
rial.

Authenticating visual content with multi-sensor data¹

Daphne Estrada Ulises Montenegro Tobias Becerra
daphne.estrada1@gmail.com ulinicolasmonte@gmail.com tobias.bec1704@gmail.com
com om

Luca de Leo Guido Freire
luca@baish.com.ar freireguido@outlook.com

With
Apart Research

Abstract

The fidelity and realism of synthetic images generated by Generative Artificial Intelligence have increased significantly in the last year, making it progressively more difficult to differentiate them from real images. The impact of this problem is massive, affecting from national security to civil instability to mental health issues.

In a world where AI generated content will become the norm, we introduce **rial.**, a platform that allows users and enterprises to create and verify authentic images.

Keywords: Image generation, Deepfake, Content Authoring, Watermarking, Information Security.

¹ Research conducted at the [hackathon name with link], 2025

1. Introduction

Advances in Generative Artificial Intelligence have made it increasingly difficult to distinguish synthetic images from those captured in the real world. As models improve, their resolution, coherence, and fidelity become closer to reality. Frontier models already produce photorealistic content that is virtually indistinguishable from reality (1.1).

These advances translate in a change of paradigm where trusting images that are shared online to be real is no longer the default. As the burden of proof of visual evidence scales, the demand for a platform that facilitates access to this information increases. Without the capability to differentiate reality from synthetic images, disinformation campaigns become more efficient in creating civil unrest through information manipulation, creating false evidence to use in court, and defrauding companies and public institutions. The risks of letting this information run free are catastrophic, and could level civilization.

On the other hand, the availability and diversity of sensor data that devices like smartphones can produce is continuously growing. Major manufacturers like Apple and Samsung have incorporated LiDAR and hardware attestation in their flagship devices, and the cost of this technology continues to decline, making them more available.

We propose **rial**. - a platform that allows users to capture authentic images backed by multi-step verification proofs. Images that are created through our app must complete several steps to aid in collecting sensor data. Users can also easily check if any image is authenticated by uploading it to the platform.

2. Methods

rial. works like a license for real images. Methods to identify whether an image is real based on algorithmic detection of the raw pixels of an image, are inevitably conditioned on the quality of image generation. In **rial**. we guarantee that the images taken with our app are real, by using LiDAR technology to measure an image’s profundity. If the picture is being taken to a screen (that could have an AI-generated image) the app will not verify it as ‘real’. Once the image is taken, the user can export the image and whare it with a unique hash generated by the app. After this, anyone can verify that the image was taken by **rial**. by uploading an image that is in our database or manually inserting the hash.

We use

1. Hardware Attestation: establish device trust.

The capture session begins with a hardware-level attestation handshake with the device. This prevents device spoofing (e.g. emulators).

2. Multi-sensor Fusion: confirm camera–scene consistency.

During capture, LiDAR, IMU and GPS streams are collected and synchronized with the camera feed to ensure the device’s physical location, orientation, and depth-perception match the scene.

- 3. Translating the image hash to a UUID** Users are able to upload any image to our platform to find whether it has been verified by rial. and share it together with a UUID generated in our platform.

Since most platforms perform some sort of compression, we use a similarity-preserving hash to run the search. **rial.** then shows the full image, the sensor data that has been collected on upload, and the original person that uploaded it, as well as our authentication certificate.

3. Results

We have developed the technology to guarantee that a picture that is being taken with **rial.** is not ai-generated, but a real picture being captured by a camera. Nevertheless, there is still a lot of work to be done, in order to integrate all of the steps for the application to be completely user-friendly.

We have effectively:

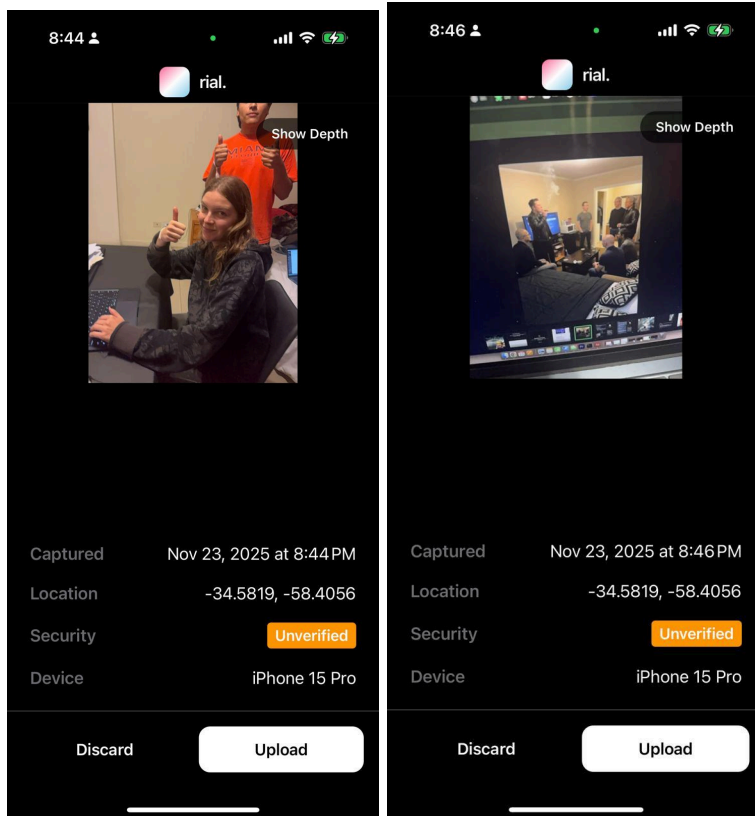
- Developed a user friendly application that has access to a phone camera and uses the built-in LiDAR technology.
- Created a web app that can access the application's images storage and compare the uploaded image's hash with the ones stored in our database.
- Habilitated a system to easily share a link associated with the photo taken within the app.
- Downloaded the application on an iPhone 15 PRO and tested its usage
- Developed a [Verification Webpage](#).

Visual demonstration of usage:

[Link to video](#)

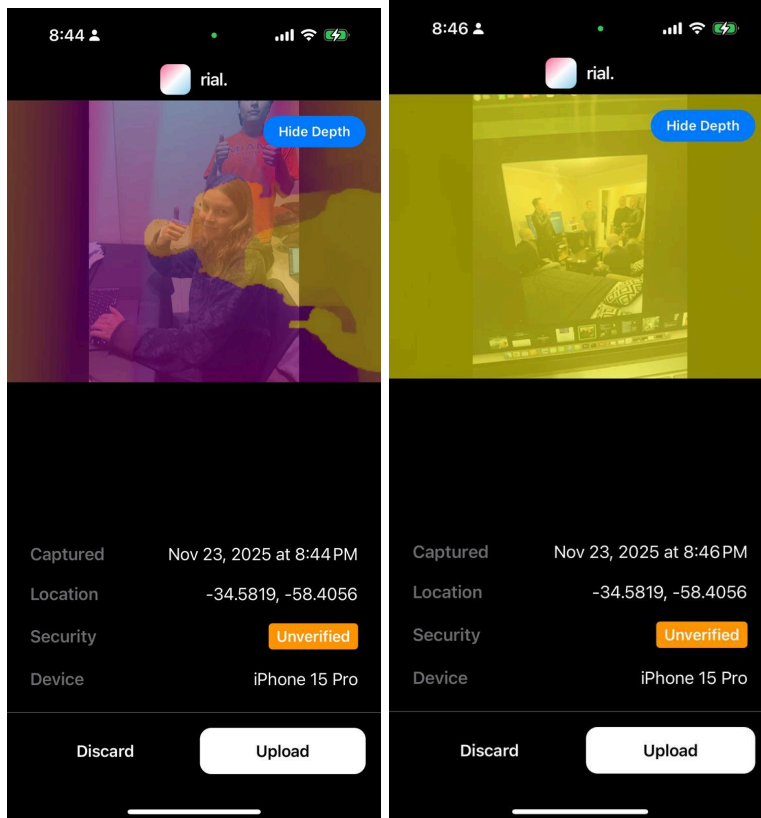
Step by step of taking a picture:

1. Open the app and take an image.



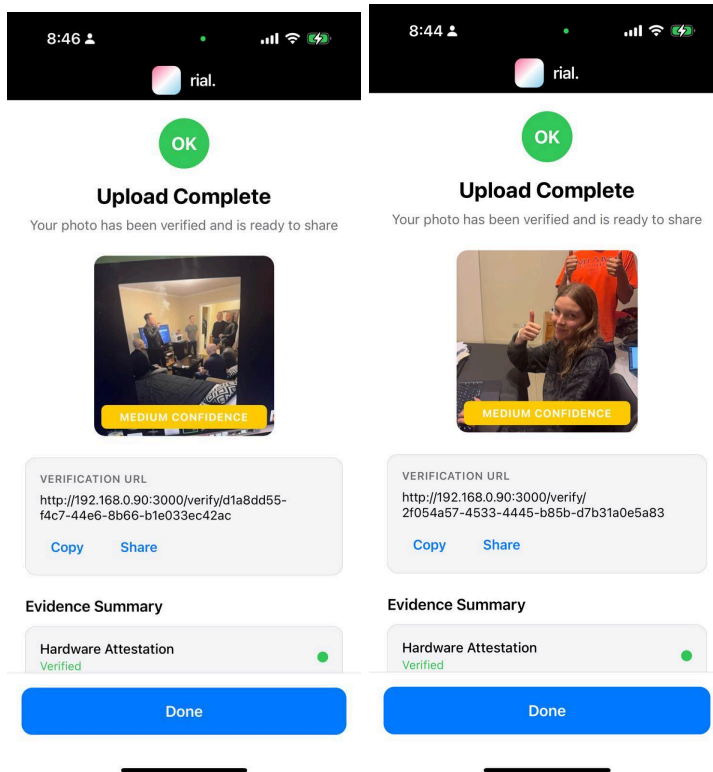
We took a picture of a person (left) and a picture of an image displayed in the computer (right)

2. Profundity is measured with LiDAR sensors.



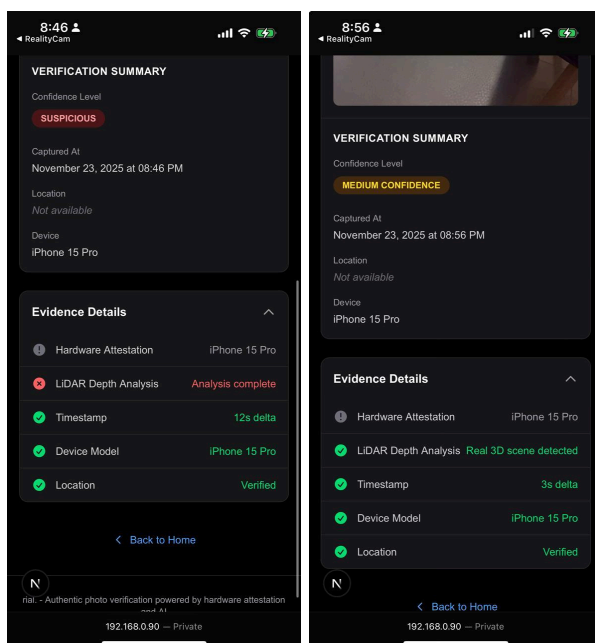
The real picture has different layers of profundity, while the picture of the screen has the same profundity throughout the picture. We also see the exact coordinates and time in which the picture was taken, the camera with which it was taken (the iPhone model). For the time being, we in order to obtain this last verification that the image was taken with an iPhone, we need approval from Apple, which takes more time than we had for this hackathon.

3. Uploading image



After taking the image, it can be shared with a unique url, with an incorporated UUID.

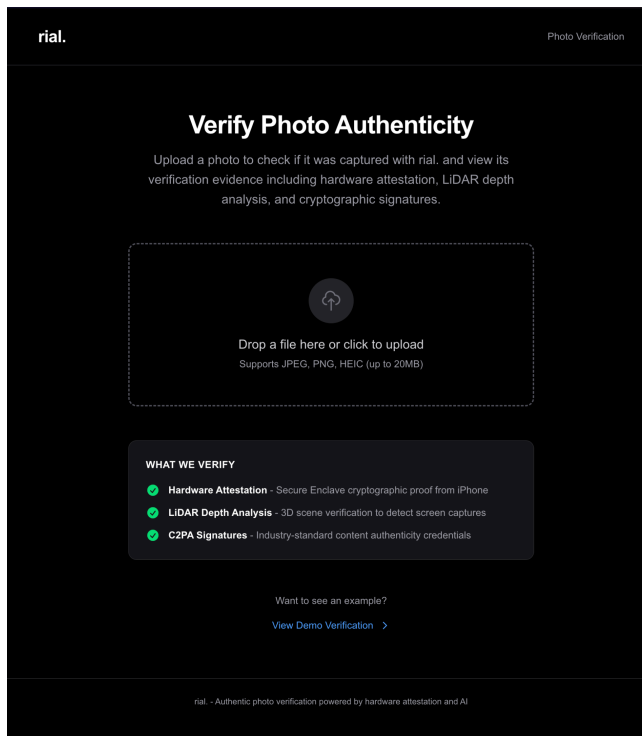
4. The link has the information of the authentication:

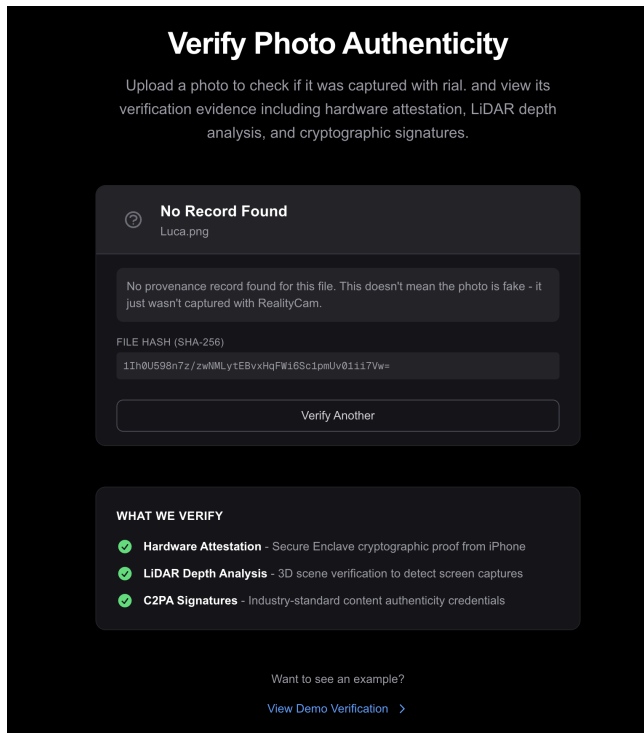


The real image shows a ‘Medium Confidence’ because we are still missing the hardware attestation. The fake image shows ‘Suspicious’.

Step by step of verifying an image is taken with rial.:

1. Access the web application through the app (Screenshot)
2. Upload image
3. Show results.





As the uploaded image isn't in our record, the app cannot verify its authenticity.

4. Discussion and Conclusion

During the Apart hackathon, we were able to develop the technology to verify that an image is being taken in real time, and not generated with AI technology. After taking a picture, the application can certify the time and place where it was taken, with which device, and generate a unique hash that can be effectively exported together with the image. Furthermore, we developed a web application in which one can upload an image and verify that it is in the **rial.** database.

There is still a lot of work to be done in order to make the app commercially viable. The next steps would be to solve the hardware attestation (we need approval from Apple), generate a smoother export experience, and test the technology in complex scenarios in order to fine-tune the profundity detection. Furthermore, we would like to test the application for moving images.

We believe the cases of use are infinite, since the problem of fake images affects journalism, national security and even mental health. To have a way to verify that images are real has become an urgent matter. Until now, solutions to this problem promise to identify if an image is being generated by AI (1.3), but as we know that AI will exponentially get better in generating realistic images, we don't believe this is a scalable solution, therefore we propose a platform to guarantee that an image is real.

As a conclusion to our project, we believe **rial.** has the potential to be used worldwide to secure the authenticity of images, solving a problem that has not yet

been addressed with the adequate urgency, its usage and its impact crosses industries and frontiers.

5. References

1.1 Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence* [Report]. Data & Society.
https://datasociety.net/wp-content/uploads/2019/09/DataSociety_Deepfakes_Cheap_Fakes.pdf

1.2 West, D. M. (2024). *How artificial intelligence and disinformation impact elections* [Policy analysis]. Brookings Institution.
<https://www.brookings.edu/articles/how-do-artificial-intelligence-and-disinformation-on-impact-elections/>

1.3 Goyal, S., Bunel, R., & Stimberg, F. (2025, October 10). *SynthID-Image: Image watermarking at internet scale* [arXiv preprint]. arXiv.
<https://doi.org/10.48550/arXiv.2510.09263>

6. Appendix

Security Considerations

rial. works if it is 100% reliable, if its database was hacked, it would be extremely dangerous to have fake images circulating as if they were verified by **rial**. This is

why it is extremely important to work on the app's cybersecurity. A possible solution to this problem is to have a decentralized crypto database.

[Verification Webpage](#)

Github Code

<https://github.com/LucaDeLeo/realitycam>

<https://github.com/ulimonte05/v0-rial-landing-page>