

## 易损数字水印若干问题的研究

华先胜<sup>1)</sup> 石青云<sup>2)</sup>

<sup>1)</sup>(北京大学数学科学学院信息科学系, 北京 100871)

<sup>2)</sup>(北京大学信息科学中心视觉与听觉处理国家重点实验室, 北京 100871)

**摘 要** 易损数字水印算法可用于多媒体内容真实性的保护, 为更有效地设计和使用易损水印, 首先通过研究其算法应具有的特点及易损水印与鲁棒水印的差别; 然后在可信赖的数码相机这个应用背景的基础上, 提出了一个简单的易损水印应用框架; 最后, 讨论了变换域易损图象数字水印算法的误差问题和逆变换后象素值溢出的问题, 同时给出了两种解决方法, 并利用此方法对一种基于小波变换的易损水印算法做了改进.

**关键词** 数字水印 易损水印 认证

**中图分类号:** TP309.7 TP391.4 **文献标识码:** A **文章编号:** 1006-8961(2001)11-1089-07

## Research on Fragile Watermarking Problems

HUA Xian-sheng<sup>1)</sup>, SHI Qing-yun<sup>2)</sup>

<sup>1)</sup>(School of Mathematical Sciences, Peking University, Beijing 100871)

<sup>2)</sup>(National Laboratory on Machine Perception, Center for Information Sciences, Peking University, Beijing 100871)

**Abstract** In this paper, we discuss several problems on fragile watermarking, which is used to ensure the credibility of multimedia. Firstly, we describe some main properties that an efficient fragile watermarking scheme should have. And then we discuss the differences between robust watermarking and fragile watermarking algorithms, which are important for us to develop efficient fragile watermarking scheme. Thirdly, a simple application framework for fragile watermarking, which is called trustworthy digital camera, is proposed. This fragile watermarking framework can be used for ensure facticity for images taken by digital camera. In the end, we present two approaches, pre-processing and using integer transform, to solve round-off error and overflow error problems for frequency domain fragile watermarking techniques. Experimental results show that these two approaches are efficient for improving other fragile watermarking algorithms.

**Keywords** Watermarking, Fragile watermarking, Authentication

## 0 引 言

随着多媒体技术和网络技术的飞速发展及广泛应用, 对图象、音频、视频等多媒体内容的保护已成为迫切需要解决的问题. 大家知道, 对多媒体内容的保护一般可以分为如下两个方面: 一是版权保护; 二是内容完整性(真实性)保护, 即认证(或称为“篡改提示”). 其中, 对于内容完整性保护, 由于传统的加

密方法对内容的保护只局限在加密通信的信道中或其他加密状态下, 因此其一旦解密, 则毫无保护可言; 而且密码学中的数据完整性的认证方法对多媒体内容的保护也无能为力; 这一方面是由于多媒体内容的真实性认证往往需容忍一定程度的失真, 而密码学中的认证方法却不容许一个比特的改变; 另一方面是由于用于多媒体认证的认证信息往往需要直接嵌入到多媒体内容当中, 不另外保存, 而密码学中的认证方法则需另外保存信息认证码(MAC). 由

基金项目: 国家重点基础研究发展规划资助项目(G1998030606)

收稿日期: 2000-03-28; 改回日期: 2000-12-22

于密码学对多媒体内容保护能力的局限,因此一种新的保护途径应运而生,即数字水印技术,它甚至被认为多媒体内容保护的最后一道防线<sup>[1]</sup>.

所谓数字水印技术就是将多媒体内容相关或不相关的一些标示信息直接嵌入到多媒体内容当中,但不能影响原内容的使用价值,并且要求不容易被人的知觉系统觉察或注意到.通过这些隐藏在多媒体内容中的信息,就可以达到确认内容创建者、购买者,或者内容是否真实完整的目的.

