第35卷 第22期 计 算 机 工 程 2009年11月
Vol.35 No.22 Computer Engineering November 2009
·安全技术· 文章编号：1000—3428(2009)22—0125—03 文献标识码：A 中图分类号：TP391

基于差值扩展和纠错编码的可逆图像认证

文家福，王嘉祯，刘爱珍，刘会英
(军械工程学院计算机工程系，石家庄 050003)

摘 要：针对一些敏感数字图像在认证水印嵌入过程中不能引入失真的问题，提出一种能够定位图像篡改块的可逆图像认证方案，利用纠错编码使认证数据能抵抗可能受到的篡改攻击，并用差值扩展的方式将编码后的认证数据嵌入到图像中。仿真实验结果表明，若认证通过，则图像可完全恢复到原始状态，否则，图像中篡改的块可被定位，并完全恢复其他未篡改的区域。

关键词：图像认证；可逆数字水印；差值扩展；纠错编码

Reversible Image Authentication Based on Difference Expansion and Error Correction Code

WEN Jia-fu, WANG Jia-zhen, LIU Ai-zhen, LIU Hui-ying
(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003)

【Abstract】 Aiming at the problem that some sensitive digital images can not bring in inevitably distortion in the process of authentication data embedding, a reversible image authentication scheme with tampering localization is proposed. In this scheme, authentication data is encoded using error correction code to prevent them from malicious manipulation and difference expansion is exploited to conceal the encoded data into image. Simulation experimental results demonstrate that if the image is authentic, the distortion due to embedding can be completely removed from the original state, otherwise, the tampered blocks can be located and other areas can be restored.

【Key words】 image authentication; reversible digital watermark; difference expansion; error correction code

1 概述

数字多媒体信息具有获取容易、复制简单、传播迅速、处理容易等优点，给人们的生活带来极大便利。然而，技术发展的同时，也带来了安全隐患。攻击者可以毫不费力地篡改信息的内容，使用户无法判断数字信息的真伪。因此，数字信息的真实性、完整性认证具有重要的实用价值，基于数字水印的认证技术是解决该问题的有效方法之一[1]。

在多数情况下，认证数据作为水印信息在嵌入到数字载体的过程中会引入不可逆的失真。然而，在医学原始照片、法庭证据照片、军事遥感图像等的认证中，即使是对数据图像的极小改变都是不允许的，图像的任何修改都会影响图像的可信度。这就需要在认证完成后，图像能完全恢复到原始状态。

2 相关问题

能将含印载体数据恢复到原始状态或非常接近原始状态的水印技术，称为可逆数字水印技术。文献[2-4]提出一些利用可逆水印进行图像认证的方法，比如，无损压缩图像最低位平面的方式，得到一部分空间嵌入图像 *hash* 计算后的数据；利用差值扩展在隐藏信息的同时嵌入认证码验证图像的完整性；使用带密钥的 *hash* 函数计算图像认证码，并用差分直方图位移的方式将认证码嵌入到图像中。所有这些认证方法都只能验证图像的完整性。然而，在一些视觉内容的认证中，篡改的定位能力也非常重要。如果在发生篡改时，能定位篡改的区域，则其他未篡改的区域仍然具有使用价值，且能暗示篡改者的动机。

常用的图像篡改定位方法是基于块的认证。由于可逆水印本身的特点，要利用可逆水印进行篡改定位，需要解决以下几方面的问题：

(1)容量：基于块的认证需要大量的认证数据，所以，水印嵌入算法必须有足够的嵌入容量。

(2)鲁棒性：可逆水印一般需要嵌入一部分附加信息作为水印提取后图像的恢复信息。当图像受到篡改时，要保证能正确提取这部分附加信息。

(3)敏感性：在可逆水印嵌入算法中，一些区域不能嵌入水印。需要一种合适的篡改检测方案，能检测图像任何位置的篡改。

文献[3]提出的基于差值扩展的可逆数字水印算法是种容量较大的可逆水印算法，文献[5]对像素对的分类方式和嵌入方法进行简化。本文在这些可逆水印嵌入算法的基础上，解决了上述 3 种问题，提出一种可以定位篡改块的可逆图像认证方案。

