文章编号　1004-924X(2016)增-0640-09

结合感知哈希与数字水印的遥感影像认证方法

王玉海[1],朱长青[1],苏守宝[2*],丁凯孟[1,2]
(1. 南京师范大学 虚拟地理环境教育部重点实验室,江苏 南京 210023;
2. 金陵科技学院,江苏 南京 211169)

摘要:针对遥感影像的完整性认证需求,结合感知哈希与数字水印各自的特点,提出一种基于感知哈希与数字水印的遥感影像认证方法。该方法的关键在于克服感知哈希与数字水印之间的相互影响:首先对影像进行格网划分;然后通过离散小波变换(DWT)提取影像格网单元的水平和垂直中频系数,经过主成分分析(PCA)处理后生成感知哈希序列;接下来,基于"交错"策略,将感知哈希序列嵌入影像。在影像的认证端提取嵌入影像的感知哈希序列,并将其与重建值进行对比,进而实现影像的完整性认证。该方法将感知哈希与数字水印有机结合,克服了感知哈希进行遥感影像认证的过程需要额外传输认证信息的不足。结果表明,篡改测试实例的归一化 Hamming 距离为 0.218 7～0.398 4,能够有效识别恶意篡改,且嵌入哈希序列的格网单元的平均 PSNR 约为 38～39,不影响遥感影像的可用性。

关　键　词:遥感影像;认证;感知哈希;数字水印;交错策略
中图分类号:TP391.4　　**文献标识码**:A　　**doi**:10.3788/OPE.20162413.0640

An authentication method based on perceptual hashing and watermarking for remote sensing image

WANG Yu-hai[1], ZHU Chang-qing[1], SU Shou-bao[2*], DING Kai-meng[1,2]

(1. *Key Laboratory of Virtual Geographic Environment of Ministry of Education, Nanjing Normal University, Nanjing* 210023, *China*;
2. *Jinling Institute of Technology, Nanjing* 211169, *China*)
* *Corresponding author, E-mail: showbo@jit.edu.cn*

Abstract: Aiming at the requirements of complete authentication of remote sensing image in application, an authentication method based on perceptual hashing and watermarking for remote sensing image is proposed. The key of the method is to overcome the mutual influence between perceptual hashing and watermarking. Firstly, the remote sensing image is partitioned into girds which are then preprocessed; secondly, horizontal and vertical middle frequency coefficients are extracted by DWT(Discrete Wavelet Transtorm) and treated by PCA(Principal Component Analysis) to generate perceptual hash value, which is embedded into the diagonal middle frequency coefficient based on interleaving strategy. The authentication process is implemented via the comparison between the extracted perceptual hash value and the reconstructed one. As the method organically combined perceptual hashing and

收稿日期:2016-05-16;**修订日期**:2016-06-03.
基金项目:国家自然科学基金资助项目(NO. 61375121);金陵科技学院博士科研启动基金资助项目(NO. jit-b-201520);科研基金孵化项目(No. jit-fhxm-201604)

watermarking, it overcomes the defect that the perceptual hashing based authentication needs extra channel to transmit hash values. The experiments demonstrate that the Hamming distance of the tampering tests is between 0.218 7 and 0.398 4, thus the detailed tampering of the image can be effectively detected, and the average PSNR of the grids with perceptual hash value embedded is about 38 to 39, which means the availability of the image is not affected.

Key words: remote sensing image; authentication; perceptual Hash; digital watermarking; interleaving strategy

1 引　言

随着对地观测技术的发展，遥感影像在国土、测绘、农业等涉及国家国土安全和利益的行业获得广泛应用。但是，由于信息处理技术的发展、人为的恶意攻击、计算机网络存在的固有缺陷等因素的影响，遥感影像在传输、存储与使用等过程中很容易遭受各种无意或有意的篡改攻击，遥感影像的完整性、真实性问题也日渐突出。完整性、真实性受到攻击的遥感影像，其承载的地表环境、资源等地学信息的完整性、真实性也会受到质疑，这种情况下，遥感影像的使用价值将大打折扣甚至不再具有实用价值。所以，遥感影像的认证技术的研究具有很强的理论与现实意义。

传统的认证技术一般采用密码学 Hash 函数和数字签名实现数据的认证。但是，Hash 函数与数字签名是对数据进行二进制级别的认证，而不是对数据的有效内容信息进行认证，因此，即使数据发生一个比特的细微改动，相应的认证信息都会发生剧烈变化。然而在实际应用中，遥感影像数据进行格式转换、水印嵌入等操作之后，虽然二进制表示发生变化，但其有效内容并没有改变，并不影响其正常使用，所以传统认证技术不能很好地实现遥感影像的认证。感知哈希(Perceptual Hashing)为遥感影像的认证提供了一种新的解决途径。

