

# EMPalm: Exfiltrating Palm Biometric Data via Electromagnetic Side-Channels

Haowen Xu\*, Tianya Zhao<sup>†</sup>, Xuyu Wang<sup>†</sup>, Lei Ma\*, Jun Dai\*, Alexander Wyglinski\*, Xiaoyan Sun\*

\*Worcester Polytechnic Institute, USA Email: {h xu4, lma5, jdai, alexw, xsun7}@wpi.edu

<sup>†</sup>Florida International University, USA Email: {tzhao010, xuywang}@fiu.edu

**Abstract**—Palm recognition has emerged as a dominant biometric authentication technology in critical infrastructure. These systems operate in either single-modal form, using palmprint or palmvein individually, or dual-modal form, fusing the two modalities. Despite this diversity, they share similar hardware architectures that inadvertently emit electromagnetic (EM) signals during operation. Our research reveals that these EM emissions leak palm biometric information, motivating us to develop EMPALM—an attack framework that covertly recovers both palmprint and palmvein images from eavesdropped EM signals. Specifically, we first separate the interleaved transmissions of the two modalities, identify and combine their informative frequency bands, and reconstruct the images. To further enhance fidelity, we employ a diffusion model to restore fine-grained biometric features unique to each domain. Evaluations on seven prototype and two commercial palm acquisition devices show that EMPALM can recover palm biometric information with high visual fidelity, achieving SSIM scores up to 0.79, PSNR up to 29.88 dB, and FID scores as low as 6.82 across all tested devices, metrics that collectively demonstrate strong structural similarity, high signal quality, and low perceptual discrepancy. To assess the practical implications of the attack, we further evaluate it against four state-of-the-art palm recognition models, achieving a model-wise average spoofing success rate of 65.30% over 6,000 samples from 100 distinct users.

## I. INTRODUCTION

Palm recognition technologies, encompassing unimodal approaches based on palmprint or palmvein and multimodal methods that fuse the two, have rapidly emerged as highly secure and reliable biometric authentication techniques [1], [2]. In particular, multimodal fusion of palm textures with vascular structures yields high entropy, strong forgery resistance, and lasting physiological stability [3]. Consequently, palm-based authentication has been widely adopted across government and commercial sectors, including the FBI, the Department of Homeland Security, Amazon, and Tencent [4], [5].

Traditional palm recognition systems rely on either palmprint or palmvein imaging, using visible light for palmprint textures and near-infrared (NIR) sensing for subcutaneous veins [6]. Modern systems overcome the limitations of single-modality approaches—often affected by environmental or physiological factors—by adopting dual-mode architectures that capture both features simultaneously [3], [7]–[9], thereby improving accuracy and robustness. However, in both single- and dual-mode designs, sensor circuits carry time-varying currents that, by Maxwell’s equations [10], inevitably emit electromagnetic (EM) radiation. In addition, high-speed transmission of biometric images over buses or flat cables can turn

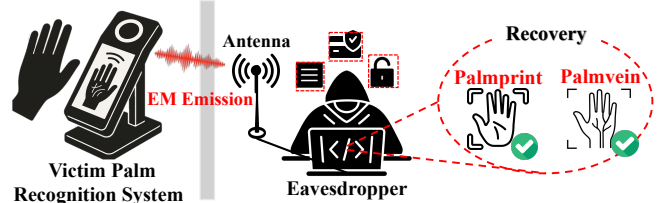


Fig. 1: Attack scenario of EMPALM.

wiring into unintended antennas, exposing sensitive information through EM emissions.

Although prior studies on EM leakage in contexts such as iris recognition and embedded cameras have provided valuable insights [11]–[13], EM leakage in palm recognition—particularly in dual-modal designs—remains largely unexplored. This gap is even more critical as palm recognition systems are increasingly deployed in high-security applications, including national intelligence agencies [14] and financial institutions [15]. To demonstrate this, we show that biometric image data in palm recognition systems, including both single- and dual-modal architectures, can be eavesdropped via EM side channels. As illustrated in Figure 1, an eavesdropper can covertly collect EM emissions from palm scanners using a concealed antenna, and reconstruct the palm images all while the victim assumes their biometric data remains secure within the scanner.

**Challenges.** An effective eavesdropping of dual-modal palm recognition systems faces four key challenges.

- *Interleaved Dual-Modal Emissions.* Palmprint and palmvein data can be transmitted in alternating fashion, producing interleaved emissions that complicate modality separation.
- *Noisy Wide-band Spectrum.* EM emissions span wide and device-dependent frequencies, making it non-trivial to identify biometric-relevant bands.
- *Bit-Level Grayscale Collisions.* Bit-packed formats cause multiple grayscale values to map to identical EM patterns, collapsing subtle intensity differences and fine details.
- *Degraded Image Texture.* The reconstructed images exhibit degraded textures due to electromagnetic interference, environmental noise, and information loss during reconstruction.

**Our Approach.** In this paper, we present EMPALM, the first

eavesdropping attack that recovers palmprint and palmvein images from palm recognition systems via EM side channels. By exploiting unintentional EM emissions captured from eight experimental devices and two commercial palm recognition systems, EMPALM reconstructs preliminary biometric images through a multi-step pipeline. To address the challenge of *Interleaved Dual-Modal Emissions*, we reverse-engineer transmission protocols and implement frame boundary detection, modality classification, and signal disentanglement for synchronized palmprint–palmvein reconstruction. To cope with the *Noisy Wide-band Spectrum*, we design a rapid localization framework that integrates spectrum analysis, temporal profiling, and device characterization to identify informative frequency bands. To resolve *Bit-Level Grayscale Collisions*, we introduce a multi-band image combination strategy that leverages higher-order harmonics to restore collapsed intensity variations and preserve fine details. Finally, to mitigate *Degraded Image Texture*, we formulate the task as image restoration and employ a structure-guided diffusion model to recover high-fidelity palmprint creases and palmvein patterns.

**Contributions.** In summary, our contributions are as follows:

- *EM Side-channel Attack Surface Exploitation.* We reveal EM leakage in palm biometric recognition, enabling effective spoofing of recognition models and exposing the feasibility of physical attacks.
- *End-to-End Attack Framework.* We propose an end-to-end framework that includes frequency localization, single-band reconstruction, multi-band combination and diffusion-based restoration, enabling robust image recovery from both single- and dual-modal palm recognition systems across diverse devices without requiring large paired datasets.
- *Comprehensive Experimental Evaluation.* We conduct comprehensive experiments on seven prototype and two commercial palm acquisition devices, and four state-of-the-art palm recognition models, achieving strong performance across metrics and evaluating EMPALM under diverse impact factors.

## II. PRELIMINARIES

### A. Palm Recognition

Figure 2 illustrates the general recognition pipeline comprising four essential steps: image collection, image pre-processing (ROI localization), feature extraction, and matching. The pipeline begins with image acquisition where palm images are captured by the imaging hardware, followed by Region of Interest (ROI) localization on the System on Chip (SoC) [16] to ensure accurate feature analysis, then feature extraction derives discriminative characteristics from the pre-processed ROI. In the matching phase, the pipeline diverges based on operational mode: enrollment stores extracted features as templates in the database, while verification (1:1 matching) and identification (1:N matching) compare query features against stored templates for decision-making. This foundational pipeline architecture applies to both palmprint and palmvein recognition systems.

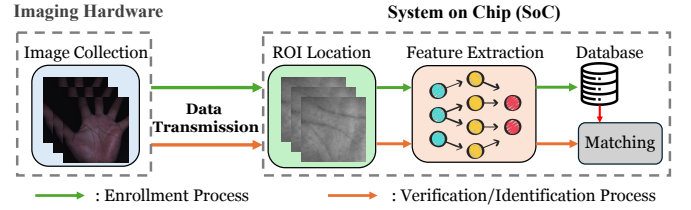


Fig. 2: Workflow of palm recognition systems.

**PalmPrint Recognition.** Palmprint recognition [17] utilizes the surface-level features of the human palm, such as principal lines and wrinkles, to perform identity verification. The field has evolved from early statistical methods to modern deep learning approaches [18], significantly improving recognition accuracy and robustness.

**PalmVein Recognition.** Palmvein recognition [19] captures the internal vascular structure of the palm using NIR imaging technology. By relying on subcutaneous vascular patterns rather than the superficial skin textures used in palmprint recognition, palmvein recognition achieves greater stability and robustness, being less affected by external conditions such as skin dryness, scars, *etc.*

**Dual-Modal Palm Recognition System.** To enhance recognition performance and security, modern systems increasingly adopt dual-modal architectures [3], [7]–[9] that jointly acquire palmprint and palmvein information. Figure 3 illustrates the general dual-modal systems. Similar to single-modal systems, dual-modal palm recognition follows the standard biometric pipeline of image acquisition, ROI localization, feature extraction, and matching. In contrast to single-modal designs, modern systems employ both visible and infrared imaging, which are then transmitted as an interleaved stream to the SoC for decoding and ROI extraction. The two modalities are then processed independently for identity verification [20], and their matching results are fused at the decision level. This dual-modal architecture enhances matching reliability and improves robustness against spoofing attempts and environmental variations, offering significant advantages over single-modal approaches.

### B. Image Transmission Principles

In embedded image acquisition, sensors generate RAW images containing unprocessed pixel data from a single color component defined by the front-end filter array. These RAW images are then transferred to the image signal processor (ISP) through high-speed serial links [21], most notably the MIPI Camera Serial Interface 2 (MIPI CSI-2) [22], where the de-bayering process is applied to interpolate missing color values of each pixel based on spatial correlations with surrounding pixels.

**Information-bearing EM Emissions in MIPI CSI-2.** As illustrated in Figure 4a, CSI-2 organizes image transmission hierarchically [23], with frames divided into rows and each row further decomposed into columns. Within each frame, the protocol structures the transmitted data into well-defined

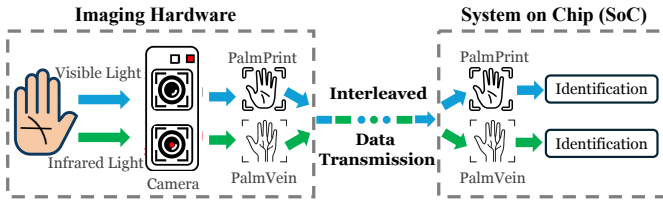


Fig. 3: System design of Dual-modal palm recognition.

packets, specifically: each row transmission begins with a Line Start (LS) short packet, followed by a Long Packet containing a Header and Pixel Payload, and ends with a Line End (LE) short packet. Rows are separated by line blanking intervals, while frame blanking intervals delimit frame boundaries. This structured packetization not only enables reliable high-speed transmission but also induces distinctive EM emissions. As shown in Figure 4b, these emissions manifest on multiple time scales: at the frame level, aggregated signals appear as periodic bursts, each corresponding to one frame, whereas at the line level, finer-grained periodic patterns align with individual row transmissions.

