

文章编号: 2096-1472(2016)-11-49-05

基于信息隐藏技术的数字水印系统模型设计

张天星

(福建船政交通职业学院, 福建 福州 350007)

摘要: 针对数字水印技术应用广泛但指标计算及评价机制普遍不够完善的现状, 本文在研究常用算法的基础上建立了一个能够满足实际应用的数字水印系统基本功能模型, 完成了对数字水印的指标计算及评价机制。该模型基于信息隐藏技术, 综合运用了多种数字水印算法, 结合相关的技术手段, 完成了相对较为完善的数字水印生成、嵌入、检测和提取功能。最后通过一个简单的实例应用验证了本数字水印系统在多媒体版权保护及应用上的良好特性。

关键词: 信息隐藏; 数字水印; 系统模型

中图分类号: TP399 **文献标识码:** A

Design of the Digital Watermarking System Model Based on Information Hiding Technology

ZHANG Tianxing

(Fujian Chuanzheng Communications College, Fuzhou 350007, China)

Abstract: At present the digital watermarking technology is widely used, but the index calculation and the evaluation mechanism are not perfect. This paper establish a digital watermarking system model with basic function for the practical application. Based on information hiding technology, comprehensive digital watermarking algorithms are used in this model, combined with relevant technical means, which could be completed a relatively complete digital watermark generation, embedding, detection and extraction functions. Finally, a simple example is used to verify the good performance of this digital watermarking system in multimedia copyright protection and application.

Keywords: information hiding; digital watermarking; the system model

1 引言(Introduction)

信息隐藏学是一门新兴的交叉学科, 在多个领域有着广阔的应用前景。而数字水印技术除了具备信息隐藏技术的一般特点外, 还具有更加安全、透明的特征和较强的鲁棒性质^[1,2]。因此数字水印技术已经越来越多地应用在各种领域, 但是目前的应用研究对于数字水印的指标计算及评价机制普遍还不够完善, 本系统模型设计主要目的就是在研究比较各种数字水印算法的基础上, 完成了对数字水印的指标计算及评价机制^[3]。

本文目的在于通过对信息隐藏及数字水印技术领域的常用算法的研究, 提出可行的改进措施及方案, 综合相关的技术手段, 建立能够完成实际应用的数字水印系统模型并实现数字水印系统的基本功能及应用。

2 应用需求分析(Analysis of application requirement)

一套完整的数字水印系统模型, 都必须包含嵌入和检测两大部分。嵌入过程至少具有两个输入量: 一个是水印信息, 它一般是以图像文字等形式适当处理后作为待嵌入的水印信号(图1); 另一个就是载体数据, 主要指准备嵌入水印的

数字载体作品^[4]。水印嵌入部分的输出结果为含水印的载体作品, 通常用于传输和转录。当含有水印的载体通过信道传输到接收方后, 而检测部分的目的是试图尽可能的判断出水印是否存在, 若存在则提取出水印信号用于版权的检测(图2)或授权的鉴别等进一步的操作^[5]。

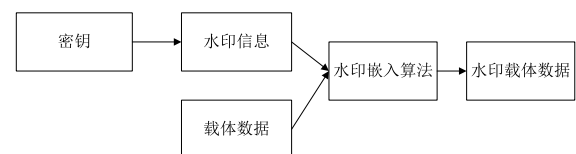


图1 嵌入式数字水印信号

Fig.1 Embedded digital watermark

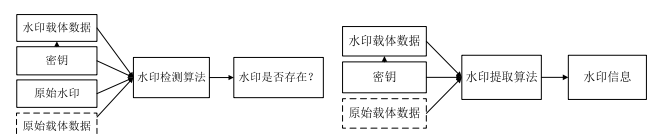


图2 数字水印检测及恢复

Fig.2 Detection and recovery of digital watermarking

由以上分析可知, 本系统需要建立基于信息隐藏技术的

一套数字水印系统模型,确定框架的主要功能及模块内容。在本系统模型中,首先将需要嵌入的数字水印进行了简单的粗处理,再将处理完的数字水印嵌入到相应的载体中,等载体作品需要鉴定作品产权时候,再将嵌入的数字水印进行相应检测并跟其分离提取,然后对数字水印的质量和正确性进行测试和评估^[6]。

