基于上下文的分块图像联合压缩加密算法*

管丽娜, 邓家先†
(海南大学 信息科学技术学院, 海口 570228)

摘 要: 为了研究图像压缩与加密同步进行及提高安全性问题,提出了一种基于改进零树结构的分块图像联合压缩加密算法,将图像对应不同分块区域映射到相应子带中。利用密钥对图像压缩产生的原始上下文进行修正,然后与判决一起送往自适应算术编码器实现图像联合压缩加密。由于自适应算术编码的概率跳转规律复杂,相对概率固定的区间分裂算术编码安全性更好。对所提出的算法进行仿真,结果表明:与原始图像压缩算法相比较,所提出的算法具有基本相当的压缩效率;而采用的图像分块方法能够灵活地控制不同区域图像的相对质量及更好地实现信息安全防护;使用不同的密钥可以进行分块加密,实现了对重要信息的隐私和机密保护。

关键词: 改进零树结构; 上下文; 联合压缩加密; 自适应算术编码
中图分类号: TN919.81;TP391 **文献标志码**: A **文章编号**: 1001-3695(2013)09-2795-04
doi:10.3969/j.issn.1001-3695.2013.09.059

Joint compression-encryption of block image based on context

GUAN Li-na, DENG Jia-xian†
(*College of Information Science & Technology*, *Hainan University*, *Haikou* 570228, *China*)

Abstract: This paper proposed a novel algorithm, in which the data of block regions mapped to the corresponding sub-band coefficients in order to make the image compression and encryption realized simultaneously and improve security. It used the key to modify the original context. And then it sent the modified context and the corresponding decision to arithmetic coder to implement the joint compression-encryption. The security encryption by the adaptive arithmetic coding is better than the one by arithmetic coding based on interval splitting (ACIP). The distribution of the adaptive arithmetic coding is more complex than the probability distribution of ACIP which is fixed. It simulated the proposed algorithm. The results show that the scheme has the same compression efficiency compared with the original image compression algorithm. The relative quality of different regions can be controlled flexibly. It can have a better information security efficiency to use the way of image block. Different keys can be used to encrypt the coefficients of different regions, which can realize the important information privacy and confidentiality protection.

Key words: improved zero-tree structure; context; joint compression-encryption; adaptive arithmetic coding

0 引言

随着网络技术和数字图像技术的不断发展,数字图像逐渐成为人们获取信息的重要来源,其安全性以及传输图像信息效率的提高也越来越受关注。为满足当前互联网上高速安全传输图像,传统的做法是将图像的压缩与加密分成两步来完成。然而,这样做将失去压缩与加密同步完成所具有的设计灵活与计算简化的一些优势。因此,将图像压缩和加密技术有机结合成为当前国内外研究的热点[1~4],即在进行熵编码的同时,数据加密也同时实现,这种方法称之为联合压缩加密(joint compression-encryption)。

近年来,部分研究者使用算术编码进行联合压缩加密,利用密钥对算术编码的区域分裂进行控制,实现联合数据压缩加密。当算术编码对应的联合概率与实际输入序列的联合分布相当时,就能实现高效数据压缩。

本文提出一种基于自适应算术编码的联合压缩加密算法。对零树编码进行改进,引入自适应算术编码,利用给定密钥对原始上下文进行修正,从而实现联合压缩加密;将图像进行分块,有利于灵活控制分块图像的相对质量及保证其安全性的实现。

1 算术编码基本原理及安全性对比

对于长度为 N 的二进制序列 $D=[D_0,D_1,\cdots,D_{N-1}]$,其中 $D_i(i=0,1,2,\cdots,N-1)$ 取值于集合 $\{0,1\}$。假设 D_i 服从独立同一分布,即

$$\begin{bmatrix} D_i \\ P_{D_i} \end{bmatrix}=\begin{bmatrix} 0 & 1 \\ p & 1-p \end{bmatrix} \tag{1}$$

令 n 表示序列取值的编号,定义为

$$n=\sum_{i=0}^{N-1} d_i 2^{N-i-1} \tag{2}$$

其中:d_i 表示 D_i 的取值。那么,第 n 个序列对应的联合概率 p_n 为

$$p_n=p^{N-\sum_{i=0}^{N-1} d_i}(1-p)^{\sum_{i=0}^{N-1} d_i} \tag{3}$$

第 n 个序列对应的累积概率为

$$P_n=\sum_{i=0}^{n-1} p_i \tag{4}$$

算术编码的基本原理就是将概率区间划分为 2^N 个子区间,使得序列的每种取值与唯一的一个概率子区间相对应,即

收稿日期: 2012-11-26; **修回日期**: 2013-01-14 **基金项目**: 海南省自然科学基金资助项目(613155)

作者简介:管丽娜(1989-),女,浙江金华人,硕士研究生,主要研究方向为数字图像处理;邓家先(1964-),男(通信作者),湖北钟祥人,教授,博士,主要研究方向为数字图像处理、数字滤波器设计、自适应信号处理(jxiandeng@126.com).

