

一种高检测率用于彩色图像完整性证明的脆弱盲水印

刘 伟¹, 王凤英²

(1 莱芜职业技术学院, 山东 莱芜 271100; 2 山东理工大学, 山东 淄博 255049)

摘 要: 提出了一种高检测率的用于彩色图像完整性证明的脆弱盲水印算法。将原始图像 R、G、B 色彩分量图像分块, 对各分块进行一次整数小波变换; 将小波系数经函数处理后映射为混沌初值, 经过迭代、量化生成二值水印信息, 然后随机嵌入到小波变换域。本算法利用混沌系统对初值极端敏感性特点增强了水印信息的安全性, 提高了脆弱水印的敏感性。

关键词: 彩色图像; 脆弱水印; 完整性证明; 混沌映射; 整数小波变换

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2011)07-0209-04

Fragile Blind Watermarking of High Detection Rate for Color Image Integrity Authentication

LIU Wei¹, WANG Feng-ying²

(Department of Computer, Laiwu Vocational and Technical College, Laiwu 271100, China)

Abstract: A fragile blind watermarking algorithm of high detection rate for color image integrity authentication was proposed. Firstly, we divided the R, G, B components of image into some blocks, operated integer wavelet transform for each block once, and changed wavelet coefficients through function mapping into the initial value of chaos. The watermark information was obtained by iterating of chaos and quantifying the chaos sequence. At last, we embedded the watermark information into wavelet transform domain randomly. The algorithm improved safety of watermark information and sensitivity of fragile watermarking.

Key words: color image; fragile watermark; tampering proof; chaotic map; integer wavelet transform

1 引言

文中提出一种用于彩色图像完整性证明的脆弱盲水印算法。该算法的特点: (1) 具有较高的图像篡改检测率, 对图像内容的篡改极其敏感。 (2) 解决了变换域算法中的溢出误差问题和舍入误差问题。 (3) 水印的生成及嵌入均结合了混沌系统对初值极端敏感性特点, 具有较高的安全性。 (4) 具有较好的不可见性。 (5) 水印的提取为盲提取, 篡改检测只用到篡改后的水印图像。

2 算法思想

首先, 将原图像分解为 R、G、B 三种色彩分量图

像, 若只考虑对图像构成内容的篡改检测, 则可依据其中一种或两种色彩分量值生成与图像内容相关的水印信息, 再嵌入第三种分量中, 但该算法不适用于对图像的某种色彩分量进行变色篡改检测, 如文献 [1], 且对于变换域算法来讲嵌入的水印量有限。因此, 本算法将 R 色彩分量值生成的水印信息嵌入到 R 分量经小波变换后的四个频带 (LL, HL, LH, HH) 系数中。

同样, 分别生成与 G、B 色彩分量相关的水印信息, 嵌入相应两个分量小波变换系数中。三种色彩分量中都嵌入了水印信息, 可有效检测出对图像的内容及变色修改, 且增加了水印嵌入量, 提高了篡改检测率。

收稿日期: 2010-12-01; 修回日期: 2010-12-25

基金项目: 山东自然科学基金项目 (Y2007G28); 莱芜职业学院基金项目

3 算法具体设计

3.1 图像的预处理

为减少小波变换中的溢出误差,首先对图像作预处理.产生溢出误差的点通常是像素值在 0 和 255 附近的点,可以将 R、G、B 三种色彩分量在 $[0, \delta]$ 和 $[\Delta, 255]$ 之间的值分别改变为 δ 和 Δ ,其中 δ 可取 $[0, 10]$ 之间的整数, Δ 可取 $[245, 255]$ 之间的整数^[2-6].

3.2 水印生成算法

混沌系统具有对初始值极其敏感的特征,即代入两个只有微小差异的初始值得到完全不同的混沌序列;将混沌系统对初值的敏感性特点应用于脆弱水印的构造,使用形式简单的一维 Logistic 混沌系统来生成水印信息,以满足脆弱水印对内容篡改极其敏感的要求.另外,混沌系统良好的随机性和容易再生的特点也可增加水印的安全性.

