doi:10.3969/j.issn.1000-436x.2014.04.020

压缩图像码流的分组丢失顽健可伸缩认证算法

易小伟[1,2]，马恒太[1]，郑刚[1]，郑昌文[1]
(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；2. 中国科学院大学，北京 100049)

摘 要：基于图像编码流的结构和相关性特点，提出了一种分组丢失顽健的可伸缩流认证方法。通过利用散列链和纠错编码算法构造认证算法，该方法可实现优化的码率分配以及非平等认证保护（UAP, unequal authentication protection）。首先对图像编码码流进行解析，获得层次结构信息和编解码依赖性；然后，根据码流数据对重构图像质量的重要程度，利用散列链将次重要的码流数据链接到重要数据上；最后对解码独立码流的散列值和整个码流的数字签名进行纠错编码，提高认证算法对分组丢失的顽健性。该方法仅需要对整个图像码流做一次签名，具有很低的认证代价。实验结果表明，与其他 3 种流认证算法相比，此法的认证图像具有更高的重构质量。

关键词：图像认证；顽健性；图像编码；流认证；端到端质量
中图分类号：TP391 **文献标识码**：A **文章编号**：1000-436X(2014)04-0174-08

Packet-loss robust scalable authentication algorithm for compressed image streaming

YI Xiao-wei[1,2], MA Heng-tai[1], ZHENG Gang[1], ZHENG Chang-wen[1]
(1. Integrated Information System on Science and Technology Lab, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China;
2. University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: Based on structures and dependencies of the image codestreams, a scalable stream-level authentication approach was proposed to resist packet loss. To construct the authentication algorithm by hash chaining and error-correction coding, the proposed approach can realize optimizing bit-rate allocations and unequal authentication protection. Firstly, the compressed streams of the original image are analyzed to obtain hierarchical structures and coding dependencies. Secondly, in accordance with the differentiation-importance of codestreams to the reconstructed image, sub-important packet is linked to more important packets via hash chains. Finally, these hash values of decoding-independent packets and the digital signature of the whole bitstream are encoded with an error-correction coding algorithm. The proposed scheme has a very low authentication overhead because it signs on the whole image once. Experimental results show that the authenticated image of the proposed scheme has high reconstructed quality than the other three stream-level authentication schemes.

Key words: image authentication; robustness; image coding; streaming authentication; end-to-end quality

1 引言

随着多媒体应用技术的迅猛发展和内容分发网络（CDN, content delivery network）的日益普及，图像数据的安全传输变得越来越重要。图像完整性和数据源认证等安全问题一直受到了广泛关注[1,2]。传统的方法对每个数据分组进行数字签名需要很大的计算代价和认证数据开销。另一方面，数据分组发生比特错误或丢失将导致整个码流不能被认证。然而图像在网络传输过程中误码分组丢失是无法避免的，为了保证数据的实时性、降低通信代价通常不能对分组丢失进行重传。此外，由于 CDN 网络具有异构特点，终端应用需要根据图像质量和码率需求对认证码流实现可伸缩验证。因此，设计

收稿日期：2013-01-01；**修回日期**：2014-02-24
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2012AA011206）
Foundation Item: The National High Technology Research and Development Program of China (863 Program) (2012AA011206)

一种分组丢失顽健的可伸缩图像认证算法对图像数据的安全分发具有重要的研究意义。

近年来，一种基于压缩流的图像认证方法取得了迅速的发展[3]。这类方法通过对压缩后的图像码流进行认证，对分组丢失具有很强的顽健性[4]，并且具有认证可伸缩性。文献[5]最早提出利用散列链将码流数据串联起来，这样只需要对最后的数据分组做数字签名就可以完成对整个图像流的认证。但该方法的分组丢失顽健性不是很强，任意的数据分组丢失将会导致随后的所有数据分组无法获得认证。文献[6]通过构造 MHT 树（MHT, merkle hash tree）实现对码流的认证，该方法虽然弥补了文献[5]中算法的不足，但是它的认证代价很大。EMSS 算法[7]增加每个数据分组散列链的数目提高分组丢失顽健性。文献[8]中通过引入 2 种不同的散列链来增强抵抗突发分组丢失的能力。文献[9]设计了一种基于蝶形图的视频流认证算法。通过建立失真—代价优化模型，文献[10]提出了一种适用于 JPEG-2000 图像流的认证方案。针对无线传感网络的特点，文献[11]和文献[12]设计了一种基于质量驱动的网络资源管理架构，并利用该架构提出了一种优化的认证方案。文献[13]利用 IDA 编码方法对认证数据进行纠错编码以提高分组丢失顽健性。文献[14]通过 2 次运用 IDA 编码以减小认证算法的代价。文献[15]利用 FEC 码来认证可伸缩视频流。为了实现最优的比特资源分配，文献[16~18]提出了联合信源—信道—认证的资源分配优化模型。但上述认证算法没有利用码流结构特征和编解码的相关性，因此不能够获得最优的端到端质量和最小的认证代价。

