DOI: 10.13718/j.cnki.xdzk.2017.10.016

基于误差扩展与像素容量评估的图像水印算法①

李红日[1,2]，　方　逵[2]

1. 湖南机电职业技术学院 信息工程学院，长沙 410151；
2. 湖南农业大学 信息科学技术学院，长沙 410128

摘要： 为了解决当前图像水印算法无法准确预测相邻像素间的误差值，不能根据像素的局部纹理特征差异来自适应确定其嵌入容量，导致复原水印信息存在较大失真以及水印容量较小的问题，本文提出了基于误差扩展与像素容量评估的无损图像水印算法. 首先，设计动态混淆方法，对水印信息完成加密；再考虑 3 个相邻像素，引入边缘像素预测机制，准确预测载体图像的每个像素值，获取其对应的误差值；随后，利用载体图像中的任意 3 个相邻像素的方差，设计像素容量评估方法，对其水印容量完成评估；借助误差扩展技术，设计水印信息嵌入机制，根据像素容量评估结果，将不同容量的水印数据植入到载体图像的不同像素中，获取水印图像；最后，建立水印提取方法，结合解密密钥，准确复原水印信息. 实验数据表明：与当前图像水印技术相比，所提算法具有更高的水印质量与水印容量.

关　键　词： 图像水印；误差扩展；像素值预测；像素容量评估；水印嵌入；动态加密；水印提取

中图分类号： TP391　　**文献标志码：** A　　**文章编号：** 1673－9868(2017)10－0109－10

随着多媒体技术的发展与因特网的广泛应用，图像因其含有丰富的内容与较高的直观表达特性，在军事、医学等领域占有重要地位[1－2]. 然而，近年来随着软件技术的日益完善，市场上出现了多种强大的编辑工具，在开放的网络中传输时，它们能够肆意修改图像，且不留下篡改痕迹，导致用户无法对其真实性进行判定，对图像信息安全造成了隐患[3]. 因此，如何确保图像信息的真实性，确保其在网络传输中不被攻击与篡改，已成为各领域的研究热点[4]. 如朱丹丹等人[5]为了提高水印图像的抗几何攻击能力，提出了基于伪 Zernike 矩和 Contourlet 变换的抗几何攻击图像水印算法，利用 Contourlet 变换处理载体图像，获取其低频子带；然后依据嵌入水印前、后系数的相关性，利用 Zernike 矩的幅值将水印信息嵌入到图像的低频区域中，通过设计相应的水印提取技术，复原水印信息，该算法具有良好的抗几何攻击能力. 但是，该技术是将水印信息集中在低频区域，忽略了像素之间的差异，将相同容量的水印嵌入到每个像素中，易导致信息丢失，从而造成复原水印信息失真. Saeid Fazli 等人[6]为了提高水印图像的安全性，联合 DWT、DCT 与奇异值分解，设计了相应的图像水印技术，借助 DWT 机制，将载体图像变为 4 个频域子块，联合 DCT 方法，构建水印嵌入技术，将水印信息植入到子块中，最后，通过奇异值分解技术，提取其角点，设计水印提取技术，复原水印信息，测试数据表明其水印算法具有较高的安全性，能够抵御几何变换攻击. 然而，载体图像角点易受几何变换攻击的影响，导致其特征不稳定，降低了水印图像的不可感知性，且其无法将不同容量的水印数据自适应嵌入到相应的像素中，导致其提取的水印信息存在较大失真. Wang 等人[7]为了提高水

① 收稿日期：2017－05－23
基金项目：国家自然科学基金项目(61101235)；湖南省教育厅科学研究项目(15C0486).
作者简介：李红日(1980－)，男，湖南邵阳人，硕士，副教授，主要从事图像处理、数据挖掘、物联网技术与安全的研究.

印图像的安全性与不可感知性，提出了基于极谐变换与几何校正的水印算法，利用非下采样 Shearlet 变换来获取载体图像的鲁棒特征，通过设计水印嵌入技术，将水印信息隐藏到载体图像中，并利用极谐变换来设计几何校正技术，对水印图像的几何变换参数进行预测，从而准确校正水印图像，精确复原水印信息，实验结果验证了其水印算法的不可感知性与复原质量. 虽然该技术设计了几何校正机制，能够利用预测的几何攻击参数来校正水印图像，使其提取的水印信息失真较小，但是其忽略了局部像素之间的差异，无法实现水印容量的合理分配，导致整个算法的水印容量较小.

本文通过定义像素容量评估机制，提出了一种高容量的无损图像水印技术，对水印容量进行自适应分配. 为了提高算法的抗几何攻击能力与水印信息的不可感知性，联合 Lucas 序列与 Fibonacci 序列，设计动态混淆方法，对水印信息完成加密；引入边缘像素预测机制，获取像素的预测差值；随后，设计像素容量评估方法，对平滑区域中的每个像素分配更多的水印数据，而对其他区域则分配更小的水印数据，从而提高算法的水印容量，有效防止水印信息丢失，避免复原水印的失真；基于误差扩展技术，联合预测误差值与像素容量评估结果，设计水印信息嵌入机制，完成水印信息的自适应嵌入，获取水印图像；利用解密密钥与水印检测技术，准确复原水印信息. 最后，验证了所提水印技术的安全性与水印容量.

