

一种基于正交化分形编码和混沌相结合的脆弱数字水印技术

殷骏佳 刘文波

(南京航空航天大学自动化学院 南京 210016)

摘要: 以图像篡改定位为目的,提出了一种基于正交化分形编码和混沌相结合的脆弱数字水印技术。该算法利用宿主图像的分形编码参数信息作为混沌映射的初值,从而通过混沌映射产生混沌二值水印,所产生的混沌二值水印再嵌入到宿主图像中,从而实现图像的篡改定位。算法能有效的检测图像是否被恶意篡改,并且不同宿主图像能够产生不同的混沌二值水印,加强了算法的保密性,在处理大批量图像的时候优势更明显。实验数据表明,算法可行有效,拥有良好的图像篡改定位能力。

关键词: 脆弱水印;分形编码;混沌;图像认证

中图分类号: TP2 **文献标识码:** A **国家标准学科分类代码:** 510.1050

Fragile watermarking algorithm based on orthogonal fractal coding and chaos

Yin Junjia Liu Wenbo

(College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: For the purpose of image tampering localization, a fragile digital watermarking method is proposed on the basis of orthogonal fractal coding and chaos. The algorithm use the fractal coding parameters as a key to create the chaotic binary watermark to be embedded into the fractal coding field, so as to realize the image authentication. The algorithm can effectively detect whether the image is malicious tampered, and different host image will produce different chaotic binary watermark, which strengthen the confidentiality of the algorithm, especially in the face of mass image processing. The simulation results show that the proposed algorithm is efficacious and practical, and has precise tamper localization to grayscale images.

Keywords: fragile watermarking; fractal coding; chaos theory; image authentication

1 引言

随着互联网和多媒体技术的高速发展,信息媒体的数字化为数据的存取和传输提供了极大的便利。但是,数字信息有着易被修改的特点,因而人们可以轻易地对其进行非法拷贝,修改和处理。此外,数字形式的事发现场照片、犯罪现场记录作为法庭证据等都需要对图像的真实性进行验证,以证明所需要的图像是否真实可靠。基于数字水印的图像认证技术则是解决此类问题的有效方法之一。

1995年, Walton首次提出用脆弱数字水印的方法实现图像认证,这是该领域最早的文献之一,虽然其算法不够安全,篡改定位能力较差,但该方法原理清晰简单,为之后的研究指明了方向。此后,出现了许许多多用于图像认证的数字水印方案^[1]。其中,有一类是基于分形编码的脆弱数字水印方案在图像认证中脱颖而出^[2-5]。

目前,这类算法大致分为两类:一类通过对宿主图像的分形码进行分类实现^[6];另一类则是利用分形图像压缩技术实现图像的认证和自动恢复。两者各有优缺点,前者虽有一定的篡改定位能力,但是不能自动恢复原图像;后者的水印嵌入与分形编码无关,而在水印提取又必须通过分形编码,因此算法在分形编码上会耗费大量时间。随后,又有人将分形编码参数的获取与水印嵌入在分形编码过程中同时进行,充分利用了分形编码,真正实现将分形编码与脆弱水性数字水印相结合,但其水印保密性不强。

为此,在其基础上本文提出一种将分形编码与混沌相结合的脆弱数字水印技术。水印的产生由分形编码参数与混沌序列共同产生,然后再嵌入其分型压缩域,每张宿主图像产生的水印都会不同,且不易识别,极大的增强了水印的保密性。实验结果表明,本文算法具有很好的篡改定位能

力和保密性。

2 图像分形编码方法

2.1 基本分形编码算法

假设 W 为图像的一个压缩变化,那么分形编码的任务就是要找到这么一个压缩变化 W ,使得 W 的不动点尽可能接近我们的待编码图像。

采用最简单的固定分块方法,将大小为 $M \times M$ 的原始图像 I 分割成大小不同的两类子块:一类为 $B \times B$ 的 Range 块,称为 R 块;另一类为 $B \times B$ 的 Domain 块,称为 D 块, $B = 2^b$, b 为整数。其中, R 覆盖整幅图像 I 并且相互不重叠,而 D 块分割时可以相互重叠。 D 块经四邻域像素平均收缩为 R 块大小。另外,还要对码块 D 进行 8 种等距变换: 0° 、 90° 、 180° 、 270° 旋转变换和垂直中线、水平中线、 45° 、 135° 对角线反射变换^[7]。

每个 D 块通过仿射变换 L 可以与某个 R 块匹配。通过使用合适的仿射变换 $L: D \rightarrow R$,使得 $R_i \approx L_i(D_j)$, $D_j \in \Omega$ 。针对第 i 个 D 块 D_i 仿射变换 L_i 可表示为:

$$L_i(D_j) = \lambda_i(\gamma_i(D_j)) = s_j \gamma_j(\gamma_i(D_j)) + o_i \quad (1)$$