感知哈希是指一个多媒体对象的感知特征通过压缩后生成简短摘要，即将具有相同感知内容的多媒体数字表示唯一地映射为一段数字摘要，并满足感知鲁棒性和安全性[1]。感知哈希与密码学 Hash 函数的显著区别在于：多媒体数据经过格式转换、数据压缩等不改变数据内容的操作，相应的感知哈希序列均不变或者变化很小。已经有诸多学者展开感知哈希的相关研究[2-7]。虽然遥感影像与普通图像在数据格式和数据存储等方面有许多相似性，但作为重要的地理空间数据，遥感影像有着空间数据独有的特征，因此需要依据其数据特点和应用环境设计遥感影像感知哈希算法。文献[2]、[5-6]提出了专门针对遥感影像数据特征的感知哈希算法，一定程度上满足了遥感影像基于感知内容的认证需求。

但是，基于感知哈希进行遥感影像的认证将会产生这样的问题：感知哈希序列(认证信息)与遥感影像数据是分离的。这就需要在传输、存储遥感影像数据的同时，对相应的感知哈希序列也要进行安全地传输、存储。在实现数据认证的同时，感知哈希自身的安全性也需要得到足够重视。如果感知哈希序列本身遭到了截获或者破坏，遥感影像的认证也就无法实现。然而，实际情况下，安全传输通道的建立与维护不仅会增加经济开销，而且增加了认证信息管理的难度。数字水印技术将信息嵌入到数字载体中，使其成为数据不可分离的一部分，这就为感知哈希信息的隐蔽传输提供了可行途径。已经有学者研究基于数字水印的数据隐蔽传输技术，并取得了良好的效果[8-14]。

本文针对感知哈希在遥感影像认证过程中存在的问题，以经过几何校正的遥感影像为研究对象，基于遥感影像的数据特征，研究将感知哈希和数字水印技术进行有机结合的认证方法。

2 相关工作

2.1 感知哈希概述

根据多媒体对象的不同，感知哈希可分为图像感知哈希、音频感知哈希、视频感知哈希等[1]。与传统密码学 Hash 函数类似，感知哈希技术能够将任意长度的输入信息转换为简短的输出序列。但是，密码学 Hash 函数(如 MD5、SHA-1)对数据进行二进制级别的认证时，只要输入数据

发生一个比特的变化，输出的序列都会完全不同。而由于感知哈希是基于多媒体数据的感知内容构造哈希序列的，故其克服了密码 Hash 函数的上述缺点。

感知哈希算法一般具有如下特征：鲁棒性，感知内容相同或者相近的图像的感知哈希序列应当相同或者相近；可区分性，是指感知内容不相同的图像数据应当产生不同的感知哈希序列；单向性：从感知哈希序列中得不到图像内容的有效信息；摘要性：感知哈希算法生成的序列所占据的存储空间应尽可能的小，以便于图像的认证或检索等操作。上述特征中，鲁棒性是感知哈希与密码学 Hash 函数最大的区别。

目前，图像感知哈希算法一般按照如下框架进行：图像预处理，使原始图像更便于特征提取；特征提取，通过离散余弦变换（DCT）、离散小波变换（DWT）、SVD 等方法提取图像的特征信息；特征量化，去除所提取特征的冗余；量化后的特征进行压缩编码与加密等操作，得到最终的感知哈希序列。其中，特征提取是关键步骤，设计感知哈希算法的首要工作就是选择合适的特征提取方式。

本文考虑到边缘特征在遥感影像应用中的重要的地位，以边缘特征为基础生成感知哈希序列。边缘特征是道路、河流等地物目标的载体，也是遥感影像识别、理解与分析的基础。另一方面，如果遥感影像的边缘特征发生较大变化，往往意味着某些地物信息遭到了篡改。因此，基于边缘特征的感知哈希算法能够满足遥感影像的认证需求。

文献[5]提出一种基于边缘特征的遥感影像感知哈希算法。该方法对影像进行自适应的预处理后，采用 Canny 算子提取边缘特征，并通过奇异值分解对提取的边缘特征进行处理，有着较高的认证精度，能够有效检测遥感影像的局部细节篡改情况。

但是，遥感影像的辐射特征容易受到多种因素的影响，其边缘特征存在一定的模糊性，因此，以 Canny 算子为代表的空域边缘检测算子的鲁棒性不高，容易受到噪声干扰。同时，Canny 算子的计算复杂度相对较高，算法灵活性方面也存在较大不足。因此，本文基于 DWT 和主成分分析 PCA，通过提取遥感影像水平和垂直中频子带的最优不相关特征，构造影像感知哈希序列。这里，PCA 不仅仅是为了压缩数据量，更重要的是降低噪声的影响，增强算法的鲁棒性。

