GhostShot: Manipulating the Image of CCD Cameras with Electromagnetic Interference

Yanze Ren*, Qinhong Jiang*§, Chen Yan*†, Xiaoyu Ji*, and Wenyuan Xu*
*Zhejiang University, §The Hong Kong Polytechnic University
{yzren, qhjiang, yanchen, xji, wyxu}@zju.edu.cn

***Abstract*—CCD cameras are critical in professional and scientific applications where high-quality image data are required, and the reliability of the captured images forms the basis for trustworthy computer vision systems. Previous work shows the feasibility of using intentional electromagnetic interference (IEMI) to inject unnoticeable image changes into CCD cameras. In this work, we design an attack of enhanced capability, `GhostShot`, that can inject any grayscale or colored images into CCD cameras under normal light conditions with IEMI. We conduct a schematic analysis of the causality of the IEMI effect on the shapes, brightness, and colors of the injected images, and achieve effective control of the injected pattern through amplitude-phase modulation. We design an end-to-end attack workflow and successfully validate the attack on 15 commercial CCD cameras. We demonstrate the potential impact of `GhostShot` on medical diagnosis, fire detection, QR code scanning and object detection and find that the falsified images can successfully mislead computer vision systems and even human eyes.**

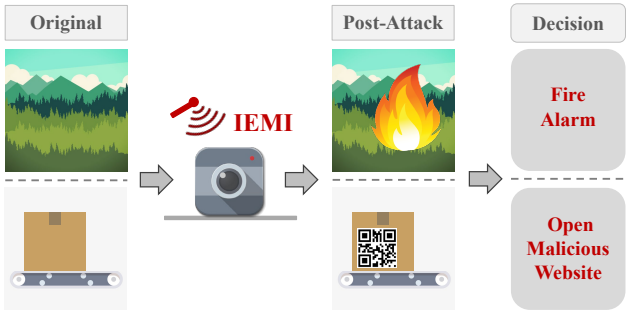


Fig. 1: Attackers can manipulate computer vision systems by injecting monochrome or color images, leading to erroneous decision-making.

I. Introduction

CCD (charge-coupled device) is the earliest type of semiconductor device used in digital cameras. Compared with CMOS (complementary metal-oxide semiconductor) sensors, CCD image sensors are a major digital imaging technology that outperforms CMOS by their excellent photometric performance, lower noise, and better low-light sensitivity [61]. Despite the prevalence of CMOS in the consumer market due to cost considerations, CCD image sensors are still widely used in professional and scientific applications where high-quality image data are required, including medical diagnostics [6], [19], [45], security surveillance [25], [8], industrial inspection [16], astronomical studies [47], etc., and their global market share is predicted to grow steadily and reach 20.5 billion dollars by 2030 [50]. As CCD cameras play a significant role across various industries, what is less well-understood is how reliably they behave under intentional attacks.

Previous work [26] has shown the feasibility of injecting signals into CCD image sensors using intentional electromagnetic interference (IEMI), which can cause unnoticeable changes in targeted pixels and disrupt barcode detection. Nonetheless, noticeable image perturbations could only be injected in a dark environment. Informed by earlier research, this paper aims to explore the further capabilities and limits of IEMI attacks on CCD cameras. Specifically, we wonder if it is feasible to ***inject arbitrary patterns into the image captured by a camera in any ambient light conditions***. For example, as illustrated in Fig. 1, can IEMI create a non-existing fire pattern or textured QR code in a camera's output? Moreover, is it possible for the falsified images to mislead computer vision systems or even human eyes?

The ability to inject arbitrary image patterns can serve as a foundation enabling various creative adversarial scenarios. Yet achieving such an attack, if feasible, is highly challenging as it requires the injected image pattern to be as realistic as possible in every aspect, including morphology, brightness, and coloration. Otherwise, the counterfeit image may have a limited adversarial impact and can be easily identified. An ideal attack is required to achieve the following primary capabilities. (a) *Morphology Control:* to create an accurate pattern, the attacker should be able to inject arbitrary shapes in desired image positions and avoid any image discontinuity caused by unwanted noise. Although it has been proved that IEMI can change the pixel values, the injected shapes still have rough edges and are filled with noises, leading to a low shape resolution and making the pattern less recognizable. (b) *Brightness Control:* the injected pattern needs to be recognizable under various light conditions, which requires noticeably increasing or decreasing the value of the original pixel in dark and bright image backgrounds. In most cases, the injected pattern will also contain a variety of grey scales, e.g., a QR code is made of black and white pixels, demanding precise control of brightness over different areas of the injected pattern. (c) *Coloration Control:* realistic patterns are mostly colorful. Previous work has only demonstrated the injection

† Chen Yan is the corresponding author.

Network and Distributed System Security (NDSS) Symposium 2025
24-28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-8-3
https://dx.doi.org/10.14722/ndss.2025.242065
www.ndss-symposium.org

of grayscale patterns. To the best of our knowledge, no work has yet achieved the capability to inject colored patterns into CCD cameras. In addition to the above challenges, the lack of a theoretical understanding of the interference that causes the structural patterns in CCD cameras hinders the achievement of a more powerful attack.

In this work, we overcome these challenges and validate the feasibility of injecting monochrome and colorful patterns of arbitrary shape and brightness into CCD cameras under normal light conditions. We first conducted a theoretical causality analysis of image pattern injection from three aspects: morphology, brightness, and coloration, and performed capability investigation respectively. Our results indicate that by carefully designing the amplitude and phase of the EMI signal, an attacker can effectively control the shape, brightness, and color of the injected patterns. To materialize such an attack, we designed an end-to-end attack workflow, `GhostShot`, and evaluated it on 15 commercial CCD cameras, all of which confirmed the applicability of the attack. To demonstrate potential real-world impacts, we conducted case studies on medical diagnosis, fire detection, object detection and QR code scanning. We found that `GhostShot` can successfully mislead computer vision systems to detect non-existing road objects, cancer patterns, and forest fires and to interpret fake QR codes. We further demonstrated the potential of using the injected images to deceive human eyes and validated the feasibility of dynamic video injection.

Our contributions are summarized as follows:

- We analyze the causality of injecting monochrome and colored patterns into the images of CCD cameras with IEMI. We have experimentally examined the capability and limits of arbitrary control over the pattern's morphology, brightness, and coloration.
- We design an end-to-end attack workflow and validate the attack feasibility on 15 commercial-of-the-shelf (COTS) CCD cameras. We demonstrate the potential real-world impacts of `GhostShot` on computer vision systems with four case studies and discuss the feasibility of deceiving human eyes.
- We propose hardware and software methods for defending against the attacks.

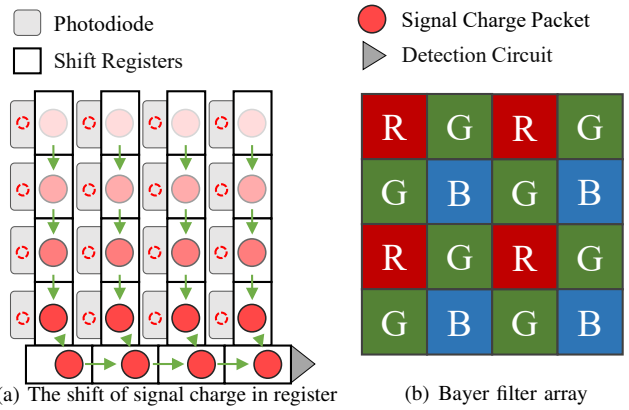
II. CCD Imaging System Overview

A typical CCD imaging system primarily comprises the following three components: CCD image sensor, analog front end (AFE) and digital back end (DBE).

A. CCD Image Sensor

The CCD image sensor is the central element of a CCD imaging system, playing critical roles in photoelectric conversion, the storage and transfer of signal charges, and the measurement and amplification of charges.

Photoconversion and charge storage. The photodiode is responsible for converting incident light into signal charge, with the quantity dependent on the exposure time. Due to the photoelectric effect, light exposure causes electrons to escape atomic confines and become free charges. The basic component of the CCD is the MOS capacitor, consisting of metal electrodes, oxide film, and semiconductors. By applying a positive voltage to the metal electrode, carrier holes in the p-type silicon are depleted, creating a register region at the metal-oxide interface to collect free charge.



(a) The shift of signal charge in register (b) Bayer filter array

Fig. 2: Illustration of (a) the transfer and readout of signal charge in the CCD sensor and (b) the Bayer filter array.

Signal charge transfer. When electrodes are positioned closely and excited by a high voltage, their underlying potential wells become interconnected, resulting in a shared distribution of the initial signal charge from the first electrode. Subsequently, a reduction in voltage applied to the first electrode causes the charge to fully transfer to the second electrode's well. Within a pixel array, a systematic modification of voltages enables an efficient transfer and read-out of signal charges. The signal charges transfer sequentially in row order. Fig. 2(a) illustrates the sequential transfer of signal charge, exemplified by the ITCCD.

Signal charge measurement. All signal charges will ultimately be conveyed to the output circuitry, where they will be processed and amplified. Floating Diffusion Amplifier (FDA) is commonly used in CCDs to measure signal charge, comprising a charge node and two MOSFETs for reset (MOS1) and conversion (MOS2). MOS2 converts the charge to voltage, and MOS1 resets the node to the reference level for the next signal.

B. Analog Front End

The analog front end (AFE) is a set of analog circuitry that conditions and digitizes the analog signal from the image sensor. AFE consists of the correlated double sampling (CDS) circuitry, black level adjust circuitry, analog-to-digital converter (ADC), etc.

Correlated Double Sampling. The raw output signal from a CCD image sensor generally contains noise of multiple forms, including thermal noise, reset noise, and dark current noise. The CDS is the most commonly used circuit for noise reduction in AFE. The CDS circuit samples the reset level and the video level within the one-pixel period, amplifying the difference to produce a cleaned signal, effectively deploying a difference amplifier to eliminate the noise.

Black-Level Adjust. AFE also generates the reference black level by using signals from optical black pixels in an

image sensor. Optical black pixels are located at the periphery of an imaging array, playing an essential role in tracking the dark current variation across the operating temperature range to determine the accurate black level. A signal from an optical black pixel is typically stored on a capacitor, which is then subtracted from a signal from a photosensitive pixel to reduce noise.

Analog to Digital Converter. ADC converts an input analog signal to a proportional digital signal. The ADC's bit depth primarily determines the precision. CCD cameras designed for general consumer use typically feature 10 to 12 bits, whereas professional-grade cameras may offer 12 to 14 bits for even finer detail capture. Another important ability of the ADC is the sampling rate. For low-resolution imaging needs, a sample rate of 20 MPixels/sec is sufficient, while high-resolution cameras require sampling rates greater than 50 MPixels/sec. To maintain excellent visual quality, high-definition television (HDTV) requires more than 75 MPixels/sec.

C. Digital Back End

The digital back end (DBE) receives signals from the AFE and conducts a sequence of processes, including image processing, compression, and storage. Image processing aims to achieve better output image quality, involving components such as color interpolation, white balance, color correction, and gamma correction, which are carried out in an image signal processor (ISP).

Color interpolation. Color interpolation, also known as demosaicing or debayering, is the process of reconstructing a full-color image from raw monochrome data captured by an image sensor. For most single-board color cameras, a Color Filter Array (CFA) is overlaid on the surface of the image sensor, enabling each pixel to capture light of only one specific color. The missing colors at each pixel position can be interpolated with values from adjacent pixels through algorithms such as bilinear interpolation, bicubic interpolation, and others. The Bayer filter array is the most common CFA, composed of alternating RG pixels in odd rows and GB pixels in even rows, as shown in Fig. 2(b). Other types of CFA include CYGM, CMYW, etc.

Color balance. White balance is the adjustment of color temperature settings to accurately reproduce colors under varying lighting conditions, ensuring that the colors appear more realistic. Color correction is used to improve color accuracy by adjusting the raw color data captured by the image sensor. Gamma correction is also employed to adjust the brightness levels of an image, which helps to achieve balanced illumination.

