安徽省百所高校百万大学生科普

创

意

创

新

大

赛

申

报

书

作品名称：（基于网络安全的屏摄溯源取证系统）

参赛大分类：（科普展演）

参赛子分类：（科普讲解）

1. 作品简介

我的作品是作品是一款基于网络安全的屏摄溯源取证系统，旨在解决电子屏幕数据泄密问题。系统通过隐形水印技术，在不影响屏幕显示效果的前提下，将溯源信息嵌入屏幕内容中。当屏幕内容被拍摄或截屏时，水印信息会随图像流转，从而实现对泄密行为的精准溯源。系统具备终端水印嵌入、后台管理、水印提取取证等功能，适用于保密单位、企业等场景，有效填补了传统数据安全管理的盲区。

1. 作品代表展示图、效果图

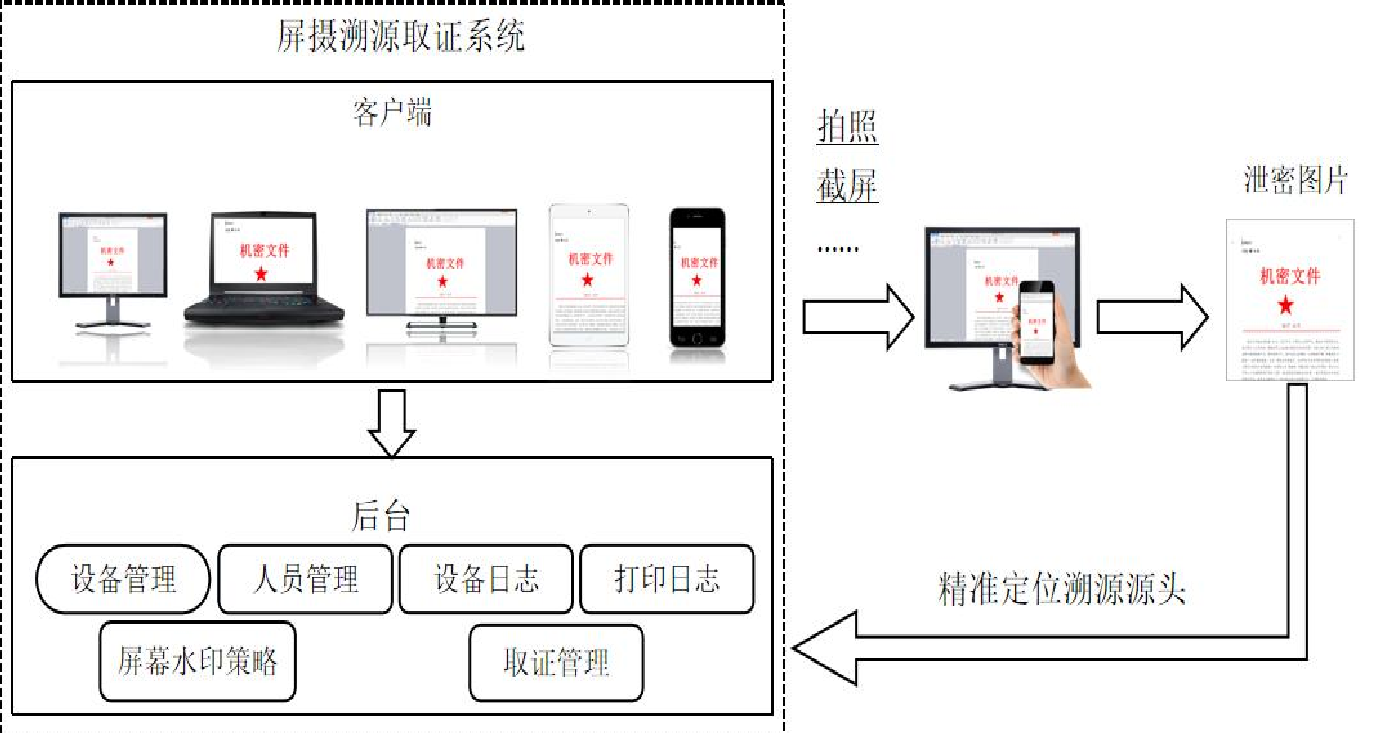


图1 业务逻辑示意图

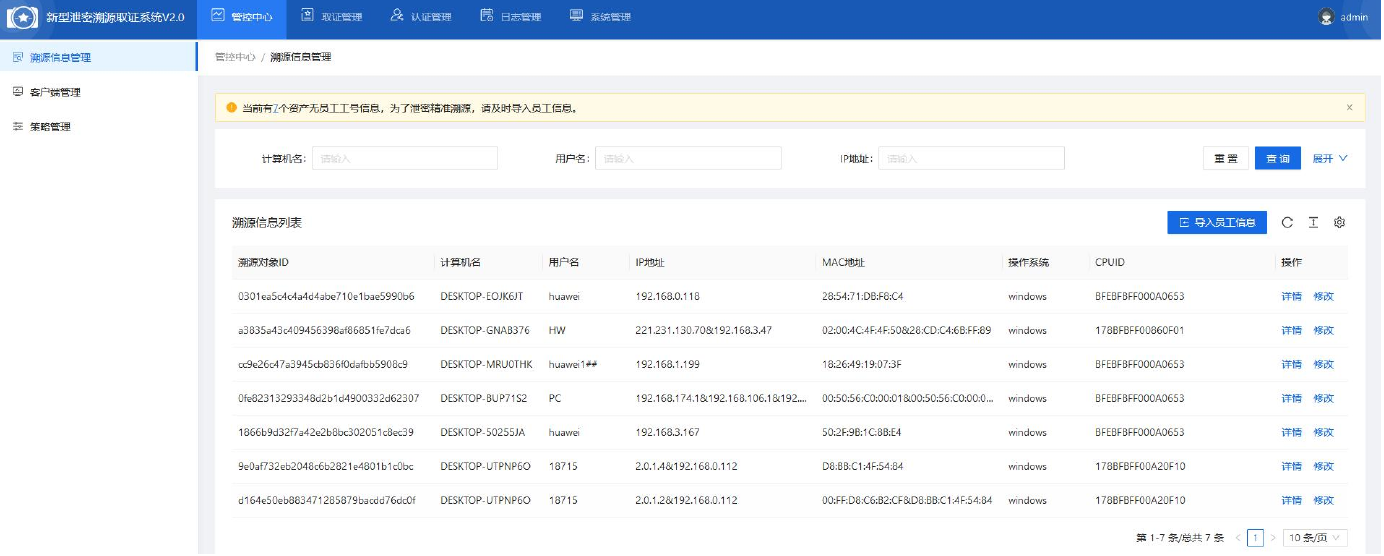


图2 溯源信息管理界面

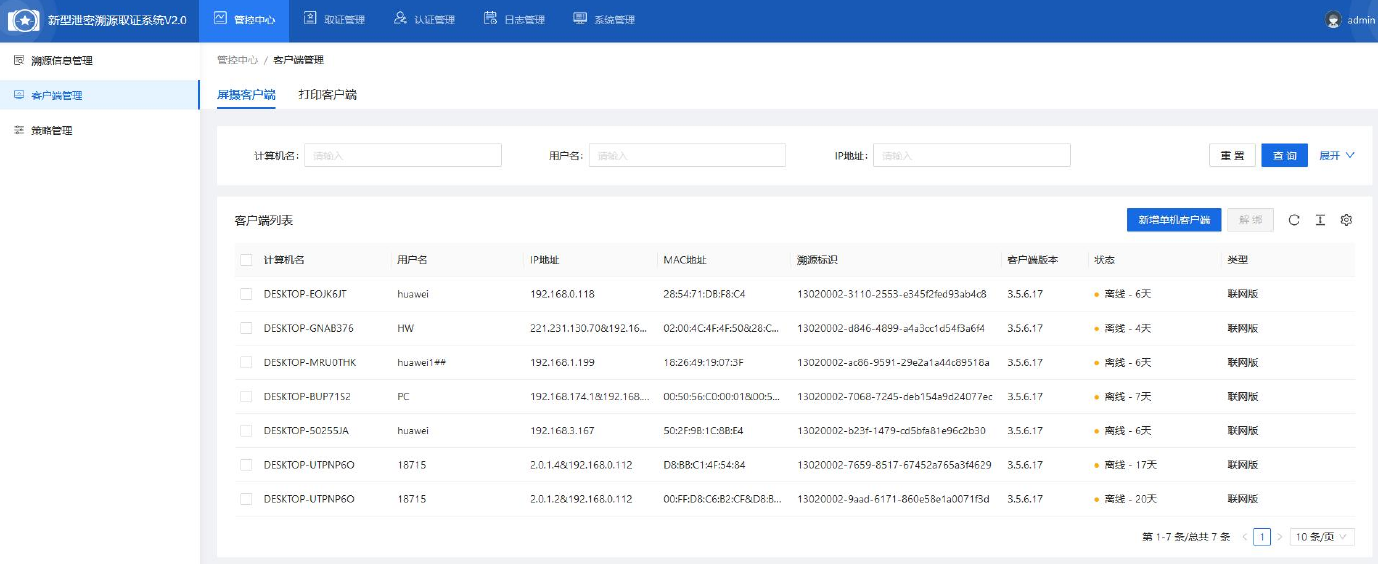


图3 客户端管理界面

