文章编号:1000-5013(2014)03-0287-06 **doi**:10.11830/ISSN.1000-5013.2014.03.0287

应用 P-Fibonacci 加密的模糊自适应水印算法

冯祥斌,陈永红

(华侨大学 计算机科学与技术学院,福建 厦门 361021)

摘要: 结合 P-Fibonacci 加密算法和模糊归类,提出一种自适应水印新算法.利用 P-Fibonacci 加密具有良好的均匀性及安全性,将水印图像的像素位置打乱,消除了二维数字水印图像的像素空间相关性,使嵌入水印后的块效应降低.对原始载体图像进行分块,结合人类视觉系统的纹理和照度掩蔽特性,得到纹理模糊函数和各图像子块的归类结果,并自适应地确定水印的嵌入强度.对载体图像的各子块进行离散小波变换(DWT),将经 P-Fibonacci 加密算法加密后的水印信息重复嵌入各子块 DWT 域的低频部分.实验结果表明:该算法抗 JPEG 压缩、高斯噪声、滤波等常见的信号攻击和几何攻击具有很好的鲁棒性.

关键词: P-Fibonacci 变换; Fibonacci P-code; 位平面; 数字水印; 模糊归类; 自适应; 离散小波变换

中图分类号: TP 391.41 **文献标志码**: A

随着互联网技术的不断发展,数字信息的非法复制已经开始对多媒体信息的所有权构成威胁.研究者提出了使用数字水印来证明多媒体信息的所有权[1].根据原始图像在嵌入阶段的处理方式的不同,水印系统可以分为空间域水印[2-3]和变换域水印[4-7].由于直接作用于空间域而不需要经过变换,使得空间域水印技术复杂度相对较低.对于频域水印,水印是通过修改经过离散余弦变换(DCT)或者离散小波变换(DWT)得到的频带进行嵌入的.DWT 具有良好的空间定位、频率扩展和多分辨率特性.此外,随着图像加密技术的发展,图像置乱技术已经成为安全传输和保密存储的重要手段之一.为了对图像的(x, y)位置进行置乱,Sharinger[8]提出了一种基于混沌 Kolmogorov 流方法,Miyamoto 等[9]提出了非连续 Baker 变换,Zou 等[10-11]提出了限制域方法.然而,以上方法是周期性的且具有一定的针对性.基于此,本文提出了一种基于 P-Fibonacci 加密的模糊自适应水印新算法.

1 置乱原理

借鉴递归序列的加密算法理念,对水印信息加密使用的是结合 Fibonacci P-code 位平面分解和 P-Fibonacci 变换的新型加密算法.该加密算法的流程图如图 1 所示.图 1 中:P_D 是分解参数;P_E 是加密参数.设计原理有如下 3 点.

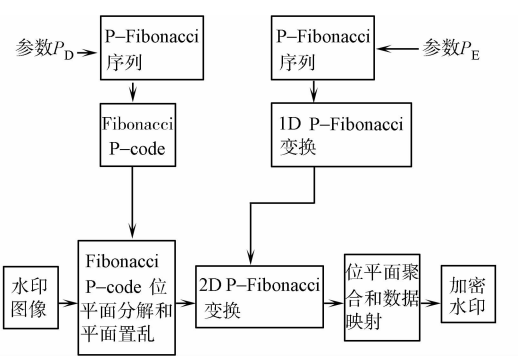

图 1 仿真效果图

Fig. 1 Simulation effect diagram

1) 将水印信息图像分解成 Fibonacci P-code 位平面,并打乱这些位平面的顺序.

2) 基于 2D P-Fibonacci 变换对位平面的大小进行调整,对所有的位平面逐个进行加密.

3) 结合所有已加密的位平面,并把这些图像数据映射回输入水印图像的原始数据范围内,得到最

收稿日期: 2012-11-17

通信作者: 陈永红(1974-),男,教授,主要从事图像处理、计算机控制、信息安全技术的研究.E-mail:djandcyh@163.com.

基金项目: 福建省自然科学基金资助项目(2011J05151);华侨大学高层次人才科研启动项目(10Y0199);教育部留学回国人员科研启动基金资助项目(2009 年度)

终的加密水印.

