

Abusing Intended Feature And Bypassing Facial Recognition

Author – Ishwar Kumar

TenguCon 2024

\$ WHOAMI \$

- Aspiring Security Researcher
- Bug Bounty Hunter
- CTF Player
- Uni Student @Comp.Sci.Eng.
- Ranked Top15 researcher @NCIIPC



Ishwar Kumar [Get verified](#)

@Ravenzbb

Security Researcher 

 Internet & Cyber Cafe [medium.com/@Ishwar-Kumar](#)

 Joined April 2020

3,734 Following **439** Followers

[Edit profile](#)



- T (Target Application) = *Kwikipic*



Let's Get Started

Manage your photos seamlessly

Sign up or Login

Get your photos in one tap!

Share pictures with friends and family without clogging your gallery. Find your event photos instantly!



Save phone memory

Don't worry about losing data. Store all photos in encrypted aws s3 buckets for free. Manage personal gallery and shared group albums using SOTA Face Recognition



Set group settings based on your needs

Select who can upload. Choose if users can see all photos or just their own. Select people whose photos you want to auto-sync to your phone gallery.



APPLICATION USES A.I. ? COOL 😊

- The application uses Artificial Intelligence to map out the face of any particular user from the group photos
- Automatically find and categorize user images based on their face.
- Saves time by eliminating the need for manual photo searching.

USER SIGNUP WITH MOBILE/EMAIL



VERFIY WITH OTP (ONE TIME PASSWORD)



VERIFY & PASS LIVE FACE DETECTION FEATURE



AFTER BEING VERIFED SUCESSFULLY YOU WILL BE REDIRECTED TO HOMEPAGE

< Set up Profile



Add a profile photo*

It is mandatory as it will be used for facial recognition to find your photos from groups

Cannot be skipped and is necessary to complete in order to move forward

< Set up Profile



Add a profile photo
It is mandatory as it will be used for facial
recognition to find your photos from groups

First Name
John

Last Name
Doe



Allow Kwipic to take pictures and record
video?

WHILE USING THE APP

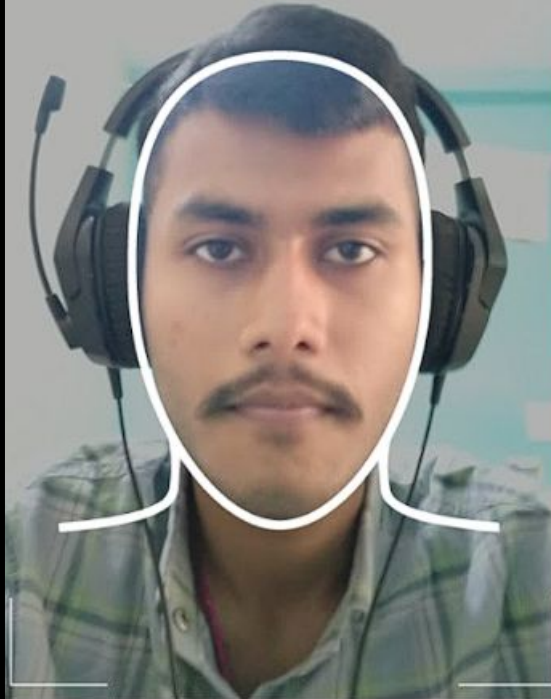
ONLY THIS TIME

DON'T ALLOW

Continue

< Take a Selfie

Fit your face exactly within the border



Click

You can only re-upload your own selfie.
OR, go to settings to add new profiles.

[*Click here to read Selfie Instructions](#)

< Take a Selfie

Fit your face exactly within the border

Instructions for taking Selfie ✖



- 1 Fit your entire face. Do not crop facial features.
- 2 Your eyes, nose and chin should be clearly visible.
- 3 No Mask & Specs.
- 4 Only 1 face per profile. Go to settings to add more profiles.

Click

You can only re-upload your own selfie.
OR, go to settings to add new profiles.

[*Click here to read Selfie Instructions](#)

Face **Detection** **Criteria** Being Used:



I'm not a robot



reCAPTCHA

[Privacy](#) - [Terms](#)

1. The face should be of a human.

2. The human face should be looking straight.

Something **seems odd** in here ?