用于版权保护的数字水印一般称为鲁棒水印(Robust Watermarking),利用这种水印技术即可在多媒体内容的数据中嵌入创建者、所有者的标示,或者嵌入购买者的标示信息(即序列号).在发生版权纠纷时,创建者或所有者的信息用于标示数据的版权所有,而序列号用于追踪违反协议而为盗版提供多媒体数据的用户.一般来说,用于版权保护的数字水印要求有很强的鲁棒性和安全性,即除了要求在一般图象处理(如:滤波、加噪声、替换、压缩等)中生存外,还需能抵抗一些恶意攻击<sup>[2]</sup>.虽然鲁棒水印是目前研究的热点,但离实际应用尚有较远距离.用于多媒体内容真实性鉴定(或篡改提示)的水印一般称为易损水印(Fragile Watermarking),这种水印同样是在内容数据中嵌入不可见的信息.由于当内容发生改变时,这些水印信息会发生相应的改变,因此可以用来鉴定原始数据是否被篡改.另外,这种易损水印也应对一般图象处理(如:滤波、加噪声、替换、压缩等)有较强的免疫能力(鲁棒性),同时又要有较强的敏感性,即,既允许一定程度的失真,又要能将失真情况探测出来.

数字水印还有其他用途,如:在多媒体内容中嵌入说明信息的注释水印、隐藏通信收发双方及通信过程存在性的隐蔽通信等<sup>[1]</sup>.本文讨论的是易损数字水印中的若干问题.

## 1 易损数字水印算法应具有的特点

### 1.1 易损数字水印简介

易损数字水印包括:

#### (1) 嵌入水印

设原始数据为  $I$ , 通过适当算法在  $I$  中嵌入信息(水印)  $w$ , 得到  $I'$ , 其中, 若  $w$  与原始数据相关, 则嵌入水印后的数据  $I'$  可以表示为<sup>[1]</sup>:

$$I' = I \oplus f(I, w)$$

这里要求  $I$  和  $I'$  在人的知觉上没有明显差别, 并且没有损坏  $I$  的使用价值(嵌入水印的流程如图1所示).

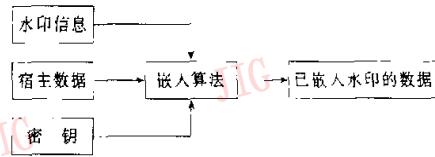


图1 嵌入水印流程

#### (2) 检测认证

检测时, 要求仅仅通过  $I$  的一个可能修改过的版本  $I''$ :

$$I'' = I' \oplus n(I') = I \oplus f(I, w) \oplus n(I')$$

或者再加上水印信息  $w$ , 即可判断  $I''$  是否与  $I'$  相同, 而不必利用关于  $I$  或  $I'$  的其他任何信息; 如果不完全相同, 还需指出其差别所在(检测水印的流程如图2所示).

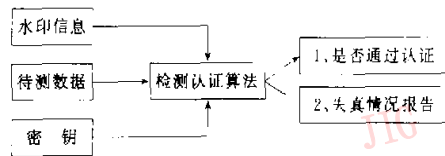


图2 检测水印流程

在实际应用中, 一般还有密钥参与运算, 而且往往将水印信息或其参数(如伪随机噪声的参数)作为密钥的一部分.

### 1.2 易损数字水印算法的特点

易损数字水印算法一般要求有以下特点:

#### (1) 直接嵌入多媒体的内容当中

早期用于多媒体认证的算法多借鉴密码学中的方法, 一般是利用一个 Hash 函数来生成一个信息认证码, 但此认证码需另外存储<sup>[4]</sup>. 这种方法有如下3个弱点: 其一是增加了存储空间; 二是原始数据与认证码分离存放, 不便管理; 三是这种方法不容许一个比特的失真, 而且也难以探测失真情况. 而基于数字水印的认证算法, 由于是直接认证信息嵌入到多媒体内容之中, 因此既不需要另外的存储空间, 还能够探测到原始数据一定程度的失真情况.

#### (2) 不易觉察, 不损坏原始数据的使用价值

在多媒体内容嵌入水印之后, 人的知觉系统很难感觉到或注意到与原始数据的差别, 即水印需要具有“透明性”, 而且不能损害数据的使用价值.