用概率区间$[P_n, P_{n+1})$表示第 n 个序列，然后用$\lfloor -lb(p_n) \rfloor$位二进制符号作为编码输出。

换言之，一般的算术编码是一个递推过程，所产生的浮点概率会落入一个相应的概率子区间，这样就可以用该子区间中的任何值来表示对应的编码序列。如果概率值稍有变化，其对应的概率区间也会随之而改变，从而无法译码出原始的编码序列，由于累计效应，会导致后续译码出现错误。

从上文讨论可以看出，二进制算术编码输出与描述该序列出现 0、1 的个数相关，而且与 0、1 出现的先后顺序相关。

区间分裂算术加密的基本思想也是如此[1,5]。攻击者可以根据得到的密文，通过分析或者假设得到对应的概率 p，所以区间分裂的密码安全性存在不足。为了保证算术密码的安全性，可以使用密钥对输入数据、输出密文进行置换，从而增加加密输出的隐蔽性。

区间分裂算术加密安全性不足的主要原因在于使用固定概率 p。如果对需要加密的数据进行分类，每类数据对应的概率分布不同，序列对应的概率区间划分会更为复杂，产生的密文的隐蔽性就会更强。下面简述自适应算术编码的基本原理。

假设数据共有 M 类，即序列第 i 个变量 D_i 属于 M 个类别中的一种。为方便起见，变量类别用 CX 表示，变量 D_i 可以表示为 $D_i(CX)$，CX 取值于 $0,1,\cdots,M-1$。第 CX 类的第 j 个变量对应的条件概率可以表示为

$$p(CX, D_j(CX)) = p\{(CX, D_j(CX)) \mid (CX, D_{j-1}(CX)), \cdots, (CX, D_0(CX))\} \tag{5}$$

第 CX 类变量个数为 $n(CX)$，则 CX 类变量联合概率分布为

$$p_{n(CX)} = \prod_{j=0}^{n(CX)-1} p(CX, D_j(CX)) = p(CX, D_0(CX)) p(CX, D_1(CX) \mid (CX, D_0(CX))) \cdots p(CX, D_{n(CX)-1}(CX) \mid (CX, D_{n(CX)-1}(CX)) \cdots (CX, D_0(CX))) \tag{6}$$

满足

$$\sum_{i=0}^{M-1} n(CX) = N \tag{7}$$

其中，$p(CX, D_0(CX))$为 CX 类变量的初始分布。自适应算术编码的条件概率是十分复杂的，不仅与当前变量取值及其类别有关，而且与前面变量的取值相关。

不考虑不同类别变量之间的关联性，对于给定长度为 N 的序列，其编号 n 仍然由式(2)得出，该序列的联合概率表示为

$$p_n = \prod_{i=0}^{N-1} p(CX, D_i(CX)) = \prod_{i=0}^{M-1} \prod_{j=0}^{n(CX)-1} p(i, D_j(i)) \tag{8}$$

由于 $p(CX, D_j(CX))$不再是式(3)的简单形式，相对区间分裂而言，序列的联合概率要复杂得多。将式(8)得到的序列联合概率代入式(4)，就可以计算出序列对应的累积概率，累积概率相应也十分复杂。描述该序列的概率区间$[P_n, P_{n+1})$不仅与序列的取值有关，与序列上下文分布也密切相关。由此可见，使用自适应算术编码器对数据进行加密，所产生的密文相对区间分裂算术编码要复杂得多，因此自适应算术加密也相对更加安全。区间分裂的联合算术压缩加密面临几个问题：

a)由于受到运算精度的限制，基于区间分裂的算法编码难以实现大量数据的算术编码。即使对于区间分裂的二进制算术编码而言，实现百位以上的二进制编码也是十分困难的。而图像压缩所产生的二进制判决数量远不止如此，一般高出几个数量级，都是兆级以上。因此，在工程上实现区间分裂的联合算术压缩加密是困难的，或者说几乎不可能实现。

