文章编号:1000-582X(2012)08-087-05

Logistic 映射控制的安全算术编码及其在图像加密中的应用

代才莉[1,2],包万宇[2]

(1. 重庆大学 通信工程学院,重庆 400044;2. 重庆电子工程职业学院通信工程系,重庆 401331)

摘 要:提出了一种通过 Logistic 映射改变模型中符号的顺序及符号的概率值的安全算术编码,将其应用于图像数据的压缩加密中,使其在网络中安全传输更方便,在编码过程中通过完全混沌的序列保证改变模型的均匀性,从而满足图像压缩编码的安全性要求。算法能够应用于任何针对多媒体数据的算术编码器(包括视频,图像,音频等),并且对编码的效率影响甚微,而且基于编码压缩的加密方式相对于其他同类加密方式所具有的明显优势在于,压缩过程大量减少了信息的冗余性,并在此过程中引入加密,这对试图推测出图像信息以及找到密钥的攻击具有良好的鲁棒性。

关键词:算术编码;图像加密;动态模型;Logistic 映射

中图分类号:TP391.4　　**文献标志码**:A

Logistic map controlled secure arithmetic coding and its application in image encryption

DAI Caili[1,2], *BAO Wanyu*[2]

(1. College of Communication engineering, Chongqing University, Chongqing 400044, P. R. China;
2. Chongqing College of Electronic Engineering, Chongqing 400044, P. R. China)

Abstract: A logistic map controlled secure arithmetic coding is proposed, the Logistic map is used to control the order of the symbols in the model and change the probabilities of the symbols, which is applied to the image encryption. The proposed scheme makes the image transmit more secure and comfortably on the Internet, and that is done at little expense in terms of coding efficiency. In the coding process, it ensures the uniformity of the model being changed by the chaotic sequence, thus to meet the security requirements of image compression. The algorithm can be applied to any arithmetic codec based on multimedia data including video, image and audio. Its most strength compared with other cipher mode is that, there is a significant reduction in the redundancy of information during the compression process, and it is robust when attempting to estimate the information of the image and discovering the key. The scheme can effectively resist differential analyses from both cryptography and coding.

Key words: arithmetic coding; image encryption; adaptive-model; logistic map

在 1948 年 Shannon 的论文中已经出现算术编码的影子,在上世纪 60 年代 Elias 正式提出了算术编码的思想,1987 年 Witten 等人在文献[1]中提出了算术编码在数据压缩方面的应用,指出其比

收稿日期:2011-10-18

基金项目:国家"863"资助项目(2003AA132050);博士点基金资助项目(200806110016);国家留学基金委建设高水平大学资助项目;重庆大学"211 工程"三期创新人才培养计划建设项目(S-09108)

作者简介:代才莉(1982-),女,重庆大学博士,主要从事计算机、通信技术方向研究,(Tel)13996334047;(E-mail)daicaili2001@163.com。

Huffman编码具有更好的压缩效率，提高了10%左右；但由于其编码复杂性和实现技术的限制以及一些专利权的限制，所以并不像Huffman编码那样被广泛应用。随着实现技术的改进，在近年来算术编码以其良好的压缩性能成为无失真压缩方法的主流，并被广泛应用到一些最新的多媒体压缩标准中，例如JPEG2000、H.264等。另一方面，算术编码并不是采用固定码字来表示每个符号，它的压缩模式是将一段消息用一个[0,1)的真子集(子区间)来表示，而这个区间被初始化为[0,1)，并且每编码一个符号区间就缩小一次。使每一个新区间都能唯一的表示一段消息。

而正是这样的编码模式对数据安全是非常有利的，同时算术编码在多媒体技术中的广泛应用，使业界对其安全性进行了广泛研究。中国内外专家对算术编码的安全性进行了大量的理论研究[2-10]，但是除了Marco Grangetto等人[4]提出的RAC还相对安全以外，其余的加密算法均已被破解。另一方面，虽然现今像DES和AES这样的基于分组加密的算法非常流行，但直接将其应用到多媒体数据中却有一些明显的缺点[11-12]。如对PC机来说需要太多的计算资源；分组加密模式因为其时延问题很不适宜应用到实时通信系统中；像DES，AES这样的加密标准都是针对独立同分布的数据源进行操作，而多媒体数据是典型的非独立同分布数据源等等。所以将编码和加密结合起来是当前研究的趋势。提出了一种基于二元符号概率区间的变动及置换的安全二进制算术编码，并将其应用到图像加密中，减少了图像数据过多的冗余信息，保证了其在网络传输中的安全性。