1.1 P-Fibonacci 序列

P-Fibonacci 序列是一种递归序列,其定义如下

$$F_{\mathrm{p}}(i)=\begin{cases}0, & i<0,\\ 1, & i=0,\\ F_{\mathrm{p}}(i-1)+F_{\mathrm{p}}(i-p-1), & i>1.\end{cases}\tag{1}$$

式(1)中:i 是序列的位置索引;非负数整数 p 是一个距离参数.

根据式(1),P-Fibonacci 序列是随着 p 值变化而变化的,当 $p=1$ 时,其为经典 Fibonacci 数列.

1.2 1D P-Fibonacci 变换

设 $F_{\mathrm{p}}(i)$和 $F_{\mathrm{p}}(i+1)$是在式(1)中定义的 P-Fibonacci 序列的两个连续的元素.那么 1D P-Fibonacci 变换可以表示为

$$(T_1,T_2,\cdots,T_N)^{\mathrm{T}}=(F_{\mathrm{p}}(i)+\varepsilon)(1,2,\cdots,N)^{\mathrm{T}}\bmod F_{\mathrm{p}}(i+1).\tag{2}$$

式(2)中:$F_{\mathrm{p}}(i)+\varepsilon<F_{\mathrm{p}}(i+1)$提供了最小偏移量 ε 条件范围限定;$N=F_{\mathrm{p}}(i+1)-1$ 指明了输入序列的最大值;非负整数 i 是 P-Fibonacci 序列的索引位置;常数 ε 是一个最小整数偏移量,使得 $F_{\mathrm{p}}(i)+\varepsilon$ 和 $F_{\mathrm{p}}(i+1)$的最大公约数是 1.

1.3 2D P-Fibonacci 变换

设 $\boldsymbol{A}$ 是一幅大小为 $M\times N$ 的 2D 图像,$\boldsymbol{C}_{\mathrm{r}}$ 与 $\boldsymbol{C}_{\mathrm{c}}$ 分别表示行系数矩阵和列系数矩阵.那么 2D P-Fibonacci 变换可以表示为

$$\boldsymbol{E}=\boldsymbol{C}_{\mathrm{r}}\boldsymbol{C}_{\mathrm{c}}.\tag{3}$$

式(3)中:$\boldsymbol{E}$ 表示加密后的图像;$\boldsymbol{C}_{\mathrm{r}}(u,v)=\begin{cases}1,\text{对于}(u,T_u),\\ 0,\text{其他};\end{cases}$ $\boldsymbol{C}_{\mathrm{c}}(x,y)=\begin{cases}1,\text{对于}(T_y,y),\\ 0,\text{其他}.\end{cases}$ T_u 和 T_y 是式(2)产生的,$1\leqslant u,v\leqslant M$,$1\leqslant x,y\leqslant N$.由此可以看出:1D P-Fibonacci 变换是 2D P-Fibonacci 变换的特殊情况.当 $\boldsymbol{A}=(1,2,\cdots,N)^{\mathrm{T}}$ 时,1D P-Fibonacci 变换可以表示为

$$(T_1,T_2,\cdots,T_N)^{\mathrm{T}}=\boldsymbol{C}_{\mathrm{r}}(1,2,\cdots,N)^{\mathrm{T}}.\tag{4}$$

2D P-Fibonacci 变换可以用于加密 2D 和 3D 图像.根据式(3)的定义,为了加密 $M\times N$ 的 2D 图像,行系数矩阵 $\boldsymbol{C}_{\mathrm{r}}$ 必须是 $M\times M$ 矩阵,列系数矩阵 $\boldsymbol{C}_{\mathrm{r}}$ 必须是 $N\times N$ 矩阵.

设 $\boldsymbol{E}$ 是一幅加密后的 2D 图像,$\boldsymbol{C}_{\mathrm{r}}^{-1}$ 和 $\boldsymbol{C}_{\mathrm{c}}^{-1}$ 是式(3)中 $\boldsymbol{C}_{\mathrm{r}}$ 和 $\boldsymbol{C}_{\mathrm{c}}$ 的逆矩阵.那么,2D P-Fibonacci 变换的逆变换可以表示为

$$\boldsymbol{R}=\boldsymbol{C}_{\mathrm{r}}^{-1}\boldsymbol{E}\boldsymbol{C}_{\mathrm{c}}^{-1}.\tag{5}$$

式(5)中:$\boldsymbol{R}$ 为重构图像.

