

以不可见水印作为电子印花税票的附加取证特征

曹晴心

陕西科技大学电子信息与人工智能学院, 西安 710021, 陕西, 中国

摘要: 电子印花税票 (e-meterai) 是印度尼西亚政府由税务总局 (DGT) 发行的官方数字产品。随着传统文书日益转为数字形式, 其使用范围不断扩大, 作用与纸质印花税票相同。该产品以嵌有印尼专属编码的快速响应码为特征, 并具备显性、隐性与取证三类特征。本研究旨在试验为其增加一项以不可见水印形式呈现的取证特征。本文采用离散傅里叶变换 (DFT) 与尺度不变特征变换 (SIFT) 两种水印嵌入技术, 以判定何者更适该应用。嵌入水印后, 本文还模拟了高斯噪声、椒盐噪声、均值滤波、旋转、平移与斑点噪声等多种攻击。对每种攻击均计算归一化互相关 (NCC) 值: 在 DFT 与 SIFT 技术下, 高斯噪声攻击分别为 0.863 与 0.976, 椒盐噪声攻击分别为 0.929 与 0.984, 均值滤波攻击分别为 0.975 与 0.984, 旋转攻击分别为 0.173 与 0.097, 平移攻击分别为 0.172 与 0.032, 斑点噪声攻击分别为 0.972 与 0.996。

关键词: DFT; 电子印花税票; 取证; SIFT; 数字水印

Invisible Watermarking as an Additional Forensic Feature of E-meterai

QingXin Cao

School of Electronic Information and Artificial Intelligence, Shaanxi University of Science and Technology, Xi'an
710021, Shaanxi, China

Abstract: The e-meterai is an official digital product of the Indonesian government issued by the Directorate General of Taxation (DGT). Its usage has become increasingly widespread as conventional documentation transitions to digital formats, serving the same function as its printed counterpart. This product features a quick-response code embedded with unique Indonesian codes and offers overt, covert, and forensic features. This study aims to experiment with adding a forensic feature in the form of an invisible watermark. We employed two watermark embedding techniques, discrete Fourier transform (DFT) and scale-invariant feature transform (SIFT), to determine which is more suitable for this application. After embedding the watermark, we also simulate various attacks including gaussian noise, salt and pepper noise, averaging filter, rotation, translation, and speckle noise. For each attack, we calculated with normalized cross-correlation (NCC) values, obtaining 0.863 and 0.976 for the gaussian noise attack, 0.929 and 0.984 for the salt and pepper attack, 0.975 and 0.984 for the averaging filter attack, 0.173 and 0.097 for rotation attacks, 0.172 and 0.032 for translation attack, and 0.972 and 0.996 for speckle noise attack, using DFT and SIFT techniques, respectively.

Keywords: DFT; E-Meterai; Forensic; SIFT; Watermarking



一、引言

数字世界的发展日益凸显出视觉内容的安全性与真实性的重要性。数字图像被广泛用于社交媒体、新闻媒体、科学文献、创意产业与专业文档。随着数字图像使用量上升,与版权、伪造和篡改相关的挑战也急剧增加。因此,数字水印技术因其手段与应用的多样性而被视为一种可行的解决方案。

近年来,不可见水印研究取得显著进展。研究者开发了大量算法,力求增强水印抵御压缩、裁剪与像素篡改等各类攻击的稳健性,使水印在经历这些改动后仍保持完整且可检出,从而维护视觉内容的完整性。这些水印算法着眼于在不损害图像质量的前提下高效嵌入水印。这种平衡至关重要,因为它既保护了数字内容,又保持了其可用性与美学价值。因此,在日益依赖数字技术的世界中,不可见水印已成为应对数字图像安全与真实性问题的关键研究方向。已有一系列研究把不可见水印作为应对图像篡改的方案,都力求在提升图像质量的同时防止篡改,分别面向医学影像与艺术作品。LV 采用了不同的技术,用水印比对深度伪造图像,使被篡改的图像更易被检出。WEN 等提出的另一种方法称为“年轮水印”,可产生强健的不可见水印 [1]。

