基于差错控制编码的水印检测

许文丽, 王育民
(西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071)

摘 要: 提出了一种基于差错控制编码(ECC)的水印检测方法, 并且依据编码原理提出了进行水印检测的门限值的确定方法. 基本思想是利用 ECC 对原始水印信息进行编码, 水印检测时把提取出的待测编码水印与反馈水印进行比较, 将其差值与设定的门限值进行比较, 从而来判断水印存在与否. 实验是基于 DWT, 采用的是 ECC 的 Turbo 码进行水印检测. 仿真结果表明, 该方法大大减少了水印图像在传输中的错误, 水印的鲁棒性得到了极大的提高.

关键词: 差错控制编码; 水印检测; Turbo 码
中图分类号: TP391 文献标识码: A 文章编号: 0372-2112 (2005) 07-1187-04

Watermark Detection Based on Error Control Codes

XU Wen-li[1], WANG Yu-min
(National Key Laboratory of ISN, Xidian University, Xi'an, Shaanxi 710071, China)

Abstract: In this paper, a method for watermark detection based on error control codes and a method for determining threshold for watermark detection are proposed. The basic idea is that watermark be encode with ECC, and then the extracted watermark subtract the feedback one, finally compare the subtractive result with the threshold selected for watermark detection. Thus the existence or not of watermark can be detected. The Turbo code of error control codes is used in the experiment. The simulation results using an algorithm based on DWT show that the errors of watermark image presented during the transportation is reduced greatly and the robustness of it is enhanced with the method proposed.

Key words: error control codes; watermark detection; Turbo code

1 引言

水印检测的目的是判断一幅图像中存在水印的可能性, 现存的大多数鲁棒水印系统中的水印可分为两大类: 无意义水印和有意义水印. 在前者中, 将一个单一的伪随机序列作为水印嵌入到图像中, 水印检测器计算收到的图像和已知水印序列之间的线性相关值, 把计算结果与设定的门限值进行比较, 以此来判断载体作品中是否嵌入了水印, 但是无意义水印的实际应用价值不大; 在后一类中, 水印信号是代表一定意义的文本、声音、图像或视频信号. 为了提高原始水印信息的保密性和抗剪切攻击的鲁棒性, 在水印嵌入到宿主图像前可进行扩频、位分解、置乱、变换或几种方法相结合的预处理. 另外, 数字水印作为在数字宿主产品这一信道中传输的信号, 要遭受各种有意无意噪声的攻击, 为了提高水印信息的鲁棒性, 可以采用通信中的差错控制码(Error Control Code-ECC)技术, 对数字版权信息进行编码, 生成数字水印信息, 以提高数字水印在信道中传输的可靠性, 以及抗干扰、抗攻击的能力.

数字水印检测大多采用相关检测的方法[1]和基于假设检验理论的方法. 采用这些方法进行水印检测时, 关键问题是如何确定检测阈值, 检测阈值与人们所期望的检测器错误概率紧密相关. 检测阈值选取得越低, 水印检测器产生漏检错误的概率越小, 但虚警概率会增加; 相反, 检测阈值越高, 虚警概率越小, 漏检概率就越大. 在设计水印系统时, 一般会根据具体的应用背景确定总错误率的上限或者虚警错误率的上限, 然后依据设计指标里的错误率要求来确定检测阈值. 这些方法都是先建立检验统计量模型, 然后根据统计量的分布, 计算其均值和方差, 从而来确定虚警概率和漏警概率, 并以此来求得门限值[2].

文中为了提高要嵌入的有意义信息(如版权信息)的安全保密性, 首先对版权信息进行伪随机化, 然后充分利用了差错控制码中 Turbo 码的特性及其纠错性能, 对伪随机化后的版权信息进行差错控制编码, 以进一步降低水印在传输过程中的误码率, 增强水印在传输过程中的可靠性和抗剪切攻击的鲁棒性, 文中还提出了基于 Turbo 码的水印信息检测门限值的计算方法.

2 差错控制码及其特性

为降低水印在传输过程中的误码率, 通常在版权信息嵌入到载体作品前对其进行差错控制编码, 来增强水印的可靠性. 目前用于水印生成的差错控制码主要有[4]: ①汉明(Hamming)码, 它是一种基本的线性分组码. ②BCH(Bose-ChauHurHoQuengHem)码, 它是一类特殊的循环码, 而循环码是特殊的线性分组码. ③RS(Reed-Solomen)码, 它是非二进制 BCH 码. ④卷积码. ⑤Turbo 码.

