融合同态加密与PRNU指纹的图像设备识别与身份隐私保护方法

张品昌[1]，沈元章[1]，樊卫北[1]，董振江[1]，沈玉龙[2]，姜晓鸿[3]，肖甫[1]
（1. 南京邮电大学计算机学院，江苏 南京 210023；2. 西安电子科技大学计算机科学与技术学院，陕西 西安 710126；
3. 日本公立函馆未来大学情报科学研究院，日本 函馆 041-8655）

摘　要：针对工业互联网环境下图像设备易被伪造与身份信息易泄露的问题，提出了一种融合同态加密与物理指纹特征的图像设备识别与身份隐私保护方法。该方法采用图像传感器的光响应非均匀性（PRNU）指纹作为设备唯一标识，并引入基于离散余弦变换（DCT）与奇异值分解（SVD）的盲水印技术，建立PRNU指纹与盲水印之间的映射关系，从而提升在图像篡改场景下的识别鲁棒性。为实现隐私保护，进一步设计了基于ElGamal算法的同态加密机制，在加密域中完成身份识别过程，防止敏感信息在传输与计算过程中的泄露。实验结果表明，所提方法显著增强了识别准确性、抗篡改能力及数据隐私保护能力，具备在不可信工业通信环境中部署的可行性和实用性。

关键词：图像设备识别；PRNU指纹；盲水印；同态加密；ElGamal算法
中图分类号：TP309.7
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025119

Image device identification and identity privacy protection method via integration of homomorphic encryption and PRNU fingerprints

ZHANG Pinchang[1], SHEN Yuanzhang[1], FAN Weibei[1], DONG Zhenjiang[1],
SHEN Yulong[2], JIANG Xiaohong[3], XIAO Fu[1]
1. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
2. School of Computer Science and Technology, Xidian University, Xi'an 710126, China
3. School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan

Abstract: To address the challenges of device spoofing and identity leakage in image acquisition systems within industrial Internet environments, a secure and robust image device identification method was proposed that integrated homomorphic encryption and physical-layer fingerprinting. Specifically, photo-response non-uniformity (PRNU) fingerprints, which characterized intrinsic sensor-level features, were employed as unique device identifiers. A blind watermarking scheme based on discrete cosine transform (DCT) and singular value decomposition (SVD) was incorporated to establish a robust mapping between PRNU fingerprints and embedded watermarks, ensuring traceable identification even under tampering attacks. Furthermore, an ElGamal-based homomorphic encryption mechanism was designed to perform similarity matching and recognition in the encrypted domain, effectively preserving the privacy of device fingerprints and noise residuals. Experimental results demonstrate that the proposed method significantly enhances recognition accuracy, tamper-resilience, and data privacy protection, and it has the feasibility and practicality for deployment in untrusted industrial communication environments.

Keywords: image device identification, PRNU fingerprinting, blind watermarking, homomorphic encryption, ElGamal algorithm

收稿日期：2025–05–26；**修回日期：**2025–06–22
通信作者：董振江，dongzhenjiang@njupt.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2023YFB3107500）；国家自然科学基金资助项目（No.62272241）；江苏省重点研发计划基金资助项目（No.BE2023025）
Foundation Items: The National Key Research and Development Program of China (No.2023YFB3107500), The National Natural Science Foundation of China (No.62272241), The Primary Research and Development Program of Jiangsu Province (No.BE2023025)

0　引言

在信息技术高速发展的21世纪，工业互联网作为新一代信息技术与制造业深度融合的重要载体，已成为推动现代制造智能化转型的关键引擎[1]。随着物联网、大数据与人工智能等技术在工业互联网环境中的广泛部署，图像设备作为信息感知和过程监控的重要节点，被广泛应用于智能制造、安全监控、智慧交通等领域，在保障系统稳定运行与质量控制中发挥着重要作用[2-4]。然而，设备大规模接入及通信环境的不可信性显著提升了设备身份伪造与图像篡改的风险，亟须构建安全可靠的图像设备身份识别机制。

传统的图像设备识别方法主要通过分析图像中的统计特征（如颜色滤波阵列（CFA, color filte array）去马赛克算法[5-7]、白平衡[8]及JPEG压缩等后处理操作[9-10]），或利用卷积神经网络（CNN, convolutional neural network）自动提取高维特征以判断图像来源[11]。尽管这些方法在品牌或型号级别上具备一定的识别能力，但通常难以区分同一品牌或型号下的具体设备个体。此外，CNN在面对对抗样本时鲁棒性较差，易受到攻击干扰，降低了识别系统的可靠性[12]。

相较而言，光响应非均匀性（PRNU, photo response non-uniformity）指纹作为一种源于相机传感器制造过程中微观缺陷的物理层特征，能够表征不同像素对相同光照强度响应的微小差异。该指纹由Lukas等[13]首次提出，具有内容无关性、稳定性强和唯一性高等优点，能有效实现设备级别的个体识别。近年来，PRNU指纹广泛应用于图像来源追溯、设备认证和图像篡改检测等研究方向，被认为是突破传统方法识别精度瓶颈的重要手段。伴随该方法的不断发展，多种基于PRNU指纹的图像设备识别方法被提出。Li等[14]通过去除插值噪声，进一步提升了源相机识别精度。通过使用来自每个颜色通道的PRNU指纹，Hou等[15]提出了一种检测图像中色调修改的取证策略。Iuliani等[16]将从静止图像中提取的PRNU指纹推广到图像源识别。Pande等[17]开发了一种硬件架构，利用PRNU噪声进行图像源识别，并演示了任务的加速，使其适合实时应用场景。

然而，作为一种人工生成指纹，PRNU指纹易受多因素影响（如场景细节[18]、周期性图像处理[19]、低通滤波[20-21]等）。在工业互联网场景下，不可信节点可能会在通信过程中对图像进行恶意篡改，从而显著降低PRNU指纹的识别精度。为此，本文拟引入一种基于离散余弦变换（DCT, discrete cosine transform）和奇异值分解[22]（SVD, singular value decomposition）的盲水印技术[23-24]（一种基于频域的数字水印技术[25-26]，具有卓越的鲁棒性），通过预先构建PRNU指纹与盲水印之间的映射关系，并在图像采集阶段向图像中嵌入特定的盲水印，实现图像设备身份的结构化构造。即使图像内容遭受篡改，仍可凭借盲水印的强鲁棒性，通过盲水印与PRNU指纹的映射关系溯源至原始设备，从而实现PRNU指纹与盲水印的联合识别。

然而，PRNU指纹作为与设备身份强绑定的物理特征，一旦泄露将无法替换或重构，存在较高的隐私安全风险。在工业互联网等开放网络环境中，不可信节点可能通过识别过程中的交互数据推断出图像源设备的身份信息，进而引发隐私泄露问题。

为此，本文提出了一种融合同态加密与PRNU指纹的图像设备识别与身份隐私保护方法。一方面，引入基于DCT与SVD的盲水印技术，构建PRNU指纹与盲水印之间的映射关系，并在图像采集阶段嵌入鲁棒盲水印，实现对设备身份的稳健构造与溯源识别；另一方面，采用基于ElGamal算法的同态加密[27-28]机制，使识别过程在加密域内完成，有效防止PRNU指纹与图像噪声残差等敏感信息泄露。本文的主要贡献如下。

1) 针对设备身份易被伪造的问题，利用图像设备的物理层特征，即PRNU指纹进行识别，不仅可以增强识别性能，而且PRNU指纹可直接从图像设备拍摄的图像中提取，具有操作便捷和适用性强的优势。

2) 针对图像在篡改攻击下识别失效的问题，引入基于DCT和SVD的盲水印技术，通过提取的PRNU指纹构建图像设备身份，实现PRNU指纹和盲水印的联合识别。借助盲水印的鲁棒性，该方法能够实现篡改攻击下的图像溯源和完整性检测，从而增强识别的可靠性。

3) 针对不可信节点可能截获敏感设备身份信息的问题，引入基于ElGamal算法的同态加密机制，使识别过程能够在加密域内完成，从而有效保护PRNU指纹和图像噪声残差等敏感信息，显著降

低数据泄露和被篡改的风险，增强识别过程的安全性与可靠性。

1　系统模型

1.1　PRNU 指纹识别系统

本文方法基于如图1所示的PRNU指纹识别系统，该系统包含客户端与服务器之间的通信流程，主要分为注册阶段与识别阶段2个部分。注册阶段在离线可信环境中完成，客户端从图像设备中提取PRNU指纹，并将其作为身份模板存储至服务器端的模板数据库。在识别阶段，客户端发送包含身份声明和待识别图像噪声残差的请求至服务器，服务器根据声明信息检索相应的指纹模板，并与接收到的噪声残差进行相似性匹配。最终，服务器将计算得到的相似性得分与预设阈值进行比较，若相似性得分高于阈值则判定为识别成功，反之则视为识别失败。

1.2　攻击者模型

本文在威胁建模中引入半诚实攻击者模型，即假设攻击者拥有对系统的完全访问权限，能够被动观察系统运行过程，但不会主动篡改协议流程。在该模型下，攻击者将严格遵循协议执行顺序，但可通过对交互信息和系统行为的分析，尽可能多地推测出隐私数据和敏感参数。此外，本文假设不存在客户端与服务器之间的共谋行为，即两者不会通过私下通信破坏协议的安全性，且即使攻击者同时侵入客户端和服务器，也无法完全控制双方行为。因此，注册阶段在离线可信环境中完成，以确保PRNU指纹模板在系统初始化阶段未遭篡改，从而保障系统的初始安全性。

1.3　设计目标

本文方法旨在实现图像设备身份识别的鲁棒性与隐私性统一，具体目标如下。

1) 联合识别能力。实现PRNU指纹与盲水印的融合识别机制，即使在图像遭受篡改的情况下，仍可借助盲水印的鲁棒性及其与PRNU指纹之间预先构建的映射关系，准确溯源至对应的图像设备，实现设备身份的稳健判定。

2) 识别过程的隐私保护。通过引入同态加密机制，在加密域中完成PRNU指纹的相似性匹配计算，防止攻击者通过监听通信交互过程推断设备身份，有效保障了PRNU指纹及图像噪声残差等敏感信息的机密性与完整性。

2　基于PRNU指纹和盲水印的图像设备识别

传统PRNU指纹识别方法通过计算图像噪声残差与指纹模板之间的相关性，判断图像是否来自某一特定设备。然而，在图像遭受剪裁、旋转、压缩等篡改攻击的情况下，噪声残差往往会失真或丢失，导致识别性能显著下降，甚至完全失效。为此，本文提出了一种结合PRNU指纹与盲水印技术的图像设备识别方法，该方法不仅能够在图像被篡改的条件下实现有效识别，还具备对图像完整性进行判别的能力。具体而言，通过构建PRNU指纹与盲水印之间的映射关系，将设备身份信息嵌入图像中，从而在识别阶段可借助提取的盲水印信息回溯至目标设备。同时，结合盲水印对应的指纹与图像噪声残差之间的相关性，实现图像源设备的验证与篡改区域的完整性检测。

