数字水印处理技术

孙圣和,陆哲明
(哈尔滨工业大学自动化测试与控制系,哈尔滨 150001)

摘 要: 近年来,数字水印技术开始广泛用于数字图像,音频,视频和多媒体产品的版权保护.本文综述了数字水印技术的起源,分类和算法.本文提出了水印处理技术基本框架和基本要求,介绍了现有的各种水印生成算法,水印嵌入算法和水印检测算法,提出了几种有效的算法和研究思路,并展望了水印处理技术的应用前景.

关键词: 版权保护;数字水印;多媒体
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2000) 08-0085-06

Digital Watermarking Techniques

SUN Sheng-he, LU Zhe-ming
(*Dept. of Automatic Test and Control, Harbin Institute of Technology, Harbin* 150001, *China*)

Abstract: In recent years, digital watermarking has been widely used in copyright protection for digital images, audio, video and multimedia products. This paper presents a general watermarking framework (GWF) and fundamental demands. introduces various existing watermark generation algorithms, embedding algorithms and detection algorithms. This paper also presents some efficient watermarking algorithms and several investgative trains of thoughts, and forecasts the application foreground of the digital watermarking.

Key words: copyright protection; digital watermarking; multimedia

1 引言

照片、绘画、语音、文本、视频等数字形式的产品在最近十年已经非常普遍.制造商、销售商和用户都发现利用数字设备制作、处理和存储数字多媒体产品非常方便.同时,数字网络通讯正在飞速发展.在这种环境下,数字产品很容易被复制、处理、传播和公开.盗版者正是利用数字产品的这些性能来破坏制造商和用户的合法权力以获得个人利益.因而,人们必须考虑多媒体产品在数字网络分布系统中的安全问题.对数字多媒体产品的非法操作或行为,通常包括下列三种情况.

(1)非法访问:即未经允许从某个网站中非法复制或翻印数字产品.

(2)故障篡改:盗版者恶意地修改数字产品以抽取或插入特征并进行重新发送,从而使原始产品的版权信息丢失.

(3)版权破坏:盗版者收到数字产品后未经版权所有者的允许将其转卖.

基于加密术、数字签名和数字水印的技术[1]都可以用来对付数字产品侵权问题.基于私用或公共密钥的加密术[2]可以用来数据访问控制.加密后的产品是可以访问的,但只有那些具有正确密钥的人才能解密.数字签名技术已经用于检验短数字讯息的真实可靠性[2].数字签名的标准(DSS)[3]已经被正式采纳.通过使用私有密钥,原始制作者对每个数字产品进行签名,而公共的检测算法用来检查产品的内容是否符合相应的签名.这种数字签名在数字图像,视频或音频中的应用并不方便也不实际,因为在原始数据中需要加入大量的签名.

数字水印技术是一种相当新的技术[4].它与传统的信息隐含技术,即所谓的信息伪装技术(steganography)[5].与加密术相比,信息伪装技术不会引起人们去怀疑在无害的媒介(如数字图像)中可能携带了重要的隐含信息.水印处理技术的目的是隐含秘密的个人信息以便保护数字产品的版权[6~8]或证明产品的真实可靠性.信息伪装技术和水印技术的主要区别在于攻击者的目的不同.信息伪装技术的攻击者试图揭露携带的信息,而在水印处理系统中,盗版者要么试图去除水印来破坏版权要么复制被篡改后的产品以获得虚段的内容验证.

本文目的是介绍水印处理技术的基本框架和目前文献中提出的各种算法,并介绍作者提出的一些算法和研究思路以及未来的研究动态.在本文的第 2 部分介绍数字水印的分类及其应具备的特性.第 3 部分介绍水印处理系统的基本框架.第 4 部分介绍水印处理技术的相关问题及其文献中的一些算法.第 5 部分给出了作者的一些算法和研究思路.第 6 部分作了全文总结和水印技术的未来展望.

