基于混沌的 DWT 域多功能图像数字水印算法

郭 锐[1],朱从旭[1,2]
GUO Rui[1],ZHU Cong-xu[1,2]

1.中南大学 信息科学与工程学院,长沙 410083
2.广东省电子商务市场应用技术重点实验室,广州 510320
1.School of Information Science & Engineering,Central South University,Changsha 410083,China
2.Guangdong Province Key Lab of Electronic Commerce Market Application Technology,Guangzhou 510320,China
E-mail:guorui6962@tom.com

GUO Rui,ZHU Cong-xu.Multipurpose image watermarking algorithm based on chaos and DWT.Computer Engineering and Applications,2008,44(23):83-85.

Abstract: In this paper,a multipurpose image watermarking algorithm based on chaos and DWT (Discrete Wavelet Transform) is proposed.The original watermark is divided into the robust watermark and the semi-fragile watermark for copyright protection and image authentication.According to different applications,the robust watermark is also divided into two kinds of watermark,one has small capacities and relatively high robustness,the other has large capacities and relatively low robustness.They are embedded to different parts of DWT domain,so is the semi-fragile watermark.The security of the watermarks is enhanced by utilizing general cat map to scramble the robust watermark and using Logistic chaotic system to generate the semi-fragile watermark.Simulation results show that watermarked images have good visual quality,the robust watermark can resist common image processing operations,and the semi-fragile watermark can detect and localize precisely the content tampers.
Key words: multipurpose image watermarking;copyright protection;image authentication;chaos

摘 要:提出了一种基于混沌的 DWT 域多功能图像数字水印算法。原始水印分为鲁棒水印和半脆弱水印,分别用于版权保护和图像认证。根据不同的应用,鲁棒水印又分为容量小但鲁棒性要求相对高和容量大但鲁棒性要求相对低的两种,它们和半脆弱水印分别嵌入 DWT 域的不同部分。并利用广义猫映射置乱鲁棒水印和 Logistic 混沌系统生成半脆弱水印以提高安全性。实验表明,嵌入水印后的图像视觉质量好,其中鲁棒水印能抵抗各种常规图像处理,半脆弱水印能准确地检测并定位内容篡改。
关键词:多功能图像数字水印;版权保护;图像认证;混沌
DOI:10.3778/j.issn.1002-8331.2008.23.026 **文章编号**:1002-8331(2008)23-0083-03 **文献标识码**:A **中图分类号**:TP391

1 引言

随着计算机网络和多媒体技术的发展,数字媒体的知识产权保护和认证等问题成为了一个重要而紧迫的研究课题。数字水印技术就是在这种情况下产生的,它为解决这些问题提供了一个有效的途径。现有的图像数字水印可以分为鲁棒水印和脆弱水印两类。鲁棒水印[1]用来版权保护,它要求水印能抵抗各种各样的攻击,而脆弱水印用来图像认证,任何轻微的图像处理都会破坏水印。作为认证水印,半脆弱水印[2]比完全脆弱水印更有实际应用价值,因为这种水印能够区分内容的变化是善意处理还是恶意篡改。目前大多数的图像数字水印算法只能实现单一的保护功能,不能同时拥有版权保护和图像认证功能。近年来,一些同时满足以上两种功能的数字水印算法已经出现,并达到了预期的效果[3-5]。

本文提出了一种基于混沌的 DWT 域多功能图像数字水印算法,该算法利用混沌加密水印以提高安全性,把鲁棒水印和半脆弱水印分别嵌入 DWT 域的不同部分。为了结合某些实际应用,鲁棒水印又分为两部分,一部分水印容量小但鲁棒性要求高一些,例如用户 ID 号;另一部分水印容量大但鲁棒性要求低一些,例如用户信息,它们也分别嵌入 DWT 域的不同部分。鲁棒水印和半脆弱水印都是二值水印。水印检测时不需要原始图像,因此是一种盲水印方案。

2 算法描述

2.1 水印嵌入算法

由于二值水印要嵌入图像小波变换的系数中,本文采用如图 1 所示的量化方法,通过量化函数 $Q(f)$把每一个载体小波

基金项目:广东省电子商务市场应用技术重点实验室开放基金(the Open Foundation of Guangdong Province Key Lab of Electronic Commerce Market Application Technology under Grant No.2007GDECOF003)。
作者简介:郭锐(1981-),男,硕士生,主要研究图像数字水印技术;朱从旭(1963-),男,博士,副教授,CCF 会员,主要研究信息安全理论与技术。
收稿日期:2007-10-18 **修回日期**:2008-01-21