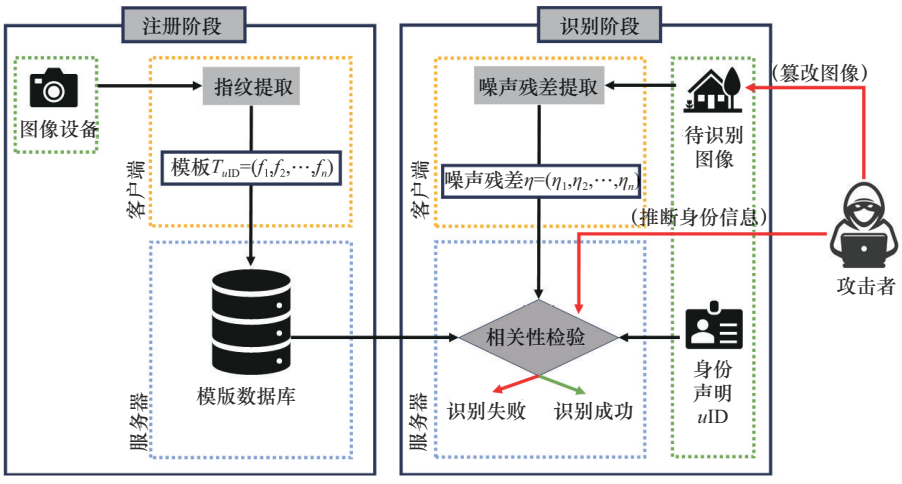


图1　PRNU指纹识别系统

2.1　图像设备识别方法

本文提出的图像设备识别方法流程如图 2 所示，主要包括 3 个核心步骤，分别为设备身份构造、特征提取与相关性检验。首先，设备身份构造阶段旨在建立 PRNU 指纹与盲水印之间的一一映射关系。通过特定算法提取设备的 PRNU 指纹，并将其与预设的盲水印信息绑定，生成唯一的设备身份标识。设备身份构造完成后，相机在图像采集阶段将对应水印嵌入所拍摄图像中，以便于后续识别。其次，特征提取阶段从待识别图像中提取嵌入的盲水印信息与噪声残差。借助频域变换、滤波增强等图像处理技术，可在不破坏 PRNU 指纹完整性的前提下实现有效特征提取，确保后续识别的稳定性与准确性。最后，相关性检验阶段通过比较图像噪声残差与盲水印对应的 PRNU 指纹之间的相似性，完成设备身份确认。为提高检验的精度与鲁棒性，本文采用交叉相关性（CC, cross-correlation）和峰值相关能量（PCE, peak to correlation energy）作为双重评估指标，分别从数值幅度与结构形态 2 个维度量化相关性。综合以上步骤，该方法不仅能够在图像遭篡改的场景下实现设备身份的稳健识别，还具备图像完整性校验能力，构建了一套兼顾安全性与可靠性的图像设备设别方案。

2.2　设备身份构造

1) PRNU 指纹提取。PRNU 指纹提取首先需要从相机图像中分离出特定像素矩阵 $\boldsymbol{I}$（维度为 $h \times w$）的噪声残差 $\boldsymbol{\eta}$。本文采用的噪声提取方法是基于自适应维纳滤波的多级小波噪声增强。该方法分别对矩阵 $\boldsymbol{I}$ 的红、绿、蓝通道进行处理，首先从每个颜色通道中去除全图均值，然后分别减去每个颜色通道的行均值和列均值，最终将 3 个颜色通道的噪声残差进行合并。为了进一步优化噪声特征，在离散傅里叶变换（DFT, discrete Fourier transform）域中应用噪声峰值去除步骤，去除残余的周期性伪影，并对残差的频谱进行白化以增强 PRNU 指纹的鲁棒性。最终，结合来自同一相机 c 拍摄的一组图像样本 $I_k\left(k = 1,2,\cdots,F_c\right)$，可以通过最大似然估计方法得到相机的 PRNU 指纹 $\boldsymbol{f}_c$ 为

$$\boldsymbol{f}_c = \frac{\sum_{k=1}^{F_c} \boldsymbol{\eta}_k I_k}{\sum_{k=1}^{F_c} I_k^2} \tag{1}$$

给定以 PRNU 指纹 $\boldsymbol{f}_c$ 为特征的相机 c 和噪声残差为 $\boldsymbol{\eta}^{(q)}$ 的待识别图像 $I^{(q)}$。通过比较图像噪声残差和相机 PRNU 指纹，可以确定该图像是否用给定的相机拍摄。这种相似性匹配可以通过相关性检验来

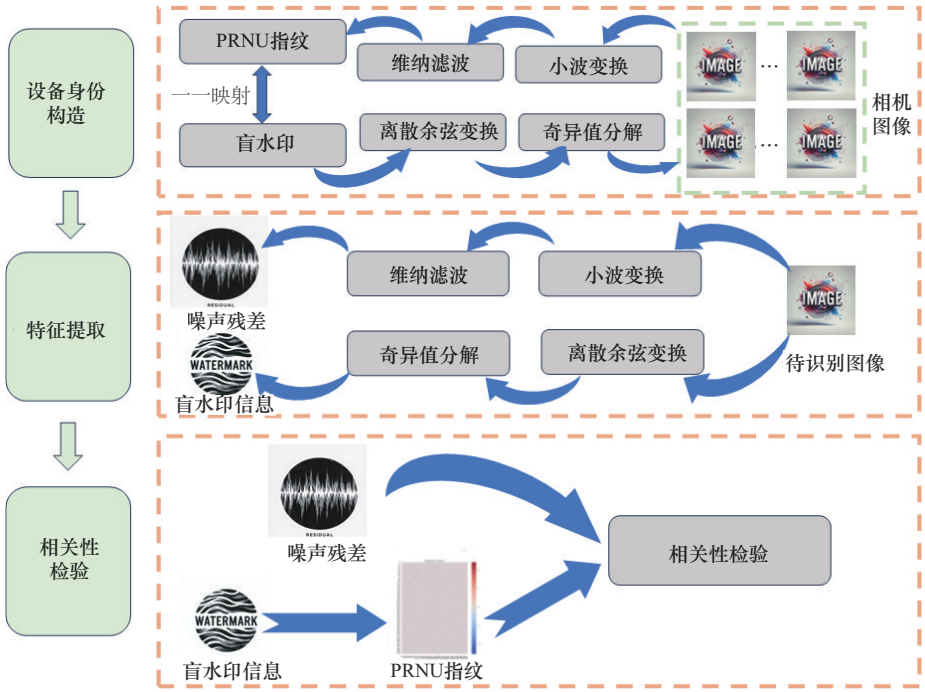


图2　图像设备识别方法流程

判断，定义为

$$\rho\left(\boldsymbol{f}_c,\boldsymbol{\eta}^{(q)}\right)=\sum_{i=1}^{h}\sum_{j=1}^{w}\hat{\boldsymbol{f}}_c(i,j)\boldsymbol{\eta}^{(q)}(i,j) \tag{2}$$

当$\rho\left(\boldsymbol{f}_c,\boldsymbol{\eta}^{(q)}\right)\geqslant\tau$，则判定$I^{(q)}$包含$\boldsymbol{f}_c$，将查询图像归属于相机$c$，其中$\tau$是一个适当设置的阈值，目的是将虚警概率约束在期望的目标值以下。

2) 盲水印嵌入。本文采用基于DCT和SVD的盲水印技术。在水印嵌入过程中，首先对载体图像进行DCT，提取每个变换块中的第一个系数，并将其组成矩阵，随后进行SVD得到奇异值矩阵，再通过与水印矩阵的迭代操作完成水印的嵌入。在盲水印算法中，设$g(x)$为原始图像，$\mathrm{wm}(x)$为水印图像，α为嵌入强度，则带水印的图像$g'(x)$可以表示为

$$g'(x)=g(x)+\alpha\left(\mathrm{wm}(x)\right) \tag{3}$$

在此过程中，需选取特定的值α使嵌入后的图像在视觉效果和水印强度之间取得平衡。

图3给出了盲水印嵌入前后结果对比（水印信息为字符串形式），在视觉上几乎无法察觉。这表明盲水印技术可以在不损害图像原有信息的前提下，将水印无痕嵌入。这一措施可以确保原有图像的质量和特征得到良好保存，并防止水印遮挡导致原有图像信息的丢失。此外，嵌入盲水印后，仍可以确保后续对图像的噪声残差进行完整提取。

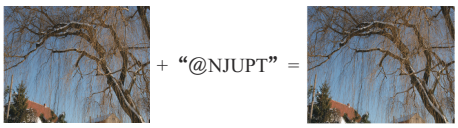


图3　盲水印嵌入前后结果对比

图4展示了本文方法中的设备身份构建过程，即采用注册绑定式映射构建PRNU指纹与盲水印的映射关系，具体流程如下。

1) 注册阶段。在离线可信环境中，系统为每台设备提取PRNU指纹$\boldsymbol{f}$，并自动生成一个唯一标识水印$\mathrm{wm}(x)$（可为随机字符串、设备序列号哈希值或自定义标识图像）。

2) 绑定存储。将二元组$\left(\boldsymbol{f},\mathrm{wm}(x)\right)$作为设备的身份凭证，并将其存储于服务器数据库中。

3) 水印嵌入。设备在采集图像时，自动将与其绑定的水印$\mathrm{wm}(x)$嵌入图像中。

在识别阶段，通过提取待识别图像的盲水印$\mathrm{wm}(x)$检索服务器中绑定的指纹模板$\boldsymbol{f}$，实现设备溯源。该映射不需要复杂密码学转换，依赖系统预注册的绑定关系，兼具高效性与可管理性。

