

基于离散余弦变换的数字水印算法研究

刘涤

(武汉商学院, 武汉 430058)

摘要: 数字多媒体产品随着信息化和网络的发展, 在网络上得到了广泛传播。为了保护数字产品的著作权和产地信息的标识, 将数字水印技术应用到数字媒体产权的保护中。主要介绍了基于离散余弦变换(DCT)的数字水印算法, 并研究了该算法。

关键词: 数字水印; 离散余弦变换; 水印攻击

DOI:10.16184/j.cnki.comprg.2023.09.019

1 概述

数字多媒体技术综合了信息科学领域的多种技术成果, 包括计算机技术、通信技术、视听技术等。在计算机网络飞速发展的今天, 数字化已经称为信息表示的重要手段。数码影像、数字图像及音频等都有大量的应用。网络的兴起, 使得这些技术成果能够被轻易地在网络上发布、下载、篡改、复制、散布, 从而引起信息安全问题、盗版问题和版权纷争问题。

在网络环境下的版权保护与信息安全保障, 受到社会各界普遍关注。其中, 如何防止数字产品被侵权、盗版和随意篡改, 已经成为学术界、企业界等急需解决的技术课题。信息隐藏技术应运而生, 而作为信息隐藏技术研究领域的重点, 数字水印是一种有效的实现版权保护的方式。

2 数字水印技术

数字水印起源于纸币上的水印、邮票上的水印等古老的水印技术, 在光线的照射下, 隐藏的影像便可以展现出来。这些水印的作用在于对商品信息、产地来源进行辨别真伪和标识。这些传统的水印在数字环境下的应用, 使人们可以根据实际应用需要在多媒体中使用水印技术。数字水印主要用于保护数码产品的版权、标识数码产品的信息。

2.1 数字水印技术的特点

为了验证数字媒体产品的归属版权、在网络传输环境中保证数字产品的质量, 或者通过技术检测数字产品在经过网络传输后的质量变化, 人们会在数字媒体产品例如, 图片、视频、音频等中嵌入一些人们视觉察觉不到的信息。这些信息用来识别数字产品是否被篡改、是否是正版等。这些通过变换算法嵌入到数字产品中的信息就是数字水印。

数字水印形式化的表达式如公式(1)所示:

$$w = \{w_i | w_i \in O, i=0, 1, 2, \dots, M-1\} \quad (1)$$

数字水印的特点如下。

(1) 不可识别性。当水印信息嵌入多媒体产品时, 不会让观察者从视觉和听觉方面有所察觉, 也不会损坏

原数字产品。

(2) 鲁棒性。又称稳健性, 是指水印在遭到恶意攻击(例如, 图像压缩、旋转、噪声、滤波等)时, 可以通过提取水印的方法把水印提取出来或者说明水印是存在的。如果攻击者为了掩盖数字产品的归属信息, 想将水印信息删除, 就会造成水印载体的完全损坏。

(3) 可证明性。加入水印可以提供完整可靠的数字产品归属证明。数字水印是将信息作为水印嵌入数字产品以证明数字产品归属方, 在需要时提取出来验证产品的版权、归属及真伪。

2.2 数字水印方法的分类

数字水印嵌入的方法主要有时空域法、变换域法和压缩域法, 这是根据数字水印嵌入位置的不同而使用的技术。

(1) 时空域法是一种直接在图像的每个像素上进行水印嵌入的方法, 这种方法不需要对图像进行任何变换。

(2) 变换域法这种变换是将载体图像进行特定的正交变换, 然后将水印嵌入。常用的变换域法主要包括离散余弦变换(DCT)、离散小波变换、矢量变换、傅里叶变换等。

(3) 压缩域法将数字产品中的一些冗余信息嵌入原始图像中。压缩域法主要分为3大类, 即JPEG压缩域、MPEG压缩域、VQ压缩域。

3 DCT方法

DCT是数据压缩中以实数的余弦函数为变换中心的常用的一个变换编码的方法。这种变换计算速度较快, 具有很好的压缩能量和去相关能力。因此, 它广泛应用于数字音频信号压缩和图像压缩等领域。

二维DCT $N \times N$ 像素矩阵 $I(i, j)$ DCT变换如公式(2)

基金项目: 武汉商学院校级项目基金, 课题编号: 2019-28。

作者简介: 刘涤(1980—), 女, 硕士, 讲师, 研究方向为信息与编码。

所示:

$$f(u, v) = \frac{1}{\sqrt{2}} c(u) c(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} I(i, j) \times \cos\left[\frac{(2i+1)u\pi}{2N}\right] \cos\left[\frac{(2j+1)v\pi}{2N}\right],$$

$$i, j = 0, 1, \dots, N-1 \quad (2)$$

$$\text{这里, } c(x) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{当 } x = 0 \\ 1, & \text{其他} \end{cases}$$