式中:映射 γ_i 为将 D_i 块平移到 R_i 块所在的位置及空域压缩操作,映射 λ_i 则包括等距变换 $q(j)$ ($j = 1, 2, \dots, 8$),对比度调节 s_i 和亮度调节 o_i 。根据最小二乘法准则,得到最佳匹配 s_i 和 o_i 。4 个参数 $\{k, p(i), s_i, o_i\}$ 组成了 R 块的分形编码,其中 k 表示 8 种等距变换的类型, $k = 1, 2, \dots, 8$, $p(i)$ 表示 $R(i)$ 的最佳匹配位置。分形编码的解码则通过下面的仿射变换迭代式作用于任意初始图像完成:

$$R^n = s_j(D^{n-1}) + oU \quad (2)$$

2.2 正交化分形编码

正交化分形编码算法的基础是基本分形编码。在正交分形编码中,利用对比度调节因子 S_i 、 R_i 块均值 \bar{R}_i 以及等距变换之后 D_i 块均值 $\overline{D_i^{q(j)}}$ 代替了原来的对比度调节因子 S_i , 灰度补偿因子 o 。经过替换之后,新的仿射变换迭代式为:

$$R_i^k = \bar{R}_i \cdot U + S_i(\gamma_i^k(D_i^{k-1}) - \overline{\gamma_i^k(D_i^{k-1})} \cdot U), \\ \overline{D_i^0} = \overline{D_i^{q(j)}} \quad (3)$$

这样一来,新的分形编码参数为 $\{k, p(i), s_i, \bar{R}\}$ 。由于 \bar{D}_i 可在分形编码中获得, \bar{R}_i 可由解码中重构的图像得到,且 \bar{R}_i 在迭代过程中保持不变,因此无需再增加参数的计算量,从而大大减少编码时间,同时也为水印的嵌入提供了可能^[8]。

3 图像认证方法

在正交分形编码中, R 块的均值在解码过程中是恒定不变的,这样一来,便可以利用这个性质把 R 块均值 \bar{R} 作为水印嵌入的载体。当一幅嵌有水印的图像被恶意篡改的时候,势必会造成分形编码参数 \bar{R} 的变化,所嵌入的水印也很大可能会随之改变。

因此,提出一种在 R 域嵌入水印的算法,该算法对 R 块均值的改变有很强的敏感性,是一种脆弱水印。水印由混沌序列经过二值化处理之后产生,而混沌序列的初值则由 R 块信息提供,这样一来,分形编码参数 R 块信息被充分利用,同时由于混沌序列对初值的敏感性特点,只要稍微改变由 R 块产生的信息,就会改变混沌初值,就可以产生完全不一样的二值水印,增强了水印的保密性。

3.1 kent 混沌映射

混沌具有对初始条件的敏感依赖性,内在随机性、非周期和遍历性特征,通过短暂时间的迭代,2 个相差不多的初始值可以产生毫不相关的 2 个序列^[9-10]。采用 kent 映射作为水印信息的产生方式, kent 映射混沌轨迹点密度分布均匀,有利于增强水印信息间的不相关性。

Kent 映射的定义为:

$$x_{n+1} = \begin{cases} x_n/a, & 0 \leq x_n \leq a \\ (1-x_n)/(1-a), & a \leq x_n \leq 1 \end{cases} \quad (4)$$

式中:参数 $a \in (0, 1)$ 。当 $a \in (0, 1)$ 时,映射处于混沌状态,且 $0.4 < a < 0.5$ 时较为理想,能够让 Kent 混沌序列避免受到计算机有限字长和有限精度的影响,该文中取 $a = 0.45$ 。

3.2 基于正交化分形编码和混沌相结合数字水印算法

假设宿主图像为 $I_{N \times N}$,将宿主图像经过正交化编码后得到的编码参数为 $\{k, p(i), s_i, \bar{R}\}$, $\bar{R} = \{\bar{R}_1, \bar{R}_2, \bar{R}_3, \dots, \bar{R}_m\}$ 。然后,将所生成的二值水印图像 $W_{n \times n}$ (像素值 0、1) 嵌入到宿主图像 R 块中,根据自己设定的 0、1 关系对其均值进行修改,即实现了水印的嵌入。

