基于压缩感知的图像盲水印算法

温健阳 宫宁生 陈 岩
(南京工业大学计算机科学与技术学院 南京 211816)

摘 要 针对现代数字水印的设计要求,结合压缩感知理论,提出一种图像盲水印算法。该算法利用自然载体图像在小波域中稀疏的特性,将加密后的水印嵌入载体图像离散小波变换系数中。提取水印时,无需原始载体图像或其他先验知识,根据向量空间、矩阵方程的一些性质,以及压缩感知的重构算法,只需一个密钥(随机数种子)即可从嵌有水印的载体图像中精确提取水印并重构原始载体图像。实验证明,该水印算法具有良好的特性,能够满足实际应用的要求。

关键词 压缩感知,盲水印,图像重建
中图法分类号 TP301.6,TP309,TN911.73 **文献标识码** A

Blind Image Watermark Algorithm Based on Compressed Sensing

WEN Jian-yang GONG Ning-sheng CHEN Yan
(College of Computer Science & Technology, Nanjing Tech University, Nanjing 211816, China)

Abstract Aiming at modern image watermark design requirements, a compressed sensing (CS) based watermark algorithm was proposed. Since natural digital image is sparse in wavelet domain, cipher watermark image is embedded in the wavelet transform coefficients of the carrier image. If only the cipher key (a random seed) is known, the watermark image can be perfectly recovered, according to some properties of vector space and matrix and a CS reconstracion algorithm, dispensing with the original carrier image or other prior information. The experiments prove that this performance of watermark algorithm is so fine, and it can entirely fulfil the requirements of practical application.

Keywords Compressed sensing, Blind watermark, Image reconstraction

数字图像水印技术作为一种信息隐藏、数据认证、版权保护的重要技术手段,受到了国内外研究人员的长期关注,相应的算法也不断被提出。但是人们对水印算法隐蔽性、鲁棒性、安全性的要求却日益提高,一些传统算法已经不能完全满足现代应用的需要。

压缩感知(Compressive Sensing,CS)理论由 Candès[1] 和 Donoho[2] 于 2006 年正式提出,其核心思想是将压缩与采样同时进行,即将高维原始信号通过一个测量矩阵向低维空间线性投影,得到低维的测量值。可以证明,当原始信号、测量矩阵满足一定条件时,可以通过求解一个最优化问题从测量值中恢复出原始信号。该理论突破了传统 Nyquist-Shannon 采样定理的束缚,使人们得以通过远少于传统方法的测量值精确重构高维信号,这项研究成果给现代信号处理带来了极大的灵活性。

本文基于压缩感知理论,针对现代数字水印的设计要求,提出了一种图像盲水印算法,并从理论、实验两方面论证了该算法的良好特性。相较于目前常用的图像水印算法,本文算法只需一个密钥(随机数种子),无需原始载体图像或其他先验知识,即可从嵌有水印的载体图像中精确提取水印,重构原始载体图像。

1 基础概念

1.1 空间和运算

设 V 是实数域$\mathbb{R}$上的一个 N 维 Euclid 空间,可将一维有限长实值离散信号看成分布于该空间中的向量。在 Euclid 空间 V 中有标准内积:

$$\langle x,z\rangle = z^{\mathrm{T}}x = \sum_{i=1}^{N} x_i z_i \tag{1}$$

当 $p\geqslant 1$ 时,在 Euclid 空间 V 中定义范数 ℓ_p:

$$\|x\|_p = \begin{cases} (\sum_{i=1}^{N} |x_i|^p)^{\frac{1}{p}}, & p\in[1,\infty) \\ \max\limits_{1\leqslant i\leqslant N} |x_i|, & p=\infty \end{cases} \tag{2}$$

当 $p<1$ 时,式(2)中定义的范数已经无法满足三角不等式。但为了方便讨论,本文将 ℓ_0 范数记为:

$$\|x\|_0 = |supp(x)| \tag{3}$$

其中,$supp(x)=\{i:x_i\neq 0\}$ 表示 x 的支撑集,简称为支撑;$|\Omega|$ 表示集合 Ω 的基数,即集合 Ω 中元素的个数。

如果信号 x 满足:

$$sup\|x\|_0 = K \tag{4}$$

则称信号 x 是 K-稀疏的。

本文受国家重点基础研究发展计划(973 计划)(2005CB321901),软件开发环境国家重点实验室开放课题(BUAA-SKLSDE-09KF-03)资助。
温健阳(1992-),男,硕士生,主要研究方向为数字信号处理、图像处理,E-mail:wjy200701007@sina.com;宫宁生(1958-),男,教授,主要研究方向为模式识别、图像处理;陈 岩(1992-),男,硕士生,主要研究方向为模式识别、图像处理。

根据式(1)的内积定义可以导出 ℓ_2 范数 $\|x\|_2=\langle x,x\rangle^{\frac{1}{2}}$。因为有限维赋范线性空间必完备，显然，按范数 $\|x\|_2=\langle x,x\rangle^{\frac{1}{2}}$ 完备的 Euclid 空间 V 是一个 Hilbert 空间。

本文将两维维数分别为 M,N 的灰度图像 I 看成分布于 $M\times N$ 维 Hilbert 空间上的矩阵，由上述向量的内积、范数运算可以诱导出相应的矩阵运算。这给讨论图像重建过程中的逼近和优化问题带来了方便，并使我们得以在此空间中对图像或图像变换进行谱分析和多尺度分析。

