一种基于 MSB 构造密钥的零水印算法①

A Non-Watermarking Algorithm Based on MSB Structare Key

牛万红[1]　颜惠琴[2]　(1.宁夏大学 远程教育学院 宁夏 银川 750021;
2.宁夏大学 数学计算机学院 宁夏 银川 750021)

摘　要： 提出一种基于最高有效位(Most Significant Bit)构造密钥的零水印算法。先将二值水印图像置乱并扩展为载体图像的大小，再将其像素值与载体像素的 MSB 进行对应比较，当比较结果为真时，用一个零矩阵来标记载体像素的位置，被标记过的零矩阵作为密钥来检测水印。由于水印信息遍布载体图像的 MSB 而且不改变载体图像的信息，使得算法表现出较好的抗攻击性能。通过与文献[4]“一种基于混沌阵列的鲁棒零水印算法”的比较实验，表明了该算法的有效性。

关键词： 零水印 最高有效位 鲁棒性

1　引言

水印是用于版权保护、身份认证、篡改提示的一种有效方法。由于该技术大多采取对图像信息进行一定修改来嵌入水印信息的方式，存在水印不可感知性与提取时鲁棒性之间的矛盾。比如：LSB 水印算法通过载体图像像素的最低有效位来隐藏水印信息，即对像素的最低位做信息替换。这样对载体图像的品质影响最小，所隐藏的信息在视觉上很难被发现，满足水印的不可见性。然而 LSB 算法对空域的各种信号处理操作很敏感，使得水印非常脆弱。而将水印嵌入到像素较高位面时，水印的鲁棒性会大大提高，但对图像品质影响太大，甚至水印可见。

近来“零水印”[1]技术被提出来解决上述问题。一种有效的零水印策略是利用载体图像作为一种编码字典，而将水印信息在编码字典中的位置信息作为密钥；由于嵌入水印时不修改原始图像，且可根据密钥提取相应位置的信息恢复水印，这样就很好地平衡了数字水印算法的鲁棒性、水印的嵌入信息量以及不可觉察性之间的关系。通过在相应的信息数据库注册对应的零水印信息，就可以将原图像保护在水印下,这就为版权归属提供了一个完全、可靠的证明[2]。

文献[1,3]中提出了两种零水印构造方法，一种是在空域中利用高阶累积量来形成水印，该方法对小角度旋转及压缩具有较好的鲁棒性，但计算量大，对乘性噪声鲁棒性不佳，无法抵御 DA 转换攻击(数字信号转为模拟信号)；另一种是在变换域中利用 DCT 变换系数构造水印，该算法对一般的图像处理具有比前一方法更佳的鲁棒性，但无法抵御旋转等几何变换。文献[4]提出基于混沌阵列的零水印构造算法具有一定安全性，对一般的图像处理也具有很好的鲁棒性，但由于其水印信息是按照密钥指定的位置构造的，能够构造水印信息的容量较小，且在载体中分布形式单一，故仍对几何攻击十分敏感。

本文算法针对文献[4]提出改进，通过置乱水印信息并扩展为载体图像的大小，再与载体像素的 MSB 进行比较来构造关于零水印的密钥，以实现信息的隐藏。仿真实验表明，本文算法具有更好的鲁棒性，尤其在抗几何攻击的性能方面优于文献[4]算法。

2　零水印构造

改进算法思路如下：

一幅 uint8 型灰度载体图像的二进制编码分为 8'

① 基金项目:宁夏大学青年科学基金(QN200801)
收稿时间:2009-03-30

个位面，如图 1 所示。

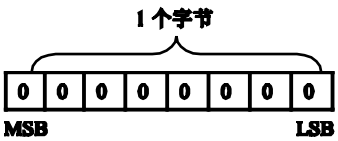
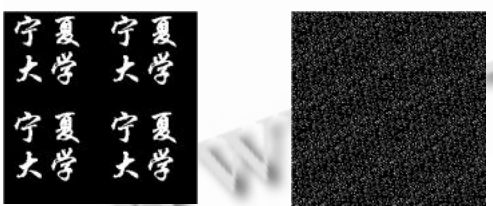