2.2 基于数字水印的隐蔽传输

信息隐藏技术的发展为感知哈希提供了一种可靠的隐蔽信道。隐蔽信道最初的定义是：不是被设计或本意不是用来传输信息的通信信道[13]。信息隐藏技术利用人类感觉器官对数字信号的感觉冗余，将秘密消息隐藏在载体信息中，使人不知道或者不怀疑秘密信息的存在。数字水印技术是信息隐藏的重要分支。数字水印技术通过将版权等水印信息嵌入图像数据，从而避免了复杂的数据库操作，也避免了版权等信息的额外传输。脆弱/半脆弱水印虽然也能够实现图像认证，但是，其主要利用了水印本身的性质，对于嵌入的内容并不关注[15]。目前，数字水印的研究成果较多[16-18]，研究重点侧重于水印算法自身的鲁棒性、抗攻击性。

文献[8-14]研究了基于数字水印的数据隐蔽传输技术。Han Q 等人[8]提出一种感知特征信息嵌入人脸图像的算法，实现了人脸图像的认证；林丕源等人[9]基于信息隐藏技术与椭圆曲线实现农业信息安全传输；Weng L 等人[10]通过离散余弦变换（DCT）提取图像低频系数，将生成的哈希序列嵌入图像，但该方法没有顾及遥感影像的数据特征，因此不适合遥感图像的认证；Eswaraiah R 等人[11]提出一种基于整数小波的水印算法，将医学图像的重要区域嵌入图像，能够实现重要区域的修复；Baby D 等人[12]提出一种基于 DWT 的彩色图像隐蔽传输方法。

本文利用数字水印作为认证信息的载体，将数字水印技术和感知哈希进行有机的结合，使感知哈希序列成为影像数据的一部分，这样就使得感知哈希序列随时可以被提取并用于认证，不需要建立额外的传输信道，也不再需要额外的存储空间存储相应的感知哈希序列，同时避免了复杂的数据库管理操作。

这里的关键问题在于：感知哈希是通过提取影像的特征生成哈希序列的，而数字水印则需要对影像进行一定的修改，这就需要保证两者之间不能相互影响。也就是说，感知哈希序列嵌入影像数据之后，不能影响感知哈希的再次计算。

3 本文方法流程

本文基于遥感影像的数据特征，通过“交错策

略”，分别在影像 DWT 后不同的中频子带进行感知哈希序列生成与数字水印嵌入的操作，使其相互不受影响。DWT 是目前常用的图像数字水印算法。目前，基于对水印信息量、透明性以及稳健性等方面的考虑，基于 DWT 域图像数字水印算法将水印信息嵌入在 DWT 域的低频或中频系数中[16]。本文方法侧重水印的信息承载作用，同时顾及水印与感知哈希的相互影响，因此选择中频嵌入信息。此外，由于遥感影像普遍具有的数据海量性特点，因此本文方法首先对遥感影像进行隐形格网划分，将其划分为相同大小的格网单元，针对格网单元进行感知哈希序列的提取与嵌入。

如图 1 所示，本文方法首先通过隐形格网将遥感影像分割成大小相等的区域；提取每个格网单元的水平与竖直中频系数，并生成相应的感知哈希序列；生成的感知哈希序列嵌入影像。在用户端，从影像中提取、解密感知哈希序列，并采用相同方法重新计算各格网的感知哈希序列，继而完成遥感影像的内容完整性认证。

原始影像首先进行 $W\times H$ 的格网划分（W 和 H 均为正整数）。理论上，格网划分的粒度越细，算法的认证精度更高。但是，如果格网划分的粒度过于精细，计算时间将会大大增加。因此，选择格网单元的大小需要综合考虑算法性能与开销，W 和 H 根据影像实际大小而定。

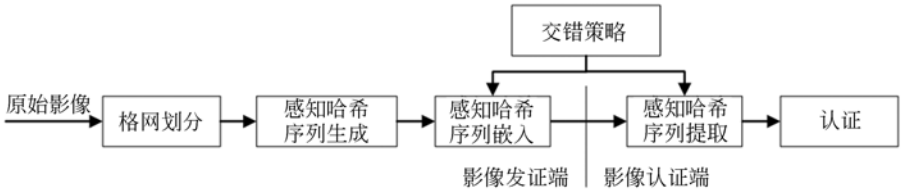


图 1　总体流程

Fig. 1　Flow chart of proposed method

3.1　基于 DWT 变换与 PCA 生成感知哈希序列

计算影像格网单元的感知哈希序列。本文参考感知哈希的一般流程，按照如下步骤进行感知哈希的计算：格网单元预处理之后，基于 DWT 进行格网边缘特征的提取，然后基于 PCA 对边缘特征进行压缩与去噪处理，再通过 RC4 算法加密得到格网单元的感知哈希序列。具体流程如下：

预处理，将格网单元转化的单通道影像（如果原始影像为单波段影像，则不需要进行该步骤）；然后，通过双线性插值将其标准化为 $m\times m$ 大小的缩略图，记为 $G(x,y)$。此举旨在将不同分辨率的影像调整为相同分辨率，使最终生成的感知哈希序列长度固定。这里，以 $m=64$ 为例进行研究与分析。