类似的,1D P-Fibonacci 变换的逆变换可以定义为

$$(T_1,T_2,\cdots,T_N)^{\mathrm{T}}=\boldsymbol{C}_{\mathrm{r}}^{-1}(T_1,T_2,\cdots,T_N)^{\mathrm{T}}.\tag{6}$$

2 Fibonacci P-code 位平面分解

2.1 Fibonacci P-code

非负的十进制数 D 可以用以 2 为底的多项式表示为

$$D=\sum_{i=0}^{n-1}a_i2^i=a_02^0+a_12^1+\cdots+a_{n-1}2^{n-1}.\tag{7}$$

式(7)中:$(a_{n-1},\cdots,a_1,a_0)$是非负十进制数 D 的二进制表示.这个概念可以扩展到 Fibonacci P-code,因此,Fibonacci P-code 的定义为

$$D=\sum_{i=0}^{n-1}c_iF_{\mathrm{p}}(i)=c_0F_{\mathrm{p}}(0)+c_1F_{\mathrm{p}}(i)+\cdots+c_{n-1}F_{\mathrm{p}}(n-1),\qquad i=0,1,\cdots,n-1.\tag{8}$$

式(8)中:n 和 p 是非负整数系数序列;$c_i\in(0,1)$;$(c_{n-1},\cdots,c_1,c_0)$成为 D 的 Fibonacci P-code,即

$$D=p(c_{n-1},\cdots,c_1,c_0).\tag{9}$$

式(9)中:p 是式(1)中的 P-Fibonacci 序列的距离参数.

对于一个给定的 p 值，特定的十进制数的 Fibonacci P-code 并不是唯一的. 为了使每个非负十进制数得到一个唯一的 Fibonacci P-code，文中将采用文献[12]的规则来使 Fibonacci P-code 唯一，即

$$D = F_{\mathrm{p}}(i) + s. \tag{10}$$

式(10)中：$F_{\mathrm{p}}(i)$是式(1)在给定的 p 值下产生的 P-Fibonacci 序列的第 i 个元素($0 \leqslant i \leqslant n$)；非负十进制数 s 的前提是 $0 \leqslant s \leqslant F_{\mathrm{p}}(i-p)$.

2.2　Fibonacci P-code 位面分解

与传统的位平面分解方法类似，一幅图像也可以分解为多个 Fibonacci P-code 平面. Fibonacci P-code 位平面的数量 n_{B} 取决于图像的最大值 $I_{\max}$. 为了使该分解方法能作用于所有的 p 值，设定 $p \leqslant I_{\max}$，n_{B} 可以通过 $I_{\max}$ 计算得出；否则，如果 $p > I_{\max}$，那么 n_{B} 是通过 p 值进行计算得出. 这表示在 $p > I_{\max}$ 的情况下，Fibonacci P-code 位面数仅由 p 值决定. 对于一幅给定的灰度图像，Fibonacci P-code 位平面分解的结果是由参数 p 的值决定的并且不同的 p 值对应的 Fibonacci P-code 位面的内容是不同的. 这使得 Fibonacci P-code 位面分解更加适合于图像加密.

3　新型图像加密算法

P-Fibonacci 加密算把原始图像分解成多个 Fibonacci P-code 位平面，打乱这些位平面的顺序，调整其大小以满足 2D P-Fibonacci 变换的大小要求，并通过 2D P-Fibonacci 变换对所有位平面进行加密. 用式(7)定义的二进制码融合所有加密后的位平面，把这些图像数据映射回原始图像数据范围，可得到最终的加密图像.

用$\{X_0, X_1, \cdots, X_{L-1}\}$，$X_0 < X_1 < \cdots < X_{L-1}$表示输入图像 $\boldsymbol{I}(m,n)$的离散强度级. 当 $\boldsymbol{I}(m,n) = X_k$，数据映射函数定义为

$$\boldsymbol{E}(m,n) = k. \tag{11}$$

式(11)中：$\boldsymbol{E}$ 为输出的加密图像；$k = 0, 1, \cdots, L-1$.

