

# 一种半脆弱数字水印算法

樊洁, 李建军

(内蒙古科技大学 信息工程学院, 内蒙古 包头 014010)

**摘要:**随着移动设备的广泛使用,利用微信、QQ、邮箱等APP平台传播多媒体数据越来越便捷。为了保护多媒体数据的完整性,并对多媒体数据的完整性进行认证,数字水印技术应运而生。针对完整性认证和篡改定位,提出了一种半脆弱数字水印算法。通过将原始图像进行整数小波变换,以避免浮点数的舍入误差;将图像进行二级整数小波变换,利用矩阵范数量化方法,将水印嵌入到整数小波域的中、高频细节子带中;采用 Logistic 混沌序列对水印信息进行加密,以达到提高水印安全性的目的。再利用整数小波逆变换,得到含水印图像。通过涂改、剪切、压缩、加噪等常用攻击方法,实验结果表明,算法兼具鲁棒性、脆弱敏感性,能够准确定位篡改区域,是一种有效的半脆弱数字水印方案。

**关键词:**半脆弱数字水印;整数小波;矩阵范数量化;奇异值分解;混沌置乱

**中图分类号:**TP391

**文献标识码:**A

**文章编号:**1673-629X(2017)02-0069-03

**doi:**10.3969/j.issn.1673-629X.2017.02.016

## A Semi-fragile Digital Watermarking Algorithm

FAN Jie, LI Jian-jun

(School of Information Engineering, Inner Mongolia University of Science and Technology, Baotou 014010, China)

**Abstract:** With the widespread use of mobile devices, WeChat, QQ, mail and other APP platform to spread multimedia data is more convenient. In order to protect and authenticate the integrity of the multimedia data, the digital watermarking technology is emerged. Aiming at its integrity authentication and tamper location, a semi-fragile digital watermarking algorithm is proposed. Integer wavelet transform is made for the original image to avoid rounding error of floating-point numbers, and that of second level is conducted for image to embed watermarks to intermediate and high frequency progeny details of integer wavelet domain with matrix norm quantization. In order to guarantee the security of watermark, the watermark information is encrypted by the Logistic chaotic sequence. Then the inverse integrated wavelet transform is applied to obtain the watermarking image. By altering, shearing, compression, noise adding and other common attack methods, the experiments show the algorithm has both robustness and sensitivity, and also exactly locates distorted parts, which is an effective semi-fragile digital watermarking method.

**Key words:** semi-fragile digital watermarking; integer wavelet; matrix norm quantization; SVD; chaotic scrambling

## 0 引言

随着网络技术的发展,多媒体信息很容易被篡改,因此多媒体数据的完整性和真实性越来越受重视。基于此,需要对多媒体数据进行保护和认证,数字水印技术中的一个分类—认证水印技术可以很好地完成这项任务。

文献[1]把水印进行分块,将分块的水印信息嵌入到原图的空域中,并进行 Hash 函数置乱,然后进行异或运算得到含水印图像;文献[2]研究了半脆弱数字水印算法,将图像进行小波变换后嵌入水印信息;文献[3]对于抗 JPEG 压缩攻击设计了半脆弱水印;文献

[4]将原始图像进行奇异值分解,在图像的奇异值中嵌入水印信息。

半脆弱水印的特点是具有鲁棒性,同时具有脆弱敏感性。文中通过将原始图像进行整数小波变换,以避免浮点数的舍入误差;将图像进行二级整数小波变换,利用矩阵范数量化方法,将水印嵌入到整数小波域的中、高频细节子带中;采用 Logistic 混沌序列对水印信息进行加密,以达到提高水印安全性的目的。然后利用整数小波逆变换,得到含水印图像。通过涂改、剪切、压缩、加噪等常用攻击方法,实验结果表明,算法能够准确定位篡改区域。

收稿日期:2015-12-02

修回日期:2016-04-20

网络出版时间:2017-01-10

基金项目:中央高校基本科研业务专项资金项目(GK201504017);包头市科学技术项目(2014S2001-2-1-15)

