基于小波变换的零水印算法

马建湖 何甲兴
(吉林大学数学研究所,长春 130012)

摘 要 为了实施图像的版权保护,提出了一种基于小波变换的零水印算法。该算法采用经典密码学中的方法嵌入水印。为验证该算法的性能,还对该算法进行了一系列的实验,并且与另一种水印算法的实验结果进行了比较。通过比较发现,该算法对剪切、涂抹、压缩等攻击的鲁棒性远远超过了另一种水印算法。最后对该算法进行了推广,它可以用来隐藏任何数字图像的信息,不仅仅是水印。因此该算法可用于数字图像信息的隐藏。

关键词 水印 小波变换 鲁棒性
中图法分类号: TP307 **文献标识码**: A **文章编号**: 1006-8961(2007)04-0581-05

A Wavelet-Based Method of Zero-Watermark

MA Jian-hu, HE Jia-xing
(*Institute of Mathematics, Jilin University, Changchun* 130012)

Abstract In order to protect the copyright of the image, this paper brings forward a image non-watermarking method based on DWT, where methods of classical Cryptology is employed. A series of experiments have been cavried out and the results proved that the presented method has much better robustness comparing with another watermark method, and the method is further broaden to hide any other digital image information besides watermark.

Keywords watermark, wavelet transform, robustness

1 引 言

随着数字技术和因特网技术的快速发展,多媒体作品传播的范围和速度突飞猛进,但同时盗版现象也愈演愈烈。于是保护数字音像产品的版权,维护创作者的合法利益,成为关系文化市场繁荣的重大课题。数字水印技术正是在这个背景下诞生的,它通过在原始数据中嵌入秘密信息——水印来证明多媒体作品的所有权。

到目前为止已经有很多文献对零水印的嵌入进行过研究,提出了不少零水印算法。所谓零水印就是在嵌入水印的同时不改变公开图像,因此这种算法具有很强的不可见性和保密性。文献[1]最早提出了零水印的概念;文献[2]~[4]提出了基于小波变换的零水印算法,文献[2],[3]算法对于剪切和JPEG 压缩攻击具有较好的鲁棒性;文献[5]提出的检测方案将零水印与人工智能、计算机视觉、常规水印技术有机结合起来,它对于旋转攻击也具有一定的鲁棒性;文献[6]提出了基于小波包的零水印算法,它对于剪切、噪声、JPEG 压缩等攻击具有较好的鲁棒性;文献[7]提出了基于小波变换和离散余弦变换的零水印算法,并且两种算法可以同时应用,它对于 JPEG 压缩攻击具有较好的鲁棒性。本文提出了一种基于小波变换的零水印算法,该算法以离散小波变换为工具,采用经典密码学中的方法将 256 级灰度水印嵌入在公开图像中。

2 具体水印算法

2.1 算法基本思想

由于图像的灰度值都是整数,因此在水印的嵌

基金项目:国家自然科学基金专项基金项目(60542002)
收稿日期:2005-04-25;改回日期:2006-03-23

第一作者简介:马建湖(1981~),男。2004 年获吉林大学数学学院获学士学位,现为吉林大学数学学院计算数学硕士研究生。研究方向为数值逼近与数字图像处理。E-mail:jianhuma@email.jlu.edu.cn

入与提取过程中难免会遇到整数到实数以及实数到整数的变换,这就不可避免的引入了误差。本文的基本思想是将图像的灰度值换算成二进制整数,首先得到了一个二值序列,然后利用经典密码学中的方法对该二值序列进行一系列的处理来实现水印的嵌入以及密钥的加密;最后将得到的一幅图像作为最终的密钥。在整个生成密钥的过程中,由于全部都是整数到整数的运算,从而避免了上述误差。由于该算法还充分结合了小波变换的空间-频率分解特性和零水印不改变公开图像的优点,将水印嵌入到公开图像的低频部分,因此该算法不仅具有良好的不可见性,而且具有很强的鲁棒性。

2.2 水印的置乱

在嵌入水印之前,为了增加保密性,就要对原始水印图像做置乱变换。本文使用的是 Arnold 变换进行置乱(也称猫脸变换)。Arnold 变换是 Arnold 在遍历理论的研究中提出的一种变换,对于正方形图像,其变换公式如下:

$$\begin{bmatrix}\hat{x}\\ \hat{y}\end{bmatrix}=\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}(\mathrm{mod}\ N)$$

