基于脆弱性数字水印的图象完整性验证研究

宋玉杰 谭铁牛
(中国科学院自动化所,模式识别国家重点实验室,北京 100080)

摘 要 计算机网络技术的飞速发展与信息媒体的数字化,使得在网络环境中对数字产品实施有效的内容保护成为一个迫在眉睫的现实问题.传统的数字签名技术只是用于对通信领域的信息传送进行篡改检测,而脆弱性数字水印技术则为网络环境下多媒体的内容保护提供了一个有效的解决方案.与鲁棒性水印不同的是,脆弱性水印主要用于检测发生在多媒体数据中的篡改,并对其定位.为了推动我国在此前沿领域研究工作的进一步深入,这里就当前脆弱性数字图象图象水印技术的基本特征、一般原理、研究现状、攻击方法及发展方向进行一个综述.

关键词 脆弱性数字水印 真伪鉴别
中图法分类号: TP309.7 **文献标识码**: A **文章编号**: 1006-8961(2003)01-0001-07

A Brief Review on Fragile Watermarking Based Image Authentication

SONG Yu-jie, TAN Tie-niu
(*National Lab of Pattern Recognition Institute of Automation Chinese Academy of Sciences, Beijing* 100080)

Abstract Effective multimedia authentication is an increasing important issue in a networked environment. Fragile digital watermark thus come into being. Unlike traditional digital signature which is bounded with the content, fragile watermarking works effectively for multimedia content authentication by embedding a watermark (such as identification data, serials number, text or image etc.) to multimedia documents without influencing the vision or hearing effect of multimedia. Fragile digital watermarking is of great importance in courtroom defence, reliable e-business, medical image databases, etc. When the conetent of multimedia is suspected, the extraction of fragile watermark can be used to detect and localize tampers, even present the category of tampering. To motivate the relative research in this field, we attempt to give a brief overview of fragile digital watermarking into the context of image authentication in this paper. The basic characteristics of fragile watermarking is first outlined. Then comes the discussion of current algorithms, which not only includes basic schemes - spatial domain based algorithms and transform domain based methods, but also sums up the four typical types of fragile watermarking with different applications. Possible attacks and future research topics come in the following and future direction is outlined in the end. There still need a long way for fragile digital watermarking to go into standilization and actual applications.

Keywords Fragile watermarks, Image authentication

0 引 言

随着网络技术应用向各领域的渗透与信息媒体的数字化广泛应用,给人们带来了极大的好处与便利——它使得数字图象、音频和视频等数字信息产品的迅速传输成为可能,同时也带来了一系列问题,即使得恶意的个人或团体几乎不用任何努力就可以得到大量电子版形式的有版权的作品,并且可进行非常完美的复制,甚至可进行非法篡改及传播,这在音像、出版、影视和软件等行业已经引起了人们的广泛关注.如果不能对数字产品进行合理保护的话,那么数字产品的版权所有者与合法发行者就会限制数字信息产品在网络上的发行,而这就会阻碍全球范

基金项目:国家杰出青年基金(59825105)
收稿日期:2001-09-24;改回日期:2002-03-20

围电子商务的发展.因此如何在网络环境中,对数字产品实施有效的版权保护和内容保护已成为一个迫在眉睫的现实问题.

为了解决以上问题,以加强数字产品的版权保护与安全,必须解决以下 3 个问题:(1)作品的原创者可以驳斥任何其他宣称对该作品具有创作权(即版权所有问题)的言行;(2)由于创作者和版权所有者需要跟踪该作品的发行,因此他们必须能检测出任何试图非法的发行;(3)必须能够检测出对原作品进行相似性篡改的发行行为(即信息完整性的检测).关于多媒体的版权保护已有论文阐述[1],而多媒体内容的完整性认证,尤其是图象的完整性验证,是近几年来随着网络技术的发展而产生并发展起来的,当前的解决方案主要集中在脆弱性数字水印技术.为此,本文将重点介绍基于脆弱性数字水印技术的图象内容完整性验证的基本特征、一般原理、现有算法、鲁棒性问题与攻击行为及发展方向.

