基于 GSM 模型的扩频水印安全性分析

张 东 [1,2] 倪江群 [1] 李大捷 [2]

摘 要 近年来, 数字水印安全性的研究日益受到重视. 对数字水印安全性的攻击是指对水印通信中密钥的估计, 水印的安全性可以用对水印密钥估计的 Cramer-Rao 界 (Cramer-Rao bound, CRB) 来衡量. 扩频水印的安全性具有重要的研究价值. 以往的研究假设图像载体呈高斯分布, 忽视了实际自然图像载体分布的非高斯性对水印安全性的影响. 本文利用高斯尺度混合 (Gaussian scale mixture, GSM) 模型描述自然图像载体的非高斯特性, 从理论上分析了扩频水印在 KMA (Known message attack) 和 WOA (Watermarked only attack) 攻击下的 CRB 和 MCRB 界 (Modified Cramer-Rao bound), 得出了扩频水印安全性与观测次数、秘密载波长度、水印嵌入能量以及嵌入信息分布特征的关系. 本文的工作对于设计新一代的安全、鲁棒水印具有重要的意义.

关键词 GSM 模型, 扩频水印, 安全性, Cramer-Rao 界
中图分类号 TP309

Security Analysis on Add-SS Watermarking with GSM

ZHANG Dong[1,2] NI Jiang-Qun[1] LEE Dah-Jye[2]

Abstract Watermarking security has emerged as the domain of extensive research in recent years. Attack to the security of watermarking is to estimate the secret keys used in watermarking communications. The security level of watermarking system can be evaluated by Cramer-Rao bound (CRB) for secret keys estimation. As a widely used method, the security issue of add spread spectrum (Add-SS) based watermarking has drawn great attention. The previous works on watermarking security were mainly based on the assumption that host signal was Gaussian distributed and ignored the impacts of non-Gaussian characteristics of nature images. With incorporation of the Gaussian scale mixture (GSM) model for host signals, this paper presents a theoretical analysis on the security of Add-SS watermarking system. By giving the CRB and MCRB (modified Cramer-Rao bound) for the estimation of secret carriers under KMA (known message attack) and WOA (watermarked only attack), this paper also reveals the factors that may influent the Add-SS watermarking security such as the times of observation, the length of secret carriers, the embedding energy, and the distribution of embedded messages. The results obtained in this paper will be helpful for designing the new secure and robust watermarking system.

Key words Gaussian scale mixture (GSM), add spread spectrum (Add-SS) watermarking, security, Cramer-Rao bound (CRB)

随着数字水印技术的不断发展, 有关水印安全性的研究日益受到重视. 传统的水印系统设计主要考虑三个方面的性能, 即水印鲁棒性、不可见性和水印的容量. 近年来, Cayre 等在数字水印安全性方面的开创性工作[1] 使得安全性正成为新一代水印系统设计中需考虑的第四个性能指标.

根据密码学领域的 Kerckhoffs[2−3] 原理, 没有任何一种加密的算法能够得到永久的保密. 水印算法也不例外, 即有关水印的嵌入和提取算法终会公开. 要保证水印通信的安全, 只能依赖水印的密钥. 水印通信中密钥的安全性决定了水印通信的安全. 对于扩频水印算法[4], 密钥就是产生扩频载波的随机数[1]; 而对于基于量化索引调制 (Quantization index modulation, QIM) 的水印算法, 密钥就是用于抖动量化网格的随机序列[5].

水印安全性的概念与水印的不可见性和水印容量有明显的区别, 但是其与水印鲁棒性的区别却值得进一步明确. 对水印鲁棒性的攻击指的是对水印通信信道的攻击, 其目的是增加水印通信的误码率[3]; 而对水印安全性攻击的目的是获取有关水印密钥的知识. 对水印鲁棒性的攻击可能是有意的或者无意的, 而对水印安全性的攻击一定是有意的. 对于水印安全性的攻击目前主要分为以下几种情况[1]: KMA (Known message attack), KOA (Known original attack) 和 WOA (Watermarked only attack). KMA 是指攻击者已知嵌入了水印的

收稿日期 2008-07-10 收修改稿日期 2008-10-06
Received July 10, 2008; in revised form October 6, 2008
国家自然科学基金 (60773200), 广东省自然科学基金 (7003722) 资助
Supported by National Natural Science Foundation of China (60773200) and Natural Science Foundation of Guangdong Province (7003722)
1. 中山大学信息科学与技术学院 广州 510275 2. 美国杨柏翰大学电气与计算机工程系 普罗沃 84602
1. School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, P. R. China 2. Department of Electrical and Computer Engineering, Brigham Young University, Provo 84602, USA
DOI: 10.3724/SP.J.1004.2009.00841

信号和嵌入信息本身, 通过多次观察来估计水印密钥; KOA 是指攻击者除了掌握隐藏水印的信号, 还拥有未嵌入水印的信号载体; 而 WOA 是最为困难的一种情况, 即攻击者只拥有嵌入了水印的信号.

近年来, 在有关水印安全性的研究中, Cayre 等的工作[1] 被认为是具有开创性意义的. 他们明确区分了水印安全性与鲁棒性的定义, 并通过求 Fisher 信息矩阵 (Fisher information matrix, FIM) 给出了扩频水印载波估计误差的 Cramer-Rao 边界 (Cramer-Rao bound, CRB). 在文献 [3] 中, Comesaña 等根据 Shannon 信息论, 利用求水印信号和扩频载波的互信息的方法分析了扩频水印的安全性. Pérez-Freire 等[5] 通过分析水印抖动量化调制的支撑集来研究基于 QIM 的水印安全性. Ni 等[6] 的工作则充分考虑了自然图像载体的统计特征, 利用 Shannon 互信息的方法对扩频水印安全性进行了理论分析和实际的攻击, 得到了对秘密载波的更加准确的估计.

目前针对水印安全性的分析, 大多假设图像载体呈高斯分布, 所得到的分析结论都以高斯分布为基础. 众所周知, 自然图像小波系数的边缘分布呈现很强的非高斯性, 即高尖峰和重脱尾. 因此, Cayre 等基于载体高斯分布的水印安全性分析与实际的情况有很大差别. 本文根据自然图像的统计特性, 利用高斯尺度混合 (Gaussian scale mixture, GSM) 模型描述其小波系数的分布, 并以 FIM 对扩频水印的安全性进行理论分析, 得到了对秘密载波无偏估计的 CRB 和 MCRB (Modified Cramer-Rao bound) 界. 该结果对于设计更为安全的水印算法具有重要的意义.

本文第 1 节和第 2 节分别给出了图像 GSM 模型和性能, 以及水印安全性分析的一般方法; 第 3 节和第 4 节分别为基于 GSM 模型的扩频水印安全性的理论分析和实验仿真结果; 第 5 节为本文的结论.

1 自然图像的小波域 GSM 模型

GSM 模型是一种描述自然图像小波系数统计特征的有效模型, 近年来被成功地用于图像处理和计算机视觉领域[7].

众所周知, 自然图像小波系数的边缘分布呈现很强的非高斯性, 表现为其分布呈现很明显的高尖峰和重脱尾 (如图 1 所示), 传统的高斯模型不能准确地描述自然图像小波系数的统计特性.

