第 58 卷 第 7 期 2009 年 7 月
1000-3290/2009/58(07)/4449-08

物 理 学 报
ACTA PHYSICA SINICA

Vol.58,No.7,July,2009

一种基于 Logistic 混沌系统和奇异值分解的零水印算法*

宋 伟† 侯建军 李赵红 黄 亮

(北京交通大学电子信息工程学院,北京 100044)

(2008 年 11 月 4 日收到;2008 年 11 月 24 日收到修改稿)

改变了传统通过修改图像内容进行版权保护的做法,描述了一种基于混沌理论和奇异值分解(singular value decomposing,SVD)的零水印方案.利用了 Logistic 混沌系统的初值敏感性映射信息隐藏的位置,增强了算法的安全性;采用了奇异值的不变特性构造注册中心的水印,保证了在不改变宿主图像任何信息的同时进行有效地版权保护;将有意义的二值图像作为水印图像,解决了零水印方案水印为无意义二值序列的问题;同时深入分析了水印容量和算法安全性之间的关系.通过对标准测试图像、卡通、医学、风景、遥感、诗画等图像进行实验测试以及和其他算法比较表明,该算法简单有效,适用性强,而且对滤波、噪声、JPEG 压缩、剪切等攻击表现出了较强的鲁棒性.

关键词:零水印,混沌系统,Logistic 系统,奇异值分解

PACC:0545

1. 引 言

近年来,将混沌理论应用于版权保护的数字水印技术成为一个新的研究方向[1—10].现阶段水印技术按照应用领域分为脆弱性数字水印技术和鲁棒性数字水印技术.脆弱性数字水印技术[1,2]多用来进行图像完整性认证,其特点是图像的任何变换都被检测出来,算法较为简单;而鲁棒性数字水印技术[3—5]多用于版权归属认证,目标是图像在传输过程中经过一些常规或非常规的变化后,比如格式转化,JPEG 压缩、滤波、噪声或剪切等攻击时,一定程度上能够提取出里面所含的水印,其主要方法是找到图像的不变特性,通过修改不变特性嵌入水印.

然而,对于一些敏感的图像,诸如远程医疗图像、实时遥感图像等,由于其细节像素的重要意义,图像任何像素的变化对图像造成的失真,都会影响医生或者遥感专家做出判断,同时大量该种类型数字图像的存在必然会涉及到版权问题.零水印方案作为这类图像版权归属认证的主要方法,以无失真修改宿主图像,算法简单有效而著称,目前已有一些零水印方案存在[6—12],然而均存在一些问题.

1)零水印方案以保存二进制的无意义序列为注册中心的水印[6—9],这样的水印由于缺乏可视性容易引起争端,单凭相似度进行版权归属认证缺乏依据;文献[10]将小波低频系数转化成的二进制序列与置乱后的灰度水印图像转化成的二进制序列进行取反操作,然后进行移位运算,将得到的二值序列每八位作为一个像素值,保存在注册中心,为水印图像可视化提供了一个全新的思路,在视觉上有了很大提高;然而算法将处理后的灰度图像存储在注册中心,对于版权所有者来说,存储数量之大带来的存储费用之高让数字版权保护失去了意义.

2)用混沌系统拟合水印保存相应的密钥,思路可行,但实现起来复杂度较高,不适合现实操作;文献[8]和文献[9]用密钥控制 Logistic 映射,以固定的步长搜索出与特征水印相同的二值序列,使得密钥的保存更加简单.然而对于大量的数字图像来说,图像的信息不同导致水印二值序列不同,每次都采用相同的方法和步骤控制 Logistic 映射进行搜索,增加了算法实时处理的时间,这给高效处理带来了很多困难.

* 国家高技术研究发展计划(863)(批准号:2007AA01Z241-2)和北京交通大学研究基金(批准号:2006XM002)资助的课题.

† E-mail:06111031@bjtu.edu.cn

3)零水印方案中没有考虑注册中心的二值序列的分布问题,安全的水印图像中 0 和 1 分布应该均匀,且杂乱无章,从而保障水印在注册中心的安全性.如果零水印方案均是 0 或者均是 1,纵然可以提高水印的检测效率,相似度很高,也无法说明版权的所属性,且没有安全性可言.文献[7]用阈值的方法调整 0 或者 1 的比例,使两者个数尽可能相等,但阈值的选择对 0 和 1 比例影响较大,不易把握.

4)现有算法通过选择阈值的方式判断水印相似度最终确定版权所属,不够精确,且阈值的选择很难确定,一定程度上影响了水印虚警和漏警的存在.