1 算术编码简介

算术编码采用的是区间分割的思想，通过对区间的递归分割实现编码过程。编码是将符 X_{1i} 号按已知的顺序在[0,1)的实数半开区间上进行排列。根据每个符号的概率大小赋予一个互相不重叠的子区间，即这个子区间的长度就是该符号的概率大小。由于所有符号的概率之和为1，因此所有子区间必须正好填满从0到1的区间。编码区间由3个变量所表示HIGH，LOW及RANGE，随着每个信源符号的加入区间逐步减小，每次减少的程度取决于当前加入的信源符号的概率，直到编码的消息符号序列结束，便将整段消息映射到了一个唯一的[0,1)内的子区间。而解码时只要按照同样的概率模型进行就能得到原始的消息序列。

下面简要介绍算术编码的过程。采用固定模型编码时，假设已知每个信源符号的先验概率，根据这一概率分布，在[0,1)之内，分别对每个信源符号指定一段与其相对应的数值间隔，间隔的大小与该符号的概率相符。由于提出的算法是基于二元(即只有2个信源符号0和1)模型的，给出一个二元模型的算术编码例子来说明其编码的过程。设range表示编码输出数值的落入范围，low表示编码区间的下界，high表示编码区间的上界，range=high-low。最初的初始区间为[0,1)，初始值即为range=1，low=0，high=1。符号0和1的概率分别为 $P(0)$ 和 $P(1)$。

如图1所示，若编码符号为0，则

low=low，high=low+range·$P(0)$，range=high−low；

若编码符号为1，则

low=low+range·$P(0)$，high=high，range=high−low。

重复上述步骤，直到整个符号流结束便可将一段消息映射到区间range上，并用区间上的一个数C(S)表示。而解码时根据解码规则，如果 $0\leqslant C(S)\leqslant P(0)$，则第一个编码的字符为0，且 $C(S_{new})=(C(S)-0)/P(0)$；若 $P(0)\leqslant C(S)\leqslant 1$，则第一个编码的字符为1，且 $C(S_{new})=(C(S)-P(0))/P(1)$。持续上述步骤，直到解码出最后一个码字为止。

