基于跨层优化资源分配的图像流认证方法

易小伟[1, 2*], 马恒太[3], 赵险峰[1, 2], 于海波[1, 2], 郑昌文[3]

[1] 中国科学院信息工程研究所 信息安全国家重点实验室 北京 中国 100093
[2] 中国科学院大学 网络空间安全学院 北京 中国 100049
[3] 中国科学院软件研究所 北京 中国 100190

摘要 图像流认证的丢包鲁棒性问题是图像认证研究的难题之一。现有的流级认证算法通常是在信源-信道分离编码条件下针对某种特定的图像编码方式而设计的, 在抵抗丢包能力方面具有很大的局限性。针对上述问题, 提出一种丢包鲁棒的图像认证优化模型, 并在此基础上提出了在信源-信道联合编码条件下实现信源-认证-信道码率的跨层优化资源分配(Cross-Layer Optimization Resource Allocation, CLORA)方法。首先以可信图像的端到端质量和认证代价为优化目标, 结合基于图认证和基于前向纠错码(Forward Error Correction, FEC)认证方法, 建立认证优化模型(Authentication Optimization Model, AOM), 将图像认证的抗丢包优化问题等价成构造最优认证图(Optimal Authentication Graph, OAG)。然后利用图像码流的编码相关性和认证相关性, 给出了求解 OAG 问题的等价条件, 并在低计算复杂度下给出了构造 OAG 图的两个原子操作。最后提出了基于 CLORA 框架的认证优化方法。由于 AOM 模型仅利用码流的编码相关性信息, 因而可以适用于不同的图像编码算法。JPEG 2000 码流的实验结果表明, 在相同丢包率下本文算法的端到端可信质量比已有算法平均提高了 1.6dB, 能够获得更优的丢包鲁棒性和端到端率失真(Rate-Distortion, R-D)性能。

关键词 图像认证; 丢包鲁棒性; 可信质量; 认证代价; 信源信道联合编码
中图法分类号 TP309.2 **DOI 号** 10.19363/j.cnki.cn10-1380/tn.2018.12.010

An Image Stream Authentication Scheme Based on Cross-Layer Optimization Resource Allocation

YI Xiaowei[1, 2*], MA Hengtai[3], ZHAO Xianfeng[1, 2], YU Haibo[1, 2], and ZHENG Changwen[3]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[3] Institute of Software Chinese Academy of Sciences, Beijing 100190, China

Abstract Packet-loss robustness of image stream authentication is one of the difficulties in image authentication research. Current stream-level authentication algorithms are designed for certain image coding under source-channel separate coding, so there are very limited on resistance of packet loss. In this paper, an image authentication optimization model with packet-loss robustness and a cross-layer optimization resource allocation (CLORA) of source-authentication-channel bitrate under joint source-channel coding are consecutively proposed to solve the above-mentioned problem. Firstly, in order to achieve the optimum end-to-end quality of the authentic image and authentication overhead, an authentication optimization model (AOM) is proposed based on combining two kinds of authentication methods, which include graph-based method and forward error correction (FEC) based method. Therefore, under the AOM, the optimization problem of packet-loss robustness in image authentication is equivalent to constructing the optimal authentication graph (OAG). Secondly, equivalent condition of the OAG is solved by using the coding-dependence of the image streams and the authentication relationship. And then according to the equivalent condition, two elementary operations to construct OAG are given with a very low computational complexity. Finally, an optimized authentication method is proposed by using the CLORA framework. Because the coding-dependence of the codestreams only is utilized in the AOM, the proposed AOM is suited to all kinds of image coding algorithms. Experimental results of JPEG 2000 streams demonstrate that the end-to-end authentic quality of the propose scheme increases by 1.6 dB than the existing authentication schemes with the same packet-loss rates. Therefore, our scheme obtains better packet-loss robustness and better end-to-end rate-distortion (R-D) performance.

通讯作者: 易小伟, 博士, 助理研究员, Email: yixiaowei@iie.ac.cn。
本课题得到国家自然科学基金课题(No. 61303259, No. U1536105)、国家科技支撑计划课题(No. 2014BAH41B01)、国家重点研发计划课题(No. 2016YFB0801003)、中国科学院战略性先导科技专项课题(No. XDA06030600)资助。
收稿日期: 2016-06-19; 修改日期: 2016-09-02; 定稿日期: 2016-09-05

Key words Image authentication; packet-loss robustness; authentic quality; authentication overhead; joint source- channel coding

1 背景

随着多媒体应用的普及, 安全问题越来越受到人们的重点关注[1]。用户需要能够验证接收到的图像是来自可信的服务端, 并且图像内容没有被攻击者篡改。尤其在无线网络中, 由于其开放性攻击者能够更容易地攻击图像数据。不同于通常的数据认证, 为了满足网络应用和传输要求, 需要在有损信道条件下提供对图像流质量的可伸缩验证[2-3]。

传统的技术通常直接利用密码学算法对图像数据做数字签名, 因此即便是只有一个比特差错图像数据也不能被正确认证。此外, 这种认证方式具有非常高的计算开销和空间代价[3]。然而网络中的信道差错是不可避免的, 并且网络的带宽和实时性要求是严格受限的。为了提升算法的鲁棒性, 基于内容的认证算法[4-6]通过对图像的特征描述符做签名来实现对整个图像的认证。但是此类方法在安全性上存在很大的局限性[3], 在验证判决上存在一定的虚警率(False Acceptance Ratio, FAR)和漏警率(False Rejection Ratio, FRR), 并且算法的可靠性依赖于所选取的特征集。

近年来, 一类在码流级或数据包实施图像内容认证的算法[7-18]获得了广泛的应用, 它能够提供理论上可证明的安全性。流级认证方法主要包括基于图构造的认证算法[7]和基于前向纠错码(Forward Error Correction, FEC)编码的认证算法[8]。文献[7]利用哈希链将数据包的哈希值串接到其它数据包, 然后对最后的数据包签名。当某个数据包发生丢失情况, 其他数据包可以通过哈希链进行认证。文献[8]利用 FEC 编码认证数据, 它能够抵抗确定的数据包丢失。文献[9]提出了一种适用于JPEG 2000图像流的认证方案。文献[10]设计了一种基于蝶形图的视频流认证算法。文献[11]利用 FEC 编码来认证可伸缩视频流。文献[12]提出了一种基于蝶形图的可伸缩认证算法。文献[13]利用编解码相关性设计了适用于JPEG 2000流的优化认证方案。文献[14]联合 FEC 编码和哈希链提出了一种适用于 JPEG 2000 标准的优化可伸缩认证方法。文献[15]提出了一种适用于 H.264 可伸缩视频流的认证和访问控制方法。文献[16]采用 RS 编码来分段认证文件流, 以抵抗传输或存储中的数据丢失和数据差错。为了提高认证算法对信道丢包的鲁棒性, 文献[17-18]通过建立率失真优化模型提出了CCSDS 图像压缩码流的优化认证方法。在文献[7-12, 16]中没有考虑编解码依赖性, 文献[13, 15]利用编解码相关性设计了适用于 JPEG 2000 流和视频流的优化方案, 然而这些算法仅采用了哈希链, 并不能保持验证相关性与编解码相关性的一致性。

为了实现灵活性和效率间的优化权衡, 通过建立失真-代价优化模型, 针对无线传感网络的特点, 文献[19-20]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认证方案。为了实现最优的比特资源分配, 文献[21-23]提出联合信源-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, 因此不能获得最优的端到端质量和最小的认证代价。

在给定信道误码丢包条件下, 为了使认证算法在较低的认证代价下获得最优的端到端可信质量, 本文在第二部分提出了一个一般化的认证优化模型(Authentication Optimization Model, AOM)。该模型通过联合采用哈希链技术和前向纠错码(Forward Error Correction, FEC)技术, 将流认证问题等价成对认证图(Authentication Graph, AG)的构造。在该优化模型框架下, 满足了获得最优端到端性能的 2 个条件: (1)最优的端到端可信质量。对每个接收到的数据包, 如果它能够被解码则也可以被验证, 进而提高图像的可信质量。也即, 认证算法不会降低图像内容的端到端质量。(2)零认证代价冗余。如果接收到的数据包不能被解码, 那么该数据包同样不能被验证。因为不能解码数据包对图像内容质量没有贡献, 因此用于验证这些对重构图像质量无贡献数据包的认证数据事实上冗余的。第三部分通过利用码流的编解码相关性, 在很低的计算复杂度下给出了 AOM 模型的近似最优解。第四部分结合 JPEG 2000 标准的编码流特征给出了具体的签名生成算法和可伸缩验证算法。第五部分提出了跨层优化资源分配(Cross-Layer Optimization Resource Allocation, CLORA)方法, 在信源-信道联合编码条件下实现信源-认证-信道码率的优化分配。第六部分仿真实验在算法的丢包鲁棒性和端到端率失真(Rate-Distortion, R-D)性能等方面, 同其它经典认证算法进行比较, 验证了 AOM 模型和 CLORA 方法的有效性。最后是本文的结论。