3 图像认证方案

该方案需要嵌入的水印信息包括 2 个部分：图像认证数和图像恢复数据。在水印嵌入前，先将这 2 部分数据进行纠错编码，再嵌入到图像中。这样，图像在受到篡改后，虽然提取的数据中可能会有错误，但在解码后仍能得到正确的水

基金项目：河北省科技厅基金资助项目(05213579)
作者简介：文家福(1981－)，男，博士研究生，主研方向：数字水印，图像认证；王嘉祯，教授、博士生导师；刘爱珍，讲师；刘会英，硕士研究生
收稿日期：2009-07-20 **E-mail：**yygyjf@sina.com

印信息。

3.1 水印嵌入算法

文献[3]的差值扩展嵌入算法是利用 2 个相邻的像素点隐藏 1 位数据。假定有 2 个像素的值为 x 和 y，且 $0 \le x, y \le 255$，需要嵌入的比特为 $b \in \{0,1\}$，则定义 x 和 y 的整型均值 l 和差值 h：

$$l = \left\lfloor \frac{x+y}{2} \right\rfloor, h = x - y \tag{1}$$

其中，$\lfloor\ \rfloor$ 是向下取整函数。通过 l 和 h 反过来可以计算得到像素对的值 x 和 y，其逆变换为

$$x = l + \left\lfloor \frac{h+1}{2} \right\rfloor, \quad y = l - \left\lfloor \frac{h}{2} \right\rfloor \tag{2}$$

当嵌入水印时，通过式(1)计算 l 和 h，将 h 用二进制表示，再将比特 b 追加到 h 的最低位之后，得到新值 $h' = 2 \times h + b$。用新的差值 h' 和原始的均值 l 可以计算得到新的像素对 x' 和 y'，作为图像的像素值。

水印提取时，再用式(1)计算均值 l 和差值 h'，将差值 h' 用二进制表示，其最低位即为隐藏的信息位 b，去掉最低位后得到原始的差值 h。最后通过 l 和 h，利用式(2)即可得到原始的像素对 x 和 y。

可以看出，该算法是利用扩大像素对差值来嵌入 1 位数据。在水印嵌入过程中，像素对的值分别由 x 和 y 改变为 x' 和 y'，这就可能会使 x' 和 y' 的值超出灰度级的表示范围，称为溢出。如对于 256 级灰度图像 x' 和 y' 必须满足 $0 \le x', y' \le 255$。在嵌入数据未知的情况下，嵌入条件表示为

$$|2 \times h + 1| \le \min(2(255 - l), 2l + 1) \tag{3}$$

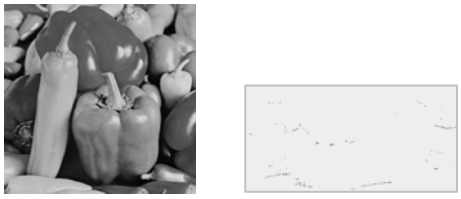
为解决像素值的溢出问题，文献[3]根据像素对的可扩展情况，把像素对分为 4 类。在嵌入过程中，先在选择的可扩展像素对集合中嵌入水印数据，然后将集合中像素对在图像中的位置以二值映射图的形式表示，将二值映射图进行无损压缩，再将压缩后的二值映射图以最低有效位压缩的方式嵌入选择的像素对差值中。

该算法的优点是容量比较大，但直接用于图像认证存在 2 个缺陷：

(1)算法实现复杂，需要多次操作才能完成水印的嵌入和提取，容易受到攻击。

(2)图像恢复所需要的附加信息在图像遭到篡改后不能正确提取。

本文对文献[3]的嵌入方法进行改进，将像素对仅分为 2 类：可扩展差值像素对(记为 I 类)和不可扩展像素对(记为 II 类)，满足嵌入条件(3)的像素对称为可扩展差值像素对，其余的像素对称为不可扩展差值像素对。用 I 类像素对位置的二值映射图作为可逆水印图像恢复的附加数据，构造映射图时，I 类赋予 0，II 类赋予 1。映射图尺寸为原图的一半。图 1 给出了 Pepper 图像及 II 类像素对的分布。可以看出，II 类像素对在图像中只占很少的部分。



