

文章编号:1001-9081(2010)11-3044-02

抗 JPEG 压缩并精确定位篡改自嵌入水印算法

岳晓丽,徐江峰

(郑州大学 信息工程学院, 郑州 450001)

(yxl20081997@sina.com)

摘要:为了提高自嵌入水印算法篡改定位的精确度和抗 JPEG 压缩性能,提出了一种用于图像篡改定位和恢复的双水印算法。该算法对图像进行一级小波分解,分别在高频和低频分量中嵌入认证水印和自恢复水印。仿真实验表明,该算法不仅能对篡改区域实现精确定位,而且具有较好的鲁棒性,可以抵抗一定的 JPEG 压缩。

关键词:自嵌入;双水印;篡改定位;小波变换;JPEG 压缩

中图分类号: TP391.41;TP309 **文献标志码:** A

Self-embedded watermarking algorithm for precise image tamper location against JPEG compression

YUE Xiao-li, XU Jiang-feng

(School of Information Engineering, Zhengzhou University, Zhengzhou Henan 450001, China)

Abstract: To improve the precision of tamper location and the capability of resisting against JPEG compression, this paper presented a new image dual-watermarking scheme for both tamper detection and tampered image recovery. The basic principle of this scheme was to let the original image be performed by the 1-level discrete wavelet transformation. Then the authentication watermarking and self-recovery watermarking were respectively embedded into high-frequency and low-frequency component of original image. The experimental results show that the proposed scheme not only can detect and locate tamper accurately, but also is robust to resist against JPEG compression.

Key words: self-embedding; dual-watermarking; tamper localization; wavelet transform; JPEG compression

0 引言

根据识别篡改的能力,用于认证的数字水印可分为完全脆弱水印和半脆弱水印。完全脆弱水印主要用于完全级的认证,而半脆弱水印主要用于内容级认证。利用认证水印可检测原始信息的真实性,并能检测到篡改区域。但大多数情况下,人们希望检测到篡改的同时,能对篡改区域做出恢复。因此,近年来出现了不少对篡改区域做出修复的自嵌入水印算法。1999年 Fridrich 提出了一种基于离散余弦变换(Discrete Cosine Transform, DCT)的分块自嵌入脆弱水印算法^[1],该算法将一幅图像的重要内容作为水印嵌入自身之中,从而能够在检测篡改的同时近似地恢复被篡改的内容。但该算法可逆,抗伪造攻击的能力不强,同时数据编码位长不合理,致使恢复图像的质量不好。针对这些问题,文献[2-4]分别通过改进编码位长、把 SPIHT 压缩图像嵌入原始图像的最低位及使用奇异值分解等方法,提高了被篡改图像的恢复质量。然而这些算法将水印嵌入在原始图像的最低有效位,必定产生对包括 JPEG 压缩在内的常规图像操作不具备鲁棒性;同时由于篡改定位时需要设定阈值,导致篡改定位精确度不够高。

针对上述问题,本文提出了一种半脆弱双水印自嵌入算法。该算法首先对图像进行一级小波分解,利用 SPIHT 压缩算法对图像分块压缩得到自恢复水印,而后将其嵌入到小波分解的低频分量,并把认证水印嵌入到高频分量中。其中,认

证水印用来对篡改进行定位,自恢复水印用来对篡改区域进行恢复。

1 相关理论

1.1 图像的小波变换

小波变换是一种崭新的信号分析理论,由于其具有较好的时频分析特性,在许多领域得到了广泛的应用,并已成为 JPEG2000 压缩标准的核心技术。小波变换对图像有较好的集中作用,根据需要可以得到不同层次、不同方向子图。其中低频子带具有较强的抵抗外来影响的能力,稳定性较好;而高频子带容易受外来噪声、图像处理操作等的影响,稳定性较差。因此本文算法将自恢复水印嵌入低频子带可以较好地满足鲁棒性;而将认证水印嵌入到高频子带中,则可以较好地满足其对攻击的脆弱性,从而可以有效地区分篡改并能对篡改精确定位。

1.2 SPIHT 算法

SPIHT 算法,即多级树集合分裂算法,它基于 Shapiro 的嵌入式零树编码算法,它采用有效的空间方向树结构和比特平面编码方法,不仅能获得很高的压缩编码效率,而且产生的码流是嵌入式的,支持解码器的多码率解码,有利于图像的渐进传输。即使不采用算术编码,仍能获得很高的编码效率^[5]。基于 SPIHT 算法的优点,本文算法采用此压缩算法对原始图像进行压缩,得到自恢复水印,有效地减少了嵌入信息量。

