数字高程模型数据整数小波水印算法*

罗 永+, 成礼智, 陈 波, 吴 翊

(国防科学技术大学 理学院,湖南 长沙 410073)

Study on Digital Elevation Mode Data Watermark via Integer Wavelets

LUO Yong+, CHENG Li-Zhi, CHEN Bo, WU Yi

(College of Science, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: Phn: +86-731-4215550, E-mail: yngluo@163.com, http://www.nudt.edu.cn

Received 2003-12-31; Accepted 2004-06-10

Luo Y, Cheng LZ, Chen B, Wu Y. Study on digital elevation mode data watermark via integer wavelets. *Journal of Software*, 2005,16(6):1096−1103. DOI: 10.1360/jos161096

Abstract: In this paper an efficient approach via wavelet for digital watermark in DEM(digital elevation mode) data is developed, which effectly protects the copyright of DEM data and avoids the unauthoritative user. A technique based on lifting scheme is presented to construct the compactly supported wavelets whose coefficients are composed of a free variable. When t=1, the integer wavelets based on lifting scheme only use integral addition and shift, so it's fast and easily realized via hardware. A method is presented to build the wavelet coefficient set which can embed watermark information. The bit is inserted in the high activity texture regions with the maximum strength of Just Noticeable Distortion (JND) tolerance of Human Visual System (HVS). Keeping the terrain figure and hypsography, the digital watermark is robust. A hash one-way is constructed by the Rabin method, and the digital watermark arithmetic can be public.

Key words: digital elevation mode; lifting scheme; integer wavelets with parameter; digital watermark

摘 要: 提出了一种高效、安全的数字高程模型(digital elevation mode,简称 DEM)数据小波水印算法,以解决 DEM 数据版权保护和限制非法使用的问题.在理论上,基于提升理论构造了一种包含自由变量 t 的紧支撑小波,选取参数 t=1 的 9/7 整数小波基,只需要整数加法和移位实现,运算量低,便于硬件实现.提出可嵌入水印的小波系数集生成方法,扩展了基于视觉系统(HVS)小波域量化噪声的视觉权重(JND)分析方法,使其适用于 DEM 数据,并能够自适应地确定水印嵌入的强度.该算法在保证地形形状和起伏特征的前提下,提高了水印的鲁棒性.应用 Rabin 方法生成的单向 Hash 函数,水印算法可以完全公开.

关键词: 数字高程模型;提升理论;带参数整数小波变换;数字水印

* Supported by the National Natural Science Foundation of China under Grant No.10171109 (国家自然科学基金); the Defense Pre-Research Project of the 'Ninth Five-Year-Plan' of China (国家"九五"国防预研基金); the National Research Foundation for the Doctoral Program of Ministry of Education of China under Grant No.20049998006 (国家教育部博士点基金)

作者简介: **罗永**(1976−),男,湖南益阳人,博士生,主要研究领域为应用数学,信息安全,信号与图像处理;**成礼智**(1962−),男,博士,教授,博士生导师,主要研究领域为信息科学中新型算法与软件,小波变换与图像处理,应用数学;**陈波**(1981−),男,主要研究领域为图像压缩,小波理论;**吴翊**(1948−),男,教授,主要研究领域为应用数学,统计,数据处理.

中图法分类号: TP309 文献标识码: A

数字地形模型(digital terrain mode,简称 DTM)[1]是以数字的形式按一定的结构组织在一起,表示实际地形特征的空间分布模型.DTM 主要由栅格(regular square grid,简称 RSG)与不规则三角网(triangulated irregular networks,简称 TIN)两种数据格式表示.这两种格式的数据本质相同,都是地形形状大小和起伏特征的数字描述.

按照平面上等间距规划采样或内插所建立的 DTM,称为栅格数据的 DTM,可以写成矩阵形式:

$$\begin{bmatrix} Z_{00} & Z_{01} & \cdots & Z_{0(n-1)} \\ Z_{10} & Z_{11} & \cdots & Z_{1(n-1)} \\ \cdots & \cdots & \cdots & \cdots \\ Z_{(n-1)0} & Z_{(n-1)1} & \cdots & Z_{(n-1)(n-1)} \end{bmatrix},$$

其中 Z_{ij} 为格网结点 i, j 上的地形属性数据,当该属性为海拔高程时,该模型称为数字高程模型(digital elevation mode,简称 DEM),如图 1 所示.现实中,DEM 应用十分广泛.

