

基于深度鲁棒水印的屏摄内容保护软件

V1.0

- 使用说明

版本	V1.0
文档状态：	已完成
作者：	李响、徐奕涵、郭玳豆、秦川
负责人：	李响
日期：	2024 年 7 月 2 日

目录

1	简介	3
1.1	编写目的	3
1.2	使用对象	3
1.3	产品范围	3
2	产品概述	5
2.1	软件结构	5
2.2	算法结构	5
2.3	软件模块描述	6
2.4	算法模块描述	7
3	使用说明	11
3.1	注册登录	11
3.2	主界面介绍	12
3.3	单张图像水印嵌入和提取	13
3.4	屏摄图像水印提取	15
3.5	打印拍摄图像水印提取	16
3.6	批量图像水印嵌入和提取	18

1 简介

近年来，基于深度神经网络的数字水印研究方法的快速发展，有效提升了数字多媒体内容的保护能力。但是，随着新媒体技术和便携智能摄影设备的发展，数字多媒体信息不仅仅可以通过电子信道进行传输和分发，同样也可以通过跨媒介信道进行传输和分发，例如，屏幕-拍摄，打印-拍摄和扫描-拍摄。在数字多媒体信息传输方式发生转变的同时，随即也暴露出来一个严重的问题：针对抵抗电子信道失真的数字水印方法并不适用于抵抗跨媒介信道失真的场景，特别是屏摄过程和打印拍摄过程。为了解决该问题，我们使用 PyQt 技术开发了一个基于深度鲁棒水印的屏摄内容保护软件，该软件通过将编码器产生的水印信息膜叠加到原始图像上生成含水印图像。之后，将该含水印图像投放到电子屏幕上，并用摄影设备拍摄此图像，从而得到一张捕获图像（也就是“屏摄图像”），最后，由解码器进行水印的提取。严格来讲，经由屏摄过程得到的捕获图像可能受到了各种失真，例如，光照度失真、色彩失真、摩尔纹失真以及运动模糊等，这样就对我们的解码器提出了更高的要求——解码器需要能将捕获图像中所包含的水印信息准确地提取出来。与常规的基于深度神经网络的数字水印方法不同，此软件中原始图像不需要输入编码器，而是将自定义的水印信息通过编码器生成特定的信息膜（该信息膜仅与水印信息相关），再将信息膜覆盖在原始图像之上来完成水印嵌入。这意味着，该信息膜可以叠加在任意的原始自然图像上。由于无需对原始图像直接进行修改而是将其与信息膜叠加，因此，该软件的运行效率得到了有效的提升。此外，该软件还支持对批量原始图像进行水印嵌入和提取，进一步节省了水印信息嵌入的时间。仿真结果表明，通过该软件生成的含水印图像在经过各种模拟失真和真实屏摄场景、打印拍摄场景下，具有超过 90% 的提取准确率，在保证一定图像质量的同时具有更强的鲁棒性和更高的实际应用价值。

1.1 编写目的

本文档为使用说明文档，为软件的使用与维护提供信息基础。

1.2 使用对象

本文档的使用对象主要为软件测试与使用人员。

1.3 产品范围

本软件致力于为数字媒体内容版权保护提供基于深度鲁棒水印的解决方案，有效应对屏幕拍摄、打印拍摄等跨媒介信道传输带来的版权保护挑战。软件通过编码器生成水印信息膜，并将其叠加到原始图像上，形成含水印图像。即使在经过屏幕拍摄、打印拍摄等传输过程后，水印信息依然能够被准确提取，从而实现对数字媒体内容的有效保护。