收稿日期:2010-05-11;修回日期:2010-07-09。

作者简介:岳晓丽(1983-),女,河南郑州人,硕士研究生,主要研究方向:数字水印;徐江峰(1965-),男,河南禹州人,教授,博士,主要研究方向:信息安全、混沌加密通信。

2 自嵌入算法

2.1 水印嵌入

兼顾篡改定位、篡改恢复图像质量、自恢复水印鲁棒性等因素,本文采用对原始图像做一级小波分解,而后分别在高频和低频分量中嵌入认证水印及自恢复水印。其嵌入过程如图 1 所示。

详细步骤如下:

- 1) 对原始图像进行一级小波分解,得到高频和低频分量。
- 2) 利用 SPIHT 压缩算法,将原始图像分块压缩,然后将分块压缩编码 Arnold 置乱,量化嵌入到低频分量中。
- 3) 结合人类视觉掩蔽模型,将认证水印嵌入到高频分量

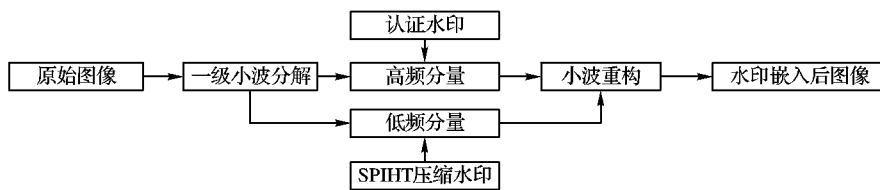


图1 水印嵌入流程

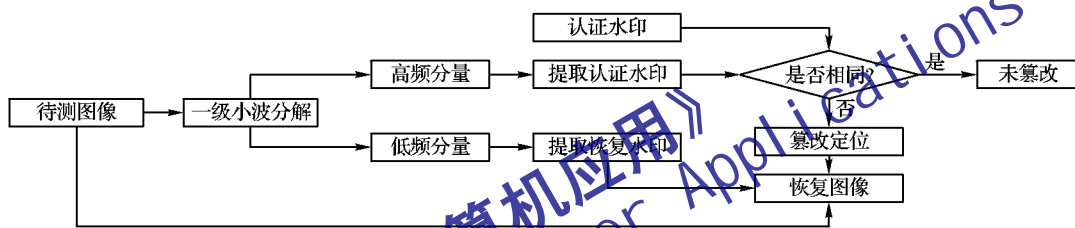


图2 篡改检测和恢复流程

在对原始图像分块编码、解码的过程中,分块的大小可以选取 8×8 , 16×16 , 32×32 等,但块越小解码后的图像的块效应就越明显。同时还应注意,编码和解码过程中块的大小相差 2 个数量级,例如编码时分块采用 32×32 ,解码时则应当采用 16×16 ,这主要是由于实验是在小波域进行的;同时码率应取 0.25,这样使得编码后的码流量刚好与低频系数数量相当,以实现完全替换。

3 实验仿真

实验使用大小为 $256 \times 256 \times 8$ 的标准灰度图像作为实验对象, 128×128 的二值图像作为认证水印,恢复水印则采用 SPIHT 压缩编码算法,编码时采用 32×32 的分块形式进行压缩,解码相应进行 16×16 的分块解压缩。图 3(a) 和 (b) 分别显示了水印嵌入前后的图像,水印嵌入后图像峰值信噪比为 31.6053 dB;图 3(c) 是二值认证水印;图 3(d) 是在没有篡改的情况下,提取的自恢复水印,从视觉上看与原始图像有一定的差别,但图像的特征内容已经完整地保存了下来。



图3 原始图像、水印嵌入图像及认证水印图像

3.1 JPEG 压缩

作为半脆弱自嵌入水印算法,算法的鲁棒性是评测其性能的一个方面。鲁棒性是指含水印产品在经过常规信号处理操作后仍能检测出水印的能力^[6]。对图像的常规处理操作

中的水平和垂直分量。

- 4) 一级小波重构得到水印嵌入后图像。

2.2 篡改检测和恢复

本文算法利用认证水印进行篡改检测和定位,如果发现篡改,则使用自恢复水印恢复被篡改区域,其流程见图 2。

详细步骤如下:

- 1) 对接收到的图像进行一级小波分解。
- 2) 从高频分量中提取认证水印,得到提取的认证水印与原始水印信息进行比对,从而确定图像是否被篡改,及定位篡改。
- 3) 如果篡改,从低频系数中提取自恢复水印,反置乱后进行解码得到用于篡改恢复图像。用此图像的相应部分替换图像篡改部分,即可得到自恢复图像。

主要包括空间滤波、有损压缩等。由于图像的信息量大不利于传输,JPG 格式成为网络传输过程中常用的图片格式,因此水印图像要能抵抗一定程度的 JPEG 压缩攻击。图 4 显示了算法抵抗 JPEG 压缩的性能。从实验结果,可以看出当压缩因子为 65 时,自恢复水印仍具有较强的鲁棒性。

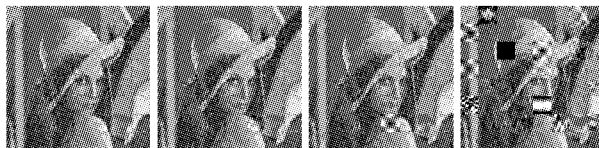


图4 JPEG 压缩提取恢复水印图

3.2 剪切、替换篡改定位及恢复

可恢复水印算法作为认证水印算法的一种,其篡改检测性能可以通过考查算法的漏警概率 (Probability of False Acceptance, PFA) 和虚警概率 (Probability of False Rejection, PFR) 来衡量^[7]。

本文算法通过增加认证水印的方法,有效地解决了虚警检测的问题。本文分别对水印嵌入图像进行剪辑、替换等篡改,部分实验结果如图 5~6 所示。

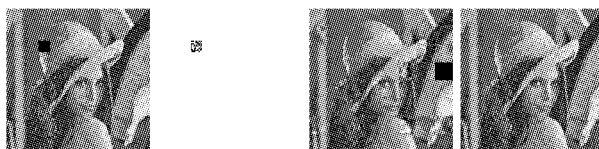


图5 剪切篡改定位和修复过程

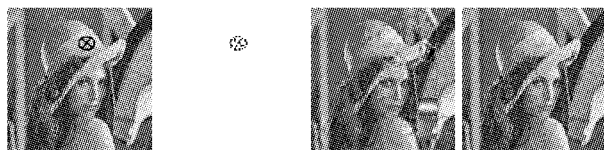
图5显示了剪切篡改定位和修复的过程。从图5(b)可

(下转第 3083 页)

30%,而性能问题则定义为首次产生性能告警时产生性能问题。资源性能数据采集组件采集的 MSC 中继群原始统计指标经过 KPI 计算组件、性能状态分析组件、性能问题分析组件处理后,产生的性能问题和性能告警上传给性能监控客户端呈现,如图 4 所示,性能监控客户端呈现了长途软交换局向接通率低的问题(对应图中告警标题栏的长途软交换局向接通率低),性能问题采用列表形式呈现,体现性能问题状态的性能告警以子树节点的形式连接在相应的性能问题上。处于不同生命周期的性能问题分栏呈现,新产生的性能问题呈现在未处理栏,处于问题处理阶段的呈现在正在处理栏,处于观察阶段的呈现在处理完毕栏,而已解决的呈现在已清除栏。性能问题列表中包括网元名称、对象、告警标题、最坏级别、当前状态、告警首次产生时间、告警最近产生时间等属性列,详细展示告警内容。监控人员在监控客户端对性能问题进行处理,主要是记录处理的情况,包括处理人、处理时间、处理意见、是否处理完毕等,当前选中的性能问题,其问题处理记录显示在监控客户端右下方的子窗口中。而开始记录首次处理记录后,该性能问题自动从未处理栏进入正在处理栏,如果在处理记录中标记了处理完毕,并设定观察期,则性能问题自动进入处理完毕栏。如果在观察期内对应的中继去话溢出率告警一直没有产生,则该性能问题自动迁入已清除栏,并暂存一段时间后从监控客户端消失。性能问题处理过程中,利用监控客户端可查询历史性能值,并提供 KPI 趋势图等分析手段,即性能问题分析组件的功能。

(上接第 3045 页)

