一种基于混沌阵列的鲁棒零水印算法*)

高山青　罗向阳　刘　镔　刘粉林
(解放军信息工程大学 信息工程学院　郑州 450002)

摘　要　本文提出了一种基于混沌阵列的鲁棒零水印算法。它首先构造一个混沌阵列，然后利用该混沌阵列来在图像中寻找"嵌入[1]"位置，得到该位置的像素值的最高有效位，再通过和水印信息的比较结果来在混沌阵列中设置标志，构造出最终的水印阵列。实验表明，该水印方案具有良好的鲁棒性，能够抵抗剪切、加扰、旋转、滤波、缩放、JPEG 压缩等常见的有意和无意攻击。

关键词　混沌阵列，零水印，鲁棒性，最高有效位

A Robust Zero-Watermarking Algorithm Based on Chaotic Array

GAO Shan-Qing　LUO Xiang-Yang　LIU Bin　LIU Fen-Lin
(Information Engineering Institute, The PLA Information Engineering University, Zhengzhou 450002)

Abstract　This paper presents a robust zero-watermarking algorithm based on chaotic array. It constructs a chaotic array, then uses the chaotic array to find out the "embedded" position. After getting the position, it compares the MSB (most significant bit) of the image with the watermark information. It gets the last watermark array by setting the values of the chaotic array based on the results of the comparison. The results of experiment show that the scheme has good performance in common intentional or unintentional attacks such as cropping, additive noise, multiplible noise, rotating, filtering, scaling, and JPEG compression.

Keywords　Chaotic array, Zero-watermark, Robustness, MSB

1　引言

随着数字信号处理技术和计算机互联网络的迅速发展，人类进入了以数字信息为特征的信息社会，数字多媒体产品越来越盛行。但是由于数字产品易于复制和修改的原因，盗版问题也越来越严重，对数字产品的版权进行很好的保护以保证作品作者、所有者以及合法用户的权利，成为人们越来越关注的热点问题。数字水印技术就是为解决这个问题而在近年迅速发展起来的。数字水印是用来进行数字产品版权保护的技术。它可以用来标识作者、所有者、发行者、使用者，并携带有版权保护和认证信息，目的是鉴别出非法的复制和盗用，保护数字产品的合法拷贝和传播[1]。

目前已经提出了许多数字水印方法，针对图像来说，大致可分为两类：频域水印算法和空域水印算法。这两类算法都是通过对图像的空域信息或频域信息作了一定的修改来嵌入水印信息。为了避免被觉察到修改，很多水印算法考虑到了HVS(人类视觉系统)的特性，采用一些特殊技术来掩盖对数字产品的修改[2~5]。但是，不论采用多么精妙的算法，总是要改变原始图像的一定信息，因此就存在被检测到并被有效攻击的可能性。针对这种情况，人们提出了零水印的概念。文[6~8]中讨论了零水印的概念和一些应用。零水印算法，即不修改原图像来构造水印，利用被保护图像的重要特征来构造水印信息，很好地避开了不可感知性与鲁棒性之间的矛盾，进一步提高了水印的鲁棒性[8]。

由于混沌阵列既具有可控的低通特性又具有很好的相关特性，目前利用混沌的数字水印技术逐步成为研究的热点。文[9]提出了一种首先用混沌动态系统对水印信息进行预处理，而后将其扩频调制在图像的空间域，并且使水印嵌入强度自适应于图像的基于混沌的数字图象水印算法。文[5]提出了一种使用混沌阵列，基于 HVS 视觉掩盖自适应的公开图像水印算法。文[10]提出了采用混沌序列置乱水印，而后基于混沌序列在宿主图像 DCT 域的中频带随机选择少量参考点，并在其领域内用奇偶量化法批量嵌入乱序水印比特的水印算法。受上述文献的启发，本文提出了一种基于混沌阵列的鲁棒零水印算法，并编程实现仿真，经过大量的剪切、加扰、失真、滤波、缩放、JPEG 压缩等实验证实，本算法具有较强的鲁棒性，可以抵抗常见的有意和无意攻击。