### III. MOTIVATION AND THREAT MODEL

#### A. Motivation of EMPALM

Palm recognition has seen increasing adoption across both palmprint and palmvein modalities [4], [5], [24], [25]. Compared to traits such as iris and face, it offers greater robustness to illumination, larger feature-rich regions, easier acquisition without user cooperation, and stronger resistance to spoofing, making it well-suited for practical deployment.

Despite these advantages, palm recognition systems inevitably expose sensitive information during data transmission. Our research identifies a critical vulnerability: the EM leakage in this stage are strongly correlated with image data and can be reconstructed into raw images and subsequently restored into palm biometric patterns. Through denoising and enhancement, attackers can recover high-quality palmprint and vein features, posing severe risks since these immutable patterns cannot be revoked or replaced, leading to long-term privacy and security threats.

To our best knowledge, no prior work has investigated EM side-channel leakage from palm recognition systems, and certainly none has addressed dual-mode palmprint-vein systems. Therefore, this study aims to explore the feasibility of such attacks and to assess their threat level to existing palm recognition deployments.

#### B. Threat Model

The adversary’s objective is to exploit EM emissions leaked from biometric acquisition and recognition systems to reconstruct palm biometric features, thereby enabling unauthorized access, identity theft, and financial fraud.

**Victim Device.** The victim devices are biometric acquisition and recognition systems equipped with either single-mode or dual-mode cameras. During operation, raw biometric data are

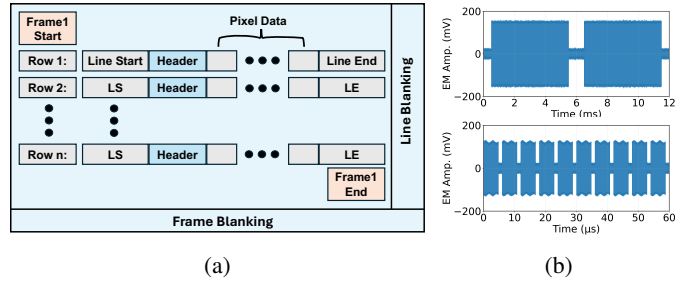


Fig. 4: EM leakage in MIPI CSI-2 image transmission. (a) CSI-2 data organization. (b) Frame-level and Line-level transmission’s EM leakage.

transmitted internally, typically via high-speed interfaces such as CSI2, which inevitably generate EM emissions that may expose sensitive biometric information.

**Adversary Capabilities.** The adversary cannot physically access or tamper with the victim systems, nor modify hardware, firmware, or software. However, by capturing the EM emissions leaked during image acquisition and real-time biometric recognition, the adversary can remotely extract information sufficient to recover palm biometric features. Using commercially available antennas, low-noise amplifiers (LNAs), and software-defined radios (SDRs), the adversary can operate from a concealed distance without raising suspicion.

**Attack Scenarios.** As shown in Figure 1, we consider real-world deployment scenarios where palm-based biometric systems are widely used, including secure building entry points, identity verification kiosks, and palm payment terminals deployed by major retailers [24]. The eavesdropper discreetly installs compact EM signal capturing devices behind walls, under counters, or within fixtures near the target systems. When a user performs palm-related authentication, the concealed device proactively captures the EM emission leaked during the image acquisition process. The adversary is able to reconstruct a usable palm template just within a few seconds.

### IV. ATTACK DESIGN

Figure 5 provides an overview of EMPALM. We first introduce its core four modules in terms of the overall workflow, and elaborate in the following respective subsections.

(1) *EM Band Localization.* Since palm-related emissions are buried within a noisy wide spectrum, this module identifies informative sub-bands that carry biometric information. A two-stage procedure is used: (i) band filtering, which applies statistical metrics to discard noise-dominated regions, and (ii) image validation, which reconstructs preliminary images from candidate bands to confirm palm-relevant structures.

(2) *Dual-Modal Image Reconstruction.* From each localized band, intercepted EM signals are transformed into palm images. In the single-modal case, reconstruction is straightforward; however, dual-modal systems are more challenging because palmprint and palmvein transmissions are interleaved asynchronously. We design a disentanglement method that

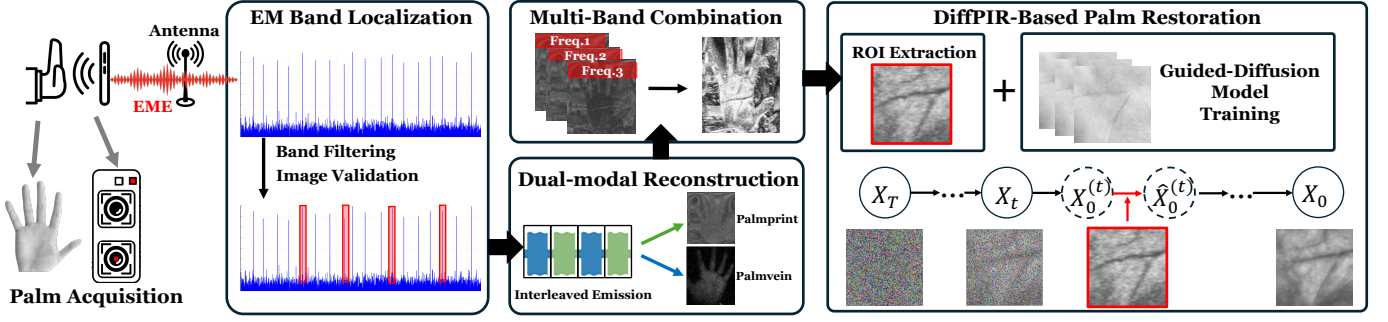


Fig. 5: Overview of EMPALM.

separates and aligns the two modalities, enabling synchronized multi-modal reconstruction.

(3) *Multi-Band Combination*. Individual bands suffer from stochastic noise and bit-level ambiguities due to the bit-packed acquisition format. To overcome these limitations, reconstructions from multiple informative bands are integrated through a multi-band optimization strategy for both modularities. By leveraging harmonic relationships across frequencies, this module consolidates complementary features, restores collapsed intensity variations, and preserves structural details.

(4) *DiffPIR-Based Palm Restoration*. The fused images then undergo ROI extraction and diffusion-based restoration. Using DiffPIR, a plug-and-play restoration framework, we suppress residual noise and correct band-limited distortions. This enhances palmprint creases and vein patterns with high perceptual fidelity, producing reconstructions suitable for spoofing attacks and further biometric analysis.

#### A. EM Leakage Bands Localization

Figure 6 illustrates the diverse signal characteristics captured across different EM sub-bands. While certain frequencies—such as 109 MHz, 118 MHz, and 405 MHz—yield palm images with discernible biometric features, many other bands are dominated by irrelevant emissions or structured noise (e.g., the 250 MHz band reveals HDMI screen content). Without prior knowledge, pinpointing a sub-band that contains useful biometric signals within a wide spectrum is a non-trivial task.

While each informative sub-band may capture only a partial and limited aspect of the palm’s structure, it can simultaneously exhibit strong structured noise patterns. This combination—limited signal coverage and dominant noise—amplifies the difficulty for downstream restoration, making it harder to recover a clean and complete biometric image from any single band. To address this, we aim to exhaustively identify signals from all sub-bands that may carry complementary biometric cues. This insight makes the problem significantly harder than single-band reconstruction: in practice, we do not know a priori how many informative bands exist or where they are located within the spectrum.

To address this challenge, we propose an automated frequency identification method, outlined in Algorithm 1, which integrates statistical signal characterization with visual interpretability. The method begins by partitioning the full

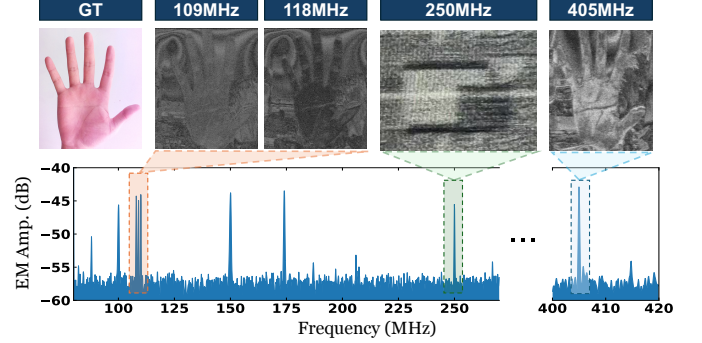


Fig. 6: Illustration of signals from different frequency bands.

EM spectrum  $S(f)$  into discrete sub-bands over the range  $[f_{\min}, f_{\max}]$  (Line 1), and proceeds in two stages: (1) *Band Filtering*, where candidate bands are selected based on spectral energy and statistical features, and (2) *Image Validation*, where preliminary reconstructions are assessed to confirm the presence of palm-relevant structures.

**Band Filtering (Lines 2–6).** For each sub-band, the corresponding time-domain signal  $s_i(t)$  is extracted (Line 3), and a set of statistical metrics are computed to discriminate structured digital transmissions from stochastic background noise. Specifically, the signal energy  $E_i$  (Line 4) quantifies overall activity within the band, the spectral entropy  $H_i$  (Line 5) measures the degree of spectral disorder with lower values indicating structured periodic emissions, and the peak auto-correlation  $A_i$  (Line 6) captures repetitive temporal patterns characteristic of high-speed image transmissions. Together, these metrics enable us to filter out idle or noise-dominated bands while retaining those with structured signal components, which are more likely to carry biometric information. Sub-bands that satisfy all three criteria are passed as candidates to the next stage.

