基于混沌冗余和阈值控制的联合算术码双向编译码快速算法

鄢懿，涂国防，张灿，高绍帅，陈德元
（中国科学院大学电子电气与通信工程学院，北京 101408）

摘 要：JPEG2000 是一种具有高效压缩性能的图像压缩标准，但抗差错能力和安全性不能满足实际应用要求。基于此，提出一种基于混沌冗余和阈值控制的联合算术码双向编译码快速算法，在编码端保留多个冗余符号，用混沌系统控制冗余符号的比例增强算术码编码的安全性；在译码端采用阈值控制和双向译码相结合，实现基于最大后验概率的联合快速译码。仿真结果表明，所提算法相对现有算法改善了重建图像质量，同时降低译码复杂度，具有良好的抗差错性和安全性。

关键词：加密抗差错算术码；混沌映射；阈值控制；双向译码；JPEG2000
中图分类号：TN911.2
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018029

Fast bidirectionally-decodable arithmetic coding with chaotic redundancy and threshold control

YAN Yi, TU Guofang, ZHANG Can, GAO Shaoshuai, CHEN Deyuan
School of Electronic, Electrical and Communication Engineering, University of Chinese Academy of Sciences, Beijing 101408, China

Abstract: Although the JPEG2000 compression standard has high coding efficiency, its error resistance and security can't meet the requirements of practical application. Based on this, a fast bidirectionally-decodable arithmetic coding method with chaotic redundancy and threshold control was proposed. At the encoder, the chaotic map controlled the probabilities of multiple redundant symbols to enhance the security of arithmetic coding. At the decoder, threshold control and bidirectional decoding were combined to realize fast decoding based on maximum a posteriori estimation. Simulation results show that the proposed method improves the reconstructed image quality with better error resistance and security.

Key words: secure error resistant arithmetic coding, chaotic map, threshold control, bidirectional decoding, JPEG2000

1 引言

JPEG2000 作为新一代静态图像压缩标准[1]，广泛应用于雷达遥感、多媒体、数据库、无线通信等领域。相比于 JPEG 标准，JPEG2000 具有高压缩性、渐进式传输、感兴趣区域编码以及码流的随机访问等优点。但由于使用了算术码[2]，JPEG2000 对误码非常敏感，在有噪信道中出现的单个误码会使整个码块被丢弃。

一种解决误码扩散的方法是采用抗差错算术码。Boyd 等[3]提出了一种在编码过程中添加单冗余符号的方法使算术码具有检错能力。Grangetto 等[4]在算术码的译码过程中采用序列估计，通过输入序列的软信息，并利用单冗余符号检错，实现最大后验概率译码。Bi 等[5]将算术码的译码过程表示为有限状态机模型，采用 Viterbi 软译码算法进行译码。Zezza 等[6]将单冗余符号算术码应用到 JPEG2000 中。这些抗差错算术码均在编码过程中

收稿日期：2017-01-10；**修回日期**：2018-01-19
通信作者：涂国防，gft@ucas.ac.cn
基金项目：国家自然科学基金资助项目（No.61571416, No.61271282）；中国科学院奖励基金资助项目（No.2017-06-17）
Foundation Items: The National Natural Science Foundation of China (No. 61571416, No.61271282), Award Foundation of Chinese Academy of Sciences (No.2017-06-17)

仅增加单冗余符号，译码端采用软判决译码，译码复杂度较高。

另一种解决错误扩散的方法是对数据块中的编码数据进行错误检测和掩盖。Gao 等[7]提出部分反向比特流方法，将码流分为 2 个部分，并将后半部分码流进行反转，使同步码在 2 个方向同步。Gao 等[8]提出双向可译变长数据块方法，对编码后得到的数据进行平移、反转和异或，使译码器能实现双向译码。但这 2 种方法都是针对视频数据进行处理，并不能直接用于 JPEG2000 的码流结构中。

由于数据的可访问性，传输数据容易遭到窃听，保障信息的安全性显得尤为重要。由于混沌理论具有良好的特性，近年来，混沌加密受到了研究者的广泛重视。Mi 等[9]将混沌与算术编码结合，通过 Logistic 映射和明文得到的密码流，控制算术编码过程中的区间位置，从而对明文进行加密。Wang 等[10]将混沌应用到 DNA 编码中，先用 PWLCM 生成一个密码图像，将明文图像和密码图像按 DNA 编码规则编码，用 Logistic 映射选择当前行/列的编码规则。

为了提高 JPEG2000 的抗差错性和安全性，本文提出一种基于混沌冗余和阈值控制的联合算术码双向编译码快速算法。该算法在算术码编码模型中保留多个冗余符号，用混沌系统控制冗余符号的比例，增强算术码编码的安全性；在译码端通过计算相应的阈值，采用阈值控制的软硬判决相结合方法进行快速译码降低译码复杂度；同时，针对算术码错误扩散的问题，采用双向译码的方法，提升算术码的纠错能力。仿真结果表明，所提算法在实现高效压缩的同时，具有良好的抗差错性和安全性。

2 基于加密抗差错和阈值控制的联合算术码双向编译码

本文提出的基于混沌冗余和阈值控制的联合算术码双向编译码快速算法框架如图 1 所示。原始图像预处理后进行离散小波变换，对产生的小波系数量化，按照二进制位分层的方法，从最高有效位平面到最低有效位平面依次进行算术编码，然后根据码率控制后组装成最终的压缩码流；压缩码流经有噪信道后拆分得到各个码块数据，进行算术译码和位平面译码，再反量化、离散小波反变换和后处理，得到重建图像。所提算法的主要工作在图 1 中虚线部分，包括以下 3 点。

