基于四叉树的多媒体安全编码方案

廉士国 王执铨 李忠新
(南京理工大学自动化系,南京 210094)

摘 要 由于图像、音频、视频等媒体数据具有数据量大,实时性要求高等特点,这对于加密算法也提出了相应的要求,而且由于采用传统的基于数论的加密算法对数据完全加密不能满足实时性要求,因此产生了对部分加密算法的研究,但这些算法也不能完全保证数据格式不变和压缩比不变等更高的要求;如果将压缩编码和加密过程相结合,则既能满足实时性要求,又能保持数据格式不变。鉴于四叉树结构常被应用于图像编码中,为此提出了两种四叉树置乱算法,并将其用于四叉树编码、小波零树编码、基于四叉树的分形编码等图像和视频编码中。理论分析和实验结果表明,由于这些算法将加密与编码过程相结合,因此具有以下优点:具有较高的安全性,且加密效果好;不仅能保持编码格式不变,而且便于对数据的直接操作;既能保持压缩比不变,又不增加额外数据;具有较快速度,能满足实时性要求等。

关键词 图像加密 四叉树编码 多媒体加密
中图法分类号: TP309.7 TN919.81 **文献标识码**: A **文章编号**: 1006-8961(2004)03-0353-07

Secure Multimedia Encoding Schemes Based on Quadtree Structure

LIAN Shi-guo, WANG Zhi-quan, LI Zhong-xin
(*Department of Automation, Nanjing University of Science and Technology, Nanjing* 210094)

Abstract For multimedia data is often voluminous and requires real-time operations, multimedia encryption algorithms should meet extra requirement compared with textual data encryption algorithms. Traditional algorithms such as DES, RSA, can't meet some real time requirement. Some selective encryption algorithms can't completely keep the file format and compression ratio unchanged. In order to meet such requirement, the algorithms should combined encryption process with encoding process. Due to the wide application of quad-tree structure in image or video encoding, two types of quadtree permutation algorithms are proposed here. They are used in quadtree-based image encoding, wavelet zerotree encoding (EZW, SPIHT), and quadtree-based fractal image or video encoding. The encryption algorithms combine encryption with compression, and have some advantages. Firstly, it is secure, and the encryption result is too confused to be understood. Secondly, it keeps the file format unchanged, and thus it is easy to operate compressed and encrypted data directly. Thirdly, it keeps the compression ratio unchanged, that is to say that the encryption operations do not produce extra data. Lastly, it is fast and can meet real-time requirement.

Keywords image encryption, quadtree encoding, multimedia information encryption

1 引 言

自从计算机产生以来,信息安全一直是人们关注的话题,而作为它的一个重要分支,信息加密技术也得到了广泛研究。传统的基于数论的密码,因其具有安全性高的特点,故已经获得了广泛的应用,尤其是在网络普及、信息发达的今天,网络上传输的各种有关经济、政治或者军事等敏感性数据,都离不开数据加密技术。随着多媒体技术的发展,数据格式已经不仅仅是文本了,由于图像、音频、视频等数据都获得了广泛应用,因此,数据加密的范围也扩大了。与

基金项目:博士点基金项目(20020288025);江苏省自然科学基金项目(BK2001054)
收稿日期: 2003-05-29;改回日期:2003-10-08

传统的文本等数据不同，图像、视频等多媒体数据具有数据量大、实时性要求高等特点，而传统的基于数论的密码则由于计算复杂性高，不能很好地满足实时性要求，因此，对于多媒体数据加密，需要有新的合适的算法。

