doi:10.3788/gzxb20134201.0121

基于改进零树编码的图像联合压缩加密算法

邓家先,任玉莉
(海南大学 信息科学技术学院,海口 570228)

摘 要:在认真研究算术编码和算术加密的基础上,提出了一种基于改进零树编码的图像联合压缩加密算法.使用密钥对图像压缩产生的原始上下文和原始判决进行修正,实现了图像联合加密.阐述了上下文修正和判决修正算法的规则,对其安全性进行分析.结合比特平面编码技术,可以使用不同密钥对不同小波分辨率的系数分别加密,实现分辨率选择性加密,以满足不同应用需求.对零树编码进行改进,加入自适应算术编码,并对联合压缩加密算法进行仿真.结果表明:相对原始图像压缩算法而言,所提出的图像联合压缩加密算法具有基本相当的压缩效率;相对区间分裂的联合加密算法而言,所提出算法具有更好的安全性.

关键词:图像压缩;改进零树编码;联合压缩加密;算术加密;渐进性选择性加密
中图分类号:TN919.81 **文献标识码**:A **文章编号**:1004-4213(2013)01-0121-6

Image Joint Compression-encryption Algorithm Based on Improved Zero-tree Coding

DENG Jia-xian, REN Yu-li
(*College of Information Science and Technology, Hainan University, Haikou* 570228, *China*)

Abstract: On the basis of careful research on arithmetic coding and arithmetic encryption, a kind of image joint compression encryption algorithm based on improved zero-tree coding is proposed, where a key is used to modify the original context and the original decision produced in the process of image compression, and the image joint compression-encryption is realized in this way. In this work, the rule of the context modification and the decision modification algorithm is discussed and its security is analyzed. In order to meet different application requirements, different keys are used to encrypt separately the different wavelet resolution coefficients during bit-plane coding, so the resolution selective encryption is realized. Moreover, the Zero-tree coding was improved, and adaptive arithmetic coding is introduced to the improved Zero-tree coding, and then joint compression-encryption algorithm proposed is simulated. The simulation results show that the proposed image joint compression-encryption algorithm has the same compression efficiency compared with the original image compression algorithm; and the proposed algorithm has better security than the joint compression-encryption algorithm based on the interval splitting.

Key words: Image compression; Improved zero-tree coding; Joint compression-encryption; Arithmetic encryption; Progressive selective encryption

0 引言

随着信息理论与技术的发展,国际上出现了一种新的趋势,将加密算法融合到图像数据压缩的算法[1-3]中,在对图像数据进行熵编码的同时实现数据加密,这种方法称之为图像联合压缩加密[4-6](Joint Compression-Encryption).有些学者使用多种Huffman树实现图像联合压缩加密,还有部分研究者使用算术编码进行联合压缩加密[1,3,7],即利用密钥对算术编码的区域分裂进行控制,从而实现图像联合压缩加密.

国内外关于算术加密主要集中在两个方面,一

第一作者:邓家先(1964—),男,教授,主要研究方向为数字图像处理和自适应信息处理.Email:jxiandeng@126.com
导师(通讯作者):任玉莉(1987—),女,主要研究方向为数字图像处理.Email:haida_yuli@163.com
收稿日期:2012-06-25;**录用日期**:2012-08-24

种是讨论纯粹的数据加密问题[1-2]；另一种是讨论各种简单模型下的算术压缩加密问题[1,7-8]. 他们所使用的算术编码模型相对比较简单，比如假设信源输出符号的概率分布是固定的，或者是简单的马尔科夫信源[9]，从而便于得出有意义结论. 但是在不进行输入数据的置换或者密文置换条件下，简单的区间分裂算术加密是很容易遭到攻击[2].

目前，图像编码大都使用基于小波变换的比特编码技术[10-12]，主要有块编码[13-14]、集合树编码[15]或者树块编码. 这些算法利用子带系数之间的相似性，或者相邻系数甚至子带系数之间相关性进行编码，取得了好的压缩效果. 使用算术编码器可以对这些编码算法产生的判决进行熵编码，进一步提高编码效率. 在图像压缩领域，所使用的算术编码大多是Q编码器、QM编码器、MQ编码器，这几种算术编码器都是假设信源是马尔科夫信源，因此算术编码都是自适应的. 图像压缩领域取得的研究成果表明，自适应算术编码器能够实现高效数据压缩[11-13].