另外,文献[7]对 DT-CWT 域内的图像块进行奇异值分解,选取第二、三、四个奇异值构造水印,图像块的大小最少为 8×8,对水印容量造成影响.基于图像块技术的水印容量应该选取多少才能和安全性之间达到均衡到目前为止很少有文献进行说明.因此水印的可视化、水印安全和容量之间关系亟待解决.

本文利用 Logistic 混沌系统映射出图像信息的提取位置,将具有实际意义的二值图像作为水印图像,利用奇异值分解的不变特性产生二值序列,将该二值序列和水印图像进行处理转换成均匀分布的伪水印图像保存在注册中心,提高安全性,同时通过分析图像块的选择对算法安全性的影响,对水印容量进行了理论上的分析.

2. 基础理论

2.1. Logistic 混沌系统和位置信息提取

Logistic 映射系统是数字水印中最常用的一种混沌系统[13,14],其定义如下:

$$x_{n+1}=\lambda x_n(1-x_n),\lambda\in[0,4],\quad x_n\in(0,1),\tag{1}$$

其中,λ 为 Logistic 混沌系统的控制参数,x_n 为映射的混沌序列.

算法利用 Logistic 混沌系统映射图像块位置信息,具体方法如下:

1)利用密钥 K 作为 Logistic 系统的初值,映射出长度为 $m\times n$($m\times n$ 为图像块的个数)的混沌序列,$X=\{x_1,x_2,x_3,\cdots x_{m\times n}\}$:

$$X=\mathrm{Logistic}(K,m\times n).\tag{2}$$

2)按照光栅扫描方式将 X 转换成大小为 $m\times n$ 的二维混沌序列 X'':

$$X''=\begin{bmatrix} x_1 & \cdots & x_n \\ & \cdots & \\ x_{(m-1)\times n+1} & \cdots & x_{m\times n}\end{bmatrix}.\tag{3}$$

(3)按照制定的某种方式(设映射关系为 f),如冒泡法,稳定排序法等将 X 重新整理成一维混沌序列 X':

$$X'=f(X).\tag{4}$$

4)通过依次查找一维混沌序列和二维混沌序列对应的横纵坐标,建立图像块之间相关关系,组成一个查找表(Look Up Table,LUT),具体程序如下:

```
For i = 1:2:m × n;
[i1,j1] = find(X'' = X'(i));
[i2,j2] = find(X'' = X'(i + 1));
End.
```

即图像块($i1$,$j1$)和图像块($i2$,$j2$)建立相关关系.通过循环,构成所选图像块的相关关系,提取图像信息.

文献[1]中指出,自适应水印算法中,为了算法的安全性,LUT 需要满足以下条件:

1)LUT 构成的图像块一一对应,不能重复;

2)LUT 随着密钥的不同在图像中随机分布;

3)LUT 映射的图像块之间的距离不能太近;

4)密钥空间要足够大.

Logistic 混沌系统由于其伪周期的特性,使得 X' 和 X'' 中无重复的元素,同时图像块之间的关系由密钥控制,初值极端敏感性和很大的密钥空间使得图像块之间一一对应,互不重复,构成的 LUT 满足上述条件.

2.2. 奇异值分解(SVD)原理

对于任一实矩阵 A,可以等于两个标准正交矩阵 U 和 V 以及由降序排列的奇异值组成的对角阵 D 的乘积,即 $A=UDV^{\mathrm{T}}$.奇异值能够刻画矩阵数据的分布特征,且对角阵 D 保留了矩阵的代数本质,令奇异值分解在很多领域有较多应用[15—17].

提取特征具有攻击不变性是水印嵌入和提取过程中最重要的特征.奇异值分解具有行列互换不变,旋转不变,转置不变,镜像变换不变等重要特性.因此,基于奇异值理论的数字水印技术具有很强的数学基础.

3. 零水印方案

3.1. 伪水印的构造算法

基于混沌理论和奇异值分解的伪水印构造方案步骤如下.

