TrojPix: Electromagnetic Covert Channels via Imperceptible Pixel Modulation

Guoming Zhang[1,2], Huiting Zhang[1], Zhenwei Lu[1], Heqiang Fu[1], Xin Gao[1], Riccardo Spolaor[1], Yetong Cao[1], Yanni Yang[1,2], and Pengfei Hu[1,2*]
[1]*Shandong University* [2]*Quan Cheng Laboratory*

Abstract

Air-gapped networks rely on physical isolation to prevent external connectivity. Prior electromagnetic (EM) covert channels have exploited emissions from video cables, memory buses, and CPUs, yet they rarely achieve high throughput, long range, and visual imperceptibility simultaneously, limiting practical utility in air-gapped settings. We show that imperceptible pixel modulation can deterministically induce controllable EM emissions on digital video cables, enabling control without system privileges or hardware modifications. Building on this insight, we present TrojPix, a covert channel that maintains on-screen imperceptibility while delivering high-speed, long-range communication over digital video cables. We realize a lightweight communication scheme that combines pixel-to-sample mapping with adaptive decoding, enabling sample-rate-level robust communication over extended ranges. We evaluate TrojPix across nine commercial-off-the-shelf (COTS) monitor manufacturers and fifteen COTS digital video cables under realistic conditions, demonstrating its effectiveness in two attack modes: fake screen-off and foreground embedding. TrojPix achieves a peak throughput of 8.1 Mbps and a maximum range of 208 m, revealing a practical and stealthy threat to the security of air-gapped networks.

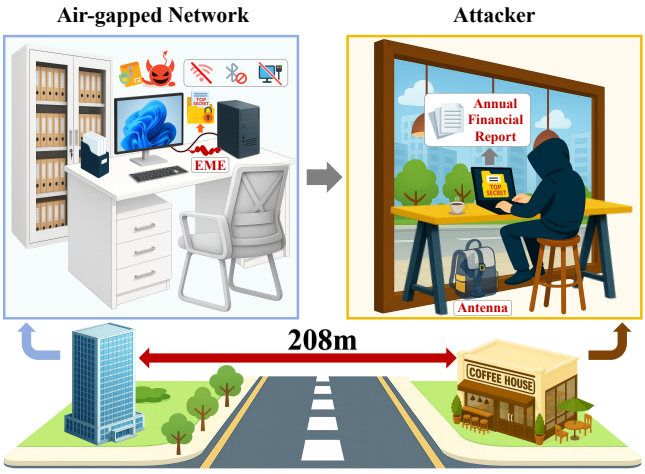


Figure 1: TrojPix exposes the risk of a novel covert communication attack against air-gapped networks, where malware introduces imperceptible pixel-level modifications that leave the on-screen content visually indistinguishable from normal display, yet induce controllable EM emissions from digital video cables. These emissions can be remotely captured by an adversary at distances of up to 208 meters.

1 Introduction

Air-gapped networks have long been considered a fundamental security problem in the defense of critical infrastructures [1–5]. By enforcing a physically isolated environment detached from external networks, they prohibit all forms of wireless communication (e.g., Wi-Fi, Bluetooth) and restrict the use of removable storage media, thereby minimizing potential data leakage vectors. Due to this strict level of isolation, air-gapped systems are widely deployed in military command centers [6], government agencies [7], financial institutions [8], and nuclear power control system [9] where strict confidentiality is paramount. However, air-gaps do not provide absolute security, as adversaries can still leverage covert channels to exfiltrate information across the isolation boundary.

Prior research has demonstrated that side-channel leakages generated during device operation can be manipulated to enable covert communication, include thermal [10], acoustic [11], ultrasonic [12], optical [13], electric power [14], magnetic [15–17], and EM [18–24]. However, most existing studies struggle to achieve balanced performance in multiple key dimensions. As shown in Tab. 1, the approaches in [10–17] fail to penetrate walls, which limits their applicability in realistic environments; the methods in [18–24] generally cannot achieve both high transmission rates and long communication distances simultaneously. The work in [21] achieved the highest data rate (up to 300 kbps), but the transmission distance was limited to only 3 meters, reducing its practical value. In

* Corresponding Author.

Table 1: Comparison of physical covert channels.

Method	Type	Leakage Source	Rate (bps)	Distance (m)	Wall Pen.
BitWhisper [10]	Thermal	CPU	0.002	0.4	×
DiskFiltration [11]	Acoustic	HDD	3	20	×
AcousticMesh [12]	Ultrasonic	Speaker	20	19.7	×
CTRL-ALT-LED [13]	Optical	LED	3.33k	9	×
PowerHammer [14]	Power	Power line	1k	2	–
ODINI [15]	Magnetic	CPU	40	1	–
Matyunin [16]	Magnetic	HDD	2	0.12	–
MagView [17]	Magnetic	CPU	8.9	0.06	–
AirHopper [18]	EM	Video cable	480	7	✓
USBee [19]	EM	USB bus	640	–	✓
GSMem [20]	EM	RAM Bus	1k	1.5	✓
BitJabber [21]	EM	DRAM	300k	3	✓
NoiseSDR [22]	EM	DRAM	2.56k	5	✓
STATn [23]	EM	GPIO	250	2.25	✓
TEMPEST-Lora [24]	EM	Video cable	21.6k	87.5	✓
TrojPix (Ours)	EM	Video cable	**8.1M**	**208**	✓

contrast, the work in [24] demonstrated the longest communication distance (87.5 meters), but the rate was only 21.6 kbps. In addition, most schemes neglect visual imperceptibility. For example, in [24], the communication process can be easily detected visually, leading to poor stealth. Overall, existing techniques fail to simultaneously deliver high throughput and long-range communication and lack effective integration of visual stealth, which severely limits their deployment and applicability in air-gapped environments.

In this paper, we present TrojPix, the first system that achieves visually imperceptible covert communication by exploiting EM emissions from digital video cables. By applying subtle pixel modulations that remain invisible to the human eye yet induce controllable EM emission, TrojPix turns commodity video cables into unintended antennas, enabling through-wall communication with a peak rate of 8.1 Mbps and a maximum transmission range of 208 m. To achieve TrojPix, we need to address three major challenges.

1) How can imperceptible pixel modifications yield controllable EM emissions? A central challenge for video-based covert communication is achieving reliable receiver-side detectability while remaining imperceptible to the human eye. By analyzing the video transmission process, we demonstrate that modification to pixel values alters the Transition-Minimized Differential Signaling (TMDS) symbolization, inducing controllable EM emissions along video cables. By characterizing the coupling between pixel values and emission intensity, we enable software-defined control that effectively balances visual imperceptibility with demodulation robustness, establishing the foundation for software-defined EM covert communication over standard digital video cables.

2) How to achieve high-speed communication? Achieving sampling-rate-level throughput requires efficient recovery of digital information from EM emissions. We therefore propose Pixel-to-Sample Mapping (P2S-Map), which establishes a precise correspondence between two-dimensional pixel blocks and one-dimensional sampling instants. Pixels of video frames are partitioned into content-adaptive blocks at the transmitter side, and each block is modulated with subtle modifications, producing distinct intensity features in the time domain. This approach enables data transmission rates approaching the receiver's sampling rate, with synchronization supported by matched-filter correlation(MFC) and preamble detection, followed by peak detection and clock alignment to ensure robust decoding, even in the presence of timing jitter.

3) How to extend the attack range while maintaining communication quality? Increasing distance leads to severe path loss and multipath fading, which significantly reduces the signal-to-noise ratio (SNR). To address this challenge, we integrate robust front-end gain, precise synchronization, and distortion-tolerant decoding. Low-noise amplification (LNA) and band-pass filtering boost in-band energy at the receiver side, while multi-band sampling and fusion further improve performance. Robustness is reinforced through cross-row resilience coding (CRRC) to mitigate burst errors, and apply an adaptive decision threshold (ADT) aligned with channel conditions to stabilize information recovery under SNR fluctuations. Collectively, these mechanisms strengthen channel robustness and counteract range-induced degradation, enabling reliable communication over significantly longer distances.

In summary, our contributions are as follows:

- We present TrojPix, the first visually imperceptible, high-speed covert channel attack that exploits controllable EM emissions through pixel modulation.
- We formulate controllable EM emissions as constrained modulation problem and introduce P2S-Map, which enables sample-rate-level transmission and incorporates synchronization with adaptive decoding, thereby achieving robust long-range covert communication.
- We systematically evaluate TrojPix across nine COTS monitor manufacturers and fifteen COTS digital video cables, demonstrating its practicality in real-world settings. Experimental results show that TrojPix achieves a peak rate of up to 8.1 Mbps, and a maximum transmission range of 208 m.

The paper is organized as follows. Section 2 introduces background information. Section 3 conducts feasibility analysis. Section 4 explains the threat model. Section 5 presents the design plan for TrojPix. Section 6 evaluates TrojPix. Section 7 discusses the defense measures and future work. Section 8 introduces the relevant work, and concludes in Section 9.

2 Background

2.1 Fully-Digital Radios

Conventional Software-Defined Radio (SDR) has made wireless communication more flexible [25]: protocols and waveforms can be determined by software rather than relying on

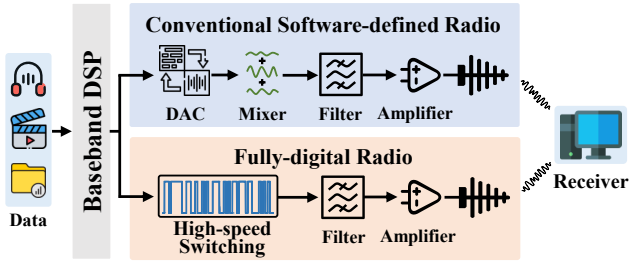


Figure 2: Principle of different radio architectures.