2　水印嵌入和提取算法

2.1　混沌阵列的产生

混沌序列的主要优点：(1)通过改变混沌系统参数及初始值可以得到数量巨大的序列，并且序列长度是任意的；(2)混沌序列没有周期，类似于一个随机过程，因此具有很好的保密性；(3)混沌序列的产生和复制很方便，只要给出一个混沌迭代公式和一个初值，就能产生一个混沌序列[5]。

因为混沌序列具有上述优点，文[5]中采用 Tent-Map 映

*)基金项目：国家自然科学基金(60374004)；河南省杰出青年基金(0412000200)；河南省高校杰出科研人才创新工程(2001KYCX008)。高山青　硕士研究生，研究方向为信息安全与数字水印；罗向阳　硕士，助教，主要研究方向为信息隐藏；刘　镔　硕士研究生，研究方向为混沌加密与信息隐藏；刘粉林　教授，博导，主要研究方向为控制理论，信息安全。

[1] 零水印算法不需要对载体对象进行修改，为了描述算法的方便，本文延用"嵌入"这个术语。

射来产生两个混沌序列 $w_p(i)$ 和 $w_q(j)$，再利用公式 $w_{p,q}(i,j)=w'_p(i)\times w_q(j)$，采用向量相乘的方法来产生混沌阵列。但是，采用该方法产生的混沌阵列降低了混沌阵列的随机性。因为两个混沌序列向量相乘时，如果列向量中第 i 个值为 0，阵列中对应的第 i 行就全为 0，而每一个列向量中为 1 的位置，阵列中相应的行就是行向量。即列向量中有多少个 1，阵列中就有多少行相同的行向量，而其它行全为 0。

由于上述问题和我们算法的需求，本文采用直接产生 $m\times n$ 的混沌序列来构成混沌阵列的方法，该方法充分利用混沌的随机性。考虑到混沌系统在计算机上实现时会产生动力学退化的问题[11,12]，文[13]中提出了一种采用加扰和扩散的方法的混沌系统来改善混沌系统的动力学退化问题，能得到随机性良好、周期足以满足实际需要的伪随机序列，所以本文中采用该混沌系统来产生混沌阵列[见附录 A]。

产生混沌阵列的具体方法为(设要产生 $m\times n$ 的混沌阵列)：

(1)根据附录 A，用户选定密钥 $K=(e,a,x_0)$。

(2)设定迭代次数为 $m\times n$ 次。

(3)使用附录 A 中式(A2)进行迭代 $m\times n$ 次，得到混沌轨迹。

(4)给混沌轨迹设置阈值 $T_c=0.5$，将得到的轨迹二值化，得到长为 $m\times n$ 的 0、1 混沌序列。即如果 $f(x)<T_c$，置为 0；如果 $f(x)\geqslant T_c$，置为 1，二值化为 0、1 序列。

(5)将(4)中得到的序列按每段 n 个数分成 m 段，按顺序把这 m 段数排列成 $m\times n$ 的混沌阵列。

2.2 水印的嵌入过程

以灰度图像为例，设我们要在图像 I 中用密钥 K 嵌入水印 M，其中 $K=(e,a,x_0)$。

(1) 用户选定密钥 $K=(e,a,x_0)$，利用 2.1 节中的方法产生一个大小为 $m\times n$ 的混沌阵列。

(2) 用户选定要嵌入的水印信号 M，将其转化为 0、1 序列，放到一维数组 W 中，数组的长度为水印序列的长度，设长度为 l。

(3) 记 $V(i,j)$为混沌阵列中第 i 行、第 j 列的值，值为 0 或 1；记 $J(i,j)$为图像中第 i 行、第 j 列点的像素值的最高位，值为 0 或 1；记 $W[k]$为第 k 个水印信息值，值为 0 或 1。

