◎学术探讨◎

用于图像认证的数字水印技术综述

王艳辉[1],王相海[1,2]
WANG Yan-hui[1],WANG Xiang-hai[2]

1.辽宁师范大学 计算机与信息技术学院,辽宁 大连 116029
2.南京大学 计算机软件新技术国家重点实验室,南京 210093
1.College of Computer and Information Technology,Liaoning Normal University,Dalian,Liaoning 116029,China
2.State Key Laboratory for Novel Software Technology,Nanjing University,Nanjing 210093,China
E-mail:xhwang@graphics.nju.edu.cn

WANG Yan-hui,WANG Xiang-hai.Overview on digital watermarking for image authentication.Computer Engineering and Applications,2007,43(2):33-37.

Abstract: With the development of Internet and digital of the multimedia information,image authentication based on digital watermarking is a hot research focus.This paper proposes the features of the fragile watermarking and the frame of the authentication system,then focuses on the algorithms and state of the fragile and semi-fragile watermarking based on authentication technology.Finally,the future development of digital watermarking for image authentication is also analyzed and conjectured in the paper.

Key words: image authentication;fragile watermarking;semi-fragile watermarking;tamper detection

摘 要:随着网络技术和媒体信息数字化的飞速发展,用于图像认证的数字水印技术成为目前研究的热点。主要阐述了当前用于认证的数字图像水印技术的特征、认证系统框架,详细讨论了脆弱水印和半脆弱水印的算法和研究现状,并对认证数字水印技术的未来发展方向进行了展望。

关键词:图像认证;脆弱数字水印;半脆弱数字水印;篡改检测
文章编号:1002-8331(2007)02-0033-05 **文献标识码**:A **中图分类号**:TP391

1 引言

数字水印作为一种信息隐藏技术,目前得到广泛地研究和发展[1,2]。该技术的应用前景非常广阔,包括版权保护、完整性认证、数字指纹、广播监测、拷贝控制等。数字化信息可以迅速高效传输给人们的同时,也存在着潜在的风险,恶意的个人与团体可能很容易修改信息,因此数字化信息的认证作为信息安全的一个重要领域,成为目前的一个研究热点。图像认证系统在医学、商业、法律和新闻等方面均有很广泛地应用。认证水印是利用人类知觉系统的冗余,在不影响数字媒体感官质量的前提下将与媒体内容提要相关或不相关的标志信息作为水印直接参与嵌入媒体内容中,当媒体内容需要认证时,可根据提取的水印信息来判断其是否真实完整。

本文首先对图像认证水印的目的和目前图像认证系统的框架、分类情况进行了叙述,然后对脆弱水印的特征进行了分析,在此基础上,对脆弱水印和半脆弱水印技术的发展情况进行了分析和讨论,最后展望了图像水印认证技术未来的发展方向。

2 图像认证水印系统的分类及过程

图像认证主要是检测图像内容的原始性,即图像有没有被恶意篡改。基于图像认证的数字水印技术根据不同的认证目的,对篡改的敏感性要求也不尽相同。一般说来,对图像的操作可以分为两类:一类是非恶意篡改,例如 JPEG 压缩、文件格式转换、滤波等;另一类是恶意篡改。图像认证系统的主要目标是实现对第二类操作的检测。根据是否容忍图像在一定程度下被修改,可以把现有的图像认证系统分为如下四类:(1)精确认证,也称硬认证[3,4]或完全级认证[5],注重图像数据的整体性,不允许对图像有任何修改。该认证系统要求能够检测出任意的篡改,通常采用脆弱(易损)水印[6]来实现。(2)模糊认证,也称软认证[3,4]或选择级认证[7],注重保护图像内容传递的信息,而不是图像内容的具体表示形式。对诸如格式转换、有损压缩、去除噪声等操作,检测时被认为是可接受的改动,即认为是非恶意的篡改。通常使用半脆弱(半易损)[8,9]水印技术实现。这类水印具有一定的稳健性, 对于像素变化的敏感性相对脆弱水印要差一些。(3)对图像内容的认证[10]:有些应用中,用户仅对于图像的某些内容或视觉效果感兴趣,因此如果对图像的操作没有影响

基金项目:国家自然科学基金资助项目(60372071);辽宁省自然科学基金资助项目(20032105);辽宁省高等学校优秀人才支持计划资助项目(RC-04-11);大连市科技基金资助项目。

