文章编号: 1007-1423(2023)05-0022-06 DOI: 10.3969/j.issn.1007-1423.2023.05.004

基于DCT的暗水印技术的研究与应用

张蕊怡，袁 嵩

（武汉科技大学计算机科学与技术学院，武汉 430065）

摘要：各大公司或者企业越来越注重内部电子文件资料的安全性问题。针对电子文件形式的资料泄露问题，研究了一种基于DCT变换的数字水印技术，开发了一款辅助用户添加与提取暗水印的系统。该系统使用了Hough变换与Arnold置乱算法，提供了一种生成不严重干扰用户视觉，又能够抗提取、抗旋转、抗裁剪等一系列攻击的暗水印应用方案，该方案在保障公司内部电子文件不泄露的同时也兼顾了个人信息的安全性问题，满足了实际生产环节中公司或者企业保护电子文件的需求。

关键词：暗水印；数字水印；DCT变换；鲁棒性

0 引言

在当前高速发展的信息化时代，电子文件形式的资料已经成为众多公司或者企业发展不可或缺的一部分。并且这一部分电子资料作为公司生存发展的关键所在，一旦泄露甚至扩散往往会给公司带来较大甚至难以衡量的损失，因此，内部电子文件资料的安全性问题被众多公司或者企业投以大量关注。

传统方法的核心思想是：借助明水印技术，给用户所查看的资料附上标明用户账户、签名、IP地址、日期等信息的明水印，一旦发生资料泄露等恶性事件时，这些明水印便可以用于解决版权纠纷问题，并同时追溯寻找资料泄露的源头。但是该方法明显会过度干扰用户的视觉体验，而暗水印技术秉持着尽最大可能不破坏原数据欣赏、使用价值原则[1]，恰好有效地避免了这一点。

但在实际生产环境中，如何根据具体的应用场景研发出更具针对性和实用性的系统是一个较为关键的问题。

1 需求分析

首先，在实际公司应用中，常见情形中的泄露渠道是员工散播了含有公司内部文件的截图。因而想要溯源到最初泄露资料的源头，就需要在水印中带有诸如员工ID、IP地址、操作时间等与员工个人或操作相关的信息。但由于水印可携带的信息往往有限，故而实际应用中的系统对此需要进行一定的取舍和处理。

其次，在实际传播的过程中有很大可能会出现对原图片进行了旋转、裁剪和涂抹攻击的情况，原本嵌入图像中的水印会随着图像信息的损失一并受损。而随着图片受损程度的提高，便越加难以提取水印中的有效信息，最终失去解决版权问题和追溯泄露源头的功能。因此，实际应用的水印需要具有一定的鲁棒性，同时系统所提供的提取水印的手段还需要有能力处理一部分图片遭受攻击的情况。

最后，还需要考虑到水印中的信息是否会被提取甚至篡改的情况，即对水印信息的加密也是在实际开发中需要被纳入考虑的重要一环，

收稿日期：2022-11-12 **修稿日期：**2022-11-23

基金项目：国家级大学生创新创业训练计划项目(202210488016):基于云桌面的暗水印技术研究与应用

作者简介：张蕊怡(2001—),女,湖北荆州人,本科,研究方向为软件工程;袁嵩(1976—),男,湖北武汉人,博士,副教授,研究方向为智能计算

主要考虑以下三个问题：水印中是否需要包含一部分敏感信息；如何处理因水印中的敏感信息被他人提取而导致的额外信息泄露问题；水印信息是否会被篡改导致溯源错误反而被不法分子利用。

2　关键技术

2.1　Hough变换

为了有效解决实际应用场景中会发生的旋转攻击问题，本系统选择使用Hough变换对图像进行几何形状检测。由于本文所涉及的水印图片实际上是二值图像，每个像素仅分为有效信息和无效信息，所以使用Hough变换速度相对较快，其中本文使用了Canny算子实现图片中边缘的检测与边缘的提取流程。

Hough算法从核心思想上来看，是使用表决方式来实现的一种参数估计技术，其中的原理借助了Hough参数空间与图像空间的点线对偶性，将图像空间中的检测问题转换到参数空间中进行。在使用该算法的过程中，将Hough参数空间分割为多个patch。分别为每个区间计算累积矩阵，最终计算的结果如果能够大于最初设定的阈值，便认为这个区间的交点存在公共直线，反之则舍弃[2]，具体流程如图1所示。