由于多媒体易于被修改,因此在其内容受到怀疑的时候,一个能够可靠验证篡改发生与否的真伪鉴别系统就显得非常重要[2].如在许多应用数据库的场合,所有者或授权者一般对于图象的真伪验证是感兴趣的,因为他们非常关心原有图象是否被修改过;如在医学数据库中,原有图象是否发生变化,对于诊断结果是非常重要的;又如在法庭上,不论是被告,还是原告的证人提供的作为证据的照片,由于法官判案是以事实为依据,因此必须保证这些照片的真实性,才能为正确地判案提供有力的证据;在新闻出版报刊杂志业,工作人员必须防止由恶意攻击者对所发表照片进行篡改而带来的损失;在网络上进行电子商务时,购买者必须能知道从销售者手中买的是真品.所有这些应用,都要求对多媒体信息的完整性与真伪性进行验证.

谈及多媒体内容完整性认证,首先应当提及的是,在保密通信中具有重要作用的数字签名技术.大家知道,在保密通信中,信息发送者是用其私钥,通过对所传内容进行加密运算来得到签名函数,由于发信者的私钥只有他本人才有,所以他一旦完成了签名,便保证了发信人无法抵赖曾发过该信息(即不可抵赖性).当信息接收者收到报文后,就可以用发送者的公钥对数字签名的真实性进行验证.经验证无误的签名电文,即确保信息报文在经签名后未被篡改(即完整性).数字签名尽管可以与所传内容一起存放,也可单独存放,但多媒体信息经过加密后,容易引起攻击者的好奇和注意,并有被破解的可能性,而一旦加密文件经过破解后,其内容就完全透明了;而且密文不允许有一点点的改动(甚至包括一般传输中的压缩),否则接收者无法恢复正确信息.在多媒体数据量如此巨大的今天,尽管压缩技术是为了提高传输的速度不得不采取的有效措施,但也可能造成有用信息破坏[3].而近年来发展起来的数字水印技术则克服了传统数字签名技术的缺点.所谓脆弱性数字水印技术就是在保证多媒体一定视(或听)觉质量的前提下,将数字、序列号、文字、图象标志等作为数字水印嵌入到多媒体数据中,当多媒体内容受到怀疑时,可将该水印提出用于多媒体内容的真伪鉴别,并且指出篡改位置,甚至攻击类型等.作为多媒体信息真伪鉴别的一个非常重要技术,数字脆弱水印的概念在国外始于 1994 年,而真正引起各国研究学者的关注则是在 1997 年.关于脆弱性数字水印的研究综述报告,在国外仅在 1998 和 1999 年分别有一篇[2,3],国内尚无报道.

1 脆弱性数字水印的基本特征

脆弱性数字水印作为数字水印的一种,除了具有水印的基本特征,如不可感知性、水印的安全、一定的鲁棒性外,还应能够可靠地检测篡改,并根据具体场合的不同而具有不同的鲁棒性,同时属于公开水印算法.它具有如下一些基本特征:

(1) 检测篡改　脆弱性水印最基本的功能就是能可靠地检测篡改,其理想的情况是能够提供修改或破坏量的多少及位置,甚至能够分析篡改的类型,并能对被篡改的内容进行恢复.

(2) 水印提取不需要原始图象　和鲁棒性水印相比,脆弱性数字水印可以很好地应用于一些特定的场合.比如对于可信赖的数码相机,在拍摄成像时,水印虽可被自动嵌入,但此时无法得到原始图象,而脆弱性数字水印的提取正好不需原始图象.

(3) 鲁棒性与脆弱性　水印的鲁棒性与脆弱性应随应用场合的不同而不同.如果用于版权保护,则希望水印足够鲁棒,并能承受大量的、不同的物理和几何失真,包括有意的(如恶意攻击)或无意的(如图象压缩、滤波、扫描与复印、噪声污染、尺寸变化等等)破坏,若攻击者试图删除水印,则将导致多媒体产品的彻底破坏;如果用于图象的内容篡改鉴别时,则希望水印是在满足一定鲁棒性条件下的脆弱,譬

如在许多应用场合,图象压缩就属于被容许的篡改,它要求水印能够在抵抗一定压缩下,同时还能检测出恶意的篡改.