III. Threat Model

A. Attacker's Goal and Attack Categories

We consider an adversary that aims to contactlessly inject an arbitrary image into the captured image of a CCD camera through intentional electromagnetic interference (IEMI). The injected image may spoof the computer vision system's behavior to result in accidents (e.g., inject a fire pattern to result in a false fire alarm or inject a cancerous cell pattern to cause medical malpractices), or spoof human behaviors for malicious purposes (e.g., scan malicious QR codes or being misled by malicious text). Compared with swapping the whole camera or holding a fake image in front of camera which could instantly expose the attacker's malicious intent, the attacker can manipulate a camera's image or video stream in real-time without physically touching the camera. Besides, the attacker can inject ghost patterns seamlessly without affecting the authentic image background, which can avoid abrupt image changes that may alert the victim systems or users. We consider two potential categories for the adversary:

- *Creating attack* to inject a targeted image with arbitrary chromaticity and morphology into the captured image to spoof computer vision systems and human eyes, where a new object appears.
- *Hiding attack* to inject perturbations to spoof computer vision systems, where an object in an original image disappears under the attack.

B. Attacker Capabilities and Assumptions

We make the following assumptions for the attacker to achieve the aforementioned attacks:

Prior Knowledge. We assume the adversary can obtain the target camera's model, which can acquire information about the target CCD camera from publicly available sources (e.g., manuals and datasheets), or may obtain a similar camera for assessment beforehand. For example, she may learn the design of the camera's resolution and frame rate from public documents or by reverse engineering.

IEMI Capability. We assume that it is feasible for the adversary to have access to off-the-shelf devices such as software-defined radios, amplifiers, and antennas to generate malicious IEMI signals to inject a targeted image into the CCD camera.

Attack Scenarios. The adversary can manipulate a camera's image or video stream in real-time without physically touching the target camera, and the COTS camera is in its original package during the attack, leaving no traces of the attack. We envision two potential attack scenarios at different distances: (1) Proximity attack: Similar to previous works [59], [1], [21], the attacker may construct a camouflaged portable EMI prototype and position it next to an unattended camera, acting as an insider to carry out a remotely controlled attack. (2) Attack at a distance: the attacker can increase the attack distance using high-end equipment such as directional antennas and high-gain power amplifiers to conduct attack at a distance.

IV. Capabilities of IEMI on CCD Cameras

In this section, we present preliminary experiments to perform a systematic analysis of the effects of IEMI on CCD cameras. We first analyze the reasons IEMI can effectively interfere with the CCD cameras. Then, we examine these effects from three perspectives: morphology, brightness, and color, and separately investigate the maximum capability of the injection.

A. Preliminary Experiments on CCD Cameras

We use a similar experimental setup as the existing IEMI attacks [21], [26], [42], [41]: an arbitrary signal generator

(a) Ground Truth (b) $f_{in} = 48.0008MHz$ (c) $f_{in} = 48.0038MHz$ (d) $f_{in} = 54.0325MHz$ (e) $f_{in} = 54.0688MHz$

Fig. 3: Periodic stripes with varying morphology and chromaticity can be injected into the captured images at different frequencies during preliminary experiments.

(Keysight N5712b) to generate an IEMI source, a power amplifier (Mini-Circuits ZHL-100W-GAN+) to amplify the signal, and a rubber rod antenna to transmit the IEMI signal to the victim CCD camera. The experiment setup is shown in Fig. 11(a). We choose an analog output and a digital output CCD camera (SHL-223 and MV-GED130C) respectively for the preliminary analysis. The under-test CCD camera is connected to the computer to display the captured image in real time. The camera lens is covered with a lens cap, which captures the picture in total black under normal conditions, as shown in Fig. 3(a).

We conduct a frequency sweeping experiment from 20 MHz to 100 MHz with a step size of 0.1 MHz, and the signal amplitude is -5 dB. The experiment results show that the periodic stripes with different morphology and chromaticity appear in the captured images during the test, as shown in Fig. 3, indicating that although the COTS CCD cameras go through thorough electromagnetic compatibility tests and anti-interference design, they are susceptible to the IEMI signals at different frequencies. Besides, we also observe that the number of stripes changes when fine-tuning the successful injection frequency. For example, we can inject monochrome stripes and colored stripes at the frequency of 48.0008MHz and 54.0325MHz respectively. Furthermore, we observed that an excessive intensity of the injected signal may lead to overexposure in the camera or result in communication errors.

Potential Coupling Interface. As described in Section II-B, the output signal of the CCD requires an extensive analog signal-processing pathway which includes CDS, black-level calibration, and ADC. Due to the hardware structure of the CCD camera in Fig. 2, we suppose the long analog signal pathway unintentionally serves as the receiving antenna to be interfered with by the IEMI signals, and the precise coupling efficiency depends on the design and materials of the circuit itself [35]. By conducting a preliminary frequency sweep on the same model of the target camera, the optimal coupling frequency can be determined.

After demonstrating the feasibility of falsifying the captured image of CCD with IEMI, we wonder if an attacker can inject a targeted image into the CCD camera. If so, the attacker should have the ability to manipulate the morphology, brightness, and color. To investigate the possibility of this hypothesis, we conducted a systematic analysis of the capability and constraints of morphology manipulation (Section IV-B), brightness manipulation (Section IV-C), and color manipulation (Section IV-D), respectively.

B. Capability of Morphology Modulations

During the frequency sweeping experiment, we observed black and white stripes of various morphology in some frequency bands, as shown in Figs. 3(b) and 3(c). We analyzed the root cause of stripes and investigated the potential for implementing control over morphology.

1) Causality Analysis: As introduced in Section II-B, the analog signal output from each R/G/B pixel is transmitted to the ADC to be converted into a digital signal. According to the Nyquist-Shannon sampling theorem, the sampling rate should be at least twice the signal's maximum frequency. If the system samples data at an insufficient sampling rate, the sampled signal fails to maintain the original spectrum characteristics, generating a lower frequency signal due to the aliasing effect [33]. Suppose the injected EMI signal is a regular sinusoidal wave at a frequency f_{in} as follows:

$$s(t) = V_{in} sin(2\pi f_{in} t + \varphi_0) \tag{1}$$

Let f_s denote the sampling rate of the ADC, and the sampled signal after the aliasing effect can be written as follows:

$$P[n] = V_{in} sin(2\pi f_{alia} \times \frac{n}{f_s} + \varphi_0) \tag{2}$$

Due to the aliasing effect, f_{in} and f_s determine the sampled frequency f_{alia} as follows:

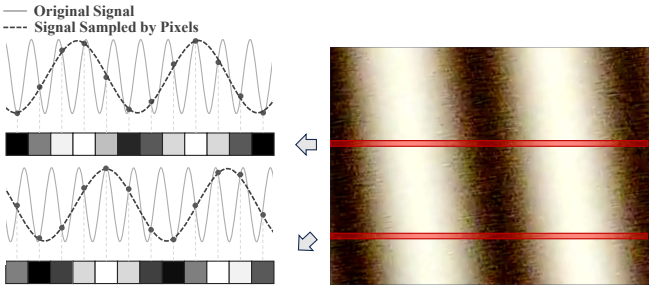
$$f_{alia} = |f_{in} - N \times f_s| \tag{3}$$

where $0 \leq f_{alia} \leq 0.5 f_s$, and $N \in \mathbb{N}$.

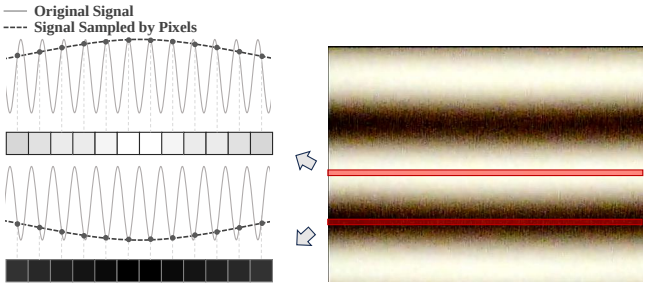
Since all pixel signals are output sequentially in row-major order, aliased sinusoidal signals cause the emergence of alternating stripes in the captured image. The morphology of the stripes primarily depends on the envelope of the aliased signal, which is represented differently across various frequency bands:

$$f_{enve} = \begin{cases} |f_{alia}|, & when |f_{alia} - 0.5 f_s| \geq 0.25 f_s \\ |f_{alia} - 0.5 f_s|, & when |f_{alia} - 0.5 f_s| < 0.25 f_s \end{cases} \tag{4}$$

For a camera with a row transmission frequency of f_{row}, when $f_{enve} \geq f_{row}$, multiple contiguous sine waves are distributed across a single row, thus forming vertical and oblique stripes. When $f_{enve} < f_{row}$, a single sine wave is distributed across multiple consecutive lines, which consequently causes the formation of horizontal stripes, as illustrated in Fig. 4. Specifically, when $f_{in} = N \times f_s$, $f_{enve} = 0$, the attack signal becomes a constant signal after sampling, at which point the stripes disappear, translating into the uniform monochrome area across the entire image.



(a) When $f_{envе} \geq f_{row}$, the stripes remain vertical



(b) When $f_{envе} < f_{row}$, the stripes remain horizontal

Fig. 4: The mechanism for the formation of stripes. The relationship between $f_{envе}$ and f_{row} determines the number and direction of the stripes.

2) Ability Investigation: For a CCD camera to capture frames at a frame rate of f_{fps}, the number of alternating horizontal stripes can be calculated by the following equation:

$$Stripe\_Number = \frac{f_{envе}}{f_{fps}} \tag{5}$$

The spacing of the oblique stripes can be calculated by the following equation:

$$Stripe\_Angle = \arctan \frac{|f_{envе} - N \times f_{row}|}{f_{row} \times N_{columns}} \tag{6}$$

The angle of the oblique stripes can be calculated by the following equation:

$$Stripe\_Spacing = \frac{f_{row} \times N_{columns}}{f_{fps}} \tag{7}$$

Insight 1: The direction and number of stripes can be controlled by fine-tuning the frequency of the injected signal.

In addition to the stripes induced by the sinusoidal part of the injected signal, morphology manipulation can also be achieved through amplitude modulation. Inspired by the mechanism of the CCD sensor introduced in Section II-A, all pixels are read out in a serialized sequence for digitization and we can inject signals that affect the pixels of specific positions. In particular, for a pixel $P[n]$ at the position (x,y), we can modulate the injection signal as follows through amplitude modulation [28], [26]:

$$P[n] = V_{in}(x, y) \times sin(2\pi f_{in} n + \varphi_0), \tag{8}$$

where $V_{in}(x, y)$ is the amplitude sequence generated by the target image. It can be ascertained from Eq. (8) that the injected

(a) Striped NDSS (b) Clear NDSS

Fig. 5: The injected image is influenced by both carrier and amplitude modulation concurrently. By appropriately adjusting the carrier frequency, a clear image without stripes can be injected.

image exhibits the result of the combined influence of the sine carrier signal and the modulation amplitude. When an attacker modulates a specific pattern on the carrier frequency that fails to meet $f_{in} = \frac{N}{2} \times f_s$, the injected pattern is striped, as shown in Fig. 5(a). By adjusting the frequency of the carrier signal to satisfy $f_{in} = \frac{N}{2} \times f_s$, a clean pattern without stripes (Fig. 5(b)) can be injected.

C. Capability of Brightness Modulations

Previous work implemented an injection attack for brightness enhancement in dark environments[26]. In this section, we theoretically analyze the possibility of reducing brightness and provide experimental validation.

1) Causality Analysis: When $|f_{alia} - 0.5f_s| \geq 0.25f_s$, all the pixels in the alternated G/B and R/G pixels are stimulated consecutively by the injection signal, resulting in black-white stripes, as shown in Fig. 7(a). For alternating black-white stripes, we observe that the brightness of light sections exceeds the base level when unattacked, whereas dark sections fall below, which indicates the possibility of brightness reduction. This phenomenon occurs because the sampled sine wave signal is superimposed on the original signal, with the positive half-cycle increasing brightness and the negative half-cycle decreasing brightness.

