

电子印章是数字签名的一种表现形式。随着信息安全技术的发展，电子签名技术应运而生。随着计算机的普及和互联网技术的发展，与传统的纸质文档进行加盖印章证明其合法性相比，数字签名技术拥有更多的优势。在很多情况下，电子公文是在网络环境下传送的，在这个过程中，发送方和接收方是不相见的，因此传统的签名盖章方式是无法解决的。因此，采用数字签名技术来代替手写签名，从而证明电子公文的合法性。为了提高印章来源的可靠性，本课题设计并实现基于数字水印的加密电子印章服务，为电子印章的可靠性检测提供一个有力的补充。

2.国内外研究现状：

早在 1997 年 8 月，德国颁布了世界上第一步电子签名法，此后，其他一些国家也纷纷颁布类似的数字签名法律法规。由于历史和文化的差异，国外很少使用印章，但是出现了很多著名的数字签名的产品，例如 Adobe 公司开发的 AdobeAcrobat 数字签名等。我国于 2003 年 6 月 1 日开始实行《中华人民共和国电子印章条例》，2005 年 4 月 1 日起施行《中华人民共和国电子签名法》，并于 2015 年 4 月 24 日修订，确立了数字签名与手写签名、盖章具有同等的法律效力。虽然我国的电子印章技术起步较晚，但在电子印章系统的理论与应用研究方面都取得了许多的成果。数字水印的研究。作为电子合同有效性的的重要依据，电子印章的安全性受到了广泛关注，为了在不改变电子印章的显示图像情况下，对其进行来源有效性的检测，利用数字水印技术能够在不影响宿主媒体质量的情况下，在电子印章图像中嵌入不易被人察觉的标识信息，从而对电子印章来源有效性的检测证明。

数字水印分类。

- (1)按水印检测划分:按这种方法划分,可将数字水印分为私有水印和公有水印。
- (2)按水印的稳健性划分:按水印对各种攻击操作的稳健性程度可将数字水印分为易碎水印和稳健水印。
- (3)按水印的可见性划分:按嵌入水印后数字产品中水印是否可见可将数字水印分为可见水印和不可见水印。
- (4)按水印所附载的媒体划分:按水印所附载的媒体,可将数字水印划分为图像水印、音频水印、视频水印、文本水印以及用于三维网格模型的网格水印等。
- (5)按水印的嵌入位置划分:按水印的嵌入位置,可以将数字水印划分为空间域水印和变换域水印。
- (6)按水印嵌入与提取(或检测)所使用的密钥划分:按水印嵌入与提取(或检测)所使用的密码是

否相同,可分别分为对称水印和非对称水印。

数字水印算法。

1、空域算法

这类算法中典型的水印算法就是将待隐藏的信息嵌入到随机选择的图像点中,最不重要的像素位,

这可以保证嵌入的水印是不可见的,但是这种不重要的像素位,极有可能会被滤波过滤掉,此类算法的鲁棒性差。

2、Patchwork 算法

此方法是随机选择 N 对像素点 (A_i, B_i) ,然后将每个 A_i 点的亮度值加 1,每个 B_i 点的亮度值

减 1,这样整个图像的平均亮度保持不变,此方法对 JPEG 压缩、FIR 滤波以及图像裁剪有一定的抵抗力,但是能存储信息的容量不大。

3、变换域算法

(1)离散傅里叶变换 (DFT),该方法是利用图像的 DFT 来嵌入信息。(2)离散余弦变换 (DCT),DCT

能把空间域上的图像转换到变换域上进行研究,从而能够很容易了解到图像的空间频域成分,进行相应的处理。(3)离散小波变换 (DWT),DWT 是一种时间—频率信号的多分辨率分析方法,在时频两域都具有表征信号局部特征的能力。

4、压缩域算法

基于 JPEG、MPEG 标准的压缩域数字水印系统不仅节省了大量的完全解码和重新编码过程,而且

在数字电视广播及 VOD(Video on

甲代表人(签字):

乙代表人(签字):

甲方盖章处

乙方盖章处