**Image Validation (Lines 7–12).** For each candidate signal  $s_i(t)$ , a grayscale image  $I_i$  is reconstructed by a utility algorithm TEMPESTRDR (SDR) [26], which can reconstruct images directly from IQ data (Line 8). Specifically, let  $P_{orig} \in \mathbb{R}^{H_{orig} \times W_{orig}}$  denote the original image, and let  $P_{rec}^{[f_l, f_h]}$  represent the attempted reconstruction from EM signals within the frequency band  $[f_l, f_h]$ :

---

**Algorithm 1: Frequency Band Localization**

---

**Input:** EM spectrum  $S(f)$ , frequency range  $[f_{\min}, f_{\max}]$   
**Output:** Informative sub-bands  $\mathcal{F}_{\text{img}}$

```
1 Divide  $[f_{\min}, f_{\max}]$  into sub-bands  $\{f_i\}_{i=1}^N$ ;  
2 for  $i \leftarrow 1$  to  $N$  do  
    // Stage 1: Band Filtering  
3 Extract  $s_i(t)$  from  $S(f_i)$ ;  
4  $E_i = \|s_i(t)\|^2$ ; // Signal energy  
5  $H_i = \mathcal{H}(\text{FFT}(s_i(t)))$ ; // Spectral ent.  
6  $A_i = \max(\text{ACF}(s_i(t)))$ ; // Autocorr.  
    peak  
    // Stage 2: Image Validation  
7 if  $E_i > \theta_E$  and  $A_i > \theta_A$  and  $H_i < \theta_H$  then  
8  $I_i = \text{TEMPESTSDR}(f_i^{\text{low}}, f_i^{\text{high}})$ ; // SDR  
    Algo  
9  $\mathcal{H}(I_i)$ ; // Image entropy  
10  $\mathcal{E}(I_i) = \|\nabla I_i\|$ ; // Edge intensity  
11 if  $\mathcal{H}(I_i) > \theta_{\mathcal{H}}$  and  $\mathcal{E}(I_i) > \theta_{\mathcal{E}}$  then  
12  $\mathcal{F}_{\text{img}} \leftarrow \mathcal{F}_{\text{img}} \cup \{f_i\}$   
13 return  $\mathcal{F}_{\text{img}}$ 
```

---

$$P_{\text{rec}}^{[f_l, f_h]} = \mathcal{R}\{n(t) + b_{\text{clk}} + H_{[f_l, f_h]}[\mathcal{D}(P_{\text{orig}})]\} \quad (1)$$

where  $\mathcal{R}$  denotes the reconstruction operator,  $n(t)$  represents environmental noise,  $b_{\text{clk}}$  is the clock-induced offset,  $H_{[f_l, f_h]}$  represents the electromagnetic transfer function, and  $\mathcal{D}$  is the digital encoding function.

After the TEMPESTSDR reconstruction, two visual indicators are then evaluated to ensure that the reconstructed band captures palm-relevant structures rather than incidental artifacts: image entropy  $\mathcal{H}(I_i)$  (Line 9), which reflects the richness of intensity variation expected in palm images, and edge intensity  $\mathcal{E}(I_i)$  (Line 10), which emphasizes the presence of crease and vein patterns. While high entropy or edges alone may occasionally arise from unrelated artifacts, our framework leverages their joint occurrence as a reliable proxy for palm-related information. Only bands exhibiting consistently high values in both measures are selected as the candidates (Lines 11–12), and are returned as final outputs (Line 13).

### B. Dual-Modal Image Reconstruction

Although we utilize TEMPESTSDR to reconstruct raw images to facilitate frequency localization, modern dual-mode palm recognition systems typically alternate between capturing palmprint and palmvein modalities [23], [27]. When TEMPESTSDR is naively applied to such interleaved transmissions, the resulting reconstructions contain entangled content from both modalities—often mixed in unpredictable and non-uniform ways. As a result, these raw images are largely unusable for downstream processing, necessitating more so-

phisticated disentanglement strategies before any meaningful restoration or analysis can take place.

To address this issue, given the candidate bands, we analyze the eavesdropped EM signals and observe that dual-modal systems follow a consistent frame-interleaved transmission pattern, where palmprint and palmvein data alternate regularly across consecutive frames. Exploiting this temporal structure, we separate the interleaved signals by frame parity, enabling accurate modality disentanglement:

$$M_k = k \bmod 2 \quad (2)$$

where  $M_k = 0$  corresponds to palm print frames and  $M_k = 1$  corresponds to palmvein frames, based on the observed alternation pattern.

Based on this temporal separation, we perform independent reconstruction for each modality:

$$P_{\text{print}}[r, c] = \frac{1}{N_{\text{print}}} \sum_{j=0}^{N_{\text{print}}-1} |s_{IQ}^{(2j)}[r, c]| \quad (3)$$

$$P_{\text{vein}}[r, c] = \frac{1}{N_{\text{vein}}} \sum_{j=0}^{N_{\text{vein}}-1} |s_{IQ}^{(2j+1)}[r, c]| \quad (4)$$

where  $N_{\text{print}}$  and  $N_{\text{vein}}$  represent the number of frames for each modality (typically  $N_{\text{print}} = N_{\text{vein}} = N_f$  for balanced capture).

This temporal separation strategy enables effective modality-specific reconstruction, successfully disentangling palmprint and palmvein images that would otherwise be corrupted by mixed reconstruction. The effectiveness of this approach hinges on accurate frame synchronization to ensure correct modality assignment. Additional implementation details, including synchronization mechanisms and modality-specific enhancements, are provided in Appendix A.

### C. Multi-band Image Combination

While the dual-modal image reconstruction effectively disentangles the modalities into separate palmprint and palmvein images, it inevitably incurs information loss due to the bit-packed acquisition formats commonly used in sensor hardware (e.g., RAW10). In such formats, multiple bit positions are compressed into repeating binary patterns, which become electromagnetically indistinguishable within a single frequency band. This aliasing effect causes subtle grayscale variations to collapse, leading to noticeable gradient artifacts and the erosion of fine structural details in the reconstructed images.

Our key insight is that while individual frequency bands suffer from these ambiguities, the harmonic relationships across multiple bands preserve complementary information. When the fundamental frequency  $f$  cannot differentiate between bit positions with identical periodicities, the harmonic at  $2f$  often carries discriminative phase or amplitude variations necessary for accurate recovery. This observation motivates our multi-band optimization framework:

$$\min_{\alpha_i} \|S(I_{\text{reconstructed}}) - v_{\text{target}}\|^2 + \lambda \Phi(I_{\text{reconstructed}}), \quad (5)$$

where the first term enforces intensity consistency over uniform regions, and  $\Phi(\cdot)$  is a regularizer encouraging the preservation of structural details such as palm creases and vein edges.

The reconstructed image is expressed as

$$I_{\text{reconstructed}} = \sum_{i=1}^N \alpha_i \cdot B_i(f_i^{\text{low}}, f_i^{\text{high}}), \quad (6)$$

where  $B_i$  denotes the filtered image obtained from frequency band  $i$ . The candidate bands are restricted to the validated outputs from the previous stage:

$$\{B_i\}_{i=1}^N \subseteq \mathcal{I}_{\text{img}}, \quad (7)$$

with  $\mathcal{I}_{\text{img}}$  denoting the set of informative sub-band reconstructions identified by the frequency localization algorithm.

Here,  $S(\cdot)$  denotes a segmentation operator for uniform regions,  $v_{\text{target}}$  is their expected constant intensity, and the optimization adaptively assigns weights  $\{\alpha_i\}$  to balance surface uniformity with preservation of palmprint and vein structures. In practice, amplitude thresholding suppresses noise before fusion, and the number of combined bands is selected to trade off reconstruction fidelity against computational cost.

#### D. Diffusion-based Palm Restoration

While the proposed multi-band image combination alleviates bit-level grayscale collisions and restores critical structural details, in practical EM side-channel acquisition of palmprint and palm vein data, reconstructed images are still degraded by hardware mismatches, electromagnetic interference, and environmental noise. These factors introduce artifacts, distortions, and blur that obscure fine biometric details and reduce recognition quality. A general approach for restoring a clean signal from its degraded measurement is to first model the task as a linear inverse problem [28].

**Linear Inverse Problem.** Many image processing tasks, such as deblurring, denoising, and super-resolution, can be formulated as linear inverse problems, where the goal is to restore an image from noisy measurements given through a known linear degradation model [29]. Formally, the degradation process can be expressed as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \quad (8)$$

where  $\mathbf{x} \in \mathbb{R}^n$  denotes the clean image,  $\mathbf{y} \in \mathbb{R}^m$  the degraded measurement,  $\mathbf{H} \in \mathbb{R}^{m \times n}$  a known linear degradation operator, and  $\mathbf{n} \sim \mathcal{N}(0, \sigma_y^2 \mathbf{I})$  additive white Gaussian noise with variance  $\sigma_y^2$ . When  $\mathbf{H}$  is known and fixed, image restoration can be formulated as a supervised learning problem, where neural networks are trained end-to-end on paired clean and degraded samples synthesized by  $\mathbf{H}$ . In contrast, our setting involves unknown and heterogeneous degradations that are challenging to characterize explicitly. The transmission and reconstruction pipeline introduces a mixture of distortions, including non-Gaussian noise and structured interference.

**DiffPIR for Palmprint and Palmvein Restoration.** Due to the diversity of noise types in our setting and the lack of access

to their individual degradation models, we adopt the plug-and-play DiffPIR framework [28] to address these challenges. DiffPIR is an image restoration approach that leverages a pretrained diffusion model as a powerful, task-agnostic prior. By learning from large collections of clean images, this prior enables generalization to various noise distributions and allows restoration without requiring explicit degradation models—making it well-suited for our scenario.

Our key innovation is to decouple prior learning from the degradation model. We formulate restoration as an optimization problem:

$$\min_{\mathbf{x}} D(\mathbf{x}, \mathbf{y}) + \lambda P(\mathbf{x}), \quad (9)$$

where  $\mathbf{y}$  is the observed noisy measurement,  $D(\mathbf{x}, \mathbf{y})$  is the data fidelity term, and  $P(\mathbf{x})$  represents the negative log-prior over natural images, learned from clean image via a diffusion model.

Unlike traditional inverse problem solvers that require a known degradation operator  $\mathbf{H}$  in Eq. 8, we do not rely on explicit knowledge of  $\mathbf{H}$ . Instead, we approximate the measurement process using a learned mapping or statistical constraint. Specifically, the fidelity term can be expressed as

$$D(\mathbf{x}, \mathbf{y}) = \|\phi(\mathbf{x}) - \mathbf{y}\|^2 \quad (10)$$

where  $\phi(\cdot)$  denotes a feature extractor or surrogate forward model that operates in the measurement space. This substitution allows us to enforce consistency between reconstructed images and observed data without requiring an exact analytical degradation operator. This flexibility is critical in our EM restoration setting, where distortions arise from heterogeneous and unknown transmission artifacts.