不可见水印通过在内容本身中嵌入不可察觉的标记来保护数字内容,使未授权用户难以发现并移除水印。离散小波变换(DWT)与奇异值分解(SVD)等技术常被用于满足水印的稳健性、不可感知性与容量要求,从而提升其在保护知识产权、防止版权侵害方面的效力 [2]。水印系统还采用 Arnold 变换、混沌映射与秘密信号注入等手段进一步增强安全性,遏制数字数据的非法传播 [3]。

另一项长期用于水印的技术是离散余弦变换(DCT),它相较其他方法具有独特优势。基于 DCT 的水印可把水印嵌入图像的频率系数中,增强对最低有效位(LSB)攻击的稳健性并缩短执行时间 [4]。DCT 在频域水印中被广泛使用,可在不同色彩空间中插入水印:彩色图像的 DCT 水印更宜采用红绿蓝(RGB)空间,而离散傅里叶变换(DFT)技术更宜采用二值方式 [5]。基于 DCT 的水印方法可通过新技术实现高速处理与低计算开销,在保持高质量与高效率的同时兼容多种嵌入比与压缩场景 [6]。

DFT 同样可用于在图像中嵌入安全数据。已有研究探索了把 DCT 用于水印,在容量与不可感知性方面取得了良好结果 [7]。一项关于 DWT 与 SVD 相结合的混合水印方案的研究表明其不可感知性与稳健性均有提升,在医学影像保护方面尤为明显 [8]。另一种创新方法采用基于 DWT 的模糊均衡优化(FEO)技术嵌入水印,对安全攻击具有高稳健性,并显著提升了峰值信噪比(PSNR)。一种把对数极坐标变换(LPT)与 DCT 相结合的医学图像水印新算法,在保持图像质量稳健性的同时实现了患者信息的无损嵌入。

在水印方案中把 DFT 与 SVD 结合可提升视觉失真与稳健性方面的表现。与经典技术相比,基于 DFT 的方法具备不可感知性与更高的安全性,对未授权检测具有很强的抵抗力。DFT 常与 DWT 等其他变换配合使用,以提升水印质量、不可感知性与稳健性,是数字图像认证与版权保护的有力工具。

数字水印的应用已十分广泛,涵盖广播监测、认证、遗留系统、使用控制、医疗应用、版权保护、所有权识别与拷贝控制等方面。这些应用共同凸显出数字水印技术在不同领域所提供的广泛能力。

数字水印的一项重要应用是版权保护:在数字内容中嵌入水印以确立所有权、防止未授权使用或传播。在医疗领域,数字水印可把患者信息或病历安全地嵌入图像或文档中,有助于医疗数据的准确追踪与核验。追踪溯源式拷贝控制在数字内容中嵌入唯一标识或代码,以追溯其来源并监测其传播,从而抵御盗版并确保内容分发网络中的责任可追究。使用控制指通过嵌入的水印来规范和管理数字内容的访问与使用权限。内容认证则保证真实性与完整性的验证。

水印技术中另一项值得关注的方法是尺度不变特征变换(SIFT)。这类图像水印技术在既有研究文献中尚

未被明确讨论，但已有多种先进水印方法，如基于基追踪的稀疏系数加性水印、基于卷积生成对抗神经网络的深度学习水印提取、基于直方图平移的局部水印以增强抗攻击能力、结合 Canny 边缘检测的 LSB 嵌入以提升安全性，以及用于安全数据传输的 DCT 不可见水印。这些技术聚焦于稳健性、安全性、容量与抗攻击能力，展示出数字图像水印在保护多媒体数据方面应对各类挑战的多样思路。

SIFT 技术在多媒体安全领域具有若干优势。SIFT 描述子对关键点周边的局部信息进行编码，无需视角模拟即可提供仿射不变性。当与奇异值分解（SVD）、全相位双正交变换（APBT）等水印技术结合时，基于 SIFT 的水印算法对 JPEG 压缩、高斯模糊、下采样与缩放等多种攻击表现出很强的稳健性。把 SIFT 与水印方法融合可增强数字图像的安全属性，保证真实性、完整性与版权保护。此外，SIFT 提取特征点时对旋转、压缩与缩放具有高度不变性，这也提升了基于 SIFT 的图像水印方案的整体效果与可靠性。