#### (3) 检测认证时, 不需要原始数据

用于版权保护的鲁棒水印在一些应用背景下,检测时,允许使用需要原始数据的私有水印算法<sup>[2]</sup>,但对于易损数字水印而言,则必须设计不需原始数据即能检测、认证的算法,这一方面是由于,易损水印是用来保护多媒体内容真实性的,如果能确知原始数据,就不存在真实性保护问题了;另一方面,一些应用背景下根本没有原始数据,如可信赖的数码相机,为保证照片的真实性,就需要在拍摄成象时自动嵌入水印,否则无法实现真实性的鉴定(参见本文第 3 节)。

#### (4) 安全性

一个数字水印系统要走向商业应用,一般来说,其算法应该公开,以便使得算法的安全性完全依赖于密钥,而不是通过对算法进行保密来取得安全性,这就要求算法的密钥空间需足够大,且分布比较均匀。另外,易损水印算法还需能抵抗“伪认证”攻击(参见本文第 2 节)。

#### (5) 鲁棒性

多媒体数据经过一定强度的滤波、加噪声、压缩等处理,且通过检测程序进行检测认证后,其得到的是数据完整性(真实性)程度,而不只是“通过认证”或“不通过认证”两种结果。

在实际应用中,有时需要更强的鲁棒性,如数字图象分辨率的改变、图象旋转,以及只有部分图象等,在这些情况下,仅根据这些变化后图象来探测其失真情况,难度较大,但新一代基于特征的数字水印方案可望解决这些问题<sup>[3]</sup>。

#### (6) 标示能力

对于待测数据有失真的情况,检测算法能指明失真的区域,甚至指明频域上的失真情况、分析造成失真的原因等。

## 2 易损水印与鲁棒水印的差别

由于易损水印在很多方面与鲁棒水印有较大差别,因此在设计易损水印算法和应用框架时,需充分考虑到这些差别。

#### (1) 目的不同

因为判断数据的失真情况是易损水印的目的,所以易损水印并不注重嵌入了多少数据,而只注重在安全的前提下尽可能地报告失真情况。当然,一般来说,嵌入的信息越多,越有利于失真情况的报告。

#### (2) 易损水印算法需要有标示能力

要求算法不仅能检测到水印,而且对于数据有失真的情况时,检测算法还要能指明失真的区域,甚至能指明频域上的失真情况,并能分析造成失真的原因。

#### (3) 易损水印更注重不影响原数据的使用价值

因为易损水印是用来保护多媒体内容真实性的,所以它比鲁棒水印更注重嵌入水印对原始数据在知觉上的影响程度,即要求不仅不易觉察,还应不损坏原始数据真实性及其使用价值。

#### (4) 必须设计不需原始数据即能进行检测、认证的算法

如本文第 1 节中所述,易损水印必须设计为公开水印算法,即检测水印时,不需要知道嵌入水印前的原始数据。

#### (5) 易损水印对舍入误差和象素值溢出敏感

嵌入水印的运算,特别是变换域的水印算法,往往会带来舍入误差,而且变换域水印算法在逆变换时会产生象素值溢出的现象,在鲁棒水印算法中,如果算法鲁棒性较好,则一般可忽略这些误差和溢出情况的影响;但对于易损水印,溢出和误差将会造成嵌入水印的图象,在未经篡改的情况下,就出现不能完全通过认证的现象(参见本文 4 节)。

#### (6) 攻击上的差别

鲁棒水印需要抵抗的攻击可分为基本攻击、鲁棒攻击、表示攻击、解释攻击、实现过程中的攻击等<sup>[4]</sup>,而易损水印要防止的攻击则与此完全不同,它不需要抵抗上述攻击,只需要抵抗“伪认证”攻击,因为对易损水印的攻击不是将水印信息去掉或使其不能被检测到,而只是设法篡改多媒体的内容却不损坏水印信息,也就是使多媒体的内容发生改变后,仍然能通过认证,如 Deepa Kundur 的基于小波的易损水印算法,如果不采用“量化密钥”,则根据一幅已嵌入易损水印图象的数据,即可使任意一幅与其尺寸相同的图象完全通过认证<sup>[5]</sup>。

## 3 一个简单的易损水印应用框架

在实际应用中,仅有算法还不能完全解决问题,往往需要一系列对应的措施才能真正实现保护多媒体内容的目的。下面以可信赖的数码相机为应用背景,提出一个简单的易损水印应用框架。

由于数字图象很容易编辑、处理,因此,数字照片的真实性成为大家十分关心的问题,例如新闻照

片、用于法庭作证的照片等。目前,数码相机生成的照片之所以在法律上没有效力,也是因为不能鉴定其真实性的缘故,因此文献[4]中Friedman提出了一种基于数字签名的方法,用来确认数码相机照片的真实性。此方法是利用公开密码体制,再通过相机中的私有密钥来生成图象的数字签名,作为另一文件保存,与图象一同发行。这样普通用户通过公开密钥,再结合图象文件及其数字签名文件,即可验证图象的真实性,但这种方法也具有前文提到的3个缺点,即增加了存储空间、不便管理数字签名信息、不容许一个比特的失真,并且不能探测失真情况。