将此实数域 $\mathbb{R}$ 上的 $M\times N$ 维 Hilbert 空间 $(V,\langle\cdot\rangle,\|\cdot\|)$ 简记为 $\mathbb{R}^{M\times N}$。

1.2 矩阵方程

考虑矩阵方程：

$$Ax=b \tag{5}$$

$$\text{with } A\in\{\Omega\in\mathbb{R}^{M\times N}:rank(\Omega)=\min(M,N)\}$$

$$x\in\mathbb{R}^N,b\in\mathbb{R}^M$$

注意到 A 是一个 $M\times N$ 维的满秩矩阵。

1)当 $rank(A|b)=rank(A)=\min(M,N)=N\leqslant M$ 时，式(5)是一个适定方程，有唯一解。

2)当 $rank(A|b)=rak(A)=\min(M,N)=M<N$ 时，此时 A 是行满秩矩阵，式(5)是一个欠定方程，在数学上有无穷多组解。本文第 2 节将结合实际讨论该问题。

3)当 $rank(A|b)>rank(A)$ 时，必有 $M>N$，A 是列满秩矩阵，式(5)是一个超定方程，没有通常意义上的解，但在数值计算领域，往往通过 ℓ_2 范数最小化来求得近似解 $\hat{x}$：

$$\hat{x}=\arg\min\|A\hat{x}-b\|_2=\arg\min\|A\hat{x}-b\|_2^2 \tag{6}$$

其中，

$$\begin{aligned}\|A\hat{x}-b\|_2^2&=(A\hat{x}-b)^{\mathrm{T}}(A\hat{x}-b)\\&=(A\hat{x})^{\mathrm{T}}A\hat{x}-2b^{\mathrm{T}}A\hat{x}+\|b\|_2^2\end{aligned} \tag{7}$$

对 $\hat{x}$ 求偏导数，得：

$$\frac{\partial}{\partial\hat{x}}\to 2A^{\mathrm{T}}A\hat{x}-2A^{\mathrm{T}}b\overset{\triangle}{=}0\Rightarrow\hat{x}=(A^{\mathrm{T}}A)^{-1}A^{\mathrm{T}}b \tag{8}$$

式(8)通常称为该超定矩阵方差的最小二乘解。

从向量空间的角度，方程(5)无解是由于：

$$b\notin span\{col(A)\} \tag{9}$$

式(9)表示向量 b 不在矩阵 A 列向量的集合张成的向量空间中，而 b 在空间 $span\{col(A)\}$ 上的投影 p 为：

$$p=A(A^{\mathrm{T}}A)^{-1}A^{\mathrm{T}}b \tag{10}$$

令 $p=A\hat{x}$，同样可以得到式(8)。

从广义逆矩阵的角度，列满秩非方矩阵 A 的 Moore-Penrose 逆：

$$\begin{aligned}&\forall A\in\{\Omega\in\mathbb{R}^{M\times N}:M>N\wedge rank(\Omega)=N\}\\&A^{+}=(A^{\mathrm{T}}A)^{-1}A^{\mathrm{T}}\end{aligned} \tag{11}$$

同样可以导出式(8)的结果。

2 压缩感知理论[3]

考察一维有限长实值离散信号 $x\in\mathbb{R}^N$，此信号可由一组基 $\Psi\in\mathbb{R}^{N\times N}$ 来表示：

$$x=\Psi s \tag{12}$$

其中，$s\in\mathbb{R}^N$ 是 x 在基 Ψ 上的系数向量。显然，s 和 x 在信号表示方面是等价的，当 $sup\|s\|_0=K$ 时，则称 x 在基 Ψ 下是 K-稀疏的。

此时，构造一个测量矩阵 $\Phi\in\mathbb{R}^{M\times N}$ 对信号 x 进行观测，设所得观测值为 $y\in\mathbb{R}^M$，即：

$$y=\Phi x=\Phi\Psi s=\Theta s \tag{13}$$

其中，$\Theta=\Phi\Psi\in\mathbb{R}^{M\times N}$ 为感知矩阵，如图 1 所示。

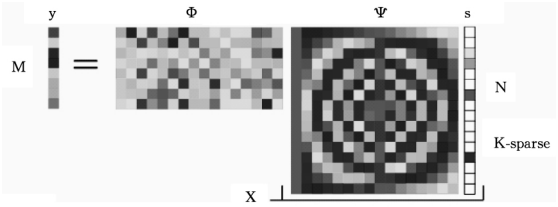


图 1 测量矩阵 Φ 对信号 $x=\Psi s$ 进行观测，得观测值 y

图 2 感知矩阵 $\Theta=\Phi\Psi$ 对 K-稀疏($K=4$)的 s 进行观测

需要注意的是，式(13)是一个欠定矩阵方程，不能通过常规的方法来求解。Candès 等[4]证明了当 Θ 满足一定条件(3.4 节将具体讨论)，且 $M\geqslant O(K\log N)$ 时，N 维稀疏信号 s 可由 M 维的观测值 y 通过求解最小化 ℓ_0 范数问题精确重构：