b)区间分裂所假设的概率分布与实际概率分布不相符，必然会导致压缩效率降低，图像联合压缩加密的必要性就值得商榷。

c)在不进行置换情况下，密文的安全性不足，而如果进行数据置换、密文置换，势必需要在编译码过程中进行数据缓存，系统实时性难以实现。

基于离散小波变换或者离散余弦变换的比特平面编码技术在图像压缩领域得到广泛应用。比特平面编码主要有集合树编码、块编码或者树块编码，都会产生二进制判决，这些判决主要包括集合重要性，在当前比特平面的系数是否为 0，系数是正还是负等。自适应算术编码通过对送入编码器的某类判决进行算术编码，对判决进行自适应统计，并调整概率分布，从而实现高效数据压缩。图像压缩领域的成果表明，使用自适应算术编码能够取得好的压缩效果。

目前，在图像压缩领域广泛使用的 MQ 或者 QM 算术编码器都是自适应的，基本原理与上文描述相同。本文提出的图像联合压缩加密算法是以 MQ 算术编码为基础。

2 上下文修正原理图像联合压缩加密

如图 1 所示，算术编码器输入上下文 CX 和判决 D。其中：CX 用于对输入数据进行分类(即上下文的变量分类)，而 D 是对应类别的判决。D 是二进制数据，CX 是描述数据之间关联性的测度，这样同类数据之间的关联性就通过上下文对应的条件概率和初始分布进行描述。

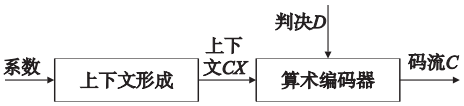


图1 MQ编码模型

上下文 CX 数量可以根据需要或者实际情况自主选择，而每类上下文初始分布的选择应当根据该类变量的概率初始分布加以选择。

从上文分析可知，给定序列的累计概率与上下文是密切相关的，而输出码流就是累计概率的一种描述，所以自适应算术编码器输出码流与上下文是密切相关的。具体地，对于给定序列，算术编码器输出码流与上下文种类(即上文中 M 的取值)有关，而且与每类上下文的数量、上下文出现先后顺序是相关的。

使用密钥对上下文进行修改就能够改变判决所属类别，从而扰乱序列对应的累计概率，那么描述累计概率及其子区间的编码输出码流自然会发生变化，从而实现加密；同理，使用密钥对判决进行修改，同样可以改变累计概率分布，从而实现加密。

上下文修正原理如图 2 所示。

$$CX = CX_1 \oplus \text{key} \tag{9}$$

其中：CX_1 为原始上下文，key 为密钥，CX 为修正后的上下文，⊕为定义的加法运算。原始上下文 CX_1 是根据输入数据产生的，CX_1 与密钥进行运算产生 CX。

图2 上下文修正原理

如果系统加密、解密产生的原始上下文相同，且加密、解密密钥相同，使用相同的运算，那么系统解密上下文 CX 就与加密的上下文 CX 相同。反之，如果解密使用的密钥与加密所使用的密钥不同，就会造成解密使用的上下文与加密时的不同，从而造成数据分类错误，解密出来的数据与原始数据出现差

异,出现解密错误。进一步地,一旦出现解密的数据错误,一方面会导致后续数据产生原始上下文有可能出错,从而产生连锁反应,出现连续解密错误;另一方面,后续数据解密时累计概率开始出错,同样导致连锁反应,出现连续解密错误。

所定义的加法运算应当尽可能保证密钥的唯一性,即不同密钥运算出的上下文 CX 序列应当是唯一的,尽可能不出现不同密钥运算出相同的上下文序列。

由于自适应算术编码器需要使用上下文和判决,从理论上讲,使用密钥对上下文或者判决进行修正都可以实现联合压缩加密。其原理如图 3 所示。

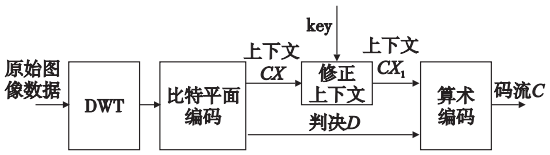


图3　上下文修正的图像联合压缩加密原理

变换产生的系数经过比特平面编码产生二进制判决 D 和判决对应的原始上下文 CX。为了实现联合压缩加密,利用密钥对原始上下文 CX 进行修正得到 CX_1,与判决 D 一起送往算术编码器进行算术编码,产生编码码流。