其中,(x,y)为原始坐标,$(\hat{x},\hat{y})$为变换后的坐标,mod 为取余运算,N 为图像的宽或高。该变换通过像素点位置的置换来置乱图像。当遍历了原始图像所有的点之后,便进行了一次 Arnold 变换。Aronld 变换具有周期性,在恢复置乱图像时就可利用其周期性。

2.3 公开图像的处理

对于公开图像的处理可采用小波变换。对公开图像进行二次小波变换(本文实验采用的是达别西 2 小波基),由于小波变换后的低频频带 LL_2 的系数包含了公开图像的基本信息(见图 1),是图像能量集中的频带,因此本文就把水印嵌入到低频频带 LL_2,这将增强算法的鲁棒性。

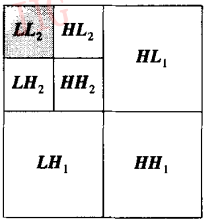


图 1 小波变换示意图

Fig. 1 The sketch map of DWT

2.4 水印的嵌入与提取

先把置乱的水印和经过小波变换的公开图像的低频频带 LL_2 的灰度值转化为二进制整数,然后按下面的公式嵌入水印。

$$S_{m,n}=\sim F_{m,n}\wedge G_{m,n}$$

其中,S 为密钥图像的灰度值的二进制整数,F 为置乱的水印图像的灰度值的二进制整数,G 为经过小波变换的公开图像的低频频带 LL_2 的灰度值的二进制整数,~为按位求反运算,~0 = 1,~1 = 0,例如:~10011100 = 01100011,∧为按位异或运算,0∧0 = 0,1∧1 = 0,1∧0 = 1,0∧1 = 1,例如:10011100∧01010010 = 11001110。最后把运算结果进行加密处理,转化为像素值保存为一幅图像。这个图像就是最终的密钥。提取水印时,先读取密钥图像的灰度值,并进行解密处理。对公开图像进行二次小波变换。然后按下面的公式提取水印:

$$F_{m,n}=(\sim S_{m,n})\wedge G_{m,n}$$

其中,F 为用于置乱的水印图像的灰度值的二进制整数,S 为解密后的密钥图像的灰度值的二进制整数,G 为经过小波变换的公开图像的低频频带 LL_2 的灰度值的二进制整数,~为按位求反运算,∧为按位异或运算。将得到的结果保存为图像,然后对该图像进行置乱变换的逆变换就得到了水印图像。

2.5 密钥的加密与解密

密钥实际上就是 0 和 1 组成的序列,我们可以对它进行移位等运算,对它的排列顺序做一些置乱变换,然后每八位作为一个灰度值存为一幅图像,这就是最终的密钥。假设一个八位二进制整数为 $a_1a_2a_3a_4a_5a_6a_7a_8$,$(a_i=0,1)$,其密钥的加密与解密的置乱变换如下:

加密:$a_1a_2a_3a_4a_5a_6a_7a_8\rightarrow a_3a_4a_7a_8a_1a_2a_5a_6$

解密:$a_3a_4a_7a_8a_1a_2a_5a_6\rightarrow a_1a_2a_3a_4a_5a_6a_7a_8$

例如像素值为 156 的情况:

加密:$156=(10011100)_2\rightarrow(01001011)_2=75$

解密:$75=(01001011)_2\rightarrow(10011100)_2=156$

3 算法实验

本文实验中的图像都是 256 级灰度图,其中水印图像 Lena 为 128×128pixels,公开图像 Barb 为 512×512pixels。两幅图像的峰值信噪比(peak signal noise ratio, PSNR)和相似度(NC)按下面公式计算:

$$PSNR=10\lg\frac{255^2N}{\sum_{m,n}(f(m,n)-\hat{f}(m,n))^2}$$

$$NC = \frac{\sum_{m,n} f(m,n)\hat{f}(m,n)}{\sum_{m,n} f^2(m,n)}$$

其中,$f(m,n)$,$\hat{f}(m,n)$分别为两幅图像在(m,n)处的灰度值。

本文零水印算法的实验结果见图 2。

(a) 水印图像 Lena　(b) 公开图像 Barb　(c) 密钥图像　d) 提取水印(NC = 1.000 0)

图 2　零水印算法实验结果

Fig. 2　The result of the method of zero-watermark

4　鲁棒性实验

为了验证该算法的鲁棒性,下面进行了一些实验。图 3 分别是抵抗剪切、涂抹、噪声以及压缩等攻击的实验结果(本文实验中对图像加高斯噪声和 JPEG 压缩使用的是 Photoshop7. 0)。结果表明,该算法对这些攻击都具有很强的鲁棒性。