小波域 GSM 模型用一个随机场来描述图像小波系数 $\boldsymbol{x}$ 的分布, 该随机场由一个高斯随机场和一个尺度随机变量构成[7]. 记 $\boldsymbol{x}=\{\boldsymbol{x}_i, i\in I\}$ 为 GSM 模型中的随机矢量序列, 其中 I 为矢量的位置索引. $\boldsymbol{x}$ 可以表示为

$$\boldsymbol{x}=s\cdot\boldsymbol{u}=\{s_i\cdot\boldsymbol{u}_i, i\in I\} \tag{1}$$

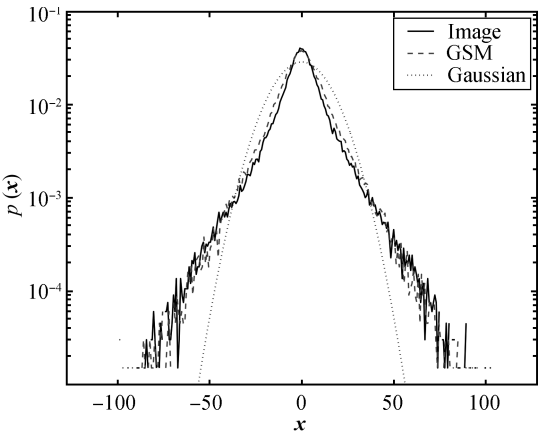
其中的 "=" 表示分布意义上的相等. $\boldsymbol{u}\sim N(0,Q)$ 为一个高斯随机场, 其均值为 0, 协方差阵为 Q; s 是一个值为正的尺度随机变量, 用于控制图像小波系数的方差. s 和 $\boldsymbol{u}$ 相互独立. 给定 s, $\boldsymbol{x}$ 的概率密度函数表示为

$$P_{\boldsymbol{x}|s}(\boldsymbol{x}|s)=\frac{1}{(2\pi)^{\frac{N}{2}}|s^2Q|^{\frac{1}{2}}}\exp\left(-\frac{\boldsymbol{x}^{\mathrm{T}}Q^{-1}\boldsymbol{x}}{2s^2}\right) \tag{2}$$

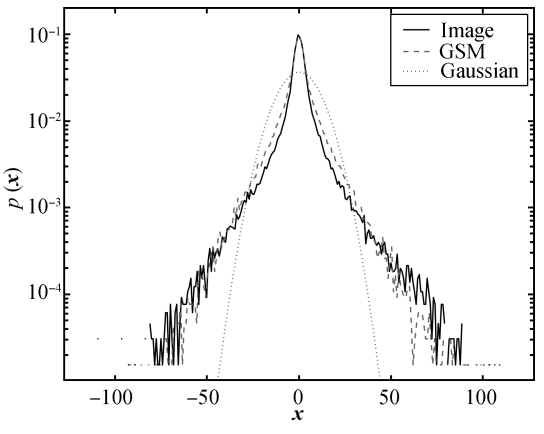
s 可由最大似然算法估计得到[7]

$$\hat{s}=\arg\max_s\{\log(\boldsymbol{x}|s)\}=\sqrt{\frac{\boldsymbol{x}^{\mathrm{T}}Q^{-1}\boldsymbol{x}}{N}} \tag{3}$$

如果假定 x_i 为标量, 模型 (1) 退化为标量 GSM 模型. 此时, 对于不同的 i 和 j, x_i 与 x_j 相互独立; 给定



(a) Baboon



(b) Boat

图 1 利用 GSM 模型和高斯模型描述自然图像小波系数边缘分布的性能比较

Fig. 1 The performances of GSM- and Gaussian-model for describing the marginal histogram of wavelet coefficients of natural images

s_i, x_i 的分布为高斯, 即有 $p_{x_i|s_i}(x_i|s_i)\sim N(0,s_i^2\sigma_u^2)$, 其中 u 为全局高斯随机场, 不失一般性, 可以假定 σ_u^2 为单位值.

图 1 (a) 和 1 (b) 是分别用 GSM 模型和高斯模型拟合自然图像 Baboon 和 Boat 小波系数统计分布的性能比较. 其中实线为图像 HL1 子带系数的实际边缘分布, 虚划线和虚点线分别为 GSM 模型和高斯模型对图像实际分布的拟合. 可以发现 GSM 模型能够很好地拟合图像小波系数的分布, 而传统的高斯模型则难以对自然图像小波系数分布的高尖峰和重脱尾特征进行准确的描述.

2　水印安全性的分析方法

对于扩频水印系统, 扩频载波 (扩频序列) 由密钥产生, 该载波经嵌入信息调制后嵌入到图像载体中, 从而生成水印图像 (为叙述方便, 以下将嵌入了水印的图像简称为水印图像). 对于攻击者而言, 只需要有效估计出扩频载波就可以达到攻击水印安全的目的[1] (例如: 去除、替换和破坏水印信号), 因此在对水印安全的攻击中对密钥的估计等价为对扩频载波的估计. 扩频水印系统不是绝对安全的[1], 在水印通信中会泄漏出关于扩频载波的信息. 对水印通信安全的攻击就是通过对水印图像的多次观察, 估计出有关扩频载波的信息; 而水印安全性分析则是评估水印系统的安全性能并研究影响信息泄漏的有关因素.

考察信息泄漏的方法主要有两大类. 一种方法是利用 Shannon 的信息理论[3]. 该方法中, 令 Z 表示秘密的扩频载波; 用 $h(Z)$ 表示在水印通信之前扩频载波的熵, 它衡量了扩频载波的不确定度; 令 $h(Z|Y)$ 表示水印通信之后, 在已知水印图像的条件下, 扩频载波的条件熵. 这里 $h(\cdot)$ 表示随机变量的微分熵. 扩频载波和水印图像的互信息可以表示为

$$I(Z,Y)=h(Z)-h(Z|Y) \tag{4}$$

即由于水印通信, 对于秘密载波不确定度的减少量. 对于水印通信安全的攻击者来说, $I(Z,Y)$ 表示了水印系统关于扩频载波的信息泄漏. 另一种方法基于 FIM 来考察对于秘密扩频载波进行估计的准确程度. 记 $\boldsymbol{\Theta}=(\theta_1,\theta_2,\cdots,\theta_K)^{\mathrm{T}}$ 为需要估计的一组参数, $\boldsymbol{y}$ 为观察值. 对于一个无偏的估计器, 记 $\boldsymbol{\Theta}$ 的估计值为 $\hat{\boldsymbol{\Theta}}=(\hat{\theta}_1,\hat{\theta}_2,\cdots,\hat{\theta}_K)^{\mathrm{T}}$. 该估计对应的 FIM (式中用 J 表示) 为一个 $K\times K$ 矩阵[8]

$$J=\mathrm{E}(\{\nabla_{\boldsymbol{\Theta}}\ln p(\boldsymbol{y}|\boldsymbol{\Theta})\}\{\nabla_{\boldsymbol{\Theta}}\ln p(\boldsymbol{y}|\boldsymbol{\Theta})\}^{\mathrm{T}}) \tag{5}$$

J 中的每个元素为

$$J_{ij}=\mathrm{E}\left[\frac{\partial\ln p(\boldsymbol{y}|\boldsymbol{\Theta})}{\partial\theta_i}\times\frac{\partial\ln p(\boldsymbol{y}|\boldsymbol{\Theta})}{\partial\theta_j}\right] \tag{6}$$

根据 Cramer-Rao 不等式[9], 在 FIM 可逆的条件下, 估计量均方误差的下界即为 CRB, 定义为

$$\mathrm{var}[\hat{\boldsymbol{\Theta}}-\boldsymbol{\Theta}]\geq\mathrm{CRB}(\boldsymbol{\Theta})=\mathrm{tr}(J^{-1}) \tag{7}$$

其中, $\mathrm{tr}(\cdot)$ 表示求矩阵的迹. J 是衡量信息泄漏的量; CRB 是描述根据观察信息估计参数准确程度的量. 在本文中, 需要估计的参数是扩频载波. 信息泄漏得越多, 攻击者掌握的关于载波的知识就越丰富, 可以得到的估计误差就越小, 对秘密载波的估计就越准确, 而相应的水印安全性则越低.

