DOI:10.13718/j.cnki.xsxb.2021.01.009

# 基于离散余弦变换与最优嵌入强度预测的鲁棒图像水印算法①

滕春燕[1], 杨德运[2,3]

1. 江苏联合职业技术学院徐州财经分院 信息技术系, 江苏 徐州 221008;
2. 山东大学 软件学院, 济南 250100; 3. 泰山学院 信息科学技术学院, 山东 泰安 271000

**摘要:** 为了解决当前图像水印方案难以兼顾系统的抗几何攻击能力与视觉隐秘性的问题, 提出了基于离散余弦变换与最优嵌入强度预测的鲁棒图像水印算法. 把宿主目标划分为若干个 8×8 的非重叠子块; 引入离散余弦变换 DCT(Discrete Cosine Transform)处理每个子块, 输出相应的低频与高频子带; 从低频子带中选择一个系数作为参考系数, 借助 JPEG 量化表, 选择与参考系数相接近的 4 个不同系数; 从选择的系数中确定出一个与参考系数最为接近的系数, 存储其位置, 视为密钥, 并找出幅度值最大的系数; 利用不同攻击类型的鲁棒性来构建人工蜂群算法的适应度函数, 通过训练样本来获取最优嵌入强度值; 借助水印融合原则, 把密钥信息植入到参考系数与幅度值最大的系数中, 得到水印结果; 最后, 根据其存储位置, 提出水印复原方案, 完成水印数据的检测. 测试数据显示: 与已有的水印方案相比, 所提技术具有更好的水印效果, 在多种几何攻击下, 均具备更优的视觉隐秘性与鲁棒性.

**关 键 词:** 图像水印; 离散余弦变换; 人工蜂群; 嵌入强度预测; 参考系数; 适应度函数

**中图分类号:** TP391 **文献标志码:** A **文章编号:** 1000-5471(2021)01-0050-09

随着数据通信和互联网的进步, 数字图像出现了爆炸性增长[1], 同时也伴随着较为严重的信息安全问题[2]. 图像水印技术作为一种信息隐秘技术, 可以解决图像传输过程中存在的信息安全问题[3-6].

文献[7]的研究结果指出, 水印嵌入强度会影响水印图像的密钥信息隐秘性与稳健性, 因此, 需要对其进行优化, 确定一个最佳的嵌入强度, 以平衡不可感知性与鲁棒性. 为此, 根据文献[7]的思想, 本文利用人工蜂群机制, 提出了基于离散余弦变换 DCT(Discrete Cosine Transform) 与最优嵌入强度预测的鲁棒图像水印算法. 通过引入离散余弦变换来分解宿主图像子块, 从中选择一个参考系数和 4 个嵌入系数. 根据水印图像的质量与不同攻击类型的鲁棒性来构建适应度函数, 通过迭代人工蜂群算法来对样本进行训练, 以获取最优嵌入强度值. 根据该优化的嵌入强度构建水印嵌入方法, 将水印信息隐藏到宿主图像中, 使其可以较好地兼顾视觉隐秘性与抗攻击能力. 最后, 对所提方案的信息隐秘性与抗几何变换能力实施了测试.

## 1 离散余弦变换

对于尺寸为 $L\times H$ 的图像 $f(x,y)$, 可以利用两个连续的 1D-DCT 来计算其 2D-DCT[8]:

$$C(u,v)=S(u)S(v)\sqrt{\frac{2}{LH}}\sum_{x=0}^{L-1}\sum_{y=0}^{H-1}f(x,y)\cos\left[\frac{\pi}{L}u\left(x+\frac{1}{2}\right)\right]\cos\left[\frac{\pi}{H}v\left(y+\frac{1}{2}\right)\right] \tag{1}$$

其中: $C(u,v)$ 是 2D-DCT 变换系数; $x,y$ 是 $f(x,y)$ 中像素点的位置; $L\times H$ 代表图像尺寸; $u,v$ 是像素

① 收稿日期: 2019-04-03
基金项目: 国家自然科学基金项目(61379015); 山东省自然科学基金项目(ZR2011FM004); 江苏省自然科学基金项目(BD2012129); 江苏省高校"青蓝工程"资助项目(苏教师[2014]23 号).
作者简介: 滕春燕, 硕士, 副教授, 主要从事图像处理、信息安全、软件技术的研究.

点$(x, y)$在 DCT 域内对应的位置数；$S(u)$,$S(v)$ 都是 $C(u, v)$ 的核变换

$$S(u)=\begin{cases}\sqrt{\frac{1}{2}} & u=0\\ 1 & 1\leqslant u\leqslant L-1\end{cases},\quad S(v)=\begin{cases}\sqrt{\frac{1}{2}} & v=0\\ 1 & 1\leqslant v\leqslant H-1\end{cases}\tag{2}$$

通常，式(1) 主要是用于将图像分割为 $8\times 8$ 后的非重叠子块，从而输出对应的低频与高频子带. 为了重构图像，需要用到式(1) 的逆变换，其模型为[8]：

$$f(x, y)=S(u)S(v)\sqrt{\frac{2}{LH}}\sum_{x=0}^{L-1}\sum_{y=0}^{H-1}C(u, v)\cos\left[\frac{\pi}{L}u\left(x+\frac{1}{2}\right)\right]\cos\left[\frac{\pi}{H}v\left(y+\frac{1}{2}\right)\right]\tag{3}$$

初始图像 $f(x, y)$ 被式(1) 变换后，其大部分能量主要集中在低频系数上，充分反映载体图像的背景，有效避免了显著性目标，能够改善其隐秘性，对 JPEG 压缩等几何变换具有良好的稳健性[9]. 所以，在所提水印方案中，主要是择取宿主图像对应的低频系数来实现水印嵌入. 以图 1(a) 为样本，对其实施 DCT 处理后，输出数据见图 1(b).

