一种支持密文转码的JPEG2000图像加密算法

傅 勇[1,2] 易小伟[1,2] 马恒太[1]
(中国科学院软件研究所天基综合信息系统重点实验室 北京 100190)[1]
(中国科学院大学 北京 100049)[2]

摘 要 针对异构化程度不断加剧的通信网络环境对码率转换能力的需求,提出了一种支持密文域转码的层次化加密算法CT-HEA。与以往基于JPEG2000图像的加密算法相比,CT-HEA针对率失真优化截断模型的特点,按照图像质量层和分辨率对压缩流重新进行截断与合并,对重组后的码流采用密码学算法进行分层加密。该算法支持对加密压缩流的透明码率转换。仿真实验结果表明,CT-HEA算法复杂度低、保密性好,具有灵活的安全转码特性和低的转码代价。

关键词 图像加密,JPEG2000压缩,安全转码
中图法分类号 TN919.8 **文献标识码** A

JPEG2000 Digital Image Encryption Algorithm Supporting Ciphertext Transcoding

FU Yong[1,2] YI Xiao-wei[1,2] MA Heng-tai[1]
(Science and Technology on Integrated Information System Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)[1]
(University of Chinese Academy of Sciences, Beijing 100049, China)[2]

Abstract Aiming at the increasing demand for transcoding capacity caused by the aggravating isomerization degree in communication networks, a digital image hierarchical encryption algorithm supporting ciphertext domain transcoding named CT-HEA(Ciphertext Transcoding-Hierarchical Encryption Algorithm) was proposed. Compared with the traditional JPEG2000 image encryption algorithms, aiming at the feature of rate-distortion optimized truncation model, CT-HEA truncates and combines the compressed codestream according to image quality layer and resolution, applies hierarchical encryption to the codestream after reorganization by using cryptographic algorithms. It supports transparent transcoding operations directly on the encrypted and compressed bitstream. Simulation results demonstrate that CT-HEA is characterized by low complexity, high performance of secure, high secure transcoding flexibility and low transcoding overhead.

Keywords Image encryption, JPEG2000 compression, Secure transcoding

1 引言

随着多媒体技术的日趋成熟,图像、音频和视频等多媒体数据在网络中传输已经十分普遍[1]。同传统的文本信息相比,数字图像具有直观性强、信息量大、冗余度高等特点。为了节省网络带宽和提高传输效率,在图像数据传输中普遍采用数据压缩技术。由于数字图像中可能包含重要数据的"敏感"信息[2],例如非公开会议图像、个人隐私图像和军事图像等,因此,图像数据的安全传输是内容分发网络(Content Delivery Network,CDN)中面临的一个严峻挑战[3]。

通常CDN是一个严重的异构网络[4]。在CDN中存在许多不同类型的终端设备,例如台式计算机、笔记本电脑和移动手持设备,它们对多媒体应用的需求具有明显的差异性。对同一图像数据,台式计算机需要高分辨率和高质量的图像,然而由于屏幕限制,在大部分移动手持设备上仅仅利用低分辨率和低质量的图像就能满足用户需求。此外,由于网络带宽的约束,需要为有线网络和移动无线网络提供不同码率的图像数据。因此,CDN网络中的中间节点需要对服务器发送的图像数据进行码率转换,以适应不同客户端和网络环境的需求。设计一种支持密文转码的加密方法对图像数据的端到端安全传输具有重要的研究意义。

对基于小波变换的图像压缩算法,由于小波系数常用算术编码器进行编码,因此可采用针对算术编码的加密方案。这类针对熵编码的内置式加密算法能够保持压缩码流的语法结构。文献[5]针对JPEG2000压缩标准,设计了一种保持码流结构的图像加密算法。文献[6]基于EBCOT编码的分类提出了一种图像部分加密方案。近些年来,很多基于混沌系统的数字图像加密方案被不断提出。文献[7]设计出一种性能优异的基于混沌系统的矩阵置乱算法,该算法只选择小波系数的低频分量进行置乱加密,而图像内容信息通常分散于

到稿日期:2013-08-30 返修日期:2013-11-14 本文受中国科学院创新基金项目(CXJJ-11-S101)资助。
傅 勇(1989—),男,硕士生,主要研究方向为空间信息安全,E-mail:sven_fy@163.com;易小伟(1987—),男,博士生,主要研究方向为空间信息对抗;马恒太(1970—),男,博士,副研究员,主要研究方向为卫星组网仿真、信息安全。