①置 $i=1,j=1,k=1$。

②从头扫描混沌阵列，寻找阵列中 $V(i,j)=1$ 的位置，找到后转③。

③判断：如果 $J(i,j)=W[k]$，置 $V(i,j)=2,k\leftarrow k+1$，转④；如果 $J(i,j)\neq W[k]$，转④。

④判断 k 是否大于 l，如果大于，水印信息已全部嵌入到图像中，嵌入结束，转(4)；否则在混沌阵列中寻找下一个 $V(i,j)=1$ 的位置，找到后转③。

(4) 第(3)步做完后的混沌阵列即为最终水印阵列。

注：算法中假设只使用最高位就可嵌完水印信息，实验表明通常也是这样，故我们只描述了这种情况。如果水印信息很大，只使用图像的最高位嵌入不完水印信息，可以用同样的方法，把还未嵌入的水印信息嵌入到混沌阵列中还没有修改过的图像相应位置的次高位，只需要嵌入后置 $v(i,j)=3$。提取时，先提取 $v(i,j)=2$ 的图像相应位置像素值的最高位信息，再提取 $v(i,j)=3$ 的相应位置像素值的次高位信息。同理，可设置不同的标记把水印嵌入到其它位。

下面以一个模拟的小例子来说明嵌入的过程。

设要在一幅 8×8 的图像中嵌入 01010011 的水印信息。为了说明的方便，我们把图像像素的最高位提取出来构成的 8×8 阵列，如图 2.1 所示；混沌生成的 8×8 阵列如图 2.2 所示。水印信息放入一维数组 $W[k]$中，本例中 $l=8$，得到 $W=\{0,1,0,1,0,0,1,1\}$。

$$\begin{pmatrix}0&0&0&0&0&1&1&0\\1&1&0&0&1&0&0&0\\1&0&0&0&1&0&0&1\\0&1&1&0&1&0&1&1\\1&0&1&1&1&0&0&0\\1&1&0&0&1&1&0&0\\1&0&0&1&1&0&0&0\\0&1&0&1&0&1&1&0\end{pmatrix}$$

图 2.1 图像像素最高位阵列

$$\begin{pmatrix}1&0&1&1&0&1&0&0\\1&0&1&0&0&1&0&1\\0&1&1&1&0&1&0&1\\0&0&1&0&1&0&1&1\\1&1&1&0&1&0&0&0\\1&1&0&0&1&0&1&0\\1&1&1&0&1&0&0&1\\0&0&0&1&1&0&0&0\end{pmatrix}$$

图 2.2 采用混沌生成的混沌阵列

$$\begin{pmatrix}2&0&1&1&0&2&0&0\\1&0&2&0&0&1&0&1\\0&1&1&1&0&1&0&2\\0&0&1&0&1&0&1&1\\1&2&1&0&1&0&0&0\\1&1&0&0&1&0&2&0\\2&1&1&0&2&0&0&1\\0&0&0&1&1&0&0&0\end{pmatrix}$$

图 2.3 水印嵌入后的最终水印阵列

下面开始嵌入：

开始时，$k=1$，待嵌入的水印信息为 $W[1]$。从头开始扫描混沌阵列(如图 2.2)，寻找混沌阵列中 $V(i,j)=1$ 的位置。本例中，因为阵列图 2.2 中 $V(1,1)=1$，因此判断 $J(1,1)$是否等于 $W[1]$。由图 1 可见，$J(1,1)=0$，而 $W[1]=0$，$J(1,1)=W[1]$，所以置 $V(1,1)=2$，已嵌入了 1 比特水印信息，$k\leftarrow k+1$。待嵌入的水印信息为 $W[2]=1$，在混沌阵列中找下一个 $V(i,j)=1$ 的位置。找到的下一个位置为(1,3)，因为 $J(1,3)=0$，而 $W[2]=1$，二者不等，所以直接寻找下一个位置，得到(1,4)。同理，$J(1,4)=0$，不等于 $W[2]$，直接找下一位置，得到(1,6)。$V(1,6)=1$，等于 $W[2]$，故置 $V(1,6)=2$，又嵌入了 1 比特水印信息，$k\leftarrow k+1$。待嵌入的水印信息为 $W[3]=0$，寻找下一个 $V(i,j)=1$ 位置。以此类推，直到所有的水印信息都嵌入完为止。嵌入后的最终阵列如图 2.3 所示。