收稿日期: 2004-04-17; 修回日期: 2005-05-17
基金项目: 国家"十五"军事通信技术预研(No. 41001040303); 国家 863 计划项目(No. 2002AA144060)

到目前为止,Turbo 码在现有信道编码方案中是最好的. 它巧妙地将卷积码和随机交织器结合在一起, 在实现随机编码思想的同时, 通过分量码的并行级联实现了由短码(分量码) 构造长码(Turbo 码) 的方法, 并采用软输出迭代译码来逼进最大似然译码, 达到了近 Shannon 理论极限的性能. 尤其在低信噪比(SNR) 下表现出的接近于 Shannon 极限的优异的误比特率(BER) 性能, 这使得它不但在抵御加性高斯噪声方面性能优越, 而且具有很强的抗衰落、抗干扰能力. Turbo 码译码器的迭代译码方式使得其性能远优于其他译码器. 仿真实验表明, 迭代译码的误比特率都随着信息序列长度的增加而降低. 正是由于 Turbo 码的特性及其优异的纠错性能, 文中采用了 Turbo 码对水印信息进行编码, Turbo 码编码器的结构框图如图 1 所示, 本文采用的 Turbo 码编码器是生成矩阵为(7,5), 码率为 1/2 的两个相同的递归系统卷积码作为分量码的 Turbo 码编码器, 如图 2 所示.

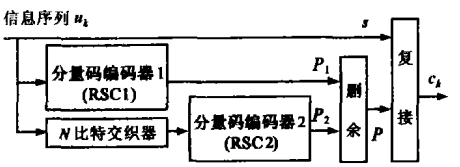

图 1 Turbo 码编码器结构框图

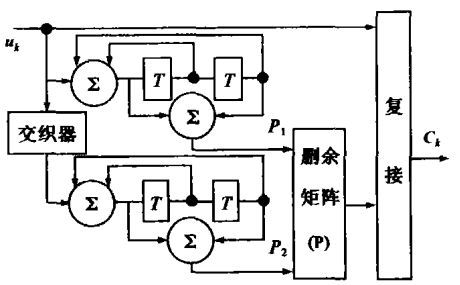

图 2 (7,5) Turbo 码编码器

Turbo 码编码器主要由分量编码器、交织器以及删余矩阵和复接器组成, 由于 Turbo 码主要是在低信噪比条件下具有性能优势, 所以文中选择递归系统卷积(RSC) 码作为分量码. 两个分量码的输入信息序列 $\boldsymbol{u}_k=\{u_1, u_2, \cdots, u_N\}$ 是相同的, 信息序列在送入第一个分量编码器进行编码的同时作为系统输出 s_k 直接送至复接器. 两个分量编码器输出的校验序列分别为 $\boldsymbol{u}_k^{p1}$ 和 $\boldsymbol{u}_k^{p2}$. 为了提高码率和效率, 可以将两个校验序列经过删余后得到 $\boldsymbol{u}_k^{p}$ 再与系统输出 s_k 一起经过复接构成码字序列 $\boldsymbol{c}_k$.

Turbo 码译码器的基本结构如图 3 所示.

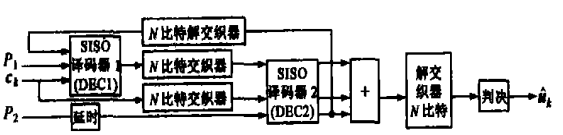

图 3 Turbo 码译码器结构框图

译码器 DEC1 对分量码 RSC1 进行最佳译码, 产生信息序列 $\boldsymbol{u}$ 中每一比特的似然信息, 并将其中的"新信息"经过交织作为先验信息送给 DEC2, DEC2 对 RSC2 进行最佳译码, 将产生的似然比信息中的"外信息"经过解交织送给 DEC1, 进行下一次译码. 这样, 经过多次迭代, DEC1, DEC2 的外信息趋于稳定, 似然比渐进值逼近于整个码的最大似然译码, 然后对此似然比进行判决, 就可得到信息序列 $\boldsymbol{u}$ 的每一比特的最佳估值序列 $\hat{\boldsymbol{u}}$.

3 基于差错控制编码的水印检测

基于差错控制码的水印系统框图如图 4 所示, 其中水印检测过程如图 5 所示, 详细过程见 3.3 节水印检测部分.