SIFT 还通过提供抗多种攻击的稳健性与安全性来强化版权保护。借助卷积生成对抗神经网络等深度学习技术，研究者开发出可把水印不可察觉地嵌入图像的新算法，即使在遭受改动或攻击后版权信息仍能保持完整。Arnold 变换等加密算法与密码密钥的使用进一步增强了水印过程的安全性。用深度神经网络实现的端到端文档图像水印方案与基于压缩域的数字视频水印算法，展示了在保证水印稳健性与不可感知性方面的进展，从而增强了多媒体内容的版权保护。SIFT 的做法包括：用特征检测器选择用于嵌入的局部区域，用平稳小波变换（SWT）去噪，并用直方图平移把水印嵌入去噪后的局部区域；也可在空间域中改变图像像素，通过对分块不变最大奇异值量化而无需执行 SVD 变换来嵌入水印。

电子印花税票（e-meterai，亦可称电子印章）是一种用于验证电子文档真实性的官方数字印章，其作用类似于纸质文档上的实体印章。该印章提供法律保障，使人确信文档未被更改且依然有效。电子印章的功能包括验证日期与签发机构，并确保文档内数据的完整性与真实性。图 1 为印度尼西亚共和国税务总局（DGT）正式发行的电子印花税票样例及其特征。



Figure 1 E-meterai

图 1 电子印花税票

印度尼西亚使用的电子印花税票呈现为带有印尼特色图案的快速响应（QR）码。该数字印章以标志性的“Garuda Pancasila”（潘查希拉神鹰）为核心，并含有“Meterai Elektronik”（电子印花税票）、数字“10000”、“Sepuluh Ribu Rupiah”（一万印尼盾）以及每枚印章各不相同的唯一编码等文字元素。这种视觉与文字元素的组合不仅可认证文档，还与纸质文档上的传统实体印章一样维护其法律效力。

电子印章的安全特征通常可分为三个层级：显性、隐性与取证。显性特征是肉眼易于辨识的安全元素，如

“Garuda Pancasila”图案与其他可见标记；隐性特征则需借助专门工具核验，如扫描仪与PDF阅读器中的签名面板；取证特征只能由系统主管机构等授权实体（如印尼Peruri公司）检验，可能包括审计日志、密码学手段与代码生成器。三个层级共同保证完整性与真实性，为抵御篡改与未经授权访问提供多层防护。图像中的取证特征指可用于检测伪造或篡改的独特特性或痕迹，它们在图像取证中对区分真实内容与被处理内容至关重要。现有技术包括用SLIC、SIFT与FLANN等算法进行复制—粘贴伪造检测、机器学习方法，以及以颜色等关键特征构建可迁移取证特征（TFF）的通用检测器。

随着数字技术不断发展，提升电子印章认证与安全特征的需求愈发迫切，不能再仅依赖序列号加以区分。为满足这一需求，本文为电子印花税票增加一项新的取证特征——不可见水印，并用DFT与SIFT两种不同技术加以实现，目的是评估何者表现更佳并选用最合适者。与显性特征不同，该水印不着痕迹地发挥作用，确保不干扰电子印花税票的主要特征。通过引入不可见水印，本文力求增强电子文档的完整性与真实性，为防伪与防篡改提供额外一层保护。

二、方法

在水印领域，DFT与SIFT两种技术各有独特优势。DFT借助SVD与混沌映射加密提供稳健性与安全性，保证不可感知性并提升性能；SIFT则以对各类图像变换与失真的稳健性著称，是图像特征提取与匹配的有力工具。

本文所用图像为尺寸709×709像素的原始电子印花税票，作为嵌入水印的宿主图像；同时用印度尼西亚共和国税务局的徽标作为水印图像，其尺寸与宿主图像相同，同为709×709像素。图2与图3分别给出所用的宿主图像与水印图像。



Figure 2 Host Image

图2 宿主图像



Figure 3 Watermark Image

图3 水印图像

图 2 为作为宿主图像的电子印花税票，图 3 为作为水印图像的税务总局徽标。两幅图像采用相同尺寸，以确保水印在宿主图像上均匀分布；这种做法使水印分布更均衡，若不损坏宿主图像便难以将其移除。

