用于图像认证的小波域双重脆弱水印算法研究

李占德,张政保,文家福,黄子龙
(军械工程学院 计算机工程系,河北 石家庄 050003)

摘 要:针对当前小波域脆弱水印图像认证算法不能有效抵抗矢量量化攻击以及虚警率和漏警率较高的问题,基于混沌理论和块相关策略,提出一种小波域双重脆弱水印图像认证算法。算法首先对载体图像分块并建立块相关映射表;再对每一图像块作一级整数提升小波变换,利用 Logestic 混沌系统生成基于近似子带 LL 特征的水印信号;最后将水印信号分别嵌入相关图像块的细节子带 HL 和 LH。实验结果表明,该算法不仅能很好地抵抗矢量量化攻击,而且具有较低的虚警率和漏警率,能很好地实现图像完整性认证功能。

关键词:双重脆弱水印;块相关;混沌系统;篡改定位
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2011)02-0181-04

Wavelet Domain Double Fragile Watermarking Algorithm for Image Authentication

LI Zhan-de, ZHANG Zheng-bao, WEN Jia-fu, HUANG Zi-long
(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: Aiming at problems of wavelet domain fragile watermarking image authentication algorithm being nonresistance to the vector-quantization attack and with high False Alarm Probability(FAP) and Miss Alarm Probability(MAP), a wavelet domain double fragile watermarking algorithm is proposed in this paper. Firstly, the image is divided into many sub-blocks, and a block-dependent mapping table is created; then each sub-block is executed the lwp2, and watermark is created using the Logestic Chaos system with the LL; Last, the watermark is embedded into its correlative sub-block's HL and LH. Experimental results show that the algorithm not only resists well the vector quantization attack, but also has lower FAP and MAP, and does well in image authentication.

Key words: double fragile watermarking; block dependence; chaos system; tamper localization

0 引 言

随着信息技术的迅猛发展,数字产品的安全问题愈发成为严重的社会问题。比如,对医学图像的篡改可能造成误诊,用于法庭证据的图像经过篡改可能扭曲事实真相,这就需要对图像的真实性和完整性进行验证。传统的密码技术已不能很好地满足图像完整性验证的需求,脆弱水印技术为解决这些问题提供了一种有效途径[1]。

基于离散小波变换域的数字水印技术具有良好的多分辨表示和时频局部等特性,且兼容 JPEG2000 压缩标准,因此基于 HVS 的小波域数字水印已成为当今水印算法的主流。目前已有不少基于 HVS 的小波域量化数字水印算法[2,3],主要采用均值量化和非均值量化嵌入策略[4,5]。量化步长取值较小,则会影响水印的抗攻击性;量化步长取值较大,会给图像质量带来较大影响。同时,为了提高篡改定位的精度,算法普遍采用块独立的认证方案[6,7],存在不能有效抵抗矢量量化攻击的问题[8]。

本文分析现有算法存在问题,基于混沌理论和块相关策越,提出一种小波域双重脆弱水印图像认证算法,并分析了算法的性能。利用混沌系统建立图像块映射关系,及生成基于图像块内容特征的水印信号,可有效抵抗矢量量化攻击;采用将水印信号分别嵌入相关图像块细节子带 HL 和 LH 的策略,在保证较低漏警率的同时,可有效降低虚警率和漏警率。

1 相关理论

1.1 整数提升小波变换

图像小波多级变换的实质是图像的多分辨率分解。一幅图像经小波变换分解后,产生 LL、HL、LH 和 HH 四个子带。继续对低频部分 LL 进行多级分解,分

收稿日期:2010-06-08;**修回日期**:2010-09-13
基金项目:河北省自然科学基金资助项目(F2011506007)
作者简介:李占德(1984-),男,硕士研究生,研究方向为网络信息安全、图像认证;张政保,教授,硕士生导师,研究方向为信息安全、多媒体信息处理。