$$\hat{s}=\arg\min\|\hat{s}\|_0\quad \text{s.t.}\ \Theta\hat{s}=y \tag{14}$$

而当 $K\leqslant M\ll N$ 时，由少量的观测值即可精确重建高维原始信号。以上就是压缩感知的基本原理。

压缩感知理论下一般信号的采集与重构[5]如图 3 所示。

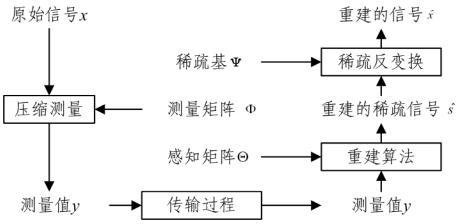


图 3 压缩感知理论下一般信号的采集与重构

由以上讨论可知，压缩感知在实际应用时需要注意：1)稀疏基的构造；2)测量矩阵 Φ 的构造；3)重建算法的设计。

3 本文算法设计

本节主要阐述水印算法的设计思想，本文算法的具体实现步骤见第 4 节。

3.1 数字水印的设计要求

数字水印可定义为永久嵌入在其他数字信息中的具有一定意义的数字信息，并且不影响载体数据的可用性。因此，数字水印在设计时应当考虑以下几个特性。

1)隐蔽性

隐蔽性指水印信息不影响载体信息的正常使用，这不仅要求人体视听感官对添加的水印不敏感，还要求具有统计学上的隐蔽性，即通过统计学方法无法确定载体中是否含有水印。

2)鲁棒性

鲁棒性指载体在经过各种有意、无意的信号处理或外部

攻击后，仍可从中恢复出有效水印的特性。

3)安全性

安全性指在未获得密钥的情况下，水印信息难以被破译、篡改或伪造。

4)盲源提取

盲源提取是指在提取水印时，只需要密钥，无需原始载体图像，符合这一要求的水印算法叫做盲水印。目前，很多文献研究的水印算法都是非盲的，但在实际应用中，为了提取水印而同时保存、传输原始载体图像和含水印图像是不合理的，因为这会造成所需存储空间、传输带宽不必要的成倍增加。

本文算法只需有密钥和含水印图像，即可提取水印信息，精确重建原始图像，符合实际应用的要求。

5)数据容量

嵌入容量指单位规模的载体能够承载的水印信息量，水印算法的数据容量越大，一定规模的载体就能够承载越多的水印信息。过大的数据容量往往会影响水印的隐蔽性和鲁棒性，所以在算法设计时需要在这 3 个特性间寻求平衡。

6)算法效率

算法效率指将水印信息嵌入载体图像得到含水印图像的时间。对于任何一种算法，执行效率都是制约其实际应用的一大因素，而在实时性要求不高的数字图像水印领域，算法效率的重要性往往低于隐蔽性、鲁棒性等更为核心的特性。

3.2 本文水印算法理论模型

先讨论一个图像纠错问题，考虑这样一个信号模型：

$$\begin{aligned}&y=Af+e\\&\text{with } A\in\{\Omega\in\mathbb{R}^{M\times N}:M>N\}\\&f\in\mathbb{R}^N,e\in\mathbb{R}^M,y\in\mathbb{R}^M\end{aligned}\tag{15}$$

其中，f 是原始信号，A 是已知的线性编码矩阵，e 是未知的随机误差，y 是含有误差的观测值。如何从观测值 y 中恢复出原始信号 f？Candès 和 Tao[6,7] 给出了一种解决方案：

在实际情况下，往往 A 是满秩的，且 e 是 K-稀疏的。构建一个 $F\in\mathbb{R}^{(M-N)\times M}$，满足 $FA=0$（即 F 行向量张成的子空间和 A 列向量张成的子空间正交，亦即 $span(row(F))\perp span(col(A))$）。此时有：

$$\begin{aligned}&\tilde{y}=F(Af+e)=Fe\\&\text{with } A\in\{\Omega\in\mathbb{R}^{M\times N}:M>N\wedge rank(\Omega)=N\}\\&e\in\{\Omega\in\mathbb{R}^M:sup\,\|\,\Omega\,\|_0=K\}\\&F\in\{\Omega\in\mathbb{R}^{(M-N)\times M}:M>N\wedge\Omega A=0\}\\&f\in\mathbb{R}^N,\tilde{y}\in\mathbb{R}^M\end{aligned}\tag{16}$$

比较式(13)和式(16)，易知这是一个压缩感知问题，根据第 2 节的讨论，从 $\tilde{y}$ 中重建 e，得到 e 的估计值 $\hat{e}$。再利用 1.2 节关于超定矩阵方差的讨论，可以求得 f 的估计值 $\hat{f}$：

$$\begin{aligned}&\hat{f}=A^+(y-\hat{e})\\&\text{with } A\in\{\Omega\in\mathbb{R}^{M\times N}:M>N\wedge rank(\Omega)=N\}\\&A^+\triangleq(A^{\mathrm{T}}A)^{-1}A^{\mathrm{T}}\\&\hat{f}\in\mathbb{R}^N,y\in\mathbb{R}^M,\hat{e}\in\mathbb{R}^M\end{aligned}\tag{17}$$