为了提供针对压缩码流的认证保护，本文首先介绍了 CCSDS IDC（consultative committee for space data systems image data compression）编码器[19~21]的编码流程以及码流的组织结构。在此基础上，进一步分析了 CCSDS 图像压缩码流的结构特征和码流的编解码相关性。然后设计了一种基于位平面编码的分层组包策略，该组包策略能够保持编码流的结构属性。进而提出了一种可伸缩的流认证算法。最后，本文比较分析了算法的性能。

2　CCSDS IDC 码流结构

CCSDS 图像数据压缩算法的流程如图 1(a)所示，CCSDS IDC 编码器主要包括 2 个功能模块：离散小波变换（DWT, discrete wavelet transform）模块和位平面编码（BPE, bit-plane encoder）模块。DWT 模块通过离散小波变换去除输入图像数据的相关性，然后 BPE 模块对去相关数据进行位平面编码输出编码数据流。编码后码流的组织结构如图 1(b)所示。

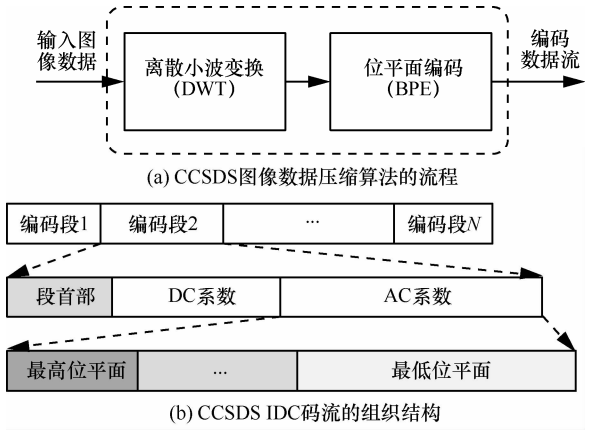


图 1　CCSDS 图像数据压缩算法的流程与 CCSDS IDS 码流的组织结构

在位平面编码过程中，BPE 模块首先按照光栅扫描顺序将小波系数组织成若干个独立的编码段（segment），然后依次对每个编码段进行熵编码。每个编码段由多个编码块（block）组成，而每个编码块包含 1 个 DC 系数和 63 个 AC 系数，这些系数分布在不同的子代。DC 系数集中了图像的大部分能量和主要内容信息，而 AC 系数主要包含图像的纹理信息和细节信息。

每个编码段除段首部数据外，还包括 DC 系数编码数据和 AC 系数编码数据。BPE 模块采用 Rice 编码算法对量化的 DC 系数进行编码，而对 AC 系数采用位平面编码算法。最后每个编码段生成嵌入式的编码比特流已提供数据的渐进式传输。

位平面编码算法对 AC 系数按照从最高位平面（MSB）到最低位平面（LSB）的顺序依次进行编码，因此高位平面的编码数据较低位平面的编码数据对重构图像的质量影响较大。

3　流认证算法

本节首先分析了 CCSDS IDC 编码流的特点包括层次化结构、编解码依赖关系和重要性差异。然后通过联合散列链和 ECC(error-correcting code)编码技术提出了一种低复杂度的实现算法。最后阐述了本文算法如何实现可伸缩认证。

3.1　CCSDS IDC 编码流分析

在第 2 节中介绍了 CCSDS IDC 的编码流程和

码流的组织结构，根据位平面编码过程可以推断压缩后的图像码流主要体现了如下 3 个特点。

1) 层次结构。BPE 编码器对小波系数依次按照位平面进行渐进式编码，生成后的编码流可以根据位平面划分为不同的质量层。随着嵌入式码流的解码层数的增加，图像的质量逐渐增强和图像的总码率也变大。

2) 编解码依赖关系。一方面，各子带的小波系数按照相对位置被组织成不同的段，每个段内的小波系数进行独立熵编码。因此不同段的解码相互独立。另一方面，对每个段内的小波系数进行嵌入式位平面编码。因此在同一编码段内的不同位平面编码流是解码线性依赖的。换言之，低位平面的码流解码与它的上层码流是相关的。如果其上层某个位平面的编码数据不能被正确解码，那么当前层的码流同样不能被解码。

3) 重要性差异。由于不同子代的小波系数对重构图像的质量贡献度不同，例如低频的直流系数（DC 系数）相比高频的交流系数（AC 系数）更能提高图像的质量。因此高位平面的编码数据比较低位平面的编码数据对图像质量的提升更重要。

为了保持编码流的结构属性，本文采用一种分层的组包策略，如图 2 所示。压缩流依次按照 DC 系数、AC 系数从高位平面到低位平面分别进行码流打包。分层组包策略具有以下几个特点。