步骤 1　先将大小为 $M \times N$ 原始图像 $I_{M\times N}$ 划分为互不重叠、大小为 $(M/m) \times (N/n)$ 的图像块 I_l $(l = 1,2,\cdots,m \times n)$：

$$\boldsymbol{I} = \begin{bmatrix} \boldsymbol{I}_1 & \cdots & \boldsymbol{I}_n \\ & \cdots & \\ \boldsymbol{I}_{(m-1)\times n+1} & \cdots & \boldsymbol{I}_{m\times n} \end{bmatrix}. \tag{5}$$

步骤 2　将图像块进行奇异值分解：

$$[\boldsymbol{U}_l, \boldsymbol{D}_l, \boldsymbol{V}_l] = \mathrm{svd}(\boldsymbol{I}_l). \tag{6}$$

步骤 3　密钥控制 Logistic 混沌系统，映射图像块位置信息，构造查找表 LUT：

$$\mathrm{LUT} = f(\mathrm{Logistic}(K, m \times n)). \tag{7}$$

步骤 4　提取图像信息：比较被 LUT 选出的相邻两图像块分解后相同位置的奇异值，构造图像信息 W'：

$$\begin{aligned} w' &= 1, d_u^i \geqslant d_v^i, \\ w' &= 0, d_u^i < d_v^i, \end{aligned} \tag{8}$$

其中 $(u, v) \in l$ 表示 LUT 中对应的相邻两个图像块，$d_{u(v)}^i$ $(i \in \{1,2,\cdots,\min((M/m),(N/n))\})$ 表示图像块 $\boldsymbol{I}_{u(v)}$ 的第 i 个奇异值.

步骤 5　生成注册中心的伪水印序列：考虑水印在注册中心的安全性，水印图像必须为表现混乱但和认证内容有关且均匀分布的二值序列. 另外，版权认证过程中水印图像应具有可视性，将具有版权意义的水印图像 W 和提取的信息图像 W' 进行运算得到伪水印序列 W''：

$$W'' = \mathrm{xor}(W', W), \tag{9}$$

其中，xor 表示异或运算，即当 W' 和 W 中元素相同时输出为 0，不同时输出为 1.

3.2. 水印的检测算法

水印检测过程和伪水印构造算法相同.

步骤 1　将待检测图像 $\boldsymbol{I}'_{M\times N}$ 划分为互不重叠大小为 $(M/m) \times (N/n)$ 的图像块 $\boldsymbol{I}'_l$ $(l = 1,2,\cdots,m \times n$ (式(5)))；

步骤 2　将图像块进行奇异值分解(式(6))；

步骤 3　构造查找表 LUT(式(7))；

步骤 4　构造图像信息 W'(式(8))；

步骤 5　将保存在注册中心的伪水印图像 W'' 和提取的图像信息 W' 进行异或操作，生成版权认证水印图像 W：

$$W = \mathrm{xor}(W', W''). \tag{10}$$

4. 实验结果及分析

为了验证算法的有效性，实验过程中选取大小为 512×512 的各种类型灰度图像作为宿主图像(如图 1)，分别为标准测试图像 Lena，卡通图像，医学眼底图像，诗画图像[18]，自然风景和遥感图像，选取具有文字意义和图像意义的两个 32×32 的二值图像作为水印测试图像(如图 2).

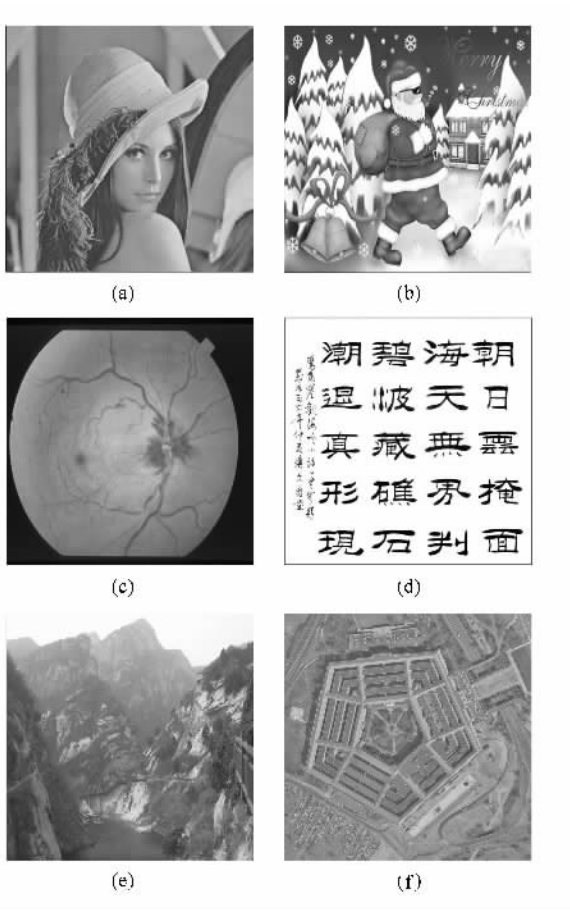

图 1　宿主测试图像　(a) Lena 图像；(b) 卡通图像；(c) 医学眼底图像；(d) 诗画图像；(e) 自然风景图像；(f) 遥感图像

4.1. 奇异值选取对性能影响

奇异值分解的不同奇异值代表图像能量不同，实验选择 Lena 图像，将误比特率(Bit Error Rate，BER)