Sheikh 和 Baraniuk[4] 提出一种将式(16)模型应用到数字信号水印中的思想，本文的水印算法即是基于这种思想的实现，于是提出水印模型：

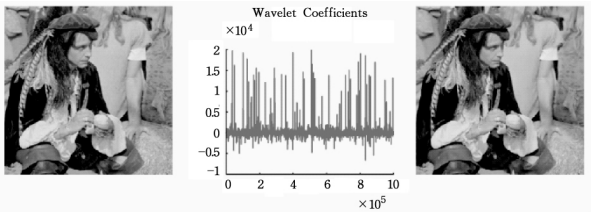
$$\begin{aligned}&D'=AW+D\\&\text{with } A\in\{\Omega\in\mathbb{R}^{M\times N}:M>N\wedge rank(\Omega)=N\}\\&D\in\{\Omega\in\mathbb{R}^{M\times N}:sup\,\|\,\Omega\,\|_0=K\}\\&W\in\mathbb{R}^{M\times N},D'\in\mathbb{R}^{M\times N}\end{aligned}\tag{18}$$

其中，W 是水印信息，A 是加密矩阵，D 是原始载体变换域系数，D' 是嵌入水印后的变换域系数。

3.3 稀疏表示

根据第 2 节的讨论，通过压缩感知重建的信号必须是稀疏的，即式(18)中的 D 是稀疏的，这就要求在嵌入水印之前对载体图像进行稀疏表示。近十年来，由于压缩感知、深度学习、特征提取、结构化信号处理等领域的需要，人们对信号稀疏性分析的研究日益深入，也产生了很多关于稀疏基（字典）的理论和算法[8]。为了水印算法整体的低复杂、高效率，选择常用的图像变换对原始载体图像进行稀疏化。

自然图像在变换域里往往都是稀疏或近似稀疏（能量集中在少数分量上，绝大多数分量接近 0）的，如图 4 所示。



(a) (b) (c)

图 4 图像 Pirate 在小波域中的近似稀疏性[9]

图 4(a)是 Pirate 的原始图像；图 4(b)是图像 Pirate 的小波系数，可知图像能量集中在少数系数上，绝大部分系数接近 0；图 4(c)是抽取这些小波系数中绝对值最大的 2.5% 的系数（丢弃了那些接近 0 的，占小波系数总量 97.5% 的系数）重建的图像。

常用的图像变换有：谱分析中的快速傅里叶变换、离散余弦变换和多尺度分析中的 Wavelet、Beamlet、Bandelet、Ridgelet、Curvelet 等，它们都能够对信号进行较好的稀疏分解。本文选用小波（Wavelet）分解对载体图像进行稀疏表示，在稀疏的水平细节分量、垂直细节分量、对角细节分量中重复嵌入水印信息，提取时利用投票来确定最终的水印信息，提高了算法的鲁棒性。

在 Matlab 下，需要设置小波延拓模式（dwtmode('symw');），否则提取出的水印边缘会出现问题。

3.4 测量矩阵

对于式(13)，感知矩阵 Θ 必须满足一定条件才能通过压缩感知算法重建信号。Candès 和 Tao[6] 对此进行了讨论，并给出了数学证明。根据其研究有如下定义。

定义 1[6,10] 对于 $\Theta\in\mathbb{R}^{M\times N}$，如果

$$\begin{aligned}&\exists\,\delta_K\in(0,1)\\&\forall\,T\in\{\Omega\subset\{1,2,3,\cdots,N\}:|\Omega|\leqslant K\}\\&\forall\,c\in\mathbb{R}^{|T|}\\&(1-\delta_K)\,\|\,c\,\|_2^2\leqslant\|\,\Theta_T c\,\|_2^2\leqslant(1+\delta_K)\,\|\,c\,\|_2^2\end{aligned}\tag{19}$$

则称 Θ 满足 K 阶约束等距条件（Restricted Isometry Property，RIP），简记为 $\Theta\in RIP^K$。

说明：

1)集合 T 是 Θ 中部分列向量的索引集；2)$\Theta_T\in\mathbb{R}^{M\times|N|}$ 是由集合 T 确定的列向量组成的矩阵；3)K 阶是由“$\forall\,T\in\{\Omega\subset$

$\{1,2,3,\cdots,N\}:|\Omega|\leqslant K\}$"中的"$K$"确定的。

定理 1[11]

$$\begin{aligned}&\forall s\in\{\Omega\in\mathbb{R}^N:sup\,\|\Omega\|_0=K\}\\&\forall\Theta\in\{\Omega\in\mathbb{R}^{M\times N}:\Omega\in RIP^{2K}\}\\&y\overset{\triangle}{=}\Theta s\\&\rightarrow\exists\,!\hat{s}\overset{\triangle}{=}\arg\min\|\hat{s}\|_0\quad\text{s.t.}\,\Theta\hat{s}=y\end{aligned}\tag{20}$$

即式(13)中,对于 K-稀疏的信号 s,如果感知矩阵 Θ 满足 $2K$ 阶 RIP(即定理 1 对于 $\forall T\in\{\Omega\subset\{1,2,3,\cdots,N\}:|\Omega|\leqslant 2K\}$ 成立),则式(14)的解 $\hat{s}$ 存在且唯一。

注意,在本文水印算法中,先将信号经过小波变换稀疏化,再利用测量矩阵进行观测,此时测量矩阵 Φ 即等同于感知矩阵 Θ。

根据 Candès 和 Tao[6,12] 的讨论,Gauss 随机矩阵作为测量矩阵具有良好的性能,Candès,Tao[12] 和 Baraniuk[13] 从理论上证明了 Gauss 随机矩阵、Bernoulli 随机矩阵有很大概率满足 RIP。