3 系统总体模型设计(Design of system general model)

3.1 系统模型的构成

本数字水印系统主要由三个部分组成:水印生成、水印嵌入和水印的检测及提取^[7]。根据不同的应用,这三个部分的设计要求各有侧重,各有不同。

(1)水印生成阶段:水印信息一般都包含了有意义的需要隐藏的信息如版权、发行者、产品的使用及标识等信息。为了保护隐藏这些有意义的水印信息,在它们作为水印之前都进行相应的加密处理,以保证生成的水印信号唯一而有效性。因此水印的生成可以由生成函数来确定,而水印和生成函数通常都基于加密系统、混沌序列、伪随机数生成函数、置乱算法等。设W1为有意义的需要隐藏的信息,G为水印生成的函数,W为生成的水印,则有 $G = T \cdot R$ 。

为了得到基于数字产品的水印W,需要知道用于修改原始水印信息的算法T,而对于T的算法要求也会根据不同应用的需求而改变^[8]。有的应用要求建立易损水印或用于版权争议的稳健水印,即当数字产品的差别也能产生不同的水印;有的应用则要求数字水印对数字产品及其相似的产品版本有依赖性,如半易损水印。在基于信息伪装的应用中,由于信息伪装要求隐藏信息的不可检测性,因此对于算法T通常不作要求。

算法R用于输出基于密钥K原始水印W。R可以是基于加密系统的、基于伪随机函数的、基于混沌序列的、基于置乱算法的。当R为加密系统服务时,K表示加密的密钥信息。而为了生成伪随机函数,R为伪随机函数服务时,K则表示伪随机发生器的种子^[9]。当R为混沌序列服务时,K表示生成混沌序列初始参数值。当R基于置乱算法时,K表示置乱的次数。算法R可以用于通常的数字水印系统,同时由于算法R的存在即使攻击者成功的提取出了水印,也无法解密隐藏信息。数字水印生成策略图,如图3所示。

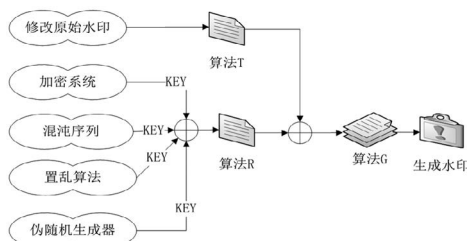


图3 数字水印生成策略图

Fig.3 Generation strategy of digital watermarking

(2)水印嵌入算法及策略:将预处理后生成的水印信息嵌入到原始的载体数字产品中,就是水印嵌入的过程,其中水印信息用 $W=\{w(i)\}$ 表示,载体数字产品用 $S=\{s_0(i)\}$ 表示。因此通常的水印嵌入过程可以表示为:

$s_w(i)=s_0(i) \cup h(i) \cup w(i)$ 。其中 $\cup$ 表示叠加处理, $H=h(i)$ 表示水印的伪装或加权处理,常用的两种嵌入规则如下:

加法嵌入规则 $s_w=s_0+h(i)*w(i)$

乘法嵌入规则 $s_w=s_0*(1+h(i)*w(i))$

s_0 表示采样强度/幅度(空域/时域)或者是变换域的系数值。

近年来,另一种融合嵌入规则得到了广泛的关注,其嵌入规则是:

$s_w=(1-h(i))*s_0+h(i)*w(i)$,这种规则对原始数据 s_0 和水印 w 进行了综合考虑,在不影响人类视觉的前提下,适当的对 s_0 进行一定程度的修改。

嵌入水印的强度一般用水印加权 h 来代表。水印的强度越大则鲁棒性越好,但是会影响水印的透明性^[10]。因此需要在水印的鲁棒性和透明性之间进行折中,兼顾两方面的需求以取得最好的效果。数字水印嵌入策略图,如图4所示。