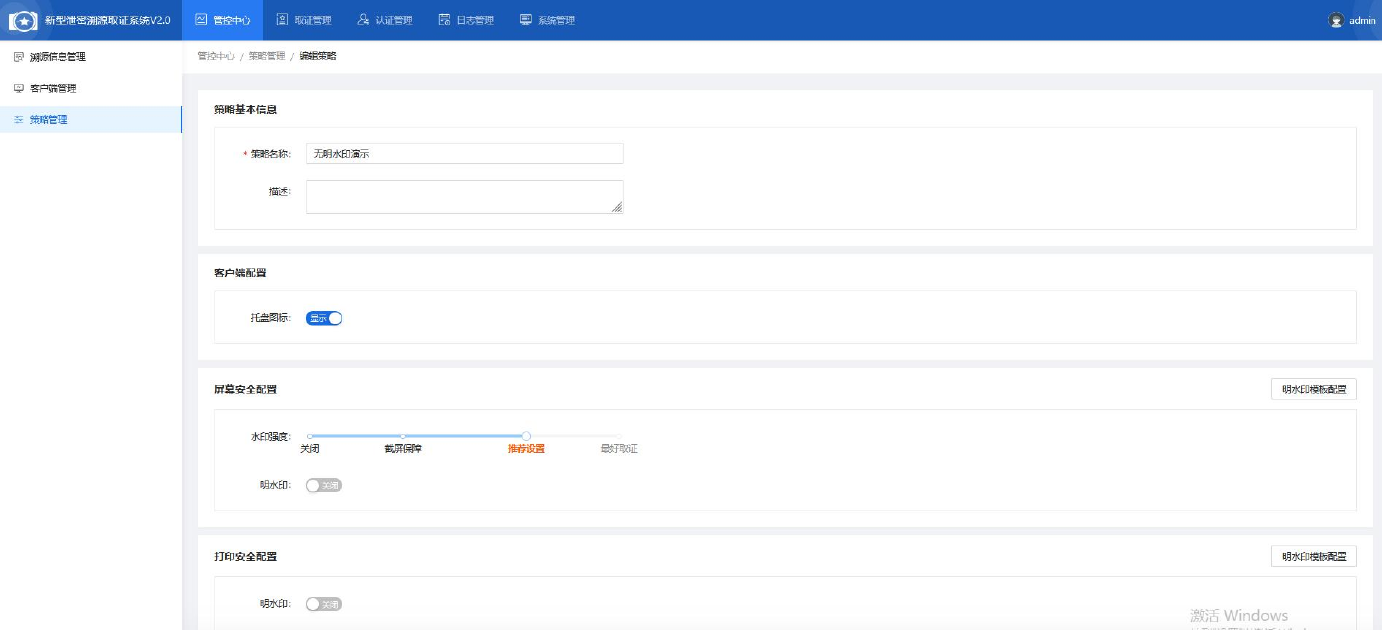


图4 策略管理界面



图5 微信小程序输出取证报告

1. 科学原理及方法
2. **系统总体架构设计**

屏摄溯源系统的整体架构基于SpringBoot构建。通过Nginx实现外部API 调用负载均衡，其中网关服务实现身了份认证、限流实现服务之间调用负载均衡。 服务注册中心采用Eureka Server，所有服务均注册至Eureka注册中心，实现服务的治理。数据库表管理使用liquBase，保证版本以及后续平滑升级，采用 Redis作为缓存系统，提升系统QPS。MinIO作为文件系统，支撑系统分布式部署，算法服务需接入MinIO文件系统，业务系统与算法服务之间关于文件部分通信。业务系统传入文件位于MinIO中的路径，由算法服务自行从文件系统中拉取到本地进行处理，处理完成后上传至MinIO,并将上传后的路径告知业务系统，取证能力由算法部分抽取并对外提供API接口能力。总体架构设计如图6 所示：

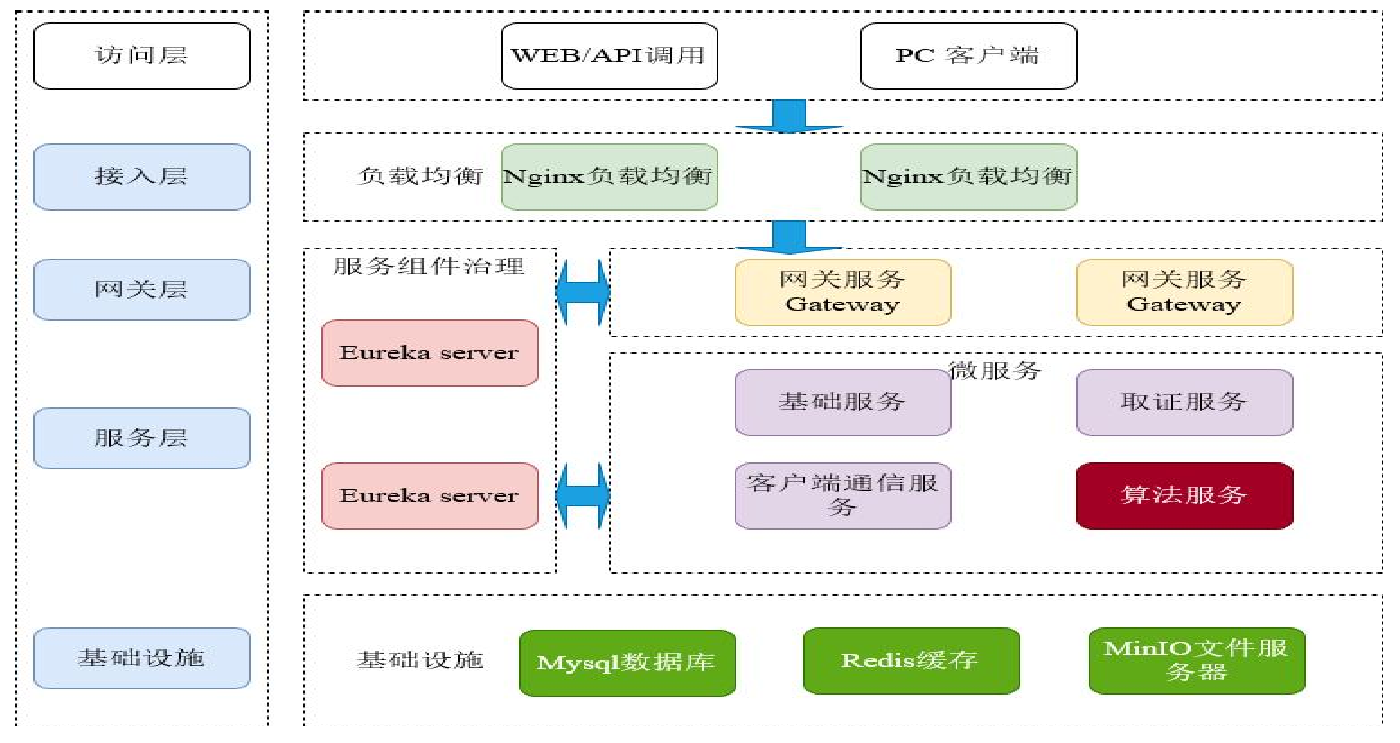


图6 总体架构图

其中，**前台服务包括**：

1. API网关：主要进行防篡改、鉴权校验、限流等操作；
2. Nginx负载均衡：根据流量和服务容量去负载流量的功能；

3、水印业务服务：包含水印嵌入转发、水印日志、溯源对象新增、溯源标识绑

定、客户端通讯、客户端配置管理等等；

**后台服务包括**：

1、基础服务：包括任务转发，水印日志，溯源对象API，客户端通讯以及客户

端管理；

2、取证服务：包括查询取证列表、上传取证文件、预处理操作、提取、查询结

果、查看取证报告、导出取证报告等功能；

3、算法服务：主要进行图片水印嵌入功能实现；

4、客户端通讯服务：主要进行与服务端的实时心跳接口通信。

1. **系统算法模块和实现过程**

**2.1 系统开发环境搭建**

表1 系统开发环境



**2.2 算法优化**

屏摄溯源取证系统的根本目的主要是对于隐形水印的嵌入，其效果必然应不易被察觉，具有较强的信息隐藏性能。基于此，本文提出一种图片水印嵌入方法保证浅色或深色背景下的水印可视效果一致。采用的技术方案包括如下步骤：