定理 2[12-14] 对于一个 Gauss 随机矩阵或者 Bernoulli 随机矩阵:

$$\begin{aligned}&\Phi\in\mathbb{R}^{M\times N}\\&K\leqslant\frac{C_1M}{\log\frac{N}{K}}\\&\rightarrow P(\Phi\in RIP^K)\geqslant 1-e^{-C_2M}\end{aligned}\tag{21}$$

其中,C_1,C_2 是仅依赖于 RIP 常数 δ_K 的常数,$P(\Phi\in RIP^K)$ 表示 Φ 满足 K 阶 RIP 的概率。

根据以上讨论,本文选用 Gauss 随机矩阵作为测量矩阵。

3.5 重建算法

式(14)的 ℓ_0 范数最小化问题是一个 NP-hard 问题,无法直接通过穷举得到全局最优解。考虑到 ℓ_1 范数为范数 ℓ_0 的最优凸近似,有一种思路是通过求解 ℓ_1 范数最小化问题来替代,将 ℓ_0 范数问题归约到数学理论已经非常成熟的凸优化领域。Candès,Romberg,Tao[15] 和 Donoho[2] 从理论上证明了在压缩感知问题中,当感知矩阵 $\Theta\in RIP^{2K}$,且 $\delta_{2K}<\sqrt{2}-1$ 时,求解 ℓ_1 范数和 ℓ_0 范数是等价的。本文在实验中尝试用凸优化算法 Split-Bregman 迭代重建压缩感知图像,收敛速度很快。

文献[16,17]通过大量实验发现,在常用的重建算法中,一种贪婪算法——压缩采样匹配追踪算法(Compressive Sampling Marching Pursuit,CoSaMP)[18] 精确重建的概率最高,本文使用的即是这种重建算法。其算法流程描述如下[19]:

任务:$\hat{s}=\arg\min\|\hat{s}\|_0\quad\text{s.t.}\,\Theta\hat{s}=y$

输入:感知矩阵 Θ、测量值 y、稀疏度 K

初始化:迭代次数 t=0,残差 r=y,选取列向量的索引集 $\Lambda_0=\varnothing$

主循环:

步骤 1 t=t+1;

步骤 2 选出 Θ 中和 r 内积的 ℓ_2 范数最大的 2K 列,其索引集为 Ω;

步骤 3 更新索引集 $\Lambda_t=\Lambda_{t-1}\cup\Omega$;

步骤 4 重建 $\tilde{s}=\Theta_{\Lambda_t}^{+}y\in\mathbb{R}^{2K}$,$\Theta_{\Lambda_t}$ 表示矩阵 Θ 中由索引集 Λ_t 确定的列向量组成的矩阵,$\Theta_{\Lambda_t}^{+}$ 表示 Θ_{Λ_t} 的 Moore-Penrose 逆;

步骤 5 选取 $\tilde{s}$ 中 K 个最大的分量,得 $\hat{s}=(\tilde{s})^K\in\mathbb{R}^K$,更新索引集 $\Lambda_t=\{\tilde{s}$ 中 K 个最大分量的索引$\}$;

步骤 6 更新残差 $r=y-\Theta\hat{s}$;

终止条件:迭代次数 t=K

输出:系数向量估计 $\hat{s}$

需要说明的是:1)步骤 2 每次迭代入选 $2K$ 个列向量,加快了收敛速度;2)步骤 4 使用了 1.2 节关于超定矩阵方程讨论的内容;3)步骤 5 每次迭代剔除索引集中 K 个最小的分量,降低了陷入局部极小的可能性。

3.6 逐列压缩感知

经过第 2 节的介绍,可以看到压缩感知算法压缩、重建的对象是列向量,而图像在本文模型下是一个矩阵。如果将 $M\times N$ 维的矩阵重塑(reshape)成一列有 $M\times N$ 个元素的列向量,这样重建算法需要迭代的次数过多,严重影响收敛性。

有学者提出分块压缩感知(Block Compressed Sensing,BCS)的概念,即对整幅图像进行分块,将每一小块重塑成列向量。本文对此进行了实验,发现 BCS 重建的图像存在严重的分块效应,即分块的边缘重建效果差,有肉眼可观的明显失真。根据李然等人[20] 的研究,主要由 3 个原因造成:分块稀疏度不均匀、频谱泄漏和块尺寸受限,由此他们提出了"全局重构模型",对于算法的运算量有一定增加。

本文将图像矩阵看作是列向量的集合,对其进行逐列压缩感知,不增加运算量,且无明显失真。

3.7 测量矩阵、加密矩阵与密钥

本文以 Matlab 为实验平台,以 randn 函数生成 Gauss 随机测量矩阵 $\Phi\in\mathbb{R}^{(M-N)\times M}$,随机数种子(一个非负整数)可以作为密钥,这样避免了对整个随机矩阵的存贮,即节省了空间,也保证了水印算法的安全性。