作者简介:王相海,博士,教授,CCF 高级会员,主要研究领域为 CG、CAGD、图像编码和多媒体信息处理。

到图像的内容或视觉效果,都认为是可接受的,即能容许不影响视觉效果的任何篡改。该类系统的鲁棒性通常比前二类要好。(4)自嵌入水印[11]:把图像本身作为水印嵌入,不仅能检测到被篡改的区域,而且可能恢复被篡改的区域。自嵌入水印可以是脆弱的也可以是半脆弱的。

用于认证的水印嵌入过程与一般鲁棒性水印嵌入在原理上基本相同,从数字信号的角度可以看作是对原始图像的调制过程。嵌入的水印信息可以是与原始图像内容相关的信息,比如原始图像的边缘特征[12]、模式块映射[13]、块均值[14]、DCT 变换系数、DWT 变换系数、校验和等;嵌入的水印信息也可以是与原始图像内容不相关的信息, 比如密钥确定的 M 序列或者是标识创作者版权的有意义的二值图像等。图像认证时,首先从被测图像中提取水印信息,将提取的水印信息与原始水印信息相比较,若二者一致,则认为图像未被篡改;若二者不致,则认为图像已经被篡改,同时给出篡改的类型是恶意还是非恶意的篡改。若嵌入时采用提取特征嵌入,则提取时只需将提取的水印信息与被测图像的内容或特征进行比较,而不必再提取原始水印信息。

3 认证水印的特性

3.1 不可感知性(不可见性)

嵌入水印之后的图像要求有很好的不可见性[17],即在人眼的视觉范围内感觉不到变化,这一点和鲁棒性水印相同。

3.2 检测篡改及篡改的可恢复性

脆弱水印系统必须能够高效地检测出图像的篡改,通常情况下应该能够提供篡改信息的多少(即篡改的程度)及篡改发生的位置(即篡改的定位)。目前脆弱水印的定位能力可以分为二种:(1)像素级的定位能力,也称单像素认证,如在文献[2,3]中,Wu 等人提出的把篡改检测与篡改定位相分离的脆弱水印算法可以抵抗目前已知的各种攻击,可把篡改定位精细到一个像素,是目前较好的一种脆弱水印方法;(2)分块级的定位能力,也称分块认证[18],如 Fridrich 等人在文献[19]中所提出的分块认证可以把篡改定位到大小为 128 个像素的子块上。此外,在图像认证过程中,个别认证系统要求根据图像被篡改的位置恢复出图像被修改前的真实面目,即篡改的可恢复性。一般来说篡改的可恢复包括两种形式:一种是精确恢复,也就是恢复成和原来完全相同的效果;另一种是模糊恢复,就是把修改的地方恢复后和原来的内容不完全相同。对于图像认证来说,只需要实现模糊恢复,因为图像认证容忍恢复后的图像和原来图像间存在一定程度的差别,只要这种差别不影响对图像重要内容的解释即可。目前恢复方法有三种[20]:(1)在原有的图像上嵌入冗余信息,可以是错误纠正码(ECC)[21];(2)在图像中嵌入原图像的低分辨率版本[22];(3)盲恢复[23],该种方法仅当对图像的修改是可逆的,才可进行。

3.3 检测时不需要原始图像

在某些应用背景下,为保证照片的真实性,需要在拍摄成像时自动嵌入水印,此时原始数据就无处得到,而且如果能确知原始数据,就不存在内容提要的真伪鉴别了,因此用于认证的水印系统检测时不应该需要原始图像。

