用于图象认证的数字水印技术

张 静 张春田
(天津大学电子信息工程学院, 天津 300072)

摘 要 随着多媒体网络通讯技术的飞速发展,数字信息的安全维护问题日益突出.目前,采用数字水印技术(即脆弱性数字水印和半脆弱性数字水印)进行数字图象的真实性、完整性认证已成为信息认证领域的研究热点.为使国内广大科技人员能够较全面地了解数字水印图象认证技术的发展现状,给出了用于图象认证的数字水印系统的基本框架、性能要求及常见的攻击方法,介绍了现有的各种算法,分析和总结了各自的优缺点,并提出了下一步的研究方向.

关键词 计算机图象处理(520·6040) 数字图象认证 脆弱性数字水印 半脆弱性数字水印
中图法分类号: TP309.7 TP391.41 **文献标识码**: A **文章编号**: 1006-8961(2003)04-0367-07

Digital Watermarking Techniques for Image Authentication

ZHANG Jing, ZHANG Chun-tian
(*School of Electronic Information Engineering, Tianjin University, Tianjin* 300072)

Abstract The growth of networked multimedia systems has made digital data acquisition, exchange and transmission a simple task, but the ease of copying and editing also facilitates unauthorized use, misappropriation and misrepresentation, which makes it necessary to authenticate the multimedia data. At present, it has been a hotspot to authenticate digital images by the use of watermarking. According to the objectives of authentication, an image authentication system can be classified into complete verification and content verification. Watermarking for complete verification (known as fragile watermarking) considers image data as untouchable messages such that the data for authentication have to be exactly the same as the original. Content verification is a characteristic of multimedia data authentication. Watermarking for content verification (known as semi-fragile watermarking) considers "information preserving" image manipulations, such as compression and format conversion, as acceptable. This paper presents the general framework of digital watermarking for image authentication, discusses the fundamental demands and common attacks, introduces various existing algorithms and analyzes their advantages and disadvantages. The paper also introduces the current state of the techniques and proposes several research topics at next stage.

Keywords Computer imgae processing, Digital image authentication, Fragile watermarking, Semi-fragile watermarking

0 引 言

数字信息时代,以 Internet 为先锋的网络化浪潮为人们获取和交流信息带来了极大便利,然而,网络信息的全透明性和易操作性,却使得恶意攻击者可以轻易地对其进行篡改或伪造,由此可能造成极为严重的政治影响、经济损失.因此,如何在网络环境中进行有效的信息安全维护,已成为当前迫切需要解决的难题之一.目前,数字水印和数字签名两项技术已被应用于数字图象的真实性、完整性认证[1~4].基于数字签名的认证系统,一般是将签名与原始图象捆绑在一起存储或传输,但由于签名独立于图象数据而存在,因此其很容易被删除;而基于数字水印的认证系统则

基金项目:国家自然科学基金(69972032);天津市自然科学基金(013601311)
收稿日期:2001-08-16;改回日期:2002-08-15

将水印信息内嵌在原始图象中,水印信息与图象数据结合在一起,故水印不易被除去,而且数字水印技术还可以采用双水印系统(即脆弱性水印与鲁棒性水印相结合)对数字化产品进行多重目的的保护[1]. 在当今信息认证领域中,数字水印技术因其具有广阔的应用前景而日益为学界和商界所关注.

1 数字水印图象认证系统框架、性能要求及可能的攻击

1.1 用于图象认证的数字水印系统框架

用于图象认证的数字水印系统包括水印嵌入和图象认证两个过程,其基本框架如图 1 所示.

