EMIRIS: Eavesdropping on Iris Information via Electromagnetic Side Channel

Wenhao Li, Jiahao Wang, Guoming Zhang*, Yanni Yang, Riccardo Spolaor, Xiuzhen Cheng, Pengfei Hu
School of Computer Science and Technology, Shandong University, Qingdao, China
Email: {li_wenhao, wangjiahao0304}@mail.sdu.edu.cn, {guomingzhang, yanniyang, rspolaor, xzcheng, phu}@sdu.edu.cn

Abstract—**Iris recognition is one of the most secure biometric methods due to the uniqueness and stability of iris patterns, as well as their resistance to forgery. Consequently, it is frequently used in high-security authentication scenarios. However, systems using Near-Infrared (NIR) sensors may expose the iris information of users, leading to significant privacy risks. Our research found that the electromagnetic (EM) emissions generated during data transmission of NIR sensors are closely related to iris data. Based on this observation, we propose EMIRIS, a method for reconstructing the iris information using EM side channels. By deconstructing the digital signal transmission format of the NIR sensors and the mapping mechanism of the iris data matrix, we can reconstruct iris information from EM signals and convert it into iris images. To improve the quality of the reconstructed iris, we model the denoising and restoration of iris texture details as a linear inverse problem and tailor a diffusion model to solve it. Extensive experimental evaluations show that EMIRIS can effectively reconstruct iris information from commercial iris recognition devices, achieving an average SSIM of 0.511 and an average FID of 7.25. Even more concerning, these reconstructed irises can effectively spoof the classical iris recognition model with an average success rate of 53.47% on more than 3,000 iris samples from 50 different users.**

I. INTRODUCTION

Since being introduced by John Daugman, iris recognition [1] has made substantial progress in the field of biometrics and has become a widely used and highly regarded technology. The iris possesses a considerable amount of entropy and remains stable throughout an individual's life [2]. These characteristics contribute to iris recognition's superiority over face and fingerprint recognition in terms of accuracy and the lowest false match rate (FMR) [3]. It is widely acknowledged that iris recognition technology is the most promising form of biometric identification in the twenty-first century [4] and has been integrated into critical applications such as ATM machines [5], [6], access control systems [7], IoT [8], and mobile devices [9]. Furthermore, numerous countries and organizations have incorporated iris information as a central biometric identifier in their identification programs, with the Aadhaar [10] program being a notable example, having collected data from billions of individuals.

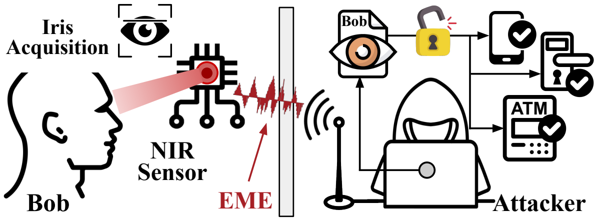


Fig. 1. Attack scenario of EMIRIS.

Iris recognition devices typically employ near-infrared (NIR) sensors to capture iris data [3]. The NIR wavelengths, ranging from 700 to 900nm, are imperceptible to the human eye, thus preventing pupil contraction and dilation. More importantly, the iris texture is more discernible in the NIR spectrum, which increases the entropy available for identification and enhances the system's accuracy and security. However, the time-varying currents within sensor circuits generate electromagnetic (EM) waves, as dictated by Maxwell's equations, and the data transmission wires can act as antennas, broadcasting this information and potentially providing adversaries with unauthorized access to critical data. The study of electromagnetic emissions (EME) from sensors has been applied in various attack scenarios. Initially, researchers exploited this radiation to recover cryptographic keys from System on Chip (SoC) [11], underscoring the risks of key leakage. More than that, EM side-channel attacks on physical devices pose an even greater threat. Prior to the comprehensive implementation of EM leakage standards, these emissions were shown to be capable of eavesdropping on computer screens [12]. Modern sensors have significantly mitigated EM leakage to much lower levels, rendering most current studies feasible only at very close distances to the target device (typically 1-10cm), which is impractical for real-world applications. Recently, there has been research on inferring images using EM emissions [13]. They utilize the EM emissions from RGB cameras to reconstruct low-resolution images. Nonetheless, these reconstructed images often suffer from a significant loss of critical details. However, to the best of our knowledge, no research has been conducted on the EM emissions of NIR sensors, and none of the existing techniques are applicable to the reconstruction of iris information.

In this paper, we present EMIRIS, the first eavesdropping attack capable of reconstructing iris information from near-infrared sensors. It leverages the unintentional EME generated by the NIR sensors during data transmission to reconstruct digital information and maps it to iris grayscale matrix, which

* Corresponding author.

Network and Distributed System Security (NDSS) Symposium 2025
24-28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-8-3
https://dx.doi.org/10.14722/ndss.2025.240200
www.ndss-symposium.org

can subsequently be converted to image to deceive iris recognition systems. To achieve EMIRIS, we need to address three major challenges:

1) How to reconstruct iris information with EM emissions from NIR sensors? The EM emissions of NIR sensors are transmitted as one-dimensional signals in the time domain. However, the target iris is two-dimensional, containing indices and values. Mapping these one-dimensional wireless signals to a two-dimensional matrix is challenging. To address this, we analyze the data transmission format of the NIR sensor. We find that the voltage signal of each data unit is converted into a one-dimensional digital signal for transmission. In the signal processor, these signals are mapped into a grayscale matrix according to a specific pattern. By correlating the captured EM signals with the digital signals, we propose an EM-to-Iris mapping method to determine which parts of the EM signal correspond to a specific index in the data matrix, thereby reconstructing a two-dimensional iris matrix where each element represents a grayscale value.

2) How to increase distance while maintaining the quality of the reconstructed iris? Due to regulations and low-power designs, modern electronic devices emit significantly weaker EM radiation, limiting the range of most side-channel attacks. In our work, increasing the distance leads to greater attenuation of EM emission, causing more distorted reconstructed iris data. Thus, maintaining attack effectiveness while increasing distance is a challenge. To address this, we use Low-Noise Amplifiers (LNA) and apply frequency- and time-domain equalization algorithms to improve the quality of EM signal. Additionally, we propose an integrated spatial enhancement approach to optimize distorted iris data, emphasizing iris details while enhancing eye contours, thus maximizing the retention of iris and eye features.

3) How to enhance iris texture details to spoof iris recognition systems? Distance-induced electromagnetic attenuation, channel noise, and mapping errors can cause distortion and noise in the reconstructed iris grayscale matrix, leading to loss of fine details and affecting ML-based iris recognition model decisions. To denoise and enhance texture details, we model the reconstruction process as a linear inverse problem and use a diffusion model to solve this problem. For this process, we leverage a pre-trained probabilistic diffusion model trained by clean iris data as the prior. Then, the half-quadratic-splitting method is adopted to reconstruct the degraded iris iteratively. The proposed reconstruction method is a plug-and-play method and does not need numerous clean-degraded image pairs to train a generative model, hence the degraded iris can be reconstructed more efficiently.

In summary, our major contributions are:

- In this paper, we introduce EMIRIS, the first approach designed to reconstruct iris information, which can be used to spoof iris recognition systems. It leverages EM emissions from near-infrared sensors to generate grayscale matrices and employs EM signal and image enhancement algorithms to achieve high-quality iris image reconstruction.
- We model the iris enhancement process as a linear inversion problem, to solve this problem, we propose a plug-and-play method that leverages a pre-trained probabilistic diffusion model as the prior and adopts the half-quadratic-splitting method to reconstruct the degraded iris iteratively.
- We conduct extensive experiments using multiple datasets and ML-based iris recognition models to validate EMIRIS. Our method effectively reconstructs iris images from different devices and spoofs iris recognition models, achieving an average SSIM of 0.511, an average FID of 7.25, and a spoofing success rate of 53.47% on 3,324 iris samples.

The remainder of the paper is organized as follows. We discuss the background and feasibility in Section II. In Section III, we describe the motivation and threat model of this work. Section IV presents the overview and methodology of the system. We experimentally evaluate our EMIRIS prototype in Section V. Section VI explores potential defense options and offers additional insights on EMIRIS. Finally, we conclude our paper in Section VIII.

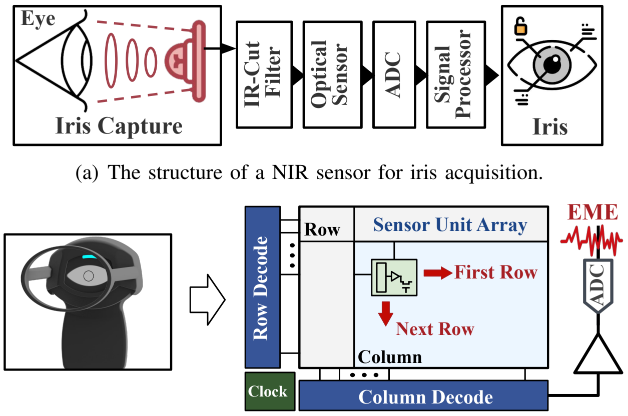
II. Preliminaries

This section first describes the components of the iris recognition system, then analyzes the principles of digital signal transmission of the NIR sensors, and finally explores the feasibility of EM emissions being used to reconstruct the iris information through a preliminary experiment.

A. Iris Recognition

The iris is an essential component of the eye and is responsible for controlling the diameter and size of the pupil to adapt to different ambient light. The textural structure of the human iris develops from the third month of embryonic life, becomes fully formed by the eighth month, and remains relatively stable throughout life, except for biological changes caused by disease and normal aging [14]. According to [3], a typical iris recognition system comprises three main parts: iris information acquisition, iris information processing, and iris feature extraction and matching. In the first part, the iris acquisition device captures iris information from users at a distance of 20cm to 40cm, and this information is subsequently transmitted and stored on terminal devices. The second part involves iris segmentation using methods such as edge detection and the Hough transform. The data are then normalized using the Daugman rubber-sheet model [3] to facilitate feature extraction. The third part uses processed iris data for feature extraction and matching.

Advancements in iris recognition technology have optimized algorithms in each of these parts, particularly with the rapid development of deep learning (DL) models, which significantly enhance iris recognition capabilities. Nevertheless, the fundamental three-step process remains unchanged. As illustrated in Figure 1, this paper focuses on attacking the iris information acquisition phase by analyzing the EM emissions generated by the NIR sensors. The reconstructed iris is subsequently optimized and input into the iris recognition model to attack the iris recognition system.



(a) The structure of a NIR sensor for iris acquisition.

(b) NIR iris recognizer and its internal transmission principle.

Fig. 2. Principle of iris data acquisition by NIR sensor.

B. Near-Infrared Sensor

The iris acquisition system must capture high-quality iris data to extract sufficient information for the recognition task. To achieve this, NIR sensors are commonly chosen for iris acquisition because iris textures are more pronounced in the NIR spectrum compared to the visible light spectrum. Near-infrared light falls between visible light and mid-infrared light on the electromagnetic spectrum, with wavelengths ranging from 780nm to 2526nm [15], which are invisible to the human eye. NIR sensors are initially designed for medical and industrial applications. Advances in semiconductor technology have reduced the cost of these sensors, making NIR sensors widely used for iris data acquisition.

Figure 2 illustrates the process and principles of iris capture and transmission by an NIR sensor. Initially, the front end of the NIR sensor receives light and uses an NIR filter to filter out specific wavelengths of light (typically at 850 nm). Then, the optical sensor detects and processes the filtered light. Specifically, these light signals are converted into electric charges by photodiodes, with the amount of charge being proportional to the intensity of the light. To read these electric charges, the optical sensor scans row by row and column by column, sequentially reading the charges of each row and converting them into voltage signals. These voltage signals are then sent to an output amplifier. The amplified electrical signals are converted into digital signals by an analog-to-digital converter (ADC). These digital signals are transmitted to the signal processor via parallel or serial interfaces (such as MIPI CSI-2, USB, etc.). In the signal processor, the received digital signals are denoised, corrected, and enhanced to ultimately generate the iris grayscale image. During the transmission process, the wires can act as antennas, which could cause data from these digital signals to be unintentionally broadcast into the air by EM signals.

