基于压缩传感的图像哈希水印算法研究*

周 燕[1]，张德丰[1]，马子龙[2]
（1. 佛山科学技术学院计算机系，广东 佛山 528000；
2. 哈尔滨工业大学电子工程系，黑龙江 哈尔滨 150001）

摘 要：现有基于图像内容的水印算法在鲁棒性和篡改检测方面存在不足，提出了一种基于压缩传感的图像哈希水印算法。该算法利用压缩传感对图像进行随机投影，得到的压缩测量值作为图像内容特征，通过HMAC（Hash-based Message Authentication Code，基于哈希的消息认证码）算法生成图像摘要，并以水印的方式嵌入到原始图像中；认证时，提取图像中的水印，并对认证图像进行压缩传感随机投影，得到原始图像和认证图像的摘要，通过摘要对比，实现图像认证和篡改检测。仿真实验表明，该方法不仅具有较强的鲁棒性和安全性，还具有较好的篡改检测能力。

关键词：压缩传感；内容特征；HMAC算法；数字水印；图像认证
中图分类号：TP301.6 **文献标志码**：A **文章编号**：0529-6579（2010）06-0058-06

The Research of Image Hash Watermarking Algorithm Based on Compressed Sensing

ZHOU Yan[1], *ZHANG Defeng*[1], *MA Zilong*[2]
（1. Department of Computer Science, Foshan University, Foshan 528000, China;
2. Department of Electrical Engineering, Harbin Institute of Technology, Harbin 150001, China）

Abstract: For the reason that the robustness and tamper detection for existing content-based watermarking algorithms are poor, an image hash watermarking algorithm is proposed based on compressive sensing. It conducts random projection on image using compressive sensing, and gets compressive measurements which represent the content features of image. By the HMAC algorithm, the image digest is generated and embedded into the original image as watermark. When authentication, the watermark is extracted from the tampered image, and random projection on the tampered image is conducted. By comparing the image digests between original and tampered images, the image authentication and tamper detection are implemented. Experimental results show that the proposed algorithm not only has strong robustness and security, but also has good ability of tamper detection.

Key words: compressive sensing; content feature; HMAC algorithm; digital watermark; image authentication

近年来，由Donoho，Candes[1]及华裔科学家Tao等人提出的压缩传感理论，受到了广泛关注。该理论利用信号的稀疏性先验知识，通过合适的优化算法，可由少量的测量值重建原始信号。这些测量值代表了图像的内容特征，利用该特性可由测量值生成数字水印[2-3]。本文提出了一种基于压缩传感的图像哈希水印算法，首先对原始图像进行压缩传感随机投影，得到图像的压缩测量值，然后利用HMAC（Hash-based Message Authentication Code，基于哈希的消息认证码）算法生成哈希水印并嵌

* 收稿日期：2010-03-24
基金项目：广东省自然科学基金资助项目（9151040701000002，10152800001000016，10452800001004185）
作者简介：周燕（1979年生），女，讲师；E-mail：zhouyan791266@163.com

入到原始图像中；认证时，首先提取认证图像中的水印，经过非对称解密，得到代表原始图像的摘要；然后对认证图像进行压缩传感随机投影，利用 HMAC 算法生成代表认证图像的摘要；最后通过比较原始图像和认证图像的摘要，实现图像认证和篡改检测。

1　基于压缩传感的水印模型及算法实现

1.1　压缩传感理论分析

压缩传感（Compressive Sensing，CS）假定信号在某些基下能用少量非零系数表示。设 $x \in \mathbb{R}^n$ 代表一个自然信号，$y \in \mathbb{R}^m, m < n$ 是通过 $y = Ax$ 得到的线性随机投影。测量矩阵 $A \in \mathbb{R}^{m \times n}$ 必须满足 RIP[4-5]，即 A 中所有 k 列组成的子集与线性测量都接近正交。测量矩阵可以从给定的统计分布（如高斯或贝努利）中随机抽样组成[6-7]。假设 x 是 k – 稀疏（有 $k << n$ 个非零元素），压缩传感的目标是通过给定的测量值 y 重构出稀疏信号 x。这个问题可以转换为如下的优化问题：