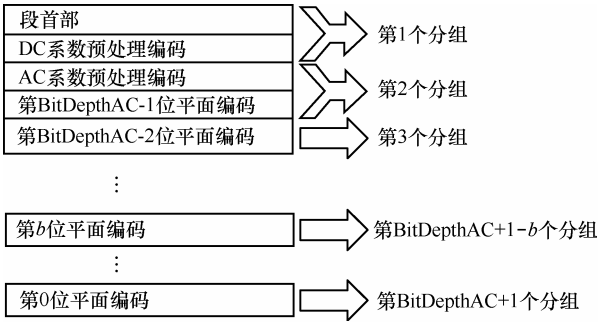


图 2 基于 BPE 编码的分层组包策略

1) 保持了压缩流的层次化结构。基于可伸缩流的编码特性，这些信息为支持灵活的可伸缩认证提供了基础。

2) 维持了码流间的编解码相关性。通过这种策略生成的数据分组只包含某个编码段的数据，不同编码段的数据不会分在同一个分组。这样就保证了下一个编码段能够被独立正确地解码，同时实现了差错控制。

3) 根据码流的特征，在同一个编码段内数据分组的重要度按照码流输出顺序逐渐减弱。这将为流认证算法实现不平等保护提供依据。

另外，由于 CCSDS IDC 编码器对 AC 系数进行位平面编码时采用可变长编码（VLC, variable length coding）算法，因此每个数据分组的大小可以是不一样大小。通常地，高位平面的数据具有更大相关性，因而能够实现较大的压缩比，所以压缩后比低位平面的数据量要更小。

3.2 本文算法

考虑到信道误码分组丢失的影响，数据分组丢失将会导致其他数据分组不能被认证或解码。在接收方仅当数据分组同时能够被认证和解码时，该数据分组才能起到提升图像质量的作用。为了获得最优的端到端质量，认证算法需要保证每个可解码的数据分组能够被验证[22]。

基于上述思想，本文通过利用散列链和纠错编码方法设计了一种快速的流认证算法，该算法能够获得近似最优的性能。图 3 是针对 CCSDS IDC 编码流设计的认证算法，包含 N 个独立的编码段、每个编码段由 1 个 DC 层和 K 个 AC 层组成。每一行表示同一质量层的数据分组，每一列表示一个编码段的数据分组。例如，第 n 个编码段的第 k 个质量层的数据分组记为 $P_k^n\{k=0,\cdots,K,n=1,\cdots,N\}$。值得注意的是，在实际情况中，每个编码段可能包含不同数目的质量层，但这不影响认证算法的执行。因为相同质量层可以包含来自不同位平面的编码数据分组，这只会改变某个编码段散列链的长度。但是为了算法的描述方便，这里假定每个编码段都包含 K+1 个质量层。图中 v_{ECC}、v_{sig} 分别表示纠错编码节点和签名节点。图中的有向边 $e(P_l,P_m)$ 表示计算 P_l 的散列值并链接到 P_m，$e(P_n,v_{\mathrm{ECC}})$ 表示对 P_n 做纠错编码，$e(P_m,v_{\mathrm{sig}})$ 表示对 P_m 的特征做数字签名。

认证算法的基本思想主要包含如下两部分：1) 在相同的编码段内，采用线性散列链按照数据分组的编解码依赖关系进行链接；2) 对不同编码段数据分组的认证信息进行纠错编码。具体的认证过程按照如下步骤进行。

step1 对于每个编码段 $S_n(n=1,\cdots,N)$，计算 P_k^n 的散列值并且将该散列值链接到 P_{k-1}^n，即 $P_{k-1}^n \leftarrow P_{k-1}^n \| H(P_k^n)(k=K,\cdots,1)$。其中 $H(\cdot)$ 是散列函数，“||”表示串接操作。

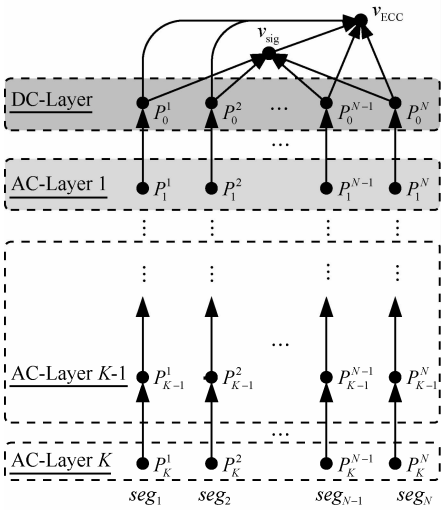


图 3　CCSDS IDC 编码流的认证算法

step2　计算 DC 层数据分组的散列值 $\{H(P_0^n)\}_{n=1}^N$，生成码流的数字签名 $(H(C),P_{sig})$，其中 $C \triangleq H(P_0^1) \| \cdots \| H(P_0^N)$，$P_{sig} \triangleq \mathrm{Sig}_{pri}(H(C))$（$\mathrm{Sig}_{pri}(\cdot)$ 是数字签名函数，*pri* 是发送方的私钥）。