1 边缘像素预测机制

JPEG-LS 预测技术[8]能够分析 3 个相邻像素之间的纹理差异，见图 1. 其中，x 为预测像素，其相邻的 3 个像素为 a,b,c，通过 a,b,c 像素来判别 x 是属于水平边缘还是垂直边缘. 利用 JPEG-LS 预测技术来处理像素 x，其预测值为 X'，

$$X'=\begin{cases}\min(a,b) & \text{if } c\geqslant\max(a,b)\\ \max(a,b) & \text{if } c\leqslant\min(a,b)\\ a+b-c & \text{else}\end{cases} \tag{1}$$

根据式(1)可知，当 $c\geqslant\max(a,b)$，且 $\max(a,b)=a$ 时，意味着存在垂直边缘，即预测值 $X'=b$；反之，则其存在水平边缘，预测值 $X'=a$. 但是像素 c 有可能既不在最大值区间，也不在最小值区间，使其有可能不在边缘上. 这种情况下，像素 a,b,c 是非常接近的，意味着预测像素 x 位于图像中的平滑区域. 图 2 显示了图像边缘检测过程.

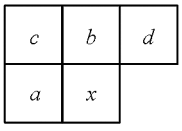


图 1 JPEG-LS 预测模式

根据上述描述可知，JPEG-LS 预测技术是只记录这个预测误差值，而不存储初始像素值，从而有效降低内存载荷[8]. 另外，预测误差值在携带水印信息前，通过误差扩展处理，可以降低像素的失真度.

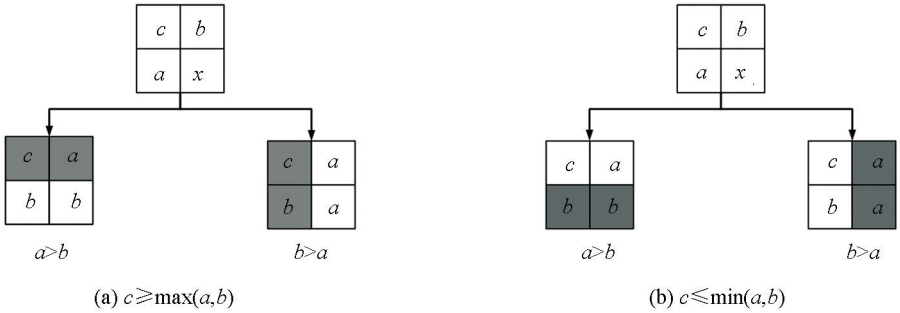


图 2 JPEG-LS 预测技术的边缘检测

2 误差扩展技术

为了避免像素失真，本文引入了误差扩展技术[9]对 2 个相邻像素的差值进行扩展，通过修改这个扩展误差值来嵌入一个密钥位. 其主要过程如下：

1）若 M_{xy} 为初始灰度图像，其中 x，y 是图像尺寸；再将 M_{xy} 分割为 Z 个不重叠子块，且每个子块由 2 个相邻像素构成，其大小为 $Z=\frac{(x+y)}{2}$. 令 $P_{k,l}$，$P_{k,r}$ 分别是第 k 个子块的左、右像素值. 则对于每个子块，其像素差值 d_k 与整数均值 m_k 的计算模型为

$$\begin{cases} d_k = P_{k,l} - P_{k,r} \\ m_k = \left\lfloor \dfrac{(P_{k,l}+P_{k,r})}{2} \right\rfloor \end{cases} \tag{2}$$

2）若像素差值 d_k 太大，易导致明显的伪效应，使其不适用信息隐藏. 反之，对其 d_k 进行扩展后，则可将水印数据隐藏到每个子块中. 若 s 为 1 位二值密钥信息，根据如下扩展函数，将 s 嵌入到子块的差值，则

$$d'_k = d_k \times 2 + s \tag{3}$$

3）根据上述获取的误差扩展值 d'_k，将包含水印信息的像素均等分割为新的子块 $P'_{k,l}$，$P'_{k,r}$，

$$\begin{cases} P'_{k,l} = m_k + \left\lfloor \dfrac{(d'_k+1)}{2} \right\rfloor \\ P'_{k,r} = m_k - \left\lfloor \dfrac{d'_k}{2} \right\rfloor \end{cases} \tag{4}$$

利用新的子块 $P'_{k,l}$，$P'_{k,r}$ 替代初始子块 $P_{k,l}$，$P_{k,r}$，完成信息嵌入过程.

3　无损图像水印算法

本文引入的高容量无损图像水印算法的过程见图 3，主要有：① 基于动态混淆技术的水印图像加密；② 水印信息嵌入；③ 水印信息的提取.