3.4 安全性

水印认证系统的安全性依赖于密钥,这要求密钥空间足够大,从而增强了水印认证的安全性。

4 脆弱水印和半脆弱水印发展和研究现状

4.1 用于精确认证的脆弱水印技术的发展

(1)空间域方法

空间域方法通常包括基于像素的脆弱水印和基于分块的脆弱水印两类。基于像素的脆弱水印算法最早的空间域方法是基于 LSB 的方法,即在图像最低有效位平面嵌入水印,这种方法的缺点是对于噪声非常敏感、容易被破坏、不能容忍对图像的任何修改。文献[25]对图像的 7 个最高有效位及尺寸通过 Hash 函数运算获得原始图像的某些特征, 该特征与一有意义的二值水印图像经过异或操作并经公开密钥加密后嵌入到图像中最低有效位。当图像内容受到怀疑时,首先将图像的 7 个最高有效位与图像尺寸经过 Hash 运算后得到某些特征,然后将图像最低有效位公开解密后的结果与该特征通过异或操作后就得到嵌入的水印模式。该算法具有定位特性,从提出的水印可以非常直观地看出被篡改的区域。与文献[25]一样,文献[26]也是在空间域嵌入了一个视觉上有意义的二值水印。在嵌入水印之前,版权所有者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 LUT(Look-Up-Table),水印的嵌入是根据 LUT 对空间域的像素进行量化实现的, 该类技术的安全性是由推断 LUT 的困难程度决定的[27],如果知道了二值水印,则算法的安全性会大大降低,即使不知道水印图像,也可以采用拼贴攻击对其进行有效地攻击[28],为此,文献[27]提出了基于位置的 LUT,从而大大增加了搜索空间。基于 LSB 的水印算法经适当改进后,不仅可以用于图像的完整性认证,还可以用于破损图像的恢复。文献[39]采用差错控制编码对最低有效位置零后的图像像素值进行 RS 编码,把编码后的结果嵌入在原始图像的最低有效位上。这种算法不仅具有检错能力,还具有一定的纠错能力。

Wong 等人在文献[30,31]中提出了一种基于分块的脆弱水印认证算法,算法的主要思想是把图像分割为各个独立的小块,然后分别在各小块上嵌入各自的水印,该类分块独立算法的缺点是不能抵抗伪造真实图像的量化攻击,其原因在于各个分块是独立的。Celik 等人使用分层的分块认证方法来消除上述算法的分块独立性[33,34],Fridrich 等人则使用分块编号和图像唯一索引来消除分块独立性, 其效果比 Celik 的方法更好,篡改定位能力更强一些[19]。然而,所有这些基于脆弱水印分块认证算法的共同特点是只能把篡改定位精确到图像分块上,与基于脆弱数字水印的单像素认证算法相比,该类算法的优点是安全性较高,缺点是篡改定位能力差一些。

(2)变换域方法

随着 DCT、小波变换等被广泛用于图像的有损压缩中,许多鲁棒性水印的算法采用了 DCT 变换或小波变换,从而极大地提高了鲁棒性。由于许多脆弱性水印系统要求能够抵抗有损压缩,这在变换域中更容易实现,此外,变换域更容易对图像被篡改的特征进行描绘,因此更多的算法采用在变换域中实现。

文献[22]对原始图像经 JPEG 量化后的 DCT 低频系数进行二进制编码,把编码后的数据嵌入到图像的最低有效位。这种图像自嵌入方法可以对原始图像进行恢复。Wu 在文献[9]中把一个有意义的二值水印模式嵌入经过量化的 DCT 系数中,量化矩阵为 JPEG 压缩中采用的量化矩阵。此外,在 LUT 中把经 DCT 量化后的值(即水印的可能嵌入位置)随机映射为 0 或 1,从而形成一个由图像的某些特征与{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它压缩方法可能会把水印破坏掉。

Kunder 和 Xie 分别在文献[15]和文献[35]中提出了基于小波变换的方法。Kunder 是通过量化 Harr 小波变换系数来嵌入水印的,而 Xie 则是通过把水印加入到经过 SPIHT 压缩的小波系数中。由于小波分解细数包含了频率和空间信息,这样就可以对水印图像的篡改进行定位和特征分析。文献[36]使用块相关的方法在小波域改变特定的小波系数来嵌入水印,由于使用块之间的依赖关系,因此对于矢量量化攻击能力强。

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,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。但由于嵌入的水印量比较有限,对篡改的定位一般是 8×8 大小的块,不如空间域水印定位的精确。

4.2 用于模糊认证的半脆弱水印技术的发展

脆弱水印不允许对图像进行任何轻微的篡改,而实际应用中,数字图像因其数据量较大,通常以压缩方式存储或传输,同时图像处理软件各异,图像格式众多,最终用户所要认证的通常是原始图像经有损压缩或其它保持图像内容的操作处理后的图像,因此,对图像进行内容级认证的半脆弱水印在现实生活中更为实用。