1) 加密抗差错算术码：MQ 编码器中保留多个冗余符号，密钥通过混沌映射生成混沌序列，控制 MQ 编码器中冗余符号的比例，增强算术码的安全性。

2) 阈值控制的算术码译码：根据当前的信道条件和传输要求，通过计算相应的阈值，MQ 译码器采用阈值控制的软硬判决相结合方法进行快速译码，实现译码性能和复杂度的折中。

3) 双向编译码方法：位平面编码中，对位平面的每个条带独立编码，条带编码后得到的数据块进行平移、反转和异或，生成双向可译码流；译码时，先进行正向译码，当正向译码出现错误时，对码流进行反向译码，纠正译码错误，减少错误扩散。

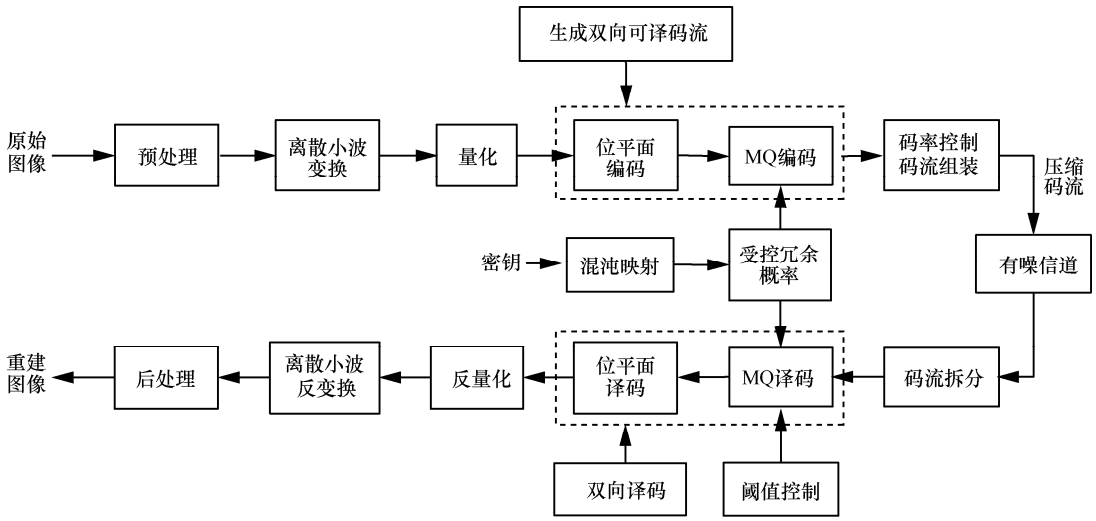


图 1 基于混沌冗余和阈值控制的联合算术码双向编译码快速算法框架

2.1　加密抗差错算术码

JPEG2000 中的 MQ 编码器是自适应的二进制算术编码，每次编码时将区间分割为大概率符号（MPS, most probable symbol）区间和小概率符号（LPS, least probable symbol）区间，概率分别为 $1-Q_e$ 和 Q_e。编码时设置 2 个专用寄存器 A 和 C，A 寄存器代表区间宽度，C 寄存器代表子区间的起始位置。

为了提高算术码的抗差错性能，在 MQ 编码器中添加 3 个受控冗余符号 μ_1、μ_2 和 μ_3，分别放在编码区间的最左端、2 个编码符号的中间和编码区间的最右端[11]，如图 2 所示。3 个冗余符号的概率分别为 Q_{f1}、Q_{f2} 和 Q_{f3}，概率之和为 Q_f。冗余符号在编码区间中所占用的区间总量是固定的，通过混沌映射生成密码流控制冗余符号的比例，实现安全性。采用二维 Logistic 混沌映射[12]来产生序列密钥，其动力学方程为

$$\begin{cases} x_{n+1}=\alpha_1 x_n(1-x_n)+\beta_1 y_n^2 \\ y_{n+1}=\alpha_2 y_n(1-y_n)+\beta_2(x_n^2+x_n y_n) \end{cases} \tag{1}$$

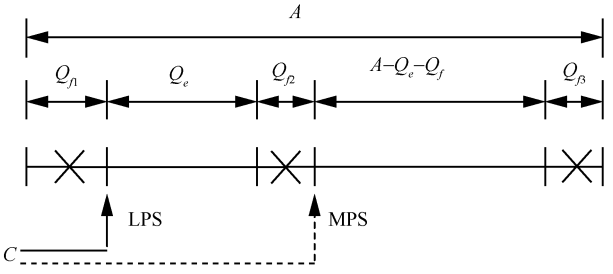


图 2　添加多个冗余符号的 MQ 编码器编码区间

当混沌参数满足 $2.75<\alpha_1\leqslant 3.4$、$2.7<\alpha_2\leqslant 3.45$、$0.15<\beta_1\leqslant 0.21$、$0.13<\beta_2\leqslant 0.15$ 时，处于混沌状态，得到的 $x_n, y_n\in(0,1)$。因此，可以通过以下方法设计基于混沌映射的加密抗差错算术码算法。

1) 初始化混沌映射的初值和参数。

2) 用二维 Logistic 混沌映射生成混沌序列 x_1^L 和 y_1^L。

3) 分配冗余符号概率：$Q_{f1}=Q_f\dfrac{x}{2}$，$Q_{f2}=Q_f\dfrac{y}{2}$，$Q_{f3}=Q_f-Q_{f1}-Q_{f2}$。