若水印图像小于宿主图像，则只能嵌入宿主图像的某些部位，例如角落或纹理丰富的区域以便隐藏。随后本文用 DFT 与 SIFT 技术处理这两幅图像，DFT 技术的步骤见图 4。

DFT 是把空间域数据转换为频域数据的数学方法，可通过修改图像的频率分量来嵌入水印。如图 4 所示，在应用 DFT 之前，本文先确保宿主图像与水印图像的格式与尺寸正确：载入宿主图像与水印图像的灰度版本——灰度图像可简化处理，且足以满足许多水印应用的需要；同时核对水印图像的尺寸，若图像过大则缩放以适配宿主图像。随后对宿主图像应用 DFT，把它从空间域变换到频域：本步骤用快速傅里叶变换（FFT）算法计算宿主图像的 DFT，得到复值频谱，再把零频分量移至频谱中心以便操作与可视化。

嵌入水印时，本文从变换后的宿主图像中选取频率系数，选用中频分量以兼顾稳健性与不可感知性；随后把水印的像素值加到所选系数上以完成嵌入，即对水印进行缩放后加到所选频率系数上。接着应用逆 DFT 把频域数据还原至空间域：对修改后的频谱执行逆 FFT，得到空间域中的含水印图像，随后保存该图像。之后，本文对含水印图像模拟攻击，这些攻击涉及会破坏水印的图像操作，包括加噪、椒盐噪声、均值滤波、旋转与平移等；再从受攻击图像中提取水印以观察攻击效果。这些攻击的目的是检验水印的稳健性，本文用归一化互相关（NCC）值加以衡量。

如图 5 所示，SIFT 技术的初始步骤与 DFT 技术的做法相似，因为这些初始步骤是水印应用中的标准流程。差别在于水印嵌入过程：SIFT 先检测关键点——之所以选择这些点，是因为它们对图像变换具有稳健性——再通过修改所检测关键点处像素的强度值来嵌入水印。