如果能够利用数字水印技术,在数码相机生成数字照片的同时,在其内容中嵌入易损水印,则可望更好地解决其真实性鉴定的问题。下面的一个简单的应用系统正是针对这个问题提出来的,在该方案中,认证信息直接嵌入照片内容中,不需另外存储;而且,由于易损数字水印对一般图象处理具有一定的鲁棒性,并能在一定程度上(视算法优劣而定)探测失真情况,从而使得照片真实性的认证具有更大的灵活性和实用性。

### 3.1 易损水印应用系统框架需要解决的问题

数码相机易损水印应用系统框架需要解决如下问题:

- (1) 图象创建者能否证明图象真实性?
- (2) 除图象创建者外的其他人员能否验证图象的真实性?
- (3) 图象创建者能否“作弊”,即制造“伪认证”?
- (4) 除图象创建者外的其他人员能否制造“伪认证”?

系统框架在实际应用中时,还应决定如下问题:

- (1) 水印嵌入由谁完成?
- (2) 密钥由谁选择?
- (3) 密钥由谁保管?
- (4) 认证由谁完成?

### 3.2 易损水印应用系统框架的实现

本文提出的应用框架涉及4个参与者:

- (1) 摄影者:图象创建者;
- (2) 认证中心:为摄影者提供真实性证明、为验证请求者验证真实性的公证单位;
- (3) 验证请求者:除摄影者外的其他提出验证照片真实性的人;
- (4) 水印模块:数码相机中固化的用来嵌入易损水印的模块。

整个系统按如下方式实现:

(1) 水印的嵌入由固化在相机中的水印模块完成,摄影者无法修改、窥测水印模块中的固有信息;在相机成象的同时,易损水印即自动嵌入(图3);

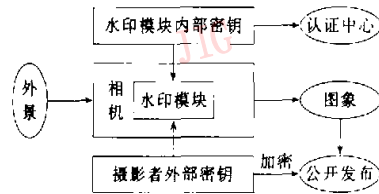


图3 水印嵌入流程

(2) 密钥分为两部分(图4);其一为“水印模块”制造者固化在模块当中的密钥,交认证中心保管,其他任何个人,包括摄影者在内都无法得知此密钥,本文称之为水印模块内部密钥;另一部分为水印模块的标志信息和摄影者选择的水印信息,以及其他由摄影者决定的信息(例如图象尺寸,也可以不要这一部分信息),称为摄影者外部密钥;

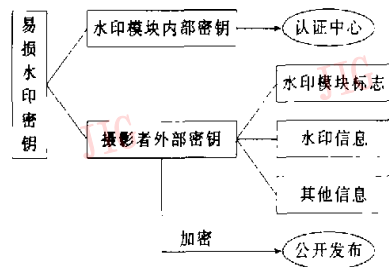


图4 密钥的组成和管理

(3) 摄影者发布图象的同时,公开发布所用外部密钥的加密版本。这种对摄影者外部密钥的加密可由水印模块完成,也可在外部完成,但要保证认证中心可解密;

(4) 认证时,由摄影者或其他验证请求者提交图象和被加密后的摄影者密钥(即在摄影者公开发布照片的同时发布的密钥),交认证中心;认证中心将提交的摄影者外部密钥解密,根据其中的水印模块标志,选择相应的水印模块内部密钥,并结合外部密钥中的其他信息来验证图象的真实性,并给出失真情况报告(图5)。

在此系统中,由于摄影者公开了所用外部密钥的加密版本,所以任何人都可以提交验证请求。而且,由于摄影者和其他验证请求人都无法得知水印模块内部密钥,所以都无法制造“伪认证”。