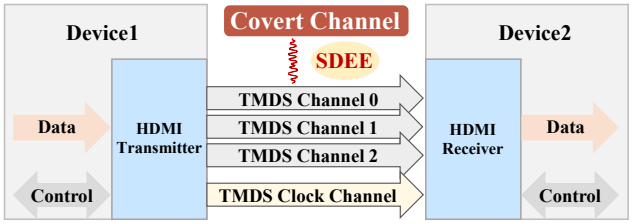


Figure 3: TMDS channel structure.

fixed-function hardware. As shown in the upper part of Fig. 2, the baseband signal is first converted into an analog waveform by a Digital-to-Analog Converter (DAC), then passed through a mixer, filter, and amplifier, before being transmitted through an antenna to the receiver. However, SDR still requires analog components in the signal transmission process. These components not only increase system complexity, but also make it difficult to achieve high integration and cross-platform reuse.

To address this issue, Fully Digital Radio (FDR) has emerged [26]. Its core principle is to perform signal generation primarily in the digital domain, avoiding additional analog modules. Specifically, as shown in the lower part of Fig. 2, it approximates the desired continuous waveform through a sequence of high-speed binary signal switches and achieves modulation of amplitude, frequency, and phase by controlling duty cycle, period, and edge timing. After simple filtering, these binary sequences can produce the desired RF signals in the target frequency band. This approach brings an important insight: any interface capable of producing high-speed binary signals can essentially serve as a programmable RF source.

2.2 Software-Defined EM Emissions

The insights of FDR extend beyond the communication devices themselves. In fact, the vast majority of high-speed digital interfaces in modern electronic systems—whether buses, memory, or peripheral connections—generate EM leakage during operation. These leaks were previously regarded as unintended side effects, but according to Maxwell's equations, time-varying currents inevitably accompany EM emission. Therefore, these leakage signals inherently possess the same "emission" properties. Based on this, researchers have proposed the concept of Software-Defined Electromagnetic Emission (SDEE) [27]. Unlike FDR, which relies on dedicated binary switching circuits to generate radio signals, SDEE treats the unintended EM leakage generated by any device during operation as a programmable communication channel. Within this framework, software not only determines the device's surface-level behavior (e.g., computation or display) but also indirectly shapes its detectable EM characteristics. By carefully modulating digital sequences, the resulting leakage can be leveraged to realize covert transmission.

2.3 EM Leakage of Digital Video Cable

In this context, the EM leakage of video transmission cables becomes a typical example of SDEE. Taking HDMI as an example, its principle is to transmit uncompressed digital video over a single physical link via high-speed serial transmission. The core mechanism is based on TMDS [28], as shown in Fig. 3, where three independent differential pairs continuously carry pixel data at extremely high rates. At the transmitter, the color information for each pixel is encoded in TMDS to optimize the DC balance and reduce EM interference, and then sent as differential signals. On the receiver side, clock recovery, serial-to-parallel conversion, and TMDS decoding are performed to reconstruct the original pixel data stream.

However, according to EM field theory, any high-speed switching current inevitably induces EM radiation along the transmission line. During such high-speed transmission, the digital video cable can unintentionally act as an antenna, radiating part of the information into the surrounding space, thereby offering attackers a potential channel for unauthorized access. From the perspective of SDEE, this implies that a digital video cable is not only a transmission medium but also a programmable EM emitter, whose radiation patterns are directly shaped by pixel arrangements and brightness variations. In other words, while the video stream renders images on the screen, it simultaneously "modulates" the external EM space. This property opens up new possibilities for attackers: by deliberately crafting the video content, they can re-purpose these leakage signals as a covert communication channel—without degrading the user's viewing experience—to achieve cross-device information transmission.

3 Feasibility Analysis

Imperceptible Display Modifications. To explore whether modifications to the displayed content can influence the unintentional EM emissions of digital video cable, and whether such emissions can be distinguished under slight, visually imperceptible changes to the content, we conduct a preliminary experiment. In the experiment, a near-field magnetic probe is used to capture EM radiation signals generated during screen data transmission. Comparative tests are carried out by adjusting the brightness of pixels in specific screen regions. The display operates at a 60 Hz refresh rate with a resolution of

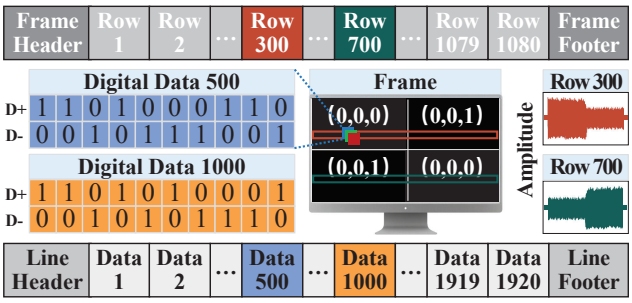


Figure 4: Illustration of EM signal variations induced by pixel modifications.

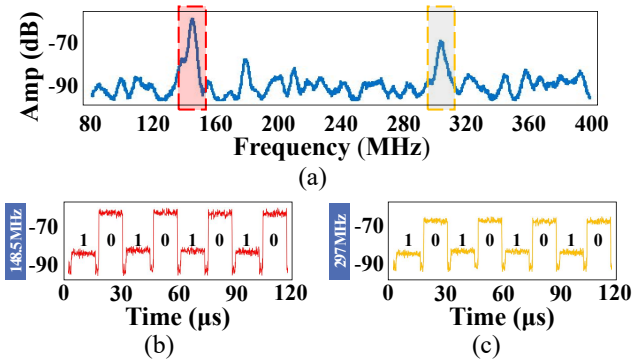


Figure 5: Demonstration of covert information transmission on different frequency bands.

1920×1080, and TMDS encoding is employed to convert each 8-bit pixel component into 10-bit symbols for transmission.

As shown in Fig. 4, we only modify the least significant bit of the blue channel within the boxed rectangular region of the screen. This change has almost no perceptible impact on the visual output. However, signals captured by the oscilloscope still reveal differences in EM emissions across both identical and different rows, thereby confirming that such visually imperceptible pixel modifications are detectable at the EM signal level.

Bit Transmission. To further evaluate the feasibility of achieving bit-level covert transmission by manipulating EM emmisions from digital video cables, we analyze both the spectral and temporal characteristics of the leaked signals. In our experiments, the display renders an image with a resolution of 1920×1080, and only the least significant bit of the blue channel in the pixel values of partial data blocks is modified. As shown in Fig. 5(a), the corresponding EM spectrum exhibits spectral peak at the fundamental (148.5 MHz) and its second harmonic (297 MHz).

We extract the time-domain waveforms corresponding to the two bands, as shown in Fig.5(b) and Fig.5(c), the alternating binary sequence "10101010" is clearly visible in both bands. This observation indicates that during the display row scanning, subtle variations induce distinct differences in EM emission intensity, enabling discrimination between binary "0" and "1." Notably, this signature is evident not only at the fundamental frequency but also at its harmonic bands.

The above results confirm that by correlating pixel patterns with the EM emissions generated by digital video cables, it is possible to achieve stable covert communication without introducing any perceptible visual changes. In Section 5, we will elaborate on the principles and implementation mechanisms of covert communication based on pixel modulation.

4 Threat Model

This paper investigates the covert communication scenario shown in Fig. 1. The attacker's goal is to steal sensitive data from an air-gapped network. Specifically, we assume the following scenario and attacker capability:

Emission Source. The victim's computer operates in a high-security environment with all communication interfaces disabled. Its display remains on and is connected to at least one digital video cable.

Attacker Capability. We assume that the attacker implants malware carrying TrojPix onto the victim's computer. This malware operates solely in user mode, requiring neither system privileges, administrator rights, nor direct access to peripherals. The software scans the computer in the background to locate confidential files. It can obtain the resolution of the victim's monitor, then generate a visually camouflaged attack video and play it secretly to construct a covert channel. Meanwhile, the attacker uses a set of commercial radio devices to receive EM signals from a distance or outside the room and reconstruct the information at the computer terminal.

Scenario 1: Fake Screen-Off Mode. The malware can force the display into a disguised "screen-off" state, presenting a black screen or a visually similar interface to an actual shutdown, nearly indistinguishable from a genuine standby state. From the user's perspective, the monitor appears to be turned off, but in reality, the digital video cable continues to conduct covert data transmission. Once user interaction (e.g., mouse movement) is detected, the screen instantly resumes, and the transmission is immediately halted, thereby minimizing the likelihood of user detection.

Scenario 2: Foreground Embedding Mode. The malware embeds covert information in real time into the current display content while running in the background, and this method is applicable to any image. It achieves modulation through subtle pixel-level modifications or color adjustments that are visually indistinguishable, ensuring that the user perceives no anomalies during normal usage. Once user interaction is detected, the transmission is immediately terminated to guarantee that the screen display fully matches the user's perception, further reducing the risk of exposure.

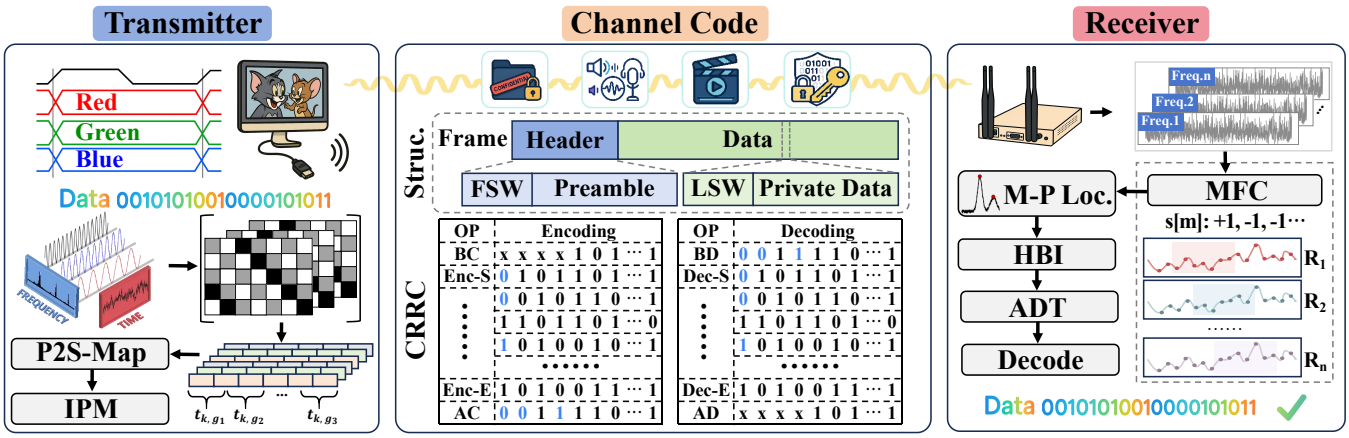


Figure 6: The overview of TrojPix.