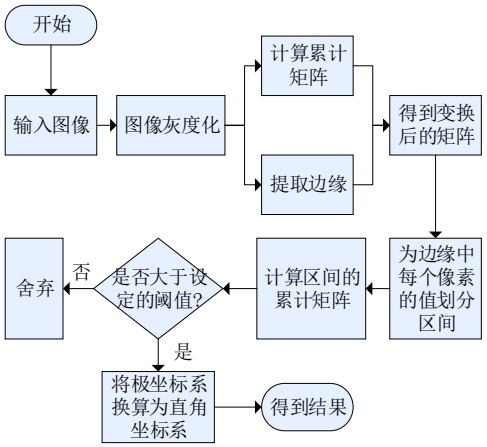


图1　Hough变换实现倾斜校正流程

2.2　Arnold置乱

在水印嵌入之前，为了增强水印图像安全性，防止水印被提取，要对嵌入水印的图像进行置乱[3]。

本文所使用的Arnold变换（猫脸变换）主要是通过一种裁剪错切后再取模拼接的过程达到置乱的效果。与其他的置乱算法相比，Arnold变换与其逆变换计算开销相对较小。

同时由于置乱之后水印的信息在理论上是相对离散的，在遭受攻击时水印损失相对更加均匀，从而使得提取结果在同样的损失率下具有更高的辨识度。基于以上考虑，本项目对水印图像的置乱变换采用Arnold变换，全体像素移动距离的期望值计算方式如公式（1）所示。

$$E = \frac{1}{M*N}\sum_{x=1}^{M}\sum_{y=1}^{N}\mathrm{delta}(x,y) \tag{1}$$

2.3　DCT变换

离散余弦变换（DCT）是一种特殊的离散傅里叶变换（DFT），该变换在保持精度的情况下更加高效[4]。图像经过8×8分块后再进行DCT变换，此时进行水印的嵌入操作，最后DCT反变换得到所需要的图片[5]。

一维DCT变换公式（其二）：

$$F(u) = C(u)\sum_{i=0}^{N-1} f(i)\cos\left[\frac{(2i+1)\pi u}{2N}\right] \tag{2}$$

$$C(u) = \begin{cases} \sqrt{\dfrac{1}{N}}, u = 0 \\ \sqrt{\dfrac{2}{N}}, u \neq 0 \end{cases} \tag{3}$$

二维DCT的公式：

$$F(u,v) = C(u)C(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)\cdot \cos\left[\frac{(2i+1)\pi u}{2N}\right]\cos\left[\frac{(2j+1)\pi v}{2N}\right] \tag{4}$$

其矩阵形式：

$$F = \boldsymbol{A}f\boldsymbol{A}^{\mathrm{T}} \tag{5}$$

$$\boldsymbol{A}(i,j) = C(i)\cos\left[\frac{(2j+1)\pi i}{2N}\right] \tag{6}$$

其逆变换公式为：

$$f(i,j) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(u)C(v)F(u,v)\cdot \cos\left[\frac{(2i+1)\pi u}{2N}\right]\cos\left[\frac{(2j+1)\pi v}{2N}\right] \tag{7}$$

3 系统主要功能实现

系统主要使用Java语言和Python语言进行编码实现，其中系统并不包含提供可视化的前端，而是主要编写后台代码以提供一系列便于嵌入其他系统开发应用之中的API。

本系统的Java后台代码主要分为Controller层、Service层、DAO层、Entity类以及其他便于系统运行的工具等部分。系统主要采用了Spring Boot框架实现自动配置以降低搭建项目的复杂程度，应用了控制反转(IOC)和面向切面编程(AOP)的思想。

3.1 生成水印图片

首先在实际应用中，系统需要提供依照公司需求生成水印图片的功能，本系统提供两种规格的水印，每一个规格可选择提供员工的ID、IP地址、时间等信息。这些参数信息可以选择不由人工输入，而由系统自主检测信息实现自动补全参数，本文涉及的生成水印流程如图2所示。