所有频带上，这使得密文图像的边缘仍然可见，因此该算法存在安全性缺陷。文献[8]提出了一种采用混沌系统的高速高安全性 JPEG2000 加密方案。文献[9]对基于 KDWPT(Key-Dependent Wavelet Packet Transforms)的联合压缩加密方案进行了性能分析。文献[10]提出了一种支持灵活访问控制的分层广播加密方案。随着网络异构化程度的加剧，可伸缩性在图像加密算法评估指标中的地位日益突出。

本文基于 JPEG2000 标准中实现码率控制的核心算法——带优化截断的嵌入块编码(Embedded Block Coding with Optimized Truncation，EBCOT)，针对密文域码率转换提出了一种图像层次化加密方法 CT-HEA。CT-HEA 依据 EBCOT 截断后的质量分层对码流进行重组、加密、打包，从而保留其多分辨率和多质量层解码的可伸缩性，通过对密文码流的透明转码支持，在实现图像数据端到端安全分发的同时满足了异构网络对转码的需求。

2 JPEG 2000 简介

2.1 标准简介

JPEG2000 图像的编解码流程如图 1 所示，在编码前，源图像首先被分割成大小相等、相互不重叠的矩形块——分片(Tile)。这种分割有两种作用：1)以 Tile 为基本单位独立编码，在处理较大的图像时可节省内存空间；2)将每个 Tile 看成小的源图像，对其每个分量分别进行单独编码，可在图像特定位置截取出具有特定宽高比的重构子图。

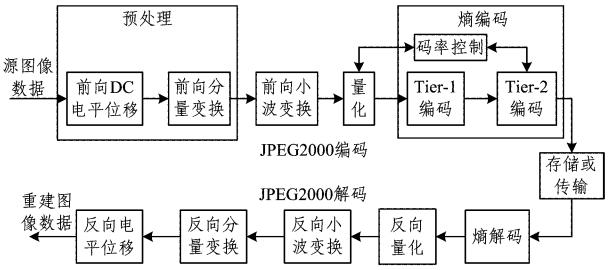


图 1 JPEG2000 编解码流程框图

JPEG2000 编码的核心部分主要集中在两个部分：小波变换模块和熵编码模块。离散小波变换模块对每个 Tile 的每个分量采用 Mallat 塔式小波变换，将其分解成若干子带图像，每个子带包含许多小波系数，这些小波系数描述了该区域的局部统计特性和局部频率特性，以便后续能更有效地进行编码。

得到的小波系数是用连续的实数来表示的，考虑到人类视觉系统对图像的分辨率有一定的界限，通过适当的量化减小小波系数的精度，在一定程度上减少空域和频域上的冗余度，但这些数据在统计意义上还存在一定的相关性，为此采用熵编码来消除数据间的统计相关性。在进行熵编码之前，首先将每个量化后的子带分割成小矩形块，称为码块，每个码块独立编码，这就是嵌入式块编码。又由于在熵编码阶段采用了截断点优化算法，故而也称 EBCOT 编码。

为进行 EBCOT 编码，需先将码块中的量化系数组织成“位平面”。EBCOT 编码过程分成两级，如图 2 所示。EBCOT 第一级编码(Tier-1 编码)：位平面算术编码从最高有效位平面逐平面编码至最低有效位平面，得到码块编码位流，然后按照率失真优化原则，截取成不同长度的位流段形成 3 个编码通道，截断点和失真值以压缩的形式同码块位流保存在一起，形成码块的嵌入式压缩位流。EBCOT 第二级编码(Tier-2 编码)：对编码后的码块位流采用压缩后率失真(PCRD)优化算法思想，计算码块位流在每一层上的截断点。将所有码块位流按照截断点分层组织，形成具有不同质量级的数据单元——包(Packet)，这些包按照一定的累进顺序输出给最终码流。

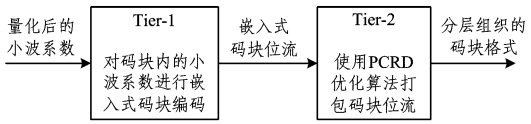


图 2 EBCOT 两层编码策略

2.2 码率控制

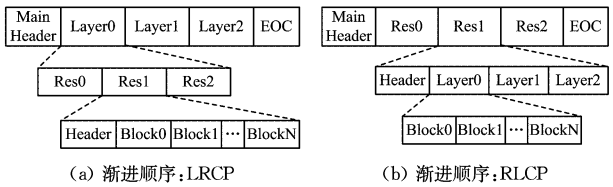
如图 1 所示，在 JPEG2000 编解码系统中，码率控制可通过两个不同的机制来实现：1)选择各子带系数的量化步长；2)码流截断。对于采用整数变换(可逆分量变换和整数小波变换)的编码而言，因为量化步长固定地设为 1，所以只能采用码流截断的方法来实现码率控制。