## V. EVALUATION

We conduct comprehensive experiments of EMPALM on diverse hardware and real-world palm datasets for both recovery fidelity and attack effectiveness. We start with introducing the experimental setup in Section V-A, then evaluate the effectiveness of EMPALM in Section V-B, and finally examine the impact of practical factors on EMPALM in Section V-C.

### A. Experimental Setup

**Hardware.** To reproduce palm recognition processes, we built a modular acquisition platform using single-board computers (SBCs) connected to visible-light and Near-Infrared sensors. The SBC controllers include Raspberry Pi 3B+ (S1), Raspberry Pi 5 (S2) and NVIDIA Jetson Nano (S3). We use three devices for palmprint acquisition: OV5647 (V1), IMX219 (V2) and IMX708 (V3), and use three NIR devices for palmvein acquisition: 23H166-LED (IR1), IMX219-160 (IR2) and HW200 (IR3). Besides the above single modal devices, a dual-modal device, HAOKAI-H220 (DUAL), is employed for simultaneous palmprint and palmvein capture. To further evaluate EMPALM's performance against real-world devices, we include two commercial off-the-shelf (COTS) devices C1 and C2. We withhold disclosure of the exact models of the tested commercial devices to provide vendors

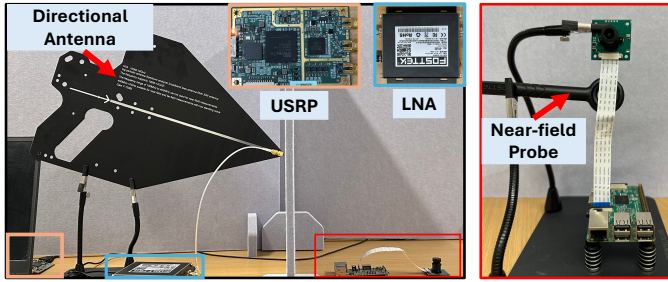


Fig. 7: EM signals acquired using a directional antenna and a near-field probe.

TABLE I: Palm Acquisition Devices.

| Type       | Device            | Task  |
|------------|-------------------|-------|
| Prototype  | OV5647 (V1)       | print |
|            | IMX219 (V2)       | print |
|            | IMX708 (V3)       | print |
|            | 23H166-LED (IR1)  | vein  |
|            | IMX219-160 (IR2)  | vein  |
|            | HW200 (IR3)       | vein  |
|            | HAOKAI-H220(DUAL) | dual  |
| Commercial | C1                | dual  |
|            | C2                | dual  |

sufficient time to develop solutions addressing the identified risks. Table I summarizes the palm acquisition devices.

Figure 7 illustrates the EM acquisition system, which is built on a Universal Software Radio Peripheral (USRP) B200 SDR [30], equipped with a FOSTTEK near-field magnetic probe for close-range measurements or an Eujgoov directional antenna (0.1–12 GHz) for long-range reception. We use a FOSTTEK FST-RFAMP06 low-noise amplifier (LNA) with a gain of 40 dB to enhance weak EM emissions. The USRP operates at a sampling rate of 10 MS/s with an RF bandwidth of 20 MHz, and streams data to a workstation over USB 3.0 for real-time processing.

**Software.** For the configuration of USRP, we employ TempestSDR on the Ubuntu operating system (Release 24.04.5). For DiffPIR training, as described in Section IV-D, we use PyTorch (Release 2.4.0) with CUDA (Release 12.1).

**Attack Setup.** To evaluate the robustness of EMPALM, we setup the attack against the target palm recognition system in both close-range and long-range configurations. In the close-range setting, a magnetic field probe is positioned near the transmission interface between the image sensor and the SBC with minimal interference, and in the long-range setting, a directional antenna intercepts radiated emissions without physical contact.

**Datasets.** We employ four public benchmark datasets of two palmprint and two palmvein datasets, including the SCUT-PV-v1 (SCUT) dataset [19], [31], [32], the CASIA Multi-Spectral Palmprint Image Database V1.0 (CASIA-M) [33], the Tongji Contactless Palmprint Dataset (Tongji) [34] and the CASIA Palmprint Image Database (CASIA) [35]. To

TABLE II: Dataset Statistics.

| Dataset        | Task  | # Image | # Subject |
|----------------|-------|---------|-----------|
| SCUT           | vein  | 11,000  | 550       |
| CASIA-M        | vein  | 7,200   | 100       |
| Tongji         | print | 12,000  | 300       |
| CASIA          | print | 5,502   | 312       |
| CASIA + Tongji | print | 17,502  | 600       |
| CASIA-M + SCUT | vein  | 18,200  | 650       |

ensure meaningful evaluation on high-quality target models, we merge the Tongji and CASIA datasets into a combined palmprint dataset, and merge the SCUT and CASIA-M into a combined palmvein dataset. Table II summarizes the dataset statistics.

**Target Palm Recognition Models.** We evaluate our spoofing attack on two categories of target palm recognition models: palmprint-based and palmvein-based. For palmprint-based models, we follow PCE-Palm [36] and Diff-Palm [37], and adopt three backbone architectures: ResNet50 [38], MobileFaceNet [39], and PalmNet [40], all with an input resolution of 224×224. Specifically, ResNet50 is a deep residual network with skip connections for strong discriminative learning, MobileFaceNet is a lightweight CNN optimized for resource-limited devices, and PalmNet integrates Gabor filters with a PCA-based unsupervised scheme to produce highly discriminative descriptors from limited, label-free data. All palmprint models are trained with ArcFace [41] with parameters margin  $m=0.5$ , scale  $s=48$  recommended by [37]. For palmvein-based models, we follow PVTTree [42] and adopt ResNet101 [38] trained with ArcFace (margin  $m=0.5$ , scale  $s=64$ ) for 20 epochs on synthetic and real datasets using 8 GPUs and a batch size of 32. Table III summarizes all target models, their training datasets and their true accept rate (TAR@1e-4) after training.

**Restoration Model Training.** We employ DiffPIR as our image restoration model. To account for modality differences, we train two separate models for palmprint and palmvein with their respective dataset. Following [28], the network is configured with 64 channels, two residual blocks per resolution, and attention at the  $16 \times 16$  resolution. We set the diffusion process to 1,000 steps with a linear noise schedule, and adopt the Adam optimizer with a learning rate of  $2 \times 10^{-4}$ .

TABLE III: Target recognition models for attack evaluation.

| Model              | Task  | Training Dataset | TAR@ 1e-4 (%) |
|--------------------|-------|------------------|---------------|
| ResNet50 [38]      | Print | CASIA + Tongji   | 94.81         |
| MobileFaceNet [39] | Print | CASIA + Tongji   | 96.26         |
| PalmNet [40]       | Print | CASIA + Tongji   | 93.80         |
| ResNet101 [38]     | Vein  | CASIA-M + SCUT   | 94.87         |

**Evaluation Metrics.** We conduct comprehensive evaluations using multiple metrics following established practices in the literature.

- *Peak Signal-to-Noise Ratio (PSNR)*: Evaluates pixel-wise fidelity between reconstructed and ground truth images,

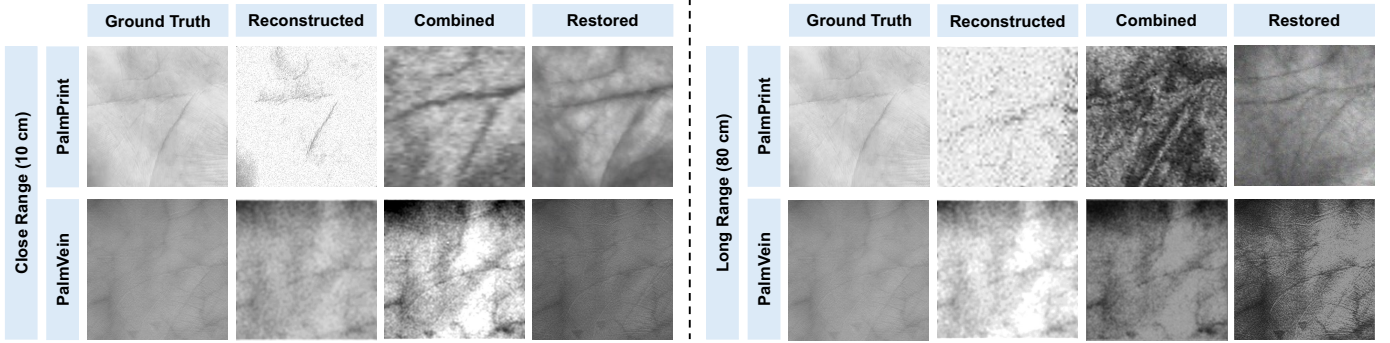


Fig. 8: Reconstruction examples of palmprint (device V1, random select) and palmvein (device IR1, random select) in the single-modal setting, with close-range acquisition at 10 cm (left) and long-range acquisition at 80 cm (right). Ground Truth: the original high-quality palm print image; Reconstructed: the initial single-band reconstructed image; Combined: the image combined by reconstructed images from multi bands; Restored: the image restored from the combined image by diffusion model.

with higher values indicating better pixel-level reconstruction accuracy.

- *Structural Similarity Index Measure (SSIM)*: Assesses perceptual similarity in terms of luminance, contrast, and structure, ranging from -1 to 1 where 1 indicates perfect structural similarity.
- *Fréchet Inception Distance (FID)*: Measures perceptual quality by comparing deep feature statistics extracted from a pre-trained Inception-V3 network, with lower values indicating reconstructed images are closer to real images in the feature space.
- *Spoof Success Rate (SSR)*: Quantifies the proportion of reconstructed palmprint and palmvein images that successfully bypass target biometric recognition models. A higher SSR indicates greater susceptibility of the recognition system to EM side-channel-based spoofing attacks.

Among these metrics, PSNR, SSIM, and FID evaluate the visual reconstruction quality of restored images, while SSR directly measures the attack effectiveness by assessing whether reconstructed biometric samples can successfully deceive recognition systems.

### B. Effectiveness Evaluation

We progressively evaluate EMPALM across multiple dimensions, including its effectiveness in single- and dual-modal restoration, its ability to spoof target recognition models, and its performance in attacking real-world COT devices.