5 Design

In this section, we present the system architecture of TrojPix. Fig. 6 provides an overview of our system and its modules. In what follows, we introduce the three modules that comprise transmitter design, frame structure and coding, and receiver design in convert communication.

5.1 Transmitter Design

5.1.1 TMDS Bitstream and Spectral Characteristics

In a TMDS-based digital cable transmission, each pixel is mapped to three color channels, and each channel carries a n_b-bit word. The bit period is $t_b = 1/xyfn_b = t_p/n_b$, where x and y denote horizontal and vertical resolutions, f is the refresh rate, n_b is the number of bits per pixel per channel, and t_p is the pixel period.

For a single channel, the serialized TMDS words form a bitstream. Let $c_k \in \{0,1\}$ denote the k-th transmitted bit, i.e., the binary digit obtained by serializing the pixel words. The emitted voltage can be written as

$$\hat{v}(t) = \sum_{k=-\infty}^{\infty} c_k\, b(t - kt_b) = c(t)\, X_{t_b}(t), \tag{1}$$

where $b(t)$ is the unit-bit pulse. The bit sequence can be further expressed using a Dirac comb representation. Define the Dirac comb [29], and we obtain the convolution form

$$\hat{v}(t) = b(t) * \big[c(t)\, X_{t_b}(t)\big]. \tag{2}$$

Taking the Fourier transform and using the convolution–multiplication duality yields

$$\mathcal{F}\{\hat{v}\}(f) = B(f)\,\Big[C(f) * \mathcal{F}\{X_{t_b}\}(f)\Big]. \tag{3}$$

By the transform property of the Dirac comb, $\mathcal{F}\{X_{t_b}\}(f) = 1/t_b X_{1/t_b}(f)$, and therefore

$$\mathcal{F}\{\hat{v}\}(f) = \frac{1}{t_b} B(f) \cdot \Big[C(f) * X_{1/t_b}(f)\Big]. \tag{4}$$

The spectrum thus consists of periodic replicas spaced by $1/t_b$. Compared with per-pixel modulation, resolving individual bits requires a n_b times higher bandwidth. Consequently, the sampling frequency must satisfy $f_s \geq 1/2t_b = n_b/2t_p$. However, in many practical receivers, the effective sampling is closer to $f_s \gtrsim 1/2t_p$, which acts as a low-pass filter of the TMDS waveform: individual bits cannot be resolved, and only the *per-pixel average* is preserved. Importantly, because different colors correspond to different TMDS bit patterns, these averages still retain substantial, recognizable information.

5.1.2 Pixel Period and Modulation Window

To achieve active control of EM radiation, precise temporal modulation must be coordinated at the granularity of individual pixels. We define the pixel period $t_\mathrm{p} = 1/f_p$ and frame period as $t_\mathrm{r} = 1/f_r$, where f_p is the cable's pixel clock and f_r is the frame rate. The modulation is confined to the effective area (EA) region, with no modulation taking place in the inactive area (IA). For pixel m in row k, denote the unit rectangular pixel pulse by $p(\cdot)$ and the row period by T_row. Then the pixel pulse train under gating is

$$\begin{aligned} s(t) \;&= \chi_{\mathrm{EA}}(t) \sum_{k=1}^{Y} \sum_{m=1}^{X} a_{k,m}\, p\big(t - t_f - (k-1)t_\mathrm{r} - (m-1)t_\mathrm{p}\big) \\ &\quad + \chi_{IA}(t)\, s_{IA}(t), \end{aligned} \tag{5}$$

where $a_{k,m}$ denotes the pixel modulation coefficient and t_f is the start time of EA; $\chi_{\mathrm{EA}}(t) \in \{0,1\}$ is the EA gate, $\chi_{IA}(t) = 1 - \chi_{\mathrm{EA}}(t)$ its complement for the IA, and $s_{IA}(t)$ is the baseline waveform during blanking.

The effective modulation window is written as

$$s_e(t) = \alpha \eta_{\mathrm{code}}\, \beta\, \chi_{\mathrm{EA}}(t), \tag{6}$$

where α denotes the fraction of the EA period used for signal modulation, η_{code} denotes the coding efficiency (ratio of useful bits to transmitted bits), and β represents the magnitude constraint factor imposed by visual perception limits.

5.1.3 Pixel-Sample Mapping

To allocate time at the sample granularity, let F_s be the receiver sampling rate and let each symbol span S_{sys} samples (a DSSS-like spreading factor [30], chosen by the channel conditions). Define the ideal number of pixels per symbol

$$\pi_{\text{sym}} = \frac{S_{\text{sys}} F_{\text{PIX}}}{F_s}, \tag{7}$$

where F_{PIX} is the pixel clock. With F_s fixed, a larger S_{sys} yields a wider per-symbol pixel span, increasing processing gain and interference tolerance at the expense of a lower symbol rate.

For a precise pixel-sample mapping, we introduce a non-decreasing sequence of pixel-edge indices $\{C_g\}_{g\geq 0}$, where C_g is the starting pixel index of symbol g in the 1-D scan order (row-major). The set of pixel for symbol g is $X_{\text{sym}}(g) = \{\, x \mid C_g \leq x < C_{g+1} \,\}$, so $|X_{\text{sym}}(g)| \approx \pi_{\text{sym}}$. Therefore, the duration time of the symbol cells is $t_{k,g} = (C_{g+1} - C_g)\, T_{\text{clk}} \;\approx\; S_{\text{sys}}/F_s$. This formalization divides the continuous pixels into symbol cells of approximately equal value.

This structure provides a controllable trade-off between gain and throughput, and allows the symbol rate to scale proportionally to F_s when other parameters are fixed.

5.1.4 Imperceptible Pixel Modulations

Depending on the prevailing channel conditions and the specific transmission requirements, we employ different channel coding strategies, a small modification δ is added to the selected pixels, as elaborated in the following.

a) Intra–Row OOK Modulation. To change the emitted EM power while preserving visual quality, we apply a small same-polarity modification to all pixels within a symbol window, i.e., on the pixel set $X_{\text{sym}}(g)$ mapped from bit $b_g \in \{0,1\}$. For an 8-bit grayscale, let $L^{(0)}_{k,m} \in [0,255]$ be the original pixel value and $\delta > 0$ the modification step; we define

$$L^{(1)}_{k,m} = \begin{cases} \text{clip}\big(L^{(0)}_{k,m} + \delta\big), & b_g = 1,\ (k,m) \in X_{\text{sym}}(g), \\ L^{(0)}_{k,m}, & b_g = 0, \end{cases} \tag{8}$$

where $\text{clip}(\cdot)$ limits the value to the display range. Under high-speed row scanning, the $\pm\delta$ luminance changes within the window translate into a measurable intensity difference in the radiated waveform, producing a "symbol–to–radiation strength" mapping.

b) Inter–Row Differencing. For long-range links and image conditions with pronounced intensity variations, we further introduce inter–row differencing to reduce visual artifacts and increase radiated power. Neighboring rows are paired as $(2u,\, 2u+1)$; within the same symbol window we apply opposite polarities so that visual energy cancels while RF energy adds coherently. With a row participation flag $v_m \in \{0,1\}$,

$$(L^{(1)}_{2u,m}, L^{(1)}_{2u+1,m}) = \begin{cases} \Big(\text{clip}(L^{(0)}_{2u,m} + \delta v_m),\ \text{clip}(L^{(0)}_{2u+1,m} - \delta v_m)\Big), & b_g = 1, \\ (L^{(0)}_{2u,m}, L^{(0)}_{2u+1,m}), & b_g = 0. \end{cases} \tag{9}$$

where $m \in X_{\text{sym}}(g)$. Due to the limited sensitivity of the display pipeline to high-frequency content in the vertical direction, modifications applied to adjacent rows, which are spatially proximate, effectively cancel in the perceptual domain. This cancellation enables further amplification of the emitted power while preserving visual imperceptibility.

5.2 Frame Structure and Coding

During covert transmission, the video emission is highly susceptible to sudden disturbances such as display jitter, occlusion, and radio-frequency interference, which can cause substantial channel variations and may even lead to the loss or severe corruption of entire pixel rows. Such errors typically occur in bursts rather than independently. To enhance robustness and mitigate row-level impairments, the transmitter employs a CRRC scheme, with corresponding decoding performed at the receiver. By dispersing burst errors into isolated symbol errors, CRRC significantly reduces the burden of error correction, thereby improving transmission reliability and link resilience.

5.2.1 Frame Structure

Each communication frame is organized into two main components: the **Header** and the **Data** section.

- **Header:** The header provides essential control information for reliable reception. It includes a frame synchronization window (FSW) and a preamble that encodes the frame identifier and serves as a known reference for synchronization and threshold initialization.
- **Data:** The data section carries the effective payload. It begins with the line synchronization window (LSW), followed by the private data field that encodes the user's confidential information.

