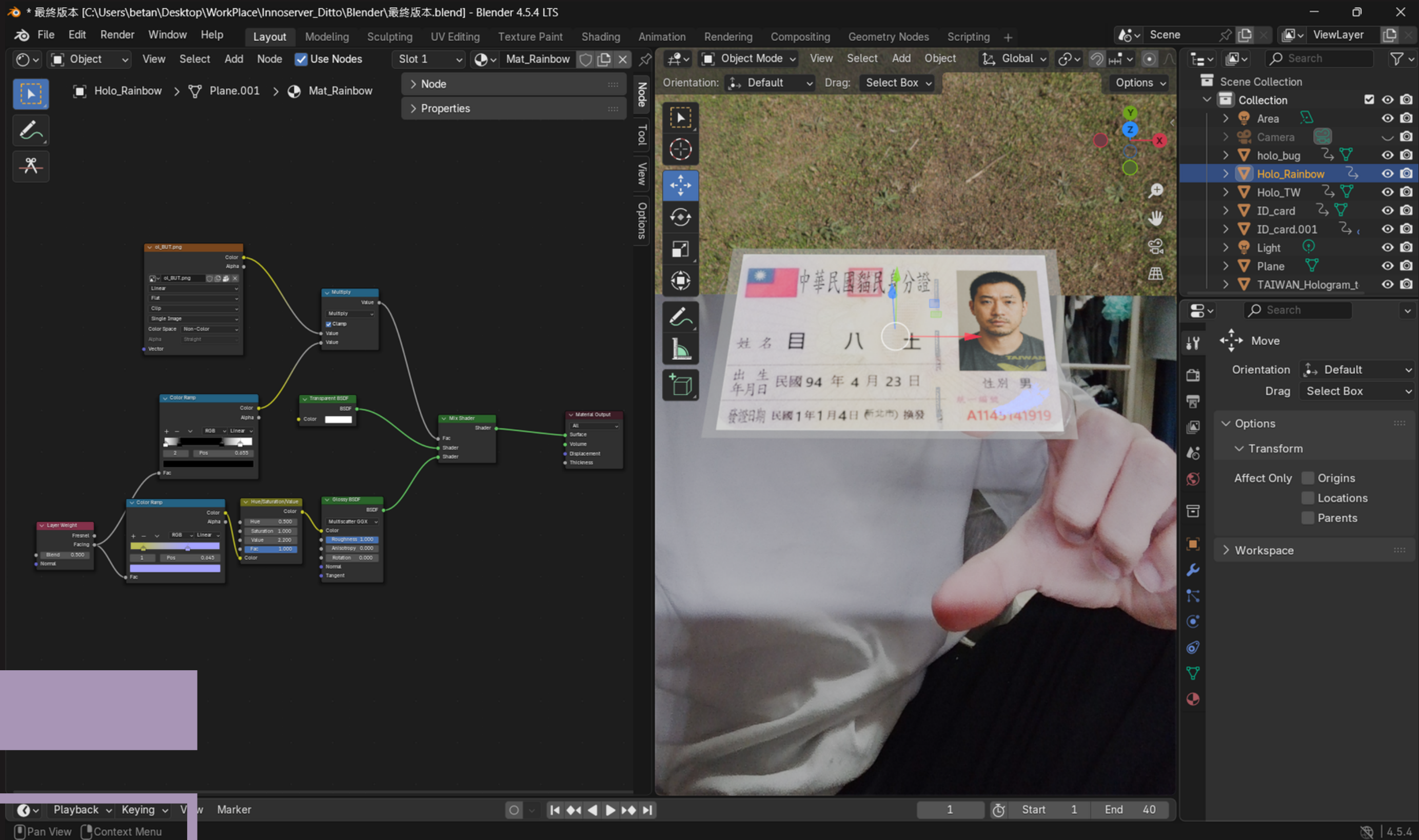
BYPASS IDFD



BYPASS IDFD



BYPASS IDFD



BYPASS IDFD



BYPASS IDFD



BYPASS IDFD

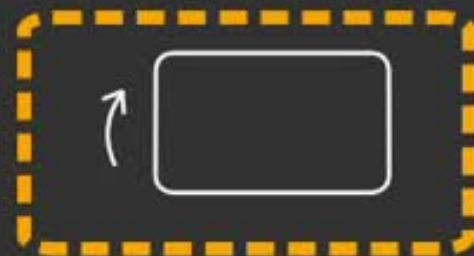


BYPASS IDFD



BYPASS IDFD

請在框線中向上翻轉您的身分證



Powered by Taiwan Mobile

HOW 2 BYPASS

- DeepFake