目前，国内外从事图像联合压缩加密的研究者原来主要从事加密研究，研究成果的理论意义是不言而喻的. 但由于采用区间分裂的算术编码实现联合压缩加密，其密文安全性同样存在不足，容易受到攻击. 此外，由于算术编码所使用的概率划分是固定的，与实际图像数据分解后系数的概率分布不同，不利于取得好的压缩效果.

从图像压缩研究者的角度来看，基于区间分裂的图像联合压缩加密所使用的算术编码器与实际图像数据压缩中所使用的算术编码器不同. 图像压缩广泛使用自适应算术编码器，更利于图像数据压缩；而在算术加密中，往往采用比较简单的算术编码模型和算法，主要进行算术加密方面的理论研究，而与实际应用存在一定的差距，不利于提高图像压缩效率[1].

针对图像联合压缩加密所使用的算术编码比较简单，其安全性难以保证，难以取得好的压缩效率等不足，本文提出一种基于改进零树编码的图像联合压缩加密算法，对零树编码进行改进，引入自适应算术编码，并利用给定密钥对原始上下文和判决进行修正，从而实现联合压缩加密. 所设计算法能够在实现图像数据压缩的同时，也实现了算术加密；加密算法对压缩效率几乎没有影响；能够实现分辨率选择性加密，即不同分辨率使用不同密钥，这样就给不同权限用户提供不同质量的重建图像；由于所使用的算术编码是自适应的，相对区间分裂的算术编码而言，所提出算术加密算法的密文安全性更好.

1 改进零树编码

零树编码是由Shapiro提出了一种基于小波变换和比特平面编码方法[15]，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学术地位. 以三级小波变换为例，LL_3 子带的一个系数对应 HL_3、LH_3、HH_2 子带系数，除了 LL_3 子带之外，每个三级子带系数对应二级子带4个系数，而每个二级子带系数对应一级子带4个系数，从而构成一棵树，称之为零树，如图1.

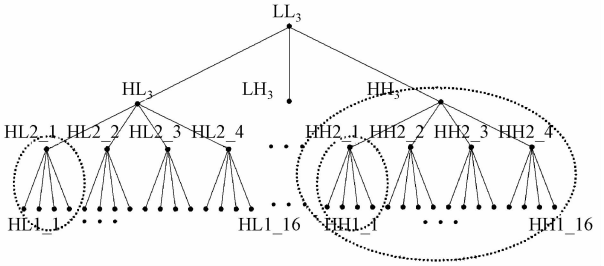

图1 零树结构

Fig. 1 The structure of zero-tree

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 LL_3 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.

为了利用算术编码对数据进行进一步压缩，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2所示.

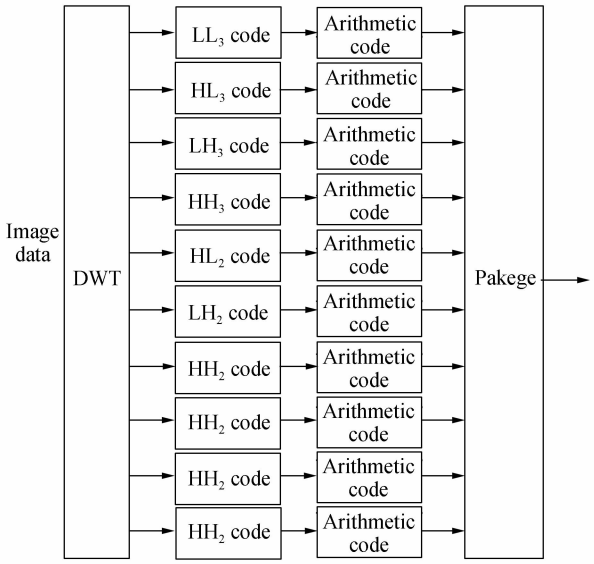

图2 改进零树编码

Fig. 2 Improved zero-tree coding

在同一比特平面内，按照图2中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.

LL_3 编码是对 LL_3 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_1 和判决 D_1，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 HL_3、LH_3、HH_3 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. 比如 HL_3 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.

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. 由于比特平面编码产生判决分为集合判决和系数判决，为了与之相对应，上下文也分为集合上下文、系数上下文两大类.