(a) 初始图像

(b) DCT变换结果

图 1　DCT 方法处理结果

## 2　人工蜂群算法

人工蜂群(ABC, artificial bee colony) 是一种有效的自然启发优化技术，它是一种基于群体的优化算法[10-11]. ABC 算法主要是通过将蜜蜂群体分成 3 组来执行：

1) 受雇蜜蜂. 它们从不同的来源收集食物，然后返回蜂房储存食物并表演摇摆舞，以表明它们访问过的食物的质量.

2) 观察蜜蜂. 它们观看舞会，以了解高品质的食物来源，并据此告知受雇的蜜蜂要探索的邻近来源.

3) 侦查蜜蜂. 它们主要是随机探索新的食物来源.

ABC 算法主要是通过引入上述 3 个群体来搜索最优或近似最优解，主要过程如下：

Step 1：初始化. 随机产生一个大小为 $N_S$ 的蜂源，每个目标 $X$ 均位于 $X_{\min}=(X_{\min,1}, X_{\min,2}, \cdots, X_{\min,D_s})$ 与 $X_{\max}=(X_{\max,1}, X_{\max,2}, \cdots, X_{\max,D_s})$ 之间，其中，$D_s$ 是解空间的维度. 则蜂源的产生函数如下：

$$x_{i,j}=x_{\min,j}+r(0,1)\cdot(x_{\max,j}-x_{\min,j})\tag{4}$$

其中：$i=1,2,\cdots, N_S$ 是蜂源的数量；$j=1,2,\cdots, D_s$ 是解的维度；$r(0, 1)$ 是一个随机数.

Step 2：雇佣蜂阶段. 雇佣蜂更新它们的位置(解) 以产生新的种群. 每个解 $X_i$ 是通过如下函数修改其邻近元素 $X_{i,j}$ 来更新的：

$$y_{i,j}=x_{i,j}+\varphi_{i,j}\cdot(x_{i,j}-x_{k,j})\tag{5}$$

其中：$y_{i,j}$ 是更新位置 $Y_i$ 中的第 $j$ 个元素；$\varphi_{i,j}\in[-1, 1]$ 是一个随机数；$k=1,2,\cdots, N_S$ 是第 $k$ 个蜂源. 为了保持更新的有效性，需要保持 $k\neq i$，并根据各自对应的适应度函数来比较 $X_i$ 与 $Y_i$，若 $Y_i$ 的适应度值大于 $X_i$，则用 $Y_i$ 替代 $X_i$.

Step 3：观察蜂阶段. 在该过程中，每个观察蜂通过任选一个解，使用式(5)来更新，并根据概率值来确定一个最优解[10]

$$P_i = \frac{f(s_i)}{\sum_{j=1}^{N_S} f(s_j)} \tag{6}$$

其中：$P_i$ 是第 $i$ 个解对应的选择概率；$f(s_i)$ 是第 $i$ 个解的适应度.

Step 4：侦查蜂阶段. 侦察蜂随机搜索新的解. 在ABC算法中，定义了一个值，名为“Trials”. 所有的更新解均有一个初始的Trials值，为零. 如果一个解的Trials值超过了预设值(称为“Limits”)，则利用式(4)产生的随机解来替代它.

Step 5：检查算法迭代终止条件. ABC算法是一种迭代方法，它不断重复前面Step 2－Step 4，直到满足停止准则. 一般而言，通过设置一个表示最大迭代次数的预定值来定义停止准则.

## 3 基于离散余弦变换与最优嵌入强度预测的鲁棒图像水印算法

基于离散余弦变换与最优嵌入强度预测的鲁棒图像水印算法示意图见图2. 将安全密钥融入到水印检测阶段，可增强系统的安全性. 基于离散余弦变换与最优嵌入强度预测的鲁棒图像水印算法主要分为两个部分，分别见图2(a)和图2(b). 选择离散余弦变换后的低频系数可有效增强水印系统的不可感知性；利用不同攻击类型的鲁棒性来构建人工蜂群算法的适应度函数，通过对其迭代，以预测最优嵌入强度值，从而设计水印嵌入机制，可较好地平衡水印隐秘性与抗几何变换能力. 最后，借助水印检测方案来恢复密钥数据.