在框線內完整拍攝
身分證 反面

在框線內完整拍攝
身分證 正面



HOW 2 BYPASS

- DeepFake



HOW 2 BYPASS

- DeepFake



HOW 2 BYPASS

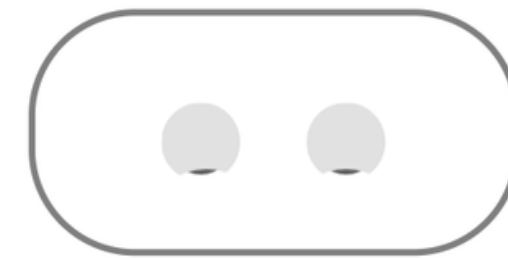
- PAD



如同過馬路前看來車一樣

看一下左邊
看一下右邊

請保持將臉完整的對準圓框



請拉近手機與眼睛的距離

對著鏡頭閉眼
內心默數 2秒 後張開
請移除口罩、帽子或墨鏡等任何遮住臉的物品

換我試試看

Powered by Taiwan Mobile

BYPASS PAD

sensity-ai/dot

The Deepfake Offensive Toolkit



7

Contributors

23

Issues

5k

Stars

483

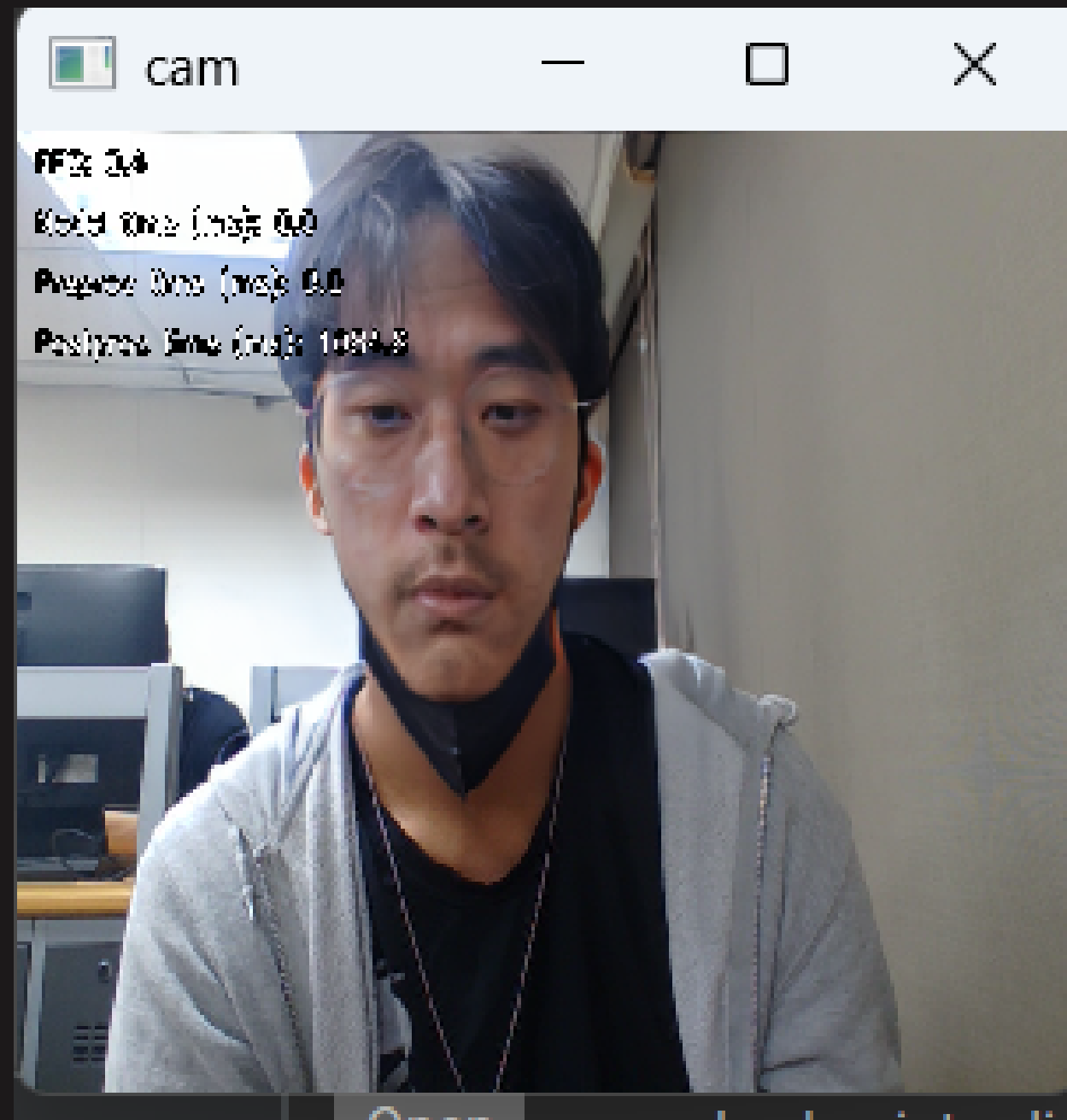
Forks



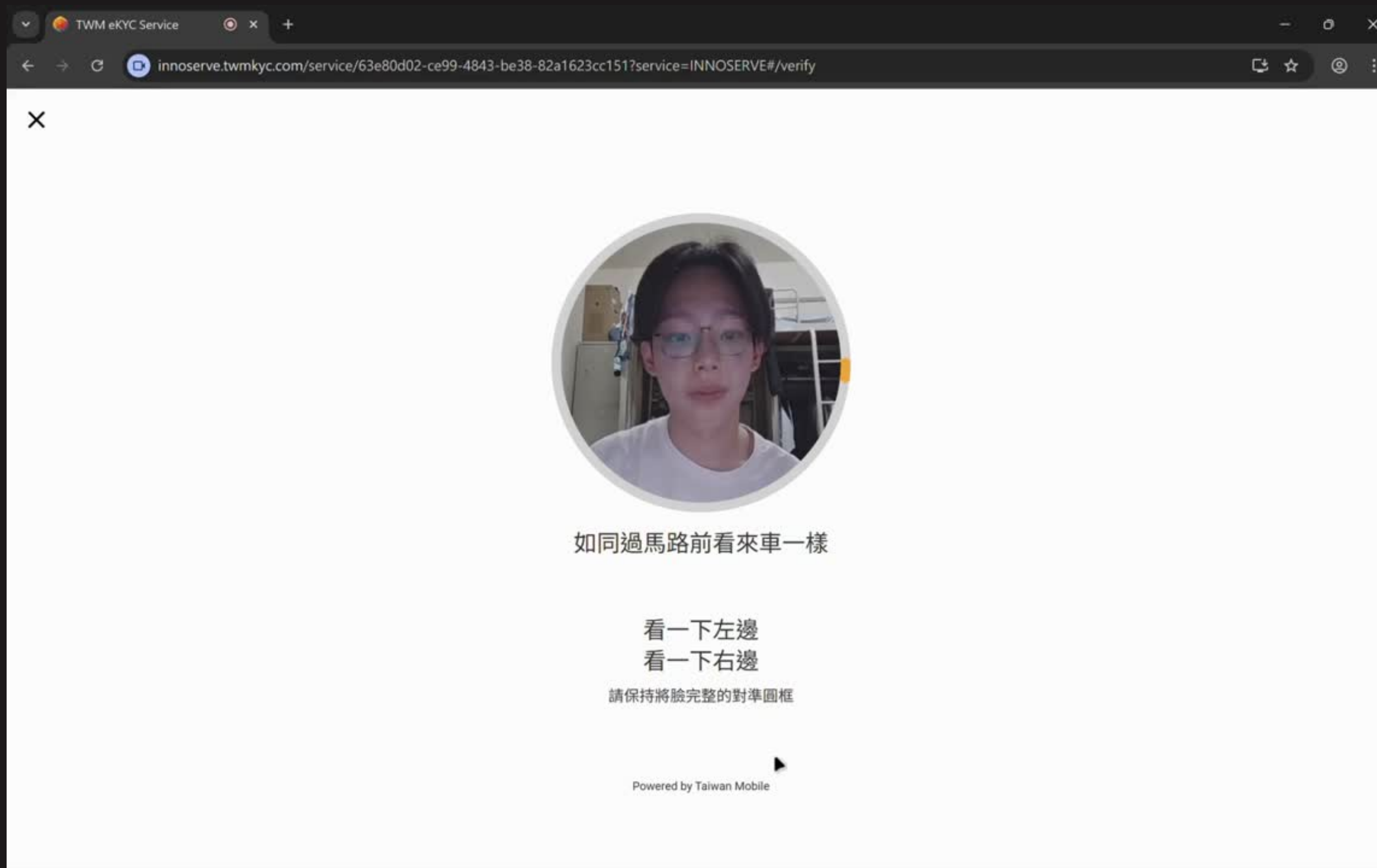
sensity-ai/dot: The Deepfake Offensive Toolkit

