基于非均匀 DCT 的量化索引调制隐写

邓　艺[①]　　赵险峰[②]　　冯登国[②]

[①](中国科学技术大学电子工程与信息科学系　合肥　230026)

[②](中国科学院软件研究所信息安全国家重点实验室　北京　100190)

摘　要：基于量化索引调制(QIM)的隐写技术正日益受到隐写分析的威胁。该文将通常在 DCT 域隐写的做法改为在非均匀 DCT 域进行，将参数作为密钥，提出了一种 NDCT-QIM 图像隐写方法。由于在攻击者猜测的域中，嵌入信号具有扩散性，NDCT-QIM 方法不利于隐写分析对隐写特征的检测，分析和实验表明，它能够更好地抵御基于梯度能量、直方图及小波统计特征等常用统计量的隐写分析，增强了隐写的隐蔽性。

关键词：信息隐藏；信息安全；图像隐写；非均匀离散余弦变换；量化索引调制

中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2010)02-0323-06

DOI: 10.3724/SP.J.1146.2008.01399

Quantization Index Modulation Steganography Based on the Nonuniform DCT

Deng Yi[①]　　Zhao Xian-feng[②]　　Feng Deng-guo[②]

[①](*Department of Electronic Engineering and Information Science*, *University of Science and Technology of China*, *Hefei* 230026, *China*)

[②](*State Key Laboratory of Information Security*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*)

Abstract: Steganography based on Quantization Index Modulation (QIM) is being increasingly threatened by steganalysis. This paper improves the existing steganographic methods embedding data in Non-uniform Discrete Cosine Transform (NDCT) domain instead of more commonly used Discrete Cosine Transform (DCT) domain, and proposes the NDCT-QIM image steganography which uses the parameters of NDCT as its secret key. Since the embedded signal disperses in the domain guessed by an attacker, the NDCT-QIM method makes steganalysis difficult to detect the characteristics of steganography. The analysis and experiments show that it improves the covertness of embedded signal, and is more resistant to the commonly used steganalysis methods, including those respectively based on testing gradient energy, histogram, wavelet characteristics, etc.

Key words: Data hiding; Information security; Image steganography; Non-uniform Discrete Cosine Transform (NDCT); Quantization Index Modulation (QIM)

1　引言

近年来，隐写(steganography)作为信息隐藏的重要分支，越来越引起人们的关注。隐写将机密信息(亦称隐秘信息)隐藏在其他载体中，通过载体的传输实现保密通信[1]。它可以为基于密码的保密通信增加额外的安全。随着多媒体技术的发展，现代隐写技术更多地利用数字媒体(如图像、视频、音频等)具有的感知冗余性将信息隐藏在它们中。目前，隐写方法按照信息嵌入方式主要包括 LSB 替换[2]、BPCS 方法[3]、扩频方法[4]和 QIM 方法[5]。隐写安全主要通过隐秘数据的隐蔽性来衡量，它是指攻击者难以发现载体中存在隐藏数据的性质。本文的目的是提高 QIM 隐写的安全性。

基于量化和矢量量化技术，Chen 和 Wornell 提出了 QIM 信息隐藏方案[5]，QIM 能够嵌入大量数据并抵抗许多攻击，但也会改变载体的某些统计特征，例如图像的梯度能量、直方图特征及小波统计特征等，使它易受到隐写分析(steganalysis)的威胁。目前，针对 QIM 的隐写分析方法主要包括：Lie 和 Lin 提出的梯度能量检测方法和 Laplacian 分布特征检测方法[6]，Malik 和 Subbalakshmi 等提出的基于核密度估计的 QIM 检测方法[7]，Lyu 和 Farid 提出的基于小波高阶统计的检测方法[8]，Xuan 等人提出的基于图像小波特征函数的统计矩的检测方法[9]等。为了抵御这些隐写分析，近来一些改进的 QIM 方法被提出：Noda 和 Niimi 等提出了直方图保持方法[10]，Solanki 和 Sullivan 等提出了统计恢复方法[11]，但它们都只是保持了直方图的一阶统计不变，并不能有