式(18)使用的加密矩阵 A 对水印有着加密、置乱的效果。常用的置乱 Arnold 变换虽然简单、置乱效果好,但是具有周期性,容易被穷举法破解。

根据 $\Phi A=0$,在 Matlab 中可以通过求零空间的 null 函数生成加密矩阵 $A\in\mathbb{R}^{M\times N}$,即任一满足 $\Phi A=0$ 的矩阵 A 均可人为选作加密矩阵。虽然由 $\Phi A=0$ 确定的矩阵 A 不是唯一的,但在程序中由函数计算出的 A 是唯一的。因此,只需密钥即可确定唯一的测量矩阵 Φ 和唯一的加密矩阵 A。

4 本文算法的实现步骤

4.1 水印的嵌入

水印嵌入算法如图 5 所示。

步骤 1 选定作为水印的二值图像 $W\in\mathbb{R}^{M\times N}$(为方便运算,本文将"0、1"二值的 W 映射到"−1、1"二值);

步骤 2 由特定随机数种子(作为密钥)生成 Gauss 随机测量矩阵 $\Phi\in\mathbb{R}^{(M-N)\times M}$;

步骤 3 根据 $\Phi A=0$,生成列满秩的加密矩阵 $A\in\mathbb{R}^{M\times N}$;

步骤 4 将载体图像 I 进行一阶二维离散小波变换,得到近似分量 $D_A\in\mathbb{R}^{M\times N}$、水平细节分量 $D_H\in\mathbb{R}^{M\times N}$、垂直细节分量 $D_V\in\mathbb{R}^{M\times N}$、对角细节分量 $D_D\in\mathbb{R}^{M\times N}$;

步骤 5 将加密后的稀疏水印 $AW\in\mathbb{R}^{M\times N}$ 以强度 α 加性嵌入载体图像小波细节分量中,得:

$$\begin{aligned}D_H'&=D_H+\alpha AW\\D_V'&=D_H+\alpha AW\end{aligned}\tag{22}$$

$D_D' = D_H + \alpha AW$

步骤 6　由小波分量 D_A、D_H'、D_V'、D_D' 进行小波反变换，得到嵌入水印后的图像 I'。

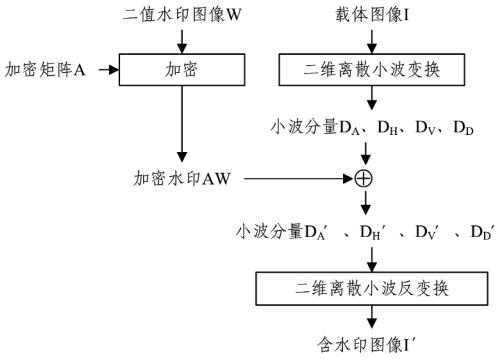


图 5　水印嵌入流程图

4.2　水印提取和原始图像重建

水印提取和原始图像重建过程是水印嵌入的逆过程，如图 6 所示。

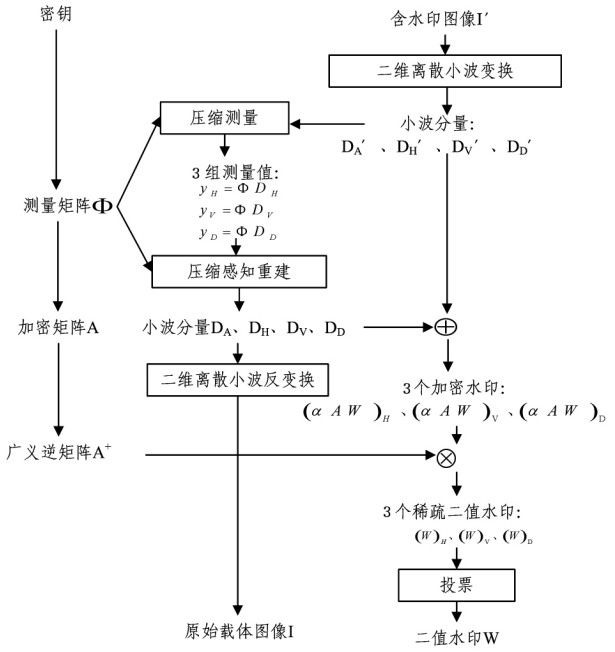


图 6　水印提取和原始图像重建流程图

步骤 1　由密钥生成 Gauss 随机测量矩阵 $\Phi \in \mathbb{R}^{(M-N)\times M}$；

步骤 2　将含水印图像 I' 进行一阶二维离散小波变换（在 Matlab 中设置 dwtmode 为'symw'），得到近似分量 $D_A \in \mathbb{R}^{M\times N}$、水平细节分量 $D_H' \in \mathbb{R}^{M\times M}$、垂直细节分量 $D_V' \in \mathbb{R}^{M\times M}$、对角细节分量 $D_D' \in \mathbb{R}^{M\times M}$；

步骤 3　由 $\Phi A = 0$，用测量矩阵 Φ 对 3 组小波细节分量进行观测，得到 3 组测量值：

$$\begin{aligned} y_H &= \Phi D_H' = \Phi D_H + \alpha \Phi AW = \Phi D_H \in \mathbb{R}^{(M-N)\times M} \\ y_V &= \Phi D_V' = \Phi D_V + \alpha \Phi AW = \Phi D_V \in \mathbb{R}^{(M-N)\times M} \\ y_D &= \Phi D_D' = \Phi D_D + \alpha \Phi AW = \Phi D_D \in \mathbb{R}^{(M-N)\times M} \end{aligned} \tag{23}$$