$$\text{minimize} \quad \|x\|_0 \quad \text{s.t.} \quad y = Ax \tag{1}$$

其中 l_0 范数（$\|\cdot\|_0$）表示向量 x 中非零元素的个数。为了得到这个问题的精确求解，需要穷举搜索所有 $\left(\frac{n}{k}\right)$ 种可能的 k – 稀疏解，计算非常复杂。压缩传感的最近研究结果表明[8]：如果信号 x 充分稀疏，通过求解以下的 l_1 最小化问题[9]，就可以近似重构出 x：

$$\text{minimize} \quad \|x\|_1 \quad \text{s.t.} \quad y = Ax \tag{2}$$

这个问题可以转化为一个线性规划问题[10]。如果测量数目满足 $m \geqslant C \cdot k\log_2(n/k)$，那么问题（2）和（1）是等价的。如果 x 不是稀疏的，但在某些正交基下可以稀疏表示，则上述结果同样适用。本文主要利用压缩传感对原始图像和认证图像进行随机投影。

1.2　压缩传感的水印模型及算法分析

本文提出的基于压缩传感的图像哈希水印模型如图 1 所示。原始图像经过压缩传感随机投影，得到的压缩测量值作为图像内容特征，利用 HMAC 算法生成图像摘要，经过非对称加密，形成加密的水印信息，嵌入到原始图像的中低频系数上。

压缩传感的关键是构建测量矩阵[11]，测量矩阵是否合理影响着测量数据的多少。当测量矩阵为 Fourier 矩阵时[12]，$O(K * \log(N))$ 的投影测量数据量能将 N 维空间的 K – 稀疏信号精确重建。Fourier

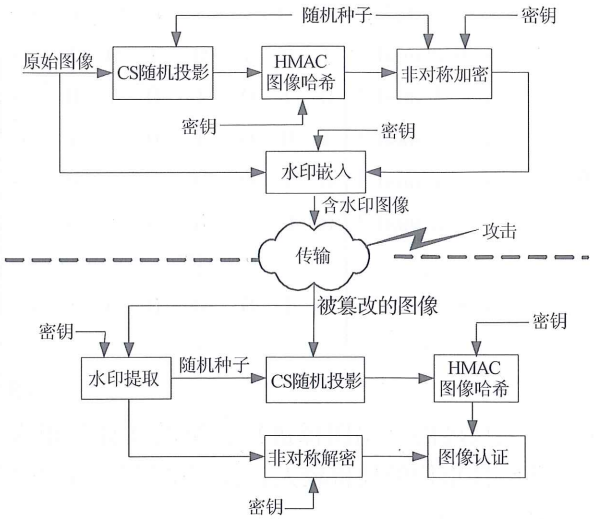


图 1　基于压缩传感的图像哈希水印模型

Fig. 1　The module of image hash watermark based on Compressive Sensing

测量矩阵的构造算法如下：

设图像的大小 N 是素数，定义 $p_0 = 1$，p_i 是第 i 个素数，那么有

$$p_0 = 1, p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \cdots \tag{3}$$

令 $q \in \mathbb{N}$，对于 $p_{q-1} < k \leqslant p_q$，可以通过如下 K 个素数（$K \in \mathbb{N}$ 并且 $K \geqslant k$）

$$k \leqslant p_q < p_{q+1} < \cdots < p_{q+K-1} \tag{4}$$

来构造一个测量矩阵

$$\Phi \in \left\{0, \frac{1}{\sqrt{K}}\right\}^{\left(\sum_{j=0}^{K-1} p_{q+j}\right) * N} \tag{5}$$

测量矩阵的行用 $r_{j,h}$ 表示，$j \in [0, K) \cap Z$，$h \in [0, p_{q+j}) \cap Z$，对于每一行的第 n 列（$n \in [0, N) \cap Z$），有

$$(r_{j,h})_n = \delta((n-h) \bmod p_{q+j}) = \begin{cases} 1 & \text{if } n \equiv h \bmod p_{q+j} \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