2 认证优化模型(AOM)

为了实现认证算法在认证代价和丢包鲁棒性方

面的优化性能, 本文首先从现有的流级认证算法中抽象出一般化的认证优化模型(Authentication Optimization Model, AOM)。AOM 模型结合了基于图认证算法和基于 FEC 认证算法, 适用于任何图像或视频编码数据, 而与具体的编码方式无关。利用图论原理, AOM 模型将认证优化问题等价成对认证图(Authentication Graph, AG)构造。下面给出 AOM 模型的具体描述。

定义 1. 认证图 G 是一个有向无环图(Directed Acyclic Graph, DAG), 记作 $\langle V_G, E_G \rangle$。其中 $V_G = V_{\text{pkt}} \bigcup \{v_{\text{FEC}}, v_{\text{sig}}\}$, V_{pkt} 表示数据包节点的集合, v_{FEC} 和 v_{sig} 分别表示 FEC 编码节点和签名节点, E_G 是有向边的集合。

对 $\forall P_i, P_j \in V_{\text{pkt}} (i \neq j)$, 有向边 $e(P_i, P_j) \in E_G$ 表示将数据节点 P_i 的哈希值链接到节点 P_j。对 $\forall P_{\text{sig}} \subseteq V_{\text{pkt}}$, 如果对 $\forall P_i \in P_{\text{sig}}$ 都 $\exists e(P_i, v_{\text{sig}}) \in E_G$, 那么有向边集合 $\{e(P_i, v_{\text{sig}}) : P_i \in P_{\text{sig}}\}$ 表示对节点集合 P_{sig} 做签名。同样地, 假设 $P_{\text{FEC}} = \{P_j : \forall e(P_j, v_{\text{FEC}}) \in E_G, P_j \in V \setminus \{v_{\text{FEC}}\}\}$, 如果对 $\forall P_j \in P_{\text{FEC}}$ 都 $\exists e(P_j, v_{\text{FEC}}) \in E_G$, 那么有向边集合 $\{e(P_j, v_{\text{FEC}}) : P_j \in P_{\text{FEC}}\}$ 表示对节点集合 P_{FEC} 做FEC编码。

定义 2. 节点冗余度 δ_m 表示图 G 中节点 P_m 的入度, 也即 $\delta_m = degree_{\text{in}}(P_m)$。

对某个给定图像编码流, 我们的目的是构造一个最优的 AG 图 G^*, 使得端到端的码率 R 和失真值 D 的加权平均值最小,

$$G^* = \arg\min_{AG}(R + \lambda D) \tag{1}$$

其中拉格朗日乘子 $\lambda > 0$ 用于调节 R 和 D 两者的比重, 总码率 R 包括信源码率 R_s 和认证码率 R_a。

$$R = R_s + R_a \tag{2}$$

假设 $R_{\text{acc}}^{(n,k)}$ 表示第 n 个编码段前 k 个编码层的累加编码码率, 则 R_s 等于所有编码段码率的总和,

$$\begin{aligned} R_s &= \sum_n R_{\text{acc}}^{(n,k)} \\ &= \sum_n (R_{\text{hdr}}^n + l_{\text{DC}}^n + \sum_{i=k}^{MSB} l_i^n) \end{aligned} \tag{3}$$

其中 $R_{\text{hdr}}^n, l_{\text{DC}}^n, l_i^n$ 分别表示第 n 个编码段中段头大小、DC 系数编码长度和第 i 个位平面编码长度。MSB 为最高有效位平面的数目。

假设 $SIZ_{\text{sig}}, SIZ_{\text{hash}}$ 分别为数字签名和哈希值的大小, 编码节点 $v_{\text{FEC}} \in V_G$, R_a 可以通过下式计算,

$$R_a(G) = \frac{\lceil \delta(v_{\text{FEC}})\theta \rceil SIZ_{\text{hash}} + SIZ_{\text{sig}}}{1-\theta} + SIZ_{\text{hash}} \sum_{P_m \in V_{\text{pkt}}} \delta(P_m) \tag{4}$$

其中 θ 为纠错编码参数, 用来控制认证算法的丢包鲁棒能力。总认证代价包括数字签名和 FEC 编码代价((4)式中第 1 项)加上所有数据包哈希值大小((4)式中第 2 项)。

假定每个数据包带来的的质量失真值是线性可加的, 可信图像的端到端失真值 D 可以表示成如下,

$$D(G) = D_0 - \sum_{P_m \in V_{\text{pkt}}} [1 - p_{\text{loss}}(P_m)] \sigma(P_m) \tau_G(P_m) \Delta D_m \tag{5}$$

其中, D_0 表示当所有数据包都丢失时的总失真值, $p_{\text{loss}}(P_m), \sigma(P_m), \tau_G(P_m)$ 依次指 P_m 的丢失概率、可解码概率和可验证概率。ΔD_m 表示解码 P_m 时失真值的减少量。

假设整幅图像频域的子代记为 b_i, 则可以计算 ΔD_m 为

$$\Delta D_m = \sum_{b_i} \sum_{j \in b_i} G_{b_i} (\hat{y}[j] - y[j])^2 \tag{6}$$

在上式中, G_{b_i} 是子代 b_i 的能量增益因子, $\hat{y}[j], y[j]$ 分别指 b_i 中第 j 个频带系数的重构值和原始值。

通过上述分析, 认证算法的设计可归结为求解认证优化模型(1)—(6), 进而构造出最优的认证图。

3 AOM 模型求解

考虑到信道误码丢包的影响, 数据包丢失将会导致其他数据包不能被认证或解码。在接收方仅当数据包同时能够被认证和解码时, 该数据包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包能够被验证[14]。根据 AOM 模型中(5)式, 欲使得 $D(G)$ 最小, 则对 $\forall P_m \in V_{\text{pkt}}$ 使得 $\sigma(P_m)\tau_G(P_m)$ 最大。另一个方面, 对于给定的 $P_m \in V_{\text{pkt}}$ 将具有不同的 ΔD_m。根据(4)式, 应该对不同的 P_m 采用不平等认证保护(Unequal Authentication Protection, UAP)使得 $R_a(G)$ 最小。

通常可以采用迭代方法搜索 AOM 模型的最优解 G^*, 但是由于 AG 图中一般包含上千个节点(尤其对超高分辨率图像), 因此迭代方法的搜索空间很大。为了降低解空间的搜索代价, 本文利用图像码流的编解码相关性给出了构造最优认证图(Optimal Authentication Graph, OAG)的等价条件。

假定 $\phi_G(\cdot)$ 表示 AG 图构造函数, 其输入值(定义域)是编码数据包集合 V_{cp} 和输出值(值域)是网络传输数据包集合 V_{tp}。$\mapsto_{\text{c}}$ 和 $\mapsto_{\text{a}}$ 分别表示编码相关性和认证相关性。例如, $P_x \mapsto_{\text{c}} P_y$ 表示数据包 P_x 的编解码依赖于数据包 P_y, 也即如果 P_y 不能被解码则 P_x 也无法被正确解码。同样地, $P_x \mapsto_{\text{a}} P_y$ 表示数据包 P_x 的认证依赖于数据包 P_y, 也即如果 P_y 不能被验证则 P_x 也无法被正确验证。(5)式中 $\sigma(P_m)$ 和 $\tau_G(P_m)$ 可以进一步表示为

$$\begin{aligned}\sigma(P_m) &= \Pr(P_m\text{可解码} \mid P_m\text{被接收到}) \\ &= \begin{cases} 1, & P_m\text{编解码独立.} \\ [1-p_{\text{loss}}(P_l)]\sigma(P_l), & P_m \mapsto_{\text{c}} P_l. \end{cases}\end{aligned} \tag{7}$$

和

$$\begin{aligned}\tau_G(P_m) &= \Pr(P_m\text{可验证} \mid P_m\text{被接收到}) \\ &= \begin{cases} 1, & e(P_m, v_{\text{FEC}}) \in E_G. \\ \sum\limits_{\substack{\phi_G(P_m)\mapsto_{\text{a}}\phi_G(P_l) \\ P_l\in V_{\text{pkt}}}} [1-p_{\text{loss}}(P_l)]\tau_G(P_l), & \text{否则.} \end{cases}\end{aligned} \tag{8}$$

根据(7)和(8)式可以得到, AOM 模型(1)－(6)的解取决于 AG 图中节点间的认证相关性和编码相关性。因此, 下文我们首先分别得到最优端到端可信质量和零认证冗余的等价条件。然后利用认证相关性和编码相关性进一步给出构造 OAG 图的等价公式。

引理 1. 假定可解码数据包集合记作 $\Sigma_G \subseteq V_{\text{pkt}}$, 可验证数据包集合记作 $T_G \subseteq V_{\text{pkt}}$, 则下面两个命题等价:

(1) 认证图 $\langle V_G, E_G\rangle$ 达到最优的端到端可信质量。

(2) 对 $\forall P_m \in V_{\text{pkt}}$, 如果 $P_m \in \Sigma_G$ 那么 $P_m \in T_G$ 或者 $P_m \in \Sigma_G \bigcap T_G$。

证明: (1) $\Rightarrow$ (2). 由于认证图 $\langle V_G, E_G\rangle$ 达到最优的端到端可信质量, 即(5)式中可信图像质量的率失真期望值 $E_G[D]$ 最小。因此对 $\forall P_m \in V_{\text{pkt}}$, 如果 $\sigma(P_m)=1$, 那么 $\exists G = \langle V_G, E_G\rangle$, s.t. $\tau_G(P_m)=1$, 也即认证算法不会引入额外的图像质量减低。故对 $\forall P_m \in V_{\text{pkt}}$, 如果 $P_m \in \Sigma_G$ 则 $P_m \in T_G$ 或者 $P_m \in \Sigma_G \bigcap T_G$, 即如果 P_m 是可解码的则能够被验证进而提升可信图像的质量。

(2) $\Rightarrow$ (1). 反证法。假设认证图 $\langle V_G, E_G\rangle$ 不能达到最优的端到端可信质量, 那么 $\exists P_m \in V_{\text{pkt}}$, s.t. $\sigma(P_m)=1$ 且 $\tau_G(P_m)=0$。这是因为在 $\langle V_G, E_G\rangle$ 中, 可解码节点 P_m 带来 ΔD_m 的质量失真值。因此可以得到 $P_m \in \Sigma_G \bigcap \neg T_G$, 这与 $P_m \in T_G$ 相矛盾。所以假设不成立, 也即认证图 $\langle V_G, E_G\rangle$ 达到最优的端到端可信质量。

证毕。

定义 3. 认证图 $\langle V_G, E_G\rangle$ 是零认证冗余的, 如果对 $\forall P_m \in V_{\text{pkt}}$, 验证节点 P_m 的认证数据 r_m 是不可消去的。即若去掉 r_m 则 P_m 不能被验证, 降低可信图像的质量。

引理 2. 假定可解码数据包集合记作 $\Sigma_G \subseteq V_{\text{pkt}}$, 可验证数据包集合记作 $T_G \subseteq V_{\text{pkt}}$, 下面两个命题是等价的。

(1) 认证图 $\langle V_G, E_G\rangle$ 是零认证冗余的。

(2) 对 $\forall P_m \in V_{\text{pkt}}$, 若 $P_m \Subset \Sigma_G$ 则 $P_m \Subset T_G$。

证明: (1) $\Rightarrow$ (2). 反证法。假设命题(2)不成立, 即 $\exists P_m \in \neg\Sigma_G \bigcap T_G$, 那么在认证图 $\langle V_G, E_G\rangle$ 中存在认证代价冗余 R' (用于验证 P_m)。这是因为即便是消去 R', P_m 无法被验证, 可信图像的质量同样不会降低。根据定义 3 可知, $\langle V_G, E_G\rangle$ 不是零认证冗余的。但是这与命题(1)相矛盾。故假设不成立, 即对 $\forall P_m \in V_{\text{pkt}}$, 若 $P_m \Subset \Sigma_G$ 则 $P_m \Subset T_G$。

(2) $\Rightarrow$ (1). 给定认证图 $\langle V_G, E_G\rangle$, 由(2)可以得到: 对 $\forall P_m \in V_{\text{pkt}}$, 如果 P_m 不能解码那么它无法被验证。根据定义 3 可以得到, $\langle V_G, E_G\rangle$ 是零认证冗余的。

证毕。

下面利用上面引理 1 和引理 2 的结论, 我们给出构造 OAG 图的等价条件。

定理 1. AOM 模型(1)－(6)的最优解等价于下面的命题:

$$\begin{aligned}&\exists G^* = \langle V, E\rangle, \forall\, P_u, P_v \in V_{\text{cp}}, \phi_{G^*}(P_u), \phi_{G^*}(P_v) \in V_{\text{tp}}, \text{满足} \\ &\begin{cases} \text{(i)若} P_u \text{编码独立的, 则} e(P_u, v_{\text{FEC}}) \in E_{G^*}. \\ \text{(ii)否则,} \phi_{G^*}(P_u) \mapsto_{\text{a}} \phi_{G^*}(P_v) \text{当且仅当} P_u \mapsto_{\text{c}} P_v. \end{cases}\end{aligned} \tag{9}$$

证明: (1)对 $\forall P_m \in V_{\text{tp}}$, 从(9)-(i)可以得到, 如果 P_m 是编码独立的, 那么 $e(P_m, v_{\text{FEC}}) \in E(G^*)$。再根据(8)式有 $\tau_{G^*}(P_m)=1$。所以, 由 $P_m \in \Sigma_{G^*}$ 可以得到 $P_m \in T_{G^*}$。另一方面, 如果 P_m 是解码依赖于 P_l 的, 即 $\phi_{G^*}^{-1}(P_m) \mapsto_{\text{c}} \phi_{G^*}^{-1}(P_l)$, 那么 $\exists P_k \in V_{\text{tp}}$ 和编码独立的节点 P_k 满足

$$\phi_{G^*}^{-1}(P_m)\mapsto_{\mathrm{c}}\phi_{G^*}^{-1}(P_l)\mapsto_{\mathrm{c}}\cdots\mapsto_{\mathrm{c}}\phi_{G^*}^{-1}(P_k).$$

利用(9)-(ii)可以得到

$$P_m\mapsto_{\mathrm{a}}P_l\mapsto_{\mathrm{a}}\cdots\mapsto_{\mathrm{a}}P_k.$$

此外, 再根据上面的证明有: 如果 P_k 是编码独立的, 则 P_k 能够被验证。进而推得 P_m 是可验证的。因此, 我们可以得到如果 P_m 是可解码的则 P_m 可以被验证。

根据引理 1, $\langle V_{G^*},E_{G^*}\rangle$ 能够获得最优的端到端可信质量。

(2) 同样地, 对 $\forall P_m\in V_{\mathrm{tp}}$, 如果 P_m 是不可解码的, 那么下面的编码链存在断点

$$\phi_{G^*}^{-1}(P_m)\mapsto_{\mathrm{c}}\phi_{G^*}^{-1}(P_l)\mapsto_{\mathrm{c}}\cdots\mapsto_{\mathrm{c}}\phi_{G^*}^{-1}(P_k).$$

不妨设该断点为 $\phi_{G^*}^{-1}(P')$, 根据(9)-(ii)可得, 数据节点 P' 是断点, 所以 P_m 无法被验证。因此, 我们可以得到如果 P_m 是不可解码的则 P_m 不能被验证。

根据引理 2, $\langle V_{G^*},E_{G^*}\rangle$ 是零认证冗余的。

综合上述(1)和(2)可以得到, $\langle V_{G^*},E_{G^*}\rangle$ 在满足零代价冗余条件下能够达到最优的端到端可信质量。因此 $\langle V_{G^*},E_{G^*}\rangle$ 是一个 OAG 图。

证毕。

基于定理 1 的结论, 下文通过利用哈希链和纠错码技术给出构造 OAG 图的两个基本操作。在很低复杂度情况下, 认证算法能够达到更优的端到端性能。

在 (5) 中, 为了保证当 $e(P_m,v_{\mathrm{FEC}})\in E_G$ 时 $\tau_G(P_m)=1$ 成立, 需要选择合适的 FEC 编码参数 θ。通常编码参数 θ 与当前信道编码条件相关, 比如丢包概率和比特差错率。根据(9)式, OAG 图能够通过下面两种基本操作实现:

(RI)构建线性哈希链。

根据(9)-(ii)可以得到, OAG 图的认证相关性与编码相关性是一致的。因此, 如果满足关系 $P_m\mapsto_{\mathrm{c}}P_l$, 那么在认证图 $\langle V_G,E_G\rangle$ 中需要保持关系 $\phi_G(P_m)\mapsto_{\mathrm{a}}\phi_G(P_l)$, 即在 $\langle V_G,E_G\rangle$ 中生成有向边 $e(P_m,P_l)$。

(RII)确定编码独立集合 P_{ind}。

根据(9)-(i)可以得到, 在 OAG 图中编码独立数据包需要能被独立验证。因而对 $\forall P_k\in P_{\mathrm{ind}}$, 在 $\langle V_G,E_G\rangle$ 中生成有向边 $e(P_k,v_{\mathrm{FEC}})$。

另外, 由于数字签名同信源编码无关, 因而 v_{sig} 需要链接到 v_{FEC} 以实现对签名数据的抗丢包保护, 也即 $e(v_{\mathrm{sig}},v_{\mathrm{FEC}})\in E_G$。在构造 OAG 图过程中, 通过反复利用基本操作(Ⅰ)和(Ⅱ)直到图中的所有节点都满足(9)式。