调整各子带的量化步长可以控制压缩图像的码率，量化步长增大，则量化子带系数的动态范围减小，编码比特流的码长即码率也相应减小。该方法操作简单，但存在一个潜在的缺点，即每次量化步长改变，量化子带系数也随之改变，则需重新进行一次 Tier-1 编码，而 Tier-1 编码需要相当大的计算量，因而该方法在计算量有一定限制的编码器中不太实用。所以，一般在编码器中选择量化步长只进行一次，用来进行粗略的码率控制。

更为精细的码率控制可以通过码流截断即选择装配到最终码流中的编码通道来实现。编码器可以计算出每个编码通道对码率的贡献，以及对应的图像失真减小值。码率控制时，可以根据各编码通道每比特对应的图像失真减小值，按从大到小的优先顺序选择编码通道装配到最终码流中，直至达到总的码率要求。该方法对于选择不同的失真度量(如均方误差、视觉加权均方误差等)具有相当的灵活性。

2.3 码流语法结构

一个图像的 Tile 数据在进行 Tier-2 编码时，按照 4 个维度：质量层级(Layer)、分量(Component)、分辨率等级(Resolution)和子区(Precinct)渐进顺序的不同，有多种数据组织方式可供选择用于码流装配，其中较常用的两种渐进方式是 LRCP 和 RLCP，假设某图像只有一个分量，编码参数设置为 3 个质量层、3 个分辨率级数和 1 个子区，则其压缩码流的语法结构如图 3 所示。



(a) 渐进顺序：LRCP　　(b) 渐进顺序：RLCP

图 3 码流语法的层次化结构

其中，Main Header 表示文件头，Header 表示对应分辨率的包头，Layer n 和 Res n(n=0,1,2)分别表示各个质量层和分辨率，Block n(n=1,2,…,N)表示码块 n 在对应分辨率和质量层下的编码码流，EOC 表示文件结束标识。

从图中可以看出，JPEG2000 的码流是按照某种渐进顺序进行组织打包的，从质量层和分辨率的维度来看，压缩码流具有层次化的语法结构，从解码来看，码流可以在任意处截断

并重建图像，具有非常高的可伸缩性。

3 本文算法

本节针对 JPEG2000 压缩码流层次化的语法结构特点提出了一种层次化加密算法，以及基于图的密钥生成和更新方案，然后阐述了在该加密方法下如何实现灵活有效的安全码率转换，最后在理论上对 CT-HEA 算法进行了安全性分析。

3.1 CT-HEA 算法

为了保证图像内容的秘密性，码流不能以明文的形式进行传输。最典型和有效的解决方法是对编码后的数据进行加密，在整个传输过程中码流数据都以密文的形式存在，在不知道对应密钥的情况下，非法的数据访问操作是不可行的。这样就实现了压缩码流的端到端安全传输。

一个图像经过 JPEG2000 压缩编码后所形成的码流序列可以简单地看作是标志段和包数据的组合，根据码流的语法结构以及质量的层次化结构特征对 JPEG2000 压缩码流进行分解，按质量层和分辨率可将其组织成二维结构，如图 4 所示。在空间维度上，对生成的 JPEG2000 压缩码流按空间可伸缩性可分解成 Res_0、Res_1、Res_2 3 个分辨率。在质量维度上，可将每个码块的编码流组织成一个基本层 L_0 和若干个质量扩展层$\{L_n\}$ $(n=1,2,\cdots,N)$。

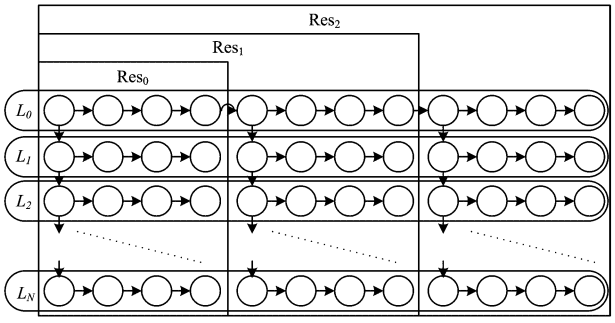


图 4 JPEG2000 码流组织结构及密钥生成依赖关系图

基于二维结构对图像编码数据部分进行分解，得到一个码包序列。为了实现安全性，层次化加密方法对每个码包单独进行加密。这样在不破坏原始压缩位流的前提下保证了码包的安全性。对每个数据码包的加密方式如图 5 所示。假设原始码流第 b 个码块中第 l 个质量层的数据码包记为 $P(b,l)$，加密后的数据码包记为 $P^*(b,l)$，那么加密过程可用下式来表示：