接下来，通过 DWT 变换提取格网单元的边缘特征。图像经过 DWT 变换之后，并没有实现数据压缩，只是对原始图像的能量进行重新分配。DWT 变换的实质是小波函数和原图像的卷积，能够有效地从图像中提取高频和低频信息。二维 DWT 变换具有水平和垂直方向选择性，而且这些特性与人类的视觉特性相吻合。图像经过小波变换后，虽然能量集中在低频部分，但是高频部分能够很好地刻画图像的非平稳特征。

如图 2 所示，格网单元进行 2 层小波分解之后，LH_1、HL_1、HH_1 为高频子带，它们分别保持了格网单元竖直方向上的高频边缘信息、水平方向上的高频边缘信息和对角线方向上的高频信息。而 LH_2、HL_2、HH_2 就是中频子带。LH_2、HL_2、HH_2 和 LL_2 实际上是低频部分 LL_1 多二次小波变换的结果，因此 LH_2、HL_2、HH_2 同样包含了丰富的边缘信息。尽管高频部分包含了丰富的

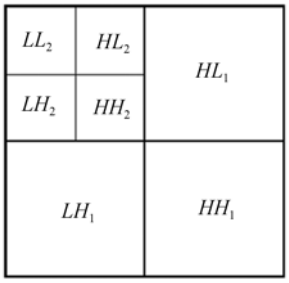


图 2　小波变换后频域分布图

Fig. 2　Frequency-domain bounds after wavelet decomposition

边缘细节信息，但是容易遭到噪声的影响，不利于算法鲁棒性。中频部分则能够兼顾鲁棒与脆弱的均衡性，可以很好地反应遥感影像的边缘特征。此外，中频系数的个数只有高频系数的 1/4，数据量更少、更精炼，最终的感知哈希序列也较短，利于算法的实用性。

本文方法提取垂直中频子带 LH_2 和水平中频子带 HL_2 作为格网单元的边缘特征。对 $G(x,y)$ 进行两级小波分解后，提取垂直中频子带 LH_2 和水平中频子带 HL_2，构造两个中频系数矩阵，分别记为 $\mathbf{M}_{LH2}$、$\mathbf{M}_{HL2}$，矩阵元素就是相应的中频系数，每个矩阵大小是 $(W/4)\times(H/4)$。基于“极大值”的选择规则，选取两个中频系数矩阵对应位置最大的系数值作为融合结果，得到的矩阵称为融合矩阵，记为 $\mathbf{M}_{IF}$。

接下来，通过 PCA 对中频系数矩阵进行压缩与去噪处理。PCA 是一种以 K-L 变换为基础的统计分析方法，其目的是产生最优不相关特征，常用于对高维数据的降维，具有很好的压缩效果。通过线性变换 PCA 将原始空间转换到维数较低的主成分空间，转换之后的新特征称为主成分，各个主成分之间满足不相关性。根据其对应方向上的方差贡献率进行降序排列。这样，就可以用一部分不相关的新向量来描述原数据集中的主要信息。经过 PCA 分解对 $\mathbf{M}_{IF}$ 去除矩阵元素的线性相关性，然后对主成分进行标准化处理，得到该格网单元的感知哈希序列，记为 PH_{ij}。

将所有格网单元的感知哈希序列 PH_{ij} 进行串联，经过加密算法（基于密钥长度灵活性的考虑，本文方法采用 RC4）加密后，构成影像最终的感知哈希序列，记为 PH。

3.2 基于交错机制的嵌入规则

目前，数字水印技术研究的重点在于增强算法的鲁棒性[16-18]。数字水印技术要求水印信息尽可能地覆盖整个图像，以抵抗裁剪等攻击。但是，本文方法则更侧重于数字水印的信息承载作用，更注重水印的不可感知性与安全性（不被恶意篡改或利用）。从一个角度来说，如果含水印影像遭到破坏而无法提取认证信息，这也说明影像数据遭到了篡改攻击。因此，本文方法的关键在于克服感知哈希与数字水印之间的相互影响。

本文方法在进行水印信息（即感知哈希序列）的嵌入时，需要顾及两个方面：首先，避免水印嵌入规则与感知哈希序列的相互影响；其次，感知哈希序列嵌入影像数据后，不影响遥感影像数据的可用性。