step3　对认证信息 $(C \| P_{sig})$ 进行 IDA 编码，计算得到 $F \triangleq \mathrm{IDA}(C \| P_{sig},\theta)$。其中 IDA(·) 是 IDA 编码函数，$\theta$ 是 IDA 编码参数。

step4　划分认证编码数据 F 成 N 等分 $\{F_i\}_{i=1}^N$，将分片 F_n 链接到 DC 层数据分组 P_0^n，即 $P_0^n \leftarrow F_n \| P_0^n (n=1,\cdots,N)$。

通过分析编码流的编解码相关性，联合采用散列链和纠错编码方法保证了认证关系和编解码依赖关系的一致性。因此认证算法不会导致额外的图像质量的下降。此外，实现了对码流的非平等认证保护（UAP, unequal authentication protection）。一方面，通过利用散列链接将不同质量层的数据分组按照重要度链接起来，将次重要的数据分组链接到较重要的数据分组后面，从而保证了重要度高的数据分组比较低重要度数据分组具有更高的可认证概率。另一方面，通过调节 IDA 编码参数 θ，使得 DC 层的数据分组能够抵抗更强的信道误码分组丢失，但是同时也增加了认证代价。

3.3　可伸缩认证

文中提出的流认证算法仅仅需要对整个图像码流做一次数字签名，但是可以有多种不同的认证方式，实现了“一次签名，可伸缩认证”。该特点对实际中异构的 CDN 网络具有重要的意义，服务器只需要对原始图像数据做一次编码和认证，而在接收端的应用能够根据自身需求（例如，图像质量和分辨率等）和信道带宽（有线网络和无线网络）实现对码流的可伸缩认证。通过利用这一特性，服务器只需要向网络中分发一份可信数据，而不需要针对不同的应用终端做多份图像数据压缩和认证，极大地节省了服务器开销和网络带宽消耗。

接收方按照如下步骤执行码流的可伸缩验证。

step1　假设接收到的 DC 层数据分组集合 $\{\tilde{P}_0^n\}$，计算 $\rho \triangleq 1-\left|\{\tilde{P}_0^n\}\right|/N$。如果 $\rho \leqslant \theta$ 则执行 step2，否则结束码流并开启新会话。

step2　从 $\{\tilde{P}_0^n\}$ 取出 $\{\tilde{F}_i\}$，进行 IDA 解编码获得 $\tilde{C} \| \tilde{P}_{sig} \triangleq \mathrm{IDA}^{-1}(\{\tilde{F}_i\})$（其中 $\mathrm{IDA}^{-1}(\cdot)$ 为 IDA 译码函数）。验证码流数字签名 $(H(\tilde{C}),\tilde{P}_{sig})$，如果 $\mathrm{Ver}_{pub}(\mathrm{H}(\tilde{C}),\tilde{P}_{sig}) = \mathrm{TURE}$（其中 $\mathrm{Ver}_{pub}(\cdot)$ 为签名验证函数，*pub* 是发送方的公钥）则执行 step3，否则结束码流并开启新会话。

step3　对所有接收到 $\{\tilde{P}_0^n\}$，抽取 $\tilde{C}$ 的第 n 个分片 $\tilde{C}_n$，并计算 $H(\tilde{P}_0^n)$。如果 $\tilde{C}_n = H(\tilde{P}_0^n)$ 则 $\tilde{P}_0^n$ 是可信的，否则丢弃 $\tilde{P}_0^n$。

注：重复执行 step4 和 step5 直到图像质量或码率达到预期预置值。

step4　验证随后接收到数据分组 $\tilde{P}_k^n (k>0)$，如果 $\tilde{P}_{k-1}^n$ 是可信的则执行 0，否则丢弃 $\tilde{P}_k^n$。

step5　从 $\tilde{P}_{k-1}^n$ 取出 $H(P_k^n)$，并计算 $H(\tilde{P}_k^n)$。如果 $H(P_k^n) = H(\tilde{P}_k^n)$ 则 $\tilde{P}_k^n$ 是可信的，否则丢弃 $\tilde{P}_k^n$。

4　性能分析

4.1　安全性分析

在本文算法中，采用散列链、数字签名和纠错编码方法来构建优化认证算法。与已有的流级认证算法一样，认证算法的安全性可以通过公钥基础设施（PKI）得到保证，并且算法的安全性强度依赖于所选择的密码学算法[3]。下文分析了本文算法在抵抗一些通常攻击方面的安全性。