(4) 不可感知性与感知性　同鲁棒性水印一样,在一般情况下,脆弱性数字水印也是不可见的.

(5) 水印安全和密码　一般来讲,一个脆弱性水印系统的算法是公开的,而水印的安全性又依赖于密钥,因此密钥的空间应该足够大.

2　一般原理和现有算法

脆弱性水印的添加与一般鲁棒性水印添加在原理上是基本相同的,而且从数字信号处理的角度可以看作是对原始图象的调制过程,但由于脆弱性数字水印要检测出篡改处,并定位,因此水印应先与图象的特征融合在一起,然后才能嵌入到图象中. 图 1 与图 2 分别示出了水印的添加与图象的完整性验证框图. 在脆弱性水印的添加过程中,首先根据要进行真伪鉴别的层次,对原始图象进行特征提取,为保证水印的定位功能与安全性,还需要将原始水印与提取出的特征及密钥,经嵌入运算得到实际要嵌入的内容,并以此取代原始图象中的特征,才能得到添加水印后的图象;水印提取时,首先对待检验的图象进行特征提取,然后根据相同的密钥,通过水印提取运算来提取出水印. 为了对篡改内容进行较好定位,有

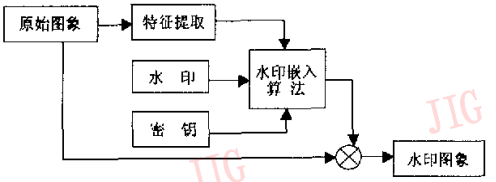


图 1　水印的添加过程

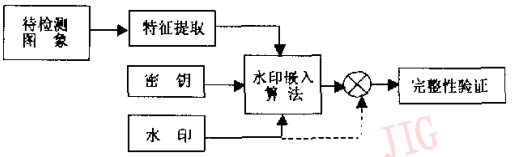
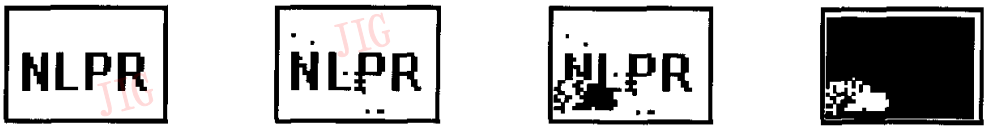


图 2　图象的真伪鉴别

时还需要与原始水印进行比较.

图 3 给出了一个脆弱性数字水印实现的例子,图 3(a)为原始图象,图 3(e)为水印,图 3(b)为嵌入水印后的图象,图 3(c)为被篡改的嵌入水印后的图象,图 3(f)为从图 3(b)中提取出的水印,图 3(g)为从图 3(c)中提取出的水印,图 3(h)为图 3(g)与图 3(f)的差值,图 3(d)为通过图 3(h)对篡改图象的定位. 需要指出的是,由于嵌入算法是在原图 8×8 大小的小块中嵌入一位水印,因此只能对原图 8×8 大小的块的篡改进行定位.

(a) 原始图象　(b) 嵌入水印后的图象　(c) 被篡改的嵌入水印后的图象　(d) 篡改部位标注



(e) 水印　(f) 从图 3(b)提取出的水印　(g) 从图 3(c)提取出的水印　(h) 图 3(g)与(f)的差

图 3　脆弱性数字水印实现的一个例子

从目前发表的文献[4]来看,根据识别篡改的能力可以将脆弱水印划分为以下 4 个层次:

(1) 完全脆弱性水印[5,6]　指的是水印能够检测出任何对图象像素值进行改变的操作或对图象完整性的破坏,如在医学图象数据库中,由于图象的一点点改动可能都会影响最后的诊断结果,因此此时嵌入的水印就应当属于完全脆弱性数字水印.