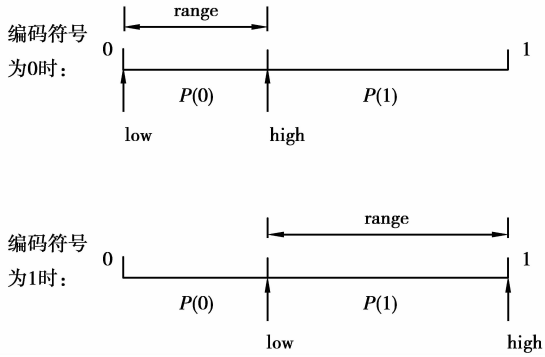


图1 二元模型编码过程

2 Logistic映射

Logistic映射定义

$$X_{n+1}=rX_n(1-X_n),$$

其中，r 为分支参数3.569 946…$\leqslant r\leqslant 4$，$0<X_n<1$。

这个看似简单的映射蕴含着现代混沌理论的基本思想，包括倍周期到混沌、分岔图等非线性理论的基本框架和模式。如图2所示，当 $r=4$ 时，Logistic

映射是完全混沌的，且其输入输出都分布在(0,1)上。因此使用了 Logistic 映射且取 $r=4$，来产生加密所用的随机序列，以保证其均匀性。

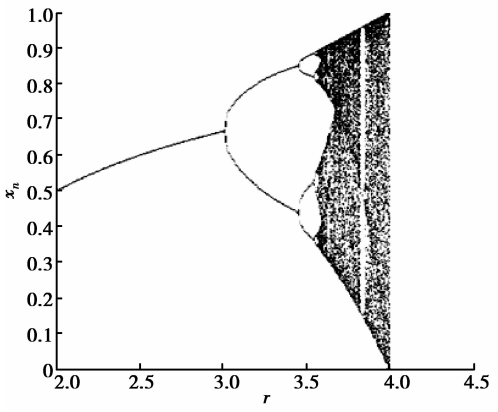


图 2　r 不同时 X_n 的取值分布

3　安全算术编码及应用

算术编码有一种区别于其他编码的特殊性质，其解码过程对差错是非常敏感的，差错会很快的扩散到整个解码块中。事实上，只要在解码过程中有一个错误，就会导致随后解码的信息没有任何的意义，这也正是设计一个具有良好鲁棒性的加密算法所需要的特性。算法的提出也正是基于这点。特别说明，本算法的程序实现将概率模型用十进制表示，采用文献[1]中的方法建立模型，即以频数 Freq(0)和 Freq(1)(整数 1 到 16 383)表示各符号的概率 $P(0)$和 $P(1)$。算法的具体过程如下：

首先，采用 Logistic 映射产生 2 组混沌序列 X_1 和 X_2，将 2 组映射的初始值作为密钥进行保密。这里为了说明方便，取 $r=4$，$X_{10}=0.123\ 456$，$X_{20}=0.234\ 567$。

其次，通过混沌序列 X_1 判断编码模型是否置换及各符号概率值是否改变，即加密流程如图 3 所示。

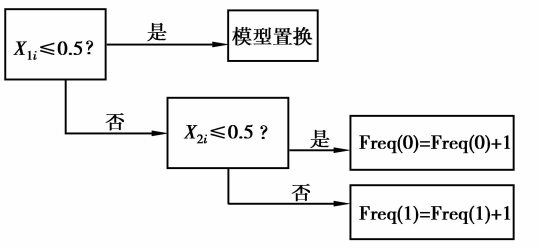


图 3　加密流程图

若 $X_{1i}\leqslant 0.5$，则编码的概率模型进行置换，否则判断 X_{2i}是否小于 0.5，若是，则 Freq(0)自加一，即改变概率模型中符号 0 的概率 $P(0)$；若不是则 Freq(1)自加一。而模型的置换过程采用第 2 节图 1 的例子来说明，如图 4 所示。根据[1]中的定义可知每个符号的频数 Ferq 的取值范围为[1,1638 3]，所以频数的加一变化对符号概率的改变是非常小的，即这对算术编码的压缩效果影响甚微；另一方面，模型中符号顺序的置换并不改变每个符号的概率值，只是顺序的交换，所以不会影响编码的压缩效率。

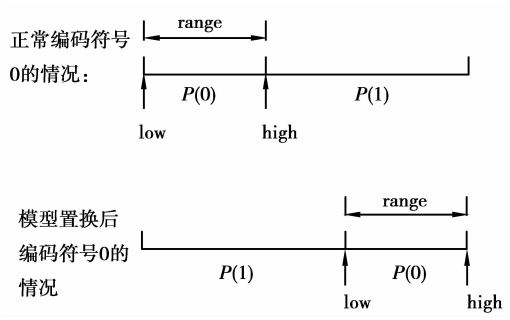


图 4　模型置换过程

使用本算法进行图像加密时，首先对图像数据进行预处理，将十进制的像素值转换为八位二进制，即只有符号 0 和 1，再对其进行编码压缩及加密。具体实现过程如上述算法所示。解密时只需将正确解码的序列转换为十进制恢复图像数据。

4　实验结果及安全性分析

4.1　从密码学角度的安全性分析

1)密文均衡性测试

为了测试密文中符号的均衡性(0,1 分布的均衡性)，对 Logistic 映射的初始值进行改变时的密文中 0,1 的个数比进行了测试，这个过程中改变了初始 X_{10}的值，而 X_{20}的值保持不变。测试结果如表 1 所示。从表 1 可以看出密文的均衡性在 0.5 左右，即算法有很好的加密效果。

表 1　0,1 均衡性测试结果

不同的初始值	$X_{10}=$ 0.123 456	$X_{10}=$ 0.123 457	$X_{10}=$ 0.123 446	$X_{10}=$ 0.123 356	$X_{10}=$ 0.122 456
密文中 0/1 个数比	0.524 8	0.524 1	0.495 3	0.506 4	0.509 7