为了实现自适应算术编码并取得好的编码效果,需要对比特平面编码产生的判决进行分类,判决分类使用相邻系数或者相邻集合的重要性产生,称之为上下文。本文采用简单方法,只是利用同分辨率相邻集合重要性形成上下文,8 个邻居(2^8 = 256)可以产生 256 种上下文,经过合并形成 4 种集合上下文。图 4 为集合相邻关系,X 表示当前集合重要性,E_0、E_1、E_2、E_3 表示对角邻居集合重要性,L_0、L_1 表示水平方向邻居集合重要性,V_0、V_1 表示垂直方向邻居。其中 0 表示该集合不重要,1 表示集合重要。集合上下文 CX_n 为

$$CX_n = (V_0 | V_1 | L_0 | L_1) \times 2 + (E_0 | E_1 | E_2 | E_3) \tag{10}$$

其中,| 表示逻辑或运算。显然,当所有邻居集合都不重要时,$CX_n = 0$;水平、垂直集合都不重要,且对角集合至少一个重要,则 $CX_n = 1$;水平、垂直集合至少一个重要,且对角集合都不重要,则 $CX_n = 2$;水平、垂直集合有一个重要,且对角也至少一个重要,则 $CX_n = 3$。

E_0	V_0	E_1
L_0	X	L_1
E_2	V_1	E_3

图4　集合邻居

为了得到加密使用的上下文,可以对密钥进行循环移位,取移位后的最低若干位二进制数据 d_k 与原始上下文进行运算,即

$$CX_1 = (d_k + CX) \bmod (L) \tag{11}$$

其中:mod( )表示取模运算;L 取值可以根据用户进行选择,原则上,L 需满足下列不等式

$$L \leqslant \max(d_k) + L_1 \tag{12}$$

如果式(12)不成立,模运算本身就没有意义。

3　改进零树编码和分块提取

零树编码是由 Shapiro[6] 提出的一种基于小波变换和比特平面编码方法,利用小波子带系数之间的相似性进行高效数据压缩,是最早基于小波变换的图像压缩算法之一,在图像压缩领域具有独特的学术地位。以三级小波变换为例,LL3 子带的一个系数对应 HL3、LH3、HH3 子带系数。除了 LL3 子带之外,每个三级子带系数对应四个二级子带系数,而每个二级子带系数对应四个一级子带系数,从而构成一棵树,称之为零树,如图 5 所示。

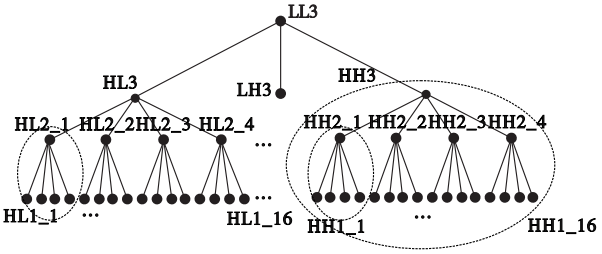
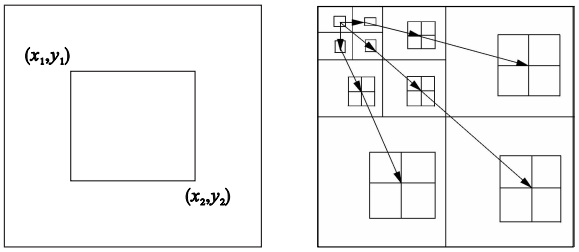


图5　零树结构

零树编码按照比特平面的先后顺序进行排序,在同样比特平面内按照 LL3 子带系数的顺序对相应的树进行编码,这种逐次逼近的编码算法能够取得好的编码效果。

在同一比特平面内,按照 LL3、HL3、LH3、HH3、LH2、…、HH1 的子带顺序进行编码,编码产生上下文和判决一起送往对应的算术编码器进行进一步压缩。LL3 编码是对 LL3 子带中的系数进行编码,产生系数在当前比特平面的上下文 CX 和判决 D,然后送往对应的算术编码器进行进一步压缩,并产生独立码流。同理,将 HL3、LH3、HH3 系数及其子孙构成各自集合,2 级子带的系数及其子孙构成各自子集合。如 HL3 分为 HL2_1、HL2_2、HL2_3、HL2_4 共四个集合。三级子带系数及其集合一起编码,形成各自码流。以此类推,这样各个分辨率子带系数编码输出各自码流,共 10 组编码输出码流。这种编码方式实现了分辨率压缩,并为实现分辨率加密带来方便。