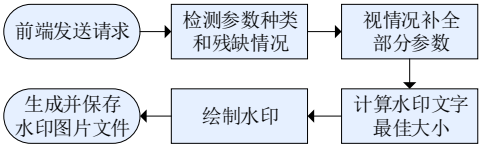


图2 生成水印流程

其中，系统提供了3种不同精确度的日期表示方式，考虑到通常的时间表示方式中部分数字的位数进制小，位数利用率低，故在最高精度的情况下使用基于格林日期的毫秒表示方式进行存储，合理地节省了信息存储空间，尽可能地减小了数字水印的添加给用户造成的视觉干扰。

随后在确认参数的情况下自动判断对应规格下文字应有的大小，最终生成并提供一张合格的水印图片用以完成后续的嵌入功能。

实际系统中该模块主要使用Java语言实现，首先通过拦截器提前处理空白参数和用户登录的安全性验证，其中使用了JWT机制实现token令牌存储用户的账户基础信息，便于自动补全用户的ID，然后将拦截器作为bean写入配置中。

在后台Controller层中判断是否需要自动填入IP地址并视情况自主填入参数，调用Service层提供的函数。

其中，在生成正常的水印图片后，对水印图片使用了Arnold置乱实现混沌加密，以此保证水印的抗提取性和抗篡改性。同时也因为置乱的效果，使得图片遭受攻击后，损失的水印有效像素位置相对分散，从而尽可能地保证整体的可读性。

3.2 嵌入水印

本系统首先将等待嵌入水印图像的原始图片分为RGB三个通道，在得到RGB图像的三层矩阵表示后，每个通道依次进行8 × 8的分块与DCT变换处理。再将之前工作步骤中生成的已混沌加密水印图像嵌入图片子块，最终生成所需密钥图像。对三个通道的操作使得水印具有鲁棒性，针对图片颜色通道的攻击在这一操作下将会失去其效用，其具体流程如图3所示。

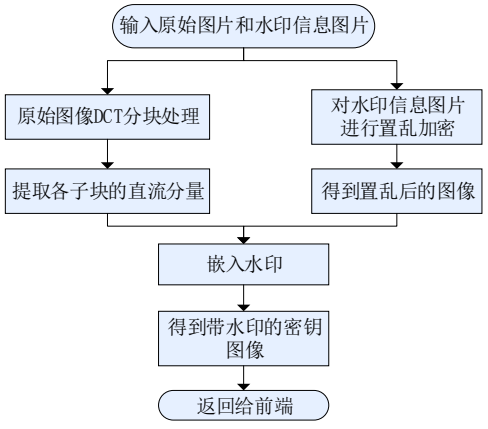


图3 嵌入水印流程

在实际应用过程中，公司或者企业所提供的原始图片往往不能完全进行8 × 8的分块，本文所开发系统中对最后无法分割的边缘子块进行了舍弃。在嵌入水印时采用了阳水印的实现方式，以减少水印信息对用户视觉的干扰。

3.3 提取水印

本系统针对已嵌入水印的图片提供水印提取功能，其中根据图片的不同受损情况分别提供三种提取手段，具体流程如图4所示。

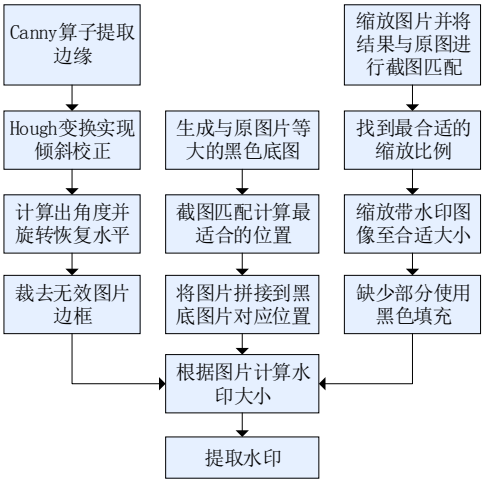


图 4　三种水印提取处理方式流程

第一种情况针对被旋转图片进行水印信息的提取，首先通过Canny算子实现边缘提取，再使用Hough变换对图像进行几何形状检测，通过合理设置阈值筛选出合适的旋转角度并将其恢复水平。最后裁剪掉无效的图像边框得到的图片即可进行提取水印操作。

第二种情况针对被裁剪图片进行水印信息的提取，将被裁剪后的图片与不包含水印的原始图片计算截图匹配，使用OpenCV所提供的matchTemplate()函数实现，找出二者最大匹配位置后，将待检测图片恢复拼接。最后得到的图片即可进行提取水印操作。