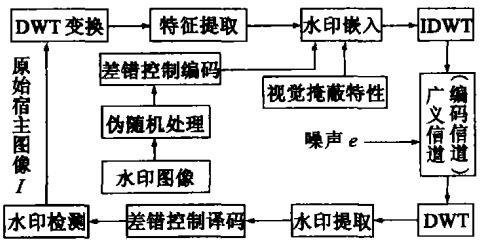

图 4 基于差错控制编码的水印系统框图

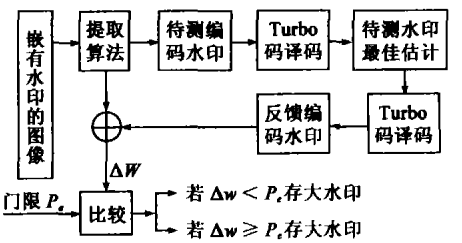

图 5 基于 Turbo 码的水印检测过程

3.1 数字水印的产生

3.1.1 原水印图像信息与伪随机序列相乘或异或

文中的版权信息是有意义的图像, 为了提高版权图像信息的保密性和抗剪切攻击的鲁棒性, 一种简单的方法是将原水印信息与伪随机序列进行相乘或异或操作, 另一种简单的方法是对原水印信息进行伪随机排序. 文中采用前一种方法, 令伪随机序列 $\boldsymbol{p}$ 与原始水印序列 $\boldsymbol{m}$ 的长度相等为 N, $m_i \in \{0, 1\}$, $p_i \in \{0, 1\}$, 这两个序列进行如下异或操作 $w_i = m_i \oplus p_i$, 得到待嵌入的水印信息 $\boldsymbol{w}=\{w_i \mid w_i \in \{0, 1\}, 0 \leqslant i \leqslant N-1\}$; 若 $m_i \in \{-1, 1\}$, $p_i \in \{-1, 1\}$, $0 \leqslant i \leqslant N$, 则这两个序列进行相乘操作 $w_i = m_i \cdot p_i$, 得到有待嵌入的水印信息 $\boldsymbol{w}=\{w_i \mid w_i \in \{-1, 1\}, 0 \leqslant i \leqslant N-1\}$.

3.1.2 差错控制编码水印的生成 将原始水印信息进行伪随机处理后, 对其进行差错控制编码, 采用图 2 所示的 Turbo 码编码器. 两个递归系统卷积码的码率为 1/2, 编码后, 总的码率为 1/3, 经过采用删余矩阵 $\boldsymbol{p}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ 后, 码率就会提高到 1/2. 这样, 系统输出与校验比特复接后的码字序列为 $\boldsymbol{c}=\{u_0, u_0^{p}{}_1, u_2, u_2^{p}{}_2, u_3, u_3^{p}{}_3, \cdots, u_{N-1}, u_{N-1}^{p}{}_2\}$.

3.2 基于 DWT 的水印嵌入

首先对原始宿主图像进行小波变换: 选取适当的小波基对原始图像 I 进行 L 级小波分解, 图像经小波分解后, 子带图像 LL_L 集中了原始图像的绝大多数能量, 为原始图像的逼近

子图, 具有较强的抵抗外来影响的能力, 稳定性好. 但其视觉感知重要, 在此嵌入水印, 不可见性差, 水印嵌入的信息量少. 所以将水印嵌入到边缘细节子带 (LH, HL, HH) 中, 按幅值大小对系数进行排序, 选取前 M 个幅值最大的系数, 利用乘性嵌入公式 $X_i^w = X_i(1+\alpha w_i)$, 将水印信息嵌入到原始图像中.

3.3 水印提取及基于差错控制码的水印检测

首先将接收机接收到的嵌有水印信息的图像进行 DWT 变换, 根据水印嵌入的位置密钥, 找出嵌入水印的系数, 根据 $w_i = \dfrac{X_i^w / X_i - 1}{\alpha}$, 提取出待测编码水印信息, 然后将待测编码水印交给 Turbo 码译码器, 经过多次迭代得到待测水印的最佳估值序列, 再用 Turbo 码编码器对估计出的水印序列进行编码成为反馈编码水印, 最后将反馈编码水印与待测编码水印进行比较, 如果之差小于门限值 P_e 就称检测到了水印, 否则声明没有水印存在, 基于 Turbo 码的水印检测过程如图 5 所示.