C. Feasibility Study

To capture these unintended EM emissions and analyze their relationship with iris information, we conduct preliminary experiments. We select a near-infrared sensor (HK5M-H150.1) to capture the iris and a near-field magnetic field antenna to detect the EM emissions emitted during data transmission. To more clearly highlight the correlation between EM emissions and grayscale values, we use white (850nm infrared reflective board) and black (black plastic board) surfaces to increase image contrast. As shown in Figure 3, the white areas correspond to lower EM intensity, while the opposite is true for the black areas. The experimental results confirm a correlation between EM intensity and grayscale values during iris data transmission and that data transmission occurs sequentially from left to right and from top to bottom.

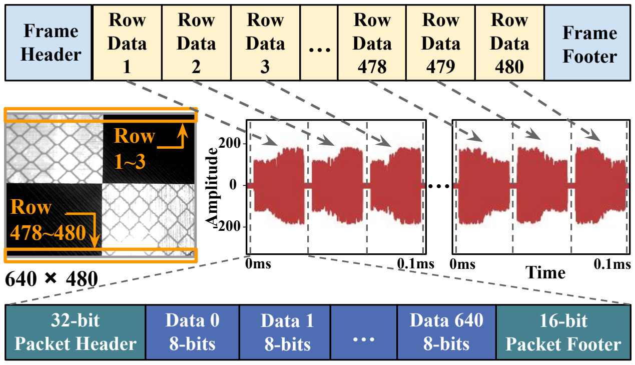
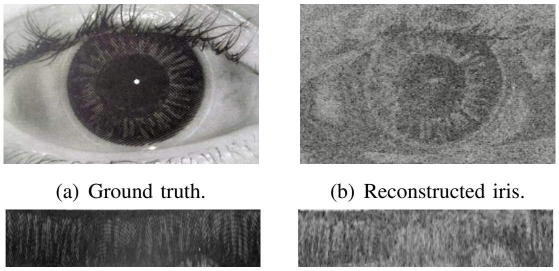


Fig. 3. EM emissions and data transmission.



(a) Ground truth.

(b) Reconstructed iris.

(c) Original iris segmentation and normalization.

(d) Reconstructed iris segmentation and normalization.

Fig. 4. Reconstruction of an iris using EM emissions from the NIR sensor.

In order to continue to explore the correlation between EM emissions and grayscale values is sufficient to reconstruct iris information, we conduct a feasibility study experimentally. We use the same NIR sensor to capture the data from human eyes, with a bit depth of 8 and a resolution of 640 × 480. We use a near-field magnetic antenna to capture EM emissions and process the received EM signals using amplitude demodulation. We sequentially map the amplitude of the EM signal to gray values according to the format in Figure 3 and finally obtain the experimental results in Figure 4, where (a) and (b) are the iris captured by the NIR sensor (ground truth) and the reconstructed iris of the human eye, and (c) and (d) are the images of the iris after segmentation and normalization are performed, respectively. It can be clearly seen that the reconstructed iris is very similar to the ground truth, but some tiny iris texture features are lost due to noise, insufficient sampling rate, and bandwidth. These preliminary results show that it is feasible to reconstruct the iris by correlating EM emissions with grayscale values. We will introduce the iris reconstruction and optimization methods in detail in Section IV to further improve the quality of the reconstructed iris.

III. Motivation and Threat Model

This section describes our motivation for designing EMIRIS as a way to reveal possible threats to iris recognition systems. In addition, we provide a detailed description of the attack scenarios and the capabilities of the adversary.

A. Motivation of EMIRIS

Iris recognition technology is widely used in critical areas such as defense, security, and payment verification, mainly because of its high accuracy and uniqueness. Despite the significant advantages of iris recognition, NIR sensors in these systems pose substantial privacy risks due to the possibility of data transmission leakage. In this study, we identify a critical vulnerability: the EM emissions leaked by the NIR sensor during iris data transmission are closely related to grayscale values. These EM emissions could be used to reconstruct iris information via side-channel attack, which will be injected into the iris recognition system, causing false acceptance. Moreover, this biological information is virtually impossible to alter artificially, creating an ongoing threat once compromised. To our knowledge, there are no specific cases of unintentional leakage of iris information due to EM leakage. Therefore, this work aims to explore the feasibility of our attacks and to assess its threat level to existing iris recognition systems.

B. Threat Model

In this paper, we consider the attack scenario illustrated in Figure 1, where the victim is undergoing iris recognition or iris acquisition. An NIR sensor captures the iris information and transmits it to the iris recognition model for identification. Due to its low-frequency band (typically in the MHz range and below), the EM emissions generated by the NIR sensor can easily penetrate building materials such as concrete and wood. An attacker can use a directional antenna outside the room or at a distance to capture these EM signals, which can then be used to reconstruct the iris information. These reconstructed iris are optimized at the attacker's computing terminal and used to spoof the iris recognition model. In particular, we assume the following scenario and attacker capabilities:

- The attacker can only place the antenna in a location that does not arouse suspicion, such as outside the room or at a distance.
- The attacker cannot install any devices or sensors in the room or on the target device.
- The victim is capturing iris information using an NIR sensor.
- The attacker cannot access the target NIR sensor to obtain the iris data.
- The attacker has no information about the victim and cannot capture the victim's iris through a high-definition camera.

IV. Design of EMIRIS

In this section, we present the system architecture of EMIRIS. Figure 5 provides an overview of our system and its modules. In what follows, we introduce the three modules that compose EMIRIS and their roles in reconstructing high-quality iris from the EM emissions.

1) EM Emissions to Iris Matrix Mapping (EIM) module first receives the unintentionally leaked EM signals from the NIR sensor. These signals are amplified by a low-noise amplifier and optimized in the digital domain to eliminate time-delay distortion and frequency response distortion. In this module, we analyze the principles of processing and transmitting data in NIR sensors. Then, we use the correlation between EM emissions and grayscale values to map the one-dimensional EM signals into a two-dimensional iris matrix according to the digital domain transmission format.

2) Iris Data Enhancement (IDE) aims to optimize the raw iris data extracted by EIM, initially enhancing eye features and eliminating some noise. To achieve this goal, we propose a comprehensive spatial enhancement method. First, we design a sharpening process that combines three well-known sharpening techniques to highlight contours, textures, and subtle features in the iris. Next, we apply Dynamic Histogram Equalization (DHE) to the sharpened iris to further optimize the contrast. Finally, we use a median filter to remove salt-and-pepper noise.

3) Iris Denoising and Detail Generation (IDG) The iris denoising and detail generation module is designed to eliminate distortions caused by mapping errors, insufficient practical sampling rate, and wireless channel noise during iris reconstruction. These distortions not only affect the iris quality but also lead to the loss of detailed features. Therefore, this module also needs to realize the detailed generation of iris. To this end, we model the denoising and iris detail enhancement process as a linear inverse problem and leverage a pre-trained diffusion model as the data prior, then we adopt the HQS method to solve this problem in a plug-and-play manner to reconstruct the iris images with high-quality.

A. EM Emissions to Iris Matrix Mapping

Figure 2 illustrates the data transmission principle of an NIR sensor for each frame of iris data. In each frame, the data units are scanned row by row and processed column by column. Each row of data unit is read and converted from analog to digital one by one. Once all the data units in a row are read, the column controller moves to the next row and repeats the process. It is important to note that the system clock controls the reading and scanning speed of each row, creating a time interval between the data streams of consecutive rows. As shown in Figure 3, this time interval is also reflected in the EM signal, which facilitates the extraction of different grayscale values from different rows. During data transmission, to ensure the stability of the entire frame cycle, the system clock typically introduces slight time redundancies. These redundancies (which may be on the order of microseconds) are sufficient to split frames in a one-dimensional data stream.

In order to extract iris information from EM signals, we need to analyze the transmission format of the data stream. Taking the resolution $W \times H$ as an example (as shown in Figure 3), there are W data units in each row, and there are a total of H rows in each frame. In this case, the data needs to be frame synchronized using the frame header and frame footer. In each frame, row synchronization is achieved using long data packets, each of which contains a packet header (occupying 32 bits), W packets of data (each occupying 8 bits), and a packet footer (occupying 16 bits). Each frame contains H such long packets. In addition, the EM emissions may contain other components such as channel noise and multipath effects, etc.,

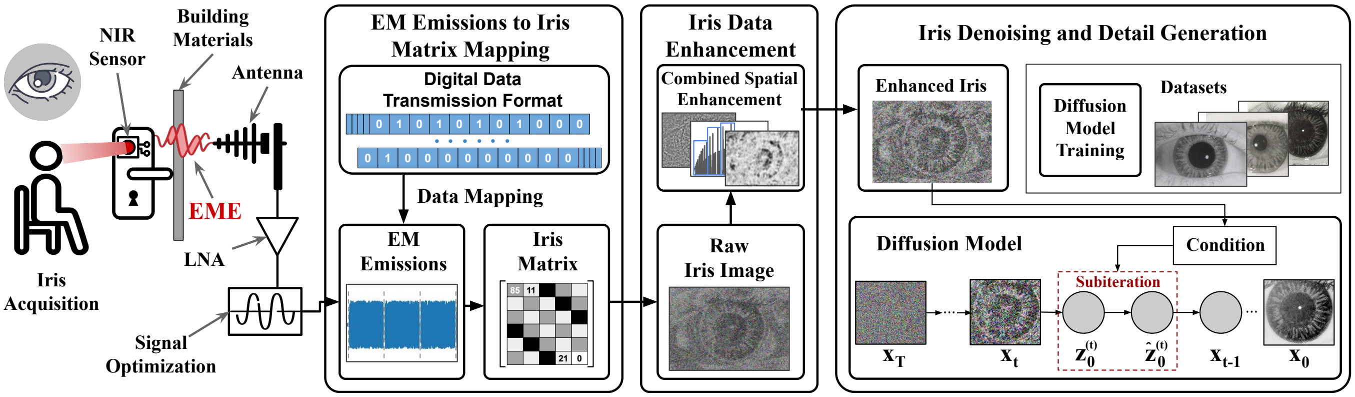


Fig. 5. System overview of EMIRIS.

which can cause the generated iris to contain noise. Therefore, we model the reconstruction of the grayscale matrix using EM emissions as the following equation,

$$\mathsf{IRIS}_{\text{raw}}(f) = M_{\text{E2I}}\{f, E, M_{\text{D2I}}(D_{\text{digi}}, G)\} + W(f), \quad (1)$$

where $\mathsf{IRIS}_{\text{raw}}(\cdot)$ represents the raw grayscale matrix of iris, f denotes the central frequency, $M_{\text{D2I}}(\cdot)$ is a function that maps one-dimensional digital data to a two-dimensional matrix based on grayscale, and G represents the grayscale values corresponding to each data unit. E signifies the temporal electromagnetic radiation signal. $W(f)$ represents the noise due to the channel effect in a certain frequency band. $M_{\text{E2I}}(\cdot)$ is a function that maps the one-dimensional electromagnetic radiation signal to a two-dimensional matrix according to the mapping pattern defined by $M_{\text{D2I}}(\cdot)$, where each value in the matrix represents the intensity of the EM emission.

It is worth noting that the presence of $W(f)$ in Eqn. (1) significantly affects the quality of the reconstructed iris, which is due to the delay distortion and channel effect. In order to optimize the reconstructed iris, we need to improve the quality of the EM signal. The low noise amplifier can effectively increase the signal-to-noise ratio of the received signal, but it cannot eliminate the negative factors mentioned above. Therefore, in addition to the use of signal amplifiers, the optimization of EM signals using signal processing methods in the digital domain is also necessary. The single carrier frequency domain equalization (SC-FDE) technique [16] has a lower peak-to-average power ratio and lower sensitivity to carrier frequency deviation. Therefore, here we use a time-domain equalizer to eliminate the effects due to time-delay distortion, while a linear frequency-domain equalizer is utilized to counteract frequency response distortion due to multipath propagation. Let the received signal be discrete data $s[n]$, then the signal after equalization is as follows,

$$\tilde{s}[n] = \sum_{m=0}^{L-1} b_m s[n-m], \quad (2)$$

$$\hat{s}[n] = \mathsf{IDFT}\{\mathsf{DFT}(\tilde{s}[n])H[k]\}, \quad (3)$$

where L is the memory window of the time domain equalizer, b_m are the filtering coefficients of the time domain equalizer, k denotes the discrete frequency index, and $H[k]$ is the frequency response of the frequency domain equalizer. Then, we replace E in Eqn. (1) with the optimized signal $\hat{s}[n]$ to obtain the raw iris data.