5.2.2 Channel Modeling

We represent the valid payload transmitted over the digital video cable as a binary sequence of length n, $c = [c_0, c_1, \ldots, c_{n-1}] \in \{0,1\}^n$. Line interference is modeled as

a burst-error vector e, which produces the received sequence.

$$r = c \oplus e, \qquad e = [0,\ldots,0,\underbrace{1,\ldots,1}_{W},0,\ldots,0], \tag{10}$$

where W denotes the length of the burst and the burst begins at the index ℓ. If the entire row is corrupted, then $W = n$.

To capture the characteristics of burst errors, we adopt the *Gilbert–Elliott (GE)* channel model [31,32]. The channel state $C(t) \in \{G,B\}$ alternates between "good" and "bad" states with symbol error rates $p_g \ll p_b$, and transition probabilities $\Pr(G \to B) = \alpha, \Pr(B \to G) = \beta$. In the bad state, contiguous errors of length W occur, thereby modeling line interference as a row-level manifestation of the GE burst channel. When interleaving is applied, burst errors are dispersed across different codewords; for an interleaver with span x, the resulting *effective* error rate can be approximated as $p' \approx \frac{1}{x}\sum_{\ell=0}^{x-1} p_\ell$, where p_ℓ denotes the residual error probability in the ℓ-th interleaved position.

5.2.3 Coding and Interleaving

Following the channel model described above, we now introduce coding and interleaving techniques to enhance robustness against burst errors. The input bitstream is first partitioned into blocks of length k, denoted by $\{m_i\}$. Each block is then encoded into a codeword of length n bits:

$$c_i = \mathrm{Enc}(m_i) \in \{0,1\}^n, R_c = k/n. \tag{11}$$

To prevent a single-line burst from corrupting an entire codeword, we introduce an interline interleaving strategy, where the j-th coded symbol of codeword i is mapped onto the row index

$$\mathrm{Ip}_i(j) = \big(r_0(i) + j \cdot \chi\big) \bmod H. \tag{12}$$

Here, H represents the number of encoded rows, χ is the row-stride of the interleaver, and $r_0(i)$ is a per-codeword seed. In this way, adjacent bits of a codeword are not placed on the same line but are dispersed across different lines. The transmitted sequence is the permuted stream $y_s = \pi(c_0, c_1, \ldots, c_M)$, where $\pi(\cdot)$ denotes the interleaving operation.

5.2.4 Error Dispersion and Recoverability

In a progressive-row video channel, a burst disturbance spanning B continuous pixel corrupts all transmitted symbols on those lines. For any encoded codeword c_i, the *worst-case* number of symbols corrupted after interleaving is upper bounded by $E_{\max}(B,\chi) \le \lceil B/\chi \rceil$, where χ denotes the interleaver span. Hence, by ensuring $\chi \ge \lceil B/t \rceil$, the system guarantees that, even under a burst affecting B consecutive lines, the number of corrupted symbols per codeword remains bounded by the channel decoder's correction capability t.

Consequently, the probability of successful recovery can be lower-bounded as $P_{\mathrm{succ}} \ge \sum_{i=0}^{t} \binom{n}{i} (p')^i (1-p')^{n-i}$, where p' denotes the effective symbol error rate of the Gilbert–Elliott channel after interleaving.

5.3 Receiver Design.

5.3.1 Multi-Band Sampling and Fusion

To complement the transmitter-side design, the receiver performs band-wise demodulation and then fuses per-band evidence using channel-aware weights estimated from per-band SNR and preamble correlation.

Consider the g-th symbol window. Let X_g denote the set of pixel indices within the window, $q_g[m,n] \in \{+1,-1\}$ the demodulation mask aligned with the transmitter, and $I_k[m,n]$ the recovered pixel value at location (m,n) from the k-th subband. The per-band coherent accumulation statistic is

$$z_{g,k} \;=\; \frac{1}{|X_g|} \sum_{(m,n)\in X_g} q_g[m,n]\, I_k[m,n], \tag{13}$$

where $z_g \;=\; [z_{g,1},\ldots,z_{g,K}]^\top$. Let $w = [w_1,\ldots,w_K]^\top$ denote nonnegative reliability weights derived from SNR and preamble correlation estimates. Cross-band linear fusion then yields the combined statistic

$$Z_g \;=\; \sum_{k=1}^{K} w_k\, z_{g,k} \;=\; w^\top z_g. \tag{14}$$

5.3.2 Matched-Filter Correlation

In high–speed video covert communication, a loss of row/frame synchronization can catastrophically corrupt symbol decisions (e.g., entire rows of pixels). Therefore, we require a synchronization method that remains reliable under noise, texture, multipath, and strong jitter.

Let the known template sequence be a bipolar template $s[m] \in \{-1,+1\}$ of length L, and let $r[n]$ be the received sequence. The matched–filter correlation at lag n is

$$R[n] \;=\; \sum_{m=0}^{L-1} r[n+m]\; s^*[m]. \tag{15}$$

where $(\cdot)^*$ denotes complex conjugation.

To remove channel–gain variations, video–brightness drift, and row–to–row amplitude mismatch, we adopt the normalized cross–correlation [33]

$$\widehat{R}[n] \;=\; \frac{\left| s^H r_n \right|}{\|s\|_2\, \|r_n\|_2} \;\in\; [0,1], \tag{16}$$

where $r_n \triangleq \big[r[n],\ldots,r[n+L-1]\big]^T$. $\widehat{R}[n]$ closer to 1 indicates that the received signal closely matches the template at that position, whereas values closer to 0 indicate a complete mismatch. Thus, the candidate synchronization index is chosen as

the Maximum Peak Location $n_{\max} = \arg\max_n \widehat{R}[n]$. To reject spurious peaks caused by image texture or multipath, we introduce a peak–sharpness gate based on a peak–to–secondary ratio together with a double–threshold rule:

$$\gamma = \frac{\widehat{R}[n_{\max}]}{\max\limits_{n \neq n_{\max}} \widehat{R}[n]}, \qquad \widehat{R}[n_{\max}] \geq \tau_r, \ \ \gamma \geq \gamma_{\text{th}}. \tag{17}$$

Here, τ_r controls the absolute peak height (match confidence), while γ_{th} controls the sharpness of the mainlobe with respect to neighboring sidelobes.

5.3.3 HBI–Aware Row Boundary Detection.

With progressive scanning of the digital video cable, the w segments immediately preceding a row boundary c typically lie in the horizontal IA, whereas the subsequent w segments belong to the EA. Define the forward and backward windows $\mathcal{W}_+(c) = \{c, c+1, \ldots, c+w-1\}$ and $\mathcal{W}_-(c) = \{c-w, \ldots, c-1\}$, and let $h_m \geq 0$ denote a symmetric window function applied to suppress edge ringing. Denote by $r[\cdot]$ the in-segment statistic; the corresponding windowed energies are given by

$$E_+(c) = \sum_{m=0}^{w-1} h_m \left| r[c+m] \right|^2, \tag{18a}$$

$$E_-(c) = \sum_{m=0}^{w-1} h_m \left| r[c-1-m] \right|^2. \tag{18b}$$

Let σ_{gap} denote the noise estimated within IA. We then construct a composite statistic that integrates a standardized energy gap with an energy ratio, incorporating a small stabilizing term $\lambda > 0$:

$$\ln \beta(c) \ = \ 2 \ln \left(\frac{\left| E_+(c) - E_-(c) \right|}{\sigma_{\text{gap}} \sqrt{\sum\limits_{m=0}^{w-1} h_m^2}} \right) + \alpha \ln\left(\frac{E_+(c)+\lambda}{E_-(c)+\lambda} \right) \ \geq \ \ln \beta_{\text{th}}. \tag{19}$$

The threshold β_{th} is set from the empirical distribution of *IA–only* statistics; when $\beta(c) \geq \beta_{\text{th}}$, the following w segments are declared to belong to the AE. The forward window is anchored in IA as background; the Hann window h_m suppresses boundary ringing. The parameters α and β_{th} are adapted to the estimated SNR.

5.3.4 Adaptive Decision Threshold

Since each frame in our covert channel begins with a known pilot, we leverage this segment to adaptively estimate the decision threshold. This design choice is motivated by the low-SNR and long-range operating regime, where a fixed threshold would lead to severe performance degradation. By exploiting the statistics of the preamble symbols, ADT dynamically selects and updates the threshold, significantly improving decoding robustness while preserving the lightweight nature of the receiver.

Specifically, by scanning candidate thresholds on the pilot symbols, the optimal threshold $T^\star$ is selected by minimizing the preamble bit-error rate. To suppress slow drift, the online threshold $T_t = (1-\alpha)T_{t-1} + \alpha T^\star$ can be exponentially smoothed. The decision polarity is determined from the preamble orientation statistic, denoted as flag $\in \{+1, -1\}$, and v_i represents the decision statistic (e.g., the fused metric z_g) for the i-th symbol.

For the data segment, symbol decisions are obtained as

$$\hat{b}_i = \mathbf{1}\{ \text{flag} \cdot (v_i - T_t) > 0 \}, \tag{20}$$

where $\mathbf{1}\{\cdot\}$ is the indicator function. The estimated bit sequence is then de-interleaved and FEC-decoded (Forward Error Correction):

$$\hat{m} = \text{Decode}\big(\text{DeInterleave}(\hat{b})\big). \tag{21}$$

By explicitly minimizing $\text{BER}_{\text{p}}(T)$ in the preamble symbol, ADT adaptively selects the threshold $T^\star$ and applies it to subsequent transmitted data, thus significantly improving the decision margin and recovery performance under low SNR or long-range conditions.

6 Evaluation

In this section, we provide a detailed introduction to the experimental setup, evaluation metrics, and the impact performance of TrojPix in the real world and various influencing factors.

6.1 Experimental Setup

As shown in Fig. 7, we demonstrate the covert communication process of TrojPix in real-world scenarios. The transmitter employs a monitor connected via a video cable to play the attack video. The receiver's acquisition system consists of a USRP X310 device equipped with a UBX-160 daughterboard. A TFN W3 directional antenna is used for signal collection in the real environment. A FOSTTEK FST-RFAMP 09 LNA is used to enhance signal quality. The sampling rate is set to 10 MHz. The encoding and decoding of covert communication information are implemented using Python 3.10.9.