解出更低频率的低频信号和高频信号，从而实现多分辨率分析。小波变换将信号分成低频和高频信息，低频部分集中了信号的大部分能量，高频部分集中了信号的大部分细节。小波变换还能很好的进行频率到空间的定位。图像二级小波分解及定位见图 1。

当嵌入水印的图像小波系数被篡改，并且完成了小波逆变换，嵌入水印的图像像素一定会取整形成一个新的图像。取整操作会导致图像像素的改变，所以会引起嵌入水印后的图像中的水印和原来的水印有区别。整数提升小波变换将系数变成整数，从而解决了无法精确重构小波系数，而且算法简单、速度快、对内存的需求量小[9]。所以，本文采用整数提升小波变换进行水印的嵌入和提取。

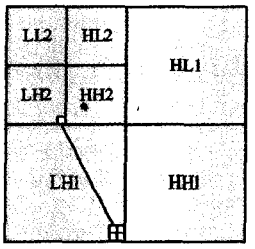


图 1 图像二级小波分解示意图

1.2 混沌系统

混沌指一种貌似无规则地运动，在确定性非线性系统中，不附加任何随机因素也可以出现类似随机的行为，但支配这种运动却可以用确定型的方程来描述。混沌系统最大的特点就在于系统的演化对初始条件非常敏感，初始状态的微小不确定性将会迅速地按照指数速度扩大，在混沌系统中不可能对系统的状态进行长期的预测。

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程。这种过程既非周期又不收敛，并且对初始值有极其敏感的依赖性[10]。依据混沌系统对初始值的敏感依赖性，可以提供数量众多、非相关、类随机而又确定可再生的信号。混沌序列是一个伪随机序列，很容易由迭代方程或非线性方程生成。

一类非常简单却被广泛研究的动力系统是 Logistic 映射，其定义如下：

$$x_{k+1} = \mu x_k(1 - x_k) \quad 0 < \mu \leq 4 \tag{1}$$

其中，μ 称为分支参数。当 $3.5699456\cdots < \mu \leq 4$ 且 $0 < x_k < 1$ 时，Logistic 映射处于混沌状态，给定的不同的初始值 x_0 和分支参数 μ，所得序列非周期、不收敛且不相关[8]。

经过变换，Logistic 映射在 $(-1,1)$ 上的定义可以表示为：

$$x_{k+1} = 1 - \lambda x_k^{\,2}, \quad \lambda \in (0,2) \tag{2}$$

随着 λ 的逐渐增大，迭代会出现多次突变，当 $\lambda = 1.40115$ 时，系统进入混沌状态，产生具有 0 均值、δ - like 自相关性及互相关为 0 的混沌序列，该序列具有高斯白噪声的统计特性。

利用 Logistic 混沌映射生成的实值混沌序列建立图像块之间的循环块相关关系，称之为混沌排序，过程如下：假设图像块数为 P，将密钥 k 作为 Logistic 混沌映射的初始值 x_0 代入式(1)，生成长度为 P 的实值混沌序列 $\{x_1, x_2, \cdots, x_P\}$；利用选择排序法对其进行排序，生成有序序列 $\{y_1, y_2, \cdots, y_P\}$；并记录序列 $\{x_1, x_2, \cdots, x_P\}$ 中每个元素在序列 $\{y_1, y_2, \cdots, y_P\}$ 中的位置次序，建立块关联关系查找表 LUT。

2 水印生成与嵌入

假设载体图像 I 大小为 $M \times M$ 像素，互不重叠图像块大小为 $m \times m$ 像素。在小波域中高低频部分具有不同的特点：低频部分集中了图像的大部分能量，所以在低频部分集中了图像的大部分信息；高频部分代表了图像的边缘及纹理部分，在这里嵌入水印，人眼虽然不容易发觉。将混沌理论引入数字水印算法，利用 Logistic 映射产生基于小波变换低频系数特征的水印信号，并将该水印信号潜入小波变换高频系数。