这样就可以得到 Q_{f1}、Q_{f2}、Q_{f3} 这 3 组受混沌控制的冗余符号概率。编码过程中，当输入信源符号是 LPS 时，$A=Q_e$，$C=C+Q_{f1}$；当输入信源符号是 MPS 时，$A=A-Q_e-Q_f$，$C=C+Q_e+Q_{f1}+Q_{f2}$。

2.2　阈值控制的算术码译码

假设信源序列 $\boldsymbol{u}=\{u_1,u_2,\cdots,u_L\}$ 经算术编码后得到码字序列 $\boldsymbol{b}=\{b_1,b_2,\cdots,b_N\}$，通过二进制相移键控（BPSK, binary phase shift keying）调制和加性高斯白噪声（AWGN, additive white Gaussian noise）信道得到的接收序列为 $\boldsymbol{r}=\{r_1,r_2,\cdots,r_N\}$。最大后验概率（MAP, maximum a posteriori）译码，即根据已知接收序列，通过寻找最大后验概率来进行译码[13]。根据贝叶斯定理，有

$$P(\boldsymbol{u}\mid\boldsymbol{r})=\frac{P(\boldsymbol{r}\mid\boldsymbol{u})P(\boldsymbol{u})}{P(\boldsymbol{r})}=\frac{P(\boldsymbol{r}\mid\boldsymbol{b})P(\boldsymbol{u})}{P(\boldsymbol{r})} \tag{2}$$

将式(2)取对数得到路径的度量，即

$$\begin{aligned} m&=\ln P(\boldsymbol{r}\mid\boldsymbol{b})+\ln P(\boldsymbol{u})-\ln P(\boldsymbol{r}) \\ &=\sum_{i=1}^{N}\left(\ln P(r_i\mid b_i)+\ln P(u_i)-\ln P(r_i)\right)=\sum_{i=1}^{N}m_i \end{aligned} \tag{3}$$

对于 AWGN 信道软判决输出，经推导，有

$$m_i=\begin{cases} \ln P(u_i)+\ln 2+\left(2\dfrac{E_\mathrm{b}}{\sigma^2}\dfrac{r_i}{\sqrt{E_\mathrm{b}}}\right)- \\ \ln\left[\exp\left(2\dfrac{E_\mathrm{b}}{\sigma^2}\dfrac{r_i}{\sqrt{E_\mathrm{b}}}\right)+1\right], b_i=1 \\ \ln P(u_i)+\ln 2-\ln\left[\exp\left(2\dfrac{E_\mathrm{b}}{\sigma^2}\dfrac{r_i}{\sqrt{E_\mathrm{b}}}\right)+1\right], b_i=0 \end{cases} \tag{4}$$

MQ 译码器是以字节为单位读取码字序列进行译码的，因此，在按照式(3)和式(4)进行 MAP 序列估计时，以字节为单位，每个状态可以伸展出 256 个分支。由于伸展的分支数较多，只能采用深度优先算法，本文选择堆栈算法作为搜索的算法[14]。在算法的每一步，只延伸最顶端路径的后续分支及相应的分支度量，然后，将这些新的分支路径与堆栈中的其他路径按度量大小进行排序，度量最大的路径放在堆栈最顶端，并去除度量较小的路径。如此不断重复，以最大度量为基准延伸路径。

增加译码时的留存路径数量，可以提升译码性能，但同时增加了译码复杂度。为了权衡译码性能和复杂度，本文提出一种通过阈值控制实现软硬判决相结合的方法。对于每个接收到的 r_i，用似然比来定义它的可靠度，在 AWGN 信道中，

可以写成

$$\Lambda_i = \ln \frac{P(b_i = 1 \mid r_i)}{P(b_i = 0 \mid r_i)} = \frac{2\sqrt{E_\mathrm{b}}}{\sigma^2} r_i \tag{5}$$

给定一个阈值 Γ，当 $\Lambda_i < -\Gamma$ 时，只延伸 $b_i = 0$ 的分支；当 $\Lambda_i > \Gamma$ 时，只延伸 $b_i = 1$ 的分支；当 $-\Gamma \leqslant \Lambda_i \leqslant \Gamma$ 时，延伸 $b_i = 0$ 和 $b_i = 1$ 的分支。因此，对于第 i 个比特，因阈值控制而错失正确路径的概率为

$$\begin{aligned} P_\mathrm{miss} &= P(\Lambda_i > \Gamma, b_i = 0) + P(\Lambda_i < -\Gamma, b_i = 1) \\ &= \frac{1}{2} P(\Lambda_i > \Gamma \mid b_i = 0) + \frac{1}{2} P(\Lambda_i < -\Gamma \mid b_i = 1) \end{aligned} \tag{6}$$

将式(5)代入式(6)，可得

$$\begin{aligned} P_\mathrm{miss} &= \frac{1}{2} P\left(r_i > \frac{\sigma^2}{2\sqrt{E_\mathrm{b}}} \Gamma \mid b_i = 0\right) + \\ &\quad \frac{1}{2} P\left(r_i < -\frac{\sigma^2}{2\sqrt{E_\mathrm{b}}} \Gamma \mid b_i = 1\right) \\ &= \frac{1}{2} \int_{\frac{\sigma^2}{2\sqrt{E_\mathrm{b}}}\Gamma}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(r_i + \sqrt{E_\mathrm{b}})^2}{2\sigma^2}\right] \mathrm{d}r_i + \\ &\quad \frac{1}{2} \int_{-\infty}^{-\frac{\sigma^2}{2\sqrt{E_\mathrm{b}}}\Gamma} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(r_i - \sqrt{E_\mathrm{b}})^2}{2\sigma^2}\right] \mathrm{d}r_i \\ &= \frac{1}{2} erfc\left[\sqrt{\frac{E_\mathrm{b}}{2\sigma^2}}\left(\frac{\sigma^2 \Gamma}{2E_\mathrm{b}} + 1\right)\right] \end{aligned} \tag{7}$$