步骤 4　利用压缩感知重建算法，由 3 组测量值 y_H、y_V、y_D 分别重建原始图像小波细节分量 D_H、D_V、D_D；

步骤 5　由小波分量 D_A、D_H、D_V、D_D 进行小波反变换，得到重建的原始载体图像 I；

步骤 6　将原始图像 I 和含水印图像 I' 的 3 对小波细节分量相减，得到 3 个加密水印：

$$\begin{aligned} (\alpha AW)_H &= D_H' - D_H \\ (\alpha AW)_V &= D_V' - D_V \\ (\alpha AW)_D &= D_D' - D_D \end{aligned} \tag{24}$$

步骤 7　根据 $\Phi A = 0$，生成列满秩的加密矩阵 $A \in \mathbb{R}^{M\times N}$，再求 A 的广义逆矩阵 $A^+ \in \mathbb{R}^{N\times M}$；

步骤 8　由 A^+ 分别求得 3 个稀疏二值水印（嵌入强度 α 是程序中的常量）：

$$\begin{aligned} (W)_H &= \frac{1}{\alpha} A^+ (\alpha AW)_H \\ (W)_V &= \frac{1}{\alpha} A^+ (\alpha AW)_V \\ (W)_D &= \frac{1}{\alpha} A^+ (\alpha AW)_D \end{aligned} \tag{25}$$

步骤 9　由 3 个稀疏二值水印 $(W)_H$、$(W)_V$、$(W)_D$ 投票，得到最终的稀疏二值水印 W（反映射回"0、1"二值）。

5　实验结果与性能分析

5.1　实验图像

原始载体图像 $I \in \mathbb{R}^{256\times 256}$，如图 7 所示。

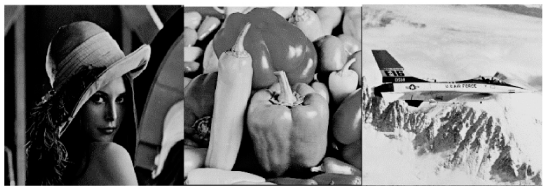


图 7　实验选用的载体图像 Lena，Peppers 和 Jet

水印图像 $W \in \mathbb{R}^{32\times 128}$（由于使用 sym3 小波基，实际 $W \in \mathbb{R}^{33\times 130}$），如图 8 所示。

图 8　原始水印图像

以强度 $\alpha = 30$ 嵌入水印后，载体图像 $I' \in \mathbb{R}^{256\times 256}$，如图 9 所示。

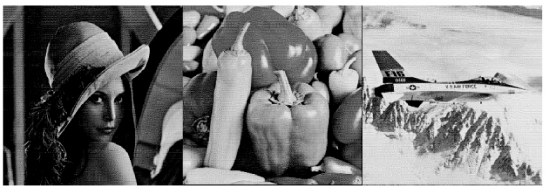


图 9　嵌入水印后的载体图像

提取的水印图像 W，如图 10 所示。

图 10　提取的水印图像

5.2　图像评价指标

常用来评价隐蔽性的指标有峰值信噪比（Peak Signal Noise Ratio，PSNR）、**结构相似度指标**（Structural SIMilarity index，SSIM）。**本文统一使用较常用、计算较简便的** PSNR **来评价水印的隐蔽性，PSNR 的计算公式如下：**

$$PSNR = 10\log\left(\frac{(2^n-1)^2}{MSE}\right) \tag{26}$$

其中，n 表示图像的位深，一般灰度图像位深为 8bit，即 $n=8$，PSNR 的峰值（Peak）为 $2^n - 1 = 255$；MSE 表示图像间的均方

差(Mean Square Error,MSE),计算公式如下:

$$MSE=\frac{1}{MN}\| I-I' \|_2^2, I, I'\in \mathbb{R}^{M\times N} \tag{27}$$

其中,I 和 I' 分别表示原始载体图像和嵌入水印后的载体图像。

常采用误码率(Bit Error Ratio,BER)和归一化相关系数(Normal Correlation,NC)来评价水印算法的鲁棒性。

二维图像 BER 的计算公式如下:

$$BER=\frac{\| W-W' \|_0}{MN}\times 100\%, W, W'\in \mathbb{R}^{M\times N} \tag{28}$$

二维图像的 NC 计算公式如下:

$$NC=\frac{\langle W, W'\rangle}{\| W \|_2^2}, W, W'\in \mathbb{R}^{M\times N} \tag{29}$$

式(28)、式(29)中 W 和 W' 分别表示嵌入的原始水印图像和提取出的水印图像。

5.3 不同嵌入强度下性能分析

Matlab 平台下,嵌入强度 α 和载体图像嵌入水印前后 PSNR、水印图像提取前后 NC 的关系如表 1 所列。

表 1 不同嵌入强度下载体图像 PSNR 和水印 NC 嵌入强度

嵌入强度 α	Lena		Peppers		Jet	
	PSNR	NC	PSNR	NC	PSNR	NC
$\alpha=5$	44.4585	0.8877	44.4894	0.8553	44.3962	0.8585
$\alpha=10$	38.4405	0.9795	38.4164	0.9849	38.4969	0.9546
$\alpha=15$	35.1355	0.9935	35.1286	0.9957	35.1297	0.9935
$\alpha=20$	33.2432	0.9968	33.2806	0.9989	33.1522	0.9946
$\alpha=25$	31.7953	0.9968	31.8952	1	31.7749	1
$\alpha=30$	31.0963	1	30.9514	1	30.8635	1
$\alpha=35$	30.3337	1	30.3248	1	30.2380	1
$\alpha=40$	29.8130	1	29.9491	1	29.8548	1

