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

鄢 懿[①] 张 灿[*①] 郭振永[①②] 高绍帅[①] 陈德元[①]
[①](中国科学院大学电子电气与通信工程学院 北京 101408)
[②](中国科学院电子学研究所 北京 100190)

摘 要：该文针对深空通信、移动通信等资源受限网络中的信息有效性、可靠性和安全性传输，提出一种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。该算法在编码端通过混沌映射 1 控制在算术码内嵌入多个禁用符号，将信道编码检错与密码流的扰乱相结合；同时，通过混沌映射 2 控制信源符号的算术编码，将信源编码与信息安全相结合，实现了联合信源信道与信息安全编译码。实验结果表明，该算法与现有的同类算法相比，当误包率为 10^{-3} 时，改善编译码性能 0.4 dB，同时增强了可靠性和安全性。

关键词：联合信源信道与安全编译码；算术码；禁用符号；混沌映射
中图分类号：TN911.2 **文献标识码**：A **文章编号**：1009-5896(2016)10-2553-07
DOI: 10.11999/JEIT151429

Joint Source Channel and Security Arithmetic Coding Controlled by Chaotic Keys

YAN Yi[①] ZHANG Can[①] GUO Zhenyong[①②] GAO Shaoshuai[①] CHEN Deyuan[①]
[①](*School of Electronic, Electrical and Communication Engineering, University of Chinese Academy of Sciences, Beijing* 101408, *China*)
[②](*Institute of Electronics, Chinese Academy of Sciences, Beijing* 100190, *China*)

Abstract: In order to transfer effective, reliable and secure information in resource-constrained networks such as deep space communications and mobile communications, a joint source channel security arithmetic coding method controlled by chaotic keys is proposed. At encoding, the first chaotic map allocates the probability of multiple forbidden symbols in arithmetic code, combining error detection by channel coding and disorder of key streams; meanwhile, the second chaotic map controls the source symbols in arithmetic code, combining source coding and information security. Simulation results show that the proposed method can not only achieve 0.4 dB signal-to-noise ratio gains compared with the existing similar arithmetic codes under the condition of same error rate, but also be of high reliability and security.

Key words: Joint source channel and security encoding/decoding; Arithmetic coding; Forbidden symbols; Chaotic map

1 引言

传统的无线通信系统大都是依据香农的分离理论进行设计，将信源编码、信道编码和信息安全 3 环节分别进行。其优点是设计简单、通用性好，可以分别形成标准和算法。分离算法没有充分利用各自的先验信息、冗余信息和信道的状态信息，难以逼近信道容量的最优性能。另外，在深空通信、移动通信等资源受限网络中，难以满足分离理论的假设前提[1]。因此，将信源编码、信道编码和信息安全相结合的联合编译方法是一个具有挑战性的研究课题。

算术码是一种具有高效压缩性能的熵编码，已被越来越多的图像(JPEG2000)和视频(H.264/AVC)压缩国际标准所采纳。算术码是一种无失真的编码方法，能有效地压缩信息冗余度，但对信道的误码非常敏感。如何使算术码具有更好的抗信道误码能力也就成为一个研究的重点。文献[2]提出在算术编码中添加冗余信息，使算术码解码器能够利用冗余信息进行检错。文献[3,4]在解码端利用禁用符号带来的受控冗余信息对编码序列进行序列译码。文献[5]提出适用于 H.264 中算术码的改进 MAP 序列估

收稿日期：2015-12-17；改回日期：2016-05-05；网络出版：2016-07-04
*通信作者：张灿 czhang@ucas.ac.cn
基金项目：国家自然科学基金(61571416, 61271282, 61032006)
Foundation Items: The National Natural Science Foundation of China (61571416, 61271282, 61032006)

计。文献[6]在译码端提出快速检错方法。文献[2-4]使用添加禁用符号的联合信源信道编码算法，禁用符号的位置都是确定的，而确定位置的单个禁用符号很难纠正错误码流中的比特反转[7]。

为了使算术码具有安全性，文献[8]引入一个二元随机序列，用来控制信源符号在概率模型中的顺序，扰乱了编码区间，提出了随机算术编码算法。文献[9]将混沌理论应用到算术编码中，利用一个混沌系统产生的混沌密钥流，改变概率模型。文献[10]采用 SMS4 分组密钥控制随机算术编码的区间选择，将图像数据的压缩与安全相结合。