利用上述方法构造的认证图 $\langle V_G,E_G\rangle$ 能够保证对 $\forall P_k\in V_{\mathrm{pkt}}$, 至少存在一条从数据包节点 P_k 到签名节点 v_{sig} 的路径。因而实现对每个数据包的验证, 进而能够实现对整个图像码流的“一次签名, 全部认证”。

在计算效率方面, 由于在构造认证图时仅采用(Ⅰ)和(Ⅱ)两种操作, 因而认证算法的计算开销主要包括 2 个部分: (1)判断是采取基本操作(Ⅰ)或(Ⅱ)的计算开销。(2)基本操作(Ⅰ)和(Ⅱ)的计算代价。对于求解 AOM 模型, 也即构建 OAG 图的计算开销是指判断采取基本操作(Ⅰ)或(Ⅱ)的计算代价, 而这部分代价相对于通常的迭代搜索算法的计算量是非常小的, 因为数据节点间的编解码相关性能够在编码器中很容易被确定。

4 本文算法

利用 JPEG 2000 码流特点和上文提出的 AOM 模型, 本文实现了一种适用于 JPEG 2000 流的最优认证算法。为了构建 OAG 图, 首先分析了 JPEG 2000 流的编解码相关性和各部分重要性。然后利用哈希链技术和 FEC 码技术来实现签名生成算法。最后论述了在 OAG 图下, 如何实现可伸缩验证。

4.1 JPEG 2000 码流特征

JPEG 2000 编码器按照分片(Tile)、分量(Component)、分辨率(Resolution)、辖区(Precinct)、质量层(Layer)和包(Packet)对图像进行编码并组织码流。编码器生成的 JPEG 2000 流是一种具有可伸缩性的嵌入式码流, 它能够在任意位置截断而不影响码流的正确解码。假设编码后数据包记为 $P_m(n,l)$, 其中 m,n,l 分别表示数据包所处的分辨率级别、编码块序号和质量层编号, 那么 JPEG 2000 流的特征可以表示为:

(1) 编码块之间的编解码是独立的。因而编码独立数据包集合 P_{ind} 可以表示为(10)式,

$$\begin{aligned}P_{\mathrm{ind}}=\{&P_1(1,0),\cdots,P_1(n,0),\cdots,P_1(N,0),\\&P_2(1,0),\cdots,P_2(n,0),\cdots,P_2(N,0),\\&\cdots\ \cdots,\\&P_m(1,0),\cdots,P_m(n,0),\cdots,P_m(N,0),\\&\cdots\ \cdots,\\&P_M(1,0),\cdots,P_M(n,0),\cdots,P_M(N,0)\}\end{aligned}\tag{10}$$

其中上述 JPEG 2000 编码流包含 M 个分辨率等级、一个基本质量层和 L 个增强质量层, 每个分辨率等级由 N 个编码块组成。

(2) 在一个编码块内, 每个数据包的编解码仅仅依赖于其前继数据包, 编码块内数据包的线性编解码依赖关系可表示成(11)式,

$$P_m(n,L)\mapsto_{\mathrm{c}}\cdots\mapsto_{\mathrm{c}}P_m(n,l)\mapsto_{\mathrm{c}}\cdots\mapsto_{\mathrm{c}}P_m(n,0) \quad (11)$$

其中$1\leqslant m\leqslant M$,$1\leqslant n\leqslant N$。

(3) 重要性差异。事实上, 不同的编码数据包 $P_m(n,l)$ 对重构图像质量的贡献值是存在差异的。例如, 基本层(Layer 0)的编码数据包 $\{P_m(n,0)\}$ 对提供重构图像的基本质量是必需的。根据离散小波变换(Discrete Wavelet Transform, DWT)的性质, 变换后图像的能量主要集中在频域的左上子带, 即

$$\Delta D_{P_u}^{(n_0,l_0)}>\Delta D_{P_v}^{(n_0,l_0)}(u<v) \quad (12)$$

其中 $\Delta D_{P_u}^{(n_0,l_0)}$ 表示数据包 $P_u(n_0,l_0)$ 的失真值。因此根据(12)式的分析, 需要对编码数据包采取不平等认证保护(UAP), 也即重要的数据包需得到更严格的认证保护。

4.2 签名生成算法

根据 AOM 模型, 构建 OAG 图可以通过规则 RI 和 RII 两种基本操作来完成。在发送方通过构造 OAG 图, 为整个图像码流生成数字签名。JPEG2000 编码流的最优认证图如图 1 所示, 码流包括 3 个分辨率等级、1 个基本质量层和 L 个增强质量层。OAG 图的构建过程主要分为 3 个步骤, 如下所示:

Step 1. 根据规则 RI 和(11)式, 对于每个编码块内的数据包 $\{P_m(n,l)\}_{l=0}^{L}$, 利用哈希链将数据包 $P_m(n,l+1)$ 链接到数据包 $P_m(n,l)$, 即生成从节点 $P_m(n,l+1)$ 到 $P_m(n,l)$ 的有向边。

Step 2. 提取数据包 $P_m(n,l)$ 的特征(指纹), 然后对整个码流的特征进行签名。数据指纹生成可以利用密码学哈希函数来实现, 例如 SHA-1 和 SHA-512。如图 1 所示, $h_i(i=1,\cdots,6)$ 是节点 P_i 的哈希值, h_{56} 是第 3 级分辨率中所有节点哈希值 $h_5,\cdots,h_6$ 串接后的哈希值, 即 $h_{56}=h_5\|\cdots\|h_6$。$h_1,h_2,\cdots,h_{3456}\in P_{\mathrm{sig}}$ 表示对节点集合 P_{sig} 的指纹做数字签名, 例如 RSA 算法。即生成从节点 $h_1,h_2,\cdots,h_{3456}$ 到 v_{sig} 的有向边。

Step 3. 根据规则 RII 和(10)式, 利用 FEC 编码器例如 IDA 算法, 对 L_0 层的数据包 $\{P_i\}$ 的认证信息进行编码, 即生成从 L_0 层含认证信息节点 $h_1,h_2,\cdots,h_{3456}$ 及签名节点 v_{sig} 到 FEC 编码节点 v_{FEC} 的有向边。

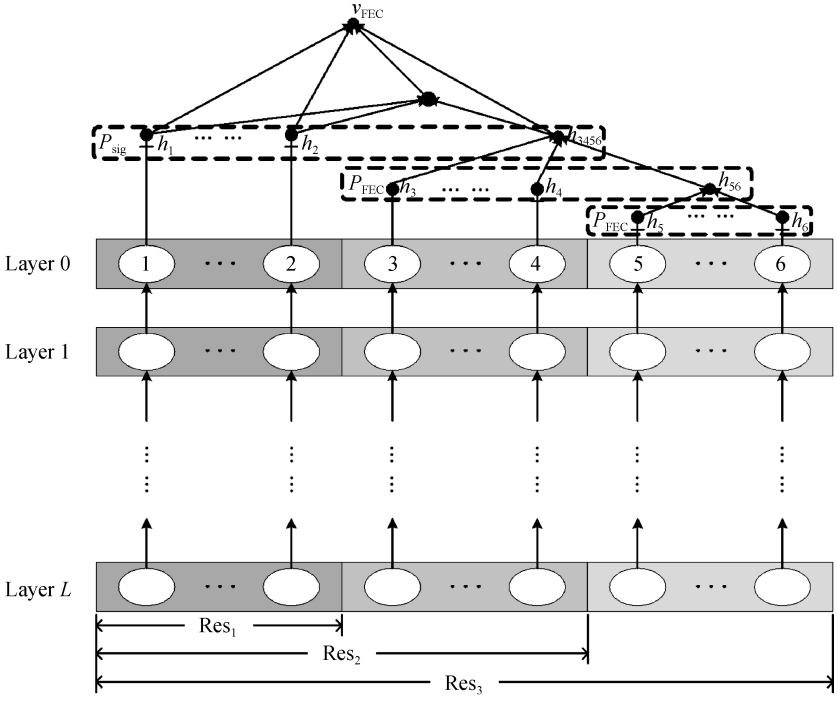

图 1 JPEG 2000 编码流的 OAG 图构造

Figure 1 OAG graph construction of JPEG 2000 encoded stream

为了获得更为灵活的数据包验证方式及支持多分辨率解码, 编码节点集合 P_{FEC} 按照空间分辨率形式进行组织, 例如图 1 的 JPEG 2000 编码流包含 3 个分辨率等级, 并且在不同分辨率等级的哈希值通过哈希树结构进行链接。

OAG 图的构造可以通过执行算法 1 来实现, 具体描述如下:

算法 1. OAG 图构造算法

输入: 发送方私钥 pri、FEC 编码参数有序集合 $\langle\theta_1,\cdots,\theta_M\rangle\left(\forall 1\leqslant i<j\leqslant M,\text{满足}\theta_i\leqslant\theta_j\right)$、码流包集合 $\left\{P_m(n,l)\right\}_{m=1,\cdots,M,n=1,\cdots,N}^{l=1,\cdots,L}(M>1,L>1)$