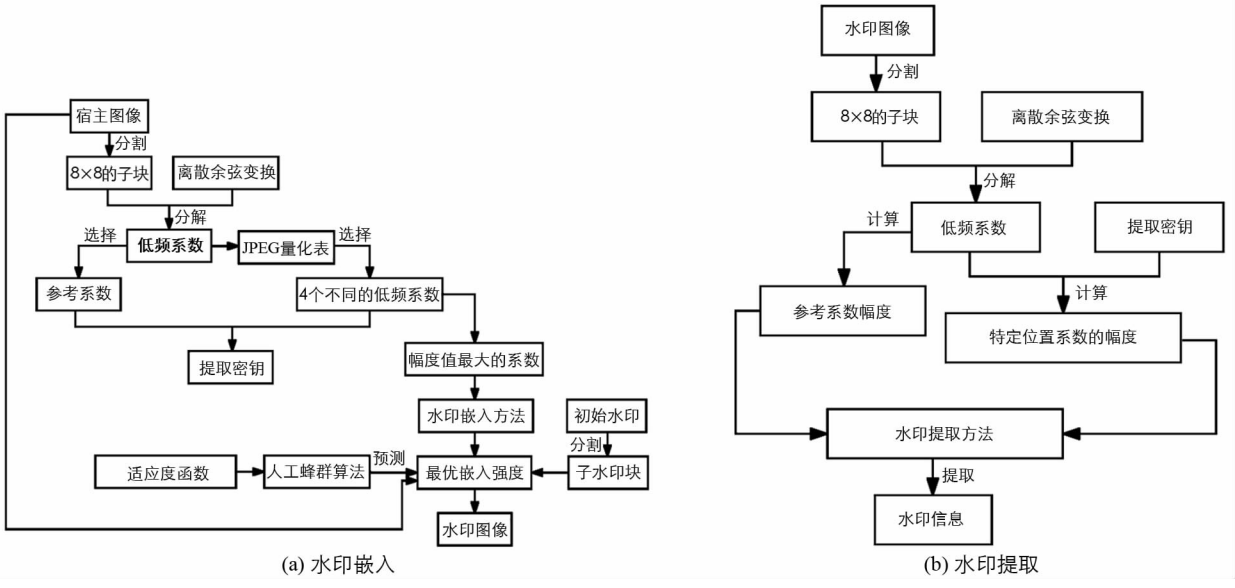



图2 本文鲁棒水印算法分解示意图

### 3.1 水印嵌入

1) 令 $I=\{f(x,y), 0\leqslant x<M, 0\leqslant y<N\}$ 是大小为 $M\times N$ 的宿主图像，并将其分割为若干个 $8\times 8$ 的非重叠子块，从而得到图3所示JPEG量化表；

2) 利用“1 离散余弦变换”章节的分解过程，处理每个子块

$$I_{m,n}^{\mathrm{DCT}} = \mathrm{DCT}(I_{m,n}) \tag{7}$$

利用式(7)处理所有的子块，可输出对应的低频子带与高频子带. 为了便于描述，令低频子带的系数为 $C=\{C_1,C_2,\cdots,C_z\}$，其中 $z$ 是低频系数的数量.

3) 从 $C=\{C_1,C_2,\cdots,C_z\}$ 任意选择一个系数作为参

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 11 | 10 | 16 | 24 | 40 | 51 | 61 |
| 12 | 12 | 14 | 19 | 26 | 58 | 60 | 55 |
| 14 | 13 | 16 | 24 | 40 | 57 | 69 | 56 |
| 14 | 17 | 22 | 29 | 51 | 87 | 80 | 62 |
| 18 | 22 | 37 | 56 | 68 | 109 | 103 | 77 |
| 24 | 35 | 55 | 64 | 81 | 104 | 113 | 92 |
| 49 | 64 | 78 | 87 | 103 | 121 | 120 | 101 |
| 72 | 92 | 95 | 98 | 112 | 100 | 103 | 99 |

图3 $8\times 8$ 子块对应的JPEG量化表

考系数 $C_{ref}$（一般位于左上角处）；再根据 JPEG 量化表（图 3），从 $C=\{C_1,C_2,\cdots,C_z\}$ 中确定出与 $C_{ref}$ 具有相近值的 4 个不同的系数 $C_1,C_2,C_3,C_4$；

4）从 $C_1,C_2,C_3,C_4$ 中选择一个与 $C_{ref}$ 最为接近的系数

$$\min C_w \left| |C_{ref}|-|C_w| \right|,\ w=1,2,3,4 \tag{8}$$

其中：$C_w$ 是系数；$|\cdot|$ 是求绝对值运算.

5）记录选择系数 $C_w$ 的位置，将其视为选择密钥；

6）从系数 $C_{ref}$ 与 $C_w$ 中确定出最大的幅度值 $V_{\max}$：

$$V_{\max}=\max(|C_{ref}|,|C_w|) \tag{9}$$

7）根据 $V_{\max}$ 把子水印隐藏到参考系数和选择系数中：

$$\begin{cases} |C_w|^*=[V_{\max}+\alpha]\cdot I(w_{m,n}=1)+|C_w|\cdot I(w_{m,n}=0) \\ |C_{ref}|^*=[V_{\max}+\alpha]\cdot I(w_{m,n}=0)+|C_{ref}|\cdot I(w_{m,n}=1) \end{cases} \tag{10}$$

其中：$|C_{ref}|^*$ 与 $|C_w|^*$ 是嵌入水印后的参考系数与选择系数；$\alpha$ 是嵌入强度，主要通过优化技术来预测其最佳值；$I()$ 是指示函数，其值只有“0”和“1”，当输入条件 $w_{m,n}=1$ 时，则 $I(w_{m,n}=1)=1$.