收稿日期:2000-03-08;修回日期:2000-04-16
基金项目:国家自然科学基金资助

2 数字水印的分类及其应有特性

2.1 数字水印的分类及其算法分类

数字水印是加在数字图像、音频或视频中的信号,这个信号使人们能够建立产品所有权,辨识购买者或提供数字产品的一些额外信息.数字水印一般用在静止图像和视频图像中,所以下面论述中如没有特殊申明,都暗指水印技术用在静止图像和视频图像中.数字水印的分类方法各种各样.从加水印后图像中水印是否可见可分为可见水印和不可见水印两大类.本文主要讨论不可见水印,所以下面论述中如没有特殊申明,都是指不可见水印.从来源来分,可分为独立于图像的水印和图像自适应的水印.独立于图像的水印可以是随机产生的也可以是事先给定的,而图像自适应的水印是利用原始图像的特性生成的水印.从加水印图像的抗滤波或压缩等能力即鲁棒性来分,可以分为易碎水印,半易碎水印和鲁棒水印.易碎水印对任何图像变换或处理都非常敏感,半易碎水印是对某些特定的图像处理方法有鲁棒性而对其它的处理不具备鲁棒性.鲁棒水印对常见的各种图像处理方法都具备鲁棒性.从水印检测是否需要原始图像参与来分,可以分为私有水印和公有水印.私有水印的检测需要原始图像的参与而公有水印的检测不需要原始图像的参与.

水印处理算法也可分为两大类,即可见水印处理算法和不可见水印处理算法.本文主要讨论不可见水印处理算法.不可见水印处理算法可以分为空间域和变换域两种.空间域水印处理是用各种各样的方法直接修改图像的像素(如直接修改像素的最低位).该类算法对有损压缩和滤波有较好的鲁棒性,但是能够嵌入的水印信息不能太多,否则从视觉上可以看出来.而变换域水印处理是对图像进行各种各样的变换后嵌入水印,如离散余弦变换,离散傅里叶变换,小波变换,线性调频 Z 变换等.

2.2 数字水印处理技术的应用分类

水印处理技术应用大致可以归为如下几类:

(1)增强版权保护的可见水印技术 图像可以通过因特网得到,所有者关心的是图像能够被商业性地使用.所有者希望所有者的标记能够在图像中明显可见,但并不阻止该图像用于其他方面(如学者研究).其基本思想是使得任何商业性地使用该图像都能看见所有者的标记,从而增强版权和收取许可税.

(2)用来表明产品所有权的可见水印处理 图像可以通过因特网得到,所有者希望所有权清晰可见,这样能够鼓励顾客惠顾该产品.比起(1)来说,(2)对税的损失不太关心.

(3)用于可信赖摄像机的不可见水印技术 图像通过数字相机获取.这里所有者希望表明所摄的图像是原始的而并没有被编辑过,不可见水印是在摄像时嵌入.

(4)用于检测数字库中的图像是否被更改的不可见水印技术 图像(如人们的指纹)已经被扫描并存储到一个数字库里.所有者希望能够检测到图像的任何更改,而不需要与原始的被扫描图像进行对比.这里的基本思想是所有者能从图像中抽取出不可见水印用来检查图像是否被更改.在数字库发行到因特网时尤其需要这种水印处理.显然这里需要的是易碎水印.

(5)用于检测盗用图像的不可见水印技术 数字图像的销售商担心他的图像被个人购买后将使得该图像能够免费地被他人得到,这样就丧失了所有者的许可税.该技术正是针对该问题的.

(6)用来对所有权作证的不可见水印技术 数字图像的销售商可能怀疑他的某幅图像被编辑和未付版税就被公布.这里,对销售商数字图像里的水印进行检测将用来证实公开发布的图像是销售商的所有物.

(7)用来确定盗用者身份的不可见水印技术 数字图像的销售商可能怀疑他的某幅图像被编辑和未付版税被公布.销售商在发行他的图像时加入不可见水印来指明图像销售给谁.抽取出来的水印用来确认购买者的身份.这样就允许销售商终止与购买者之间的生意以避免承担风险.

从上面的分类来看,(1)和(2)都是可见水印处理技术;(3)、(4)都属于易碎水印处理技术,即如果加水印后的图像的修改和变化可能引起所嵌水印的改变或消失;(5)~(7)都属于鲁棒水印处理技术,即加水印图像受到攻击后还能抽取出相应的水印.

2.3 数字水印的应有特性

下面我们分别介绍可见水印,易碎水印和鲁棒水印的应有特性

(1)可见水印的应有特性;

(a)水印在图像中可见;

(b)水印在图像中不太醒目;

(c)水印很难被去除;

(d)水印加在不同的图像中具有一致的视觉突出效果.

第(a),(b),(c)条特性比较容易满足,第(d)条特性不容易满足.在实验中发现相同的水印加在不同的图像中具有不同的视觉结果.

(2)易碎水印的应有特性:

(a)水印在通常或特定视觉条件下不可见;

(b)水印能被最普通的图像处理技术改变;

(c)未经授权者很难插入一个伪造水印;

(d)经授权者能很快地抽取出水印;

(e)水印能在图像剪切操作后仍存在;

(f)从抽取出来的水印中能看出哪里被改变.