软件主要模块：

- （1）编码器模块：将自定义水印信息进行编码生成特定信息膜，用于水印嵌入。

(2) 图像矫正模块：自动对含水印的屏幕拍摄图像或打印拍摄图像进行矫正，消除图像变形。

(3) 解码器模块：从含水印的屏幕拍摄图像或打印拍摄图像中提取水印信息，并显示提取结果。

软件主要接口：

(1) 图像加载接口：支持加载单张或批量原始图像，以及加载含水印的屏幕拍摄图像或打印拍摄图像。

(2) 水印信息输入接口：支持用户输入自定义水印信息。

(3) 水印信息输出接口：将提取的水印信息以文本形式显示。

(4) 结果展示接口：展示原始图像、信息膜、含水印图像、屏摄图像/打印拍摄图像、矫正图像等。

2 产品概述

2.1 软件结构

本软件主要使用 PyQt5 框架进行界面开发，主要开发语言为 Python，深度学习框架采用 TensorFlow 1.15。软件结构如图 2-1 所示。

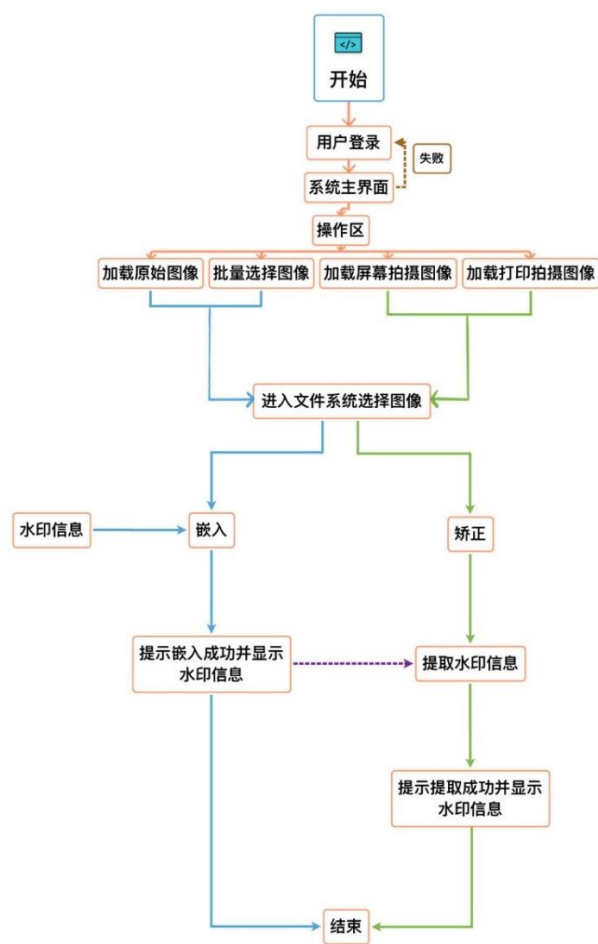


图 2-1 软件结构图

2.2 算法结构

软件中所使用的基于深度鲁棒水印的抗屏摄水印方法，其主要包括：编码器、鉴别器、噪声层及解码器四个部分。待嵌入信息输入编码器中生成信息膜，附加在载体图像上生成含水印图像。利用噪声模拟网络对含水印图像进行攻击，使模型学习抵抗屏幕拍摄噪声的能力。随后，将附加噪声的含水印图像输入解码网络以提取水印信息。同时，使用一个鉴别器网络来监督编码网络的训练，两者进行对抗训练，以最小化水印图像的视觉感知。为了更灵活地权衡水印图像的鲁棒性和透明性，在训练过程中设置了一个嵌入超参数。算法结构如图 2-2 所示。

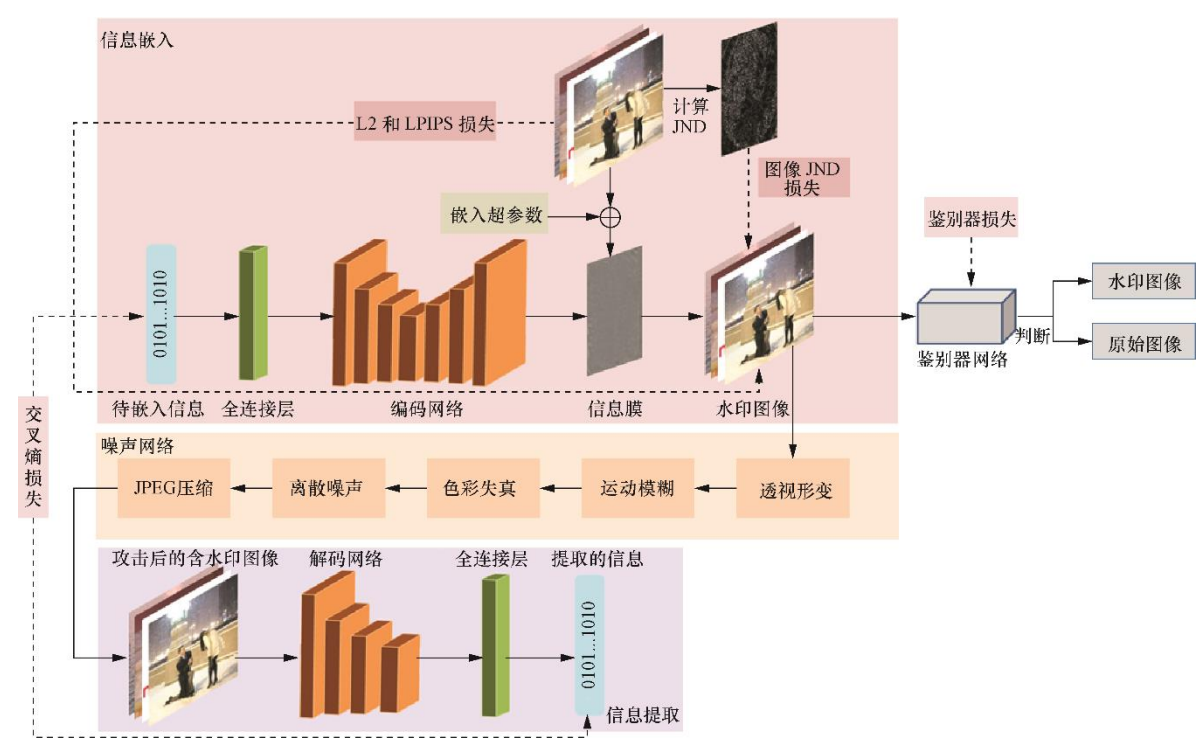


图 2-2 算法结构图

2.3 软件模块描述

● 编码器模块

当用户成功登录并进入软件主界面后，有两个选项可以实现图像的编码，分别是“加载原始图像”和“批量选择图像”。（以下以选择“加载原始图像”为例说明，选择“批量选择图像”同理）进入文件软件后，任意选择一张原始图像，选择完成后该张图像即刻显示在“原图”框中。在文本输入框中键入想要嵌入的水印信息，点击执行编码过程，编码完成后会在相应的图像框中显示已经编码好的图像，并弹出提示框通知编码完成。同时，主界面上会显示单次运行时间。由于采用的算法模型所能容纳的水印容量是经过 BCH 编码后的 32 bit，真实信息容量是16 bit所以，当输入的水印信息满足该条件时才会执行嵌入过程。

