# 一种基于 Hash 函数的脆弱水印算法

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

**摘 要**：当前空域脆弱水印算法存在安全性不高及不能有效抵抗矢量量化攻击的缺陷。针对该缺陷，提出一种用于数字图像完整性认证及内容篡改证明的脆弱水印算法。算法首先对图像进行 8×8 分块，利用 Logistic 混沌映射对图像分块进行置乱编号；再采用 Hash 函数生成基于图像分块内容和位置信息的水印信号；最后将水印信号嵌入到图像分块像素值的低两位平面。实验结果及理论分析表明，提出的脆弱水印算法在保证安全性的同时，有效地抵抗了矢量量化攻击。

**关键词**：脆弱水印；Hash 函数；混沌映射；完整性认证；篡改定位
**中图分类号**：TP301.6　　**文献标识码**：A　　**文章编号**：1673-629X(2011)02-0151-04

# Fragile Image Watermarking Algorithm Based on Hash Function

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

**Abstract**: At present, the flaws of the airspace fragile image watermarking algorithm are the low security and lack of effective resistance to the vector attacks. To solve the problem, a fragile watermarking scheme is presented for tamper-proof digital authentication and content tamper testification. Firstly, dividing the image into blocks of 8×8, using the Logistic chaotic map generates the block watermark; Then create the fragile image watermarking based on image-blocking by Hash function; Finally, embedding the watermarking signals into the 2 bit LSB of the blocks of image. Experimental results indicate that the fragile image watermarking algorithm based on Hash function can not only ensure the security in system, but also efficiently resist the vector quantization attacks.

**Key words**: fragile watermarking; Hash function; chaotic map; integrity authentication; tamper localization

## 0 引 言

随着网络技术的发展，多媒体内容的完整性认证，尤其是图像的完整性验证，引起了人们的高度重视。数字图像由于数据量大、冗余性高、对失真不敏感、保密性低、易编辑和修改且格式繁多等特点，传统的密码技术已经不能很好地满足图像完整性认证的需求。脆弱水印技术为解决这些问题提供了一种有效途径[1~3]。

Walton 在文献[4]中首次提出一种基于易碎水印的图像认证算法，通过计算像素值的校验和来产生易碎水印。这种方法简单、高效，但是不够安全，并且篡改定位能力较差。Wong 在文献[5]中首次提出一种基于分块独立算法，主要思想是把图像分割为各个独立的小块，然后分别在各个小块上嵌入各自的水印，该算法可将篡改定位到独立子块。文献[4]是将所有像素值中的高 7 位的检验和作为水印嵌入到图像的最低有效位(LSB)平面，该算法可以很好地实现图像中被修改内容的位置检测，但对伪认证攻击却无能为力。文献[6]把图像低频子带系数通过正、负调制嵌入大于某个给定阈值的小波域系数，提出的脆弱水印具有一定的篡改定位能力，但定位精度不高，并且对于阈值选取往往比较困难。

针对以上问题，文中利用 Logistic 混沌映射对图像分块进行置乱编号，达到了对图像分块置乱的目的，并将其作为 Hash 函数的参数之一生成水印信号，使攻击者很难通过破解密钥找到正确的水印生成参数，也就无法正确伪造水印，有效抵抗了伪认证攻击，同时有效提高了图像篡改检测的概率及篡改定位的精度。有效克服了文献[4,6]方案的不足。

## 1 哈希函数

哈希函数(Hash Function)又称单向散列函数，是进行数据加密/编码的一种算法，一般用于数字签名、消息的完整性检测和消息的起源性检测等[7]。单向散列函数 Hash ($M$) 作用于一任意长度的消息 $M$，它返

**收稿日期**：2010-06-06；**修回日期**：2010-09-22
**基金项目**：河北省科技计划基金项目(05213579)
**作者简介**：黄子龙(1986-)，男，硕士研究生，研究方向为信息安全、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。

回一固定长度的散列值 $H$:

$$H = \mathrm{Hash}(M) \tag{1}$$

其中 $H$ 的长度为 $m$。

输入为任意长度且输出为固定长度的函数有很多种,但单向散列函数还具有使其单向的如下特性:

· 给定 $M$,很容易计算 $H$。

· 给定 $H$,根据 $H = \mathrm{Hash}(M)$ 计算 $M$ 很难。

· 给定 $M$,要找到另一消息 $M'$ 并满足 $\mathrm{Hash}(M) = \mathrm{Hash}(M')$ 很难。

在一些应用中,仅有单向性是不够的,还需要称之为抗碰撞(Collision-Resistance)的条件:

要找出两个随机的消息 $M$ 和 $M'$,使 $\mathrm{Hash}(M) = \mathrm{Hash}(M')$ 满足很难。

因为消息摘要为 $m$ bit,任何人想要得到两个具有相同摘要的消息,大约需要尝试 $2^{m/2}$ 个消息。若 $m = 64$,则需检查 $2^{32}$ 个消息,这在计算上是可行的。大多数的单向散列函数产生 128 位的散列值。这迫使试图进行生日攻击的人必须对 $2^{64}$ 个随机文件进行散列运算才能找到散列值相同的两个文件。NIST 在其安全散列标准(SHS)中用的是 160 位的散列值。这使生日攻击更难进行,需要 $2^{80}$ 次随机散列运算。

## 2 混沌映射

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。通过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。混沌伪随机序列已被广泛应用于扩频通信、密码学和图像处理等领域,在数字水印技术中也得到广泛应用[8,9]。

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:

$$x_{k+1} = \mu x_k(1 - x_k) \tag{2}$$

其中,$0 < \mu \leq 4$ 称为分支参数,$0 < x_k < 1$,$k = 0, 1, \cdots$ 为迭代次数。当 $3.5699456\cdots < \mu \leq 4$ 时,Logistic 映射处于混沌状态,给定初值 $x_0 \in (0,1)$ 和迭代次数 $n-1$,由式(1)生成长度为 $n$ 的混沌序列 $\{x_k\}$,$k = 0, 1, \cdots, n-1$。由于混沌系统对初值有极端敏感性,给定的不同的初值 $x_0$ 和分支参数 $\mu$,可生成不同的混沌序列。

利用 Logistic 混沌序列来产生图像分块编号,能够置乱图像分块的编号,可以增强算法抵抗矢量量化攻击的能力。过程如下:假设图像分块总数为 $P$,将密钥 $k$ 作为 Logistic 混沌映射的初值代入式(2),生成长度为 $P$ 的混沌序列 $\{x_1, x_2, \cdots, x_P\}$。利用选择排序法对混沌序列进行排序,生成有序序列 $\{y_1, y_2, \cdots, y_P\}$,记录 $\{x_1, x_2, \cdots, x_P\}$ 中每一元素在 $\{y_1, y_2, \cdots, y_P\}$ 中的位置,产生图像分块置乱编号。

## 3 算法设计

### 3.1 算法思路

文中利用哈希函数对输入的高敏感性特点,实现脆弱水印的嵌入和对篡改的识别。图像经分块处理,并经 Logistic 混沌映射产生图像分块编号,能有效抵抗矢量量化攻击;结合图像分块的内容、编号及图像编号,经哈希变换后,形成需要嵌入的 128 位的信息摘要,亦即待嵌入水印信号,能有效提高算法的安全性。在检测中,只要利用相同方法对脆弱水印进行哈希变换,所生成的待测信息摘要与原信息摘要进行比较,即可验证图像是否被篡改,从而对图像完整性和安全性进行了有效识别。

### 3.2 水印的生成及嵌入

在文献[10,11]中提到,采用基于图像内容的水印信号策略可以增强算法的安全性。基于分块的认证算法是一种常见的认证技术,既能分辨图像被修改的区域,又能证明剩余的部分没有被修改。这类依赖于图像内容的水印算法更适用于图像认证,不仅可以增强算法抵御统计攻击的能力,又避免了在检测端额外提供原始水印信号。

设载体图像 $I$ 的大小为 $M \times N$,分块大小为 8×8,水印的生成与嵌入流程见图 1,步骤如下:

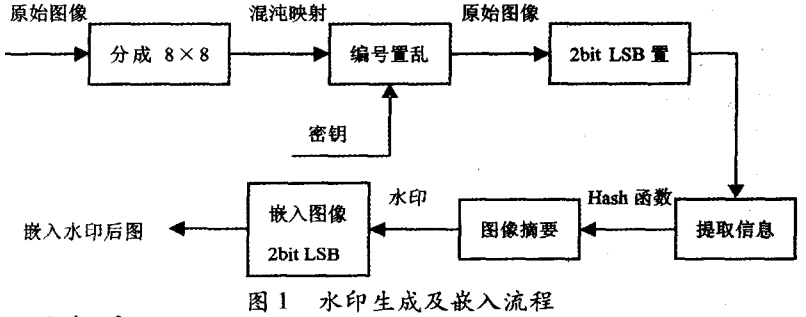



图 1 水印生成及嵌入流程

(1) 将 $I$ 划分为 $P$ 个互不重叠的 $8 \times 8$ 的图像分块 $I_p$,$p$ 为图像分块编号,$p = 1, 2, \cdots, \frac{M}{8} \times \frac{N}{8}$。

(2) 选取密钥 $k$,利用 Logistic 混沌映射产生图像分块编号 id。

(3) 将 $I_p$ 的低两 LSB 平面置零得到 $\bar{I}_p$,$\bar{I}_p$ 中像素值记为 $V_m$,$m = 1, 2, \cdots, 64$。用所有像素点 $V_1, V_2, \cdots, V_{64}$,与原图像编号 ID 及置乱后图像分块 id 作为 Hash 函数的输入并产生图像分块摘要。

$$M = \mathrm{Hash}(V_1, V_2 \cdots V_{64}, \mathrm{ID}, \mathrm{id}) \tag{3}$$

其中 $M$ 为 128 位散列值。

(4) 将 $M$ 嵌入 $I_P$ 的低两位平面像素。

(5) 重复步骤(3)、(4)直到所有的 8×8 图像分块完成水印嵌入。

### 3.3 水印的提取及认证

水印的提取及认证包括嵌入水印提取、参考水印计算及篡改定位等几个部分,如图 2 所示。提取过程不需要原始图像参与,只需知道嵌入密钥,是完全的盲提取算法。

提取和认证过程如下:

(1) 将 $I'$ 划分为 $P$ 个互不重叠的 8 × 8 的图像分块。

(2) 选取密钥 $k$,利用 Logistic 混沌映射产生图像分块编号 id 。

(3) 对于图像分块 $I_P$,按公式(4) 提取图像分块 $I_P$ 的低两 LSB 平面得到水印 $\tilde{W}_p$。重复步骤(3) 可提取 $I'$ 水印信号 $\tilde{W}_1, \tilde{W}_I = \sum_{p=1}^{P} \tilde{W}_p, p = 1,2,\cdots,P$ 。

$$\tilde{W}_p = \mathrm{LSB}_{1,2}(I'_p) \tag{4}$$

(4) 利用水印生成步骤(3)生成图像 $I'$ 的水印信号 $\tilde{W}_1, \tilde{W}_I = \sum_{p=1}^{P} \tilde{W}_p, p = 1,2,\cdots,P$ 。

(5) 对提取出的水印 $\tilde{W}_I$ 与原生成水印 $\tilde{W}_I$ 逐分块进行比较:

若 $\tilde{W}_p \oplus \tilde{W}_p = 0$,则判定图像分块未被篡改;若 $\tilde{W}_p \oplus \tilde{W}_p = 1$,则判定图像遭到攻击或篡改。

## 4 实验结果及分析

文中选择大小为 512×512 的 256 级灰度图像“house”和“car”进行仿真实验,来测试算法性能。其中 $L = 332, \mu = 4.0, k_1 = 0.27253, k_2 = 0.30147$。

### 4.1 实验结果

图 3(a)、(b)、(c)和(d)分别给出了“house”原始图像,含水印后的图像,添加人物后的图像以及篡改定位图像;