(a) 剪切 1/2 ($PSNR$ = 7.77dB)　(b) 从(a)中提取水印 (NC = 0.986 2)　(c) 涂抹 ($PSNR$ = 15.14dB)　(d) 从(c)中提取水印 (NC = 0.995 3)

(e) 加 10% 高斯噪声 ($PSNR$ = 19.87dB)　(f) 从(e)中提取水印 (NC = 1.001 9)　(g) JPEG 压缩 (品质 5)　(h) 从(g)中提取水印 (NC = 1.001 0)

图 3　鲁棒性实验结果

Fig. 3　The results of robustness experiments

5　与其他水印算法实验结果的比较

文献[8]提出了一种基于小波变换的水印算法,该算法嵌入的是二值水印。而本文嵌入的是 256 级灰度水印,嵌入水印信息量大。这点要优于文献[8]的算法。下面使用本文提出的零水印算法做了和文献[8]中相同的实验,并将这两种算法的实验结果进行了比较。

5.1　抗压缩实验结果比较

表 1 是对公开图像进行 JPEG 压缩后,两种算法提取水印相似度的比较(Q 为压缩品质参数)。

表 1 不同质量 JPEG 图像实验结果比较

Tab. 1 Comparison of the results under JPEG attack

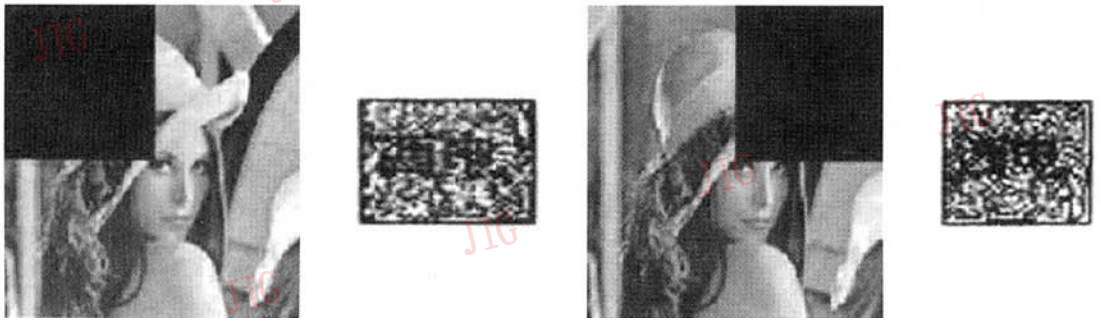
Q(压缩品质)	文献[8]算法相似度	本文算法相似度
10	0.954	1.001
9	0.920	1.001
8	0.787	1.001
7	0.673	1.001

本文算法结果明显优于文献[8]算法的结果。

5.2 抗剪切实验结果比较

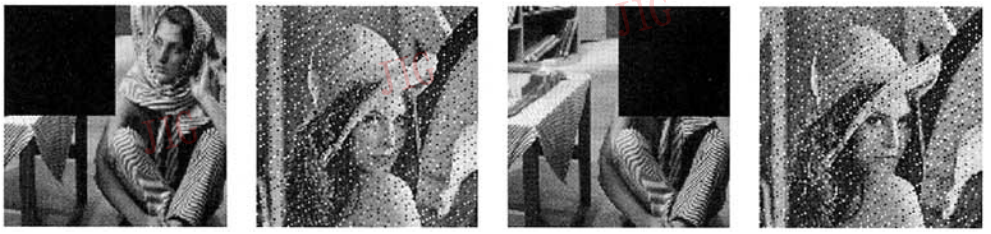
由图 4 的比较可以看到,对公开图像进行 1/4 剪切,剪切部分以黑色代替,文献[8]算法提取出的水印已经不太容易识别,而本文算法提取的水印则可以很容易进行识别。

通过以上实验结果的比较,本文算法在嵌入水印量、抗压缩、抗剪切等方面均优于文献[8]提出的算法。



(a) 剪切掉左上角的图像 (*PSNR* = 13.323dB)　(b) 从(a)中提取水印 (*NC* = 0.678)　(c) 剪切掉右上角的图像 (*PSNR* = 11.409dB)　(d) 从(c)中提取水印 (*NC* = 0.710)