(2) 半脆弱水印[7~12]　在许多实际的应用场合

中,往往需要水印能够抵抗一定程度的有益的数字信号处理操作,如 JPEG 压缩等.这类水印可以比完全脆弱性水印稍微鲁棒一些,即允许图象有一定的改变,它是在一定程度上的完整性检验.

(3) 图象可视内容的鉴别[13] 在有些场合,由于用户仅仅对于图象的视觉效果感兴趣,也就是说,能够容许不影响视觉效果的任何篡改,因此此时嵌入的水印主要是对图象的主要特征进行真伪鉴别,即比前两类水印更加鲁棒.

(4) 自嵌入水印[14,15] 即把图象本身作为水印加入.这不仅可以鉴别图象的内容,而且可以部分恢复被修改的区域.如图象被剪掉一部分或被换掉一部分,就可以利用这种水印来恢复原来被修改的区域,但自嵌入水印可能是脆弱的或半脆弱的.

脆弱性水印按照实现方法的不同,又可分为空间域方法和变换域方法两类:

(1) 空间域方法[16~18]

最早的空间域方法是基于 LSB 的方法,即在图象最低有效位平面嵌入水印,然而,这种仅仅修改图象最低有效位的方法不仅对噪声非常敏感,而且容易被破坏掉,同时这种方法不能容忍对图象的任何修改.这种想法最早是在文献[19]中提到的.文献[20]对文献[19]的方法进行了改进,即水印的添加是通过在空间域中加入 M 序列,水印的检测是通过相关检测器实现的.在嵌入和检测过程中,由于使用了块结构,从而实现了对于篡改的定位.文献[6]中描述了另外一种脆弱性水印,该水印是针对图象的 7 个最高有效位及尺寸,通过密码学中的 Hash 函数运算来获得原始图象的某些特征,该特征与一有意义的二值水印图象可经过异或操作,并经公开密钥加密后,嵌入到图象中的最低有效位.当图象内容受到怀疑时,首先将图象的 7 个最高有效位与图象尺寸,经过 Hash 运算后,得到某些特征,然后将图象最低有效位公开解密后的结果与该特征进行异或操作后,就得到嵌入的水印模式.该算法具有定位特性,即从提出的水印可以非常直观地看出被篡改的区域.文献[5]中同文献[6]一样,也是在空间域嵌入了一个视觉上有意义的二值水印,即在嵌入水印之前,版权所有者可事先把要加水印的某些特征随机映射为 0 或 1,从而形成一个二维列表,即 LUT (Look-Up-Table),而水印的嵌入则是通过该 LUT 对空间域像素进行量化来实现的.对于文献[5],正如在文献[21]中指出的那样,该类技术的安全性是由推断 LUT 的困难程度决定的,如果知道二值水印的话,那么表入口的搜索空间就会大大减少,而在文献[21]中提出的基于位置的 LUT,则大大增加了搜索空间.必须指出的是,空间域的方法的优点是能够嵌入较多的水印,但非常易于被精心设计的攻击所攻破,即被"伪认证"通过.