**Effectiveness of Single-Modal Restoration.** We conduct independent restoration experiments for Palmprint and Palmvein images using EM signals from the respective devices, V1, V2, V3 (palmprint) and IR1, IR2, IR3 (palmvein). Figure 8 presents all intermediate and final images recovered by each stage of the EMPALM pipeline, under both close and long-range settings. As shown, EMPALM progressively refines the image through each stage, ultimately producing restored images that closely approximate the ground truth.

Figure 9 reports the SSIM, PSNR, and FID of EMPALM (hatched bars) across different devices. On palmprint images

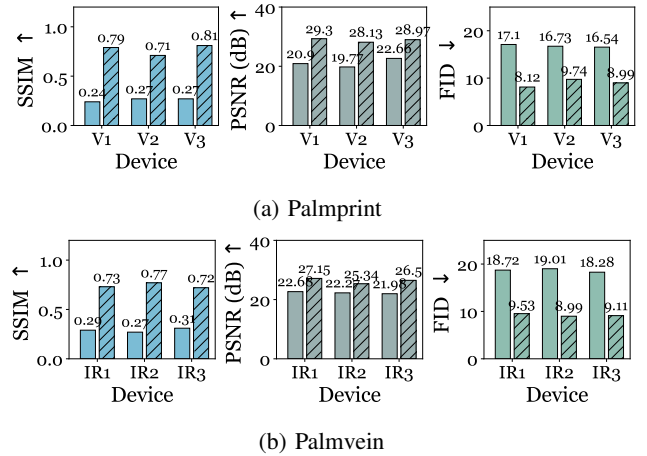


Fig. 9: SSIM, PSNR and FID of EMPALM on Single Modal. Solid bars: single band, hatched bars: multi-bands combined.

from three devices, EMPALM achieves up to 0.81 SSIM, 29.3 PSNR, and 17.1 FID, while on palmvein images from three devices, it achieves up to 0.77 SSIM, 27.15 PSNR, and 19.01 FID. The slightly lower metrics on palmvein reflect its inherent stability and robustness against external perturbations and reconstruction attacks. Despite this increased difficulty, EMPALM still manages to extract high-fidelity representations, demonstrating its generalizability across both more- and less-sensitive biometric modalities.

As the core of the EMPALM, we further compare the performance of EMPALM with (hatched) and without (solid) multi-band combination. The poor performance of single-band restoration validates information loss as we hypothesized in Section IV-C. Meanwhile, multi-band Combination delivers consistent and significant gains across all metrics, demonstrating improvement on multiple perspectives of reconstruction quality: fine-grained structural similarity (SSIM), global fidelity (PSNR), and perceptual realism (FID). Specifically,

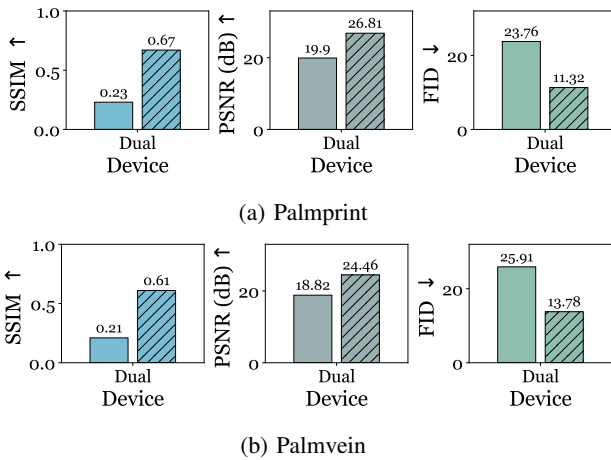


Fig. 10: SSIM, PSNR and FID of EMPALM on Dual Modal. Solid bars: single band, hatched bars: multi-bands combined.

SSIM increases by 0.55 (palmprint) and 0.50 (palmvein), PSNR increases by 8.4 dB (palmprint) and 4.52 dB (palmvein), and FID decreases by 8.98 (palmprint) and 10.02 (palmvein). Taken together, these results confirm that multi-band combination improves reconstruction comprehensively across structural, global, and perceptual dimensions.

**Effectiveness of Dual-Modal Restoration** We further evaluate the dual-modal scenario, where visible-light and NIR signals are transmitted asynchronously and interleaved on the same interface. Figure 10 reports the effectiveness of EMPALM for dual-modal scenarios (hatched). EMPALM achieves SSIM of 0.67, PSNR of 26.81 dB, and FID of 11.32, on the palmprint task, and SSIM of 0.61, PSNR of 24.46 dB, and FID of 13.78 on the palmvein task. These results validate that the universal principles of signal separation and reconstruction framework, demonstrating their effectiveness to handle dual-modal transmissions in practice (Section IV-B).

Compared with EMPALM without multi-band combination (solid), the use of multi-band combination (hatched) consistently enhances reconstruction quality, similar to the single-modal case. For palmprint images, it improves SSIM by 0.40, PSNR by 5.64 dB, and reduces FID by 12.13; for palmvein images, the gains are 0.44 in SSIM, 6.91 dB in PSNR, and 12.44 in FID. The results demonstrate that multi-band combination remains crucial for high-fidelity restoration, even in the more challenging interleaved transmission scenario.

**Effectiveness of Spoofing Target Models.** To ensure a fair evaluation of our attack, we follow the prior palm recognition works [36], [37], [42] and adopt the recognition models described in Table III. These architectures represent widely used and well-validated CNN baselines, providing a representative foundation for our evaluation.

Figure 11 presents the spoofing success rates (SSR) achieved by EMPALM against different target models. The results demonstrate substantial effectiveness across all tested architectures, with an overall average spoofing success rate of 65.3%. Among the palmprint models, PalmNet (print)

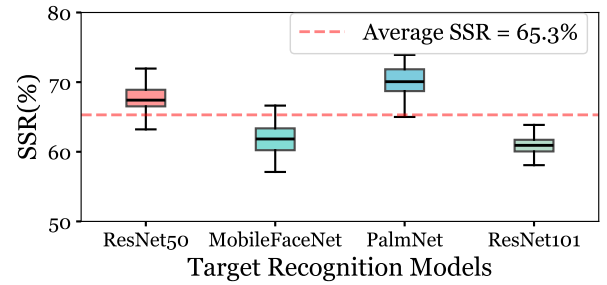


Fig. 11: Spoofing Success Rate of Different Models

exhibits the highest vulnerability with success rates reaching approximately 72%, while ResNet50 (print) achieves around 68% and MobileFaceNet (print) shows slightly lower rates at approximately 62%. The palmvein model ResNet101 demonstrates comparable susceptibility with success rates around 61%. Palmvein patterns are inherently harder to spoof due to their subtle, sub-surface nature, which makes them more resistant to EM leakage and reconstruction—unlike the more prominent, surface-level features of palmprints that are easier to capture and exploit. These findings confirm that our EM-based reconstruction method poses a significant security threat across diverse models used in palm biometric systems.

An interesting observation is that among all palmprint models, PalmNet exhibits the highest vulnerability to EMPALM. Unlike generic CNN-based models, PalmNet adopts a hybrid architecture that integrates Gabor filters with a PCA-based unsupervised scheme. This design choice makes PalmNet particularly susceptible to attacks from EMPALM, as its strong capabilities at recovering principal textural features. This observation underscores a key insight: models that depend heavily on low-level or principle-component-derived features may inadvertently expose themselves to greater risk when such features are recoverable through external leakage. These findings highlight the need for model designs that are robust to side-channel reconstructions, potentially by avoiding over-reliance on easily reconstructible signal patterns and incorporating safeguards that account for fine-grained biometric information.

**Effectiveness of Attacking COTS Devices.** To further evaluate the practicality of EMPALM in real-world settings, we extend our experiments to commercial-off-the-shelf (COTS) palm recognition devices C1 and C2. We focus on assessing whether EMPALM is effective on these commodity systems, in terms of its reconstruction quality and effectiveness in spoofing attacks. Table IV reports the results of EMPALM on the two COTS devices. Despite the differences in hardware design and shielding strategies, our results confirm that EMPALM can successfully extract biometric information from COTS devices, with the reconstructed images demonstrating substantial spoofing capability against recognition models, highlighting the generality and severity of this threat.

TABLE IV: Effectiveness of EMPALM on two COTS devices.

| Device | SSIM $\uparrow$ | PSNR (dB) $\uparrow$ | FID $\downarrow$ | Average SSR (%) $\uparrow$ |
|--------|-----------------|----------------------|------------------|----------------------------|
| C1     | 0.64            | 27.8                 | 11.3             | 52.5                       |
| C2     | 0.61            | 26.4                 | 12.7             | 49.1                       |

### C. Impacts of Practical Factors

Unless otherwise specified, all impact experiments were conducted under a default configuration. The palm recognition software (PalmNet) and sensor models (V1 for palmprint, IR1 for palmvein) were used, with the sensor connected to the SBC (S1) under evaluation. A receiving antenna was placed at a fixed distance of 0.5 meter and paired with a 40 dB LNA to ensure sufficient signal strength.

**Impact of Different SBCs.** To examine how different SBCs affect the performance of EMPALM, we evaluated it on three single-board computers: Raspberry Pi 3B+ (S1), Raspberry Pi 5 (S2) and NVIDIA Jetson Nano (S3). Each device was configured with identical palmprint recognition software and connected to the same sensor model. The receiving antenna was placed at a fixed distance of 0.5 meters with 40 dB LNA, ensuring consistent experimental conditions across all tests. As reported in Table V, the performance of EMPALM remain highly stable across different SBCs, confirming that the exploitable EM leakage originates from the sensor's data transmission rather than the underlying computing hardware. This demonstrates that the vulnerability is broadly applicable regardless of deployment platform.

TABLE V: Impact of different SBCs on EMPALM.

| Device | SSIM $\uparrow$ | PSNR (dB) $\uparrow$ | FID $\downarrow$ | Average SSR (%) $\uparrow$ |
|--------|-----------------|----------------------|------------------|----------------------------|
| S1     | 0.72            | 29.41                | 8.73             | 62.7                       |
| S2     | 0.74            | 29.49                | 8.52             | 66.5                       |
| S3     | 0.72            | 29.24                | 9.12             | 60.1                       |

**Impact of Different LNAs.** To investigate the effect of low-noise amplifiers on EMPALM, we conduct experiments using LNAs with different gain levels: no gain, 20dB, 30dB, and 40dB. The three gain levels correspond to different device models: ZK09-BM (20dB), Teyleten (30dB), and FST-RFAMP06 (40dB).