在重构加密图像时，授权用户必须拥有上述安全密钥和图像大小调整的方法. 在解密过程中，P-Fibonacci 加密算法首先把加密图像数据映射回原始数据范围；随后，将图像分解为二进制位平面(在加密过程中产生的 Fibonacci P-code 位平面)，将所有位平面的顺序恢复到与原始顺序一致，使用 2D Fibonacci 变换对所有位平面进行解密，把所有位平面大小调整为原始大小；最后，组合所有解密后的位平面得到重构图像.

4　基于 P-Fibonacci 加密的水印算法

根据载体图像局部块纹理复杂度的不同，可以对水印的嵌入强度进行自适应的调整，这也能够使嵌入水印的鲁棒性和不可见性达到良好的平衡. 因此，对图像块按照纹理复杂度的不同进行自适应模糊归类，可以分为 3 类：用 S1 表示纹理复杂度较低的类；用 S3 表示纹理复杂度较强的类；其他归类为 S2. 因为图像像素灰度的突变点可以用边缘点表示，图像块中的边缘点数量越多，纹理复杂度就越高. 根据此性质，可以用边缘点的数量进行图像块的归类.

4.1　基于 P-Fibonacci 加密的水印嵌入流程

设水印的二值图像可以用矩阵表示为 $\boldsymbol{W} = \{w(x,y), 1 \leqslant x, y \leqslant M\}$，其中 $w(x,y)$表示水印图像在位置(x,y)的像素值. 原始载体图像可以表示为 $\boldsymbol{F} = \{f(x,y), 1 \leqslant x, y \leqslant N\}$，其中 $f(x,y)$表示载体图像在位置(x,y)的像素值，并且 N 能被 M 整除. 水印嵌入有如下 4 个步骤.

1) 使用文中提出的 P-Fibonacci 新型图像加密算法对水印 $\boldsymbol{W}$ 进行加密，生成加密后的水印 $\boldsymbol{W}'$.

2) 对载体图像 $\boldsymbol{F}(x,y)$进行分块处理，把原始图像分成 $N/(2M) \times N/(2M)$个大小为 $2M \times 2M$ 的不相互覆盖的子图像，记作 $\boldsymbol{B}_k$，$k = 0, 1, \cdots, N/(2M) \times N/(2N)$. 每个子图像的边缘点数量为 $\mathrm{sum}\{e(x,y) = 0, (x,y) \in \boldsymbol{B}_k\}$，其中 $e(x,y)$是图像 $\boldsymbol{F}(x,y)$中提取的二值化边缘图的数学表示. 分析每个子图像对 3 类的隶属程度，并根据最大隶属度原则进行归类，隶属函数表示为

$$A_i(\mathrm{sum})=\begin{cases}1, & \mathrm{sum}\leqslant T_1,\\ \exp(-(\dfrac{\mathrm{sum}-T_i}{\alpha_i})), & T_1<\mathrm{sum}<T_3,\\ 1, & \mathrm{sum}>T_3.\end{cases}\tag{12}$$

式(12)中:$i=1,2,3$.

根据各子块的边缘点数量进行统计并排序,用 max 表示边缘点数量最大值,用 min 表示数量最小值,T_2 为 max 和 min 的平均值;然后,根据各子块图像边缘点数量的分布情况设定 T_1 和 T_3 的阀值,并使得对 S_1 类隶属度为 1 的数据都落在区间[min,T_1]之内,对 S_3 类隶属度为 1 的数据落在[T_3,max]内,而用 a_1,a_2,a_3 分别表示数据落在区间[T_1,max],[T_1,T_3]和[min,T_3]的标准差.

3) 对分类后的原始图像的子块 B_k 进行 DWT 变换,得到低频子带 $\boldsymbol{LL}_k$,利用步骤 2 中的归类结果,根据人眼的视觉掩蔽特性,使嵌入水印的强度同图像子块的纹理复杂度成正比,达到自适应水印嵌入的效果,嵌入水印的方法可以为

$$\boldsymbol{LL}'_k(x_i,y_i)=\boldsymbol{LL}_k(x_i,y_i)+\delta\times\boldsymbol{W}'_i.\tag{13}$$

式(13)中:δ 为自适应嵌入强度.