2008-11-03 收到，2009-11-23 改回

国家自然科学基金重点项目(60633030)和国家自然科学基金(60573049)资助课题

通信作者：邓艺　yyyyxf@hotmail.com

效对抗基于其他统计特征的隐写分析。

我们发现，导致传统 QIM 隐写方法易被检测的一个重要因素是嵌入域固定，它们大多在离散余弦变换(DCT)域嵌入信息，使隐写分析能在准确的域中发现并收集特征。本文通过将 DCT 改造为非均匀 DCT(NDCT)，提出了 NDCT-QIM 隐写方案，它在NDCT域使用QIM嵌入信息，并将构造NDCT的参数作为部分密钥，由此使该隐写方法能够更好地对抗以上隐写分析。NDCT 已经首先被应用到数字水印上，并显著地提高了水印的安全性[12]。当前，一些由密钥控制的变换(下称钥控变换)可使算法不在固定的域中嵌入信息，可能有助于提高隐写的隐蔽性，它们主要包括钥控正交变换、非均匀离散 Fourier 变换(NDFT)、参数化小波变换等，但是，它们的应用仅局限于数字水印，主要包括 Fridrich 等人基于钥控正交变换提出的图像鲁棒水印[13]，谢玲等人基于NDFT提出的鲁棒音频水印算法[14]以及 Dietl 等人提出的基于参数化小波变换的图像鲁棒水印[15]。现有的钥控变换在应用中还存在一些问题：钥控正交变换的构造方法复杂，在不同密钥参数下得到的变换可能完全不同，因此产生的变换域不够稳定，不利于信息的嵌入；由于 NDFT 的频谱为复数，为使信息嵌入后通过逆 NDFT 回到实数域，NDFT 的构造须保持频谱的共轭，这就限制了变换参数和嵌入位置的选取；由于采用了特定的小波生成方式，当前的参数化小波变换所能使用的参数量受到了限制。本文使用的 NDCT，在一定程度上解决了这些问题。本文的组织是，第 2 节给出 NDCT 及其逆变换的构造，第 3 节描述了 NDCT-QIM 隐写方案，第 4 节分析算法的性质和对隐写分析的影响，第 5 节给出了实验结果，最后，第 6 节给出了结论。

2 NDCT 的构造

为了提高隐写的隐蔽性，更好的抵御隐写分析，本文将 DCT 改造为 NDCT ，提出了 NDCT-QIM 隐写方案，本节首先介绍 NDCT 的构造。

设 $\boldsymbol{X}_{N\times N}$ 为图像或图像分块，对它的 2 维 NDCT 变换可以用矩阵形式表示为

$$\boldsymbol{Y}_{N\times N}=\boldsymbol{C}_{N\times N}\cdot\boldsymbol{X}_{N\times N}\cdot\boldsymbol{R}_{N\times N}^{\mathrm{T}} \tag{1}$$

其中 $\boldsymbol{C}$ 为列变换矩阵，它等于

$$\boldsymbol{C}=\sqrt{\frac{2}{N}}\begin{bmatrix}1/\sqrt{2} & 1/\sqrt{2} & \cdots & 1/\sqrt{2}\\ \cos\dfrac{\alpha_1\pi}{2N} & \cos\dfrac{3\alpha_1\pi}{2N} & \cdots & \cos\dfrac{(2N-1)\alpha_1\pi}{2N}\\ \vdots & \vdots & \ddots & \vdots\\ \cos\dfrac{\alpha_{N-1}\pi}{2N} & \cos\dfrac{3\alpha_{N-1}\pi}{2N} & \cdots & \cos\dfrac{(2N-1)\alpha_{N-1}\pi}{2N}\end{bmatrix} \tag{2}$$