3.2.1 水印图像的产生

1) 这里先介绍产生 kent 映射初值 x_{m0} 的方法。水印图像是利用 kent 混沌映射产生,经过二值化处理后得到混沌二值图像,又因为混沌映射对初值的敏感性,所以初值的选择对来说就尤为重要。利用宿主图像正交化编码后产生的 \bar{R} 块信息 ($\bar{R} = \{\bar{R}_1, \bar{R}_2, \bar{R}_3, \dots, \bar{R}_m\}$) 经过特定的方法产生需要的混沌初值。采用的一种方法是在所有 \bar{R} 块中得到像素值最大块的像素值,记为 R_{\max} ; 整体 \bar{R} 块平均值记为 R_{mean} ,为了提高保密性,约定一个密钥 ($0 < k_1 < 1$),将它们通过下式计算出所要进行 Kent 混沌映射的初值。

$$x_{m0} = \frac{1}{2} \left(\frac{R_{\text{mean}}}{R_{\max}} + k_1 \right), k_2 \in (0, 1) \quad (5)$$

2) 接着,将初值 x_{m0} 代到 Kent 混沌映射式子中去进行迭代运算,生成混沌序列,截取其中长度与 \bar{R} 块数一致,即长度为 m 的一段序列;然后将这段序列进行二值化变成一段由 m 个 0、1 组成的混沌二值序列,再把它按序排列成 $n \times n$ ($m = n \times n$) 的二值图像,即得到水印图像 $W_{n \times n}$ 。

3.2.2 水印的嵌入

假设宿主图像 $I_{N \times N}$,所产生的混沌二值水印图像 $W_{n \times n}$,宿主图像经正交化编码得到的编码参数为 $\{k, p(i)$,

$s_i, \bar{R}\}, \bar{R} = \{\bar{R}_1, \bar{R}_2, \bar{R}_3, \dots, \bar{R}_m\}$ 。因为水印是二值图像, 只有 0, 1 两种情况, 为实现水印的嵌入, 只需对 R 均值块进行修改, 使其构成满足能够区分 0, 1 两种情况的特定关系即可。

当然, 为了提高稳定性, 对 \bar{R} 块进行预处理, 选择低第 4 位作为水印嵌入的位置。预处理运算为:

$$\bar{R}'_i = D(\bar{R}_i) = \frac{\bar{R}_i}{16} \quad (6)$$

式中: $D(\bar{R}_i)$ 表示预处理函数, \bar{R}'_i 表示预处理后的结果。通过式(7) 完成对 \bar{R} 块水印的嵌入。

$$\bar{R}'_i = \begin{cases} \bar{R}_i & \text{mod}(D(\bar{R}_i), 2) = 0 \\ \bar{R}_i - 1 & \text{mod}(D(\bar{R}_i), 2) = 1 \\ \bar{R}_i - 1 & \text{mod}(D(\bar{R}_i), 2) = 0 \\ \bar{R}_i & \text{mod}(D(\bar{R}_i), 2) = 1 \end{cases} \quad (7)$$

\bar{R}'_i 通过 $D(\cdot)$ 的逆运算得到含水信息的 R 块均值 $\bar{R}'_{w1}, \bar{R}'_{w2}, \dots, \bar{R}'_{wm}$ 。

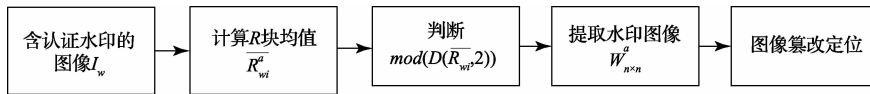


图 2 水印提取过程

4 仿真实验

为了验证本文图像认证功能的有效性, 在仿真实验中, 分别对 256256 的 peppers 和 lena 两张图像进行实验, 其宿主图像如图 3 所示。先进行分形编码, 根据第二节讲述的水印产生方法, 两图像分别产生的尺寸为 6464 的混沌二值水印图如图 4 所示。分形解码及认证水印嵌入后的图像如图 5 所示。



图 3 256×256 宿主图像

3.2.3 水印的提取

有了新的含有水印信息的 R 均值块 \bar{R}'_w , 就可以代替原来的 \bar{R} 均值块进行分形解码运算, 得到含水水印的分形编码图像。当进行水印提取时, 只需重新计算含有水印的图像的 R 块均值, 记作 \bar{R}'_{wi} 。利用式(8) 判断并提取出二值水印序列 $\omega_i^a = \{\omega_1^a, \omega_2^a, \omega_3^a, \dots, \omega_m^a\}$, 即二值水印图像 $\omega_{n \times n}^a$ 。

$$\omega_i^a = \begin{cases} 0, \text{mod}(D(\bar{R}'_{wi}), 2) = 0 \\ 1, \text{mod}(D(\bar{R}'_{wi}), 2) = 1 \end{cases} \quad (8)$$