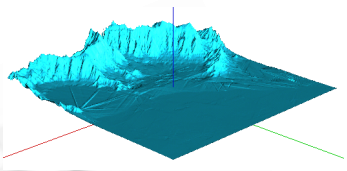


Fig.1 3-D show of DEM data

图 1 DEM 数据三维显示图

由于 DEM 数据具有很高的经济和军事应用价值,对其进行保护很有必要.一方面需要保护其版权,使得知识产权拥有者能够获得相应的经济利益;另一方面,需要保证其安全,非法用户不能正确使用数据.现在大部分的研究集中在 DTM 数据的生成方式[1]上,一些学者采用信息隐藏技术对不规则三角网数据的保护进行了研究[2,3].本文应用小波数字水印技术实现 DEM 数据保护.本文主要研究基于整数小波变换的 DEM 数据数字水印技术,采用小波变换来实现信息的隐藏和提取.这项研究不同于一般的图像数字水印,由于 DEM 数据记录的是实际的海拔高度,数据取值范围可以从–11034(马里亚纳海沟)到 8848(珠穆朗玛峰),且为浮点.该项研究的难点在于:一方面,在保证水印安全的同时,如何保证数据的精度,另一方面,由于数据取值范围大(至少需要 4 个字节记录一个数据),为浮点数据,因此降低硬件实现成本也是一个很重要的问题.但这项研究是很有意义的:将版权标志以数字水印的方式嵌入到 DEM 数据中,可以保护数据的版权;将数据的重要参数(数据的地理坐标等)隐藏起来,就可以限制非法用户的使用(没有这些参数,数据没有任何价值),从而解决 DEM 数据的安全问题.

数字水印的概念最早出现于 1994 年的图像处理会议(ICIP'94)[4].数字水印是指在数字化的数据内容中嵌入不明显的记号,通过一些计算操作可以被检测或者被提取.其水印与源数据紧密结合并隐藏其中,成为源数据不可分离的一部分.本项研究中,源数据是 DEM 数据,水印数据是版权标志或者是 DEM 数据重要的参数信息.嵌入水印的过程保证 DEM 数据描述的地形信息基本不变(保持地形形状和地面起伏状态).

DEM 数据的生成与显示都可能不在 PC 上,其水印算法的硬件实现是必要的.为了降低硬件实现的成本,设计低成本高效率的水印算法非常重要.本文基于提升理论构造了带一个自由变量 t 的整数小波变换,参数 t 在一定范围内的变化总可以构成小波.选取 $t=1$ 整数小波基,它只需要作一次提升,运算量低,且只需要整数移位和加法,便于硬件实现.

通过抬升 DEM 数据小数位(放大 DEM 数据),保持了 DEM 数据的精度.扩展了 Watson[5]的基于视觉系统(HVS)小波域量化噪声的视觉权重(JND)分析,使其适用于 DEM 数据.通过对 JND 合理的缩放,自适应地确定水印嵌入的强度.在保证地形形状和起伏特征的前提下,提高了水印的鲁棒性.

为了提高水印算法的通用性和安全性,本文提出了一种可嵌入水印的小波系数集生成方法,应用 Rabin 方法生成单向 Hash 函数[6],可以将水印算法完全公开.对于合法用户和版权拥有者,只要密钥不泄漏,就能保证数据的安全.

1 小波构造理论

1.1 应用提升理论构造对称双正交小波滤波器

本文将设计双正交小波对称 9/7 完全重构滤波器作为例子,其他类型的完全重构滤波器的构造方法类似.

由于消失矩条件是构造小波的必要条件[7−13],因此获得对称双正交小波完全重构滤波器$\{h,g,\tilde{h},\tilde{g}\}$,消失矩条件是必要的.设 N 和 $\tilde{N}$ 分别表示小波及其对偶的消失矩长度,也就是 $h^{(k)}(-1)=0,k=0,1,...,N-1$ 和 $g^{(k)}(1)=0,k=0,1,...,\tilde{N}-1$[8−10].

对于 9/7 对称双正交小波完全重构滤波器,设 $h_k=h_{-k}$ 和 $\tilde{h}_k=\tilde{h}_{-k}$, $k=0,1,2,3,4$[12],得到

$$\begin{cases}h_e(z)=h_0+h_2(z+z^{-1})+h_4(z^2+z^{-2})\\ h_o(z)=h_1(z+1)+h_3(z^2+z^{-1})\end{cases}\text{和}\begin{cases}g_e(z)=-\tilde{h}_o(z^{-1})=-[\tilde{h}_1(1+z^{-1})+\tilde{h}_3(z+z^{-2})]\\ g_o(z)=\tilde{h}_e(z^{-1})=\tilde{h}_0+\tilde{h}_2(z+z^{-1})\end{cases}\tag{1}$$

下面对于 h_3 取值,分两种情形讨论 9/7 滤波器的提升分解.