在实际分析中, 有时 J^{-1} 并不存在, 尤其是存在一些未知的、但是并不需要进行估计的干扰参数时. 在计算传统的 CRB 时, FIM 的定义如式 (5) 所示. 在随机干扰参数 $\boldsymbol{u}$ 存在的情况下, 有 $p(\boldsymbol{y}|\boldsymbol{\Theta})=\int_{-\infty}^{\infty}p(\boldsymbol{y}|\boldsymbol{u},\boldsymbol{\Theta})p(\boldsymbol{u})\mathrm{d}\boldsymbol{u}$. 由于一般情况下该积分很难解析表达, 所以此时难以求出传统的 CRB[10]. 一种替代的办法是使用改进的 CRB (或 MCRB) 来衡量对于参数估计的最小界, MCRB 定义为[10]

$$\mathrm{MCRB}(\boldsymbol{\Theta})=\mathrm{tr}\left(\left\{\mathrm{E}_{\boldsymbol{y},\boldsymbol{u}}\left[\left(\frac{\partial\ln p(\boldsymbol{y}|\boldsymbol{\Theta},\boldsymbol{u})}{\partial\boldsymbol{\Theta}}\right)\times\left(\frac{\partial\ln p(\boldsymbol{y}|\boldsymbol{\Theta},\boldsymbol{u})}{\partial\boldsymbol{\Theta}}\right)^{\mathrm{T}}\right]\right\}^{-1}\right) \tag{8}$$

式 (8) 表明基于 $\boldsymbol{y}$ 有关 $\boldsymbol{\Theta}$ 和 $\boldsymbol{u}$ 的条件似然函数, 可以通过对观察信号和干扰参数求统计平均得到待估计参数的 MCRB. 虽然 MCRB 比传统的 CRB 更 "松", 但它更容易计算到[10−11]; 如果干扰信息为已知的确定量, MCRB 就是传统的 CRB.

在本文中, 分别利用 CRB 和 MCRB 作为对秘密载波在 KMA 和 WOA 情况下的安全性的度量指标. CRB 或 MCRB 的值越小, 表示对秘密载波的无偏估计误差越小, 水印的安全性越低; 反之则表示安全性越高.

3　扩频水印的安全性分析

3.1　扩频水印模型

在常用的扩频水印模型[3−4,6] 中, 水印图像信号由图像载体与水印信号相加得到. 水印信号为经过嵌入信息调制后的秘密载波. 该嵌入过程可以表示为

$$\boldsymbol{y}^j=\boldsymbol{x}^j+\frac{\gamma}{\sqrt{N_c}}\sum_{i=1}^{N_c}\boldsymbol{z}_i a_i^j \tag{9}$$

其中, $\boldsymbol{x}^j=(x_1^j,\cdots,x_{N_v}^j)^{\mathrm{T}}$ 和 $\boldsymbol{y}^j=(y_1^j,\cdots,y_{N_v}^j)^{\mathrm{T}}$ 分别表示第 j 次观察中的图像载体信号和水印图像信号; $\boldsymbol{z}_i$ 为第 i 个秘密载波列向量, 并用 Z 表示由

所有秘密载波列向量构成的矩阵, a_i^j 表示第 j 次观察中第 i 位嵌入信息; γ 为载波的嵌入强度; N_c 用于表示秘密载波的数目; N_o 表示观察的次数; N_v 表示每次观察时图像载体和水印图像的维数, 这里假定秘密载波和图像载体维数相同. 定义载体和水印的相对功率比为 DWR (Document to watermark ratio), 有 $\mathrm{DWR} = 10\lg(\sigma_x^2/\gamma^2\sigma_a^2)$, 其中 σ_x^2 为载体平均功率, 而 $\gamma^2\sigma_a^2$ 为水印的嵌入功率.

以下的分析中, 利用 GSM 模型对自然图像载体 $\boldsymbol{x}^j$ 的统计特性进行描述, 假设载体系数相互独立, 每次观察之间也相互独立, 调制方法采用二进制相移键控 (Binary phase shift keying, BPSK), 并且假设信息嵌入之前进行了伪随机化, 因此 a_i^j 的取值也相互独立. 由于在 KOA 情况下攻击者已经掌握了载体图像, 此时利用 GSM 模型不会带来额外的帮助. 因此本文仅对 KMA 和 WOA 情况下的扩频水印安全性进行分析, 有关 KOA 的安全性分析可以参见文献 [1].

3.2 KMA 情况

在 KMA 攻击的条件下, 攻击者不仅拥有水印图像, 而且知道嵌入图像的信息. 攻击者的目标就是通过对水印信号的多次观察实现对秘密扩频载波的估计.

3.2.1 单载波估计

为了方便说明, 首先以单载波的情况进行分析. 此时, $N_c = 1$, 每次嵌入的信息只有 1 位, 攻击者拥有对水印图像 N_o 次独立的观察和对应的嵌入信息. 由于图像载体各维之间也相互独立, 对于第 j 次观察中的第 k 维, 有 $y_k^j = x_k^j + \gamma a_1^j z_{1k}$, 其中, z_{1k} 表示载波 (此时只有一个载波) 的第 k 位分量; a_1^j 表示对应第 j 次观察时的嵌入信息, 即 $a_1^j = 1$ 或 -1. 用标量 GSM 模型来描述水印载体的分布, 则 x_k^j 为零均值的高斯分布, 其方差为 $s_k^{j2}\sigma_u^2$. 由此可以得到在观测集 $Y^{N_o} = (\boldsymbol{y}^1, \cdots, \boldsymbol{y}^{N_o})$ 下的似然函数和对数似然函数分别为

$$f(Y^{N_o}|\boldsymbol{z}_1) = f(\boldsymbol{y}^1, \cdots, \boldsymbol{y}^{N_o}|\boldsymbol{z}_1) = \prod_{j=1}^{N_o}\prod_{k=1}^{N_v}\frac{1}{\sqrt{2\pi s_k^{j2}\sigma_u^2}}\exp\left(-\frac{\left(y_k^j - \gamma a_1^j z_{1k}\right)^2}{2s_k^{j2}\sigma_u^2}\right) \tag{10}$$

$$\log f(Y^{N_o}|\boldsymbol{z}_1) = \sum_{j=1}^{N_o}\sum_{k=1}^{N_v}\left[\log\frac{1}{\sqrt{2\pi s_k^{j2}\sigma_u^2}} - \frac{\left(y_k^j - \gamma a_1^j z_{1k}\right)^2}{2s_k^{j2}\sigma_u^2}\right] \tag{11}$$

求对数似然函数对被估计参数的偏导数, 得到

$$\frac{\partial}{\partial z_{1i}}\log f(Y^{N_o}|\boldsymbol{z}_1) = \gamma\sum_{j=1}^{N_o}\frac{a_1^j x_i^j}{s_i^{j2}\sigma_u^2} \tag{12}$$