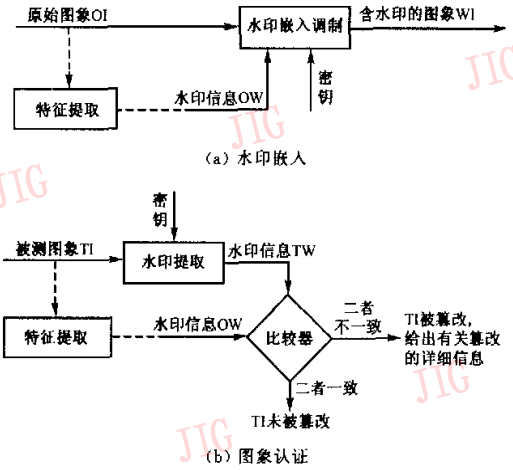

图 1 用于图象认证的数字水印系统框图

水印嵌入过程中,嵌入的水印信息可以是与原始图象内容相关的信息(如提取原始图象的内容或特征作为水印信息),也可以是与原始图象内容不相关的信息(如用密钥确定的 M 序列或标识创作者版权的二值商标图象等). 图象认证时,首先从被测图象中提取水印信息,将提取的水印信息与原始水印信息相比较,若二者一致,则认为图象未被更改;若二者不一致,则认为图象已被更改,并给出有关图象改动的详细信息. 若提取出原始图象的内容或特征作为水印信息嵌入图象,并确保水印的嵌入不会改变图象的这些内容或特征,则图象认证时,只需将提取的水印信息与被测图象的内容或特征进行比较,而不必再另外提供原始水印信息. 目前所存在的各类水印认证算法,其区别主要在于水印信息的生成和嵌入调制两个方面.

1.2 数字水印图象认证系统的基本要求

数字图象认证的基本目的是检测图象是否被恶意篡改或更换,一个有效的图象水印认证系统除应满足数字水印的不可见性、水印检测不需要原始图象外,一般还应具有如下特性:

(1)对篡改的敏感性

当图象受到不同程度的破坏或被恶意篡改后,系统应能做出相应反应,并能通过快速的检测算法对其真伪做出判断. 在大多数应用环境中,需要根据图象损害的性质或程度来决定是否需要重新传送原始图象,因此认证检测结果应能指示出被篡改图象的损害位置或估测出图象遭受了何种性质的更改.

根据具体认证目的不同,图象认证系统对篡改的敏感性要求也不尽相同[2]. 图象认证的具体目的可分为完全级认证和内容级认证两类. 完全级认证要求对图象的任何数据部分均不允许更改,检测器对图象任何轻微的改动都会做出拒绝判决;而内容级认证则是强调保护图象内容所传递的信息,而不是图象内容的具体表示方式,因此,对于任何保持图象内容的操作,如代码转换、格式转换、有损压缩、去除噪声等,检测器都应该认为是可接受的更动,而不会做出拒绝判决.

(2)安全性

系统应具有很强的抗非法破解能力,以免攻击者破译水印系统后非法复制、伪造水印图象,使得篡改后的图象依然能被检测器接受.

(3)可靠性

系统应具有较小的误检率和漏检率. 由于认证检测结果直接关系到图象的真伪及其所具有的价值大小,因此误检率和漏检率是评价认证系统性能的重要指标,确保检测的准确可靠应是认证系统设计的关键.

1.3 对数字水印图象认证系统可能实施的攻击行为

对数字水印认证系统的攻击与对鲁棒性水印系统的攻击完全不同,对鲁棒性水印进行攻击的目的是破坏或除去图象中的水印信息,使检测器最终检测不到原始的水印信息;而水印认证系统由于本身具有对破坏和篡改的敏感性,故用于鲁棒性水印的攻击手段对水印认证系统一般是无效的,水印认证系统需要抵抗的是"伪认证"攻击,即设法篡改图象的内容数据却不损坏水印信息,使得图象被恶意篡改或更换后,依然能通过认证. 目前,关于数字水印认证技术的攻击算法报道还较少,据已有的文献来

看,对水印认证系统可能实施的有效攻击有以下几种:

(1)统计分析[5]

当采用同一密钥在不同内容的图象上嵌入同样的水印信息时,攻击者可能会对大量的水印图象进行统计分析,从中寻找出水印存在的规律,进而对图象进行保持水印信息的篡改.

(2)重新嵌入水印[6]

这种攻击的实施方法有两类:一类是攻击者先破译水印的嵌入方案,然后在篡改后的图象上重新嵌入水印;另一类则是由于使用特定的设备嵌入水印造成的,如一些数字相机在摄取图象数据后会自动生成含有水印的图象,攻击者将篡改后的图象重新用数字相机摄入就可以实现对系统的攻击.

(3)拼贴攻击(collage-attack)[7]

该类攻击主要用于分块操作的水印认证算法,攻击者先搜集多幅采用同一方案嵌入水印的图象,然后在保持像块相对位置的同时,将属于不同图象的像块拼接起来形成新的、篡改后的图象.若攻击者在拼接像块的同时,又设法提高拼接图象的主观视觉质量,则该攻击模式对绝大多数分块操作的水印认证算法都是有效的.