Logistic 映射表示形式如下:

$$\begin{aligned} x_{n+1} &= f(x_n) = ux_n(1-x_n) \\ x_n &\in [0, 1], \quad n = 1, 2, \dots \end{aligned} \quad (1)$$

其中, n 表示迭代次数, u 为初始参数,当 $u > 3.57$ 时,系统处于混沌状态.

对于 $N \times N \times 24$ 的原始彩色图像,其水印生成步骤如下:

Step1: 将原始图像分解为 R、G、B 三种色彩分量,则每种色彩分量可以看成是一个 8 bit 的灰度图像.

Step2: 对 R 色彩分量图像分块,分块大小为 $m \times m$ ($m = 4, 6, 8, 10, \dots$),则共有 $\lfloor N^2/m^2 \rfloor$ 个分块.

Step3: 随机产生各分块的水印嵌入位置.为避免攻击者通过分析算法达到去除水印的目的,用混沌迭代来产生水印嵌入位置 (p, q) . 选择密钥作为混沌初值,代入式(1),经过 $i + 4c$ 次迭代,考虑到迭代初期生成的混沌序列随机性较差,将前 i 次迭代值丢掉不要,选取第 i 次迭代后的随机序列 $\{y_{i+1}, y_{i+2}, \dots, y_{i+4c}\} \in [0, 1]$,通过映射函数 $M(y) = y(\frac{m}{2} - 1) + 1$ 映射为 $\{s_{i+1}, s_{i+2}, \dots, s_{i+4c}\} \in [1, \frac{m}{2}]$,选取 (s_{i+1}, s_{i+2}) 作为第一个分块的水印嵌入位置,其它分块依次类推,选取 (s_{i+4c-1}, s_{i+4c}) 作为最后一个分块的水印嵌入位置;其中 m 为分块大小, $c = \lfloor N^2/m^2 \rfloor$ 为分块个数.

Step4: 对分块进行一次整数小波变换(可解决

变换域算法中舍入误差问题),得到近似分量 LL、水平细节分量 HL、垂直细节分量 LH 和对角高频分量 HH 的变换系数矩阵.

Step5: 计算近似分量 LL 系数矩阵中除去嵌入点 (p, q) 之外的其他点的系数绝对值的均值(简称绝对均值). 设 (i, j) 处变换系数为 $x_{i,j}$ ($1 \leq i, j \leq m/2$), 计算均值 $\bar{x} = \frac{1}{(m/2)^2 - 1} \sum_{i \neq p} \sum_{j \neq q} |x_{i,j}|$.

Step6: 将均值 $\bar{x} \in R$ 通过函数 $M(\bar{x}) = \frac{\pi}{2} \cdot$

$|\arctg(\bar{x})|$ 映射为混沌初值 $x_0 \in [0, 1]$, 然后带入式(1), 经过 l ($l > 1$) 次迭代后, 对生成的实值序列 $\{y_1, y_2, \dots, y_l\}$ 进行量化处理. 定义量化函数:

$$Q(y(i)) = \begin{cases} 0, & y(i) \leq 0.5 \\ 1, & y(i) > 0.5 \end{cases} \quad (1 \leq i \leq l)$$

在量化后得到的二值序列中选择第 l 位数用作嵌入到该分量系数矩阵 (p, q) 处的水印信息. 为保证水印信息的安全性, l 的选取也可作为水印生成时的密钥.

Step7: 对其他方向的三个分量分别进行 5、6 步骤的处理.

Step8: 依次对 R 色彩分量图像各分块进行 4 ~ 7 步操作.

至此, 基于 R 色彩分量值共生成了 $4 \lfloor N^2/m^2 \rfloor$ bit 水印信息.

Step9: 分别对 G、B 色彩分量图像做与 R 色彩分量图像同样的处理, 得到相应水印信息.

3.3 水印嵌入算法

在水印生成阶段, 对色彩分量图像的每个分块进行一次整数小波变换, 然后根据四个方向分量的变换系数产生 4bit 水印信息. 将这 4bit 的水印信息, 通过对变换系数的量化, 分别嵌入到四个方向分量中, 水印嵌入位置的选择见 3.2 节 Step3. 可以看到这种水印嵌入方法有利于提高篡改识别率. 具体嵌入步骤如下:

(1) 将依据 R 色彩分量图像产生的水印信息嵌入到其各分块的四个方向分量中.