其中 $\alpha_k\in(0,N)$， $k=1,2,\cdots,N-1$， $\alpha_{k-1}<\alpha_k$， $\boldsymbol{R}$ 为行变换矩阵，它的表示和式(2)类似，仅需用 β_k 替换 α_k； α_k 和 β_k 是控制 NDCT 非均匀性的参数，它们的值一般在 k 附近，可由密钥控制。当 $\alpha_k=\beta_k=k$，NDCT 成为 DCT，而 α_k-k 和 β_k-k 决定了第 k 个频率采样点的非均匀性。设 $\boldsymbol{C}$ 和 $\boldsymbol{R}$ 可逆，相应的 INDCT 为 $\boldsymbol{X}_{N\times N}=\boldsymbol{C}_{N\times N}^{-1}\cdot\boldsymbol{Y}_{N\times N}\cdot\boldsymbol{R}_{N\times N}^{-\mathrm{T}}$，其中，上标 –T 表示转置后求逆。由于矩阵行之间和列之间的不相关性没有显著降低，$\boldsymbol{C}^{-1}$ 和 $\boldsymbol{R}^{-1}$ 稳定存在，但在本文的算法中，我们仍然在生成 $\boldsymbol{C}$ 和 $\boldsymbol{R}$ 时判断它们的可逆性，具体过程如下：用乘同余法产生两个在[0,1]间的均匀分布的伪随机序列，将它们乘上 δ 后作为 α_k-k 和 β_k-k，再得到 α_k 和 β_k，最后得到 $\boldsymbol{C}$ 和 $\boldsymbol{R}$。若发现 $\boldsymbol{C}$ 或 $\boldsymbol{R}$ 的行列式值接近零，则放弃这组 α_k 和 β_k，重新生成下一组 α_k 和 β_k，但在 $N=8$ 和 $\delta\le0.5$ 时我们未发现这种情况。

3 基于 NDCT 的 QIM 隐写方案

基于上节介绍的 NDCT 和标准 QIM，本文提出了 NDCT-QIM 隐写方案，它的输入参数是隐秘信息 m、原图像 $\boldsymbol{X}$ 及由乘同余法噪声发生器的初态 s 组成的密钥，嵌入算法包括以下步骤：

(1)将图像 $\boldsymbol{X}$ 分为 $N\times N$ 的分块，对每一块分别进行步骤(2)–步骤(4)：

(2)将当前图像分块记为 $\boldsymbol{B}$，用噪声发生器生成当前 NDCT 变换矩阵参数子序列 α_k 和 β_k， $1\le k\le7$； 由式(2)得到变换矩阵 $\boldsymbol{C}$ 和 $\boldsymbol{R}$，计算 $\boldsymbol{F}\leftarrow\mathrm{NDCT}(\boldsymbol{B})$；将当前噪声发生器的状态按固定的间隔变化一次。

(3)利用 QIM 方法将隐秘信息嵌入到 NDCT 低频系数(即 NDCT 系数矩阵的左上角部分，包括 $F(1,2),\cdots,F(1,5),F(2,1),\cdots,F(2,4),F(3,1),\cdots,F(3,3),F(4,1),F(4,2),F(5,1)$)，定义量化函数为

$$Q_i(x)=Q(x-d_i)+d_i \tag{3}$$

其中 $Q(x)=q\lfloor x/q\rfloor$， q 为量化步长， $d_0=-q/4$， $d_1=q/4$，则量化后系数为

$$F'(x,y)=\begin{cases}Q_0(F(x,y)), m(k)=0\\ Q_1(F(x,y)), m(k)=1\end{cases} \tag{4}$$

(4)对量化后系数进行 NDCT 反变换，得到当前隐写分块 $\boldsymbol{B}' \leftarrow \mathrm{INDCT}(\boldsymbol{F}')$。

(5)将所有隐写分块合并得到隐写图像 $\boldsymbol{X}'$。

针对 $\boldsymbol{X}'$，相应的提取算法首先包括以上(1)、(2)步，得到隐写图像各分块 NDCT 系数 $\boldsymbol{F}''$，然后利用反量化规则从 $\boldsymbol{F}''$ 的低频系数中提取信息：计算 $p=\mathrm{round}(F''(x,y)-q/4)/(q/2))$，其中 $\mathrm{round}(x)$ 表示取最接近 x 的整数，则隐秘信息为