A. 当 $h_3\neq 0$ 时,应用 Euclidean 算法,得到下面的提升结构

$$P(z)=\begin{bmatrix}h_e(z) & g_e(z)\\ h_o(z) & g_o(z)\end{bmatrix}=\begin{pmatrix}1 & \alpha(1+z^{-1})\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ \beta(1+z) & 1\end{pmatrix}\begin{pmatrix}1 & \gamma(1+z^{-1})\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ \delta(1+z) & 1\end{pmatrix}\begin{pmatrix}\varsigma & 0\\ 0 & \frac{1}{\varsigma}\end{pmatrix}\tag{2}$$

对于任何给定的系数 $h_k=h_{-k}$ 和 $\tilde{h}_k=\tilde{h}_{-k}$,式(1)并不是构成小波的充分条件.为了获得 9/7 小波滤波器,还需要引入一个新的条件:消失矩满足 $N=2$ 和 $\tilde{N}=4$[12],得到

$$h^{(k)}(z)|_{z=-1}=0,k=0,1\text{ 和 }g^{(k)}(z)|_{z=1}=0,k=0,1,2,3\tag{3}$$

比较式(1)和式(2),得到

$$\left.\begin{aligned}h(z)&=\alpha\beta\gamma\delta\varsigma(z^{-4}+z^4)+\beta\gamma\delta\varsigma(z^{-3}+z^3)+\varsigma(\alpha\beta+\alpha\delta+\gamma\delta+4\alpha\beta\gamma\delta)(z^{-2}+z^2)\\ &+\varsigma(\beta+\delta+3\beta\gamma\delta)(z^{-1}+z)+\varsigma(1+2\alpha\beta+2\alpha\delta+2\gamma\delta+6\alpha\beta\gamma\delta)\\ \varsigma g(z)&=\alpha\beta\gamma(z^{-4}+z^2)+\beta\gamma(z^{-3}+z)+(\alpha+\gamma+3\alpha\beta\gamma)(z^{-2}+1)+(1+2\beta\gamma)z^{-1}\end{aligned}\right\}\tag{4}$$

基于消失矩条件等式(3)和归一化条件 $h(1)=2$, $\tilde{h}(1)=1$,得到下面包含 5 个方程的方程组,

$$\left.\begin{aligned}&1+\delta(4\alpha+4\gamma-2)+2(2\alpha-1)\beta(1+4\gamma\delta)=0\\ &1+2\alpha+2\gamma+4\beta\gamma+8\alpha\beta\gamma=0\\ &2+6\alpha+6\gamma+16\beta\gamma+40\alpha\beta\gamma=0\\ &[1+\delta(4\alpha+4\gamma+2)+2(2\alpha+1)\beta(4\gamma\delta+1)]\varsigma=2\\ &1+(4\beta-2)\gamma-2\alpha(1+4\beta\gamma)=\varsigma\end{aligned}\right\}\tag{5}$$

方程的解能够表示为

$$\alpha=\frac{-2t+1}{4(t-1)},\beta=-(t-1)^2,\gamma=\frac{1}{4t(t-1)},\delta=t^3-\frac{7}{4}t^2+t,\varsigma=\frac{2}{t}\tag{6}$$

由式(3)~式(6),得到了一个带有自由变量 t 的双正交 9/7 完全重构滤波器.

为了得到双正交 9/7 小波滤波器,需要应用 Daubechies 不等式[7,10]来确定参数 t 的范围.首先,定义 $h_9(z)=\left(\frac{1+z^{-1}}{2}\right)^2F(z)$ 和 $\tilde{h}_7(z)=\left(\frac{1+z^{-1}}{2}\right)^4Q(z)$,这里 $F(z)$和 $Q(z)$都是包含参数 t 的多项式.对于整数 k,解如下的不等式:

$$B_k=\sup_{t\in R,|z|=1}|F(z)F(z^2)...F(z^{2^{k-1}})|<2^{\frac{3}{2}},\overline{B}_k=\sup_{t\in R,|z|=1}|Q(z)Q(z^2)...Q(z^{2^{k-1}})|<2^{\frac{7}{2}}\tag{7}$$

当 k=40 时,得到当 $t\in[0.780,1)\cup(1,1.852]$,式(7)满足.基于式(3)~式(6)提供的系数,总能够获得双正交 9/7 小波.特别地,如果取 $t=1.230174$,就得到了著名的 CDF9/7 小波[10].