8）利用 $|C_{ref}|^*$ 与 $|C_w|^*$ 替代宿主图像中对应位置的系数，形成水印子块的 DCT 系数：

$$\begin{cases} |I^w_{m,n}(i,j)_{C_w}|=|C_w|^* \\ |I^w_{m,n}(i,j)_{C_{ref}}|=|C_{ref}|^* \end{cases} \tag{11}$$

其中：$(i,j)_{Cw}$ 是选择系数的位置；$(i,j)_{Cref}$ 是参考系数的位置.

9）利用 DCT 逆变换，将水印系数转换到空域，输出水印子块图像.

### 3.2　水印检测

1）令水印图像为 $I^w$，并将其分割为一系列的 $8\times8$ 的非重叠子块；

2）借助 DCT 方法对每个水印图像的子块实施分解，输出低频系数：

$$I^{w\mathrm{DCT}}_{m,n}=\mathrm{DCT}(I^w_{m,n}) \tag{12}$$

3）计算水印子块图像中参考系数的幅度值：

$$|C_{ref}|^w=|I^{w\mathrm{DCT}}_{m,n}(i,j)_{C_{ref}}| \tag{13}$$

4）根据水印过程中存储的密钥，选择位于 $(i,j)_{Cw}$ 处的系数；

5）再计算选择系数的幅度值：

$$|C_w|^w=|I^{w\mathrm{DCT}}_{m,n}(i,j)_{C_w}| \tag{14}$$

6）借助步骤 5）的幅度值，构建水印检测函数，以恢复水印内容：

$$w_{m,n}=\begin{cases}1 & \text{if } |C_w|^w>|C_{ref}|^w \\ 0 & \text{else}\end{cases} \tag{15}$$

7）利用步骤 1）－步骤 6）处理所有的水印子块，以提取完整的水印信息.

## 4　最优嵌入强度的预测

一般而言，为了增强水印系统的抗攻击能力，通常会取较大的 $\alpha$ 值；然而，取较大的 $\alpha$ 值会削弱其不可感知性[7]. 因此，为了最大程度地平衡水印图像的不可感知性与鲁棒性，本文利用人工蜂群算法 ABC[11] 来预测一个最优的嵌入强度，其过程见图 4. 由图 4 发现，本文主要是利用峰值信噪比[12] PSNR(peak signal noise ratio) 与归一化相关

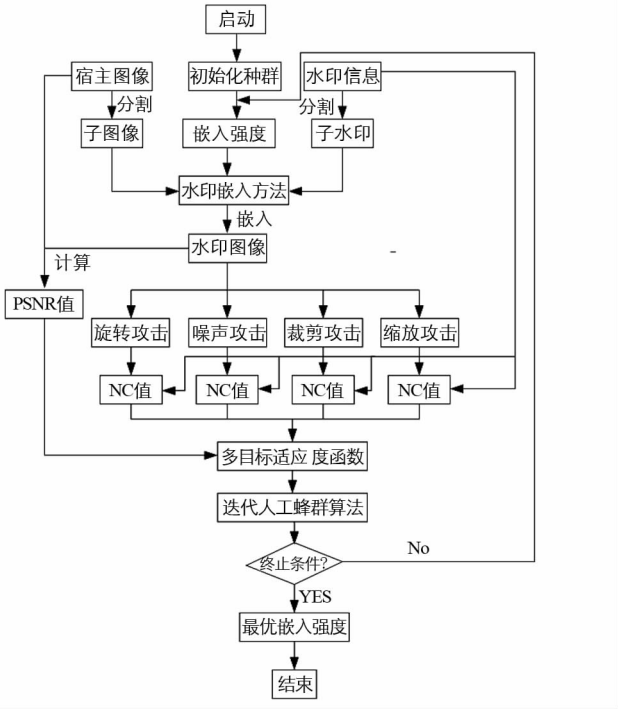



图 4　基于 ABC 算法的嵌入强度优化过程

系数(normalized correlation-coefficient)[13] $N_Q$ 来建立ABC算法的适应度函数. 其中，PSNR是反映水印图像质量优劣的经典指标，其值越大，说明其水印不可感知性越好，其计算模型为[12]：

$$P_{\mathrm{PSNR}}(I,\ I')=10\lg\left(\frac{255^2}{\frac{1}{n\times n}\sum_{i=1}^{n}\sum_{j=1}^{n}[I(i,\ j)-I'(i,\ j)]^2}\right) \tag{16}$$

其中：$P_{\mathrm{PSNR}}$ 为PSNR值；$I$，$I'$ 分别是宿主目标与水印结果；$n$ 是图像的高度或宽度；$(i,\ j)$ 是像素坐标.

$N_Q$ 是反映水印系统鲁棒性的经典指标，其值越大，表明在几何内容操作下所获取的水印与初始水印更加接近，其计算公式

$$Q(I,\ I')=\frac{\sum_{i=1}^{n}\sum_{j=1}^{n}W(i,\ j)W'(i,\ j)}{\sum_{i=1}^{n}\sum_{j=1}^{n}[W(i,\ j)]^2} \tag{17}$$

根据PSNR与 $N_Q$ 值，建立人工蜂群算法的适应度函数：

$$f=\min\left\{\frac{q}{P_{\mathrm{PNSR}}+\sum_{i=1}^{q}Q_i}\right\} \tag{18}$$

其中 $q$ 代表几何攻击类型的种类，在本文中，取 $q=4$. $Q_i$ 代表初始水印与在第 $i$ 种几何攻击下的复原水印之间的归一化相关系数值.