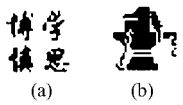

图 2 水印测试图像 (a)文字水印;(b)图像水印

$$\mathrm{BER} \triangleq \frac{\sum_{i=1}^{p}\sum_{j=1}^{q}(W'(i,j)-W(i,j))^2}{p\times q} \tag{11}$$

作为评判标准测试不同的奇异值对水印鲁棒性的影响.其中,W'和 W 分别表示提取出的水印图像和原始水印图像,p 和 q 表示水印图像的大小.

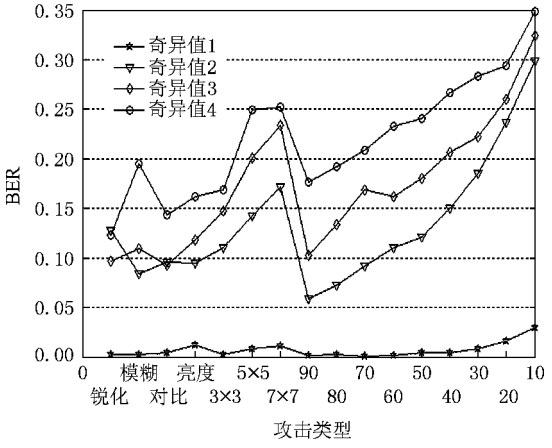

图 3 不同奇异值水印鲁棒性测试

算法的鲁棒性指图像在遭受各种类型攻击时能很好地提取其中的水印,从而进行版权所属认证,它是水印算法性能重要评判指标.实验中选取常规图像处理:锐化、模糊、对比度增强(50%)、亮度增强(50%)、中值滤波(3×3,5×5,7×7)、JPEG 压缩(压缩因子分别为 90,80,…,10).实验发现,文字水印和图像水印作为测试水印图像误比特率相同.图 3 表明,第一个奇异值提取图像信息构成水印信息误比特率低、鲁棒性强,在遭受图像处理过程中,图像的变化能和水印较好地保持同步.该算法采用第一个奇异值提取图像信息构造伪水印.

4.2. 伪水印图像性能测试

保留在注册中心的进行版权认证的伪水印信息必须保证其混乱的视觉效果、均匀分布且和图像内容有关.根据文献[19]提出的衡量伪随机二值序列的方法,通过均衡性和相似性对伪水印序列进行测试.

4.2.1. 均衡性测试

二值序列的均衡性,指序列中 0 和 1 的基本相近程度,E 越小,表明序列中 0 和 1 分布越均匀.其定义为

$$E = \frac{|N_1 - N_0|}{N}, \tag{12}$$

其中 N_1,N_0 和 N 分别表示序列中 1 的个数,0 的个数和序列总长度.

表 1 不同宿主图像水印均衡性测试

	文字水印			图像水印		
	N_1	N_0	E	N_1	N_0	E
Lena	503	521	0.0176	511	513	0.0020
卡通	485	539	0.0527	479	545	0.0645
医学	502	522	0.0195	544	480	0.0625
诗画	589	435	0.1504	567	457	0.1074
遥感	499	525	0.0253	543	481	0.0605
风景	502	522	0.0195	498	526	0.0273

表 1 表明对于不同类型的宿主图像,由文字水印或图像水印和图像信息构成的二值序列均衡性较好,诗画图像由于存在大量均匀区域,均衡性稍差;但均衡性 E 也相对降低,满足水印均匀分布的要求.

4.2.2. 相似特性测试

水印图像由于与宿主图像内容相关,因此不同宿主图像的伪水印应该相互独立.为了验证图像之间的相关关系,定义相似度:

$$\mathrm{sgn}(x,y) \triangleq \begin{cases} 1, x = y, \\ 0, x \neq y, \end{cases} \tag{13}$$

$$\rho \triangleq \frac{\sum_{i=1}^{p}\sum_{j=1}^{q}\mathrm{sgn}(w'_{i,j},w_{i,j})}{p\times q}. \tag{14}$$

(13)式为符号函数,(14)式中 $w_{i,j}$ 和 $w'_{i,j}$ 分别表示原始水印 W 和验证水印图像 W' 的第(i,j)个元素,p 和 q 表示水印图像的大小.