1、根据随机模块R和二值化的待嵌入信息进行编码，得到二值化的水印图

案；

2、将所述水印图案按横向与纵向平铺至待嵌入图片的长宽，得到水印矩阵；

3、在RGB颜色空间中根据水印矩阵的内容，对待嵌入图片每个像素点三通道参数值进行修改，修改幅度与像素点的灰度值成反比。

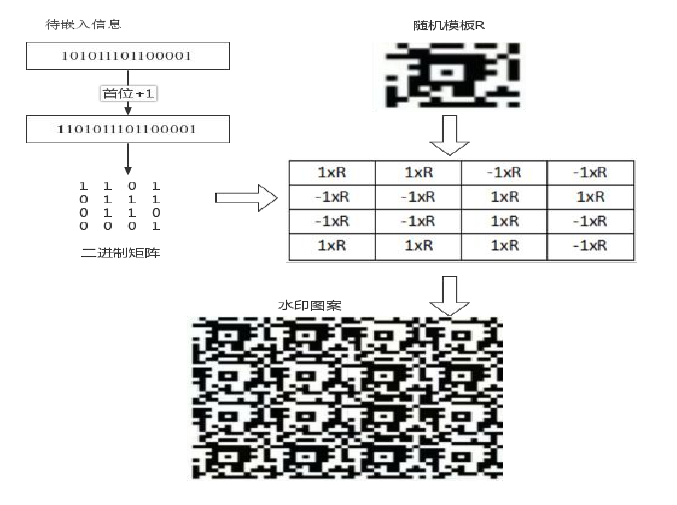


图7 水印编码原理图

以上阐述的水印嵌入方法，包括水印图案生成模块，用于根据随机模块R 和二值化的待嵌入信息进行编码得到二值化的水印图案；水印矩阵生成模块，用于根据水印图案生成与待嵌入图片尺寸相同的水印矩阵；水印叠加模块，用于根据待嵌入图片中像素点的灰度值、水印矩阵、预设的修改幅度对每个像素点三通道参数值进行修改得到嵌入水印的图片，其中的修改幅度与像素点的灰度值成反比，即浅色背景下修改幅度小、深色背景下修改幅度大，这样就实现了修改幅度的自适应修改，提高了水印的隐形效果，不易被察觉。

一般而言，为了识别拍摄的屏幕图像中是否含有水印，需要进行完整的水印提取过程，包括定位水印嵌入区域这一相对耗时的过程。因此，这种识别方式不适合用于大规模可疑屏摄图像的筛选。因此，需要一种更加快速的屏摄水印模式识别方案。所以本文提出的水印识别算法的提取流程如图8所示：