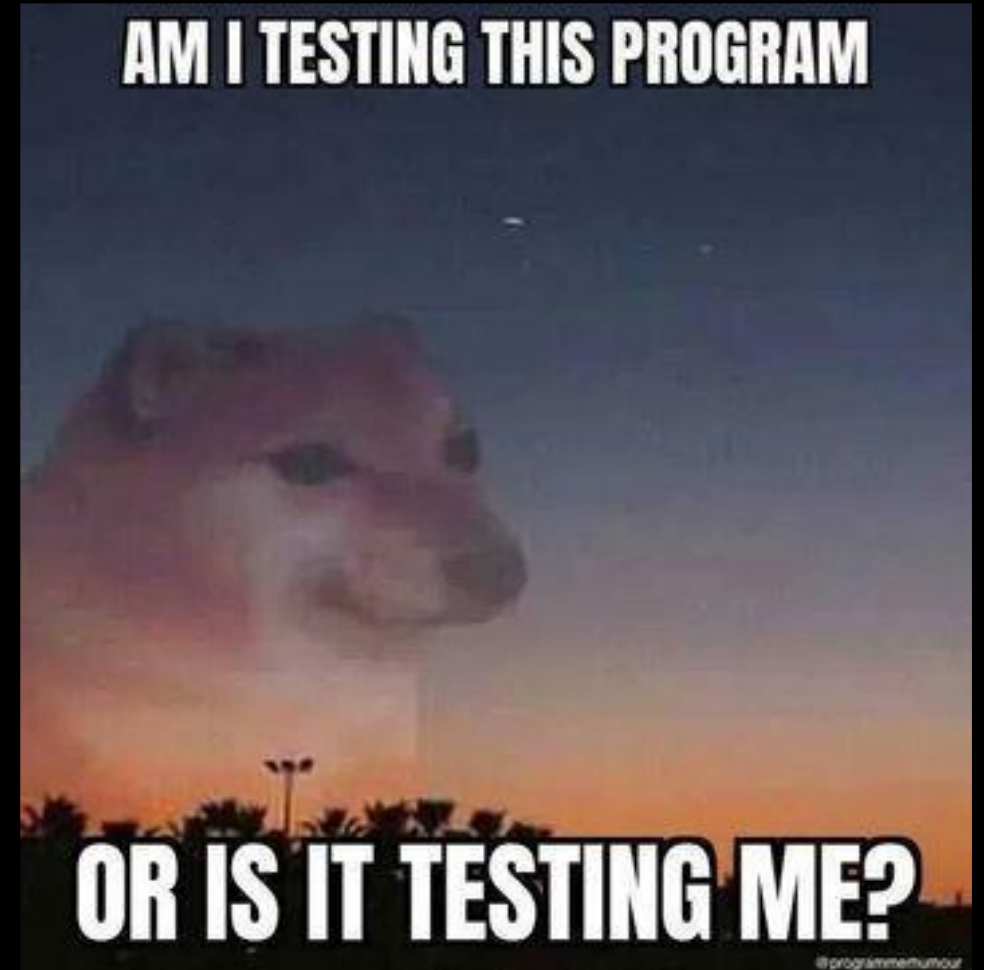


Yes, it is flawed but what it is ? 😊



- 1. A.I. fails to detect the difference between a real live detected human face and another deepfake.**
- 2. Fulfilling the above two conditions anyone can simply import the picture and verify his/her identity and bypass this crucial step of security.**

Testing Various **Bypass** Methods



- Conducted a test with a physical photograph, it got blur and ended up **being detected & rejected**.
- Used a deepfake Image from the Intended feature (Imported from gallery) and it **bypassed the check**



Google

First Name

Last Name

Email
juanitabrown@gmail.com ✓

+91 Phone

Verify your details

☐ I agree with the Terms and Conditions and Privacy Policy

Verified!

Continue



The deepfake Image I used to bypass the security check and got successfully verified as the user

< Set up Profile



Add a profile photo*
It is mandatory as it will be used for facial
recognition to find your photos from groups

First Name
John

Last Name
Doe

E-mail
juanitabrown@livinitlarge.net ✓

+91 Phone ⓘ

ⓘ Verify your details later to use them for login

☒ I agree with the [Terms and Conditions](#) and [Privacy Policy](#)

Continue



First Name

Last Name

E-mail
juanitabrown@livinitlarge.net ✓

+91 Phone ⓘ

ⓘ Verify your details later to use them for login

☐ I agree with the [Terms and Conditions](#) and [Privacy Policy](#)

Verified!

Continue

< Set up Profile



Verified!

First Name
John

Last Name
Doe

E-mail
juanitabrown@livinitlarge.net ✓

+91 Phone ⓘ

ⓘ Verify your details later to use them for login

☒ I agree with the [Terms and Conditions](#) and [Privacy Policy](#)

Continue

WRITE UP FOR THE VULNERABILITY DISCUSSED



ANY QUESTIONS ?

REACH ME OUT AT TWITTER - @RAVENZBB