图 1　一个像素的二进制表示

为了水印算法的安全性，我们先将二值水印图像用 arnold 方法置乱[5]。arnold 方法是 Arnold 在遍历理论研究中提出的一种变换，它实际上是一种点的位置移动。我们将该技术应用到二维图像平面，目的是用来扰乱图像的组成部分，破坏图像的自相关性，使得人眼无法从中提取有价值的信息，这样能在一定程度上保护图像信息。然后将置乱的水印图像扩展为载体图像的大小，图 2 中分别给出了水印未置乱的扩展图(a)和置乱后的扩展图(b)，我们利用图(b)，将其信息与载体像素 MSB 进行对应比较。当比较的结果为真时，用一个零矩阵来标记载体像素的位置，最后被标记过的零矩阵作为密钥，在盲检测水印时使用。由于水印信息的扩展使得水印信息遍布到载体图像的所有 MSB 位置，有利于抗击剪切和旋转等几何攻击。这种在不改变载体像素 MSB 的情况下构造零水印的方法，很好的解决了水印的不可见性和鲁棒性之间的矛盾。水印检测时，利用密钥提取水印，不需要原始图像和水印图像，算法的原理简单，实用性强。该算法对原始图像数据没有进行任何修改，因而不存在真正意义上的“嵌入水印图像”，符合零水印概念。



(a) 水印未置乱的扩展　　(b) 水印置乱后的扩展

图 2　水印图像的尺寸扩展为载体图像的尺寸

2.1 零水印密钥的构造步骤

步骤 1 采用一幅有意义的二值图像作为水印信息，将其用 arnold 方法置乱。本文置乱次数为 20。

步骤 2 利用 Matlab 提供的 cat 函数将置乱的水印图像扩展为载体图像尺寸的大小。

步骤 3 用扩展的水印图像像素值与载体像素的 MSB 进行对应比较，见图 3。再用一个与载体图像相同尺寸的零矩阵来标记比较结果为真时载体像素的位置，作为密钥。如，在 MSB 比较为真时，修改零矩阵对应的值为 1，不相等时则不修改。密钥矩阵 key 如图 4 所示(实际是一幅与载体相同大小的二值图像)。

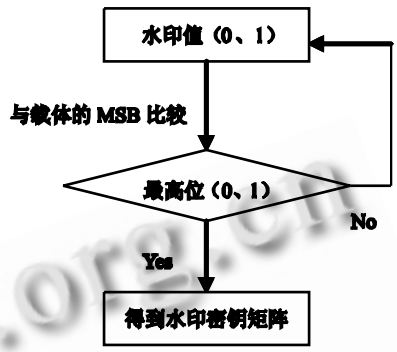


图 3　载体像素与水印像素值比较流程

图 4　密钥矩阵 key

2.2 水印检测步骤

步骤 1 根据密钥矩阵 key，用函数 bitget()在被测图像中提取(被扩展的)水印信息。

如果 key(i，j)=1，则从载体中相应像素的 MSB 提取(被扩展的)水印；如果 key(i，j)≠1，则把载体中相应像素的 MSB 取反后提取(被扩展的)水印。

步骤 2 将提取的水印信息恢复为原始尺寸。

步骤 3 用 arnold 逆算法恢复水印图像。

3　实验分析

本文算法在 Matlab7.1 平台上实现，以灰度图像 lena.bmp(256×256 像素)为载体，nxdx128.bmp 为水印(128×128 像素)进行仿真试验。

我们从主观和客观两方面来衡量算法性能。利用人眼直接观察水印提取结果作为主观性能参数；客观性能参数采用水印序列的相关性来检验水印是否存在，并采用峰值信噪比衡量提取水印的质量。