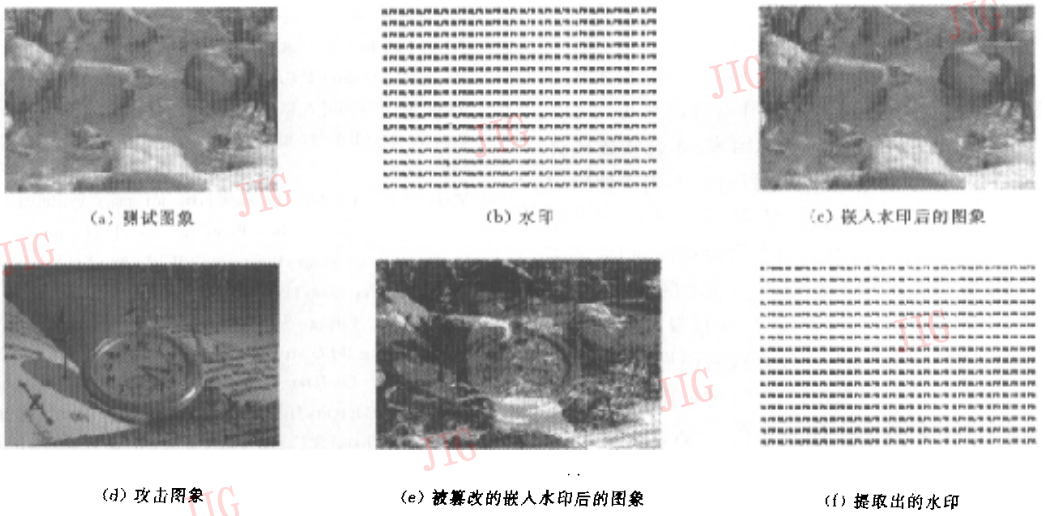
(2) 变换域方法

同鲁棒性数字水印一样,为提高水印的鲁棒性,许多算法均采用了变换域方法.在脆弱性数字水印研究中,变换域方法也有许多优点,如许多脆弱性水印系统的应用场合是要求水印能抵抗有损压缩的,这在变换域中更容易实现,而且容易对图象被篡改的特征进行描绘.DCT、小波变换等已经被广泛用于图象的有损压缩中,而许多鲁棒性水印的算法也均采用了 DCT 变换或小波变换,从而极大地提高了水印鲁棒性.受文献[5]启发,Wu 在文献[22]中,把一个有意义的二值水印模式嵌入到经过量化的 DCT 系数中,其量化矩阵为 JPEG 压缩中采用的量化矩阵.同样,在 LUT 中,把 DCT 量化后的值(即水印的可能嵌入位置)随机映射为 0 或 1,即可形成一个由图象的某些特征与{0,1}组成的二维列表.在某一位置嵌入 1 时,首先在 LUT 中查看该位置对应的{0,1}值,如果为 1,则该系数不变,如果为 0,就把该位置的系数量化为与它距离最近的系数;0 的嵌入与此相似.虽然水印是在压缩的形式下加入的,但是进一步的压缩或其他压缩方法可能会把水印破坏掉.文献[23]、[24]提出了基于小波变换的方法,其中,文献[23]是通过量化 Harr 小波变换系数来嵌入水印的,而 Xie 是通过把水印加入到经过 SPIHT 压缩的小波系数中来进行水印嵌入.由于小波分解包含了频率和空间信息,因此就可以用其对嵌入水印后图象的篡改进行定位和特征分析.变换域方法突出的优点就是能够较好地与现有的压缩标准(如 JPEG,JPEG2000)结合起来,并且能够在容许一定压缩比的情况下,检测出发生的篡改并定位,但由于嵌入水印的量比较有限,对篡改的定位一般是 8×8 大小的块,因此不如空间域水印定位精确.

3 脆弱性数字水印的鲁棒性问题与攻击行为分析

在鲁棒性水印中,水印的鲁棒性是与攻击行为密切相关的,同样,在脆弱性水印中,水印的脆弱性也是

与水印攻击相关的. 目前已有大量文献陆续描述了很多鲁棒性水印的攻击方法[25~28]，如简单攻击、同步攻击、迷惑攻击、删除攻击等. 由于脆弱性水印与鲁棒性水印的用途不同，因此脆弱性水印所面临的攻击主要不是将水印信息去掉或使水印的检测失败，而是设法在不损害水印信息的情况下篡改多媒体产品的内容，这就是所谓“伪认证”攻击. 一些水印方法虽可很容易地检测出图象的随机变化，但却不能检测出精心组织过的修改. 其一个简单的例子就是在图象最低有效位嵌入水印的情况下，如果攻击者不考虑水印的存在来对图象进行某些篡改，则非常容易使水印对篡改的检测失败，因为此时水印无法检测出发生的篡改，更不用说对篡改进行定位，如图 4 所示. 图 4(a)、(b)、(c)分别为测试图象、水印、嵌入水印后图象，图 4(d)为攻击者选取的攻击图象，将图 4(d)的次最高有效位(即第 7 位)替代图 4(c)中嵌入水印后图象的次最高有效位得到图 4(e)，由图 4(e)可以看出，嵌入水印后的图象已经严重被篡改，但从图 4(e)提取出的水印(图 4(f)) 仍然可得出“认证通过”的结论，实际上，此时图象已经被严重篡改过. 对于这类攻击方法需要从脆弱性水印方法本身的设计来减少虚警错误与漏检错误，同时需保护水印的添加与提取过程，以减少攻击者通过推断水印添加方法来对水印检测过程进行攻击的可能性.