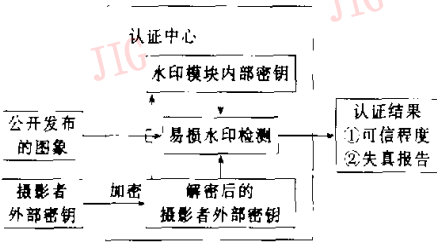


图5 认证过程

### 3.3 几点讨论

#### (1) 使用多组水印模块内部密钥

为加强安全性,可在水印模块中设置多组内部密钥,摄影者可选择其中之一,这样摄影者外部密钥中却需要包含所选内部密钥的编号。

#### (2) 摄影者外部密钥的其他保管方案

如果摄影者不公开所用外部密钥,虽可使照片的发布更简单,但却使认证过程更复杂,因为验证请求者需要通过摄影者提交外部密钥才能进行认证,而且,这种方式在实际应用中还有其他缺陷,如:验证请求者无法保密他的验证企图,但是,如果能够在嵌入易损水印的同时或之前,嵌入一个鲁棒水印,并将其用来存放水印模块的标志和内部密钥的编号,则摄影者就不必选择、保管、公布外部密钥,从而使认证更方便。

#### (4) 使用密码学中的方法

水印模块内部密钥的产生、存储,摄影者外部密钥的加密,以及验证请求者与认证中心的通信中的安全问题可用密码学中已有的方法解决。

#### (5) 摄影者外部密钥的加密

摄影者外部密钥的加密可用如下两种方法:其一是使用对称密钥体制,即水印模块和认证中心使用相同的加密、解密密钥;二是采用非对称密钥体制(公开密钥体制),即水印模块用摄影者的私有密钥来加密(由摄影者输入密钥),而认证中心利用摄影者的公开密钥解密;或者水印模块用认证中心的公开密钥加密,认证中心用自己的私有密钥解密。

## 4 舍入误差及溢出问题的处理

前文提到,易损水印算法对计算中的舍入误差及象素值溢出较为敏感,下面将针对变换域的水印算法提出两种解决舍入误差和象素值溢出问题的方案,并将这两种方法试用于文献[6]中的易损水印算法。

### 4.1 预处理

一般说,嵌入易损水印后,各象素值虽变化不大,但是由于对于接近象素值取值范围边界的象素可能会产生象素值溢出现象,如在 256 级灰度图象中,象素值在 0 附近和在 255 附近的点容易产生溢出现象,因此,如果在嵌入水印前,采用线性映射的方法,将  $[0, 255]$  范围内的点重新映射到  $[l, h]$ , 其中  $5 \leq l < h \leq 250$ , 则能避免溢出的出现,即

$$\tilde{p} = (h-l) \frac{p}{255} + l$$

其中,  $p$  和  $\tilde{p}$  分别表示映射前后的象素值。当然,由于灰度值在 0 和 255 附近的象素个数一般比较少,也可以采用直接对这些点的值进行重新设置的方法,如在 256 级灰度图象中,可将象素值限制在  $[5, 250]$  范围内,即将象素值在 5 以下的点均修改为 5, 而将象素值在 250 以上的点修改为 250。

根据此想法,对文献[6]中 Deepa Kundur 的算法增加预处理过程,达到了预期的效果,算法中采用 Haar 小波,在大小不同的图象 Lena、Benz、Mandrill 和 Girl 图象(图 6)中,以量化强度  $\Delta=1$  分别嵌入 5 000、10 000、20 000 bits 的信息,如果采用预处理(用线性映射的方式,预处理范围均为  $[5, 250]$ )的方法,对已嵌入水印的图象,在未作其他修改的情况下检测水印,均没有检测到失真的比特,而且几乎没有带来视觉上的影响(见表 1~3)。

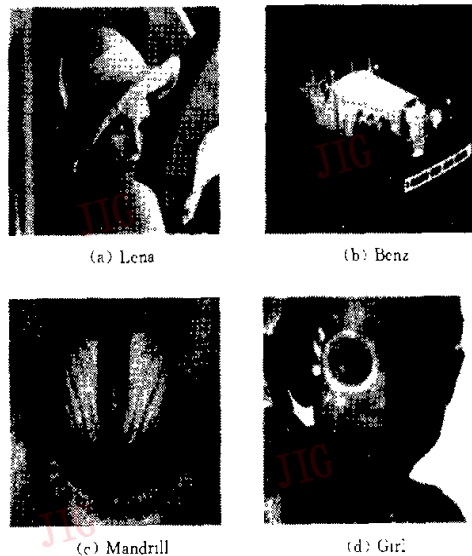


图6 原始图象

表1 Deepa算法“预处理”前后的比较(1):嵌入5 000 bits 水印

	失真比特数(bit)		PSNR(dB)		MSE	
	Deepa	改进后	Deepa	改进后	Deepa	改进后
Lena	6	0	45.510	45.286	1.828	1.925
Benz	4	0	45.589	44.740	1.796	2.183
Mandrill	1	0	45.771	45.421	1.722	1.865
Girl	18	0	45.638	44.285	1.776	2.424