① 相关性公式：定义被恢复出的水印信号序列 f_w 和原始水印信号序列 f 的相似程度为

$$NC(f_w, f) = f \cdot f_w / \sqrt{f_w \cdot f_w} \quad (1)$$

相似度判定准则为：事先设定一个阈值 T,若 >T，可以判定被测图像中含有水印，否则，没有水印。用上式检测提取出来的水印和原水印的客观相似性，考虑到使虚警概率和误判概率都达到最小，给定阈值为 10，检测值大于 12 就认为有水印的存在，详细见文献[6]。

②水印图像的峰值信噪比( )：峰值信噪比需要先计算均方差[7]

$$MSE = \frac{1}{M * N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (f(i,j) - f_w(i,j))^2 \quad (2)$$

$PSNR$ 的计算公式如下：

$$PNSR = 10 \log_{10} \frac{255^2}{MSE} \quad (3)$$

(2)、(3)式中 $f(i,j)$ 是原始水印的像素值；$f_w(i,j)$ 是被恢复的水印图像的像素值；M、N 分别是图像的高、宽。通过峰值信噪比来衡量提取的水印质量。

图 4 中，(a)为原始图像，(b)为本文算法未攻击提出的水印，(c)为用(1)式计算的水印相关值。

(a)原始图像　(b)提取的水印　(c)水印存在的相关值

图 4　原始图像、提取的水印及水印相关值

在相同条件下，本文算法与文献[4]算法的比较实验如下：

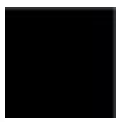
3.1 JPEG 压缩、镜像和抖动攻击实验

含水印图像在受到 JPEG 压缩(质量因子为 5)、镜像、抖动攻击时[8]，两种算法的主客观比较实验结果分别见表 1 和表 2。

表 1　客观数据对比(PSNR,单位 db)

算法\攻击	JPEG 压缩攻击	镜像攻击	抖动攻击
文献[4] PSNR	59.1624	54.2252	57.2952
本文 PSNR	62.2541	54.6855	54.6855
文献[4] NC	33.2988	11.1055	NaN
本文 NC	38.3564	22.0600	22.0600

表 2　提取水印的主观效果对比

算法\攻击	JPEG 压缩攻击	镜像攻击	抖动攻击
攻击效果			
文献[4]算法提取水印			
本文算法提取水印			

从表 1，表 2 可以看出，本文算法的客观指标 PSNR、NC 和主观视觉效果均好于文献[4]算法的相应客观指标和视觉效果，而且抗压缩性能极强，甚至能抵抗质量因子为 1 的 JPEG 压缩。

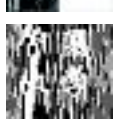
3.2 剪切攻击实验

含水印图像受 1/4、1/3、1/2 剪切比例的攻击时，两种算法的主客观比较实验结果分别见表 3 和表 4。

表 3　剪切攻击时的客观数据对比(PSNR，单位 db)

算法\攻击	剪切 1/4	剪切 1/3	剪切 1/2
文献[4] PSNR	55.0077	53.6758	52.2933
本文 PSNR	76.6577	76.6577	76.6577
文献[4] NC	27.1546	24.5279	21.8400
本文 NC	44.3058	44.3058	44.3058

表 4　剪切攻击时提取水印的主观效果对比

算法\攻击	剪切 1/4	剪切 1/3	剪切 1/2
攻击效果			
文献[4]算法提取水印			
本文算法提取水印			

从表 3、表 4 可以看出，含水印图像受到不同比例的剪切攻击时，本文算法无论从客观指标(PSNR 或 NC)方面或主观视觉效果方面衡量，抗剪切性能均优于文献[4]算法。

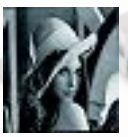
3.3 旋转攻击实验

含水印图像受到 1° 、5° 、10° 的旋转攻击时，两种算法的主客观比较实验结果分别见表 5 和表 6。

表 5　旋转攻击时的客观数据对比(PSNR，单位 db)

算法\攻击	旋转 1°	旋转 5°	旋转 10°
文献[4] PSNR	61.0895	56.3252	54.6783
本文 PSNR	61.5476	56.2011	55.0855
文献[4] NC	35.9514	23.5481	16.2924
本文 NC	37.4000	26.5452	23.4152