4) 对各图像子块进行 DWT 反变换,重构得到嵌有水印的图像 $\boldsymbol{F}(x,y)'$.

4.2 基于 P-Fibonacci 加密的水印检测流程

作为水印嵌入的逆过程,水印的提取过程描述为以下 5 个过程.

1) 对载入的原始图像进行分块分类处理,得到各分块的纹理复杂度隶属结果和相应的嵌入强度 δ.

2) 对原始图像的各个分块进行 DWT 变换,得到小波域的低频子带 $\boldsymbol{LL}_k$.

3) 对嵌入水印的图像 $\boldsymbol{F}(x,y)'$进行 DWT 变换,得到其小波域的低频子带 $\boldsymbol{LL}'_k$.

4) 利用假设检测的方法进行水印的检测,同时用前有水印的图像子块系数减去原始载体图像子块的系数再除以嵌入强度,从而提取出水印.

5) 对水印信息图像实施 P-Fibonacci 算法的逆过程进行解密,得到加密前的水印信息,并把各个分块的 $N/(2M)\times N/(2M)$个水印进行叠加,对其进行求平均处理得到提取的水印图像.

5 实验仿真结果

实验采用的是大小为 512 px×512 px 的 Lena 的图像,如图 2 所示. 水印信息使用的是 64 px×64 px 的二值灰度图像,如图 3 所示.

图 2 仿真效果图

Fig. 2 Simulation effect diagram

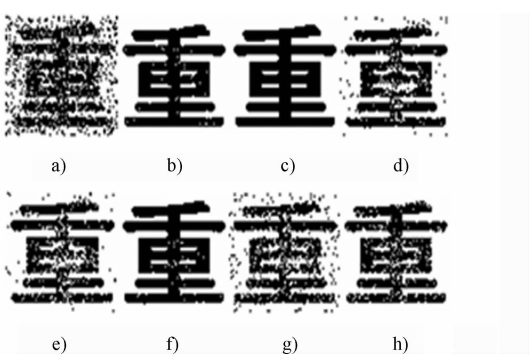

图 3 各种处理后的得到的水印

Fig. 3 Extracted watermark with various processing

通过统计各子块的边缘点数得到各类的嵌入强度,分别取 $\delta_1=3,\delta_2=5,\delta_3=7$. 嵌有水印图像和原始图像的峰值信噪比 $R_{SN}=42.818\ 0$,提取得到的水印和原始水印的相似度 NC=1,视觉掩蔽性良好. JPEG 压缩处理后的数据图,如图 4 所示. 从图 4 可知:即使在 JPEG 压缩因子小于 20 时(即压缩掉图像 80%的信息),提取的水印信息仍然能够辨别并可以用来证明版权归属,此时对应的 NC=0.663 1.

添加椒盐噪声后的数据图,如图 5 所示. 从图 5 可以看出:该算法对于椒盐噪声攻击具有良好的鲁棒性,即使在较大强度,如强度为 0.12 时,NC 也能保持较大数值为 0.905 6.