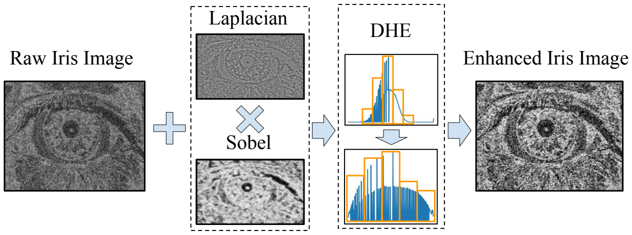


Fig. 6. Iris Data Enhancement Process.

B. Iris Data Enhancement

The raw iris data from the EIM module is typically of poor quality due to the combined effects of channel noise, mapping errors, and optical sensor inaccuracies. These adverse factors lead to reduced contrast, which in turn affects the reconstruction of iris details. Sharp-edged irises contain more high-frequency information, which provides crucial structure and detail during the iris reconstruction process. To generate high-quality irises, we propose a combined spatial enhancement method to highlight the details and edges of the iris texture. First, we sharpen the raw iris data using the first derivative, with the specific equation as follows:

$$M_s(a,b) = mag(\nabla\mathsf{IRIS}_{\text{raw}}) = \sqrt{g_a^2 + g_b^2}, \quad (4)$$

where $M_s(\cdot)$ is a gradient magnitude map of the same size as the original iris matrix, which is created when a and b are varied at all positions of $\mathsf{IRIS}_{\text{raw}}$, $mag(\cdot)$ represents the magnitude of the matrix gradient, g_a and g_b denote the gradient of the matrix in the horizontal and vertical directions, respectively, which is computed here using the Sobel operator. Then, the second-order derivative is used to sharpen the raw iris matrix:

$$M_l(a,b) = \mathsf{IRIS}_{\text{raw}}(a,b) + c[\nabla^2\mathsf{IRIS}_{\text{raw}}(a,b)], \quad (5)$$

where $M_l(a,b)$ denotes the grayscale value of the sharpened matrix at position (a,b), and c is a constant (taken as 1 here) used to adjust the degree of influence of the Laplace operator on the raw iris. Smoothing the Sobel matrix using a 5×5 box filter and multiplying it with the Laplace-sharpened matrix results in an optimized iris data as follows,

$$\mathsf{IRIS}_{\text{shp}} = [M_s * H_{5\times5}] \cdot M_s + \mathsf{IRIS}_{\text{raw}}. \quad (6)$$

We further processed the sharpened iris data $\mathsf{IRIS}_{\mathrm{shp}}$ using a dynamic histogram equalization technique to preserve details better and avoid over-enhancement and noise amplification:

$$\mathsf{IRIS}_{\mathrm{opt}} = \mathsf{IRIS}_{shp} \times \left(\frac{\sum i = 0^k P(r_i)}{\sum P(r_i)} \right), \tag{7}$$

where $P(r_i)$ is the probability density function of the gray level r_i and the cumulative density function is applied for gray range assignment. After enhancing the contrast and redistributing the pixel values, we apply an Adaptive Frequency Median (AFM) filter [17] to eliminate non-linear salt-and-pepper noise.

C. Iris Denoising and Detail Generation

In real-world scenarios, capturing EM signals using software-defined radios and a standard laptop often results in mismatches between the sampling rate and the digital signal transmission rate. This mismatch can lead to imperfections in the reconstructed irises, with distortion being the most prominent issue. Mapping errors and wireless channel effects also degrade the quality of the reconstructed irises, potentially rendering them unintelligible. Additionally, EM emissions may include signals from multiple transmission wires, which can interfere with or superimpose on each other, causing additional noises. This results in linear distortion in the iris data. While the IDE module has done preliminary iris data enhancement, additional techniques are essential to correct these distortions and accurately reconstruct the detailed features of the iris. To denoise the reconstructed iris, linear inversion problems are adopted to model it, and diffusion models [18], [19] are leveraged to solve the linear inversion problem.

1) Linear Inverse Problems: Linear inverse problems aim to recover an image from noisy measurements given a linear degradation model. A general linear inverse problem can be formulated as:

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{n}, \tag{8}$$

where we aim to recover the signal $\boldsymbol{x} \in \mathbb{R}^n$ (i.e. $\mathsf{IRIS}_{\mathrm{opt}}$) from the noisy measurement $\boldsymbol{y} \in \mathbb{R}^m$, $\boldsymbol{H} \in \mathbb{R}^{m \times n}$ is a known linear degradation matrix, and $\boldsymbol{n} \sim \mathcal{N}\left(0, \sigma_{\boldsymbol{y}}^2 \boldsymbol{I}\right)$ is an i.i.d. additive Gaussian noise with known variance. For our iris reconstruction problem, the degradation matrix $\boldsymbol{H}$ mainly consists of three parts, firstly, because of the limited bandwidth of the receiver, some grayscale values in the received iris matrix will be missed. Secondly, the imperfection of the EM signal and the limited sampling rate of the device may also cause pixel missing and distortion. Third, since the EM signal is a mixture of the data and clock lines, this leads to errors in some gray values in the reconstructed iris. The underlying structure of $\boldsymbol{x}$ can be modeled via a probabilistic generative model denoted as $p_\theta(\boldsymbol{x})$, via Bayes' theorem, given $\boldsymbol{y}$ and $\boldsymbol{H}$, the posterior of the signal $\boldsymbol{x}$ can be posed as: $p_\theta(\boldsymbol{x} \mid \boldsymbol{y}) \propto p_\theta(\boldsymbol{x}) p(\boldsymbol{y} \mid \boldsymbol{x})$, where the term $p(\boldsymbol{y} \mid \boldsymbol{x})$ is defined via Eqn. (8), recovering $\boldsymbol{x}$ can be done by sampling from this posterior.

2) Diffusion Models: It has been demonstrated that diffusion models have a superior ability to generate high-quality images compared to previous generative models such as GANs [20]. They generate high-quality image $\boldsymbol{x}_0$ from a noise $\boldsymbol{x}_T$ via a Markov chain $\boldsymbol{x}_T \rightarrow \boldsymbol{x}_{T-1} \rightarrow \cdots \rightarrow \boldsymbol{x}_1 \rightarrow \boldsymbol{x}_0$, which has the following distribution:

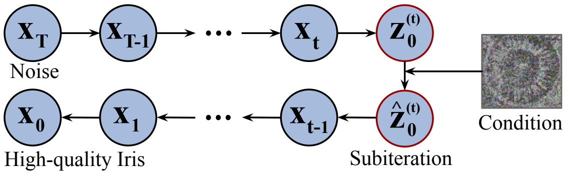


Fig. 7. Iterative process of our diffusion model.

$$p_\theta\left(\boldsymbol{x}_{0:T}\right) = p_\theta^{(T)}\left(\boldsymbol{x}_T\right) \prod_{t=0}^{T-1} p_\theta^{(t)}\left(\boldsymbol{x}_t \mid \boldsymbol{x}_{t+1}\right),$$

which is called the reverse process. The forward process is defined by:$q\left(\boldsymbol{x}_{1:T} \mid \boldsymbol{x}_0\right) = \prod_{t=1}^T q\left(\boldsymbol{x}_t \mid \boldsymbol{x}_{t-1}\right)$, and typically, $q\left(\boldsymbol{x}_t \mid \boldsymbol{x}_{t-1}\right) = \mathcal{N}\left(\boldsymbol{x}_t; \sqrt{1-\beta_t}\boldsymbol{x}_{t-1}, \beta_t \boldsymbol{I}\right)$, where $\{\beta_t\}_{t=1}^T$ are the variance scheduler parameters. By the good properties of Gaussian, we can sample $\boldsymbol{x}_t$ from $\boldsymbol{x}_0$ directly via:

$$\boldsymbol{x}_t = \sqrt{\bar{\alpha}_t}\boldsymbol{x}_0 + \sqrt{1-\bar{\alpha}_t}\epsilon,$$

where $\alpha_t = 1 - \beta_t$, $\bar{\alpha}_t = \prod_{s=1}^t \alpha_s$ and $\epsilon \sim \mathcal{N}(\mathbf{0}, \boldsymbol{I})$. To train a diffusion model, a factorized variational inference distribution is introduced to derive the evidence lower bound (ELBO) of the maximum likelihood to train the model $\boldsymbol{\epsilon}_\theta$, which aims to predict the noise added to $\boldsymbol{x}_t$ from $\boldsymbol{x}_0$. And the reverse process of the denoising diffusion probabilistic model can be formulated as:

$$\boldsymbol{x}_{t-1} = \frac{1}{\sqrt{\alpha_t}}\left(\boldsymbol{x}_t - \frac{\beta_t}{\sqrt{1-\bar{\alpha}_t}}\boldsymbol{\epsilon}_\theta\left(\boldsymbol{x}_t, t\right)\right) + \sqrt{\beta_t}\epsilon_t,$$

by which we can generate $\boldsymbol{x}_0$ from $\boldsymbol{x}_T$ step by step.

Furthermore, the diffusion process $\boldsymbol{x}(t) \in \mathbb{R}^d$, $t \in [0, T]$ can be defined by stochastic differential equation [19] as:

$$d\boldsymbol{x} = \boldsymbol{f}(\boldsymbol{x}, t)\, dt + g(t)\, d\boldsymbol{w}, \tag{9}$$

where $\boldsymbol{w}$ is the standard d-dimensional Wiener process. In order to generate samples from the pre-defined distribution $\mathcal{N}(\mathbf{0}, \boldsymbol{I})$, one can reverse SDE of Eqn. (9) and obtain:

$$d\boldsymbol{x} = \left[\boldsymbol{f}(\boldsymbol{x}, t) - g(t)^2 \nabla_{\boldsymbol{x}} \log p_t(\boldsymbol{x})\right] dt + g(t)\, \bar{\boldsymbol{w}}, \tag{10}$$

where dt corresponds to time running backward and $d\bar{\boldsymbol{w}}$ to the standard Wiener process running backward. Note that now the drift term of the reversed SDE depends on the time-dependent score function $\nabla_{\boldsymbol{x}_t} \log p_t\left(\boldsymbol{x}_t\right)$, which can be approximated by a neural network $\boldsymbol{s}_\theta$ trained through denoising score matching [21], once $\boldsymbol{s}_\theta$ is trained, it can be incorporated into Eqn. (10) to generate samples.

3) Denoising Diffusion Models for Inverse Problems Solving: Note that we aim to reconstruct the iris $\boldsymbol{x}$ given the degraded version $\boldsymbol{y}$, and thus our goal is sample from the posterior distribution $p(\boldsymbol{x} \mid \boldsymbol{y})$. To do this, note that

$$\nabla_{\boldsymbol{x}} \log p(\boldsymbol{x} \mid \boldsymbol{y}) = \nabla_{\boldsymbol{x}} \log p(\boldsymbol{y} \mid \boldsymbol{x}) + \nabla_{\boldsymbol{x}} \log p(\boldsymbol{x}). \tag{11}$$

Incorporating Eqn. (11) into Eqn. (10), we can sample from the conditional posterior via the following SDE:

$$\begin{aligned} d\boldsymbol{x} = {} & \left[\boldsymbol{f}(\boldsymbol{x}, t) - g^2(t) \nabla_{\boldsymbol{x}} \left(\log p_t(\boldsymbol{x}) + \log p_t(\boldsymbol{y} \mid \boldsymbol{x})\right)\right] dt \\ & + g(t)\, d\boldsymbol{w}, \end{aligned} \tag{12}$$

where the posterior is divided into $\log p_t(\boldsymbol{x})$ and $\log p_t(\boldsymbol{y} \mid \boldsymbol{x})$, and $\nabla_{\boldsymbol{x}} \log p_t(\boldsymbol{x})$ can be approximated by neural network $\boldsymbol{s}_\theta$.