B. $h_3=0$,此时,9/7 滤波器多相表示为

$$\begin{cases}h_e(z)=h_0+h_2(z+z^{-1})+h_4(z^2+z^{-2})\\ h_o(z)=h_1(z+1)\end{cases},$$

相应提升分解为

$$P(z)=\begin{bmatrix}1 & -\frac{9}{16}(1+z^{-1})+\frac{1}{16}(z+z^{-2})\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ \frac{1}{4}(1+z) & 1\end{bmatrix}\begin{bmatrix}2 & 0\\ 0 & \frac{1}{2}\end{bmatrix}\tag{8}$$

9/7 滤波器系数满足

$$\begin{cases} h_0=\dfrac{23}{32},\quad h_1=h_{-1}=\dfrac{1}{4},\quad h_2=h_{-2}=-\dfrac{1}{8},\quad h_3=h_{-3}=0,\quad h_4=h_{-4}=\dfrac{1}{64}; \\ \tilde{h}_0=\dfrac{1}{2},\quad \tilde{h}_1=\tilde{h}_{-1}=\dfrac{9}{32},\quad \tilde{h}_2=\tilde{h}_{-2}=0,\quad \tilde{h}_3=\tilde{h}_{-3}=-\dfrac{1}{32}; \end{cases} \tag{9}$$

式(9)实际上为一个 7-5 小波滤波器,对应于式(6)中 t=1 的情形.

式(9)对应的整数小波变换(记为 9/7-1 小波),由式(8)可知仅经过了一次提升,算法结构简单.并且小波系数的分母都是 2 的幂,从而整数除法只需要移位就可以完成.整数乘法分解为移位和加法实现,如$(\cdot\times 5)$可以分解为$(\cdot\times 4+\cdot)$,$(\cdot\times 4)$为(·左移 2 位).以上特点表明,该小波变换非常有利于硬件实现.

1.2 小波运算量分析

根据 JPEG 2000 中的要求,CDF 9/7 小波的运算过程中需要保留其系数的十进制小数 15 位,若采用提升格式,每个像素在每一提升步需要 6 次浮点乘法,8 次浮点加法.为了实现小波的整数实现,JPEG 2000 建议采用 2000 年 Admas 在提出的整数 9/7 小波(记为 9/7-F),计算格式为

$$9/7-\mathrm{F}\begin{cases} d_1(n)=d_0(n)+\left\lfloor\dfrac{1}{128}(203(s_0(n+1)-s_0(n)))+\dfrac{1}{2}\right\rfloor \\ s_1(n)=s_0(n)+\left\lfloor\dfrac{1}{4096}(217(-d_1(n)-d_1(n-1)))+\dfrac{1}{2}\right\rfloor \\ d(n)=d_1(n)+\left\lfloor\dfrac{1}{128}(113(s_1(n+1)+s_1(n)))+\dfrac{1}{2}\right\rfloor \\ s(n)=s_1(n)+\left\lfloor\dfrac{1}{4096}(1817(d_1(n)+d_1(n-1)))+\dfrac{1}{2}\right\rfloor \end{cases}.$$

如果通过移位和加法来计算上式,每个像素点每一提升步至少需要 21 个加法与 16 次移位.而对于参数取 t=1 对应的简单系数 9/7 小波的提升格式,需要 8 次移位和 8 次加法,9/7-F 小波所需要的加法与移位分别为 9/7-1 小波对应运算的 2.5 倍和 2 倍.同时,注意到 9/7-1 小波的提升格式分解中分数之分母最大的仅为 16,远小于 9/7-F 小波所给出的 4096,因此,9/7-1 小波比 9/7-F 小波更适合于硬件实现.各种不同小波所需运算量在表 1 中列出.