● 图像矫正模块

图像矫正模块主要针对的是对含水印的屏摄图像实施透视变换操作，使其大小和维度与原始图像保持一致。在本软件中，不仅能够对屏幕拍摄图像进行水印信息的提取，针对打印拍摄的图像也有很高的适配度。进入文件软件后，任意选择一张屏幕拍摄图像/打印拍摄图像，选择完成后该图像会出现在“屏摄图/打印图”框中，点击“矫正”，软件会自动截取出所需内容，完成后该图像即刻显示在“矫正图”框中。

● 解码器模块

解码器模块的主要功能是从拍摄后的图像中提取信息并输出或者直接对含水印的图像进行解码。先通过图像校正模块得到矫正之后的含水印图像，再执行解码过程，解码完成后会输出提取的信息，并弹出提示框提示解码完成。同时，主界面会显示相应的运行时间和提取准确率。

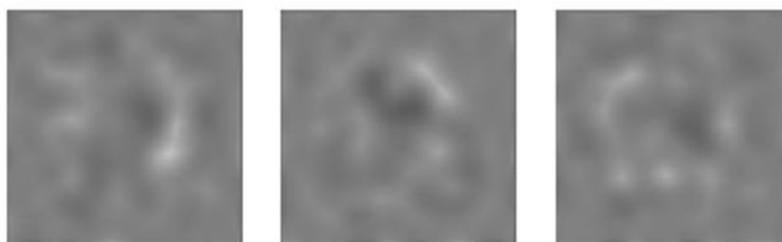
2.4 算法模块描述

● 编码器

编码器主要实现将水印信息生成相应的信息膜。我们使用了U-Net架构，编码网络的输入是一个长度为32比特的随机二进制字符串。首先将水印信息通过一个线性全连接层进行预处理，一维的水印信息被扩充形成一个 $50 \times 50 \times 3$ 的张量，然后上采样形成 $400 \times 400 \times 3$ 的张量。通过一系列的深度卷积计算和特征学习，输出一张仅含有水印信息的信息膜。图2-3显示了一组信息膜的示例。实际使用时，只需要用训练得到的信息膜直接叠加到任意载体图像就可以实现水印的嵌入。模型训练时采用信息膜与水印图像相加的嵌入方式来生成水印图像，同时在信息膜前乘上一个嵌入超参数：

$$I_{\text{en}} = I_o + \alpha \times I_m \quad (1)$$

其中， I_o 表示原始载体图像， I_{en} 表示水印图像， I_m 表示带有水印信息的信息膜， α 表示嵌入超参数。实验证明，训练过程中通过自适应地改变 α 的大小，可以有效调整模型所生成的水印图像的视觉质量，这样可以帮助生成适合不同场景和需求的水印模型。编码器结构如图2-4所示。



● 图2-3 不同二进制信息生成的信息膜。从左到右对应的二进制信息分别为：“0111101010100000000101011010100”、“00111110010001001100101011100010”和“00011110101011101101010110010101”