反 DCT 变换如公式 (3) 所示:

$$I(i, j) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u) c(v) F(u, v) \times \cos\left[\frac{(2i+1)u\pi}{2N}\right] \cos\left[\frac{(2j+1)v\pi}{2N}\right],$$

$$u, v = 0, 1, \dots, N-1 \quad (3)$$

4 基于 DCT 的数字水印技术处理过程

(1) 水印图像处理。先将水印信息进行灰度处理, 再将处理后的图像经过二值转换。

(2) 将载体图像中的黑白水印图像读取到二维数组。载体图像可以是彩色的, 也可以是黑白的, 如果是彩色图像, 则水印从绿色信道嵌入、提取出来的质量比从红色信道和蓝色信道嵌入、提取出来的质量要好。

(3) 将载体图像分成 8×8 像素块, 然后对 8×8 像素块逐一进行 DCT。

(4) 在经过 DCT 的载体图像中嵌入经过处理的水印图像。

(5) 在分块图像块嵌入水印信息后, 分块进行反 DCT, 并合并这些图像, 就可以生成嵌入水印的图像。

(6) 对嵌入水印的图像进行 DCT, 这样可以提取出水印。

5 实验结果

实验是在 Matlab 2022a 软件中进行测试的。将一张彩色的载体图像经过灰度处理后, 将经过处理的水印图像通过 DCT 算法进行嵌入, 再通过 DCT 的逆变换算法将水印提出, 如图 1 所示。其中, 载体图像大小调整成 512×512 , 水印图像的大小调整成 64×64 。从结果可以看出嵌入水印后的载体图像在没有受到攻击的情况下, 提出的水印图像与原水印图像基本一致, 还原程度较高。



图 1 水印嵌入载体图像后在未受到攻击时提取水印结果

下面通过对上述嵌入水印的载体图像开展常见的攻击方式, 来测试水印在经过攻击后是否稳定。

(1) 噪声攻击。对嵌入水印的载体图像分别加入两种噪声攻击后提取水印结果如图 2 和图 3 所示。从图 2 和图 3 中可以看出, 嵌入水印的载体图像在收到噪声攻击后, 对载体图像质量是有影响的, 但对提取的水印图像影响不大, 仍可以轻松辨认出水印信息文字。图 2 是嵌入水印的载体图像加入 0.01 强度的高斯噪声后的图像和提取出来的水印图像。图 3 是嵌入水印的载体图像加入 0.01 强度的椒盐噪声后的图像和提取出来的水印图像。

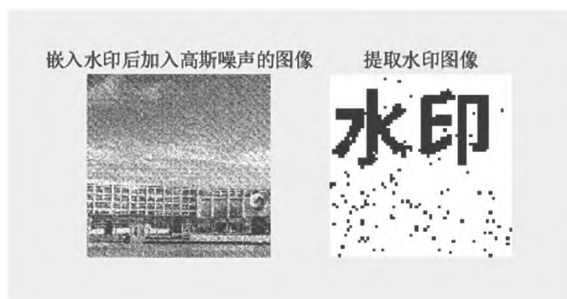


图 2 嵌入水印后加入高斯噪声攻击后的载体图像及提取水印结果

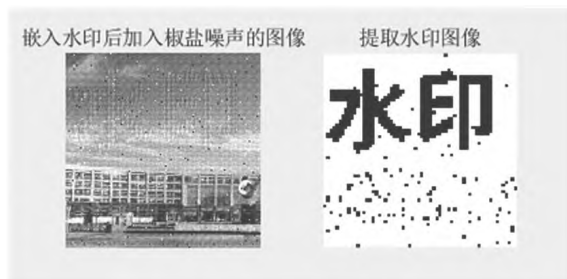


图 3 嵌入水印后加入椒盐噪声攻击后的载体图像及提取水印结果

(2) 旋转攻击。对嵌入水印的载体图像加入旋转操作后, 再提取水印的结果如图 4 和图 5 所示。从图 4、图 5 中可以看出, 嵌入水印的载体图像在加入旋转操作后, 对载体图像的影响不大, 与原始载体图像基本一致。当旋转角度变大时, 能够观察到嵌入水印的载体图像发生逆时针旋转。旋转攻击对提取出来的水印有影响, 特别是当旋转角度增大时, 影响更大。图 4 是嵌入水印的载体图像旋转 0.1° 后的载体图像和提取出的水印图像。图 5 是嵌入水印的载体图像旋转 1° 后的载体图像和提取出的水印图像。从结果可以看到, 旋转 0.1° 后, 提取的水印能轻松识别水印信息文字, 旋转 1° 后, 提取出的水印已无法辨认水印信息文字。