根据第 2 节的说明, FIM 的元素可由式 (13) 和 (14) 确定. 对于 FIM 中的对角元素, 有

$$J_{ii}(\boldsymbol{z}_1) = \int f(Y^{N_o}|\boldsymbol{z}_1)\times \left(\frac{\partial}{\partial z_{1i}}\log f(Y^{N_o}|\boldsymbol{z}_1)\right)^2 \mathrm{d}\boldsymbol{y}^1\cdots\mathrm{d}\boldsymbol{y}^{N_o} = \gamma^2\sum_{j=1}^{N_o}\frac{1}{s_i^{j2}\sigma_u^2} \tag{13}$$

对于 FIM 中的非对角元素, 有

$$J_{ik}(\boldsymbol{z}_1) = \int f(Y^{N_o}|\boldsymbol{z}_1)\left(\frac{\partial}{\partial z_{1i}}\log f(Y^{N_o}|\boldsymbol{z}_1)\right)\times \left(\frac{\partial}{\partial z_{1k}}\log f(Y^{N_o}|\boldsymbol{z}_1)\right)\mathrm{d}\boldsymbol{y}^1\cdots\mathrm{d}\boldsymbol{y}^{N_o} = 0, \quad \forall\, i\neq k \tag{14}$$

所以, 在单载波条件下, 可以求出 FIM 为

$$J(\boldsymbol{z}_1) = \frac{\gamma^2}{\sigma_u^2}\sum_{j=1}^{N_o}\begin{bmatrix}\frac{1}{s_1^{j2}} & 0 & \cdots & 0\\ 0 & \frac{1}{s_2^{j2}} & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \frac{1}{s_{N_v}^{j2}}\end{bmatrix} \tag{15}$$

根据 Cramer-Rao 定理, 可以得到在 KMA 攻击下, 对单载波的估计的界为

$$\mathrm{CRB}(\boldsymbol{z}_1) = \mathrm{tr}(J(\boldsymbol{z}_1)^{-1}) = \frac{1}{\gamma^2}\sum_{i=1}^{N_v}\frac{\sigma_u^2}{\sum_{j=1}^{N_o}\frac{1}{s_i^{j2}}} \tag{16}$$

CRB 反映了对参数无偏估计的准确程度. 由式 (16) 可知, 在 KMA 条件下对单载波无偏估计的最小均方误差与秘密载波的长度和观察的次数有关. 秘密载波越长, 越难以对秘密载波进行准确估计; 同时, 观察次数越多, 获得的有关秘密载波的信息越多, 对其估计也就越准确. 考虑到 GSM 模型对图像小波系数非高斯分布的刻画, 以上 CRB 与秘密载波的长度以及观察次数的关系也是非线性的.

在文献 [1] 中, Cayre 等利用高斯模型描述图像载体, 通过计算 FIM 得到了 KMA 条件下对秘密单载波的无偏估计界, 记为 $\mathrm{tr}(J_C(\boldsymbol{z}_1)^{-1}) = (N_v\sigma_x^2/\gamma^2 N_o)$, 其中 σ_x^2 为载体图像小波系数的方

差. 以下比较式 (16) 和 Cayre 的结果. 为公平起见, 假定 $(1/N_oN_v)\sum_{i=1}^{N_v}\sum_{j=1}^{N_o}s_i^{j2}\sigma_u^2=\sigma_x^2$, 即 GSM 模型和高斯模型中载体图像小波系数的平均方差相等. 由 "算数平均 – 调和平均" 不等式[12]

$$\frac{1}{N}\sum_{j=1}^{N}\frac{1}{m_j}\geq\frac{N}{m_1+m_2+\cdots+m_N}\tag{17}$$

其中 m_j 均为正数, 可知

$$\begin{aligned}&\mathrm{tr}(J(\boldsymbol{z}_1)^{-1})=\\&\frac{1}{\gamma^2}\sum_{i=1}^{N_v}\frac{\sigma_u^2}{\sum\limits_{j=1}^{N_o}\dfrac{1}{s_i^{j2}}}\leq\frac{1}{\gamma^2N_o^2}\sum_{i=1}^{N_v}\sum_{j=1}^{N_o}s_i^{j2}\sigma_u^2=\\&\mathrm{tr}(J_C(\boldsymbol{z}_1)^{-1})\end{aligned}\tag{18}$$

式中, 当 $s_i^1=\cdots=s_i^{N_o}$ 时, "$\leq$" 取 "=". 式 (18) 表明: 文献 [1] 中基于高斯模型的扩频水印系统的安全性能评估是相对 "放大" 的. 比较高斯模型, 利用 GSM 模型可以更加准确地描述自然图像小波系数的统计分布, 据此对秘密载波进行的无偏估计和对扩频水印安全性的评价也更为准确.

3.2.2　多载波估计

在 KMA 条件下, 对多个秘密载波进行估计时, 其对应的调制信息 (嵌入信息) 已知. 此时在观测集 $Y^{N_o}=(\boldsymbol{y}^1,\cdots,\boldsymbol{y}^{N_o})$ 下的对数似然函数和 FIM 分别如式 (19) (见本页下方) 和式 (20) 所示.

$$J(Z)=\mathrm{E}\left\{\left[\frac{\partial\log f(Y^{N_o}|Z)}{\partial(\boldsymbol{z}_1^{\mathrm{T}},\cdots,\boldsymbol{z}_{N_c}^{\mathrm{T}})^{\mathrm{T}}}\right]\left[\frac{\partial\log f(Y^{N_o}|Z)}{\partial(\boldsymbol{z}_1^{\mathrm{T}},\cdots,\boldsymbol{z}_{N_c}^{\mathrm{T}})^{\mathrm{T}}}\right]^{\mathrm{T}}\right\}\tag{20}$$

FIM 中的各元素可由以下方法求出

$$\begin{aligned}&\mathrm{E}\left[\left(\frac{\partial\log f(Y^{N_o}|Z)}{\partial z_{mn}}\right)\left(\frac{\partial\log f(Y^{N_o}|Z)}{\partial z_{pq}}\right)\right]=\\&\frac{\gamma^2}{\sigma_u^4N_c}\mathrm{E}\left(\sum_{j=1}^{N_o}\frac{a_m^jx_n^j}{s_n^{j2}}\sum_{k=1}^{N_o}\frac{a_p^kx_q^k}{s_q^{k2}}\right)=\\&\frac{\gamma^2}{\sigma_u^2N_c}\sum_{j=1}^{N_o}\frac{a_m^ja_p^j}{s_n^{j2}}\delta_{n,q}=\frac{\gamma^2}{\sigma_u^2N_c}J_{(m,n)(p,q)}\end{aligned}\tag{21}$$

其中 z_{mn} 表示第 m 个载波的第 n 维, $J_{(m,n)(p,q)}$ 对应于 FIM 中第 $(m-1)\times N_v+n$ 行、第 $(p-1)\times N_v+q$ 列的元素, 即 FIM 按照以下规律构成

$$J(Z)=\frac{\gamma^2}{\sigma_u^2N_c}\times\begin{bmatrix}J_{(1,1)(1,1)}&J_{(1,1)(1,2)}&\cdots&J_{(1,1)(N_c,N_v)}\\J_{(1,2)(1,1)}&J_{(1,2)(1,2)}&\cdots&J_{(1,2)(N_c,N_v)}\\\vdots&\vdots&\ddots&\vdots\\J_{(N_c,N_v)(1,1)}&J_{(N_c,N_v)(1,2)}&\cdots&J_{(N_c,N_v)(N_c,N_v)}\end{bmatrix}\tag{22}$$

以上 FIM 可以看作由 $N_c\times N_c$ 个分块矩阵构成, 每个分块矩阵为 $N_v\times N_v$ 的对角矩阵. 与文献 [1] 中得到的 KMA 条件下的 FIM 相似, 式 (22) 是对于嵌入信息敏感的, 即嵌入信息的取值影响到式 (22) 的逆存在与否. 这里采用文献 [1] 中的方法, 令 N_o 趋于无穷大, 近似地分析观测次数无穷大时 FIM 的特征以及对应的 CRB.

