TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)

CamEye

AI-Powered Counter-Surveillance Detection for Government, Defense & Enterprise Security

Find hidden cameras, Bluetooth tracking tags and camera-equipped smart glasses — including offline devices that never transmit a signal.



CamEye-M1
Wi-Fi-only camera detection by AI traffic-pattern analysis

CamEye-M2
All M1 Wi-Fi functions plus Bluetooth camera & tag detection

CamEye-RF
Electromagnetic-emission camera detection plus smart-glasses detection

The Covert Surveillance Threat Has Changed

Small, cheap, disguised — and often silent on a conventional sweep

Government agencies, defense organizations and corporate security teams now face surveillance devices bought online for a few dollars. They stream over Wi-Fi, hide behind Bluetooth, record silently to memory cards, or arrive in the room on a visitor's face. Each type needs a different way to find it.

Four device classes security teams must find

Wi-Fi Streaming Cameras

CamEye-M1 · M2 · RF

HOW THEY ARE USED

- Hidden in chargers, clocks, smoke detectors and décor
- Stream live video and audio to a remote operator

WHY THEY ARE HARD TO FIND

- Wi-Fi spaces are crowded with phones, laptops and access points — signal strength alone cannot show which device is a camera

Bluetooth Cameras & Tracking Tags

CamEye-M2

HOW THEY ARE USED

- AirTag-class tags and BLE devices planted in vehicles, bags or gifts
- Track the movements of officials and the location of assets

WHY THEY ARE HARD TO FIND

- Low-power, intermittent signals that look like ordinary consumer Bluetooth

Offline Storage Cameras

CamEye-RF

HOW THEY ARE USED

- Record to an SD card and are collected later — no network needed
- Also includes wired cameras and cameras with radios switched off

WHY THEY ARE HARD TO FIND

- They transmit nothing, so Wi-Fi, Bluetooth and RF transmitter scans cannot see them

Camera-Equipped Smart Glasses

CamEye-RF

HOW THEY ARE USED

- Worn openly by insiders or visitors in meetings and secure areas
- Capture people, screens and documents without drawing attention

WHY THEY ARE HARD TO FIND

- They look like ordinary eyewear and pass visual inspection

Where conventional sweep tools fall short

RF field-strength detectors

React to any transmitter — phones, access points, IoT — without identifying which one is a camera. Devices that do not transmit are missed.

Optical lens finders

Need line of sight and slow manual scanning; difficult in large or cluttered spaces, and blind to worn devices outside the scan path.

Manual inspection

Results depend on the operator's skill and leave no objective, auditable record of what was checked.

CamEye's approach: identify the device by **what it does** — the traffic pattern of video streaming, the signature of Bluetooth tags, the electromagnetic emissions of an active camera circuit — and record every sweep in a report.

Complementary Detection Methods

Choose a detector to match the threat and operating conditions.

LAYER 1 / M1 + M2	**Wi-Fi traffic-pattern AI** Streaming Wi-Fi cameras
LAYER 2 / M2	**Bluetooth (BLE) signal analysis** Smart glasses, tags and classified Bluetooth devices
LAYER 3 / RF	**Electromagnetic-emission AI** Active camera circuits, including offline cameras
SMART GLASSES / S	**Bluetooth / Wi-Fi data and activity** Connected glasses; tracking during data activity

Product lineup



Wi-Fi only

CamEye-M1

Portable Wi-Fi camera detection using AI traffic patterns and signal-strength tracking.



Wi-Fi + Bluetooth

CamEye-M2

Wi-Fi AP classification; smart glasses, tags and Bluetooth categories; signal tracking.



Electromagnetic

CamEye-RF

Detects active camera circuits: wired, wireless or SD-card cameras and camera-equipped glasses.



Smart-glasses detection

CamEye-S

Bluetooth / Wi-Fi data and activity analysis; connected-glasses detection and location tracking.

Threat coverage

Threat	M1	M2	RF	S
Wi-Fi streaming cameras	**Yes**	**Yes**	**Yes**	**Patterns***
Bluetooth-enabled cameras	-	**Yes**	**Yes**	-
Tracking tags	-	**Yes**	-	-
Phones concealed in vehicles / belongings	-	**Yes**	-	-
Offline cameras recording to SD cards	-	-	**Yes**	**Patterns***
Wired cameras	-	-	**Yes**	-
Camera-equipped smart glasses	-	**Activity***	**Yes**	**Activity***

* M2 / S: smart-glasses data and activity analysis; tracking requires data activity. S also supports miniature / storage-camera signal patterns. A dash for S means not specified. Added M2 capabilities and S specifications are development targets; results depend on device and site conditions.

96.65%
Wi-Fi camera detection accuracy

0.35%
False-positive rate, non-camera devices

4
Registered Korean patents

500+
Public sites in Korea since 2019

96.65% / 0.35%: ETRI Wi-Fi traffic-analysis results, not RF or S performance figures.