在这些特性中,有些特性在特定的应用环境下不一定都满足.

(3)鲁棒水印的应有特性:

(a)水印在通常或特定视觉条件下不可见;

(b)加水印的图像经过普通的图像处理技术后水印仍然保持在图像中;

(c)未经授权者很难检测出水印;

(d)经授权者能很快地抽取出水印;

(e)加水印的图像经过印刷或重新扫描后水印仍然能被抽取出来.

3 水印处理系统的基本框架

3.1 数字产品的基本发布模型

数字产品的实际发布机制的详细描述是相当复杂的,包括原始制作者、编辑、多媒体集成者、重销者和国家官方等等.本文给出了一个简单的发布模型,如图 1 所示.

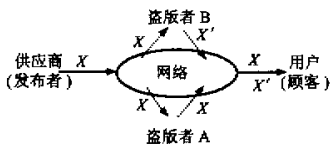

图 1　数字产品网络发布的基本模型

图中的"供应者"是版权所有者、编辑和重销者的统称.图中的'用户'也可称为顾客,他通过网络接收到数字产品.而图中的'盗版者'是未经授权的供应者,他们未经合法版权所有者的许可重新发送产品或有意破坏原始产品并重新发送其不可信的版本.这样顾客难免会间接收到盗版的副本.下面描述的水印处理系统的基本框架正是基于图 1 所示的数字产品基本分布环境的.

3.2 水印处理系统框架

在文献中可见各种形式的水印信号.通常,我们可以定义水印为如下的信号 W

$$W = \{w(k) \mid w(k) \in U, k \in \hat{W}^d\} \tag{1}$$

这里 $\hat{W}^d$ 表示维数为 d 水印信号域,$d = 1,2,3$ 分别表示声音、静止图像和视频图像.水印信号可以是二值形式($U = \{0,1\}$ 或 $U = \{-1,1\}$)[9,10],或者是高斯噪声形式[11].有时称 W 为'原始水印'以便把它和变换域水印形式 $F(W)$(往往在许多水印嵌入和检测算法中出现)区分开来.

水印处理系统的基本框架可以定义为六元体$(\boldsymbol{X}, \boldsymbol{W}, \boldsymbol{K}, G, E, D)$.

(1) $\boldsymbol{X}$ 代表所要保护的数字产品 X 的集合

(2) $\boldsymbol{W}$ 代表所有可能水印信号 W 的集合

(3) $\boldsymbol{K}$ 是标识码(也称为水印密钥)的集合

(4) G 表示利用密钥 K 和待嵌入水印的数字产品 X 共同生成水印的算法,即

$$G: \boldsymbol{X} \times \boldsymbol{K} \rightarrow \boldsymbol{W}, W = G(X, K) \tag{2}$$

(5) E 表示将水印 W 嵌入数字产品 X_0 中的嵌入算法,即

$$E: \boldsymbol{X} \times \boldsymbol{W} \rightarrow \boldsymbol{X}, X_w = E(X_0, W) \tag{3}$$

这里,X_0 代表原始的数字产品,X_w 代表嵌入水印后得到的数字产品.

(6) D 表示水印检测算法,即

$$D: \boldsymbol{X} \times \boldsymbol{K} \rightarrow \{0,1\}$$
$$D(X,K) = \begin{cases} 1, & \text{如果 } X \text{ 中存在 } W(H_1) \\ 0, & \text{若 } X \text{ 中不存在 } W(H_0) \end{cases} \tag{4}$$

这里,H_1 和 H_0 代表二值假设,分别表示水印的有无.

3.3 基本定义

通常,要在被未知原因有意或无意修改的数字产品中检测水印.因此,引入如下定义来表示产品的感知相似性(Perceptual Similarity).

(1)感知相似性:设数字产品 $X, Y \in \boldsymbol{X}$,则符号 $X \sim Y$ 表示 X 和 Y 具有相同的感知形式.而符号 $X \nsim Y$ 表示 X 和 Y 是完全不同的数字产品,或表示 Y 是相对于 X 质量下降的数字产品.

通常,感知相似性是以客观标准为基础的.但是,主观误差估计也可以用来确定感知相似性.

检测算法 D 区分不同水印的能力通常是有限的.因此我们可以引进如下的定义.