如果每次观察中, 各个图像载体对应的 s_i^j 相等, 即 $s_i^j=s$ $(1\leq i\leq N_v, 1\leq j\leq N_o)$, 则当 N_o 趋于无穷大时, 式 (22) 中主对角线元素为 N_o/s^2, 主对角线以外的非零元素 $\sum_{j=1}^{N_o}(a_m^ja_n^j/s_i^{j2})=(1/s^2)\sum_{j=1}^{N_o}a_m^ja_m^j\to0$. 这样式 (22) 近似成为一个对角阵, 可以求出该对角阵的逆, 进而得到对应的 CRB 为

$$\mathrm{CRB}(Z)_C=\mathrm{tr}(J_C(Z)^{-1})=\frac{N_c^2N_vs^2\sigma_u^2}{N_o\gamma^2}\tag{23}$$

这便是文献 [1] 中的结果, 在此记为 $\mathrm{CRB}(Z)_C$.

如果每次观察中, 各个图像载体对应的 s_i^j 不相等, 这是自然图像载体的一般情况. 当观测次数无限大时, 式 (22) 中的主对角线元素为 $\sum_{j=1}^{N_o}(1/s_i^{j2})$ $(i=1,\cdots N_v)$. 由于 $a_m^ja_n^j$ 随机取值 (1 或 −1), 且 s_i^{j2} 均为正值, 所以主对角线以外的元素远小于主对角线上的元素. 这种现象随着观测次数增大而趋于明显. 文献 [13] 中对 GSM 模型的研究表明, 自然图像中尺度随机变量的概率密度函数满足 $p(s^2)\propto(1/s^2)$. 由于 s^2 恒为正值, 不失一般性, 可以假设 s^2 同分布. 根据嵌入信息和尺度变量的独立性以及大数定律可知

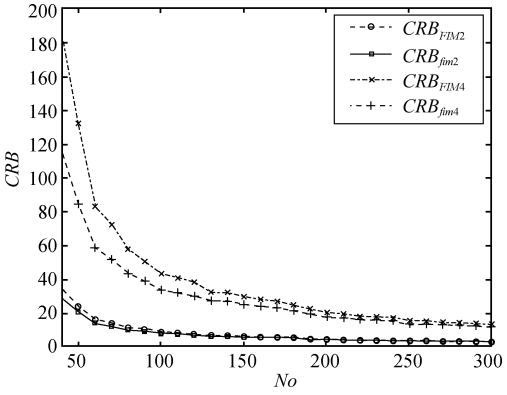
$$\log f(Y^{N_o}|Z)=\sum_{j=1}^{N_o}\sum_{k=1}^{N_v}\left[\log\frac{1}{\sqrt{2\pi s_k^{j2}\sigma_u^2}}-\frac{\left(y_k^j-\dfrac{\gamma}{\sqrt{N_c}}\sum\limits_{m=1}^{N_c}a_m^jz_{mk}\right)^2}{2s_k^{j2}\sigma_u^2}\right]\tag{19}$$

$$\sum_{j=1}^{N_o}\frac{a_m^j a_n^j}{s_i^{j2}}\xrightarrow{N_o\to\infty}N_o\mathrm{E}\left(\frac{a_m^j a_n^j}{s_i^{j2}}\right)=0 \tag{24}$$

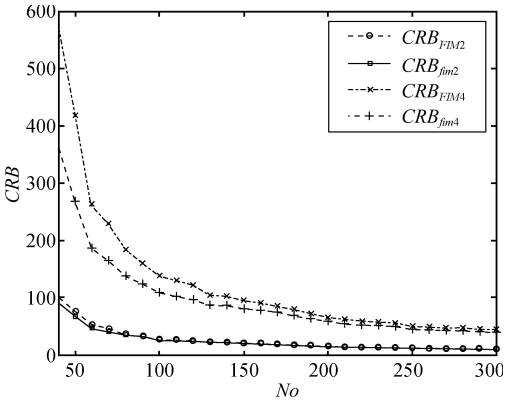
此时, 式 (22) 退化为仅保留其主对角线元素的对角阵, 于是可以用式 (22) 中的主对角线元素构成的对角阵来简化处理, 通过求其逆矩阵的迹得到对应的 CRB, 记为 CRB_{fim}

$$\mathrm{CRB}_{fim}(Z)=\frac{N_c^2\sigma_u^2}{\gamma^2}\sum_{i=1}^{N_v}\frac{1}{\sum\limits_{j=1}^{N_o}\dfrac{1}{s_i^{j2}}} \tag{25}$$

实验仿真结果进一步验证了式 (25) 的正确性. 记式 (22) 逆矩阵的迹为 CRB_{FIM}, 图 2 给出了对于自然图像, 简化的 CRB_{fim} 和 CRB_{FIM} 的关系. 图 2 (a) 和 2 (b) 分别为载波长度为 512 维, DWR 为 15 dB 和 20 dB 条件下 CRB_{fim} 和 CRB_{FIM} 的曲线. 图中载体随机选自 8 幅自然图像小波分解的 HL2, LH2 和 HH2 的子带系数, 曲线名称下标中的 "2" 和 "4" 分别表示所使用的扩频载波数. 实验结果表明, 随着观测次数 N_o 的增大, CRB_{fim} 和 CRB_{FIM} 趋于接近. 由式 (25) 同时可知, 在 KMA 条件下, 由于需要估计的各条载波地位平等, 即当嵌入功率 $\gamma^2=1$ 时, $N_c=1$, 对多载波进行估计的 CRB_{fim} 与对单载波 ($N_c=1$) 估计的 CRB 有相同的形式. 此时, 式 (25) 与式 (16) 相同.



(a) DWR = 15 dB



(b) DWR = 20 dB

图 2 CRB_{FIM} 和 CRB_{fim} 性能比较

Fig. 2 Comparison of CRB_{FIM} and CRB_{fim}

3.3 WOA 情况

在 WOA 情况下, 攻击者仅仅拥有对水印图像的观察值, 需要根据这些观察值来估计秘密载波. 对于攻击者来说, 这是对水印安全性攻击中最为困难的一种. 此时, 只有秘密载波是攻击者的估计目标, 但是未知的嵌入信息却会影响到对秘密载波的正确估计[1, 14].

由于秘密载波和嵌入信息都是未知参量, 在 WOA 条件下不能保证 FIM 的逆存在[1], 从而难以直接求出传统的 CRB. Cayre 在单载波估计的情况下[1], 通过引入对载波能量的约束条件, 使用文献 [10] 中介绍的方法构建了载波约束条件的零空间 H, 在 $(H^{\mathrm{T}}\cdot FIM\cdot H)^{-1}$ 存在的条件下求得估计秘密载波的 CRB. 而在多载波情况下, 必须假设攻击者已知 N_m 个嵌入信息, 从而得到 $N_m\times N_c$ 个附加的约束关系, 用与单载波情况下相同的方法得到了相应的 CRB.