在过去 10 年间，针对图像、视频的加密方法得到了很好的研究。这些算法大概可以分为以下 3 类：(1)完全加密方法，这类方法是将多媒体数据视为一般的文本数据，通常使用传统密码来直接加密数据，其虽然安全性很高，但是由于改变了原来的数据格式，同时花费的加解密时间较多，因此较难满足实时性要求，例如，使用混沌方法加密图像数据[1]和使用 DES 算法加密视频数据[2]等；(2)部分加密算法，这类方法仅加密多媒体数据流的一部分数据，其与完全加密方法相比，虽然安全性较低，也会不同程度地改变数据结构，但却可以获得较高的加密速度，如，VEA 算法[3]就是用 DES 密码只加密一半数据，另一半数据是原始两半数据的简单异或的结果。在对 MPEG 或 H.263 等视频文件的加密[4]中，只加密其中的 I 帧或 I 块等；(3)加密与压缩编码相结合的算法，这类算法将加密过程与压缩编码过程相结合，同步完成，这样，由于既保持了较快的加解密速度，又保持了数据格式的不变性，且而利于数据在不解密情况下的可操作性，且这类算法的安全性与具体的加密和压缩过程有关，例如使用修改的 DCT 变换来代替标准的 DCT 变换[5]，由于修改后的变换所含有的参数可以用作密钥，因此可将其用于图像、音频和视频的变换编码中来实现压缩和加密；又如 MHT (multi-huffman trees) 方法[6]是采用多个 Huffman 树来编码，同时每棵 Huffman 树都有相应的多个变异树，其加密过程是通过密钥来控制 Huffman 树的选择。MSI (multi-state indexes) 方法[6]是在自适应算术编码过程中，通过密钥来控制编码区间的选择和编码区间范围的改变。

可见，将加密与压缩编码相结合是多媒体数据加密的新方向。如今，四叉树结构被广泛应用于图像和视频编码中，如四叉树编码[7~9]、小波零树编码 (EZW[10] 和 SPIHT[11])、基于四叉树的分形编码[12~14]等。为此，本文提出利用四叉树置乱来实现图像或视频编码的方法。本文首先对四叉树的置乱方法做了深入分析，并就基于四叉树的几种压缩编码方法(四叉树编码、小波零树编码和基于四叉树的分形编码等)提出了相应的加密方案；然后就这 3 类编码方法分别给出了增加安全性的方法；最后通过实验证明了此类算法具有速度快、保持数据格式不变、保持压缩率不变等优点。

2 四叉树

如今，二叉树已广泛应用于计算机数据处理中，四叉树与二叉树相似，也已经得到了广泛的应用。由于其具有与平面 4 个方向相一致的特点，因此很适合应用于图像编码，如四叉树图像压缩编码、小波零树编码等。在四叉树中，第 1 个节点称为树根，而没有子节点的节点称为叶子节点，除树根和叶子节点之外的节点称为中间节点，其每一中间节点(包括树根)都有 4 个子节点。四叉树的高度定义为从树根到最低层树叶的层数，树根的高度为零。一个典型的四叉树如图 1 所示。其中，R 表示树根，I 表示内部节点，L 表示叶子节点，H 为树的高度。对于一般的四叉树，可用表示四叉树的叶子节点数，用表示内部节点数，则它们的关系为

$$M = 3N + 1 \tag{1}$$

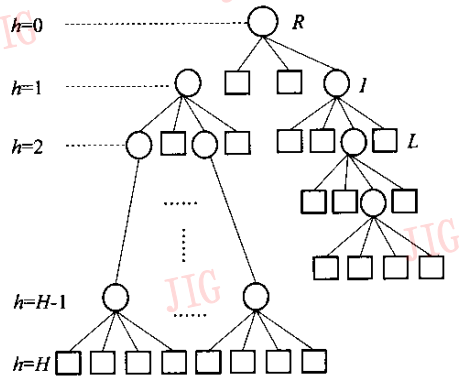


图 1 四叉树结构图

与二叉树中定义的完全二叉树相似，本文也在此处定义完全四叉树，即，所有叶子节点都出现在 H 高度上的四叉树是完全四叉树。此时，叶子节点数与树的高度的关系满足

$$M = 4^H \tag{2}$$

3 四叉树的置乱

在四叉树中，每一个父节点都有 4 个子节点，当这 4 个子节点具有不同的加权时，则它们的位置就有所区别了，例如，在四叉树分块压缩编码中，每个子节点代表不同的图像块；在小波零树压缩编码中，

每个子节点则代表不同的小波变换系数,由于置乱四叉树的各个节点改变了空间域或频率域的图像参数,从而会改变原始图像。这样,足够的置乱空间就可以用来加密图像和视频数据,这正是本文分析四叉树置乱的原因。以下给出两种四叉树置乱方法(简称置乱方法)。