水印信息作为原始宿主图像中传输的信号, 由于信道中存在噪声及各种有意无意攻击, 使得嵌入的为 w_i 时不一定判为 w_i, 从而对提取出的水印序列造成误判. 下面讨论一个比较实际的信道, 输入信道的信号是二相移相键控 (BPSK), 信道噪声是加性高斯白噪声 (AWGN), 信道输出量化成二进制, 由通信原理[6] 可知, 这种信道的误码率 P_e 为:

$$P_e = \frac{1}{2\pi}\int_{2E/N_0}^{\infty} e^{-x^2/2}dx \approx \frac{1}{2}e^{-E_b/N_0} \quad (\text{无编码}) \qquad (1)$$

式中 E_b 是信道中传输的每一符号的能量, N_0 是单边噪声功率谱密度.

若应用差错控制码编码, 码率为 R, 则有效信息的能量 E_s 为

$$E_s = E_bR \qquad (2)$$

采用差错控制编码时, 每产生一次错误译码事件, 便产生一个信息元的译码错误, 根据式 (6) $P_e = \dfrac{1}{2}e^{-dR\frac{E_b}{N_0}}$ 可知, 对于固定的 E_b/N_0, 有编码的误码率 P_e 中 e 指数项比无编码时要大 dR 个因子, 称 $r = 10\lg dR$ (dB) 为渐进编码增益 (纯编码增益). 由此可见, 对水印信息经过差错控制编码后, 对提取出的水印信息进行译码时, 误码率大大降低了.

对一个 n 比特的随机序列, 假定采用 BPSK 调制, 则相应于第 i 个 n 维码矢量 $\boldsymbol{c}_i = [c_{i1}, c_{i2}, \cdots, c_{in}]$ 的发送信号可以等效为一个 n 维矢量 $\boldsymbol{s}_i = [s_{i1}, s_{i2}, \cdots, s_{in}]$, $i = (1, 2, \cdots m)$, $s_{ik} = \begin{cases} 1 & \text{当 } c_{ik} = 1 \\ -1 & c_{ik} = 0 \end{cases}$ 即 $s_{ik} = 2c_{ik} - 1$. 设接收端得到的接收序列为 $\boldsymbol{r}_i = [r_{i1}, r_{i2}, \cdots, r_{in}]$, 对于 AWGN 信道, 设相应的噪声序列为 $\boldsymbol{n}_i = [n_{i1}, n_{i2}, \cdots, n_{in}]$, 当发送信号为 $\boldsymbol{s}_i$, 接收机判决为 $\boldsymbol{s}_j$ 的成对错误概率为:

$$\begin{aligned} p_e(\boldsymbol{s}_i \to \boldsymbol{s}_j) &= p\left\{\sum_{k=1}^{n}|r_{ik} - s_{ik}|^2 \geqslant \sum_{k=1}^{n}|r_{ik} - s_{jk}|^2\right\} \\ &= p\left\{\sum_{k=1}^{n} n_{ik}(s_{jk} - s_{ik}) \geqslant 2d\right\} \end{aligned} \qquad (3)$$

定义随机变量 $A = \sum_{k=1}^{n} n_{ik}(s_{jk} - s_{ik})$, 由于 n_{ik} 是均值为零, 方差为 σ^2 的高斯随机变量, 所以 A 服从均值为零, 方差为 $\sigma_A^2 = 4d\sigma^2$ 的高斯分布, d 是这一对码字序列之间的汉明距离, 从而

$$p_e(d) = p_e(\boldsymbol{s}_i \to \boldsymbol{s}_j) = Q\left[\sqrt{2dR\frac{E_b}{N_0}}\right]$$

其中

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-\frac{t^2}{2}}dt \text{ 是误差函数} \qquad (4)$$

从性质:

$$Q(x) \leqslant \frac{1}{2}e^{-\frac{x^2}{2}}, \ x \geqslant 0 \qquad (5)$$

得

$$p_e(d) \leqslant \frac{1}{2}e^{-dR\frac{E_b}{N_0}} \qquad (6)$$

由此可得, AWGN 信道上分组码的误码率为

$$\begin{aligned} p_e &\leqslant \sum_{d=d_{\min}} A_d p_e(d) = \sum_{d=d_{\min}} A_d Q\left(\sqrt{2dR\frac{E_b}{N_0}}\right) \\ &\leqslant \frac{1}{2}\sum_{d=d_{\min}} A_d e^{-dR\frac{E_b}{N_0}} \end{aligned} \qquad (7)$$

其中 A_d 是汉明距离为 d 的码字数, A_d 的值可通过码的重量枚举函数 $A(X)$ 来获得.