综上所述，文献[2-7]都是采用添加禁用符号，提出了联合信源信道编译码算法；文献[8-10]采用密钥控制算术编码的区间选择，开发了联合信源与安全编译码算法。本文将算术编码的压缩和信道编码的检错与压缩数据流的扰乱相结合，提出了一种新的基于混沌密钥控制的联合信源信道与安全算术编译码算法。在误包率为 10^{-3} 时，该算法改善编译码性能 0.4 dB，并保障了信息传输的可靠性和安全性。

2 算术编码及混沌映射

假设 A 表示一个有限符号集 $\{a_1,a_2,\cdots,a_q\}$ 构成的离散信源，$\boldsymbol{s}=\{s_1,s_2,\cdots,s_L\}$ 是信源 A 产生的由 L 个信源符号组成的随机序列。假定信源是独立同分布的，其概率分布为 $P_i=P(a_i)$。

传统算术编码是根据信源符号序列出现的概率，将 $[0,1)$ 这一基准区间，划分为互不重叠的子区间，每一个子区间的宽度等于各符号序列的概率。这样不同的符号序列将与各子区间一一对应，每个子区间内的任意一个实数都可以用来表示相应的符号序列。如果将该实数用一个二进制数表示，那么这个二进制数值就是这个信源输出序列所对应的码字[11]。

算术码的高压缩性能同时也意味着压缩序列中的冗余信息非常少，即使压缩序列仅有一个误码也会造成无限的误码扩散，因此利用算术码的残存冗余进行检错译码就变得非常困难。要提高算术码的抗差错性能，就需要增加受控的冗余信息[12]。在算术编码器中引入了一个禁用符号 μ 的受控冗余信息，该禁用符号在信源符号的概率模型中占有固定的概率 $P(\mu)$，编码模型如图 1 所示(两个信源符号情况)。该禁用符号在实际码流中是不会出现的，而一旦解码器解出了禁用符号，则检测到码流中出现了错误。

由于每次编码时都在当前区间中保留一定比例禁用空间，其他信源符号的概率相应缩小 $(1-P(\mu))$ 倍，加入禁用区间后压缩每信源符号增加的冗余信息量为 $-\log_2(1-P(\mu))$ bit/symbol。因此平均码长变为 $H-\log_2[1-P(\mu)]$，此时纠错算术码的相对信道码率为 $R=H/(H-\log_2(1-P(\mu)))$，码率的大小取决于信源熵 H 和禁用符号的概率 $P(\mu)$。在熵固定的情况下，可以通过改变 $P(\mu)$ 的大小，灵活调整码率。在这类方法中，可以灵活选择受控冗余的位置，也可以增加多个受控禁用符号在不同的位置。

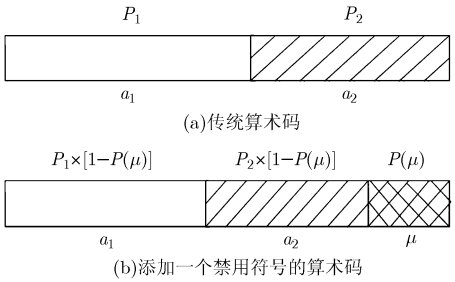

图 1 算术码编码模型

混沌是一种特殊的动力学系统，由于非周期、不收敛且对初始值和外部参数敏感的特性，使得混沌广泛用于加密领域中。典型的混沌映射有 Logistic 映射，Henon 映射，Cubic 映射，Sine 映射，Tent 映射，Chebyshev 映射等，通过对比生成混沌序列的伪随机性和稳定性[13]，在安全性与计算复杂度折衷的条件下，本文选择 Chebyshev 映射对算法进行加密。Chebyshev 映射定义分别为

$$x_{n+1}=\cos(\lambda\cdot\cos^{-1}x_n),\quad x_n\in[-1,1] \tag{1}$$

当参数 $\lambda\geq 2$ 且为整数时，Chebyshev 映射处于混沌状态。Chebyshev 映射很容易实现，可以提供数量众多、非相关、类随机而又确定的序列，初值和参数的敏感性高。对于不同的初值和参数，Chebyshev 映射可以生成完全不相关的混沌序列。

3 联合信源信道与安全算术码编码

为了实现在资源受限网络中信息有效性、可靠性和安全性传输，本文在编码端通过 Chebyshev 映射 1 控制多个禁用符号，将禁用符号与乱序相结合；同时，通过 Chebyshev 映射 2 控制算术编码位置，提出并设计了一种基于混沌映射控制的联合信源信道与安全算术码编译码算法(如图 2 所示)，具体步骤如下：