因此测量矩阵 Φ 可以表示为

$$\Phi = \frac{1}{\sqrt{K}} \begin{Bmatrix} r_{0,0} \\ r_{0,1} \\ \vdots \\ r_{0,P_q-1} \\ r_{1,0} \\ \vdots \\ r_{1,P_{q+1}-1} \\ \vdots \\ r_{K-1,P_{q+K-1}-1} \end{Bmatrix} \tag{7}$$

利用上面公式可以得到如下的测量矩阵：

$$\Phi\sqrt{K}=\begin{array}{r}\\ n\equiv 0 \bmod 2\\ n\equiv 1 \bmod 2\\ n\equiv 0 \bmod 3\\ n\equiv 1 \bmod 3\\ n\equiv 2 \bmod 3\\ \vdots\\ n\equiv 1 \bmod 5\\ \vdots\end{array}\begin{array}{c}\begin{array}{cccccccc} n\in[0,N) & 0 & 1 & 2 & 3 & 4 & 5 & 6 & \cdots\end{array}\\ \left[\begin{array}{cccccccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots\\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & \cdots\\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & \cdots\\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & \cdots\\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & \cdots\\ & & & \vdots & & & & \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & \cdots\\ & & & \vdots & & & & \end{array}\right]\end{array} \tag{8}$$

由于对大尺度的整幅图像进行投影的计算量很大，并且非线性重构的代价较大，我们采用分块随机投影，其算法如下：

1）设原始图像 X 的大小 $N = I_r \times I_c$，将图像分成大小为 $B \times B$ 的块，第 i 个图像块的向量形式记为 x_i，其中 $i = 1 \ldots n$，$n = N/B^2$。

2）从测量矩阵 Φ 得到 $M_B \times B^2$ 的矩阵块 Φ_B，其中 $M_B = |(M \times B^2)/N|$。

3）对 x_i 采用相同的矩阵块 Φ_B 进行投影测量，得到测量值向量：

$$y_i = \Phi_B x_i \tag{9}$$

4）对于整幅图像，测量矩阵 Φ 可以用如下的块对角矩阵表示：

$$\Phi = \begin{bmatrix} \Phi_B & & & \\ & \Phi_B & & \\ & & \cdots & \\ & & & \Phi_B \end{bmatrix} \tag{10}$$

在该算法中，不需存储 $M \times N$ 的矩阵 Φ，仅需存储 $M_B \times B^2$ 的矩阵块 Φ_B。显然，当 B 较小时需要的存储较小并能快速实现，而当 B 较大时能得到较好的重建效果，根据经验，取块的尺度 $B = 32$。

以压缩传感随机投影得到的压缩测量值作为哈希函数的输入，对输出的图像摘要进行非对称加密，得到加密的哈希水印。哈希函数采用带密钥的 HMAC 算法[13-14]，该算法需要一个加密散列函数 H（可以是 MD5 或者 SHA－1）和一个密钥 K。HMAC 的计算公式如下：

$$\text{HMAC} = H(K \text{ XOR opad}, H(K \text{ XOR ipad}, M)) \tag{11}$$

其中，ipad 是由 B 个字节 0x36 组成的字符串，opad 是由 B 个字节 0x5C 组成的字符串。B 表示数据块的字节数（MD5 和 SHA－1 的分割数据块字长都是 64），L 表示散列函数的输出数据字节数（MD5 中 L =16，SHA－1 中 L =20）。密钥 K 的长度可以小于等于 B，当大于 B 时，首先使用散列函数 H 对 K 进行转换，然后用 H 输出的 L 长度字符串作为在 HMAC 中实际使用的密钥。HMAC 算法如下：

1）在密钥 K 后面添加 0 来创建一个字长为 B 的字符串；

2）将第 1）步生成的 B 字长的字符串与 ipad 做异或运算；

3）将随机投影得到的压缩测量值填充至第 2）步的结果字符串中；

4）用 H 作用于第 3）步生成的数据流；

5）将第 1）步生成的 B 字长字符串与 opad 做异或运算；

6）将第 4）步的结果填充进第 5）步的结果中；

7）用 H 作用于第 6）步生成的数据流，输出最终结果。

哈希水印的嵌入主要有两种方法[15-16]，本文采用第二种方法[16]。将原始图像进行分块，将哈希水印嵌入到分块的中低频系数上，反转各分块系数，就完成水印的嵌入。