令宿主图像、水印信息分别为 $I$ 与 $W$，则水印嵌入强度的优化过程为：

1) 令宿主子图像为 $I_{\mathrm{sub}}$，子水印为 $w_{\mathrm{sub}}$，若 $I_{\mathrm{sub}}$ 的尺寸是 $M_{\mathrm{sub}}\times N_{\mathrm{sub}}$，则 $w_{\mathrm{sub}}$ 的尺寸 $M_{w\text{-}\mathrm{sub}}\times N_{w\text{-}\mathrm{sub}}$ 的计算公式为：

$$M_{w\text{-}\mathrm{sub}}=\frac{M_{\mathrm{sub}}}{8} \tag{19}$$

$$N_{w\text{-}\mathrm{sub}}=\frac{N_{\mathrm{sub}}}{8} \tag{20}$$

2) 将所有的宿主子图像 $I_{\mathrm{sub}}$ 视为ABC算法的初始蜂源，用于嵌入水印信息，并设置最大迭代次数为 $T_{\max}$，初始化 $T=0$；

3) 随机选择一个蜂源与一个嵌入强度，根据“3.1 水印嵌入”章节，将水印信息隐藏到宿主子图像 $I_{\mathrm{sub}}$，形成水印图像，根据式(16)，计算其与初始宿主子图像之间的PSNR值；再从水印结果中恢复密钥内容，并借助式(17)，计算其与源子水印之间的 $N_Q$ 值；同时，基于式(18)计算此时的适应度函数；

4) 雇佣蜂利用式(4)来更新子图像 $I_{\mathrm{sub}}$ 对应的蜂源（嵌入强度），并根据步骤2)，计算不同嵌入强度对应的适应度函数值；

5) 利用式(18)替代式(6)中的适应度 $f(s_i)$，此时，侦查蜂利用式(6)来获取蜂源（嵌入强度）的选择概率 $P_i$；

6) 随后，侦查蜂基于贪婪策略[14]来更新全局最优蜂源；

7) 侦查蜂根据步骤5)得到的 $P_i$ 确定物源，且利用式(5)在其领域搜索，以输出新的蜂源，并计算其对应的适应度函数值；

8) 如果蜂源经过 $L$ 次更新保持不变，则将其丢弃；否则，用新的蜂源来替代它；

9) 记录此时的最优蜂源；

10) 判断是否符合迭代终止条件，如果达到 $T_{\max}$ 次，则输出最优嵌入强度；反之，则继续执行步骤4).

对于所有的宿主子图像，利用上述过程来预测其对应的最优嵌入强度，以此完成水印信息的隐藏，最大程度地改善水印图像的视觉隐秘性与抗几何攻击能力，并将这些嵌入强度组合成一个集合 $\mathrm{Optimal}\_\alpha=\{\alpha_1,\ \alpha_2,\ \cdots\alpha_v\}$，$v=\dfrac{M\times N}{8\times 8}$.

## 5 实验结果与分析

将本文算法与文献[6-7]算法进行对比实验. 不失一般性，从USC-SIPI数据库中任选2幅图像，将二

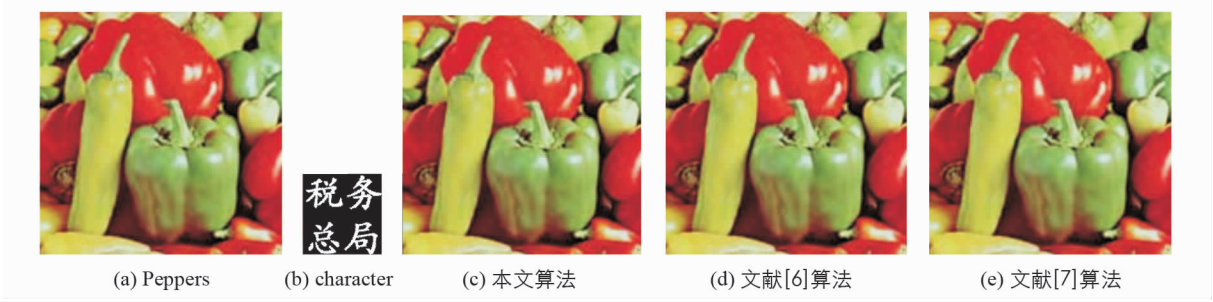
者视为宿主目标，见图 5(a)－5(b)，大小都是 256×256；将图 5(c)－5(d) 作为源水印，尺寸均为 64×64. 实验参数为：$T=0$，$L=8$，$T_{max}=600$，$N_S=100$；观察蜂数量为 50 个、雇佣蜂数量为 50 个、嵌入强度 $\alpha\in[3,15]$.

### 5.1　不可感知性的测试分析

利用所提方法与文献[6]、文献[7]的嵌入过程，将图 5(c)－5(d) 分别隐藏到宿主图像(图 5(a)－5(b))中，形成的水印图像见图 6,7. 由测试结果发现，3 种方案所输出的水印图像都具备良好的视觉不可感知性，其与初始宿主图像几乎一模一样，难以直接从中获取有关水印的任何信息.