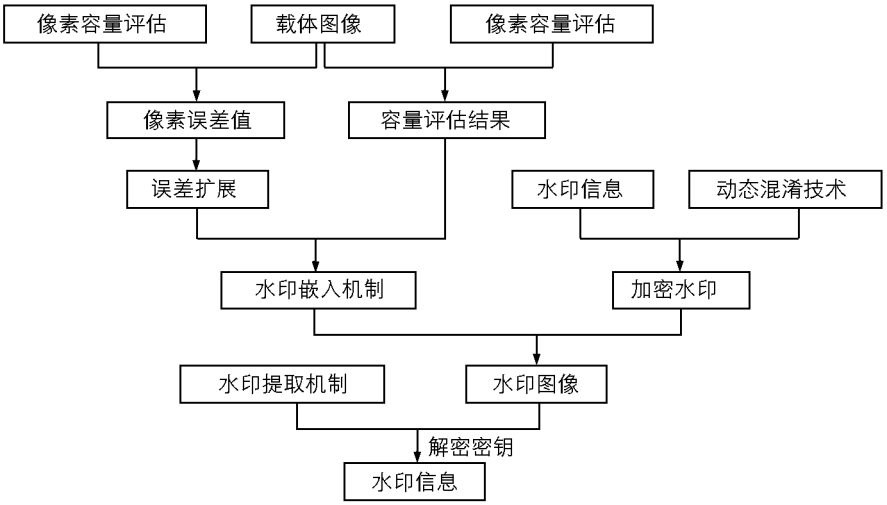


图 3　本文无损图像水印算法过程

3.1　基于动态混淆的水印信息加密

水印图像的抗几何攻击能力较弱，一旦其遭遇几何攻击，容易导致水印信息丢失或篡改，最终使得水印信息提取质量较差，存在较大的失真. 为了提高水印信息在载体图像中的不可感知性，并改善其抗几何攻击能力，本文综合 Fibonacci 序列与 Lucas 序列[10-11]，设计了动态加密技术，彻底消除混沌加密周期性.

Fibonacci 序列[10]是动态更新的整数变化序列，根据其初始种子[(0，1)，(1，1)]的差异，产生截然不同的输出序列，其函数如下：

$$F_n=\begin{cases}0 & n=1\\ 1 & n=2\\ F_n+F_{n-1} & n\geqslant 3\end{cases} \tag{5}$$

$$F_n=\begin{cases}1 & n=1\\ 1 & n=2\\ F_n+F_{n-1} & n\geqslant 3\end{cases} \tag{6}$$

综合上式可知，随着 n 的实时变化，当其种子变化时，能够输出2个整数序列0，1，1，2，3，5，8，13，21，34…与1，1，2，3，5，8，13，21，34，55….

同样地，Lucas序列[11]与Fibonacci序列类似，其函数是：

$$L_n=\begin{cases}2 & n=1\\ 1 & n=2\\ L_{n-1}+L_{n-2} & n\geqslant 3\end{cases} \tag{7}$$

若初始种子为(2，1)条件下，当 n 不断变化时，Lucas可输出整数数组2，1，3，4，7，11，18，29，47….

依据Lucas、Fibonacci序列性质可知，在图像加密的反复迭代过程中，随着迭代数量 n 的实时更新，其产生的随机序列也是不同的，从而在每一轮迭代期间，都是用不同的加密核来实现像素混淆，提高了密文的安全性，有效增强其抗几何攻击能力. 因此，本文利用2D Arnold映射[12]的思想，综合Lucas、Fibonacci序列，设计了动态混淆技术：

$$\begin{bmatrix}x'\\ y'\end{bmatrix}=\begin{bmatrix}F_nF_{n+1}\\ L_nL_{n+1}\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}\bmod N \tag{8}$$

其中，$(x，y)$为水印图像 $f''(i，j)$的像素位置；$(x'，y')$是加密后的像素位置；F_n，L_n 分别为Fibonacci、Lucas序列；N 是图像宽度.

用户首先设置好Fibonacci、Lucas序列的初始种子，将其作为密钥，再依据式(8)，对水印信息完成多轮加密. 因迭代数量n是不断变化的，其 F_n，F_{n+1}，L_n，L_{n+1} 序列值产生较大差异，最终使得动态混淆技术的加密核 $\begin{bmatrix}F_n & F_{n+1}\\ F_n+F_{n+2} & F_{n+1}+F_{n-1}\end{bmatrix}$ 出现理想的随机性. 若初始水印信息为 S_k，则对其完成上述加密后，输出水印密文 s_k，此时，再将其嵌入到水印图像中，能够提高水印图像的抗几何攻击能力，显著改善水印信息的不可感知性.

3.2 水印信息的嵌入

1) 根据人眼视觉，载体图像最上边与最左边的元素被保留，不嵌入水印信息. 令 $P_{i,j}$ 为载体图像 $f(i，j)$ 的第一个像素，在载体图像中的位置为(2，2)，则其相邻的3个像素为 $P_{1,2}$，$P_{2,1}$，$P_{1,1}$. 根据边缘像素预测机制可知，通过 $P_{1,2}$，$P_{2,1}$，$P_{1,1}$，可以找到像素 $P_{i,j}$ 的预测值. 根据式(1)计算像素 $P_{i,j}$ 的预测值 $P'_{i,j}(i\neq 1$ 或 $j\neq 1)$，其中，$x=P_{i,j}$，$a=P_{i-1,j}$，$b=P_{i,j-1}$，$c=P_{i-1,j-1}$. 再按照光栅扫描排序机制[13]，依据像素预测机制，可获取其他像素的预测值.