(a) 图像分块　　(b) 分块图像小波变换后的图像

图6　图像分块后的小波变换情况

本文在上下文修正的情况下对图像进行分块处理,即小波变换后,主要利用小波分解后各子带系数所呈现出的树状层次分解结构、子带间明显的相似性与方向性,将图像分为两部分。以小矩形块为例,假设在一幅图像中选择了一个小矩形块,其左上角和右下角的两个顶点坐标分别为(x_1, y_1)和(x_2, y_2),如图 6(a)所示,经过一级小波分解后,其中左上角的 LL_1 子带中的小矩形块的位置可以用以下两个对角顶点坐标(x_1^1, y_1^1)和(x_2^1, y_2^1)来确定:

$$x_1^1 = \lfloor \frac{x_1}{2} \rfloor - 1, y_1^1 = \lfloor \frac{y_1}{2} \rfloor - 1 \tag{13}$$

$$x_2^1 = \lceil \frac{x_2}{2} \rceil + 1, y_2^1 = \lceil \frac{y_2}{2} \rceil + 1 \tag{14}$$

其中:$\lfloor \cdot \rfloor$表示向下取整运算,$\lceil \cdot \rceil$表示向上取整运算。其他三个子带 LH_1、HL_1、HH_1 中的矩形块系数位置可以通过平移得到。进行 N 级分解的情况以此类推,这里不再赘述。

图像分块如图 6(a)中矩形所示,算法计算出最低频子带

及其他剩余子带,如图 6(b)所示。设定由(x_1,y_1)和(x_2,y_2)坐标围成的矩形块为块 1,余下图像区域部分为块 2。

为了利用算术编码对数据进一步压缩,同时考虑能够实现分辨率渐进性编码,对零树编码进行改进,改进后的编码器结构如图 7 所示。

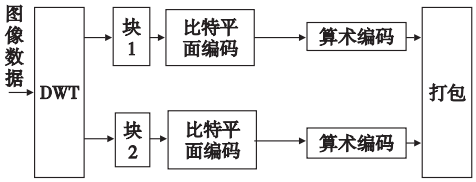


图7 改进零树编码

4 实验结果与分析

首先使用图像 Lena 对所提出的联合压缩加密算法进行仿真,式(12)取 $L=L_1$,当输出码率分别为 0.5、0.75、1.0、1.25、1.5、1.75、2.0 时,联合加密重建质量与原始算法重建质量(PSNR)如表 1 所示。从中可以看出,两者重建图像质量基本相同。

表 1 原始算法与联合压缩加密重建图像质量比较

码率 R	原始压缩算法/dB	上下文修正/dB	码率 R	原始压缩算法/dB	上下文修正/dB
0.5	36.00	36.02	1.5	41.19	41.19
0.75	37.83	37.86	1.75	42.75	42.75
1.0	39.17	39.17	2.0	43.43	43.43
1.25	40.08	40.08			

这就表明,只要参数选择合理,联合压缩加密与原始算法具有同样的压缩效果。

由表 2 可以看出,当输出总码率分别为 1.0, 1.75, 2.75, 3.5 时,上下文修正以及在上下文修正下使用不同的密钥对块 1 和块 2 进行加密,所取得的重建图像质量与原始算法重建质量基本相同(以 Lena 图和 goldhill 图为例)。因此,在不影响图像质量及加密安全性的前提下,可以灵活控制块 1 和块 2 的相对码率,调整两者的相对压缩质量。此外,由于图像区域经由分块之后,可以根据用户需要设置不同的密钥来对块状图像进行加密,这对图像内容的安全性有较大的提高;还能根据不同的优先级,编码多个块状区域,从而满足更多用户的需求。

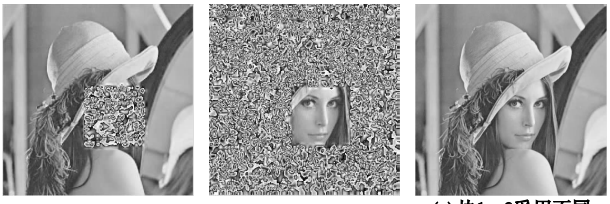
表 2 在不同码率下,原始算法、图像分块联合压缩加密使用相同密钥和不同密钥下的重建图像质量比较