表 2 不同宿主图像水印相似特性测试

	Lena	卡通	医学	诗画	遥感	风景
Lena	1.000	0.4893	0.4678	0.4961	0.5078	0.5400
卡通	0.4893	1.000	0.5176	0.4893	0.5479	0.3770
医学	0.4678	0.5176	1.000	0.4619	0.4834	0.4922
诗画	0.4961	0.4893	0.4619	1.000	0.4883	0.5420
遥感	0.5078	0.5479	0.4834	0.4883	1.000	0.4912
风景	0.5400	0.3770	0.4922	0.5420	0.4912	1.000

理论上,对于两幅大小相等的二值图像,如果图

像中 0 和 1 的个数近似相等，即二值图像的均衡性近似为 0，则不相关图像间相似度为 0.5，相关图像相似度为 1.

证明　假设图像中 1 的个数为 N_1，0 的个数为 N_0，$N = N_1 + N_0$ 表示总个数，则 0 和 0 匹配的概率为 $p_0 = 50\%$，1 和 1 匹配的概率为 $p_1 = 50\%$，则不同图像的相似度为

$$\rho = \frac{p_1 \times N_1 + p_0 \times N_1}{N} = \frac{0.5 \times (N_1 + N_1)}{N} = 0.5. \quad (15)$$

实验以文字水印测试不同宿主图像构造伪水印图像的相似度. 表 2 表明，相同图像由于完全匹配，相似度为 1；不同类型图像的相似度近似为 0.5，验证了理论的正确，同时再次验证了图像的均衡性近似为 0，这为由 SVD 构造伪水印图像提供理论和实际依据.

4.3. 算法普适性测试

实际生活中由于图像特征，如纹理、亮度、均匀程度等不同被分成很多类型，算法对不同类型图像的适用程度决定了算法的普适程度和实际应用价值.

试验中选取常规图像处理：锐化、模糊、对比度增强(50%)、亮度增强(50%)、中值滤波(3×3，5×5，7×7)、JPEG 压缩(压缩因子分别为 90，80，…，10)、椒盐噪声(0.02，0.04)和高斯噪声(0.02，0.04). 攻击后图像和原始图像之间质量差别通过峰值信噪比(PSNR，(16)式)进行衡量，提取出水印和原始水印之间的差异用相似度((14)式)衡量，测试不同宿主图像经过常规攻击后的鲁棒性.

$$\mathrm{PSNR} = 10\lg\left(\frac{255^2}{\mathrm{MSE}}\right), \quad (16)$$

$$\mathrm{MSE} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(\boldsymbol{I}'(i,j) - \boldsymbol{I}(i,j))^2}{M \times N}, \quad (17)$$

其中，$\boldsymbol{I}'$ 和 $\boldsymbol{I}$ 分别表示攻击前后的宿主图像，M 和 N 表示图像的大小.

图 4 表明，图像经过攻击后质量明显下降，尤其经过亮度增强、滤波、低质量压缩及噪声攻击后，图像产生较大失真. 然而由图 5 可得：严重失真下的图像提取出的水印图像相似度很高，大部分都在 0.95 以上. 诗画图像作为特殊图像类型，噪声攻击改变了图像空白区域像素值的分布，从而极大地改变了奇异值分解的奇异值，被攻击后提取水印相似度相对较低. 然而其他失真图像提取水印相似度都在 0.90 以上，表明算法对于不同类型宿主图像，抗攻击能力强、普适性好.