CamEye-M1

PRODUCT / WI-FI ONLY

Portable Wi-Fi Camera Detector (Wi-Fi Only) — AI Traffic-Pattern Analysis



- Wi-Fi-only, tablet-style portable detector for on-demand counter-surveillance sweeps
- Identifies Wi-Fi cameras by the distinctive data-flow pattern that video streaming creates — **not** by MAC address or vendor lists
- Tells cameras apart from smartphones, laptops and other devices
- Excludes registered (authorized) IP cameras to keep results clean
- Pinpoints the hiding place by signal-strength (RSSI) tracking
- Shows results on screen and generates a detection report for each site — no monitoring server required

How it works

1 Collect
Gathers wireless traffic from devices around the operator, per device.

2 Analyze
AI evaluates each device's traffic flow for the pattern of video transmission.

3 Classify
Separates cameras from phones, laptops and IoT; skips authorized cameras.

4 Locate & Report
Follows signal strength to the device and records the result in a site report.

Why it matters to security agencies

- **No dependence on MAC/OUI lists** — detection is based on behavior, so cameras from unknown makers or with randomized addresses are still identified
- **Content-blind** — analyzes traffic patterns only; video content is never collected or decoded
- **Standalone** — works on site without a server or central system
- **Objective record** — an auto-generated report documents every sweep

Typical missions

- Pre-meeting sweeps of conference and briefing rooms
- Hotel rooms and residences during official travel
- Offices of senior officials and executives
- Incident response when a leak or recording is suspected

96.65% Detection accuracy
0.35% False-positive rate

ETRI accredited test, report ETRI-2021-3000-113

Specifications (CamEye-M platform)

Form factor	Tablet-style portable detector with touchscreen user interface
Dimensions	265 × 196 × 20 mm (body diagonal approx. 13 in)
Weight	650 g
Power	Built-in rechargeable battery Charging: 220 V AC / 15 V DC, 1.6 A
Detection	AI wireless traffic-pattern analysis · RSSI tracking · authorized-camera exclusion
Output	On-screen results · per-site detection reports


Carry bag


Detector unit


Wireless LAN adapter


Charging adapter

CamEye-M2

Wi-Fi + Bluetooth detection, classification and on-site tracking



- Retains M1 Wi-Fi camera detection, authorized-camera exclusion and site reports.
- Adds smart-glasses / miniature-camera analysis, AP context and Bluetooth device categories.
- Track suspicious devices by signal strength while data activity occurs.

From a device list to an actionable inspection

1 Detect

Analyze Wi-Fi traffic patterns and Bluetooth data / activity events.

2 Classify

Separate authorized / unrecognized APs and prioritize device categories.

3 Track

Follow live signal-strength graphs and proximity indications.

4 Record

Keep detection times, AP, evidence and location in inspection records.

Established functions, broader operating scenarios

- Camera / tag inspections: Wi-Fi cameras, BLE cameras, tracking tags and concealed phones.
- Exam halls, meeting rooms and R&D labs: identify smart glasses and miniature cameras, including phone-hotspot connections.
- VIP travel and vehicle sweeps: check luggage, gifts and vehicles for suspicious Bluetooth devices.
- Standalone results, PDF detection reports and OTA remote updates remain available.

Specifications & equipment

265 × 196 × 20 mm · 650 g · tablet-style touchscreen
Built-in battery: up to 4 hours · Charging: 220 V AC / 15 V DC, 1.6 A
Carry bag · detector unit · wireless adapter · charging adapter

Added capabilities and battery-runtime specifications are development/design targets; confirm final supply specifications. Detection and tracking depend on device activity and site conditions.

CamEye-M2 | Detect, Classify & Track

Extend Wi-Fi and tag detection with connection context and device categories.

1 Detect Wi-Fi / BLE activity → **2 Classify** AP / device type → **3 Track** signal strength

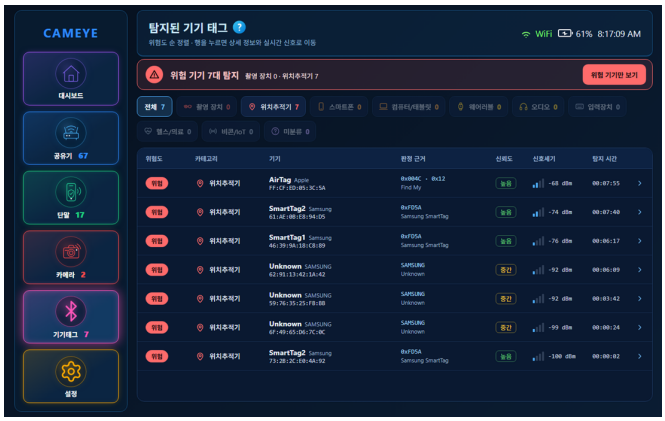
01 Wi-Fi | Separate authorized and unrecognized APs



- Group traffic-generating Wi-Fi devices by their connected access point (AP).
- Register authorized APs to highlight unrecognized networks and devices connected directly to phone hotspots.
- Use video-traffic patterns and activity events to assess miniature cameras; display detection type and rate.