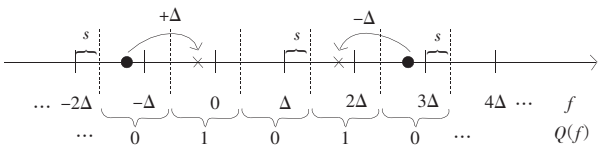

图1 量化策略

系数f映射为0或1。

$$Q(f)=\begin{cases}0,\text{if } 2k\cdot\Delta+s\leqslant f<(2k+1)\cdot\Delta+s\\1,\text{if } (2k+1)\cdot\Delta+s\leqslant f<(2k+2)\cdot\Delta+s\end{cases}\tag{1}$$

其中k是整数,s是自定义的偏移量,用来增加安全性,Δ是量化参数且大于0,在实验中Δ随着嵌入的级数变化而变化。上面的量化函数又可以写为式(2)形式:

$$Q(f)=\begin{cases}0,\text{if } \lfloor f-s/\Delta\rfloor\text{是偶数}\\1,\text{if } \lfloor f-s/\Delta\rfloor\text{是奇数}\end{cases}\tag{2}$$

量化嵌入原理是:假设要嵌入f的水印比特是b,如果$Q(f)=b$,那么不要修改f;如果$Q(f)\neq b$,那么修改f使$Q(f)=b$,修改方法如式(3)所示:

$$f=\begin{cases}f+\Delta, & \text{if } f\leqslant 0\\f-\Delta, & \text{if } f>0\end{cases}\tag{3}$$

2.2 小波多极分解和嵌入系数的选择

小波变换是近几年兴起的一个崭新的信号分析理论,它的基本思想就是对信号进行细致的频率分离即多分辨率分解,图2是一个小波三级分解示意图。通过三级小波变换,原始图像被分解为一个低频近似子图和9个高频细节子图,LL、HL、LH和HH分别表示原始图像的近似、水平方向细节、垂直方向细节和对角方向细节。一般来说,低频近似子图集中了被分解图像的大部分能量,它对图像有着关键的影响,如果应用中对含水印图像的视觉质量要求较高,那么这部分不用来嵌入水印。在实验中使用的载体图像是Lena 512×512的8位灰度图像,表1表示载体图像通过三级Haar小波变换得到的近似子图和细节子图的能量。能量计算公式是式(4)。

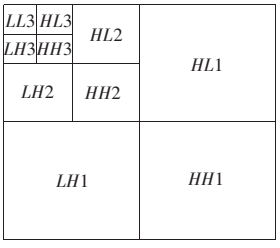

图2 图像小波三级分解图

表1 三级小波分解近似子图和细节子图的能量

子块	1级	2级	3级
近似子图	–	–	3.864
垂直方向细节	0.023	0.062	0.172
水平方向细节	0.016	0.038	0.098
对角方向细节	0.010	0.025	0.066

$$e_k=\frac{1}{N_k\cdot M_k}\sum_i\sum_j|I_k(i,j)|\tag{4}$$

k表示子图所在的级数,I_k表示子块的系数,N_k和M_k表示子块的尺寸。由表1可知级数越高子图含有原始图像的能量越多,另外垂直方向子图又比水平和对角方向子图含有的能量多。因为子图含有的能量越多,嵌入的水印就越鲁棒,而低频近似子图不用来嵌入水印,所以先前提到的鲁棒性要求低而容量大的鲁棒水印嵌入$LH2$,鲁棒性要求高而容量小的鲁棒水印嵌入$LH3$。又因为对角方向子图含有能量最少,最容易受到攻击,考虑到半脆弱水印也要有一定的鲁棒性,所以把它嵌入水平方向子图$HL1$。

2.3 水印的嵌入

在水印嵌入过程中,W_{R1}和W_{R2}分别为大容量鲁棒水印和小容量鲁棒水印,$\boldsymbol{W}_F$为半脆弱水印图像矩阵。其中,W_{R1}和W_{R2}是有意义的二值图像,它们先通过广义猫映射[6]进行置乱,再分别嵌入$LH2$和$LH3$;而$\boldsymbol{W}_F$是由Logistic混沌系统[7]生成的二值矩阵,先用混沌系统预迭代1 000次,以后每迭代一次产生的值用量化函数映射成水印比特,最后把它嵌入$HL1$。