Table 1 Comparison of the wavelets operation performance

表 1 小波的运算量比较

Operation	CDF 9/7(float)	9/7-1	9/7-F(JPEG 2000 standard)
Integer addition	0	34.125	102.056
Integer move	0	23.625	28.125
Float addition	10.500	0	0
Float multiplication	7.875	0	0

2 适用于 DEM 数据的小波域量化噪声的视觉权重分析

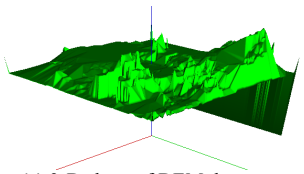
在使水印具有更强的抗攻击能力的同时,满足不可见性,引入了基于视觉系统(HVS)小波域量化噪声的视觉权重分析.Watson 对双正交 9/7 小波在图像压缩中的量化噪声进行了研究,给出了不同子带的视觉模型[5]:

$$Q_{l,f}=\frac{2}{A_{l,f}}a10^{l\left(\log\frac{2^l f_0 g_f}{r}\right)^2}.$$

上面的模型是针对图像进行的分析,图像的灰度取值范围是[0~255]的整数,而 DEM 数据是用浮点数记录的实际地形的海拔(海拔最高的珠穆朗玛峰为 8848 米,低于海平面则取负值).因此 Watson 的视觉模型不能直接应用到 DEM 数据.但是由于 DEM 数据可以视为用灰度来描述地形起伏特征的图像,所以可以通过对量化因子的调整,将该模型拓展到 DEM 数据上来.

图 2(a)为 DEM 数据的三维显示图像,图 2(b)是数字高程模型数据归一化到[0~255]整数以后,数字图像模拟显示.为了保证 DEM 数据的精度,在嵌入水印过程中,并不是将其归一化到[0~255],而是要放大 DEM 数据抬升

小数位(如×10000 抬升 4 位小数).同时采用对量化因子作缩放调整的方式,以适应 DEM 数据.



(a) 3-D show of DEM data
(a) DEM 数据三维显示图

(b) 2-D show of digital image transformed from DEM data
(b) DEM 数据转化为二维数字图像

Fig.2 The show of 3-D DEM data and 2-D digital image
图 2 DEM 数据三维显示与二维数字图像显示

根据 Watson 的视觉模型,设 l 表示多分辨分解的层数,这里 l=1,2,3,4;f 表示频率方向,f=1,2,3 分别表示水平、垂直、对角方向的细节子图;$A_{l,f}$ 为各个子带的基函数;r 为显示视觉分辨率;α 定义为最小域值,取 α =0.495 的函数,定义为

$$g_f=\begin{cases}1, & f=1\\ 1, & f=1\\ 0.534, & f=3\end{cases}.$$

这样,得到不引起图像失真的各级小波系数的量化因子,见表 2.

Table 2 Quantizing factor of four levels bi-orthogonal 9/7 wavelets transform in image
表 2 图像双正交 9/7 小波 4 级小波变换的量化因子

l	f=1	f=2	f=3
1	23.03	58.76	23.03
2	14.68	28.41	14.69
3	12.71	19.54	12.71
4	14.16	17.68	14.16

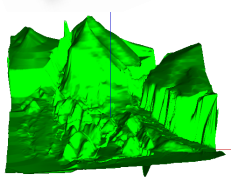
由于图像的量化矩阵是根据人眼的视觉系统(HVS)提出来的,所以量化矩阵也同时给出了在不同分解尺度下图像可以容纳噪声的最大能力.采用整数小波变换来实现 DEM 数据数字水印算法,满足水印在不可见性的前提下将其与水印嵌入强度联系起来,得到可见阈值(JND)为 $T_{l,f}=[BQ_{l,f}/2]$([·]表示取整,β 是缩放因子).

3 DEM 数据水印技术

3.1 DEM数据分析

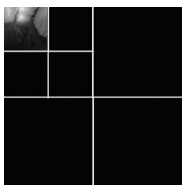
DEM 数据是用浮点数记录的海拔数据,在保持地形形状和起伏特征基本不变的前提下,人眼对地形的微小起伏变化不能分辨,或者地形的海拔数据作微小的调整对于应用来说是可以接受的.从图 2 中可以看出 DEM 数据相关度比较大,说明其信息冗余度比较大.在保持其特征的前提下,通过调整频域系数,可以将水印信息隐藏到 DEM 数据中.

小波变换分解二维信号的基本思路是利用小波滤波器提供的低通和高通滤波器系数,对信号进行分解,得到 xy-像平面上的 4 块子信号:LL(两个方向上全为低频成分),LH(x 方向低频 y 方向高频成分),HL(y 方向低频 x 方向高频成分),HH(两个方向上全为高频成分),然后对子图 LL 作进一步的小波分解,继续沿袭该过程,分解多次后得到多级小波分解数据.