(a) Peppers　(b) Lena　(c) character　(d) Tortoise

图 5　宿主图像与待嵌入水印




(a) Peppers　(b) character　(c) 本文算法　(d) 文献[6]算法　(e) 文献[7]算法

图 6　图像 Peppers 上的水印不可感知性测试

(a) Lena　(b) Tortoise　(c) 本文算法　(d) 文献[6]算法　(e) 文献[7]算法

图 7　3 种算法的水印不可感知性测试结果

利用人眼主观感觉难以反映技术与文献[6]、文献[7]的水印隐秘性的差异，因此，本文借助经典的灰度分布差分图[4]进行客观评价. 通常，若水印图像与宿主图像的灰度分布拟合度越高，意味着此技术的不可感知性越好. 在此次试验中，将图 7(a)，7(c)－7(e) 作为样本，统计了宿主图像与 3 种技术所获取的水印图像之间的差分图，形成的灰度分布见图 8；又依据式(16)得到了 3 种技术的峰值信噪比[12]PSNR，数据见表 1. 由图 8 可知：本文算法形成的水印图像和宿主图像之间的灰度分布很接近，几乎没有起伏效应；文献[7]算法也呈现出理想的差分曲线分布，灰度拟合情况较好；文献[6]方法的差分图不佳，与宿主图像的灰度分布拟合偏差较大，有明显的起伏效应，这种灰度分布起伏容易被攻击者发现，使其不可感知性有待提高. 由表 1 可知：本文算法得到的 PSNR 值最大，约为 44.78 dB；文献[7]算法的 PSNR 值为 43.19，与本文算法较为接近；文献[6]方法的 PSNR 值最小，约为 40.56 dB. 主要原因是本文算法利用了 DCT 机制来分解宿主子图像，从每个子块中选择低频系数作为嵌入位置，使得嵌入水印对宿主图像修改范围较小，且引入了人工蜂群机制来优化嵌入强度，根据该优化值将水印信息隐藏到 DCT 系数中，最大程度地平衡了视觉隐

秘性与鲁棒性，使其很好地保持了宿主图像的灰度分布特征，因此，本文算法具有更高的视觉不可感知性. 文献[7]技术则是利用离散小波变换来分解宿主子图像，通过SIFT方法来提取每个子图像的特征点，并将这些特征点作为嵌入位置，使其对宿主图像的修改程度较小，而且利用了粒子群算法来优化其嵌入强度，较好地兼顾了不可感知性与鲁棒性. 但是，该技术是将整个子块的SIFT特征点作为嵌入位置，对宿主图像的修改范围要大于本文算法，故其不可感知性略低. 而文献[6]技术则是利用提升小波变换与奇异值分解来实现水印嵌入，将宿主图像的HL子带作为嵌入位置，对宿主图像的修改范围较大，而且嵌入强度主要是一个经验固定值，故其不可感知性更低.

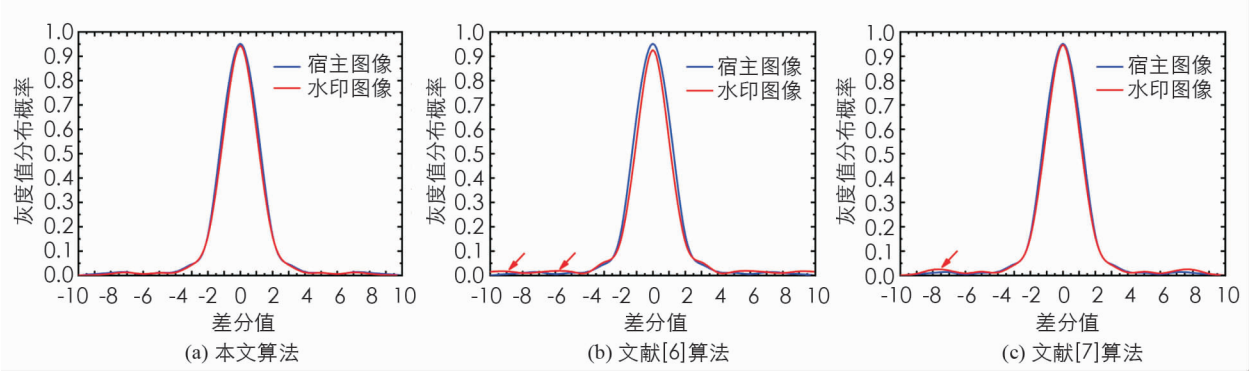



图8 不同水印技术的差分曲线图

**表1 各水印图像的PSNR值**

| 名称 | 本文算法 | 文献[6]算法 | 文献[7]算法 |
|---|---|---|---|
| PSNR值/dB | 44.78 | 40.56 | 43.19 |

## 5.2 鲁棒性测试

把图7(c)—7(e)当作对象，施加表2所示的几何攻击，形成一系列的篡改样本. 随后，基于本文方法、文献[6]与文献[7]的水印检测方法，从这些篡改样本中提取水印，并根据式(17)相应的归一化系数$N_Q$和位正确率BCR(Bit Correct Ratio)来量化鲁棒性. BCR的计算公式为

$$B(W, W') = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}\overline{W(i, j)\oplus W'(i, j)}}{n\times n} \tag{21}$$

其中：$W(i, j)$是初始水印；$W'(i, j)$是提取水印；$\oplus$是XOR算子；$\overline{()}$是NOT算子.