2.1 水印生成

利用混沌序列作水印信号，具有易于生成、数量极多和对初始条件敏感的优势。基本思想是将密钥作为混沌系统初值，迭代生成混沌序列来调制图像块近似子带 LL 系数，产生混沌初值，再经混沌迭代生成水印信号。步骤如下：

(1)将图像 I 划分为 n 个互不重叠的 $m \times m$ 大小的图像块 I_p（p 为块编号，I_p^{ll} 代表图像块 I_p 的小波低频子带 LL)，进行一级整数提升小波变换。选取密钥 k_1，利用混沌排序建立块相关映射表 LUT。

(2) 将 k_1 作为初值代入式(1)，生成长度为 n 的混沌序列 $S:\{s_1, s_2, \cdots, s_n\}$，将 s_p 带入式(3)调制 I_p^{ll} 的像素值 $P:\{p_1, p_2, \cdots, p_{m^2/4}\}$ 产生 I_p 混沌初值 x_0^p；将 x_0^p 代入式(1)生成长度为 l 的混沌序列，选取后 $m^2/4$ 个元素，依阈值 α 二值化及 $\frac{m}{2} \times \frac{m}{2}$ 变形产生 I_p 的水印信号 w_p。

$$x_0^p = s_j\left(\sum_{i=1}^{m^2/4} p_i\right) / \frac{m^2}{4}\max(P) \tag{3}$$

$s_j \in S, j = 1,2,\cdots,n; p_i \in P, i = 1,2,\cdots,m^2/4$。

(3)重复步骤(1)、(2)生成所有图像块的水印信号。

2.2 水印嵌入

本文基于小波低频子带特征生成水印信号，这是因为低频子带集中了图像的主要能量，是对图像的最

佳逼近。而高频子带是对图像细节特征的描绘,人眼不太敏感。因此,为降低虚警/漏警率和提高定位精度,本文将水印信号分别嵌入图像块一级小波变换的 HL 和 LH 子带,嵌入量化步长为 2。嵌入步骤如下:

(1)对图像块 I_p,查找 LUT,找出其相关图像块 I_q。按公式(4)将 w_P 分别嵌入 I_q^{lh}、I_q^{hl}。

$$\begin{cases} I_q^{hl(i,j)} = I_q^{hl(i,j)} - \mathrm{mod}(I_q^{hl(i,j)},2) + w_p(i,j) \\ I_q^{lh(i,j)} = I_q^{lh(i,j)} - \mathrm{mod}(I_q^{lh(i,j)},2) + w_p(i,j) \end{cases} \tag{4}$$

其中,$I_q^{hl(i,j)}$、$I_q^{lh(i,j)}$ 代表图像块 I_q 的细节子带 HL 和 LH 的小波系数。

(2)重复步骤(1)对所有图像块嵌入水印信号。

3　水印提取与认证

要判断一个图像是否被篡改,需要提取水印信号,生成参考水印信号,并比较二者是否相等进行篡改认证。

3.1　水印提取

假定可疑图像为 I',水印提取步骤如下:

(1)将 I' 划分为 n 个互不重叠的 $m \times m$ 大小的图像块 I_p';选取密钥 k_1,建立块相关映射表 LUT。

(2)对于图像块 I_p',查找 LUT,找出其相关块 I_q',按公式(5)提取水印 w_p'。

$$\begin{cases} W_p'^{hl(i,j)} = \mathrm{mod}(I_q'^{hl(i,j)},2) \\ W_p'^{lh(i,j)} = \mathrm{mod}(I_q'^{lh(i,j)},2) \end{cases} \tag{5}$$

(3)利用水印生成步骤(2)生成 n 组参考水印 w_p'。

3.2　篡改认证

对于可疑图像块 I_p' 的认证,利用密钥 k_1 查找 LUT,找到与图像块 I_p' 相关的图像块 I_q',认证步骤如下:

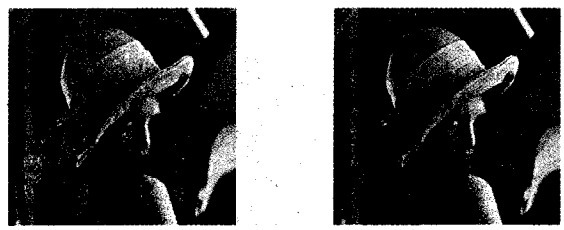
(1)如果 $w_p' = w_p'^{hl} = w_p'^{lh}$,判定图像块 I_p' 未被篡改,图像块 I_q' 水印未被篡改;如果 $w_p' = w_p'^{hl}$ 或 $w_p' = w_p'^{lh}$,标记图像块 I_p' 为待查状态,判定图像块 I_q' 水印被篡改。

(2)如果 $w_p' \neq w_p'^{hl}$,$w_p' \neq w_p'^{lh}$ 且 $w_p'^{hl} = w_p'^{lh}$,判定图像块 I_p' 被篡改,图像块 I_q' 水印未被篡改;如果 $w_p' \neq w_p'^{hl}$,$w_p' \neq w_p'^{lh}$ 且 $w_p'^{hl} \neq w_p'^{lh}$,标记图像块 I_p' 为待查状态,判定图像块 I_q' 水印被篡改。

(3)对所有图像块进行上述步骤(1)、(2)操作。对标记为待查状态的图像块 I_p',如果其水印被篡改,则判定图像块 I_p' 被篡改;反之,则判定图像块 I_p' 未被篡改。

4　实验及分析

本文选用 512 × 512 的 256 级的灰度图像“lena.bmp”,在 Matlab7.1 平台上进行实验。其中图像块大小为 8 × 8;Logestic 混沌系统分支参数 $\mu = 4.0$,迭代次数 $l = 256$,二值化阈值 $\alpha = 0.5$;密钥 $k_1 = 0.1500$,$k_2 = 0.3900$。整数提升小波变换选择“haar”小波基。图 2 为载体图像和含印图像(PSNR 为 47.78dB),图 2 为实验及结果。



(a)载体图像　　(b)含印图像

图 2　水印嵌入

4.1　攻击实验

为验证算法抵抗攻击的敏感性和定位攻击的精确性,对含印图像进行一系列攻击实验,如图 3 所示:(a)为对含印图像进行 95% JPEG 压缩,(b)为对含印图像局部区域(方形区域)增强 1 个像素值,(c)为剪切含印图像脸部区域,(d)为涂画含印图像;(e)、(f)、(g)、(h)为对应的检测结果。实验(a)、(b)为非恶意操作,(c)、(d)为恶意操作。

从实验结果可以看出,无论对 95% JPEG 压缩和局部像素增强等非恶意操作,还是对局部剪切和覆盖等恶意篡改,算法都具备很强的敏感性和精确的定位精度。

4.2　性能分析

(1)嵌入失真。

峰值信噪比(PSNR)常被用来评测含印图像和载体图像的差别。一般来说 PSNR 值在 39dB 以上,人眼基本分辨不出载体图像和含印图像间的差别[11]。实验中 PSNR 等于 47.78dB,嵌入失真较小。

(2)虚警/漏警率。

①当提取的双重水印信号相同并且与生成的参考水印信号也相同的情况下,才判定可疑图像块未被篡改。所以漏判的漏警率:

$$P = \frac{1}{2^{m^2/4}} \times \frac{1}{2^{m^2/4}} = \frac{1}{2^{m^2/2}}$$

②当提取的双重水印信号相同并且与生成的参考水印信号不相同的情况下,才判定可疑图像块被篡改。所以错判的虚警率:

$$P = \frac{1}{2^{m^2/4}} \times \left(1 - \frac{1}{2^{m^2/4}}\right) = \frac{1}{2^{m^2/4}} - \frac{1}{2^{m^2/2}}$$