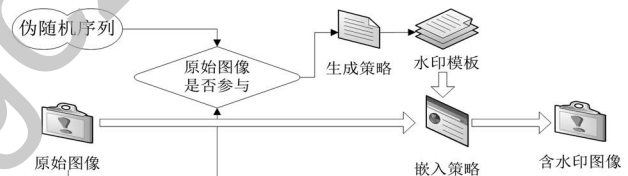


图4 数字水印嵌入策略图

Fig.4 Embedding strategy of digital watermarking

(3)水印检测算法及策略

在已知载体数字产品中检测是否存在目标水印或者进一步解密恢复目标水印并把它从载体数字产品中分离提取出来的过程就是水印检测。水印检测根据检测过程是否需要原始的载体数字产品可以分成非盲(nonblind)水印检测和盲(blind)水印检测两种^[11]。从检测效果来分析,一般需要较好检测率和较高稳健可靠性时候,通常采用非盲水印检测,而盲水印检测应用的范围广泛而且计算的效率更高。在水印的检测过程中,可能会产生两种误报:

一种是数字产品中实际不存在水印而检测出有水印存在(虚报)。

另一种是数字产品中实际存在有水印而检测显示水印不存在(漏报)。

这二种错误发生的概率称为虚警率 P_{fa} 和漏警率 P_{miss} 。总的错误率 P_{error} 是两者相加的和,即 $P_{error}=P_{fa}+P_{miss}$ 。在实际应用中可以预先设定可以接受的错误率 P_{error} 、 P_{fa} 或者 P_{miss} 。

对于水印检测算法一般要求具有良好的可靠性和计算效率。在实际的应用中可以根据其应用的场合适当的降低。数字水印检测策略图如图5所示。

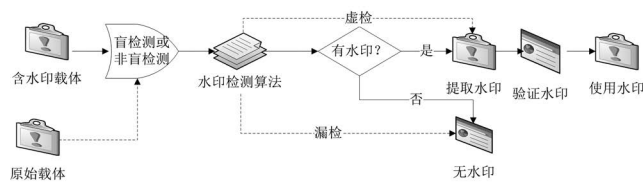


图5 数字水印检测策略图

Fig.5 Detection strategy of digital watermarking

综上所述基于信息隐藏的数字水印系统的基本框架模型图,如图6所示。

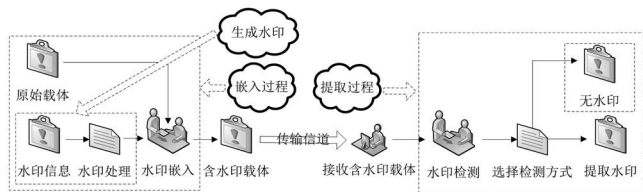


图6 数字水印系统基本框架图

Fig.6 Basic framework of digital watermarking system

3.2 核心机制的设计

首先,本系统对数字水印及载体图像的预处理主要运用置乱算法、混沌序列,以及已有的密码技术来实现。在系统中实现的置乱算法包括Arnold及幻方置乱,实现的混沌序列包括Logistic映射函数及混合光学双稳模型生成混沌序列,能够对生成的混沌序列进行归一化的处理和相应的序列调制(如0,1序列;−1,1的双极性序列)。能够方便的应用已经成熟的密码技术来实现相关的加密(如HASH函数、RSA等)。

其次,本系统设计实现数字水印嵌入的采用了多重算法,包括常见的LSB、DCT、DWT算法,以及基于HVS的自适应算法。利用这些算法能完成双重及多重水印的嵌入,也能够完成对WAV音频载体的数字水印嵌入。

在利用系统进行数字水印的嵌入时,系统找到能嵌入数字水印的鲁棒性最强的区域,在不影响载体透明性的情况下,嵌入标志、算法、数字水印大小等的系统信息。在检测时提取此系统信息,如果此信息不存在,可以选择通过指定提取算法来进行数字水印的提取,也可以选择由系统调用所有的数字水印的提取函数对疑似含水印载体进行数字水印提取,最后由人工判别是否提取成功。提取水印的算法和嵌入水印的算法一般是配套。

之外,由于本系统对数字水印算法的评估参考是基于数字水印抗攻击能力的判断,因此需要对数字水印的抗攻

击功能进行各种攻击,其中部分的攻击方法也可以作为对数字水印或者载体预处理的一部分,如中值滤波、图像的几何处理等。同时还能计算出相应的技术指标值(如NC、PSNR等),并根据计算出的指标值提示数字水印的透明性及鲁棒性的特点^[12]。