文献 [1] 中为了求得估计秘密载波的 CRB, 需要假定攻击者已知 N_m 个嵌入信息, 这并不符合 WOA 攻击的要求. 考虑到实际的 WOA 中, 如果存在未知的干扰参数, 特别是在非高斯噪声条件下, 载波估计的 CRB 并不一定能用封闭的形式表达[15], 本文利用 MCRB 对 WOA 情况下扩频水印安全性进行评估.

在 WOA 情况下, 根据 MCRB 对秘密载波矢量进行估计, 可以定义对应的 FIM 为: $J_M(Z)=\mathrm{E}_{Y,\boldsymbol{a}}(\boldsymbol{\psi}\boldsymbol{\psi}^{\mathrm{T}})$, 其中

$$\boldsymbol{\psi}=\frac{\partial\log p(Y^{N_o}|Z,\boldsymbol{a})}{\partial(\boldsymbol{z}_1^{\mathrm{T}},\cdots,\boldsymbol{z}_{N_c}^{\mathrm{T}})^{\mathrm{T}}} \tag{26}$$

$\log p(Y^{N_o}|Z,\boldsymbol{a})$ 的计算式见式 (27).

$$\log p(\mathrm{Y}^{N_o}|Z,\boldsymbol{a})=\sum_{j=1}^{N_o}\sum_{k=1}^{N_v}\left[\log\frac{1}{\sqrt{2\pi s_k^{j2}\sigma_u^2}}-\frac{\left(y_k^j-\dfrac{\gamma}{\sqrt{N_c}}\sum\limits_{m=1}^{N_c}a_m^j z_{mk}\right)^2}{2s_k^{j2}\sigma_u^2}\right] \tag{27}$$

$$[J_M(Z)]_{(m,n)(p,q)} = \mathrm{E}_{Y,\boldsymbol{a}}\left(\frac{\partial \ln p(\mathrm{Y}^{N_o}|Z,\boldsymbol{a})}{\partial z_{mn}}\frac{\partial \ln p(\mathrm{Y}^{N_o}|Z,\boldsymbol{a})}{\partial z_{pq}}\right) \tag{28}$$

而且 $\mathrm{var}[\hat{Z}-Z] \geq \mathrm{tr}(J_M(Z)^{-1}) = \mathrm{MCRB}(Z)$. 其中, $J_M(Z)$ 和载波 Z 的下标含义与第 3.2 节中所述相同. 由于

$$\mathrm{E}_{Y,\boldsymbol{a}}\left(\frac{\partial \ln p(Y^{N_o}|Z,\boldsymbol{a})}{\partial z_{mn}}\frac{\partial \ln p(Y^{N_o}|Z,\boldsymbol{a})}{\partial z_{pq}}\right) = \mathrm{E}_{\boldsymbol{a}}\left(\mathrm{E}_{Y|\boldsymbol{a}}\left(\frac{\partial \ln p(Y^{N_o}|Z,\boldsymbol{a})}{\partial z_{mn}}\frac{\partial \ln p(Y^{N_o}|Z,\boldsymbol{a})}{\partial z_{pq}}\right)\right) \tag{29}$$

可以看出, 计算 $J_M(Z)$ 是先求出在假设秘密载波和嵌入信息已知情况下的 FIM, 然后对嵌入信息求期望值. 因此

$$\mathrm{E}_{Y|\boldsymbol{a}}\left(\frac{\partial \ln p(Y^{N_o}|Z,\boldsymbol{a})}{\partial z_{mn}}\frac{\partial \ln p(Y^{N_o}|Z,\boldsymbol{a})}{\partial z_{pq}}\right) = \frac{\gamma^2}{\sigma_u^2 N_c}\sum_{j=1}^{N_o}\frac{a_m^j a_p^j}{s_n^{j2}}\delta_{n,q} \tag{30}$$

$$[J_M(Z)]_{(m,n)(p,q)} = \mathrm{E}_{\boldsymbol{a}}\left(\frac{\gamma^2}{\sigma_u^2 N_c}\sum_{j=1}^{N_o}\frac{a_m^j a_p^j}{s_n^{j2}}\delta_{n,q}\right) = \frac{\gamma^2}{\sigma_u^2 N_c}\sum_{j=1}^{N_o}\frac{\mathrm{E}_{\boldsymbol{a}}(a_m^j a_p^j)}{s_n^{j2}}\delta_{n,q} \tag{31}$$

由式 (31) 可见, $J_M(Z)$ 与嵌入信息的分布有关. 若嵌入信息经过伪随机化且均值为零, 则 $\mathrm{E}_{\boldsymbol{a}}(a_m^j a_p^j) = \sigma_a^2$ $(m=p)$ 或 0 $(m\neq p)$, 其中 σ_a^2 为嵌入序列的方差.

$$[J_M(Z)]_{(m,n)(p,q)} = \frac{\sigma_a^2\gamma^2}{\sigma_u^2 N_c}\sum_{j=1}^{N_o}\frac{1}{s_n^{j2}}\delta_{m,p}\delta_{n,q} \tag{32}$$

由此可得, 在 WOA 条件下估计秘密载波的 MCRB 为

$$\mathrm{MCRB}(Z) = \mathrm{tr}(J_M(Z)^{-1}) = \frac{\sigma_u^2 N_c^2}{\sigma_a^2\gamma^2}\sum_{i=1}^{N_v}\frac{1}{\sum_{j=1}^{N_o}\frac{1}{s_i^{j2}}} \tag{33}$$

若嵌入信息的方差为 1, 则 WOA 情况下的结论与 KMA 情况下的结论相同. 在一般情况下, 秘密载波在 WOA 情况下的安全性与嵌入序列的方差有线性关系.

求 MCRB 的过程中, 只需要假定干扰信息的分布, 而不需要攻击者已知 N_m 条干扰信息, 因此利用 MCRB 计算秘密载波的估计界更为接近 WOA 攻击的条件.

4　仿真结果及其分析

本节根据以上有关基于 GSM 模型扩频水印安全性的理论分析结果, 对多幅具有不同纹理特征的自然图像 (包括 Aerial, Baboon, Barb, Boat, F16, Lena, Peppers 和 Sailboat), 分别计算相应扩频水印系统在 KMA 和 WOA 条件下的 CRB 和 MCRB, 并与 Cayre 的结果[1] 进行比较和分析. 实验中使用双正交 9/7 小波对自然图像进行 2 层分解, 随机选取 HL2, LH2 和 HH2 的子带系数作为载体, 载波维数为 512, 载波的数目分别为 1, 2 和 4.

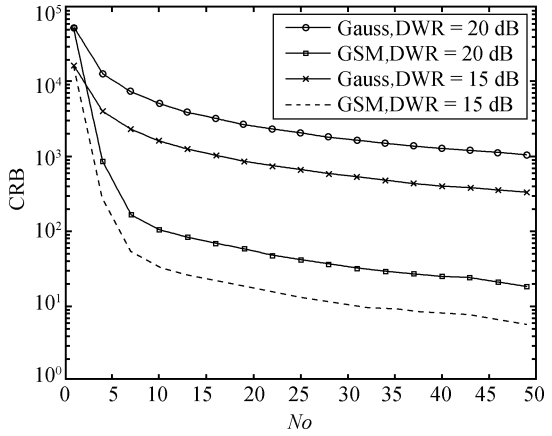
4.1　KMA 条件下的 CRB

图 3 (a) (见下页) 是载波长度为 512, DWR 分别为 20 dB 和 15 dB 条件下, 当观测次数 (N_o) 增大时, 基于 GSM 模型和高斯模型的 CRB 比较. 由于 GSM 模型可以更准确地描述自然图像小波系数的统计分布, 与高斯模型相比, 其具有更低的 CRB, 即对秘密载波的估计更加准确. CRB 在观察次数较小时下降很快, 这说明攻击者的前几次观察对估计秘密载波的贡献很大, 之后的观察中携带的载波信息与以前获得的信息会有重复, 所以对估计秘密载波的贡献逐步减小.