在用 512×512 灰度图像嵌入 64×64 单色水印图像仿真实验时发现：只在最高位嵌入信息时，只需要扫描到图像的第 79228 个像素就能嵌完 64×64=4096 位的水印图像，扫描像素的比例为 79228/(512×512)=30.24%。这说明该算法的嵌入容量很大。如果考虑到还能通过在混沌阵列中设定不同的标记以嵌入到其它位，特别是对彩色图像，可以嵌入到不同的颜色分量中，甚至还可以将水印嵌入到混沌阵列中 0 对应的位置，水印的容量还将大大扩大。当然，由于每个像素最多只能嵌入一位信息，因此理论上本算法的嵌入容量上限是嵌入和载体图像像素数相同 bit 的水印信息。

在仿真实验中，只嵌入 64×64=4096 的水印信息，4096/(512×512)=0.015615，嵌入比太小，为了保证得到较好的鲁棒性，本文引入了一个扩散因子 α，在混沌阵列中每隔 α 个 1 才检测一次的方法进行扩散，将水印比较均匀地嵌入到整个图像中，提高了抗攻击的能力，得到了较好的效果。

设图像像素数为 u，水印信息为 vbit。通过实验，本文给

出一个获得扩散因子 α 的经验公式：

$$\alpha'=[(v/u)\times 8\times 100] \quad (1)$$

设水印嵌入的最后一个位置是(c,d)，图像大小为 $m\times n$，定义一个均匀系数 γ：

$$\gamma=(c\times n+d)/(m+n) \quad (2)$$

用(1)式得到 α'，在实际嵌入时，首先用 α' 作为扩散因子嵌入水印，然后用式(2)计算 γ，判断 γ 是否$\geqslant 0.9$，若是，令 $\alpha=\alpha'$，否则 $\alpha'\leftarrow\alpha'+1$，重复上述过程，直到 $\gamma\geqslant 0.9$，令 $\alpha=\alpha'$。α 为最终的扩散因子。扩散因子也可作为用户密钥的一个分量。

产生后的零水印需在 IPR(Intellectual Property Rights，知识产权)信息数据库注册，它负责维护一个水印数据库来验证数字产品的所有权。零水印一旦注册后，就可以认为原图像已在水印技术的保护下[6]。本算法的水印信息是嵌入后的最终阵列 Z，需要将该信息进行注册。为了降低 IPR 信息数据库的存储开销，也可以用摘要算法如 MD5、SHA 等安全摘要算法[14]先对 Z 进行摘要，只注册摘要信息。由于摘要算法的单向性和安全性，只注册最终水印阵列 Z 的摘要并不会降低该水印算法的性能。

2.3 水印提取

当可能是在该零水印保护下的图像 I' 产生版权纠纷时，图像的合法拥有者 A 可以利用水印的嵌入方法再重新生成最终水印阵列 Z 或是直接从 IPR 中心得到 Z，由于该矩阵在 IPR 中心注册过，因此如果用该矩阵可以从 I' 中提取出我们的原始水印信息，则说明的版权确是归 A 所有。需要注意一下的是，假设 A、B 两人都声称对图像拥有版权，并且都能从有纠纷的图像 I' 中提取出各自的水印，A 采用零水印算法，并在 IPR 中心注册过。但是，如果 A 所注册的图像中已含有了 B 采用合法、可信的算法嵌入的水印，并且确实可以从被 A 注册的图像中提取出来，那么说明该图片的版权所有者为 B 而不是 A，A 是用别人的图像去进行了非法注册，不应予以承认；如果 B 不能从被注册的图像中提取出他所声称的水印，即 A 注册的图像中并没有含有 B 的水印信息，那么说明该图片的版权拥有者为 A。