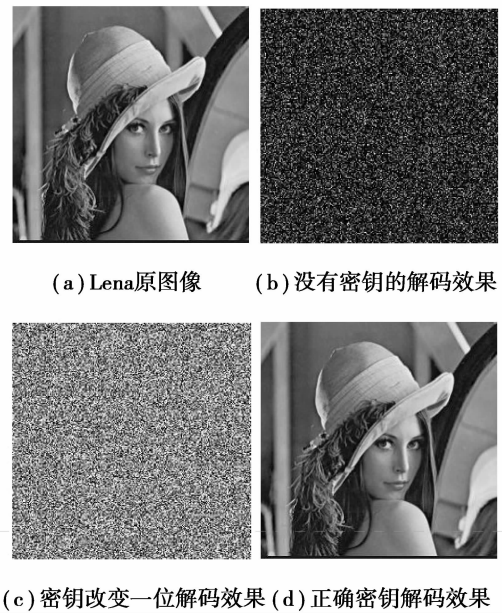
2)密钥敏感性分析

雪崩效应是一个广泛应用的衡量加密算法设计好坏的标准，根据严格的雪崩效应准则，若改变密钥中的任意一位，将导致密文分组中几乎所有数据位的变化[8]，即密钥的雪崩效应。实验对仅改变密钥任意一位的密文进行分析，改变 X_{10} 和 X_{20} 其中某个值的任一位(十进制的任意一位)，整个数据的改变率如表2所示，X_{1_i} $(i=0,1)$ 表示改变 X_{10} 中的任意一位，X_2 表示改变 X_{20} 中任意一位，可见改变密钥的任一位密文中几乎所以数据均被改变，说明本算法具有良好的雪崩效应。

表2 密钥改变一位加密数据变化率

密钥变化一位	加密数据变化率/%
$X_{10}=0.123\ 446$	99.600 2
$X_{11}=0.193\ 456$	99.663 3
$X_2=0.234\ 568$	99.602 0
X_1 和 X_2	99.621 8

对算法密钥的敏感性测试结果如图5所示，图5(a)为未进行压缩加密的Lena图像，而图5(b)为Lena图像经加密压缩后，在没有密钥的情况下由标准解码器解码后的效果，另外，仅改变其中一位密钥的解码器解码之后的效果以及用正确密钥解码之后的图像分别在图5(c)和图5(d)中可以看到，结果表明在以上2种情况下解密后的图像都是没有任何意义的。



(a)Lena原图像 (b)没有密钥的解码效果

(c)密钥改变一位解码效果 (d)正确密钥解码效果

图5 密钥敏感性测试效果图

3)差分分析

对于明文图像来说，如果图像像素中有一个细微的变换可以导致在密文图像中有重大的差别，则对于图像来说，差分攻击就是无效的。因此，进行了一个特殊的实验，即只在明文图像中改变一个像素值，然后分别压缩加密得到相应的密文，利用文献[8]中提出的NPCR作为测试的标准，由于测试对象为压缩文件，并不是可读图像，对NPCR进行重新定义，首先给出一个像素值不同的明文图像所对应的2个经压缩加密之后的密文 C_1 和 C_2，位置 i 处对应的密文记为 $C_1(i)$，$C_2(i)$，定义数组 $D(i)$，其值由 $C_1(i)$，$C_2(i)$ 决定，如果 $C_1(i)=C_2(i)$，$D(i)=0$，否则 $D(i)=1$。NPCR定义为

$$\mathrm{NPCR}=\frac{\sum_i D(i)}{\mathrm{size}(D)}\times 100\%。$$

对大小为256×256的灰度图像进行了测试，结果如图6，NPCR值在0.996附近波动，说明算法对明文的敏感性非常好，是能够抵御差分分析的。

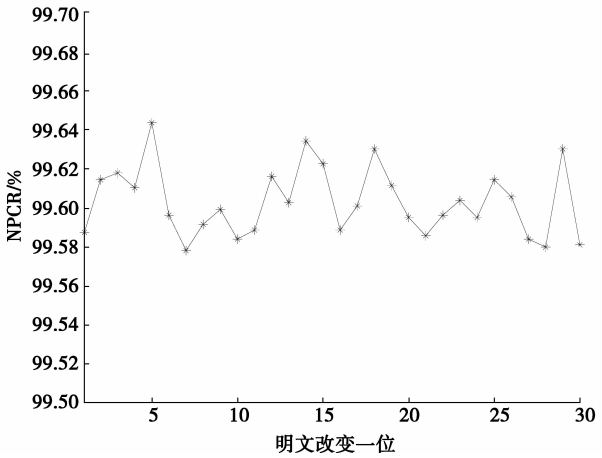


图6 明文改变一位NPCR值的波动

4.2 从编码角度的安全性分析

提出的算法可以抵抗Bergen等人在文献[2]中提出的选择明文攻击，因为文中的破解方法是通过确定固定模型里符号的顺序及概率来进行的，即整个算法的安全性及抵抗此种攻击的关键在于密钥的安全性。但与之不同的是本算法的模型为动态模型，且模型中符号的顺序和概率值由2个完全混沌的序列所控制。因此，提出的算法能够抵抗Bergen提出的选择明文攻击。