Figure 12 presents the performance of EMPALM across different LNA configurations. Without amplification (0dB), EM signals are too weak for meaningful palm restoration (SSIM  $\downarrow$  0.1, SSR = 0%). The 20dB amplifier shows minimal improvement (SSR = 12.4%), remaining insufficient for practical attacks. However, substantial improvements emerge with 30dB amplification (SSIM = 0.65, SSR = 48.6%), which further increase with the 40dB amplifier (SSIM = 0.71, SSR = 67.2%). These results demonstrate a clear correlation between LNA gain and attack effectiveness, with a notable threshold effect between 20dB and 30dB where the amplification becomes sufficient to capture fine-grained biometric features through EM emissions.

**Impact of Different probe Angles.** To evaluate the impact of probe orientation, we position the receiving probe 2 centimeter

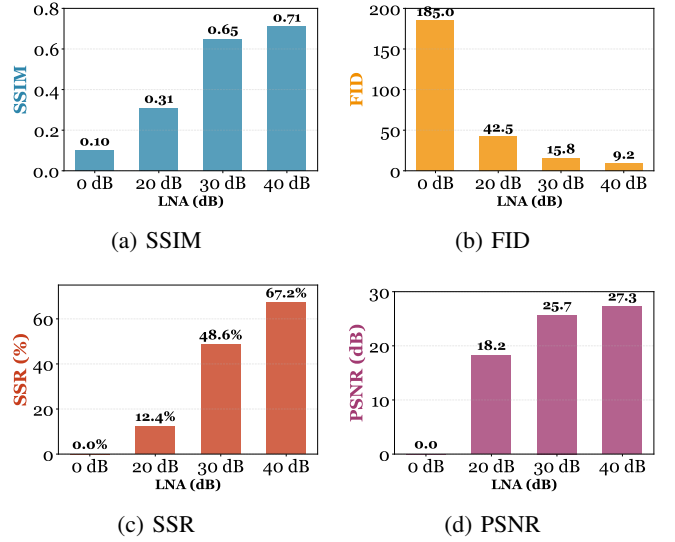


Fig. 12: Impact of different LNAs on EMPALM.

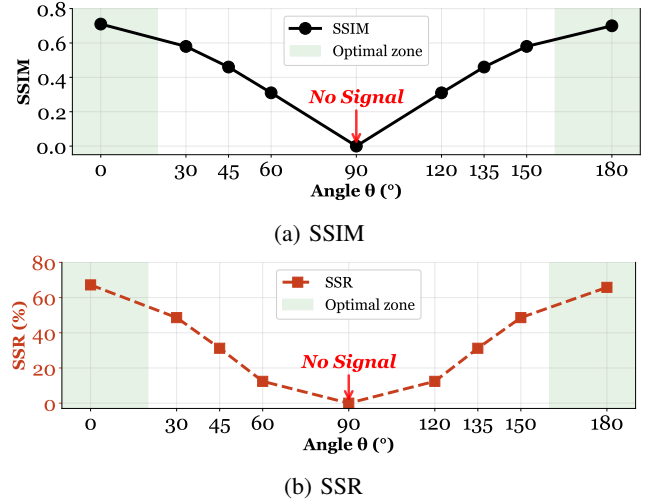


Fig. 13: Impact of antenna angle on EMPALM. (a) SSIM and (b) SSR under varying angles  $\theta$ . Results indicate optimal reception zones and a complete signal loss at  $\theta = 90^\circ$ .

away from the target palm sensor in the near-field region and vary the probe angle  $\theta$  from  $0^\circ$  to  $180^\circ$ . Figure 13 illustrates the relationship between probe angle and restoration quality measured by SSIM. The highest restoration quality is achieved when the receiving probe achieves optimal electromagnetic coupling with the sensor's internal signal paths at  $0^\circ$  (SSIM = 0.71, SSR = 67.2%) and  $180^\circ$  (SSIM = 0.70, SSR = 65.8%), where the probe orientation maximizes interception of the radiated EM fields. As the angle moves away from  $0^\circ/180^\circ$ , restoration quality drops, reaching moderate levels at  $30^\circ$ – $150^\circ$  and failing completely at  $90^\circ$  (SSIM = 0, SSR = 0%). The symmetric degradation pattern suggests dipole-like radiation characteristics, indicating a predictable angular dependency that adversaries can exploit to optimize interception and spoofing.

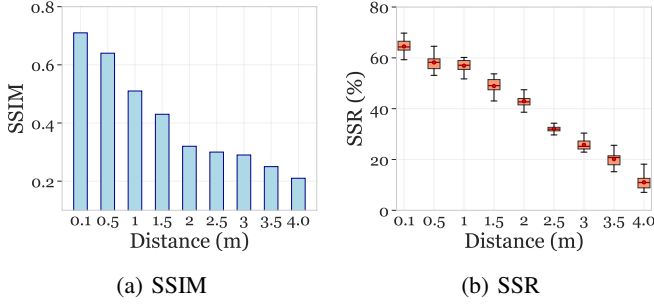


Fig. 14: Impact of different distances on EMPALM. (a) SSIM and (b) SSR under varying distances

**Impact of Different Distances.** We evaluated EMPALM’s performance using directional antennas at distances from 0.1 meter to 4.0 meter with 0.5 meter intervals. As shown in Figure 14a, SSIM values decrease from 0.72 at 0.1 meter to 0.21 at 4.0 meter due to EM signal attenuation. The attack success rate (Figure 14b) also exhibits a significant decline, dropping from 65% at 0.1 meter to 10% at 4.0 meter. Notably, EMPALM remains effective within a 2-meter range, achieving 43% SSR and 0.32 SSIM at 2 meter—sufficient for practical attacks in typical office environments. Beyond 2 meter, performance degrades significantly due to multipath effects and reduced SNR, though the directional antenna configuration substantially extends the viable attack range compared to omnidirectional alternatives.

These results demonstrate that EMPALM poses a credible threat in real-world scenarios where adversaries can position themselves in adjacent spaces.

**Impact of Different Environmental Noises.** To evaluate EMPALM’s robustness against real-world noises, we tested the EMPALM across four daily-life environments where palm-print recognition can be commonly deployed: office, home, supermarket, and outdoor settings. We maintained a fixed distance of 1.5 meter and collected 50 EM traces in each environment during peak activity hours to capture representative noise conditions. As shown in Figure 15, EMPALM achieved consistent metrics across all environments, demonstrating the general effectiveness of EMPALM in daily-life scenarios. This robustness to ambient interference validates EMPALM’s practical threat potential in real-world deployments.

**Impact of EM Shielding Materials.** Following EMIRIS [11] and EMeye [13], we evaluated the impact of five shielding materials—copper wire mesh (M5), aluminum foil (M4), metalized fabric (M3), conductive coating (M2), and conductive fabric (M1)—on EMPALM, with each material uniformly wrapped around the sensor’s data transmission cables. All other experimental settings remained identical to those described above.

Figure 16 presents the effects of different shielding materials on EMPALM. For better interpretation, the materials are ordered in ascending order of their theoretical electromagnetic shielding capabilities. Aligning with the theoretical electromagnetic shielding capabilities, the evaluation re-

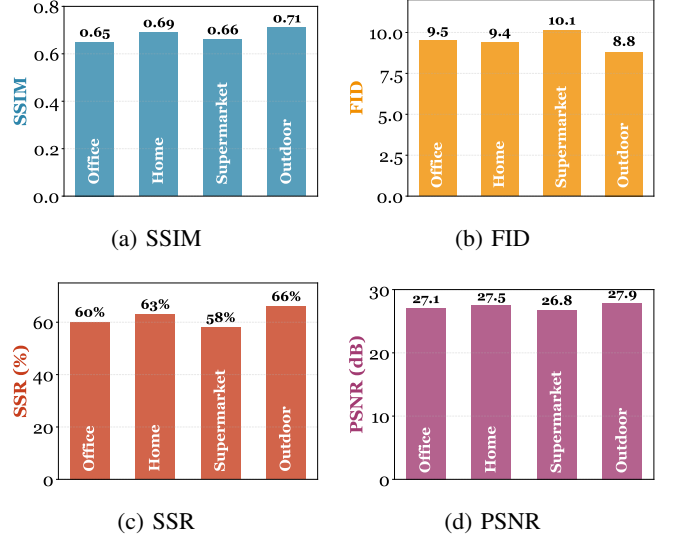


Fig. 15: Impact of different environment noises on EMPALM.

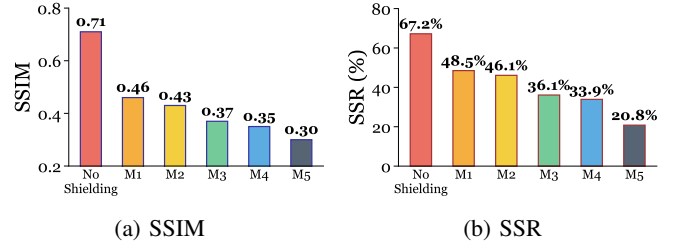


Fig. 16: Impact of EM shielding materials on EMPALM. (a) SSIM and (b) SSR under varying EM shielding materials.

sults show distinct effects across materials. Conductive fabric (SSIM: 0.46, SSR: 48.5%) and conductive coating (SSIM: 0.43, SSR: 46.1%) provide only moderate protection. Metalized fabric (SSIM: 0.37, SSR: 36.1%) and aluminum foil (SSIM: 0.35, SSR: 33.9%) suppress EMPALM more effectively. Copper mesh delivers the strongest shielding (SSIM: 0.30, SSR: 20.8%), significantly reducing reconstruction quality and spoofing success. These differences reflect material conductivity, thickness, and structural density, with metallic foils and meshes blocking EM leakage more efficiently than fabrics or coatings. Overall, although EM shielding materials substantially degrade EMPALM’s effectiveness, they fail to fully mitigate the underlying side-channel vulnerability.