图像认证问题可以看作是假设检验问题，有如下两个假设：

H_0：图像不可认证

H_1：图像可认证

从待认证图像中提取水印，经过非对称解密，得到原始图像的摘要，用 h_1 表示。待认证图像同样采用分块随机投影，利用 HMAC 算法得到待认证图像的摘要，用 h_2 表示。定义两者的汉明距离如下：

$$d(h_1, h_2) = \frac{1}{L}\sum_{k=1}^{L} |h_1(k) - h_2(k)| \tag{12}$$

其中，L 是哈希的长度。如果：

$$d(h_1, h_2) < \eta \tag{13}$$

则认为图像是可认证的，η 是一个确定性阈值。

2 实验结果与分析

为了验证本文算法的有效性，分别从水印鲁棒性以及篡改定位两方面对算法进行仿真实验和分析，实验环境为 Windows XP、Matlab 7.0。

鲁棒性要求加入的水印能抵抗各种常规的信号处理，如平移、缩放、旋转、锐化、滤波等，以及一般性攻击，如裁剪。通过对加入水印的图像进行各种攻击，然后从受攻击图像中提取水印，并与原始水印进行对比来验证水印的鲁棒性。通常使用 RMSE（均方根误差）和 PSNR（峰值信噪比）来衡量水印的鲁棒性。RMSE 的值越小，则水印的抗

攻击能力越强。设 n 表示图像的大小（像素），m 表示压缩传感随机测量数，m/n 表示压缩测量比率。图 2 给出了 Lena 图像在几种常规信号处理下所对应的 RMSE 与压缩测量比率之间的关系，图 3 给出了 Lena 图像在不同的裁剪比例下所对应的 RMSE 与压缩测量比率之间的关系。当压缩测量比率较低时，极少量的压缩测量值无法完全表示图像的内容特征，当含水印图像受到攻击时，水印容易受到破坏，因此从受攻击图像中提取的水印与原始水印之间的 RMSE 值较大。当达到一定的压缩测量比率（这里是 0.05）以后，RMSE 变得很小，表明水印具有很强的鲁棒性。随着压缩测量比率的提高，RMSE 变化不大，表明一定数量的压缩传感随机测量值就能够很好地表示图像的内容特征，由此生成的水印具有很强的鲁棒性。

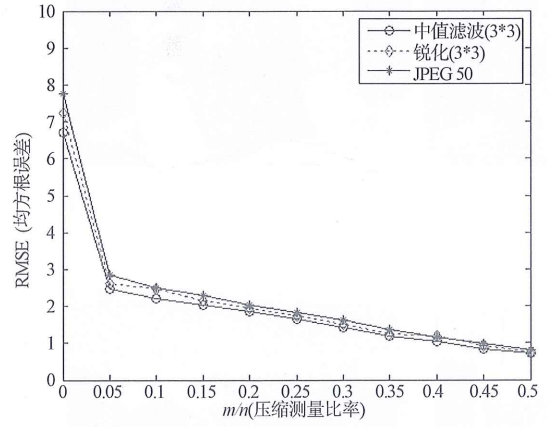


图 2　针对常规信号处理的水印鲁棒性分析

Fig. 2　Watermark robustness towards common signal processing

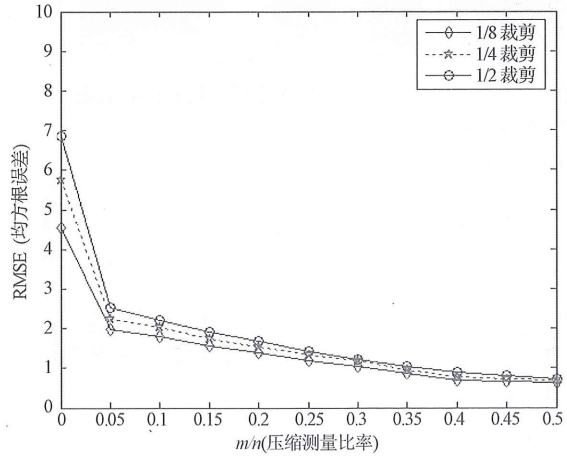


图 3　针对剪裁几何攻击的水印鲁棒性分析

Fig. 3　Watermark robustness towards cropping attack

除 RMSE 以外，还可以利用 PSNR 来衡量水印的鲁棒性，PSNR 定义如下：

$$\mathrm{PSNR} = 10\lg\left[\frac{255 \times 255}{\frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n} | W_O(i,j) - W_T(i,j) |^2}\right] \tag{14}$$