其中，$erfc(z) = \dfrac{2}{\sqrt{\pi}} \int_z^{\infty} \mathrm{e}^{-\eta^2} \mathrm{d}\eta$。

也可将阈值 Γ 表示为

$$\Gamma = 4\sqrt{\frac{E_\mathrm{b}}{2\sigma^2}} erfc^{-1}(2P_\mathrm{miss}) - \frac{2E_\mathrm{b}}{\sigma^2} \tag{8}$$

增大 Γ，更多的路径被延伸了，译码性能得到了改善，但是增加了复杂度；减小 Γ，复杂度变小了，但是正确路径很可能被忽略了。因此，可以通过限制错失正确路径的概率 P_miss 合理控制阈值 Γ 的大小，实现译码性能和复杂度的折中。

2.3 基于 JPEG2000 标准的双向编译码方法

理论上来说，与其他译码算法一样，本文提出的阈值控制的算术码译码算法也可能译码失败。特别是当信道中出现突发差错时，由于累积度量变化较大，将正确路径删除的概率就很大。而对于 JPEG2000，译出码块中若发生错误，则整个码块将被丢弃，影响图像质量。

为了减少错误扩散问题，本文将文献[8]提出的双向编译码方法扩展到 JPEG2000 中，并对码流结构进行调整。在传统 JPEG2000 中，原始图像经离散小波变换和量化后的数据以码块为单位，按照二进制位分层的方法，从最高有效位平面到最低有效位平面进行 3 个通道扫描建模。每个位平面内，每 4 行数据组成 1 个条带，3 个通道编码时都从上到下依次扫描每个条带。本文提出条带独立的位平面编码，即在每个位平面中，同时对每个条带进行 3 通道扫描，实现多条带的并行编码，如图 3 所示。每个条带单独进行熵编码，令 $\boldsymbol{T}_n = t_n(1) \mid t_n(2) \mid \cdots \mid t_n(l_n)$ 表示第 n 个条带编码后得到的码流，$t_n(i)$ 为码流中的第 i 个比特，l_n 为码流长度。则整个位平面输出码流可以表示为

$$\begin{aligned} \boldsymbol{T} &= \boldsymbol{T}_1 \mid \boldsymbol{T}_2 \mid \cdots \mid \boldsymbol{T}_n \\ &= t_1(1) \mid t_1(2) \mid \cdots \mid t_1(l_1) \mid t_2(1) \mid \cdots \mid t_n(l_n) \end{aligned} \tag{9}$$

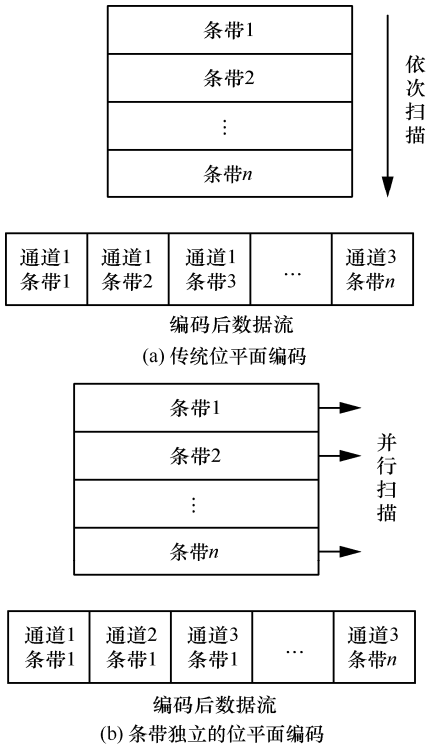


图 3 位平面编码中的扫描顺序

将单个条带码流进行反转，得到 $\boldsymbol{T}'_n = t_n(l_n) \mid t_n(l_n - 1) \mid \cdots \mid t_n(1)$，令条带反转码流串为 $\boldsymbol{T}' = \boldsymbol{T}'_1 \mid \boldsymbol{T}'_2 \mid \cdots \mid \boldsymbol{T}'_n$，如图 4 所示，生成双向可译码流为

$$\boldsymbol{D} = \left(\boldsymbol{T}_1 \mid \boldsymbol{T}_2 \mid \cdots \mid \boldsymbol{T}_n \mid \underbrace{0 \mid \cdots \mid 0}_{w\text{个}0}\right) \oplus \left(\underbrace{0 \mid \cdots \mid 0}_{w\text{个}0} \mid \boldsymbol{T}'_1 \mid \boldsymbol{T}'_2 \mid \cdots \mid \boldsymbol{T}'_n\right) \tag{10}$$