(2)水印等价性:若水印 W_1 和 W_2 满足 $D(X, W_1) = 1 \Rightarrow D(X, W_2) = 1$,则称水印 W_1 和 W_2 是等价的,表示为 $W_1 \simeq W_2$.

通常水印的等价性是指水印间的高相关性.显然相同的水印是等价的,反之不然,即等价的水印可能相差很大.

3.4 基本特性和必要条件

水印处理系统的基本框架必须满足一些特定的条件以便形成一套适用于版权保护和产品内容鉴定的值得信赖的根据.

(1)不可见性:对于不可见水印处理系统,水印嵌入算法不应产生可见的数据修改.即加水印后的产品必须相似于原始产品,即 $X_w \sim W_0$.

(2)密钥唯一性:不同的密钥应产生不等价的水印,即对于任何产品 $X \in \boldsymbol{X}$ 和 $W_i = G(X, K_i)$, $i = 1,2$,满足 $K_1 \neq K_2 \Rightarrow W_1 \neq W_2$.

(3)水印有效性:在水印处理算法中只采用有效的水印.对于特定的产品 $X \in \boldsymbol{X}$,当且仅当存在 $K \in \boldsymbol{K}$ 使得 $G(X, K) = W$,则称水印 W 是有效的.

(4)不可逆性:函数 $W = G(X, K)$ 不可逆,即 K 不能根据 W 和函数 G 逆推出来.不满射的函数 G 直接满足这个条件.但这在水印处理算法中并不是必要条件.在实际应用时,不可逆意味着对于任何水印信号 W,很难再找到其它有效水印与该水印信号等价.

(5)产品依赖性:在相同的密钥条件下,当 G 算子用在不同的产品时,应该产生不同的水印信号.即对于任何特定的密钥 $K \in \boldsymbol{K}$ 和任何 $X_1, X_2 \in \boldsymbol{X}$ 满足 $X_1 \nsim X_2 \Rightarrow W_1 \neq W_2$.

(6)多重水印:通常对已知水印信号的产品用另一个不同的密钥再作水印嵌入是可能的,这往往是盗版者在重销时可能做的工作.若 $X_i = E(X_{i-1}, W_i)$, $i = 1,2,\cdots$,那么对于任何 $i \leqslant n$,原始水印必须在 X_i 中还能检测出来,即 $D(X_i, W_1) = 1$,这里 n 是一个足够大的整数使得 $X_n \sim X_0$ 而 $X_{n+1} \nsim X_0$.

(7)检测的可靠性:肯定检测的输出必须有一个合适的最小的置信度.如果 P_{fa} 是检测的虚警概率,则它满足 $P_{fa} < P_{thres}$ 这里 P_{thres} 是产品供应者所选择的合适的概率阈值.

(8)鲁棒性:设 X_0 是原始的产品而 X_w 是加水印的产品并且 $D(X_w, W) = 1$,又设 M 是一个多媒体操作算子.则对于任何 $Y \sim X_w$, $Y = M(X_w)$,满足 $D(Y, W) = 1$,而且对于任何 $Z = M(X_0)$,满足 $D(Z, W) = 0$.

(9)计算有效性:水印处理算法应该比较容易用软硬件实现.尤其是水印检测算法必须足够快以满足在产品发行网络中对多媒体数据的管理.

4 水印处理系统的基本问题及其算法

在水印处理系统中,最重要的两个基本操作是水印嵌入

(G,E)和水印检测(G,D),如图 2 所示的,这里已经包括了水印生成问题.当然在网络中,水印攻击问题也是一个非常普遍的问题.下面我们着重讨论这四个问题和文献中的一些算法.

4.1 水印生成

水印信号的产生通常基于伪随机数发生器或混沌系统.m 序列或高斯噪声信号等不相关信号很容易产生.产生的水印信号 W 往往需要作进一步的变换以适应水印嵌入算法.为了分析方便,我们把算子 G 分解为如下两个部分

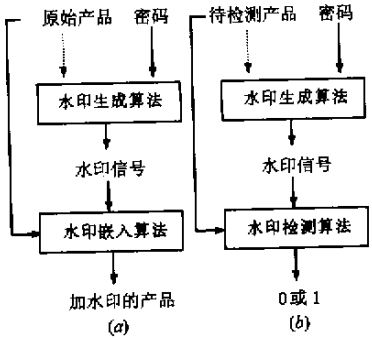

图 2 水印处理算法(a)水印嵌入算法(b)水印检测算法

$$G = T \circ R, R: \boldsymbol{K} \to \boldsymbol{W}, T: \boldsymbol{W} \times \boldsymbol{X} \times \boldsymbol{K} \to \boldsymbol{W} \tag{5}$$

第一部分 R 输出原始水印 $\tilde{W} \in \boldsymbol{W}$,该原始水印只由密码 $K \in \boldsymbol{K}$ 产生.当 R 基于伪随机数发生器时,密码 K 直接映射为伪随机数发生器的种子[8,12].当 R 基于混沌系统时,密码集由许多初始条件的适当变换而产生[13].这两种方法所产生的密码集足够大并且满足密码唯一性条件,而且由 R 产生的水印是有效的水印.此外,R 是不可逆的.