集合上下文可以根据同分辨率相邻集合重要性产生，也可以进行扩展，比如将其他分辨率相应集合的重要性与当前分辨率集合重要性一起，共同形成集合上下文. 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 个邻居可以产生 256 种上下文，经过合并形成 4 种集合上下文. 图 3 为集

E_5	V_0	E_1
H_0	X	H_1
E_2	V_1	E_3

图 3　集合邻居

Fig. 3　The neighbor of set

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，H_0，H_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CXs为

$$CXs=(V_0|V_1|H_0|H_1)\times 2+(E_0|E_1|E_2|E_3) \quad (1)$$

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

与优化截断的嵌入式分块编码(Embedded Block Coding with Optimized Truncation，EBCOT)算法一样，系数上下文进一步细化分为零编码上下文、幅值细化上下文、符号编码上下文，其上下文计算采用 EBCOT 中的方法[10-14]，这里不再赘述.

2　图像联合压缩加密

算术编码器实际是将给定序列映射为一个概率子区间，编码器输出的码字就是对应概率子区间的一种描述. 对于简单的基于区间分裂的算术编码而言，输入的二进制判决 0、1 的概率是固定的，通过改变判决就可以实现算术加密. 而对于自适应算术编码器而言，其输入包括上下文和判决两部分，不同上下文对应判决的初始分布不完全相同，而且后续输入判决的条件概率分布也不完全相同. 对于给定的序列，如果上下文不同，对应的概率子空间也不相同，编码输出的码字也不相同. 如果改变给定序列中的任何一个上下文或者判决，就会导致概率子空间的不同，并会对后续判决的条件概率分布产生影响.

自适应算术编码不仅能够有效提高编码效率，同时也可以用来进行算术加密. 利用同一算术编码器实现数据压缩和数据加密，这种方法称为联合压缩加密. 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.

基于判决修正的算术加密原理如下：

设 key 表示加密密钥，$D_1=(d_1,d_2,\cdots d_N)$ 表示编码产生的长度为 N 的二进制判决矢量，定义一种运算

$$D_1=f(D,\text{key}) \quad (2)$$

其中 $D=(d_{11},d_{12},\cdots d_{1N})$ 也是长度为 N 的矢量，且其中每个元素仍然是二进制的.

利用密钥对比特平面编码产生的二进制判决运算，使得修正后的部分二进制判决与原来的二进制判决不同，如果系统解码使用的密钥与编码使用密钥不同，则会出现译码错误，从而实现数据加密.

设 key_1 表示解密密钥，$\hat{D}=(\hat{d}_1,\hat{d}_2,\cdots\hat{d}_N)$ 表示解码后的判决矢量，当 $\text{key}_1=\text{key}$ 时，则 $\hat{D}=D$. 也就是说，如果解密时使用正确密钥，则应当正确重建原始判决序列，显然就对式(2)定义的运算提出了要求，满足

$$\hat{D}=f^{-1}(D_1,\text{key})=f^{-1}(f(D,\text{key}),\text{key})=D \quad (3)$$

其中 f^{-1} 为式(2)对应的逆运算，这就要求式(2)定义的运算对正确密钥是可逆的.

基于上下文修正的加密原理如下：

设 key 表示加密密钥，CX 表示比特平面编码产生的原始上下文，对应取值范围为 $(m,m+1,\cdots,m+L)$，修正后上下文为 CX_1，对应取值范围为 $(m,m+1,\cdots,m+L')$，上下文修正可以表示为

$$CX_1 = g(CX, \mathrm{key}, n) \tag{4}$$

其中 $g(,)$ 表示定义的某种运算，n 表示该类上下文出现的顺序，L，L' 分别表示原始上下文和修正上下文的种类. 如果加密、解密过程中，对应比特平面编解码产生的上下文相同，且使用相同密钥，修正上下文使用相同的变换，则送往算术编码器和算术解码器的上下文也相同，不会产生上下文引起的解密错误. 也就是说，加密、解码使用相同的运算，所以式(4)不需要是可逆的.