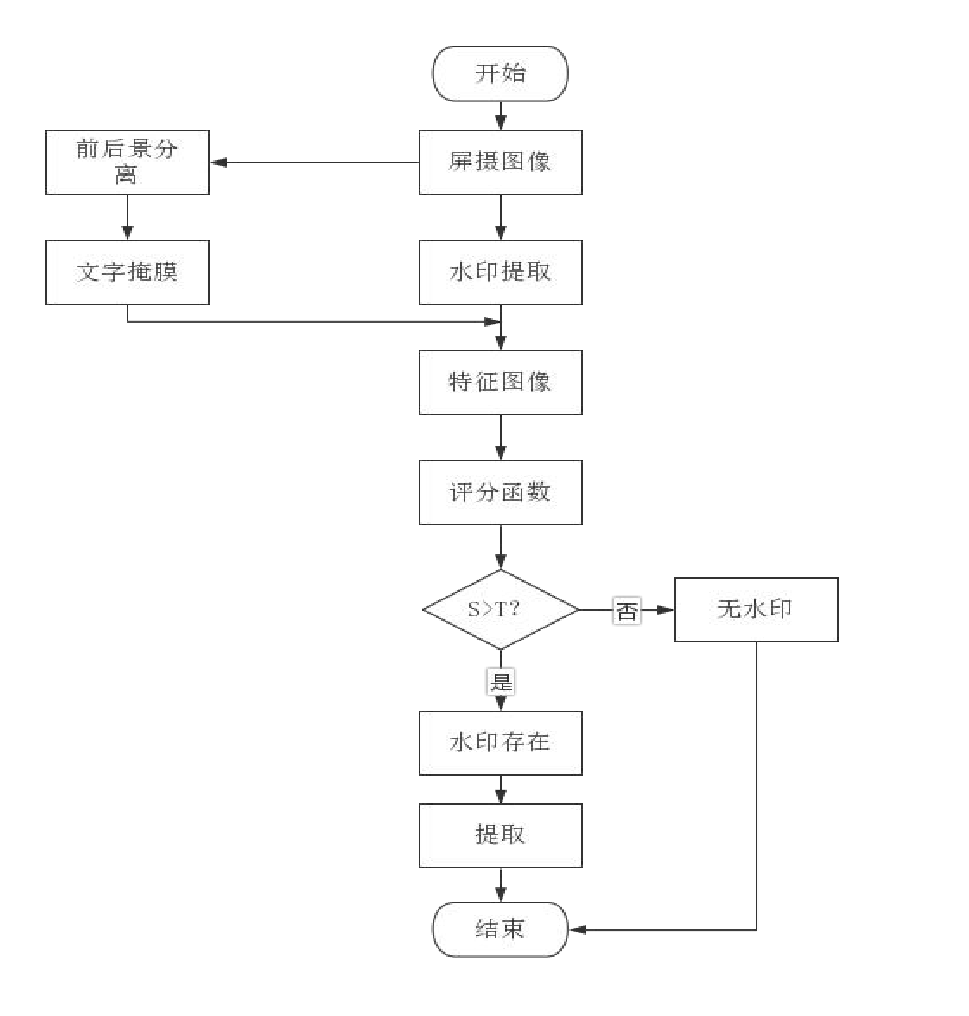
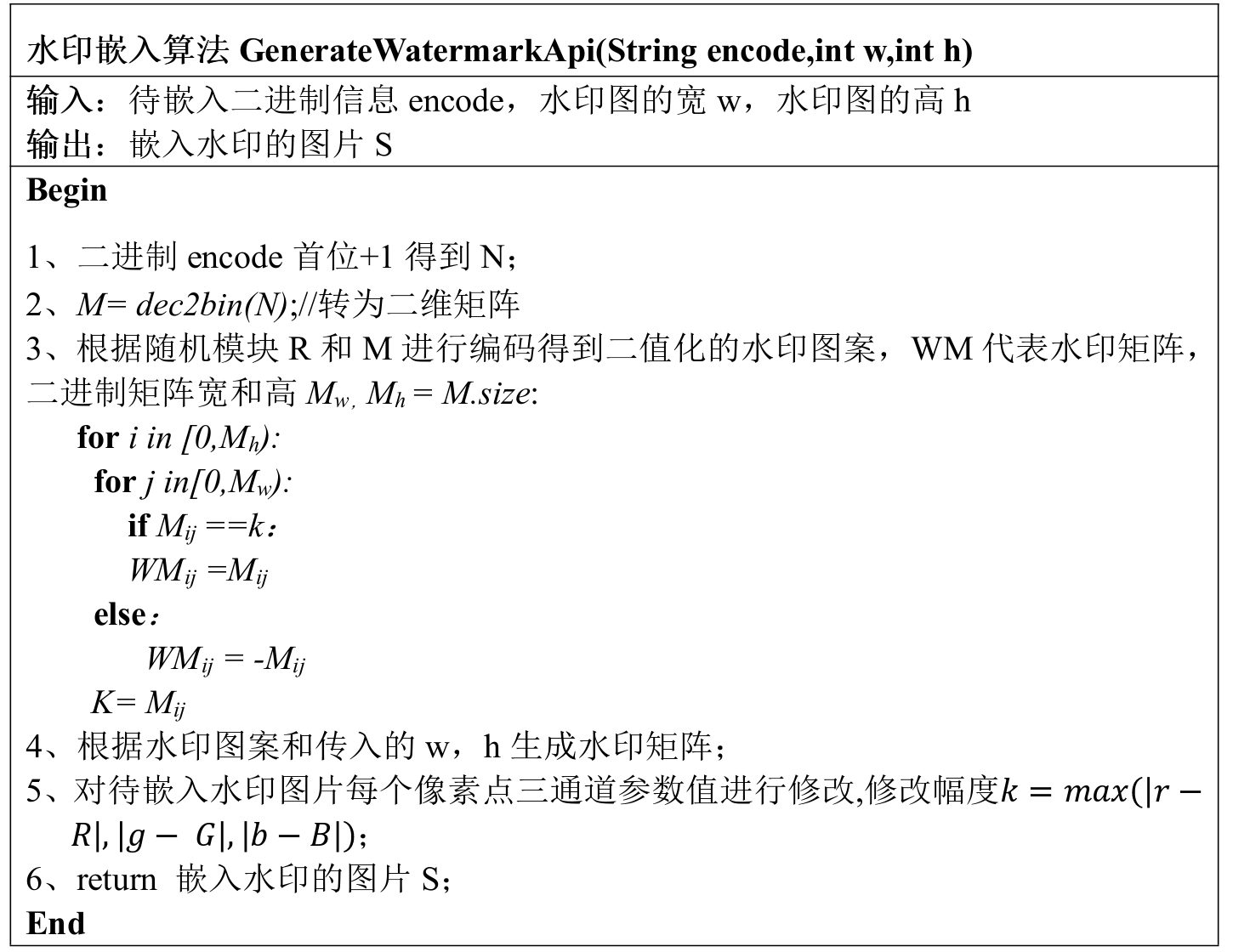
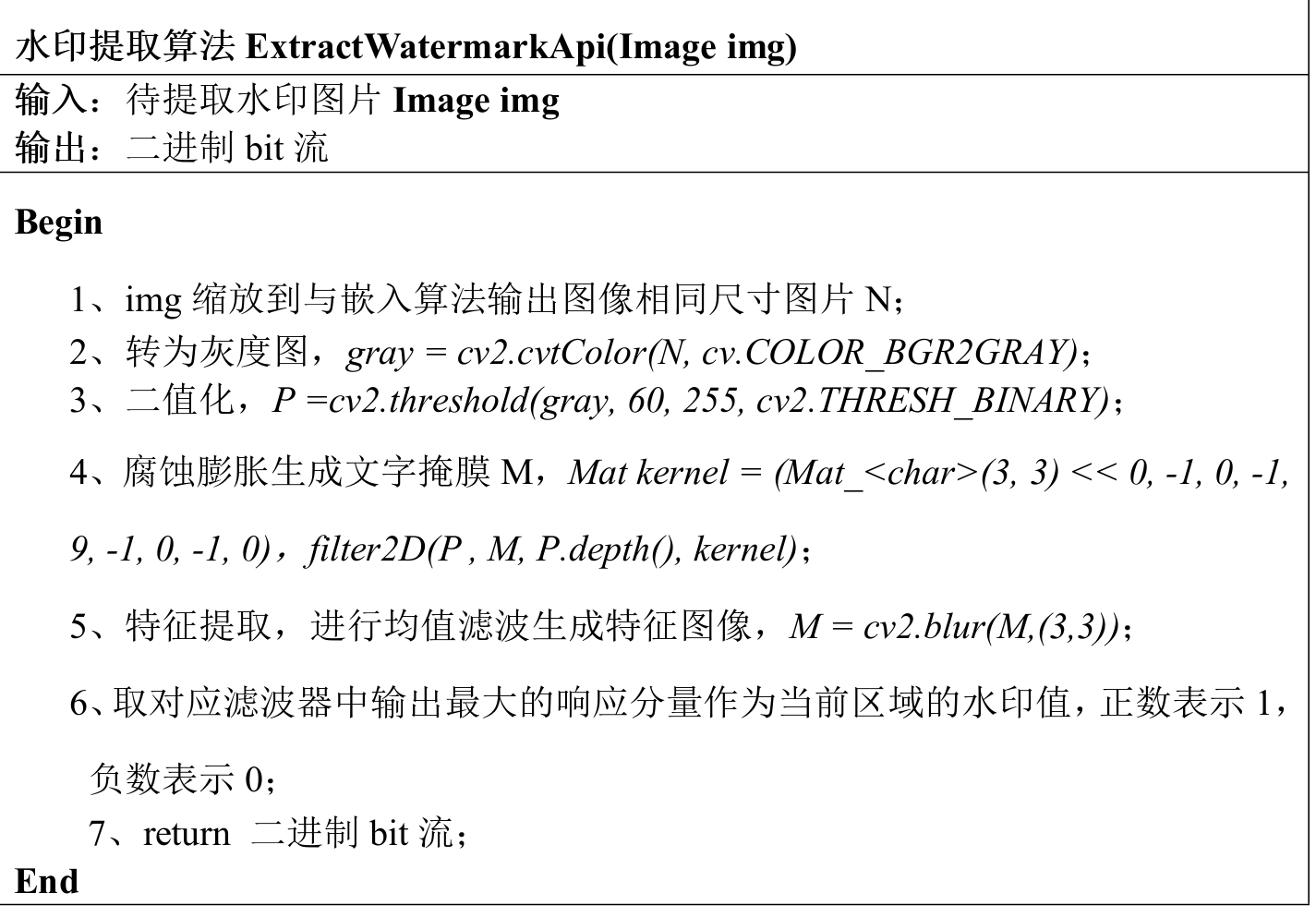