3.3 篡改区域的确定

当需要确定一副图像的篡改区域, 将提取出来的二值水印图像 $W_{n \times n}^a$ 与原来的二值水印图像 $W_{n \times n}$ 根据式(9) 比较差异, 若被篡改, 则在原图像上定位出篡改区域。

$$W = W_{n \times n}^a \oplus W_{n \times n} \quad (9)$$

图 1 和图 2 分别表示水印嵌入过程和水印提取认证过程。

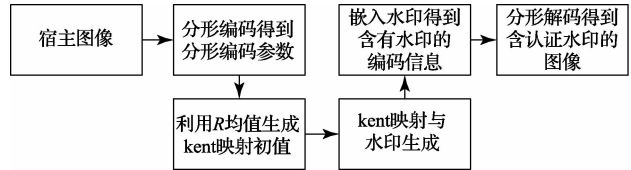


图 1 水印嵌入过程



图 4 各自产生的混沌二值水印



图 5 分形解码后含水水印图像

接下来,分别对上述两幅已嵌入水印的图片进行篡改。对peppers中在青椒上面加了一只瓢虫;在lena中帽子后沿处复制了其本身的一块头发。篡改后的图像如图6所示。



图6 篡改后图像

按照本文的水印认证算法,对被篡改后的图像进行篡改定位,结果如图7所示,提取出来的认证水印如图8所示。



图7 篡改定位

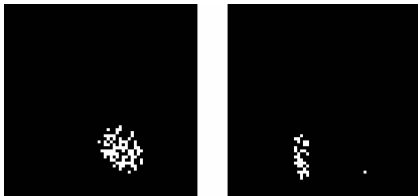


图8 提取的认证水印与原水印差异对比

从图7、图8上看到,被篡改的地方被明确的显示出来。另外,实验中还分别验证了分形编码压缩图像,及含水印图像与原宿主图像之间的峰值信噪比,如表1所示。

表1 篡改定位结果 PSNR 结果对比

宿主图像	与分形编码	与含认证
	压缩图像	水印图像
	PSNR1	PSNR2
peppers	34.5692	34.4227
lena	32.3904	32.3013

从表中可以看出,分形编码压缩图像与含认证水印图像的峰值信噪比相差不大,说明图像质量下降主要由分形编码本身引起的,而非水印的嵌入。

5 结 论

利用分形编码压缩对图片进行压缩,然后利用宿主图像分形编码信息作为水印产生的“钥匙”,而且所产生的水印还拥有混沌的特性,只要初值稍有一点不同,水印则完全不同,并且每张不同图像产生的混沌二值水印都不同,看似杂乱无章,实则有迹可循,同时也实现了盲提取。在面对大批量图像进行认证时,本算法的优越性就尽显无遗。攻击者若不知道双方约定的密匙,则难以获得原始水印,也就难以对图像进行有效的版权窃取,从而本算法可以很好的定位被篡改的区域,而且拥有很好的保密性。

参考文献

- [1] WANG X Y, ZHANG J M. A novel image authentication and recovery algorithm based on chaos and Hamming code[J]. Acta Physica Sinica, 2014(2): 020701-1-020701-11
- [2] WANG X, ZHANG D, GUO X. A novel image recovery method based on discrete cosine transform and matched blocks[J]. Nonlinear Dynamics, 2013, 73(3):1945-1954.
- [3] ZHANG X, XIAO Y, ZHAO Z. Self-embedding fragile watermarking based on DCT and fast fractal coding[J]. Multimedia Tools and Applications, 2014:1-20.
- [4] SULAIMAN A H, BAJI F S. Fractal based fragile watermark[C]. Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on, IEEE, 2009, 2:139-143.
- [5] 彭玉楼,何怡刚. 基于小波和混沌映射的函数水印算法[J]. 仪器仪表学报, 2010, 31(12):2768-2773.
- [6] 纪正彪. 一种图像边缘检测的分形误差算法[J]. 国外电子测量技术, 2009, 32(9):17-19.
- [7] 黄晓晴,于盛林. 一种在分形编码图像中嵌入盲灰度水印的方法[J]. 仪器仪表学报, 2011(12):2754-2760.
- [8] 黄晓晴,于盛林. 以图像认证为目的的分形编码数字水印算法[J]. 中国图象图形学报, 2012, 17(2):183-190.
- [9] 杨正超. 彩色图像的自恢复水印算法研究及其实现[D]. 北京:北京交通大学, 2013.
- [10] 李振鹏,武全胜,张文超,等. 一种基于 Arnold 置乱和小波变换的二值图像水印算法[J]. 电子测量技术, 2008, 31(6):9-12.

作者简介

殷骏佳,1990年出生,硕士研究生。主要研究方向为测试计量技术与仪器、数字水印。

E-mail: yinjunjiayinjunjia@126.com

刘文波,1966年出生,博士研究生,教授。主要研究方向为信号处理及应用、非线性动力系统分析及工程应用,计算机测试与控制技术。

E-mail: wenboliu@nuaa.edu.cn