6.2 Metrics

- **Bit Correct Rate (BCR).** To assess the accuracy of the covert channel, we adopt the BCR, defined as the proportion of correctly recovered bits at the receiver. BCR provides a direct measure of the reliability of covert communication. Unless otherwise specified, all BCR values in the evaluation are computed on the raw bitstream; error-corrected results are reported explicitly when used.

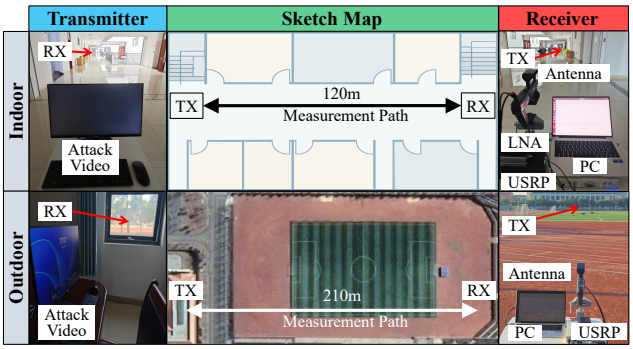


Figure 7: Attack scenarios in real-world settings. Left: monitor displaying the embedded attack video. Right: SDR-based receiver setup. The experiments are conducted and evaluated in both indoor and outdoor environments.

- **Signal-to-Noise Ratio (SNR).** We evaluate covert channel quality via PSD-based SNR using Welch's method [34], and the occupied bandwidth B is identified. The in-band power is P_{total}, while the noise power is approximated as $P_n = N_0 \cdot B$ from adjacent out-of-band regions. Thus, the signal power is $P_s = P_{\text{total}} - P_n$, and the SNR in dB is $\text{SNR}_{\text{dB}} = 10\log_{10}(P_s/P_n)$.
- **Structure Similarity Index Measure (SSIM).** To evaluate image similarity [35], we adopt SSIM, which jointly compares luminance, contrast, and structural information between two images. A higher SSIM value indicates greater perceptual similarity.
- **Learned Perceptual Image Patch Similarity (LPIPS).** To assess perceptual similarity between the embedded and original images, we adopt LPIPS [36], which measures their perceptual distance. Lower LPIPS values indicate closer perceptual alignment between the generated and reference images.

6.3 Experimental Results

6.3.1 Impact of Different Video Cables

To evaluate the impact of cable manufacturer and length on TrojPix, we test 15 COTS digital video cables from multiple manufacturers, including UGREEN, SAMZHE, HP, CHOSEAL, JIANGDUN, JINGHUA, PHILIPS, and DELL, covering six common lengths (0.5 m, 1 m, 1.5 m, 2 m, 3 m, and 5 m). We evaluate on Dell U2417H monitor fixed at 1920×1080 resolution and 60 Hz refresh rate, while the receiving antenna is positioned 20 meters from the target.

Tab. 2 reports the performance of TrojPix across different cable manufacturers and lengths. The average BCR reaches 99.20% across all cables, with an average SNR of 15.99 dB. After applying FEC, the BCR improves to 100% on all tested cables. At the same length, differences among manufacturers are minor; for instance, at 1 m, Choseal achieves the highest BCR (99.18%), while HP is slightly lower (99.10%). Within a single manufacturer (e.g., UGREEN), the BCR increases with cable length, reaching 99.60% at 5 m. In general, the SNR values remain comparable under all conditions, demonstrating that TrojPix consistently delivers stable and robust performance across different cable manufacturers and lengths.

Table 2: Impact of different video cables.

Manuf.	Length	BCR	SNR (dB)
SAMZHE	0.5m	99.08%	15.77
	1m	99.12%	15.87
HP	0.5m	99.06%	15.74
	1m	99.10%	15.83
PHILIPS	2m	99.38%	16.78
CHOSEAL	1m	99.18%	15.67
JIANGDUN	1.5m	99.00%	15.71
JINGHUA	1.5m	98.78%	13.73
DELL	1.8m	99.21%	15.34
UGREEN	0.5m	99.12%	15.12
	1m	99.13%	15.19
	1.5m	99.19%	15.54
	2m	99.22%	15.92
	3m	99.29%	16.17
	5m	99.31%	16.35

All values are measured at 20 m; with FEC, the results are completely correct for all cables.

6.3.2 Impact of Different Monitors

To evaluate the impact of monitors on TrojPix, we assess covert communication performance on twelve COTS displays from nine major manufacturers: DELL, AOC, Redmi, PHILIPS, Lenovo, SAMSUNG, LG, HUAWEI, and TCL. The resolution is fixed at 1920×1080@60 Hz. A 1.5 m UGREEN video cable is used, and the receiving antenna is positioned 20 m from the transmitter.

Tab. 3 summarizes the evaluation results, with an average BCR of 99.13% and an average SNR of 15.25 dB. Among all models tested, TCL T27M6C achieves the highest BCR (99.26%), while even the lowest performing display (Redmi Mi) still maintains 99.01%. Interestingly, although the SAMSUNG LS27D800 attains the highest SNR, its BCR is not the highest, likely due to EM leakage from internal cabling interfering with the covert signal. Overall, TrojPix has an average BCR of 99.13% in heterogeneous display environments, demonstrating strong robustness against monitor variations.

6.3.3 Impact of Resolution

To evaluate the impact of display resolution on TrojPix, we test five commonly used settings: 800×600, 1280×720,

Table 3: Evaluation on different monitors.

Brand	Manuf.	BCR	SNR (dB)
DELL	S2421HSX	99.19%	15.12
	U2417H	99.19%	15.54
AOC	U2790B	99.08%	15.58
	U27B35	99.25%	15.33
Redmi	Mi Monitor	99.01%	15.05
PHILIPS	PHL	99.16%	14.68
	27E1N1820	99.02%	14.18
Lenovo	N2721U	99.10%	14.99
SAMSUNG	LS27D800	99.26%	16.00
LG	27US550	99.01%	14.81
HUAWEI	MateViewSE	99.07%	14.96
TCL	T27M6C	99.23%	16.18
With FEC, the results are completely correct for all monitors.			

1366×768, 1600×900, and 1920×1080. The refresh rate is fixed at 60 Hz, using a DELL U2417H monitor with 4 video cables: SAMZHE (1 m), HP (0.5 m), PHILIPS (2 m), UGREEN (1.5 m). The receiving antenna is positioned 20 m from the target device.

Fig. 8(a) shows the evaluation results under different resolutions. The observed BCRs exhibit only negligible variation across the five configurations: the highest is 99.19% at 1366×768, and the lowest is 99.11% at 800×600—an almost indistinguishable difference. Likewise, the variations in SNR remain minimal. These results indicate that the display resolution has little impact on covert communication performance, since resolution is handled at the display end and remains independent of the underlying data transmission. Consequently, data embedding is feasible at arbitrary display resolutions.

6.3.4 Impact of Distance

To evaluate the impact of distance on TrojPix, we conduct covert communication experiments at a distance ranging from 20 m to 120 m with increments of 20 m. The transmitter is DELL U2417H fixed at 1920×1080@60 Hz.

To further evaluate the result of transmission distance, Fig. 8(b) reports the evaluation results across different distances. As distance increases, the BCR of the raw bitstream declines due to signal attenuation and multipath effects. Although the use of a directional antenna and a low-noise amplifier improves the SNR, they cannot fully compensate for severe signal loss at long range. In particular, TrojPix still achieves a BCR of 99.19% at 20 m and 91.02% at 120 m.

To explore the maximum attack range, we gradually increase the distance in an outdoor environment while keeping the same RF front-end and modulation settings. At 208 meters, we are still able to successfully recover a complete data packet, with the preamble acquired, the lock established, and the cyclic redundancy check passed. These results demonstrate that TrojPix exhibits strong resilience against distance-induced degradation and remains practically viable in real-world scenarios.

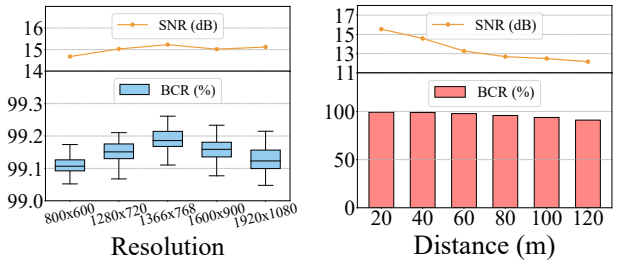


Figure 8: Impact of resolution and distance.

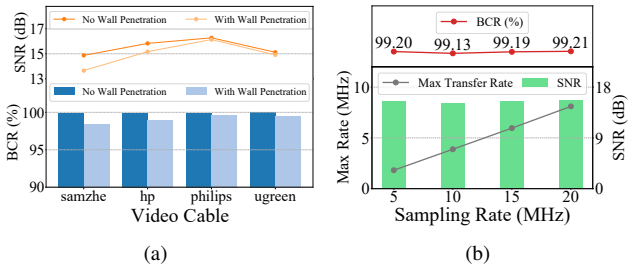


Figure 9: Impact of video cable and sampling rate.

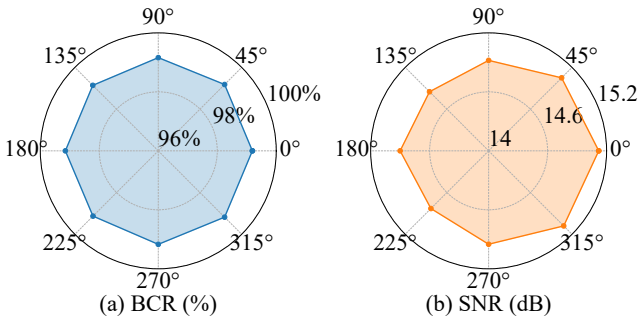
6.3.5 Through-Wall Evaluation

We evaluate the performance of TrojPix with the EM signal penetrating through a wall. The wall is made of concrete and is 30 cm thick, while the receiving antenna is positioned at a distance of 10 m from the target device. In addition, we consider the same settings as in Section 6.3.3 in terms of cables and display model. The resolution fixes at 1920*1080@60Hz.