码率控制		Lena 图像重建质量/dB			goldhill 图像重建质量/dB		
块 1 码率 R_1	块 2 码率 R_2	原始压缩算法	上下文修正	上下文修正(块 1、2 使用不同密钥)	原始压缩算法	上下文修正	上下文修正(块 1、2 使用不同密钥)
0.75	0.25	33.55	33.61	33.61	30.86	30.85	30.85
0.5	0.5	36.79	36.81	36.81	33.31	33.27	33.27
0.25	0.75	38.96	38.97	38.97	34.82	34.80	34.80
1.0	0.75	39.08	39.09	39.09	34.95	34.93	34.93
0.75	1.0	39.98	39.98	39.98	36.48	36.45	36.45
1.5	1.25	41.07	41.06	41.06	38.28	38.26	38.26
1.25	1.5	42.55	42.53	42.53	39.13	39.12	39.12
2.5	1.0	39.98	39.98	39.98	36.48	36.45	36.45
1.75	1.75	43.65	43.64	43.64	40.29	40.27	40.27
1.5	2.0	44.47	44.46	44.46	41.79	41.76	41.76

从表 3 和图 8 可看出,采用不同密钥对块 1 和块 2 进行加密,重建图像质量能基本保持,且增大了保密性。

表 3 正确密钥、密钥出错及使用不同密钥对重建图像质量(单位 PSNR)影响(上下文修正加密算法)

码率	无密钥错误	块 1 密钥错误	块 2 密钥错误	块 1、2 采用不同密钥
0.5	36.81	17.91	9.68	36.81
1.0	39.98	17.90	9.69	39.98
1.5	42.54	18.30	9.69	42.54
2.0	44.46	18.19	9.69	44.46



(a) 块1密钥出错 (b) 块2密钥出错 (c) 块1、2采用不同密钥正确解码

图8 编码码率为R=2.0时,不同密钥下的解码

5 结束语

采用自适应算术编码,相对于区间分裂的联合算术加密而言,所提出的图像联合压缩加密有更好的安全性。在此基础上对图像进行分块处理,可以灵活设置不同的密钥对图像进行加密,从而满足不同级别用户的需要,且在所提出的算法之上提高了安全性能。

参考文献:

[1] KIM H, WEN J T, VILLASENOR J D. Binary arithmetic coding with key-based interval splitting [J]. IEEE Trans on Signal Process Letter, 2006, 13(2): 69-72.

[2] BOSE R, PATHAK S. A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system [J]. IEEE Trans on Circuits and Systems I: Regular Papers, 2006, 53(4): 848-857.

[3] MAO Yi-nian, WU Min. A joint signal processing and cryptographic approach to multimedia encryption[J]. IEEE Trans on Image Processing, 2006, 15(7): 2061-2075.

[4] KIM H, WEN J T, VILLASENOR J D. Secure arithmetic coding[J]. IEEE Trans on Signal Process, 2007, 55(5): 2263-2272.

[5] KATTI R S, SRINIVASAN S K, VOSOUGHI A. On the security of randomized arithmetic codes against ciphertext-only attacks[J]. IEEE Trans on Information Forensics and Security, 2011, 6(1): 19-27.

[6] SHAPIRO J M. Embedded image coding using zerotrees of wavelet coefficients[J]. IEEE Trans on Signal Processing, 1993, 41(12): 3445-3462.

[7] SUN Hung-min, WANG King-hang. Designing an arithmetic code for multimedia files compression and encryption[C]//Proc of the 2nd International Workshop on Computer Science and Engineering. 2009: 444-448.

[8] 栗风永,徐江峰. 基于 Hush 系统和多混沌系统的图像加密算法[J]. 计算机工程与设计,2010,31(1):141-144.

[9] 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.

[10] 段黎力,廖晓峰,向涛. 基于 Markov 性质的一阶安全算术编码及应用[J]. 物理学报,2010,59(10):6744-6751.

[11] 邓家先,吴成柯,陈军. 基于率失真斜率提升的干涉多光谱图像压缩[J]. 光学学报,2004,24(3):299-303.

[12] 刘号,董育宁. 基于 SPIHT 的 ROI 图像压缩编码新算法[J]. 南京邮电大学学报:自然科学版,2011,31(1):70-75.

[13] 杨华千,了晓峰,WONG K W,等. 基于 SPIHT 的图像加密与压缩关联算法[J]. 物理学报,2012,61(4):040505-1.