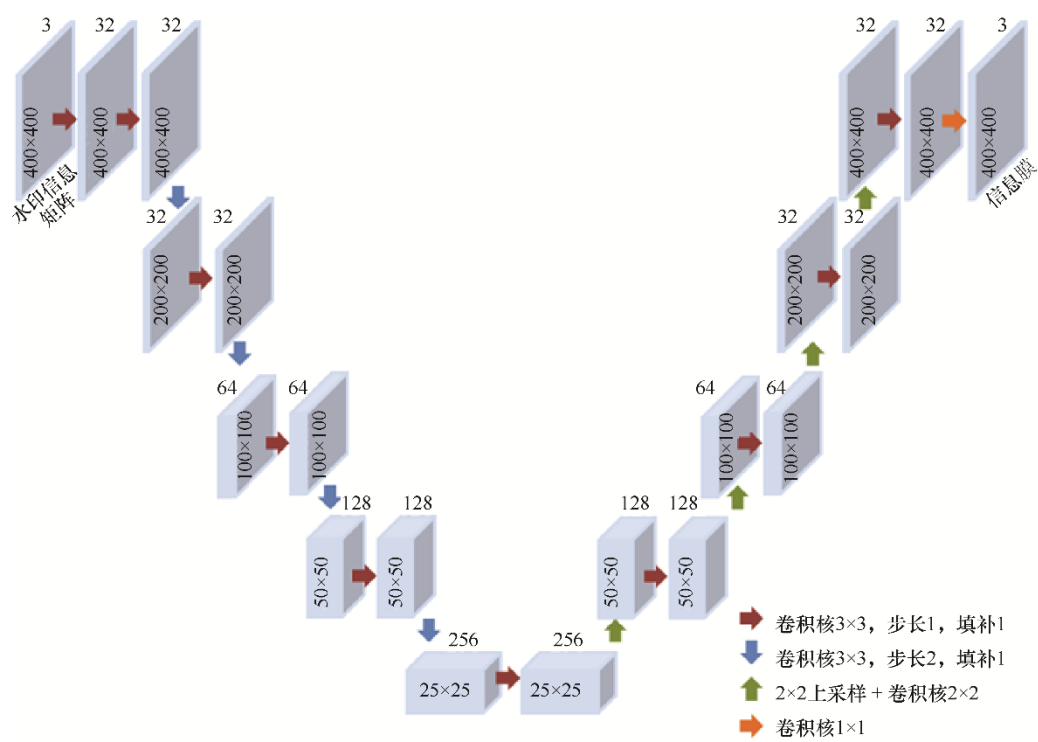


图2-4 编码器的工作原理

● 解码器

解码器主要用于将编码图像下采样为一系列二进制字符串，本软件解码器的网络架构如图 2-5 所示。为了提高在摄像头捕获和校正编码图像期间对角度变化的鲁棒性，本软件采用空间变换网络（STN）[21]将带有噪声的编码图像输入解码器。由于 STN 需要一个线性层来拟合透视变换的权重，所以使用了几个卷积层和 ReLU 层来产生图像的空间变换参数。根据空间变换参数，STN 会将图像进行仿射变换，修正形变。使用 STN 可以使水印提取层对屏幕拍摄过程产生的变形更加鲁棒。最后，解码器结合一个全连接层和一个 ReLU 层来产生与水印数据长度相同的二进制输出。

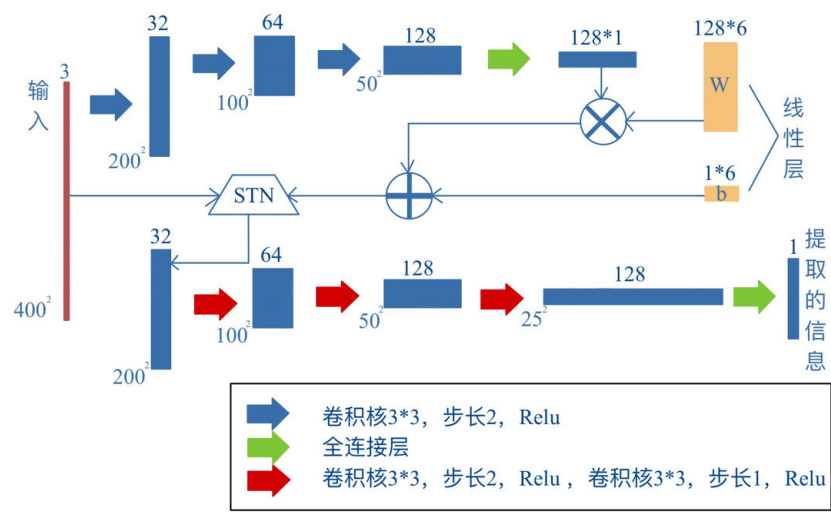


图 2-5 解码器的工作原理

● 鉴别器

为了提高编码图像的质量，实现较低的感知失真，本软件使用一个鉴别器与编码器进行对抗训练。鉴别器网络由 5 个卷积层和最大池化层组成，其输出是一个二进制数字 0/1，指示图像是否带有水印。在训练过程中，当鉴别器不再能够区分原始图像和编码图像时，训练过程达到平衡。鉴别器结构如图 13 所示。

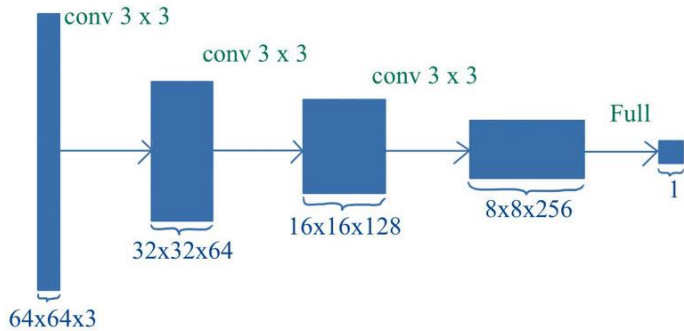


图 2-6 鉴别器的工作原理

● 噪声层

噪声层的主要作用是增加模型的鲁棒性和泛化能力，防止过拟合，并提高模型对于干扰和噪声的鲁棒性。在我们的软件中，用一系列数学模型来模拟由物理成像而引起的畸变。其中包括透视变换、运动模糊、随机离散噪声、色彩失真、JPEG压缩噪声五种噪声，用于来模拟真实拍摄屏幕过程中会产生噪声。模拟真实的屏幕拍摄噪声示例如图2-7所示。



图2-7 模拟真实的屏幕拍摄噪声

● 图像矫正模块

DeepLab V3+使用了自适应空间金字塔池化（ASPP）模块来实现多尺度信息融合。它通过在不同的空间分辨率下对输入进行池化，从而获取不同尺度的特征，然后将这些特征进行融合。ASPP模块中包含多个并行的池化操作，每个池化操作使用不同的卷积核大小和步幅，以获得不同的感受野大小和下采样率。这些池化操作的结果被级联在一起，并进行一次卷积操作，以产生最终的特征表示。在我们的软件中,主要是用该模型实现屏摄图像的自动矫正功能，其实现原理如图2-8所示。