(1)将信源数据输入到添加了多个受控禁用符号的算术编码器中，进行联合信源信道与安全编码：

(a)Chebyshev 映射 1 的初值和参数构成密钥 1，密钥 1 通过混沌映射生成密码流 1，用来控制多个禁用符号的比例；

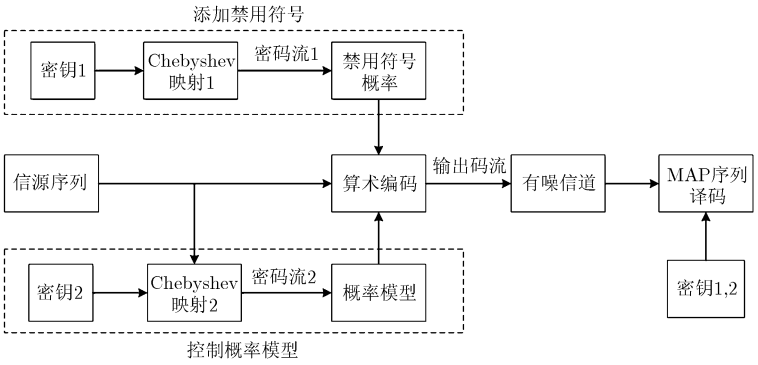

图 2　联合信源信道与安全算术码的编译码框图

(b)Chebyshev 映射 2 的初值和参数构成密钥 2，密钥 2 与信源序列通过混沌映射生成密码流 2，用来控制信源符号的概率模型；

(2)算术码编码器输出码流经过有噪信道，接收端根据两个混沌密钥得到禁用符号比例和概率模型，基于最大后验概率(MAP)准则进行译码。

有噪信道对接收序列造成误码后，会随着解密过程而在明文中发生扩散，从而造成更多的误码，降低了纠错性能；同时，信道误码会增大系统攻击者的攻击难度，从而会增强安全性。对于纠错性能与安全性能的矛盾关系，编码器根据当前的信道条件和传输要求，采用密钥熵不变，明文仅增加概率很小的禁用符号的方法，在纠错性与安全性上进行折衷，实现联合信源信道与安全编码。

3.1 添加禁用符号

对一个信源字母表大小为 q 的算术编码器，引入 $q+1$ 个禁用符号 $\mu_0,\mu_1,\cdots,\mu_q$，对应的概率为 $P(\mu_0),P(\mu_1),\cdots,P(\mu_q)$。所有的信源符号都被禁用符号间隔开来，禁用符号和信源符号交替出现[14]，图 3 所示为两个信源符号情况。

禁用符号在编码区间中所占用的区间总量概率是固定的，则满足

$$P(\mu_0)+P(\mu_1)+\cdots+P(\mu_q)=P(\mu),\quad P(\mu_i)\ge 0 \tag{2}$$

本文通过混沌映射生成密码流控制禁用符号的比例，提高算术编码安全性。利用 Chebyshev 映射生成编码每次迭代时禁用符号 μ_q 的概率 $P(\mu_q)$ 为

$$P\left(\mu_q^n\right)=P(\mu)\cdot|x_n|=P(\mu)\cdot\left|\cos\left(\lambda\cdot\cos^{-1}x_{n-1}\right)\right| \tag{3}$$

其中，$P(\mu_q^n)$ 代表输入第 n 个符号时禁用符号 μ_q 的概率。为了简化计算，将剩余的禁用符号概率 $P(\mu_0^n),P(\mu_1^n),\cdots,P(\mu_{q-1}^n)$ 进行等概率分配，即

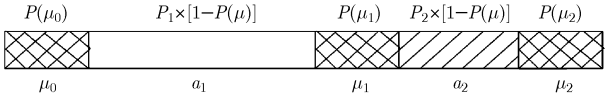

图 3　添加多个禁用符号的算术码模型

$$P\left(\mu_0^n\right)=P\left(\mu_1^n\right)=\cdots=P\left(\mu_{q-1}^n\right)=\frac{1}{q}\left[P(\mu)-P\left(\mu_q^n\right)\right] \tag{4}$$

3.2 安全算术编码的控制概率模型机制

由于禁用符号的总概率比较小，如果仅用密钥控制禁用符号的比例，容易受到窃听者的攻击。本文利用随机算术编码，通过 Chebyshev 映射产生一组密码流来控制编码符号的位置，提升算法的安全性。但无论加密算法多复杂，独立于明文的密码流都容易受到已知明文攻击[9]。为了加强安全性，在产生随机密码流的时候必须将明文考虑进去。设计方法如下：