Fig. 9(a) shows that the BCR of SAMZHE decreases the most, dropping by 1.49% after signal penetration, while PHILIPS experiences the smallest drop of only 0.3%. Overall, the average BCR declines from 99.96% before penetration to 99.14% after penetration. The overall performance remains stable, indicating that wall materials exert only a limited impact on the covert communication effectiveness of TrojPix, thereby demonstrating the robustness of TrojPix in complex transmission environments.

6.3.6 Impact of Sampling Rate

To evaluate the impact of the sampling rate on TrojPix, we consider four sample rates: 5 MHz, 10 MHz, 15 MHz, and 20 MHz. The settings of cables, display model, and resolution are the same as in Section 6.3.5, at distance of 20 m.



(a) BCR (%) (b) SNR (dB)

Figure 10: Impact of angle.

Fig. 9(b) presents the results of covert communication at different sampling rates. The BCRs at 5 MHz, 10 MHz, 15 MHz, and 20 MHz are 99.20%, 99.13%, 99.19%, and 99.21%, respectively, with the BCR probability being extremely high. We also evaluate the maximum achievable transmission rate, which increases with sampling rate, yielding 1.8 MHz, 3.8 MHz, 5.9 MHz, and 8.1 MHz for 5 MHz, 10 MHz, 15 MHz, and 20 MHz, respectively. Using devices that support higher sampling rates can further increase the maximum transmission rate.

6.3.7 Impact of Angle

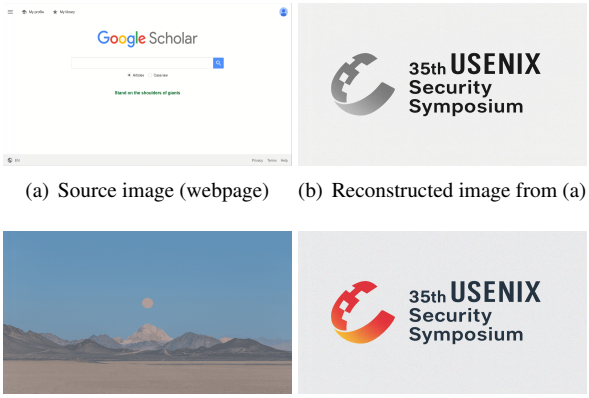
To evaluate the impact of angle on TrojPix, we perform our covert communication with the receiving antenna at different orientations ranging from 0° to 360° with 45° increments. The receiving antenna is positioned 20 m from the target device. In addition, we use the same settings as Section 6.3.6.

Fig. 10 presents the evaluation results under different orientations. The BCR and SNR exhibit only small fluctuations with angle, indicating stable performance. In all antenna orientations considered, TrojPix achieves an average BCR of 99.16% and an average SNR of 14.96 dB, demonstrating strong angular robustness and communication stability.

6.3.8 Transmission in Different Scenarios

We evaluate the perceptual imperceptibility and communication reliability of TrojPix under images with varying texture complexity. In particular, we select two representative examples: a popular webpage (Fig. 11(a)) and a natural scene (Fig. 11(c)). Therefore, we embed payloads into video frames driven by these source images for transmission tests. The embedded images exhibit negligible perceptual differences, with SSIM of 0.998 and 0.999, and LPIPS scores of 0.002 and 0.005 for the popular webpage and the natural scene.

On the receiver side, reconstructed images based on decoded bits are shown in Fig. 11(b)(d). Even under complex textured backgrounds, TrojPix achieves BCRs of 99.82% / 99.36%, respectively. These results demonstrate that TrojPix maintains near-perfect channel reliability while preserving



(a) Source image (webpage) (b) Reconstructed image from (a)

(c) Source image (natural scene) (d) Reconstructed image from (c)

Figure 11: Transmission under different visual scenarios. Payloads are embedded into video frames derived from source images and reconstructed at the receiver.

perceptual quality that is indistinguishable from the originals. We observe that complex textures introduce mild content dependency, leading to slight variations in the effective channel state. However, adopting stronger content-adaptive modulation and coding strategies could further enhance the robustness of TrojPix.

We further conduct a subjective perceptual study with 50 volunteers, where participants are asked to compare the displayed content before and after running TrojPix and report any visually perceivable changes. As shown in Tab. 4, none of the participants report any perceivable visual differences. This confirms that TrojPix does not introduce noticeable visual artifacts during operation, demonstrating its strong perceptual imperceptibility in practice.

6.3.9 Transmission of Different Size of Files

To evaluate the capability of TrojPix in transmitting real files, we selected file segments of various sizes (10 KB, 100 KB, 1 MB, and 10 MB) from the enwik8 corpus of the Mahoney dataset [37] and use them as transmission payloads. The transmitter is a DELL U2417H monitor fixed at 1920×1080@60 Hz, with a 1.5 m Ugreen video cable, and the receiving antenna is positioned 10 m away.

Tab. 5 shows the evaluation results for different file sizes. As file size increases, the transmission rate remains high at 2.016 Mbps for the 10 MB payload. The system performs efficiently with no significant variation in BCR, and both bit and character accuracy remain at 100%, demonstrating TrojPix's strong reliability and efficiency in file transfer scenarios.

6.3.10 Impact of Shielding

To evaluate the impact of electromagnetic shielding on TrojPix, we conducte comparative experiments using sev-

Table 4: User study on perceptual visibility.

Users	Perceptible	Imperceptible
Male (25)	0	25
Female (25)	0	25

Table 5: Transmission performance across different file sizes.

File Size	Time	BCR	Char Accuracy
10 KB	33 ms	100%	100%
100 KB	420 ms	100%	100%
1 MB	4.13 s	100%	100%
10 MB	41.6 s	100%	100%

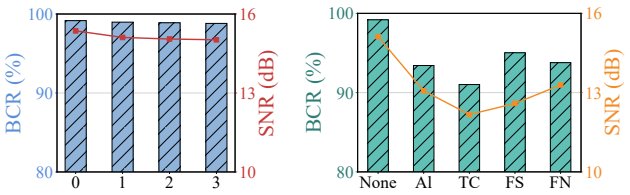
eral representative materials, including aluminum foil tape (Al), tinned copper mesh (TC), ferrite sheet (FS), and high-permeability ferronickel alloy (FN). The video cable already incorporates native shielding; each material is additionally wrapped around the cable, and the distance between the receiver and the target device is fixed at 20 m.

Fig. 12(a) shows the results under different shielding conditions, where "None" denotes the baseline without additional shielding. Among the tested materials, tinned copper braided shielding causes the most pronounced performance degradation, reducing the success rate to 91.02%, followed by aluminum foil tape, ferronickel alloy, and ferrite sheet. Notably, while shielding materials cause varying degrees of performance drop, the success rate remains above 91% in all cases. Overall, enhanced electromagnetic shielding can partially degrade TrojPix communication but remains insufficient to fundamentally block the covert channel.

6.3.11 Impact of Multiple Monitors

To evaluate the impact of nearby active monitors on the covert communication performance of TrojPix, we gradually introduce one to three additional monitors operating normally within a distance of 0.5 m from the target display. The configuration of the target monitor remains identical to that in the previous experiments, and all displays are set to a resolution of 1920×1080 at 60 Hz. 1.5 m UGREEN video cables are used, and the distance between the receiving antenna and the target device are fixed at 20 m.

Fig. 12(b) summarizes the results under varying numbers of nearby monitors, where "0" denotes the baseline case without any adjacent monitors. The results show that increasing the number of nearby monitors leads to slight but observable performance degradation. The BCR decreases from 99.19% at 0 to 98.81% at 3 monitors, and SNR also shows a mild drop from 15.54 dB to 15.02 dB. Nevertheless, the overall impact remains limited and does not result in a significant loss of communication reliability.



(a) Nearby monitors (b) Shielding materials

Figure 12: Impact of nearby monitors and shielding materials.

7 Discussion

In this section, we give methods to mitigate TrojPix covert channel attack, followed by a discussion of future work.

7.1 Defense

EM Shielding and Signal Interference: Analysis shows that one of the key factors for TrojPix to realize covert communication lies in its potential risk of EM information leakage; therefore, physical layer protection measures can be taken. On one hand, EM shielding can be implemented based on the Faraday cage principle, using shielding materials wrapped around key components to attenuate field strength leakage, as shown in Section 6.3.10. On the other hand, EM interference equipment can be deployed in the vicinity of the area of use, transmitting suppressive interference signals to cover the target frequency band, in order to cover the characteristics of the effective EM information and block its propagation path. Although this alleviates TrojPix's threat to some extent, it does not eliminate it, and deploying shielding materials and interference equipment adds an economic burden. Therefore, the use of EM leakage-free video interfaces (e.g., fiber-optic or wireless, etc.) can be more effective in mitigating the hazards posed by EM leakage.

Random Transmission and Pixel Smoothing: Another key factor for TrojPix to realize covert communication originates from the sequential transmission characteristic of the TMDS protocol. To mitigate the risk of EM information leakage caused by this, the transmission sequence of TMDS signals can be changed from a fixed to a random mode, and since the attacker cannot predict the random sequence, it is difficult to recover the effective information even if the leaked signals are intercepted. For the exploitable bit-flip characteristics in TMDS coding, it is necessary to implement smoothing to minimize the number of bit-flips between adjacent pixels, so that the characteristics of the leaked EM signals corresponding to different information contents tend to be the same, thus eliminating their ability to carry communication information. However, compared with pixel smoothing, which mainly involves the adjustment of coding algorithms, the implementation of the randomized transmission mode requires a higher cost, which not only requires the replacement of hardware

equipment, but also requires the redesign of the transmission architecture to adapt to the new randomization mechanism, and thus requires a comprehensive trade-off in practice.