2) Ability Investigation: When $f_{in} = N \times f_s$, $f_{alia} = 0$, the unmodulated attack signal becomes a constant signal after sampling. The attack signal superimposed on the original normal readout signal results in the formation of a uniform monochrome area across the entire image. The sampled signal after the aliasing effect of Eq. (2) can be written as follows:

$$P[n] = V_{in} sin(\varphi_0) \tag{9}$$

At this time, the image's brightness is determined by the input amplitude V_{in} and phase φ_0. When $\varphi_0 > 0$, there is an increase in image brightness due to the positive aliased signal. Conversely, when $\varphi_0 < 0$, the negative aliased signal causes a decrease in brightness. Combined with the morphological control methods mentioned in Section IV-B, it is possible to independently control the brightness of individual pixels, as shown in Fig. 6.

Insight 2: The brightness of the image could be increased or decreased by controlling the phase of the injected signal.

(a) NDSS with decreased brightness. (b) NDSS with brightness control.

Fig. 6: The injected NDSS with brightness control. The average brightness of the background is 181, whereas the NDSS section shows an average brightness of 120, illustrating a reduction in brightness.

It is worth noting that due to the range limitations of the ADC sampling output, if the camera's original signal has already reached saturation, the superimposed attack signal will not be able to make it brighter. Conversely, if the camera's original signal is too weak, the superimposed attack signal will not be able to make it darker.

D. Capability of Coloration Modulations

During the preliminary experiments, we found that in addition to the black and white stripes, there are also colored stripes, as shown in Figs. 3(d) and 3(e), which are regularly distributed in some frequency intervals. We provide an analytical and theoretical explanation for this phenomenon and propose an arbitrary color control method.

1) Causality Analysis: As introduced in Section II-C, the Bayer filter array overlaid on the CCD sensor is arranged in a line alternating fashion of green-blue (G/B) and red-green (R/G), so that each pixel measures only one color. Though the rows are physically adjacent, the pixel signals are transmitted sequentially, with only one row transmitted at any given time. Therefore, at specific design frequencies, the injection could locate the target pixel without interfering with adjacent pixels or rows. When $|f_{alia} - 0.5f_s| < 0.25f_s$, the sampled signal after the aliasing effect of Eq. (2) can be written as follows:

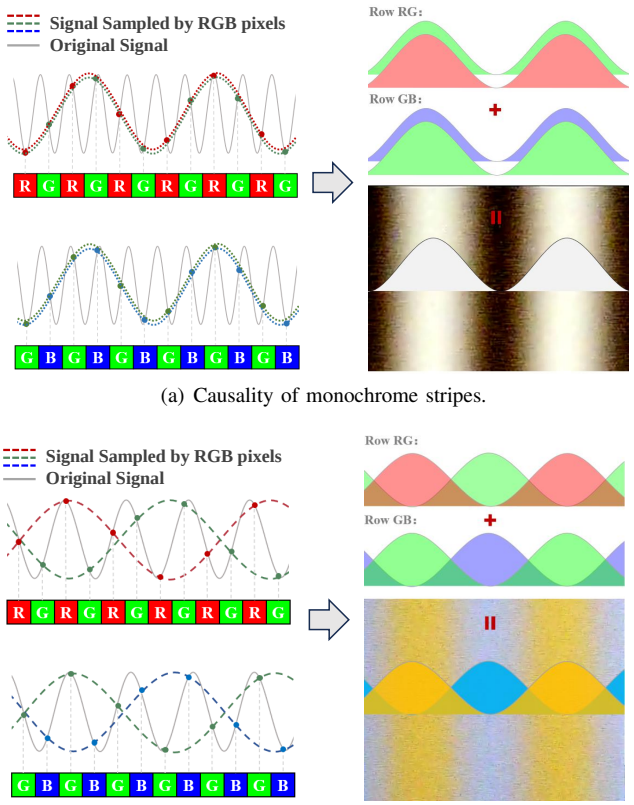
$$P[n] = (-1)^n \times V_{in} sin(2\pi f_{enve} \times \frac{n}{f_s} + \varphi_0) \tag{10}$$

At this time, only one type of pixel in each G/B or R/G line is stimulated. Taking the R/G line as an example, the position index of the red and green pixels is $n = 2m$ and $n = 2m + 1$ respectively, where $m \in \mathbb{N}$. The stimulation of the red and green pixels by the injected signal can be written as follows:

$$P[n]_R = V_{in} sin(2\pi f_{enve} \times \frac{2m}{f_s} + \varphi_0) \tag{11}$$

$$P[n]_G = -V_{in} sin(2\pi f_{enve} \times \frac{2m+1}{f_s} + \varphi_0) \tag{12}$$

We can observe from Eqs. (11) and (12) that the signals injected into the red and green pixels are periodic sinusoidal signals that have identical amplitudes in opposing directions. The situation is similar for G/B lines. Thus, there will be an alternation of color stripes, as shown in Fig. 7(b).



(a) Causality of monochrome stripes.

(b) Causality of colored stripes.

Fig. 7: Illustrations of the causality of (a) monochrome stripes and (b) color stripes. Due to the different relationships between the input signal frequency and the sampling frequency, the signal sampled by RGB pixels yields varied results, resulting in both monochrome and colored stripes.

2) Ability Investigation: When $f_{in} = (N + 0.5) \times f_s$, i.e., $f_{alia} = 0.5f_s$, $f_{enve} = 0$, the sampled signal after the aliasing effect of Eq. (2) can be written as follows:

$$P[n] = (-1)^n \times V_{in} \times sin\varphi_0 \tag{13}$$

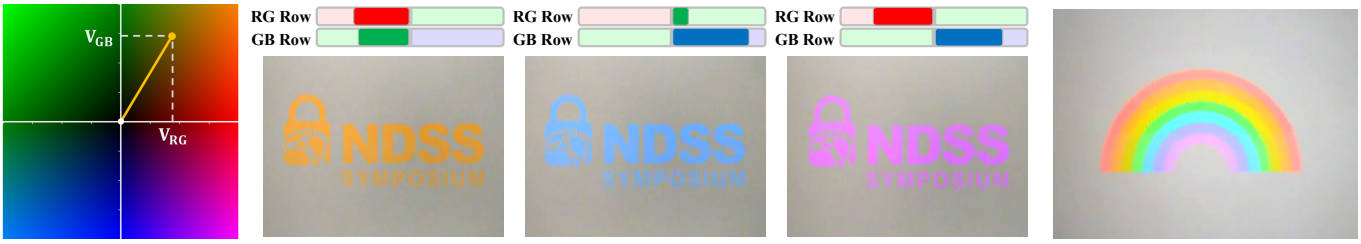
At this time, the unmodulated attack signal becomes a periodic oscillating signal with fixed amplitude after sampling and the captured image becomes a uniform single color. We can change the phase of the injection signal to control the R/G and B/G lines separately, which can be written as follows:

$$P[n]_{RG} = (-1)^n \times V_{inRG} \times sin(\varphi_{RG0}) \tag{14}$$

$$P[n]_{GB} = (-1)^n \times V_{inGB} \times sin(\varphi_{GB0}), \tag{15}$$

where φ_{RG0},φ_{GB0} is set to $\pi/2$ or $-\pi/2$ to select the required color channel while maximizing signal amplitude. We can change phases to choose whether to interfere with R pixels or G pixels in the RG lines and B pixels or G pixels in the BG lines. Thus, we can manipulate the color of the injected image by adjusting the amplitude of RG and GB lines, i.e., V_{inRG} and V_{inGB}.

Insight 3: The coloration of the image could be manipulated by controlling the amplitude and phase of the injected signal.



(a) Color space (b) Orange NDSS (c) Blue NDSS (d) Purple NDSS (e) The injected rainbow

Fig. 8: Illustrations of (a) the feasible color space, (b) to (d) NDSS with different colors, and (e) a rainbow containing seven colors.

Fig. 8(a) illustrates the color space we can manipulate. The positive half-axis region of the X and Y axes corresponds to $\varphi_{RG0}, \varphi_{GB0} = \pi/2$, while the negative half-axis represents $\varphi_{RG0}, \varphi_{GB0} = -\pi/2$. The values of the X and Y axes represent distinct values of V_{inRG} and V_{inGB}. Figs. 8(b) to 8(d) shows three examples of the colored NDSS captured by the camera under different amplitudes and phases. Fig. 8(e) shows an injected rainbow image featuring seven distinct colors, demonstrating our ability to inject multiple colors into a single image.

It is worth noting that the proposed chromaticity manipulation method is a linear combination of two types of three R/G/B pixels, i.e., we can manipulate the chromaticity on a color plane rather than on a three-dimensional color space. From the HSV color space perspective, chroma can be controlled arbitrarily, brightness is limited to the injection amplitude, and the saturation component is uncontrollable. However, it is only necessary to achieve synchronization at the level of row signals, and there are no high demands on the modulation speed. To realize a complete color space, precise pixel-level modulation is required. However, this requires the modulation speed capability of the equipment to reach the level of matching the camera's sampling rate, which is usually above 10 MHz.

V. Attack Design

As introduced in Section IV, the brightness and coloration of the image could be manipulated through the amplitude and phase of the injecting signal. Motivated by this, we propose the use of amplitude-phase modulation for the injection of arbitrary monochrome (black-and-white) or color images. The end-to-end attack workflow is shown in Fig. 9, which consists of four modules: image preprocessing (Section V-A), image signal generation (Section V-B), signal modulation (Section V-C) and signal transmission (Section V-D).

To initiate an attack, the attacker first formulates a strategy based on the scenario, including the selection of the target image, color or monochrome injection, and the requirement for the injection position. Based on various scenarios, attacks can be categorized into two types: creating attack and hiding attack. For creating attack, attackers need to select injection images based on the actual scenario, whereas for hiding attack, attackers can employ stripe-based perturbations for concealment.

A. Target Image Prepossessing

Upon acquiring the image to be injected, the initial step involves preprocessing, which encompasses scaling and padding, brightness normalization, color and contrast adjustment, and noise reduction.

Scaling and Padding: To ensure that the injected image appears in its entirety and at an appropriate size within the target camera's field of view, the target image should be suitably scaled to be slightly smaller than the resolution of the target image sensor. The specific scaling ratio must be determined further based on the attack scenario and the target of the attack.

Color and Contrast Adjustment. Once the image is injected in the form of an electromagnetic signal, it will undergo a series of digital processing procedures, such as white balance and gamma correction. Direct modulating and injecting the original image will inevitably cause color deviation and contrast shift. Therefore, to faithfully reconstruct the targeted image, we pre-adjust its color and contrast, which can be determined by pre-testing in a camera of the same type as the target.

Noise Reduction. The noise contained in the original target image can degrade the image quality, thereby affecting the visual effects of injection and the recognition performance of the injected image. By applying the denoising method, it is possible to enhance image quality, improve visual effects, and increase recognition accuracy. We applied K-SVD as the denoising algorithm, which could efficiently remove image noise while preserving important structural details based on sparse coding.

Brightness Normalization. As the image data is modulated onto the carrier for transmission during the subsequent signaling modulation process, it is necessary to normalize the value of all pixels, facilitating the generation of image signal data. Normalization can be carried out by dividing the pixel value at each position in the original image by the maximum value for each pixel.

B. Image Signal Generation

After preprocessing the target image, we next generate the amplitude and phase sequences required for modulation from the processed image. In particular, we calculate the amplitude and phase corresponding to each pixel based on its RGB values and then arrange them sequentially according to the signal readout order of the CCD (row by row). Based on the different

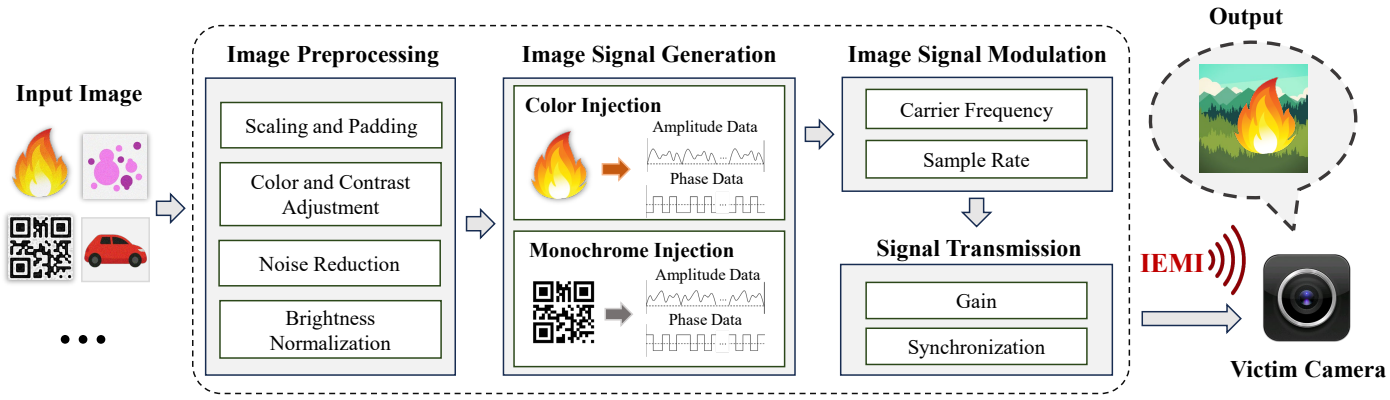


Fig. 9: The attack workflow. The attacker first selects the input image according to the attack scenario. Based on the choice between monochrome or color injection, the attack then derives the amplitude and phase data from the preprocessed image. Finally, the attacker performs the modulation and transmission of the generated signal.

effects of attacks, we divide the attacks into two paradigms, monochrome injection and color injection.