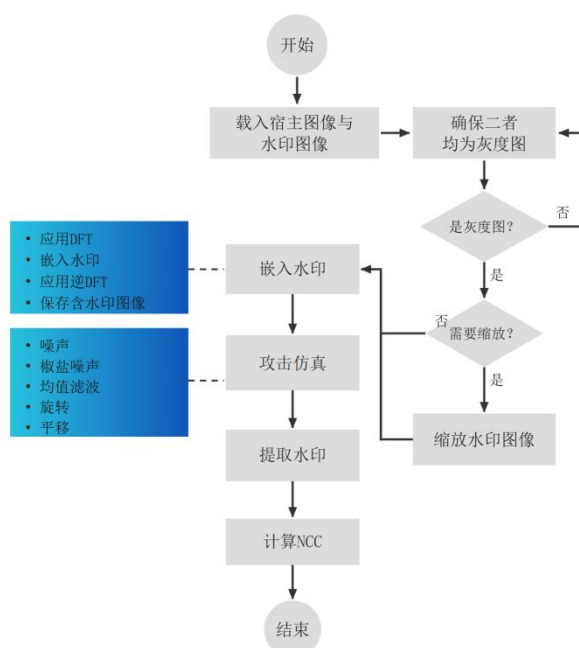


Figure 4 The Steps of the DFT Technique

图 4 DFT 技术的步骤

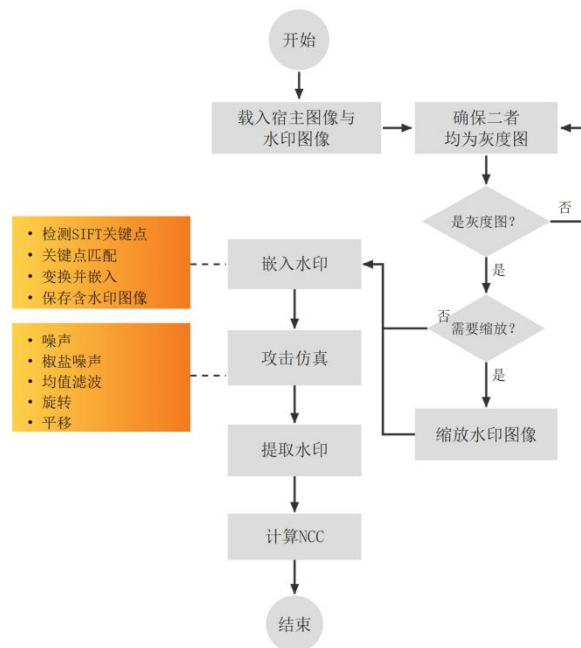


Figure 5 The Steps of the SIFT Technique

图 5 SIFT 技术的步骤

嵌入水印后，本文应用逆变换以获得含水印图像，确保其与宿主图像处于同一域中；这一步对于保持含水印图像的实用性至关重要。本文同样对含水印图像模拟多种攻击，与 DFT 技术中所做的类似，包括加噪、滤波、旋转与平移；攻击之后从受攻击图像中提取水印，并用 NCC 值评估其稳健性，从而评价基于 SIFT 的水印技术的有效性。上述实验步骤均在 Google Colab 笔记本上用 Python 编程语言完成。两种技术均用到若干库，见图 6。

```

import cv2
import numpy as np
from numpy.fft import fft2, ifft2, fftshift, ifftshift
import matplotlib.pyplot as plt

```

Figure 6 Library Set

图 6 所用库

图 6 中导入了实验所需的库：“cv2”库用于图像处理，“numpy”库用于数值计算，“fft”模块用于 DFT 技术，“matplotlib”库用于实验结果可视化。导入这些库之后，本文编写了用 DFT 技术把水印嵌入宿主图像的函数，见图 7。

```

def dft_watermarking(host_image, watermark, alpha=0.1):
    dft_image = fft2(host_image)
    dft_image_shifted = fftshift(dft_image)
    watermark_resized = cv2.resize(watermark, (host_image.shape[1], host_image.shape[0]))
    watermarked_dft = dft_image_shifted + alpha * watermark_resized
    watermarked_image = ifft2(ifftshift(watermarked_dft)).real
    return watermarked_image

```

Figure 7 DFT Watermarking Function

图 7 DFT 水印嵌入函数

图 7 给出通过操作图像频率分量把水印嵌入宿主图像的函数：把缩放后的水印加到宿主图像的 DFT 上，再变换回空间域，该函数即可实现稳健的水印效果；其中的“alpha”可控制水印的可见度与强度。与 DFT 不同，SIFT 技术识别并匹配宿主图像与水印图像之间的关键点，其函数见图 8。

```
def apply_sift_watermarking(host_image, watermark):
    # Convert images to grayscale
    gray_host = cv2.cvtColor(host_image, cv2.COLOR_BGR2GRAY)
    gray_watermark = cv2.cvtColor(watermark, cv2.COLOR_BGR2GRAY)

    # Initialize SIFT detector
    sift = cv2.SIFT_create()

    # Detect keypoints and descriptors
    kp1, des1 = sift.detectAndCompute(gray_host, None)
    kp2, des2 = sift.detectAndCompute(gray_watermark, None)

    # Use FLANN matcher to match descriptors
    index_params = dict(algorithm=1, trees=5)
    search_params = dict(checks=50)
    flann = cv2.FlannBasedMatcher(index_params, search_params)
    matches = flann.knnMatch(des1, des2, k=2)

    # Store all good matches as per Lowe's ratio test
    good_matches = []
    for m, n in matches:
        if m.distance < 0.7 * n.distance:
            good_matches.append(m)

    # Draw matches
    result = cv2.drawMatches(host_image,
                             kp1, watermark,
                             kp2, good_matches,
                             None, flags=cv2.DrawMatchesFlags_NOT_DRAW_SINGLE_POINTS)

    return result
```