表2 Deepa算法“预处理”前后的比较(2):嵌入10 000 bits 水印

	失真比特数(bit)		PSNR(dB)		MSE	
	Deepa	改进后	Deepa	改进后	Deepa	改进后
Lena	6	0	43.770	43.636	2.729	2.815
Benz	7	0	43.794	43.226	2.715	3.094
Mandrill	2	0	43.965	43.891	2.610	2.765
Girl	38	0	43.866	42.864	2.670	3.363

表3 Deepa算法“预处理”前后的比较(3):嵌入20 000 bits 水印

	失真比特数(bit)		PSNR(dB)		MSE	
	Deepa	改进后	Deepa	改进后	Deepa	改进后
Lena	2	0	42.561	42.437	3.606	3.710
Benz	12	0	42.531	42.151	3.614	3.963
Mandrill	6	0	42.653	42.494	3.522	3.662
Girl	72	0	42.637	41.852	3.543	4.245

#### 4.2 采用整形变换

设原始图象为  $I$ , 将其做小波变换(或 DCT 变换等)后的系数记为  $T$ ; 将因嵌入水印而做部分修改后的系数记为  $\tilde{T}$ ; 将  $\tilde{T}$  再做逆变换后所得到的图象记为  $I'$ ; 将图象  $I'$  再做小波变换所得到的系数记为  $\tilde{T}'$ . 由于图象做小波变换后的系数一般是浮点数, 如果不修改系数, 再做反变换, 则得到与原图相同的结果, 但是, 由于嵌入水印需修改部分变换域系数, 这样再做反变换后的结果可能不再是整数, 因而产生舍入误差, 而经舍入后的像素值, 如再重新做变换, 其所得到的系数将不再与第 1 次因嵌入水印而修改后的系数相同, 即  $\tilde{T}' \neq \tilde{T}$ .

为解决这个问题, Deepa 在文献[6]中采用 Haar 小波, 并将嵌入水印时的系数改变量定为  $\Delta \times 2^i$  的形式. 由于 Haar 小波变换的特点, 小波系数减少或增加  $\Delta \times 2^i$  后, 其逆变换的结果仍为整数, 从而不存在舍入误差. 但是, 这样处理却限制了可选择小波的种类. 其实, 如果采用整形小波变换, 就可以解决此问题, 因为只要嵌入水印时, 小波系数的改变量为整数, 且逆变换时, 没有像素值溢出, 就不会出现舍入误差,

从而这时  $\tilde{T}' = \tilde{T}$  是成立的. 另外, 对于 DCT 域的方法, 也可以采用 DCT 变换的整数形式.

实验中, 本文是采用提升的方法来实现(9-7)小波的整数形式变换<sup>[7]</sup>的. 从实验结果看, 预处理范围为  $[5, 250]$ , 采用(9-7)小波(为对比, Deepa 的算法也采用此小波), 不仅可有效地减少舍入误差的影响, 而且视觉上带来的损失也很小(见表4). 如果希望将失真比特数减小到 0, 则可以进一步调整预处理范围, 例如对于 Benz 和 Mandrill 图象, 在预处理范围分别为  $[7, 250]$  和  $[6, 250]$  时, 其失真比特数均减小到 0. 实际上, 还可以通过统计原图中像素值靠近 0 和 255 的像素点的个数或比例, 来估计能将失真比特数减小至 0 的预处理范围. 也可通过对嵌入后的图象进行检测尝试, 来逐步改变预处理范围, 直到失真比特数减小至 0 为止.

表4 选用(9-7)小波时, Deepa算法采用整型变换前后的比较(嵌入5 000 bits 水印)

	失真比特数(bit)		PSNR(dB)		MSE	
	Deepa	整型变换	Deepa	整型变换	Deepa	整型变换
Lena	265	0	44.623	41.938	2.213	4.162
Benz	885	3	44.339	41.662	2.394	4.435
Mandrill	248	2	44.540	41.773	2.286	4.323
Girl	295	0	43.142	40.870	3.151	5.322

## 5 总 结

本文探讨了有关易损数字水印的几个问题, 包括算法要求、易损水印与鲁棒水印的区别, 以及结合数码相机这个实际应用背景等问题, 提出了一个简单的易损水印应用框架; 最后还具体讨论了易损水印算法舍入误差和溢出问题的处理, 并提出了两种有效的解决方案, 可用于改进其他的变换域易损水印算法.