1) Monochrome Injection: To achieve optimal injection with maximum contrast, we divide all pixels based on the average value of the converted grayscale image and implement injections that either increase or decrease brightness accordingly. The amplitude and phase of the injection signal can be obtained by the following equations:

$$A_{mono}(x,y) = |Y(x,y) - Y_{avg}| \tag{16}$$

$$\varphi_{mono}(x,y) = \frac{\pi}{2} \times sign(Y(x,y) - Y_{avg}) \tag{17}$$

where Y(x,y) represents the brightness of the pixels at the corresponding location in the target image, which can be calculated by the following equation [57]:

$$Y(x,y) = 0.299 * R(x,y) + 0.587 * G(x,y) + 0.114 * B(x,y) \tag{18}$$

where R(x,y), G(x,y), and B(x,y) represent the red, green, and blue components of the corresponding pixel location, respectively. Y_{avg} represents the average brightness of all the pixels in the target image. The function $sign(x)$ returns 1 for positive x and -1 for negative x. In addition, the attacker can flexibly adjust Y_{avg} to enhance either the bright part or the dark part of the injection, depending on the situation. As discussed in Section IV-C, the upper and lower limits of increasing and decreasing brightness are influenced by ambient light. Therefore, when the ambient brightness is too high, it is appropriate to increase Y_{avg} to enhance the details of the dark areas; conversely, when the ambient brightness is low, Y_{avg} can be reduced to emphasize the bright areas.

2) Color Injection: The analysis in Section IV-D identifies the essence of the generation of different colors as the result of injected signals with distinct phases and amplitudes into the RG and GB rows. Since we can only select one color respectively from the RG row and the GB row each by altering the signal phase, we choose to interfere with two color channels with higher values out of the R, G, and B channels of the target pixel. According to the RGB value of the target pixel and the row where the target pixel is located, the amplitude and phase required for color injection are shown in Table I. $R(x,y), G(x,y), B(x,y)$ represent the R, G, and B color channels of the target pixel, while $C_{min}(x,y)$ denotes the minimum value among them. According to Eq. (14) and Eq. (15), altering the phase will concurrently result in a change in the overall amplitude of the signal. Therefore, we select the signal's phase to be $\frac{\pi}{2}$ or $-\frac{\pi}{2}$ to ensure interference with the correct color channel, and independently adjust the amplitude through V_{in} to simplify the modulation.

TABLE I: The requirements of the amplitude and phase of attack signals for color injection.

$C_{min}(x,y)$	RG rows		GB rows	
	V	ϕ	V	ϕ
$R(x,y)$	$\frac{G(x,y)-R(x,y)}{255}$	$-\frac{\pi}{2}$	$\frac{B(x,y)-R(x,y)}{255}$	$-\frac{\pi}{2}$
$G(x,y)$	$\frac{R(x,y)-G(x,y)}{255}$	$\frac{\pi}{2}$	$\frac{B(x,y)-G(x,y)}{255}$	$-\frac{\pi}{2}$
$B(x,y)$	$\frac{R(x,y)-B(x,y)}{255}$	$\frac{\pi}{2}$	$\frac{G(x,y)-B(x,y)}{255}$	$\frac{\pi}{2}$

C. Image Signal Modulation

After generating the amplitude and phase sequences from the preprocessed image, we perform amplitude and phase modulation to generate the attack signal as follows:

$$P[n](x,y) = V_{in}(x,y) \times sin(2\pi f_{in} n + \varphi(x,y)), \tag{19}$$

where $V_{in}(x,y)$ and $\varphi(x,y)$ are the amplitude and phase of the pixel $P[n]$ at the position (x,y) on the targeted image respectively, as shown in Fig. 10. The following section details the design of the carrier frequency and sample rate in modulation.

1) Carrier Frequency: The selection of the carrier frequency involves considerations of the coupling efficiency, whether the injection is monochrome or colored, and the influence on the morphology. The coupling efficiency of the attack signal dictates the maximum amplitude of the signal that can be injected. As mentioned in Section IV-A, the effective injection frequency range depends on the coupling frequency of the structure of the circuit itself. We can obtain

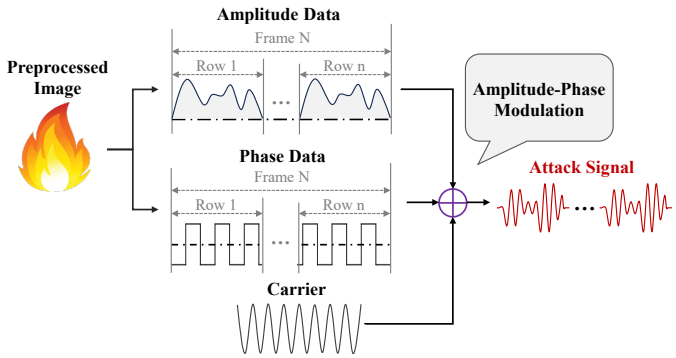


Fig. 10: Illustration of the generation of attack signal. First, extract the amplitude and phase data from the preprocessed image. Then implement amplitude-phase modulation.

the optimal frequency band with the utmost coupling efficiency by conducting a preliminary frequency sweep. It should be noted that, due to the potential existence of multiple injection points in the specific camera circuit, there may be multiple discontinuous electromagnetic sensitive frequency ranges. The frequency specifically used for injection should be chosen from the range with the highest injection efficiency and the lowest signal-to-noise ratio. Furthermore, based on the analysis in Sections IV-C and IV-D, different frequency bands are associated with monochrome and color injections respectively. Therefore, one needs to identify the more accurate frequency bands corresponding to the monochrome or color injection among all feasible options. Finally, according to the analysis in Section IV-B, the morphology injected is affected by fine-tuning of the frequency. When the frequency precisely meets the condition $f_{in} = \frac{N}{2} \times f_s$, patterns without stripes can be injected. Therefore, it is necessary to continue fine-tuning the frequency within the frequency band with the optimal coupling efficiency to find the precise frequency that satisfies the above equation, which is utilized as the carrier frequency in modulation.

2) Sample Rate: The sample rate is a critical parameter in signal modulation which represents the number of samples per second that are modulated onto the carrier. In order to inject a pattern without distortion, it is essential to ensure that the time to transmit a row of data from the modulated image aligns with the time to transmit a row of pixel signals when the image sensor is operating normally. This can be accomplished by appropriately adjusting the sample rate, which is determined by the following equation:

$$Sample\_Rate = \frac{Image\_Width}{T_{row}} \tag{20}$$

where $Image\_Width$ represents the width of the preprocessed image, i.e. the total number of pixels in a row. T_{row} denotes the time required by the camera to normally transmit a row of pixel signals, which can be calculated by the following equation:

$$T_{row} = \frac{1}{F \times N_{rows}} \tag{21}$$

where F represents the frame rate of the camera, and N_{rows} donates the total number of rows in the camera's image sensor. If the sample rate does not satisfy Eq. (20), it would lead to drift in the position and color of the injected image in consecutive frames.

D. Signal Transmission

After the signal has been modulated, it is transmitted from the signal generation device to an amplifier for amplification and then conveyed through an antenna. Throughout this process, our primary considerations are focused on two aspects: gain and synchronization.

1) Gain: The changes in power during the signal transmission process can be calculated from the simplified version of the Friis transmission equation [28]:

$$P_r = P_t G_t G_r (\frac{\lambda}{4\pi d})^2 \tag{22}$$

where λ is the signal wavelength, and d represents the attack distance. P_r and P_t respectively represent received power and transmitted power. G_t and G_r represent the gain of the transmitting antenna and the gain of the receiving antenna, which has taken the effects of the radiation angle into account. Assuming that the attacker has performed the injection at a distance of d_0 with a transmit power of P_{t0} beforehand, she can set the transmit power to achieve the same attack effect at a distance of d by using the following equation:

$$P_t = (\frac{d}{d_0})^2 P_{t0} \tag{23}$$

2) Synchronization and Position: In certain attack scenarios, the injection pattern needs to occur at a specific location, requiring the injected signal to be time-synchronized with the camera's original signal. We refer to the method in previous work [21], demonstrating the feasibility to synchronize the signals by detecting electromagnetic leakage of the target camera. The electromagnetic signals leaked from the target camera and synchronization methods are detailed in Appendix A.

VI. Evaluation

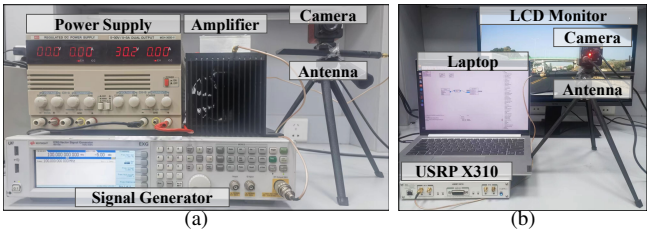
We first evaluate the GhostShot attack on 15 commercial-off-the-shelf cameras and quantify the impact of the attack distance and angle. Then, we evaluate the impact of attacks in four computer vision scenarios, including medical diagnosis (Section VI-C), fire detection (Section VI-D), code scanning (Section VI-E), and night vision object detection (Section VI-F). Furthermore, we show the effects of GhostShot attacks on misleading human vision in Section VI-G.

A. Experimental Setup

We conduct all experiments in a shielded chamber following regulations and also wear electromagnetic shielding clothing, and the experiment setup is shown in Fig. 11(b). When testing the cameras outside the lab, we did not observe similar interference from other electronic devices, as the attack is effective only with intentional signals of specific frequencies and waveforms. The attack devices used in the laboratory setting include an Ettus USRP X310 with two UBX-160 RF daughter boards (which support a maximum signal bandwidth of 160 MHz) for signal generation, a Mini-Circuits ZHL-100W-GAN+ amplifier for EMI signal amplifying, and an antenna for EMI signal transmission. It is worth noting that

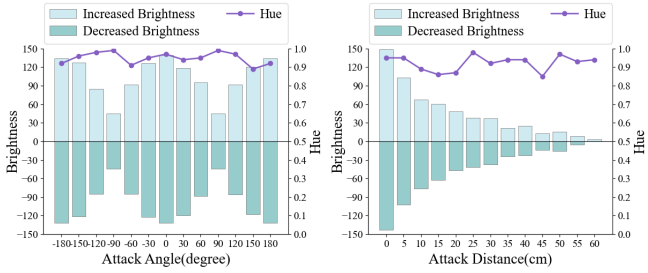
TABLE II: Feasibility of attack on 15 COTS cameras.