2) 为了充分利用不同像素的差异，根据每个像素自身的水印容量来确定其最大水印数据嵌入量，本文定义了像素容量评估机制. 由于在图像平滑区域像素的预测更加准确，其预测误差值接近0，因此，可以将更多的水印数据嵌入此类像素中. 为此，本文引入混合进制系统[14]，将水印数据转换成不同的基数. 通过这种方式，若基数值越大，则其具有更大的水印容量. 令3个像素 $P_{i-1,j}$，$P_{i,j-1}$，$P_{i-1,j-1}$ 的方差为 δ_{ij}^2，且初始像素 $P_{i,j}$ 的基数为 b_{ij}；则方差 δ_{ij}^2 为

$$\delta_{ij}{}^2=\frac{P_{i-1,j}^2+P_{i,j-1}^2+P_{i-1,j-1}^2}{3}-m_{ij}{}^2 \tag{9}$$

$$m_{ij}^2=\frac{P_{i-1,j}+P_{i,j-1}+P_{i-1,j-1}}{3} \tag{10}$$

依据式(9)，可得基数 b_{ij} 为

$$b_{ij}=\min\left(\left|\frac{\Delta}{\delta_{ij}^2}\right|,\ t\right) \tag{11}$$

其中，Δ 为常量；t 为阈值，用来控制像素的最大水印容量.

为了防止水印数据的嵌入进制系统容量超过 8 位，本文严格限制阈值 t 的范围在[0，255].

令初始水印信息为 S_k；加密后的水印信息为 s_k，将其转换为二进制值 $s_{d,k}$. 根据基数 b_{ij}，可获取像素 $P_{i,j}$ 对应的水印嵌入容量为

$$r_{i,j}=s_{d,k}\bmod b_{i,j} \tag{12}$$

3) 再计算初始像素值 $P_{i,j}$ 与预测值 $P'_{i,j}$ 的差值 $d_k=P_{k,l}-P_{k,r}$. 然后，根据式(9) ～ (11)，计算初始像素值 $P_{i,j}$ 对应的基数 b_{ij}，利用式(13) 对初始差值 d_{ij} 进行扩展 b_{ij} 次，则

$$d'_{i,j}=d_{i,j}\times b_{ij}+r_{ij} \tag{13}$$

通过式(13)的扩展，充分将水印数据 $r_{i,j}$ 隐藏到 d'_{ij} 中.

4) 联合式(13)的 $d'_{i,j}$，可以获取水印像素

$$P''_{i,j}=P'_{i,j}+d'_{i,j} \tag{14}$$

反复执行上述嵌入过程，直到所有的载体像素被处理后，最终输出水印图像 $f'(i,j)$.

3.3　水印信息的提取过程

根据上述的加密密钥 N，以及 Fibonacci、Lucas 序列的种子，通过相应的水印提取机制，复原水印信息.

1) 由于载体图像的最上边与最左边的元素被保留，不嵌入水印信息，故此位置的像素无需检测；

2) 对于水印图像 $f''(i,j)$ 中其他位置的像素 $P''_{i,j}$，其相邻的 3 个像素为 $P''_{i-1,j}$，$P''_{i,j-1}$，$P''_{i-1,j-1}$. 根据式(1)，获取 $P''_{i,j}$ 的预测值 $P'_{i,j}$；依据式(9) ～ 式(10)，计算 $P''_{i-1,j}$，$P''_{i,j-1}$，$P''_{i-1,j-1}$ 的方差 δ_{ij}^2，再利用式(11)，可获取 $P''_{i,j}$ 对应的基数 b_{ij}；

3) 计算新的差值 $d'_{i,j}=P''_{i,j}-P'_{i,j}$. 根据如下函数，提取二进制水印信息 $r_{i,j}$，则

$$r_{i,j}=d'_{i,j}\bmod b_{i,j} \tag{15}$$

同样，通过计算 $\left\lfloor\dfrac{d'_{i,j}-r_{i,j}}{b_{i,j}}\right\rfloor$ 的比值，依据式(13)，可获取初始差值 $d_{i,j}$. 然后将基数为 $b_{i,j}$ 的水印信息 $r_{i,j}$ 转换成十进制值，输出加密水印数据 s_k；

4) 依据参数 N，以及 Fibonacci、Lucas 序列的种子，对加密水印数据 s_k 完成解密，复原水印信息 S_k.

4　仿真结果及分析

为了测试所提算法的水印性能，利用 Matlab 工具来验证，并将文献[5]与文献[6]作为对照组. 其中，文献[5]是利用了 Zernike 矩和 Contourlet 变换来将水印信息嵌入到 Contourlet 子带中，具有较强的抗几何攻击能力，利用 Zernike 矩来提高水印图像的抗旋转攻击能力，是当前图像水印方案中较为常用的手段，在水印领域被广泛使用. 文献[6]则是综合了 DWT、DCT 与奇异值分解来实现水印信息隐藏，这 3 种最常见的方法，在数字图像水印以及图像信息安全领域被广泛使用，尤其是 DCT、奇异值分解，能够有效改善水印图像的抗几何攻击能力，被诸多国内外学者借鉴与使用. 因此，文献[5]、文献[6]具有较好的代表性. 测试条件为：DELL，3.5 GHz，双核 CPU，500 GB 硬盘与 4G 内存. 从 USC-SIPI 图像集[15]中选择 3 幅图像作为载体图像，如图 4(a)－4(c)所示，其尺寸均为 256×256；同时，把图 4(d)－4(f)视为水印数据. 其中，Fibonacci、Lucas 序列的种子均为(1，1). 同时通过大量实验测试，确定参数 Δ 与阈值 t 的最优值分别为 12，8. 水印性能的评估指标为：① 不可感知性；② 鲁棒性.