输出: 数据可信的传输包 $\left\{\hat{P}_m(n,l)\right\}$

/*构建线型哈希链*/

01: FOR $m=1,\cdots,M$, $n=1,\cdots,N$, $l=L,\cdots,1$

02: $P_m(n,l-1):=P_m(n,l-1)\|H\left(P_m(n,l)\right)$;

// $H(\bullet)$ 是密码学哈希函数, “||”表示串接操作。

/*生成数字签名*/

03: FOR $m=1,\cdots,M$, $n=1,\cdots,N$

04: $h_m(n):=H\left(P_m(n,0)\right)$;

05: FOR $n=1,\cdots,N$

06: $h_M\|=h_M(n)$;

//“||=”表示串接赋值操作。

07: $\tilde{h}_{M-1}:=H(h_M)$;

08: FOR $m=M-1,\cdots,2$

09: {

10: FOR $n=1,\cdots,N$

11: $h_m\|=h_m(n)$;

12: $h_m:=h_m\|\tilde{h}_m$;

13: $\tilde{h}_{m-1}:=H(h_m)$;

14: }

15: FOR $n=1,\cdots,N$

16: $P_{\text{sig}}\|=h_1(n)$;

17: $P_{\text{sig}}:=P_{\text{sig}}\|\tilde{h}_1$;

18: $S:=SIG_{pri}\left(H\left(P_{\text{sig}}\right)\right)$;

// $SIG_{pri}(\bullet)$ 是密码学数字签名函数。

//生成数字签名为 $\left(P_{\text{sig}},S\right)$。

/*编码认证信息*/

19: $F_1:=FEC\left(P_{\text{sig}}\|S,\theta_1\right)$;

// $FEC(\bullet)$ 是 FEC 编码函数。

20: FOR $m=2,\cdots,M$

21: $F_m:=FEC\left(h_m,\theta_m\right)$;

22: FOR $i=1,\cdots,M$

23: $\left\langle F_i^1,\cdots,F_i^k,\cdots,F_i^N\right\rangle:=PTN\left(F_i\right)$;

// $PTN(\bullet)$ 是均匀分割函数。

24: FOR $m=1,\cdots,M$, $k=1,\cdots,N$

25: $\hat{P}_m(k,0):=P_m(k,0)\|F_m^k$;

通过上述分析, 签名生成算法能够实现对编码数据包的非平等认证保护(UAP), 主要有在两个方面: 一方面, 对每条哈希链, 认证相关性与不同质量层的重要性一致, 这保证了重要度高的编码数据包具有更高的可验证概率。另一方面, 由于哈希树的非平衡性, 对高分辨率层级数据包的验证依赖于低分辨率层级的数据包。此外, 可以通过设置合适的 θ_m 值以提高第 m 个分辨率层级编码数据包的丢包鲁棒性。

4.3 可伸缩验证

上文提出的 JPEG2000 流认证算法具有很好的灵活验证性, 服务器仅需要对整个码流做一次签名, 但是支持在用户节点的多种码流验证方式, 码流可伸缩验证的特点可以归纳成如下几个方面:

(1) 由于哈希链的作用, 通过增加或减少验证码流的质量层数目, 可以实现可信图像质量与码率之间的动态平衡。

(2) 由于哈希树的作用, 可以按照分辨率层级对码流进行逐分辨率验证。

(3) 由于在 AOM 模型下, 编解码相关性被完整的保持, 因而认证算法能够支持码流的渐进传输。

上述 3 个编码流可伸缩验证的特性对异构网络中图像数据安全传输分发具有重要意义。对于服务器而言, 它仅需要对高质量图像做认证, 并且在存储服务器上保存认证图像的一份拷贝, 网络节点可以根据设备需求和网络状态对可信码流进行可伸缩验证, 包括图像质量、总码率和空间分辨率等多种码流验证模式。

5 跨层优化资源分配方法(CLORA)

为了解决 AOM 模型中 FEC 编码参数的选取问题, 以及不同重要度码流的非均衡差错保护(Unequal Error Protection, UEP)问题, 本文基于信源-信道联合编码(Joint Source-Channel Coding, JSCC)的思想提出了跨层优化资源分配(Cross-Layer Optimization Re-

source Allocation, CLORA)方法。

CLORA 方法实现最优的信源码率 R_s、认证码率 R_a 和信道码率 R_c 分配 (r_s^*, r_a^*, r_c^*), 其中 r_x^* 表示信源码率、认证码率或信道码率占总码率 R 的最优比重。下面基于上文提出的基于率失真的认证优化模型(AOM), 结合联合信源信道编码(JSCC)的思想, 给出 CLORA 算法及其求解方法。

在给定总码率 R 条件下, CLORA 优化算法的目的提供最优的信源码率 R_s、认证码率 R_a 和信道码率 R_c 分配 (r_s^*, r_a^*, r_c^*), 使得端到端可信图像质量失真值 D 最低, 即

$$(r_s^*, r_a^*, r_c^*) = \arg\min_{r_s, r_a, r_c} D \tag{13}$$

其中信源码率 R_s、认证码率 R_a 和信道码率 R_c 满足下述约束条件:

$$r_s + r_a + r_c = 1 \tag{14}$$

$$0 < r_s = \frac{R_s}{R} < 1 \tag{15}$$

$$0 < r_a = \frac{R_a}{R} < 1 \tag{16}$$

$$0 \leqslant r_c = \frac{R_c}{R} < 1 \tag{17}$$

由(14)—(17)式很容易得到, 总码率 R 包括信源码率 R_s、认证码率 R_a 和信道码率 R_c, 即可表示为

$$R = R_s + R_a + R_c \tag{18}$$

其中信源码率 R_s 计算公式见(3)式, 认证码率 R_a 计算公式见(4)式, 信道码率 R_c 与具体的编码算法有关。假设信道编码采用 RS(n,k) 码, 则信道码率 R_c 的计算式表示为(19)式,

$$R_c = \frac{n}{k}(R_s + R_a) \tag{19}$$

根据(5)式, 可信图像质量的端到端失真值 D 可以表示成(20)式,

$$D = D_0 - \sum_{P_m}[1 - p_{\text{loss}}(P_m, R_c)]\sigma(P_m)\tau_{G^*}(P_m, R_a)\Delta D_m(P_m, R_s) \tag{20}$$

其中, D_0 表示当所有可信编码数据包 P_m 都失效时的端到端失真值, $p_{\text{loss}}(P_m, R_c)$ 表示数据包 P_m 的丢失或无法信道纠错概率, 它与对 P_m 采取的信道编码强度有关。$\sigma(P_m)$ 表示数据包 P_m 的可解码概率, $\tau_{G^*}(P_m, R_a)$ 表示数据包 P_m 的可验证概率, 它与最优认证图 G^* 及对 P_m 采取的认证保护强度有关。$\Delta D_m(P_m, R_s)$ 表示信源解码数据包 P_m 时失真值的减少量, 它与 P_m 的信源码率有关。

(20)式中 $\sigma(P_m)$ 和 $\tau_{G^*}(P_m, R_a)$ 的计算见(7)式和(8)式, 根据上文定理 1 的结论, 在最优认证图(OAG) G^* 中所有可被解码的数据包都能被验证, 即

$$\begin{aligned} &\forall P_m \in V_{\text{pkt}}, \sigma(P_m) = 1 \\ &\Rightarrow \tau_{G^*}(P_m, R_a) = 1 \end{aligned} \tag{21}$$

为了求解上述 CLORA 优化模型, 可以通过简单的迭代搜索算法对 (r_s, r_a, r_c) 的解空间做搜索, 本文给出一种更高效的求解方法。通过对层次化组包后的信源编码流分析可以发现, 与选择的加密算法和认证算法无关, 信源码率 R_s 是固定的。这是因为对给定信源编码算法和图像数据源, 编码后的码率是一定的, 特别是采取无损数据压缩模式。

根据(15)—(18)式可以得到(22)式, 即

$$\begin{aligned} R &= R_s + R_a + R_c \\ &= R_s + \frac{r_a}{r_s}R_s + \frac{r_c}{r_s}R_s \\ &= R_s\left(1 + \frac{r_a + r_c}{r_s}\right) \end{aligned} \tag{22}$$

从(22)式中可得, 当 R_s 一定、 R_a 和 R_c 变化时, 总码率 R 满足(22)式,

$$R \propto \frac{r_a + r_c}{r_s} \tag{23}$$

在不同信道误码条件下, 通过搜索测试 R_a 和 R_c 变化时相应的失真值 D, 即获得 (r_s, r_a, r_c) 所对应的失真值 D。进而能够计算得到 $(r_a + r_c)/r_s$ 下对应的失真值 D, 再根据(23)式和率失真原理, 计算出斜率最小的点即为最优码率分配策略, 表示成(24)式,

$$(r_s^*, r_a^*, r_c^*) = \arg\min_{(r_s, r_a, r_c, D)} D \Big/ \frac{r_a + r_c}{r_s} \tag{24}$$