(a) 测试图象　(b) 水印　(c) 嵌入水印后的图象

(d) 攻击图象　(e) 被篡改的嵌入水印后的图象　(f) 提取出的水印

图 4　对脆弱性数字水印攻击的一个例子

另外一类攻击方法是对脆弱性水印进行安全性攻击，由于脆弱性水印的安全性是与密钥密切联系在一起的，而且攻击者非常有可能通过对水印的研究推断出密钥或减少密钥的搜索空间，一旦推断出密钥，攻击者就有可能在任意一幅图象中添加水印，这样就破坏了水印的安全性，因此，设计密钥时，必须考虑其搜索空间应足够大，而且不同密钥之间最好是正交的，这样才能保证密钥很难被推断出.

4　脆弱性水印发展亟待解决的问题

数字水印技术是近几年来，国际学术界兴起的一个前沿研究领域. 不同的应用目的(如数据跟踪、数据监视、真伪鉴别和版权保护等)产生了不同的设计目的和水印算法，而用于多媒体产品真伪鉴别的脆弱性数字水印，作为水印技术的一个重要分支，仍然是一个未成熟的研究领域.

当前图象脆弱性水印的研究主要从完全脆弱水印、半脆弱水印、图象可视内容的真伪鉴别与自嵌入式水印 4 个层次进行研究. 其中，在完全脆弱水印的层次上，如何有效地抵抗“伪认证的攻击”是一个急需解决的问题；在半脆弱水印的层次上，目前已有能够抵抗 JPEG 压缩的脆弱性水印算法，但尚无抵抗 JPEG2000 的脆弱性水印算法，而且由于实际工作中，用户一般不知道采用的压缩标准是哪种，因此设计一种与压缩标准无关的半脆弱性水印算法也是非常必要的；在图象可视内容真伪鉴别的层次上，如何对图象的可视内容进行定义是一个关键的问题，而且也是一个比较难的问题；而在自嵌入式水印层次上，最重要的功能就是要能对篡改进行定位，并且恢

复被篡改的内容,因此如何能够有效地恢复被篡改的部分,也是一个非常有意义的研究方向.

目前大多数的水印研究均集中于图象脆弱性水印的研究,而对视频脆弱性水印技术则研究得非常少[29],且尚无对音频脆弱性水印的研究.一个完整的多媒体产品真伪鉴别系统应该包括图象、音频与视频,而且这种真伪鉴别,最后应该与版权保护结合在一起,形成一整套系统,以保护多媒体产品的版权与内容;还有数字签名技术作为一个相对成熟的理论,可与脆弱性数字水印技术互补,尤其在以压缩形式存在的多媒体产品的真伪鉴别方面可起到一定作用.可喜的是,已有少数学者[30,31]正在考虑把脆弱性水印与鲁棒性水印结合在一起,所有这些都是非常值得探讨的问题.

在设计一个完整的真伪鉴别系统时,为确保系统的安全性,密码的产生、发布和管理以及与其他系统的整合都是必不可少的考虑因素.在公钥密码体制中,系统的安全性是这样来解决的,即由密钥管理中心分配一对公钥和私钥,而后用公钥加密,用私钥解密,脆弱性水印系统是否可以借鉴该经验?由于实际应用对水印的保密安全有不同程度的要求,因此对于如何实现保密,一种可能是,非授权的用户对给定包含水印的图象,既不能读取或解码嵌入的水印,也不能检测到水印的存在;另外一种可能是,允许未授权的用户能够检测水印的存在,但若没有密码的话,则不能读取水印的内容.所有这些都将依赖于庞大的信任关系的确定及相应国际标准的建立.