2.4 水印的检测

水印的提取过程也就是以上的逆过程。特别要说的是,在获得两个版本的脆弱水印矩阵$\boldsymbol{W}_{F1}$和$\boldsymbol{W}_{F2}$后,定义如下篡改检测矩阵:

$$\boldsymbol{T}=|\boldsymbol{W}_{F1}-\boldsymbol{W}_{F2}|\tag{5}$$

如果$\boldsymbol{W}_{F1}=\boldsymbol{W}_{F2}$,即$T$=0,这时意味着含水印图像没有遭到篡改。否则,$T$中的“1”元素表示载体图像相应的像素被篡改。

因为半脆弱水印方案要求区分图像内容的变化是善意的图像处理还是恶意的内容篡改引起,水印应该对善意处理(如一般图像处理和传输过程噪声的影响)具有鲁棒性;而对内容的恶意篡改具有脆弱性。考虑到实际中的恶意篡改行为,其攻击目标一般有特定的范围,因此篡改点比较集中;相反,那些对图像善意的处理,其分布一般是全局的,而且应该是基本均匀的。因此,可以先计算出$\boldsymbol{T}$中“1”的个数占元素总个数的比率,即得到全局的平均改变率E_0;然后再计算$\boldsymbol{T}$中每个局部4×4块中“1”的个数占块内元素总数的比率,即得到局部改变率E_1。如果$E_1<qE_0$(q是一个预设的阈值),可以认为该子块的变化是善意处理带来的偶然变化,于是将该4×4子块的值可以全改为“0”;如果$E_1\geqslant qE_0$,则认为该子块的变化是恶意篡改引起的,于是维持$\boldsymbol{T}$中该4×4子块的值不变。通过这种预处理后得到的篡改检测矩阵为$\boldsymbol{T}_1$,则$\boldsymbol{T}_1$中的“1”值点所对应的图像区域将被判定为恶意篡改区。

3 实验结果

实验采用Lena 512×512的8位灰度图像作为宿主图像;用于版权保护的鲁棒水印图像W_{R1}为128×128的“中南大学”字样二值图像,W_{R2}为64×64的“印”字样二值图像,如图3所示;另一个由Logistic混沌系统生成的大小为256×256的二值矩阵将作为半脆弱水印$\boldsymbol{W}_F$。采用两个常用指标值来度量算法的有效性。

图3 原始Lena图像、鲁棒水印W_{R1}和W_{R2}

(1)归一化相似度NC,度量所提取的水印和原始水印的相似程度,其定义为:

$$NC=\frac{\sum_{x=1}^{M}\sum_{y=1}^{M}w(x,y)*\widetilde{w}(x,y)}{\sum_{x=1}^{M}\sum_{y=1}^{M}w(x,y)*w(x,y)}\tag{6}$$

(2)峰值信噪比PSNR,度量隐秘载体图像与原始图像之间的质量差别,其定义为:

$$PSNR=10\lg\frac{N*N*\mathrm{Max}(f^2(x,y))}{\sum_{x=1}^{N}\sum_{y=1}^{N}(f(x,y)-\tilde{f}(x,y))^2} \quad (7)$$

首先考察鲁棒水印的性能。表 2 是在不同攻击下得到的 *NC* 值。图 4 分别是嵌入水印后的载体图像（*PSNR*=45.689 0）和未受攻击时提取的两种鲁棒水印（NC_1=1，NC_2=1（NC_1、NC_2 分别表示大、小容量鲁棒水印的相似度））。图 5 分别是含水印图像受到不同攻击时提取的两种鲁棒水印。其中，图 5(a)JEPG 压缩载体图像（质量参数=75%），NC_1=0.893 0，NC_2=0.903 5；图 5(b)加入高斯噪声（方差=0.01），NC_1=0.783 1，NC_2=0.798 2；图 5(c)加入椒盐噪声（密度=0.02），NC_1=0.851 7，NC_2=0.864 2；图 5(d)中值滤波（5×5 窗口），NC_1=0.953 5，NC_2=0.964 2；图 5(e)中央剪切 14%面积，NC_1=0.993 6，NC_2=0.997 7。

表 2　常见各类攻击下的水印相似度

JPEG 压缩	质参 70%	质参 75%	质参 80%
NC_1	0.846 0	0.893 0	0.920 4
NC_2	0.862 1	0.903 5	0.927 3
高斯噪声	方差 0.01	方差 0.02	方差 0.03
NC_1	0.783 1	0.704 8	0.656 0
NC_2	0.798 2	0.723 6	0.685 7
椒盐噪声	密度 0.02	密度 0.03	密度 0.04
NC_1	0.851 7	0.826 2	0.764 3
NC_2	0.864 2	0.831 8	0.785 9
中值滤波	10 次 3×3	1 次 5×5	1 次 7×7
NC_1	0.979 8	0.953 5	0.909 4
NC_2	0.986 6	0.964 2	0.927 5
图像剪切	中剪 14%	下剪 20%	上剪 49%
NC_1	0.993 6	0.992 1	0.991 2
NC_2	0.997 7	0.996 2	0.995 4