Figure 8 SIFT Watermarking Function

图 8 SIFT 水印嵌入函数

图 8 中的函数用 SIFT 方法把水印嵌入宿主图像，并给出两幅图像之间匹配关键点的可视化结果。它先把两幅图像转为灰度，通过只关注强度值来简化处理；随后创建 SIFT 检测器对象，为每幅图像识别关键点并计算描述子；再用基于 FLANN 的匹配器在两组描述子之间寻找对应关系，优化最佳匹配的搜索；应用 Lowe 比值检验滤除劣质匹配，只保留可靠匹配。该函数通过在宿主图像与水印图像的匹配点之间连线，实现匹配关键点的可视化，从而直观呈现嵌入过程。这一技术保证水印稳健且能抵抗常见的图像变换，是一种有效的水印嵌入手段。如实验步骤所述，本文通过计算各自的 NCC 值来评估每种水印技术，NCC 计算函数见图 9。

```
def calculate_ncc(image1, image2):
    product = np.mean((image1 - image1.mean()) * (image2 - image2.mean()))
    stds = image1.std() * image2.std()
    if stds == 0:
        return 0
    else:
        ncc_value = product / stds
        return ncc_value
```

Figure 9 NCC Measurement Function

图 9 NCC 计算函数

如图 9 所声明的 NCC 函数，通过量化两幅图像像素强度之间的相关性（并计入其均值与标准差）来有效评估二者的相似度。归一化互相关通过比较像素值来评估模板与图像某一区域的相似程度。NCC 取值介于-1 与 1 之间，是判定图像对应准确程度的关键。近期进展通过用“孪生”卷积网络处理图像，优化了真匹配与假匹配

NCC 值之间的对比度，从而增强了 NCC 的稳健性。NCC 值越接近 1，表明原始水印与所提取水印之间的相似度越高，说明该水印能够承受某些类型的失真。

三、结果与讨论

水印通常由嵌入数字图像中的徽标、名称或符号构成，起唯一标识的作用。本文分别用 DFT 与 SIFT 技术把水印图像嵌入宿主图像，再通过计算 NCC 值比较二者的表现。考虑到各自的优势与不足，这一比较对于评估把这些技术应用于电子印花税票产品的可行性十分必要。两种技术的水印嵌入结果见图 10 与图 11。

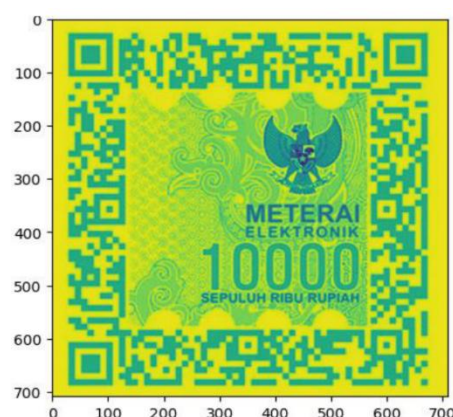


Figure 10 DFT Watermarking

图 10 DFT 水印嵌入结果

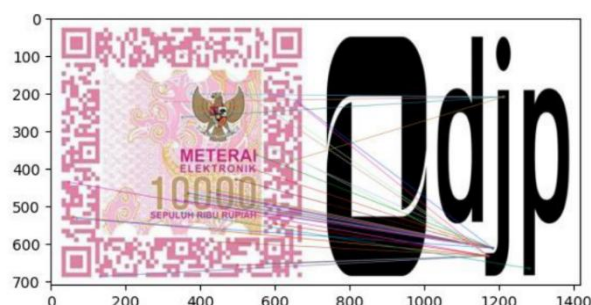


Figure 11 SIFT Watermarking

图 11 SIFT 水印嵌入结果

图 10 为用 DFT 技术嵌入水印后、尚未转换为彩色的原始图像；图 11 为 SIFT 水印技术的结果，突出显示了宿主图像中嵌入水印的关键点位置。随后两幅图像都被还原为原始形态，此时已具备不可见水印这一新的取证能力，见图 12 与图 13。



Figure 12 E-meterai with DFT

图 12 嵌入 DFT 水印的电子印花税票



Figure 13 E-meterai with SIFT

图 13 嵌入 SIFT 水印的电子印花税票

图 12 与图 13 看上去完全相同，因为取证特征肉眼不可见，只有授权人员在需要时才能将其提取出来。高斯噪声攻击在整幅图像上加入随机噪声。高斯噪声的均匀特性会在图像各处引入随机的像素值变化，从而掩盖水印，使其难以直接检测或提取。椒盐噪声攻击是检验图像水印方案稳健性的常用方法，它引入脉冲噪声影响随机像素，通常把这些像素置为最小值（盐）或最大值（椒）。