3.1　第 1 种四叉树置乱方法

这种置乱方法是将同属于一个父节点的 4 个子节点置乱,而保持节点间父子关系不变。对于这种置乱算法,可给出以下定理。

定理 1　高度为的四叉树,若采用在同属于一个节点的 4 个子节点间进行置乱的方法,则能够产生不同的四叉树个数(即置乱空间)为

$$K_H^{\text{tree1}} = \prod_{h=1}^{H} 24^{N_{h-1}} \tag{3}$$

其中,H 表示四叉树的高度,N_h 表示 h 高度上的内部节点的个数,K_H^{tree1} 表示高度为 H 的四叉树,采用此种置乱方法置乱获得的不同的四叉树的个数即其置乱空间。

证明　一个内部节点的 4 个子节点的置乱种类为 4!。设在 h 高度上有 N_h 个内部节点,则在 $h+1$ 高度上的置乱空间为

$$K(h) = (4!)^{N_h} \tag{4}$$

如图 1 所示,若在 $h=1$ 高度上有 2 个内部节点,则在 $h=2$ 高度上有 $(4!)^2$ 种置乱四叉树。因为按照以上置乱方法,每个高度上的置乱四叉树都不会重复,所以,按以上方法将整个四叉树置乱的置乱空间为

$$K_H^{\text{tree1}} = \prod_{h=1}^{H} K(h) = \prod_{h=1}^{H} 24^{N_{h-1}} \tag{5}$$

由定理 1 可得,高度为 H 的四叉树,其最少可能的置乱空间为 24^H,即,每个高度上只有一个内部节点($N_h=1$,其中 $h=0,1,\cdots,H-1$)。

3.2　第 2 种四叉树置乱方法

这种方法是将同一高度的节点(包括叶子节点和内部节点)进行置乱。对于这种置乱算法,可给出以下定理。

定理 2　高度为的四叉树,若采用在同一高度上的所有节点间进行置乱的方法,则能够产生不同的四叉树个数为

$$K_H^{\text{tree1}} = \left(\prod_{h=H_0}^{H} \frac{N_h + M_h)!}{N_{h-1}!} \right) \cdot (N_{H_0-1}!) \tag{6}$$

其中,N_h 表示 h 高度上的内部节点个数,M_h 表示 h 高度上的内部节点个数,H_0 表示本高度以上(不包含本高度)的任何高度上都没有叶子节点。如图 1 所示的四叉树中,$H_0=1$。K_H^{tree2} 表示高度为 H 的四叉树采用此种置乱方法置乱获得的不同的四叉树的个数即其置乱空间。

证明　设在 h 高度上有 N_h 个内部节点和 M_h 个叶子节点,则在 h 高度上的置乱空间为

$$K(h) = \frac{(N_h + M_h)!}{N_{h-1}!} \tag{7}$$

而将整个四叉树置乱的置乱空间为

$$K_H^{\text{tree2}} = \prod_{h=H_0}^{H} K(h) = \left(\prod_{h=H_0}^{H} \frac{(N_h + M_h)!}{N_{h-1}!} \right) \cdot (N_{H_0-1}!) \tag{8}$$

由定理 2 得,在这种置乱方法下,高度为 H 的四叉树,其最少可能的置乱空间与第 1 种置乱方法类似,均为 24^H,即,每个高度上只有一个内部节点($N_h=1$,其中 $h=0,1,\cdots,H-1$)。

3.3　以上两种四叉树置乱方法的比较

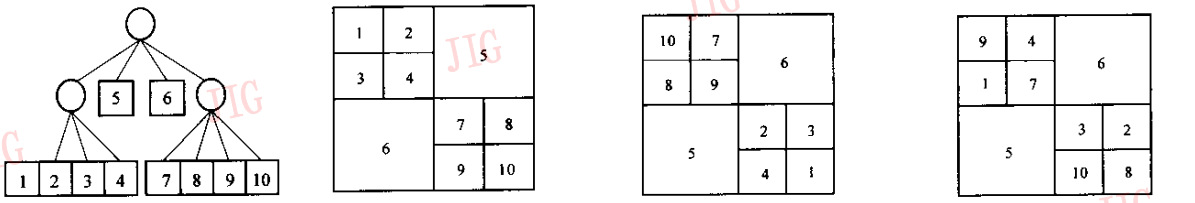
①两种置乱方法的置乱种类都与四叉树的高度有关,即高度越高,叶子节点和中间节点越多,置乱的种类也就越多。