表 6　旋转攻击时提取水印主观效果对比

算法\攻击	旋转 1°	旋转 5°	旋转 10°
攻击效果			
文献[4]算法提取水印			
本文算法提取水印			

从表 5、表 6 可以看出，含水印图像受到 1° 、5° 、10° 的旋转攻击时，文献[4]算法和本文算法的 PSNR 值基本持平，但 NC 值前者小于后者。从主观视觉效果来看，文献[4]算法受超过 1° 的旋转攻击后视觉效果明显下降，水印已无法辨析，而本文算法的水印却依然可辨，甚至可抗击 15° 的旋转攻击。

在抗噪声、滤波、锐化、直方图均衡等攻击的性能方面，两种算法的客观指标和提取水印的主观视觉效果基本相当且都表现出很好的抗攻击性能。限于篇幅，本文没有给出。

3.4 无水印测试

零水印的检测除了要辨认受攻击图像的版权的能力外，还必须有区分不同图像版权的能力。这里我们以一组无水印图像为例分别和含水印的 lena.bmp 图像作对比检测，这 4 幅图像灰度分布较均匀且表达的内容相近，见图 5。

(a)　(b)　(c)　(d)

图 5　一组无水印图像

测试结果见表 7。

表 7　内容相近的一组图像 NC 值比较

检测的图像\算法	文献[4]算法的 NC 值	本文算法的 NC 值
Lena.bmp &(1)	13.7615	5.4810
Lena.bmp &(2)	14.2485	6.1768
Lena.bmp &(3)	14.1886	13.4444
Lena.bmp &(4)	14.2945	10.7537

从表 7 可以看出，文献[4]算法的 NC 值平均为 14.1233，而本文算法的平均 NC 值还不到 9，低于预先设定的阈值 10。可见文献[4]算法的误警率较高，在区别不同的、内容相近的无水印图像方面，本文算法的检测性能优于文献[4]算法。

上述实验表明，本文算法具有以下几方面优点：

(1)由于水印信息被扩展后遍布到载体图像的 MSB，因而抵抗各种攻击的性能极强。在抵抗压缩、镜像、抖动、不同比例的剪切、旋转攻击的性能方面优于文献[4]算法。

(2)通过把水印信息置乱，在载体中构造密钥矩阵，使得非授权用户很难检测到水印的存在，因而水印的安全性很好。

(3)水印提取不需要原始图像和原始水印图像，做到了盲检测。

(4)原理简单，算法实用。

4　结论

零水印技术克服传统水印嵌入方法存在不可见性

(下转第 50 页)

(上接第 69 页)

和鲁棒性的矛盾，并且使图像信息无损，水印隐藏效果好。本文提出的一种基于最高位面构造零水印的算法，有效的实现了这一技术。通过对比文献[4]的实验表明，该算法不仅在抵抗各种攻击的性能方面优于文献[4]算法，而且在区别不同的、内容相近的无水印图像方面也优于文献[4]算法，具有更好的鲁棒性。

参考文献

1 温泉,孙锬锋,王树勋.基于零水印的数字水印技术研究.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.

2 谢贤智,归奕红. 零水印技术对数字图像版权保护的应用研究.广西工学院学报, 2007,18(3):113－116.

3 温泉,孙锬锋,王树勋.零水印的概念与应用.电子学报, 2003,31(2):214－216.

4 高青山,罗向阳,等.一种基于混沌阵列的鲁棒零水印算法.计算机科学, 2005,32(9):76－81.

5 Arnold VI, Avez A. Ergodic problems of classical mechanics. Mathematical Physics Monograph Series. New York: W A Benjamin, Inc., 1968.

6 Cox IJ, Joe Kilian, Fthomson. Secure spread spectrum watermarking for multimedia. IEEE Trans. on Image Processing, 1997,12(6):1673－1687.

7 陈灏.空域数字图像水印算法研究与实现.现代电子技术, 2007,249(10):149－165.

8 Gonzalez R,著;阮秋琦,等,译.北京:电子工业出版社, 2005.