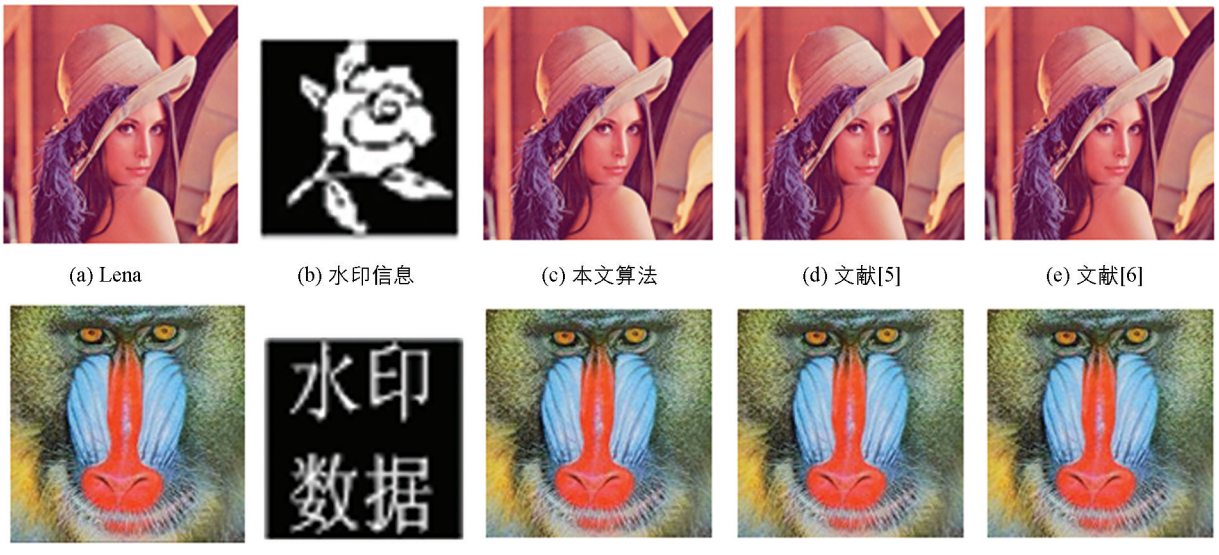
4.1　不可感知性能测试分析

根据所提技术、文献[5]与文献[6]的水印信息嵌入过程，将图 4(d)－4(f)隐藏到载体图像中，获取的水印图像见图 5.

(a) Lena (b) Mandrill (c) Sea

(d) Tortoise (e) Characters (f) words

图 4 实验载体图像与待嵌入的水印数据



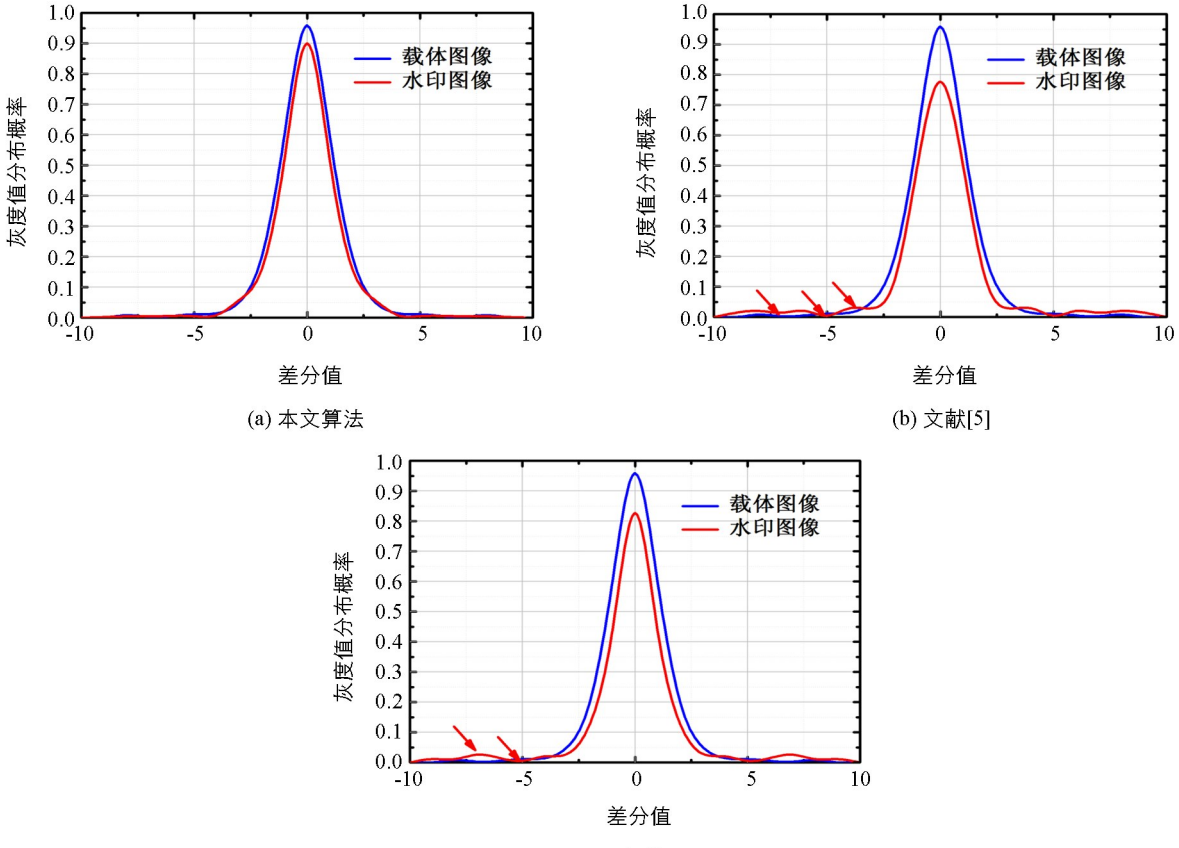
(a) Lena (b) 水印信息 (c) 本文算法 (d) 文献[5] (e) 文献[6]