图 3 (b) 比较了 GSM 模型和高斯模型下, 观察次数为 50 次, DWR 分别为 20 dB 和 15 dB 时, CRB 随载波长度 (N_v) 变化的关系. 由于高斯模型认为各次观察中载体方差相同, CRB 与载波的维数成线性关系; 而基于 GSM 模型的分析中, 各次观察的载体方差由尺度因子控制, 由于各次观测的图像载体系数方差不同, 使得由秘密载波长度增加所带来的估计不确定度的增加量不相同, 即有非线性关系. 一般地, CRB 会随载波维数增长而增大, 表明增加秘密载波长度可以加大估计的难度, 从而提高了水印系统的安全性.

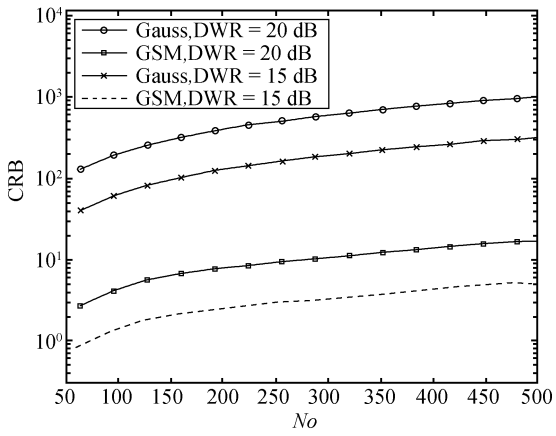
由图 3 (a) 和 3 (b) 可以看出, DWR 越低, 表示嵌入水印的功率相对越高; 相应的 CRB 值越低, 表示对秘密载波估计的准确性越高, 与此 DWR 对应的水印安全性就越低.

图 3 (c) 和 3 (d) 分别表示在 KMA 条件下, 当 DWR 为 15 dB 和 20 dB 时, 对多载波 (载波数为 2 和 4) 进行无偏估计的 CRB, 其中载波的长度为 512. 图中标记 $\mathrm{GSM_{fim}}$的曲线表示为了简化计算由式 (25) 得到的 CRB; 而标记 Gauss 的曲线为根据文献 [1] 中的基于高斯模型方法计算的 CRB. 图中曲线标记的数字表示估计的载波数. 可以看出基于 GSM 的 CRB 具有更低的值.



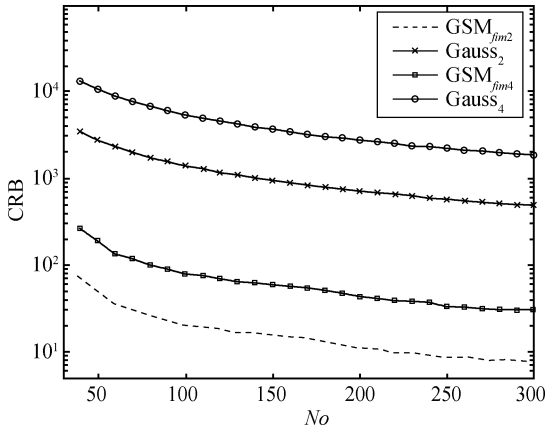
(a) 单载波 $N_v = 512$

(a) Single-carrier $N_v = 512$



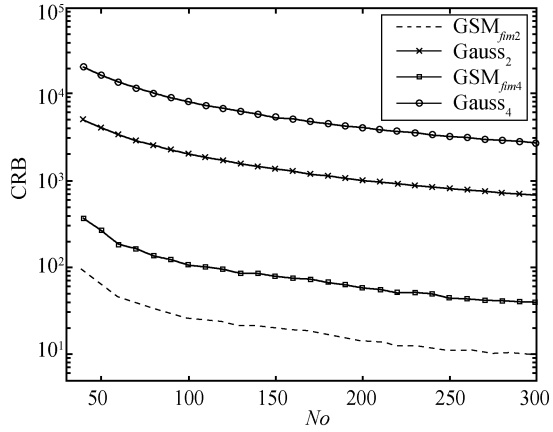
(b) 单载波 $N_o = 50$

(b) Single-carrier $N_o = 50$



(c) 多载波 DWR = 15 dB

(c) Multi-carrier DWR = 15 dB



(d) 多载波 DWR = 20 dB

(d) Multi-carrier DWR = 20 dB

图 3 KMA 条件下对秘密载波估计的 CRB

Fig. 3 CRB of estimation on secret carrier under KMA

4.2 WOA 条件下的 MCRB

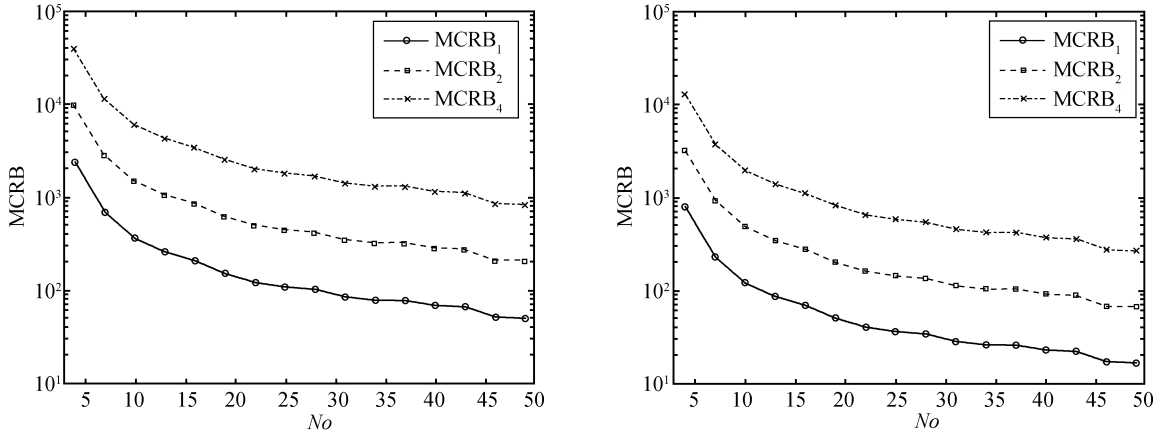
图 4 (a) 和 4 (b) (见下页) 分别是在 WOA 条件下, DWR 为 15 dB 和 20 dB, 载波长度为 512 时的 MCRB. MCRB_1, MCRB_2 和 MCRB_4 分别为单载波、2 载波和 4 载波估计时的 MCRB. 由于 MCRB 和 CRB 都是对于参数估计总的误差的度量, 随着载波数目的增多, 在相同条件下总的估计误差增加; 而随着观察次数的增多, 对于参数估计的误差逐渐降低. 通过比较图 4 (a) 和 4 (b) 可以看出, 在其他条件相同时, 高的 DWR 值导致了高的 MCRB 值, 即嵌入水印功率越低, 水印的安全性越高.