CCD Camera System and Sensor Configureation							Freq.Mono.(MHz)		Freq.Color(MHz)		Brightness [-255,255]	Hue [0°,360°]
Type	Vendor	Model	Sensor Model		Res.	FPS	Range	Opt.	Range	Opt.		
Analog CCTV	MingChuangDa	\	Sony	ICX811	976×582	50	53.2-57.6	55.6	67.6-71.1	69.2	-105∼133	360°
	ShunHuaLi	SHL-223		ICX811	976×582	50	44.7-51.7	48.1	43.1-44.6	43.5	-138∼156	360°
		SHL-019-1		ICX873	720×576	50	70.5-74.7	72.6	64.8-70.4	67.5	-124∼139	360°
	Szrs	\		Unknown	640×480	60	85.2-89.2	87.3	51.3-53.5	52.6	-110∼148	360°
	LantTian	TD-813		ICX663	976×582	60	47.4-48.7	47.9	57.3-59.8	58.0	-137∼145	360°
	Mintron	MTV-37S10P		ICX405	798×548	50	94.4-98.2	96.0	60.8-64.9	62.4	-116∼128	360°
		MTV-73X11HP		ICX409	798×548	50	97.2-99.1	98.2	67.2-69.1	68.4	-92∼117	360°
	KangShi	\		ICX811	976×582	60	56.5-57.2	56.7	57.3-63.4	60.9	-108∼131	360°
	Hayear	\		Unknown	1280×1024	60	81.5-86.0	83.7	74.3-77.1	75.6	-87∼114	360°
Digital Ethernet	Basler	ACA1300-30GC		ICX445	1296×966	60	\	\	59.5-67.2	63.6	-59∼64	360°
	MindVison	MV-UBD130C	Sharp	Unknown	1280×960	35	\	\	41.3-66.5	53.9	-46∼62	360°
		MV-GED130C		Unknown	1280×960	43	\	\	63.7-68.2	66.0	-55∼69	360°
		MV-UBD32C		Unknown	640×480	140	\	\	58.8-69.4	64.2	-88∼103	360°
	DaHeng	MER-032-120GC		RJ33B	656×492	120	48.3-76.6	62.3	81.7-100	92.8	-34∼41	360°
	Hikivision	MV-CE013-50GC		RJ33B4A	640×480	30	\	\	64.4-68.0	66.2	-37∼59	360°



(a) (b)

Fig. 11: Illustration of the experiment setup used in (a) preliminary studies and (b) evaluation experiments.



(a) (b)

Fig. 12: The impact of (a) attack angle and (b) attack distance on the attack.

the signal generator needs to have a high capability of data modulation to achieve the capability of arbitrary injection mentioned in Section V. The under-test CCD cameras are positioned in front of an LCD monitor that displays images simulating various visual scenarios. During the evaluations, all commercial cameras are tested in their original packages and default settings without modification. To validate the potential impact on image applications, we conduct the following case studies with a 7cm attack distance shown in Fig. 11(b).

B. Attack on Various Cameras

1) Impact of Camera Models: We evaluate the attacks on 15 cameras, including 9 analog CCTV cameras and 6 digital cameras, as shown in Table II in the Appendix. The image sensors used in these cameras are mainly from Sony and Sharp with specific models. We perform a frequency sweeping test on each camera within 20-100MHz in steps of 0.1MHz and record the ranges where the monochrome bands and color bands appear with high coupling coefficients and low signal-to-noise ratios. We also locate and find the frequency where $f_{envе}$ = 0 according to Section IV-B, which will serve as the carrier frequency in subsequent modulations. We record the absolute value of brightness variation caused by injection in the same area, and conduct the amplitude-phase modulation for each color frequency band to verify the achievable chroma range.

Results: We observe similar striping phenomena in both analog CCTV cameras and digital cameras across 15 different models in their original packages (all metal cases), and the corresponding results are recorded in Table II. Given that digital cameras typically have a higher resolution and ADC sampling rate, it follows that each individual color or monochrome stripe should have a broader range as suggested by Eq. (4), which is validated in the experiment. The actual measured attack frequency range follows the rules stated in Sections IV-C and IV-D. However, due to the camera circuit's variable coupling efficiency at different frequencies, the actual measured attack frequency range is a subset of the theoretical frequency range. Finally, the absolute value of the injected brightness variation suggests that analog output cameras are more susceptible to EMI than digital cameras.

2) Impact of Attack Angle: We select a representative camera (SHL-223) as the subject for evaluation in the impact of attack distance and angle and the following case study experiments. We maintain a constant attack distance and the transmission power and fix the position of the target camera. The angle of attack is adjusted by altering the position of the attack antenna within the same horizontal plane as the target camera, varying from -180° to 180°, in steps of 30°. For each position, we perform monochrome injections separately for increasing and decreasing brightness to measure the resulting changes in average brightness. Additionally, we conduct color injections to measure the average hue of the injected images. The results are recorded in Fig. 12(a).

According to the results, when the antenna is located on the

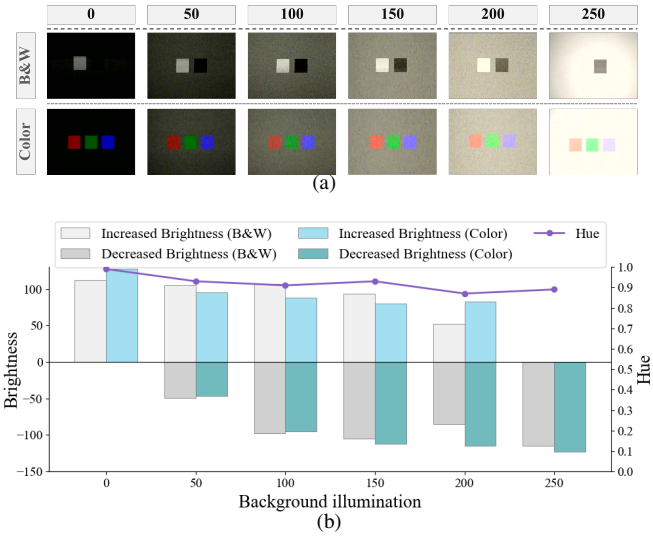


Fig. 13: Illustration of (a) attack under various light conditions and (b) evaluation of the impact of ambient brightness

starting axis, i.e., parallel to the plane of the camera lens, the changes in average brightness are maximal. As the antenna shifts towards both sides, the injection amplitude gradually decreases, reaching minimized injection when the angle hits 90 degrees. However, the hue of the injected images shows minimal variations with angle. Furthermore, the attack results show that within the ranges of -180°-0° and 0-180°, the impact of the angle on the attack is symmetrical. This is due to the symmetrical geometric structure of the antenna and camera.

3) Impact of Attack Distance: We position the antenna parallel to the lens, keep the attack angle and the transmission power constant, and change the distance between the antenna and the camera in increments of 5 cm. We perform similar monochrome and color injections as mentioned in Section VI-B2 to measure the changes in average brightness and hue. We test the absolute value of the brightness change caused by the injection in the range of 0 to 60 cm and recorded the results in Fig. 12(b). According to the results, the brightness of the injection reaches its maximum at 0 cm and gradually decreases as the distance increases. This is due to power attenuation during the propagation of electromagnetic waves. Also, the hue of the injected image does not show significant variation with changes in distance.

4) Impact of Ambient Brightness: We vary the background brightness level from 0 to 250 in a step of 50 and perform color injection and greyscale injection respectively, as shown in Fig. 13(a). For greyscale injection, we injected squares of black and white and assessed the values of increased and decreased brightness. For color injection, we injected squares of red, green, and blue, and evaluated the increased and decreased brightness values as well as the hue of the injected color. We snapped 10 images at each brightness setting and computed the average scores. The results indicated the capability of the attack shows overall resilience at different brightness levels, as illustrated in Fig. 13(b). At a background brightness of 0, the attack cannot further decrease the brightness but can achieve the optimum increase of 127. Conversely, at a brightness of 250, the optimum decrease of -123 is achieved, while no further increase is possible. At intermediate levels, the attack demonstrates the ability to both increase and decrease brightness, with the sum of absolute changes peaking at the brightness of 100.

TABLE III: Attack performance in medical diagnosis.

Dataset	Model	Status	Metrics			
			Precision	Recall	Accuracy	F1-Score
Camelyon16	DSMIL	Benign	0.68	0.59	0.66	0.63
		Attack	0.37	0.33	0.40	0.34

TABLE IV: Attack performance in fire detection.

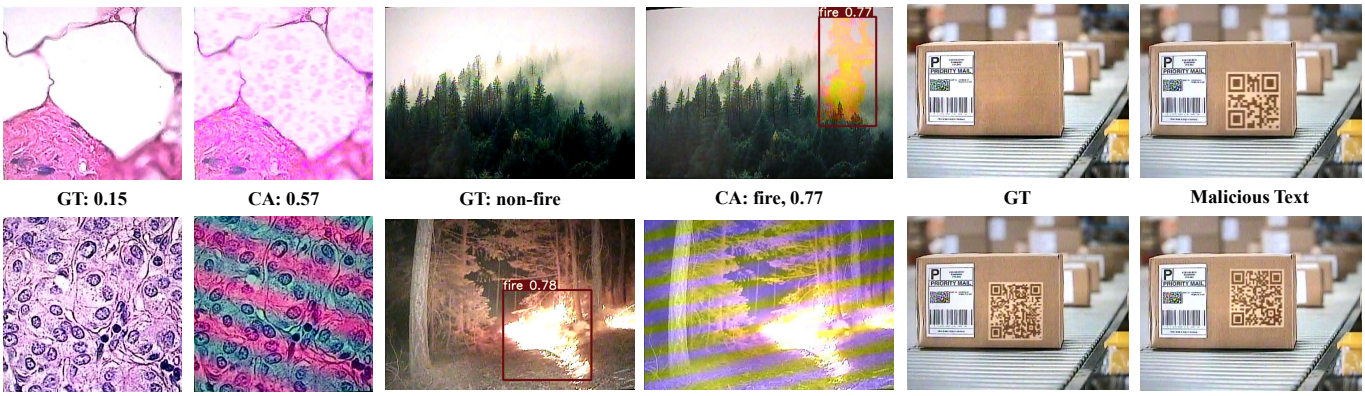
Dataset	Model	Status	Metrics			
			Precision	Recall	Accuracy	F1-Score
NASA 2018	Yolov5	Benign	0.91	0.63	0.79	0.75
		Attack	0.09	0.08	0.15	0.09
	FireNet	Benign	0.94	0.58	0.77	0.72
		Attack	0.11	0.09	0.18	0.10
D-Fire	Yolov5	Benign	0.96	0.68	0.83	0.80
		Attack	0.14	0.11	0.21	0.12
	FireNet	Benign	0.93	0.65	0.80	0.76
		Attack	0.05	0.04	0.17	0.05

C. Case Study 1: Medical Diagnosis

CCD cameras are widely used in medical microscopy due to their lower noise and higher sensitivity [6], [45], [19]. We evaluate the impact of attacks on automated diagnostic systems in intelligent healthcare. We evaluated CA (Creating Attack) and HA (Hiding Attack) on the cancer diagnosis model based on DSMIL (Dual-Stream Multiple Instance Learning Network) [30]. We randomly select a Whole Slide Image (high-resolution images obtained through scanning) from the Camelyon16 dataset, divide it into patches of the corresponding model entry size, and select 100 cancer-negative samples for CA and 100 cancer-positive samples for HA. For CA, we pre-process and extract features detected as cancer from the positive samples and use them as input images to generate the attack signal. For HA, we conceal the original features of the images with stripes, as shown in Fig. 14(a). We evaluated the model's accuracy, precision, recall, and F1 score before and after the attack, with the results presented in Table III. The results show that the attack significantly degraded the model's performance. In addition, we implemented the attack on two types of microscopes to demonstrate the practical threats of the attack in a real-world scenario, as detailed in the Appendix D.

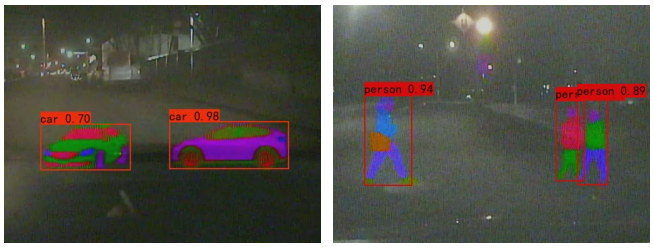
D. Case Study 2: Fire Detection

CCD cameras possess an exceptional dynamic range, making them ideal for a variety of security surveillance applications [8], including fire monitoring [49] and security surveillance [25], etc. Many CCD cameras [14], [40] are used in commercial intelligent fire detection systems [18], [17], enabling automatic fire detection and alarm activation. We assess the attacks on two fire detection models, YOLOv5 [12] and FireNet [32], across two fire datasets, NASA 2018 [37] and D-Fire [7]. We randomly selected 100 non-fire images and 100 fire images from each dataset and conducted CA and



(a) Medical diagnosis (b) Fire detection (c) QR code scanning

Fig. 14: Case studies on medical diagnosis, fire detection and QR code scanning.