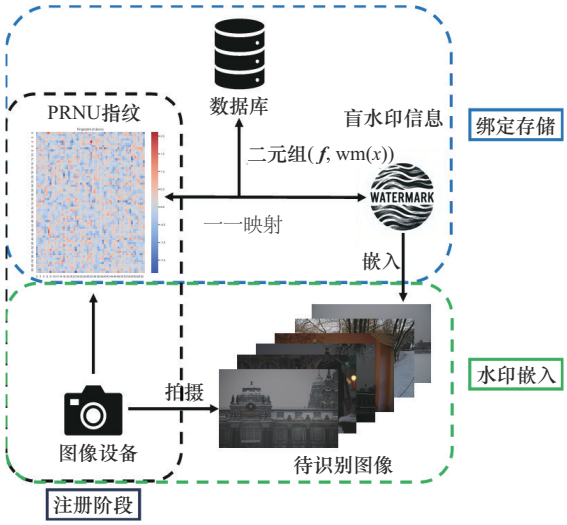


图4　设备身份构建过程

2.3　特征提取

特征提取的主要目的是通过有效的算法和技术，从有识别需求的图像中提取盲水印信息和噪声残差。这一过程为后续的识别、验证和分析提供可靠的数据基础。

1) 噪声残差提取。提取图像噪声残差的过程与PRNU指纹提取过程相似，主要通过小波变换和维纳滤波等步骤进行。由于噪声与图像细节的高度混合，直接从图像中提取噪声残差具有一定的挑战性。因此，首先采用小波变换对图像进行多尺度分解，并利用其优异的局部特征表征能力在频域区分噪声分量与图像细节。继而引入维纳滤波器，通过最小化均方误差优化图像质量并进一步抑制噪声干扰。通过2种技术的结合，可以有效提取图像的噪声残差信息，提高后续识别的精度。图5展示了经此流程处理的噪声残差提取结果，直观呈现了分离效果。

2) 盲水印提取。在盲水印提取过程中，首先对包含水印的图像进行DCT，从空间域转换为频域。其次，在频域中对转换后的图像进行SVD，将图像矩阵分解为3个矩阵的乘积，并利用修改过的奇异值提取潜在的盲水印信息。在水印提取阶段，为了有效区分水印信号与噪声或其他干扰，通常采用k均值聚类法对提取的数据进行处理，从而

提高水印提取的准确性与识别效率。完成聚类后，通过预设的密码对提取出的水印序列进行洗牌恢复，以确保盲水印信息的完整性。水印提取过程可表示为

$$\mathrm{wm}(x) = h\left(\sigma_{\mathrm{embed}} - \sigma_{\mathrm{orig}}, \alpha\right) \tag{4}$$

其中，$\mathrm{wm}(x)$是提取的水印信号，σ_{embed}和σ_{orig}分别是嵌入水印后的奇异值和原始图像的奇异值，α是水印强度参数，$h(\cdot)$是用于从奇异值差异中提取水印的函数。同时，水印强度和图像失真程度可以通过调整参数α来控制，参数越大，水印的鲁棒性越强，但可能会导致更大的图像失真。在提取水印信息$\mathrm{wm}(x)$后，通过匹配事先存储的身份凭证，可检索数据库中的指纹模板$\boldsymbol{f}$，进而计算噪声残差与指纹模板的相关性，以实现图像识别。

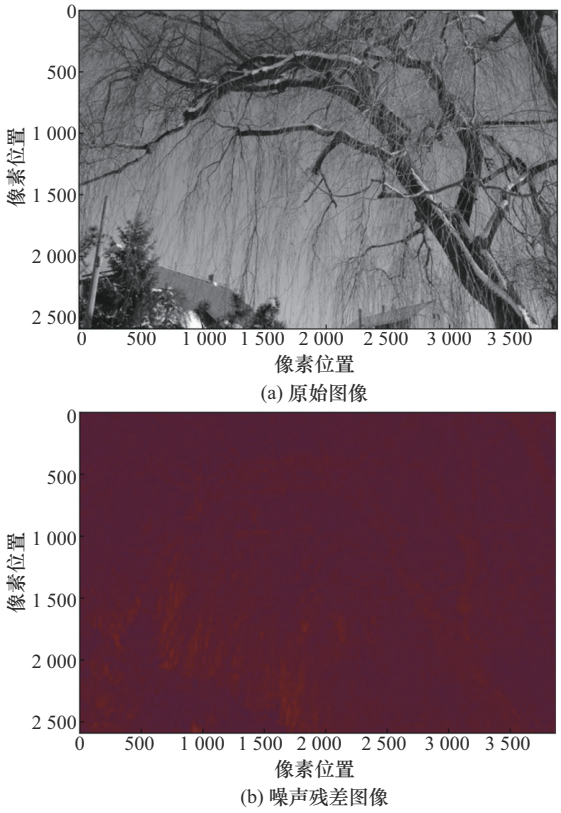


图5　噪声残差提取结果

2.4　相关性检验

在相关性检验阶段，采用CC和PCE这2个评判指标。CC主要用于衡量线性相关性，而PCE则关注结构相似性。通过2种指标的结合，能够全面地评估PRNU指纹与噪声残差之间的相关性，从而提升识别的准确性和鲁棒性。

2.4.1　交叉相关性

交叉相关性是一种广泛应用于信号处理的评判指标，能够有效衡量2个信号之间的相关性。在图像设备识别过程中，通过计算PRNU指纹与噪声残差的分量乘积和，可以量化两者之间的相似度，从而评估其相关性（由于后续同态加密需要，本文提及的交叉相关性值都没有进行归一化操作）。在离散情况下，交叉相关性可以通过式(5)计算。

$$\mathrm{CC} = \sum_{i=1}^{n} x_i y_i \tag{5}$$

其中，x_i和y_i分别表示PRNU指纹和噪声残差的第i个分量，CC表示它们之间的交叉相关性值。

2.4.2　峰值相关能量

峰值相关能量是一种重要的信号噪声分析技术，通过比较图像中心像素与其邻域像素的能量值，量化图像的结构相关性，从而有效评估信号噪声模式。在图像设备识别过程中，CC值通常作为计算PCE的输入。该方法不仅能够反映PRNU指纹与噪声残差之间的线性相关性，还兼顾了图像的结构信息。PCE的计算式如式(6)所示。

$$\mathrm{PCE} = \frac{\max\left(\left|R_{xy}(k)\right|\right)}{\sqrt{\sum_{k} R_{xx}(k) \sum_{k} R_{yy}(k)}} \tag{6}$$

其中，$R_{xy}(k)$是信号x和信号y的归一化互相关函数，k是时间或空间偏移，$R_{xx}(k)$和$R_{yy}(k)$分别是信号x和信号y的归一化自相关函数。PCE值越高，表示2个信号在某个特定偏移处的相关性越强，即它们之间的相似度越高。

3　基于同态加密的安全识别

为了保证识别过程中设备指纹和图像信息不被窃取，本文提出了一种基于ElGamal(2, 2)阈值加密算法的同态识别方法，以期在加密域中实现图像设备的有效识别。

3.1　ElGamal(2, 2)阈值加密算法

ElGamal加密算法的安全性依赖于底层循环群的决策性DDH（decisional Diffie-Hellman）假设，该假设确保了离散对数问题（DLP, discrete logarithm problem）的计算困难性。在ElGamal加密算法中，设G是由生成元g生成的大小为p的循环群，私钥a是1到群阶之间的随机数，公钥h为生成元g的a次幂。

$$\langle g\rangle = G,\ |G| = p,\ a \in_R (0,|G|),\ h = g^a \quad (7)$$

用于加密明文m并生成元组(c_1,c_2)的加密函数E定义为

$$E(m) = [\![m]\!] = (c_1,c_2) = (g^r, mh^r),\ r \in_R (0,|G|) \quad (8)$$

其中，r为加密过程中引入的随机数，其使ElGamal加密具有概率性，即使同一消息的不同加密也会产生不同的密文。双括号$[\![\cdot]\!]$为加密值，如果m是向量或矩阵，则$[\![m]\!]$的元素按分量加密。拥有私钥a的任何一方都可以利用解密函数D进行解密，其定义为

$$D(c_1,c_2) = c_1^{-a}c_2 = (g^r)^{-a}\left(m(g^a)^r\right) = m(g^{-ar}g^{ar}) = m \quad (9)$$

ElGamal (2, 2)阈值加密算法是ElGamal加密算法的门限加密版本，适用于需要多个参与者协同解密的场景。由于本文的交互模型只有两方，因此可以将密钥分成2个随机部分，即$a = a_1 + a_2$。拥有密钥a_1的一方能够执行部分解密D_1，其定义为

$$D_1(c_1,c_2) = [m] = (c_1, c_2c_1^{-a_1}) = (g^r, mg^{ar}g^{-a_1r}) = (c_1', c_2') \quad (10)$$

其中，[·]表示部分解密的密文。该密文不会泄露任何信息，因为它与公钥g^{a_2}加密的密文无法区分。第一阶段解密后，拥有密钥a_2的一方可以进行最终解密D_2，从而恢复出最终的明文，表示为

$$D_2(c_1',c_2') = (c_1'^{-a_2})(c_2') = (g^r)^{-a_2}(mg^{ar-a_1r}) = m(g^{-a_2r}g^{ar-a_1r}) = m \quad (11)$$

该算法确保只有在参与双方的协作下，才能实现完全解密，从而有效保护识别过程中数据的安全性。

3.2 同态加密

ElGamal加密本身具有乘法同态性。

$$[\![m_1m_2]\!] = [\![m_1]\!][\![m_2]\!] \quad (12)$$

因此，有

$$(c_1,c_2)(c_1',c_2') = ((g^r)(g^{r'}),(mh^r)(m'h^{r'})) = (g^{r+r'}, mm'h^{r+r'}) \quad (13)$$

通过将明文m编码为生成元g的指数，即g^m作为新的明文，利用ElGamal加密算法的乘法同态性来实现同态加法和同态减法，分别表示为

$$[\![g^{m_1}g^{m_2}]\!] = [\![g^{m_1}]\!][\![g^{m_2}]\!] = [\![g^{m_1+m_2}]\!] \quad (14)$$

$$[\![g^{m_1}g^{-m_2}]\!] = [\![g^{m_1}]\!][\![g^{-m_2}]\!] = [\![g^{m_1-m_2}]\!] \quad (15)$$

由式(12)~式(15)可知，理论上一般的线性操作都可以在加密域中进行，然而在实际背景中，基于ElGamal加密算法的同态加法操作仅支持指数为非负整数的情形。因此，在图像设备的安全识别过程中，本文采用基于线性操作的CC作为同态识别的检验指标，并采用预处理操作减少在线计算开销。