②用在同一高度上所有节点间进行置乱的方法(方法 2)获得的四叉树的种类要比采用在同属于一个父节点的 4 个子节点间进行置乱的方法(方法 1)获得的四叉树的种类多。如果将四叉树置乱方法用于加密,那么,用第 1 种置乱方法加密的穷举空间就小于第 2 种置乱方法。

③采用第 2 种置乱方法的加密效果更好,而且图像恢复也更困难。由置乱结果看,不但第 2 种置乱方法置乱种类多于第 1 种置乱方法,而且,从图像可理解性的角度来看,第 2 种置乱方法使得图像的混乱程度更高,加密效果更好,例如,图 2(a)、图 2(b)所示的图像四叉树分割,经过置乱后的图像如图 2(c)、图 2(d)所示。

从图 2(c)可见,采用第 1 种置乱方法,图像块 1,2,3,4 和 7,8,9,10 只能在各自的四分之一区域的内部进行置乱;而从图 2(d)可见,若采用第 2 种置乱方法,则可以使得图像块 1,2,3,4,7,8,9,10 从原来的四分之一区域移动到另外的四分之一区域,即可在两个四分之一区域内置乱,这样就增加了置乱程度。

④第 1 种四叉树置乱方法由于保持了父节点与子节点之间的父子关系,因此对于某些压缩编码应用,则可以保持某些性质不变,例如,在小波零树编



(a) 四叉树结构 (b) 四叉树对应的分割 (c) 第 1 种方法置乱 (d) 第 2 种方法置乱

图 2 图像四叉树分割和置乱

码中,若保持父节点和子节点的父子关系不变,就可以保持压缩比基本不变。

⑤计算机实现中,第 2 种置乱方法需要的缓存要比第 1 种置乱方法需要的缓存大。

4 基于四叉树的图像编码加密算法

如果认为二叉树是针对一维数据的数据结构,那么就可以认为四叉树是针对二维数据的数据结构,八叉树是针对三维数据的数据结构。四叉树的特点决定了它很适合用于图像分割和编码中,如,直接利用四叉树分块的压缩编码[7]、将小波变换与四叉树相结合的 EZW[10]和 SPIHT[11]编码、将分形编码与四叉树相结合的自适应图像分形压缩编码[12]等。下面将针对这几种编码方法给出相应的加密算法。

4.1 四叉树图像分块压缩加密算法

四叉树图像分块压缩编码是一种无损图像压缩编码方法。它是针对图像中相邻点间具有相关性,即相邻点间具有相似的像素灰度值,将图像进行逐层四叉分解,直至分解得到的各个节点图像块中的像素灰度值唯一为止。由于这样只需要存储每个图像块的位置和一个灰度值即可,从而达到了图像压缩的目的。

对于直接利用四叉树分块压缩编码算法压缩的图像,可使用第 3 节中介绍的第 2 种四叉树置乱方法来加密。由于该图像经四叉树置乱以后,如果树的高度有限,则四叉树的内部节点和叶子节点也会相对较少,因此密钥空间也就减少了。由于这使得破译过程仅仅是穷举四叉树的过程,从而安全性也就大大降低。鉴于这些考虑,在采用第 2 种方法置乱图像后,还需增加扩散环节,即,同时加密叶子节点。所谓加密叶子节点,也就是加密图像块的像素值,这样就可使得破译过程不仅仅是穷举四叉树的过程,还要有破译节点的过程,这就大大增加了破译难度,也就提高了密码强度。例如,假设四叉树的置乱空间为 K_{tree},叶子节点的加密空间为 K_{leave},则密码系统的密钥空间增加为

$$K = K_{\text{tree}} \cdot K_{\text{leave}} \tag{9}$$

其中,叶子节点的加密可以采用传统的加密算法,如流加密算法、DES 加密算法[3]或者混沌流加密算法等。四叉树分块压缩加密系统如图 3 所示。

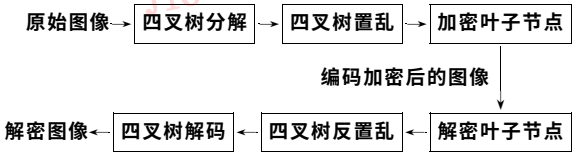


图 3 四叉树图像分块压缩和加密算法流程图

实验结果表明,在进行四叉树分块图像压缩加密编码时,如果图像对应的四叉树高度足够高,如,Lena(256×256)图像对应的四叉树高度为21 834,Boats(256×256)图像对应的四叉树高度为21 761,则其对应的置乱空间分别至少为 $K_{\text{tree}}=24^{21\,834}$ 和 $K_{\text{tree}}=24^{21\,761}$,这对于穷举攻击是困难的。