2　数字水印图象认证技术

2.1　用于图象完全级认证的数字水印技术

用于图象完全级认证的数字水印一般采用脆弱性水印技术,脆弱性水印算法大都由空间域 LSB 水印算法演变而来.

Walton 提出的检查和(Checksum)算法[8]首先计算每个像素字节的最高 7 位的 Checksum 值(Checksum 值定义为一系列固定长度的二进制序列的模 2 和),算法在图象中随机选取固定数目的像素,将每个像素的最低有效位变成与对应的 Checksum 比特位相同,以完成水印的嵌入.图象认证时,只需检测图象的 Checksum 值与提取的水印信息是否一致即可.这种方法简单易行,但如果图象被篡改,该算法只能给出图象已被改动的信息,却不能指示图象的改动位置.

Yeung 和 Mintzer 将一个二值图象作为水印嵌入到原始图象中[9],算法利用伪随机发生器对图象的每一个颜色通道生成一个查找表来控制像素值的修改,水印嵌入完成后,再采用一个改进的误差扩散处理器将水印嵌入引起的视觉影响扩散开来,从而进一步提高了图象嵌入水印后的主观视觉质量.图象认证时,根据提取的二值水印图象是否完整来判断被测图象的真伪.该算法简单快速,易于硬件实现,是至今被研究较多的一种算法,但该算法的安全性取决于查找表的破译难度,若所嵌入的二值图象为已知信息,则算法的安全性将大大降低[5].即使不知道二值水印图象,也可以采用拚贴方法对其进行有效的攻击[7].

Wong 取一个与原始图象大小相同的二值图象作为水印信息[10],算法首先将原始图象与水印图象分成相同大小的对应块,对每个图象块进行操作,然后将根据最低有效位置零后的像素值得到的 Hash 结果与水印信息进行异或操作,把异或结果经私钥加密后嵌入在原始图象的最低有效位上.图象认证时,将最低有效位经公钥解密后,与最低有效位置零后像素的 Hash 值进行异或操作,若被测图象未被更改,则异或操作将会得到完整的二值水印图象;否则,将会得到破损的水印图象.该算法将密码学中的公开密钥体制引入到数字水印认证系统中,使得每一个图象接收者均可以进行认证检测,从而使得水印认证系统更加实用化.

基于 LSB 的水印算法经适当改进后,不仅可以用于图象的完整性认证,还可以用于破损图象的复原.

Fridrich 和 Goljan 对原始图象经 JPEG 量化后的 DCT 低频系数进行二进制编码,并把编码后的数据嵌入到图象的最低有效位[11].这种图象自嵌方法既可以用来进行图象认证,而且当图象破损后,还可以根据提取的水印信息近似地复原图象.Lee 和 Won 则采用差错控制编码技术对最低有效位置零后的图象像素值进行 RS 编码,把编码后的结果嵌入在原始图象的最低有效位上[12].这种算法不仅具有检错能力,还具有一定的纠错能力.

图象的完全级认证不允许对图象进行任何轻微的改动,而实际应用中,数字图象因其数据量较大,通常以压缩方式存储或传输;再者,由于图象处理软件各异,图象格式众多,故最终用户所要认证的通常是原始图象经有损压缩或其他保持图象内容的操作处理后的图象,因此,对图象进行内容级认证在现实生活中更为实用.

2.2　用于图象内容级认证的数字水印技术

用于图象内容级认证的数字水印系统属于半脆

弱性数字水印系统.根据所采用的具体技术不同,半脆弱性数字水印算法又可细分为以下几类:

(1) 与 JPEG 编码器、解码器相结合的半脆弱性数字水印算法

这类水印认证算法一般是根据 JPEG 编、解码器的特点而设计的,故算法通常对 JPEG 压缩具有较好的鲁棒性,而对其他的图象操作反应敏感.