5.4 不同攻击下鲁棒性分析

Matlab 平台下,当嵌入强度 $\alpha=30$ 时,模拟不同攻击,水印的鲁棒性分析如表 2 所列。

表 2 不同攻击下水印 BER 和 NC

攻击类型	Lena		Peppers		Jet	
	BER(%)	NC	BER(%)	NC	BER(%)	NC
高斯噪声(V=0.001)	2.68	0.9773	1.79	0.9719	2.42	0.9260
高斯噪声(V=0.005)	14.31	0.8650	14.34	0.8618	14.66	0.8693
椒盐噪声(D=0.01)	0.21	0.9978	0	1	0.33	0.9989
椒盐噪声(D=0.05)	8.46	0.9082	8.58	0.9017	11.05	0.8909
高斯滤波(3×3,α=0.3)	0	1	0	1	0	1
高斯滤波(3×3,α=0.5)	0.16	0.9978	0	1	0	1
JPEG 压缩(Q=70)	5.34	0.9093	5.01	0.8942	5.34	0.9179
JPEG 压缩(Q=50)	15.97	0.7408	13.01	0.7711	14.45	0.7732
中心块剪切(25)	5.62	0.9093	8.32	0.9125	11.68	0.9017
中心块剪切(50)	30.79	0.6631	31.68	0.6695	31.05	0.6544

结束语 本文针对现代数字水印的设计要求,结合压缩感知理论,提出了一种图像盲水印算法。本文算法只需一个密钥(随机数种子),无需原始载体图像或其他先验知识,即可从嵌有水印的载体图像中精确提取水印,重构原始载体图像。文中对提出的水印算法进行了详细的理论分析,并通过大量实验验证了算法的良好特性。

参 考 文 献

[1] Candès E J. Compressive sampling[C]// Proceedings of the International Congress of Mathematicians. Madrid, Spain: 2006: 1433-1452

[2] DonohoD L. Compressed sensing[J]. IEEE Transactions on Information Theory, 2006, 52(4): 1289-1306

[3] Baraniuk R G. A lecture on compressive sensing[J]. IEEE Signal Processing Magazine, 2007, 24(4): 118-120, 124

[4] Sheikh M, Baraniuk R G. Blind Error-Free Detection of Transform-Domainwatermarks[C]// IEEE International Conference on Image Processing. Sept. 2007: 453-456

[5] 闫敬文,刘蕾,屈小波. 压缩感知及应用[M]. 北京:国防工业出版社, 2015: 57-58

[6] Candès E J, Tao T. Decoding by linear programming[J]. IEEE Transactions on Information Theory, 2005, 51(12): 4203-4215

[7] Candes E, Rudelson M, Tao T, et al. Error correction via linear programming[C]// IEEE Symposium on Foundations of Computer Science(FOCS 2005). IEEE, 2005: 668-681

[8] Elad M. 稀疏与冗余表示理论及其在信号与图像处理中的应用[M]. 曹铁勇,杨吉斌,赵斐,等,译. 北京:国防工业大学出版社, 2015: 186-199

[9] Candè E J, Wakin M B. An Introduction To Compressive Sampling[J]. IEEE Signal Processing Magazine, 2008, 25(2): 21-30

[10] 李树涛,魏丹. 压缩传感综述[J]. 自动化学报, 2009, 35(11): 1369-1377

[11] Candès E J. The restricted isometry property and its implications for compressed sensing[J]. Comptes Rendus Mathematique, 2008, 346(9/10): 589-592

[12] Candès E J, Tao T. Near-Optimal Signal Recovery From Random Projections: Universal Encoding Strategies? [J]. IEEE Transactions on Information Theory, 2007, 52(12): 5406-5425

[13] Baraniuk R, Davenport M, Devore R, et al. A Simple Proof of the Restricted Isometry Property for Random Matrices[J]. Constructive Approximation, 2015, 28(3): 253-263

[14] 许志强. 压缩感知[J]. 中国科学:数学, 2012, 42(9): 865-877

[15] Candès E J, Romberg J K, Tao T. Stable signal recovery from incomplete and inaccurate measurements[J]. Communications on Pure & Applied Mathematics, 2005, 19(5): 410-412

[16] 杨海蓉,张成,丁大为,等. 压缩传感理论与重构算法[J]. 电子学报, 2011, 39(1): 142-148

[17] 方红,杨海蓉. 贪婪算法与压缩感知理论[J]. 自动化学报, 2011, 37(12): 1413-1421

[18] Needell D, Tropp J A. CoSaMP: Iterative signal recovery from incomplete and inaccurate samples [J]. Applied & Computational Harmonic Analysis, 2008, 26(3): 301-321

[19] 李峰,郭毅. 压缩感知浅析[M]. 北京:科学出版社, 2015: 70-71

[20] 李然,干宗良,朱秀昌. 基于分块压缩感知的图像全局重构模型[J]. 信号处理, 2012(10): 1416-1422