**表2 几何失真变换及其参数值**

| 名称 | 角度旋转 | 缩放 | 椒盐噪声 | 图像中心裁剪 |
|---|---|---|---|---|
| 参数值 | 30° | 1.5 | 0.03 | 20% |

表3显示了本文算法与文献[6]、文献[7]算法所提取的水印与初始水印之间的$N_Q$与$B$值. 由表3数据发现，当水印图像遭受几何变换攻击时，3种技术所提取的水印质量都存在失真，鲁棒性由强到弱依次为文献[6]算法、本文算法、文献[7]算法. 主要是因为文献[6]算法利用SVM方法设计一种几何校正方法，在水印提取前，对遭遇几何攻击的水印图像实施变换参数的预测，并根据预测结果对攻击水印图像完成校正，使其具有更高的鲁棒性，所复原水印具有更好的质量. 而本文算法则是利用人工蜂群算法对遭遇多种几何攻击的水印图像进行训练，以预测最优的嵌入强度，以此来完成水印嵌入，最大程度地改善水印系统的鲁棒性. 文献[7]算法虽然也利用了粒子群算法来预测最优的嵌入强度，利用优化后的嵌入强度来获取水印图像，但是此技术采用的SIFT方法是依赖强度梯度检测的宿主图像特征点来实施水印嵌入，不能描述图像的非纹理区域的特征，使得鲁棒性较弱.

## 5.3 算法复杂度分析

令载体的大小为$M\times N$，根据所提算法的过程可知，其水印嵌入的复杂度主要集中在离散余弦变换DCT处理、JPEG量化以及人工蜂群算法的3个过程. 对于大小为$M\times N$图像，将其分割为$8\times 8$的子块，

总共含有$(M\times N)/64$个子块. 利用DCT来分解每个子块，对于其相应的复杂度为$o[(M\times N)/64]$. JPEG量化的复杂度为$o(z)$，$z$为低频系数的数量. 另外，人工蜂群算法的复杂度为$o(T_{\max}\times(M\times N)^2/64^2)$，其中$T_{\max}$为迭代次数. 因此，所提算法的总复杂度为$o[(M\times N)/64+z+T_{\max}\times(M\times N)^2/64^2]$.

**表 3　鲁棒性测试结果**

| 名称 | 实验结果 | 旋转 | 缩放 | 椒盐噪声 | JPEG 压缩 |
|---|---|---|---|---|---|
| 本文算法 | $B$ | 0.905 | 0.918 | 0.925 | 0.912 |
| | $N_Q$ | 0.926 | 0.941 | 0.949 | 0.937 |
| | 提取水印 |  |  |  |  |
| 文献[6] | $B$ | 0.921 | 0.939 | 0.943 | 0.928 |
| | $N_Q$ | 0.953 | 0.974 | 0.981 | 0.969 |
| | 提取水印 |  |  |  |  |
| 文献[7] | $B$ | 0.879 | 0.915 | 0.918 | 0.857 |
| | $N_Q$ | 0.904 | 0.940 | 0.945 | 0.896 |
| | 提取水印 |  |  |  |  |

文献[6]的水印嵌入复杂度主要在于小波变换处理、奇异值分解以及支持向量机的训练，其中，小波变换的复杂度为$o[(M\times N)\lg(M\times N)]$，奇异值分解的复杂度为$o(1\ 024\ m^3)$，其中$m$为每个子块的奇异值数量. SVM的复杂度为$o(4a^2)$，$a$为样本数量. 因此，文献[6]的总复杂度为$o[(M\times N)\lg(M\times N)+1\ 024m^3+4a^2]$.

文献[7]的水印嵌入复杂度主要集中在SIFT特征点检测、奇异值分解、水印信息的离散小波变换处理以及粒子群算法的优化等4个过程，其中：SIFT算子的复杂度为$o(128n)$，$n$为特征点数量. 奇异值分解的复杂度为$o(4\ m^3)$，$m$为每个子块的奇异值数量. 水印的离散小波变换处理复杂度为$o[(k\times h)\lg(k\times h)]$，$k\times h$为水印图像的尺寸. 粒子群算法的复杂度为$o(4Ts^2)$，$T$为迭代次数，$s$为粒子群数量. 因此，文献[7]的总复杂度为$o(128n+4m^3+(k\times h)\lg(k\times h)+4Ts^2)$.

根据上述分析可知，文献[7]的复杂度最低，效率最高. 而本文算法的复杂度由于采用了人工蜂群算法，复杂度最高.

## 6　结　　论

为了较好地平衡水印图像的视觉隐秘性与抗几何攻击能力，本文提出了基于离散余弦变换与最优嵌入强度预测的鲁棒图像水印算法. 在嵌入过程中，利用离散余弦变换方法来处理宿主子图像，从中确定出合适的低频系数作为嵌入位置. 并基于峰值信噪比与不同类型攻击下的归一化相关系数来建立适应度函数，通过执行人工蜂群机制，对每个子图像及其相应的子水印进行水印嵌入强度的优化预测. 根据优化的嵌入强度，将水印信息隐藏到宿主子块中，形成水印图像. 在水印检测阶段，利用水印嵌入过程中产生的安全密钥，从水印图像中恢复密钥内容，并将所提水印方案与已有的水印方法实施了对比测试，试验数据显示了所提技术不仅具有更高的水印视觉隐秘性，同样也具备较强的鲁棒性，可以有效抵御多种不同的几何变换攻击类型.