Wu 和 Liu 提出了一个基于私有查找表的半脆弱水印算法[13].该算法首先提取图象的特征并结合一些自定义信息形成水印;然后构造一个私有查找表将 JPEG 量化后每个可能出现的 DCT 系数映射成 1 或 0,由此实现水印嵌入.检测器根据查找表提取水印信息与原始水印信息进行对照比较来判断图象的完整性.算法运行速度较快,也可应用于 MPEG 视频认证,而且还可与鲁棒性水印算法结合起来,以实现对图象进行版权保护和完整性认证的双重功能.

Noguchi 等人则用水印信息取代 JPEG 量化后的 DCT 高频系数[14],为确保水印的不易察觉性,在水印嵌入后,算法将一个修改后的量化表置于 JPEG 压缩码流的头文件中,解码时,首先采用修改后的量化表进行反量化,然后对解码后的图象再进行 DCT 变换,取出位于高频系数上的水印信息与原始水印信息进行比较来判断图象的完整性.但这种方法水印的嵌入量较少,而且篡改者可以通过改动 DCT 低、中频系数来实现对系统的攻击.

Lin 和 Chang 推导出数字图象经 JPEG 压缩编码前后,图象 DCT 系数上的两个不变特性[15],即:①当 DCT 系数被调整到某个量化等级 Q_H 的整数倍后,若采用小于 Q_H 的量化级进行 JPEG 压缩编码,则该 DCT 系数会被精确地恢复;②在 JPEG 压缩编码前后,一对编码块中两个对应 DCT 系数的相对大小关系是不变的.

他们用第 2 个不变特性生成水印信息,用第 1 个不变特性进行水印嵌入.算法允许图象在一定的范围内进行 JPEG 有损压缩编码,而对其他的恶意攻击做出反应,系统误检率为 0.但算法的局部检错能力不够理想.

(2)从鲁棒性水印算法演变而来的半脆弱性水印算法

该类算法主要是借鉴鲁棒性图象水印算法的一些经典方法(如扩频水印、提取图象重要特征生成水印等)来设计相应的认证算法,这样的认证算法一般具有比较全面的、适中的鲁棒性,更确切地应该称之为"半鲁棒性水印算法".

Fridrich 提出了一适用于数字相机的半鲁棒性认证算法[16],该算法从原始图象的每个 8×8 图象块提取具有一定鲁棒性的 m 位二进制信息,将提取的二进制信息和数字相机的 ID 以及该图象块的序号一起经扩频处理后嵌入在该图象块的 DCT 中频系数上.图象认证时,从被测图象中提取二进制信息经同样的扩频处理后,与提取的水印信息作相关运算,并对运算结果选取适当的门限来进行认证检测.该算法对恶意的图象篡改,如替换或添加图象特征能作出报警反应,对常见的图象处理操作,如 JPEG ($Q\geq55\%$)压缩、亮度/对比度调整、滤波、直方图均衡等都具有较好的鲁棒性.在文献[17]中,Fridrich 进一步给出了从原始图象中提取鲁棒性二进制信息的方法,该方法提取出的信息对常见的图象处理操作(包括旋转、缩放在内)都具有不变性.

Lin 等人在原始图象每个 8×8 图象块的 DCT 中频系数上叠加一个不同的伪随机序列[18],算法根据自然图象中一般平滑区较多,边缘区较少的特点,认为在没有边缘存在的情况下,图象相邻像素差值信号的能量主要是由水印嵌入引起的,该算法通过一个改进的相关运算来进行图象认证.对于 JPEG 有损压缩($Q\geq90\%$)后被篡改的图象,算法检测篡改区域的准确率为 90%左右,但图象边缘和纹理越多,算法的可靠性越差.Tefas 和 Pitas 提出了用二维混沌动态系统对二值水印信息进行扩频预处理,将预处理后的水印信息调制在原始图象的空间域或变换域;图象认证时,根据提取水印信息的正确率来判断图象的真伪[19].该算法较简单,水印嵌入位置由混沌映射控制,虽然不是基于分块操作,但也能够指示图象篡改位置.算法对于高质量的 JPEG($Q>90\%$)压缩具有鲁棒性.

Rey 和 Dujelay 则提取出图象的边缘特征作为水印信息嵌入到图象中,通过比较被测图象的边缘与所提取的水印信息是否一致来判断图象的真伪[20].该算法面临的一个问题是水印的嵌入可能会轻微改变图象内容,使得嵌入水印后的图象和原始图象的特征略有不同,从而导致系统误检率增大.为解决这个问题,算法在嵌入水印时,采用循环嵌入方式,即每次嵌入后都重新计算图象特征,直到满足要求为止.但这种算法并未给出是否任何原始图象和嵌入水印后图象的特征差异都能经这种循环嵌入方

法来消除.