Step1: 对 R 色彩分量图像分块近似分量系数的量化. 定义近似分量系数 x_{i_u} 的量化函数为:

$$Q_1(x_{i_u}) = \begin{cases} 0, & r\Delta \leq x_{i_u} \leq (r+1)\Delta, \quad r = 0, \pm 2, \pm 4, \dots \\ 1, & r\Delta \leq x_{i_u} \leq (r+1)\Delta, \quad r = \pm 1, \pm 3, \pm 5, \dots \end{cases}$$

其中, Δ ($\Delta > 0$) 为近似分量系数的量化阶距. 嵌入规则如下: 若 $Q_1(x_{i_u}) = w_u$, 则 $x_{i_u}^w = x_{i_u}$; 否则按下

式修改:

$$x_{i_u}^w = \begin{cases} x_{i_u} + \Delta, & x_{i_u} \leq 0 \\ x_{i_u} - \Delta, & x_{i_u} > 0 \end{cases}$$

其中, w_u 为根据该分量系数矩阵生成的水印信息, $x_{i_u}^w$ 为量化后的变换系数. 通过该量化函数完成近似分量系数矩阵中水印嵌入位置 (p, q) 处系数的量化, 从而实现近似分量水印的嵌入.

Step2: 对细节分量系数的量化. 定义细节分量系数 x_{i_u} 的量化函数为:

$$Q_2(x_{i_u}) = \begin{cases} 0, & \lfloor \frac{x_{i_u}}{2\Delta'} \rfloor \text{为奇数} \\ 1, & \lfloor \frac{x_{i_u}}{2\Delta'} \rfloor \text{为偶数} \end{cases}$$

其中, $\lfloor \cdot \rfloor$ 表示向下取整, $\Delta' (\Delta' > 0)$ 为细节分量系数的量化阶距. 嵌入规则如下: 若 $Q_2(x_{i_u}) = w_u$, 则 $x_{i_u}^w = x_{i_u}$; 否则按下式修改:

$$x_{i_u}^w = \begin{cases} x_{i_u} + 2\Delta', & x_{i_u} \leq 0 \\ x_{i_u} - 2\Delta', & x_{i_u} > 0 \end{cases}$$

其中, w_u 为根据细节分量系数矩阵生成的水印信息, $x_{i_u}^w$ 为量化后的变换系数. 通过该量化函数完成细节分量系数矩阵中水印嵌入位置 (p, q) 处系数的量化, 从而实现三个细节分量水印的嵌入.

Step3: 对嵌入水印后的变换系数进行整数小波逆变换, 重构分块图像.

Step4: 对各个分块分别进行上述操作.

至此, 在 R 色彩分量图像各个分块的四个方向分量中分别随机嵌入了 1 bit 的水印信息. 之所以一个方向分量只嵌入 1 bit 水印信息而不是更多, 主要考虑到水印的不可见性, 水印信息嵌入过多, 不可见性会变差. 另外, 在水印生成算法中, 将图像分块四个方向分量的小波变换系数的绝对均值作为混沌初值, 带入混沌映射, 经混沌迭代、量化后生成 4 bit 水印信息, 若该分块遭到篡改, 篡改后的小波变换系数的绝对均值一定会发生改变, 在理论上, 此时从各分量中提取出的 1 bit 水印信息与图像未篡改前嵌入的 1 bit 水印信息完全不同, 这足以证明各分量变换系数发生了改变, 图像遭到篡改. 将水印信息嵌入到四个方向分量, 是为了提高篡改检测率.

(2) 按照步骤(1), 分别将依据 G、B 色彩分量图像产生的水印信息嵌入到相应各分块的四个方向分量中.

3.4 水印提取与认证

水印提取是水印嵌入的逆过程, 整个水印提取

过程不需要原始图像. 水印信息的提取步骤如下:

(1) 将水印图像分解为 R、G、B 三种色彩分量图像.