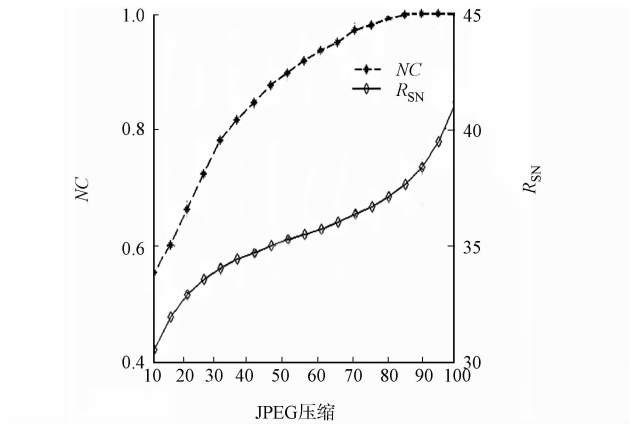

图 4　JPEG 压缩处理后的数据图

Fig. 4　Data figure with JPEG compression

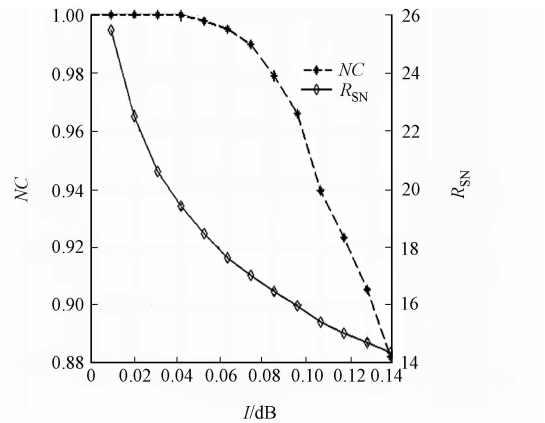

图 5　添加椒盐噪声后的数据图

Fig. 5　Data figure with salt and pepper noise

常用攻击鲁棒性数据表，如表 1 所示. 从表 1 可知：该算法对于中值滤波、高斯滤波、高斯噪声攻击具有很强的鲁棒性；水印提取后效果较好；对于几何攻击中的剪切有很好的抗攻击性能；当中心剪切为 300×300 的大小区域，NC 值仍然能达到 0.950 0；常用信号处理叠加后的攻击、常用信号处理与几何攻击（剪切）叠加后的攻击对嵌入水印后的图像进行攻击，提取的水印效果也较好，版权信息是可辨别的.

表 1　常用攻击鲁棒性数据表

Tab. 1　Data table of the robustness with common attacks

攻击类型	S_{NR}	NC	攻击类型	S_{NR}	NC
3×3 中值滤波	34.881 8	0.935 7	3×3 中值滤波＋0.03 椒盐噪声	20.462 3	0.905 5
5×5 中值滤波	31.088 7	0.749 9	3×3 中值滤波＋0.05 椒盐噪声	18.319 8	0.876 8
3×1 高斯低通滤波	32.593 8	0.922 1	3×3 中值滤波＋0.07 椒盐噪声	16.936 8	0.849 2
3×3 高斯低通滤波	31.362 1	0.872 7	JPEG_75＋300×300 中心剪切	10.430 0	0.855 9
高斯噪声	29.684 0	0.822 7	JPEG_90＋300×300 中心剪切	10.428 6	0.920 7
中心 250×250 剪切	12.063 9	1.000 0	JPEG80＋0.06 椒盐噪声	17.548 4	0.940 3
中心 300×300 剪切	10.427 7	0.950 0	JPEG80＋0.07 椒盐噪声	17.098 9	0.928 1
中心 350×350 剪切	9.057 1	0.824 8	JPEG80＋0.08 椒盐噪声	16.358 9	0.908 1
0.06 椒盐噪声＋高斯噪声	17.711 1	0.807 6	JPEG_80＋3×3 高斯滤波	31.353 4	0.852 7
3×3 中值滤波＋JPEG_60	33.843 6	0.804 6	0.02 椒盐噪声＋300×300 剪切	10.249 2	0.922 6
3×3 中值滤波＋JPEG_70	34.140 3	0.847 3	0.04 椒盐噪声＋300×300 剪切	10.086 0	0.873 8
3×3 中值滤波＋JPEG_80	34.412 8	0.880 6	0.06 椒盐噪声＋300×300 剪切	9.923 3	0.831 9
3×3 中值滤波＋0.01 椒盐噪声	24.985 1	0.928 3	3×3 中值滤波＋300×300 剪切	10.423 3	0.817 5

6　结束语

P-Fibonacci 算法对水印进行加密，极大地消除了二维数字水印图像的像素空间相关性，同时嵌入水印后的块效应降低，使算法抗攻击的能力和安全性增强. 自适应模糊归类算法能够确定不同纹理复杂度的水印嵌入强度，使水印的不可见性保持良好的水平；而嵌入水印时采用重复嵌入的方式，也极大地增强了水印抗攻击的能力. 实验结果表明：所提出的算法使不可见性和鲁棒性达到一个良好的平衡.

参考文献：

[1] REZA M S, KHAN M S A K, ALAM M G R, et al. An approach of digital image copyright protection by using watermarking technology[J]. International Journal of Computer Science Issues, 2012, 9(2): 280-286.