7.2 Future Work

In this study, we show that the unintentional EM signals generated by digital video cables during normal display can be precisely manipulated and used to construct covert communication channels. We realize high-speed covert communication based on video cables through lightweight pixel-level modulation, and complete systematic validation in multi-dimensional scenarios. In the future, we will extend the method to all kinds of mainstream video interfaces and display devices, and test its universality under different system configurations such as refresh rates and hardware combinations. On this basis, we will also explore more efficient and flexible modulation coding and signal reception schemes to significantly improve communication rate, stability, and covertness. We also intend to investigate and develop practical protection schemes to provide a theoretical foundation and engineering reference for EM leakage protection in high-security environments.

8 Related Work

8.1 EM Side-Channel on Cryptographic Keys

Extracting cryptographic keys through EM side-channel is a serious and widely recognized threat. Early studies demonstrate that EM emissions from cryptographic hardware are sufficient to leak sensitive information. [38] shows that the EM emissions from field-programmable gate array (FPGA) devices could be exploited to reconstruct complete keys. Subsequently, [39] confirms that EM radiation can serve as a feasible vector for side-channel attacks. [40] further evaluates and discusses the risks associated with reconstructing keys from FPGA emissions.

Research later shows that attack targets expand to more complex computing platforms. [41] demonstrates how CPU emissions can be exploited to steal cryptographic keys, while [42] conducts the first physical side-channel attack on elliptic-curve cryptography in personal computers. Several works [43–47] exploit EM leakages from SoC components for key-recovery attacks. [48] shows that EM side channels could be used to extract ECDSA keys from smartphones. [40] further demonstrates that EM side channel can be used to identify cryptographic algorithms running on IoT devices.

As research deepens, attack techniques gradually evolve into more automated and efficient analysis methods. [49] introduces SCNIFFer, a low-cost automated platform to scan cryptographic chips and identify high-leakage regions for end-to-end attacks. More recent work shows that EM side channels can be highly effective in recovering complete AES keys from a variety of hardware platforms [50–53]. A common characteristic of these works is the ability to leverage large volumes of EM leakage data to infer a small and precise set of target keys.

Since the discovery of EM leakage, its application in cryptographic key extraction has remained a central research focus, but its potential for covert communication has not yet been fully explored. Building on this gap, this paper further investigates a covert communication method based on video-cable emissions and demonstrates the recovery of sensitive data at the receiver side.

8.2 Covert Communication Technology

Existing research shows that attackers can exploit various unintended physical channels [54, 55] such as sound, light, magnetic fields, and heat to achieve covert communication. [10] and [56] construct low-bandwidth thermal covert channels by modulating processor workloads to induce temperature fluctuations. [11] and [12] establish acoustic covert channels using acoustic noise and hard drive noise, respectively. [13] and [57] demonstrate optical covert channels based on hard drive indicator lights or keyboard LEDs. Meanwhile, [15–17] show that CPU and hard drive magnetic field leakage can be used to construct low-speed magnetic channels.

In comparison, channels have become a primary focus of research due to their remarkable potential. [14] establishes a power covert channel on the power line side by modulating overall system current through changes in CPU workload of a computer. Similarly, [58] exfiltrates data from a charging device by modulating workloads to decode it from the USB power channel. [17] introduces a magnetic covert channel that leaks information via CPU-induced emissions during video playback, and demonstrates that video rendering can be deliberately manipulated to generate modulated magnetic signals for data exfiltration. [18] exploits emissions from video cables in the FM band to enable covert communication within a range of several meters. [19] drives the USB bus via software to emit controllable radiation, which can then be received by software-defined radio. [20] demonstrates that leakage generated by memory buses in the cellular frequency bands can be captured by mobile basebands or SDRs. [21] leverages DRAM access patterns to modulate signals over multiple carriers, achieving covert communication at rates up to 300 kbps. [22] proposes the RF-PWM method, which transforms DRAM access noise into programmable physical-layer signals for various covert communication and attack scenarios. [23] reveals that SATA cables can serve as unintended antennas, radiating signals at both fundamental and harmonic frequencies that can be received at short distances. [24] combines emissions from video cables with LoRa technology to realize covert communication over a distance of 87.5 meters.

This paper is the first to propose a system capable of driving digital video cables to emit controllable signals while enabling visually imperceptible high-speed covert communication. Ex-

perimental results demonstrate that the system achieves a data transmission rate of 8.1 Mbps, representing more than a 27-fold improvement over SOTA (300 kbps). The maximum transmission distance reaches 208 m, approximately a 138% increase compared to SOTA (87.5 m). With respect to both core metrics—transmission rate and distance—TrojPix significantly surpasses the SOTA.

9 Conclusion

In this paper, we presented TrojPix, an innovative covert channel attack that exploited controllable EM emissions from digital video cables. By performing imperceptible pixel-level modulation, TrojPix enabled stable and high-throughput covert communication without requiring system privileges or hardware modifications. We systematically designed and evaluated an attack pipeline, from signal construction and modulation to long-distance decoding, demonstrating its practicality in real-world settings. Experimental results showed that TrojPix achieved a peak data transmission rate of up to 8.1 Mbps and a maximum transmission distance of 208 m, outperforming SOTA approaches and revealing information leakage risks posed by digital video cables that were previously underestimated.

10 Acknowledgment

This work is supported by National Natural Science Foundation of China (Grant No. 62202274, 62572286, 62422208, 62232010, 62350410480), Shandong Science Fund (Grant No. ZR2024MF108, ZR2025LZH006, ZR2024MF149), Ministry of Industry and Information Technology of China (Grant TC240A9ED-70), Research Project of Quancheng Laboratory, China (Grant QCL20250106), Project of the Major Innovation Project of Key Laboratory of Computing Power Network and Information Security, Ministry of Education (Grant 2024ZD012).

11 Ethical Considerations

In developing TrojPix, we carefully examined the ethical implications of systematically analyzing a physical-layer covert channel. Because such channels may introduce security risks, we implemented multiple safeguards to ensure that both the research process and the dissemination of results remain responsible and ethically grounded.

Stakeholders and Potential Impact. (1) Hardware manufacturers. TrojPix may place remediation pressure on display cable and interface manufacturers, as the identified EM leakage channel may necessitate improved shielding, layout redesigns, or reassessment of compliance with EM emission standards. **(2) Organizations handling sensitive information.** Enterprises and institutions operating air-gapped or high-assurance systems may need to re-evaluate procurement, deployment, and physical isolation policies, since display components previously considered benign could introduce previously unrecognized leakage risks. **(3) End users and the general public.** End users may face potential privacy risks if inadequately shielded display cables are exploited in uncontrolled environments, particularly when sensitive visual content is rendered without awareness of EM side-channel exposure. **(4) Security researchers and practitioners.** TrojPix deepens the understanding of EM behavior in modern display systems, supporting the detection, assessment, and mitigation of physical-layer covert channels, while also revealing and characterizing a new physical-layer covert communication method that can inform studies of covert communication mechanisms and channel modeling.

Impact of the Research Process and Publication. All experiments were performed on hardware fully controlled by the authors, used synthetic or non-sensitive data, and complied with safe EM emission practices. No third-party systems, real user data, or human subjects were involved, and no operational environments were affected. Publishing the results is valuable for manufacturers, standards bodies, and defenders seeking to understand and mitigate an overlooked physical-layer leakage path. At the same time, we recognize that these concepts could inform technically capable adversaries. To minimize risk, we provide only high-level analyses and omit any reproducible or operational attack details, while clearly outlining the practical constraints and preconditions.

Mitigation of Negative Impacts. To further reduce misuse, we avoid releasing end-to-end attack toolchains, optimized parameters, or deployable covert-channel configurations. Instead, we focus on design principles, constraints, and defensive strategies. We have conducted responsible disclosure with several cable manufacturers and will continue expanding communication to share high-level findings, potential weaknesses, and feasible mitigation directions—such as improved shielding, layout adjustments, or hardware-level filtering—without revealing sensitive implementation details. Feedback from vendors will be incorporated to support long-term ecosystem security improvements.

Decision to Conduct and Publish. This study was motivated by the observation that unrecognized physical-layer channels can pose persistent risks to air-gapped and high-assurance systems, and that ethical, systematic characterization is essential for building effective defenses. Our decision to publish followed a careful evaluation of risks and benefits. Withholding the findings would limit the ability of manufacturers and defenders to address a meaningful vulnerability, whereas controlled disclosure—removing operational details and incorporating vendor communication—provides clear security benefits. We therefore deem the publication of this work, in its constrained form, ethically justified.

By adhering to these principles, we aim to ensure that research on EM covert channels remains within ethical bound-

aries and advances responsible security. Our goal is not only to reveal an underexamined leakage vector but also to catalyze stronger hardware and system defenses, ultimately supporting safer deployment in high-confidentiality environments.

12 Open Science

To ensure that our research work is reproducible and to facilitate future studies, this paper provides the source code and related dataset. The code and data are available on Zenodo at https://zenodo.org/records/17905407, accompanied by comprehensive guides to help others effectively use and replicate the work. This approach follows open science practices and aims to support the research community in checking, expanding, and improving the study.

References

[1] K. Zetter. (2014, Dec.) Hacker lexicon: What is an air gap? Accessed: 2025-12-21. [Online]. Available: https://www.wired.com/2014/12/hacker-lexicon-air-gap/

[2] Z. Li, B. Chen, X. Chen, H. Li, C. Xu, F. Lin, C. X. Lu, K. Ren, and W. Xu, "Spiralspy: Exploring a stealthy and practical covert channel to attack air-gapped computing devices via mmwave sensing," in *The 29th Network and Distributed System Security (NDSS) Symposium 2022*. The Internet Society, 2022.