(2) 提取 R 色彩分量图像中的水印信息.

Step1: 对 R 色彩分量图像进行 $m \times m$ 分块, 然后按照 3.2 节 Setp3, 得到水印嵌入位置 (p, q) .

Step2: 对分块进行一次整数小波变换, 得到四个方向分量的变换系数矩阵.

Step3: 采用与嵌入过程同样的量化函数完成对水印嵌入位置 (p, q) 处系数的量化. 若水印嵌入位置的系数表示为 $\hat{x}_{i_u}$, 提取出的水印信息为 $\hat{w}_u$, 则 $\hat{w}_u = Q_2(\hat{x}_{i_u})$, 对于近似分量系数 $j = 1$, 细节分量系数 $j = 2$.

Step4: 对每个分块进行 Step2、Step3 步骤处理, 将嵌入到 R 色彩分量图像中的所有水印信息 w_R 提取出来.

(3) 同样方法, 提取出 G、B 色彩分量图像中的水印信息 w_G, w_B .

对某图像的完整性产生质疑时, 可以通过以下方式来实现认证:

依照水印生成过程, 将质疑图像分解为 R、G、B 三种色彩分量图像, 然后分别对每个色彩分量图像进行分块, 将各分块四个方向分量的小波变换系数的绝对均值映射为混沌初值, 经过混沌迭代、量化生成各色彩分量的水印信息 $\tilde{w}_R, \tilde{w}_G, \tilde{w}_B$. 按照水印提取算法, 设 $\hat{w}_R, \hat{w}_G, \hat{w}_B$ 为从质疑图像三种色彩分量图像中提取出来的水印信息. 将 $\tilde{w}_R$ 与 $\hat{w}_R, \tilde{w}_G$ 与 $\hat{w}_G, \tilde{w}_B$ 与 $\hat{w}_B$ 分别分段 (每段对应色彩分量图像中一个分块的 4 bit 水印信息) 进行比较, 若每个分段中有 1 bit 水印信息发生改变, 就可以认为该段对应的色彩分量图像块发生了篡改.

4 实验结果与分析

4.1 不可见性

脆弱水印要求加入的水印不可察觉, 为了衡量水印图像和原始图像之间的差别, 定义峰值信噪比 PSNR =

$$\frac{1}{3} 10 \log_{10} \left(\frac{\text{Max}_{I_R}^2}{\frac{1}{N \times N} \sum_{i=1}^N \sum_{j=1}^N (I_R(i, j) - I'_R(i, j))^2} \right) + \frac{\text{Max}_{I_G}^2}{\frac{1}{N \times N} \sum_{i=1}^N \sum_{j=1}^N (I_G(i, j) - I'_G(i, j))^2}$$

$$+ \frac{\text{Max}_{I_B}^2}{N \times N \sum_{i=1}^N \sum_{j=1}^N (I_B(i,j) - I'_B(i,j))^2}$$

其中, Max_{I_R} 、 Max_{I_G} 、 Max_{I_B} 分别为 R、G、B 三种色彩分量的最大值, I_R 为原图像的 R 色彩分量像素值, I'_R 为水印图像的 R 色彩分量像素值. 选取原始图像为 $256 \times 256 \times 24$ 的彩色图像 Couple 和 $512 \times 512 \times 24$ 的彩色图像 Lena. 嵌入水印后, 计算其峰值信噪比分别为 42.272 dB、42.635 dB. 由此可见该算法具有良好的不可见性. 原始图像与水印图像对比如图 1 所示.