3.3 基于ElGamal加密算法的同态识别

3.3.1 预处理

为确保加密域中同态识别的快速有效实施，现对PRNU指纹和噪声残差信息进行预处理操作。

1) 取整和取绝对值。首先将PRNU指纹和噪声残差信息分别展开为向量$\boldsymbol{f} = (f_1,f_2,\cdots,f_N)$和$\boldsymbol{\eta} = (\eta_1,\eta_2,\cdots,\eta_N)$。其次，分别计算PRNU指纹和噪声残差向量的符号矩阵$\boldsymbol{S}_f$和$\boldsymbol{S}_\eta$，表示为

$$\boldsymbol{S}_f = (\mathrm{sign}(f_1),\mathrm{sign}(f_2),\cdots,\mathrm{sign}(f_N))$$
$$\boldsymbol{S}_\eta = (\mathrm{sign}(\eta_1),\mathrm{sign}(\eta_2),\cdots,\mathrm{sign}(\eta_N)) \quad (16)$$

对所有分量进行取整和取绝对值操作，以确保参与同态计算的值均为非负整数。

$$\boldsymbol{f} = \mathrm{round}(\mathrm{abs}(f)) = \mathrm{round}(|f_1|,|f_2|,\cdots,|f_N|)$$
$$\boldsymbol{\eta} = \mathrm{round}(\mathrm{abs}(\eta)) = \mathrm{round}(|\eta_1|,|\eta_2|,\cdots,|\eta_N|) \quad (17)$$

其中，round(·)表示取整操作，abs(·)表示取绝对值操作。由于初始数据为浮点数，为保证数据精度，可以在执行取整和取绝对值操作之前，先将数据乘10或100后再进行取整处理。

2) 预先构建模板库。对于已有的PRNU指纹，系统为每个指纹生成对应的模板并存储在服务器中，以便在识别时调用。具体的模板生成步骤如算法1所示。将PRNU向量的每个元素与噪声残差所有可能取值的加密值逐一相乘（由于所有分量值均为正整数，取值范围为0到最大噪声残差值$\eta_{\max}$之间的整数），并且为了后续同态计算的需要，将明文编码为g^m的形式进行加密。通过该方法计算的模板$[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]$维度为$N(\eta_{\max}+1)$，其中每个元素代表特定分量与噪声残差可能取值的相似性得分$[\![t_{i,j}]\!]$。在线识别时仅需选取模板相应元素

进行运算，即可获得最终的相似性得分，从而减轻在线计算开销。

算法 1　基于 ElGamal 加密的 PRNU 指纹模板生成

输入　PRNU 指纹向量 $\boldsymbol{f}$（一维），噪声残差分量的最大值 $\eta_{\max}$

输出　模板 $[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]$

① 初始化参数：PRNU 指纹向量长度 N，模板 $[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]=[\![\cdot]\!]$

② for i in range$(0,N)$

③　encryted_$\boldsymbol{T}_{u\mathrm{ID}}=[\![\cdot]\!]$

④　for j in range $(0,\eta_{\max}+1)$

⑤　$[\![t_{i,j}]\!]=[\![g^{f_i\cdot j}]\!]$

⑥　encrypted_$\boldsymbol{T}_{u\mathrm{ID}}$.append$\left([\![t_{i,j}]\!]\right)$

⑦　end for

⑧　$[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]$.append$\left(\text{encrypted_}\boldsymbol{T}_{u\mathrm{ID}}\right)$

/*模板 $[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]$ 共 N 行，每行保存对应分量与可能的噪声残差取值的乘积*/

⑨ end for

⑩return $[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]$

3.3.2　安全识别协议

本文设计的安全识别协议如图 6 所示，具体包括以下内容。

1) 发起识别请求。客户端向服务器发起识别请求，并附上身份声明 uID，其中 uID 可通过提取的盲水印信息表示。服务器接收到身份声明后先查验该身份是否已经注册，如果没有则识别失败，反之则根据身份声明 uID 取出对应的指纹模板 $[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]$ 和符号矩阵 $\boldsymbol{S}_f$ 并将其发送给客户端。同时，客户端提取待识别图像的噪声残差信息，经预处理后获得图像噪声残差向量 $\boldsymbol{\eta}=\left(|\eta_1|,|\eta_2|,\cdots,|\eta_N|\right)$ 和符号矩阵 $\boldsymbol{S}_\eta$。

2) 计算 CC 与阈值 τ。客户端接收到指纹模板 $[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]$ 和符号矩阵 $\boldsymbol{S}_f$ 后，计算噪声残差和 PRNU 指纹的 CC，如算法 2 所示。根据噪声残差分量值 η_i，从模板 $[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]$ 中选取对应元素 $[\![t_{i,\eta_i}]\!]$，并依次执行同态加法操作。由于同态加法的计算结果都以指数形式保存在加密数据中，并且所有分量均为正整数，所以计算结果实际是 $\boldsymbol{f}$ 和 $\boldsymbol{\eta}$ 的分量绝对值乘积和，表示为

$$[\![\mathrm{CC}]\!]=\left[\!\!\left[g^{|f_1\eta_1|+|f_2\eta_2|+\cdots+|f_N\eta_N|}\right]\!\!\right] \tag{18}$$

与未加密情形下的 CC 值相比较，这种计算方式导致所有负乘积的绝对值之和被额外计算了 2 倍。

为了保证交叉相关性与阈值之间的差值与原始计算结果一致，引入标记变量 $M=[\![g^0]\!]$。具体而言，通过对照预先计算的符号矩阵 $\boldsymbol{S}_f$ 和 $\boldsymbol{S}_\eta$，当对应分量 f_i 和 η_i 的原乘积为负，即 $\boldsymbol{S}_f[i]\boldsymbol{S}_\eta[i]<0$ 时，标

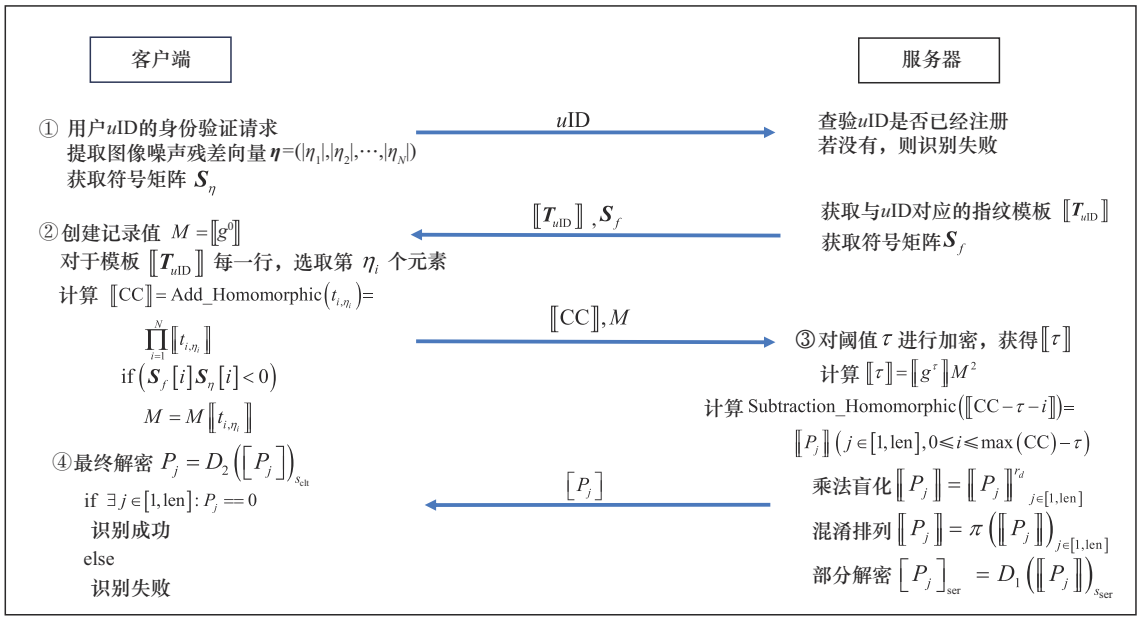


图 6　安全识别协议

记变量记录该乘积的绝对值为

$$M = M\left[\!\left[t_{i,\eta_i} \right]\!\right] = M\left[\!\left[g^{|f_i\eta_i|} \right]\!\right] \tag{19}$$

最后，将加密的阈值$[\![\tau]\!]$（以g^{τ}为明文加密）与标记变量M的平方相乘，借助同态加法实现修正，使阈值加上因符号影响而产生的修正值。修正后的阈值与交叉相关性的差值保持与原始计算结果一致，从而确保阈值判别过程的正确性和一致性。

$$[\![\tau]\!] = [\![g^{\tau}]\!]M^2 = [\![g^{\tau}]\!]\left[\!\left[g^{2[\![\sum|f_i\eta_i|]\!]} \right]\!\right] = \left(c_1, g^{\tau+2\sum|f_i\eta_i|}h^r\right) \tag{20}$$

算法2 计算交叉相关性CC与相应的阈值$[\![\tau]\!]$

输入 噪声残差向量$\boldsymbol{\eta}=\left(|\eta_1|,|\eta_2|,\cdots,|\eta_N|\right)$（一维），指纹模板$[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]$，符号矩阵$\boldsymbol{S}_f$和$\boldsymbol{S}_r$

输出 交叉相关性$[\![\mathrm{CC}]\!]$，阈值$[\![\tau]\!]$

① 初始化参数：标记变量$M=[\![g^0]\!]$，交叉相关性$[\![\mathrm{CC}]\!]=[\![g^0]\!]$（初始为0）

② for i in range$(0,N)$

③ select $\left[\!\left[t_{i,\eta_i} \right]\!\right]$ from $[\![\boldsymbol{T}_{u\mathrm{ID}}]\!]$

④ $[\![\mathrm{CC}]\!]=\mathrm{Add\_Homomorphic}\left([\![\mathrm{CC}]\!],\left[\!\left[t_{i,\eta_i} \right]\!\right]\right)$

/*经过N轮的同态加法，最终获得PRNU指纹和噪声残差的交叉相关性值*/

⑤ if$\left(\boldsymbol{S}_f[i]\boldsymbol{S}_\eta[i]<0\right)$:

⑥ $M = M\left[\!\left[t_{i,\eta_i} \right]\!\right] = M\left[\!\left[g^{|f_i\eta_i|} \right]\!\right]$

⑦ end if

⑧ end for

⑨ $[\![\tau]\!] = [\![g^{\tau}]\!]M^2 = [\![g^{\tau}]\!]\left[\!\left[g^{2[\![\sum|f_i\eta_i|]\!]} \right]\!\right]$