(1)初始化 Chebyshev 映射 2 的初值和参数，将映射迭代 N_0 次(本文取 $N_0=100$)，得到用于加密的初始状态 y_0；

(2)将混沌映射轨迹中的元素 y_n 表示成二进制形式：

$$|y_n|=0.c_1(y_n)c_2(y_n)\cdots c_P(y_n),\quad c_i(y_n)\in\{0,1\} \tag{5}$$

其中，P 为精度；

(3)提取式(5)中的 3 个比特位 $c_{j-1}(y_n)$，$c_j(y_n)$ 和 $c_{j+1}(y_n)$，其中 $j=\left\lfloor\frac{3}{4}P\right\rfloor$。进行如下操作以获得一个二进制位：

$$k_n=\begin{cases}c_{j-1}(y_n)\oplus c_j(y_n)\oplus c_{j+1}(y_n), & n=0\\ c_{j-1}(y_n)\oplus c_j(y_n)\oplus c_{j+1}(y_n)\oplus s_{n-1}, & n\ne 0\end{cases} \tag{6}$$

其中，s_{n-1} 表示输入信源序列中的第 $n-1$ 个符号；

(4)得到伪随机数 k_n，若 $k_n=0$，算术编码概率模型中，信源符号按 $a_1,a_2,\cdots,a_q$ 顺序排列；若 $k_n=1$，算术编码概率模型中，信源符号按 $a_q,a_{q-1},\cdots,a_1$ 顺序排列(如图 4 所示)；

(5)将 k_n 替代原来的 $c_j(y_n)$ 得到新的 y_n'，继续后续的混沌迭代生成 y_{n+1}。转到步骤(2)，直到所有信源符号输入结束，得到最后的编码输出。

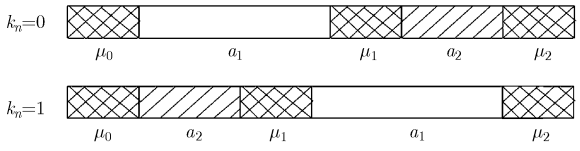

图 4 密钥控制下的概率模型

4 联合信源信道与安全算术码译码

联合信源信道与安全算术编码的码字序列 $\boldsymbol{b}=\{b_1,b_2,\cdots,b_N\}$，$N$ 为输出可变长码序列的长度。$\boldsymbol{b}$ 经 BPSK 调制通过具有噪声的离散信道，解调得到的接收序列为 $\boldsymbol{r}=\{r_1,r_2,\cdots,r_N\}$。基于最大后验概率准则的译码就是根据信道的输出序列 $\boldsymbol{r}$ 估计出一个合法的码字序列 $\boldsymbol{b}$，使得后验概率 $P(\boldsymbol{b}\mid\boldsymbol{r})$ 最大，即

$$\hat{\boldsymbol{b}}=\arg\max_{\boldsymbol{b}\in\{0,1\}^N}P(\boldsymbol{b}\mid\boldsymbol{r})=\arg\max_{\boldsymbol{b}\in\{0,1\}^N}\frac{P(\boldsymbol{r}\mid\boldsymbol{b})P(\boldsymbol{b})}{P(\boldsymbol{r})} \tag{7}$$

对式(7)取自然对数，得到具有比特深度 i 的解码度量。

$$m_i=\ln P\left(b_1^i\mid r_1^i\right)=\ln P\left(r_1^i\mid b_1^i\right)+\ln P(b_1^i)-\ln P\left(r_1^i\right) \tag{8}$$

可以将解码度量看成一个 1 阶的马尔可夫模型，如式(9)所示：

$$\left.\begin{aligned}&m_0=0\\&m_i=m_{i-1}+\ln P\left(r_i\mid b_i\right)+\ln P(b_i)-\ln P(r_i)\end{aligned}\right\} \tag{9}$$

$\boldsymbol{s}$ 是算术编码的输入序列，其对应的编码输出序列为 $\boldsymbol{b}$，二者为规定的算术编码关系，即 $P(\boldsymbol{b})=P(\boldsymbol{s})$。令编码码字 $\boldsymbol{b}$ 的第 i 个比特所对应的信息序列为 $\boldsymbol{s}_i=(s_{i,1},s_{i,2},\cdots,s_{i,J_i})$，则有

$$\ln P(b_i)=\ln P\left(\boldsymbol{s}_i\right)=\sum_{j=1}^{J_i}\ln P\left(s_{i,j}\right) \tag{10}$$