(1)由鲁棒性水印演变而来的半脆弱水印算法

该类算法主要是借鉴鲁棒性图像水印算法的经典方法,比如扩频水印、提取图像重要特征等来设计相应的认证算法,这种半脆弱水印具有一定的鲁棒性。文献[10]提出一种适用于数字相机的半脆弱水印算法,该算法从原始图像的每个 8×8 块提取 m 位二进制信息,将提取信息和数字相机的 ID 以及该块的序号一起经扩频处理,之后嵌入该图像块的 DCT 中频系数中。图像认证时,从被测图像中提取适当的门限来进行检测。该算法对常见的图像处理操作如滤波、JPEG 压缩、亮度对比等都具有很好的鲁棒性,对恶意的图像篡改操作拒绝认证。文献[37]提取图像的边缘特征作为水印嵌入到图像中,通过比较被测图像的边缘特征和提取的水印,来判断图像的真实性。此算法的缺点是误检率比较高,因为一旦图像被篡改,它的特征会随之改变,因而造成比较时的错误。文献[38]给出了从原始图像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旋转、缩放的图像处理操作,都具有不变性。文献[39]在原始图像的每个 8×8 块的 DCT 中频系数上叠加不同的伪随机序列,由于自然图像中一般平滑区较多,边缘区较少,认为在没有边缘存在的情况下,图像相邻像素差值信号的能量主要是由水印引起的,通过一个改进的运算来进行图像认证。算法的优点是对于 JPEG 有损压缩后被篡改的图像检测准确率很高,但是对于图像边缘和纹理较多的情况,算法的检测率较低,可靠性差。文献[40]提出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像的空间域或变换域。图像认证时,根据提取水印信息的正确率来判断图像的真伪。该算法的优点是实现起来比较简单,对于高质量的 JPEG 压缩具有鲁棒性,缺点是定位篡改能力不高。

(2)基于量化小波系数的半脆弱水印算法

由于小波变换在时域和频域具有良好的局部定位性质,同时与现有的图像压缩标准 JPEG2000 相融合,故小波域的数字水印认证技术有更高的实用意义。文献[15,41]通过量化小波系数来嵌入水印,利用小波空间域和频率域定位出篡改位置,并估计当前图像被篡改的程度。这种算法的缺点是很容易让攻击者得知量化步长而容易改变图像内容而使提取的水印信息仍然不变,其中文献[15]对图像的 Haar 小波系数进行量化,根据量化步长的大小来控制水印的鲁棒性,最后利用攻击估计函数将图像遭受的恶意篡改与非恶意篡改区分出来。YU 等人在文献[42]中通过量化小波系数的加权平均值来嵌入水印,认为小波系数的变化服从高斯分布,对图像进行恶意攻击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像失真引起的系数变化往往具有较小的方差,从而将恶意篡改与非恶意篡改区分开来。这种方法较直接量化小波系数有更好的鲁棒性。Paquet 等人在文献[43]中结合人类视觉系统(HVS)量化小波包系数,其算法首先生成 ID 序列,并用此 ID 序列选择小波变换函数及分解层数,在此基础上进行小波包分解,再次运用 ID 序列选择所要嵌入水印的区域及系数,利用人类视觉掩蔽特性,对不同的小波系数选择合适的嵌入强度,完成小波包系数量化的同时将 ID 序列一起嵌入,经小波包重构后得到含水印的图像,最后用密钥提取水印,结合小波包系数区域分别进行带内频域及带间空域比较得出检测结果。在文献[44]中,Eggers 先用 Scalar 编码器对水印信息进行编码得到二值码书,再用对应的 Scalar 量化函数对所选 8×8 块中的系数量化,即可把码书的各个元素嵌入相应宿主信息内。同时为了使嵌入随机化,嵌入过程引入二值伪随机序列。认证时,把待测信息与相应的量化函数、步长因子、二值伪随机序列混合运算得到验证值,若无水印则验证值近似为 0,若水印存在其验证值绝对值应接近步长因子值的一半,通过这种方法完成认证。该算法的优点是虚警率为 0,且对 JPEG 压缩稳健,能容忍一般的图像处理操作,缺点是对直方图均衡及锐化敏感。