(3)基于视觉掩模的半脆弱性水印算法

将人眼视觉掩盖模型应用于数字水印系统,往往会使嵌入水印后的图象具有更好的主观视觉质量.

Zhu 等人提出了一种基于图象空间域或频率域掩模的半脆弱性水印算法[21].该算法将每一图象块的像素用该块的视觉掩模量化后再反量化,而后将该块的视觉掩模与一伪随机序列相乘后,再与反量化后的像素叠加生成含水印的图象.在检测端,先求出被测图象的视觉掩模,再将求得的掩模与图象像素一起输入误差估测函数.这种方法能够准确检测出低于最大视觉可觉察门限 1/2 的图象改动.但由于视觉掩模人人皆可计算,所以算法的安全性主要还是依赖于产生伪随机序列的密钥,当用同一密钥生成多幅水印图象时,系统的安全性显然是不够的.

Lu 等人则对嵌入点的小波系数用对应于该点的视觉可觉察门限(JND)进行量化,对量化后的系数进行修改来实现水印嵌入,同时将原始水印信息存储起来[22].通过采用不同的检测方法,该算法既可用于进行图象版权保护的鲁棒性水印,也可用于进行图象认证的半脆弱性水印.图象认证检测时,若提取的水印信息与原始水印信息的差值超过该点的 JND 数值,则认为图象已被篡改.该算法用作图象认证时,必须存储原始水印信息.

(4) 基于量化图象小波系数的半脆弱性水印算法

由于小波变换在时域和频域均具有良好的局部定位性质,而且新出台的静止图象压缩标准 JPEG2000 是基于小波变换的,故小波域的数字水印认证技术也是当前的研究热点之一.

Xie 和 Arce 通过对图象小波系数进行非线性的排序变换来实现水印嵌入[23],这种非线性的排序变换实质上是对小波系数进行量化,即将位于不同范围内的小波系数分别量化成 1 或 0;同时还提出将这种水印算法与 SPIHT 压缩算法[24]结合起来,在编码端首先运行 SPIHT 算法,而后选择那些能够承受压缩的小波系数区进行水印嵌入,从而确保水印信息经 SPIHT 压缩后仍能成功地被恢复出来.

Kundur 等人采用与文献[23]类似的方法对图象的 Haar 小波系数进行量化,并根据量化步长来控制水印的鲁棒性[25],算法最后利用攻击估测函数将图象遭受的恶意篡改与 JPEG 压缩、中值滤波等保持图象内容的操作区分开来.

Yu 等人提出通过量化小波系数的加权平均值来嵌入水印[26],他们认为图象小波系数的变化近似服从高斯分布,对图象进行恶意攻击所导致的小波系数变化往往具有较大的方差,而由偶然因素造成图象失真引起的系数变化往往具有较小的方差,从而将恶意攻击与偶然失真区分开来.这种方法比直接量化单个小波系数具有更好的鲁棒性.

3　数字水印图象认证技术研究展望

随着网络通讯技术的迅速发展和多媒体数字产品的增多,对数字信息进行真实性和完整性认证变得日益紧迫和重要,其应用涉及电子政务、电子商务、国家安全、医院、司法、新闻出版、网络通信、科学研究、工程设计等各个领域.采用数字水印技术进行图象认证是一个方兴未艾的高新技术前沿课题,其迫切的市场需求和广泛的应用前景已吸引了众多的研究者投入到这一行列.但关于(半)脆弱性水印技术的研究目前尚处于初步阶段,在理论和实际成果方面还远不如鲁棒性水印技术那么成熟,还存在许多问题有待于深入研究.未来的水印认证技术应在如下几个方面进行探讨和研究:

(1)依赖于图象内容的水印认证算法的研究

采用基于图象内容的水印信息,既可以增强系统抵御统计攻击的能力,又避免了在认证检测端额外提供原始水印信息,而且由于图象内容一般对各类常用的图象处理操作具有鲁棒性,对恶意篡改具有敏感性,因此,这类依赖于图象内容的水印算法更适用于图象认证.目前在水印认证算法中,水印信息的生成大多与图象内容无关,虽有一部分算法采用了与图象相关的水印信息,但针对不同的应用,提取图象何种特征,生成的水印长度如何与宿主可容量相匹配,以及如何使水印的嵌入不引起图象特征发生变化,确保最终得到一个对篡改灵敏、视觉透明性好、抗攻击能力强并且局部检错能力高的水印认证系统,这些问题目前尚无令人十分满意的答案,所以在这些方面还需要进行更深入的分析和研究.