作者简介:樊洁(1991-),女,硕士,研究方向为计算机应用技术、信号处理等。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20170110.0941.004.html>

## 1 相关理论

### 1.1 奇异值、矩阵范数

若矩阵  $A \in R^{m \times n}$  非负, 则

$$A = USV^T \quad (1)$$

$$U^T A V = S = \text{diag}(\sigma_1, \sigma_2, \dots, \sigma_p) \quad (2)$$

其中,  $p = \min(m, n)$ ;  $\sigma_i$  为  $A$  的奇异值, 满足  $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_p$ ;  $U, V$  是奇异值向量。

定义: 矩阵  $A$  的 2-范数和 F-范数定义如下<sup>[5]</sup>:

$$\|A\|_2 = \sqrt{\lambda_{\max}(A^T A)} = \sigma_1 \quad (3)$$

$$\|A\|_F = \sqrt{\sum_{i=1}^m \sum_{j=1}^n a_{ij}^2} = \sqrt{\sum_{i=1}^p \lambda_i} = \sqrt{\sigma_1^2 + \sigma_2^2 + \dots + \sigma_p^2} \quad (4)$$

矩阵的 2-范数是奇异值得最大值, 矩阵的 F-范数是所有奇异值的平方和。

### 1.2 整数小波变换

传统小波变换的计算量较大, 具有浮点数舍入误差<sup>[6]</sup>。整数小波变换 (LWT) 可以克服上述问题。LWT 变换后系数是整数, 计算速度较快<sup>[7]</sup>。整数小波变换在经典小波变换的基础上经过分裂、预测和更新得到整数小波变换过程<sup>[8]</sup>, 如图 1 所示。

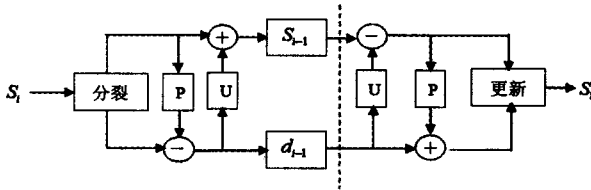


图 1 整数小波变换

## 2 一种半脆弱数字水印算法

采用 LWT 以避免浮点数的舍入误差。由于图像的低频参数具有鲁棒性、高频系数具有脆弱性、中频系数介于二者之间, 文中在原始图像整数小波域的中、高频细节子带中嵌入水印, 以保证鲁棒性、脆弱敏感性。为使篡改定位精准, 将各细节子带进行分块, 计算各块矩阵的 2-范数, 在 2-范数值中嵌入水印信息。采用 Logistic 混沌序列对水印加密, 保证水印的安全性。

图 2 为水印嵌入过程。

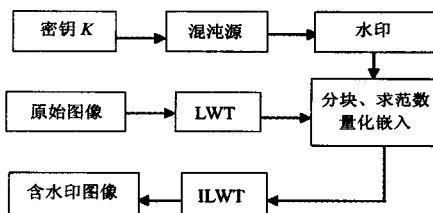


图 2 水印嵌入过程

第一步: 利用 Logistic 混沌序列对水印进行加密。

Logistic 混沌序列产生:

$$x_{k+1} = \mu x_k (1 - x_k) \quad (5)$$

其中, 分支参数  $\mu \in (3.569\ 945, 4]$ ;  $x_i \in (0, 1)$ 。

设定初值  $x_0$ 、分支参数  $\mu$ , 密钥为  $K(x_0, \mu)$ , 生成混沌序列  $X$ , 加密水印  $W$  具体过程如下:

(1) 将序列  $X$  重新进行升序排列, 得到  $X'$ 、索引序列  $l$ 。

$$[X', l] = \text{sort}(X) \quad (6)$$

(2) 将  $l$  按列排列变成二维矩阵  $L$ 。

(3) 根据矩阵  $L$  重排原始水印  $W$ , 将水印  $W$  置乱。

第二步: 整数小波变换。

首先选用 9/7 正交小波基, 将原始图像  $I$  进行二级整数小波变换, 得到 7 个子带:  $HL_2, LH_2, HH_2, HL_1, LH_1, HH_1, LL_1$ 。