假设 AWGN 信道中的高斯白噪声采样 n_i 的均值为 0，方差为 σ^2，经 BPSK 调制后的信号电平为 $\sqrt{E_b}(2b_i-1)$，则解码器的输入为 $r_i=\sqrt{E_b}(2b_i-1)+n_i$，$i=1,2,\cdots,N$。对于 AWGN 信道软判决输出，经推导有

$$m_i=m_{i-1}+\frac{2r_ib_i\sqrt{E_b}}{\sigma^2}-\ln\left[1+\exp\left(\frac{2r_i\sqrt{E_b}}{\sigma^2}\right)\right]-J_i\ln[1-P(\mu)] \tag{11}$$

实际解码时，按照最大后验概率准则进行序列估计，留存路径的数目将会随着解码深度的增加成指数增长，限于存储能力和解码延时，难以实时实现。本文采用基于广度优先的 MA 序列译码[4]，在迭代的每一步，所有存储的分支路径都向前扩展一个比特，当检测到差错时，该分支路径被剪除掉。相反地，只要分支路径比特流是正确的，更新相应的分支度量，将这些新的分支路径按度量大小进行排序，根据计算出的度量结果仅保留 M 条路径进行后续延伸(本文选 M=256)。当译完最后一个比特时，选择当前路径中度量最大的路径作为译码结果。

译码时，密钥信息通过安全信道传给接收端，而数据码流通过不安全信道进行传输。在进行 MAP 译码之前，由密钥信息生成相应的混沌序列，得到密码流，从而在译码过程中得到正确的信息。窃取者在没有密钥信息的情况下，是无法正确译出传输信息的。

5 仿真实验与分析

仿真实验是在主频为 2.93 GHz 的个人计算机上用 C 语言仿真实验实现的。为了便于比较，与文献[4]的算法所用信源相同，即信源为 Girl256×256 的 8 bit 灰度图像，其中的像素采用 JPEG 无损编码系统的预测编码方案，预测误差用一个 9 bit 的符号表示。每 256 个预测误差为一个传输包，也就是一个联合编码单元，则每个编码单元的比特数为 2304，再加上一个终止符号，总共为 2305 个输入符号构成原始信源序列。两个信源符号概率分别为 0.866 和 0.134，终止符号概率为 $P(\omega)=10^{-5}$。

5.1 纠错性能

为了分析和比较不同编译码器的编译码性能，本算法与文献[4]，文献[6]算法和分离编码算法(先经过传统算术编码进行信源压缩，然后 AES 加密[15]，最后利用码率兼容的截短卷积码进行信道保护[16])进行比较。$P(\mu)$=0.05 时的仿真结果如图 5 所示，图中可以看出，在相同的条件下，本文算法相对于其他的联合算法以及分离算法在译码性能上有显著改进。在误包率为 10^{-1} 数量级，本文算法较传统的分离算法取得 1 dB 的增益，较文献[4]，文献[6]算法分别取得 0.15 dB 和 0.06 dB 的增益；在误包率为 10^{-3} 数量级，本文算法与文献[4]，文献[6]算法比较分别取得 0.4 dB 和 0.25 dB 的增益。这是由于本文方案采用多个禁用符号的信源模型，增强了检错能力。

为了比较不同的禁用符号总概率的性能，本文采用禁用符号总概率 $P(\mu)$ 分别为 0.097 和 0.185，即信道码率分别为 4/5 和 2/3 时，仿真结果如图 6 和图 7 所示。从图中可以看出，当 $P(\mu)$ 较大的情况下，本文算法性能的改善更为明显。这是因为对于较小的 $P(\mu)$，将其分为多个部分，每个禁用符号的概率都很小，纠错功能未得到充分利用；当 $P(\mu)$ 取值较大时，多个禁用符号的概率都足够大，纠错功能得到充分利用。