假设我们只在最高位嵌入了水印信息，嵌入的水印信息是 64×64 的单色二值图像，提取水印的算法为：

从头顺序扫描最终嵌入阵列 Z，将水印阵列中值为 2 的图像的对应位置像素值的最高位提取出来，得到和原始水印信息相同大小的 0、1 串，将它们重新组合成 64×64 的水印图像，通过对该水印图像和原始水印图像比较，就可以确定该图像是否含有注册过的水印信息，进而解决版权纠纷。

还用图 2.1 中的例子来说明水印的提取过程。

从头扫描图 2.3 中的阵列，得到值为 2 位置，再从图像中相应位置提取出像素的最高位。本例中，即从图 2.1 中所示的图像像素值的最高位阵列中提取出 $J(1,1)$，$J(1,6)$，$J(3,8)$，$J(5,2)$，$J(6,7)$，$J(7,1)$，$J(7,5)$的值，得到水印信息 01010011。

由于我们的水印是嵌入到最高位，嵌入位置是由具有良好特性的混沌阵列确定的，并采用了扩散技术进行扩散，位置比较随机和均匀，因此该方案具有较强的鲁棒性，能够抵抗信号失真、图像加扰、图像扭曲、剪切等有意和无意的攻击。这些我们在仿真实验中得到了证实。又由于是零水印，我们没有对原图作任何修改，并且采用了混沌，因此非授权者难以检测到水印的存在，更难以去除或修改，具有较高的安全性。

3 仿真实验

我们在 Visual C++6.0 环境下编程实现了本文提出的算法，并对标准的 512×512 Lena 灰度图像进行嵌入 64×64 单色二值水印图像的嵌入、检测和模拟攻击实验。取混沌密钥 K=(0.001，0.25，0.25)，扩散因子 $\alpha=12$。注：本节所有的 512×512 Lena 图像都缩小为 4cm×4cm 大小，而 64×64 水印图像都保持原大小。图 3.1 是原始的 512×512 Lena 灰度图像和 64×64 单色水印图像，图 3.2 是采用本文的算法生成最终水印阵列 Z，再用 Z 从 Lena 图像中提取出来的水印图像。

图 3.1 原始的 512×512 Lena 灰度图像和 64×64 单色水印图像

图 3.2 利用嵌入水印生成的最终阵列 Z 从 Lena 图像中提取的水印图像

3.1 剪切实验

我们对图像进行了大量在不同位置的剪切模拟攻击，结果证实本算法对剪切攻击具有较强的鲁棒性。如图 3、图 4 为 1/4 剪切，1/2 剪切模拟攻击实验结果。由于水印信息是比较均匀地嵌入到整个图像中，因此可以在 1/4 剪切和 1/2 剪切的情况下提取出较清晰的水印图像。