$$m'(k)=\begin{cases}1, & p=2n\\ 0, & p=2n+1\end{cases} \tag{5}$$

由于在嵌入过程的第(4)步，对量化后系数进行 NDCT 反变换 $\boldsymbol{B}' \leftarrow \mathrm{INDCT}(\boldsymbol{F}')$ 时存在舍入误差，因此会给提取信息带来一定的误差。通过实验发现，当量化步长 q=2 时，提取误差小于 6%，而当 q=8 时，提取误差小于 0.5%。通过增大量化步长能够减小提取误差，但量化步长的增大会导致嵌入对图像的扰动变大，减弱嵌入信息的隐蔽效果，因此选择一个合适的量化步长非常重要。由 5.2 节的实验可知，q=8 时，一些常用的隐写分析对 NDCT-QIM 隐写方案的检测效果不佳，并且提取误差也很小，可由纠错码以很小的代价完成纠错。因此，q=8 为一个较为理想的量化步长。

4　算法性质分析

本文发现，NDCT-QIM 隐写具有一些有益的性质，包括嵌入信号的扩散性，梯度能量的衰减、对直方图特征的影响减小，Laplacian 分布特征的削弱，小波统计特征的变化性等，这些性质使 NDCT-QIM 隐写能够更好地对抗隐写分析。

4.1 嵌入信号的扩散性

嵌入信号的扩散性是指，由于对 NDCT-QIM 隐写的隐写分析仅能在猜测的域中进行，在任一系数的嵌入信号将扩散到本分块对应猜测域的其它位置。设 $\boldsymbol{X}$ 表示载体图像，获得嵌入域的 NDCT 由矩阵 $\boldsymbol{C}$ 定义，即 $\boldsymbol{Y}=\boldsymbol{C}_{N\times N}\cdot\boldsymbol{X}\cdot\boldsymbol{R}_{N\times N}^{\mathrm{T}}$，记隐写分析猜测的域为 $\tilde{\boldsymbol{Y}}=\tilde{\boldsymbol{C}}_{N\times N}\cdot\boldsymbol{X}\cdot\tilde{\boldsymbol{R}}_{N\times N}^{\mathrm{T}}$，假设仅在 $Y(x,y)$ 中的一个系数 $Y(m,n)$ 上嵌入信息，即

$$Y'(m,n)=Y(m,n)+a(m,n) \tag{6}$$

当 $x\neq m$，$y\neq n$ 时，$a(x,y)=0$，则 $\widetilde{\boldsymbol{Y}}$ 被修改为

$$\widetilde{\boldsymbol{C}}\cdot[\boldsymbol{C}^{-1}\cdot(\boldsymbol{Y}+\boldsymbol{A})\cdot\boldsymbol{R}^{-\mathrm{T}}]\cdot\widetilde{\boldsymbol{R}}^{-\mathrm{T}}=\widetilde{\boldsymbol{Y}}+\widetilde{\boldsymbol{C}}\cdot\boldsymbol{C}^{-1}\cdot\boldsymbol{A}\cdot\boldsymbol{R}^{-\mathrm{T}}\cdot\widetilde{\boldsymbol{R}}^{-\mathrm{T}}$$

其中 $\boldsymbol{A}=\begin{bmatrix}0 & & \\ & a(m,n) & \\ & & 0\end{bmatrix}$，设 $\boldsymbol{D}=\widetilde{\boldsymbol{C}}\cdot\boldsymbol{C}^{-1}$ 为列扩散矩阵，$\boldsymbol{S}=\boldsymbol{R}^{-\mathrm{T}}\cdot\widetilde{\boldsymbol{R}}^{-\mathrm{T}}$ 为行扩散矩阵，则由 $a(m,n)$ 在 $\widetilde{\boldsymbol{Y}}$ 上引入的噪声为

$$\boldsymbol{P}=\boldsymbol{D}\cdot\boldsymbol{A}\cdot\boldsymbol{S}=a(m,n)\cdot\begin{bmatrix}D(1,m)S(n,1) & \cdots & D(1,m)S(n,N)\\ D(2,m)S(n,1) & \cdots & D(2,m)S(n,N)\\ \vdots & \ddots & \vdots\\ D(N,m)S(n,1) & \cdots & D(N,m)S(n,N)\end{bmatrix}$$