(a) The injected cars (b) The injected persons

Fig. 15: The injection of cars and persons under low-light environment.

HA respectively. Subsequently, the post-attack images were identified with two detection models. The results are presented in Table IV, indicating that the attack could considerably impact the effectiveness of fire detection systems across different models and datasets.

E. Case Study 3: QR Code Scanning

CCD barcode scanners provide several benefits compared to other types of barcode scanners, including enhanced reliability, greater durability, and cost-effectiveness [39], [48]. Injecting a fake QR code may lead to unintentional purchases or purchases at the lowest illegal price. Moreover, the injection of malicious QR codes could result in the execution of unauthenticated commands [58], causing operating system crashes, or executing harmful instructions. We implement attacks on QR code recognition systems in the context of industrial logistics. We utilize QR codes for a short text "you're hacked!", a malicious picture and a malicious script to produce the corresponding attack signals, as shown in Fig. 14(c). We test the decoding of these QR codes with more than 10 scanning systems, and all systems could correctly decode the intended results. In real-life attacks, the QR code could correspond to malicious website links, malicious file downloads, malicious payment codes, etc., causing potentially widespread damage.

F. Case Study 4: Night Vision Object Detection

Due to the excellent imaging performance in low light conditions, CCD cameras are utilized for night vision object detection [15], [44]. We utilize three models based on YOLOv4, YOLOv7, and Mask R-CNN for object detection

(a) A notice (b) A "FAKE" pattern (c) A McDonald's logo

Fig. 16: Case study to deceit to the human.

and simulated the operation of CCD cameras in low-light night vision environments. We successfully inject two different types of objects, car and person, into 60 distinct low-light backgrounds, as shown in Fig. 15. The confidence threshold for all models is uniformly set to the default value of 0.5, which means that objects with a confidence level exceeding 0.5 can be successfully detected. For YOLOv4, YOLOv7, and Mask R-CNN, the average success rates of detecting the injected cars are 98.3%, 96.67%, and 100% respectively, and the average success rates of detecting the injected persons are all 100%.

G. Case Study 5: Deceit to the human

We conduct the attack in real-world settings and observed that it not only deceives computer vision systems but also can mislead humans to some extent. For example, in Fig. 16(a), a notice message injected onto a piece of paper could mislead people into sending important emails. In Fig. 16(b), the injected "FAKE" pattern can lead people to question the authenticity of the captured image. The injected McDonald's logo in Fig. 16(c) presents people with misleading visual information. In addition, we conducted a user study to evaluate the difficulty of noticing the injected changes for people and the attribute factors affecting the noticeability of the attack, as detailed in Appendix E.

H. Dynamic Injection

During the experiment, we discover the possibility of achieving stable injection across multiple consecutive frames. Since the attack signal is injected only in each current frame, continuous signal injection is required to persist the injected images. By controlling the sampling frequency in signal modulation, the attack signal could align with the frame rate, enabling injection at the same location across consecutive

frames. Additionally, animated injection can be achieved by injecting different images across consecutive frames. Video demos can be found on [13].

VII. Discussion

A. Countermeasures

Shielding. Though we have achieved successful attacks on 15 commercial CCD cameras in their original metal cases, specialized electromagnetic shielding design can be employed as a critical defense against the attack. We investigate the impact of various common electromagnetic shielding materials, including metal plates, fibers, sponges, and tin foil, on the attack, and the results are shown in Fig. 24 in Appendix F.

Image forgery detection. We implemented two image forgery detection methods, Noiseprint [3] and ManTraNet [52], as defense models to evaluate their effectiveness in detecting forged patterns injected by the attack. Noiseprint performs deepfake detection by extracting fingerprints of cameras while ManTraNet utilizes end-to-end deep neural network architecture to extract anomaly features. As shown in Appendix G, the results indicate that the attack can circumvent Noiseprint with high probability, while ManTraNet serves as an effective countermeasure.

Low-Pass Filters. A low-pass filter permits the passage of low-frequency signals compared to the cutoff frequency and attenuates signals with higher frequencies. Many camera manufacturers already equipped optical low-pass filters placed over image sensors, reducing the occurrence of undesired moiré patterns and false colors. Nevertheless, low-pass filter circuits are rarely utilized in practice. Since the coupling frequency of attack signals typically exceeds the pixel frequency of the image sensor, the low-pass filter circuit before ADC can effectively filter out the attack signals.

Redundancy Pixels. As introduced in Section II-B, the AFE module utilizes redundant optical black pixels to eliminate noise. A straightforward approach entails detecting anomalous signals from these redundant pixels. Since these pixels are not optically exposed, detecting abnormal signals from their outputs could effectively diagnose attacks.

B. Limitations and Future Work

The attack still has the following limitations at present. (1) There is insufficient regulation of saturation in color injection. Based on the analysis in Section IV-D, we are restricted to injecting colors with high saturation considering the current capabilities of our devices. The injection of fully saturated images can be achieved by precise modulation at the pixel level, which typically requires highly advanced modulation capabilities from the device. (2) Due to the separate frequency bands needed for monochrome and color injection, presently only one type of injection can be conducted simultaneously using a single carrier frequency. The combination of monochrome injection and color injection can be achieved by utilizing multi-carrier modulation, which enriches the diversity of scenarios for the attack. (3) Our attack specifically targeted CCD cameras, and no similar phenomena have been observed in CMOS cameras. Further investigation is needed to determine the feasibility of conducting attacks on CMOS cameras.

VIII. Related Work

Compare to previous works. Compared to previous work [26], we present the first IEMI attack that can inject arbitrary grayscale and colored images into off-the-shelf CCD cameras under normal light conditions. Compared to grayscale injection, color injection presents challenges in the following aspects: (1) Stimulating specific color channel: In color filter arrays, attack signals often induce common effects across adjacent color channels, resulting in grayscale injection. We design the signal frequency and leverage aliasing in the camera's sampling process to ensure that the sampled result predominantly affects a single color channel, allowing for the injection of color patterns. (2) Stimulating various color channels: Injections in the RG or GB rows lead to simultaneous changes in multiple color channels, making it difficult to balance injection ratios across the RGB channels. We introduce a phase-based injection method to control the proportion of color components for the first time and achieve the injection of various colors. (3) Achieving accurate color injection: The injected EMI signal causes a nonlinear increase in the injected color values, complicating the attacker's ability to predict the final result accurately. Unlike greyscale injection, even minor deviations across different color channels can result in color distortions. We implement pre-injection feedback and fine-tuning of the injected color image to reduce color deviation, ensuring that the final injected colors are accurate and aligned with the intended values.

IEMI attacks on sensors. EMI signals have been widely studied in the security research community to destroy the integrity and reliability of analog and digital sensor outputs in recent years. In 2013, Kune et al. [28] first described the IEMI attacks on sensors and examined two types of cardiac devices and microphones. Since then, IEMI attacks to manipulate the sensor's measurement have been reported on microphone [28], [53], [54], [10], [5], touchscreen [31], [11], [43], [51], [23], [60], temperature sensor [29], [46], [34], [24], [9], LiDAR [2], keyboard [22], image sensor [4], [26], [21] and so on. The consequences of these attacks range from denial-of-service to injecting malicious data or even completely manipulating the operations of sensor-based cyber-physical systems. This paper conducts a systematic security analysis of the IEMI attacks on CCD cameras and characterizes the limitations of injecting targeted images into CCD cameras with IEMI.

Attacks on cameras using physical signals. Researchers have already found that attackers can use light and laser [36], [55], [56], [38], [27], acoustic [20], and EMI [21], [26] signals to interfere with the captured image and thus spoof the camera-based computer vision systems. Compared with light, laser, and acoustic signals, attacks with EMI signals are stealthier and do not require line-of-sight. The recent work [21] has uncovered the vulnerabilities of image signal transmission with IEMI, and attackers can inject row-level color stripes into images. Another recent work [26] has shown the feasibility of injecting signals into CCD image sensors using IEMI, which can only inject grey-scale image perturbations in a dark environment. Informed by these works, this paper aims to explore the further capabilities and limits of IEMI attacks on CCD cameras and proposes the first attack to inject an arbitrary colored image with targeted chromaticity and morphology into the CCD camera under normal ambient light conditions.

IX. Conclusion

In this paper, we design the attack against CCD cameras that can inject arbitrary monochrome or color images through IEMI. We confirm the feasibility of the attack with 15 CCD cameras and demonstrated the threat of the attack to computer vision systems, as well as its ability to mislead humans through case studies. We propose hardware and software methods to defend against the attack.

Acknowledgement

We sincerely appreciate our anonymous reviewers and shepherd for their valuable comments and suggestions. This work was supported by China NSFC Grant 62201503, 61925109, 62222114, and 62071428.

References

[1] A. Barua and M. A. Al Faruque, "Hall spoofing: A non-invasive dos attack on grid-tied solar inverter," in *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 1273–1290.

[2] S. H. V. Bhupathiraju, J. Sheldon, L. A. Bauer, V. Bindschaedler, T. Sugawara, and S. Rampazzi, "Emi-lidar: Uncovering vulnerabilities of lidar sensors in autonomous driving setting using electromagnetic interference," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2023.

[3] D. Cozzolino and L. Verdoliva, "Noiseprint: A cnn-based camera model fingerprint," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 144–159, 2019.

[4] D. Dai, Z. An, Q. Pan, and L. Yang, "Magcode: Nfc-enabled barcodes for nfc-disabled smartphones," in *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, 2023.

[5] D. Dai, Z. An, and L. Yang, "Inducing wireless chargers to voice out for inaudible command attacks," in *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*.

[6] R. Davey, "Using ccd devices to capture cell images," 2022. [Online]. Available: https://www.news-medical.net/life-sciences/Using-CCD-Devices-to-Capture-Cell-Images.aspx

[7] P. V. A. de Venâncio, A. C. Lisboa, and A. V. Barbosa, "An automatic fire detection system based on deep convolutional neural networks for low-power, resource-constrained devices," *Neural Computing and Applications*, vol. 34, no. 18, pp. 15 349–15 368, 2022.

[8] Elvia, "Complete guide to security camera cmos vs ccd image sensors," 2022. [Online]. Available: https://reolink.com/blog/security-camera-cmos-vs-ccd-image-sensors/

[9] J. L. Esteves, E. Cottais, and C. Kasmi, "Unlocking the access to the effects induced by iemi on a civilian uav," in *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*. IEEE, 2018, pp. 48–52.

[10] T. Fokkens, S. Xia, A. Harmon, and C. Hwang, "Coupling path analysis for smart speaker intentional electromagnetic interference attacks," in *Proceedings of the 2023 IEEE Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMC+ SIPI)*. IEEE.

[11] M. Gao, F. Xiao, W. Liu, W. Guo, Y. Huang, Y. Liu, and J. Han, "Expelliarmus: Command cancellation attacks on smartphones using electromagnetic interference," in *Proceedings of the IEEE INFOCOM 2023-IEEE Conference on Computer Communications*.

[12] Y. Geng, "Fire-smoke-detect-yolov4: Fire and smoke detection using yolov4 and yolov5," Github, 2020. [Online]. Available: https://github.com/gengyanlei/fire-smoke-detect-yolov4

[13] GhostShot, "Demos of ghostshot attacks," (2024, Jun 14). [Online]. Available: https://sites.google.com/view/ghostshot

[14] Globalsources, "Ccd camera flame detector," 2024. [Online]. Available: https://www.globalsources.com/Flame-detector/CCD-Camera-Flame-Detector-1168255367p.htm

[15] U. Hock, "Ccd / cmos cameras: Eyes for cars," 2009. [Online]. Available: https://www.eetimes.com/ccd-cmos-cameras-eyes-for-cars/

[16] M. Intelligence, "Ccd image sensors market size share analysis - growth trends forecasts (2024 - 2029)," 2023. [Online]. Available: https://www.mordorintelligence.com/industry-reports/global-ccd-image-sensors-market-industry

[17] Irisity, "Elevating safety with ai video fire detection," 2024. [Online]. Available: https://irisity.com/iris-platform-overview/ai-fire-detection/

[18] Ithermai, "Fire prevention: Localizing fire at inception with video analytics," 2024. [Online]. Available: https://ithermai.com/#applications

[19] W. G. Jerome, "Practical guide to choosing a microscope camera," *Microscopy Today*, vol. 25, no. 5, pp. 24–29, 2017.