(2)水印认证技术与图象压缩编码算法的融合

由于数字图象通常经压缩编码后传输发布,故能抗有损压缩是图象内容级认证的主要要求.现有的水印认证算法大多与图象压缩算法是分离的,而如果能通过分析图象压缩编码的工作机理来寻找对

压缩有免疫力的图象信号特征,然后将这些特征作为水印信息在压缩编码过程中嵌入,那么这样的水印认证系统一般具有更好的可靠性,这一类的水印认证算法也最有希望被融入图象压缩标准.目前针对基于 DCT 变换的 JPEG 编、解码器设计的水印认证算法已有一些文献报道[13~15],但针对 JPEG2000 及其他的图象压缩编码(如矢量量化、分形编码等)的水印认证算法尚未见报道,相信这将会成为未来的一个研究热点.

(3)水印认证技术与公开密钥算法的结合

信息认证系统通常采用公开密钥体制,因为这样更符合实际应用需要.但目前绝大多数水印认证算法是基于私钥体制的,这就在一定程度上限制了水印认证系统的使用范围,也是数字水印认证技术不及数字签名认证技术实用的一个重要原因.因此,如何将密码学中的公开密钥算法融合到水印算法中,设计安全可靠的公钥水印认证算法,将是未来一个重要的研究方向.

(4)(半)脆弱性水印技术与鲁棒性水印技术的结合

目前,用于图象认证的(半)脆弱性水印算法与用于图象版权保护的鲁棒性水印算法一般是相互独立、自成体系的,如果既要对图象进行版权保护又要进行完整性检测时,则两套水印算法必须分别实施嵌入和检测,有时两套算法甚至可能是不兼容的,不能同时施用于图象.所以,如何将两者统一起来,实现对图象进行多重目的的保护,也是当前需要解决的问题之一.

(5)水印认证标准的建立

水印认证技术要得到广泛的应用,必须建立相应的标准,这包括水印嵌入标准、检测标准和系统功能测试标准(在注重研究水印认证算法的同时,还应重视对攻击方法的研究,这将有利于设计更安全可靠的水印认证系统),但标准的形成是一项艰巨的任务,需要综合考虑各个方面,以确保标准的通用性和有效性,这将有待于水印研究者的共同努力.

参 考 文 献

1 Dittmann J, Steinmetz A, Steinmetz R. Content-based digital signature for motion pictures authentication and content-fragile watermarking [A]. In: Proc. of the 6th IEEE International Conference on Multimedia Computing and Systems [C], Florence, Italy, 1999,2:209~213.

2 Lin C Y, Chang S F. Issues and solutions for authenticating MPEG video[A]. In:Proc. of SPIE[C], San Jose, CA, USA, 1999,3657:54~65.

3 Lin E T, Delp E J. A review of fragile image watermarks[A]. In: Proc. of the Multimedia and Security Workshop (ACM Multimedia'99) Multimedia Contents[C], Orlando, FL, USA, 1999:25~29.

4 Queluz M P. Authentication of digital images and video: Generic models and a new contribution[J]. Signal Processing: Image Communication, 2001,16(5):461~475.

5 Memon N, Shende S, Wong P. On the security of the Yeung-Mintzer authentication watermark[A]. In: Final Program and Proceedings of the IS&T PICS 99[C], Savanna, Georgia, 1999: 301~306.

6 Wu M, Liu B. Attacks on digital watermarks[A]. In: Proc. of the IEEE Record of the Asilomar Conference on Signals, Systems and Computers[C], IEEE, USA. 1999, 2: 1508~1512.

7 Fridrich J, Goljan M, Memon N. Further attacks on Yeung-Mintzer frigile watermarking scheme[A]. In: Proceedings of SPIE[C], San Jose, CA, USA, Jan. 2000,3971:428~437.