$$P^*(b,l)=E(IV_{b,l},Key,P(b,l))$$

其中，$E(\ )$为加密函数，$IV_{b,l}$表示加密使用的初始向量，Key 表示加密使用的密钥。加密函数的选择可以实现在代价和安全性之间的平衡。

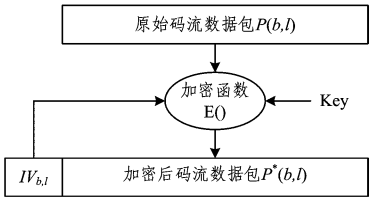


图 5 数据包加密模式图

上述层次化加密算法的优势在于加密函数的可替换性。通过选择不同负荷、不同强度的加密函数，例如分组加密密码函数 AES、DES 和流密码加密函数 RC4 等，能够实现对码流的非均衡保护。根据编码后各质量层次的重要程度不同，对重要的码流数据包（例如码块第 L_0 层的数据包）采用更强的加密保护，而对相对次重要或不重要的码流数据包（例如码块较高扩展层的数据包）采用较弱的加密保护。

整个图像码流的加密过程如表 1 所列。

表 1 基于质量分层的 CT-HEA 算法

Input: P(b,l), b=1,2,…,M, l=0,1,…,N. $IV_{1,0}$, K
Output: P*(b,l), b=1,2,…,M, l=0,1,…,N
1. $IV_{1,0}$:= 0x01010101
2. $K_{1,0}$:= KeyGen(K, ID_S, ID_r)
3. For l from 0 to N
4. For b from 1 to M
5. $IV_{b+1,l}$:= $IV_{b,l}+1$
6. P*(b,l) := E($IV_{b,l}$, $K_{b,l}$, P(b,l))
7. $K_{b+1,l}$:= KeyGen($K_{b,l}$, P*(b,l))
8. End For
9. $K_{1,l+1}$:= KeyGen($K_{1,l}$, P*(1,l))
10. $IV_{1,l+1}$:= $IV_{1,l}+1$
11. End For

3.2 密钥生成及更新

采用密码学加密函数进行数据包加密所面临的安全性问题是密钥的重复使用。如果对同一个码流中的所有数据包都使用相同的加密密钥，那么加密算法将存在严重的安全隐患。例如，RC4 加密算法只是简单地对密钥流和码流数据进行异或操作，导致它不能抵抗已知明文攻击。

为了解决密钥的重复使用问题，在加密方案中通过密钥生成函数使得每个码流数据包所采用的加密密钥都不一样。这样就避免了密钥的重复使用，增强了加密方案的安全性。图 4 显示了 JPEG2000 码流中的各数据包加密时密钥的生成和依赖关系。它们可以用一个有向无环图（Directed Acyclic Graph，DAG）来描述。在 DAG 中，每个节点表示一个码流数据包，对应的有向边表明了密钥依赖关系。图 5 显示了码流数据包的加密过程。

其中密钥 Key 的生成可分为如下两种情况：

1）在加密同一分辨率下同一质量层的码流数据包时，采用密文分组链接（Cipher Block Chaining，CBC）加密模式。依据压缩码流中码块数据包的渐进组织顺序，当前数据包节点的加密密钥由其相邻的前继节点的数据生成，也即

$$Edge(P(b,l),P(b+1,l))\in DAG$$

2）对于每个分辨率第一个码块不同层的码流数据包，码块内所有数据包的加密密钥的更新仅与对应分辨率中的第一个数据包相关。L_n 层数据包的加密密钥由 L_{n-1} 层的数据包生成，也即

$$Edge(P(1,n-1),P(1,n))\in DAG$$

具体的密钥生成算法 $KeyGen(\ )$ 可以很灵活，一种很有效的方法是利用哈希函数，例如 SHA-1 等。

$$K_{1,l+1}=SHA\text{-}1(K_{1,l}\parallel P^*(1,l))$$

$$K_{b+1,l}=SHA\text{-}1(K_{b,l}\parallel P^*(b,l))$$

其中，“$\parallel$”表示将其前后两个部分串接起来。

3.3 安全转码

基于加密方式层次化的特点和密钥生成依赖关系，在密文域码流级上可实现多空间分辨率的码率转换和多质量层的码率转换。具体实现方式描述如下：

3.3.1 基于空间分辨率的码率转换

由于在码流重组模块中整个图像码流按照空间分辨率累进组织，如图 4 所示，重组后的图像包含 3 个分辨率。并且在

同一质量层 L_n，数据包的加密密钥根据其所在分辨率呈线性依赖关系。因此，转码器可以在任意分辨率位置对原始图像码流进行截断，进而满足不同接收端对图像分辨率（或者码率）的需求。例如图 4 中的码流能够提供 3 个分辨率的码率转换。