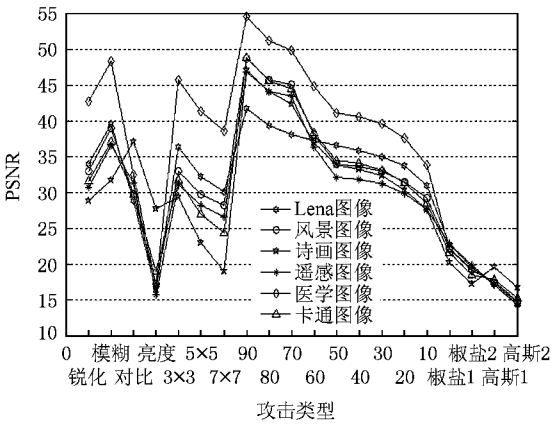

图 4　攻击后不同宿主图像质量测试

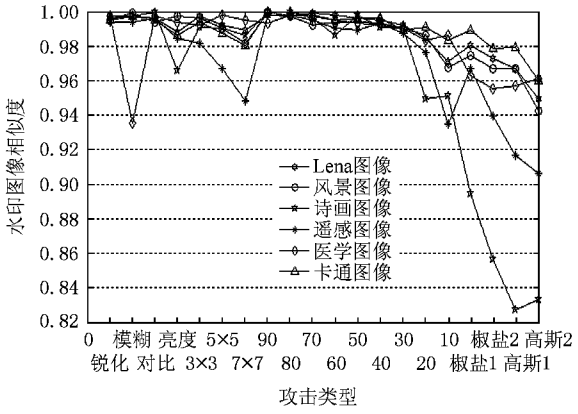

图 5　不同宿主图像水印鲁棒性测试

4.4. 算法安全性和水印容量分析

算法建立在混沌系统的基础之上，将初值作为密钥，其安全性依赖于混沌系统的初值，而算法可以完全公开，满足 Kerckhoff 准则. 图 6 选取 Lena 和图像水印分别作为宿主图像和水印图像，显示错误密钥和正确密钥提取出的水印图像，图 7 选择 1000 个不同密钥通过图像相似性判定准则验证算法的安全性. 可看出，错误密钥提取出水印的可视性效果很差，和原始水印图像的相似度为 0.5；正确密钥提取出水印和原始水印相同，相似度为 1. 表明算法具有很高的安全性，且有很大的密钥空间.

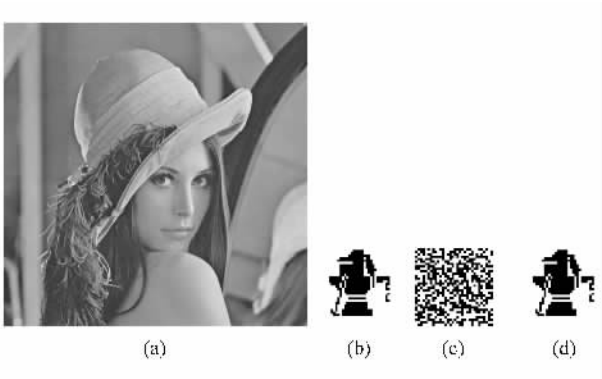

图 6 算法安全性测试 (a)宿主图像 Lena ;(b)水印图像 ;(c)错误密钥提取水印图像 ;(d)正确密钥提取水印图像

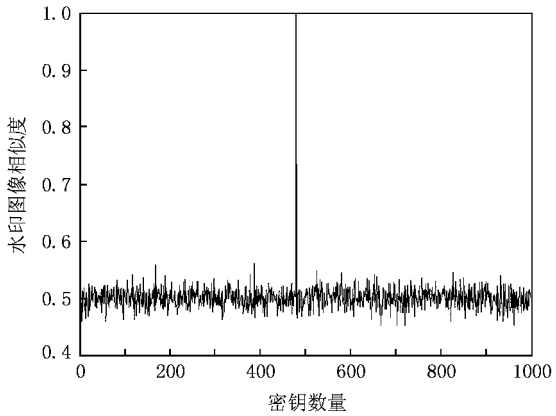

图 7 算法安全性测试

另外,零水印方案中水印图像的大小涉及到存储在注册中心的容量,必须对水印的容量和水印的安全性做一个权衡.目前文献中很少涉及对零水印容量进行分析,大多数零水印方案根据经验对图像块的选择做出判断,没有给出合理的解释.我们给出基于图像块的零水印方案水印最佳容量的理论推导.

定理 1 若 n 为偶数,当 $r < n/2$ 时,C_n^r 随 r 单调递增 ;$r > n/2$ 时,C_n^r 随 r 单调递减.若 n 为奇数,当 $r < (n-1)/2$ 时,C_n^r 随 r 单调递增 ;$r > (n+1)/2$ 时,C_n^r 随 r 单调递减.

证明

$$C_n^{r-1} = \frac{n!}{(r-1)!(n-r+1)!} = \frac{n!}{(r-1)!(n-r)!(n-r+1)},$$

$$C_n^r = \frac{n!}{r!(n-r)!} = \frac{n!}{r(r-1)!(n-r)!},$$

$$C_n^{r+1} = \frac{n!}{(r+1)!(n-r-1)!} = \frac{n!}{(r+1)(r)!(n-r-1)!},$$

假设 $C_n^{r+1} < C_n^r$,即

$$\frac{n!}{(r+1)(r)!(n-r-1)!} < \frac{n!}{r!(n-r-1)!(n-r)},$$

$$\therefore \frac{1}{(r+1)} < \frac{1}{(n-r)},$$

$$\therefore r+1 > n-r, \therefore 2r > n-1.$$

假设 $C_n^{r-1} < C_n^r$,即

$$\frac{n!}{(r-1)!(n-r)!(n-r+1)} < \frac{n!}{r(r-1)!(n-r)!},$$

$$\therefore \frac{1}{(n-r+1)} < \frac{1}{r},$$

$$\therefore r < n-r+1, \therefore 2r < n+1.$$

定理 2 当 n 为偶数时,$C_n^{n/2}$ 最大 ;当 n 为奇数时,$C_n^{(n-1)/2} = C_n^{(n+1)/2}$ 最大.