(3)使用 JPEG 编码原理的半脆弱水印算法

文献[45]提出一种基于 JPEG 编码方法的半脆弱水印技术。该方法首先对原始图像的每个 8×8 图像块进行 DCT 变换,接着把各个图像块的信号排序,用 Hilbert 对照 JPEG 量化表再把向量分解成更小子向量,进一步,把子向量纵排列形成 Hadamard 矩阵,采用 Zig-Zag 扫描法选取 DCT 系数进行奇偶性量化,将调制后的 DCT 系数嵌入水印的图像块,结合图像块形成含水印的图像。最后通过比较待测图像的量化系数与原图量化系数的奇偶性相符情况完成认证。这种方法对正常图像处理操作反应敏感。在文献[8]中,Lin 和 Chang 给出了一种可以在一定程度上抵抗 JPEG 压缩和剪裁与替换操作的半脆弱水印技术,该技术可以识别被篡改的块的位置,并且可以利用来自原图的一个粗糙图像来对篡改块进行恢复。所提出的算法基于 JPEG 压缩前后 DCT 系数的两个不变特性:一是如果 DCT 系数被修改为 JPEG 量化步长的倍数,那么在未来的 JPEG 压缩中,该系数可以被确切重建;二是 JPEG 变换前后两个 8×8 子块相同位置的系数关系保持不变。算法利用第二个特性来形成认证信号,而利用第一个特性来将其嵌入到 DCT 系数中。此算法的虚警率近似为 0,并且对大多数攻击,比如去噪、剪切、直方图均衡等检测效果好,抗 JPEG 压缩能力强。此外,Sun 和 Chang 等人把基于数字水印的 SARI 系统的设计方法扩展到

DWT 域,以适应 JPEG2000 图像压缩标准[46,47]。

(4)基于人类视觉模型系统(HVS)的半脆弱水印算法

文献[48]将每一图像块的像素通过视觉掩模量化后再反量化,之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像。在检测端,先求出被检测图像的视觉掩模,将求得的掩模与图像像素一起输入误差估测函数进行预测。该算法的优点是能够准确检测出低于最大视觉可觉察门限期 1/2 的图像改动。由于视觉掩模可以计算出来,因此该算法的缺点是安全性不高,主要依赖于产生伪随机序列的密钥。文献[49]提出一种同时嵌入鲁棒水印与半脆弱水印的算法,该算法可实现图像版权保护和完整性认证的双重功能。算法先把小波系数分成掩蔽门限位(MTUS),在整个频带里选择满足在同尺度和同方位下绝对值大于相应 JND 阈值的小波系数作为嵌入点,用小波系数与对应的掩码门限值相除且向下取整来表示 MTUS 用 CWS(Cocktail Watermarking Scheme)调整量化后的小波系数完成水印嵌入,把原量化信息作为密钥储存来恢复原图像。认证时,采用不同检测方法完成两种水印的检测。

5 展望

脆弱和半脆弱水印技术作为水印技术的一个重要分支,目前还是一个未成熟的研究领域,尚有许多问题有待于进一步深入地研究,未来的图像认证水印技术在如下几个方面需要作深入地探讨:

(1)基于图像内容的水印认证算法的研究

基于图像内容的水印信息既可以增强系统抵御统计攻击能力,又可避免在认证检测端额外提供原始水印信息,同时也可以区分恶意操作与非恶意操作,因此更适用于图像认证。目前虽然也有一部分算法采用与图像内容相关的水印信息,但针对不同的应用提取图像的何种特征,生成的水印长度如何与原始图像容量相匹配以及如何使水印的嵌入不引起图像特征的变化等问题还有待于更深入的分析和研究。

(2)水印安全性问题

实际应用对水印的保密安全有不同程度的要求。现有的半脆弱水印技术大多采用基于私钥的加密方案,大量私钥信息通常很难管理,如何将半脆弱水印认证系统与密码学中的公开密钥算法结合,设计安全可靠的公钥水印认证算法,同时建立相应的标准或协议也将是一个重要的研究方向。

(3)图像认证与图像压缩编码算法的融合

由于数字媒体信息在数据库和网上多以压缩形式存储和传输,水印信息如何在保持其与内容之间具有良好相关性的同时适应各种压缩标准,是一个值得探讨的问题。目前针对 JPEG 编、解码器设计的水印认证算法已有文献,但针对 JPEG2000 及其它图像压缩标准的认证水印算法还很少,尤其是随着 JPEG2000 编码标准的不断成熟,研究能够抵抗 JPEG 及 JPEG2000 压缩的模糊认证算法具有重大的实际意义。