(a)Pepper 图

(b)II 类像素对分布

图 1 Pepper 图像的 II 类像素对分布

在嵌入时，如果当前像素对为 I 类，则通过差值扩展的方式嵌入 1 位数据；如果为 II 类，则不对像素对进行任何更改，且跳过当前需要嵌入的 1 位数据。

在提取时，则假定所有像素对均为 I 类，提取所有像素对差值的最低位作为隐藏的水印。这样 I 类像素对上提取的信息不会有错误，但 II 类像素对上提取的信息可能会发生错误。因为 II 类像素对在嵌入时未作任何更改。由于嵌入到图像的数据进行了纠错编码，因此照样能从提取水印数据中完全恢复编码前的数据。这样使得水印的嵌入和提取非常简单，一次操作就能完成。

3.2 认证数据的生成

在本方案中，认证数据的作用与数字签名相同，应该对图像的篡改操作具有高度的敏感性。认证数据的生成方法是将图像不重叠地划分为 8×8 的图像子块。对每个图像子块，将块内的所有像素值作为 *hash* 函数的输入，计算认证比特：

$$A_i = hash(D_i, key)$$

其中，D_i 是图像子块的数据；*key* 是用户密钥。认证比特 A_i 是由 *hash* 函数计算得到的 128 bit 序列。除用户密钥外，其他信息可以公开。

基于水印容量和安全性的考虑，提取 128 bit 序列中的 16 bit 作为该图像子块的认证数据。这样，对于每个子块，攻击者伪造成功的概率只有 $1/2^{16}$。所有子块的认证数据一起构成图像的认证数据 A。

3.3 纠错编码的选择

纠错编码作为提高通信系统传输可靠性的有效手段，已广泛用于纠正数据经过不同信道传输后发生的错误。常见的纠错码有多种[6]。

本文采用应用非常广泛的 *BCH* 码作为纠错码。对于任意整数 m（$m \ge 3$）和 t（$t \le 2^{m-1}$），存在 $GF(2)$ 上的 *BCH* 编码 $BCH(n,k,t)$，码长为 $n = 2^m - 1$，其中，k 为信息元的长度；t 为纠错能力，每个码字中能纠正所有的小于或等于 t 个随机错误。显然，为了增强算法抵抗攻击的能力，应该使 t 尽可能的大。下面根据水印容量确定 *BCH* 编码效率。

设图像大小为 $M \times N$。根据嵌入算法，总的数据容量 $C = (M \times N)/2$。

按本文中的认证数据生成方法，总的认证数据 A 的大小 $size(A) = (M/8 \times N/8) \times 16$。

经过大量实验计算，二值映射图经 JBIG2 压缩后 $size(\Delta) < C/10$。所以，编码前数据的大小 $size(A + \Delta) < 0.6C$。选用信息元的长度在 60%左右的编码较为合适，所以，本文的纠错编码采用 $BCH(255,155,13)$ 进行编码，即每嵌入 255 bit 数据中，可以允许其中 13 bit 数据发生错误。

为避免图像局部篡改使某个编码块内数据提取时产生大量错误，在数据嵌入前，先对编码后的数据进行置乱。这样在提取时，图像篡改所造成的提取错误是分散的，从而大大提升纠错码实际的纠错性能。

4 算法实现

4.1 水印生成及嵌入

水印生成及嵌入的步骤如下：

Step1 将图像分为不重叠的 8×8 子块，通过 *hash* 函数计算每个子块的认证比特，提取其中 16 bit 作为认证数据。所有子块的认证数据合在一起作为图像的认证数据 A。