本文方法通过对不同的中频子带进行感知哈希与数字水印的相关操作，来消除感知哈希与数字水印间的相互影响：感知哈希的生成阶段，本文基于垂直中频子带 LH_2 和水平中频子带 HL_2 生成感知哈希序列；感知哈希的嵌入阶段，将哈希序列嵌入对角中频子带 HH_2。本文采用“基于位平面”的水印嵌入方法[18]，将哈希序列嵌入对角中频子带，以提高方案在复杂环境下的抗攻击性。水印嵌入规则为：

$$X_m=\begin{cases}1, PH_{ij}^k=1\\ 0, PH_{ij}^k=0\end{cases}, \tag{1}$$

其中，PH_{ij}^k 表示 PH_{ij} 的 k 位的值，$PH_{ij}^k=\{0,1\}$；X_m 表示影像像素值的第 m 位平面的值，$X_m=\{0,1\}$，$m=0,1,2,\cdots,7$（本文取 $m=1$）。这里，由于感知哈希序列 PH_{ij} 的长度取决于缩略图的大小和主成分标准化处理的过程，因此，第 m 位平面的可嵌入位置多于 PH_{ij} 的序列长度，这也就意味着每一位的感知哈希序列可能被嵌入多次。

如果将格网单元的感知哈希序列嵌入相同的格网单元中，那么，一旦格网单元遭到某种攻击提取不了感知哈希序列，就不能进行相应的认证，也不能判断攻击对格网单元造成的影响。因此，本文借鉴“空间局部性”原理[19]，按照“移位映射机制”确定感知哈希序列嵌入的格网单元。令 PH_{ij} 嵌入的格网单元为 X_{gk}，则映射为：

$$\begin{cases}g=(i+m)\bmod W\\ k=(j+n)\bmod H\end{cases}, \tag{2}$$

式中，g 与 k 分别表示单元感知哈希序列 PH_{ij} 的嵌入格网 X_{gk} 的坐标，mod 表示模除运算，m 和 n 分别表示横、纵坐标的映射的位移，W 与 H 分别表示影像格网划分的粒度。如果某一格网单元遭到某种攻击而发生数据内容改变，那么与其相邻的格网单元也很有可能收到类似的攻击而发生内容改变，因此，m 与 n 的选择不宜过小，本文实验中 $m=n=4$。例如，坐标为(1,1)的格网单元，其感知哈希序列嵌入坐标为(5,5)的格网单元。

3.3 认证过程

用户端对遥感影像进行认证。首先，确定感知哈希序列的嵌入区域：待认证影像采用相同的格网划分方法，提取嵌入格网单元的感知哈希序

列，并按照公式(3)将提取的感知哈希序列映射到其生成的格网单元。例如，从坐标为(5,5)的格网单元提取的感知哈希序列，其原始格网单元的坐标是(1,1)。

$$\begin{cases} i = (g + \mathrm{W} - m) \bmod \mathrm{W} \\ j = (k + H - n) \bmod H \end{cases}. \tag{3}$$

感知哈希序列的检测过程实际是嵌入的逆过程：格网单元进行两级小波变换之后，从对角中频子带 HH_2 的第 m 位平面提取 0-1 序列；由于每一位的水印信息均会被检测出多次，所以这里采用多数原则确定水印信息，进而得到嵌入格网单元的感知哈希序列。

接下来，重新计算各格网单元的感知哈希序列，并比较与提取的感知哈希序列之间差别，以此判断待认证格网单元的内容是否发生变化。Hamming 距离能够衡量两个序列之间的差异，但是感知哈希序列的长度可能随算法参数的变化而变化，因此本文采用更为直观的“归一化 Hamming 距离”来衡量感知哈希序列之间的差异。归一化 Hamming 距离计算公式如下：

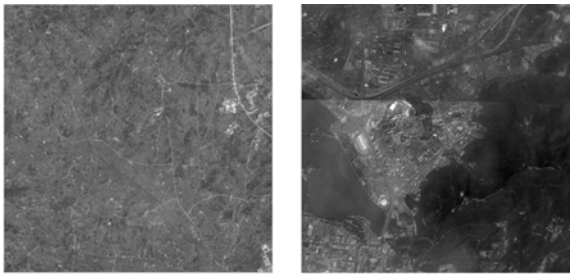
$$Distance = \left(\sum_{i=1}^{L} \left| h_1(i) - h_2(i) \right| \right) / L, \tag{4}$$

其中 h_1 和 h_2 为长度是 L 的感知哈希序列。归一化 Hamming 距离实际上是 0～1 之间的浮点数。两个哈希序列的归一化 Hamming 距离越大，说明它们的差别也越大。如果归一化 Hamming 距离低于设置的阈值 T(阈值 T 的设定应依据实际认证需求而定，本文实验中 $T=0.1$)，说明相应的区域没有发生能够感知的差别，即内容上保持不变。反之，相应的区域被恶意篡改或者内容发生较大变化。检测所有内容发生变化的区域后，对认证结果进行表述。