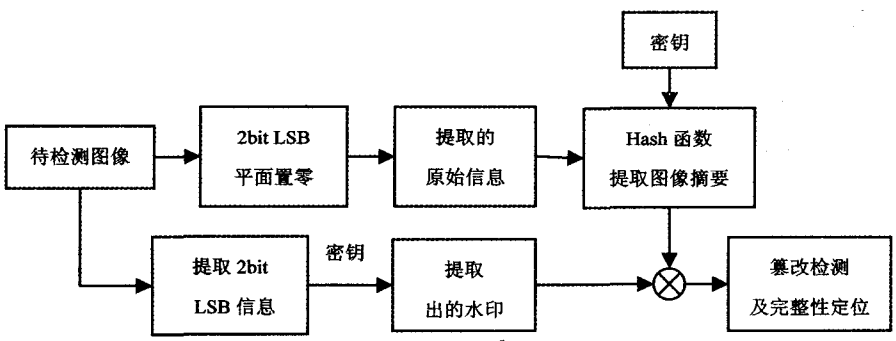
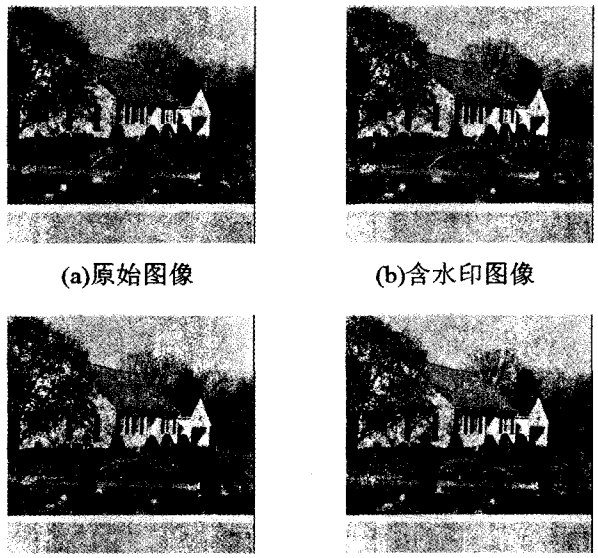



图 2　水印的提取与检测

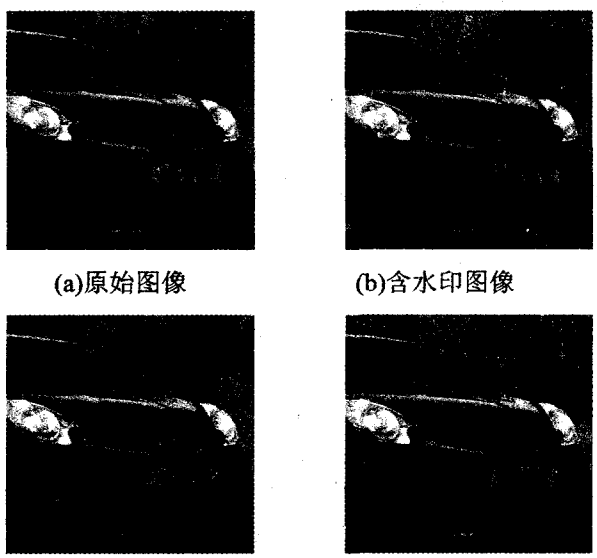
图 4(a)、(b)、(c)和(d)分别给出了“car”原始图像,含水印后的图像,将数字“6”改成“8”后的图像以及篡改定位图像。



(a)原始图像　(b)含水印图像

(c)篡改图像　(d)篡改定位图像

图 3　“house”篡改实验结果



(a)原始图像　(b)含水印图像

(c)篡改图像　(d)篡改定位图像

图 4　“car”篡改实验结果

从图中可以看出,算法在篡改定位方面具有很好的精度,可以准确地指出篡改发生的位置。

### 4.2 性能分析

(1)嵌入失真分析。

为了衡量水印图像和原始图像的差别,引入水印图像和原始图像之间的峰值信躁比(PSNR),定义为:

$$\text{PSNR} = 10\lg\left(\frac{MN\max_{m,n} I_{m,n}^2}{\sum_{m,n}(I_{m,n}-\hat{I}_{m,n})^2}\right) \tag{5}$$

其中，$M\times N$ 为图像的大小，$I$ 和 $\hat{I}$ 分别表示原始图像和水印图像。

同时，引入 MSE 用以进行计算比较，定义为：

$$\text{MSE}=\frac{\sum_{m,n}(I_{m,n}-\hat{I}_{m,n})^2}{MN} \tag{6}$$

由式(5)和(6)可得：

$$\text{PSNR} = 10\times\lg\frac{\max I_{m,n}^2}{\text{MSE}} \tag{7}$$

文中把水印信息嵌入到图像的 2bit LSB，设 $P_{e-k}$ 为像素值改变 $k(k=0,1,2,3)$ 的概率，则含水印图像和原始图像单个像素值差值平方的数学期望为：

$$E((I_{m,n}-\hat{I}_{m,n})^2)=\sum_{k=0}^{3}k^2\times P_{e-k}=\frac{7}{2} \tag{8}$$