(a1) Lena (b1) 水印信息 (c1) 本文算法 (d1) 文献[5] (e1) 文献[6]

(a2) Lena (b2) 水印信息 (c2) 本文算法 (d2) 文献[5] (e2) 文献[6]

图 5 不同算法的输出水印图像

由水印嵌入结果可知，其输出的水印图像的隐秘性较好，充分将水印数据隐藏在载体图像中，无任何视觉信息泄露. 由于主观评估无法体现 3 种技术的不可感知性能的差异，因此，本文利用差分图[16]来量化，通过测试，得到了水印图像与载体图像之间的差分图. 以图 5(c)—图 5(e)为实验对象，嵌入率为 0.6 bpp，3 种算法的输出差分图如图 6 所示. 由实验数据可知，本文算法输出的水印图像的不可感知性最高，其差分图与初始载体图像非常接近，不存在阶梯效应，见图 6(a)，而文献[5]与文献[6]所获取的水印图像的隐秘性不佳，二者的差分图均有不同程度的阶梯效应，如图 6(b)、6(c)中的箭头所示，其中文献[5]的水印技术阶梯效应较为严重. 因为本文算法利用每个像素的 3 个相邻像素来定义容量评估机制，根据每个像素的特性，评估其水印数据嵌入容量，对于平滑区域的像素，嵌入较多的水印信息，其他区域，则赋予每个像素较少的水印容量，有效防止了水印信息的丢失，并引入像素预测机制来获取每个像素的误差值，再利用误差扩展技术，将水印数据嵌入到误差值最小的载体像素中，同时，设计了动态加密技术，对水印图像进行了混淆处理，充分扰乱了水印信息，显著提高其不可感知性. 而文献[5]、文献[6]两种技术则通过相应的水印嵌入技术，将水印信息直接嵌入到载体图像中，没有对水印数据进行安全处理，从而使得二者的不可感知性要低于本文所提技术.



(a) 本文算法　(b) 文献[5]

(c) 文献[6]

图 6　不同算法输出的水印图像的差分图

4.2　鲁棒性、水印容量与抗失真性能测试

鲁棒性与抗失真性[17]是评估水印算法的 2 个重要指标，为此，本文将图 5(c1)—图 5(e1)为目标，对其施加表 1 中的几何攻击手段. 通过这 3 种算法对应的水印信息提取机制来复原初始水印数据，并引入峰值信噪比 PSNR 与相关系数 NC[2]来量化算法的失真度，测试结果见表 2. 由表可知，当水印图像遭遇外来攻击时，利用 3 种技术的水印提取方法来复原，导致所提取的水印信息与初始水印存在不同程度

的差异，但是，本文水印技术的失真度最低，其鲁棒性最佳，其复原水印信息与初始水印的相似度非常高，其对应的PSNR、NC值均为最高. 而文献[5]、文献[6]算法的失真度较大，在水印图像受到表1的攻击后，导致其复原的水印信息质量不佳，其PSNR、NC值均要低于所提技术. 原因是本文水印算法联合Lucas序列与Fibonacci序列，设计动态混淆方法，对水印信息进行了安全加密，使其像素在空间内均匀分布，不仅改善了隐秘性，同时大幅度提高了抗攻击能力，而且定义了容量评估机制，对每个像素的水印容量进行了预测，将较多的水印信息嵌入到平滑区域的像素，并利用像素预测机制来获取每个像素的误差值，通过误差扩展技术处理预测误差值，有效降低失真度. 而文献[5]则是将水印信息集中在低频区域，没有考虑每个像素之间的差异，都是将相同容量的水印数据嵌入到每个像素中，易出现像素溢出，导致信息丢失，且其水印图像的安全性较低，在网络遭遇攻击时，易因其水印信息的损坏与丢失，从而使其鲁棒性不佳. 文献[6]则是依靠载体图像的角点来实现水印数据的嵌入，在图像受到几何变换攻击时，易导致其特征不稳定，缺乏像素容量评估机制，不能根据像素自身特性来实现水印数据容量的自适应嵌入，使其抗失真与鲁棒性不理想.