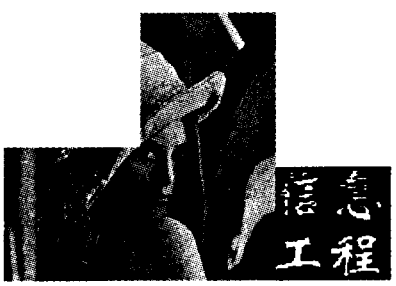

图 3.3 剪切 1/4 后的 Lena 图像及从中提取的水印图像

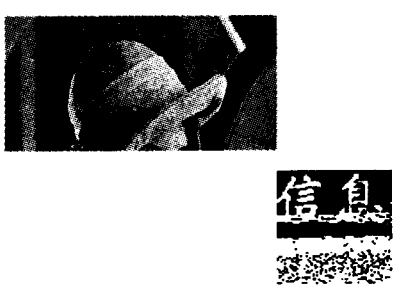

图 3.4 剪切 1/2 后的 Lena 图像及从中提取水印图像

3.2 加扰实验

我们对图像的最低位添加不同比例的随机噪声，再从中

提取出水印图像来检验我们的算法对噪声干扰的鲁棒性。因为本算法的水印信息只和最高位有关，所以在低位添加随机噪声不会影响提取出来的水印图像。实验证实了该推断，说明本算法对噪声干扰具有良好的鲁棒性。图 3.5、图 3.6 为在图像的最低位添加不同比例的随机噪声后的 Lena 图像及从加扰图像中提取出来的水印图像。

图 3.5　添加 5%随机噪声后的 Lena 图像及从中提取的水印图像

图 3.6　添加 100%随机噪声后的 Lena 图像及从中提取的水印图像

3.3　旋转实验

对于小角度肉眼不易觉察的旋转攻击，由于图像一般来说都是比较平滑的，相邻像素值之间是有一定联系的，仅仅旋转一个很小的角度，本文的算法不需要几何校正就能从中提取出较清晰的水印图像，如图 3.7、图 3.8 分别是旋转 0.5 度、1.5 度的 Lena 图像及没有进行几何校正直接提取的水印图像。从提取的图像中能够明显地看出原始水印图像的信息。

图 3.7　旋转 0.5 度后的 Lena 图像及从中提取的水印图像

对大角度的旋转，不可能直接提取出水印信息，图 3.8 显示出当旋转 1.5 度时水印信息已经很模糊了，如果角度再大一点的话直接提取出来的就是无意义的信息。但是考虑到大角度的旋转时可以容易地觉察到，可以对其进行相反角度的旋转来校正，再进行提取。如果是旋转 90、180、270，图像不会失真，我们通过相反角度的旋转就可得到和原图一样的图像；对于任意角度的旋转，图像有一定失真，提取出的水印信息将会有失真，但是仍可以清晰地辨认原始的水印信息。如图 3.9、图 3.10 为分别旋转 300 度和 270 度后进行相反角度旋转后的 Lena 图像及从中提取出的水印图像。

图 3.8　旋转 1.5 度的水印图像及从中提取的水印图像

图 3.9　旋转 300 度后再进行相反角度旋转的 Lena 图像及从中提取的水印图像

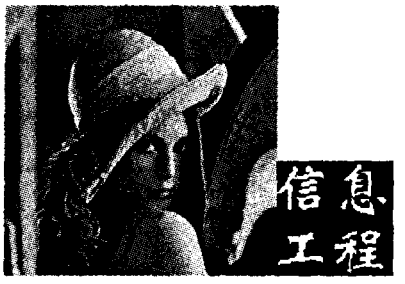

图 3.10　旋转 270 度后再进行相反角度旋转的 Lena 图像及从中提取的水印图像

3.4　滤波实验

取卷积强度为 3，用常用的 HP1、HP2、HP3 三个高通滤波器来对 Lena 图像进行高通滤波锐化处理，用常用的 LP1、LP2、LP3 三个低通滤波器来对 Lena 图像进行低通滤波平滑处理，并对图像进行中值滤波和粒化处理，再分别从滤波处理后的图像中提取出水印信号，来检验该算法对滤波处理的鲁棒性。实验证实，本文提出的算法对滤波处理具有很好的鲁棒性。常用的高通和低通滤波器如下：

$$\begin{pmatrix} 1 & -1 & -1 \\ -1 & 9 & -1 \\ -1 & -1 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -2 \\ 1 & -2 & 1 \end{pmatrix}$$