02 Bluetooth | Prioritize devices by category

- Prioritize camera devices such as smart glasses, and tracking tags including AirTag and SmartTag.
- Separate audio, wearable and other devices to focus on suspicious targets.
- Review manufacturer, device type, signal strength, detection time and assessment evidence.



03 Track suspicious devices while data activity occurs





Select a target, follow its live signal graph and move toward stronger readings. Record detection times, AP and evidence; register authorized devices for later inspections.

Added capabilities/specifications are development targets; confirm final supply details. Screens show actual CamEye-M2-based operation.

CamEye-RF

Electromagnetic Camera Detector with Smart-Glasses Detection



Finds every camera — wired, wireless or offline — and camera-equipped smart glasses.

- **Electromagnetic camera detection** — AI analysis of the electromagnetic emissions radiated by camera circuits
- Works whether or not the device transmits — detects Wi-Fi cameras and cameras that only record to SD cards
- **Smart-glasses detection** — finds camera-equipped smart glasses
- Weak-signal amplification and noise suppression for cluttered RF environments
- Detection results and history on screen

How it works — detecting the camera itself, not its radio

Active camera circuit

Sensor · ISP · Memory

Wi-Fi, SD card, wired or smart glasses

EM emissions

CamEye-RF

Receive weak signals

Amplify & suppress noise

AI pattern analysis

Detection

Camera present

On-screen alert

Stored in history

Every digital camera — whether it streams, records locally or is wired — drives an image sensor, processor and memory while it captures. CamEye-RF analyzes the unintentional signals those circuits radiate, so detection does not depend on the device sending data.

Enterprise security

- Boardrooms and executive offices
- R&D labs and IP protection
- Negotiation and M&A rooms

Government agencies

- Briefing and cabinet rooms
- Diplomatic and negotiation venues
- Entry screening for smart glasses

Defense

- Secure facilities and command sites
- Defense R&D and test areas
- Checkpoints for recording devices

What electromagnetic detection adds to a wireless sweep

Device	Wi-Fi / Bluetooth (M1 · M2)	CamEye-RF
Wi-Fi or Bluetooth camera	Seen while it transmits	**Detected**
Camera recording only to an SD card	Not visible — no transmission	**Detected**
Wired camera / camera with radio disabled	Not visible	**Detected**
Camera-equipped smart glasses	M2: smart-glasses data / activity analysis	**Detected**

Smart glasses: the insider threat in plain sight.
Camera-equipped glasses look like ordinary eyewear and can capture meetings, screens and documents. CamEye-RF detects them by the camera circuitry they carry, supporting both entry screening and in-room checks.

Display	10-inch IPS, 1280 × 800
Power	10,000–15,000 mAh battery · USB-C PD 45 W
Ports	Ethernet · USB · tripod mount

Specifications are design targets and subject to final confirmation.

CamEye-S | Smart-glasses Detector

Bluetooth / Wi-Fi data and activity-event analysis

Product overview

- Portable detection of smart glasses through Bluetooth / Wi-Fi data and activity events.
- Detects connected glasses even after advertising stops; tracks their location when data activity occurs.
- Built-in rechargeable battery supports up to 4 hours of portable operation.

Why CamEye-S?

Threat	Smart glasses can look like ordinary eyewear. Subtle recording indicators make covert filming and live transmission possible in meetings, exam rooms and exhibitions.
Detection gap	RF-emission and lens-reflection methods depend on their respective signal and visibility conditions. Conventional scanners may miss connected glasses that have stopped advertising.
CamEye-S	Analyzes Bluetooth / Wi-Fi data and activity events exchanged with a phone. Detects connected glasses and uses signal-strength tracking to locate them when data is generated.

Typical applications

- Corporate secure areas, meeting rooms and R&D labs
- Exam rooms, assessment centers and interviews
- Exhibitions and new-product launches
- Public agencies and security inspections

Why it is needed

- Rapid growth of camera-equipped smart glasses
- Gaps in detection of connected glasses
- On-site location tracking beyond detection alone

Product appearance



CamEye-S

Specifications

Body / display	CamEye-RF chassis; 10-inch IPS touchscreen (1280 x 800)
Power	Built-in battery; up to 4 hours; USB-C charging
Detection range	Around 10 m; varies with site and antenna conditions
Interfaces	10-inch touchscreen; Ethernet; USB
Software	Bluetooth / Wi-Fi data and activity-event analysis; location tracking; logs

Development specifications and performance are subject to final confirmation. Detection and tracking depend on device activity and site conditions.