图8 水印提取算法流程图

1. **水印嵌入和提取代码**





1. **系统登录安装模块和实现过程**
   1. **用户登录**

通过NSIS脚本将客户端程序打包成安装执行程序exe，通过脚本对exe安装时的注册表采取隐藏加密，主要加密方式如下：

1 注册表安装地址更改隐藏；

2 托盘图标通过服务端控制实现初始化隐藏，后期也可根据需求通过服务端控制实现显示；

3 在控制面板中对exe程序名实现更改，最大程序实现对用户的客观性隐藏；

4 对exe执行UAC控制权限升级，并添加至开机启动项，确保在用户方批量安装后实现开机自启动。

通过以上步骤，能够基本对用户实现安装时的无痕无感知要求。

用户双击exe即可运行，客户端运行后会弹出程序安装向导，用户输入需要连接的服务端IP地址 ，输入完成后，客户端与服务端随即通过HTTP协议完成实时通信，客户端与服务端会建立实时心跳，完成屏幕水印显示，通过心跳完成服务端对每个客户端的实时设置策略，如水印透明度，水印显示内容等设置。

* 1. **管控中心**

管控中心主要分为溯源信息管理，客户端管理和策略管理三个模块。分别对用户信息录入，PC机器管理以及每台PC呈现的水印显示策略做统一后台管控，能够做到批量和差异化处理，对每台机器用户水印进行有效的实时监控和数据统计，方便管理员能及时在特定的域下实现快速查询和操作。