HP1　　HP2　　HP3

$$\begin{pmatrix} 1/9 & 1/9 & 1/9 \\ 1/9 & 1/9 & 1/9 \\ 1/9 & 1/9 & 1/9 \end{pmatrix} \quad \begin{pmatrix} 1/10 & 1/10 & 1/10 \\ 1/10 & 1/5 & 1/10 \\ 1/10 & 1/10 & 1/10 \end{pmatrix} \quad \begin{pmatrix} 1/16 & 1/8 & 1/16 \\ 1/8 & 1/4 & 1/8 \\ 1/16 & 1/8 & 1/16 \end{pmatrix}$$

LP1　　LP2　　LP3

实验结果如图 3.11、图 3.12、图 3.13、图 3.14、图 3.15、图 3.16、图 3.17 和图 3.18 所示。

图 3.11　用 HP1，卷积强度为 3 滤波处理后的 Lena 图像及提取的水印信息

图 3.12　用 HP2，卷积强度为 3 滤波处理后的 Lena 图像及提取的水印信息

图 3.13　用 HP3，卷积强度为 3 滤波处理后的 Lena 图像及提取的水印信息

图 3.14　用 LP1，卷积强度为 3 滤波处理后的 Lena 图像及提取的水印信息

图 3.15　用 LP2，卷积强度为 3 滤波处理后的 Lena 图像及提取的水印信息

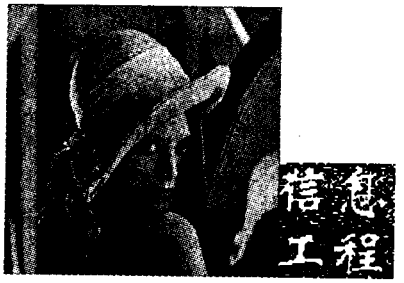

图 3.16　用 LP3，卷积强度为 3 滤波处理后的 Lena 图像及提取的水印信息

图 3.17　中值滤波后的 Lena 图像及提取的水印图像

图 3.18　粒化处理后的 Lena 图像及提取的水印图像

图 3.19　挤压到 90%再拉伸到 100%的 Lena 图像及从中提取的水印图像

图 3.20　挤压到 10%再拉伸到 100%的 Lena 图像及从中提取的水印图像

3.5　图像缩放实验

在本实验中，先对图像进行挤压再拉伸到原图大小，然后再从图像中提取出水印图像。结果发现，尽管图像有很大的失真，仍然可以从中提取出清晰的水印图像，甚至在图像被挤压到10%再拉伸到100%图像有非常大的失真时，仍可以从中提取出明显的水印信息。

3.6 JEPG压缩实验

在JPEG压缩实验，采用流行的JPEG Imager 2.0对Lena图像进行了不同压缩比的JPEG压缩实验，该软件最高支持127∶1的压缩比。结果让人惊讶：我们发现本算法对JPEG压缩具有良好的鲁棒性，即便是压缩到127∶1，仍能获得较清晰的水印图像。实验结果如下：

图3.21 JPEG压缩到12∶1的Lena图像及从中提取的水印图像

图3.22 JPEG压缩到127∶1的Lena图像及从中提取的水印图像

结束语 本文提出了一种基于混沌阵列的鲁棒性零数字水印算法。该算法利用图像像素的最高位来构造水印信息，而最高位受到有意或无意攻击而改变的可能性较小，所以抗干扰、失真、缩放、JPEG等攻击的鲁棒性较强。考虑到图像相邻象素值之间存在一定的相关性，所以本文提出的算法对旋转攻击具有较好的鲁棒性。算法中还采用了扩散技术，将小信息量的水印信息较均匀地扩散到整个图像中，故对剪切攻击具有较好的鲁棒性。又由于混沌系统的初值敏感性，不同的密钥嵌入后的水印阵列信息完全不相关，而且是零水印算法，因此非授权用户难以检测到水印的存在，更难以去除，可以防止窜改和伪造，具有较好的安全性。以上结论在用$Vc^{++}6.0$编程进行仿真实验时得到了验证。