图4 嵌入水印后旋转 0.1° 后的载体图像及提取水印结果

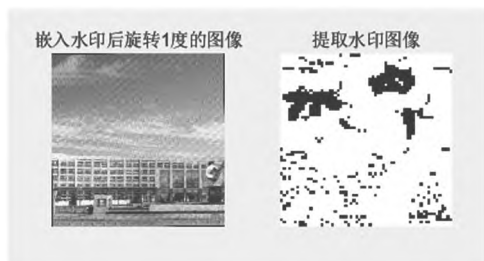


图5 嵌入水印后旋转 1° 后的载体图像及提取水印结果

在数字水印技术中,有两个参数可用于度量数字水印嵌入前后载体图像和水印图像的质量好坏。一个是PSNR(峰值信噪比),另一个是NC(相关系数)。PSNR是将嵌入水印的图像与原始载体图像进行对比,以度量失真度高低。NC是对嵌入前的水印和提取出来的水印进行对比,以度量失真度高低,也就是用来衡量水印抵抗攻击的能力高低。对原始载体图像嵌入水印后,图像的失真度不高,嵌入的水印看不见,将水印提取后,NC值为0.8486,稳定性较好。在嵌入水印的载体图像加入噪声攻击和旋转攻击后,载体图像失真度不高,嵌入的水印在没有被提取出来前不可见。将水印提取出来后,只有经过 1° 旋转的载体图像提取出的NC很低,也就是提取的水印失真度非常高,无法辨认原始水印文字信息;而其他的攻击对嵌入的水印影响不大,提取后仍可以被轻松辨识。几种水印的NC值与PSNR值如表1所示。

表1 几种水印的NC值与PSNR值

类型	NC	PSNR
未受到攻击的水印	0.8486	16.1246
受高斯噪声攻击的水印	0.7822	12.3949
受椒盐噪声攻击的水印	0.8423	15.5181
受旋转 0.1° 攻击的水印	0.8096	13.5238
受旋转 1° 攻击的水印	-0.1396	2.5029

通过上述测试发现,没有被攻击的图像提取出的水印鲁棒性较好,在受到高斯噪声攻击和旋转攻击(特别是旋转攻击)时,水印稳定性下降较快。

另外,在实验中发现如果将水印信息文字的字体变换,会影响嵌入水印的载体图像与原图像的失真度,并且对含有水印的载体图像在提取出水印后与原水印的失真度。实验过程中,将水印信息文字变换为华文行楷加粗、幼圆加粗、仿宋加粗、黑体加粗、华文楷体加粗、方正舒体加粗等字体后,再嵌入到载体图像中,提取出水印后的NC值和PSNR值的结果如表2所示。

表2 几种字体水印提取后的NC值与PSNR值

字体	NC	PSNR
华文行楷加粗	0.8916	17.1800
幼圆加粗	0.8521	11.5445
仿宋加粗	0.8652	16.6377
黑体加粗	0.8501	16.2509
华文楷体加粗	0.8784	16.0998
方正舒体加粗	0.8560	11.2981

6 结语

着重探讨了DCT变换水印的原理,并依据原理进行了数字水印的嵌入及提取实验,在实验中加入3种攻击方式来测试水印效果。下一步将探讨如何提升数字水印提取后的NC值和PSNR值,从而使提取的水印更接近原始水印图像。

参考文献

- [1] 蒋天发. 数字水印技术及其应用 [M]. 北京: 科学出版社, 2015.
- [2] 许文丽, 王命宇, 马君. 数字水印技术及应用 [M]. 北京: 电子工业出版社, 2013.
- [3] 纪佳彤, 胡蓉, 赵全友. 基于DCT变换的数字水印技术的研究与仿真 [J]. 大众科技, 2019, 21(11): 1-4.
- [4] 傅楚君, 兰胜坤. 基于DCT变换的数字水印算法 [J]. 网络安全技术与应用, 2020(7): 49-51.
- [5] 刘浩, 韩晶. MATLAB R2016a 完全自学一本通 [M]. 北京: 电子工业出版社, 2016.
- [6] 韦晓林. 基于DCT的数字水印改进算法 [J]. 测试测量, 2019, 26(2): 88-90.