以看出,认证水印对剪切进行了较为精确地定位。由于自恢复水印在使用 SPIHT 压缩算法的同时,结合了 Arnold 置乱,使得提取出来的自恢复水印中与原始图像篡改对应区域没有受到影响,图像修复才得以实现。图 6 显示了图像的替换攻击,用其他标志替换图像中帽子的区域,修复结果从视觉上可以接受。



(a) 修改后图像 (b) 篡改定位 (c) 提取自恢复水印 (d) 修复图像

图 6 替换篡改定位和修复过程

引言中提到为了定位篡改,现有算法通常是通过对每种篡改设定不同的阈值来实现,这同样可能导致定位的精确度不高。本文算法的认证水印,很好地解决了虚警检测,在精确定位篡改的同时,省去了阈值选择的麻烦。虽然出现了一定的漏检,但总体来说漏检的增加对篡改定位影响不大。

由实验结果可以看出,不论是图像的剪切还是替换,该算法均能较为精确地定位,没有显示虚警检测。虽然修复的图像不如原始图像效果好,但根据修复出来的图像依然能辨认原始图像的概貌。

4 结语

本文提出了一种高精度定位的自嵌入水印算法,与现

应用表明,将数量庞大的性能告警归并为有限的性能问题,大大提高了性能监控的效率,并能对性能问题的分析、处理和解决效果评估进行规范管理。同时,基于组件的系统结构则能支持灵活的系统集成和持续的业务演进。

5 结语

本文以 NGOSS 为指导建设电信网络性能监控系统,围绕性能问题的生命周期管理来构建业务流程,规范了性能监控端到端的业务过程,加强了性能监控的有效性。共享信息数据模型和组件体系结构则考虑了性能监控系统的方便集成和平滑业务演进。性能监控作为电信网络管理的一个新的重要功能模块,是实现下一代电信运维支撑系统的一个很好的切入点,为指导下一代电信运维支撑系统的建设提供了一个参考案例。

参考文献:

- [1] 赵勇. 电信运营支撑系统的现状与发展趋势[J]. 通信世界: B, 2009(1): 10 - 11.
- [2] 卢捍华, 王亚石, 闵丽娟, 等. 基于 NGOSS 的 OSS/BSS 框架[J]. 电信科学, 2009(10): 57 - 62.
- [3] 肖丁, 安静, 王柏. 基于构件的电信运营支撑系统的开发[J]. 计算机应用研究, 2006, 23(2): 167 - 170.
- [4] 张雷. NGOSS 新一代电信运营支撑系统[J]. 通信世界: B, 2008(1): 23 - 24.
- [5] TeleManagement Forum. GB921 concepts and principles V8.1[S], 2008.
- [6] TeleManagement Forum. GB922 SID Concepts v8.0[S], 2008.

有算法相比本文算法具有以下优点:

- 1) 提高了自嵌入水印算法的篡改定位精确度;
- 2) 提高了自嵌入水印算法的抗 JPEG 压缩性能, 提高了鲁棒性。

如何提高水印嵌入后图像质量,是我们下一步研究的内容。

参考文献:

- [1] FRIDRICH J, GOLJAN M. Protection of digital images using self-embedding [EB/OL]. [2009 - 12 - 12]. http://www.ws.binghamton.edu/fridrich/Research/nj_may14.ps.
- [2] 张鸿宾, 杨成. 图像的自嵌入及篡改的检测和恢复算法[J]. 电子学报, 2004, 32(2): 196 - 199.
- [3] 何登平, 范鹏. 一种基于图像内容的自恢复水印算法[J]. 四川理工学院报: 自然科学版, 2008, 21(4): 77 - 79.
- [4] CHE SHENGBING, CHE ZUGUO, MA BIN, et al. Image self-embedding technology research based on singular value decomposition [C]// Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM). Washington, DC: IEEE, 2008: 134 - 139.
- [5] 贾志科, 崔惠敏, 唐坤. 改进的 SPIHT 静止图像压缩编码算法[J]. 清华大学学报: 自然科学版, 2001, 41(7): 25 - 28.
- [6] 孙圣和, 陆哲明, 牛夏牧. 数字水印技术及应用[M]. 北京: 科学出版社, 2004: 354.
- [7] HE HONGJIE, ZHANG JIASHU, TAI HENGMING. A wavelet-based fragile watermarking scheme for secure image authentication [M]. Berlin: Springer-Verlag, 2006: 422 - 432.