基于图像块的零水印方案通过比较图像块内或图像块之间的不变特征量进行图像信息提取.对于由 n 个图像块组成的宿主图像,由定理 1 和定理 2 可知 :当选择图像块个数接近图像块总数的一半时,图像块的可选择性最多,亦即正确找到所选图像块的概率最小,这使得算法在保证水印容量的同时,安全性达到最高.

4.5. 算法性能优势比较

为了验证该算法和其他零水印算法之间的性能优势,实验选取图像水印测试 Lena 图像经过各种攻击后提取水印图像和原始水印图像的相似性.表 3 表明,该算法对于噪声、滤波以及 JPEG 压缩,提取水印的相似度都在 0.95 以上,有些甚至接近 1,高于其他算法 ;对于几何攻击中的较难抵抗的剪切和旋转攻击,由于奇异值的不变特性,该算法表现出了较强的鲁棒性,提取水印的相似度都在 0.95 以上 ;同时该算法提取的水印图像具有很好的可视效果,而

不是凭借阈值判断版权归属，是该算法区别于其他算法最大的特点.

表 3　算法性能对比测试

攻击测试	相似度				
	文献[6]	文献[7]	文献[8]	文献[9]	本算法
高斯噪声	0.9300	0.8594	—	0.9600	0.9668
中值滤波 1	0.9900	0.9453	—	0.9800	0.9971
中值滤波 2	0.9700	0.9063	—	0.9800	0.9922
JPEG(90)	1.0000	1.0000	0.7800	1.000	0.9981
JPEG(70)	0.9700	1.0000	0.6500	1.000	0.9991
JPEG(50)	0.9600	—	0.5700	0.9900	0.9961
JPEG(20)	0.9400	0.9570	0.1200	0.9700	0.9844
剪切(10%)	0.9900	—	0.9500	—	0.9951
剪切(20%)	0.9700	—	0.9000	—	0.9824
剪切(30%)	0.9600	—	0.8300	—	0.9668
剪切(40%)	0.9500	—	0.8200	—	0.9561
旋转 1°	0.9300	0.8164	1.0000	—	0.9971
旋转 2.5°	0.9700	—	0.9200	—	0.9902
旋转 5°	0.9600	—	0.6400	1.000	0.9863
旋转 10°	0.9500	—	0.4500	0.9500	0.9775
水印可视	不可视	不可视	不可视	不可视	可视

4.6. 算法扩展

对于彩色图像，由于其存在 R，G，B 三通道，可以用混沌系统控制其通道的选取. 如给 Logistic 混沌系统一个初始密钥，选取合适阈值将混沌序列分为三部分，每一部分对应一个通道，由于每个通道都相当于一个灰度图像，将被选中的通道利用该算法进行水印构造. 因此算法同样适用于彩色图像.

5. 结　论

本文描述了一种通过不改变图像内容进行数字版权归属认证的算法，利用混沌系统构建安全模型，利用奇异值不变特性构造注册中心伪水印图像，改变了传统的版权保护做法，有以下显著优点：1）算法以混沌系统为基础，对混沌系统的初值具有极端依赖性，算法安全性高；2）算法在空域中操作，对图像无失真，算法简单易行，可操作性强；3）以二值图像为水印图像，解决了传统零水印算法通过阈值判断相似度进行版权认证，而无可视性效果的问题；4）以图像块 SVD 的第一个奇异值为图像信息，代表了图像的特征，提高了抵抗常规攻击和几何攻击的能力，鲁棒性好；5）算法普适性好，适用于各种类型的图像，具有重要的理论意义和实际推广价值.

[1] He H J，Zhang J S 2007 *Acta Phys. Sin.* **56** 3092 (in Chinese) [和红杰、张家树 2007 物理学报 **56** 3092]

[2] Zhang J，Zhang C T 2004 *Acta Elec.* **32** 157 (in Chinese) [张　静、张春田 2004 电子学报 **32** 157]

[3] Zhou L J，Wang B，Feng J C 2008 *Acta Phys. Sin.* **57** 2750 (in Chinese) [周露娟、汪　波、冯久超 2008 物理学报 **57** 2750]