W_O 是原始水印，W_T 是从受攻击图像中提取的水印。表 1 给出了文献［17］、文献［18］以及本文算法对不同的常规信号处理的水印鲁棒性能对比。从表中可以看出，本文的水印具有更强的鲁棒性。

表 1　不同算法的水印鲁棒性比较

Table 1　Compare of watermark robustness among different algorithms

攻击方式	文献[17]算法	文献[18]算法	本文算法
中值滤波(3 * 3)	31.53	29.14	32.64
锐化(3 * 3)	22.24	23.54	24.43
高斯滤波(3 * 3)	33.73	32.85	35.12
JPEG 50	35.42	33.63	36.17
JPEG 80	38.13	37.42	39.69

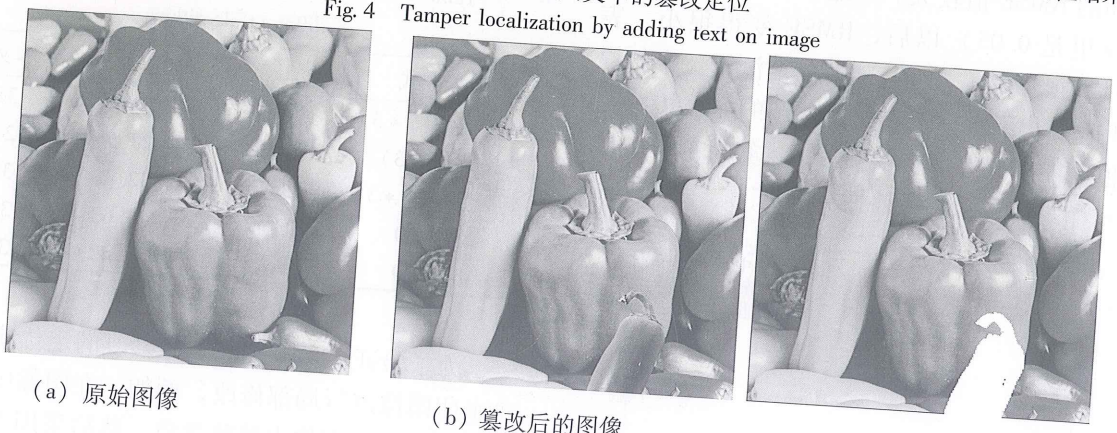
为了验证本文算法对图像篡改的定位能力，对含水印图像进行局部修改，例如：在图像中增加文本、景象，从图像中移除景象，然后采用本文算法进行篡改定位。图 4 是在图像中加入文本的篡改定位，图 5 是在图像中增加景象（插入青椒）的篡改定位，图 6 是在图像中移除景象（移除一棵小树）的篡改定位。从图中可以看出，本文算法具有较好的篡改检测和定位能力。

定义篡改检测概率为：$P = N_d/N_e$（N_e 为随机篡改的像素点个数，N_d 为实际检测到的像素点个数）。设 n 表示图像的大小（像素），k 表示图像中非零系数的个数，k/n 表示图像的稀疏度。图 7 给出了不同稀疏度的图像所对应的压缩传感测量数与篡改检测概率的关系。当测量次数较少时，其压缩测量值无法完全表示图像的内容特征，通过比较由压缩测量值表示的图像摘要来进行篡改检测和定位，其篡改检测概率相对较低。对于一幅 512 * 512 的图像，当测量次数为 400 时，篡改检测概率达到最高，随着测量次数的增加，篡改检测概率有所降低。在测量次数相同的条件下，图像的稀疏度越高（k/n 的值越小），其篡改检测概率也越高。对 Lena 的含水印图像随机篡改若干个像素点，分别采用文献［17］、文献［18－19］以及本文算法进行篡改检测，图 8 给出了这几种算法的篡改检测概率对比。从图中可以看出，本文算法具有较高的篡改检测概率。