第三种情况针对被缩放的图片，通过不断缩放图片并与原始图片进行匹配检测，找到最合适的缩放比例，最后使用OpenCV的扩展库cv2所提供的zoom操作函数得到的图片即可进行提取水印操作。

提取水印的过程中，首先需要将图片再次进行8 × 8分块，再对子块进行水印的提取。由于在之前的操作中对水印图片进行了加密置乱，故在此处需要进行Arnold逆变换来实现水印信息的解密复原，最终提取出一张水印图片返回给用户。

3.4　成果展示

本文使用峰值信噪比(PSNR)来检测嵌入水印图像后对用户视觉的干扰效果，使用结构相似性(SSIM)来检测水印提取效果。嵌入水印后的图片与原图片的对比如图5所示，含水印图片被攻击后进行提取水印操作的结果对比如表1所示。

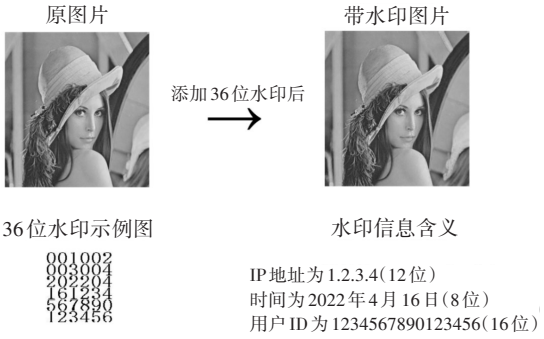
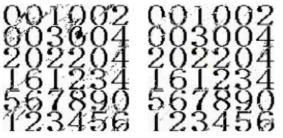
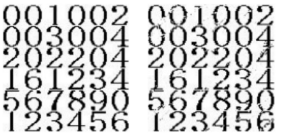
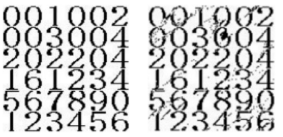
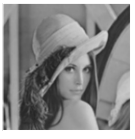
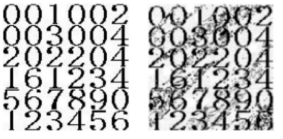
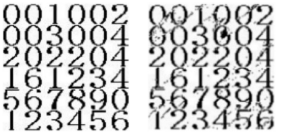
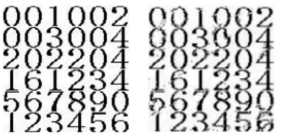


图 5　嵌入水印后的图片与原图片对比

表 1　遭受攻击的图片所提取水印与原水印对比

攻击手段	被攻击图片	原水印图片	提取水印图片
截屏			
颜色通道攻击			
缩放(65%)			
噪声			
高斯模糊			
扭曲			

4 系统接口说明

4.1 水印嵌入功能接口

接口URL：域名/watermark/add。

请求类型：Get请求。

必选参数说明：File类型的pic参数，上传等待被添加水印的原始图片。int类型的timeType参数，‘0’表示时间信息精确至日，格式为“YYYYMMDD”，‘1’表示时间信息精确至小时，距离2022年1月1日0时0分0秒所过去的小时数，‘2’表示时间信息精确至秒，距离2022年1月1日0时0分0秒所过去的秒数。

非必选参数说明：String类型的IP参数，代表水印信息中所要包含的用户的12位IP地址，如果该参数未勾选，则后续自动检测请求方IP地址信息并填入。String类型的time参数，可指定为时间或者其他字符，最高8位，如果该参数未勾选，则自动根据timeType参数指定的时间格式填入当前时间。String类型的ID参数，最多可包含16位长度的字符，如果该参数未勾选，则在后续生成的水印中舍去该部分信息。

接口功能说明：本系统提供两种规格的水印，每一个规格可选择提供员工的ID、IP地址、时间等信息。这些参数信息可以选择不由人工输入，而由系统自主检测信息实现自动补全参数，最终返回给用户一张嵌入了上述自定义水印信息的图片。