6 实验结果分析

仿真实验选取 3 幅 8 位灰度图像进行测试, 测试图像集如图 2 所示。首先通过简单地迭代搜索, 给出了跨层优化资源分配(CLORA)模型的可行解, 即最优的信源-认证-信道码率分配 (r_s^*, r_a^*, r_c^*)。然后, 分析比较了 5 种认证算法: 无认证、EMSS、SAIDA、本文算法、CLORA+本文算法, 在丢包鲁棒性和端到端率失真方面的性能, 验证了 CLORA+本文算法的有效性。实验假设信道仿真采用无记忆比特误码/包丢失模型, 图像质量度量采用峰值信噪比值(Peak Signal to Noise Ratio, PSNR), 计算方式如(25)式,

$$PSNR = 20\lg\left(\frac{2^b-1}{\sqrt{\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left\|\hat{I}_{ij}-I_{ij}\right\|^2}}\right)(\text{dB}) \qquad (25)$$

其中$\left(I_{ij}\right)_{m\times n}$,$\left(\hat{I}_{ij}\right)_{m\times n}$分别表示数字图像矩阵的原始像素值和重构像素值, b 表示图像像素的量化比特数。

(a) Elaine_512_512_8 (b) Barbara_1024_1024_8 (c) Airplane_512_512_8

图 2 测试图像集

Figure 2 Test image set

6.1 最优码率分配实验

在给定信源码率 R_s 下, 实验测试了不同误符号率(Symbol Error Rate, SER)条件下, 通过搜索认证码率 R_a 和信道码率 R_c, 得到了码率分配比率 (r_s,r_a,r_c) 与质量失真值 D 的关系, 其中认证码率 R_a 的迭代步长 θ 值设置为 0.05, 信道码率 R_c 的迭代步长设置为每次增加纠正 1 个符号, 即每次迭代(19)式中 k 值减小 2, 质量失真值 D 采用(25)式定义的重构图像的 *PSNR* 值来表示。根据上文(24)式得到, 最优的码率分配比率 (r_s^*,r_a^*,r_c^*) 可通过求 D 与 $(r_a+r_c)/r_s$ 比值的最小值获得。

图 3 分别给出了 3 幅测试图像的重构质量 $-D$ 与 $(r_a+r_c)/r_s$ 关系的散点图, 图 3 中横向轴表示 $(r_a+r_c)/r_s$ 比值, 纵向轴表示重构图像的 *PSNR* 值。图中红色框点是迭代搜索范围内斜率最大值点, 即为最优码率分配点。为了在获得近似最优解的同时控制搜索代价, 通过大量实验发现选取搜索步长的经验值为 0.01。从图 3 实验结果发现随着 $(r_a+r_c)/r_s$ 比值的增加 *PSNR* 值直到达到最大值, 并且在最优解附近散点密度较大, 相邻点的斜率很接近。这也表明搜索步长的精度选择合理, 依据此种搜索方式能获得近似最优解。

根据上述分析, 可以得到测试图像在不同 SER 条件下的最优码率分配 (r_s^*,r_a^*,r_c^*) 及对应的 *PSNR* 值, 实验结果如表 1—表 3 所示。

从表 1—表 3 的实验结果可以发现, 随着信道质量的下降, 为了保证可信的端到端质量不受到影响需要分配更高的信道码率比 r_c^*; 由于认证码率比 r_a^* 仅取决于 AG 图, 因而 r_a^* 值保持稳定, 并且从表中可以得到认证码率的比值较低为 5%—10%; 随着信源码率比 r_a^* 降低重构图像质量呈下降趋势。

表 1 不同 SER 下的最优码率分配(Elaine)

Table 1 Optimal rate allocation under different SERs (Elaine)

SER	0.005	0.01	0.015	0.02	0.025
r_s^*	0.89	0.87	0.85	0.83	0.81
r_a^*	0.06	0.06	0.05	0.05	0.05
r_c^*	0.05	0.07	0.10	0.12	0.14
PSNR (dB)	57.865	55.101	58.525	58.074	57.240

表 2 不同 SER 下的最优码率分配(Barbara)

Table 2 Optimal rate allocation under different SERs(Barbara)

SER	0.005	0.01	0.015	0.02	0.025
r_s^*	0.80	0.77	0.74	0.72	0.70
r_a^*	0.10	0.10	0.10	0.09	0.09
r_c^*	0.10	0.13	0.16	0.19	0.21
PSNR (dB)	59.456	57.345	59.172	58.640	58.175

表 3 不同 SER 下的最优码率分配(Airplane)

Table 3 Optimal rate allocation under different SERs(Airplane)

SER	0.005	0.01	0.015	0.02	0.025
r_s^*	0.88	0.86	0.84	0.81	0.80
r_a^*	0.05	0.05	0.05	0.05	0.05
r_c^*	0.07	0.09	0.11	0.14	0.15
PSNR (dB)	57.532	57.391	55.854	58.327	52.853

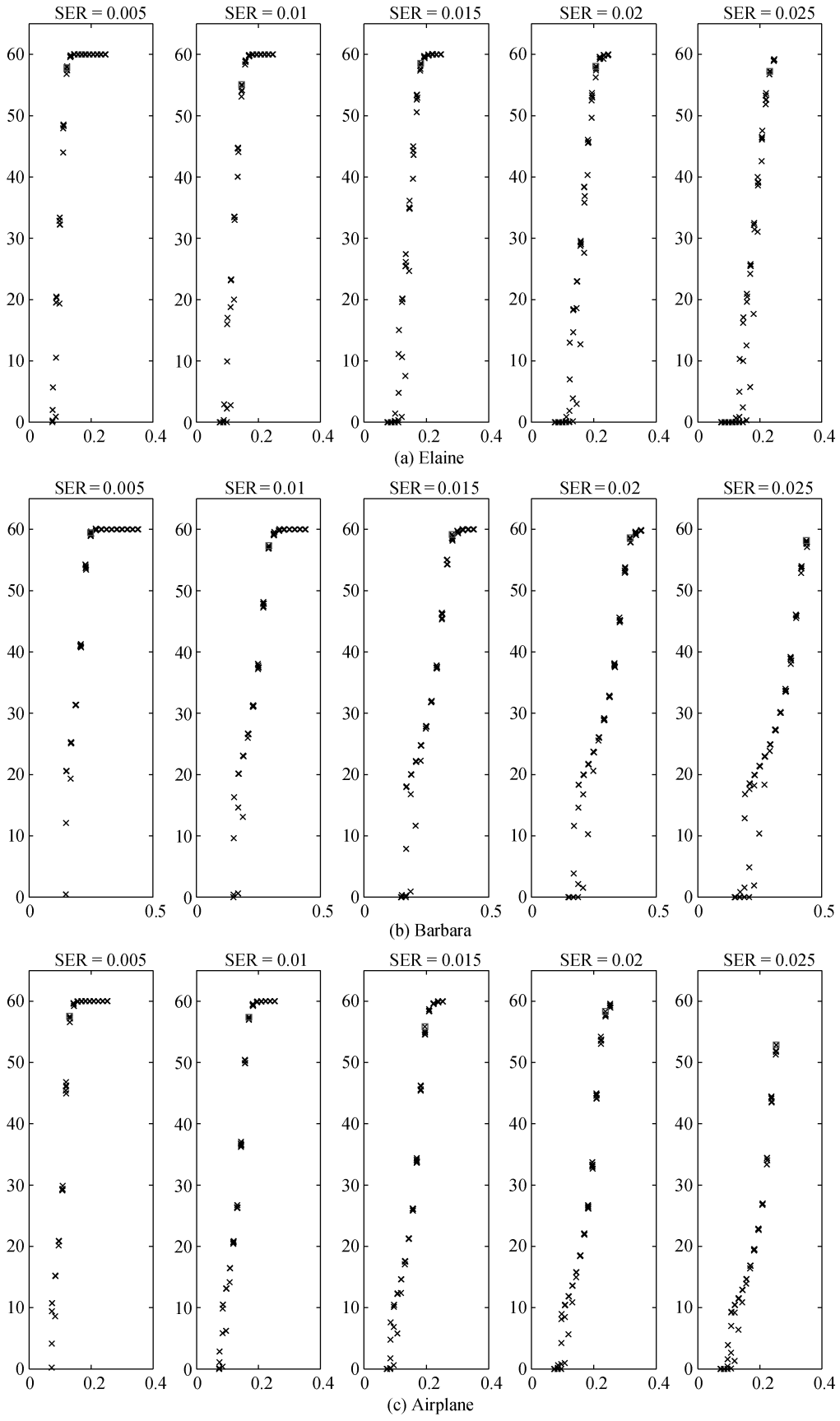

图 3　不同 SER 条件下失真值与码率分配关系散点图

Figure 3　Scatter plot of distortion value and code rate distribution under different SER conditions