第二部分 T 对原始水印进行修改以获得最后的依赖于产品的水印 W. T 最好满足

$$T(\tilde{W}, X_0) \simeq T(\tilde{W}, X_w) \simeq T(\tilde{W}, X'_w) \tag{6}$$

这里 X_0 是原始的产品而 X_w 是加水印的产品,并且 $X'_w = M(X_w)$, $X'_w \sim X_w$.

在这里需要指出的是原始水印信号也可以预先指定,而在嵌入水印前对该水印信号作适当的变换或不作变换.密码可以在水印嵌入过程中产生.

4.2 水印嵌入

水印嵌入就是把水印信号 $W = \{w(k)\}$ 加到原始产品 $X_0 = \{x_0(k)\}$ 中,最普通的嵌入准则如下[12]:

$$x_w(k) = x_0(k) + \alpha w(k), \text{(加法准则)} \tag{7}$$

$$x_w(k) = x_0(k) + \alpha x_0(k) w(k), \text{(乘法准则)} \tag{8}$$

在这里,变量 x 即可以指采样的幅值(时域),也可以是某种变换的系数值(变换域).这里,参数 α 可能随采样的不同而不同.在时域下的加法准则已经用在很多算法中[8,14].但是变换域的水印处理算法被证明是非常有用的 DFT 的相位[15]和幅值[16]已经用于水印处理算法中.基于 DFT 幅值的水印嵌入对一些基本的几何变换(即旋转和缩放)具有鲁棒性.基于离散余弦变换(DCT)的水印嵌入算法[12,17]对压缩、滤波和其他一些数字处理算子具有鲁棒性.近来,基于离散小波变换(DWT)的水印嵌入算法已经提出来[18],这些算法对 JPEG 和 JPEG2000 具有较强的鲁棒性.除此之外,文献[19]提出了基于 $n \times n$ 分块的用于数字图像和视频的水印处理技术,这些算法的原理是对图像块的 DCT 系数作一定的限制.文献[20]还提出了基于线性调频 Z 变换的数字图像水印处理技术.

综上所述,水印嵌入过程 E 可以用一个统一的操作符 $\oplus$ 来表示.加水印后产品的数据采样(象素,声音采样)可以用下式来表示

$$x_w(k) = x_0(k) \oplus h(k) w(k) \tag{9}$$

这里 $\{h(k)\}$ 是 d 维(声音 1 维,图像 2 维,视频 3 维)的水印嵌入掩码.操作符 $\oplus$ 可能包括合适的截断操作和量化操作.

4.3 水印检测

水印检测可以作用于任何产品 X,检测时最好不需要原始产品的参与.一些水印处理技术在检测时使用了原始产品[21].但是在检测时使用原始产品是个大缺陷,尤其将水印处理技术用于产品的网络发布和传播时.因此,常常考虑检测时不需要原始产品的参与.

水印检测的第一步是用算子 G 产生水印.第二步是算子 D 检测.检测可能包含下列两个错误:1. 水印被检测到,但是实际上产品中并不包含水印;2. 水印没有检测到,但是实际上产品中包含水印.这两个错误是基于一定的虚警概率和拒绝概率的.设 $c = 1 - p_{fa}$ 表示肯定检测的确定度,则

$$c \geqslant c_{thres} \Rightarrow \text{水印存在} \tag{10}$$

参数 c_{ther} 是产品供应商检测时所选择的检测确定度,式(10)直接跟 3.4 中的检测可靠性条件相关.通常,当错误的肯定检测概率趋向 0($P_{fa} \to 0$)时,则水印的否定检测概率趋向 1($P_{rej} \to 1$).

在许多情况下,检测由原始水印信号和加水印产品中抽取出来的水印信号之间的相关系数决定[4].此外,统计检测也可以用在水印检测中[8].