## VI. DISCUSSION

### A. Extended Attack Scenarios

**Deferred Attack Feasibility.** While EMPALM demonstrates strong real-time attack performance, its design as a general EM side-channel framework also enables deferred attack scenarios. In such cases, adversaries can deploy compact, covert eavesdropping devices to passively monitor and collect electromagnetic emissions over time. These devices can be configured to identify and monitor only the informative frequency bands. Once sufficient data is collected, the attacker

can then perform offline signal analysis and palm image reconstruction at a later stage. To demonstrate the feasibility of stealthy long-term eavesdropping, we implemented a miniaturized collection system using a USRP device coupled with a microcontroller. This configuration, with dimensions of merely  $6 \times 10 \times 3$  centimeters, can be inconspicuously deployed near palm recognition devices in various scenarios—hidden behind furniture, embedded in wall fixtures, or disguised as legitimate IoT devices. The small form factor and low power consumption enable battery-powered operation for extended periods. The deployed device continuously captures and stores electromagnetic IQ (In-phase/Quadrature) samples containing palm biometric information. The collected IQ data can be retrieved physically, then reconstructed and restored offline using our pipeline.

TABLE VI: Experimental results of offline palmprint reconstruction from IQ data collected using the compact setup.

| Users | SSIM $\uparrow$ | PSNR (dB) $\uparrow$ | FID $\downarrow$ | Average SSR (%) $\uparrow$ |
|-------|-----------------|----------------------|------------------|----------------------------|
| U1    | 0.66            | 26.18                | 9.94             | 53.6                       |
| U2    | 0.70            | 26.44                | 9.62             | 57.1                       |

We conducted experiments to validate this deferred attack scenario. IQ data was collected over 3 hours from 10 authentication sessions involving two participants across different trials using our compact setup. Post-collection analysis successfully recovered palm images with performance metrics shown in Table VI. The results demonstrate that offline reconstruction from stored IQ samples achieves comparable quality to real-time attacks, confirming the viability of this stealthy deployment strategy. This finding raises serious concerns about the long-term security of palm recognition systems, as adversaries can potentially conduct surveillance over extended periods before executing attacks.

**Real-world Attack Implications.** Beyond digital spoofing, the reconstructed biometric data from EMPALM enables physical attacks. Researchers at the Chaos Communication Congress demonstrated that wax hand models containing vein patterns can fool commercial authentication systems [25]. By combining EMPALM with such fabrication techniques, adversaries can execute the complete attack chain—from covert EM collection to physical access—without ever contacting the victim. This fundamentally undermines the security of palmprint and palmvein authentication systems deployed in critical infrastructure.

### B. Countermeasures

Based on the vulnerabilities analyzed in Section IV-B, we propose several countermeasures to mitigate the risks posed by EMPALM.

(1) EM shielding can be applied to the data transmission cables of palmprint and vein sensors to suppress emissions. As shown in Section V-C, correct choice of shielding materials can substantially reduce recovery quality and spoofing success.

(2) The transmission principle can be redesigned to make the channel more resilient. For example, increasing transmis-

sion complexity or decoupling transmitted packets from pixel-level information would prevent a direct mapping between EM signals and biometric image content, thereby reducing the feasibility of reconstruction attacks.

(3) Palm recognition systems themselves can be strengthened by integrating anomaly detection of abnormal input patterns, and multi-factor authentication. These mechanisms would help to prevent adversaries from using reconstructed or physically fabricated artifacts to spoof the system. Taken together, these countermeasures highlight a multi-layered defense strategy, combining hardware-level shielding, protocol-level transmission hardening, and system-level security enhancements, to mitigate the long-term risks of EM-based side-channel exploitation.

**Responsible Disclosure.** We have notified the corresponding vendors of the discovered security vulnerabilities and provided them with potential countermeasure mechanisms. This process was conducted in accordance with the principles of responsible disclosure.

### C. Limitations and Future Work

The current sampling rate and bandwidth limit the recovery of fine palmprint and palmvein details, and in some cases polarity inversion leads to grayscale inaccuracies. Future work will explore higher-fidelity signal acquisition and refined processing techniques to improve reconstruction quality. In addition, the evaluation has so far focused on short-range scenarios; studying long-range feasibility with advanced antennas and denoising remains an open direction.

## VII. RELATED WORK

**EM Side-channel Eavesdropping on Hardware.** Prior work has demonstrated EM exploitation across diverse systems: keystroke and browsing reconstruction from GPUs [43], high-fidelity iris recovery from NIR sensors [11], and video stream extraction from cameras [13]. Research has shown smartphone magnetometers can analyze EM footprints to infer applications [44], while wireless charging leaks sensitive information through EM emissions [45], [46]. Additional studies revealed EM vulnerabilities in cryptographic implementations [47], smartphone activity inference [48], USB device fingerprinting [49], and IoT activity profiling [50].

**Intentional Electromagnetic Interference on Hardware.** Recent studies have demonstrated that intentional electromagnetic interference (IEMI) can be exploited as a powerful non-contact attack vector against sensing and imaging systems. GlitchHiker [51] demonstrates that IEMI can disrupt the image signal transmission of cameras, inducing controlled glitches that manipulate captured frames. GhostType [52] shows that IEMI can inject phantom keystrokes into keyboard circuits, enabling large-scale fake inputs and denial-of-service. GhostShot [53] further reveals that IEMI can inject arbitrary grayscale or colored patterns into CCD cameras, falsifying computer vision tasks under normal lighting.

## VIII. CONCLUSION

In this paper, we propose EMPALM, the first EM side-channel attack recovering palm biometrics from recognition systems. EMPALM handles both single- and dual-modality systems by reverse-engineering transmission protocols and employing three techniques: frame boundary identification with modality disentanglement, multi-band image combination for bit recovery, and DiffPIR-based texture restoration. Our experiments show that EMPALM reconstructs high-fidelity palm images from EM signals, exhibiting strong structural similarity, high signal quality, and low perceptual discrepancy, as well as enabling successful spoofing across diverse recognition systems. These findings reveal critical vulnerabilities in existing palm recognition systems, stressing the importance of using improved shielding, protocol hardening, and multi-factor defenses for better security.

## REFERENCES

- [1] L. Fei, G. Lu, W. Jia, S. Teng, and D. Zhang, "Feature extraction methods for palmprint recognition: A survey and evaluation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 2, pp. 346–363, 2019.
- [2] C. Gao, Z. Yang, W. Jia, L. Leng, B. Zhang, and A. B. J. Teoh, "Deep learning in palmprint recognition-a comprehensive survey," *arXiv preprint arXiv:2501.01166*, 2025.
- [3] D. Fan, X. Liang, W. Jia, J. Chen, and D. Zhang, "A novel hybrid fusion combining palmprint and palm vein for large-scale palm-based recognition," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 54, no. 7, pp. 4471–4484, 2024.
- [4] F. B. of Investigation, "Next generation identification," <https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints>, 2013, accessed: 2025-08-24.
- [5] D. Zhong and J. Zhu, "Centralized large margin cosine loss for open-set deep palmprint recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 6, pp. 1559–1568, 2019.
- [6] K. W. Bowyer and M. J. Burge, *Handbook of iris recognition*. Springer, 2016.
- [7] S. O. INTELLIGENCE, "Palm print and vein recognition module," <https://www.sunnyaiot.com/shuangmuxiangji>, 2022, accessed: 2025-08-24.
- [8] N. Luo, Z. Guo, G. Wu, and C. Song, "Joint palmprint and palmvein verification by dual competitive coding," in *2011 3rd International Conference on Advanced Computer Control*, 2011, pp. 538–542.
- [9] HandPass, "Handpass 100 dual-modal palm scanning camera," [https://deptrum.com/en/site/product\\_details/454](https://deptrum.com/en/site/product_details/454), 2018, accessed: 2025-08-24.
- [10] J. C. Maxwell, *The Scientific Papers of James Clerk Maxwell...* University Press, 1890, vol. 2.
- [11] W. Li, J. Wang, G. Zhang, Y. Yang, R. Spolaor, X. Cheng, and P. Hu, "Emiris: Eavesdropping on iris information via electromagnetic side channel," *NDSS*, 2025.
- [12] J. Choi, H.-Y. Yang, and D.-H. Cho, "Tempest comeback: A realistic audio eavesdropping threat on mixed-signal socs," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 1085–1101.
- [13] Y. Long, Q. Jiang, C. Yan, T. Alam, X. Ji, W. Xu, and K. Fu, "Em eye: Characterizing electromagnetic side-channel eavesdropping on embedded cameras," *NDSS*, 2024.
- [14] DPA, "Bnd relocates to belin," <https://www.welt.de/regionales/bayern/article184668046/Bundesnachrichtendienst-Der-Umzug-der-Spione.html>, 2018, accessed: 2025-08-24.
- [15] Amazon Web Services, "Amazon one — palm-based identity service," <https://aws.amazon.com/one/>, 2023, accessed: 2025-08-24.
- [16] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05)*, vol. 1. Ieee, 2005, pp. 886–893.
- [17] A. Kong, D. Zhang, and M. Kamel, "A survey of palmprint recognition," *pattern recognition*, vol. 42, no. 7, pp. 1408–1418, 2009.
- [18] D. Zhang, W. Zuo, and F. Yue, "A comparative study of palmprint recognition algorithms," *ACM computing surveys (CSUR)*, vol. 44, no. 1, pp. 1–37, 2012.
- [19] W. Kang and Q. Wu, "Contactless palm vein recognition using a mutual foreground-based local binary pattern," *IEEE transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1974–1985, 2014.
- [20] L. Zhang, Z. Cheng, Y. Shen, and D. Wang, "Palmprint and palmvein recognition based on dcnn and a new large-scale contactless palmvein dataset," *Symmetry*, vol. 10, no. 4, p. 78, 2018.
- [21] B. K. Gunturk, J. Glotzbach, Y. Altunbasak, R. W. Schafer, and R. M. Mersereau, "Demosaicking: color filter array interpolation," *IEEE Signal processing magazine*, vol. 22, no. 1, pp. 44–54, 2005.
- [22] MIPI Alliance, "Mipi csi-2 specifications," <https://www.mipi.org/specifications/csi-2>, 2023, accessed: 2025-08-24.
- [23] A. Lee, "Mipi csi interface definitions and protocol layer overview," <https://huaqianlee.github.io/2021/09/22/Camera/MIPI%20interface%20overview/>, 2021, accessed: 2025-08-24.
- [24] W. Grant, "Palm scanning gains ground as retail biometric of choice," *PaymentsJournal*, June 2025, accessed: 2025-08-24.
- [25] CCC, "Chaos communication congress 2018," [https://media.ccc.de/v/35c3-9545-venenerkennung\\_hacken#t=759](https://media.ccc.de/v/35c3-9545-venenerkennung_hacken#t=759), accessed: 2025-08-24.
- [26] M. Marinov, "Remote video eavesdropping using a software-defined radio platform," in *MS Thesis*, 2014. [Online]. Available: <https://api.semanticscholar.org/CorpusID:261364519>
- [27] Cadence Design Systems, "Mipi csi-2 tx controller," [https://www.cadence.com/en\\_US/home/tools/silicon-solutions/protocol-ip/interface-ip/mipi/mipi-csi-2-tx-controller.html](https://www.cadence.com/en_US/home/tools/silicon-solutions/protocol-ip/interface-ip/mipi/mipi-csi-2-tx-controller.html), 2025, accessed: 2025-08-24.
- [28] Y. Zhu, K. Zhang, J. Liang, J. Cao, B. Wen, R. Timofte, and L. V. Gool, "Denoising diffusion models for plug-and-play image restoration," 2023, accessed: 2025-08-24. [Online]. Available: <https://arxiv.org/abs/2305.08995>
- [29] B. Kavar, M. Elad, S. Ermon, and J. Song, "Denoising diffusion restoration models," 2022. [Online]. Available: <https://arxiv.org/abs/2201.11793>
- [30] Ettus Research, "Ettus research usrp products," <https://www.ettus.com/products/>, accessed: 2025-08-27.
- [31] D. Luo, Y. Qiao, D. Xie, S. Zhang, and W. Kang, "Palm vein recognition under unconstrained and weak-cooperative conditions," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4601–4614, 2024.
- [32] Y. Ma, H. Huang, D. Luo, S. Zhang, W. Kang, and D. Xie, "Focal contrastive learning for palm vein authentication," *IEEE Transactions on instrumentation and measurement*, vol. 72, pp. 1–15, 2023.
- [33] Y. Hao, Z. Sun, T. Tan, and C. Ren, "Multispectral palm image fusion for accurate contact-free palmprint recognition," in *2008 15th IEEE International Conference on Image Processing*. IEEE, 2008, pp. 281–284.
- [34] L. Zhang, L. Li, A. Yang, Y. Shen, and M. Yang, "Towards contactless palmprint recognition: A novel device, a new benchmark, and a collaborative representation based identification approach," *Pattern Recognition*, vol. 69, pp. 199–212, 2017.
- [35] CASIA, "Casia palmprint image database," <http://biometrics.idealtest.org>, 2005, accessed: 2025-08-24.
- [36] J. Jin, L. Shen, R. Zhang, C. Zhao, G. Jin, J. Zhang, S. Ding, Y. Zhao, and W. Jia, "Pce-palm: Palm crease energy based two-stage realistic pseudo-palmprint generation," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 38, no. 3, 2024, pp. 2616–2624.
- [37] J. Jin, C. Zhao, R. Zhang, S. Shang, J. Xu, J. Zhang, S. Wang, Y. Zhao, S. Ding, W. Jia *et al.*, "Diff-palm: Realistic palmprint generation with polynomial creases and intra-class variation controllable diffusion models," in *Proceedings of the Computer Vision and Pattern Recognition Conference*, 2025, pp. 26367–26376.
- [38] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," *arXiv preprint arXiv:1512.03385*, 2015.
- [39] S. Chen, Y. Liu, X. Gao, and Z. Han, "Mobilefacenets: Efficient cnns for accurate real-time face verification on mobile devices," in *Chinese conference on biometric recognition*. Springer, 2018, pp. 428–438.
- [40] A. Genovese, V. Piuri, K. N. Plataniotis, and F. Scotti, "Palmet: Gabor-pca convolutional networks for touchless palmprint recognition," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3160–3174, 2019.
- [41] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *Proceedings of the IEEE/CVF*