6.2 丢包鲁棒性实验

本实验验证 CLORA 方法在不同丢包率信道下都能够达到最优的端到端重构图像质量, 仿真实验中设置SAIDA算法和本文算法的θ值为0.8, 可以抵抗足够坏的信道误码丢包。图 4 比较了在丢包率(Packet-Loss Rate, PLR)为 1%到 14%情况下 5 种算法的 *PSNR* 值。从图中可以发现, SAIDA 算法、本文算法及 CLORA+本文算法的端到端重构图像质量的 *PSNR* 值比 EMSS 算法的平均要高 0.8~3 dB, 并且它们都能够达到最优值(无认证时)。

经过分析可知, SAIDA 算法能够达到最优值是因为通过设置较大的θ值, 保证足够的认证冗余以抵抗信道误码丢包。本文算法能够达到最优值是因为上文提出的 AOM 模型能够保证所有接收到的可解码数据包都能被验证。CLORA 联合算法能够达到最优值是因为基于跨层优化资源分配的图像安全传输框架能够灵活地选择具体的安全算法。

6.3 端到端率失真性能实验

端到端率失真实验综合评估 CLORA 方法的端到端性能。仿真实验分别测试了丢包率 PLR 等于 1%和 5%条件下认证算法的端到端率失真性能, 实验结果如图 5 所示。从端到端率失真(Rate-Distortion, R-D)曲线图中可以发现, 当 PLR 等于 1%和 5%时都有, CLORA 联合算法和本文算法的端到端 R-D 性能比 EMSS 算法和 SAIDA 算法的性能要更好, *PSNR* 值平均提高了 1.6dB。此外, CLORA 联合算法的性能在本文算法性能基础上有提高。从图中还可以得到, CLORA+本文算法的端到端 R-D 曲线很接近理论上限值(无认证时 R-D 曲线), 尤其当信道条件变差时(丢包率增加), CLORA+本文算法的端到端性能几乎逼近理论上限值。

7 结论

针对图像认证的丢包鲁棒性问题, 本文首先提出一个通用的认证优化模型(AOM)。该模型以图像的端到端可信质量和认证代价为优化目标, 将认证优化问题转化成对最优认证图(OAG)的构造。AOM 模型适用于一般性的媒体流认证, 与具体的码流编码方式无关。然后本文通过利用图像码流的编解码相关性来降低搜索 OAG 图的计算复杂度, 并给出了构造 OAG 图的等价条件。在很低计算代价情况下, 结合哈希链和 FEC 码技术, 给出了构造 OAG 图的两个基本操作。最后为了解决 AOM 模型中 FEC 编码参数的选取问题, 以及不同重要度码流的非均衡差

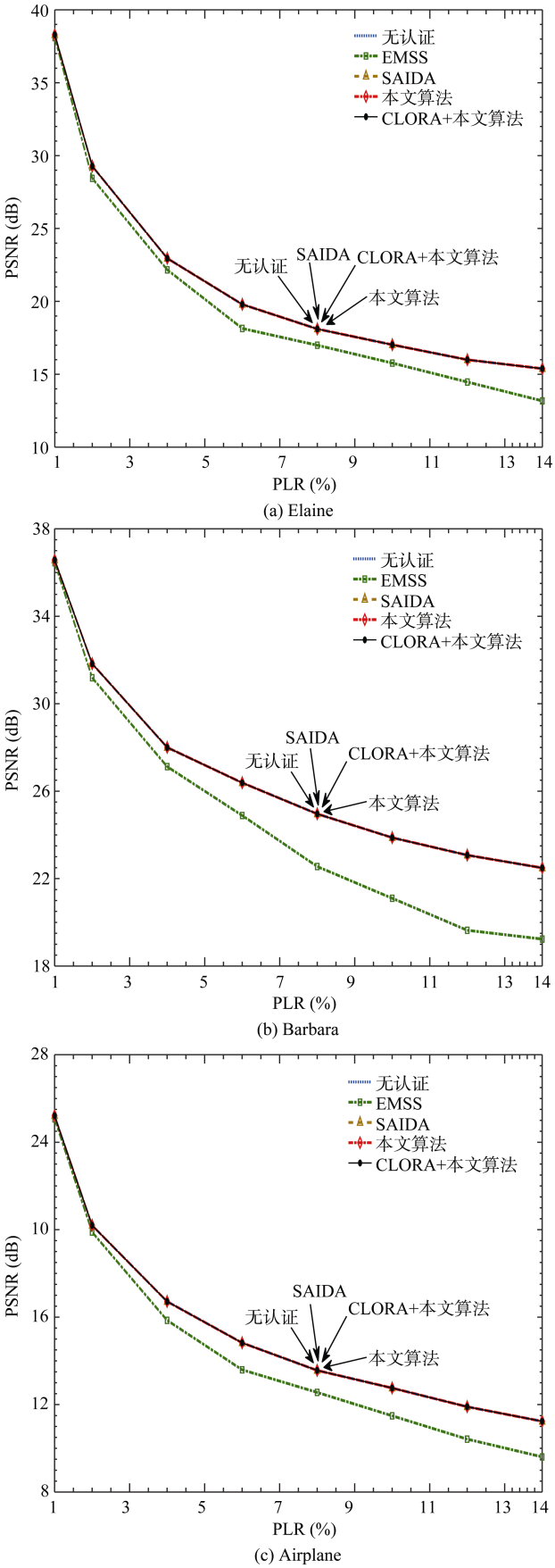

图 4 不同 PLR 下重构图像质量比较

Figure 4 Comparison of reconstructed image quality under different PLR

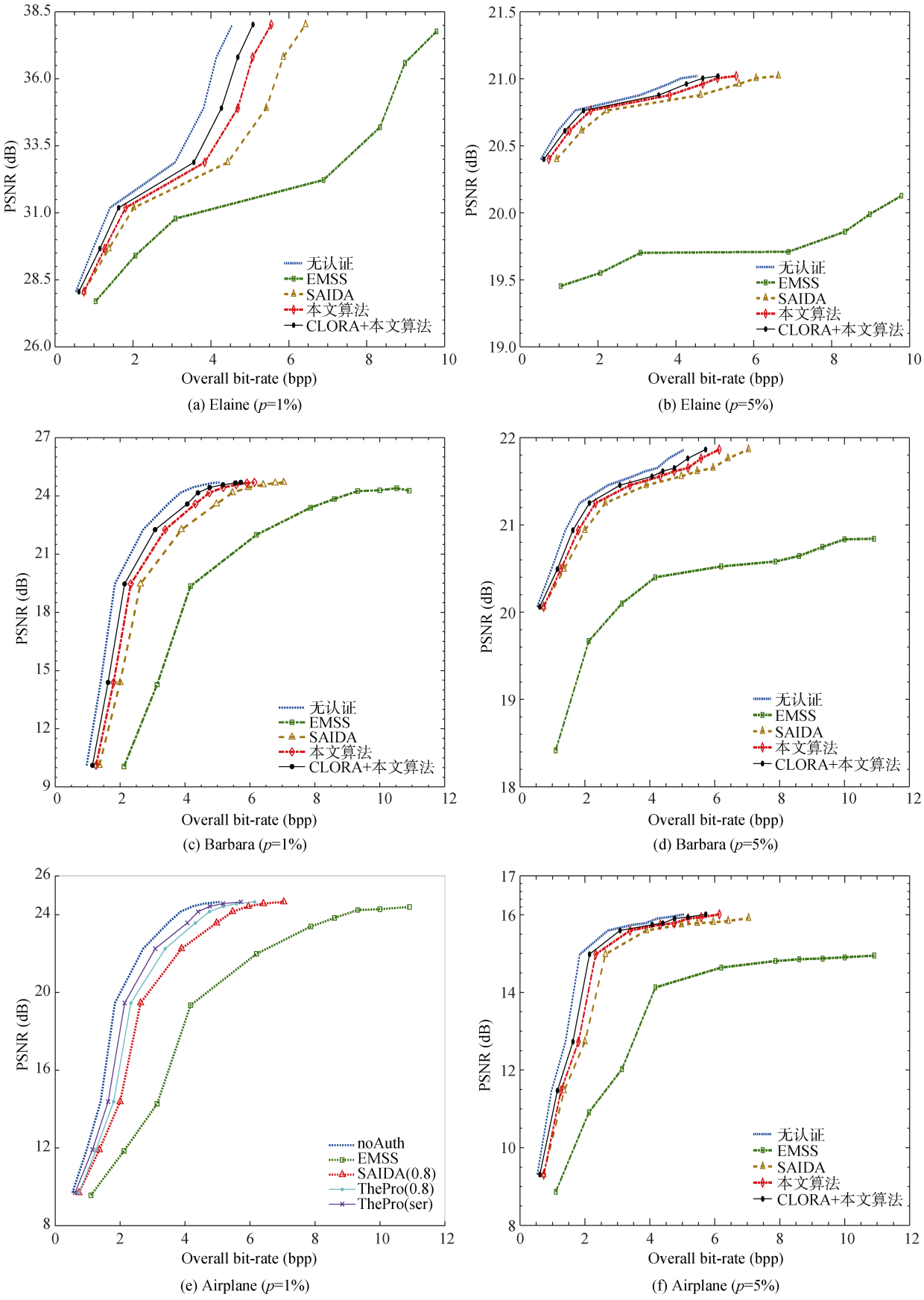

图 5　不同 PLR 下端到端 R-D 曲线比较

Figure 5　Comparison of end-to-end R-D curves under different PLRs

错保护(UEP)问题, 本文基于信源-信道联合编码(JSCC)的思想提出了跨层优化资源分配(CLORA)方法。仿真实验针对 JPEG 2000 图像流进行实现, 实验结果表明, 本文算法比 EMSS 算法和 SAIDA 算法在相同比特率下具有更强的丢包鲁棒性。在 CLORA 框架下, 本文算法的端到端可信质量比已有算法平均提高了 1.6dB, 逼近理论上限值。