4　实验与分析

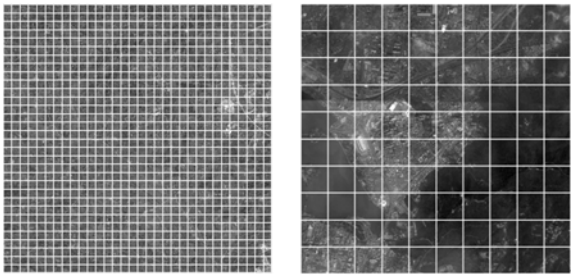
为了验证算法的有效性，选取如图 3 所示的两幅单波段遥感影像(Tiff 格式存储)为例进行测试，大小分别为 4 096 pixel×4 096 pixel、2 500 pixel×2 500 pixel。

首先，原始实验影像分别进行 32×32、10×10 的格网划分，如图 4 所示。划分之后，每个格网单元的大小分别为 128 pixel×128 pixel、250 pixel×250 pixel。



(a) 实验影像A　(b) 实验影像B
(a) Image A　(b) Image B

图 3　实验影像
Fig. 3　Experimental images



(a) 影像A　(b) 影像B
(a) Image A　(b) Image B

图 4　格网划分结果
Fig. 4　Grid partition results

4.1　可视化分析

图 5 是感知哈希序列嵌入前后的格网单元对比。其中，图 5(a)和(c)分别是影像 A 和影像 B 的原始格网单元，图 5(b)和(d)是嵌入感知哈希序列的对应格网单元。影像格网单元的内容没有发生明显改变，亦即感知哈希序列的嵌入没有影响格网单元的视觉质量。

本文采用峰值信噪比来客观评价信息嵌入前后影像的失真程度。峰值信噪比的计算公式如下：

$$PSNR = 10 \cdot \log_{10} \frac{(MN) \times \left[\max(I) - \min(I) \right]^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} \left[I(i,j) - I'(i,j) \right]^2}, \tag{5}$$

其中，I 和 I' 分别表示原始格网单元和嵌入哈希序列的格网单元，$I(i,j)$ 和 $I'(i,j)$ 表示 (i,j) 处的像素值，$M \times N$ 表示格网单元的大小。一般来说，PSNR＞ 28 时，可以认为影像在视觉上是可以接受的，反之认为视觉效果较差。计算

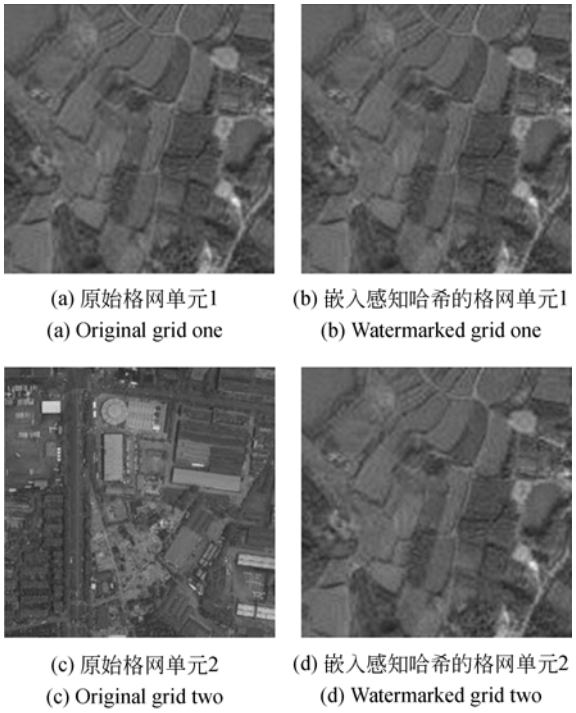


图 5　格网单元嵌入哈希序列前后的对比

Fig. 5　Comparison of grids before and after embedding hash value

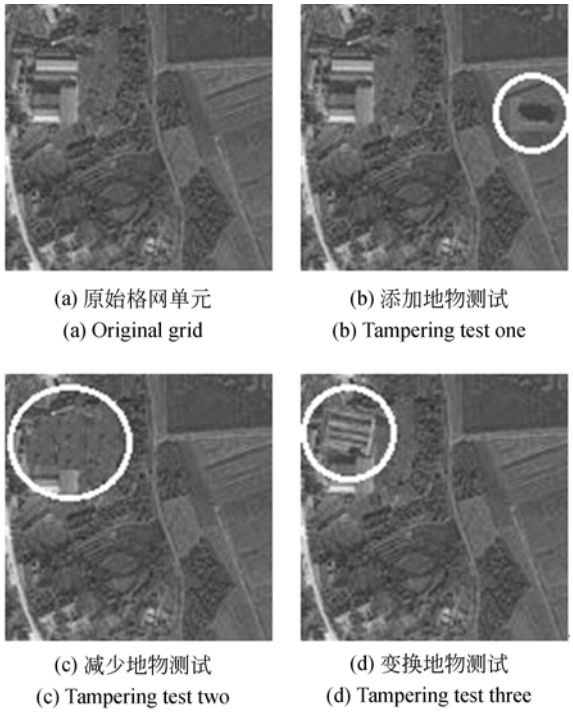


图 6　局部篡改检测测试

Fig. 6　Local tampering tests

可知，测试影像 A 的格网单元（共 1 024 个）嵌入哈希序列前后的 PSNR 平均值为 39.258 4，测试影像 B 的格网单元（共 100 个）在嵌入哈希序列前后的 PSNR 平均值为 38.891 6。其中，图 5 所示的格网单元的 PSNR 为 38.578 1。这就说明，在垂直与水平中频子带嵌入感知哈希序列，并没有影响到遥感影像本身的质量，保障了其可用性。