3.3.2 基于质量层的码率转换

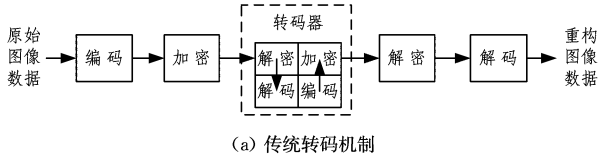
对于 JPEG2000 码流的每个码块，利用率失真优化方法计算出若干截断点之后，可以将其对应码流划分成多个质量层。由图 4 可以获悉，每个质量层的第一个码流数据包 $P(1,l)$ 的加密密钥可以通过其上层的数据包 $P(1,l-1)$ 生成。这样转码器可以在任意质量层 L_n 对码流进行截断，实现码率转换，接收端能够仅对前 n 个质量层的码流进行解码，实现在图像质量、码率和时延之间的更优权衡。

通过上面对转码器进行多模式码率转换的分析，可以结合使用上述转码模式完成灵活的图像数据转码分发。值得注意的是，在上述转码系统中，转码节点能够实现安全透明的码率转换。转码器不需要对接收到的码流进行解密解码，只需根据用户需求对码流以合适的码率进行压缩加密。采用提出的层次化加密方法，转码器只需要通过读取码流数据包的头部就可以完成对码流的转码分发。这样码流数据的内容对转码器而言是透明的，转码器节点也不需要知道数据的加密密钥，从而实现了图像数据的端到端安全传输。

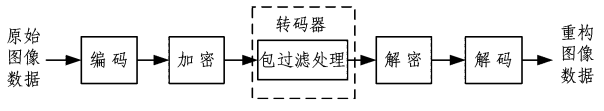
3.4 安全性分析

从密码分析学的角度来看，重构加密的 JPEG2000 图像时位流值要通过算术解码器解码并且对应的解码模型依赖于前边的位流值，唯密文攻击通常用一些常数位来替换被加密的数据，这些替换值打乱了随后的状态，因而重构的结果也是一种类似于噪声的效果图，也即 CT-HEA 能抵抗常数位替换型的唯密文攻击；由于密钥不重复使用，因此算法对已知明文攻击的抵抗能力很强；对选择明文攻击的抵抗能力依赖于所选择的加密函数，例如 AES 就能满足需求，对于 AES 的攻击，到目前为止还没有比穷尽密钥搜索攻击更有效的方法；对于穷举密钥搜索，算法安全性依赖于密钥空间的大小，128 位长度的密钥完全能满足安全性需求。

从传输过程来看，CT-HEA 算法采用如图 6(b)所示的安全透明转码机制，比图 6(a)所示的传统转码机制具有更多的优良特性，例如安全透明转码机制能够保证数据的端到端安全，因为转码器节点只需对加密码流进行操作。安全透明转码机制甚至可以在不对编码码流解码的情况下对其进行码率转换，弥补了传统转码的不足，同时实现了码率转换和码流安全，并且转码器只需做简单的包过滤处理操作，从各方面增强了系统的安全性，也提高了转码的效率。



(a) 传统转码机制



(b) 安全透明转码机制

图 6

通过以上分析，可以发现 CT-HEA 算法在保证图像数据安全的基础上有效提高了码率转换的效率。

4 仿真实验

实验采用 C 语言搭建仿真平台，对 JPEG2000 图像数据分发过程进行仿真，并对算法的加密效果、时间和空间代价、可伸缩性以及重建图像的质量进行验证，并与其他加密算法进行性能对比分析。

4.1 仿真平台

通过对互联网下图像数据分发过程的业务场景分析，可知数据分发系统由发送端、中间转码节点和接收端 3 类节点组成，其结构图如图 7 所示。

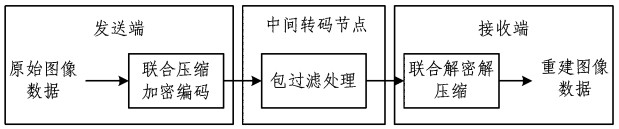


图 7 数据分发系统框图

数据分发系统的主要环节如下：

1）发送端在对图像数据压缩分包的同时进行加密，加密初始向量、分辨率序号、码块序号以及质量层序号等参数需要封装到数据包头部，待整个图像数据压缩加密完成之后，将生成的数据包发送给中间节点。