即 $a(m,n)$ 扩散到 $\widetilde{\boldsymbol{Y}}$ 的分量是 $p(x,y)=a(m,n)\cdot D(x,m)\cdot S(n,y)$。当信息嵌入不止在一个位置上时，所有的扩散分量累加为

$$p(x,y)=\sum\nolimits_{m=1,n=1}^{N,N}a(m,n)\cdot D(x,m)\cdot S(n,y) \tag{7}$$

式(7)表明在猜测的分析域中样点上的嵌入信号相互扩散，这显然会对隐写特征产生影响。本文的隐写算法仅在嵌入域的低频位置上嵌入信息，但在猜测的分析域上嵌入信息扩散到所有位置上，包括未嵌入的中频和高频位置，由于能量的扩散，这使在嵌入位置上的信息相对减弱，5.1 节的实验表明嵌入信息扩散后仅为扩散前的 70%左右。本节以下将更具体地论述隐写特征的变化。

4.2 隐蔽效果分析

以上扩散性使得基于 NDCT-QIM 的隐写具有以下性质。

4.2.1 梯度能量的衰减　对 NDCT-QIM 隐写方法，梯度能量检测[6]只能在空间域或猜测的变换域上进行。设 $a(x,y)$ 为嵌入信息后系数的变化值，由文献[6]可知，在嵌入域上图像梯度能量将增加 $\mathrm{E}[GE_a]$，它表示嵌入信息的梯度能量，为 x 方向的梯度能量和 y 方向的梯度能量之和，展开为

$$\mathrm{E}[GE_a]=\frac{1}{N-1}\sum_x\mathrm{E}[(a(x,y)-a(x-1,y))^2]+\frac{1}{N-1}\sum_y\mathrm{E}[(a(x,y)-a(x,y-1))^2] \tag{8}$$

在猜测的变换域中，$a(x,y)$ 扩散为 $p(x,y)$，根据 4.1 节的分析，$p(x,y)$ 由于扩散，相对于 $a(x,y)$ 幅度减小，相邻点的差值也普遍随之减小。设 $P(x,y)$ 平均减小为 $a(x,y)$ 的 $1/\lambda$ 倍，即

$$\mathrm{E}[p(x,y)]=(1/\lambda)\mathrm{E}[a(x,y)] \tag{9}$$

由于 $a(x,y)$ 和 $P(x,y)$ 均为随机序列，由式(8)可推得

$$\mathrm{E}[GE_p]=(1/\lambda^2)\mathrm{E}[GE_a] \tag{10}$$

这表明猜测域上图像梯度能量的增幅 $\mathrm{E}[GE_p]$ 减小为嵌入域上 $\mathrm{E}[GE_a]$ 的 $1/\lambda^2$。

4.2.2 对直方图的影响　将嵌入域系数 $F(x,y)$ 按照量化值 $\lfloor(F(x,y)+q/4)/(q/2)\rfloor$ 进行划分，设 $H(i)$ 表示量化值等于 i 的系数的个数，则 H 近似为直方图函

数。使用 QIM 嵌入信息后，$H(i)$ 的一部分样点会调制到 $i+1$，记它们的数量为 $H(i)^+$，同时 $H(i+1)$ 的一部分样点会调制到 i，记它们的数量为 $H(i+1)^-$，则信息嵌入后有

$$H'(i)=H(i-1)^+ +(H(i)-H^+(i)-H^-(i))+H(i+1)^- \tag{11}$$

由于嵌入信息为伪随机序列，根据量化规则可知

$$H(i)^+ \approx H(i)/4,\ H(i+1)^- \approx H(i+1)/4 \tag{12}$$

同理，$H(i)$ 和 $H(i-1)$ 也有此关系，由式(12)得

$$H'(i)=H(i-1)/4+H(i)/2+H(i+1)/4 \tag{13}$$

这是一个平滑过程，$H'(i)$ 和 $H'(i+1)$ 的差距会减小。

但是，对 NDCT-QIM 隐写方法，攻击者无法获得嵌入域，隐写分析只能在猜测的变换域中进行。设猜测域上的直方图函数为 $\widetilde{H}(i)$，由 4.1 节的分析可知，嵌入信号在猜测域上会扩散到其它样点并削弱，这使嵌入对猜测域上的系数值的改变幅度减小，从而使在嵌入域中从 i 调制到 $i+1$ 的 $H(i)^+$ 的一部分样点在猜测域中达不到 $i+1$ 的量化范围，因此有 $\widetilde{H}(i)^+ < H(i)^+$，同理，$\widetilde{H}(i+1)^- < H(i+1)^-$，于是有