由于所提水印方案采用了人工蜂群机制，在一定程度上增加了算法的复杂度，在未来研究中，将对其进行优化，在兼顾水印隐秘性与鲁棒性的同时，也尽可能地降低算法耗时.

**参考文献：**

[1]　聂　敏. 基于极性的立体图像盲数字水印算法[J]. 西南师范大学学报(自然科学版)，2019，44(7)：77-80.
[2]　李红日，方　逵. 基于误差扩展与像素容量评估的图像水印算法[J]. 西南大学学报(自然科学版)，2017，39(10)：109-118.
[3]　李咪丹. 基于调制网点形状的半色调图像信息隐藏防伪技术 [D]. 西安：西安理工大学，2016：9-15.
[4]　王　洪，王　聪，余金暇. 基于 Walsh-Hadamard 变换与预测误差扩展的图像水印算法 [J]. 光学技术，2018，44(4)：487-494.

[5] HUA K L, DAI B R, SRINIVASAN K, et al. A Hybrid NSCT Domain Image Watermarking Scheme [J]. EURASIP Journal on Image and Video Processing, 2017, 2017: 10.
[6] ISLAM M, LASKAR R H. Geometric Distortion Correction Based Robust Watermarking Scheme in LWT-SVD Domain with Digital Watermark Extraction Using SVM [J]. Multimedia Tools and Applications, 2018, 77(11): 14407-14434.
[7] 晁 妍, 王诗兵, 王慧玲. 基于奇异值分解和粒子群优化算法的图像水印算法 [J]. 吉林大学学报(理学版), 2018, 56(5): 1163-1169.
[8] GHAZVINI M, HACHROOD E M, MIRZADI M. An Improved Image Watermarking Method in Frequency Domain [J]. Journal of Applied Security Research, 2017, 12(2): 260-275.
[9] 董夙慧, 孙中廷, 徐永刚. 基于YCoCg-R颜色空间与离散余弦变换的自适应彩色图像水印算法 [J]. 包装工程, 2018, 39(13): 181-187.
[10] 银建霞. 人工蜂群算法的研究及其应用 [D]. 西安: 西安电子科技大学, 2012: 6-11.
[11] ALI M, AHN C W, PANT M, et al. An Image Watermarking Scheme in Wavelet Domain with Optimized Compensation of Singular Value Decomposition via Artificial Bee Colony [J]. Information Sciences, 2015, 301: 44-60.
[12] 陈文鑫, 邵利平, 师军. 结合均值调整整数变换的迭代自适应可逆图像水印算法 [J]. 计算机应用, 2015, 35(7): 1908-1914, 1938.
[13] CHEN L, ZHAO J Y. Contourlet-Based Image and Video Watermarking Robust to Geometric Attacks and Compressions [J]. Multimedia Tools and Applications, 2018, 77(6): 7187-7204.
[14] YU W J, ZHAN Z H, ZHANG J. Artificial Bee Colony Algorithm with an Adaptive Greedy Position Update Strategy [J]. Soft Computing, 2018, 22(2): 437-451.

# Robust Image Watermarking Algorithm Based on Discrete Cosine Transform and Optimal Embedding Strength Prediction

TENG Chun-yan[1], YANG De-yun[2,3]

1. *Department of Information Technology, Jiangsu United Vocational and Technical College Xuzhou Branch of Finance and Economics, Xuzhou Jiangsu 221008, China;*
2. *School of Software, Shandong University, Ji'nan 250100, China;*
3. *School of Information Science and Technology, Taishan College, Tai'an Shandong 271000, China*

**Abstract**: In order to solve the problem as impossible to both the geometric attack ability and visual concealment of the system in current image watermarking scheme, a robust image watermarking algorithm based on discrete cosine transform and optimal embedding strength prediction has beenproposed. Firstly, the host image was divided into several $8\times8$ non-overlapping sub-blocks, and the embedded watermark was divided into sub-watermark with the same number of host image. The discrete cosine transform was applied to deal with each sub block for outputting the corresponding low frequency and high frequency sub-bands. A coefficient was selected from the low frequency sub-band as the reference coefficient, and four different coefficients close to the reference coefficient were selected with the help of the JPEG quantization table. From these four different coefficients, the closest coefficients to the reference coefficients were determined which stored as the key, and the maximum amplitude coefficient were found out. The artificial bee colony algorithm was introduced to train the training samples for output a set of data by using the robustness of different attack types to construct its fitness function for predicting the optimal embedding strength value. The watermark embedding method was designed to hide the watermark content into the maximum amplitude coefficient and reference coefficient for outputting the watermark image. Finally, according to its storage location, a watermark extraction method was established to recover the watermark information. Test data show that, compared with existing watermarking schemes, this watermarking scheme has better watermarking effect, which has better visual concealment and robustness under various geometric attacks.

**Key words**: image watermarking; discrete cosine transform; artificial bee colony; embedding strength prediction; reference coefficient; fitness function

**责任编辑** 张 枸