自适应算术编码使用的各类上下文和对应判决共同确定了算术编码的概率跳转规律. 如果某类上下文的初始该类分布相同(大部分是如此)，输送到算术解码器的上下文与编码使用的上下文是同类上下文之间的一一映射，则算术解码的结果是正确的，即不能实现算术加密. 自适应算术编码器的这类特点决定了式(4)不能是一种 key 和 CX 的线性运算. 比如，式(4)将所有编码产生的类别为 5 的上下文都映射为 3，且 3，5 是同一类上下文，编码初始概率分布相同，则这类运算不能实现加密.

自适应算术编码使用的各类上下文范围一定，比如某类上下文范围为 $(m, m+1, \cdots, m+L_m)$，式(4)运算的结果应当在该范围内，即满足

如果

$$m \leqslant CX \leqslant m+L$$

则

$$m \leqslant CX_1 \leqslant m+L_m.$$

如果超出自适应算术编码使用的某类上下文范围，则进入其他类别的上下文范围，不同类别的上下文所对应的初始概率分布不同，条件概率的跳转规律也不相同，进行联合压缩加密时，可能会导致重建图像质量下降.

综合上述讨论，得出上下文修正的算术加密算法需要满足：

1)对应给定的一种上下文，不同时刻修正算法不能是一种一一映射关系，也就是说，给定 CX 和 key，对于不同的 n，式(4)运算的修正上下文不能总是固定值，即 CX_1 不是 CX 和 key 的线性运算，否则不能实现算术加密；

2)修正上下文不能超过算术编码所对应类型的范围，否则可能会导致联合压缩的效率下降；

3)上下文的运算可以是不可逆的，算术编码和解码使用相同的运算规则即可保证解密不会产生上下文引起的解密错误.

基于上下文、判决修正的联合压缩加密原理如图 4. 原始图像数据经过变换，将系数的相关冗余映射为系数的统计冗余；变换后的系数进行比特平面

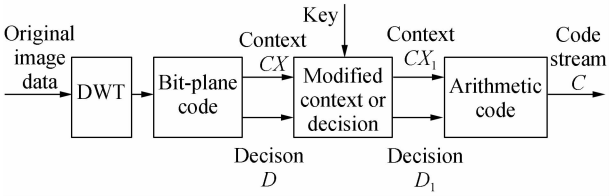

图 4 上下文、判决修正的联合压缩加密原理框图

Fig. 4 The diagram of image joint compression-encryption algorithm based on context and decision modification

编码，产生原始上下文 CX 和原始判决 D，密钥 key 对原始上下文和原始判决进行修正，产生修正上下文 CX_1 和修正判决 D_1，并送往算术编码器.

本文中，判决修正采用简单的异或，对密钥 key 进行循环移位得到密钥 key_1，即首先利用 key_1 的最低位与原始判决进行异或运算，然后密钥循环移位一次，供下一次判决修正使用.

上下文修正算法是，对密钥 key 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，对于范围为 $(m, m+1, \cdots, m+L)$ 原始上下文的计算

$$CX_1 = m + (d_k + CX) \bmod (L_m) \tag{5}$$

其中 mod() 表示模运算. 修正后的上下文范围为 $(m, m+1, \cdots, m+L_m)$. 这种上下文修正方法可以满足上文提出的上下文修正规则.

结合讨论的改进零树算法，每个小波子带的系数独立进行联合压缩加密，LL 子带使用单独密钥，其他同级别子带使用相同密钥，这样就可以实现分辨率选择性加密.

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，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就有可能出错，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.

如果系统解密时出现判决解密错误，可能导致后续的上下文错误，以及条件概率和累计概率错误，这两种情况都会导致连续解密错误.

从上文分析可知，由于自适应算术编码的概率跳转规律复杂，而区间分裂的概率分布是固定的，因此，相对区间分裂的算术编码而言，基于上下文修正和判决修正的联合压缩加密算法安全性更好.

3　实验结果与分析

使用图像 GoldHill 对所提出算法进行仿真，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(Peak Signal to Noise Ratio, PSNR)如表 1 所示. 从中可以看出，当单独使用上下文修正时，重建图像质量与原始算法的基本相同；当使用判决修正时，相对原始算法而言，重建图像质量有所下降，下降幅度达 1 dB 以上；当上下文和判决联合修正时，重建图像质量也有所下降，下降幅度也达到 1 dB 以上.