1) 伪装攻击。签名方的密钥环通过 PKI 体系进行管理和分发，所有实体（包括验证方和攻击者）都能够获得签名方的公钥 *pub*，但是无法获知它的私钥 *pri*。虽然攻击者可以利用一个假的私钥 *pri′* 伪造一个对整个码流的签名 $\hat{P}_{sig} = \mathrm{Sig}_{pri'}(H(C))$，但是验证方可以通过 $\mathrm{Ver}_{pub}(H(C),\hat{P}_{sig}) = \mathrm{FALSE}$ 来判断签名是无效的。因此攻击者无法对流认证算法成

表 1 认证算法性能比较

认证算法	O_c	O_t	P_{ver}	D_s	D_r
简单散列链[5]	NK, 1	$h+\frac{g}{NK}$	< 1	NK	1
认证树[6]	2NK-1, 1	$h\mathrm{lb}(NK)+g$	= 1	NK	1
EMSS[7]	NK+1, 1	$6h+\frac{g}{NK}$	< 1	1	NK
增强散列链[8]	NK+1, 1	$2h+\frac{g}{NK}$	< 1	p	NK
蝶形图[9]	NK+1, 1	$2h+\frac{g}{NK}$	= 1	NK	1
内容相关[10]	NK+1, 1	$(1+\frac{1}{sK}\sum_{i=1}^{s}\gamma_i)h+\frac{g}{NK}$	< 1	NK	1
SAIDA[13]	NK+Nc, N	$\frac{Kh+g}{(1-\theta)K}$	= 1	K	$(1-\theta)K$
cSAIDA[14]	NK+2Nc, N	$\frac{\lceil \rho K \rceil h+g}{(1-\rho)K}$	= 1	K	$(1-\rho)K$
本文算法	NK+c, 1	$\frac{Nh+g}{(1-\theta)NK}+\frac{(K-1)h}{K}$	= 1	NK	$(1-\theta)N$

功实施伪装攻击。

2) 重放攻击。假定攻击者重放某个或某几个 DC 层的数据分组 $\{\hat{P}_0^n\}(n=1,2,\cdots,N)$，这将导致所有收到的数据分组都无法通过验证，除非将所有 DC 层的数据分组都替换为上一个会话中所使用的包。然而，这个问题可以通过为每个传输分组添加一个时间戳或者序号来避免。如果重放 AC 层的数据分组 $\{\hat{P}_k^n\}$ $(k\geqslant 1)$，这可以通过检查 $H(P_k^n)\neq H(\hat{P}_k^n)$ 来发现重放的数据分组。其中 $H(P_k^n)$ 包含于 P_{k-1}^n 中，而 P_{k-1}^n 是可信的。

3) 篡改攻击。认证算法通过应用密码散列函数来保证数据的完整性。即便修改压缩流散列值的一个比特也将导致该数据分组不能通过完整性验证。此外，篡改后的码流数据分组将因为无法被正确解码而丢弃。

4) DoS 攻击。流认证算法不能很好地抵抗 DoS 攻击。例如，攻击者只需要修改 DC 层的任何数据分组 $\{\hat{P}_0^n\}(n=1,2,\cdots,N)$，整个码流都无法被验证，签名方需要同验证方重新开启新的会话。

值得注意的是，在本文提出的认证算法中，可以自由地替换所使用的密码学算法以实现多等级安全需求。例如，本文仿真实验使用 SHA-1 作为散列函数以及 RSA 算法进行数字签名和验证。

4.2 与其他算法比较

下面分析比较了本文算法和其他认证算法在计算代价、通信代价、验证概率、发送时延和接收时延等方面的性能。性能指标的定义如下。

1) 计算代价 O_c：发送方/接收方执行散列操作和签名操作/验证操作的次数。

2) 通信代价 O_t：每个数据分组所携带的认证信息的平均大小。

3) 验证概率 P_{ver}：有效数据分组（同时可验证和可解码）数目和可解码数据分组数目的比值。

4) 发送时延 D_s：在发送方，第一个数据分组传输前需要缓存的数据分组数目。

5) 接收时延 D_r：在接收方，第一个数据分组验证前需要缓存的数据分组数目。

表 1 比较了本文算法与其他 8 种流认证算法在上述 5 个性能指标下的性能。表中的结果基于下面一些合理的假设。

1) 图像编码流包含 N 个编码段，每个编码段具有 1 个 DC 层和 K 个 AC 层。

2) 散列值的大小为 h byte，数字签名的大小为 g byte。

3) 对于 EMSS 算法，每个节点的冗余度为 6，

并且采用“5-11-17-24-36-39”分组链接方案。

4) 对于增强散列链算法，发送方的分组缓存大小为 p 。

5) 对于蝶形图算法， N 等于 2^K 。

6) 对于 SDIDA 算法、cSAIDA 算法和本文算法，c 指进行认证信息 IDA 编码的计算代价，θ 是 IDA 编码参数，$\rho = E[p_{\text{loss}}]$ 表示预期分组丢失概率。