4.2 小波变换与四叉树相结合的压缩加密算法

小波变换与四叉树相结合的 EZW[10]和 SPIHT[11]编码算法,是利用小波变换后不同频带系数间的幅值相关关系来实现逐层累进编码的。由于这种压缩编码方法具有压缩率高、逐层累进等特点,因此又被推广应用于视频或多频谱图像序列的压缩编码中。

对于小波变换与四叉树相结合的压缩编码算法压缩的图像,可采用第 1 种四叉树置乱方法来进行加密。这是因为,只在同属于一个中间节点的 4 个子节点间进行置乱,由于可以保持节点间的父子关系,从而可保持 EZW 和 SPIHT 编码的压缩比基本不变,否则,采用第 2 种四叉树置乱方法会较大程度地改变压缩比。

对于同一棵四叉树,第 1 种置乱方法的置乱空间明显小于第 2 种置乱方法的置乱空间。为了保持算法的安全性,可同时增加对小波系数符号的加密。同时,因为 EZW 和 SPIHT 编码具有能对符号进行

单独编码的特点，所以由符号加密引起的符号改变不会改变图像编码的压缩比，例如，假设四叉树的置乱空间为 K_{tree}，四叉树个数为 N，叶子节点符号加密的加密空间为 K_{sign}，则密码系统的密钥空间增加为

$$K = (K_{\text{tree}})^N \cdot K_{\text{sign}} \tag{10}$$

其中，叶子节点的符号加密可以采用传统的加密算法，如流加密算法、DES 加密算法或者混沌流加密算法等。该方案如图 4 所示。

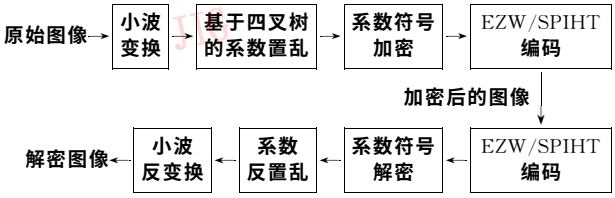


图 4　基于四叉树置乱的 EZW/SPIHT 图像压缩加密编码方案

这类算法的优点是：①置乱空间大，从而对穷举攻击的安全性高；②仅在各个频带的内部置乱，从而增加了利用小波变换的能量集中特性进行统计分析的难度；③由于采用位置置乱与符号加密相结合的方法，从而增加了已知明文攻击的难度。

4.3　基于四叉树分块的分形压缩加密算法

分形图像或视频压缩编码是利用图像的自相似性来实现压缩，且一般是有损编码过程。其常用的方法是先利用图像不同区域间的相似性来将图像分成区块和尺寸更大的域块，然后对于每一个区块，寻找与之最匹配的域块，并且仅存储匹配域块的位置和分形变换的参数（尺寸因子、差值因子和图像块对称旋转方式参数）。由于这样的存储量比原始图像大大减少了，从而实现了压缩。解码过程则是利用分形变换的迭代收缩特点，使初始图像经过多次分形变换来获得原始图像。在分形编码与四叉树相结合的自适应图像分形压缩编码算法[12,13]中，四叉树用于自适应图像分割，并通过动态改变区块的大小来使得每个区块都能够找到合适的匹配域块，以减少编码误差和改善压缩效果。

这里利用第 2 种四叉树置乱方法进行加密。由于在编码过程中，如果改变区块的位置，则区块与域块间的对应关系也会改变，从而可以实现置乱加密。在解码过程中，由于解码过程是个多次迭代过程，因此，图像块的位置改变会随着迭代次数的增加而逐渐扩散，最终获得的图像是加密后的不可理解的密文图像。其优点是，只有具有正确的密钥，才能够在解码过程中恢复图像块正确的位置，以便得到解密的图像，但在此编码过程中，由于四叉树的高度比较小，即加密的穷举空间不够大，因此需要通过分区域采用不同的四叉树置乱密钥或者同时加密其他的分形变换参数来增加密码强度。本文给出的压缩加密方案如图 5 所示。