(4)视、音频水印认证技术的研究

大量消费类数字视频产品的推出,使得以半脆弱水印为重要组成部分的视、音频真伪鉴别技术的市场需求更加迫切,然而,由于包括时间域掩蔽效应等特性的更为精确的理论模型尚未完全建立,使得目前视频、音频半脆弱水印技术的性能不太理想,同时现有的音、视频的编码格式也在一定程度上限制了水印技术的引入。因此,未来音、视频半脆弱水印技术也将会成为一个研究热点。

(5)评测标准的建立

目前在将多媒体认证水印技术推向标准化方面还有很多工作要做,比如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、对水印系统进行公正的比较和评价方法等,此外数字水印技术还面临着许多社会和法律问题需要解决。(收稿日期:2006 年 11 月)

参考文献:

[1] 孙圣和,陆哲明.数字水印技术及应用[M].北京:科学出版社,2004.

[2] Cox I J,Miller M L,Bloom J A.数字水印[M].王颖,黄志蓓,译.北京:电子工业出版社,2003.

[3] Zhu B B,Swanson M D,Tewfik A H.When seeing isn't believing[J].IEEE Signal Processing Magazine,2004,21(2):40-49.

[4] Zhu B B,Swanson M D.Multimedia authentication and watermarking[M]//Feng D,Siu W C,Zhang H.Multimedia Information Retrieval and Management.[S.l.]:Springer Verlag,2003:148-177.

[5] Lin C Y.Watermarking and digital signature techniques for multimedia authentication and copyright protection[D].New York:Columbia University,2000.

[6] Yeung M,Mintzer F.An invisible watermarking technique for image verification [C]//Proceedings of the IEEE International Conference on Image Processing,Santa Barbara,USA,1997,2:680-683.

[7] Cox I J,Miller M L,Bloom J A.Digital watermarking [M].New York:Academic Press,2002.

[8] Lin C Y,Chang S F.Semi-fragile watermarking for authenticating JPEG visual content[C]//Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II,San Jose,USA,2000,3971:140-151.

[9] Wu M,Liu B.Watermarking for image authentication[C]//Proceedings of the IEEE International Conference on Image Processing,Chicago,USA,1998,2:437-441.

[10] Fridrich J.Mehtods for detecting changes in digital images[C]//Proc of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication System,Melbourne,Australia,1998:173-177.

[11] Queluz M P.Towards robust:content based techniques for image authentication [C]//Proceedings of the IEEE 2nd Workshop on Multimedia Signal Processing,Los Angeles,1998:297-302.

[12] Fridrich J.Image watermarking for tamper detection[C]//Proceedings of the IEEE International Conference on Image Processing,Chicago,USA,1998,2:404-408.

[13] Bassali H,Chhugani J,Agarwal S,et al.Compression tolerant watermarking for image verification [C]//Proceedings of the IEEE International Conference on Image Processing,Vancouver,Canada,2000,1:430-433.

[14] Kundur D,Hatzinakos D.Towards a telltale watermarking technique for tamper proofing [C]//Proceeding of the IEEE International Conference on Image Processing,Chicago,USA,1998,2:409-413.

[15] Walton S.Image authentication for a slippery new age[J].Dr.Dobb's Journal,1995,20(4):18-26.

[16] Wolfgang R B,Podilchuk C I,Delp E J.Perceptual watermarks for digital images and video[C]//Proceedings of the IEEE,1999,87(7):1108-1126.

[17] Wu J,Zhu B,Li S,et al.A secure image authentication algorithm with pixel-level tampering localization [C]//Proceedings of the IEEE International Conference on Image processing,Singapore,2004.

[18] Wong P,Memon N.Secret and public key image watermarking schemes for image authentication and ownership verification[J].IEEE Transactions on Image Processing,2001,10 (10):1593-1601.

[19] Fridrich J.Security of fragile authentication watermarks with localization [C]//Proceedings of the SPIE,Security and Watermarking of Multimedia Contents IV,San Jose,Alifornia,2002,4675:691-700.

[20] Wu Jin-hai,Lin Fu-zhu,Image authentication based on digital watermarking[J].Chinese Journal of Computer,2004,27(9):1153-1160.

[21] 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.