对含水印图像的均值滤波攻击是施加均值滤波器使图像模糊，该滤波器把每个像素的值替换为其邻域像素的平均值，目的是降低图像质量，使水印不易被看到或检出。旋转攻击是把图像旋转一定角度，目的是破坏水印的对齐关系，使其更难被检测或提取。

对含水印图像的平移攻击是把整幅图像沿上、下、左、右任一方向移动一定量，目的是使水印偏离其预期位置。斑点噪声攻击向含水印图像引入乘性噪声，会依据图像各区域的强度不同而产生不同程度的影响，从而扭曲水印；由于其在图像不同部位差异显著，这种攻击尤为棘手。完成仿真攻击并获得结果后，本文通过计算每种攻击下的 NCC 值来评估水印技术，NCC 值见表 1。

Table 1 NCC Values of Each Attack

表 1 各类攻击下的 NCC 值

技术	高斯噪声	椒盐噪声	均值滤波	旋转	平移	斑点噪声
DFT	0.863	0.929	0.975	0.173	0.172	0.972
SIFT	0.976	0.984	0.984	0.097	0.032	0.996

DFT 与 SIFT 水印技术的 NCC 值可反映二者对各类攻击的稳健性。由上述 NCC 值可知：SIFT 对各类噪声攻击表现出更优的稳健性，在均值滤波下也略胜一筹；DFT 在应对旋转攻击方面表现更好；但两种技术在平移攻击下的表现都较差。SIFT 适用于水印需承受各类噪声失真的场景，DFT 则对旋转攻击有更强的抵抗力。两种技术都可应用于电子印花税票产品，并在若干水印攻击测试中给出良好的 NCC 值。把这些技术应用于电子印花税票产品尚属首次，因此随着数字技术的不断发展，其潜在用途十分可观。

四、结论

本文用 DFT 与 SIFT 技术开展了水印嵌入实验，二者都被用于增强电子印花税票产品的取证特征——此类产品在数字文档中的使用日益普遍。实验得到了每种技术的 NCC 值，表明二者在抵御各类图像篡改攻击方面各有所长。就 NCC 值而言，SIFT 技术总体上对常见噪声攻击与均值滤波具有更好的稳健性，因而更适合水印需要承受此类失真的应用；不过，若旋转稳健性是关键因素，尽管 DFT 在其他方面总体表现较低，仍可能更受青睐。水印技术的选择最终取决于产品所有方；但综合各项优势，本文建议对 DFT 技术给予更多考虑。面向未来的挑战，可进一步开展的研究包括在电子印花税票产品中实现量子安全。

参考文献

- [1] 孟兵, 周良柱, 万建伟, 等. 两种基于DCT变换的数字水印算法分析. 国防科技大学学报, 1999(6): 89-93.
- [2] Soualmi A, Altı A, Laouamer L. An imperceptible watermarking scheme for medical image tamper detection. International Journal of Information Security and Privacy, 2022, 16(1): 1-18.
- [3] 马承哲, 邵家琳, 袁洁, 等. 基于扩散模型的水印生成技术. 网络安全技术与应用, 2025(4): 59-60.
- [4] Luo Y, Zhou T, Liu F, et al. IRWArt: leveraging watermarking performance for protecting high-quality artwork images. Proceedings of the ACM Web Conference 2023, 2023: 2340-2348.
- [5] Laftah M M, Hamid I I, Ali N A. Video copyright protection. International Journal of Interactive Mobile Technologies, 2023, 17(8): 135-145.
- [6] Wang Y, Luo Y, Wang Z, et al. A hidden DCT-based invisible watermarking method for low-cost hardware implementations. Electronics, 2021, 10(12): 1-25.
- [7] 赵蕾, 桂小林, 邵晓杨, 等. 数字图像多功能水印综述. 计算机辅助设计与图形学学报, 2024, 36(2): 269-282.
- [8] 夏道勋, 王林娜, 宋允飞, 等. 深度神经网络模型数字水印技术研究进展综述. 科学技术与工程, 2023, 23(5): 1799-1811.