其中，w 为位平面中条带的最大码字长度。

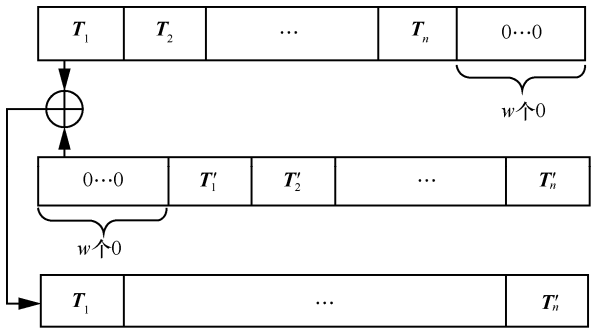


图 4　生成双向可译码流

通过双向编译码方法，压缩码流在译码端不但可以进行正向译码，当正向译码出现错误时，也可进行反向译码，实现码流的双向译码。

1) 正向译码

由式(10)可知，双向可译码流 $\boldsymbol{D}$ 是由条带码流与平移了 w bit 的条带反转码流串异或得到的。因此，译码时可以先读取接收码流的前 w bit，得到第一个条带的码流 $\boldsymbol{T}_1$。对 $\boldsymbol{T}_1$ 反转得到 $\boldsymbol{T}'_1$，平移 w bit，再与接收码流异或，就可以得到 $\boldsymbol{T}_2$。如此进行下去，就可以得到整个位平面的码流，如图 5 所示。

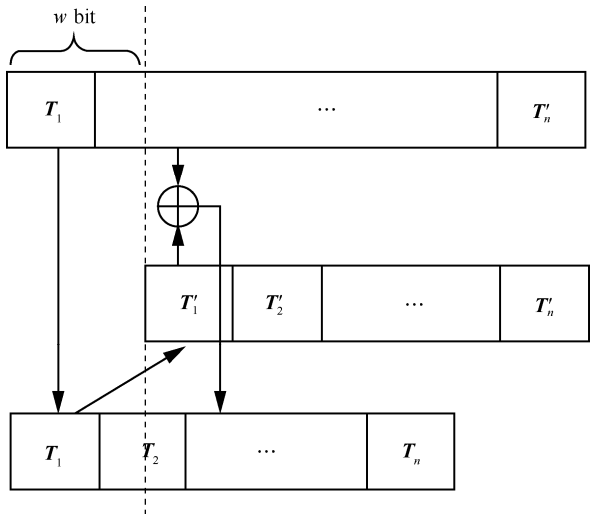


图 5　双向可译码流的正向译码

2) 反向译码

当正向译码出现错误时立即停止译码，转而进行反向译码。反向译码与正向译码类似，译码时先读取接收码流的后 w bit，得到最后一个条带的反转码流 $\boldsymbol{T}'_n$。对 $\boldsymbol{T}'_n$ 反转得到 $\boldsymbol{T}_n$，平移 w bit，再与接收码流异或，就可以得到 $\boldsymbol{T}'_{n-1}$。如此进行下去，就可以得到整个位平面的码流，如图 6 所示。

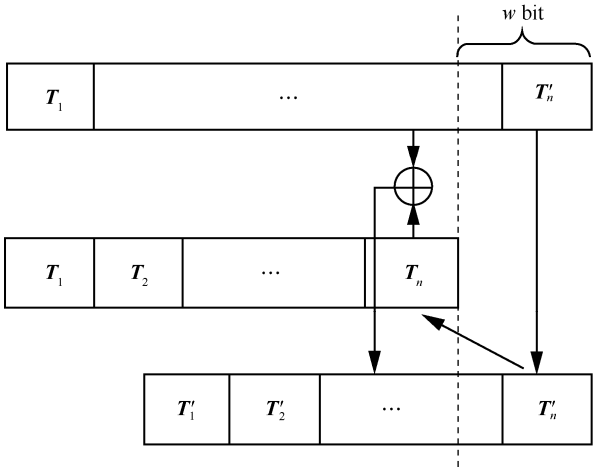


图 6　双向可译码流的反向译码

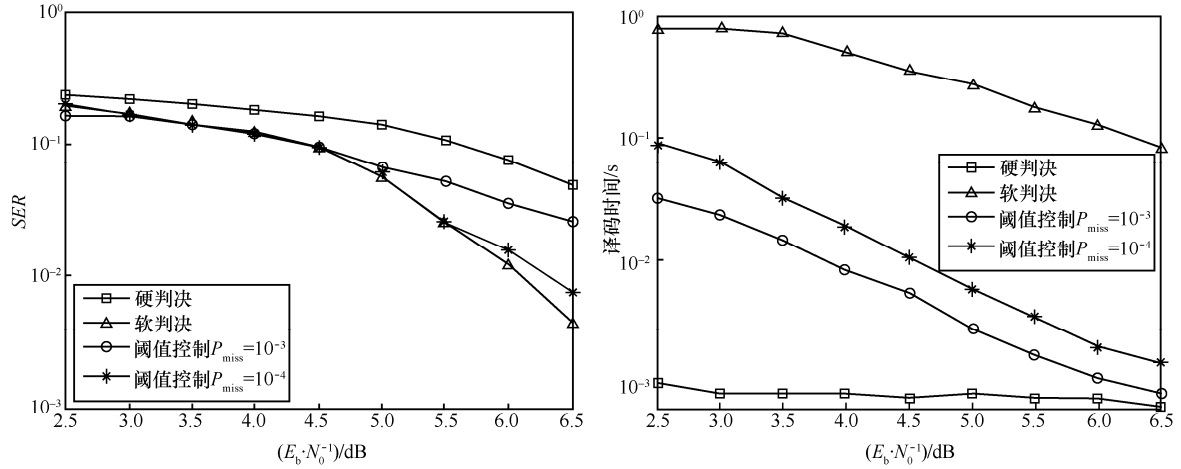
3　仿真实验与分析

为了验证本文算法的性能，分别对独立同分布信源序列和图像这 2 种信源形式进行实验。仿真过程中的信道模型是 AWGN 信道，算术码编码器是 MQ 编码器[1]，通过参考开放代码“openjpeg”编写仿真实验程序。仿真实验是在主频为 2.93 GHz 的 PC 上用 C 语言实现的。