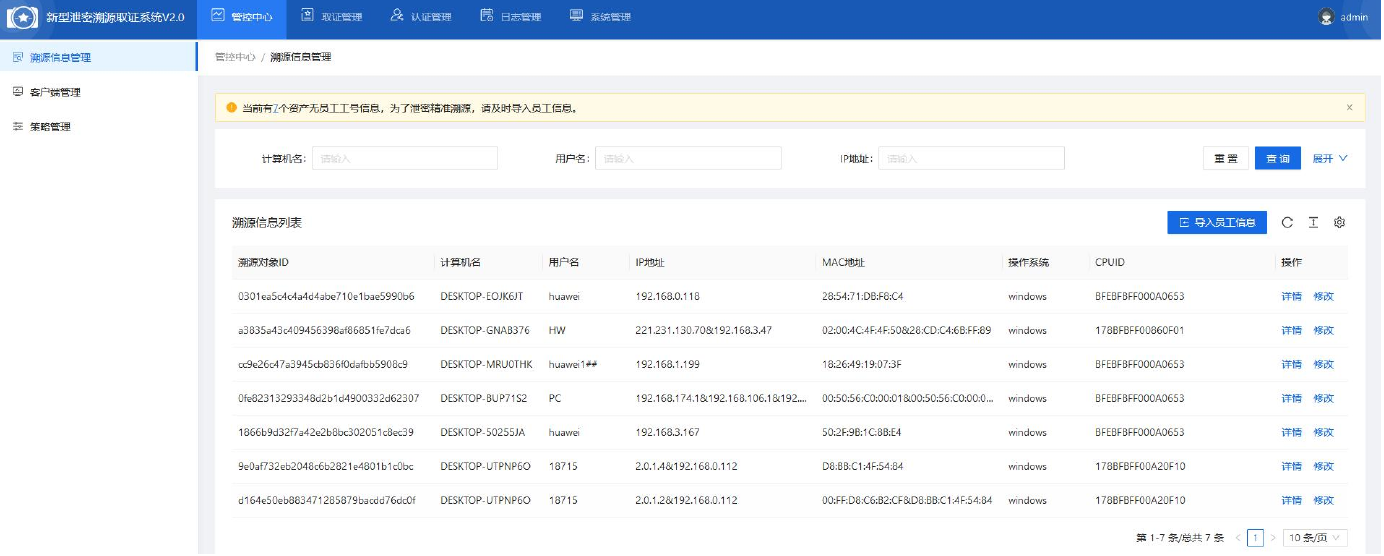


图9 溯源信息管理界面

客户端管理界面对注册的每一个PC用户的详细做了详细的信息记录，如图9所示：

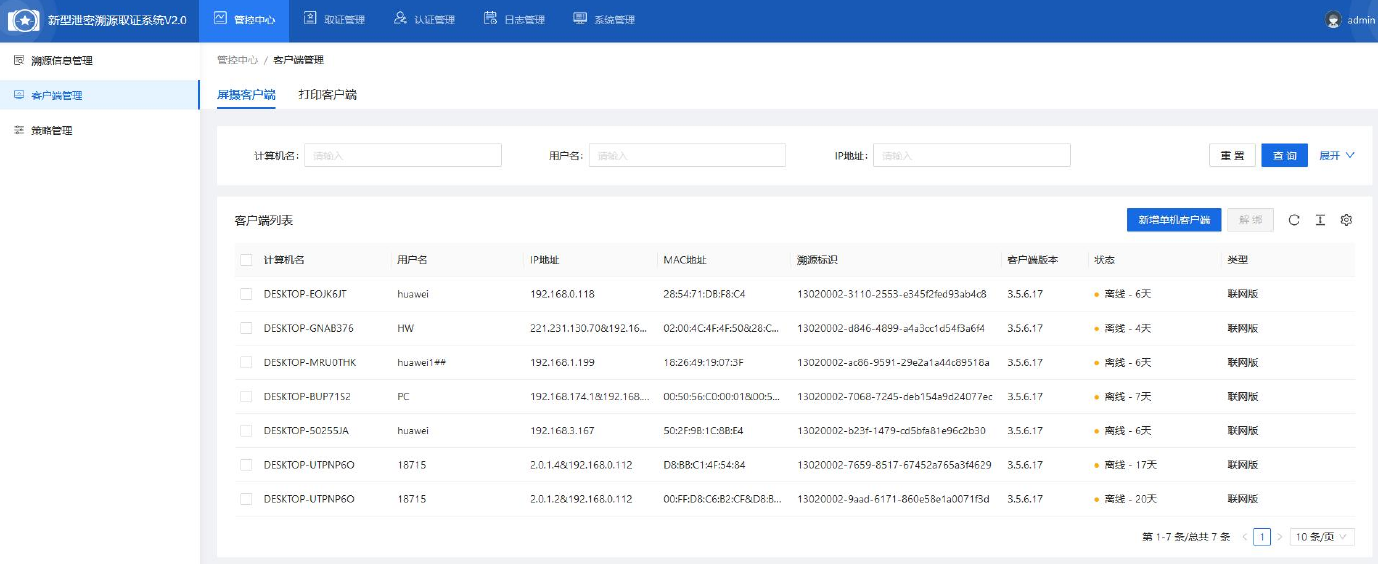


图10 客户端管理界面

策略管理界面中包括客户端托盘图标开关设置，水印强度设置，是否开启明水印

等功能，如图10所示：

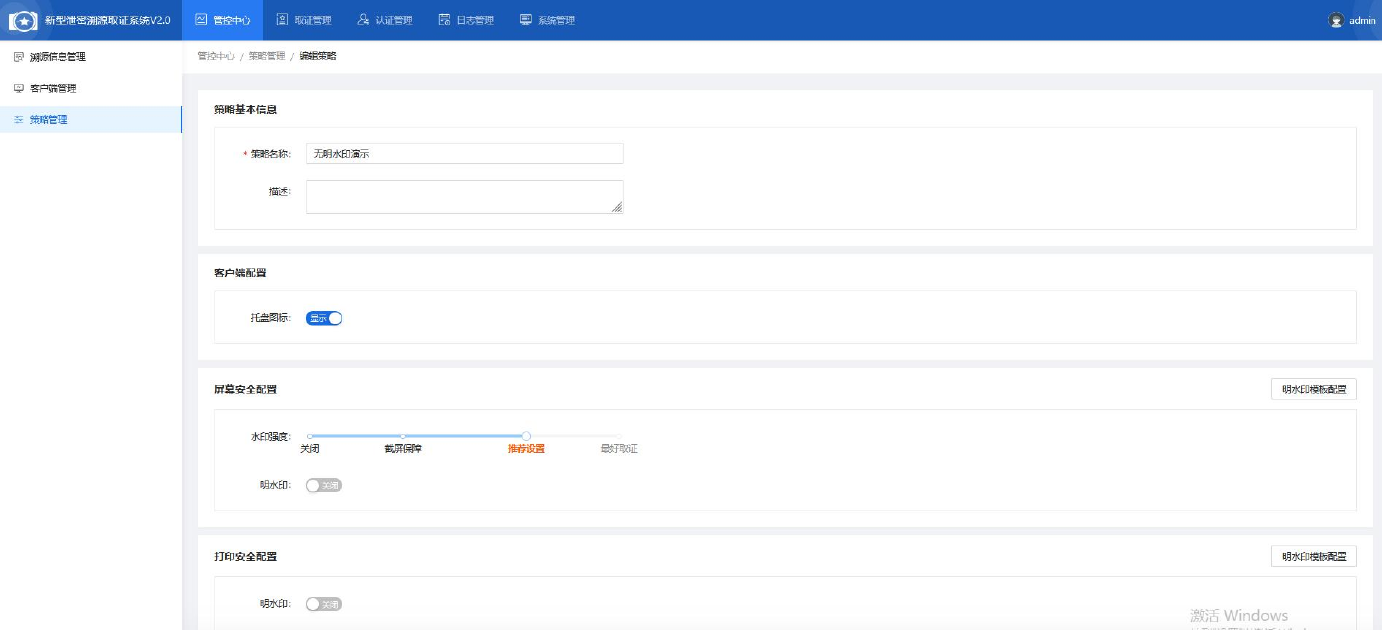


图11 策略管理界面

点击“绑定客户端”按钮会弹出界面如图11所示：

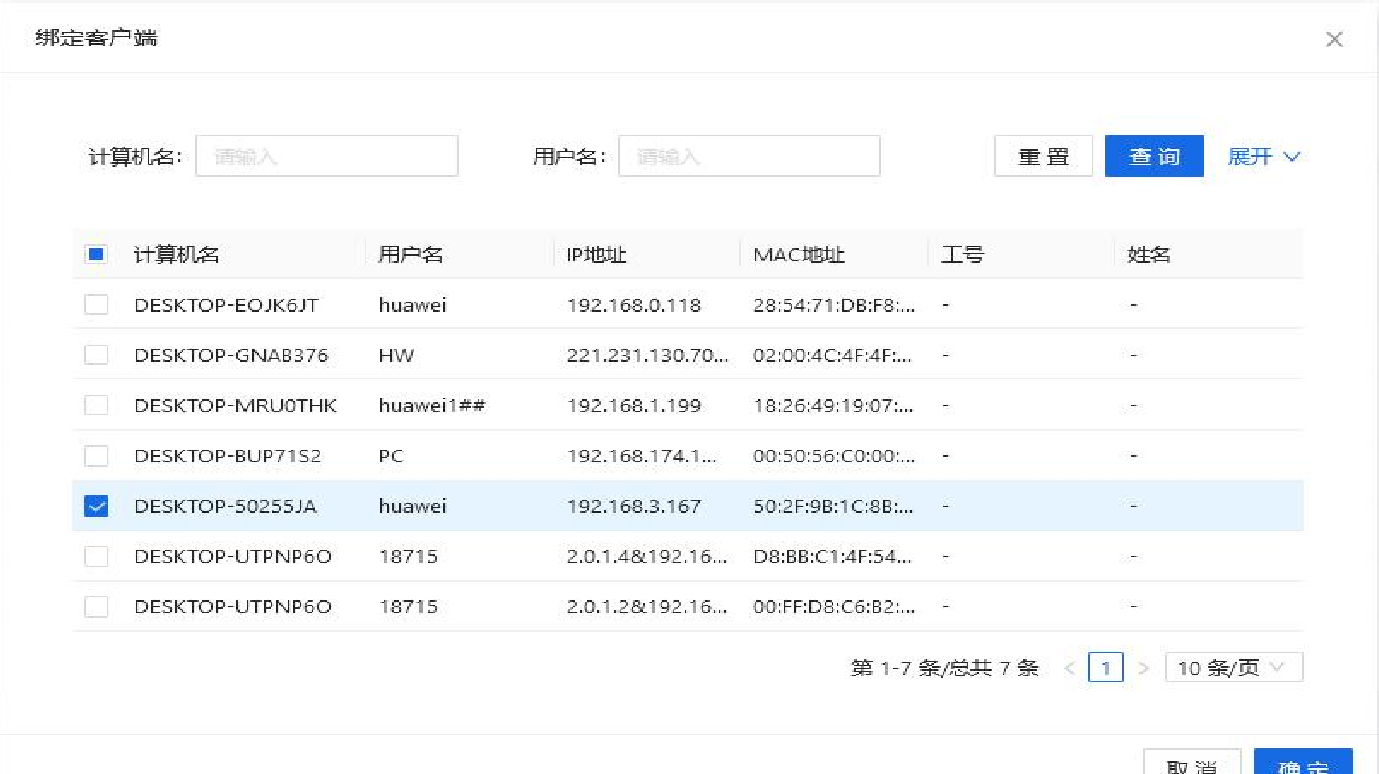


图12 绑定客户端界面

* 1. **系统管理**

系统管理包括安全登录设置、主题设置、邮件设置、级联设置、授权管理、屏幕因子更新、客户端升级等功能，界面实现部分主要是分为以下一个模块：

1、安全登录设置：为了提升后台管理员密码管理自由度，可从后台设置账户锁定，密码有效期限等；

2、主体设置：系统可根据用户需求，个性化定制logo图标主题，通过从后台上传材料，经过服务端与客户端信息交互，实现客户端实时替换主题变更。

3、邮件设置：通过SSL协议，以邮件的形式发送通知给责任人。

4、级联设置：通过级联设置，可以导入单位信息文件，一键关联上下级关系， 高效处理部门信息。

5、授权管理：主要是控制授权机器数量，和授权水印类型，可按需设置。