In order to reconstruct the iris from the degraded version, we adopt the HQS algorithm to achieve plug-and-play reconstruction. The main idea of plug-and-play iris reconstruction methods is to separate the reconstruction process into the following terms:

$$\hat{\boldsymbol{x}} = \arg\min_{\boldsymbol{x}} \frac{1}{2\sigma_n^2} \|\boldsymbol{y} - \mathcal{H}(\boldsymbol{x})\|^2 + \lambda P(\boldsymbol{x}) \tag{13}$$

where $\boldsymbol{y} = \mathcal{H}(\boldsymbol{x}_0) = \boldsymbol{H}\boldsymbol{x}_0 + \boldsymbol{n}$ is the measurement of ground truth $\boldsymbol{x}_0$ and σ_n is the standard deviation of noise $\boldsymbol{n}$. $P(\boldsymbol{x})$ is is the prior of the images. HQS algorithm decouples Eqn. (13) into two sub-problems as:

$$\begin{cases} \boldsymbol{z}_t = \arg\min\limits_{\boldsymbol{z}} \dfrac{1}{2(\sqrt{\lambda/\mu})^2} \|\boldsymbol{z} - \boldsymbol{x}_t\|^2 + P(\boldsymbol{z}) & \text{(14a)} \\ \boldsymbol{x}_{t-1} = \arg\min\limits_{\boldsymbol{x}} \|\boldsymbol{y} - \mathcal{H}(\boldsymbol{x})\|^2 + \mu\sigma_n^2 \|\boldsymbol{x} - \boldsymbol{z}_t\|^2, & \text{(14b)} \end{cases}$$

where μ is the parameter introduced for data-consistent constraint term. In order to leverage diffusion model to aid the reconstruction process, we build the connection between Eqn. (14) with the diffusion process. Assume we want to solve $\boldsymbol{z}_k$ from $\boldsymbol{x}_t$ with noise level $\bar{\sigma}_t = \sqrt{(1-\bar{\alpha}_t)/\bar{\alpha}_t}$, we let $\sqrt{\lambda/\mu} = \bar{\sigma}_t$ and note that $\nabla_{\boldsymbol{x}} P(\boldsymbol{x}) = -\nabla_{\boldsymbol{x}} \log p(\boldsymbol{x}) = -\boldsymbol{s}_\theta(\boldsymbol{x})$, we can rewrite Eqn. (14a) as $\boldsymbol{z}_t \approx \boldsymbol{x}_t + [(1-\bar{\alpha}_t)/\bar{\alpha}_t]\boldsymbol{s}_\theta(\boldsymbol{x}_t)$. To make the discussion more clear, we rewrite Eqn. (14) as:

$$\begin{cases} \boldsymbol{z}_t = \arg\min\limits_{\boldsymbol{z}} \dfrac{1}{2\bar{\sigma}_t^2} \|\boldsymbol{z} - \boldsymbol{x}_t\|^2 + P(\boldsymbol{z}) & \text{(15a)} \\ \hat{\boldsymbol{z}}_t = \arg\min\limits_{\boldsymbol{z}} \|\boldsymbol{y} - \mathcal{H}(\boldsymbol{z})\|^2 + \gamma_t \|\boldsymbol{z} - \boldsymbol{z}_t\|^2 & \text{(15b)} \\ \boldsymbol{x}_{t-1} \leftarrow \hat{\boldsymbol{z}}_t, & \text{(15c)} \end{cases}$$

where $\gamma_t = \lambda(\sigma_n/\bar{\sigma}_t)^2$. The reconstruction process is shown in Figure 7 and summarized in Algorithm 1.

Algorithm 1 Diffusion Model for Inverse Problem Solving

```
Require: $\boldsymbol{s}_\theta, \boldsymbol{y}, \sigma_n, \{\bar{\sigma}_t\}, \lambda, T$
Sample $\boldsymbol{x}_T \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{I})$, and set $\gamma_t \triangleq \lambda\sigma_n^2/\bar{\sigma}_t^2$.
for $t = T$ to 1 do
    $\boldsymbol{z}_t = \frac{1}{\sqrt{\bar{\alpha}_t}}(\boldsymbol{x}_t + (1-\bar{\alpha}_t)\boldsymbol{s}_\theta(\boldsymbol{x}_t, t))$
    $\hat{\boldsymbol{z}}_t = \arg\min_{\boldsymbol{z}} \|\boldsymbol{y} - \mathcal{H}(\boldsymbol{z})\|^2 + \gamma_t \|\boldsymbol{z} - \boldsymbol{z}_t\|^2$
    $\hat{\epsilon} = \frac{1}{\sqrt{1-\bar{\alpha}_t}}(\boldsymbol{x}_t - \sqrt{\bar{\alpha}_t})\hat{\boldsymbol{z}}_t$
    $\boldsymbol{x}_{t-1} = \sqrt{\bar{\alpha}_{t-1}}\hat{\boldsymbol{z}}_t + \sqrt{1-\bar{\alpha}_{t-1}}\hat{\epsilon}$
end for
return $\boldsymbol{x}_0$
```

V. Evaluation

In this section, we report the results of the experimental evaluation of EMIRIS to demonstrate iris reconstruction effectiveness and its performance in attacking iris recognition systems. In particular, we present the detailed setup of our experiments, the dataset, and the system performance under extensive scenarios.

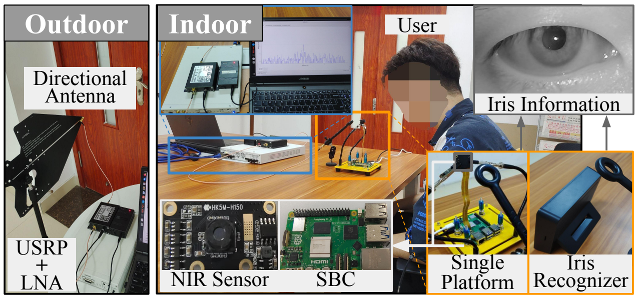


Fig. 8. Experimental setup for near-field and far-field scenario.

A. Experimental Setup

1) Hardware: To explore the sources of EM emissions and to avoid the impact of these emissions generated by the embedded terminal screen on the experiment, we built a simple platform using Single Board Computers (SBCs) connected to NIR sensors to reproduce the iris acquisition process. We select five different NIR sensors (used for iris data acquisition) to evaluate their impact on the performance of EMIRIS, namely IMX258-ZV (N1), HK5M-H150 (N2), RMONCAM S320H (N3), JRWT HW200 (N4), and HBV-1911GS (N5), which are all easily purchased on e-commerce platforms. In addition, we choose five SBCs from different vendors to evaluate their possible impact on iris reconstruction, namely, Raspberry Pi 5 (S1) [22], NVIDIA Jetson Nano (S2) [23], Odroid XU 4 (S3) [24], Banana Pi R4 (S4) [25], and Neardi LKD3588 (S5) [26]. Then, to evaluate the reconstruction performance of EMIRIS on commercial off-the-shelf iris recognition devices, we select five devices from different manufacturers, namely, IriGo Mini (D1), IrisID iCam (D2), and Mantra MIS100V2 (D3). All of these devices have embedded NIR sensors. To facilitate the reception of EM signals from the iris acquisition devices, we use a Universal Software Radio Peripheral (USRP) X310 [27] paired with a UBX-160 daughterboard [28]. We use a near-field magnetic field antenna (model: FOSTTEK NFP-ONE) to receive EM emissions at a near-distance. On the other hand, for long-distance iris reconstruction, we use a directional antenna (model: HTOOL HT8). In addition, we use a low-noise amplifier (Model: FOSTTEK FST-RFAMP06) to improve the signal-to-noise ratio of EM radiation in hardware, which can provide a signal gain of 40dBi. The adversary connects the equipment needed for the attack to a laptop equipped with an Intel Core i7-10750H CPU @2.60GHz and 16GB of RAM for software-controlled signal transmission.

2) Software: For configuring USRP modules to receive EM signals, we employ GNU Radio [29] (Release 3.10.7.0) on the Ubuntu operating system (Release 24.04.4). For model training, we use Pytorch (Release 2.3.1) with CUDA (Release 11.8).

3) Attack Setup: In the experimental scenario shown in Figure 8, the NIR sensor or iris recognition device acquires the user's iris data, which are transmitted and processed through its internal interface, where EM emissions are generated. The attacker can receive EM signals in different environments: in indoor scenarios, we use near-field magnetic antennas, while in outdoor scenarios, we use directional antennas. Then we improve the signal-to-noise ratio through a low-noise amplifier and process these signals using a laptop to obtain iris information. Subsequently, these raw iris data are fed into a diffusion model, resulting in a high-quality iris reconstruction. We utilize this reconstructed iris information for spoofing iris recognition models or commercial iris recognizers. The environmental conditions in the experiments are standard light (300lux). During the operation of the NIR sensor, significant amplitude values emerge in the target frequency band, and EMIRIS collects data during this period for reconstruction. Since the attacker cannot determine exactly when the iris information in the EM signal is suitable for recognition, they generate multiple frames of iris data from the entire EM signal and select the one with the highest quality.

B. Datasets and Model Training

To effectively train the diffusion model, we combine iris images from multiple datasets to enhance the diversity of the data. First, we use the LivDet-Iris 2020 dataset [35], which contains 5331 iris images of living human eyes. Next, we introduce the CASIA-IrisV4 dataset [36] to enrich the style and number of iris images. This dataset consists of 54,601 iris images from more than 1,800 individuals, from which we select 20,000 images as training data. In addition, we use the ND-IRIS-0405 iris image dataset [37], which contains 64,980 images captured by the LG 2200 system, from which we select 20,000 for diffusion model training. Finally, we employ the IIT Delhi Iris Database v1 dataset [38], which contains 1120 iris images captured in the NIR light environment. In summary, the dataset for this evaluation consists of grayscale iris images totaling 46,451. All these images are resized to be 640×480 pixels and then center-cropped to be 480×480. For model training, we use DDPM as our diffusion model and adopt Adam optimizer with learning rate 1e-4. We train the diffusion model with 50 epochs and set the diffusion steps to 1000. We report a complete description of the datasets used in our evaluation in Appendix.

C. Target Iris Recognition Models

We select five different architectures of typical ML-based iris recognition models: DeepIrisNet [30] (Model 1), FM-Net [31] (Model 2), ETENet [32] (Model 3), DualSANet [33] (Model 4), and TLPIM [34] (Model 5). Each model has distinct characteristics, representing different technical approaches in the field of iris recognition. Model 1 is based on a deep learning framework and Model 2 employs a multi-layer convolutional neural network, optimizing feature selection and fusion strategies. Model 3 is an end-to-end neural network designed for iris recognition without the need for traditional segmentation and normalization steps. Model 4 is a convolutional neural network based on a dual spatial attention mechanism, generating multi-level spatially corresponding feature representations. Model 5 combines transfer learning and deep network models. The detailed parameters of each model are shown in Table I. In addition, to ensure the fairness and robustness of the evaluation, we conduct a fair comparison of the performance of the five models (in Section V-F2) in a standardized test environment using the datasets mentioned in Section V-B.

D. Iris Segmentation and Normalization

Since we evaluate the performance of EMIRIS for spoofing attacks on different models, these models have inconsistent input sizes, some require input images of equal length and width, and some require segmented and normalized images. This is attributed to the fact that some models are designed with an iris segmentation module, where the iris portion of the image can be segmented and normalized. However, these models do not use the same method of iris segmentation, and not all models are equipped with this module. Therefore, for models with iris segmentation requirements, we uniformly use the iris segmentation and normalization scheme proposed by John Daugman [3]: the edges of the iris are detected using an edge detection operator, the boundaries of the iris and pupil are determined by the Circular Hough Transform [39], and the iris region is converted into a 64 pixels × 512 pixels rectangular image using the Rubber Sheet Model [40].