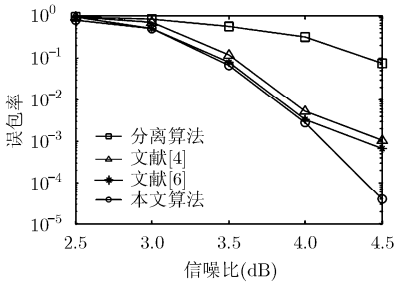

图 5　$P(\mu)=0.05$ 时各算法在相同条件下的误包率比较

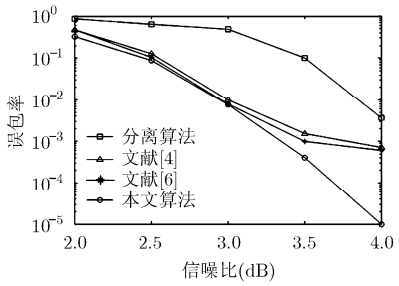

图 6　$P(\mu)=0.097$ 时各算法在相同条件下的误包率比较

为了进一步验证本文算法与现存不同联合编译码算法随禁用符号概率变化的译码性能，当信噪比 5.5 dB 时，仿真实验比较了误包率与禁用符号概率之间的关系(如图 8 所示)。从图中可以看出，对于相同的误包率，本算法只需要较小的禁用符号概率，即较小的冗余就能实现。在误包率为 10^{-3} 数量级，文献[4]算法需要禁用符号概率 $P(\mu)=0.027$，对应于信道码率为 0.935；文献[6]算法需要禁用符号概率 $P(\mu)=0.019$，对应于信道码率为 0.953；而本文算法需要禁用符号概率 $P(\mu)=0.017$，对应于信道码率为 0.959。

5.2 安全性实验与分析

本文算法的安全性依赖于混沌映射生成的伪随机序列的随机性和密钥空间大小。下面分析本算法的安全性能。实验中选取 Chebyshev 映射 1 的初值和参数分别为 $x_0=0.63$，λ_1=4；Chebyshev 映射 2 的初值和参数分别为 $y_0=0.1$，λ_2=8。

(1)密钥敏感性分析：密钥敏感性，即密钥的微小变动使得密文发生很大变化[17]。为了测试每个密钥的敏感性，保持其他密钥不变，仅变动一个密钥后比较密文的比特变化率。两个 Chebyshev 映射的初值变动 10^{-15} 时，测得密文分别变化了 49.7%和 50.2%；两个 Chebyshev 参数变化时，测得密文分别变化了 50.3%和 49.8%。所有密文变化都接近 50%，实验结果表明：本算法密文对密钥具有高度敏感性。

(2)密钥空间：密钥空间是指加密过程中所有能使用到的密钥个数。一个好的加密算法应该拥有足够大的密钥空间来抵抗蛮力攻击[18]。两个 Chebyshev 序列初值由双精度浮点数表示，精度都为 10^{-15}，因此密钥空间大小为 $10^{30}\approx 2^{100}$。此外，如果考虑 Chebyshev 的参数以及混沌映射的初次迭代次数，攻击者需要尝试更大的空间来进行蛮力攻击。

(3)密文随机性分析：为了验证随机性能，对密文进行 NIST SP800-22 国际标准[19]测试。NIST SP800-22 测试标准提出了 16 项测试内容来全面评估伪随机序列，可测试任意长的二进制序列的随机性，主要致力于判定可能存在于序列中的多种多样的非随机性。该标准对于每一个测试内容，都会计算出一个 P 值，在该标准规定的显著性水平 $\alpha=0.01$ 的前提下，若 $\alpha\le P<1$，则认为待测序列可通过该测试。此处，本文测试的密文长度为 10^6，对于每一个测试，计算出的 P 值均大于 0.01。因此，由本文算法的安全性通过了 NIST SP800-22 测试，具有很强的随机性。

(4)信息熵分析：信息熵是衡量随机性和密码系统安全性的一个重要准则[20]。若信息有 2 种状态值且出现的概率相同，则其熵为 1，表明信息是完全随机的。因此对密文希望其信息熵尽可能地接近于理想值 1，如若信息熵小于 1，则表明从理论上看密文存在一定程度的信息泄露。通过本文算法测试出密文的“0”和“1”的比率为 1.0032，信息熵为 0.9995，表明密文的信息泄露极小，算法是安全的，可以抵抗信息熵攻击。