4.2 水印提取功能接口

接口URL：域名/watermark/extract。

请求类型：Get请求。

必选参数说明：File类型的resource参数，需要上传不包含水印的原始图片。File类型的target参数，需要上传等待被提取水印的图片。

非必选参数说明：int类型的type参数，可根据图片受损情况指定水印提取的操作流程种类；‘0’表示图片仅仅受到普通攻击，比如截图、拉曲线、模糊、噪声等攻击方式；‘1’表示用户判断图片可能受到了旋转攻击；‘2’表示用户判断图片可能受到了裁剪攻击；‘3’表示用户判断图片可能受到了缩放攻击；如果该参数未勾选，则后续操作中默认等同于type为‘0’的情况。

接口功能说明：本系统针对已嵌入水印的图片提供水印提取功能，根据图片的不同受损情况分别提供三种特殊提取手段。

第一种提取手段适用于从被旋转图片中提取水印的情况；第二种提取手段适用于从被裁剪图片中提取水印的情况；第三种提取手段适用于从被缩放图片中提取水印的情况，最终返回一张进行提取操作得到的水印图片给用户。

5 结语

本文研究了一种基于DCT变换的数字水印技术，提出了一种兼顾实际生产需求和风险的暗水印应用方案，实现了能够辅助用户对图片资料进行水印签名的系统，在监控诸如办公云桌面的场景下提供合适水印的嵌入与提取功能。

该系统能在实际生产环节中生成不严重干扰用户视觉，又能够抗提取、抗旋转、抗裁剪等一系列攻击的暗水印，还一并对水印信息进行了加密，在保障公司内部电子文件不泄露的同时也兼顾了个人信息的安全性问题，满足当前实际应用中公司或者企业需求。

参考文献：

[1] 孙芳,张建良,梅爽宁.一种抗打印扫描的暗水印方法[C]//第三十届中国(天津)2016’IT、网络、信息技术、电子、仪器仪表创新学术会议论文集.天津,2016:235-238.

[2] 黄超,茅健,徐斌,等.基于最小外接矩形和Hough变换的定位算法[J].组合机床与自动化加工技术,2021(8):66-71.

[3] 赵雪燕.基于图像融合的小波变换和Arnold变换的数字水印技术[J].电脑与信息技术,2018(1):39-43,59.

[4] 吕文清.运用DFT的矢量地理数据零水印算法[J].测绘科学技术学报,2018(1):94-98,104.

[5] 黄继武,SHI Y,程卫东.DCT域图像水印:嵌入对策和算法[J].电子学报,2000(4):57-60.

Research and application of blind watermark based on DCT

Zhang Ruiyi, Yuan Song

(School of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan 430065, China)

Abstract: Most companies or enterprises pay more and more attention to the security of internal electronic documents. To solve the problem of information leakage in electronic documents, this paper proposes a method about digital watermarking technology based on DCT transform, and develops a system to assist users in adding and extracting blind watermarks. The system uses Hough transform and Arnold scrambling algorithm to provide a blind watermark application scheme which does not seriously disturb the user's vision, but also can resist a series of attacks such as extraction, rotation, and cropping. This scheme not only ensures that the company's internal electronic documents are not leaked, but also takes into account the security of personal information. It meets the needs of the companies or enterprises in real environment.

Keywords: blind watermark; digital image watermark; DCT transform; robustness

(上接第7页)

Research on trajectory planning based on reinforcement learning algorithm of deep deterministic policy gradient

Yang Youbo, Zhang Mu, Tang Jun, Lei Yinjie*

(College of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China)

Abstract: Trajectory planning is an important part of UAV's intelligent development. The existing traditional route planning algorithms have problems such as poor real-time planning ability, inability to handle dynamic scenes, and uneven tracks. Although the existing reinforcement learning algorithms can perform real-time planning, most are mainly applied in two-dimensional scenes, and there are problems such as easy collision with obstacles, low arrival rate, uneven tracks and low track quality. In view of the above problems, this paper proposed an algorithm based on reinforcement learning of improved deep deterministic policy gradient. The algorithm integrated self-attention mechanism, extracted the characteristics of obstacles, solved the problems of low arrival rate and poor real-time planning ability, redesigned the reward function, to punish the UAV's "retreat" behavior, and introduced the direction vector angle guidance mechanism to solve the problem of track smoothness. The simulation results show that the improved algorithm achieves 93.5% arrival rate in complex dynamic scenes, the average flight distance is reduced by 7.3%, the reasoning time is reduced by 26.2%, the reasoning time is short, the track meets the flight requirements of UAV.

Keywords: trajectory planning; deep deterministic policy gradient; reinforcement learning; self-attention mechanism