Step2 将原始载体图像中每 2 个相邻像素点作为像素

对，计算像素对的均值和差值。

Step3 根据嵌入条件，得到可嵌入对的二值映射图，并对映射图进行 JBIG2 压缩，得到 Δ。

Step4 将 A 和 Δ 作为水印信息 W，对 W 进行纠错编码，得到要嵌入的信息 W'。

Step5 对 W' 进行置乱，得到 W''，再采用差值扩展的方式将 W'' 嵌入到图像中，得到含印图像。

4.2 水印提取及认证

当收到含印图像后，水印的提取及认证过程如下：

Step1 将每 2 个相邻像素点作为像素对，计算像素对差值和均值。提取的像素对差值二进制表示最低位，得到提取序列。

Step2 对提取序列进行反置乱，然后进行纠错解码，得到解码后的数据。

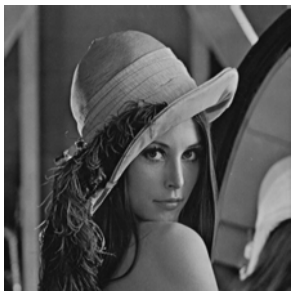
Step3 从解码后的数据中得到认证数据以及二值映射图信息。

Step4 根据二值映射图及像素对的差值和均值，恢复原始图像。

Step5 将图像分块，计算每个图像子块的认证数据，与提取的认证数据进行比较，确定图像子块是否有篡改。

5 实验结果分析

本文采用 Matlab7.1 平台进行仿真试验。图 2 给出了认证水印嵌入后的图像及其 *PSNR* 值。



(a)*PSNR*=35.56 dB

(b)*PSNR*=36.50 dB

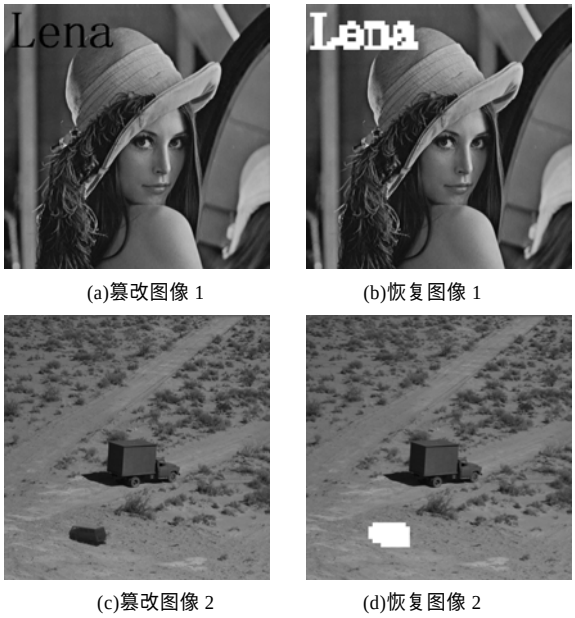
图 2 认证水印嵌入后的图像

从图 2 可以看出，当嵌入水印后，图像并未产生明显失真。如果图像遭到篡改，则图像中一些区域的像素值会发生变化。从变化区域提取的水印数据会有少量的错误。由于 *BCH*(255,155,13) 纠错编码，允许每 255 bit 数据中有不超过 1 bit 的数据错误，因此仍就能正确提取水印信息。

图像块的认证数据通过 *hash* 函数计算，块中任何像素值的改变都能被检测到。

其他未篡改的区域则能完全恢复到原始状态，使得篡改区域之外的图像仍然具有使用价值。

图 3 给出了篡改后的图像及认证结果。



(a)篡改图像 1　(b)恢复图像 1

(c)篡改图像 2　(d)恢复图像 2

图 3 篡改图像和恢复图像

采用纠错编码和置乱，消除了图像块之间的独立性，使得本方案能有效抵抗针对基于块认证算法的矢量量化攻击。在图像块 *hash* 函数计算和认证数据置乱的过程中，可以引入密钥，能很好地保证认证方案的安全性。如果图像未遭到篡改，可以完全恢复原始图像，使得图像的使用价值不受任何影响。

6 结束语

本文结合差值扩展和纠错编码，提出一种可以定位篡改块的可逆图像认证方案。该方案结构简单、实现方便，若通过认证后，则能完全恢复图像的原始状态，否则可以定位篡改的区域。实验结果表明，其对篡改具有很高的敏感性，该方案可以用于对一些重要敏感图像的认证。

参考文献

[1] Swanson M D, Tewfik A H. When Seeing Isn't Believing[J]. IEEE Signal Processing Magazine, 2004, 21(2): 40-49.

[2] Fridrich J, Goljan M. Invertible Authentication[C]//Proc. of SPIE Photonics West. California, USA: [s. n.], 2001.

[3] Tian Jun. Reversible Data Embedding Using a Difference Expansion[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 12(8): 890-896.

[4] Lee S. Reversible Image Authentication Based on Watermarking[C]// Proc. of IEEE International Conference on Multimedia and Expo. Toronto, Canada: [s. n.], 2006.

[5] 彭德云，王嘉祯. 基于错误控制编码的差值扩展可逆数字水印[J]. 计算机工程, 2007, 33(27): 18-20.

[6] 陈鲁生，沈世镒. 编码理论基础[M]. 北京：高等教育出版社, 2005.

编辑　陈　文