The Deepfake Offensive Toolkit. Contribute to sensity-ai/dot development by creating an account on GitHub.

BYPASS PAD



BYPASS PAD



驗證結果

90%

TID	InnoServe
UUID	63e80d02-ce99-4843-be38-82a1623cc151
IDFD是否通過	False
PAD是否通過	True
姓名	陳筱玲
出生年月日	78/05/20
發證日期	94/7/1(北市)換發
性別	女
身分證字號(正)	A234567890
父親	陳德明
母親	吳春美
身分證字號(背)	A234567890
配偶	N/A
役別	N/A

重新執行

整個攻擊鍊

- IDFD用影片
- Deepfake直接換照片
- PAD dot換臉

防禦建議

 驗證結果

100%

TID	InnoServe
UUID	3ffe4e41-aaff-4aec-b66b-7dc15c5b30b6
IDFD是否通過 PAD是否通過	True True

防禦建議

 驗證結果

88%

TID	InnoServe
-----	-----------

UUID	6e018104-ca01-4316-b138-06f
------	-----------------------------

IDFD是否通過	True
PAD是否通過	True

姓名	陳筱玲
出生年月日	78/05/20
發證日期	94/7/1(北市)換發
性別	女
身分證字號(正)	A234567890
父親	陳德明

姓名	陳筱玲
出生年月日	78/05/20
發證日期	94/7/1(北市)換發
性別	女
身分證字號(正)	A234567890
父親	陳德明
母親	吳春美
身分證字號(背)	A234567890
配偶	N/A
役別	N/A
出生地	臺北市
住址	臺北市內湖區葫洲里1鄰民權東路六段2
正規化住址	"臺北市\n內湖區\n葫洲里1鄰\nE
姓名(健保卡)	
出生年月日(健保卡)	
身分證字號(健保卡)	
健保卡號	

InnoServe

aff-4aec-b66b-7dc15c5b30b6

True
True

防禦建議

防禦建議

About IDFD

- 完整度與遮擋規範：
 - 強制四角入鏡，檢測邊框完整、遮擋（手指／貼紙／遮蔽物）與裁切
 - 未達標準者一律退件
- 透光檢測：
 - 新增背面透光步驟，比對透光視窗圖樣與前後幾何對位
 - 未通過者轉人工複審

防禦建議

About Deep Fake

- 欄位一致性（OCR／條碼／MRZ）：
 - 姓名、證號、生日、到期日、發證機關與條碼
 - 身分證要與前次IDFD一致
 - 視覺相似度：
 - 全域 SSIM/LPIPS + 局部關鍵點（SIFT/ORB）匹配
 - 比對版面紋理、字型、微刮痕/污點位置

防禦建議

About PAD

- 姿態挑戰擴大：
 - 要求頭部大角度轉動（YAW 約 $\pm 45^\circ$ 、PITCH 約 $\pm 25^\circ$ ）
 - 並搭配視線與表情變化，以暴露模型邊界與失真
 - 部分遮擋臉部
- 動態光照檢核：
 - 引導由背光轉正光、左右移動光源
 - 檢查皮膚高光、陰影連續性與 RPPG 一致性

防禦建議

About ALL

- 單一連續會話：
 - 於同一段錄影中依序完成「持證自拍 → 活體（PAD）→ 深偽檢測」
 - 中斷則重啟流程。
- 跨步驟人臉綁定：
 - 證件照、活體影像與深偽檢測樣本須為同一人臉嵌入
 - 設置相似度下限，任一步不一致即阻斷
- 會話／裝置綁定：
 - 全程維持相同 SESSION、裝置指紋與網路環境
 - 異常切換列為高風險樣本

THANKS FOR LISTENING