总之,目前对于多媒体产品真伪鉴别方面的水印研究还远未成熟,尚有许多问题有待于解决,尤其在将技术推向标准化方面的一些工作,包括水印嵌入算法和检测算法的理论研究、水印的构造模型、水印能量和容量的理论估计、算法的性能评价等等,尚缺乏对脆弱性水印系统进行公正的比较和评价方法,故水印系统的脆弱之处尚无法进行全面测试与衡量.多媒体产品的真伪鉴别(包括水印技术与签名技术,尤其是水印技术)还面临着许多社会和法律问题[32].这需要有一些技术标准,而只有在水印技术发展到了一定阶段,才有可能形成一定的标准(就像密码学的发展一样),最终为用户所接受.尽管围绕水印技术还有许多问题需要解决,但新的 JPEG 和 MPEG 标准已经为数字水印的嵌入做了一定准备,这无疑将进一步推动多媒体产品真伪鉴别的深入研究.

注:本文的测试图片均来源于文献[33],感谢 Fabien A. P. Petitcolas 的无私帮助.

参 考 文 献

1 Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding—A survey [J]. Proc. of the IEEE, Special Issue on Protection of Multimedia Content, 1999,87(7):1062~1078.

2 Lin T, Delp E J. A review of fragile image watermarks[A]. In: Multimedia and Security Workshop at ACM Multimedia 99[C], Orlando, FL, USA, 1999.

3 Fridrich J. Methods for detecting changes in digital images[A]. In: IEEE Workshop on Intelligent Signal Processing and Communication Systems[C], Melbourne, Australia, 1998.

4 Fridrich J. Methods for tamper detection in digital images[A]. In: Multimedia and Security Workshop at ACM Multimedia 99 [C], Orlando, FL, USA, 1999.

5 Yeung M, Mintzer F C. An invisible wtermarking technique for image verification[A]. In: International Conference on Image Processing. (ICIP'97) [C], Washington DC, USA, 1997, 2: 680~683.

6 Wong P W. A public key watermark for image verification and authentication [A]. In: Proc. of the IEEE International Conference on Image Processing (ICIP' 98) [C], Chicago, Illinois, USA, 1998,1:455~459,

7 Lin C Y, Chang S F. Semi Fragile watermarking for authenticating JPEG visual content[A]. In: Proceedings of SPIE International Conference on Security and Watermarking of Multimedia Contents II, EI' 00[C], San Jose, CA, USA, 2000.

8 Lin C Y, Chang S F. A robust image authentication method surviving JPEG lossy compression[A]. In: Proceedings of SPIE International Conference on Storage and Retrieval of Image/ Video Database, EI'98[C], San Jose, CA, USA, 1998.

9 Lin C Y, Chang S F. A robust image authentication method distinguishing JPEG compression from malicious manipulation [R], CU/CTR Technical Report 486-97 19, Dec. 1997.

10 Lin C Y, Chang S F. An image authenticator surviving DCT based variable quantization table compressions[R], CU/CTR Technical Report 490-98 24, Nov. 1997.

11 Delp J, Podilchuk C I, Lin E T. Detection of image alterations using semi-fragile watermarks [A]. In: Proceedings of SPIE International Conference on Security and Watermarking of Multimedia Contents II, EI'00[C], San Jose, CA, USA, 2000, 3971(14).

12 Marvel L M, Hartwig G, Boncelet C G. Compression compatible fragile and semi-fragile tamper detection[A]. In: Proceedings of SPIE International Conf. on Security and Watermarking of Multimedia Contents II[C], San Jose, CA, USA, 2000, 3971 (12).

13 Queluz M P. Content based integrity protection of digital images [A]. In: Proceedings of SPIE International Conf. on Security

and Watermarking of Multimedia Contents. EI'99[C]. San Jose, CA, USA, 1999,3675(9).

11 Fridrich J, Goljan M. Protection of digital images using self embedding [A]. In: Symposium Content Security and Data Hiding in Digital Media[C], New Yark, NJ, USA, May 1999.

15 Fridrich J, Goljan M. Images with self-correcting capabilities [A]. In: IEEE International Conference on Image Processing (ICIP'99)[C], Kobe, Japan, Oct. 1999.