(3)敏感性及定位精度。

①脆弱水印要具有极高的敏感性,要对一切图像

(a) 95% JPEG 压缩 (b) 局部区域增强 (c) 局部剪切攻击 (d) 覆盖攻击

(e) a 检测结果 (f) b 局部区域增强 (g) c 检测结果 (h) d 检测结果

图 3 实验及结果

操作作出反映。4.1 节进行了非恶意操作和恶意篡改的攻击实验。实验结果表明,无论对于非恶意操作还是恶意篡改,算法都具备很强的敏感性。

②载体图像按 $m \times m$ 大小分块,图像块中任一像素改变均会导致图像块被判定篡改,算法的篡改定位精度为 $m \times m$ 图像块。

(4)算法安全性。

脆弱性水印的安全性与使用的密钥密切相关,一旦密钥被推断出,攻击者就可能在任意图像中伪造水印,从而使水印失效[12]。本文利用 Logistic 混沌系统建立图像块间的映射关系,生成基于图像块特征的水印信号。由于混沌系统对初值的极端敏感性,使得密钥空间无限大,致使攻击者进行穷举攻击得到密钥的可能性几乎为零;同时基于图像块特征生成水印信号也有效抵抗了矢量量化攻击。

5 结束语

提出一种用于图像认证的小波域双重脆弱水印算法。算法具有以下优点:(1)利用混沌系统对初值的极端敏感性生成水印信号,对篡改具有高度敏感性;(2)采用基于图像特征生成水印信号和基于块相关的水印嵌入策略,增强抵抗矢量量化攻击的能力;(3)将水印信号重复嵌入小波高频子带 HL 和 LH,有效降低虚警率和漏警率。实验结果表明,算法能有效抵抗矢量量化攻击,降低虚警率和漏警率,能很好地实现图像完整性认证功能。

参考文献:

[1] 李东勤,林克正. 基于混沌映射的半脆弱图像水印算法[J]. 计算机技术与发展,2008,18(11):156-158.

[2] Kunder D, Hatzinakos D. Towards a telltale watermarking technique for tamper-proofing[C]//In: Proceedings of the IEEE International Conference on Image Processing. Chicago: [s. n.],1998:409-413.

[3] Paquest A H. Wavelet-based digital watermarking for image authentication[C]//In: IEEE Canadian Conf on Electrical and Computer Engineering. [s. l.]:[s. n.],2002:879-884.

[4] 王向阳,杨红颖,邬 俊. 一种基于自适应量化的半脆弱图像水印算法[J]. 小型微型计算机系统,2006,27(5):896-900.

[5] 顾 伟,吕皖丽,罗 斌. 基于图像分类的矢量量化数字水印算法[J]. 计算机应用研究,2009,26(7):2738-2740.

[6] 齐影虹,雷 赞. 基于混沌序列和 HVS 的盲数字水印算法[J]. 计算机应用与软件,2009,26(3):283-285.

[7] Wong P, Memon N. Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification[J]. IEEE Transactions on Consumer Electronics, 2000, 46(2):313-317.

[8] Holliman M, Memon N. Counterfeiting attacks on oblivious block-wise independent invisible water-rmarking schemes [J]. IEEE Trans Image Process,2000,9(3):432-441.

[9] 杨厚俊,崔雪英,范延滨. 基于提升小波和纠错编码的复合型盲水印技术[J]. 计算机工程,2007,33(14):142-144.

[10] 杨蒙召,李朝峰,许 磊. 基于混沌加密和零树编码的彩色图像水印算法[J]. 计算机技术与发展,2006,16(10):157-159.

[11] 程其江,吕述望,李劲松. 一种带纠错功能的鲁棒数字图像水印算法[J]. 计算机应用与软件,2009,26(10):212-214.

[12] 桑 军,向 宏,胡海波,等. 一种脆弱图像水印的安全性分析与改进[J]. 系统工程与电子技术,2009,31(5):1204-1208.