通过对表 1 分析可以得到下述结论。

1) 在计算代价方面，SDIDA 算法和 cSAIDA 算法需要对码流做 N 次签名，而其他算法仅需要签名一次。认证树算法相比于其他算法，需要多执行 NK 次散列操作建立 Merkle 散列树。SDIDA 算法和 cSAIDA 算法对每个编码段的认证信息进行独立编码，而本文算法仅需要为整个码流的认证信息做一次编码。

2) 简单散列链算法具有非常低的通信代价，但是它的验证概率最低。相反地，认证树算法具有完全的验证概率（等于 1 ），但是它的通信代价很高。这 2 种算法是极端情况，其他算法实现了两者间的平衡。EMSS 算法、增强散列链算法和内容相关算法不能获得最优的端到到质量，因为散列链的断裂将导致某些可解码的数据分组无法被验证。由于需要为每个编码段生成签名，因此 SDIDA 算法和 cSAIDA 算法具有非常高的通信代价。蝶形图算法包含很高的认证信息冗余，因为很多数据分组链接到编码无关的数据分组。本文算法保持了认证关系和编码关系的一致性，因此它能够获得最优的端到端质量和最小的认证代价。

3) 在发送时延和接收时延方面，简单散列链算法、认证树算法、蝶形图算法和内容相关算法的发送时延都为 NK 、接收时延都为 1。由于接收时延导致无法验证和解码同一质量层的数据分组，因此 EMSS 算法、增强散列链算法、SDIDA 算法和 cSAIDA 算法都无法支持图像码流的渐进传输。虽然本文算法需要接收方缓存 DC 层的数据分组以实现 IDA 解码，但是它同样支持对图像码流的渐进传输，因为 DC 层的数据分组对保证提供基本图像质量是必不可少的。

5　仿真实验与讨论

仿真实验测试了 12 幅不同分辨率下的 8 位灰度图像，分析比较了本文算法和其他 3 种典型的流认证算法。对于 CCSDS IDC 编码器，实验采用了整数 DWT 变换和基于带扫描的图像数据无损压缩模式。信道仿真采用无记忆分组丢失模型，假定数据分组丢失的概率 $p_{\text{loss}}(P_k^n)$ 都等于 ρ ，并且相互独立。

图 4 显示了在不同分组丢失率条件下无认证情况和其他 4 个认证算法重构图像的 PSNR 值。从图中可以发现，本文算法和 SAIDA 算法的 PSNR 值等于无认证时重构图像的 PSNR 值。而且在任意分组丢失率情况下，本文算法比 EMSS 算法的 PSNR 值要高出 0.3dB 到 1dB。事实上，无认证时 PSNR 值曲线是认证方案的一个理论上界。由于本文算法能够保证所有可解码数据分组都通过验证，因此它能够获得理论上的最大值。这个实验结果可以表明在分组丢失信道条件下本文算法能够获得最优的端到端认证图像质量。

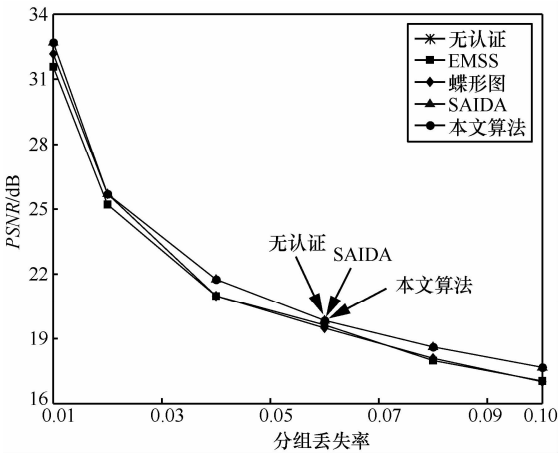
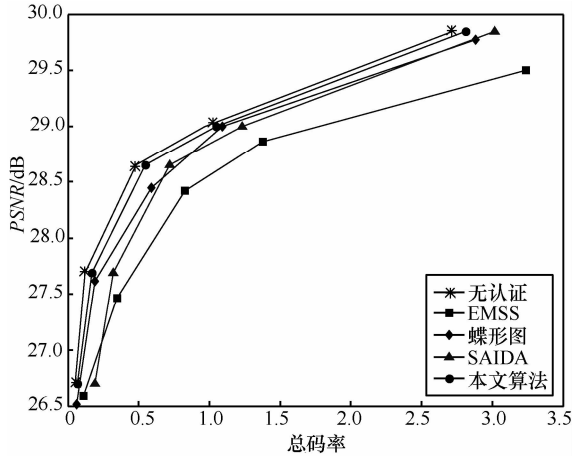
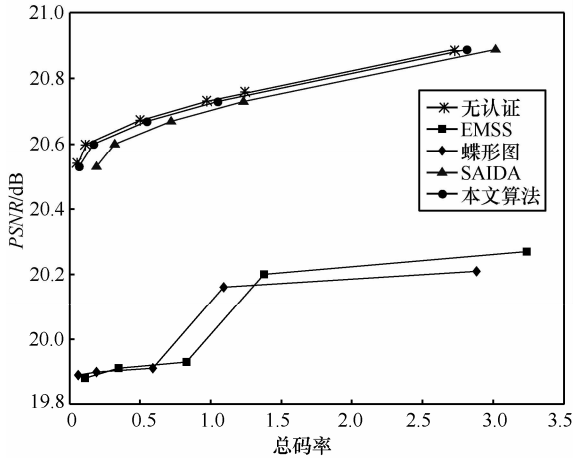