4.4 水印攻击问题和相应对策

盗版者对水印基本框架的攻击目的是想破坏它体现版权所有的能力.对含水印图像的常见攻击方法分为有意的攻击和无意的攻击两大类.水印必须对一些无意的攻击具有鲁棒性,也就是对那些能保持感官相似性的数字处理操作具备鲁棒性,常见的操作主要有:

(1)剪切;(2)亮度和对比度的修改;(3)增强、模糊和其它滤波算子;(4)放大、缩小和旋转;(5)有损压缩,如 JPEG 压缩;(6)在图像中加噪声.

通常假定在检测水印时不能获得原始产品.下面着重讨论有意的攻击及其对策.直接有意地对水印系统进行攻击有如下几种.

(1)伪造水印的抽取[22]:盗版者对于特定产品 X 生成一个信号 W' 使得检测算子 D 输出一个肯定结果.而且 W' 是一个从来不曾嵌入产品 X 中的水印信号但盗版者把它作为他/她的水印.但是,G 是不可逆的,而且 W' 并不能与某个密钥相联系,即伪造水印 W' 是无效的水印(与水印基本框架的水印有效性定义不符).水印处理算法[8,23]就很容易受此攻击.但是,有效性和不可逆性的条件导致有效的伪造水印的抽取几乎不可能.

(2)伪造的肯定检测[22]:盗版者运用一定的程序找到某

个密钥 K' 能够使水印检测程序输出肯定结果并用该密码表明对产品的所有权.但是,在水印能够以很高的确定度检测时,即虚警概率几乎是 0,该攻击方法就不再可行.

(3)统计学上的水印抽取[11]:大量的数字图像用同一密码加入水印不应该能用统计估计方法(例如平均)除去水印.这种统计学上的可重获性可以通过使用依赖于产品的水印来防止.

(4)多重水印[8]:攻击者可能会应用基本框架的特性来嵌入他自己的水印,从而不管攻击者还是产品的原始所有者都能用自己的密码检测出自己的水印.这时原始所有者必须在发布他的产品前保存一份他自己的加水印的产品,用备份产品来检测发布出去的产品是否被加了多重水印.

5　作者的一些算法和研究思路

近年来,作者对水印处理算法的研究主要集中在图像水印嵌入算法的研究,一些主要的算法和思路如下:

(1)基于 DCT 变换的二值水印信号的嵌入算法

这是基于 DCT 变换域水印处理最初研究的热门问题,也是比较成熟的问题.传统的算法往往通过修改 DCT 变换后的中频系数来实现水印嵌入,原因是人眼对图像的低频部分敏感,而对高频系数的修改将导致抗压缩能力下降.作者采取了一种折衷的方案,即采用同时加权修改中频和低频系数的方法来嵌入水印.系数的修改量通过对 JPEG 压缩量化表的量化系数的加权来确定.仿真实验结果表明采用该方法嵌入的水印,具有很强的抗 JPEG 压缩的能力.

(2)基于 DCT 变换的灰度水印信号的嵌入算法

通常的水印处理算法的水印信号都是一维或二维的二值信号,文献中对灰度级水印信号的嵌入算法不多见.作者针对这一问题,提出了如下几种处理方案.

(a)把灰度级水印信号进行分层处理.分层可以采用两种方法.一种是采用层叠滤波器(stack filter)的阈值分解技术,例如它可以把 256 灰度的图像水印信号分布 255 层二值水印信号,然后可以把其中的某一层或多层作为水印嵌入数字产品中,剩余的可以作为密码.另一种是采用比特位分解,例如它可以把 256 灰度的图像水印按字节的最低位到最高位分成 8 层,然后把其中的某些层作为水印嵌入数字产品中.

(b)DCT 域系数裂解的灰度水印嵌入算法.首先将对原始图像和灰度水印图像进行分块 DCT 变换;然后将灰度水印图像的每一个分块的 DCT 变换系数进行衰减和裂解,由一个 DCT 系数变为多个;最后将这些裂解的 DCT 系数分别嵌入到原始图像的中频系数中.仿真试验结果表明采用该方法嵌入的灰度水印是可行的,而且具有很强的抗 JPEG 压缩的能力.