[4] Peng Z N，Liu W B 2008 *Chaos，Solitons & Fractals*. **36** 946

[5] Kang X G，Huang J W，Zeng W J 2008 *IEEE Trans. Multimedia*. **10** 953

[6] Hu Y F，Zhu S A 2008 *Journal of Zhejiang University* (Engineering Science). **42** 593 (in Chinese) [胡裕峰、朱善安 2008 浙江大学学报(工学版) **42** 593]

[7] Gao S L 2008 *Journal of Sichuan University* (Natural Science Edition) **45** 493 (in Chinese) [高仕龙 2008 四川大学学报(自然科学版) **45** 493]

[8] Yang S G，Li C X，Sun F，Sun Y 2003 *Journal of Image and Graphics* **8** 664 (in Chinese) [杨树国、李春霞、孙　枫、孙　尧 2003 中国图形图像学报 **8** 664]

[9] Xiang H，Cao H Q，Wu K N，Wei Fang 2006 *Journal of Image and Graphics* **11** 770 (in Chinese) [向　华、曹汉强、伍凯宁、魏　访 2006 中国图形图像学报 **11** 770]

[10] Ma J H，He J X 2007 *Journal of Image and Graphics* **12** 581 (in Chinese) [马建湖、何甲兴 2007 中国图形图像学报 **12** 581]

[11] Boyer，J P，Duhamel P，Blanc-Talon J 2007 *IEEE Trans. Information Forensics and Security* **2** 283

[12] Teddy F 2007 *IEEE Trans. Information Forensics and Security* **2** 149

[13] Yu Z B，Feng J C 2008 *Acta Phys. Sin.* **57** 1409 (in Chinese) [余振标、冯久超 2008 物理学报 **57** 1409]

[14] Wang X Y，Wang M J 2008 *Acta Phys. Sin.* **57** 731 (in Chinese) [王兴元、王明军 2008 物理学报 **57** 731]

[15] Guo C B，Xiao C H，Liu D M 2008 *Acta Phys. Sin.* **57** 4182 (in Chinese) [郭成豹、肖昌汉、刘大明 2008 物理学报 **57** 4182]

[16] Huang Q X，Liu D，Wang F，Yan J H，Chi Y，Cen K F 2007 *Acta Phys. Sin.* **56** 6742 (in Chinese) [黄群星、刘　冬、王　飞、严建华、池　涌、岑可法 2007 物理学报 **56** 6742]

[17] Bai Y，Liu X Y，He D W，Ru H Y，Qi L，Jie M B，Zhao W，Xie

F X, Nie R J, Ma P, Dai Y D, Wang F R 2006 *Acta Phys. Sin.* **55** 2651 (in Chinese) [白 云、刘新元、何定武、汝鸿羽、齐 亮、季敏标、赵 巍、谢飞翔、聂瑞娟、马 平、戴远东、王福仁 2006 物理学报 **55** 2651]

[18] http://ghw.hebei.net.cn/Html/lishu/160957866.html

[19] Sheng L Y, Cao L L, Sun K H, Wen J 2005 *Acta Phys. Sin.* **54** 4031 (in Chinese) [盛利元、曹莉凌、孙克辉、闻 姜 2005 物理学报 **54** 4031]

A novel zero-bit watermarking algorithm based on Logistic chaotic system and singular value decomposition *

Song Wei† Hou Jian-Jun Li Zhao-Hong Huang Liang

(*School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing* 100044, *China*)

(Received 4 November 2008; revised manuscript received 24 November 2008)

Abstract

Based on chaotic system and singular value decomposition (SVD), a novel zero-bit watermarking algorithm is presented. The proposed approach changed the traditional ways that copyright is protected by modifying the contents of images. Taking advantage of the characteristics of extreme sensitivity to initial values, Logistic mapping is used to find the hiding position of information, which enhances the scheme's security. The invariant characters of SVD are applied to make the watermarks of registration center, which make the watermarked image distortion-free. and can protect the copyright effectively. Binary image is selected as watermark image so that the watermarks of existing zero-bit watermarking algorithms are no longer invisible and meaningless. The relationship between watermark capacity and security is also analyzed. Simulation of the algorithm was performed on different types of images, including standard test image, cartoon image, medical image, poem image, remote sensing image and natural scenery image, and the results were compared with existing algorithms. Results show that the propsed algrithm is simple and applicable, and can resist many attacks such as filtering, noising, JPEG compression, and shearing.

Keywords: zero-bit watermarking, chaotic system, Logistic mapping, singular value decomposing (SVD)

PACC: 0545

* Project supported by the National High Technology Research and Development Program of China (Grant No. 2007AA01Z241-2) and the Beijing Jiaotong University Science Foundation (Grant No. 2006XM002).

† E-mail: 06111031@bjtu.edu.cn