[2] MAO Jia-fa, ZHANG Ru, NIU Xin-xin, et al. Research of spatial domain image digital watermarking payload[J]. Eurasip Journal on Information Security, 2011, 2011(2011): 502748.

[3] KIM J, WON S, ZENG Wen-jun, et al. Copyright protection of vector map using digital watermarking in the spatial domain[C]// 7th International Conference on Digital Content, Multimedia Technology and Its Applications. Busan:

IEEE Computer Society Conference Publishing Services,2011:154-159.

[4] HAN Wei-yuan,YAN Yang,ZHI Hui-lai. Digital watermark encryption algorithm based on Arnold and DCT transform[C]// Proceedings of the 2011 International Conference on Electrical, Information Engineering and Mechatronics. Henan:Springer London Ltd,2012:613-621.

[5] XU Tian-qi,CHANG Di,ZHANG Xia. A video digital watermarking algorithm based on DCT domain[C]// 2nd International Conference on Consumer Electronics, Communications and Networks. Three Gorges:IEEE Computer Society Conference Publishing Services,2012:1600-1603.

[6] AGRESTE S,ANDALORO G,PRESTIPINO D,et al. An image adaptive, wavelet-based watermarking of digital images[J]. Journal of Computational and Applied Mathematics,2007,210(1/2):13-21.

[7] HABIBOLLAH D,MORTEZA M,AKHLAGIAN T F. Robust blind DWT based digital image watermarking using singular value decomposition[J]. International Journal of Innovative Computing,Information and Control,2012,8(7):4691-4703.

[8] SHARINGER J. Fast encryption of image data using chaotic Kolmogorov flows[J]. SPIE,1997,7(2):318-325.

[9] MIYAMOTO M,TANAKA K,SUGIMURA T. Truncated baker transformation and its extension to image encryption[C]// Proceedings of SPIE on Advanced Materials and Optical Systems for Chemical. Boston:Society of Photo Optical,1999:13-25.

[10] ZOU Jian-cheng,WARD R K. Some novel image scrambling methods based on chaotic dynamical system[C]// Proceedings of the 9th Joint Inter Computer Conf. Zhuhai:IEEE Computer Society Conference Publishing Services,2003:188-191.

[11] ZOU Jian-cheng,WARD R K. Introducing two new image scrambling methods[C]// Proceedings of 2003 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing. Victoria:IEEE Computer Society Conference Publishing Services,2003:708-711.

[12] GEVORKIAN D Z,EGIAZARIAN K O,AGAIAN S S,et al. Parallel algorithms and VLSI architectures for stack filtering using Fibonacci P-codes[J]. IEEE Transactions on Signal Processing,1995,43(1):286.

A Novel Fuzzy Adaptive Watermarking Algorithm Based on P-Fibonacci Encryption

FENG Xiang-bin, CHEN Yong-hong

(College of Computer Science and Technology, Huaqiao University, Xiamen 361021, China)

Abstract: A new adaptive watermarking algorithm based on P-Fibonacci encryption and fuzzy classified is proposed. The P-Fibonacci encryption has a good uniformity and safety, disrupting the watermark image's pixel position by P-Fibonacci encryption algorithm, which can eliminate the spatial correlation of the two-dimensional digital watermark image pixels, and ultimately, reducing the blockiness when embedding watermark information. Simultaneously, blocked the original carrier image, and according to the texture and illumination masking characteristics of the human visual system, obtained a fuzzy function which based on the texture characteristics of the original image, establishing the texture fuzzy function and the classification results of each sub-block, according to the results, determined the embedding strength adaptively. Then discrete wavelet transform (DWT) is performed on the sub-images, and the encrypted watermarks were embedded in the low frequency of the DWT domain repeatedly. The experimental results show that the presented algorithm has a good robustness against common signal processing attacks such as JPEG compression, Gaussian noise, filtering and geometric attack such as cropping.

Keywords: P-Fibonacci transform; Fibonacci P-code; bit-plane; digital watermarking; fuzzy classified; adaptive; discrete wavelet transform

(**责任编辑**: 陈志贤 **英文审校**: 吴逢铁)