Rolling Colors: Adversarial Laser Exploits against Traffic Light Recognition

Chen Yan¹, Zhijian Xu¹,², Zhanyuan Yin³, Xiaoyu Ji¹, Wenyuan Xu¹

¹Zhejiang University, ²The Chinese University of Hong Kong, ³The University of Chicago
Traffic Light Recognition

• Enables vehicles to detect and recognize traffic light signals
• Essential for full autonomous driving in urban areas
How does traffic light recognition work?

1. **Image**
2. **Region of interest**
3. **Light color**

- **Front view**
- **Camera**
- **Traffic light detection**
- **Traffic light recognition**

**Green Light**
What if traffic light recognition goes wrong?

- Green Light → Run a red light → Intersection Accident!
- Red Light → Sudden stop → Rear-end Crash!
Spoof traffic light recognition?

• Use fake traffic lights? ... Probably not the best idea.
Let’s use laser!

- Narrow beam of radiation → *Travel a long distance, hard to detect*
- Previous studies have shown laser’s capability on interfering cameras

Petit et al., Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR (Blackhat 2015)
Yan et al., Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles (DEFCON 2016)
Attack Scenario and Requirements

**Requirement ①**
The laser interference affects the image as little as possible

**Requirement ②**
The traffic light can be detected under laser interference

**Requirement ③**
The traffic light is recognized as being in a targeted color

1. Real scene
2. Laser diode
3. Camera
4. Traffic light detection
5. Traffic light recognition
6. Red Light
R1: Laser Interference Study

Real scene

Laser diode

Camera

Affect the entire image → Can be easily detected

Overexposure

Color shift

White unbalance

Color stripe

Only affect the traffic light region → Stealthier attack
A rolling shutter is a type of image capture in cameras that records the frame line by line on an image sensor instead of capturing the entire frame all at once.
R1: Exploiting the Rolling Shutter

- A rolling shutter is a type of image capture in cameras that **records the frame line by line on an image sensor** instead of capturing the entire frame all at once.

Video source: SmarterEveryDay  https://www.youtube.com/watch?v=dNVtMmLInoE&t=348s
R1: Exploiting the Rolling Shutter

- Inject a color stripe into the captured image with a laser pulse signal
- Full control over the stripe's number, width, and position
- Synchronize the laser pulse with the rolling shutter period (frame rate)
R2: Passing Traffic Light Detection

The injected color stripe must **NOT** affect traffic light detection

- **Requisite 1:** proper control of laser intensity
- **Requisite 2:** proper design of the stripe’s width and position

The accuracy of traffic light detection is barely affected by the color stripe if it covers the entire traffic light.
R3: Spoofing Traffic Light Recognition

Spoof traffic light detection to a targeted color (Red $\rightarrow$ Green, Green $\rightarrow$ Red)

- **Requisite:** fine-tune the laser parameters according to specific traffic lights and attack scenarios

The attack result is affected by the laser’s power, incidence angle, the traffic light itself, and even the image background.
Threat Model & Attack Workflow

Green light
Pre-recorded image → Attack Simulation

Red light
Simulated image → Laser parameters

Laser
Real scene → Camera

Captured image → Traffic light recognition → Red Light
Attack Design

**Input**

- Pre-recorded image

**Attack Building Blocks**

- **Attack Modeling**
  - Camera Modeling
    - Direct Interpolation
    - Bilinear Interpolation
  - Laser Interference Modeling
    - Photon Filtering
    - Color Strip Addition
  - Laser Effect Emulation
    - Incidence Direction
    - Lens’ Imperfectness

- **Parameter Search**
  - Wavelength
  - Minimum Strength
  - Maximum Strength
  - Incidence Direction
  - Incidence Function

- **Laser Generation**
  - Wavelength
  - Power
  - Pulse Width
  - Pulse Period
  - Incidence Angle

**Output**

- Laser

**Steps**

- Simulate laser interference
- Find effective parameters
- Map parameters to laser signals
Evaluation

• Emulated Attacks
• Real-World Attacks in Stationary Setups
• Real-World Attacks in Motion

5 Cameras

AR0132AT Eva. board
Hikvision Dashcam
Xiaomi Dashcam
OPPO K3 Smartphone
OpenMV H7

2 Models

apollo

nexar

Used on Tesla vehicles
Real-World Attacks in Stationary Setups

- **Experiment Setup**

- **Overall Performance**
  - Red $\rightarrow$ Green
  - Green $\rightarrow$ Red

- **Impact of the Traffic Light**
  - Distances: 5m - 25m
  - 5 Positions: [L, ML, M, MR, R]
  - 3 Directions: [L, M, R]

(a) Illustration of setup
(b) Real setup
Real-World Attacks in Stationary Setups

• Overall Performance

Table 2: Success rates of attacking 2 systems and 5 cameras.

| Sys. | Attack Scenario | Target Camera | Red to Green: | Green to Red: |
|------|----------------|---------------|---------------|---------------|
|      |                | Tesla | Xiaomi | Hikv | OPPO | OpMV | Avg. |               |
| Apollo | R→G          | 7.39% | 20.27% |       |      |      | 20.53%        |
|       | R→DoS         | 2.64% | 32.74% |       |      |      |      |               |
|       | G→R           | 7.37% | 41.86% |       |      |      |      |               |
|       | G→DoS         | 2.63% | 36.46% |       |      |      |      |               |
| Nexar  | R→G           | 0%    | 20.78% |       |      |      |      |               |
|       | R→DoS         | 100%  | 48.04% |       |      |      |      |               |
|       | G→R           | 100%  | 65.94% |       |      |      |      |               |
|       | G→DoS         | 0%    | 32.72% |       |      |      |      |               |

Green→Red is easier than Red→Green

Tesla camera is the most vulnerable
Real-World Attacks in Stationary Setups

• Impacts of the traffic light’s distance, position and direction.

Successful attack when the traffic light is 25 m away from the camera

Distance $\uparrow$  
Attack success rate $\downarrow$

Higher success when the traffic light is in the middle of the image

(a) No. of successful R→G at various locations
(b) Results of R→G attack at various distances
(c) Results of R→G attack at various positions
Real-World Attacks in Motion

• Effectiveness across Continuous Video Frames
• Feasibility of Tracking and Laser Aiming
• End-to-End Impact on Driving
The attack can continuously spoof traffic light recognition for more than 1 second with a success rate of 85.2%.
Feasibility of Tracking and Laser Aiming

Manual tracking and aiming equipment

Setup for long-range laser aiming experiment
(the attacker was on the roadside and 40-80 m away from the vehicle)
Feasibility of Tracking and Laser Aiming

1. Attacker can track the target camera and aim the laser at the same time even when the vehicle is moving at 20 km/h.
2. The average attack success rate of spoofing traffic light recognition is 28.4%.
End-to-End Impact on Driving

Attack Scenario 1:
Running a red light

Attack Scenario 2:
Emergency stop
Countermeasures

• Use global shutters instead of rolling shutters

• Rolling shutter improvement: expose the CMOS rows in a random sequence
Summary

• A new approach to injecting adversarial images by exploiting an inherent vulnerability of the rolling shutters in CMOS cameras

• Experimentally validated the feasibility of fooling traffic light recognition using laser

• Evaluated the attack in real-world setups on 2 traffic light recognition systems, 5 cameras, and a moving vehicle
Questions?

Attack demos: https://sites.google.com/view/rollingcolors

USSLAB homepage: http://usslab.org