6、屏幕因子更新：由于很多机器屏幕品牌型号参数均不同，而水印在呈现在屏幕上时，需要结合当前屏幕因子进行一定程度的调整，才能做到适配不同机型。

7、客户端升级：主要也是方便客户端做到静默升级，用户无感知升级，设置每次开机自动检测有无新版本上传，运行后两小时轮询一次，检查当前是否上传新版本。

1. 创意说明

主要工作和创新点如下：

1、提出一种图片隐形水印嵌入方法，能够保证浅色或深色背景下的水印可视效果一致；提出的水印提取方法，根据文字掩膜进行特征提取大大提高提取效果的鲁棒性；提出的29位二进制比特流编码方案，增强隐形水印对于用户信息的加密隐藏的同时也提高了提取结果的准确性。

2、调研用户业务需求、功能需求、安全性需求的前提下，设计并实现一个完整的屏摄溯源取证系统，并在应用安装方面采取用户无感知模式安装，实现对用户真正意义上的检测防御泄密任务，同时对算法进行工程化实现，并完成软件实现过程中的系统测试和适配工作。

1. 创作目的和方法

**5.1 创作目的：**

1、解决屏幕拍摄泄密问题，填补数据安全管理盲区。

2、提供一种隐蔽、高效的溯源取证方案，震慑潜在泄密行为。

**5.2 创作方法：**

1、采用SpringBoot框架构建系统，结合Nginx负载均衡和Redis缓存提升性能。

2、通过算法优化实现自适应水印嵌入和鲁棒性提取。

3、用户无感知安装设计，确保系统隐蔽性和易用性。

1. AI参与程度说明

本作品中水印提取算法的优化部分运用AI技术辅助分析图像特征，提高了水印识别的准确性和抗干扰能力。此外，系统测试环节通过AI工具自动化生成测试报告，优化了性能分析流程。