(a) 3-D show of DEM data
(a) DEM 数据三维显示图

(b) 2-D show of image
(b) 二维图像显示



(c) Illustration of twice wavelets decompose
(c) 二级小波分解示意图

Fig.3 Illustration of multilevel wavelets decompose of DEM data
图 3 DEM 数据多级小波分解示意图

3.2 构造单向Hash函数

根据 Hash 函数的定义[6],应用 Rabin 方法来构造单向 Hash 函数.Rabin 利用大整数的开方取模运算,当大整数位数达到 1000 比特位时,即使是万亿次(每秒)的计算机也无能为力.因此,安全性极高.

对每一个 DEM 数据取一个标识 ID_i,随机选取两个大的素数 p,q,计算参数 $n=p\times q$,这里 p 和 q 是秘密的,n 是公开的. p 和 q 均有 512 比特位,密码设为 K 有 512 比特位.图 4 是单向 Hash 函数生成随机位置的流程图.

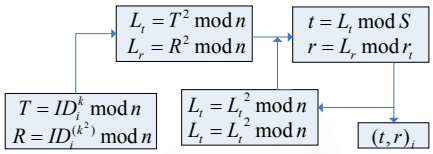


Fig.4 Construct pseudo stochastic sequence based on Rabin method

图 4 应用 Rabin 方法生成伪随机序列

通过图 4 的循环,可以得到一个序列 $\{(t,r)_i\}(0<i<Q)$(Q 为水印信息量,它决定随机序列的长度).为了防止序列中出现重复值,需要建立一个临时表,记录已经产生的(t,r).每生成一个新的(t,r),就与表中的序列对照,如果没有相同的就将其写入临时表中,然后计算下一个,如果出现相同的,则不记录到临时表中,重新计算.如果拥有参数和密码,这个序列是可以再现的.

3.3 水印嵌入算法

由于本方法不仅要检测水印的存在,还需要在没有原始 DEM 数据的情况下(盲水印)将正确的水印信息提取出来,因此,不能用通常的计算相关度的方法检测水印的存在性,而是要恢复水印数据.合法的用户通过提取隐藏的水印,可以将 DEM 数据的关键信息(如地理坐标)恢复出来,从而获得 DEM 数据的使用价值.版权拥有者也可以通过提取水印(通常是一种标识)来验证版权.

可嵌入水印的系数集 $\{M_i\}$ $(0\le i\le S-1)$生成方法(G 表示集合生成的阈值):

(1) 搜索绝对值最大的小波系数 W_{Max};

(2) 计算 $T, T=2^{[\log_2 W_{\mathrm{Max}}]}$,则 $T<W_{\mathrm{Max}}<2T$;

(3) 计算可利用集合数 S,对应于选定的阈值 P,满足 $|T/2^s|>G$;

(4) 系数搜索,生成系数集合

$$M_0=\{w_{k_0^0},w_{k_1^0},w_{k_2^0},...,w_{k_{r_0}^0}\},\text{满足}|w_{k_i^0}|\in[T,2T),$$

$$M_1=\{w_{k_0^1},w_{k_1^1},w_{k_2^1},...,w_{k_{r_1}^1}\},\text{满足}|w_{k_i^1}|\in\left[\frac{T}{2},T\right),$$

$$\cdots$$

$$M_{s-1}=\{w_{k_0^{s-1}},w_{k_1^{s-1}},w_{k_2^{s-1}},...,w_{k_{r_{s-1}}^{s-1}}\},\text{满足}|w_{k_i^{s-1}}|\in\left[\frac{T}{2^{s-1}},\frac{T}{2^{s-2}}\right),$$

$\{M_i\}$ 中每个集合包含的小波系数分别为 $r_0,r_1,...,r_{s-2},r_{s-1}$.

(5) 嵌入水印过程:首先根据(t,r)选取系数集合 M_t,然后在 M_t 中选取小波系数 $w_{k_r^t}$,通过修改小波系数 $w_{k_r^t}$,将 1 bit 水印信息 b 嵌入($T_{l,f}$ 为可见阈值(JND)确定的修改幅度,α 是缩放因子,$[\cdot]$表示取整): $w'_{k_r^t}=[w_{k_r^t}/2T_{l,f}]\times 2T_{l,f}\pm T_{l,f}\times b$.

(6) 通过单向 Hash 函数(第 3.2 节)产生的伪随机序列 $\{(t,r)_i\}$ $0<i<Q$ (Q 表示水印信息量),将所有的水印信息嵌入到 DEM 数据中.