(3)基于矢量量化的图像水印处理算法

自从 1980 年提出矢量量化器码书设计的 LBG 算法[24]以来,矢量量化技术已经成功地应用到图像压缩和语音编码中.矢量量化过程可以定义为从 k 维欧几里德空间 R^k 到其一个有限子集 C 的一个映射,其中 $C = \{c_i \mid i = 1,2,\cdots,N\}$ 称为码书,N 为码书长度.矢量量化包含两个部分:编码器和解码器.为了对一个图像进行编码,编码器首先将原始图像分成 $N_w \times N_h$ 块(矢量),每块图像含 k($k = w \times h$)个像素,即每块图像就是一个 k 维矢量.对于每一个图像块 x,矢量量化器从码书 C 中找出一个与该图像块最匹配的码字 c_p 代替该图像块.找到最近码字以后,矢量量化器用码字 c_p 的标号 p 代替输入矢量 x 进行存储和传输.矢量量化解码器根据接收到的标号很容易从码书中查到相应的码字,找到所有输入矢量的代替码字后由这些码字拼成解码图像.

作者成功地在图像的矢量量化编码过程中嵌入了秘密的水印信号,该文章[25]已经刊登在英国著名杂志 Electronics Letters 上.该文的主要思想是把码书分组并用码字的标号来隐含秘密的水印信息.

(4)不需原始图像参与检测的水印处理算法

需要指出的是在这类算法中,往往嵌入的水印信号是二值的,而且往往把原始图像产品进行分块,每一块只能嵌入 1 比特信息.文献[28]利用了 DCT 变换的零树个数的奇偶性来实现不需要原始产品参与的水印抽取.作者利用了分块 DCT 变换后的某个系数与预先设定值进行比较的方法来实现不需要原始产品参与的水印抽取.

除此之外,作者的其它几条研究思路如下

(1)声音水印信号嵌入到图像中.

(2)图像水印信号嵌入到声音信号中.

(3)动态图像的水印嵌入算法.

(4)采用其它变换(除了常用的 DFT,DCT,DWT 变换等)进行变换域水印处理.

6　总结和未来展望

数字水印技术的发展虽然只有短短的六、七年时间,国际上却已有许多家公司在研制自己的数字水印产品.我国在该领域的研究尚不普及,虽已引起一些大学、研究机构的关注,目前还没有成熟的技术或产品问世.随着数字化产品在中国的普及,特别是今后几年 Internet 用户的成倍增长以及电子商务的加速发展,在网络上直接销售数字化产品将给商家带来极大的利益,也是中国产品走向世界的极佳途径.我们应该抓住此机遇,研制出自己的数字水印产品,并形成一些标准,以适应新技术的发展.

未来的水印处理技术应该在如下方面进行探讨和研究.

(1)探讨水印处理技术与压缩编码算法的统一.数字产品的发布通常要经过编码和传输.传统的水印处理往往与压缩编码算法分开.应该在编码的过程中嵌入水印,这样的优点在于使水印对该编码算法具有鲁棒性,尽量减少无意的水印攻击.作者在文[25]已经在图像的矢量量化编码过程中嵌入水印,结果表明加入水印后的图像丝毫不受矢量量化压缩(采用同一码书)的影响.作者认为这将是未来的水印的研究方向之一.而且我们还可以探讨水印处理算法和其它的数字处理算子的统一.

(2)水印处理算法标准的建立.目前国际上的水印处理尚未形成统一的标准,形成标准已成为研究水印者的共同目标.然而,标准的算法必须有其优越性、通用性和有效性,并要得到世界各国的认同.所以形成标准是一项艰巨的任务.其中基

于 DCT 变换和小波变换域的水印处理技术是各国争相研究的热点,形成标准的可能性最大.

(3)将水印处理技术应用到其他领域,如军事和国防方面,即把数字水印处理技术用于传递秘密的军事信息,或用水印处理技术来验证军事命令、信息的真实可靠性,并探索该领域的新技术和新理论,这对于国防现代化建设和未来的信息化、网络化战争的意义重大.

参考文献:

[1] B. M. Macq and J. J. Quisquater. Cryptology for Digital TV broadcasting [J]. Proc. IEEE, 1995, 83: 944 – 957.

[2] D. R. Stinson. Cryptography, Theory and Practice [M]. New York: CRC Press, 1995.

[3] FIPS 186. digital signature standard [S]. 1994.

[4] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. A digital watermark [J]. Proc., IEEE Int. Conf. Image Processing, 1994, II: 86 – 90.

[5] N. F. Johnson and S. Jajodia. Exploring Steganography: Seeing the unseen [J]. IEEE Comput., Feb., 1998: 26 – 34.

[6] E. Koch and J. Zhao. Towards robust and hidden image copyright labeling [A]. In Proc. 1995 IEEE Workshop on Nonlinear Signal and Image Processing. IEEE, Neos Marmaras, Greece, Jun. 1995: 452 – 455.