3.3 系统结构图

数字水印系统模型结构图,如图7所示。

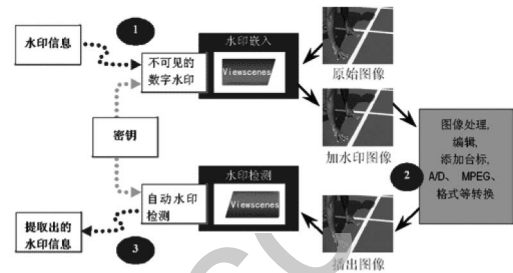


图7 数字水印系统模型结构图

Fig.7 Model structure of digital watermarking system

数字水印系统功能流程图,如图8所示。

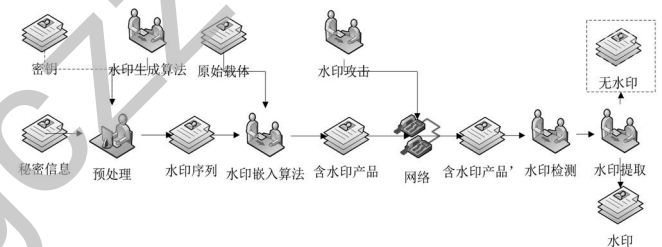


图8 数字水印系统功能流程图

Fig.8 Functional flow—process of digital watermarking system

3.4 系统的功能设计

数字水印系统主要按六个步骤来完成各个功能。

(1)对数字水印及原始载体进行预处理

确认需要嵌入的数字水印后,需要分析判定采用哪种嵌入及检测的方式(盲水印还是非盲水印)。利用相关的算法对数字水印进行嵌入前的预处理,包括转换成二进制比特序列、加密、置乱等预处理的过程,一方面增强数字水印的安全性,另一方面通过处理使数字水印的数据信息分布更加合理,从而有利于数字水印嵌入和检测。同时对原始的载体也进行相应的预处理,如载体的选择,根据不同的原始载体及需要实现的功能需要选择相应的处理步骤(如载体摘要信息的提取、原始载体的图像的图像增强、音频视频信息的滤波等处理)。数字水印及原始载体的预处理的目的在于增强数字水印的安全,使原始载体提供更大的嵌入容量,能更容易更方便的嵌入及检测到数字水印,有利于数字嵌入及检测恢复,最终生成需要嵌入的数字水印及水印载体。

(2)将数字水印嵌入到原始载体中

将水印附加到对应的原始载体上, 需要选择合适的算法。选择嵌入算法一般要综合考虑数字水印的透明性和鲁棒性, 既不能让人轻易地发现数字水印的存在, 又要保证水印载体的数字水印若被破坏或删除将降低载体质量甚至不可使用。所以根据完成数字水印功能的同时需要兼顾这两方面的应用需要, 可以同时嵌入两个或者多个数字水印, 以完成不同应用需求。数字水印嵌入流程图, 如图9所示。

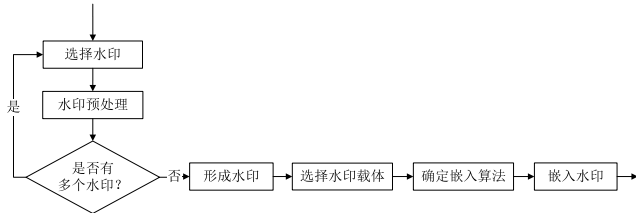


图9 数字水印嵌入流程图

Fig.9 Embedding flow-process of digital watermarking

(3)检测数字水印

接收到载体后, 需要检测载体中是否有数字水印的存在, 一般都是预先确定相应的算法和密钥再对目标载体进行针对性的检测。数字水印的检测包括盲水印检测及非盲水印检测, 非盲水印检测的准确率高但是使用范围有限, 不如盲水印检测, 在检测过程中可能会出现有虚报和漏报的情况。