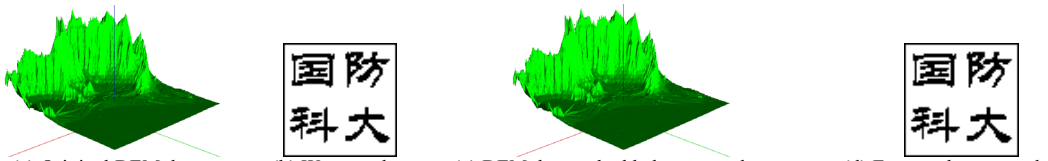
提取水印的过程就是再现伪随机序列,按照上面的过程将水印信息重新恢复出来.

4 实验及其评价

4.1 实验结果

选取参数 t=1 的提升 9/7 整数小波来实验 DEM 数据水印算法.采用的实验数据是 512×512 的 DEM 数据,记录高程的数据类型是双精度浮点.采用整数小波变换,为了保持 DEM 数据的精度,首先将数据放大 10000 倍

(抬升 4 位小数),然后将其取整.数字水印是 64×64 的二值图像,相当于长度为 4096 的二值序列,如图 5 所示.



(a) Original DEM data (b) Watermark (c) DEM data embedded watermark (d) Extracted watermark
(a) DEM 原始数据 (b) 数字水印 (c) 嵌入水印的 DEM 数据 (d) 提取的水印

Fig.5 Experiment of watermark
图 5 水印实验

4.2 安全性分析

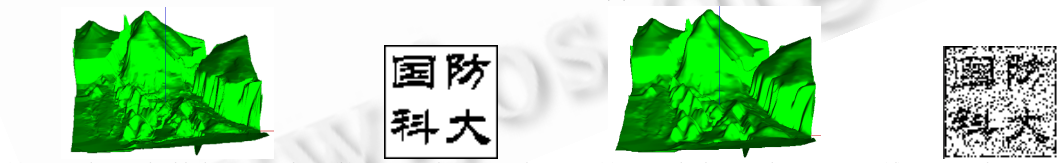
(1) 隐藏的水印是关键信息.一方面,必须保证非法用户不能获取水印;另一方面,由于水印数据是 DEM 数据的关键参数(没有这些参数,无法使用数据),因此合法用户也只有恢复出正确的水印数据才能获取 DEM 数据的使用价值.

在位置攻击下,假设非法用户已经获得了加入水印的 DEM 数据和单向 Hash 函数,但没有密码 K,一般来说,有两种方法可以获取信息.一种方法是直接的对单向 Hash 函数进行密码分析.换句话说,如果 $y=f(x)$是用于函数的单向 Hash 函数,非法用户必须找到 f^{-1} 才行.在本方法中,采用 Rabin 方法和模运算来作为单向 Hash 函数,因此那些想获取水印的非法用户必须破解 Rabin 方法.Rabin 方法的安全性是建立在很难找到复合数的模的平方根基础之上的,因此非法用户不能获取水印的位置.另一个方法是分解整数 $n=p\times q$, n 有 1024 位,$2^{1024}>10^{300}$.现在分解的最大整数是第 10 个费马数,有 150 位(10 进制),在现有的硬件条件下,分解 300 位的大整数是不可能的.如果穷举密码 K,K 为 512 位,K 有 2^{512} 种组合.如果非法用户用一台 10000MPS 的电脑计算,计算时间为 $2^{512}/(10000\times10^6\times60\times60\times24\times356)>10^{130}10^{130}$ 年.

(2) 隐藏的数据是版权信息,则嵌入水印的数据需要能够抵抗一定的攻击破坏,仍然保留可辨识的版权信息.DEM 数据通过加入噪声和进行滤波处理,会破坏水印信息,当破坏的比例在一定范围内时,水印仍然是可以辨识的.

图 6 的实验演示 DEM 数据平滑对水印的影响,采用的掩模是:

$$\frac{1}{49}\begin{bmatrix}1 & \cdots & 1\\ \cdots & \cdots & \cdots\\ 1 & \cdots & 1\end{bmatrix}_{7\times7}.$$

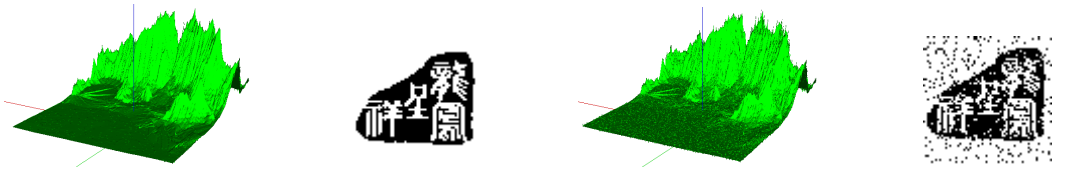


(a) DEM data embedded watermark (b) Extracted watermark (c) Smoothed DEM data (d) Extracted watermark
(a) 嵌入水印 DEM 数据 (b) 提取水印 (c) 平滑 DEM 数据 (d) 提取水印

Fig.6 Smoothing the DEM data influence the embedded watermark
图 6 平滑 DEM 数据对水印的影响

图 7 的实验演示噪声干扰对 DEM 数据水印的影响,512×512 的 DEM 数据中加入了 5000 个噪声点,噪声能量为 DEM 数据能量的 10%.