表 1　原始算法与联合压缩加密重建图像质量比较(单位 dB)

Table 1　The reconstructed image quality comparison original algorithm and joint compression-encryption algorithm (unit: dB)

Rate	Original compression algorithm	Context modify	Decision modify	Joint context and decision modify
0.50	32.07	32.05	30.09	30.56
0.75	34.00	34.01	31.93	32.63
1.00	35.20	35.20	33.88	34.15
1.25	36.86	36.84	34.99	35.36
1.50	38.04	38.02	36.45	37.03
1.75	38.88	38.86	37.86	38.06
2.00	39.96	39.90	38.60	38.87

这就表明，当使用上下文修正时，如果遵循上文给出的原则选择修正上下文范围，联合压缩加密与原始算法具有同样的压缩效果. 由于判决修正对原始判决的条件概率分布扰乱程度较大，因此重建图像质量下降较为严重；同理，当上下文和判决联合修正时，其原理与单独判决修正相同.

但是，上下文和判决联合修正时，理论上其安全性相对上下文修正更好；而上下文修正的运算比判决修正的运算更加复杂，基于上下文修正的联合压缩加密比基于判决修正的安全性要好.

使用 lena 图像测试分辨率选择性加密的效果. 与小波变换分辨率相对应，最低分辨率的四个子带(LL、HL、LH、HH)使用相同密钥，称为三级子带密钥，而同分辨率子带常用相同密钥，分别称之为二级子带密钥、一级子带密钥.

密钥错误处理时，解码处理方法是使用错误密钥进行解码. 不同分辨率解密密钥出错时，重建质量(PSNR)随码流的变化如表 2～4 所示. 其中表 2、3、4 是各个分辨率密钥出错时，上下文修正、判决修正、上下文和判决联合修正算法的重建图像质量随码率变化情况；表 3 是单独使用判决修正算法，密钥出错时，重建图像质量随码率变化情况，从表中可以看出一些共同特点，当无密钥出错时，重建图像质量随着码率增加而增加；一旦密钥出错，重建图像质量是随着码率增加而略有降低. 某级子带密钥出错时，随着码率的增加，尽管高级子带重建数据质量增加，但密钥出错对应子带以及更低级子带重建系数产生错误更加严重，经过小波逆变换，错误系数引起的图像数据错误更加严重，从而导致重建图像质量随着码率增加而略有降低.

表 2　密钥出错对重建图像质量(单位 PSNR)影响(上下文修正)

Table 2　The impact of image reconstructed quality in error key (context modify)

Rate	Non-key-error	First-level band key error	Second-level band key error	Third-level band key error
0.50	36.02	29.74	24.17	9.24
0.75	37.86	29.79	23.99	9.22
1.00	39.17	29.73	23.88	9.23
1.25	40.08	29.81	23.79	9.23
1.50	41.19	29.84	23.77	9.23
1.75	42.75	29.83	23.79	9.24
2.00	43.43	29.82	23.80	9.24

表 3　密钥出错对重建图像质量(单位 PSNR)影响(判决修正)

Table 3　The impact of image reconstructed quality in error key (decision modify)

Rate	Non-key-error	First-level band key error	Second-level band key error	Third-level band key error
0.50	33.94	30.97	21.00	9.23
0.75	35.87	31.15	20.57	9.23
1.00	37.50	31.00	20.41	9.21
1.25	39.01	30.85	20.37	9.22
1.50	39.83	30.72	20.33	9.21
1.75	40.84	30.59	20.31	9.21
2.00	42.17	30.54	20.30	9.21

表 4　密钥出错对重建图像质量(单位 PSNR)影响(上下文和判决联合修正)

Table 4　The impact of image reconstructed quality in error key (joint context and decision modify)

Rate	Non-key-error	First-level band key error	Second-level band key error	Third-level band key error
0.50	33.47	28.72	20.94	9.21
0.75	36.2	28.5	20.68	9.22
1.00	38.06	28.49	20.62	9.22
1.25	39.21	28.47	20.61	9.22
1.50	40.09	28.51	20.6	9.23
1.75	41.17	28.52	20.59	9.23
2.00	42.65	28.53	20.60	9.23

从表中同样可以看出，不同级别子带密钥错误对重建图像质量得影响不同. 由于一级子带系数对重建图像质量的贡献较低，当其出现密钥错误时，对重建质量得贡献仅仅限于该子带本身，从 2 表中可以看出，重建图像质量在 29.8 dB 左右，随着码率增

加，下降幅度也不同. 这是因为随着码率增加，重建高频子带系数的数量增加，而由于密钥出错，这些错误重建系数也相应增加，从而影响了重建图像质量.