E. Metrics

Structural Similarity Index Measure (SSIM) is a metric used to assess the structural similarity between two images: one being an undistorted reference image (the original iris image) and the other a distorted image with noise (the reconstructed iris image). SSIM ranges from -1 to 1, with larger values indicating greater similarity between images, and smaller values indicating greater differences. SSIM can be calculated as follows:

$$\mathsf{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\delta_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\delta_x^2 + \delta_y^2 + c_2)}$$

SSIM integrates the brightness, contrast, and structural information of an image to evaluate the image quality in a way that is more consistent with human visual perception.

Electromagnetic Emission Signal-to-Noise Ratio (EME-SNR) is used to measure the quality of electromagnetic emission signals. It represents the ratio between the electromagnetic emission signal and the noise. A higher EME-SNR indicates better signal quality and less noise interference.

Fréchet Inception Distance (FID) of the generated image is a metric used to evaluate the quality of the generated image. FID measures the distance between the generated image and the real image by comparing the feature distribution of the generated image and the real image. The smaller the value, the more similar the generated image is to the real image. In our experiments, FID is used to evaluate the quality of iris images processed by the Diffusion model to ensure that the generated images are highly consistent with the original images in terms of both visual and statistical properties.

Spoofing Success Rate (SSR) is defined as the proportion of generated iris images that successfully deceive machine learning models. This metric is employed to assess the effectiveness of generated images in attacking these models. Specifically, a higher spoofing rate indicates that the generated iris images are more likely to be misclassified by the model as genuine images, thereby reflecting the success of the attack. In this study, the spoofing rate is utilized to evaluate the vulnerability of various iris recognition models when confronted with reconstructed images, highlighting the potential security threats posed by EM emission vulnerabilities.

F. Experimental Results

1) EMIRIS Attacks on NIR Sensors Connected to SBCs: To investigate and verify the source of EM emissions and

TABLE I. PARAMETERS OF TARGET IRIS RECOGNITION MODELS

Models		Input Size	Activation Function	Optimizer	Learning Rate	Datasets	FRR (FAR=0.1%)	Accuracy* (%)
DeepIrisNet [30]	DCNN	128×128	ReLU	SGD	0.01	ND-iris-0405, ND-CrossSensor-Iris-2013	0.008	97.31
FM-Net [31]	FCN+MCNN	28×28	ReLU	SGD	0.01	CASIA-Iris-Thousand	4.27	95.63
ETENet [32]	DNN	160×120	ReLU	Adam	0.0001	CASIA-IrisV4, IITD	0.75	99.76
DualSANet [33]	CNN	64×512	ReLU	SGD	0.001	CASIA-IrisV4,IITD	0.58	99.69
TLPIM [34]	ResNet	256×256	ReLU	Adam	0.00001	CASIA-Iris-Thousand	0.8	96.00

∗ The accuracy here is the overall iris recognition performance of each model on the respective dataset. We will evaluate their performance on the dataset we selected in Section V-F2.

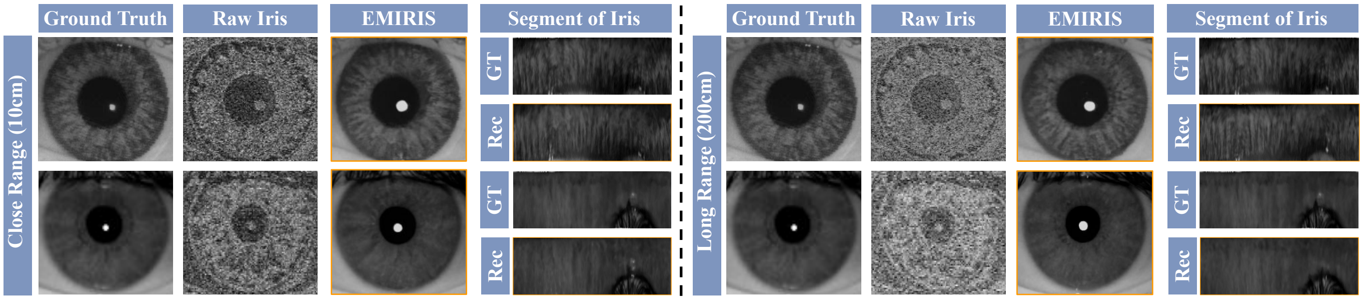
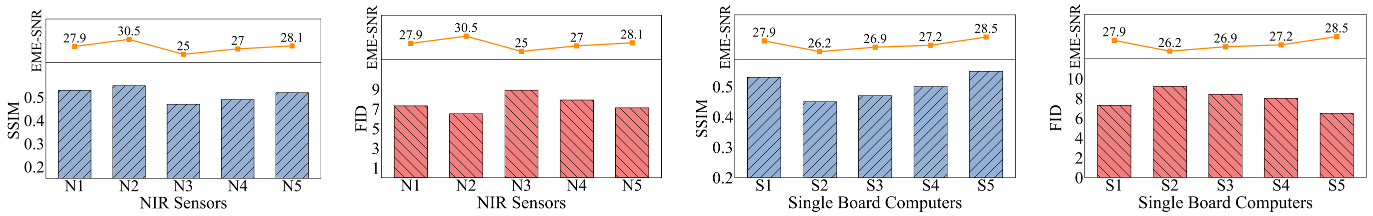


Fig. 9. Demonstration of attack performance using IMX258-ZV NIR sensor and Raspberry Pi to capture iris information. To visualize the details more, we cut down the iris section.



(a) SSIM of NIR sensors

(b) FID of NIR sensors

(c) SSIM of SBCs

(d) FID of SBCs

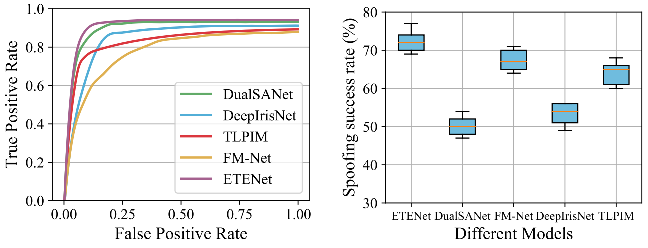
Fig. 10. Performance of EMIRIS using different NIR sensors (A: IMX258-ZV, B: HK5M-H150, C: S320H, D: HW200, E: HBV-1911GS) and SBCs (1: Raspberry Pi, 2: NVIDIA Jetson, 3: Odroid XU, 4: Banana Pi, 5: Neardi).

to avoid the EM signal from the terminal screen, we build the internal structure of a common iris recognition device on the market using commercial off-the-shelf embedded NIR sensors and Raspberry Pi 5. This single platform is shown in Figure 8. We connect the NIR sensors to the Raspberry Pi using a flexible flat cable (FFC) for data transmission. To explore the iris reconstruction effect in both near-field and far-field scenarios, we use a near-field magnetic field antenna to collect EM signals at 10cm and a directional antenna at 2m. At each distance, we capture the irises from two different users.

Figure 9 illustrates the reconstruction of iris images at two distances using two antennas aimed at the IMX258-ZV NIR sensor. Despite the presence of initial noise and distortion in the raw signal, the EMIRIS system is still capable of reconstructing the iris information that is similar to the ground truth at 10cm. At a distance of 2 meters, although the signal quality decreases and the initial raw images exhibit greater distortion, our system is still able to generate iris information with clear textures. Compared to the first user, the second user's iris texture is less distinct, resulting in a slight decline in reconstruction quality. This indicates that the structure of the iris texture significantly impacts the reconstruction effectiveness. To provide a more intuitive observation of the reconstructed iris texture features, we report the segmentation and normalization of the iris. Although we can observe minor discrepancies in some details compared to the ground truth in Figure 9, the overall feature distribution exhibits a high degree of consistency. Additionally, we observe that when conducting experiments with a standard laptop and USRP, the EM signal acquisition and mapping process takes 1.2172 seconds.

Reconstruction from Different NIR Sensors. To evaluate the performance of EMIRIS across different NIR sensors from 5 brands (namely N1 to N5, refer to Section V-A), we conduct experiments on iris information reconstruction. These sensors are connected to a Raspberry Pi, and we use a directional antenna to capture EM signals at 1 meter. For a comprehensive evaluation, we recruited 50 volunteers[1] and collected 500 iris data using five different NIR sensors at 20cm. The attack parameters of the NIR sensors are shown in Appendix. The results are shown in figures 10(a) and 10(b), where we also report the signal-to-noise ratio of the EM emissions, i.e., EME-SNR. It can be seen that the different NIR sensors produce slightly different levels of EM emissions, with model N2 producing relatively stronger levels of EM emissions, resulting in a slight improvement in the quality of the reconstructed images. Overall, the quality of the reconstructed iris using all NIR sensors remains generally stable, with an average SSIM of 0.51 and an average FID of 7.54.

[1] Ethical approval has been granted by the corresponding organization.



(a) ROC curves

(b) SSR

Fig. 11. Original performance and spoofing success rate of different models.

Reconstruction from Different SBCs. To evaluate the impact of different SBCs on the quality of iris reconstruction, we connect the NIR sensor IMX258-ZV-HM03 to 5 different SBCs mentioned in Section V-A and capture the EM signal at 1 meter using a directional antenna. The experimental results are shown in figures 10(c) and 10(d). The experimental results are shown in figures 10(c) and 10(d). It can be seen that the quality of the reconstructed irises using different SBCs remains generally stable, and an average SSIM of 0.52 and an average FID of 7.88 can be achieved.

2) Spoofing ML-based Models Using EMIRIS: To ensure a fair and reasonable representation of the baseline performance of different models, we evaluate the iris recognition success rates of five models in a standardized testing environment before conducting spoofing attacks. These models are trained and tested using a unified dataset, which contains CASIA-IrisV4, IITD, and LivDet-Iris 2020. Additionally, the prerequisite for using reconstructed iris images in spoofing attacks is that the original iris information exists in the target model's feature database. Therefore, we input the user iris data collected in the previous section into the feature database of the iris recognition models. Subsequently, we use the EM emissions generated by the sensors during iris acquisition to reconstruct the iris and evaluate the models' performance under spoofing attacks. The experimental setup for iris reconstruction is the same as described in Section V-F1.

Figure 11(a) shows the ROC curves of different models. Among these models, ETENet performs the best, primarily due to its use of a deep learning framework and attention mechanisms, which can fully utilize the detailed features of the iris. In contrast, the performance of FM-Net is slightly lower. However, all models demonstrate excellent iris recognition performance on the same dataset. Figure 11(b) shows the success rate (SSR) of using reconstructed irises to spoof different models. It can be clearly seen that the SSR of irises reconstructed with different NIR sensors fluctuates within a small range for the same model, not exceeding 10%. Additionally, there is a clear trend that the higher the EM signal SNR, the higher the SSR. Among the five models, ETENet has the highest SSR. Worryingly, it does not require preprocessing such as iris segmentation and normalization, thus extracting features from the entire eye rather than just focusing on the iris, making spoofing attacks more likely to succeed. Our system can reconstruct the eye contour with almost no distortion and, combined with the assistance of texture details, increases the success rate of spoofing attacks. FM-Net and TLPIM have a relatively high SSR because they rely on relatively simple feature selection and fusion, which makes them prone to misidentifying low-resolution irises as legitimate users. In contrast, DualSANet and DeepIrisNet have the lowest SSR. The former can extract deeper features and is highly sensitive to iris details, making it more resistant to reconstructed irises with less obvious texture details. The latter, with its dual spatial attention mechanism, can focus on iris texture areas, providing similar resistance to reconstructed irises as the former. In summary, EMIRIS can achieve an average SSR of 61.96% on different models.