⑩return $[\![\mathrm{CC}]\!],[\![\tau]\!]$

3) 阈值判别。服务器接收到交叉相关性值$[\![\mathrm{CC}]\!]$后，需要将其与阈值$[\![\tau]\!]$进行比较，而在加密域中，直接将二者相减无法得到结果，因为同态减法的结果存储在密文的指数部分，所以无论相减结果大于零还是小于零，密文始终为正。为解决这一问题，引入一个排列计算（如算法3所示），令索引i取值为从0起的连续整数，直到$\max(\mathrm{CC})-\tau$，并利用同态减法依次计算$[\![\mathrm{CC}-\tau-i]\!]$，形成排列值$\left[\!\left[P_j \right]\!\right]_{j\in[1,\mathrm{len}]}$，排列长度$\mathrm{len}=\max(\mathrm{CC})-\tau+1$。如果CC大于或等于阈值$\tau$，则该排列中必然包含零值，反之，如果CC小于阈值$\tau$，则排列中的所有值均大于零。其中，$\max(\mathrm{CC})$源于预处理操作中对PRNU指纹和噪声残差向量的取整操作，因此计算得到的交叉相关性值与原始浮点数计算结果存在细微差异。假设所有取整操作均向上取整，则有

$$\begin{aligned}\max(\mathrm{CC}) &\leqslant \left(|f_1|+1,|f_2|+1,\cdots,|f_N|+1\right)\\ &\left(|\eta_1|+1,|\eta_2|+1,\cdots,|\eta_N|+1\right)=\\ &\mathrm{CC}+\sum_{i=1}^{N}|f_i|+\sum_{i=1}^{N}|\eta_i|+N\end{aligned} \tag{21}$$

由于同态加法和同态减法操作均保存在指数上，解密后结果仍以指数形式呈现，而恢复明文则需要解决DLP，这在计算上较为复杂。然而，当明文$m=0$时，$g^m=1$，此时的计算几乎可以忽略不计（判断识别结果正是基于该事实）。所以后续的乘法盲化和随机排列操作只影响非0值。具体而言，乘法盲化操作通过对每个密文取随机数r_d次方。如果明文的指数不为0，则该指数将随之改变，同时引入的随机数进一步增强了排列的随机性。

$$[\![m]\!]^{r_d} = \left(g^{r_dr}, g^{r_dm}h^{r_dr}\right) \tag{22}$$

此外，服务器采取随机排列操作打乱所有排列的顺序，以防止攻击者通过连续排列的关系推测出原数据信息。最终，服务器对排列$\left[\!\left[P_j \right]\!\right]_{j\in[1,\mathrm{len}]}$进行部分解密，并将解密结果$\left[P_j \right]_{j\in[1,\mathrm{len}]}$发送给客户端。

算法3 加密域中交叉相关性CC与阈值的判别

输入 加密后的交叉相关性$[\![\mathrm{CC}]\!]$，修正后的阈值$[\![\tau]\!]$

输出 排列$\left[\!\left[P_j \right]\!\right]_{j\in[1,\mathrm{len}]}$

① 初始化参数：索引$i=0$，排列长度$\mathrm{len}=\max(\mathrm{CC})-\tau+1$

② while i < len

③ $[\![i]\!]=\mathrm{Elgamal.encryption}(i)$

/*计算索引i的加密值$[\![i]\!]$*/

④ $k=\mathrm{Sub\_Homomorphic}\left([\![\mathrm{CC}-\tau-i]\!]\right)$

/*利用同态减法计算$\mathrm{CC}-\tau-i$的值*/

⑤ $[\![P]\!]$.append(k)

⑥ i++

⑦ end while

⑧ $[\![P_j]\!]=[\![P_j]\!]^{r_d}_{j\in[1,\text{len}]}$ /*乘法盲化*/

⑨ $[\![P_j]\!]=\pi\left([\![P_j]\!]\right)_{j\in[1,\text{len}]}$ /*随机排列*/

⑩return $[\![P_j]\!]_{j\in[1,\text{len}]}$

4) 判断识别结果。客户端对排列$\left[P_j\right]_{j\in[1,\text{len}]}$进行最终解密，并且只需判断是否存在0（$g^0=1$）值。若存在0值，则说明识别成功，否则识别失败。

3.3.3 *安全性分析*

本文假设攻击者为半诚实类型，且不存在共谋行为。因此，讨论的攻击场景仅包括客户端受损和服务器受损2种情况。

1) 客户端受损。在协议的第1轮交互中，客户端接收经过ElGamal加密的模板$[\![\boldsymbol{T}_{u\text{ID}}]\!]$。由于采用阈值加密机制，客户端和服务器各持有一部分密钥，客户端无法单独解密矩阵。并且基于ElGamal加密算法的IND-CPA安全性，即使客户端部分解密模板，攻击者仍无法区分矩阵中的元素，也无法获取有关模板的任何敏感信息。在第2轮交互中，客户端接收部分解密的向量，并利用私钥恢复明文。然而，该向量经过乘法盲化和随机排列操作，无法被有效推断。最终，客户端只能根据解密结果是否包含0判断识别结果，符合协议预期。

2) 服务器受损。在协议的首轮交互中，服务器接收未加密的身份声明uID。该声明仅作为验证标识符而存在，不包含任何特征信息，从而避免了敏感信息的泄露。在第2轮交互中，服务器接收加密的交叉相关性值[[CC]]，由于服务器仅有部分密钥，所以无法单独解密。并且[[CC]]值仅是所选模板中加密个体的乘积值，无法根据它推测模板内容。所以整个交互过程中除了比较结果（即协议的输出）之外，没有任何特征信息泄露。

3.4 基于椭圆曲线的ElGamal同态加密算法

相较于传统ElGamal加密，基于椭圆曲线的ElGamal同态加密在相同密钥长度下能够提供更高的安全性。并且椭圆曲线的数学结构使其在相同计算复杂度下，能够实现更强的加密强度，进而在保证安全性的同时，使用更短的密钥，有效减少了对存储和计算资源的需求。

基于椭圆曲线的ElGamal同态加密算法依赖于椭圆曲线离散对数问题的计算困难性。其构建过程为：首先选择大素数p，并定义有限域F_p上的椭圆曲线$E_{a,b}$，其方程形式为$y^2=x^3+ax+b\ (\text{mod}\ p)$，其中$a$和$b$为常数，且满足判别式$4a^3+27b^2\neq 0\ (\text{mod}\ p)$，以确保曲线没有奇异点。其次，选择曲线上的基点$G$，并选取私钥$d\in Z_n$，其中$n$为基点$G$的阶。公钥$P$通过计算$P=dG$得到。

加密过程中需要将明文消息m映射为椭圆曲线上的点M，并且选择随机数$r\in Z_n$，最终生成元组(c_1,c_2)。加密函数E定义为

$$E(m)=[\![m]\!]=(c_1,c_2)=(rG,M+rP),\ r\in Z_n \tag{23}$$

解密函数D定义为

$$D(c_1,c_2)=c_2-dc_1=M+rP-drG=M \tag{24}$$

椭圆曲线中的加法和乘法并非简单的代数加法和乘法，而是定义在椭圆曲线上的点加法和点乘法。在椭圆曲线的点加法中，2个不同点$P(x_1,y_1)$和$Q(x_2,y_2)$的和$R=P+Q$是通过计算连接这两点的直线的斜率$\lambda=\dfrac{y_2-y_1}{x_2-x_1}(\text{mod}\ p)$来实现的，新点的坐标由计算式$x_3=\lambda^2-x_1-x_2(\text{mod}\ p)$给出。而对于同一点加法（即$P+P$），则是通过计算切线来实现。此时，斜率$\lambda$由点$P(x_1,y_1)$的切线斜率给出，计算式为$\lambda=\dfrac{3{x_1}^2+a}{2y_1}(\text{mod}\ p)$，而新点的坐标同样可以通过相应的计算式得出。椭圆曲线上的乘法mG（即将点G重复加m次）是通过连续的点加法实现的，常使用快速幂算法来提高计算效率。

为了实现基于椭圆曲线的ElGamal同态加密算法的同态操作，本文选用的编码方式是将明文m编码为椭圆曲线上的点mG，其中G是椭圆曲线的基点。通过这种编码方式，可以实现同态加法和同态减法。在同态加法中，若加密后的密文为(C_1,C_2)和(C_1',C_2')，则两者的和可以通过式(25)计算。

$$[\![m+m']\!]=(C_1+C_1',C_2+C_2')=((r+r')G,(m+m')G+(r+r')P) \tag{25}$$

其中，r和r'是随机数，P是公钥，m和m'分别是明文消息。对于同态减法，给定2个密文(C_1,C_2)和

$\left(C_1',C_2'\right)$，其同态减法可以通过式(26)计算。

$$[\![m-m']\!]=\left(C_1-C_1',C_2-C_2'\right)=\left((r-r')G,(m-m')G+(r-r')P\right) \tag{26}$$

为了实现门限加密，可以将私钥d分成两部分d_1和d_2，使得只有2个用户协同操作才能共同解密密文。具体地，将私钥分割成两部分后，拥有密钥d_1的一方能够执行部分解密D_1，其函数定义为

$$D_1\left(C_1,C_2\right)=[m]=\left(C_1,C_2-C_1d_1\right)=\left(rG,mG+r\left(d-d_1\right)G\right)=\left(C_1',C_2'\right) \tag{27}$$

第一阶段解密后，拥有密钥d_2的一方可以进行最终解密D_2，从而恢复出最终的明文，如式(28)所示。

$$D_2\left(C_1',C_2'\right)=C_2'-C_1'd_2=mG+r\left(d-d_1-d_2\right)G=m\,G \tag{28}$$

由于基于椭圆曲线的ElGamal同态加密算法支持明文为负数，所以识别过程中不需要进行任何修正操作。最终的识别过程依旧是令索引取值i为从0起的连续整数，直到$\max(\mathrm{CC})-\tau$，并利用同态减法依次计算$[\![\mathrm{CC}-\tau-i]\!]$，形成排列值$\left[\!\left[P_j\right]\!\right]_{j\in[1,\mathrm{len}]}$。经过乘法盲化和随机排列操作后进行解密，观察是否包含0值即可判断识别是否成功。而识别过程中的乘法盲化操作可以替代为

$$[\![m]\!]^{r_d}=\left(r_drG,r_d(mG+rP)\right) \tag{29}$$

如果m为非0值，将会被乘法盲化操作所影响，无法解密出完整的明文。并且由于椭圆曲线的离散对数问题，即使解密出明文mG，也很难恢复出m，但是如果$m=0$，则$mG=(0,0)$，此时的结果非常直观（识别结果正是基于该事实）。

4　实验结果与分析

4.1　PRNU指纹识别与CNN识别的对比分析

图7展示了PRNU指纹识别和CNN识别准确率的对比。实验基于Dresden数据集中来自索尼DSC-H50和DSC-W170这2个设备的数据。根据Bondi等[11]的实验结果，CNN识别方法难以分辨来自同一厂商不同型号的图像设备，因此其在索尼DSC-H50和DSC-W170上的识别准确率分别仅为63.5%和56%。相较之下，PRNU指纹识别方法依托于设备传感器的硬件特征，即使设备来自同一厂商，也能够保持较高的识别准确率。在该实验中，PRNU指纹识别方法对索尼DSC-H50和DSC-W170的识别准确率分别为80%和100%（像素矩阵为512×512）。