conference on computer vision and pattern recognition, 2019, pp. 4690–4699.

- [42] S. Shang, C. Zhao, R. Zhang, J. Jin, J. Zhang, R. Guo, S. Ding, Y. Wu, Y. Zhao, and W. Jia, “Pvtree: Realistic and controllable palm vein generation for recognition tasks,” in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 39, no. 7, 2025, pp. 6767–6775.
- [43] Z. Zhan, Z. Zhang, S. Liang, F. Yao, and X. Koutsoukos, “Graphics peeping unit: Exploiting em side-channel information of gpus to eavesdrop on your neighbors,” in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 1440–1457.
- [44] Z. Zhu, H. Pan, Y.-C. Chen, X. Ji, F. Zhang, and C.-W. You, “Magattack: Remote app sensing with your phone,” in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, 2016, pp. 241–244.
- [45] T. Ni, J. Li, X. Zhang, C. Zuo, W. Wang, W. Xu, X. Luo, and Q. Zhao, “Exploiting contactless side channels in wireless charging power banks for user privacy inference via few-shot learning,” in *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, 2023, pp. 1–15.
- [46] T. Ni, X. Zhang, C. Zuo, J. Li, Z. Yan, W. Wang, W. Xu, X. Luo, and Q. Zhao, “Uncovering user interactions on smartphones via contactless wireless charging side channels,” in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 3399–3415.
- [47] Y. Cheng, X. Ji, W. Xu, H. Pan, Z. Zhu, C.-W. You, Y.-C. Chen, and L. Qiu, “Magattack: Guessing application launching and operation via smartphone,” in *Proceedings of the 2019 ACM Asia conference on computer and communications security*, 2019, pp. 283–294.
- [48] Y. Fu, L. Yang, H. Pan, Y.-C. Chen, G. Xue, and J. Ren, “Magspy: Revealing user privacy leakage via magnetometer on mobile devices,” *IEEE Transactions on Mobile Computing*, 2024.
- [49] O. A. Ibrahim, S. Sciancalepore, G. Oligeri, and R. D. Pietro, “Magnetot: Fingerprinting usb flash drives via unintentional magnetic emissions,” *ACM Trans. Embed. Comput. Syst.*, vol. 20, no. 1, Dec. 2020. [Online]. Available: <https://doi.org/10.1145/3422308>
- [50] A. Amodei, D. Capriglione, L. Ferrigno, G. Miele, L. Tari, G. Tomasso, and G. Cerro, “Experimental analysis of side-channel emissions for iot devices activities’ profiling,” in *2023 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT)*, 2023, pp. 42–47.
- [51] Q. Jiang, X. Ji, C. Yan, Z. Xie, H. Lou, and W. Xu, “{GlitchHiker}: Uncovering vulnerabilities of image signal transmission with {IEMI},” in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 7249–7266.
- [52] Q. Jiang, Y. Ren, Y. Long, C. Yan, Y. Sun, X. Ji, K. Fu, and W. Xu, “Ghosttype: 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.
- [53] Y. Ren, Q. Jiang, C. Yan, X. Ji, and W. Xu, “Ghostshot: Manipulating the image of ccd cameras with electromagnetic interference,” in *NDSS*, 2025.

## APPENDIX

**Temporal Alternation and Signal Separation.** Through detailed analysis of the captured electromagnetic emanations, we observe that the dual-modal biometric system exhibits a consistent frame-interleaved transmission pattern, alternating between palmprint and palmvein acquisition. This temporal multiplexing manifests in the electromagnetic domain as distinct frame-level modulations that can be exploited for signal separation. The modality assignment is defined as

$$M_k = k \bmod 2, \quad (11)$$

where  $M_k = 0$  corresponds to palmprint frames and  $M_k = 1$  to palmvein frames. The fundamental challenge in reconstructing dual-modal signals lies in the superposition of heterogeneous image data within the aggregate electromagnetic field. Without proper separation, a naive reconstruction would compute

$$P_{mixed}[r, c] = \frac{1}{K} \sum_{k=0}^{K-1} |s_{IQ}^{(k)}[r, c]|, \quad (12)$$

which results in severe degradation of biometric features from both palmprint and palmvein patterns due to averaging across fundamentally different image characteristics.

**Frame-Level Reconstruction Process.** The reconstruction methodology for dual-modal systems extends the single-modal approach by introducing a temporal demultiplexing stage prior to image formation. For each captured electromagnetic frame, the complex-valued IQ samples undergo demodulation and envelope extraction to recover amplitude variations corresponding to pixel intensities. The separated reconstruction for palmprint images is given by

$$P_{print}[r, c] = \frac{1}{N_{print}} \sum_{j=0}^{N_{print}-1} |s_{IQ}^{(2j)}[r, c]|, \quad (13)$$

while palmvein reconstruction processes the complementary set of frames:

$$P_{vein}[r, c] = \frac{1}{N_{vein}} \sum_{j=0}^{N_{vein}-1} |s_{IQ}^{(2j+1)}[r, c]|. \quad (14)$$

Here,  $N_{print}$  and  $N_{vein}$  denote the number of frames assigned to each modality, which are typically equal when the capture duration spans an even number of frames. This separation preserves the distinct electromagnetic signatures of each biometric type: palmprint signals generally exhibit higher amplitude variations due to surface texture transitions, whereas palmvein signals show lower-contrast patterns reflecting sub-surface vascular structures.

**Synchronization and Alignment Considerations.** The efficacy of temporal separation depends critically on accurate frame alignment between electromagnetic acquisition and the underlying camera protocol. Frame boundaries within the continuous EM stream can be detected by identifying blanking intervals:

$$B(t) = \begin{cases} 1, & |s_{env}(t)| < \theta_{blank} \\ 0, & \text{otherwise,} \end{cases} \quad (15)$$

where  $s_{env}(t)$  is the signal envelope and  $\theta_{blank}$  is the blanking threshold. Frame start times are then determined by

$$t_{frame}^{(k)} = \{t : B(t - \epsilon) = 1 \wedge B(t + \epsilon) = 0\}, \quad (16)$$

which indicates transitions from blanking to active transmission. Misalignment by even a single frame causes modality inversion, quantified by the reconstruction error

$$E_{misalign} = \|P_{print}^{true} - P_{vein}^{recon}\|_2^2 + \|P_{vein}^{true} - P_{print}^{recon}\|_2^2. \quad (17)$$

Once initial alignment is established, continuous tracking compensates for clock drift between the SDR sampling clock and the camera's pixel clock. The drift rate can be estimated as

$$\delta_f = \frac{f_{camera} - f_{SDR}}{f_{SDR}}, \quad (18)$$

which requires periodic realignment every  $N_{drift} = 1/\delta_f$  frames to maintain synchronization integrity during extended captures.