$$\widetilde{H}(i)^+ < \widetilde{H}(i)/4,\ \widetilde{H}(i+1)^- < \widetilde{H}(i+1)/4 \tag{14}$$

结合式(11)、式(13)可知，猜测域上直方图平滑效果减弱，因此攻击者所得到的隐写图像的直方图与正常图像的差异减小，这将使依靠直方图特征进行的隐写分析准确率降低。直方图差异的减小也表明 QIM 嵌入带来的随机性的减小，这使一些利用随机性进行检测的方法如基于核密度估计的 QIM 检测方法检测难度加大。

4.2.3 Laplacian 分布特征的削弱 Lapalacian 分布特征检测方法以参数 λ 的方差作为检测参量，信息嵌入前后的 λ 方差有如下关系[5]：

$$\mathrm{Var}[\lambda^h] \approx \begin{cases} \left(1-\dfrac{\mathrm{E}[|\ m\ |]}{t_\tau}\right)^2 \cdot \mathrm{Var}[\lambda^0], & \left|\lambda^0 m\right| \geq 1 \\ \left(1-\dfrac{\mathrm{E}^2[|m|]}{t_\tau}\mathrm{E}[\lambda^o]\right)^2 \cdot \mathrm{Var}[\lambda^o], & \left|\lambda^o m\right| < 1 \end{cases} \tag{15}$$

其中 m 表示嵌入引起的噪声，t_τ 为检测的一个参数。由式(15)可知，$\mathrm{Var}[\lambda^h] < \mathrm{Var}[\lambda^o]$。对 NDCT-QIM 隐写方法，Laplacian 分布特征检测只能在猜测的变换域上进行，由于嵌入信息的扩散性，QIM 造成的量化噪声 a 在猜测域上衰减为加性噪声 p，p 的抖动幅度要小于 a，因此 $\mathrm{E}[|p|] < \mathrm{E}[|a|]$，代入(15)式可得

$$\mathrm{Var}[\lambda^h] < \mathrm{Var}[\lambda^{\tilde{h}}] < \mathrm{Var}[\lambda^o] \tag{16}$$

$\mathrm{Var}[\lambda^{\tilde{h}}]$ 表示猜测域上得到的 λ 方差，这表明 NDCT 削弱了 Laplacian 分布特征。

4.2.4 小波统计特征的变化性 对于 NDCT-QIM 隐写方法，各个隐写图像的隐秘数据是在任选的 NDCT 域上嵌入的，但由于一些通用检测方法例如基于小波高阶统计的检测方法的特征数据是在固定的小波域上取得的，从 NDCT 域映射到小波域后，由于扩散性，嵌入引起的噪声均值和抖动范围变小，对统计特征的扰动也随之变小，并且由于嵌入发生在不同的 NDCT 域，对统计特征的影响具有变化性，这将降低分类算法进行数据分类时的精度，进而影响检测的准确率。

由于现有的其它通用检测方法的原理与此类似，都是在固定的域上收集一些统计特征进行分类，因此上述的特性对于它们同样存在。5.2 节的实验结果表明，基于小波统计的检测方法对 NDCT-QIM 隐写方法检测准确率比传统方法低。

5 实验结果

为了验证 NDCT-QIM 隐写算法的性能，本文进行了以下实验：(1)测量了嵌入信号的扩散性；(2)用梯度能量检测方法，Laplacian 分布特征检测方法，基于核密度估计的 QIM 检测方法，基于高阶小波统计的检测方法对 NDCT-QIM 隐写算法进行了分析。实验的基本配置数据如下：量化步长 $q=8$，分块大小为 8。