利用不等式 $Q\left(\sqrt{x+y}\right) \leqslant Q\left(\sqrt{x}\right)e^{-\frac{y}{2}}$, $x, y \geqslant 0$, 由式 (7) 可得分组码的误码率为

$$\begin{aligned} P_e &\leqslant Q\left(\sqrt{2d_{\min}R\frac{E_b}{N_0}}\right) e^{d_{\min}R\frac{E_b}{N_0}} \sum_{d=d_{\min}} A_d e^{-dR\frac{E_b}{N_0}} \\ &= Q\left(\sqrt{2d_{\min}R\frac{E_b}{N_0}}\right) e^{d_{\min}R\frac{E_b}{N_0}} A(X)\big|_{X=e^{-R\frac{E_b}{N_0}}} \end{aligned} \qquad (8)$$

对于 Turbo 码, 令 $A_{wl}^{c}(Z)$ 和 $A_{w2}^{c}(Z)$ 分别是分量码编码器 RSC1 和 RSC2 的条件重量枚举函数, 则 Turbo 码的整体的条件重量枚举函数为

$$\begin{aligned} A_w(Z) &= \frac{A_{w1}^{C_1}(Z)A_{w2}^{C_2}(Z)}{C_N^w} \\ &\approx \sum_{n_1=1}^{n_{\max}}\sum_{n_2=1}^{n_{\max}} \frac{C_N^{n_1}C_N^{n_2}}{C_N^w} A(w, Z, n_1)A(w, Z, n_2) \\ &\approx \sum_{n_1=1}^{n_{\max}}\sum_{n_2=1}^{n_{\max}} \frac{u!}{n_1!\,n_2!} N^{n_1+n_2-w} A(w, Z, n_1)A(w, Z, n_2) \end{aligned} \qquad (9)$$

当 $n_1 = n_2 = n_{\max}$ 时上式达到最大值, 所以有

$$A_w(Z) \approx \frac{u!}{(n_{\max}!)^2} N^{2n_{\max}-w}[A(w, Z, n_{\max})]^2 \qquad (10)$$

将上式代入式 (8), 可得 Turbo 码的误码率为

$$\begin{aligned} P_e \leqslant Q\left(\sqrt{2d_{\min}R\frac{E_b}{N_0}}\right) e^{d_{\min}R\frac{E_b}{N_0}} \frac{u!}{(n_{\max}!)^2} \\ \cdot N^{2n_{\max}-w}[A(w, Z, n_{\max})]^2\big|_{Z=e^{-R\frac{E_b}{N_0}}} \end{aligned} \qquad (11)$$

由于译码错误, 使得 $\boldsymbol{c}_i$ 错译成码字 $\boldsymbol{c}_j$, 此时 $\boldsymbol{c}_j$ 的虚警概率为:

$$p_{fp}^{c_j} = p(\boldsymbol{c}_i | \boldsymbol{c}_j) = p_e(d) \qquad (12)$$

由此可得, 无条件虚警概率是式 (12) 与所有发生错误事件码字的数量相乘即

$$p_{fp} = \sum_{\text{all codewords}} p(fp | c_j, \forall j) \qquad (13)$$

$$p_{fp} \leqslant \sum_{d=d_{\min}} A_d p_e(d) \leqslant Q\left(\sqrt{2d_{\min}R\frac{E_b}{N_0}}\right) e^{d_{\min}R\frac{E_b}{N_0}} \cdot \frac{w!}{(n_{\max}!)^2} N^{2n_{\max}-w}[A(w,Z,n_{\max})]^2\Big|_{Z=e^{-R\frac{E_b}{N_0}}} \quad (14)$$

另一方面, 如果提取出的水印码字至少有 $t+e$ 位是错误的, 超过了检、纠错码的能力, 那么水印将会被漏掉[7]. 码长为 n 的码字中, 有 r 比特错误的概率为:

$$\binom{n}{r} p_b^r (1-p_b)^{n-r} \quad (15)$$

此处 p_b 为任一比特被译码错误的概率. 假设所有的码字是等概率的, 则漏警概率为

$$P_{\text{miss}} = \sum_{r=p_e n}^{n} \binom{n}{r} p_b^r (1-p_b)^{n-r} \quad (16)$$

此时检测概率为:

$$P_d = 1 - P_{\text{miss}} = \sum_{r=0}^{p_e n-1} \binom{n}{r} p_b^r (1-p_b)^{n-r} \quad (17)$$

至此, 用户就可根据采用的接收准则, 通过对信道噪声和接收机性能的分析, 来确定 p_e 的上限; 然后根据用户对虚警概率和检测概率的不同要求来折衷选择适合自己的 p_e, 这样就可根据选择的 p_e 来进行水印检测.