图 4　不同分组丢失率下图像质量

端到端的 R-D 曲线能够综合评估认证算法的性能，包括认证图像的端到端质量和认证码率。在实验中设定 IDA 编码参数 θ 的值等于 0.5，实验结果如图 5 所示。图 5(a)显示了在信道分组丢失率等于 1%的条件下认证算法的总码率和图像 PSNR 值之间的关系。从图中可以看出，在相同码率下本文算法的 PSNR 值要高于其他 3 种认证算法，而且与无认证时的性能很接近。在另一个方面，为了获得预置的端到端认证质量，本文算法相比于其他 3 种认证算法所需要的认证代价更小。图 5(b)比较了在信道分组丢失率为 5%的条件认证算法的综合性能。与图 5(a)有类似的结果，本文算法的 R-D 曲线一直优于 EMSS 算法、蝶形图算法和 SAIDA 算法，并且随着分组丢失率的增大，本文算法的性能几乎达到理论值上界（无认证时）。这一实验结果表明了本文算法能够实现端到端质量和认证代价之间的更优权衡。



(a) ρ = 1%，θ = 0.5



(b) ρ = 5%，θ = 0.5

图 5　端到端的 R-D 曲线

实验测试了不同 IDA 编码参数θ对本文算法性能的影响。实验设置信道分组丢失率等于 2%，仿真结果如图 6 所示。通过对θ等于 0.05、0.2 和 0.8 时 R-D 曲线的比较发现，当θ等于 0.2 时算法的性能最好。因为当θ等于 0.05（小于ρ）时算法不能保证获得最优的认证质量，而当θ等于 0.8（大于ρ）时增加认证代价不能带来更高的认证质量提升。可以通过利用领域搜索的方式求解最优的θ值，实验结果表明最优的θ值比ρ稍大。通过实验可以发现尽管当θ等于 0.8 时算法的性能不是最优，但是与θ等于 0.8 时的性能相比相差不大。

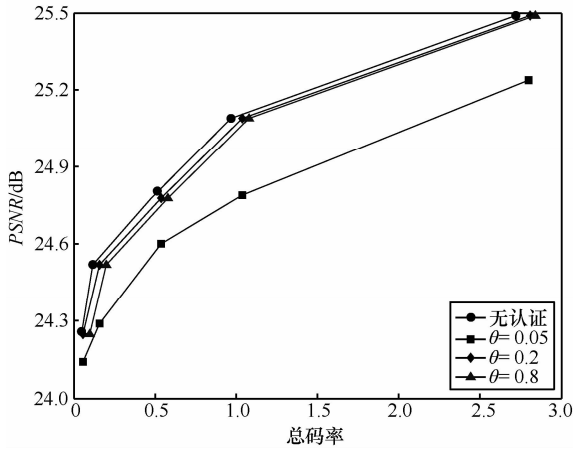


图 6　不同θ下端到端 R-D 曲线(ρ=2%)

6　结束语

本文通过联合散列链和纠错编码技术，提出了一种可伸缩的流认证算法，该算法对信道分组丢失具有更强的顽健性。为了获得优化的端到端质量，分析并利用 CCSDS IDC 编码流的层次结构特点和编解码相关性，进而实现对压缩流的非平等认证保护。性能分析和实验结果表明，本文算法的端到端 R-D 曲线比其他流认证算法更优。值得进一步研究的工作包括建立联合信源信道编码的认证优化模型、设计信道自适应的认证优化方法。

参考文献：

[1] LEI J, HAN Z, VÁZQUEZ-CASTRO M A, *et al*. Secure satellite communication systems design with individual secrecy rate constraints[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3):661-671.

[2] 文昌辞, 王沁, 黄付敏等. JPEG 彩色图像自适应加密算法[J]. 计算机辅助设计与图形学学报, 2012, 24(4): 500-505.
WEN C C, WANG Q, HUANG F M, *et al*. Self-adaptive encryption for JPEG color images[J]. Journal of Computer-Aided Design & Computer Graphics, 2012, 24(4): 500-505.