4.3 不同图像载体的 CRB 比较

图 5 (a) 和 5 (b) (见下页) 比较了在 KMA 情况下, Baboon 和 F16 分别在固定载波长度为 512 和固定观测次数为 30 次条件下, DWR = 15 dB 时的 CRB. 同时, 用带圆圈的实线表示了对应条件下基于高斯模型的 CRB. 考虑到 Baboon 与 F16 相比, 图像细节变化更为丰富, 采用 GSM 模型描述时, 前者的小波系数方差总体上会大于后者. 从图 5 (a) 和 5 (b) 中可以看到, 在不同的观察次数和载波长度下, 由 Baboon 得到的 CRB 都大于 F16 的 CRB, 故以 Baboon 作为载体的扩频水印图像将具有更高的安全性. 一般地, 对于扩频水印系统, 选择具有丰富细节变化的图像作为载体将能得到更高的安全性.

5 结论

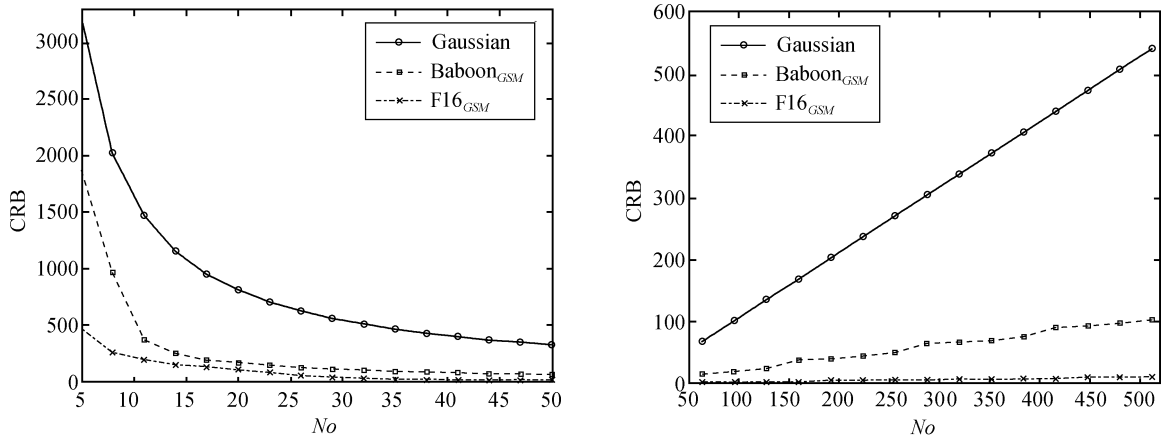
本文利用 GSM 模型刻画自然图像小波系数的统计分布, 并对扩频水印系统的安全性进行了理论分析, 得到了在 KMA 和 WOA 情况下对扩频载波估计的 CRB 和 MCRB. 分析结果表明, 由于载体图



(a) DWR = 15 dB　　(b) DWR = 20 dB

图 4　WOA 条件下的 MCRB

Fig. 4　MCRB under WOA



(a) $N_v = 512$, DWR = 15 dB　　(b) $N_o = 30$, DWR = 15 dB

图 5　不同图像载体的 CRB 比较

Fig. 5　Comparison of CRB from different natural images

像统计分布的非高斯性, 其扩频水印安全性与观测次数及扩频载波的长度具有非线性关系, 而与扩频载波的嵌入能量及嵌入信息的方差有线性关系. 与 Cayre 等的工作[1] 相比, 本文的结果可以获得对扩频水印系统安全性的更准确评价; 同时, 本文的工作对设计新一代的安全、鲁棒水印算法也具有重要的意义.

References

1 Cayre F, Fontaine C, Furon T. Watermarking security: theory and practice. *IEEE Transactions on Signal Processing*, 2005, **53**(10): 3976−3987

2 Kerckhoffs A. La cryptographie militaire. *Journal Des Sciences Militaries*, 1883, **9**: 5−38

3 Comesaña P, Pérez-Freire L, Pérez-González F. Fundamentals of data hiding security and their application to spread-spectrum analysis. In: Proceedings of the 7th Information Hiding Workshop. Barcelona, Spain: Springer, 2005. 146−160

4 Cox I J, Miller M L, Bloom J A. *Digital Watermarking*. San Francisco: Morgan Kaufmann Publisher, 2001

5 Pérez-Freire L, Pérez-González F, Furon T, Comesaña P. Security of lattice-based data hiding against the known message attack. *IEEE Transactions on Information Forensics and Security*, 2006, **1**(4): 421−439

6 Ni J Q, Zhang R Y, Fang C, Huang J W, Wang C T, Kim H J. Watermarking security incorporating natural scene statistics. In: Proceedings of the 10th International Workshop. Santa Barbara, USA: Springer, 2008. 132−146

7 Wainwright M J, Simoncelli E P. Scale mixtures of Gaussians and the statistics of natural images. In: Proceedings of the Neural Information Processing Systems. Cambridge, USA: MIT Press, 2000. 855−861

8 van Trees H L. *Detection, Estimation, and Modulation Theroy*. New York: John Wiley and Sons, 1968. 52−86

9 Cover T M, Thomas J A. *Elements of Information Theory*. New York: Wiley, 1991

10 Stoica P, Ng B C. On the Cramer-Rao bound under parametric constraints. *IEEE Signal Processing Letters*, 1998, **5**(7): 177−179

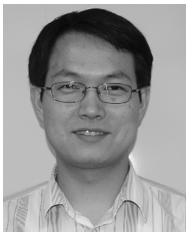
11 D′Andrea N A, Mengli U, Reggiannini R. The modified Carmer-Rao bound and its application to synchronization problems. *IEEE Transactions on Communications*, 1994, **42**(2 - 4): 1391−1399

12 Chou Y L. *Statistical Analysis*. Berlin: Elsevier Publishing Company, 1969

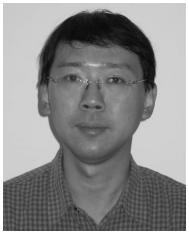
13 Portilla J, Strela V, Wainwright M J, Simoncelli E P. Image denoising using scale mixtures of Gaussians in the wavelet domain. *IEEE Transactions on Image Processing*, 2003, **12**(11): 1338−1351

14 Shun-Ichi A, Cardoso J F. Blind source separation-semiparametric statistical approach. *IEEE Transactions on Signal Processing*, 1997, **45**(11): 2692−2700

15 Gini F, Reggiannini R, Mengali U. The modified Cramer-Rao bound in vector parameter estimation. *IEEE Transactions on Communications*, 1998, **46**(1): 52−60



张 东 中山大学信息科学与技术学院讲师, 博士研究生. 主要研究方向为信息安全和多媒体信号处理. 本文通信作者.
E-mail: zhangd@mail.sysu.edu.cn
(**ZHANG Dong** Ph. D. candidate, lecturer at the School of Information Science and Technology, Sun Yat-Sen University. His research interest covers information security and multimedia signal processing. Corresponding author of this paper.)



倪江群 中山大学信息科学与技术学院教授, 博士. 主要研究方向为信息安全和多媒体信号处理.
E-mail: issjqni@mail.sysu.edu.cn
(**NI Jiang-Qun** Ph. D., professor at the School of Information Science and Technology, Sun Yat-Sen University. His research interest covers information security and multimedia signal processing.)

李大捷 美国杨柏翰大学电气与计算机工程系教授, 博士. 主要研究方向为机器视觉和模式识别.
(**LEE Dah-Jye** Ph. D., professor in the Department of Electrical and Computer Engineering, Brigham Young University, USA. His research interest covers robot vision and pattern recognition.)