16 Wolfgang R B, Delp E J. A watermark for digital images[A]. In: IEEE International Conference on Image Processing (ICIP'96)[C], Laussane, Switzerland, Oct. 1996.

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

18 Queluz M P, Lamy P, Martinho J M *et al*. Spatial watermark for image verification[A]. In: Proceedings of SPIE International Conf. on Security and Watermarking of Multimedia Contents II. EI'00[C], San Jose, CA, USA, 2000,3971(11).

19 Schyndel R V, Tirkel A, Osborne C. A digital datermark[A]. In: Proc. of the IEEE International Conference on Image Processing (ICIP'94)[C], Austin, Texas, USA, 1994, 2: 86~90.

20 Wolfgang R, Delp E. Fragile watermarking using the VW2D watermark[A]. In: Proc. of the IS&T/SPIE Conference on Security and Watermarking of Multimedia Contents[C], San Jose, California, USA, 1999:204~213.

21 Memon N, Shende S, Wong P. On the security of the Yueng-Mintzer authentication watermark[A]. In: Proc. of the IS&T PICS 99[C], Savanna, Georgia, USA, 1999:301~306.

22 Wu M, Liu B. Watermarking for image authentication[A]. In: Proc. of the IEEE International Conference on Image Processing (ICIP'98)[C], Chicago, Illinois, USA, 1998,2:437~441.

23 Kundur D, Hatzinakos D. Towards a telltale watermarking technique for tamper-proofing [A]. In: Proc. of the IEEE International Conference on Image Processing (ICIP'98)[C], Chicago, Illinois, USA, 1998,2:409~413.

24 Arce G, Xie L. Joint wavelet compression and authentication watermarking [A]. In: Proc. of the IEEE International Conference on Image Processing (ICIP'98)[C], Chicago, Illinois, USA, 1998,2:427~431.

25 华先胜. 静止图象的局部化多类数字水印[D]. 北京:北京大学, 2001.5.

26 Barnett R, Pearson D E. Attack operators for digitally watermarked images[J]. IEE Proceedings on Vision Image and Signal Processing, 1998,145(4):271~279.

27 Craver S, Yeo B L, Yeung M. Technical trials and legal tribulations [J]. Communications of the ACM, 1998,41(7): 45~54.

28 Hartung F, Su J K, Girod B. Spread spectrum watermarking: malicious attacks and counterattacks[J]. Proc. of SPIE, 1999, 3657:147~158.

29 Dittmann J, Steinmetz A, Steinmetz R. Content-based digital signature for motion pictures authentication and content-fragile watermarking [A]. In: Proc. IEEE Conference Multimedia Computing and Systems[C], Italy, 1999,2.

30 Lu C S, Liao H M, Sze C J. Combined watermarking for image authentication and protection [A]. In: Proc. 1st IEEE Int. Conf. on Multimedia and Expo[C], New York City, NY, USA, Jul. 30~Aug. 2,2000.

31 Lu C S, Huang S K, Sze C J *et al*. Cocktail watermarking for digital image protection[J]. IEEE Trans. on Multimedia, 2000, 2(4):209~224.

32 Quisquater J J, Macq B, Joye M *et al*. Practical solution to authentication of images with a secure camera [A]. In: Proceedings of SPIE International Conference on Storage and Retrieval for Image and Video Databases[C], San Jose, CA, USA, 1997,3022:290~297.

33 http://research.microsoft.com/~fabienpe/

宋玉杰　1975 年生，1996 年和 1999 年先后获山东工业大学学士与硕士学位，2002 年获中科院自动化所博士学位. 研究兴趣包括多媒体产品真伪鉴别、数字水印、图象编码等.

谭铁牛　1964 年生，1984 年获西安交通大学学士学位，1986 年和 1989 年先后获英国伦敦大学帝国理工学院硕士与博士学位. 现为中科院自动化研究所所长、模式识别国家重点实验室主任、研究员、博士生导师. 主要研究领域为图象处理、计算机视觉和模式识别等. 发表论文 100 多篇.