4.2　有效性分析

影像数据接收端，从影像中提取格网单元的感知哈希序列后，对影像的内容进行完整性认证。认证过程要能够检测出影像局部的恶意篡改。选择如图 6(a)所示的格网单元为例进行篡改敏感性测试，图 6(b)～ 6(d)所示为该格网单元的增加地物、减少地物、变换地物等篡改操作。设定通过实验设定归一化 Hamming 距离阈值 T_h 为 0.10。篡改前后的归一化 Hamming 距离分别为 0.218 7、0.359 4、0.398 4，均高于设定的阈值。这就说明，本文方法能够识别出遥感影像的局部内容篡改，能够为遥感影像的后期使用提供完整性保障。

4.3　其　它

相对于密码学 Hash 函数等传统认证方式，鲁棒性是感知哈希最重要的特点。这里，提取出感知哈希序列之后，采用格式转换（原始 Tiff 格式的影像转为 PNG 格式）与最低有效位水印嵌入（与感知哈希的嵌入位平面不同）为例来测试算法的鲁棒性。实验结果为：测试影像所有格网单元的感知哈希序列均没有发生变化。可见，本文方法能够实现影像认证的同时保持一定鲁棒性。

感知哈希的安全性方面，该方法依托于 RC4 算法的安全性。RC4 算法安全性早已经过了人们广泛研究与应用，密钥安全的情况下，安全性有着足够保障。所以，本文方法具有足够的安全性保障。

5　结　论

感知哈希技术与数字水印技术都是遥感影像安全相关的技术，有着各自的优势。本文根据遥感影像在认证中的需求，将数字水印技术和感知哈希技术有机的结合，提出了基于感知哈希与数字水印的遥感影像认证算法。该方法基于遥感影像水印技术实现感知哈希序列的隐蔽传输，避免了额外的认证信息的传输。本文方法更侧重于数

字水印的信息承载作用，重点是克服感知哈希与数字水印之间的相互影响。本文对感知哈希算法的改进之处在于，基于边缘特征的感知特征提取能够满足遥感影像的后期应用需要，并在鲁棒性与篡改敏感性之间实现折衷。实验结果表明，篡改测试实例的归一化 Hamming 距离为 0.218 7～0.398 4，能够有效识别恶意篡改；嵌入哈希序列的格网单元的平均 PSNR 约为 38～39，不影响遥感影像的正常使用，证明了该方法的有效性。

本文方法在抗攻击性方面存在一定不足，研究不影响感知哈希计算过程且鲁棒性更好的水印算法，是下一步研究的重点。

参考文献：

[1] 牛夏牧，焦玉华. 感知哈希综述[J]. 电子学报，2008，36(7)：1405-1411.
NIU X M，JIAO Y H. An overview of Perceptual Hashing[J]. *Acta Electronica Sinica*，2008，36(7)：1405-1411.（in Chinese）

[2] 丁凯孟，朱长青，苏守宝，等. 用于多光谱影像完整性认证的感知哈希算法[J]. 光学 精密工程，2015，23(10z)：676-683.
DING K M，ZHU C Q，SU S B. Perceptual hash method for integrity authentication of multispectral remote sensing images [J]. *Opt. Precision Eng.*，2015，23(10z)：676-683.（in Chinese）

[3] 王俊文，刘光杰，张湛，等. 基于小波变换和 Zernike 矩的图像区域复制篡改鲁棒取证[J]. 光学 精密工程，2009，17(7)：1686-1693.
WANG J W，LIU G J，ZHANG Z，*et al.*. Robust forensics for image regional duplication and forgery based on DWT and Zernike moment[J]. *Opt. Precision Eng.*，2009，17(7)：1686 - 1693.（in Chinese）

[4] 龚卫国，张旋，李正浩. 基于改进局部敏感散列算法的图像配准[J]. 光学 精密工程，2011，19(6)：1375-1383.
GONG W G，ZHANG X，LI Z H. Image registration based on extended LSH[J]. *Opt. Precision Eng.*，2011，19(6)：1375-1383.（in Chinese）

[5] 丁凯孟，朱长青. 一种用于遥感影像完整性认证的感知哈希算法[J]. 东南大学学报：自然科学版，2014，44(4)：723-727.
DING K M，ZHU C Q. Perceptual hash method for integrity authentication of remote sensing image[J]. *Journal of Southeast University (Natural Science Edition)*，2014，44 (4)：723-727.（in Chinese）