第三步: 嵌入水印。

(1) 首先在各层细节子带 ( $HL_2, LH_2, HH_2, HL_1, LH_1, HH_1, LL_1$ ) 进行  $q \times q$  的分块, 记为  $I_g \in R^{q \times q}$ 。计算: 2-范数  $\|I_g\|_2$ , 量化系数  $\lambda = \lfloor \frac{\|I_g\|_2}{\delta} \rfloor$ 、控制系数  $\gamma = \|I_g\|_2 - \lambda \delta$  ( $\delta$  为基于人类视觉掩蔽特性设定的量化步长<sup>[9]</sup>)。

(2) 修改矩阵 2-范数。

如果  $(\lambda + W_1) \bmod 2 = 1$  且  $\gamma < \delta/2$ , 记  $\tilde{\|I_g\|_2} = (\lambda - 1/2)\delta$ ; 若  $(\lambda + W_1) \bmod 2 = 1$  且  $\gamma \geq \delta/2$ , 记  $\tilde{\|I_g\|_2} = (\lambda + 3/2)\delta$ ; 否则, 记  $\tilde{\|I_g\|_2} = (\lambda + 1/2)\delta$ 。

(3) 修改水印参数<sup>[10]</sup>。

$$\tilde{I}_g = I_g + t I_g \quad (7)$$

其中,  $t$  为修正量, 取值为:

$$t = (\tilde{\|I_g\|_2} / \|I_g\|_2) - 1 \quad (8)$$

则

$$\tilde{I}_g = (\tilde{\|I_g\|_2} / \|I_g\|_2) I_g \quad (9)$$

第四步: 进行 2 级整数小波逆变换得到含水印图像  $I'$ 。

提取水印过程如下:

(1) 对待检测图像进行 LWT。

(2) 提取水印。

将每个细节子带 ( $HL_2, LH_2, HH_2, HL_1, LH_1, HH_1, LL_1$ ) 进行  $q \times q$  分块, 每一块记为  $I_g'$ , 并计算:  $\|I_g'\|_2$ ,  $\lambda_i' = \lfloor \frac{\|I_g'\|_2}{\delta} \rfloor$ 。如果  $\lambda_i' \bmod 2 = 1$ , 则  $w_i' = 1$ ; 如果  $\lambda_i' \bmod 2 = 0$ , 则  $w_i' = 0$ 。排列  $w_i'$  得到置乱的水印  $W''$ 。

(3) 对水印进行解密。

通过 Logistic 混沌序列逆排序将提取出的置乱水印进行解密, 得到水印  $W^*$ , 通过主观判断水印是否被

篡改;此外,采用相关检测函数 (SIM)、篡改评估函数 (  $T_{AF}$  ) 来判断水印的篡改程度。

$$SIM(W,W^*)=\frac{\sum_{i=1}^m\sum_{j=1}^n(W(i,j)\times W^*(i,j))}{\sqrt{\sum_{i=1}^m\sum_{j=1}^n(W^*(i,j))^2}}\quad(10)$$

$$T_{AF}(W,W^*)=\frac{1}{m\times n}\sum_{i=1}^m\sum_{j=1}^nW(i,j)\oplus W^*(i,j)\quad(11)$$

3 实验仿真

文中采用 Matlab 平台,选用标准灰度图像 Lena、Boat、Cameraman 等进行实验<sup>[11-12]</sup>。以 Lena(512×512)灰度图像为例,水印嵌入如图 3 所示。

为了检测该算法的鲁棒性和脆弱性,对含水印图像进行涂改攻击、剪切攻击、JPEG 压缩攻击以及加噪攻击等<sup>[8,13]</sup>。图 4 为受到攻击后提取的水印图像。