（a）原始图像　（b）篡改后的图像　（c）图像篡改定位结果

图4　图像中加入文本的篡改定位

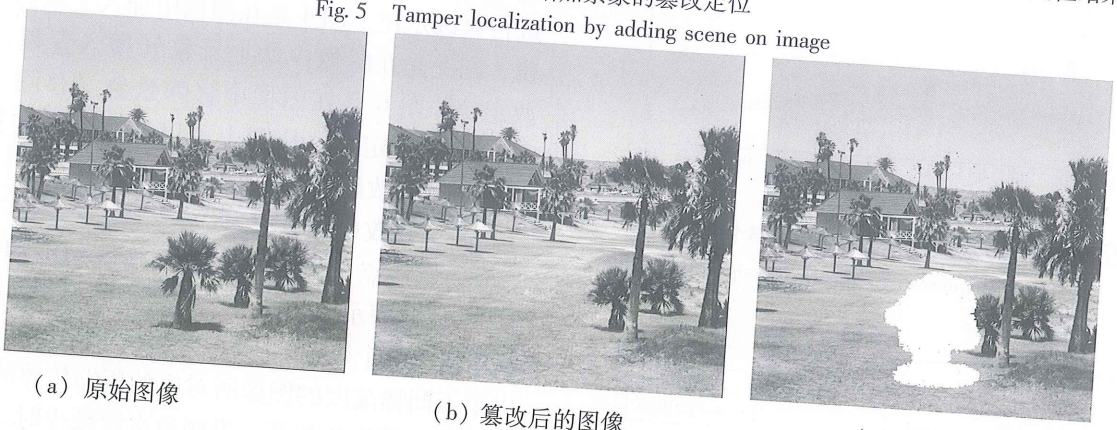
Fig. 4　Tamper localization by adding text on image