[3] SUN Q, APOSTOLOPOULOS J, CHEN C W, *et al*. Quality-optimized and secure end-to-end authentication for media delivery[J]. Proceedings of the IEEE, 2008, 96(1): 97-111.

[4] HEFEEDA M, MOKHTARIAN K. Authentication schemes for multimedia streams: quantitative analysis and comparison[J]. ACM Transactions on Multimedia Computing, Communications and Applications, 2010, 6(1):1-24.

[5] GENNARO R, ROHATGI P. How to sign digital streams[A]. Proceedings of the Advances in Cryptology[C]. Springer, 1997. 180-197.

[6] WONG C K, LAM S S. Digital signatures for flows and multicasts[A]. Proceedings of the IEEE International Conference on Network Protocols[C].1998. 198-209.

[7] PERRIG A, CANETTI R, TYGAR J, *et al*. Efficient authentication and signing of multicast streams over lossy channels[A]. Proceedings of the IEEE Symposium on Security and Privacy[C]. 2000.56-73.

[8] GOLLE P, MODADUGU N. Authenticating streamed data in the presence of random packet loss[A]. Proceedings of the Network and Distributed Systems Security Symposium[C]. 2001.13-22.

[9] ZHANG Z, SUN Q, APOSTOLOPOULOS J, *et al*. Generalized butterfly graph and its application to video stream authentication[J]. IEEE Transactions on Circuits Systems for Video Technology, 2009, 19(7):

965-977.

[10] ZHANG Z, SUN Q, WONG W C, *et al*. An optimized content-aware authentication scheme for streaming JPEG-2000 images over lossy networks[J]. IEEE Transactions on Multimedia, 2007, 9(2): 320-331.

[11] WANG W, PENG D, WANG H, *et al*. A multimedia quality-driven network resource management architecture for wireless sensor networks with stream authentication[J]. IEEE Transactions on Multimedia, 2010, 12(5): 439-447.

[12] WANG W, WANG H, HUA K, *et al*. Quality-optimized energy neutrality with link layer resource allocation for zero-power harvesting wireless communications[A]. Proceedings of the Global Telecommunications Conference[C]. 2011.

[13] PARK J, CHONG E, SIEGEL H. Efficient multicast stream authentication using erasure codes[J]. ACM Transactions on Information and System Security, 2003, 6(2): 258-285.

[14] PANNETRAT A, MOLVA R. Efficient multicast packet authentication[A]. Proceedings of the Network and Distributed Systems Security Symp[C]. 2003.

[15] HEFEEDA M, MOKHTARIAN K. Authentication of scalable video streams with low communication overhead[J]. IEEE Transactions on Multimedia, 2010, 12(7):730-742.

[16] LI Z, SUN Q, LIAN Y, *et al*. Joint source-channel-authentication resource allocation and unequal authenticity protection for multimedia over wireless networks[J]. IEEE Transactions on Multimedia, 2007, 9(4): 837-850.

[17] ZHOU L, ZHENG B, WEI A, *et al*. A scalable information security technique: joint authentication-coding mechanism for multimedia over heterogeneous wireless networks[J]. Wireless Personal Communications, 2009, 51: 5-16.

[18] ZHU X, ZHANG Z, CHEN C W. A joint layered coding scheme for unified reliable and secure media transmission with implementation on JPEG 2000 images[A]. Proceedings of the IEEE International Conference on Multimedia & Expo[C]. 2009.710-717.

[19] LI L, ZHOU G, FIETHE B, *et al*. Efficient implementation of the CCSDS 122.0-B-1 compression standard on a space-qualified field programmable gate array[J]. Journal of Applied Remote Sensing, 2013, 3(1):033543.

[20] Image Data Compression[S]. CCSDS Recommendation for Space Data System Standards 1220-B-1 Issue 1 Cor 2, 2008.

[21] 雷震霖. 空间图像 CCSDS 压缩算法研究与 FPGA 实现[D]. 大连: 大连理工大学, 2007.
LEI Z L. Study on CCSDS Space Image Compression Algorithm and FPGA Implementation[D]. Dalian: Dalian University of Technology, 2007.

[22] YI X, LI M, ZHENG G, *et al*. Quality-optimized authentication of scalable media streams with flexible transcoding over wireless networks[A]. Proceedings of the 3rd FTRA International Conference Mobile, Ubiquitous, and Intelligent Computing[C]. 2012.148-153.

作者简介：

易小伟（1987-），男，江西吉安人，中国科学院博士生，主要研究方向为多媒体通信安全。

马恒太（1970-），男，山东临朐人，中国科学院副研究员、硕士生导师，主要研究方向为组网通信、信息安全。

郑刚（1974-），男，河南宜阳人，中国科学院副研究员、硕士生导师，主要研究方向为网络管理与控制技术、信息安全。

郑昌文（1969-），男，湖北大冶人，中国科学院研究员、博士生导师，主要研究方向为计算机仿真、信息安全。