文献[8]实验结果



(e) 剪切掉左上角的图像 (*PSNR* = 10.499dB)　(f) 从(e)中提取水印 (*NC* = 0.987)　(g) 剪切掉右上角的图像 (*PSNR* = 11.461dB)　(h) 从(g)中提取水印 (*NC* = 0.990)

本文实验结果

图 4 抗剪切实验结果比较

Fig. 4 Comparison of the results under crop attack

6 算法的推广

本文利用这种算法来隐藏水印图像,实际上该算法还可以隐藏其他数字图像的信息,而且它隐藏的信息量也比较大,可以推广到数字图像信息的隐藏。利用该算法就可以把一幅 128 × 128pixels 的 256 级灰度图像的信息隐藏在一幅 512 × 512pixels 的 256 级灰度图像中。为了隐藏更多的数字图像信息,可以对公开图像进行一次小波变换。这样,一幅 512 × 512pixles 的 256 级灰度图像就能够隐藏一幅 256 × 256pixles 的 256 级灰度图像的全部信息。

7 结 论

本文提出了一种基于小波变换的零水印算法,同时对该算法进行了一系列实验,并且与另一种水印算法的实验结果进行了比较。通过比较发现,该算法对剪切、涂抹、噪声、压缩等攻击具有很强的鲁棒性。该算法还可以推广到任何数字图像信息的隐

藏,并非仅适用于水印。

参考文献(References)

1 WEN Quan, SUN Tan-fen, WANG Shu-xun. Concept and Application of Zero-Watermark[J]. Acta Electronica Sinica, 2003, **31**(2): 214 ~ 216. [温泉,孙锬锋,王树勋. 零水印的概念与应用[J]. 电子学报, 2003, **31**(2):214 ~ 216.]

2 YANG Shu-guo, LI Chun-xia, SUN Feng, *et al*. Study on the method of image non-watermark in DWT domain[J]. Journal of Image and Graphics, 2003, **8**(6): 664 ~ 669. [杨树国,李春霞,孙枫等. 小波域内的图像零水印技术的研究[J]. 中国图象图形学报, 2003, **8**(6): 664 ~ 669.]

3 YANG Shu-guo, LI Chun-xia, SUN Yao, *et al*. A non-watermark scheme based on discret wavelet transform[J]. Computer Engineering and Applications, 2003, **39**(29): 128 ~ 130. [杨树国,李春霞,孙尧等. 基于小波变换的零水印方案[J]. 计算机工程与应用, 2003, **39**(29): 128 ~ 130.]

4 YANG Hong-mei, ZHANG Chen-ming, ZHANG Wen-yin. A wavelet-based algorithm of zero watermark[J]. Journal of Shandong Agricultural University(Natural Science), 2004, **35**(3): 407 ~ 409. [杨红梅,张承明,张问银. 一种基于小波变换的零水印算法[J]. 山东农业大学学报(自然科学版), 2004, **35**(3): 407 ~ 409.]

5 JI Cheng-li, YANG Xiao-yuan, ZHANG Chong, *et al*. A transform-domain zero-watermark quadric-detecting schema combined with spatial-domain invariants [J]. Computer Engineering, 2004, **30**(14): 105 ~ 107. [季称利,杨晓元,张崇等. 结合空域不变量的变换域零水印二次检测方案[J]. 计算机工程, 2004, **30**(14): 105 ~ 107.]

6 ZHANG Chong, YU Xiao-lin, LIU Jian-ping, *et al*. A new wavelet packet image watermarking scheme combined with zero-watermark [J]. Computer Engineering and Applications, 2004, **40**(27): 84 ~ 87. [张崇,于晓琳,刘建平等. 结合零水印的小波包图像水印方案[J]. 计算机工程与应用, 2004, **40**(27): 84 ~ 87.]

7 JIANG Yu-zhen, YANG Qun-sheng. Research on image non-watermarking algorithms between DCT-domain and DWT-domain[J]. Computer Development & Applications, 2005, **18**(6): 12 ~ 14. [江玉珍,杨群生. 基于 DCT 域和 DWT 域的图像零水印算法的研究[J]. 电脑开发与应用, 2005, **18**(6): 12 ~ 14.]

8 PAN Rong, GAO You-xing. Image watermarking method based on wavelet transform[J]. Journal of Image and Graphics, 2002, **7**(7): 667 ~ 671. [潘蓉,高有行. 基于小波变换的图象水印嵌入方法[J]. 中国图象图形学报, 2002, **7**(7): 667 ~ 671.]