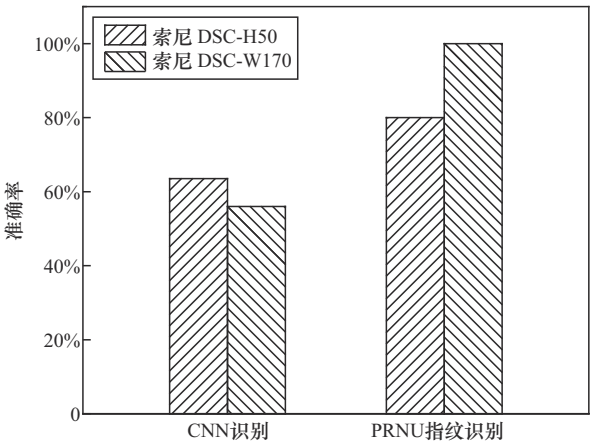


图7　CNN识别与PRNU指纹识别准确率对比

4.2　不同样本情况下的识别性能评估

图8展示了不同样本数量（Case1:200张；Case2:300张；Case3:400张）下所提设备识别的ROC曲线，探究样本数量对识别性能的影响。基于PCE的插值ROC曲线的曲线下面积（AUC, area under the curve）在Case1中低于0.9，在Case2和Case3中分别为0.96和0.98。3条曲线的AUC值均较高，表明在该实验中以PCE为评估指标在区分不同图像设备方面表现出色，能够有效地提取和利用PRNU指纹进行设备识别。同时，该实验结果也表明图像设备识别的准确性与构建PRNU指纹时用到的样本数量呈正相关。样本数量越多，识别准确率越高，这与工业互联网场景下的海量样本的特点非常契合，展现了该方法在该领域的广阔应用前景。

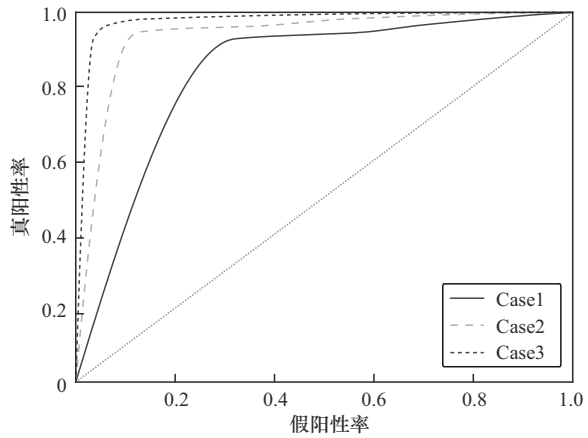


图8　不同样本数量下设备识别的ROC曲线

4.3　盲水印技术抵抗恶意攻击的实验结果

图9展示了嵌入盲水印的图片在经历多种恶意攻击（如随机裁剪、椒盐噪声、旋转攻击等）后，水印仍然可以被有效提取出来，体现了盲水印技术卓越的鲁棒性。

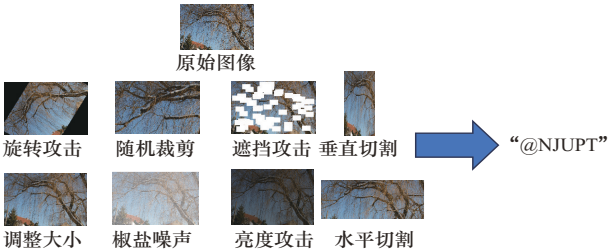
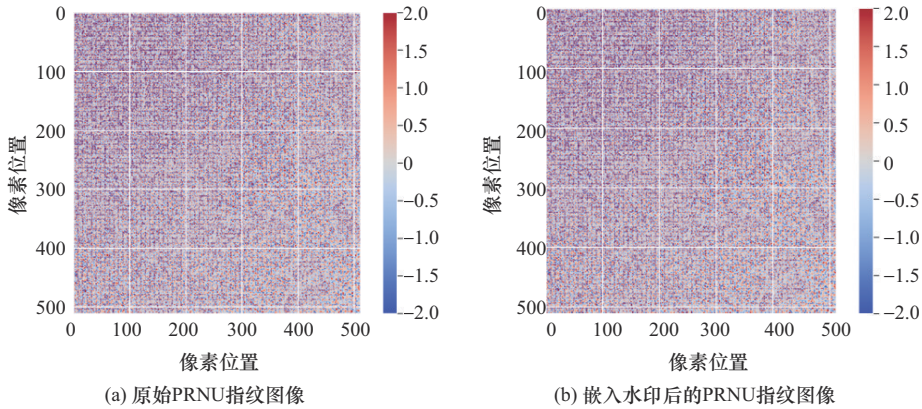


图9　盲水印鲁棒性

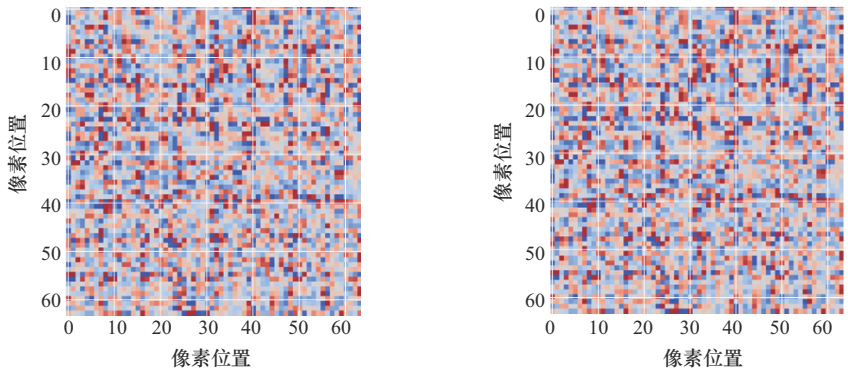
4.4　PRNU指纹与盲水印技术结合的实验结果分析

图10展示了数字图像在水印嵌入前后提取的PRNU指纹特征的对比分析结果。通过整体视觉评估和量化指标验证，可见水印嵌入对传感器固有噪声模式的影响可忽略不计。具体而言，图10(a)和图10(b)的特征分布表明，原始PRNU指纹与嵌入水印后重新提取的PRNU指纹的二维响应强度分布保持高度一致，图10(c)和图10(d)的局部放大区域进一步证实了微观尺度上的特征保存。量化评估采用4项核心指标：峰值信噪比（PSNR, peak signal-to-noise ratio）（PSNR: 16.8 dB）显示图像质量维持在较高水平；结构相似性（SSIM, structural similarity）指数（SSIM: 0.990 4）证实了两者在纹理特征上的高度一致性；皮尔逊相关系数（R=0.991 8）验证了特征间的强线性相关性；最大像素差异（maxΔ=4.066）则表明局部极值差异处于工程可接受范围。这些定量指标共同佐证，所采用的水印算法在保持传感器指纹特征完整性方面具有显著优势，满足数字取证的鲁棒性要求。

图11给出了同样本情况下嵌入盲水印技术前后（Case2:未嵌入盲水印；Case4:嵌入盲水印）的ROC曲线对比，探究嵌入盲水印是否会对识别性能产生影响。结果表明，嵌入盲水印后，基于PCE的插值ROC曲线的AUC为0.97，与未嵌入盲水印的Case2相比，ROC曲线的AUC值几乎一致。这表明引入盲水印技术后，图像设备识别的准确性几乎未受到任何负面影响。