4 实验结果

实验中使用的是经典的 512× 512 的 Lena 灰度图像作为原始图像, 原始水印是一副 32 × 32 的二值图像, 分别如图 6 (a) 和 6(b) 所示. 第一组实验是对原始图像和原始水印图像以小波基“ db1” 进行三级小波分解, 然后选取幅值最大, 且与水印序列长度相等的 M 个系数, 将水印图像系数按照第 3 节所述乘性嵌入法则及提取方法进行水印嵌入和提取操作.

(a) 原始 Lena 图像 (b) 原始水印图像

图 6

在第二组实验中, 首先对原始水印图像进行伪随机化和用两个相同的 RSC 进行 Turbo 码编码, 然后进行第一组实验的步骤. 当提取出编码水印后, 用 Log- MAP 进行 Turbo 码译码和去伪随机操作, 文中所选的适合的迭代次数是 5 次. 水印图像经 Turbo 码编码后, 尽管嵌入水印后的图像经受各种常见攻击, 可是提取出的水印依然很清晰, 仿真实验结果如图 7 所示.

实验结果表明, 水印图像经 Turbo 码编码后, 水印的可靠性和抗各种攻击的鲁棒性都得到了极大的提高, 在第一组不进行水印编码的实验中, 对嵌有水印的图像进行剪切攻击后, 提取出的水印几乎无法识别, 这说明其抗剪切攻击的能力很弱. 而在第二组实验中, 同样对嵌有水印的图像进行了各种攻击以及剪切攻击, 可提取出的水印信息却非常清晰. 由此可见, 水印信息嵌入到原始宿主图像前, 对其进行 ECC 编码, 能够大大提高其抗各种攻击的鲁棒性, 尤其在抗剪切攻击能力方面有着显著的优势.

图 7 未经编码水印的提取检测与基于 ECC 编码水印的提取检测的比较

5 结论

文中提出了基于差错控制码的水印检测算法, 及门限值的计算方法. 基于 ECC 检测水印时, 不需要参考水印, 并且每次迭代期间都采用软输出, 这比一般的检测器都减少了性能损失. 用户选择一个最大的允许输出 BER, 然后根据虚警概率和检测概率的折衷来选择输入 BER 的门限值, 以此门限值来确定水印的存在与否. 由于引入了差错控制码技术, 使得水印在传输过程中的出错率大大降低, 水印传输的可靠性以及水印抗各种攻击的鲁棒性, 尤其抗剪切攻击的能力都得到了极大提高.

参考文献:

[1] Qiang Cheng, Thomas S Huang. Domain multilicative watermarks robust optimum detection of transform[J]. IEEE Transactions on Signal Processing, April 2003, 51(4): 906- 923.

[2] 刘彤, 裘正定. 数字水印相关检测的可靠性研究[J]. 电子学报, 2002, 30(5): 685- 688.

[3] LIU Tong, QIU Zheng-ding. The reliability analysis of correlation based digital watermarking detection[J]. Chinese Journal of Electronics. 2002, 30(5): 685- 688(in Chinese).

[4] 王新梅, 肖国镇. 纠错码- 原理与方法[M]. 西安: 西安电子科技大学出版社, 2001.

[5] WANG Xin-mei, XIAO Guo-zhen. Error Correction Code- Principles and Methods[M]. Xi' an: Xidian University Publishing House, 2001(in Chinese).

[6] 宋祖顺. 现代通信原理[M]. 北京: 电子工业出版社, 2001.
SONG Zu-shun. Modern Communication Principle[M]. Beijing: Electronic industry publishing house, 2001(in Chinese).

[7] P Loo, N Kingsbury. Watermark detection based on the properties of error control codes[J]. IEE Proc-Vis. Image Signal Process. April 2003, 150(2): 115- 122.

作者简介:

许文丽 女, 1970 年生于内蒙古牙克石市, 西安电子科技大学博士研究生, 主要从事密码学, 信息隐藏, 网络与信息安全方面的研究. E-mail: xwlqxz@ sohu. com, xwl778@ sohu. com.

王育民 男, 1936 年出生于北京, 博士生导师, 长期从事信息论, 差错控制, 编码, 密码学, 语音加密以及通信网的安全等方面的研究.