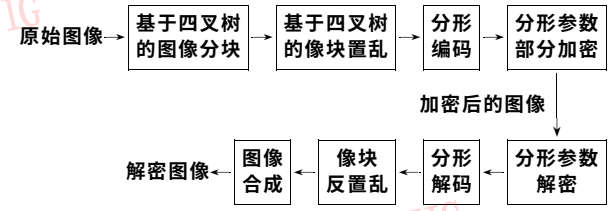


图 5　基于四叉树的分形压缩加密方案

5　实验结果

5.1　加密效果

分别以第 4 节中的四叉树分块压缩编码算法和 EZW 编码算法为例，测试了四叉树置乱加密的加密效果。测试图像为 256×256 的 Lena 灰度图，实验结果如图 6 所示。

原始图像经过四叉树置乱方法置乱后，图像不可理解，只是图像分块依稀可见，如图 6(b)所示；如果用四叉树置乱方法置乱后，再增加对灰度值的加密，则加密后图像完全不可理解，如图 6(c)所示。

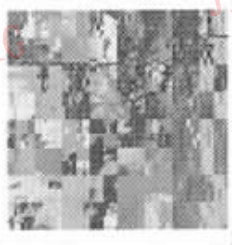
小波系数经过四叉树置乱方法置乱后，图像也不可理解，如图 6(d)所示；如果用四叉树置乱方法置乱后，再增加对高频系数符号的加密，则加密后图像更加混乱，如图 6(e)所示。

分形编码中图像区块经过四叉树置乱方法置乱后，图像不可理解，如图 6(f)所示；如果在图像区块用四叉树置乱方法置乱后，再增加对分形变换中匹配域块位置参数的加密，则加密后图像更加混乱，已经完全不可理解，如图 6(g)所示。

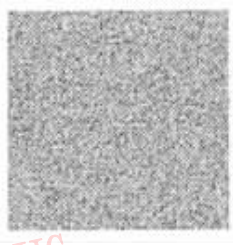
5.2　加密速度

为了测试以上 3 种算法的加密速度，作了以下实验，即，选择不同的图像，测试了各算法在压缩加密编码过程中，其加密过程所用时间占总时间的百分比。测试图像为 256×256 像素的 Lena 灰度图，Cameraman 和 Scene 灰度图，512×512 像素的 Goldhill 和 Boats 灰度图，实验结果如表 1 所示。

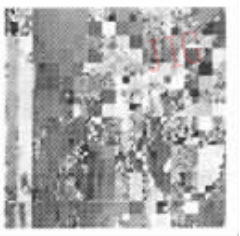
(a) 原始图像



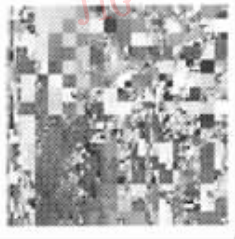
(b) 四叉树置乱后图像



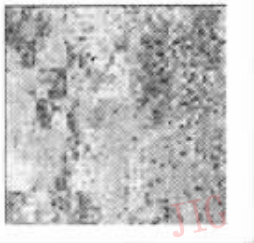
(c) 四叉树置乱，并结合叶子节点加密后图像



(d) 小波系数四叉树置乱后图像



(e) 小波系数四叉树置乱，并结合高频系数符号加密后图像



(f) 图像区块四叉树置乱后图像

(g) 图像区块四叉树置乱，并结合匹配域块位置参数加密后图像

图 6 四叉树分块压缩加密实验结果

表 1 压缩加密算法速度测试

实验图像（图像文件名/图像尺寸）	算法中加密过程占总过程的时间比例(%)		
	四叉树分块压缩加密算法（四叉树置乱＋叶子节点加密）	EZW 压缩加密算法（四叉树置乱＋高频系数符号加密）	基于四叉树分割的分形压缩加密算法（四叉树置乱＋增量和位置参数加密）
Lena(256×256)	53.44	2.76	13.16
Cameraman(256×256)	50.85	5.09	15.15
Scene(256×256)	53.74	5.43	14.21
Goldhill(512×512)	56.35	3.75	8.98
Boat(512×512)	55.43	5.61	4.72