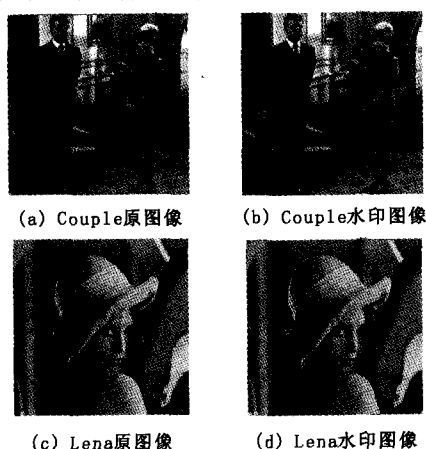


图 1 原始图像与水印图像对比图

4.2 敏感性分析

混沌系统对初始值有极其敏感的依赖性, 即对两个只有微小差异的初始值也将得到完全不同的混沌序列. 我们将小波变换后的系数取绝对均值映射为混沌初值, 即使图像有微小变化, 篡改后的系数绝对均值也一定会发生改变, 最后迭代生成的混沌序列与未篡改前生成的序列将是两个完全不同的序列, 从而保证了脆弱水印的高度敏感性.

4.3 篡改检测率分析

在 R、G、B 三种色彩分量图像的每个分块中嵌入 4bit 水印信息 (嵌入到分块经小波变换后的四个方向分量中). 当彩色图像的某个分块被篡改, 则三种色彩分量对应分块都发生改变的概率为 $\frac{1}{7}$, 两种色彩分量对应分块或只有一种色彩分量对应分块发生改变的概率均为 $\frac{3}{7}$. R、G、B 三种色彩分量对应分块共 12bit 水印信息只要有 1 位发生改变, 即判定该图像分块发生了篡改, 则总的篡改检测率 $P = \frac{1}{7}(1 - \frac{1}{2^{12}}) + \frac{3}{7}(1 - \frac{1}{2^8}) + \frac{3}{7}(1 - \frac{1}{2^4}) \approx 0.97$, 远高于同类文献 [1]、[4] 的篡改检测率 0.75、0.61.

4.4 安全性分析

(1) 水印嵌入位置的安全性

本算法采用混沌迭代随机产生各分块的水印嵌入位置 (p, q) , 混沌映射初值 x_0 可作为密钥. 由混沌系统对初值极其敏感的特征, 尽管初始值与密钥相差很小, 经过若干次迭代后得到的也是完全不同的随机序列, 这样可有效避免攻击者通过分析算法达到去除水印的目的.

(2) 水印信息选择的安全性

本算法将分块图像的小波变换系数的绝对均值映射为混沌初值, 通过混沌迭代、量化得到二值序列, 选择二值序列中的第 l 位用作嵌入到该分量系数矩阵 (p, q) 的水印信息. 将 l 的选取作为水印生成时的密钥, 同样保证了水印信息的安全性.

5 结束语

文中提出了一种高检测率的用于彩色图像完整性证明的脆弱盲水印. 将彩色图像分解为 R、G、B 三种色彩分量, 然后分别对其分块, 将分块图像的小波系数经函数处理后映射为混沌初值, 通过迭代、量化生成水印信息. 混沌映射的引入增强了算法的安全性和对图像内容篡改的敏感性. 对原始图像的预处理与采用整数小波变换减少了溢出误差和舍入误差. 实验证明, 该算法具有很高的篡改检测率和准确的篡改定位能力, 且水印提取为盲提取.

参考文献:

- [1] 贺文华. 一种彩色图像内容混沌脆弱水印算法[J]. 湖南大学学报: 自然科学版, 2009, 36(1): 55-58.
- [2] Holliman M, Memon N. Counterfeiting attacks on oblivious block-wise fragile authentication watermarking[J]. IEEE Trans, Image and Signal Processing, 2009, 9(3): 432-441.
- [3] 华先胜, 石青云. 多类水印的同时嵌入[J]. 北京大学学报: 自然科学版, 2001, 37(3): 305-314.
- [4] 王向阳, 杨红颖, 侯丽敏. 一种新的半脆弱彩色图像数字水印算法[J]. 自动化学报, 2007, 33(6): 561-564.
- [5] R. J. Cintra, et al. Fragile watermarking using finite field trigonometrical transforms [J]. Signal Process Image Commun, 2009: 1061-1069.
- [6] 刘伟, 王凤英. 基于混沌与整数小波变换的脆弱盲水印[J]. 微电子学与计算机, 2007(11): 127-130.

作者简介:

刘伟女, (1978-), 教师. 研究方向为信息安全.