（a）原始图像　（b）篡改后的图像　（c）图像篡改定位结果

图5　图像中增加景象的篡改定位

Fig. 5　Tamper localization by adding scene on image



（a）原始图像　（b）篡改后的图像　（c）图像篡改定位结果

图6　图像中移除景象的篡改定位

Fig. 6　Tamper localization by removing scene on image

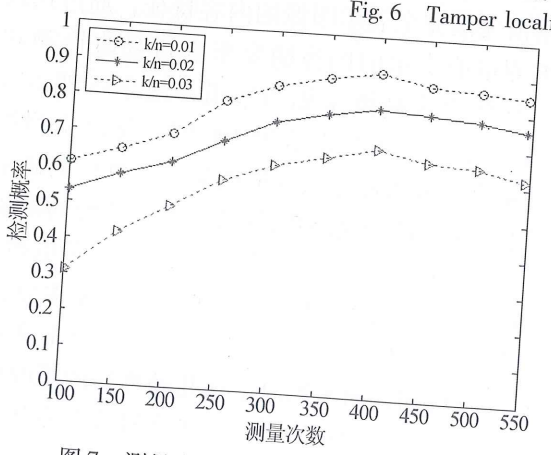


图7　测量次数与篡改检测概率的关系

Fig. 7　Relation between measurement times and tamper detection probability

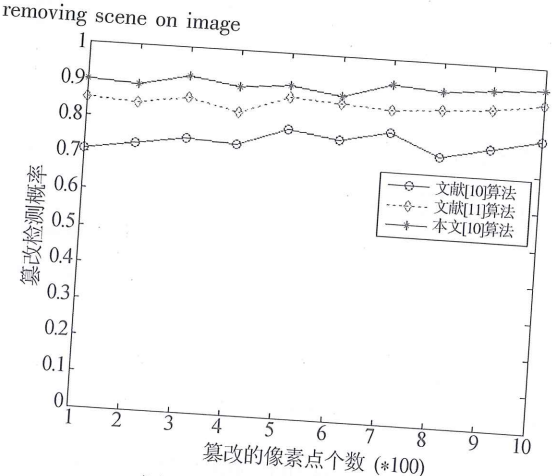


图8　篡改检测概率对比

Fig. 8　Compare of the probability of tamper detection

3　结　论

本文提出的基于压缩传感的图像哈希水印算法，通过压缩传感随机投影得到的压缩测量值可以作为图像的内容特征，由测量值生成的图像哈希水印具有很强的鲁棒性和安全性以及篡改检测能力，为新水印算法的研究提供了一个参考的途径。理论分析与实验结果表明，本文提出的算法与其他算法相比有着更高的检测概率、更强的鲁棒性以及更好的定位能力，因此有着更广阔的应用前景。

参考文献：

[1] CANDES E J, WAKIN M B. An introduction to compressive sampling [J]. IEEE Signal Processing Magazine, 2008, 25(2): 21 - 30.

[2] VALENZISE G, TAGLIASACCHI M, TUBARO S. A compressive-sensing based watermarking scheme for sparse image tampering identification [C] // Image Processing (ICIP), 2009 16th IEEE International Conference, 2009: 1265 - 1268.

[3] TAGLIASACCHI M, VALENZISE G, TUBARO S. Hash-based identification of sparse image tampering [J]. IEEE Transactions on Image Processing, 2009, 18(11): 2491 - 2504.

[4] RICHARD B, MARK D, RONALD D. A simple proof of the restricted isometry property for random matrices [J]. Constructive Approximation, 2009, 3(28): 253 - 263.

[5] CANDES E J. The restricted isometry property and its implications for compressed sensing [J]. Applied & Computational Mathematics, 2008, 346(1): 589 - 592.

[6] WOJTASZCZYK P. Stability and instance optimality for Gaussian measurements in compressed sensing [J]. Foundations of Computational Mathematics, 2010, 10 (1): 1 - 13.

[7] ZHANG G S, JIAO S H, XU X L, WANG L. Compressed sensing and reconstruction with bernoulli matrices [C]. Information and Automation (ICIA), 2010 IEEE International Conference, 2010: 455 - 460.

[8] CANDES E J, WAKIN M B. An introduction to compressive sampling [J]. IEEE Signal Processing Magazine, 2008, 25(2): 21 - 30.

[9] WOJTASZCZYK P. Stability of l1 minimization in compressed sensing [C] // Signal Processing with Adaptive Structured Representations (2009), 2009: 1 - 5.

[10] SALIGRAMA V, ZHAO M Q. Thresholded basis pursuit: Quantizing linear programming solutions for optimal support recovery and approximation in compressed sensing[C] // Preprint, 2008.

[11] RACHLIN Y, BARON D. The secrecy of compressed sensing measurements [C] //2008 46th Annual Allerton Conference, 2008: 813 - 817.

[12] IWEN M. A deterministic sub-linear time sparse Fourier algorithm via non-adaptive compressed sensing methods [C] // Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms, 2008: 20 - 29.

[13] 张宝华，殷新春. RSA 密码算法的安全及有效实现 [J]. 中山大学学报：自然科学版，2008，47(6)：22 - 26.

[14] 韩国军，刘星成. 基于校验节点的 LDPC 码的消息加权均值串行译码算法[J]. 中山大学学报：自然科学版，2010，49 (3)：47 - 51.

[15] 付炜，邢广忠. 置换 DCT 域中频系数的盲水印嵌入算法研究[J]. 计算机应用研究，2008，24(3)：160 - 162.

[16] 王员根，梁凡，肖明明. 一种彩色图像 DC 系数的自适应水印算法[J]. 中山大学学报：自然科学版，2010，49 (4)：43 - 48.

[17] TANG C W, HANG H M. A feature-based robust digital image watermarking scheme [J]. IEEE Transactions on Signal Processing, 2009, 51(4): 950 - 959.

[18] LIN K Z, LI D Q, LI S H. Fragile image watermarking algorithm based on hash functions [J]. Journal of Harbin Engineering University, 2008, 29(1): 61 - 64.

[19] 梁长垠，李昂，牛夏牧. 基于云水印的视频内容认证技术[J]. 中山大学学报：自然科学版，2009，48 (1)：26 - 30.