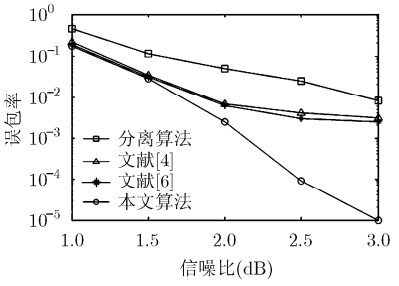

图 7　$P(\mu)=0.185$ 时各算法在相同条件下的误包率比较

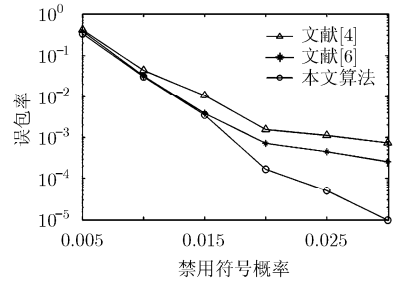

图 8 不同系统误包率与禁用符号概率之间的关系

(5)选择明文攻击分析：选择明文攻击是指攻击者有能力选择任意部分明文和对应的密文，通过分析两者间存在的关系而得到密钥的攻击。抵抗选择明文攻击的好方法是令密码流依赖于明文或密文，攻击者无法通过分析明文和密文间的关系来推导出密码流。本文算法在控制算术码概率模型时采用的密码流是和明文相关的，选择不同的明文，就会产生不同的密码流。设 $\boldsymbol{h}$ 和 $\boldsymbol{h}'$ 分别为相同密钥下不同明文生成的控制概率模型时采用的两个不同密码流，位置 n 处对应的密码流记为 h_n 和 $h_n^{'}$。定义数组 d，当 $h_n = h_n^{'}$ 时，d_n=0，否则 d_n=1。定义密码流差异率 D，其表示为

$$D = \frac{\sum_n d_n}{\text{size}(d)} \times 100\% \tag{12}$$

随机选取 100 组不同明文，将它们用同一密钥加密，然后两两测试其密码流的差异率，得到平均值为 50.1%。密码流差异率非常接近 50%，也就是说即使密钥相同，在不同明文加密中生成的密码流也完全不一样，密码流和明文是相关的。因此本加密算法可以抵抗选择明文攻击。

6 结论

根据深空通信等资源受限网络的特点，本文采用混沌映射产生随机序列，将压缩、纠错和加密 3 个环节有机结合起来，提出了一种新颖的联合信源信道与安全算术码编译码算法。在编码端通过混沌密钥 1 控制在算术码内嵌入多个禁用符号，将信道编码纠错与密码流的扰乱相结合；同时通过混沌密钥 2 控制信源符号的算术编码位置，将信源编码与信息安全相结合，实现了联合信源信道与信息安全编译码。仿真实验表明，提出的联合信源信道与安全算法改善了编码的性能，在无线通信传输中具有一定的应用前景。

参 考 文 献

[1] MAGLI E, GRANGETTO M, and OLMO G. Joint source, channel coding, and secrecy[J]. *EURASIP Journal on Information Security*, 2007, 2007(1): 1–7. doi: 10.1155/2007/79048.

[2] BOYD C, CLEARY J, IRVINE S, *et al*. Integrating error detection into arithmetic coding[J]. *IEEE Transactions on Communications*, 1997, 45(1): 1–3. doi: 10.1109/26.554275.

[3] GRANGETTO M and COSMAN P. MAP decoding of arithmetic codes with a forbidden symbol[C]. Proceedings of Advanced Concepts for Intelligent Vision Systems, Ghent, Belgium, 2002: 82–89.

[4] GRANGETTO M, MAGLI E, and OLMO G. Joint source/channel coding and MAP decoding of arithmetic codes[J]. *IEEE Transactions on Communications*, 2005, 53(6): 1007–1016. doi: 10.1109/TCOMM.2005.849690.

[5] JAMAA S B, KIEFFER M, and DUHAMEL P. Improved sequential MAP estimation of CABAC encoded data with objective adjustment of the complexity/efficiency tradeoff [J]. *IEEE Transactions on Communications*, 2009, 57(7): 2014–2023. doi: 10.1109/TCOMM.2009.07.070566.

[6] SPITERI T and BUTTIGIEG V. Maximum a posteriori decoding of arithmetic codes in joint source-channel coding[C]. International Joint Conference on e-Business and Telecommunications, Athens, 2012: 363–377. doi: 10.1007/978-3-642-25206-8_24.

[7] 夏志进, 杨铭, 崔慧娟, 等. 多禁止符号算术编码高效错误检测算法[J]. 清华大学学报(自然科学版), 2005, 45(7): 935–938. doi: 10.3321/j.issn:1000-0054.2005.07.019.
XIA Zhijin, YANG Ming, CUI Huijuan, *et al*. Efficient arithmetic code error detection algorithm with multiple forbidden symbols[J]. *Journal of Tsinghua University*(*Science and Technology*), 2005, 45(7): 935–938. doi: 10.3321/j.issn:1000-0054.2005.07.019.