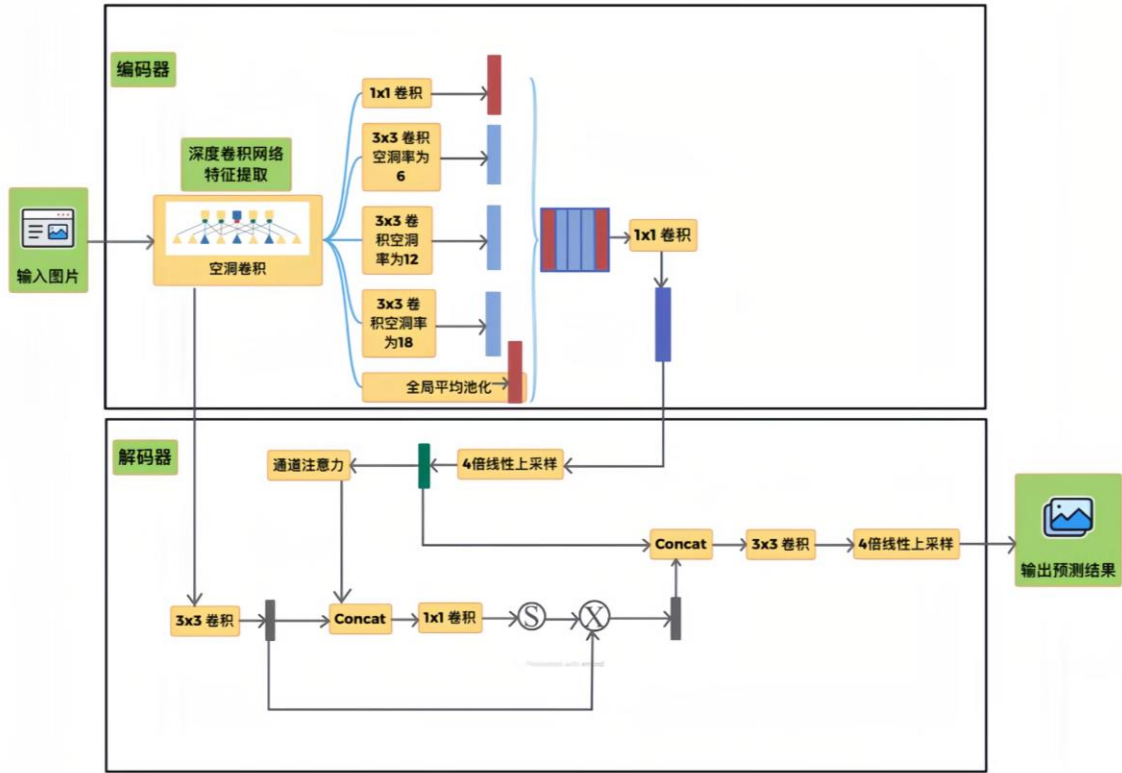


图2-8 DeepLab V3+结构图

3 使用说明

3.1 注册登录

打开该软件，首先会提示用户登录，见图 3-1。若无软件账号，用户可以先进行账号的注册，注册完成之后再行登录，账号注册界面见图 3-2。若已有账号，则用户可以直接登录，用户登录界面见图 3-3。如果账号和密码输入正确，则会弹出“登录成功”的窗口，否则会提示“密码错误”。



图 3-1 登录与注册界面



图 3-2 账号注册界面



图 3-3 用户登录界面

3.2 主界面介绍

登录成功后会进入软件主界面，主界面见图 3-4。该界面主要包括两个工作区域：“水印信息嵌入/提取显示区”、“操作区”。显示区域主要是用来实现对水印信息嵌入和提取过程的可视化，包括“原图”显示、“信息膜”显示、“含水印图”显示、“屏摄图/打印图”显示以及“矫正图”显示，除此之外，该区域还包括四个文本框，分别用来输入水印信息、显示

提取的水印信息、显示提取准确率以及显示单次软件运行时间。操作区域主要包括八个功能：“加载原始图像”、“批量选择图像”、“加载屏幕拍摄图像”、“加载打印拍摄图像”、“嵌入”、“矫正”、“提取”以及“清空”操作。



图 3-4 主界面图

3.3 单张图像水印嵌入和提取

点击“加载原始图像”按钮则可以实现对单张原始图像进行水印信息的嵌入，在弹出的文件选项中选择“imgs”文件夹，见图 3-5，任选其中的一张图像进行水印信息的嵌入，在本次示例中嵌入的水印信息是“01111000111001011101001100010100”。嵌入完成后会有相应的提示，见图 3-6。需要注意，输入的二进制水印信息长度需要满足 16 比特。对应的信息膜、含水水印图和运行时间会在界面上显示，见图 3-7。