下一步工作包括 AOM 模型和 CLORA 方法在视频流认证中的应用, 提升 CDN 网络环境下在线视频流安全分发的效能。

致　谢　本论文是“Joint FEC codes and hash chains for optimizing authentication of JPEG2000 image streaming”论文(发表于 IEEE ICME 2013, Regular Paper)的扩展与提高, 感谢审稿专家提供的宝贵修改意见及改进建议。

参考文献

[1] C. Qin, Z. C. Zhang, and C. Guo, “Perceptual robust image hashing scheme based on secret sharing,” *Journal of Computer Research and Development*, vol. 49, no. 8, pp. 1690-1698 (in Chinese), 2012.
(秦川, 张真诚, 郭成, “基于秘密共享的感知鲁棒图像 Hash 算法,” *计算机研究与发展*, 2012, 49(8): 1690-1698.)

[2] M. Hefeeda and K. Mokhtarian, “Authentication schemes for multimedia streams: quantitative analysis and comparison,” *ACM Trans. on Multimedia Computing, Communications and Applications*, vol. 6, no. 2, pp. 1–24, 2010.

[3] Q. Sun, J. Apostolopoulos, C. W. Chen, and S. F. Chang, “Quality-optimized and secure end-to-end authentication for media delivery,” *Proceedings of the IEEE*, vol. 96, no. 1, pp. 97–111, 2008.

[4] S. Lian, X. Chen, and J. Wang, “Content distribution and copyright authentication based on combined indexing and watermarking,” *Multimedia Tools and Applications*, vol. 57, no. 3, pp. 49–66, 2012.

[5] S. H. Han and C. H. Chu, “Content-based image authentication: current status, issues, and challenges,” *International Journal of Information Security*, vol. 9, no. 1, pp. 19–32, 2010.

[6] Haouzia and R. Noumeir, “Methods for image authentication: a survey,” *Multimedia Tools and Applications*, vol. 39, no. 1, pp. 1–46, 2008.

[7] Perrig, R. Canetti, J. D. Tygar, and D. Song, “Efficient authentication and signing of multicast streams over lossy channels,” in Proc. *IEEE Symposium on Security and Privacy* (S&P’00), pp. 56–73, 2000.

[8] J. M. Park, E. Chong, and H. J. Siegel, “Efficient multicast stream authentication using erasure codes,” *ACM Trans. on Information System Security*, vol. 6, no. 2, pp. 258–285, 2003.

[9] Z. Zhang, Q. Sun, and W. C. Wong, “An optimized content-aware authentication scheme for streaming JPEG-2000 images over lossy networks,” *IEEE Trans. on Multimedia*, vol. 9, no. 2, pp. 320-331, 2007.

[10] Z. Zhang, Q. Sun, and J. Apostolopoulos, “Generalized butterfly graph and its application to video stream authentication,” *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 19, no. 7, pp.: 965–977, 2009.

[11] K. Mokhtarian and M. Hefeeda, “Authentication of scalable video streams with low communication overhead,” *IEEE Trans. on Multimedia*, vol. 12, no. 11, pp. 730–742, 2010.

[12] L. Zhou, A. Vasilakos, and N. Xiong, “Scheduling security-critical multimedia applications in heterogeneous networks,” *Computer Communications*, vol. 34, no. 3, pp. 429–435, 2011.

[13] X. Zhu and C. W. Chen, “A joint layered scheme for reliable and secure mobile jpeg-2000 streaming,” *ACM Trans. on Multimedia Computing, Communications and Applications*, vol. 8, no. 8, pp. 1–23, 2012.

[14] X. Yi, Y. Fu, H. Ma, and C. Zheng, “Joint FEC codes and hash chains for optimizing authentication of JPEG2000 image streaming,” *in Proc. IEEE Int’l Conf. on Multimedia & Expo* (ICME’13), pp. 1–6, 2013.

[15] R. H. Deng, X. Ding, and S.-W. Lo, “Efficient authentication and access control of scalable multimedia streams over packet-lossy networks,” *Security Comm. Networks*, vol. 7, no. 3, pp. 611–625, 2014.

[16] X. Lv, Y. Mu, and H. Li, “Loss-tolerant authentication with digital signatures,” *Security Comm. Networks*, vol. 7, no. 11, pp. 2054–2062, 2014.

[17] X. Yi, G. Zheng, M. Li, H. Ma, and C. Zheng, “Efficient authentication of scalable media streams over wireless networks,” *Multimedia Tools and Applications*, vol. 71, no. 3, pp. 1913-1935, 2014.

[18] X. W. Yi, H. T. Ma, G. Zheng, and C.W. Zheng, “Packet-loss robust scalable authentication algorithm for compressed image streaming,” *Journal on Communications*, vol. 35, no. 4, pp. 174-181, 2014.
(易小伟, 马恒太, 郑刚, 郑昌文, “压缩图像码流的分组丢失顽健可伸缩认证算法,” *通信学报*, 2014, 35(4): 174-181.)

[19] W. Wang, D. Peng, and H. Wang, “A multimedia quality-driven network resource management architecture for wireless sensor networks with stream authentication,” *IEEE Trans. on Multimedia*, nol. 12, no. 5, pp. 439-447, 2010.

[20] W. Wang, H. Wang, and K. Hua, “Quality-optimized energy neutrality with link layer resource allocation for zero-power harvesting wireless communications,” *in Proc. IEEE Global Telecommunications Conference* (GLOBECOM’11), pp. 1-5, 2011.

[21] Z. Li, Q. Sun, and Y. Lian, “Joint source-channel-authentication resource allocation and unequal authenticity protection for multimedia over wireless networks,” *IEEE Trans. on Multimedia*, nol. 9, no. 4, pp. 837-850, 2007.

[22] L. Zhou, B. Zheng, and A. Wei, “A scalable information security technique: joint authentication-coding mechanism for multimedia over heterogeneous wireless networks,” *Wireless personal communications*, vol. 51, no. 1, pp. 5-16, 2009.

[23] X. Zhu and C. W. Chen, “A Joint Source-Channel Adaptive Scheme for Wireless H.264/AVC Video Authentication,” *IEEE Trans. on Information Forensics and Security*, vol. 11, no. 1, pp. 141-153, Jan. 2016.

易小伟 于 2014 年在中国科学院大学计算机应用技术专业获得博士学位。现任中国科学院信息工程研究所信息安全国家重点实验室助理研究员。研究领域为多媒体安全、网络信息安全对抗。研究兴趣包括: 音频隐写及隐写分析、语音取证、媒体内容挖掘与大数据分析。Email: yixiaowei@iie.ac.cn

赵险峰 于 2003 年在上海交通大学计算机系统结构专业获得博士学位, 现为中国科学院信息工程研究所信息安全国家重点实验室研究员、博士生导师。主要研究领域为信息保密与内容安全防护, 包括: 信息隐藏、隐蔽通信及其检测, 内容伪造取证, 数字水印与数字版权保护, 内容安全标识及其管控, 多媒体特定内容与目标识别, 对抗情况下的机器学习, 隐私保护等。Email: zhaoxianfeng@iie.ac.cn

郑昌文 于 2003 年在华中科技大学模式识别与智能系统专业获得博士学位。现任中国科学院软件研究所研究员。研究领域为综合信息系统, 研究兴趣包括综合信息系统总体与仿真、系统安全等。Email: changwen@iscas.ac.cn

马恒太 于 2001 年在中国科学院软件研究所计算机应用技术专业获得工学博士学位。现任中国科学院软件研究所副研究员。研究领域为信息安全。研究兴趣包括: 网络系统安全、软件安全与对抗。Email: hengtai@iscas.ac.cn

于海波 于 2006 年在吉林大学获得博士学位, 现任信息安全国家重点实验室正高级工程师、博士生导师, 研究领域为信息安全。研究兴趣主要包括信息对抗、网络与系统安全等。Email: yuhaibo@iie.ac.cn