图 3 水印嵌入



图 4 受攻击后提取的水印图像

表 1 为半脆弱水印相关检测值和篡改可信度。通过图 4 和表 1 可见,该算法可以对篡改区域进行定位,且可抵抗以上常用攻击。

表 1 受到攻击后提取出水印的 SIM 值和  $T_{AF}$  值

攻击类型	小波域中频提取出的水印		小波域高频提取出的水印	
	SIM	$T_{AF}$	SIM	$T_{AF}$
破坏性涂改	0.992 289 899	19.559 422 943	0.990 543 735 2	17.884 512 070 2
平滑涂改	0.992 675 404 7	19.076 376 147	0.968 085 106 3	18.539 527 557 79
剪切攻击	0.989 361 702 1	18.246 633 796	0.985 736 314 5	17.239 932 177 96
80% JPEG 压缩	0.952 197 378 5	12.725 773 633	0.722 222 222 2	4.339 586 064 340
加高斯噪声	0.983 423 284	17.092 699 609	0.926 713 947 9	14.961 951 356 6
加椒盐噪声	0.936 391 673	11.907 560 210	0.917 257 683 2	11.714 508 659 02

4 结束语

提出了一种半脆弱数字水印算法。对水印进行 Logistic 混沌置乱加密,保证了算法的安全性;为了避免浮点数舍入误差,采用整数小波变换,在小波域的不同层细节子带的奇异值中嵌入水印;采用在矩阵 2-范数中嵌入水印,方法简单可行,计算量小;通过对各层频带分块嵌入水印,可以较精确定位图像篡改区域。

在 Matlab 平台进行了实验仿真,结果表明该算法对于常见攻击具有一定的鲁棒性,而且可以定位篡改区域,是一种有效的半脆弱数字水印算法。

参考文献:

[1] Wong P W. A public key watermark for image verification and authentication [ C ]//Proceedings of the IEEE international conference on image processing. Chicago, Illinois, USA: IEEE, 1998:455-459.

[2] Kundur D, Hatzinakos D. Digital watermarking for telltale tamper proofing and authentication [ C ]//Proceedings of the IEEE special issue on identification and protection of multimedia information. [ s. l. ]: IEEE, 1999:1167-1180.

[3] 董 刚,张 良,张春田. 一种半脆弱性数字图像水印算法

[J]. 通信学报,2003,24(1):33-38.

[4] 陈 帆,和红杰,朱大勇. 基于图像奇异值的脆弱水印方案 [J]. 计算机应用,2006,26(1):93-95.

[5] Zhou B, Chen J. A geometric distortion resilient image watermarking algorithm based on SVD [J]. Journal of Image and Graphics, 2004, 9(4):506-512.

[6] Bergman C, Davidson J. Unitary embedding for data hiding with the SVD [ C ]//Proceedings of SPIE on security steganography and watermarking of multimedia. San Jose, CA: [ s. n. ], 2005.

[7] 张宪海,杨永田. 基于 DFT-SVD 域抗几何攻击图像水印算法 [J]. 计算机工程,2006,32(18):120-121.

[8] 李旭东,张振跃. 利用矩阵范数实现的公开水印技术 [J]. 计算机辅助设计与图形学学报,2005,17(8):1857-1861.

[9] 张小华,孟红云,刘 芳,等. 一类有效的脆弱型数字水印技术 [J]. 电子学报,2004,32(1):114-117.

[10] 王丽君,刘宏斌,王克刚,等. 多目的的图像水印方案 [J]. 计算机工程与应用,2008,44(4):104-106.

[11] 刘九芬,黄达人,胡军全. 数字水印中的双正交小波基 [J]. 中山大学学报:自然科学版,2002,41(4):1-4.

[12] 肖 亮,韦志辉,吴慧中. 一种利用人眼视觉掩盖的小波域数字水印 [J]. 通信学报,2002,23(3):100-106.

[13] 徐 仲,张凯院,陆 全,等. 矩阵论简明教程 [ M ]. 第 2 版. 北京:科学出版社,2005:27-30.