[7] J.-J. Quisquater, O. Bruyndonckx, and B. Macq. Spatial method for copyright labeling of digital images [A]. In Proc. 1995 IEEE Workshop on Nonlinear Signal and Image Processing, IEEE, Neos Marmaras, Greece, Jun. 1995: 456 – 459.

[8] I. Pitas and T. H. Kaskalis. Applying signatures on digital images [A]. In Proc. 1995 IEEE Workshop on Nonlinear Signal and Image Processing, IEEE, Neos Marmaras, Greece, Jun. 1995: 460 – 463.

[9] R. B. Wolfgang and E. J. Delp. A watermark for digital images [A]. in IEEE International Conference on Images Processing, Lausanne, Switzerland, Sep. 1996, III: 219 – 222.

[10] A. Z. Tirkel, C. F. Osborne, and T. E. Hall. Image and watermark registration [J]. Signal Processing, 1998, 66(3): 319 – 335.

[11] M. D. Swanson, B. Zhu, and A. H. Tewfik, and L. Boney. Robust audio watermarking using perceptual masking [J]. Signal Processing, 1998, 66(3): 337 – 355.

[12] I. J. Cox, J. Kiliant, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia [J]. IEEE Trans. Image Processing, Dec. 1997, 6: 1673 – 1687.

[13] G. Voyatzis and I. Pitas. Chaotic watermarks for embedding in the spatial domain [A]. in Proc. ICIP '98, Chicago, IL, Oct. 1997: 432 – 436.

[14] R. B. Wolfgang and E. J. Delp. A watermark for digital images [A]. In IEEE International Conference on Image Processing, Lausanne, Switzerland, Sep. 1996: 219 – 222.

[15] J. O. Ruanaidh, W. J. Dowing and F. M. Boland. Phase watermarking of digital images [A]. in Proc. ICIP '96, Lausanne, Switzerland, Sept. 1996, III: 239 – 242.

[16] J. J. K. Ruanaidh and T. Pun. Rotation, scale and translation invariant spread spectrum digital image watermarking [J]. Signal Processing, May 1998, 66(3): 303 – 317.

[17] A. Piva, M. Barni, and F. Bartolini. A DCT-based watermark recovering without resorting to the uncorrupted original image [A]. in Proc. ICIP '97, Atlanta, GA, Oct. 1997, I: 520 – 523.

[18] D. Kundur and D. Hatzinakos. A robust digital image watermarking method using wavelet-based fusion [A]. In International Conference on Image Processing, Santa Barbara, California, U. S. A., Oct. 1997: 544 – 547.

[19] A. G. Bors and I. Pitas. Image watermarking using DCT domain constraints [A]. in Proc. ICIP '96, Lausanne, Swizerland, Sep. 1996, III: 231 – 234.

[20] S. Pereira and T. Pun. An iterative template matching algorithm using the Chirp-Z transform for digital image watermarking [J]. Pattern Recognition, 1999, 33(2000): 173 – 175.

[21] I. J. Cox and J. P. Linnartz. Some general methods for tempering with watermarks [J]. IEEE J. Select. Areas Commun., May 1998, 16: 587 – 593.

[22] S. Craver, N. Memon, B.-L. Yeo, and M. Yeung. Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks andimplications [J]. IEEE J. Select. Areas Commun. May 1998, 16: 573 – 586.

[23] T. Leighton, I. J. Cox, J. Kiliant, and T. Shamoon. Secure spread spectrum watermarking for images, audio and video [A]. in Proc. ICIP '96, Lausanne, Switzerland, Sep. 1996, III: 243 – 247.

[24] Y. Linde, A. Buzo, and R. M. Gray. An algorithm for vector quantizer design [J]. IEEE Trans. Commun. 1980, 28(1): 84 – 95.

[25] Z. M. Lu and S. H. Sun. A digital image watermarking technique based on vector quantization [J]. Electronics Letters, 36(4): 303 – 305.

作者简介:

孙圣和 现任哈尔滨工业大学自动化测试与控制系教授,博士生导师.中国电子学会会士.他已经发表了 5 本著作和 150 多篇文章.并多次获得国家级和省部级科技成果奖.目前的研究领域包括计算机自动测试与控制,信号处理和系统辨识.

陆哲明 1974 年出生,1995 年和 1997 年获得哈尔滨工业大学学士学位和硕士学位,现为哈尔滨工业大学自动化测试与控制系博士研究生.目前主要致力于图像处理研究.