### 参 考 文 献

- Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding - a survey[J]. Proceedings of the IEEE, 1999, 87(7): 1062~1078.
- Petitcolas F A P, Anderson R J, Kuhn M G. Attacks on copyright marking system [A]. In: Second International Workshop on Information Hiding 'C., Portland, Oregon, U. S. A., April 14-17, 1998. Published in: Lecture Notes in Computer Science[J], 1998, 1525:218~238.
- Cox I J, Miller M L. A review of watermarking and the importance of perceptual modeling[J]. Proc. SPIE Conf. on Human Vision and Electronic Imaging, 1987, 3016:92~99.

4. Friedman G L. The trustworthy digital camera: restoring credibility to the photographic image [J]. IEEE Trans. on Consumer Electronics, 1993, 39(10):905~916.

5. Kutter M, Bhattacharjee S K, Ebrahimi T. Towards second generation watermarking schemes [A]. In: Proceedings 6th International Conference on Image Processing (ICIP'95) [C], Kobe, Japan, October 24-28, 1999, 329~323.

6. Kundur Deepa, Hatzinakos Dimitrios. Digital watermarking for telltale tamper-proofing and authentication [J]. Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Information, 1999, 87(7):1167~1180.

7. Calderbank A R, Daubechies I, Sweldens W *et al.* Wavelet transforms that map integers to integers [J]. Applied and Computational Harmonics Analysis, 1998, (5):332~369.



华先胜 1973 年生, 2001 年获北京大学数学科学学院信息科学系理学博士学位, 现为微软中国研究院 (Microsoft Research China) 副研究员, 研究兴趣为图象处理、数字水印、模式识别、视频处理与分析等。



石青云 1936 年生, 中国科学院院士, 北京大学数学科学学院教授、博士生导师, 北京大学信息科学中心学术委员会主任, 视觉与听觉信息系统国家实验室学术委员会主任, 主要研究领域为模式识别、图象视频编码等。

## 《中国图象图形学报》文后参考文献编排格式

### 1. 专著、论文集、学位论文、报告

[序号] 主要责任者. 文献题名 [文献类型标识]. 出版地: 出版者, 出版年. 起止页码.

- 1 刘国钧, 陈绍业, 王凤. 图书馆目录 [M]. 北京: 高等教育出版社, 1957: 15~18.
- 2 张筑生. 微分半动力系统的不变集 [D]. 北京: 北京大学数学系数学研究所, 1983.

### 2. 期刊文章

[序号] 主要责任者. 文献题名 [J]. 刊名, 年, 卷 (期): 起止页码.

- 1 金显贺, 王昌长, 王忠东等. 一种用于在线检测局部放电的数字滤波技术 [J]. 清华大学学报 (自然科学版), 1993, 33(4): 62~67.

### 3. 论文集集中的析出文章

[序号] 析出文献主要责任者. 析出文献题名 [A]. 见 (In): 原文献主要责任者 (任选). 原文献题名 [C]. 出版地: 出版者, 出版年. 析出文献起止页码.

- 1 钟文发. 非线性规划在可燃毒物配置中的应用 [A]. 见: 赵玮. 运筹学的理论与应用——中国运筹学会第五届大会论文集 [C]. 西安: 西安电子科技大学出版社, 1996: 468~471.
- 2 Middleton V, Owen M J, Elliman D G *et al.* Development in non-axisymmetric filament winding [A]. In: Proceeding of 2nd International Conference on Automated Composite'88 Noordwijkerhout [C], the Netherlands, 1988: 324~335.

### 参考文献类型及标识

参考文献类型	专 著	论文集	报纸文章	期刊文章	学位论文	报 告	标 准	专 利
文献类型标识	M	C	N	J	D	R	S	P

### 电子文献类型参考文献标识

电子参考文献类型	数据库	计算机程序	电子公告
电子文献类型标识	DB	CP	EB

### 载体类型标识

载体类型	联机网络	磁带	光盘	磁盘
载体标识	OL	MT	CD	DK