[20] X. Ji, Y. Cheng, Y. Zhang, K. Wang, C. Yan, W. Xu, and K. Fu, "Poltergeist: Acoustic adversarial machine learning against cameras and computer vision," in *Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP)*, 2021.

[21] Q. Jiang, X. Ji, C. Yan, Z. Xie, H. Lou, and W. Xu, "Glitchhiker: Uncovering vulnerabilities of image signal transmission with iemi," in *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*, 2023.

[22] Q. Jiang, Y. Ren, Y. Long, C. Yan, Y. Sun, X. Ji, K. Fu, and W. Xu, "Ghosttyp: The limits of using contactless electromagnetic interference to inject phantom keys into analog circuits of keyboards," in *Network and Distributed Systems Security (NDSS) Symposium*, 2024.

[23] Y. Jiang, X. Ji, K. Wang, C. Yan, R. Mitev, A.-R. Sadeghi, and W. Xu, "Wight: Wired ghost touch attack on capacitive touchscreens," in *Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP)*.

[24] C. Kasmi, J. L. Esteves, and P. Valembois, "Air-gap limitations and bypass techniques:"command and control" using smart electromagnetic interferences," in *Bot conf.*, 2015.

[25] S. C. King, "What is a ccd?" 2024. [Online]. Available: https://www.securitycameraking.com/securityinfo/what-is-a-ccd/

[26] S. Kohler, R. Baker, and I. Martinovic, "Signal Injection Attacks against CCD Image Sensors," in *Proceedings of the 2022 ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 22)*.

[27] S. Köhler, G. Lovisotto, S. Birnbach, R. Baker, and I. Martinovic, "They see me rollin': Inherent vulnerability of the rolling shutter in cmos image sensors," in *Proceedings of Annual Computer Security Applications Conference*, 2021.

[28] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP)*.

[29] L. C. Lavau, M. Suhrke, and P. Knott, "Securing temperature measurements: An assessment of sensors' vulnerability to iemi," in *2023 International Symposium on Electromagnetic Compatibility–EMC Europe*. IEEE.

[30] B. Li, Y. Li, and K. W. Eliceiri, "Dual-stream multiple instance learning network for whole slide image classification with self-supervised contrastive learning," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2021, pp. 14 318–14 328.

[31] S. Maruyama, S. Wakabayashi, and T. Mori, "Tap 'n ghost: A compilation of novel attack techniques against smartphone touchscreens," in *Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP)*.

[32] O. Moses, "Firenet: A real-time fire detection project," Github, 2019. [Online]. Available: https://github.com/OlafenwaMoses/FireNET

[33] H. Nyquist, "Certain topics in telegraph transmission theory," *Transactions of the American Institute of Electrical Engineers*, vol. 47, no. 2, pp. 617–644, 1928.

[34] A. Pahl and S. Dickmann, "Analysis of sensor disturbances caused by iemi," *https://doi. org/10.15488/12553*, pp. 159–165, 2022.

[35] C. R. Paul, R. C. Scully, and M. A. Steffka, *Introduction to electromagnetic compatibility*. John Wiley & Sons, 2022.

[36] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," *Black Hat Europe*, vol. 11, no. 2015, p. 995, 2015.

[37] Phylake1337, "Fire dataset," 2024. [Online]. Available: https://www.kaggle.com/datasets/phylake1337/fire-dataset

[38] A. Sayles, A. Hooda, M. Gupta, R. Chatterjee, and E. Fernandes, "Invisible perturbations: Physical adversarial examples exploiting the rolling shutter effect," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021.

[39] Scanbot, "Ccd barcode scanner," 2024. [Online]. Available: https://scanbot.io/glossary/ccd/

[40] Securityinformed, "Hikvision ds-2af5268n-a true day/night ptz outdoor dome camera," 2024. [Online]. Available: https://www.securityinformed.com/hikvision-ds-2af5268n-a-dome-camera-technical-details.html

[41] J. Selvaraj, "Intentional electromagnetic interference attack on sensors and actuators," Ph.D. dissertation, Iowa State University, 2018.

[42] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in *Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security*.

[43] H. Shan, B. Zhang, Z. Zhan, D. Sullivan, S. Wang, and Y. Jin, "Invisible finger: Practical electromagnetic interference attack on touchscreen-based electronic devices," in *Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP)*.

[44] SOFRADIR-EC, "Technologies for night-time video surveillance," 2023. [Online]. Available: http://www.nightvisioncameras.com/wp-nighttime-video-surveillance.html

[45] K. R. Spring, "Introduction to charge-coupled devices (ccds)." [Online]. Available: https://www.microscopyu.com/digital-imaging/introduction-to-charge-coupled-devices-ccds

[46] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. Hei, "Trick or Heat? Manipulating Critical Temperature-Based Control Systems Using Rectification Attacks," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS 19)*.

[47] J. Tufts, "Astronomical cameras," 2024. [Online]. Available: https://lco.global/spacebook/telescopes/cameras/

[48] Universeoptics, "Ccd barcode scanner technology explained," 2024. [Online]. Available: https://www.universeoptics.com/barcode-scanner-technology-explained/

[49] Vedard, "Fire detection camera." [Online]. Available: https://www.vedardsecurity.com/fire-detection-camera-p-127

[50] Verifiedmarketreports, "Global ccd camera market," 2024. [Online]. Available: https://www.verifiedmarketreports.com/product/ccd-camera-market/

[51] K. Wang, R. Mitev, C. Yan, X. Ji, A.-R. Sadeghi, and W. Xu, "Ghosttouch: Targeted attacks on touchscreens without physical touch," in *Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[52] Y. Wu, W. AbdAlmageed, and P. Natarajan, "Mantra-net: Manipulation tracing network for detection and localization of image forgeries with anomalous features," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2019, pp. 9543–9552.

[53] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudible attack on smart speakers with intentional electromagnetic interference," *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 5, pp. 2642–2650, 2021.

[54] C. Yan, H. Shin, C. Bolton, W. Xu, Y. Kim, and K. Fu, "Sok: A minimalist approach to formalizing analog sensor security," in *Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 233–248.

[55] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Def Con*, vol. 24, no. 8, p. 109, 2016.

[56] C. Yan, Z. Xu, Z. Yin, X. Ji, and W. Xu, "Rolling colors: Adversarial laser exploits against traffic light recognition," in *Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[57] Y. Yang, P. Yuhua, and L. Zhaoguang, "A fast algorithm for ycbcr to rgb conversion," *IEEE Transactions on Consumer Electronics*, vol. 53, no. 4, pp. 1490–1493, 2007.

[58] Y. Yu, "Badbarcode vulnerability," 2016. [Online]. Available: https://xlab.tencent.com/badbarcode/

[59] X. Zhang, Y. Tu, Y. Long, L. Shan, M. A. Elsaadani, K. Fu, Z. Lin, and X. Hei, "From virtual touch to tesla command: Unlocking unauthenticated control chains from smart glasses for vehicle takeover," in *Proceedings of 2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2024, pp. 201–201.

[60] H. Zhu, Z. Yu, W. Cao, N. Zhang, and X. Zhang, "Powertouch: A security objective-guided automation framework for generating wired ghost touch attacks on touchscreens," in *Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design*, 2022.

[61] A. Ziegenfuss, "Ccd camera technology: Sensors specialized for high content applications," 2012. [Online]. Available: https://assets.thermofisher.com/TFS-Assets/BID/Application-Notes/CCD_CameraTechnology.pdf

APPENDIX

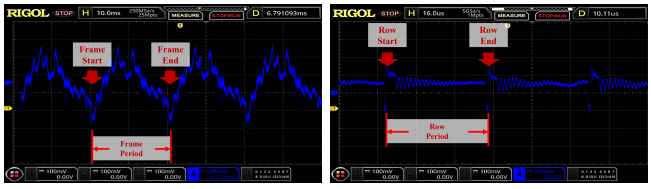
A. Electromagnetic leakage and synchronization signal

We captured the electromagnetic signals leaking from the target camera through an antenna and displayed the captured signals on an oscilloscope as shown in Fig. 17. Fig. 17(a) shows the signal presented at 10ms per cell, where the start and end of frame transmission by the camera can be observed. Fig. 17(b) shows a magnified view of the signal with a scale of 16 µs per cell, where the start and end of a single-row transmission can be clearly observed. The synchronization signal can be generated from the electromagnetic signals through simple signal processing methods such as threshold detection, as illustrated in Fig. 18.

Furthermore, to inject at the target position, a specific delay of attack signal is required. Assuming that the attacker needs to inject the target image at coordinates (x, y), with the origin at the upper left corner, the required delay can be determined by the following equation:

$$\Delta T = \left(y + \frac{x}{N_{column}}\right) * T_{row} + N * T_{frame} - T_{delay} \quad (24)$$

where T_{row} and T_{frame} represents the row and frame transmission time respectively, T_{delay} represents the hardware delay in receiving and transmitting signals. Adding the duration of N frames ensures that the total delay remains positive after subtracting the hardware delay. Once synchronized with the transmission signal, signals transmitted with a delay of Δ T would inject patterns at the target position.



(a) (b)

Fig. 17: The electromagnetic leakage of target camera recorded at (a) 10ms and (b) 16us per cell.

B. Relation between distance and power

We conduct experiments to investigate the relationship between power and distance at achieving the same injection brightness, as shown in Fig. 19. The results show that within a certain margin of error, the relationship between power and distance conforms to the results of Eq. (23).

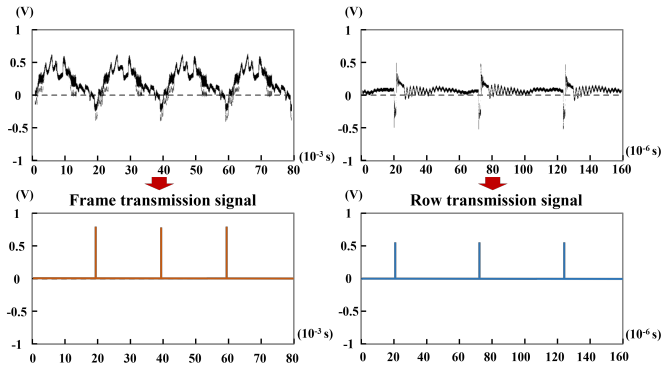


Fig. 18: The synchronization signal can be generated from the electromagnetic leakage of the target camera.

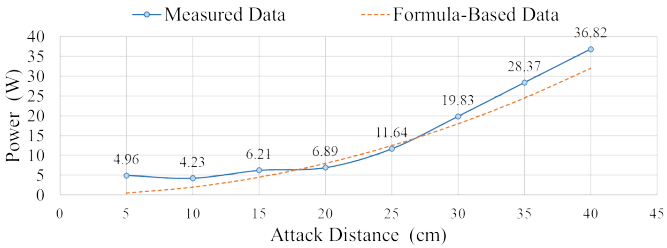
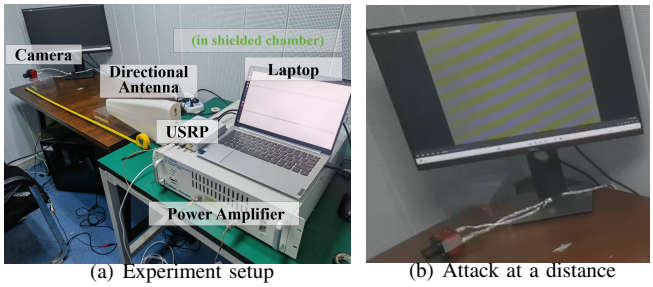


Fig. 19: The relationship between attack distance and power to achieve the same brightness.