3.1　离散无记忆信源

首先，测试算术码 MAP 序列译码时的阈值控制问题。实验所选信源序列为二进制独立同分布的伪随机序列，概率分布为(0.9, 0.1)，序列长度为 250 bit，堆栈容量为 32。测试在不考虑冗余符号情况下，MQ 译码器硬判决[1]、软判决[13]和采用阈值控制（软硬判决结合）的 MAP 译码性能，阈值控制选取了 $P_{\text{miss}}=10^{-3}$ 和 $P_{\text{miss}}=10^{-4}$ 这 2 种情况，测试结果均为 1 000 次测试得到的平均值。测试中用误符号率（SER, symbol error rate）表示译码性能，用译码时间表示复杂度。各算法在相同条件下译码性能和复杂度比较如图 7 所示。从图 7 可以看出，译码性能越好的算法，复杂度越高。在信噪比为 5.0 dB 时，阈值控制 $P_{\text{miss}}=10^{-3}$ 和 $P_{\text{miss}}=10^{-4}$ 的译码性能较软判决分别有 18%和 4%的损失，而复杂度降低了 98.9%和 97.7%。采用阈值控制的方法，仅需牺牲较少的译码性能，却能大幅度减小译码复杂度。在实际译码时，译码器可以根据当前的信道条件和传输要求，通过式(8)计算出相应的阈值，实现译码性能和复杂度的最佳平衡。

为了分析和比较不同编译码器的编译码性能，将本文算法与传统 MQ 编译码器[1]和单冗余符号算



(a) 译码性能比较　　(b) 复杂度比较

图 7　各算法在相同条件下译码性能和复杂度比较

法[6]进行比较，如图 8 所示，测试中加入了不同比例的冗余符号。从图 8 可以看出，采用冗余符号可以提高译码性能，且随着冗余符号比例增大，误符号率降低。在相同的条件下，本文算法相对于单冗余符号算法在译码性能上有显著改进：在 $SER=10^{-1}$、Q_f=0.03 时，本文算法取得 0.3 dB 增益；在 SER=10^{-3}、Q_f=0.1 时，本文算法取得 0.35 dB 增益。

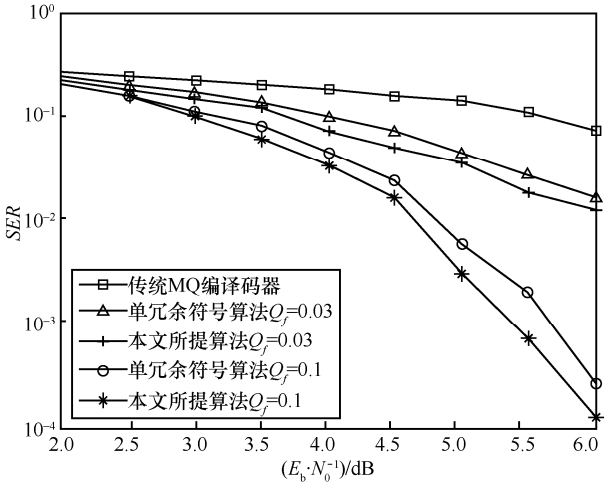


图 8　各算法在不同冗余符号下误符号率比较

3.2　存在误码的图像译码

为了测试算法的实际应用能力，本文对存在误码的图像进行仿真实验。假设误码只出现在算术码编码的图像信息中，其他重要边信息假设无误码。这里使用标准 512×512 像素的 peppers 和 couple 灰度图像进行测试，整个图像作为一个变换块，经过 5 级二维离散小波变换，码块大小为 32×32，码率为 1 比特/像素，测试信道为 AWGN 信道，冗余符号概率取 Q_f=0.03，采用峰值信噪比（PSNR, peak signal-to-noise ratio）作为衡量图像传输质量的指标。实验比较对象为传统 JPEG2000[1]、单冗余符号 JPEG2000[6]以及文献[8]算法应用到 JPEG2000 得到的双向编译码 JPEG2000，仿真结果如表 1 所示，测试结果均为 100 次测试得到的平均值。从表 1 可以看出，本文所提算法相对于对比算法在图像复原性能上有显著改进。这是由于本文算法采用多个冗余符号的算术码编码模型，同时最大限度利用正确接收的信息进行双向译码，减少了错误扩散，增强了抗差错能力，本文算法相较对比算法优势突出。

3.3　安全性

为了评估算法的安全性，分别对算法的密钥敏感性、密钥空间、抗差分攻击、统计特性方面以及加密时间和密文尺寸等性能进行分析。实验选取混沌参数为 α_1=3、α_2=3、β_1=0.17、β_2=0.14，混沌初值为 $x_0=0.1$、$y_0=0.15$。

1) 密钥敏感性

为了测试每个密钥的敏感性，在仅改变一个密钥而其他密钥不变的条件下分析密文的变化率。当混沌参数 α_1、α_2、β_1、β_2 变动 10^{-15} 时，密文变化率分别为 49.7%、50.5%、50.2%和 50.4%；当混沌初值 x_0、y_0 变动 10^{-15} 时，密文变化率分别为 50.2%

表 1　　**各算法在不同信噪比下 *PSNR* 比较**

图像	信噪比/dB	*PSNR*/dB			
		传统 JPEG2000	单冗余符号 JPEG2000	双向编译码 JPEG2000	本文算法
peppers	5	12.29	15.86	15.51	18.00
	6	14.73	18.03	18.95	23.47
	7	19.58	22.67	24.35	29.07
	8	26.85	29.75	30.23	31.92
couple	5	13.67	17.77	17.59	20.10
	6	16.06	20.22	20.62	24.72
	7	20.17	23.97	25.15	28.50
	8	26.72	29.44	29.05	30.33