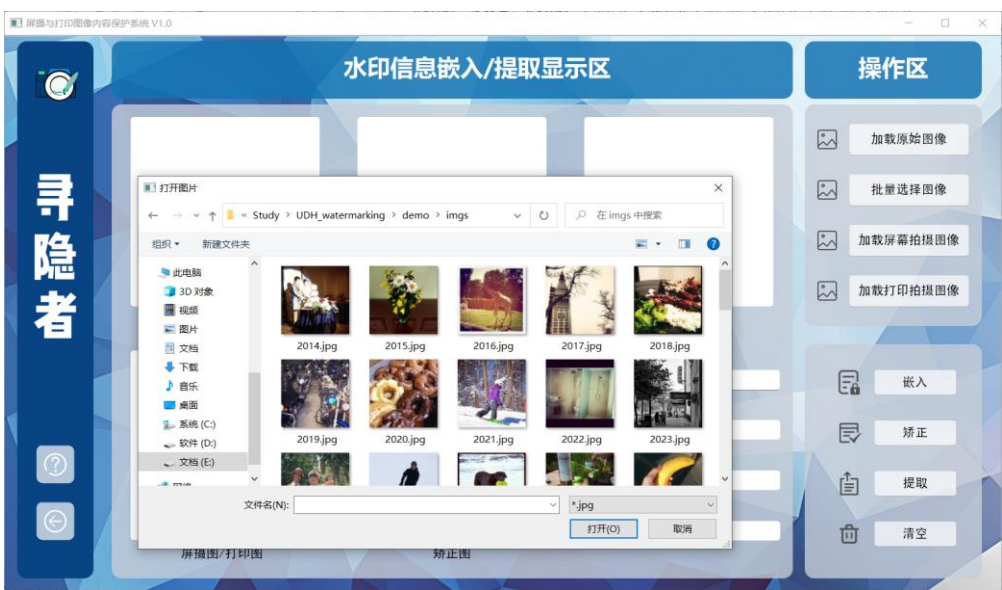


图 3-5 单张原始图像的选择

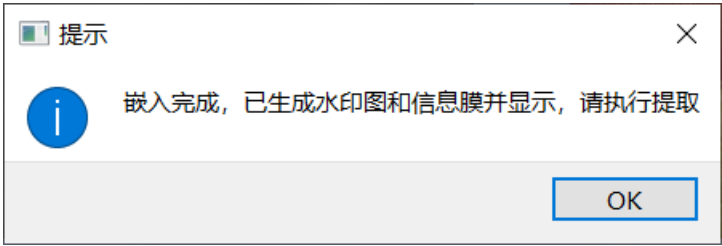


图 3-6 单张图像水印信息嵌入完成后的提示



图 3-7 单张图像水印嵌入完成后的界面显示

若对单张图像进行水印提取，则点击“提取”按钮。提取完成后，会有相应的提示，见图 3-8。同时，界面会显示提取得到的水印信息和运行时间，见图 3-9。

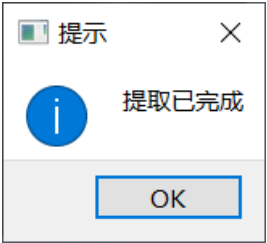


图 3-8 单张含水印图像的水印提取



图 3-9 单张含水印图像水印提取完成后的界面显示

3.4 屏摄图像水印提取

点击“加载屏幕拍摄图像”按钮，可实现对屏幕拍摄图像进行提取水印。在弹出的文件选择项中选择“screenshot”文件夹，任选其中的一张图像。选择完成后，会在界面相应的区域显示所选图像，并提示进行下一步操作，见图 3-10。点击“矫正”按钮以实现自动矫正功能，矫正完成后界面会显示矫正图，见图 3-11。点击“提取”按钮，软件开始提取图像的水印信息，完成后会出现相应提示框，同时，界面会显示运行时间，见图 3-12。