(a) Experiment setup (b) Attack at a distance

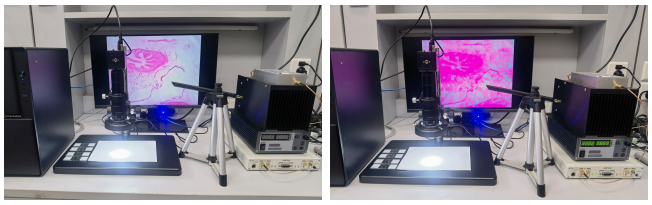
Fig. 20: Experiments to conduct an attack at a distance. The maximum attack distance reaches 1 meter by using a directional antenna.

C. Conduct attack at a distance

The attacker can increase the attack distance using high-end equipment such as directional antennas and high-gain power amplifiers. We have extended the maximum attack distance to 1 meter using a directional antenna, as shown in Fig. 20, which surpasses the distance of previous EMI attacks on cameras (0.5m in [26], 0.3m in [21]). Demos can be found on [13].

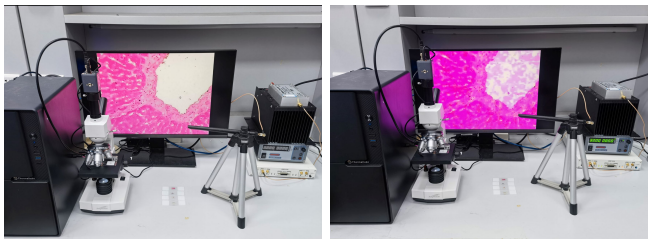
D. Test on real medical devices

We performed the attack on two types of microscopes to demonstrate the practical feasibility of the attack in real-world scenarios. Specifically, we implemented the attack on two microscopes with different magnification levels, SHL-10A and SN-BP30, both of which are applicable in real-life medical research. SHL-10A offers a maximum magnification of 135x,



(a) (b)

Fig. 21: Illustrations of SHL-10A (a) before attack and (b) after attack.



(a) (b)

Fig. 22: Illustrations of SN-BP30 (a) before attack and (b) after attack.

making it suitable for tissue-level observations, while SN-BP30 provides a magnification of 1600x, enabling cellular-level observations. Both microscopes were equipped with manufacturer-provided CCD cameras as electronic eyepieces used for recording during routine operation. To provide a clear view of the image captured by the camera in real-time, the camera was connected to a host computer that collected the images and displayed them through an LCD monitor. We successfully carried out the attack on both microscopes. As shown in Fig. 21 and Fig. 22, we successfully injected the cancer pattern designed in the medical case study into an observed kidney tissue sample.

E. User study on the noticeability of attack

To evaluate the difficulty for people to notice the attack-injected changes and to investigate the factors affecting the noticeability of the attack, we conducted a user study, which was approved by the Institutional Review Board (IRB) of our institute.

Setup: We recruited 40 participants, aged 21 to 45 years and comprised 20 males and 20 females with diverse technical backgrounds. The user study was conducted through questionnaires including images of 6 categories covered in our case studies: text, logo, cell, fire, QR code, and traffic. Each category included 2 real images and 2 images falsified by our attack. All images were displayed on the LCD monitor and photographed for fairness, where the real images were captured directly and the injected images were captured under attack. To simulate the best chances of the attacker, the injected pattern was carefully designed to match the image background and injected at a reasonable location of the image. The image orders were randomized for presentation and an attention-check question was included.

Tasks: Participants were informed that falsified images

TABLE V: The false positive rate, false negative rate, and accuracy across different cases in user study.

Cases	Metrics		
	False Positive Rate	False Negative Rate	Accuracy
Text	0.17	0.55	0.64
Logo	0.28	0.46	0.63
Cell	0.10	0.85	0.53
Fire	0.38	0.51	0.56
QR Code	0.56	0.39	0.53
Traffic	0.29	0.55	0.58
Average	0.30	0.54	0.58

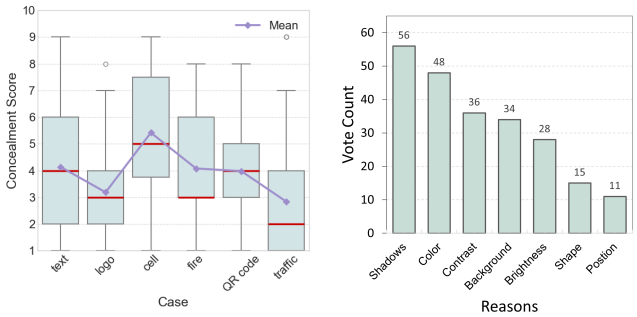
were present without knowing their total numbers and were asked to complete the following tasks: (1) *Falsification Identification*: for each image, participants were asked if they could identify whether the image had been falsified or manipulated. (2) *Concealment Assessment*: If participants identified a falsified image, they need to rate the concealment of the injected pattern on a scale of 1–10 (1 being very easy to spot, 10 being extremely difficult). (3) *Reasoning Selection*: After questions for all images were completed, participants were asked to select the primary clues for identifying falsified images.

Results: The results are presented in Table V and Fig. 23. The findings indicate that the injected cell images in the medical diagnosis scenario received the highest false negative rate of 0.85 and are the most difficult for our participants to identify. On the contrary, the injected QR codes have the lowest false negative rate of 0.39 and are the easiest to identify, though there is a high chance (0.56) that genuine QR codes can be confused with forged ones. In addition, we analyzed the reported concealment scores for the injected images across different image categories. The results in Fig. 23(a) show that participants reported the highest average concealment score of 5.42 for the injected cell images, while the reported concealment was lowest in the traffic scenario, with an average score of 2.83.

The average identification accuracy of the six image classes is 0.58, indicating that human participants can identify our injected images better than random guesses. To investigate the clues of identification, we compiled the users' votes on the reasons for identifying the falsifications. The first reason received three votes, the second received two votes, and the third received one vote. The results shown in Fig. 23(b) indicate that abnormal shadows, color, and contrast are the main reasons contributing to the identification of the injected images, where the attack could be further improved in future work.

F. Impact of shielding

We investigate the impact of various common electromagnetic shielding materials, including metal plates, fibers, sponges, and tin foil, on the attack, as illustrated in Fig. 24. The extra shielding is performed based on the intact package of the cameras. The results indicate that shielding can only mitigate rather than completely eliminate the effects of the attack. The injected brightness experiences varying degrees of attenuation due to the influence of shielding materials, while the hue



(a) (b)

Fig. 23: The result of (a) difficulty scores in recognizing the injected images and (b) the reasons for identifying the falsifications.

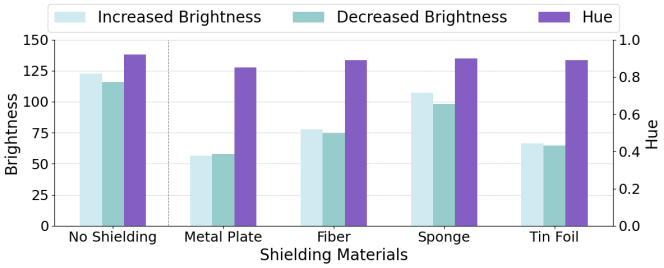


Fig. 24: Results of the impact of different shielding materials on the attack.

remains largely unaffected. Among the different materials, sponge shows the least impact on the attacks, whereas metal plates exhibit the greatest impact. While the results indicate that shielding attenuates electromagnetic signals, a complete shielding camera is challenging in practical work scenarios because CCD sensors, the target of attacks, need to be exposed to sense light properly.

G. Image forgery detection

We implemented Noiseprint and ManTraNet as defense models to detect the injected images. Noiseprint is a CNN-based deepfake detection method that leverages camera fingerprints, and ManTraNet is a unified deep neural network architecture that performs end-to-end detection and localization of image forgeries. The results are presented in Fig. 25. In Ghostshot 1 and 2, while the noiseprint and heatmap reveal distinct forged areas, the model's identified forged regions do not exactly align with the actual injected locations, leading to false detections elsewhere in images. In Ghostshot 3 and 4, the noiseprint completely failed to detect the forged areas under attack. The results of ManTraNet indicate that the attack can be detected in most cases. We also conducted a comparative experiment that applied the copy-move forgery on ground truth images in QR code scanning scenarios, which can be readily detected by both models. For ManTraNet, we observed that images injected with EMI signal not only revealed detectable areas at the injection sites but also introduced scattered detection spots throughout the rest of the image, which may result from subtle interference induced by the harmonic frequencies of the electromagnetic signals.

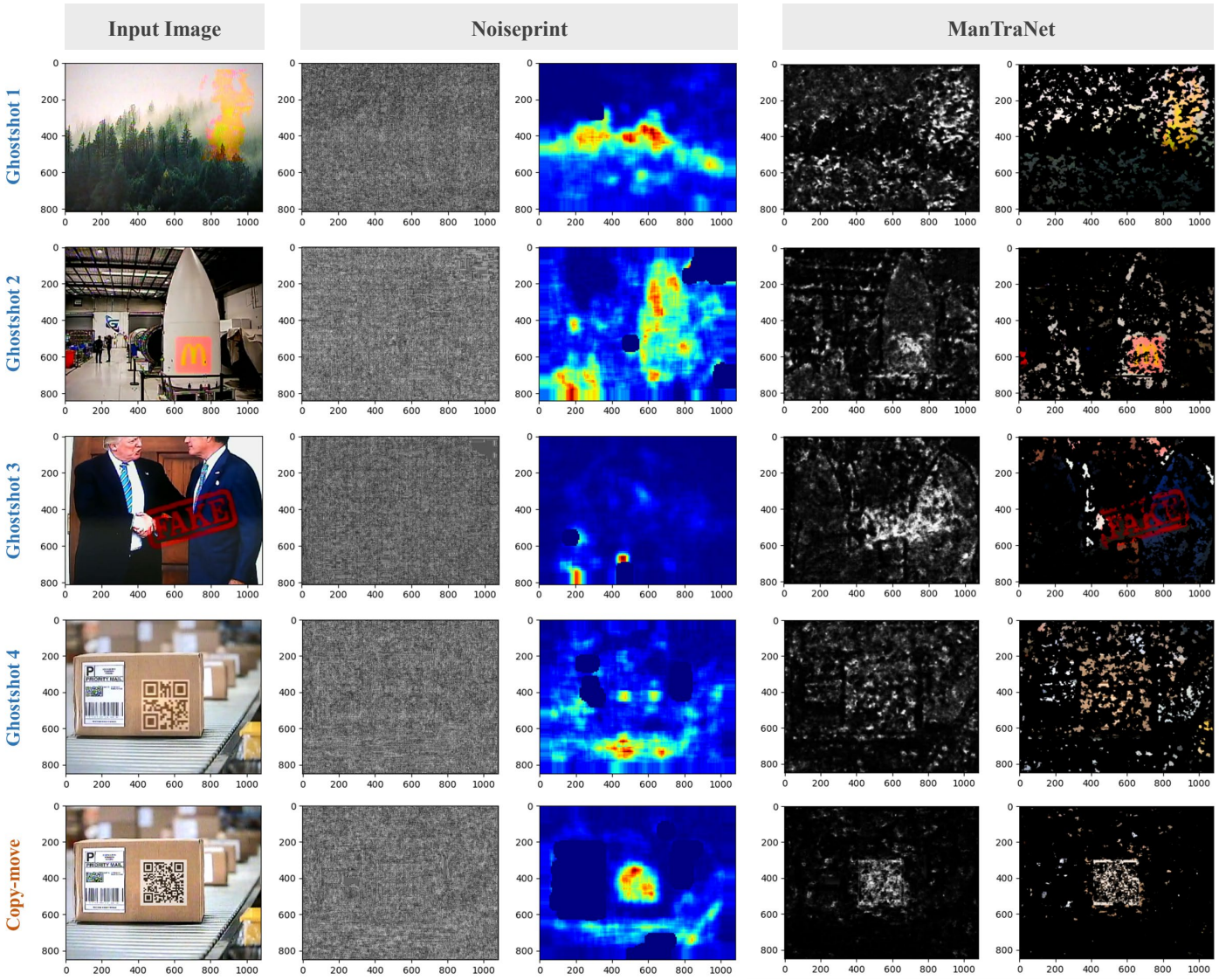


Fig. 25: The detection results of post-attack images from Noiseprint and ManTraNet. The results indicate that the attack can circumvent Noiseprint while ManTraNet could detect the attack in most cases.