2）中间节点对数据包做包过滤处理，比如只接收前 5 个质量层或前两个分辨率的图像数据，符合要求的数据包被发送给接收端。

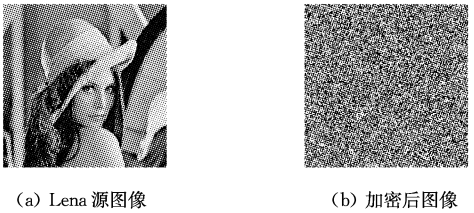
3）接收端对接收到的数据包进行解密和解压缩得到重建图像。

4.2 仿真结果

采用分辨率分别为 512×512 和 1024×1024 的灰度图像 Lena 和 Man 作为测试图像，JPEG2000 编码参数设定无损压缩、3 层小波变换（共产生 4 个分辨率级）、7 个质量层，码块大小分别设置为 16×4 和 128×4，子区设置为与码块同样大小。加密函数分别选用 AES 和 DES 算法，加密密钥长度选用 128 比特，初始向量选用 128 比特。

4.2.1 加密效果

从安全性的角度考虑，仿真实验首先对比分析了加密前后的图像内容。图 8 给出了利用 CT-HEA 算法对 Lena 图像和 Man 图像进行加密的结果，从图 8(b)来看，加密后的图像虽然能被标准解码器解码，但已经无法识别出原图像的任何信息，达到了加密和掩蔽的效果。



(a) Lena 源图像　　(b) 加密后图像

图 8

4.2.2 时间和空间代价

从转码的时间代价来考虑，仿真实验分析了 Lena 和 Man 分别采用 AES 和 DES 时，加密占图像处理总时间的百分比。实验结果如图 9 所示。从图中可以看出，无论是 AES 还是 DES，加密过程所耗费的时间所占比例均小于 2%，这表明加

密相比不采用加密所增加的时间代价很小。

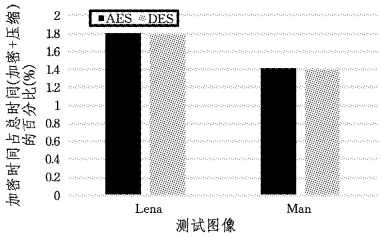


图 9　加密时间和总时间的关系

从转码的空间通信代价来考虑，仿真实验分析了 Lena 分别采用 AES 和 DES 时，加密填充部分占最终码流数据包总长度的百分比。实验结果如图 10 所示。从图中可以看出，无论是 AES 还是 DES，加密算法导致的自定义包头占总数据量的比例均小于 2%，这表明加密相比不采用加密所增加的空间代价很小。

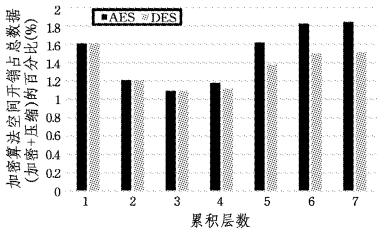


图 10　加密的空间代价与图像总数据量的关系

4.2.3　性能比较

针对 CWF(Confusion of Wavelet coefficients on the subbands in Frequency domain)、CWW(Confusion of Wavelet coefficients on the Whole image)、PEA(Partial Encryption Algorithm)和 CT-HEA 4 种 JPEG2000 图像加密方法的如下性能进行了验证：

a)加密时间开销

b)加密空间开销

c)是否支持有损压缩

d)是否支持密文域转码

表 2 给出了实验结果，实验结果说明 CT-HEA 算法在加密时间开销和空间开销方面都比前 3 种算法要小很多，同时支持有损压缩和密文转码。

表 2　JPEG2000 加密算法的性能比较

	加密时间开销%	加密空间开销%	是否支持有损压缩	是否支持密文域转码
CWW	14	0.75	否	否
CWF	19	2	是	否
PEA	3.2	0	否	否
CT-HEA	2	0(1.8 通信代价)	是	是

4.2.4　可伸缩性和重建图像质量

从重建图像质量来考虑，仿真实验还分析了安全转码前后的端到端 R-D 曲线，从图 11 中的实验结果可以看出，压缩加密码流的 R-D 曲线非常接近于原始码流的 R-D 曲线。这表明加密方案相比不采用加密所增加的码率代价非常小。图中每个数据点表示在累加不同数目的质量层时的总码率和所对应的重构图像质量。在渐进传输过程中，随着转码的质量层的增加，码率和重构图像的质量相应得到提高。利用 R-D 曲线，转码器可以为用户提供灵活高效的码率转换，例如，采用分辨率限制的转码和采用质量层限制的转码等。由于 JPEG2000 码流是一种可伸缩编码码流，码流可在任意位置截断而不影响码流的解码，因此上述灵活的转码方式能够有效地支持图像的质量或分辨率渐进传输。