可见，在 EZW 编码和基于四叉树分割的分形编码加密算法中，由于加密过程占用的时间相对较少，因而加密过程对编码速度的影响较小，如表 1 所示，其所占时间比例的最大值分别为 5.43%和 15.15%。在四叉树分块压缩加密算法中，虽然因加密过程占编码总过程的时间比例超过 50%而影响了编码速度，但是由于四叉树分块压缩编码本身就具有很高的速度，因此整个四叉树分块压缩加密过程仍然具有较高速度。综上所述，若加密过程与编码过程相结合，则能使得整个编码和加密过程具有较高的速度，即能够满足图像、视频等的实时性要求。

6 结 论

本文提出的基于四叉树置乱的压缩加密方法，经理论分析和实验结果证明，此算法具有安全性较高、运算复杂性低、保持数据编码格式不变、保持数据压缩率不变等特点，很适合用于实时性要求高的图像和视频编码传输。由于四叉树已广泛应用于图像和视频的编码中，因此这种算法具有广泛的应用前景。

参 考 文 献

1 Yen Jui-Cheng, Guo Jiun-In. A new chaotic key-based design for image encryption and decryption[A]. In: Proceedings of IEEE International Symposium on Circuits and Systems[C], Geneva, Switzerland, May 2000, **4**: 49～52.

2 Agi I, Gong L. An empirical study of MPEG video transmissions[A]. In: Proceedings of the Internet Society Symposium on Network and Distributed System Security[C], San Diego, CA, USA, Feb. 1996: 137～144.

3 Qao L, Nahrstedt K. A new algorithm for MPEG video encryption[A]. In: Proceeding of the First International Conference on Imaging Science, Systems and Technology[C],

Las Vegas, Nevada, USA, July 1997: 21～29.

4 Tang L. Methods for encrypting and decrypting MPEG video data efficiently [A]. In: Proceedings of the Fourth ACM International Multimedia Conference[C], Boston, MA, USA, November, 1996:219～230.

5 Sridharan S, Dawson E, Goldburg B. Fast fourier-transform based speech encryption system[J]. IEE Communication Speech and Vision, 1991, **138**(3):215～223.

6 Wu Chunping, Kuo Jay C. Efficient multimedia encryption via entropy codec design[A]. In: Proceedings of SPIE International Symposium on Electronic Imaging 2001[C], San Jose, CA, USA, Jan. 2001, **4314**:128～138.

7 Strobach P. Quadtree-structured recursive plane decomposition coding of images[J]. IEEE Transactions on Signal Processing, 1991, **39**(6):1380～1397.

8 Strobach P. Tree-structured scene adaptive coder[J]. IEEE Transactions on Communication, 1994, **38**(4):477～486.

9 Sulliran G J, Baker R L. Efficient quadtree coding of images and video[J]. IEEE Transactions on Image Processing, 1994, **3**(3): 327～331.

10 Shapiro J M. Embedded image coding using zerotrees of wavelet coding[J]. IEEE Transactions on Signal Processing, 1993, **41**(12): 3445～3462.

11 Said Amir. A new fast and efficient image codec based on set partitioning in hierarchical trees [J]. IEEE Transactions on Circuits and Systems for Video Technology, 1996, **6**(3):243～250.

12 Lee Shinhaeng, Omachi Shin'ichiro, Aso Hirotomo. A parallel architecture for quadtree-based fractal image coding [A]. In: Proceedings of the 2000 International Conference on Parallel Processing[C], Toronto, Canada, August 2000:15～22.

13 Frigaard C, Gade G, Hemmingsen T, *et al*. Image compression based on a fractal theory[R]. Technical Report S701, Institute for Electronic Systems, Aalborg University, Denmark, 1994.

14 Lazar M S, Bruton L T. Fractal block coding of digital video [J]. IEEE Transactions on Circuits & Systems for Video Technology, 1994, **4**(3):297～308.

廉士国　1978 年生,2000 年获南京理工大学信息工程专业学士学位,现于南京理工大学攻读博士学位。现主要研究方向为混沌密码学及多媒体加密。

王执铨　1939 年生,教授,博士生导师,1962 年毕业于哈尔滨军事工程学院,现为南京理工大学自动化系教授,博士生导师。当前感兴趣的领域为信息安全技术、混沌控制与应用、大系统的容错控制理论与应用等。

李忠新　1976 年生,2000 年获南京理工大学硕士学位,现为南京理工大学自动化系博士研究生。主要从事图像处理、虚拟现实等方面的研究。