8 Walton S. Information authentication for a slippery new age[J]. Dr. Dobbs Journal, 1995,20(4):18~26.

9 Yeung M, Mintzer F. Invisible watermarking for image verification[J]. Journal of Electronic Imaging. 1998, 7(3): 578~591.

10 Wong P W. A public key watermark for image verification and authentication[A]. In: Proceedings of the IEEE International Conference on Image Processing[C]. Chicago, Illinois, USA, Oct. 1998,1:455~459.

11 Fridrich J, Goljan M. Images with self-correcting capabilities [A]. In: Proceedings of the IEEE International Conference on Image Processing[C]. Kobe, Japan, Oct. 1999,3:792~796.

12 Lee J, Won C S. A watermarking sequence using parities of error control coding for image authentication and correction[J]. IEEE Transactions on Consumer Electronics, 2000,46(2):313~317.

13 Wu M, Liu B. Watermarking for image authentication[A]. In: Proceedings of the IEEE International Conference on Image Processing[C]. Chicago, Illinois, Oct. 1998, 2: 437~441.

14 Noguchi Y, Kobayashi H, Kiya H. A method of extracting embedded binary data from JPEG bitstreams using standard JPEG decoder[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, 2000, E83-A (8):1582~1588.

15 Lin C Y, Chang S F. Semi-fragile watermarking for authentication JPEG visual content [A]. In: Proc. of SPIE Security and Watermarking of Multimedia Contents II[C], San Jose, CA, USA, Jan. 2000, 3971: 140~151.

16 Fridrich J. Methods for detecting changes in digital images[A]. In:Proc. of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems[C], Melbourne,

Australia, Nov. 1998, 173～177.

17 Fridrich J. Visual hash for oblivious watermarking[A]. In: Proceedings of SPIE[C], San Jose, CA, USA, Jan. 2000, 3971: 286～294.

18 Lin E T, Podilchuk C I, Delp E J. Detection of image alterations using semi-fragile watermarks[A]. In: Proc. of SPIE Security and Watermarking of Multimedia Contents II[C], San Jose, CA, USA, Jan. 2000, 3971: 152～163.

19 Tefas A, Pitas I. Image authentication using chaotic mixing systems [A]. In: Proceedings of the IEEE International Symposium on Circuits and System[C], Geneva, Switzerland, May 2000, 1: 216～219.

20 Rey C, Dujelay J L. Blind detection of malicious alterations on still images using robust watermarks[A]. In: IEE Secure Image Authentication colloquium[C], London, UK, Apr. 2000.

21 Zhu B, Swanson M D, Tewfik A H. Transparent robust authentication and distortion measurement technique for images [A]. In: Proc. of IEEE Digital Signal Processing Workshop[C], Loen, Norway, Sep. 1996, 45～48.

22 Lu C S, Liao H Y M. Multipurpose watermarking for image authentication and protection[J]. IEEE Transactions on Image Processing, 2001, 10 (10): 1579～1592.

23 Xie L, Arce G. Joint wavelet compression and authentication watermarking[A]. In: Proceedings of the IEEE International Conference on Image Processing[C]. Chicago, Illinois, Oct. 1998, 2: 427～431.

24 Said A, Pearlman W A. A new fast and efficient image codec based on set partitioning in hierarchical trees[J]. IEEE Trans. on Circuits and Systems for Video Technology, 1996, 6 (3): 243～250.

25 Kundur D, Hatzinakos D. Towards a telltale watermarking technique for tamper-proofing[A]. In: Proceedings of the IEEE International Conference on Image Processing[C]. Chicago, Illinois, Oct. 1998, 2: 409～413.

26 Yu G J, Lu C S, Liao H Y M *et al*. Mean quantization blind watermarking for image authentication[A]. In: Proc. of the IEEE International Conference on Image Processing [C], Vancouver, BC, Canada, 2000, 3: 706～709.

张　静　1972 年生,天津大学信号与信息处理专业博士研究生.主要从事数字图象处理与数字水印技术研究.

张春田　1939 年生,天津大学电子信息工程学院教授、博士生导师.从事数据压缩与编码理论、信息隐藏与数字水印、数字视频、HDTV 等方面研究.