5.1 NDCT域的扩散性

随机生成两组 α_k 和 β_k，得到矩阵 $\boldsymbol{C}$，$\boldsymbol{R}$ 和 $\widetilde{\boldsymbol{C}}$，$\widetilde{\boldsymbol{R}}$，计算 $p(x,y)=\sum_{m=1,n=1}^{N,N} a(m,n)\cdot D(x,m)\cdot S(n,y)$，其中，与嵌入算法类似，$a(x,y)$ 仅在低频位置上有 $(-1,\ 1)$ 的随机值，计算低频位置上 $\rho=\sum|p(x,y)| \Big/ \sum|a(x,y)|$ 的值表示两个 NDCT 域间的扩散性，重复以上步骤。实验结果如图 1 所示，嵌入信息扩散后仅为扩散前的 70%左右。

5.2 隐写分析方法的检测

为了验证 NDCT-QIM 隐写方法对抗隐写分析方法的能力，本文使用梯度能量检测方法、Laplacian 分布特征检测方法、基于核密度估计的

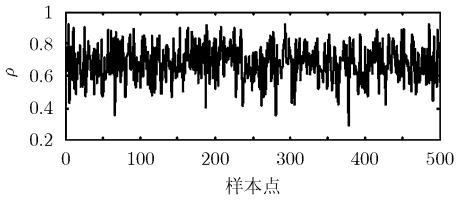

图 1 NDCT 域间的扩散性

QIM 检测方法、基于小波高阶统计特征的检测方法对本文提出的方法进行检测实验。随机选择人物、建筑、自然风景各类图像共 935 幅，统一剪切为 800×600 并转化为 8 bit 像素的灰度图像($\text{gray}=0.299\text{R}+0.587\text{G}+0.114\text{B}$)，其中 500 幅作为检测算法的训练图像，另外 435 幅作为测试图像。选取 2 种传统隐写算法 Jsteg，EzStego 进行实验，并与本文的算法进行比较。实验结果如表 1–表 4 所示。

从表 1–表 4 可以看出，在嵌入相同信息的情况下，对 NDCT-QIM 隐写方法的检测准确率远低于另外两种方法。

表 1 梯度能量检测方法检测率的比较

隐写方法	大小	漏报率 (%)	误报率 (%)	准确率 (%)
Jsteg	128×128	63.6	12.0	62.2
Jsteg	64×64	72.6	14.0	56.7
EzStego	128×128	67.4	14.4	59.1
EzStego	64×64	81.4	13.4	53.6
NDCT-QIM 方法	128×128	80.8	12.0	53.6
NDCT-QIM 方法	64×64	87.5	11.5	50.5

表 2 Laplacian 分布特征检测方法检测率的比较

隐写方法	大小	漏报率 (%)	误报率 (%)	准确率 (%)
Jsteg	128×128	63.6	14.0	61.2
Jsteg	64×64	74.2	17.2	54.3
EzStego	128×128	68.4	13.4	59.1
EzStego	64×64	72.7	18.5	54.4
NDCT-QIM 方法	128×128	72.8	13.3	55.3
NDCT-QIM 方法	64×64	80.4	15.7	52.1

表 3 基于核密度估计的 QIM 检测方法检测率的比较

隐写方法	大小	漏报率 (%)	误报率 (%)	准确率 (%)
Jsteg	128×128	61.0	3.6	67.2
Jsteg	64×64	79.6	3.0	58.7
EzStego	128×128	70.0	3.8	63.1
EzStego	64×64	80.9	5.3	56.9
NDCT-QIM 方法	128×128	81.8	2.8	57.7
NDCT-QIM 方法	64×64	91.8	4.2	52.0

表 4 基于高阶统计特征的检测方法检测率的比较

隐写方法	大小	漏报率 (%)	误报率 (%)	准确率 (%)
Jsteg	128×128	4.6	1.0	97.2
Jsteg	64×64	11.5	1.0	93.7
EzStego	128×128	44.3	3.4	77.1
EzStego	64×64	49.4	3.4	73.6
NDCT-QIM 方法	128×128	72.8	2.0	62.6
NDCT-QIM 方法	64×64	80.4	1.5	59.0