图 3-10 屏幕拍摄图像的选择

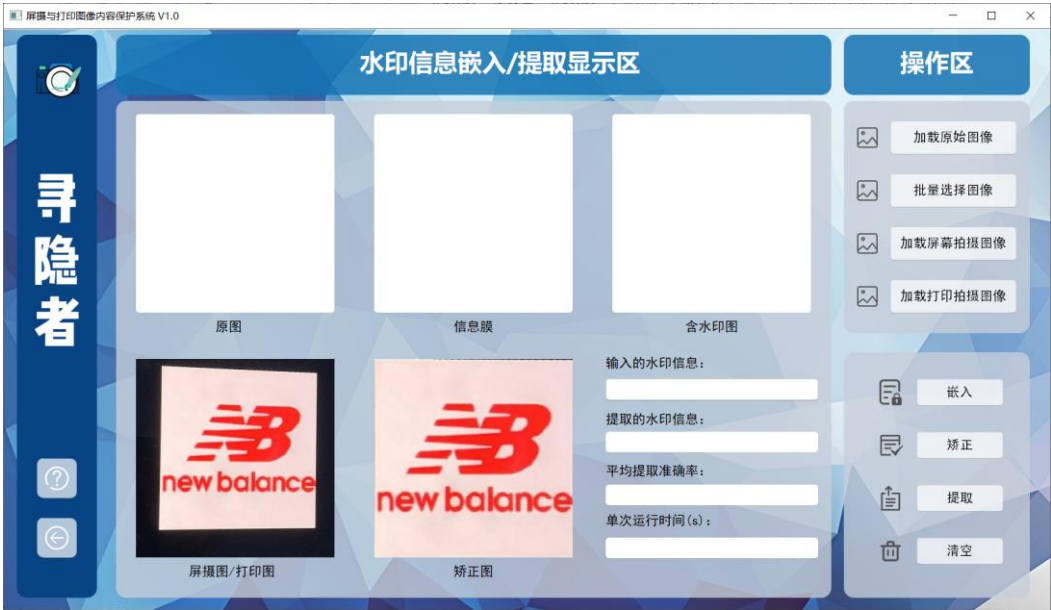


图 3-11 矫正图像的显示

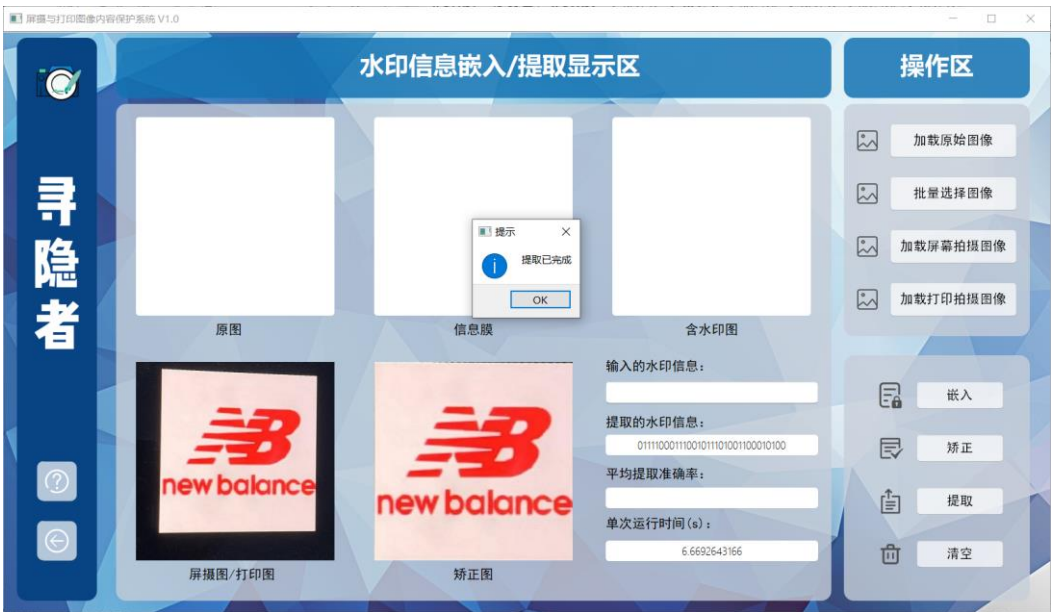


图 3-12 屏幕拍摄图像水印提取完成后的提示

3.5 打印拍摄图像水印提取

点击“加载打印拍摄图像”按钮可实现对打印拍摄图像进行提取水印，在弹出的文件选项中选择“printshot”文件夹，任选其中的一张图像。选择完成后，界面会显示所选图像，并提示进行下一步操作，见图 3-13。此时点击“矫正”按钮以实现自动矫正功能，矫正完成后界面会显示矫正图，见图 3-14。点击“提取”按钮，软件开始提取图像的水印信息，完成后会出现相应提示框，同时界面会显示运行时间，见图 3-15。



图 3-13 打印拍摄图像的选择



图 3-14 矫正图像的显示



图 3-15 打印拍摄图像水印提取完成后的界面显示

3.6 批量图像水印嵌入和提取

若对批量图像嵌入水印，则点击“批量选择图像”按钮，在弹出的文件选项中选择整个“imgs”文件夹，见图 3-16。图像加载完成后会有相应的提示，见图 3-17。在界面的文本框中输入水印信息，点击“嵌入”按钮，完成水印信息的嵌入，成功后会有相应的提示，且界面会显示单次运行时间，见图 3-18。