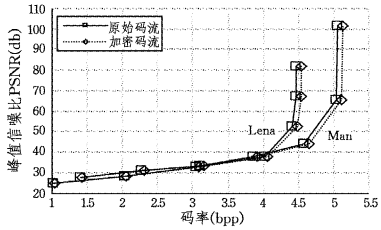


图 11　端到端的 R-D 曲线

从可伸缩性解码来考虑，仿真实验验证了算法对密文域转码的支持。实验结果如图 12 所示，其中 ResNum 表示图像包含的分辨率级数，LyrNum 表示图像包含的质量层数。从图中可以看出，接收端能够将经过转码的图像解码，而且随着分辨率级数和质量层数的累积，图像质量不断提升，这表明加密算法实现了多分辨率和多质量层解密。

图 12　多分辨率解密和多质量层解密

结束语　本文提出的 CT-HEA 算法，很好地利用了 JPEG2000 编码流的层次化结构和可伸缩特性，能够在保留原码流特性的前提下支持密文域上的安全透明转码。仿真实验结果表明，CT-HEA 与其他加密算法相比不但加密效果好、时空代价低，而且支持灵活的多分辨率以及多质量层解密，在很低的通信代价下实现了对图像数据的端到端安全分发和质量保证。

参 考 文 献

[1] 史元春，徐光祐，高原. 中国多媒体技术研究[J]. 中国图像图形学报，2010，15(7)：1023-1041

[2] 文昌辞，王沁，苗晓宁，等. 数字图像加密综述[J]. 计算机科学，2012，39(12)：6-9

[3] Zhou L，Chao H C，Vasilakos A V. Joint forensics-scheduling strategy for delay-sensitive multimedia applications over heterogeneous networks[J]. IEEE Journal on Selected Areas in Communications，2011，29(7)：1358-1367

[4] Yu H H. Scalable streaming media authentication[C]// Communications，2004 IEEE International Conference on. IEEE，2004，4：1912-1916

[5] 顾国生，韩国强，王宁，等. 一种保持码流结构的 JPEG2000 加密算法[J]. 计算机科学，2007，34(11)：222-223

[6] Yan S，Lin Q. Partial encryption of JPEG2000 images based on EBCOT[C] // Intelligent Control and Information Processing (ICICIP)，2010 International Conference on. IEEE，2010：472-476

(下转第 93 页)

误路线，让更多车辆能够更快到达目的地。

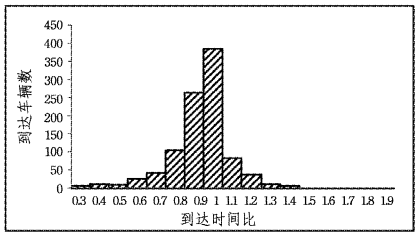


图 7　到达时间对比

结束语　本文基于真实的场景进行仿真，证明了利用基于数据的信任模型和 D-S 理论能够在存在恶意节点的环境下，不增加额外的数据交换，很好地解决了路况信息伪造问题，同时改善了车辆的行程时间。但是，当恶意节点数量超过一定比例时，基于数据的信任模型难以胜任恶意鉴别的工作，需要引入 RSU 等第三方的数据来源来提高路况信息鉴别的可靠性。另外，公交车辆路线固定，客观反映道路实际情况，作为受信车辆参与到路况信息广播中，有利于一般车辆更好地区分恶意节点。总的来说，RIDTM 算法能在车载自组织网络寻路中鉴别恶意信息、过滤异常信息，并且容易集成到已有的成熟寻路算法中，对存储空间和计算能力的要求不高，非常适用于提高常用车载自组织网络寻路算法的安全性。

参 考 文 献

[1] Nzouonta J, Rajgure N, Wang G, et al. VANET routing on city roads using real-time vehicular traffic information[J]. IEEE Transactions on Vehicular Technology, 2009, 58(7): 3609-3626

[2] Raya M, Papadimitratos P, Gligor V D, et al. On data-centric trust establishment in ephemeral ad hoc networks[C]// Proceedings of INFOCOM 2008. The 27th Conference on Computer Communications. Phoenix, USA, 2008: 1238-1246

[3] Shafer G. A mathematical theory of evidence[M]. Princeton: Princeton University Press, 1976

[4] Eschenauer L, Gligor V D, Baras J. On trust establishment in mobile ad-hoc networks[C]// Proceedings of Security Protocols. Berlin, Germany, 2004: 47-66