另外，John等人在文献[3]中提出的攻击同样仅针对二元固定模型的编码，通过选择适当的明文推测出模型中 A，B 的概率，并且在假设 A，B 顺序

已知的条件下进行的。而算法采用动态模型进行编码，且符号概率值并不固定，就使得文献[4]中提出的攻击方法由于无法确定每次编码时模型中符号顺序及概率值而失效。

5 结 论

由于 Logistic 映射完全混沌时产生的序列是均匀的，所以将用于扰乱编码模型中符号的顺序以及改变符号概率值也是服从一致分布的，即提出的基于 Logistic 映射的安全算术编码不仅利用了 Logistic 映射参数 $r=4$ 时完全混沌的性质，同时结合算术编码良好的压缩性能，对模型的敏感性等特性，通过控制编码模型中符号顺序及其概率值来实现压缩加密，并将其应用到图像中，实验结果和安全性分析表明该压缩加密算法并不影响算术编码的压缩性能，且安全性非常好，有很大的密钥空间，且对密钥十分敏感，从密码学和编码学分析的角度，对多种攻击手段都具有良好的免疫性，具有良好的应用前景。

参考文献：

[1] Witten I H, Neal R M, Cleary J G. Arithmetic coding for data compression[J]. Communications of the ACM, 1987, 30(6): 520-540.

[2] Bergen H A, Hogan J M. A chosen plaintext attack on an adaptive arithmetic coding compression algorithm [J]. Computers & Security, 1993, 12(2): 157-167.

[3] Cleary J G, Irvine S A, Rinsma-melchert I. On the insecurity of arithmetic coding [J]. Computers & Security, 1995, 14(2): 167-180.

[4] Grangetto M, Magli E, Olmo G. Multimedia selective encryption by means of randomized arithmetic coding [J]. IEEE Transactions on Multimedia, 2006, 8(5): 905-917.

[5] Wen J T, Kim H, Villasenor J D. Binary arithmetic coding with key-based interval splitting [J]. IEEE Signal Processing Letters, 2006, 13(2): 69-72.

[6] Kim H, Wen J T, Villasenor J D. Secure arithmetic coding[J]. IEEE Transactions on Signal Processing, 2007, 55(5): 2263-2272.

[7] Jakimoski G, Subbalakshmi K P. Cryptanalysis of some multimedia encryption schemes[J]. IEEE Transactions on Multimedia, 2008, 10(3): 330-338.

[8] Pareek N K, Patidar V, Sud K K. Image encryption using chaotic logistic map [J]. Image and Vision Computing, 2006, 24(9): 926 - 934.

[9] May R M, Simple mathematical models with very complicated dynamics [J]. Nature, 1976, 261: 459-467.

[10] 赵风光，倪兴芳，姜峰. 算术编码与数据加密[J]. 通信学报，1999，20(4)：92-96.
Zhao Fengguang, NI Xingfang, JIANG Feng. Arithmetic coding and data encryption[J]. Journal of China Institute of Communications, 1994, 20(4): 92-96.

[11] 谢冬青，谢志坚，李超，等. 关于一种算术编码数据加密方案的密码分析[J]. 通信学报，2001，22(3)：41-45.
Xie Dongqing, Xie Zhijian, Li Chao, et al. Cryptanalysis of data encryption scheme based on arithmetic coding [J]. Journal of China Institute of Communications, 22(3): 41-45.

[12] 郑浩然，金晨辉. 对基于算术编码的一个数据加密算法的已知明文攻击[J]. 通信学报，2003，24(11)：73-78.
Zheng Haoran, Jin Chenhui, An attack with known plaintexts to an encryption algorithm based on arithmetic coding [J]. Journal of China Institute of Communications, 2003, 24(11): 73-78.

（编辑 侯 湘）