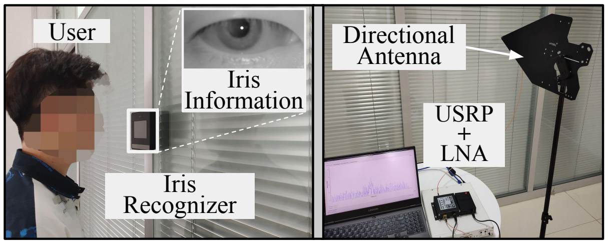


Fig. 12. Attack on commercial iris recognition device.

3) EMIRIS Attacks on Commercial Iris Recognizer: To further validate whether EMIRIS can reconstruct iris information from commercial iris recognition devices, we select three commonly used iris recognition devices on the market (D1, D2, and D3). In Section V-A, we provide the specific model information of these devices and detail the parameters of these devices and their main EM emission bands in Appendix. It is important to note that these bands are where the EM signal is strongest with our hardware setup, but they are not the only bands where emission occurs. In the experiment, the iris recognizer collects the user's iris data. We use both near-field magnetic field antennas and directional antennas to capture EM signals in indoor (10cm) and outdoor (2m) environments, as shown in Figure 8 and Figure 12. In this process, we employ a 40dB LNA to enhance the received signals and adjust the center frequency according to the EM leakage bands of different devices. The collection of iris data from the user is consistent with the description in Section V-F1, with the data being collected at a distance of 20cm from the iris recognizer.

Figure 13 demonstrates the effectiveness of iris reconstruction using EM emission from iris recognition devices. To better visualize the details of the iris, the reconstruction results are subjected to iris segmentation and normalization. It is evident that, although there is a slight variation in the reconstruction quality across the three devices, the overall reconstruction results are stable. The reconstructed iris textures exhibit a high degree of similarity to the original irises. Figure 14 reports the evaluation results using objective metrics such as SSIM and FID. It can be seen that the iris information reconstructed using device D1 has a relatively high similarity to the ground truth. However, despite device D2 having the strongest EM signal, it achieves relatively poor reconstruction results. This could be due to its EM signals being a mix of all signals from the device, including EM leakage from the screen and other internal cables and wires, which interfered with iris data-related EM signals. Moreover, Figure 14(c) reports the success rate of spoofing iris recognition models using these reconstructed results. Device D1 achieved a relatively higher SSR, attributed to the better quality of its reconstructed iris. Overall, EMIRIS successfully

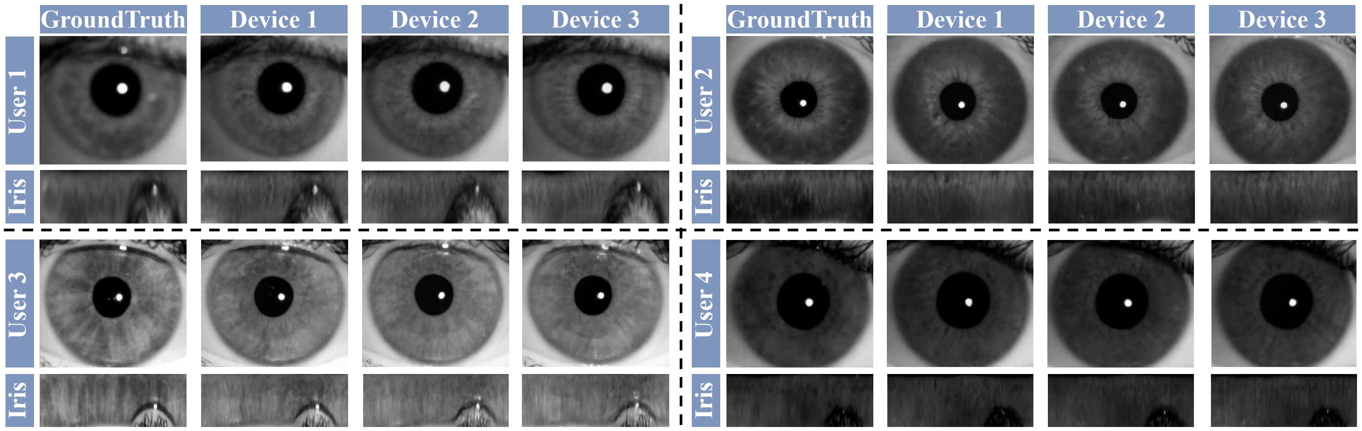
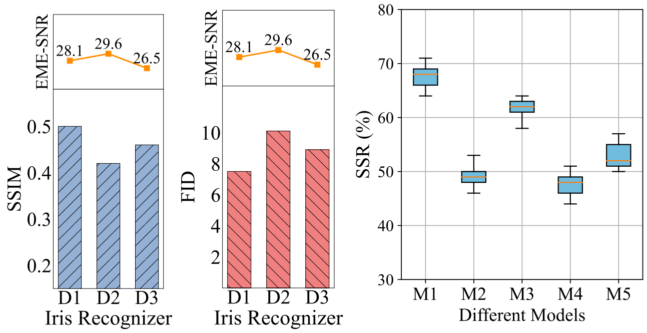


Fig. 13. Iris reconstruction from different iris recognizers, where we report the segmentation and normalization results of the iris. On the left and right are irises and their reconstructions from two different users, respectively.



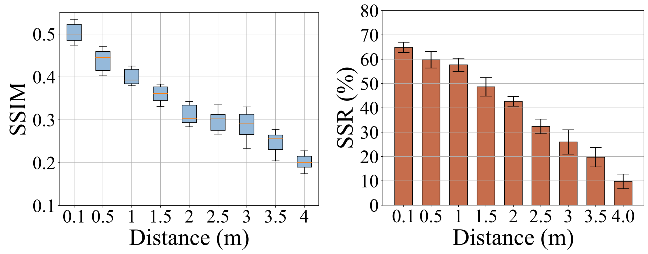
(a) SSIM (b) FID (c) SSR

Fig. 14. Attack on commercial devices and their SSR of different models.

reconstructs irises from commercial iris recognition devices and poses a threat to iris recognition systems, with an average SSR of 49.13%.

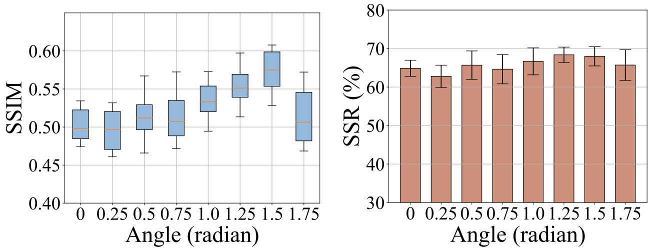
4) Impact of Distance and Angle: In this experiment, we conduct a comprehensive evaluation of EMIRIS's performance at various distances and angles. Specifically, we perform iris reconstruction at multiple distances ranging from 0.1 meters to 4 meters (with a step size of 0.5 meters) and at various angles ranging from 0 radians to 1.75 radians (with a step size of 0.25 radians). We use five different NIR sensors and three commercial iris recognizers to capture iris information at each distance and angle, and we average the reconstruction results. Finally, we select ETENet as the target model to launch the spoofing attacks.

Figure 15 shows the results of the evaluation of receiving EM signals and reconstructing irises at various distances. As distance increases, the quality of the reconstructed iris decreases due to weakening of the EM signals from the NIR sensor. Although directional antennas and LNA can enhance the SNR of EM signals, increased distance also introduces multipath effects and channel noise, significantly affecting the quality of EM signals. Figure 15(b) also shows the success rate in deceiving the model with a reconstructed iris at different distances. Similarly, as the distance increases, the attack success rate decreases. Notably, EMIRIS can still achieve an SSIM of 0.311 and an SSR of 42.61% at a distance of 2m. Although performance drops significantly at distances around 4m, the threat does not completely disappear. Figure 16 illustrates the attack performance of EMIRIS at various angles. It can be seen that different angles do not significantly affect the quality of the reconstructed iris or the SSR. However, at 1.5 radians, there is a slight improvement in system performance, probably due to the internal circuitry causing the EM signals to be more concentrated in that direction. Overall, EMIRIS can achieve an average SSIM of 0.43 and an average SSR of 51.28% at various distances and angles, demonstrating its robustness and stability.



(a) SSIM (b) SSR

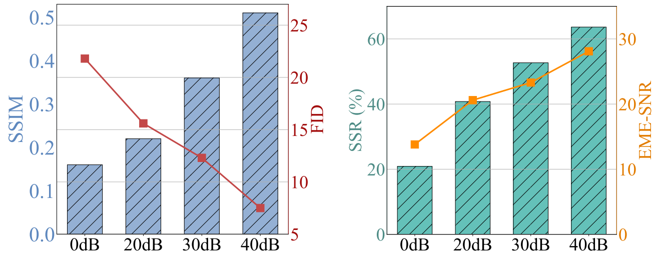
Fig. 15. Performance of EMIRIS at different distances.



(a) SSIM (b) SSR

Fig. 16. Performance of EMIRIS at different angles.

5) Impact of Different LNAs: To investigate the effect of low-noise amplifiers on iris reconstruction performance, we conduct experiments using LNAs with different gain levels: no gain, 20dB, 30dB, and 40dB. The three gain levels correspond to different device models: MAX2659 (20dB), ZRL-1150LN+ (30dB), and FST-RFAMP06 (40dB). The distance between the receiving antenna and the target NIR sensor was fixed at 0.5 meters. The target model selected is ETENet, with all other



(a) SSIM and FID

(b) SSR

Fig. 17. Performance of EMIRIS using different LNAs.

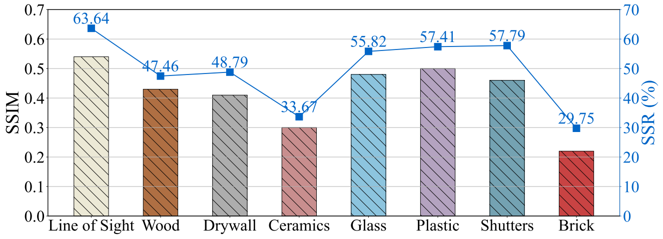


Fig. 18. Impact of different building materials on signal obstructions.

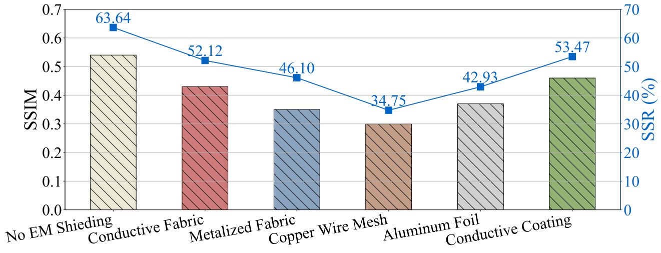


Fig. 19. Impact of different EM shielding materials.

settings the same as in Section V-F1.

Figure 17 shows the experimental results using LNAs with different gains. As the gain decreases, the quality of the reconstructed iris degrades. This is because high-gain LNAs can effectively amplify the weak EM signals received while introducing less noise. Specifically, when not using an LNA, the SNR of the EM emission signal is only 13.8 dB, and the signal containing iris information is almost entirely submerged in noise, posing a significant challenge to EMIRIS. Therefore, the success rate of spoofing attacks without using an LNA is only 20.87%. However, despite the low success rate, considering the critical application of iris information in identity verification and security, even this low success rate indicates that our system still poses a significant threat under low SNR conditions.

6) Impact of Different Building Materials: To launch EMIRIS outdoors, an attacker needs to receive EM signals from inside through walls. However, the attenuation of EM signals varies with different building materials. To investigate the impact of these obstructions on the iris reconstruction performance, we select several types of materials: Line of Sight (no material), Wood, Drywall, Ceramics, Glass, Plastic, Shutters, and Brick. These materials are selected to represent common building substances with different EM signal attenuation properties. The materials are placed between the receiving antenna and the target NIR sensor, with the distance between them fixed at 1 meter. All other settings are kept the same as in Section V-F1.