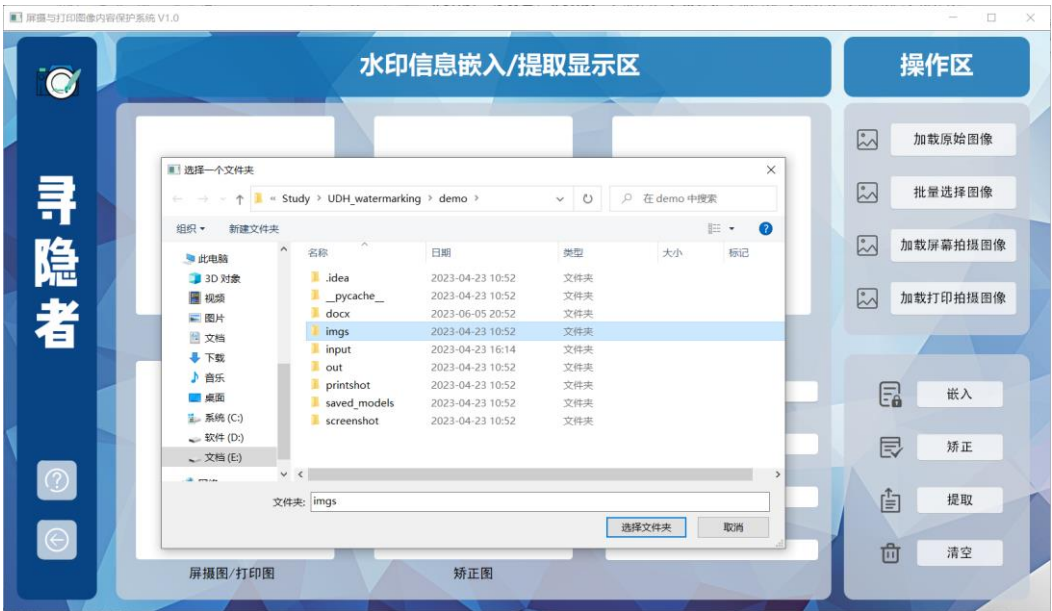


图 3-16 批量图像的选择



图 3-17 批量图像加载完成的提示

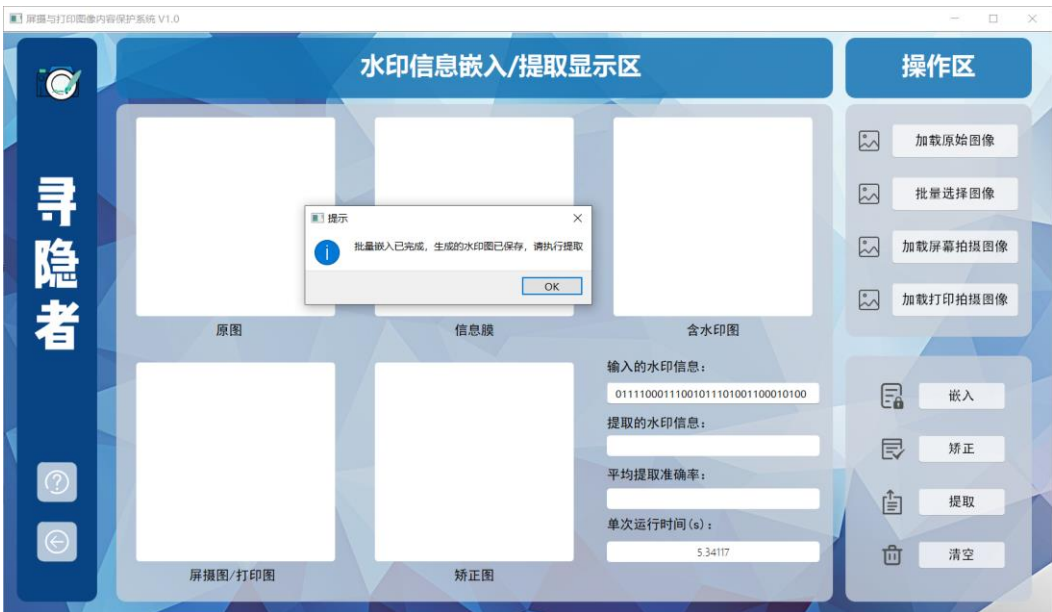


图 3-18 批量图像的水印嵌入

若对批量图像提取水印，则点击“批量选择图像”按钮，在弹出的文件选项中选择整个“encoded_images”文件夹，见图 3-19。再点击“提取”按钮，进行水印信息的提取，成功后会有相应的提示，且界面会显示平均提取准确率和单次运行时间，见图 3-20。

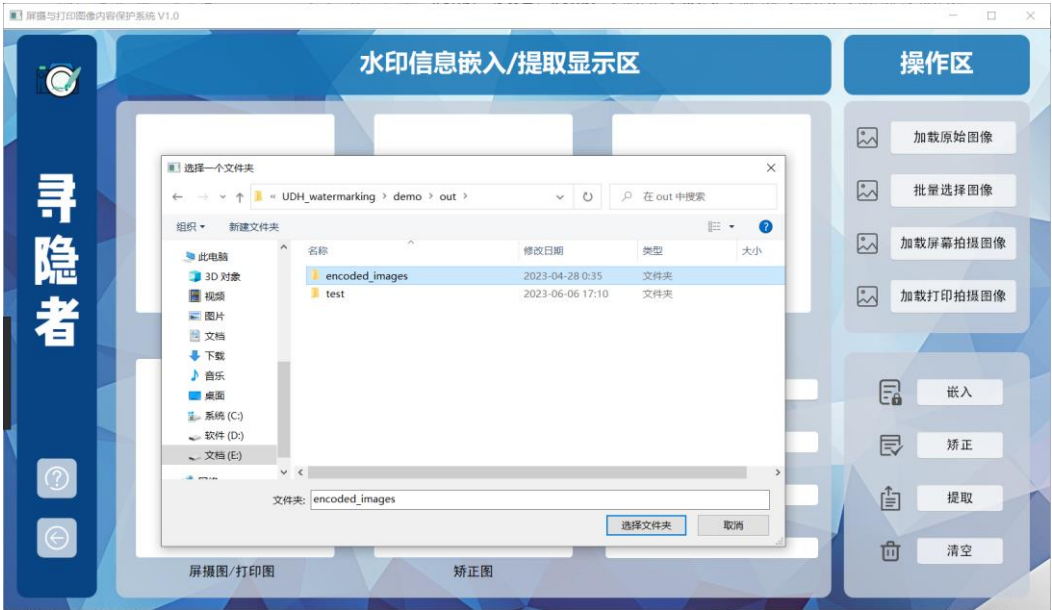


图 3-19 批量图像水印提取的选择



图 3-20 批量图像水印提取完成后的界面显示