需要注意的是：因为该算法是零水印算法，零水印算法需要IPR信息数据库中心的支持，要求注册水印信息，所以只能用于保护少量有价值的数字图片[6]。但是，随着信息技术的飞速发展，IPR信息数据库的存储量会越来越大，可信度会越来越高，本算法以其较好的鲁棒性和安全性，希望在数字产品的版权保护中能发挥一定的作用。

附录A：

文[13]提出了一种选择性扩散扰动的数字混沌系统，其基本原理为：构造如下一个具有四个子区间$[0,a)$，$[a,0.5)$，$(0.5,1-a]$，$(1-a,1]$的一维分段线性混沌映射，其中$a\in[0\sim1]$，且$a\in[0,0.5]$：

$$g(x)=\begin{cases}\dfrac{1}{a}x & x\in[0,a)\\ (x-a)/(0.5-a) & x\in[a,0.5)\\ 0 & x=0.5\\ g(1-x) & x\in(0.5,1]\end{cases}\qquad(A1)$$

选择对$g(x)$定义区间的第3子区间$c_3=(0.5,1-a]$进行扩散，将片断c_3按照$e:1-e$的比例分成两段$c_{31}=(0.5,0.5+(1-a-0.5)\times e]$，$c_{32}=(0.5+(1-a-0.5)\times e,1-a]$，$e\in\square$，作为扩散系数，$e\in[0,1]$。按照选择性扩散的扰动算法形成新的分段线性混沌映射：

$$f(x)=\begin{cases}g(x) & x\notin c_3\\ g((2\times x-1)/e) & x\in c_{31}\\ g((a+x+e)/(1-e) & x\in c_{32}\end{cases}\qquad(A2)$$

迭代开始时要给定迭代初值x_0，$x_0\in(0\sim1)$且$x_0\in(0,1)$。

关于该混沌系统的更多性质的讨论请参阅文[13]。

参考文献

1 陈明奇，钮心忻，杨义先. 数字水印的研究进展和应用. 通信学报，2001，22(5)

2 Suhail M A, Obaidat M S. Digital Watermarking-Based DCT and JPEG Model. IEEE Transactions on Instrumentation and Measurement, 2003, 52(5): 1640～1647

3 Swanson M, Zhu B, Tewfik A. Transparent robust image watermarking. In: Proc. IEEE. Int. Conf. Image Processing, Lausanne, Switzerland, Sept. 1996. 211～214

4 Busch C, Funk W, Wolthusen S. Digital watermarking: From concepts to real-time video applications. IEEE Comput. Graphics Applicat, 1999, 19: 25～35

5 孙锬锋，温泉，王树勋. 基于人类视觉的混沌阵列在图像上的水印算法. 电子学报，2003，31(1)

6 温泉，孙锬锋，王树勋. 零水印的概念与应用. 电子学报，2003，31(2)

7 温泉，孙锬锋，王树勋. 基于零水印的数字水印技术研究. 见：全国第三届信息隐藏学术研讨会论文集(CIHW'2001). 西安：西安电子科技大学出版社，2001

8 张崇，于晓琳，刘建平，季称利. 结合零水印的小波包图像水印方案. 计算机工程与应用，2004，27

9 张春田，张 静. 基于混沌映射的鲁棒性图像水印算法. 电子学报，2002，30(1)

10 王宏霞，何 晨，丁 科. 基于混沌映射的鲁棒性公开水印. 软件学报，2004，15(8)

11 Li S, Mou X, Cai Y. Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography. Progress in Cryptology - INDOCRYPT 2001, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2001, 2247: 316～329

12 Li S, Mou X, Cai Y, Ji Z, Zhang J. On the security of a chaotic encryption scheme: Problems with computerized chaos in finite computingprecision. Computer Physics Communications, 2003, 153: 52～58

13 刘嵚，张永强，刘粉林. 一种新的数字化混沌扰动方案. 计算机科学，2005(4)

14 [美]Bruce Schneier 著，吴世忠，等译. 应用密码学. 北京：机械工业出版社，2001