Figure 18 shows the experimental results under different signal obstructions. Among the various materials, glass and plastic provided the least signal obstruction, with SSIMs of 0.56 and 0.57 and SSRs of 55.82% and 57.41%, respectively. This suggests that despite some obstruction, signals can still penetrate these materials relatively, resulting in higher iris reconstruction quality and spoofing success rates. In contrast, wood and drywall provided moderate signal obstruction, with SSIMs of 0.47 and 0.49 and SSRs of 47.46% and 48.79%, respectively. This indicates that these materials have a noticeable, but not severe, attenuation effect on the signal. Ceramics and brick provided the strongest signal obstruction, with SSIMs of 0.34 and 0.30 and SSRs of 33.67% and 29.75%, respectively. This indicates that these materials significantly attenuate the EM signal, leading to a substantial reduction in the quality of the iris reconstruction and the spoofing success rate. These results demonstrate that EMIRIS exhibits robust performance. Even in the presence of obstructions to the signal by various building materials, EMIRIS remains a significant threat.

7) Impact of EM Shielding Materials: In practical applications, NIR sensor data transmission cables often use EM shielding materials. These materials can suppress electromagnetic signals, thereby affecting the strength of external EM signals and consequently the ability to reconstruct iris information using these signals. To evaluate their impact on EMIRIS, we select conductive fabric, copper wire mesh, conductive coating, foil shielding (aluminum foil), and metalized fabric as EM shielding materials. In the experiments, we uniformly wrap each type of shielding material around the data transmission wires of the NIR sensors, ensuring complete coverage to maximize shielding effectiveness. EM signals are collected using different NIR sensors under various shielding conditions, with the directional antenna fixed at a distance of 0.5 meters from the sensor and standard indoor lighting conditions.

Figure 19 demonstrates the effects of different shielding materials on the iris reconstruction quality. It shows that copper wire mesh shielding provides the best EM shielding effect, significantly reducing external EM signal interference, resulting in the lowest iris reconstruction quality (SSIM of 0.3) and the lowest spoofing success rate (34.75%). Metalized fabric and aluminum foil shielding follow, offering SSIMs of 0.35 and 0.37, respectively, and similarly reducing signal interference, lowering SSR to 46.1% and 43.93%. Conductive coatings and conductive fabrics provide relatively poorer shielding effects, resulting in SSIMs of 0.43 and 0.46, and SSRs of 52.12% and 53.47%, respectively. In summary, while these EM shielding materials can reduce the performance of iris reconstruction, they do not eliminate the threat posed by EMIRIS.

VI. Discussion

A. Defense Strategy Against EMIRIS

1) Enhancing EM Shielding: As discussed in Section V-F7, the use of EM shielding materials on transmission wires can effectively reduce the performance of such attacks. The inclusion of conductive components, especially metals, makes it difficult for electromagnetic signals to penetrate and reach distant locations. However, considering manufacturing costs, it is impractical to implement a fully covered electromagnetic shield. Therefore, it is essential to explore different mesh structures that can provide effective shielding while reducing costs. In addition, researching new EM shielding materials is crucial. Materials with excellent conductivity, such as $\mathrm{Ti_3C_2Tx}$ and Poly 3,4-ethylene dioxythiophene (PEDOT) [41], show promise in this regard.

2) Iris Data Obfuscation Transmission: The digital signal of iris information is transmitted in a sequential row-by-row order (as shown in Figure 2). Attackers exploit the EM emissions generated during this transmission to arrange the data units in sequence and reconstruct the iris information. Key-based encryption alone cannot prevent this. However, scrambling the data order before transmission is effective. On the sending side, the data sequence is scrambled and transmitted along with the sequence index, frame header, and frame footer. On the receiving side, the data is reordered using the index to restore the original sequence. Without the sequence index, attackers can only access the scrambled data.

3) Improving Iris Recognition Strategies: Our experimental evaluation indicates that current iris recognition models generally lack robustness against "fake iris" data. This is in part because the reconstructed iris textures have minimal differences from the original and in part because of the models' inadequate processing of detailed iris features. Therefore, training a model that balances both overall features and local details is necessary, as this could reduce the misrecognition rate, given that reconstructed irises are not perfect in detail. In addition, incorporating liveness detection technology can defend against such attacks. Even if attackers obtain the user's iris information, two-dimensional iris data cannot bypass liveness detection, leading to the failure of spoofing attacks.

B. Security Concerns Raised by EMIRIS

EMIRIS exposes significant security risks for iris recognition systems, mainly due to the potential for unauthorized capture and reconstruction of sensitive biometric data through electromagnetic emissions. Unlike passwords or personal identification numbers, biometric data cannot be changed once compromised, leading to long-term privacy issues. An attacker can reconstruct the iris information of a targeted individual or group of users by simply capturing EM signals in the vicinity of an iris recognition device. After obtaining iris information, attackers can potentially bypass iris recognition systems used in security-critical applications such as banking, access control, and government ID programs. This could lead to identity spoofing, unauthorized continuous access, financial threats in iris-based payment systems, and evasion of immigration controls, causing significant harm to individuals and organizations.Given the widespread use of NIR sensors in many biometric systems, the vulnerabilities exposed by EMIRIS can affect a wide range of applications. From personal devices such as smartphones to large-scale security systems, the scalability of such attacks poses a major threat. Furthermore, with the advancement of biomimicry technology, it has become possible to produce artificial eyes or contact lenses that can effectively spoof commercial iris recognition systems, further exacerbating security threats to biometric data.

C. Limitations and Future Work

Since NIR sensors are often embedded in devices such as attendance machines, ATMs, and smart locks, the other electronic components of these devices also emit EM radiation. This mixes with the iris signals, resulting in many irrelevant components. Factors such as channel effects, sensor errors, and mapping errors further affect the attack, making EMIRIS imperfect in reconstructing fine details of the iris. The limited sampling rate and bandwidth of our equipment also cause loss of fine features and, in extreme cases, the polarity inversion leads to inaccurate grayscale values of the data unit. Although these issues have a limited impact on EMIRIS's ability to attack iris recognition models, it still needs to improve in iris detail reconstruction.

To improve the security of biometric systems, we will continue to explore more effective EMIRIS attacks and develop more robust defense strategies against such attacks. We will further optimize EM signal processing to improve the signal-to-noise ratio and filter out irrelevant signals. Additionally, we will apply iris information to bionic eyes or contact lenses to bypass liveness detection protocols and explore EMIRIS's capability against commercial iris recognition devices. Meanwhile, we will continue to research defensive measures against such attacks, including testing other new EM shielding materials, exploring new signal obfuscation methods, and introducing multi-factor authentication to strengthen the security of biometric systems.

VII. Related Work

A. EM Side-channel Attacks on Cryptographic Keys

Electromagnetic side channels used for cryptographic keys are a serious threat. Gandolfi et al. [42] analyze electromagnetic power emissions to attack DES and RSA encryption algorithms. Authors in[43] reconstruct the complete key using electromagnetic emission from the FPGA device. The authors in [44] use deep neural networks to model the correlation between electromagnetic and power degradation, which in turn recovers the AES key. [45] introduces how to retrieve an AES key from a smartphone's hardware crypto processor. Researchers in [46], [47], [48], [49] leverage electromagnetic leakage from system-on-chip (SoC) components to perform key recovery attacks. The authors in [50] realize key recovery for AES with the use of deep learning and the attack distance can reach 15m. Since the discovery of electromagnetic leakage, its application in cryptographic keys has been a significant research focus. However, attacks against physical layer devices are still progressing slowly.

B. EM Side-channel Attacks on Hardware and Devices

Electromagnetic leakage attacks against physical layer devices can be traced back to the 1960s when it was used for eavesdropping [51]. To counter such security threats, the United States government subsequently established electromagnetic leakage standards, known as TEMPEST [52], [53]. In 1985, the threat of electromagnetic side-channel attacks was first publicly demonstrated by Van Eck [12]. However, since the TEMPEST standard strictly controls electromagnetic emissions from sensitive devices, such electromagnetic attacks are effective only at a distance very close to the target device. [54]

uses electromagnetic leakage from cell phones to identify the operational status of the rear and front cameras. Researchers in [55] utilize electromagnetic emissions from a phone screen to reconstruct the image the phone is displaying. [56] achieves website fingerprinting and keystroke timing inference attacks by exploiting an electromagnetic side-channel vulnerability in GPUs. Ni et al. [57] captured electromagnetic emissions during the smartphone screen unlocking process to recover users' fingerprint information, demonstrating the potential to deceive several commercial smartphones. Research on electromagnetic emissions from cameras is still relatively limited. Initially, Liu et al. [58] used unintentional electromagnetic radiation from cameras for hidden camera detection. Subsequently, Long et al. [13] utilized such electromagnetic emissions to recover transmitted frames from commercial embedded RGB cameras for private space surveillance. The authors of [59] utilized multiple 2D near-infrared iris images for iris optimization, but did not involve the potential privacy leakage issues in the iris recognition process. However, there have been no attempts to reconstruct iris images from NIR sensors.

VIII. Conclusion

In this paper, we propose EMIRIS, a novel method to reconstruct the iris information via electromagnetic side-channel attacks. By capturing and analyzing the EM emissions from near-infrared sensors, EMIRIS can reconstruct the raw iris information. We model the denoising process of the iris to a linear inverse problem. By designing a diffusion model and introducing conditional constraints, high-quality iris information can be reconstructed and effectively used to spoof iris recognition systems. Our extensive experiments reveal that EMIRIS can achieve a significant SSIM and spoofing success rate in various scenarios, highlighting the vulnerability of current iris recognition technologies to such attacks.

Acknowledgment

We thank our reviewers for their valuable comments and suggestions. This work is supported by the National Natural Science Foundation of China (Grant No. 62422208, 62202276, 62302274, 62232010, 62202274, 62350410480) and Shandong Science Fund for Excellent Young Scholars (No. 2022HWYQ-038, 2024HWYQ-021), Shandong Science Fund (No. 2023TSGC0105, ZR2023QF113)

References

[1] J. Daugman, "How iris recognition works," in *The essential guide to image processing*. Elsevier, 2009, pp. 715–739.

[2] R. A. Sturm and M. Larsson, "Genetics of human iris colour and patterns," *Pigment cell & melanoma research*, vol. 22, no. 5, pp. 544–562, 2009.

[3] K. W. Bowyer and M. J. Burge, *Handbook of iris recognition*. Springer, 2016.

[4] J. R. Malgheet, N. B. Manshor, and L. S. Affendey, "Iris recognition development techniques: a comprehensive review," *Complexity*, vol. 2021, no. 1, p. 6641247, 2021.

[5] A. Tyagi, R. Simon *et al.*, "Security enhancement through iris and biometric recognition in atm," in *2019 4th International conference on information systems and computer networks (ISCON)*. IEEE, 2019, pp. 51–54.

[6] P. Shetiya, M. Mascarenhas, and M. Deshmukh, "Atm security system using iris recognition by image processing," *International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. 7, pp. 999–1002, 2020.

[7] D. Zadnik and A. Žemva, "Image acquisition device for smart-city access control applications based on iris recognition," *Sensors*, vol. 21, no. 18, p. 6185, 2021.

[8] A. S. Shalaby, R. Gad, E. E.-D. Hemdan, and N. El-Fishawy, "An efficient cnn based encrypted iris recognition approach in cognitive-iot system," *Multimedia Tools and Applications*, vol. 80, pp. 26 273–26 296, 2021.

[9] R. Vyas, T. Kanumuri, G. Sheoran, and P. Dubey, "Smartphone based iris recognition through optimized textural representation," *Multimedia Tools and Applications*, vol. 79, pp. 14 127–14 146, 2020.

[10] U. Rao and V. Nair, "Aadhaar: governing with biometrics," pp. 469–481, 2019.

[11] 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 *Cryptographic Hardware and Embedded Systems–CHES 2015: 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings 17*. Springer, 2015, pp. 620–640.

[12] W. Van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers & Security*, vol. 4, no. 4, pp. 269–286, 1985.

[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] Y. R. Barishak, "Embryology of the eye and its adnexa," 2001.

[15] T. Gao, Y. Liu, R. Liu, and W. Zhuang, "Research progress and development of near-infrared phosphors," *Materials*, vol. 16, no. 8, p. 3145, 2023.