由此得到 MSE 与 PSNR 的数学期望分别为：

$$E(\text{MSE})=\frac{7}{2} \tag{9}$$

$$E(\text{PSNR})=45.23\text{dB} \tag{10}$$

即使在所有像素点的像素值的低两位都改变，即每个像素点的像素值都改变 3 的最坏情况下，嵌入水印的信噪比也能达到 39.59dB，完全符合文献[12]提出的含水印图像的峰值信噪比高于 35dB 的要求。可见，文中算法能得到较高的峰值信噪比，完全符合图像质量的要求。

(2)伪认证分析。

“伪认证”攻击不是将水印信号去掉或使水印的检测失败，而是设法篡改图像内容却不损害水印信号，也就是使图像内容发生改变后，仍然能通过认证。文中利用 Logistic 混沌映射对图像分块进行置乱编号，并采用 Hash 函数产生基于图像内容的水印信号，并将其嵌入到图像分块的低两位平面(LSB)，无法正确伪造水印，有效地抵抗了伪认证攻击。

(3)安全性分析。

脆弱水印的安全性是与使用的密钥联系在一起的，攻击者很可能通过对水印算法的研究推断出密钥或减少密钥的搜索空间。一旦密钥被推断出，攻击者就有可能在任意一幅图像中伪造水印，从而使水印失效。文中利用混沌系统生成图像分块编号，利用 Hash 产生基于图像分块内容及分块位置信息的水印信号。选取密钥 $k$ 作为混沌映射初值，可产生很大的密钥空间，能有效抵抗针对密钥的搜索攻击。

## 5 结束语

文中提出一种基于 Hash 函数的脆弱水印算法。

算法有以下特点：

(1) 利用 Hash 函数产生采用基于图像内容的水印信号可以增强算法的安全性；

(2) 利用 Logistic 混沌映射产生图像分块的编号可有效抵抗矢量量化攻击；

(3) 对含水印图像分块的 2bit LSB 平面进行伪随机调制和置乱，能有效增强算法抵抗伪认证攻击的能力；

(4) 该算法计算简单，容易实现，大大扩充了它的应用范围。

实验结果表明，算法同时具有块独立算法的篡改定位精度和块相关算法的抗伪认证攻击的能力，具有广泛的应用环境。

**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] 宋玉杰，谭铁牛. 基于脆弱性数字水印的图像完整性验证研究[J]. 中国图像图形学报，2003，8(1)：1-7.

[3] 张 静，张春田. 用于图像认证的数字水印技术[J]. 中国图像图形学报，2003，8(4)：367-373.

[4] Walton S. Image Authentication for a Slippery New Age[J]. Dr. Dobb'S Journal，1995，20(4)：18-26.

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

[6] LUCS，Liao H Y M. Multipurpose watermarking for image authentication and protection [J] . IEEE Trans. on Image Processing，2001，10(10)：1579-1592.

[7] 刘跃峰，马康玉. 基于基于非二进制纠错码的 Hash 函数的构造及应用[J]. 计算机工程，2004，30(4)：115-116.

[8] 刘会英. 一种带纠错编码的小波域自适应盲水印算法[J]. 计算机技术与发展，2010，20(3)：140-142.

[9] 张 瀚，王秀峰，李朝晖，等. 基于时空混沌系统的单向 Hash 函数构造[J]. 物理学报，2005，54(9)：4006-4011.

[10] 朱兴力，张家树. 基于小波系数块能量分析的自适应数字水印算法[J]. 计算机应用，2006，26(4)：830-832.

[11] 董 敏，王向阳. 基于分块量化的小波域数字水印嵌入算法[J]. 微电子学与计算机，2007，24(7)：31-34.

[12] Jiho J，Kwang B L，Yong H L. Transmit power and bit allcoations for OFDM systems in a fading channel [C]// Proc IEEE Globecom. San Francisco，CA，USA：[s. n.]，2003：858-862.