[8] GRANGETTO M, MAGLI E, and OLMO G. Multimedia selective encryption by means of randomized arithmetic coding[J]. *IEEE Transactions on Multimedia*, 2006, 8(5): 905–917. doi: 10.1109/TMM.2006.879919.

[9] MI B, LIAO X F, and CHEN Y. A novel chaotic encryption scheme based on arithmetic coding[J]. *Chaos Solitons & Fractals*, 2008, 38(5): 1523–1531. doi: 10.1016/j.chaos.2007.01.133.

[10] 李林森, 张灿, 陈德元. 基于 CCSDS IDC 的联合信源与安全编译码[J]. 中国科学院学报, 2012, 29(3): 384–391.
LI Linsen, ZHANG Can, and CHEN Deyuan. Joint source encryption coding based on CCSDS image data compression standard[J]. *Journal of University of Chinese Academy of Sciences*, 2012, 29(3): 384–391.

[11] LIN Q Z and WONG K W. An improved iterative decoding scheme based on error-resistant arithmetic code[C]. 2014 IEEE International Symposium on Circuits and Systems, Melbourne, 2014: 1704–1707. doi: 10.1109/ISCAS.2014.6865482.

[12] ZEZZA S, MASERA G, and 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. doi: 10.1109/ISCAS.2014.6865282.

[13] ZHANG C Y, XIANG F, and ZHANG L W. Study on cryptographical properties of several chaotic pseudorandom sequences[C]. 2009 International Symposium on Computer

Network and Multimedia Technology, Wuhan, 2009: 1–4. doi: 10.1109/CNMT.2009.5374713.

[14] JAMAA S B, WEIDMANN C, and KIEFFER M. Analytical tools for optimizing the error correction performance of arithmetic codes[J]. *IEEE Transactions on Communications*, 2008, 56(9): 1458–1468. doi: 10.1109/TCOMM.2008.060401.

[15] STALLINGS W, 王张宜, 杨敏, 等. 密码编码学与网络安全——原理与实践(第5版)[M]. 北京: 电子工业出版社, 2012: 106–137.

STALLINGS W, WANG Zhangyi, YANG Min, *et al*. Cryptography and Network Security: Principles and Practice (Fifth Edition)[M]. Beijing: Publishing House of Electronics Industry, 2012: 106–137.

[16] HAGENAUER J. Rate-compatible punctured convolutional codes (RCPC codes) and their applications[J]. *IEEE Transactions on Communications*, 1988, 36(4): 389–400. doi: 10.1109/26.2763.

[17] 刘泉, 李佩玥, 章明朝, 等. 基于可 Markov 分割混沌系统的图像加密算法[J]. 电子与信息学报, 2014, 36(6): 1271–1277. doi: 10.3724/SP.J.1146.2013.01246.

LIU Quan, LI Peiyue, ZHANG Mingchao, *et al*. Image encryption algorithm based on chaos system having Markov portion[J]. *Journal of Electronics & Information Technology*, 2014, 36(6): 1271–1277. doi: 10.3724/SP.J.1146.2013.01246.

[18] 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. doi: 10.3969/j.issn.1000-436x.2014.03.025.

DENG Xiaoheng, LIAO Chunlong, ZHU Congxu, *et al*. Image encryption algorithms based on chaos through dual scrambling of pixel position and bit[J]. *Journal on Communications*, 2014, 35(3): 216–223. doi: 10.3969/j.issn.1000-436x.2014.03.025.

[19] RUKHIN A, SOTO J, NECHVATAL J, *et al*. A statistical test suite for random and pseudorandom number generators for cryptographic applications, SP-800-22[R]. Washington: National Institute of Standards and Technology, 2001.

[20] 张顺, 高铁杠. 基于类 DNA 编码分组与替换的加密方案 [J]. 电子与信息学报, 2015, 37(1): 150–157. doi: 10.11999/JEIT140091.

ZHANG Shun and GAO Tiegang. Encryption based on DNA coding, codon grouping and substitution[J]. *Journal of Electronics & Information Technology*, 2015, 37(1): 150–157. doi: 10.11999/JEIT140091.

鄢　懿：　女，1990 年生，博士生，研究方向为通信与信息系统.

张　灿：　女，1954 年生，教授，研究方向为移动无线通信、无线网络安全.

郭振永：　男，1972 年生，副研究员，研究方向为信号处理.