[16] Y. Zhu and K. B. Letaief, "Single carrier frequency domain equalization with time domain noise prediction for wideband wireless communications," *IEEE Transactions on Wireless Communications*, vol. 5, no. 12, pp. 3548–3557, 2006.

[17] U. Erkan, S. Enginoğlu, D. N. Thanh, and L. M. Hieu, "Adaptive frequency median filter for the salt and pepper denoising problem," *IET Image Processing*, vol. 14, no. 7, pp. 1291–1302, 2020.

[18] J. Ho, A. Jain, and P. Abbeel, "Denoising diffusion probabilistic models," *Advances in neural information processing systems*, vol. 33, pp. 6840–6851, 2020.

[19] Y. Song, J. Sohl-Dickstein, D. P. Kingma, A. Kumar, S. Ermon, and B. Poole, "Score-based generative modeling through stochastic differential equations," in *International Conference on Learning Representations*, 2020.

[20] P. Dhariwal and A. Nichol, "Diffusion models beat gans on image synthesis," *Advances in neural information processing systems*, vol. 34, pp. 8780–8794, 2021.

[21] P. Vincent, "A connection between score matching and denoising autoencoders," *Neural computation*, vol. 23, no. 7, pp. 1661–1674, 2011.

[22] R. Pi, "Raspberry pi 5," 2024, https://www.raspberrypi.com/products/raspberry-pi-5/, last accessed on July 10, 2024.

[23] NVIDIA, "Jetson nano," 2024, https://www.nvidia.cn/autonomous-machines/embedded-systems/jetson-nano/product-development/, last accessed on July 10, 2024.

[24] O. UK, "Odroid xu4," 2024, https://www.odroid.fr/odroid-xu4, last accessed on July 10, 2024.

[25] BananaPi, "Bpi-r4," 2024, https://docs.banana-pi.org/zh/BPI-R4/BananaPi_BPI-R4, last accessed on July 10, 2024.

[26] Neardi, "Neardi_lkd3588," 2024, http://wiki.neardi.com/wiki/rk3588/zh_CN/index.html, last accessed on July 10, 2024.

[27] N. Instruments, "Usrp x310 (kintex7-410t fpga, 2 channels, 10 gige and pcie bus)," https://www.ettus.com/wp-content/uploads/2019/01/X300_X310_Spec_Sheet_9.20.2022.pdf, last accessed on July 10, 2024.

[28] NI, "Ubx 160 usrp daughterboard (10 mhz - 6 ghz, 160 mhz bw)," https://www.ettus.com/wp-content/uploads/2022/06/UBX_Data_Sheet-6.22.pdf, last accessed on July 10, 2024.

[29] GNURadio, “Gnu radio 3.10.7.0,” 2024, https://www.gnuradio.org/news/2023-07-19-gnuradio-v3.10.7.0-release/, last accessed on July 10, 2024.

[30] A. Gangwar and A. Joshi, “Deepirisnet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition,” in *2016 IEEE international conference on image processing (ICIP)*. IEEE, 2016, pp. 2301–2305.

[31] R. Tobji, W. Di, and N. Ayoub, “Fm net: Iris segmentation and recognition by using fully and multi-scale cnn for biometric security,” *Applied Sciences*, vol. 9, no. 10, p. 2042, 2019.

[32] W. Wu, Y. Chen, and Z. Zeng, “Non-segmentation and deep-learning frameworks for iris recognition,” in *Biometric Recognition: 15th Chinese Conference, CCBR 2021, Shanghai, China, September 10–12, 2021, Proceedings 15*. Springer, 2021, pp. 325–334.

[33] K. Yang, Z. Xu, and J. Fei, “Dualsanet: Dual spatial attention network for iris recognition,” in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 2021, pp. 889–897.

[34] A. Kuehlkamp, A. Boyd, A. Czajka, K. Bowyer, P. Flynn, D. Chute, and E. Benjamin, “Interpretable deep learning-based forensic iris segmentation and recognition,” in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 2022, pp. 359–368.

[35] P. Das, J. McFiratht, Z. Fang, A. Boyd, G. Jang, A. Mohammadi, S. Purnapatra, D. Yambay, S. Marcel, M. Trokielewicz *et al.*, “Iris liveness detection competition (livdet-iris)-the 2020 edition,” in *2020 IEEE international joint conference on biometrics (IJCB)*. IEEE, 2020, pp. 1–9.

[36] CASIA, “Casia iris image database 4.0,” 2024, http://biometrics.idealtest.org/downloadDB.do?id=4#/datasetDetail/4, last accessed on July 10, 2024.

[37] K. W. Bowyer and P. J. Flynn, “The nd-iris-0405 iris image dataset,” *arXiv preprint arXiv:1606.04853*, 2016.

[38] I. I. of Technology Delhi, “Iit delhi iris database,” 2024, https://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm, last accessed on July 10, 2024.

[39] K. Okokpujie, E. Noma-Osaghae, S. John, and A. Ajulibe, “An improved iris segmentation technique using circular hough transform,” in *IT Convergence and Security 2017: Volume 2*. Springer, 2018, pp. 203–211.

[40] T. Johar and P. Kaushik, “Iris segmentation and normalization using daugman’s rubber sheet model,” *International Journal of Scientific and Technical Advancements*, vol. 1, no. 1, pp. 11–14, 2015.

[41] K. S. Kumar, R. Rengaraj, G. Venkatakrishnan, and A. Chandramohan, “Polymeric materials for electromagnetic shielding-a review,” *Materials Today: Proceedings*, vol. 47, pp. 4925–4928, 2021.

[42] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic analysis: Concrete results,” in *Cryptographic Hardware and Embedded Systems—CHES 2001: Third International Workshop Paris, France, May 14–16, 2001 Proceedings 3*. Springer, 2001, pp. 251–261.

[43] Y. Hori, T. Katashita, A. Sasaki, and A. Satoh, “Electromagnetic side-channel attack against 28-nm fpga device,” *Pre-proceedings of WISA*, p. 84, 2012.

[44] 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.

[45] A. Vasselle, P. Maurine, and M. Cozzi, “Breaking mobile firmware encryption through near-field side-channel analysis,” in *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop*, 2019, pp. 23–32.

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

[47] 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.

[48] 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.

[49] 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.

[50] R. Wang, H. Wang, and E. Dubrova, “Far field em side-channel attack on aes using deep learning,” in *Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security*, 2020, pp. 35–44.

[51] P. Rohatgi, “Electromagnetic attacks and countermeasures,” *Cryptographic Engineering*, pp. 407–430, 2009.

[52] A. Auddy and S. Sahu, “Tempest: Magnitude of threat and mitigation techniques,” in *2008 10th International Conference on Electromagnetic Interference & Compatibility*. IEEE, 2008, pp. 603–611.

[53] H. Aydın, “Tempest attacks and cybersecurity,” *International Journal of Engineering Technologies IJET*, vol. 5, no. 3, pp. 100–104, 2019.

[54] 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.

[55] Z. Liu, N. Samwel, L. Weissbart, Z. Zhao, D. Lauret, L. Batina, and M. Larson, “Screen gleaning: A screen reading tempest attack on mobile devices exploiting an electromagnetic side channel,” *arXiv preprint arXiv:2011.09877*, 2020.

[56] 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)*. IEEE, 2022, pp. 1440–1457.

[57] T. Ni, X. Zhang, and Q. Zhao, “Recovering fingerprints from in-display fingerprint sensors via electromagnetic side channel,” in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 253–267.

[58] Z. Liu, F. Lin, C. Wang, Y. Shen, Z. Ba, L. Lu, W. Xu, and K. Ren, “Camradar: hidden camera detection leveraging amplitude-modulated sensor images embedded in electromagnetic emanations,” *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 6, no. 4, pp. 1–25, 2023.

[59] D. Bastias, C. A. Perez, D. P. Benalcazar, and K. W. Bowyer, “A method for 3d iris reconstruction from multiple 2d near-infrared images,” in *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 2017, pp. 503–509.

Appendix

A. Parameters of Commercial Iris Recognition Devices

Table II shows the detailed parameters of three different commercially available iris capture devices. We have an indoor light intensity of 300 lux and the distance of iris capture is set to 20 cm, which is within the normal operating range of the devices.

TABLE II. Parameters of Commercial Iris Recognizer

Devices	**IriGo Mini (D1)**	**IrisID iCam (D2)**	**Mantra MIS100V2 (D3)**
Iris Capture Range	25-40cm	28-38cm	30-45cm
Ambient Light	≤10,000 lux	≤17,000 lux	≤1,000 lux
Standard	ISO/IEC 19794-6	ISO 29794-6, IEC 67421	IEC 62471:2006
Bit Depth	8 bits	8 bits	8 bits
EM Frequency	1,347 MHz	1,271 MHz	1,410 MHz

B. Iris Dataset Used for Evaluation

In this section, we provide a detailed account of the datasets used for training our diffusion model, as shown in Table III. Specifically, we select 20,000 iris images from the CASIA-IrisV4 dataset and another 20,000 images from the ND-IRIS-0405 dataset, forming the core of our training set. Additionally, to enhance data diversity, we include 1,120 iris images from the IITD v1 dataset and 5,331 images from the LivDet-Iris 2020 dataset.

TABLE III. Iris datasets used for evaluation.

Datasets	CASIA-IrisV4	ND-IRIS-0405	IITD v1	LivDet-Iris 2020
Subjects	1,800	356	224	118
Image format	JPEG	JPEG	BMP	PNG
Environment	Variety	Standard light	Standard light	Standard light
Devices	IrisKing IKEMB-100	LG 2200	JIRIS, JPC1000	Iris ID iCAM7000
Sensors	NIR	NIR	NIR	NIR
Liveness detection	No	No	No	Yes
Age	-	18-75	14-55	-
Resolution	640×480	640×480	320×480	640×480
Images for training	54,601(20,000)	64,980(20,000)	1,120(all)	5,331(all)

C. Attack Parameters of Different NIR sensors

This section introduces the attack parameters used for the evaluation of five different NIR sensors in Table IV. Specifically, the MX258-ZV has the strongest EM signal at 1,207 MHz, with a maximum reception distance of 3.1 meters. The HK5M-H150 has the strongest EM signal at 1,129 MHz, with a maximum reception distance of 2.9 meters. The S320H has the strongest EM signal at 975 MHz, with a maximum reception distance of 3.6 meters. The HW200 has the strongest EM signal at 1,090 MHz, with a maximum reception distance of 4.2 meters. The HBV-1911GS has the strongest EM signal at 1,181 MHz, with a maximum reception distance of 4.1 meters.

TABLE IV. Attack Parameters of Different NIR sensors

#	NIR Sensors	IR Filter	EM Frequency	USNR	Max Dist
N1	MX258-ZV	800 nm	1,207 MHz	27.9 dB	3.1 m
N2	HK5M-H150	850 nm	1,129 MHz	30.5 dB	2.9 m
N3	S320H	850 nm	975 MHz	25.0 dB	3.6 m
N4	HW200	800 nm	1,090 MHz	27.0 dB	4.2 m
N5	HBV-1911GS	850 nm	1,181 MHz	28.1 dB	4.1 m

D. Distribution of Experimental Data

In this paper, the distribution of experimental data involves multiple experimental setups and device configurations, with a total of 3,324 iris data samples from 50 users. Specifically, Section V-F1 contains 1,004 data samples from 50 users, where each user collected 2 samples under the same experimental conditions, covering 5 different SBCs and 5 different NIR sensors. Section V-F3 includes data from 3 commercial iris recognition devices, collected under both near-field and far-field conditions, resulting in 600 data samples, with each user contributing 2 samples per setup. In Section V-F4, 8 iris capture devices were used with 10 users, covering 9 different distances and 8 different angles, including 1,360 data samples, 240 of which overlap with the previous two sections. Section V-F5, Section V-F6, and Section V-F7 evaluate the effects of different LNAs, building materials, and EM shielding materials, respectively, with data totals of 160, 320, and 240 samples. Each setup involved 20 users, with 2 samples collected per user. It is worth noting that overlapping data exists across the sections mentioned above.