(a) 原始PRNU指纹图像　　(b) 嵌入水印后的PRNU指纹图像



(c) 原始PRNU指纹的局部放大图　　(d) 嵌入水印后的PRNU指纹的局部放大图

图10　水印嵌入前后的PRNU指纹特征可视化对比及量化评估

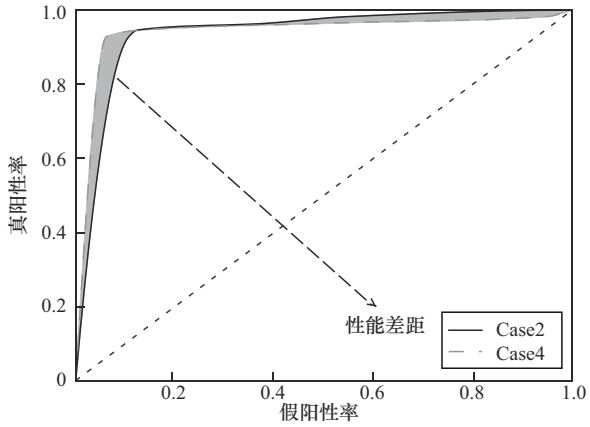


图 11　嵌入盲水印技术前后设备识别的 ROC 曲线

4.5　图片完整性鉴别

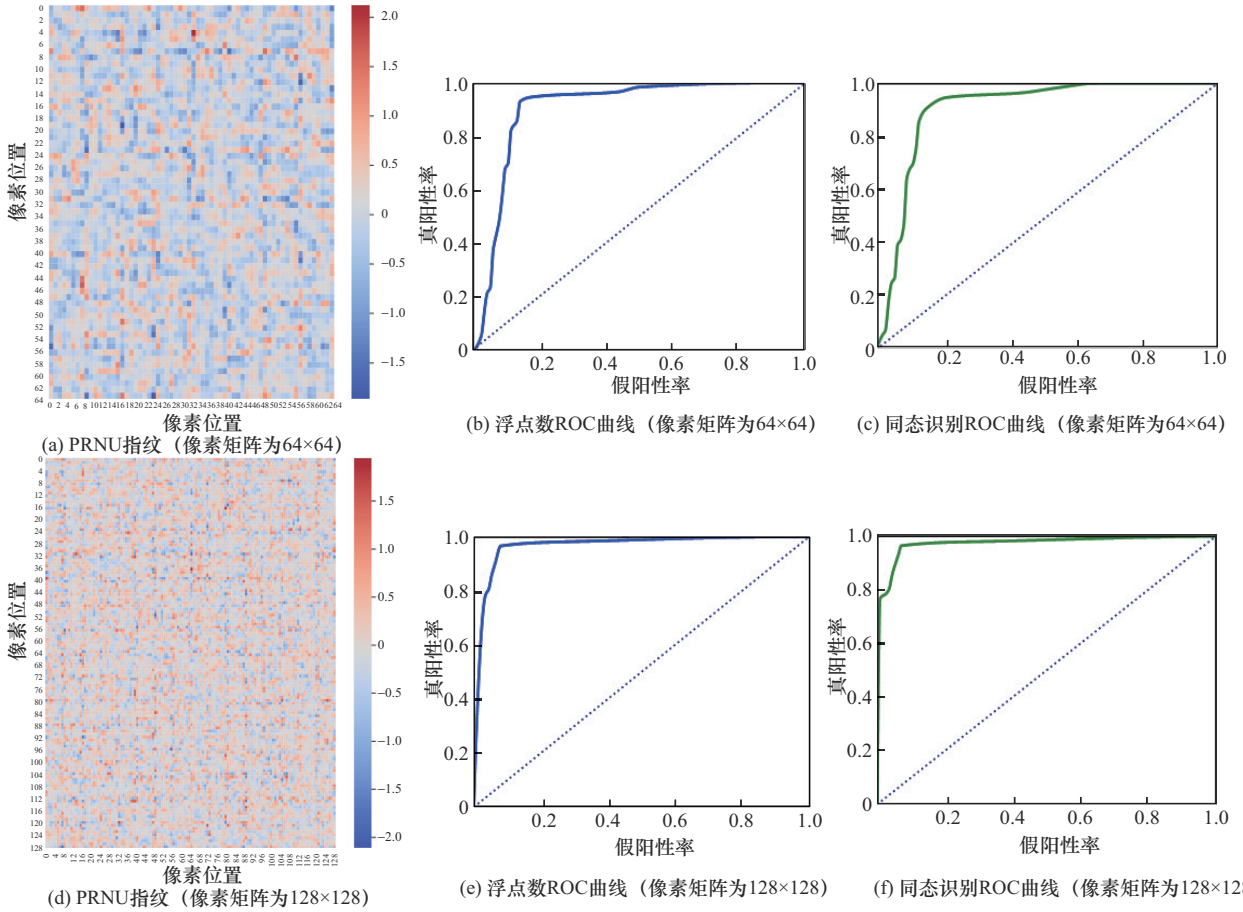
图 12 展示了在图像被篡改的情况下利用 PRNU 指纹与盲水印联合识别的方法，对篡改图像进行完整性鉴别的大致结果。该方法首先通过盲水印的鲁棒性溯源到对应的像素矩阵，提取对应的噪声残差信息，并计算二者的交叉相关性。图像的篡改会导致部分噪声残差信息缺失或改变，交叉相关性数值会出现异常变化。通过将交叉相关性与预设阈值进行比对，识别出交叉相关性未达到阈值的区域，从而判断被篡改的具体区域。尽管当前方法仅支持逐块区域检测，但通过对多块区域的逐次观测与阈值判定，可以有效评估图像完整性，量化篡改区域的范围和比例，并为后续的细粒度鉴别提供支持。

(a) 识别成功　　(b) 篡改比例为50.16%

图 12　图片完整性鉴别结果

4.6　同态加密下的安全识别

图13展示了在不同像素矩阵（64×64、128×128）条件下提取的PRNU指纹，并对其进行了可视化处理。从图13中可以明显看出，随着像素矩阵的增大，



(a) PRNU指纹（像素矩阵为64×64）　(b) 浮点数ROC曲线（像素矩阵为64×64）　(c) 同态识别ROC曲线（像素矩阵为64×64）

(d) PRNU指纹（像素矩阵为128×128）　(e) 浮点数ROC曲线（像素矩阵为128×128）　(f) 同态识别ROC曲线（像素矩阵为128×128）

图 13　不同像素矩阵下 PRNU 指纹展示及同态识别与正常识别的 ROC 曲线对比分析

PRNU指纹的可视化结果更加清晰，能够更加直观地表现出图片的特征，指纹的细节也随之更加丰富。此外，图13中还包含了2组Case3中基于PCE的插值ROC曲线，分别展示了在不同像素矩阵下的识别结果。每组包含2条ROC曲线，一条为使用原始浮点数数据的PRNU指纹进行识别的结果，另一条是对浮点数进行乘10取整后并应用基于ElGamal的同态加密方案后的识别结果。在64×64和128×128的像素矩阵情况下，同态加密后的ROC曲线与加密前的曲线几乎重合，识别性能仅有微小差异。

由此可见，当像素矩阵达到一定规模时（数据精度满足一定标准），基于同态加密的识别方法与原始识别方法的识别性能几乎一致。这一实验结果表明，基于同态加密的识别方法能够在保障数据安全的同时，还能保持与正常识别结果几乎一致的高识别准确率。

图14展示了在选取不同像素矩阵大小的情况下，识别准确率和处理时间的变化趋势。从图14可以观察到，随着像素矩阵从64×64增大到512×512，识别准确率和处理时间基本呈正比例增长。当像素矩阵为128×128时，识别准确率已达到0.95，而进一步增加到512×512时，准确率仅略微提升至0.98。然而，处理时间的增长则显著得多，128×128的像素矩阵处理时间约为160 s，而512×512的像素矩阵处理时间接近600 s，差距较大。由此可见，在对识别准确率和处理时间均有要求的情况下，128×128像素矩阵提供了一个较好的折中选择，能够在保证较高识别准确率的同时，显著减少处理时间。

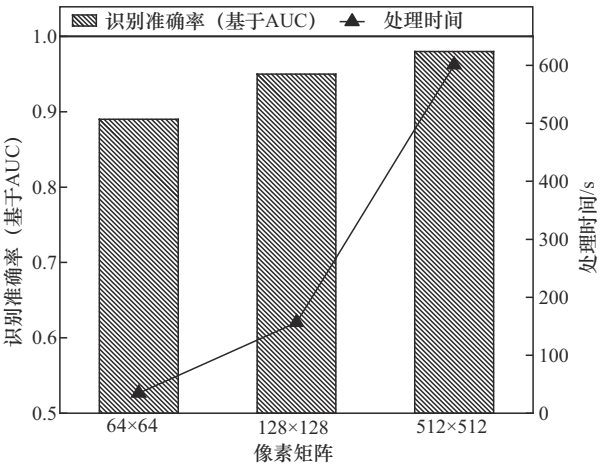


图14　识别准确率和处理时间与像素矩阵大小的关系

图15展示了不同取整方式对识别准确率和处理时间的影响，实验均基于128×128的像素矩阵进行。从图15中可以观察到，直接取整会显著降低数据的精度，导致识别准确率较低。而采用乘10再取整的方式，数据精度会得到明显提升，识别准确率的AUC值达到0.95，且处理时间在160 s左右，表现出较为理想的性能与效率平衡。然而，当进一步采用乘100再取整的方式时，识别准确率并没有显著提升，AUC值依然维持在0.95左右。由此可以得出结论，在数据精度达到一定水平后，识别准确率的提升主要受限于像素矩阵的大小。因此，如果对处理时间和识别准确率有折中需求，128×128的像素矩阵结合乘10取整的方式已足够满足要求，但如果对精度有更高要求，则需要选用更大的像素矩阵，同时付出更长的处理时间。

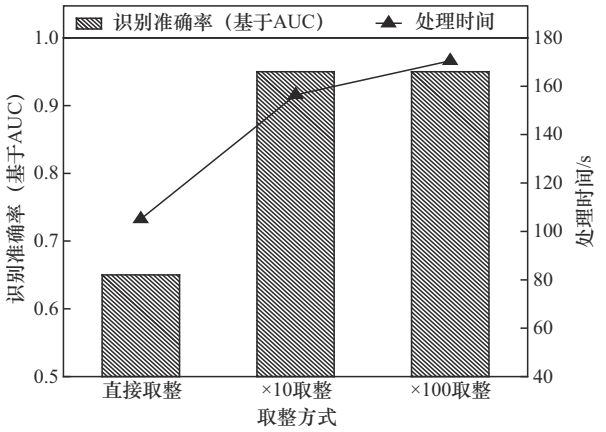


图15　识别准确率和处理时间与取整方式的关系

本文选用了基于P192、P224和P256这3种椭圆曲线的ElGamal同态加密算法。P256（secp256r1）是当前NIST推荐并广泛应用于TLS、数字证书等领域的曲线，提供约128位的安全强度，完全符合工业互联网安全Level 1的要求（通常要求128位及以上的对称密钥强度）。P224（secp224r1）提供约112位的安全强度，对于某些风险较低的Level 1场景可能足够，但考虑到长期安全性和标准趋势（如NIST SP 800-186），建议在Level 1场景中优先选择P256。P192（secp192r1）提供约96位的安全强度，已不被NIST推荐用于新的应用，其安全性不足以满足Level 1的严格要求。表1和图16展示了基于P192、P224和P256椭圆曲线的ElGamal同态加密方案，以及与传统ElGamal加密方案（安全长度约80位）在安全性和运行时间上的对比，其中，攻击者模型为半诚实攻击者，识别方法为基于同态加密与PRNU指纹的安全识别。实验结果表明，基于

表 1　基于 ElGamal 与基于椭圆曲线的 ElGamal 同态加密方案安全性与运行时间对比分析

加密方法	像素矩阵	安全级别/位	运行时间/s
ElGamal	64×64 128×128	80	34.54 156.45
基于 P192 椭圆曲线的 ElGamal	64×64 128×128	96	43.39 173.10
基于 P224 椭圆曲线的 ElGamal	64×64 128×128	112	47.11 195.58
基于 P256 椭圆曲线的 ElGamal	64×64 128×128	128	53.22 208.86

椭圆曲线的 ElGamal 同态加密方案在提升安全性的同时，运行时间变化不大，相较于传统方案，具有更优的综合表现。此外，尽管 P256 提供了最高的安全性，但其计算开销大于 P192 和 P224。现代硬件（包括专用加速器）已能高效处理该开销，因此 P256 在安全性与效率之间提供了理想的平衡。