和 49.5%。可见，密文变化率均在 50%左右，本文算法密文对密钥具有高度敏感性。

2) 密钥空间

二维 Logistic 混沌映射的初值由双精度浮点数表示，精度为10^{-15}，范围是$0<x_0<1$和$0<y_0<1$；混沌参数由双精度浮点数表示，精度为10^{-15}，范围是 $2.75<\alpha_1\leqslant 3.4$ 、 $2.7<\alpha_2\leqslant 3.45$ 、 $0.15<\beta_1\leqslant 0.21$ 和 $0.13<\beta_2\leqslant 0.15$ 。因此，密钥空间大小为5.85×10^{78}，足以抵抗蛮力攻击。

3) 抗差分攻击

像素数变化率（NPCR, number of changing pixel rate）和归一化平均变化强度（UACI, unified averaged changed intensity）是衡量图像加密算法抵抗差分攻击的重要指标，分别表示随机改变原始图像的某个像素值后，加密图像像素值发生改变的数目所占的比例以及变化程度[15]。当 2 个明文图像仅存在一个像素不同时，设它们的密文图像中第(i,j)点的像素值分别为$C_1(i,j)$和$C_2(i,j)$。若$C_1(i,j)$=$C_2(i,j)$，定义$E(i,j)$=0；若$C_1(i,j)\neq C_2(i,j)$，定义$E(i,j)$=1。则 *NPCR* 和 *UACI* 计算式为

$$NPCR=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}E(i,j)\times 100\% \tag{11}$$

$$UACI=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\times 100\% \tag{12}$$

其中，M 和 N 分别是图像像素的行数和列数。对于 8 位灰度图像，*NPCR* 与 *UACI* 的理想值分别为 99.609 4%和 33.46%。本文实验中，选取 100 组 peppers 图像进行加密，每组 2 个图像且仅有一个像素值不同，计算得到 *NPCR* 和 *UACI* 的平均值分别为 99.586 1%和 32.79%，与理想值非常接近。因此，本文算法可以有效抵抗差分攻击。

4) 统计特性

图 9 分别给出了 peppers 图像的原始图像和加密图像所对应的像素值分布直方图。由图 9(a)可知，原始图像的像素值分布是不均匀的；而图 9(b)~图 9(d)表明，文献[9]、文献[10]以及本文算法加密图像的像素值均呈现出平坦而均匀的分布特性，即加密图像的像素值在[0,255]范围内的取值概率均等，明文图像的统计特性被打破[16]。这体现出本文算法的扩散和混淆特性较好，能有效防止统计攻击，具有不弱于现有加密算法的加密强度。

5) 加密时间和密文尺寸

对 peppers 图像采用文献[9]、文献[10]以及本文算法进行加密，并对比加密时间和密文尺寸，结果如表 2 所示。从表 2 可以看出，本文算法的密文尺寸远小于另 2 种算法，这是由于编码过程中不仅对明文进行加密，还进行压缩处理。同时，本文算法加密时所消耗的时间最少，也表明本文算法更适用于实际应用。