二级子带密钥错误时，二级子带重建系数错误，可能导致集合重要性出错，对一级子带系数重建带来影响，导致一级系数重建产生错误，即出现重建系数错误向低级子带扩散. 所以二级子带密钥错误，重建图像质量下降到 24 dB 左右. 同理，三级子带密钥错误时，重建图像质量约为 9 dB，质量下降更为严重.

同理，从表 3 和表 4 可以看出，当密钥出错时，重建图像质量也相应降低，并与上下文修正密钥出错具有相同的变化规律. 图像质量下降的基本原理与上下文修正的原理相同.

图 5 是从重建图像中截取的子图像，可以看出，当二级、三级子带密钥错误时，重建图像视觉效果严重下降，而一级子带密钥错误时，尽管图像质量有所下降，但视觉效果并不是特别明显. 而随着子带等级增加，其密钥出现错误时，重建图像中视觉效果下降. 当三级子带密钥出错时，视觉上从重建图像得不到原始图像的信息.

图 5 重建图像

Fig. 5 Reconstructed image

4 结论

通过上文的理论分析和实验结果可以得出：1）使用上下文修正、判决修正都可以实现图像联合压缩加密；2）对于上下文修正而言，只要按照论文提出的规则选择参量，可以保证联合压缩加密的重建图像质量相对原始压缩算法的质量基本不变；3）能够实现图像的分辨率选择性加密；4）由于采用自适应算术编码，相对区间分裂算术加密，所提出联合压缩加密算法的条件概率分布的复杂度更高，因此密码安全性更高；5）当密钥正确时，相对原始算法而言，上下文修正的联合压缩加密算法的重建图像质量基本不变；而判决修正或者上下文和判决联合修正的联合压缩加密算法的重建图像质量均有所下降，从实验数据可以看出，下降幅度达 1 dB 以上；6）从安全性而言，上下文和判决联合修正的性能最好.

参考文献

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

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

[3] WU C, KUO C C J. Design of integrated multimedia compression and encryption systems[J]. *IEEE Transactions on Multimedia*, 2005, **7**(5): 828-839.

[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] BOSE R, PATHAK S. A novel compression and encryption scheme using variable model arithmetic coding and couple chaotic system[J]. *IEEE Transactions on Circuits System I*, 2006, **53**(4): 848-857.

[7] MAO Y, WU M. A joint signal processing and cryptographic approach to multimedia encryption[J]. *IEEE Transactions on Image Processing*, 2006, **15**(7): 2061-2075.

[8] ZHENG Hao-ran, JIN Chen-hui. An attack with know plaintexts to encryption algorithm based on arithmetic coding [J]. *Journal of China Institute of Communications*, 2003, **24**(11): 73-78.
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.

[9] DUAN Li-li, LIAO Xiao-feng, XIANG Tao. Image encryption based on arithmetic coding with order-1 Markov model[J]. *Acta Physica Sinica*, 2010, **59**(10): 6744-6751.
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.

[10] DENG Jia-xian, WU Cheng-ke, CHEN Jun. Multi-spectral image compression based on rate-distortion slope oifting[J]. *Acta Optica Sinica*, 2004, **24**(3): 299-303.
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.

[11] ISO/IEC JTC 1/SC 29/WG1 FCD 14495 public draft[OL]. (1997-06)[2012-06-02]. http://www.jpeg.org/public/jpeglinks.htm.

[12] TAUBMAN D. High performance scalable image compression with EBCOT[J]. *IEEE Transactions on Image Processing*, 2000, **9**(7): 1151-1170.

[13] TAUBMAN D, ORDENTLICH E, WEINBERGER M, *et al*. Embedded block coding in JPEG2000 [J]. *Signal Processing on Image Communication*, 2002, **17**(1): 49-72.

[14] CHRISTOPOULOS C, ASKELÖF J, LARSSON M. Efficient methods for encoding regions of interest in the upcoming JPEG2000 still image coding xtandard[J]. *IEEE Signal Processing Letters*, 2000, **7**(9): 247-249.

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