CamEye-S | Detection & Tracking

Detect activity. Follow the signal. Locate the device.

1 Detect BLE / Wi-Fi activity → **2 Track** signal strength → **3 Compare** movement trends

Detection methods

Bluetooth-based

- Analyze advertising fingerprints of smart glasses
- Capture and follow connected devices
- Assess connection activity, traffic spikes and uplink patterns

Wi-Fi & activity events

- Collect Wi-Fi group and transmission events
- Correlate timing and signal strength with Bluetooth connections
- Recognize events associated with photo transfers or live streaming

Track location when data activity occurs



Actual tracking screen - Live BLE / Wi-Fi signal-strength graphs help the operator move toward the selected glasses.

Correlated signal changes suggest the same wearer/device group (Moving together). Proximity, distance and peak indications support tracking.

Key capabilities

Activity-based detection - Distinguishes events such as standby, normal use and transmission.

Miniature-camera detection - Supports signal-pattern detection of Wi-Fi and storage cameras.

Location tracking - Uses signal strength to locate glasses while data is generated.

Portable operation - Up to 4 hours on the built-in battery for on-site inspections.

Layered Counter-Surveillance Sweep

Select complementary methods for the threat and the mission.

1 Prepare

Register authorized cameras, APs and devices.

2 Wi-Fi sweep

M1 / M2 detect traffic patterns; M2 checks AP connections.

3 BLE / activity

M2 classifies Bluetooth devices; M2 / S analyze smart-glasses activity.

4 EM sweep

RF checks active camera circuits, including offline cameras.

5 Locate

Follow signal strength; M2 / S tracking needs data activity.

6 Record

Save results, time, location and supporting evidence.

Operational scenarios

Meetings, exams & R&D labs

Use M2 to classify smart glasses and miniature cameras, including phone-hotspot connections. Add RF for offline recording devices.

VIP protection & official travel

M2 checks hotel Wi-Fi cameras and Bluetooth tags / concealed phones in vehicles, luggage and gifts. RF adds offline-camera checks.

Secure-facility entry

RF analyzes camera-circuit emissions. M2 and S use Bluetooth / Wi-Fi activity; track location while data activity occurs.

Periodic inspections

Apply consistent reports, review AP and device history, and register authorized equipment for later sweeps.

Designed for sensitive environments

- Content-blind detection: analyze traffic and signal patterns without collecting video content.
- Standalone operation: results are displayed on the detector, without an on-site monitoring server.
- Focused inspection: M2 AP registration and device categories help operators prioritize suspicious targets.
- Reviewable records: M1 / M2 site reports, RF results/history, and S tracking information/logs.

Performance depends on device and site conditions. New M2 capabilities and S specifications are development targets.

Proven Technology, Trusted in Korea

Patented, independently tested and deployed by public agencies

Registered patents (Republic of Korea)



Wireless IP Camera Detection System
KR 10-2204338



Wireless IP Camera Detection System and Method
KR 10-2204342



Hidden-Camera Safe-Zone Certification Using a Video Traffic Pattern Detector
KR 10-2423245



Automatic Collection of Mobile Device OUIs
KR 10-2521985

Testing, designation & recognition



ETRI accredited test

96.65% camera detection accuracy (116/120) and 0.35% false-positive rate (3/858).
ETRI-2021-3000-113



Innovative Product

Designated by Korea's Public Procurement Service (No. 2022-523), including CamEye-M.

Government award

2025 Minister of Science and ICT Award for outstanding national R&D achievement.

Track record in Korea

500+

public sites running CamEye systems since 2019

- Government Complex Management Headquarters, Sejong
- Korea Asset Management Corporation (KAMCO)
- Korea Expressway Corporation · Korea Electrical Safety Corporation
- Daejeon Metropolitan Council · local governments nationwide

Flagship deployment

Mapo-gu District, Seoul

181 units across 71 sites (2026), monitoring public restrooms across the district around the clock.

About NETvision Telecom

NETvision Telecom has developed wireless networking and AI technology since **2000**. Headquartered in Daejeon, Korea's science and technology hub, the company runs R&D centers in **Hanoi (2007)** and **Ho Chi Minh City (2011)**, Vietnam. CamEye is its AI-based detection line for hidden cameras and covert surveillance devices.

NETvision

NETvision Telecom Co., Ltd.
Suite 412, 199 Techno 2-ro, Yuseong-gu, Daejeon, Republic of Korea
T +82-42-931-4130 · F +82-42-931-4133
info@netvisiontel.com · www.netvisiontel.com

Patents, certifications and test results apply to the products and scope stated in the original documents. Test figures refer to CamEye's Wi-Fi traffic-analysis technology. CamEye-RF specifications are design targets.