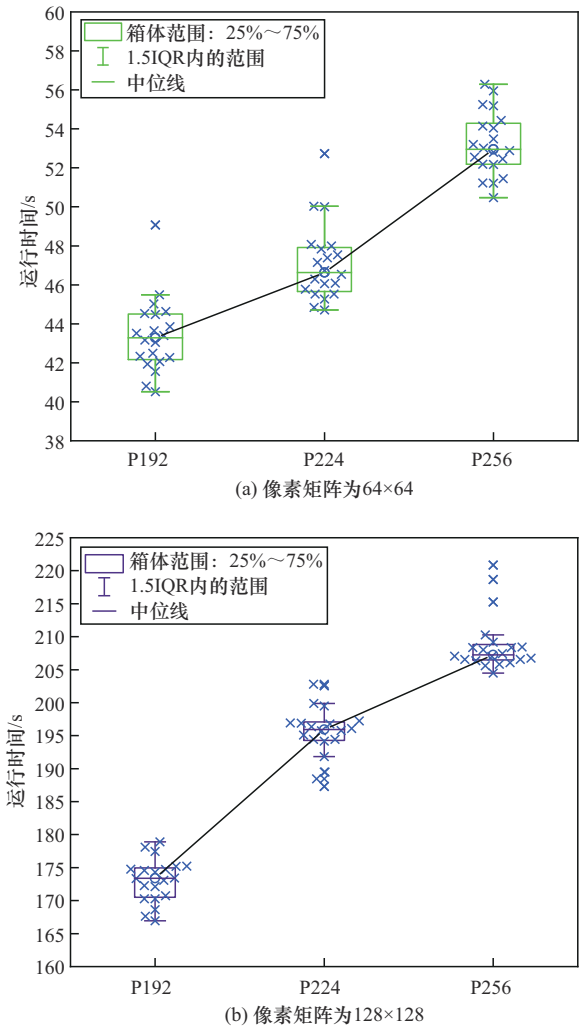


图 16　基于不同椭圆曲线（P192、P224 和 P256）的 ElGamal 加密算法同态识别时间对比

5　结束语

本文面向工业互联网中图像设备易被伪造与身份信息易泄露的安全风险，提出了一种融合同态加密与 PRNU 指纹的图像设备识别与隐私保护方法。该方法利用 PRNU 指纹作为设备的物理身份标识，并结合基于 DCT 与 SVD 的盲水印技术构建身份映射关系，实现了图像被篡改条件下的设备可溯源识别与完整性验证。同时，引入基于 ElGamal 加密算法的同态加密机制，在加密域内完成身份匹配操作，有效防止了 PRNU 指纹与图像敏感信息在交互过程中的泄露。本文方法在设备识别准确性、抗篡改鲁棒性和隐私保护能力方面均优于现有方案，能够在不可信通信环境中实现安全可靠的图像设备识别。

尽管本文方法在安全性与鲁棒性方面取得了显著成效，未来研究仍可在以下几个方向进行深化与拓展。

1) 面向资源受限边缘终端的轻量化与实时性优化。当前方案在处理大尺寸像素矩阵时计算开销较大（如图 14 所示）。为适配工业物联网中广泛存在的低算力摄像终端及满足实时监控等场景的时效性要求，本文方案可探索基于边缘计算的协同处理架构。该架构可将计算密集型任务（如同态加密匹配、高维指纹精确比对）卸载至边缘服务器或云端，终端仅负责轻量级的图像采集、特征（如降采样后的噪声残差/水印）提取与加密传输。同时，研究选择性特征提取策略（如聚焦图像关键区域或高频分量）和更高效的加密域计算算法，降低终端负载和整体处理时延，从而满足准实时应用需求。

2) 加密模板存储与匹配效率优化。算法 1 生成的加密模板维度较高，可能成为大规模部署的瓶颈。未来可研究模板的降维技术、稀疏表示方

法或基于本地部分计算的加密匹配协议，以减少模板存储开销和通信传输量，从而提升系统的可扩展性。

3) 动态PRNU指纹更新机制。考虑到PRNU指纹可能随设备老化、维修等因素发生缓慢偏移，未来可设计自适应的指纹模板更新机制。该机制可利用后续成功识别的图像及其提取的噪声残差对指纹模板进行更新，从而确保长期部署下模型识别的准确性和稳定性。

参考文献：

[1] 刘奇旭, 肖聚鑫, 谭耀康, 等. 工业互联网流量分析技术综述[J]. 通信学报, 2024, 45(8): 221-237.
LIU Q X, XIAO J X, TAN Y K, et al. Survey of industrial Internet traffic analysis technology[J]. Journal on Communications, 2024, 45(8): 221-237.

[2] 马佳利, 郭渊博, 方晨, 等. 基于数字孪生的工业互联网安全检测与响应研究[J]. 通信学报, 2024, 45(6): 87-100.
MA J L, GUO Y B, FANG C, et al. Research on industrial Internet security detection and response based on digital twin[J]. Journal on Communications, 2024, 45(6): 87-100.

[3] 田辉, 贺硕, 林尚静, 等. 工业互联网感知通信控制协同融合技术研究综述[J]. 通信学报, 2021, 42(10): 211-221.
TIAN H, HE S, LIN S J, et al. Survey on cooperative fusion technologies with perception, communication and control coupled in industrial Internet[J]. Journal on Communications, 2021, 42(10): 211-221.

[4] 曾凡一, 苘大鹏, 许晨, 等. 新增未知攻击场景下的工业互联网恶意流量识别方法[J]. 通信学报, 2024, 45(6): 75-86.
ZENG F Y, QING D P, XU C, et al. Identification method for malicious traffic in industrial Internet under new unknown attack scenarios[J]. Journal on Communications, 2024, 45(6): 75-86.

[5] BAYRAM S, SENCAR H, MEMON N, et al. Source camera identification based on CFA interpolation[C]//Proceedings of the IEEE International Conference on Image Processing 2005. Piscataway: IEEE Press, 2005: III-I69.

[6] MILANI S, BESTAGINI P, TAGLIASACCHI M, et al. Demosaicing strategy identification via eigenalgorithms[C]//Proceedings of the 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Piscataway: IEEE Press, 2014: 2659-2663.

[7] CAO H, KOT A C. Accurate detection of demosaicing regularity for digital image forensics[J]. IEEE Transactions on Information Forensics and Security, 2009, 4(4): 899-910.

[8] DENG Z H, GIJSENIJ A, ZHANG J Y. Source camera identification using auto-white balance approximation[C]//Proceedings of the 2011 International Conference on Computer Vision. Piscataway: IEEE Press, 2011: 57-64.

[9] SORRELL M J. Digital camera source identification through JPEG quantisation[M]//Multimedia Forensics and Security. Hershey: IGI Global, 2009: 291-313.

[10] MULLAN P, RIESS C, FREILING F. Towards open-set forensic source grouping on JPEG header information[J]. Forensic Science International: Digital Investigation, 2020, 32: 300916.

[11] BONDI L, BAROFFIO L, GÜERA D, et al. First steps toward camera model identification with convolutional neural networks[J]. IEEE Signal Processing Letters, 2017, 24(3): 259-263.

[12] WANG B, ZHAO M N, WANG W, et al. Adversarial analysis for source camera identification[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 31(11): 4174-4186.

[13] LUKAS J, FRIDRICH J, GOLJAN M. Digital camera identification from sensor pattern noise[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 205-214.

[14] LI C T, LI Y. Color-decoupled photo response non-uniformity for digital image forensics[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2012, 22(2): 260-271.

[15] HOU J U, LEE H K. Detection of hue modification using photo response nonuniformity[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2017, 27(8): 1826-1832.

[16] IULIANI M, FONTANI M, SHULLANI D, et al. Hybrid reference-based video source identification[J]. Sensors, 2019, 19(3): 649.

[17] PANDE A, CHEN S X, MOHAPATRA P, et al. Hardware architecture for video authentication using sensor pattern noise[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2014, 24(1): 157-167.

[18] LI C T. Source camera identification using enhanced sensor pattern noise[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 280-287.

[19] LIN X F, LI C T. Preprocessing reference sensor pattern noise via spectrum equalization[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(1): 126-140.

[20] KARAKÜÇÜK A, DIRIK A E. Adaptive photo-response non-uniformity noise removal against image source attribution[J]. Digital Investigation, 2015, 12: 66-76.

[21] LI C T, CHANG C Y, LI Y. On the repudiability of device identification and image integrity verification using sensor pattern noise[C]//International Conference on Information Security and Digital Forensics. Berlin: Springer, 2010: 19-25.

[22] JAHNKE T, SEITZ J. An introduction in digital watermarking: applications, principles, and problems[M]//E-Commerce and M-Commerce Technologies. Hershey:IGI Global, 2004: 117-141.

[23] WANG H Q, WANG K, LEI J, et al. Digital watermarking algorithm based on SVD in DCT domain[C]//Proceedings of the 2011 International Conference on Electric Information and Control Engineering. Piscataway: IEEE Press, 2011: 5851-5854.

[24] KANSAL M, SINGH G, KRANTHI B V. DWT, DCT and SVD based digital image watermarking[C]//Proceedings of the 2012 International Conference on Computing Sciences. Piscataway: IEEE Press, 2012: 77-81.

[25] MOOSAZADEH M, EKBATANIFARD G. An improved robust image watermarking method using DCT and YCoCg-R color space[J]. Optik, 2017, 140: 975-988.

[26] ERNAWAN F, KABIR M N, FADLI M, et al. Block-based Tchebichef image watermarking scheme using psychovisual threshold[C]//Proceedings of the 2016 2nd International Conference on Science and Technology-Computer (ICST). Piscataway: IEEE Press, 2016: 6-10.

[27] PEETERS J, PETER A, VELDHUIS R N J, et al. Fast and accurate like-

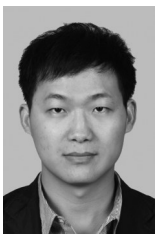
lihood ratio based biometric comparison in the encrypted domain[J]. arXiv Preprint, arXiv: 1705.09936, 2017.

[28] BASSIT A, HAHN F, PEETERS J, et al. Fast and accurate likelihood ratio-based biometric verification secure against malicious adversaries[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 5045-5060.

[作者简介]

张品昌（1985– ），男，安徽阜阳人，博士，南京邮电大学副教授、硕士生导师，主要研究方向为6G无线网络安全、物理层安全认证、无人机通信安全、人工智能安全等。

沈元章（2002– ），男，江苏淮安人，南京邮电大学硕士生，主要研究方向为物理层安全、同态加密。



樊卫北（1987– ），男，河南开封人，博士，南京邮电大学副教授、硕士生导师，主要研究方向为数据中心网络、云计算与大数据、网络可靠性、容错计算、区块链。

董振江（1970– ），男，江苏南京人，博士，南京邮电大学教授、博士生导师，主要研究方向为计算机视觉、知识图谱在车联网、高精度定位等领域的关键技术与应用。

沈玉龙（1978– ），男，江苏宿迁人，博士，西安电子科技大学教授、博士生导师，主要研究方向为云计算与数据安全、智能网络内生安全。

姜晓鸿（1966– ），男，陕西洛川人，博士，日本公立函馆未来大学教授、博士生导师，主要研究方向为无线网络安全、智能网络内生安全、卫星互联网安全等。

肖甫（1980– ），男，湖南邵阳人，博士，南京邮电大学教授、博士生导师，主要研究方向为物联网感知计算、物联网安全技术、数据中心网络。