表1 几何攻击类型及其参数值

名称	角度旋转	尺度变换	椒盐噪声	JPRG压缩
参数值	40°	0.5	0.05	35

表2 3种算法的鲁棒性测试结果

名称	实验结果	椒盐噪声	JPRG压缩	旋转	缩放
本文算法	PNSR/dB	42.05	39.67	38.83	39.14
	NC	0.992	0.983	0.943	0.961
	复原水印				
文献[5]	PNSR(dB)	41.18	40.63	36.72	39.06
	NC	0.969	0.957	0.872	0.915
	复原水印				
文献[6]	PNSR(dB)	41.37	40.94	39.58	40.16
	NC	0.976	0.964	0.922	0.948
	复原水印				

为了进一步量化这3种算法所提取的水印信息的失真度，本文以图5(a)、图5(a1)、图5(a2)为例，测试在不同嵌入率下提取水印信息的峰值信噪比PSNR曲线，结果见图7.

依图可知，随着嵌入率的增大，这3种算法提取水印信息的PSNR值都在下降，但是本文所提算法的PSNR值是最高的，且所提水印技术能够在图像的平滑区域中使得每个像素的嵌入容量超过1位；而文献[5]、文献[6]两种技术的PSNR值均要低于所提技术，且二者只能将1位的水印容量嵌入到每个像素中，无法根据像素复杂度来调整其水印容量的合理分配. 这些测试数据显示所提水印技术具有更大的水印容量与鲁棒性，能够有效抗击几何变换攻击，显著降低失真度.

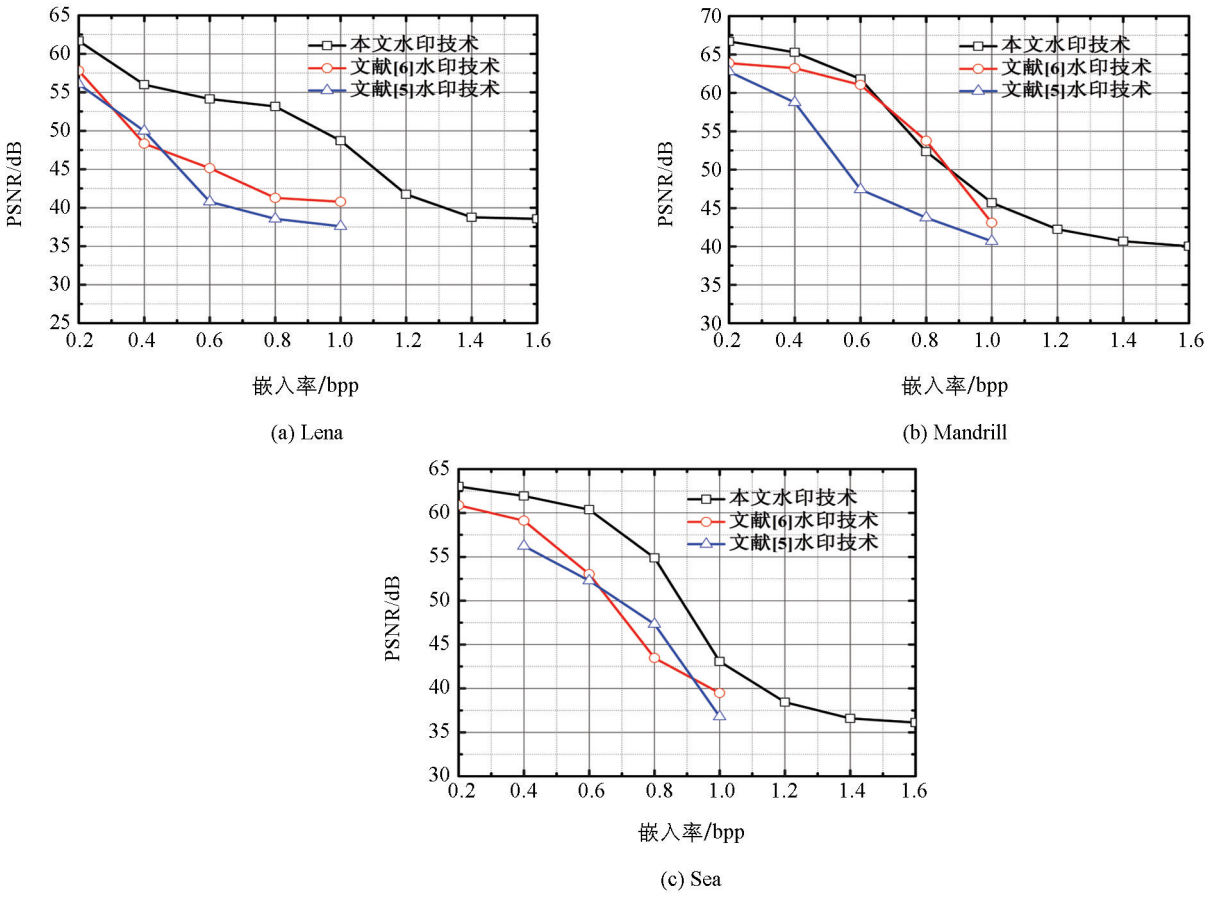


图 7　不同水印算法的 PSNR 测试结果

为了提高水印算法的容量与抗失真性能，本文提出了基于误差扩展与像素容量评估的无损图像水印算法. 通过利用每个像素自身相邻的像素值来定义像素容量评估方法，以自适应调整其相应的水印数据嵌入容量，避免破坏水印图像的敏感区域；通过引入像素预测机制，将近零预测误差值的像素作为水印数据的嵌入载体，有效降低水印信息的失真度. 同时，为了增强水印信息的不可感知性与抗攻击能力，本文联合 Lucas 序列与 Fibonacci 序列，设计动态混淆方法，对水印信息完成加密，充分混淆水印信息. 实验测试结果验证了所提水印技术的合理性与优异性.