通过上面的实验可以看出,水印标志(图 6(d)和图 7(d))仍然是可以辨识的,从而达到了保护版权的目的.实验证明,该方法抗噪声和数据平滑能力很强.另一方面,还需要提到 JPEG 压缩,由于对于 DEM 数据没有相应的 JPEG 压缩算法(量化表无法选取),但是通过对图像进行相应的水印实验,表明该方法有很强的抗 JPEG 压缩能力.这样也说明采用该方法的 DEM 数据水印抗频域干扰能力较强.



(a) DEM data embedded watermark (b) Extracted watermark (c) DEM data add in noise (d) Extracted watermark

(a) 嵌入水印 DEM 数据 (b) 提取水印 (c) 加入噪声数据 (d) 提取水印

Fig.7 Show of the influence on the watermark by adding noise into the DEM data

图 7 DEM 数据加噪声对水印的影响

5 总 结

在应用上,DEM 数据是一类经济和军事价值都很大的数据类型,对它的保护关系到国民经济和国家安全.本文采用数字水印技术来对这类数据进行版权保护和使用控制,在算法公开的前提下,仍然能够保证安全.

在理论上,基于提升理论构造出了带一个自由变量 t 的紧支撑小波,选取参数 t=1 的小波基,运算速度快,便于硬件实现.提出可嵌入水印的小波系数集生成方法,扩展了基于视觉系统(HVS)小波域量化噪声的视觉权重(JND)分析方法,使其适用于 DEM 数据,并且在保证地形形状和起伏特征的前提下,能够自适应地确定水印嵌入的强度.实验证明,该水印方法有很强的抗攻击和干扰能力,有广阔的应用前景.

References:

[1] Ware JM. A procedure for automatically correcting invalid flat triangles occurring in triangulated contour data. Computers & Geosciences, 1998,24(2):141−151.

[2] Ohbuchi R, Masuda H, Aono M. Watermarking three-dimensional polygonal models. In: Proc. of the ACM Multimedia'97. New York: ACM Press, 1997. 261−272.

[3] Cayre F, Macq B. Data hiding on 3-D triangle meshes. IEEE Trans. on Signal Processing, 2003,51(4):939−948.

[4] van Schyndel RG, Tirkel AZ, Osborne CF. A digital watermark. In: Proc. of the IEEEI Int'l Conf. on Image Processing (ICIP'94). 1994. 86−90.

[5] Watson AB, Yang GY. Visibility of wavelet quantization noise. IEEE Trans. on Image Processing, 1997,6(8):1164−1174.

[6] Merkle R. One way hash functions and DES. In: Brassard G, ed. Advances in Cryptology, Proc. of the CRYPTO'89. LNCS 435, Springer-Verlag, 1989. 428−446.

[7] Calderbank AR, Daubechies I, Sweldens W, Yeo B-L. Wavelet transforms that map integers to integers. Applied and Computational Harmonic Analysis, 1998,5(3):332−369.

[8] Mallat SG. Multiresolution approximation and wavelet orthogonal base of $L^2(R)$. Trans. of the American Mathematical Society, 1989,315(1):69−87.

[9] Daubechies I. Orthonormal bases of compactly supported wavelets. Communications on Pure and Applied Mathematics, 1988,41(7):909−996.

[10] Cohen A, Daubechies I, Feauveau J. Bi-Orthogonal bases of compactly supported wavelets. Communications on Pure and Applied Mathematics, 1992,45(5):485−560.

[11] Vetterli M, Herley C. Wavelets and filters banks: Theory and design. IEEE Trans. on Signal Processing, 1992,40(9):2207−2232.

[12] Sweldens W. The lifting scheme: A new philosophy in biorthogonal wavelet constructions. In: Laine AF, Unser M, eds. Wavelet Applications in Signal and Image Processing III. New York: SPIE, 1995. 68−79.

[13] Daubechies I, Sweldens W. Factoring wavelet transforms into lifting step. Journal of Fourier Analysis' and Applications, 1998,4(3):247−269.