(4)提取数字水印

当目标载体经过检测确定有数字水印存在时, 需要通过预先确定的算法及密钥将载体中的数字水印分离提取和恢复出来。如果提取出来的数字水印符合版权要求、产品就能被合法使用, 提取数字水印的流程图, 如图10所示。

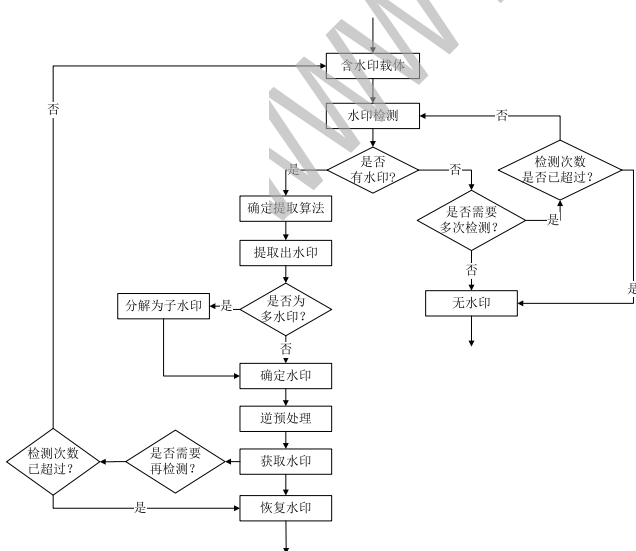


图10 提取数字水印的流程图

Fig.10 Flow chart of digital watermark's extraction

(5)测试数字水印的鲁棒性

数字水印抗攻击的能力主要以数字水印鲁棒性测试结果来衡量。比如对图像载体还包括JPEG图像可压缩、图像旋转、图像几何处理等滤波、加噪攻击能力的测试。

(6)计算及评估数字水印相关指标

数字水印的性能主要用数字水印及嵌入后的载体给予量化的数值来评估, 包括峰值信噪比(PSNR)、信噪比(SNR)、相关系数(NC)、均方差(MSE)等。其实对于人类视觉系统(HSV)及听觉系统(HAS)的阈值JND的确定也是一种评估的计算, 其目的在于度量各个元素可修改的值的范围^[13]。

4 数字水印系统的实现(Implementation of digital watermarking system)

4.1 系统开发工具

在本系统的实现中, 数字水印的嵌入、检测、提取和恢复部分的处理、相关数据的分析和图形图像的生成等算法的实现主要由MATLAB工具来完成, 对于系统界面的设计及实现, 以及一些MATLAB处理速度较慢的操作如数据的排序, 大循环语句的处理等由.NET开发平台来实现。通过MATLAB与.NET搭建的应用程序的开发环境完成整个系统模型的实现。

4.2 界面及系统功能说明

图11列出的是实现的数字水印系统模型程序的部分界面及功能。在实现的数字水印系统模型中可以对数字水印进行预处理操作包括置乱、混沌映射、数字调制和加密等。

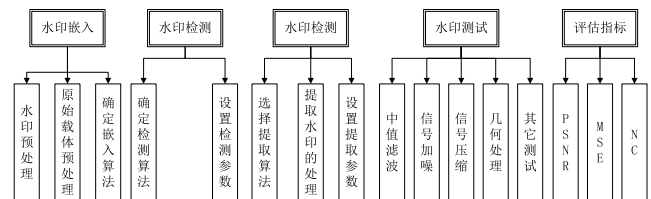


图11 数字水印系统主要功能组织图

Fig.11 Main function of the organization for the digital watermarking system

4.3 实例应用

图12是某数字载体作品在使用本数字水印系统进行Arnold置乱预处理操作的界面, 也列出的单数字水印嵌入操作的界面, 程序将根据选择的操作执行Arnold置乱或反置乱, 执行选定嵌入算法的(LSB、DWT、DCT、HSV等)数字水印嵌入, 并计算出相关的技术参数指标(PSNR、SNR、NC、MSE)。



图12 数字水印置乱预处理及水印嵌入处理界面

Fig.12 Digital watermark's scrambling pretreatment and interface of watermark embedding

在图13实例应用中, 本文讨论的数字水印系统模型程序功能都能在其中找到对应的程序命令, 包括数字水印预处理、嵌入、检测、提取和恢复、攻击及测试、相关技术指标的计算和数字水印的评价^[14], 所有功能一目了然。