[3] M. R. Na and K. Sundharakumar, "A study on air-gap networks," in *2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT)*. IEEE, 2024, pp. 1–6.

[4] M. F. Bari and S. Sen, "Noisehopper: Emission hopping air-gap covert side channel with lower probability of detection," in *2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2024, pp. 21–32.

[5] Y. Kim, H. An, and D.-G. Han, "Emphone: Electromagnetic covert channel via silent audio playback on smartphones," *Sensors*, vol. 25, no. 18, p. 5900, 2025.

[6] N. Cranfill and J. Cleveland, "Emerging technologies for the control of the defense red switch network (drsn)," in *Proceedings of MILCOM'94*. IEEE, 1994, pp. 664–668.

[7] Claroty, "How to better protect air-gapped federal critical infrastructure," 2024. [Online]. Available: https://claroty.com/blog/how-to-better-protect-air-gapped-federal-critical-infrastructure

[8] RESULTS Technology, "Air-gapped backups: How they can help secure your bank," 2023. [Online]. Available: https://www.resultstechnology.com/blog/how-air-gapped-backups-can-help-secure-your-bank/

[9] U.S. Nuclear Regulatory Commission, "Regulatory guide 5.71: Cyber security programs for nuclear facilities," 2009. [Online]. Available: https://www.nrc.gov/docs/ml0903/ml090340159.pdf

[10] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations," in *2015 IEEE 28th Computer Security Foundations Symposium*. IEEE, 2015, pp. 276–289.

[11] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise ('diskfiltration')," in *European symposium on research in computer security*. Springer, 2017, pp. 98–115.

[12] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *arXiv preprint arXiv:1406.1213*, 2014.

[13] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "Ctrl-alt-led: Leaking data from air-gapped computers via keyboard leds," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1. IEEE, 2019, pp. 801–810.

[14] ——, "Powerhammer: Exfiltrating data from air-gapped computers through power lines," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1879–1890, 2019.

[15] M. Guri, B. Zadov, and Y. Elovici, "Odini: Escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1190–1203, 2019.

[16] N. Matyunin, J. Szefer, S. Biedermann, and S. Katzenbeisser, "Covert channels using mobile device's magnetic field sensors," in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2016, pp. 525–532.

[17] J. Zhang, X. Ji, W. Xu, Y.-C. Chen, Y. Tang, and G. Qu, "Magview: A distributed magnetic covert channel via video encoding and decoding," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 357–366.

[18] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici, "Airhopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," in *2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*. IEEE, 2014, pp. 58–67.

[19] M. Guri, M. Monitz, and Y. Elovici, "Usbee: Air-gap covert-channel via electromagnetic emission from usb," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 264–268.

[20] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "{GSMem}: Data exfiltration from {Air-Gapped} computers over {GSM} frequencies," in *24th USENIX Security Symposium (USENIX Security 15)*, 2015, pp. 849–864.

[21] Z. Zhan, Z. Zhang, and X. Koutsoukos, "Bitjabber: The world's fastest electromagnetic covert channel," in *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2020, pp. 35–45.

[22] G. Camurati and A. Francillon, "Noise-sdr: Arbitrary modulation of electromagnetic noise from unprivileged software and its impact on emission security," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 1193–1210.

[23] M. Guri, "Satan: Air-gap exfiltration attack via radio signals from sata cables," in *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*. IEEE, 2022, pp. 1–10.

[24] X. Sun, Y. Zheng, W. Xi, Z. Chen, Z. Chen, H. Hao, Z. Jiang, and S. Zhong, "Tempest-lora: Cross-technology covert communication," in *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, 2025, pp. 678–692.

[25] T. F. Collins, R. Getz, D. Pu, and A. M. Wyglinski, *Software-Defined Radio for Engineers*. Artech House, 2018.

[26] W. Winoto, A. Molnar, and A. M. Niknejad, "Digital radio-frequency transmitters: An introduction and tutorial," *IEEE Solid-State Circuits Magazine*, vol. 11, no. 2, pp. 61–73, 2019.

[27] J. Ding, W. Liu, L. Ding, J. Zhang, C. Yan, and T. Song, "New threat analysis of electromagnetic information leakage in electronic equipment based on active detection," *Communications Technology*, vol. 51, no. 4, pp. 936–940, Apr. 2018.

[28] Digital Display Working Group, "Digital visual interface (dvi) specification, revision 1.0," Digital Display Working Group, Specification Rev. 1.0, Apr. 1999. [Online]. Available: https://glenwing.github.io/docs/DVI-1.0.pdf

[29] R. N. Bracewell, *The Fourier Transform and Its Applications*, 3rd ed. Boston: McGraw-Hill, 2000.

[30] Wikipedia contributors, "Direct-sequence spread spectrum — Wikipedia, the free encyclopedia," 2025, accessed: 2025-08-27. [Online]. Available: https://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum

[31] E. N. Gilbert, "Capacity of a burst-noise channel," *The Bell System Technical Journal*, vol. 39, no. 5, pp. 1253–1265, 1960.

[32] E. O. Elliott, "Estimates of error rates for codes on burst-noise channels," *The Bell System Technical Journal*, vol. 42, no. 5, pp. 1977–1997, 1963.

[33] M. Schwartz, W. R. Bennett, and S. Stein, *Communication systems and techniques*. John Wiley & Sons, 1995.

[34] P. Welch, "The use of fast fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms," *IEEE Transactions on audio and electroacoustics*, vol. 15, no. 2, pp. 70–73, 2003.

[35] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE transactions on image processing*, vol. 13, no. 4, pp. 600–612, 2004.

[36] R. Zhang, P. Isola, A. A. Efros, E. Shechtman, and O. Wang, "The unreasonable effectiveness of deep features as a perceptual metric," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 586–595.

[37] M. Mahoney, "Large text compression benchmark data," http://mattmahoney.net/dc/textdata.html, 2009, accessed: 2025-08-25.

[38] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2001, pp. 251–261.

[39] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side—channel (s)," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2002, pp. 29–45.

[40] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "Leveraging electromagnetic side-channel analysis for the investigation of iot devices," *Digital Investigation*, vol. 29, pp. S94–S103, 2019.

[41] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from pcs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2015, pp. 207–228.

[42] ——, "Ecdh key-extraction via low-bandwidth electromagnetic attacks on pcs," in *Cryptographers' Track at the RSA Conference*. Springer, 2016, pp. 219–235.

[43] J. Longo, E. De Mulder, D. Page, and M. Tunstall, "Soc it to em: electromagnetic side-channel attacks on a complex system-on-chip," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2015, pp. 620–640.

[44] C. Ramsay and J. Lohuis, "Tempest attacks against aes," *Fox-IT, Fremont, CA, USA, Tech. Rep*, 2017.

[45] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming channels: When electromagnetic side channels meet radio transceivers," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 163–177.

[46] J. Danial, D. Das, A. Golder, S. Ghosh, A. Raychowdhury, and S. Sen, "Em-x-dl: Efficient cross-device deep learning side-channel attack with noisy em signatures," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 18, no. 1, pp. 1–17, 2021.

[47] G. Haas and A. Aysu, "Apple vs. ema: electromagnetic side channel attacks on apple corecrypto," in *Proceedings of the 59th ACM/IEEE Design Automation Conference*, 2022, pp. 247–252.

[48] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom, "Ecdsa key extraction from mobile devices via nonintrusive physical side channels," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 1626–1638.

[49] J. Danial, D. Das, S. Ghosh, A. Raychowdhury, and S. Sen, "Scniffer: Low-cost, automated, efficient electromagnetic side-channel sniffing," *IEEE Access*, vol. 8, pp. 173 414–173 427, 2020.

[50] W. Yu and J. Chen, "Deep learning-assisted and combined attack: a novel side-channel attack," *Electronics Letters*, vol. 54, no. 19, pp. 1114–1116, 2018.

[51] V. V. Iyer and A. E. Yilmaz, "Using the anova f-statistic to rapidly identify near-field vulnerabilities of cryptographic modules," in *2021 IEEE MTT-S International Microwave Symposium (IMS)*. IEEE, 2021, pp. 112–115.

[52] M. R. Zunaidi, A. Sayakkara, and M. Scanlon, "Revealing iot cryptographic settings through electromagnetic side-channel analysis," *Electronics*, vol. 13, no. 8, p. 1579, 2024.

[53] P. Cao, C. Zhang, X. J. Lu *et al.*, "Side-channel analysis for the re-keying protocol of bluetooth low energy," *JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY*, vol. 38, no. 5, pp. 1132–1148, 2023.

[54] H. Liu, R. Spolaor, F. Turrin, R. Bonafede, and M. Conti, "Usb powered devices: A survey of side-channel threats and countermeasures," *High-Confidence Computing*, vol. 1, no. 1, p. 100007, 2021.

[55] C. Morales-Gonzalez, M. Harper, M. Cash, L. Luo, Z. Ling, Q. Z. Sun, and X. Fu, "On building automation system security," *High-Confidence Computing*, vol. 4, no. 3, p. 100236, 2024.

[56] R. J. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, and S. Capkun, "Thermal covert channels on multi-core platforms," in *24th USENIX Security Symposium (USENIX Security 15)*, 2015, pp. 865–880.

[57] M. Guri, B. Zadov, and Y. Elovici, "Led-it-go: Leaking (a lot of) data from air-gapped computers via the (small) hard drive led," in *International conference on detection of intrusions and malware, and vulnerability assessment*. Springer, 2017, pp. 161–184.

[58] R. Spolaor, Y. Xu, V. Moonsamy, M. Conti, and X. Cheng, "Covertpower: A covert channel on android devices through usb power line," *IEEE Transactions on Dependable and Secure Computing*, no. 01, pp. 1–16, 2025.