[6] 丁凯孟，朱长青，卢付强. 基于自适应格网划分的遥感影像感知哈希认证算法[J]. 武汉大学学报：信息科学版，2015，40(6)：716-720.
DING K，ZHU C Q，LU F. An adaptive grid partition based perceptual hashmethod for remote sensing image authentication[J]. *Wuhan Daxue Xuebao*，2015，40(6).（in Chinese）

[7] SUN R，ZENG W. Secure and robust image hashing via compressive sensing[J]. *Multimedia Tools and Applications*，2014，70(3)：1651-1665.

[8] HAN Q，WANG Z，LI Q，*et al.*. A facial image authentication method by embedding PLT-PCA features[J]. *International Journal of Digital Content Technology & Its Applic*，2012，6(10)：266-275.

[9] 林丕源，严尚维. 基于椭圆曲线和信息隐藏的农业信息安全传输方案[J]. 农业工程学报，2004，20(4)：134-137.
LIN P Y，YAN S W. Secure transmission scheme of important agricultural information on networks based on elliptic curve and information hiding [J]. *Transactions of The Chinese Society of Agricultural Engineering*，2004，20(4)：134-137.（in Chinese）

[10] WENG L，DARAZI R，PRENEEL B，*et al.*. Robust image content authentication using perceptual hashing and watermarking[J]. *Lecture Notes in Computer Science*，2012，7674：315-326.

[11] ESWARAIAH R，SREENIVASA Reddy E. Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest[J]. *Iet Image Processing*，2015，9(8)：615-625.

[12] BABY D，THOMAS J，AUGUSTINE G，*et al.*. A novel DWT based image securing method using steganography [J]. *Procedia Computer Science*，2015，46：612-618.

[13] 王永吉，吴敬征，曾海涛，等. 隐蔽信道研究[J]. 软件学报，2010，21(9)：2262-2288.
WANG Y J，WU J J，ZENG H T. Covert Channel Research [J]. *Journal of Software*，2010，21(9)：2262-2288.（in Chinese）

[14] 王宇. 遥感影像信息隐藏算法研究[D]. 南京师范大学, 2012.
WANG Y. *Research on Information Hiding for Remote Sensing Image* [D]. Nanjing: Nanjing Normal University, 20012. (in Chinese)

[15] 韩琦. 基于感知内容的人脸图像认证技术研究[D]. 哈尔滨工业大学, 2009.
HAH Q. *Research on perceptual content based facial image authentication techniques* [D]. Harbin: Harbin Institute of Technology, 2009. (in Chinese)

[16] BABY D, THOMAS J, AUGUSTINE G, *et al.*. A novel DWT based image securing method using steganography [J]. *Procedia Computer Science*, 2015, 46: 612-618.

[17] SINGH A K, KUMAR B, DAVE A, *et al.*. Robust and imperceptible dual watermarking for telemedicine applications[J]. *Wireless Personal Communications*, 2015, 80(4): 1415-1433.

[18] 任娜, 朱长青, 王志伟. 基于映射机制的遥感影像盲水印算法[J]. 测绘学报, 2011, 40(5): 623-627.
REN N, ZHU C Q, WANG ZH W. Blind watermarking method based on mapping mechanism for remote sensing image[J]. *Acta Geodaetica et Cartographica Sinica*, 2011, 40(5): 623-627. (in Chinese)

[19] PARKER J, NUNES E, GODOY J, *et al.*. Exploiting spatial locality and heterogeneity of agents for search and rescue teamwork[J]. *Journal of Field Robotics*, 2015.

作者简介：

王玉海(1971－)，男，河南济源人，博士后，1994 年于河南大学获得学士学位，2001 年、2008 年于解放军信息工程大学分别获得硕士、博士学位，现为南京师范大学虚拟地理环境教育部重点实验室博士后，主要从事地理数据安全方面的研究。

丁凯孟(1985－)，男，山西长治人，博士，讲师，2009 年于淮海工学院获得学士学位，2015 年于南京师范大学获得博士学位(硕博连读)，主要从事地理数据安全、数据认证的研究。E-mail: dingkaimeng@foxmail.com

导师简介：

朱长青(1961－)，男，江苏阜宁人，博士，教授，博士生导师，1982 年于解放军测绘学院获得学士学位，1992 年于郑州大学获得硕士学位，1997 于解放军测绘学院获得博士学位，主要从事地理数据安全、数据不确定性等研究。

苏守宝(1965－)，男，安徽六安人，博士，教授，1986 年、2004 年、2009 年于安徽大学分别获得学士、硕士、博士学位，2011 年哈尔滨工业大学卫星技术研究所博士后流动站出站，主要从事模式识别、信息安全等方面的研究。