6　结论

分析和实验结果说明，NDCT-QIM 图像隐写方法能有效地提高隐写的隐蔽性。由于针对该方法的隐写分析只能在空间域或者猜测的变换域上进行，嵌入信号具有扩散性，这使 NDCT-QIM 方法不利于隐写分析对隐写特征的检测，实现了梯度能量的衰减性，直方图的稳定性与小波统计特征的变化性等性质，它们能有效抵御梯度能量检测方法，Laplacian 分布特征检测方法，基于核密度估计的 QIM 检测方法和基于高阶统计特征的检测方法等典型的隐写分析方法的检测。

参 考 文 献

[1] Johnson N and Jajodia S. Exploring steganography: seeing the unseen[J]. *IEEE Computer*, 1998, 31(2): 26–34.

[2] Sutaone M S and Khandare M V. Image based steganography using LSB insertion technique[C]. IET International Conference on Wireless, Mobile and Multimedia Networks, Mumbai, India, 2008: 146–151.

[3] Noda H, Niimi M, and Kawaguchi E. Steganographic Methods Focusing on BPCS Steganography[M]. Heidelberg: Springer Berlin Publisher, 2007: 189–229.

[4] Huang C H, Chuang S C, and Wu J L. Digital-invisible-ink data hiding based on spread-spectrum and quantization techniques[J]. *IEEE Transactions on Multimedia*, 2008, 10(4): 557–569.

[5] Chen B and Wornell G W. Quantization index modulation methods for digital watermarking and information embedding of multimedia[J]. *Journal of VLSI Signal Processing*, 2001, 27(1–2): 7–33.

[6] Lie W N and Lin G S. A feature-based classification technique for blind image steganalysis[J]. *IEEE Transactions on Multimedia*, 2005, 7(6): 1007–1020.

[7] Malik H, Subbalakshmi K P, and Chandramouli R. Steganalysis of QIM-based data hiding using kernel density estimation[C]. Proc. MM&Sec'07. Dallas, Texas, USA, 2007:

149–160.

[8] Lyu S and Farid H. Detecting hidden messages using higher-order statistics and support vector machines[C]. Proc. IH'02. Noordwijkerhout, Netherlands, 2002, LNCS, Vol. 2578: 340–354.

[9] Xuan G, Shi Y Q, Gao J, Zou D, Yang C, Zhang Z, Chai P, Chen C, and Chen W. Steganalysis based on multiple features formed by statistical moments of wavelet characteristic function[C]. Proc. IH'05, Barcelona, Spain, 2005.LNCS, Vol. 3727: 262–277.

[10] Noda H, Niimi M, and Kawaguchi E. Application of QIM with dead zone for histogram preserving JPEG steganography[C]. Proc. ICIP'05. Genova, Italy, 2005. Vol. 2: 1082–1085.

[11] Solanki K, Sullivan K, Madhow U, Manjunath B S, and Chandrasekaran S. Statistical restoration for robust and secure steganography[C]. Proc. ICIP'05. Genova, Italy, 2005, Vol. 2: 1118–1121.

[12] Zhao X F, Xia B B, and Deng Y. Strengthening QIM-based watermarking by non-uniform discrete cosine transform[C]. Proc. IH'08. Santa Barbara, USA, 2008, LNCS 5284: 309–324.

[13] Fridrich J, Baldoza A C, and Simart R J. Robust digital watermarking based on key-dependent basis functions[C]. Proc. IH'98. Portland, Oregon, USA, 1998, LNCS 1525: 143–157.

[14] Xie L, Zhang J S, and He H J. A novel robust audio watermarking scheme based on nonuniform discrete fourier transform[J]. *Chinese Journal of Computers*, 2006, 29(9): 1711–1721.

[15] Dietl W, Meerwald P, and Uhl A. Protection of wavelet-based watermarking systems using filter parametrization[J]. *Signal Processing*, 2003, 83(10): 2095–2116.

邓 艺： 男，1980 年生，博士生，研究领域为信息隐藏.

赵险峰： 男，1969 年生，博士，副研究员，研究领域为信息安全.

冯登国： 男，1965 年生，教授，博士生导师，研究领域为网络与信息安全.