参考文献：

[1] 陈　敏，关英子. 基于超混沌数学理论的图像加密方法研究 [J]. 西南师范大学学报(自然科学版)，2017，42(7)：63－67.

[2] 郑洪英，彭钟贤，肖　迪. 加密医学图像中的视觉无损信息隐藏算法 [J]. 西南大学学报(自然科学版)，2014，36(12)：157－161.

[3] 赵春玉，时宏伟，胡可鑫，等. 基于 DCT 变换的彩色图像水印盲提取算法 [J]. 计算机工程与设计，2015，33(3)：597－602.

[4] ZONG T R，XIANG Y，IYNKARAN N，et al. Robust Histogram Shape-Based Method for Image Watermarking [J]. IEEE Transactions on Circuits & Systems for Visual，2015，25(5)：717－729.

[5] 朱丹丹，吕鲤志. 基于伪 Zernike 矩和 Contourlet 变换的抗几何攻击图像水印算法 [J]. 计算机科学，2016，43(6)：131－134.

[6] FAZLI S，MOEINI M. A Robust Color Image Watermarking Method Based on DWT，DCT，and SVD Using a New Technique for Correction of Main Geometric Attacks [J]. Optik-International Journal for Light and Electron Optics，2016，127(2)：964－972.

[7] WANG X Y，LIU Y N，LI S，et al. Robust Image Watermarking Approach Using Polar Harmonic Transforms Based Geometric Correction [J]. Neurocomputing，2015，174(25)：627－642.

[8] 张志彤，赵 耀，倪蓉蓉，等. 奇偶性分类下大容量医学图像可逆水印算法[J]. 数据采集与处理，2013，28(5)：626－632.
[9] VURAL C，BARAKLI B. Adaptive Reversible Video Watermarking Based on Motion-Compensated Prediction Error Expansion With Pixel Selection[J]. Signal，Image and Video Processing，2016，10(7)：1225－1232.
[10] CODARA P，D'ANTONA O M. Generalized Fibonacci and Lucas Cubes Arising from Powers of Paths and Cycles[J]. Discrete Mathematics，2014，339(3)：241－251.
[11] 程荣军. Lucas序列及其应用研究[D]. 合肥：安徽师范大学，2014：27－29.
[12] GU G，LING J. A Fast Image Encryption Method by Using Chaotic 3D Cat Maps[J]. Optik-International Journal for Light and Electronic，2014，125(17)：4700－4705.
[13] 袁其平，林海杰，陈志宏，等. 用支持向量回归法实现单帧图像超分辨率重建[J]. 光学精密工程，2016，24(9)：2302－2309.
[14] HONG W，CHEN T S，LUO C W. Data Embedding Using Pixel Value Differencing and Diamond Encoding with Multiple-Base Notational System[J]. Journal of Systems & Software，2012，85(5)：1166－1175.
[15] BIRAJDAR G K，MANKAR V H. Blind Method for Rescaling Detection and Rescale Factor Estimation in Digital Images Using Periodic Properties of Interpolation[J]. AEU：International Journal of Electronics and Communications，2014，68(7)：644－652.
[16] 陈 琳，王建鹏. 最优像素调整耦合基因算法的高容量图像隐写研究[J]. 计算机应用研究，2015，32(8)：2429－2432.
[17] HSU P H，CHEN C C. A Robust Digital Watermarking Algorithm for Copyright Protection of Aerial Photogrammetric Images[J]. Photogrammetric Record，2016，31(153)：51－70.

An Image Watermarking Algorithm Based on Error Propagation and Pixel Capacity Evaluation

LI Hong-ri[1,2]， FANG Kui[2]

1. *College of Information Engineering，Hunan Mechanical & Electrical Polytechnic，Changsha 410151，China*；
2. *College of Information Science and Technology，Hunan Agricultural University，Changsha 410128，China*

Abstract：In order to solve the defects of the current image watermarking algorithm，such as large distortion of restoration watermark information and small watermark capacity induced by not accurately predicting the error value between neighboring pixels，as well as not adaptively determining its embedding capacity according to the local texture characteristics of pixels，a lossless image watermarking algorithm based on error propagation and pixel capacity evaluation is proposed in this paper. Firstly，a dynamic confusion method is designed to encrypt the watermark information. Next，three adjacent pixels are considered and an edge pixel prediction mechanism is defined to accurately predict each pixel value of the carrier image and to obtain the corresponding error value. Then，a pixel capacity evaluation method is designed according to the variance of any three adjacent pixels in the carrier image to evaluate the watermark embedding capacity of each pixel. The error extension technique is introduced to design the watermark information embedding mechanism for implanting the watermark data with different capacity into different pixels of the carrier image based on the evaluation results of the pixel capacity. Finally，a watermark extraction method is established to recover the watermark information. The results of an experiment show that the proposed algorithm has higher quality of watermarking and watermarking capacity compared with the current image watermarking technology.

Key words：image watermarking；error propagation；pixel prediction；pixel capacity evaluation；watermark embedding；dynamic encryption；watermark extraction

责任编辑 崔玉洁