[5] Sun Y L, Yu W, Han Z, et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. Selected Areas in Communications, 2006, 24(2): 305-317

[6] Theodorakopoulos G, Baras J S. On trust models and trust evaluation metrics for ad hoc networks[J]. Selected Areas in Communications, IEEE Journal, 2006, 24(2): 318-328

[7] Buchegger S, Le Boudec J Y. A robust reputation system for peer-to-peer and mobile ad-hoc networks[C]// Proceedings of P2PEcon. Cambridge MA, USA, 2004

[8] Ganeriwal S, Balzano L K, Srivastava M B. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2008, 4(3): 15

[9] Mundinger J, Le Boudec J Y. Reputation in self-organized communication systems and beyond[C]// Proceedings of the 2006 workshop on Interdisciplinary systems approach in performance evaluation and design of computer & communications systems. Pisa, Italy, 2006: 3

[10] Zouridaki C, Mark B L, Hejmo M, et al. Robust cooperative trust establishment for MANETs[C]// Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks. Alexandria, VA, USA, 2006: 23-34

[11] Mejia M, Peña N, Muñoz J L, et al. A game theoretic trust model for on-line distributed evolution of cooperation in MANETs[J]. Journal of Network and Computer Applications, 2011, 34(1): 39-51

[12] Wu A, Ma J, Zhang S. RATE: A RSU-Aided Scheme for Data-Centric Trust Establishment in VANETs[C]// Proceedings of Wireless Communications, Networking and Mobile Computing (WiCOM). Wuhan, China, 2011: 1-6

[13] Gómez Mármol F, Martínez Pérez G. TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks [J]. Journal of Network and Computer Applications, 2012, 35 (3): 934-941

[14] Jøsang A. An Algebra for Assessing Trust in Certification Chains[C]// Proceedings of NDSS. San Diego, California, USA, 1999, 99: 6

[15] Chen T M, Venkataramanan V. Dempster-shafer theory for intrusion detection in ad hoc networks[J]. Internet Computing, IEEE, 2005, 9(6): 35-41

[16] Siaterlis C, Maglaris B. Towards multisensor data fusion for DoS detection[C]// Proceedings of the 2004 ACM symposium on Applied computing. Nicosia, Cyprus, 2004: 439-446

[17] Jiang T, Baras J S. Trust Evaluation in Anarchy: A Case Study on Autonomous Networks[C]// Proceedings of INFOCOM. Barcelona, Catalunya, Spain, 2006

[18] Ostermaier B, Dotzer F, Strassberger M. Enhancing the security of local dangerwarnings in vanets-a simulative analysis of voting schemes[C]// Proceedings of Availability, Reliability and Security. Prague, Czech, 2007: 422-431

[19] Sumra I A, Ahmad I, Hasbullah H, et al. Classes of Attacks in VANET[C]// Proceedings of Electronics, Communications and Photonics Conference (SIECPC). Riyadh, Saudi Arabia, 2011: 1-5

[20] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of Advances in Cryptology. Springer Berlin Heidelberg, 1985: 47-53

[21] Wegener A, Piórkowski M, Raya M, et al. TraCI: an interface for coupling road traffic and network simulators[C]// Proceedings of 11th communications and networking simulation symposium. New York, USA, 2008: 155-163

[22] Behrisch M, Bieker L, Erdmann J, et al. SUMO-Simulation of Urban MObility-an Overview[C]// Proceedings of The Third International Conference on Advances in System Simulation (SIMUL 2011). Barcelona, Spain, 2011: 55-60

[23] Haklay M, Weber P. OpenStreetMap: User-Generated Street Maps[J]. IEEE Pervasive Computing, 2008, 7(4): 12-18

(上接第 88 页)

[7] 邓绍江，李艳涛，张岱固，等. 一种基于混沌的 JPEG2000 图像加密算法[J]. 计算机科学，2009，36(5)：273-275

[8] Hong S C, Li C T, Chen H K, et al. A high speed and high security encryption scheme for JPEG2000 using a chaotic system[C]// Fuzzy Systems and Knowledge Discovery (FSKD), 2011 Eighth International Conference on. IEEE, 2011, 4: 2150-2153

[9] Stutz T, Uhl A. Complexity analysis of the Key-dependent Wavelet Packet Transform for JPEG2000 encryption[C]// 2012 19th IEEE International Conference on Image Processing (ICIP). IEEE, 2012: 2633-2636

[10] Nakachi T, Toyoshima K, Tonomura Y, et al. Layered Multicast Encryption of Motion JPEG2000 Code Streams for Flexible Access Control[J]. IEICE Transactions on Information and Systems, 2012, 95(5): 1301-1312