图 4　含水印 Lena 图像和正常提取的两种鲁棒水印

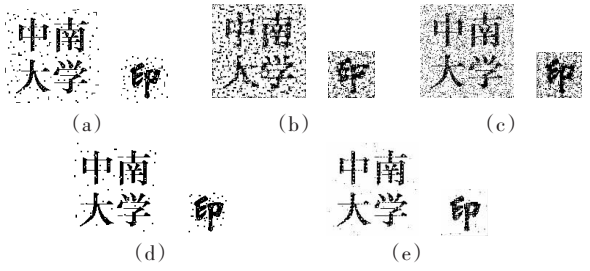

图 5　含水印图像受到不同攻击时提取的水印

然后再考察半脆弱水印的性能。图 6 分别是被恶意篡改的含水印图像和篡改检测矩阵，结果表明，每处篡改都得到检测并精确定位。图 7 分别是受善意处理的含水印图像及其相应预处理后的检测矩阵，结果表明，对于这样的非内容篡改善意处理，算法认为图像没有受到篡改（即内容是真实的）。

(a)图像左上角被剪切了 16%　　(b)在图像上添加了两处文字内容

图 6　被恶意篡改的含水印图像和篡改检测矩阵

(a)图像被 JPEG 压缩（质量参数=75%）　　(b)图像被添加椒盐噪声（密度=0.02）

图 7　受善意处理的含水印图像及其检测结果

4　结论

本文提出了一种 DWT 域多功能图像数字水印算法，具有以下特点：(1)将水印按照不同应用分别嵌入小波域的不同部分；(2)不把鲁棒水印嵌入低频近似子图，含水印图像的视觉质量保持较好；(3)利用混沌系统增加嵌入的安全性；(4)鲁棒水印能抵抗各种常规图像处理，而半脆弱水印能检测图像内容的变化是由善意处理还是恶意篡改引起的。

参考文献：

[1] Cox I J，Kilian J，Leighton F T，et al.Secure spread spectrum watermarking for multimedia[J].IEEE Transactions on Image Processing，1997，6(12)：1673-1687.

[2] Kundur D，Hatzinakos D.Digital watermarking for telltale tamper-proofing and authentication[C]//Proceedings of IEEE，Special Issue：Identification and Protection of Multimedia Information，2001，87(7)：1167-1180.

[3] Lu C S，Liao H Y M.Multipurpose watermarking for image authentication and protection[J].IEEE Transactions on Image Processing，2001，10(10)：1579-1592.

[4] Xiong S H，Zhou J L.A multipurpose image watermarking method based on adaptive quantization of wavelet coefficients[C]//Proceedings of the 1st International Multi-Symposiums on Computer and Computational Sciences(IMSCCS'06).[S.l.]：IEEE Computer Society，2006：294-297.

[5] 朱从旭，陈志刚.基于混沌和小波变换的多功能图像水印算法[C]//第六届全国信息隐藏暨多媒体信息安全学术研讨会论文，2006，38：694-697.

[6] 马在光，邱水生.基于广义猫映射的一种图像加密系统[J].通信学报，2003，24(2)：51-57.

[7] 朱从旭，陈志刚.一种基于混沌映射的空域数字水印新算法[J].中南大学学报：自然科学版，2005，2(36)：272-276.

（上接70 页）

参考文献：

[1] Byeungwoo J，Jeyun L.Fast mode decision for H.264[C]//Pro JVT of ISO/IE CMPEG & ITU-T VCEG 8th Meeting，Hawaii，USA，2003.

[2] Jeyun L，Byeungwoo J.Fast mode decision for H.264 [C]//IEEE International Conference on Multimedia and Expo，2004.

[3] Ri S H，Ostermann J.Fast mode decision for H.264/AVC using mode prediction[C]//Blanc-Talon J.LNCS 4176：ACIVS 2006，2006：254-263.

[4] Zhou Zhi，Xin Jun，Sun Ming-ting.Fast motion estimation and Inter-mode decision for H.264/MPEG-4 AVC encoding[J].Journal of Visual Communication and Image Representation，Vis Commun Image R，2006(17)：243-263.

[5] JVT reference software version 12.2[S/OL].(2005-01-24).http://ftp3.itu.ch/av_arch/jvt_site/reference_sof tware.