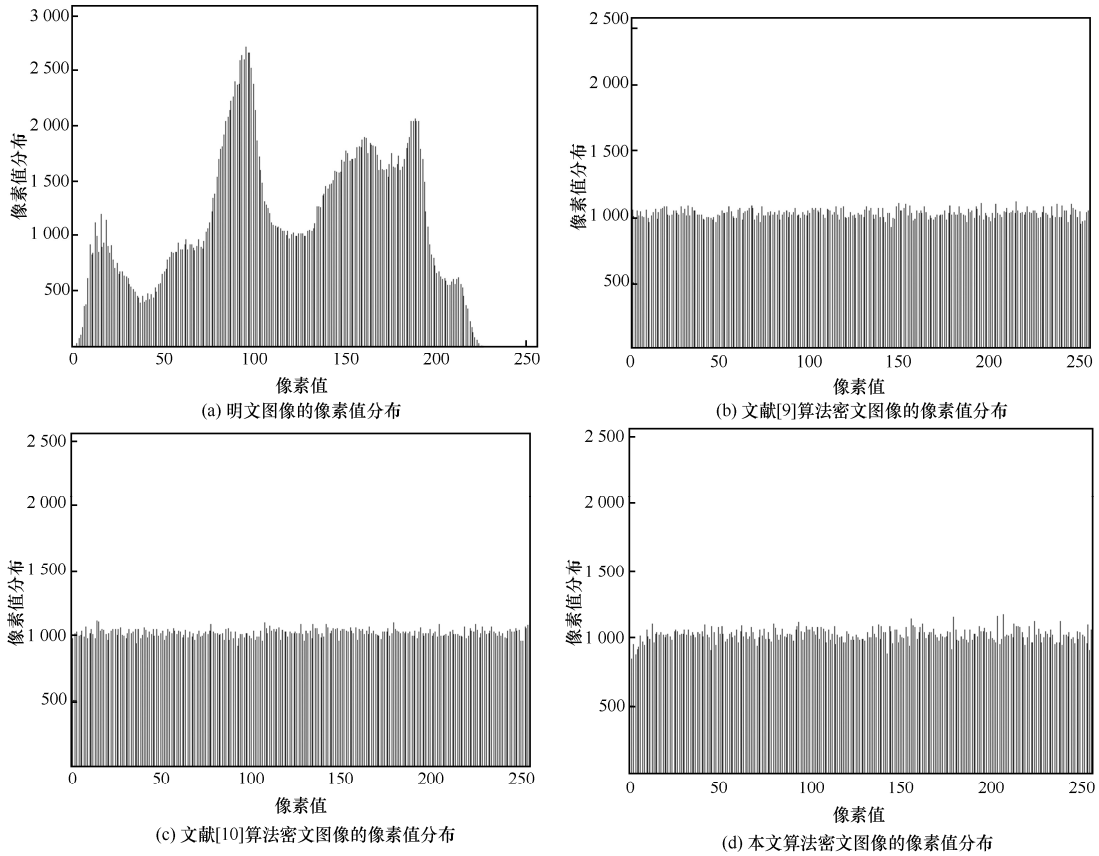


图 9　peppers 图像的直方图

表 2　　各算法的加密时间和密文尺寸比较

算法	加密时间/s	密文尺寸/KB
文献[9]算法	1.549	256.96
文献[10]算法	83.019	257.05
本文算法	0.953	31.93

4　结束语

本文提出一种基于混沌冗余和阈值控制的 JPEG2000 联合算术码双向编译码快速算法，编码时，在算术码编码模型中保留多个冗余符号，用混沌系统控制冗余符号的比例增强算术码编码的安全性；译码时，采用阈值控制和双向译码相结合，实现了基于最大后验概率的快速译码。仿真结果表明，所提算法降低了译码复杂度，提高了传输图像质量，具有良好的抗差错性和安全性。

参考文献：

[1] ISO/IEC 15444-1. Information technology-JPEG2000 image coding system-part 1: core coding system[S]. 2000.

[2] SHANNON C E. A mathematical theory of communication[J]. Bell System Technical Journal, 1948, 27(3): 379-423.

[3] BOYD C, CLEARY J, IRVINE S, et al. Integrating error detection into arithmetic coding[J]. IEEE Transactions on Communications, 1997, 45(1): 1-3.

[4] GRANGETTO M, MAGLI E, OLMO G. Joint source/channel coding and MAP decoding of arithmetic codes[J]. IEEE Transactions on Communications, 2005, 53(6): 1007-1016.

[5] BI D S, HOFFMAN M W, SAYOOD K. State machine interpretation of arithmetic codes for joint source and channel coding[C]//Data Compression Conference. 2006: 143-152.

[6] ZEZZA S, MASERA G, NOOSHABADI S. A novel decoder architecture for error resilient JPEG2000 applications based on MQ arithmetic[C]//2014 IEEE International Symposium on Circuits and Systems, Melbourne. 2014: 902-905.

[7] GAO S S, TU G F. Robust H.263+ video transmission using partial backward decodable bit stream(PBDBS)[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(2): 182-187.

[8] GAO S S, MA K K. Error-resilient H.264/AVC video transmission using two-way decodable variable length data block[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2010, 20(3): 340-350.

[9] MI B, LIAO X F, CHEN Y. A novel chaotic encryption scheme based on arithmetic coding[J]. Chaos Solitons and Fractals, 2008, 38(5): 1523-1531.

[10] WANG X Y, LIU C M. A novel and effective image encryption algo-

rithm based on chaos and DNA encoding[J]. Multimedia Tools and Applications, 2016, 2016(2):1-17.

[11] 鄢懿, 张灿, 郭振永, 等. 基于混沌密钥控制的联合信源信道与安全算术码编译码算法[J]. 电子与信息学报, 2016, 38(10): 2553-2559.
YAN Y, ZHANG C, GUO Z Y, et al. Joint source channel and security arithmetic coding controlled by chaotic keys[J]. Journal of Electronics & Information Technology, 2016, 38(10): 2553-2559.

[12] ELABADY N F, MOUSSA M I, SABBEH S F. Improving the security of image encryption by using two chaotic maps[J]. International Journal of Computer Applications, 2014, 108(19): 27-32.

[13] SPITERI T, BUTTIGIEG V. Maximum a posteriori decoding of arithmetic codes in joint source-channel coding[J]. Communication in Computer and Information Science, 2012, 222(39): 363-377.

[14] LIN Q Z, WONG K W, LI M, et al. An effective error correction scheme for arithmetic coding[J]. Mathematical Problems in Engineering, 2015(2): 1-10.

[15] BRINDHA M, GOUNDEN N A. A chaos based image encryption and lossless compression algorithm using hash table and Chinese remainder theorem[J]. Applied Soft Computing, 2016, 40(1):379-390.

[16] 邓晓衡, 廖春龙, 朱从旭, 等. 像素位置与比特双重置乱的图像混沌加密算法[J]. 通信学报, 2014, 35(3): 216-223.
DENG X H, LIAO C L, ZHU C X, et al. Image encryption algorithms based on chaos through dual scrambling of pixel position an bit[J]. Journal on Communications, 2014, 35(3): 216-223.

[作者简介]

鄢懿（1990-），女，江西景德镇人，中国科学院大学博士生，主要研究方向为联合信源信道与安全编译码。

涂国防（1954-），男，湖南长沙人，中国科学院大学教授、博士生导师，主要研究方向为联合信源信道编译码、无线通信、图像编码、信息安全和信号处理。

张灿（1954-），女，湖南长沙人，中国科学院大学教授、博士生导师，主要研究方向为移动无线通信、无线网络安全和信号处理。

高绍帅（1976-），男，山东德州人，博士，中国科学院大学教授、博士生导师，主要研究方向为无线通信、视频处理。

陈德元（1968-），男，贵州毕节人，博士，中国科学院大学副教授，主要研究方向为信道编码、联合信源信道编码。