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

[23] Kundur D,Hatzinakos D.Semi-blind image restoration based on telltale watermarking[C]//Proceedings of the 32nd Asilomar Conference on Signals,Systems and Computers,Pacific Grove,California,1998,2:933-937.

[24] van Schyndel R G,Trikel A Z,Osborne C F.A digital watermark [C]//Proceedings of the IEEE International Conference on Image Processing,Austin,Texas,1994,2:86-90.

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

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

[27] Memon N,Shende S,Wong P.On the security of the Yeung-Mintzer authentication watermark [C]//Proceedings of the IS &T PICS Symposium,Savannah,Georgia,1999:301-306.

[28] Fridrich J,Goljan M,Memon N.Further attacks on Yeung-Mintzer fragile watermarking scheme[C]//Proceedings of the SPIE,Security and Watermarking of Multimedia Contents II,San Jose,CA,2000,3971:428-437.

[29] 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.

[30] Wong P W.A watermark for image integrity and ownership verification[C]//Proceedings of the IS &T PIC Conference,Oregon,Portland,1998.

[31] Memon N,Wong P.Secret and public key authentication watermarking schemes that resist vector quantization attack[C]//Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II,San Jose,USA,2000,3971:417-427.

[32] Holliman M,Memon N.Counterfeiting attacks on oblivious-block2wise independent invisible watermarking schemes[J].IEEE Transactions on Image Processing,2000,9(3):432-441.

[33] Celik M,Sharma G,Saber E,et al.A hierarchical image authentication watermark with improved localization and security[C]//Proceedings of the IEEE International Conference on Image Processing,Thessaloniki,Greece,2001,2:502-505.

[34] Celik M,Sharma G,Saber E,et al.Hierarchical watermarking for secure image authentication with localization[J].IEEE Transactions on Image Processing,2002,11(6):585-595.

[35] Xie L,Arce G.Joint wavelet compression and authentication watermarking [C]//Proc of the IEEE International Conference on Image Processing,1998,2:427-431.

[36] Si Hua-yin,Li C T.Fragile watermarking scheme based on the block-wise dependence in the wavelet domain[C]//MM&Sec'04,Magdeburg,Germany,2004.

[37] Rey C,Dujelay J L.Blind detection of malicious alterations on still images using robust watermarks[C]//IEEE Secure Image Authentication Colloquium,London,UK,2000.

[38] Fridrich J.Visual hash for oblivious watermarking[C]//Proceedings of SPIE,San Jose,CA,USA,2000,3971:286-294.

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

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

[41] Kundur D,Hatzinakos D.Digital watermarking for telltale tamper-proofing and authentication [C]//Proceedings of the IEEE Special Issue on Identification and Protection of Multimedia Information,1999,87(7):1167-1180.

[42] Yu G J,Lu C,S,Liao H Y,et al.Mean quantization blind watermarking for image authentication[C]//IEEE International Conference on Image Processing,Vancouver BC,Canada,2000,3:706-709.

[43] Paquet H.Ward R K,Pitas I.Wavelet packets-based digital watermarking for image verification and authentication [J].Signal processing,2003,83(3):2117-2132.

[44] Eggers J,Girod B.Blind watermaking applied to image authentication[C]//Proceedings of IEEE ICASSP,Salt lake city,UT,2001:7-11.

[45] Mansour M F,Tewfik A H.Robust high capacity data embedding [C]//ICASSP 2001,Utab,2001.

[46] Sun Qi-bin,Chang Shih-fu,Kurato M,et al.A quantitative semi2fragile JPEG2000 image authentication system[C]//Proceedings of the IEEE International Conference on Image Processing,Rochester,USA,2002,2:921-924.

[47] Sun Qi-bin,Chang Shih-Fu.Semi-fragile image authentication using generic wavelet domain features and ECC[C]//Proceedings of the IEEE International Conference on Image Processing,Rochester,USA,2002,2:901-904.

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

[49] Fridrich J,Goljan M,Memon N.Cryptanalysis of the Yeung-Mintzer fragile watermarking technique [J].Journal of Electronic Imaging,2002,11(2):262-274.

[50] Quisquater J J,Macq B,Joye M,et al.Practical solution to authentication of images with a secure camera [C]//SPIE International Conference on Storage and Retrieval for Image and Video Databases,Jose,USA,1997,3022:290-297.