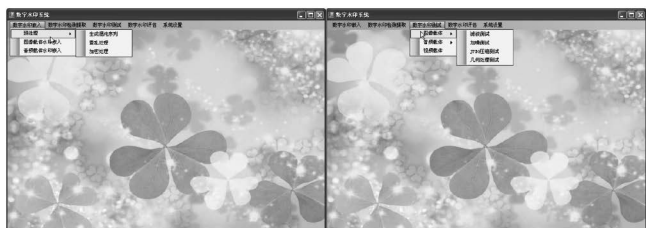


图13 数字水印系统程序实现图

Fig.13 Program implementation of digital watermarking system

本系统中对于水印算法的分析及测试由StirMark来完成。StirMark是一个由剑桥大学开发的用于数字水印研究的测试工具。StirMark用于测试的攻击手段包括线性滤波、非线性滤波、剪切/拼接攻击、同步性破坏攻击等, 可以从多方面测试水印算法的鲁棒性。目前数字水印技术方面公开发行的学术论文一般衡量水印算法好坏都以StirMark的攻击结果作为标准^[15]。

5 结论(Conclusion)

通过实例使用验证, 本文建立的数字水印系统可以较好地完成数字水印预处理、水印嵌入、水印的检测、水印提取和功能执行等流程, 并且利用MATLAB和VS.NET作为开发工具实现了综合运用基于人类视觉模型数字水印算法、双重及多重数字水印算法、双重自恢复数字水印算法、基于音频载体的数字水印算法, 以及常用的LSB、DCT、DWT等数字水印算法的数字水印技术应用。利用本系统模型实现数字水印应用时, 能在有效提高水印算法鲁棒性的同时, 兼顾数字水印对透明性的要求, 并且各种抗攻击检测下来, 综合指标

良好。

参考文献(References)

- [1] D.L.Shinfeng,C.F.Chen.A Robust DCT-Based Watermarking for Copyright Protection.IEEE Transactions on Consumer Electronics,2000(2):185-192.
- [2] Suhail M A,Obaidat M S.Digital Watermarking-Based DCT and JPEG Model.IEEE Transactions on Instrumentation and Measurement,2003(3):255-263.
- [3] Hernandez J R,AmadoM,Gonzalez P F.DCT-Domain Watermarking Techniques for Still Images:Detector Performance Analysis and a New Structure.IEEE Transactions on Image Processing,2000,9(1):55-68.
- [4] 郭永.数字水印技术在电力文档安全传输中的研究[J].信息技术,2016(10):110-111.
- [5] 刘岩,等.数字水印技术及其在电力系统中的应用[J].电力信息化,2005,3(6):91-92.
- [6] 王晓红,等.一种彩色QR码嵌入彩色图像的数字水印技术[J].光电子激光,2016(10):136-138
- [7] 穆国吉.数字水印及其在印刷行业中的应用[J].印刷质量与标准化,2014(3):17-20.
- [8] 许冬凌.数字水印相关问题浅析[J].办公室业务,2013(05):225-226.
- [9] 聂廷远,等.多重加密的数字水印生成方法[J].计算机工程与设计,2013,34(9):3054-3057.
- [10] 杨莹.几种常用的数字水印算法研究[J].计算机光盘软件与应用,2012(19):136.
- [11] 古丽江·库尔班.探讨数字水印与数字密写的差异[J].数字技术与应用,2011(1):117.
- [12] 王侠.数字水印技术的研究与应用[J].数字技术与应用,2011(3):88-89.
- [13] 刘佳鸣,张鸿宾.基于数字水印和传统加密技术的数字版权管理系统框架的研究[J].计算机科学,2008,35(4):254-256;271.
- [14] 陈旭辉.数字水印系统在高校数字图书馆中的应用[J].机电技术,2011,34(5):12-16.
- [15] 张勇,赖惠成.图像数字水印系统的框架模型及攻击方法研究[J].新疆职业大学学报,2008,16(1):75-77.

作者简介:

张天星(1977-),女,硕士,讲师.研究领域:计算机应用技术。